الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة غرداية

كلية الحقوق والعلوم السياسية
قسم الحقوق

مخبر السياحة، الإقليم والمؤسسات

التحقيق الجنائي في الجرائم الماسة بالمستند الإلكتروني

أطروحة الدكتوراه الطور الثالث (ل م د)،
تخصص: القانون الجنائي الإداري

إعداد الطالبة:
بوشارب هانية

أمام لجنة المناقشة المتكونة من:

رقم	اللقب والاسم	الرتبة العلمية	مؤسسة الانتماء	الصفة
01	مولاي إبراهيم عبد الحكيم	أستاذ محاضر "أ"	جامعة غرداية	رئيسا
02	شول بن شهرة	أستاذ التعليم العالي	جامعة الطارف	مشرفا مقررا
03	بكرارشوش محمد	أستاذ التعليم العالي	جامعة ورقلة	ممتحنا
04	عمراوي مارية	أستاذ محاضر "أ"	جامعة الجلفة	ممتحنا
05	بن بادة عبد الحليم	أستاذ محاضر "أ"	جامعة غرداية	ممتحنا
06	جديد حنان	أستاذ محاضر "أ"	جامعة غرداية	ممتحنا

السنة الجامعية: 2025/2024

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة غرداية

كلية الحقوق والعلوم السياسية
قسم الحقوق

مخبر السياحة، الإقليم والمؤسسات

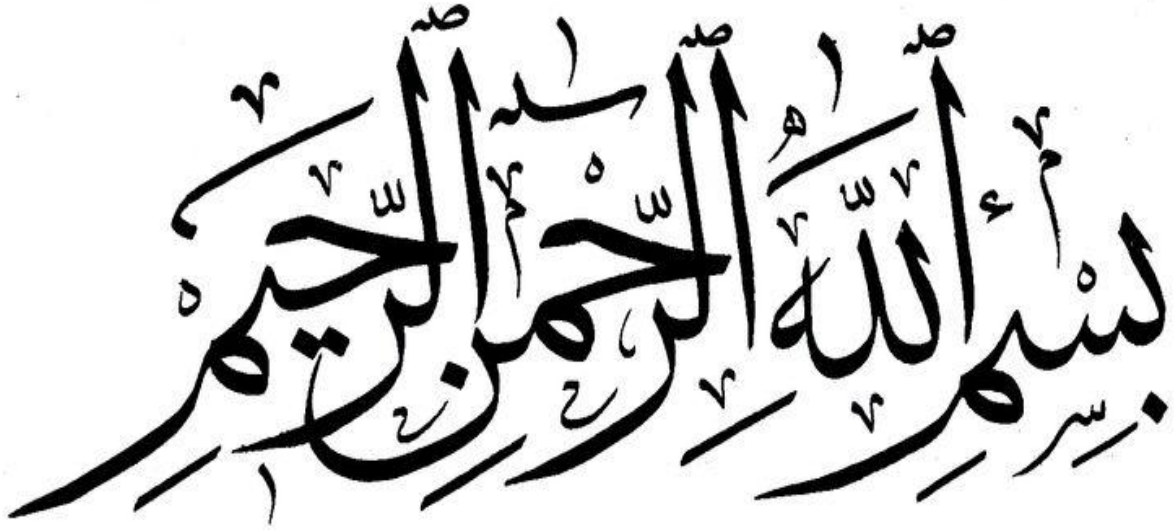
التحقيق الجنائي في الجرائم الماسة بالمستند الإلكتروني

أطروحة الدكتوراه الطور الثالث (ل م د)،
تخصص: القانون الجنائي الإداري

إعداد الطالبة:
بوشارب هانية

إشـراف الأستاذ الدكتور: شول بن شهرة
المشرفة المساعدة الدكتورة: مجدوب آمنة

السنة الجامعية: 2025/2024


بسم الله الرحمن الرحيم

الشكر والعرفان

الحمد لله تعالى، والحمدلله جل في علاه، حمدًا كثيرًا طيبًا مباركًا، ملء السماوات والأرض، على عظيم فضله وتوفيقه، فلولاه سبحانه وتعالى ما اكتملت هذه الدراسة، ولا تجاوزت ما اعترضني من عقبات وصعوبات، فهو وحده المستعان وبه التوفيق.

اللهم أجعل هذا العلم شفيعًا لي يوم تسألني عن شبابي فيما أفنيته، اللهم زدني علمًا نافعًا وبارك لي فيه، فالكمال لك وحدك، والصلاة والسلام على أشرف المرسلين محمد صلى الله عليه وسلم.

أرفع أسمى عبارات الشكر والعرفان إلى والديّ الغاليين فلولاهما بعد الله تعالى ما كنت لأصل إلى هذه المرحلة، فدعاؤهما ودعمهما غير المحدود كان النور الذي أنار دربي، والقوة التي إستندت إليها في كل مسيرتي التعليمية.

ومن دواعي العرفان والإمتنان أن أتقدم بجزيل الشكر وعظيم التقدير إلى الأستاذ الدكتور شول بن شهرة الذي شرفني بالإشراف على هذه الأطروحة، وخصني من وقته وجهده وتوجيهه بما لا يقدر بثمن فله مني كل الشكر والإمتنان، كما لا يفوتني أن أشكر الدكتورة مجدوب آمنة.

كما أتقدم بخالص الشكر والتقدير إلى أعضاء لجنة المناقشة الموقرين، لتكرمهم بقبول مناقشة هذه الأطروحة، ولكل ما قدموه من ملاحظات بناءة وتوجيهات قيمة أسهمت في إثرائها، فلهم مني كل الشكر والتقدير.

ولا يفوتني أن أعبر عن إمتناني إلى كل أساتذتي الأفاضل الذين كان لهم الفضل بعد الله تعالى في تعليمي وتوجيهي، فلن توفيهم كلمات الشكر حقهم لما كان لهم من أثر بالغ في مسيرتي التعليمية.

كما أخص بالشكر إلى كل من ساندني ووقف إلى جانبي طيلة مراحل دراستي، وإلى من كان لي عونًا وسندًا .

فجزاهم الله عني خير الجزاء، وجعل ما بذلوه في ميزان حسناتهم.

الإهداء

أهدي ثمرة جهدي المتواضع إلى:

سندي في هذه الحياة، إلى من أستمددت منه قوتي وعزيمتي، وغرس في نفسي حب المعرفة وشغف الإطلاع، وعلمني كيف أرتقي سلم الحياة بحكمة وصبر، برًا وإحسانًا ووفاءً له، إلى والدي الغالي الذي كان دعمه السند الحقيقي في كل خطوة.

نبع الحنان ونور دربي، إلى من علمتني الصبر في سبيل تحقيق ما أسعى إليه، وغرست في نفسي القوة والإصرار، وكانت لي عونًا في كل لحظات حياتي، إلى والدتي الحبيبة مصدر إلهامي وقوتي، فكانت نعم الرفيقة.

إخوتي الأعزاء الذين كانوا لي عونًا وسندًا، شجعوني ووقفوا بجانبي، فكان دعمهم سببًا في إستمراري وتقدمي.

أختي العزيزة التي كانت دائمًا بجانبي، دعمتني وشجعتني في كل الأوقات، فكانت نعم الرفيقة في درب العلم، ونعم العون في كل اللحظات.

كل أفراد عائلتي الذين شجعوني وساندوني.

قائمة المختصرات باللغة العربية:

ق.إ.ج.ج	قانون الإجراءات الجزائية الجزائري
ق.ع.ج	قانون العقوبات الجزائري
ق.م.ج	القانون المدني الجزائري
ق.إ.ج.م	قانون الإجراءات الجزائية المصري
ق.إ.ج.ف	قانون الإجراءات الجزائية الفرنسي
ق.ع.ف	قانون العقوبات الفرنسي
ج.ر.ج.ج.ش	الجريدة الرسمية الجمهورية الجزائرية الشعبية
ج.ر.ج.م.ع	الجريدة الرسمية جمهورية مصر العربية
د.ر.ط	دون ذكر رقم الطبعة
د.س.ن	دون ذكر سنة النشر
دج	الدينار الجزائري

قائمة المختصرات باللغة الفرنسية:

C.P.F	Code Pénale Français
C.P.P.F	Code de Procédure Pénale Français
C.C.F	Code civil Français

مقدمة

نتيجة للتطور التكنولوجي المتسارع انتشر إستخدام التقنيات الحديثة في مختلف مجالات الحياة، مما أضفى العديد من الجوانب الإيجابية على أنشطتنا اليومية، وقد ساهم هذا التحول في الإنتقال من المعاملات الورقية التقليدية إلى المعاملات الإلكترونية، وظهور مستند إلكتروني يتلاءم مع طبيعة البيئة الرقمية، وقد أتاح هذا المستند إمكانية إبرام العقود والمعاملات عن بعد بين أطراف لا يجمعهم تواصل مادي مباشر بل لقاء إفتراضي، الأمر الذي أفرز تحديات قانونية جديدة بإعتباره أحد أهم أدوات الإثبات في البيئة الرقمية.

إلا أن ذلك إنعكس أثره ولم يسلم المستند الإلكتروني من إمكانية التعرض لإعتداءات، مما أدى إلى ظهور نوع جديد ومستحدث من الجرائم يتمحور نشاطها في البيئة الرقمية، تكون المعطيات والمعلومات فيها عبارة عن نبضات إلكترونية غير مرئية، ما يجعلها تخلف أثرًا غير مادي، وتنفذ بأساليب تقنية متطورة لا تترك أدلة مادية تقليدية.

وقد ترتب على ذلك قصور وسائل الإثبات التقليدية عن مواكبة هذا النوع المستحدث من الجرائم، حيث لم تعد القواعد الإجرائية التقليدية كافية لضبطها أو إثباتها، وهو ما سمح في بعض الحالات بالإفلات من العقاب، نتيجة الفراغ القانوني في عدد من الجوانب التقنية المرتبطة بالجريمة الإلكترونية.

لذا أصبح من الضروري إيجاد وسائل حديثة تتلاءم مع طبيعة هذا الدليل الإلكتروني، بإعتباره الوسيلة الرئيسية لإثبات هذا النوع من الجرائم، رغم ما يطرحه من صعوبات أثناء عملية إستخلاصه ويعزى ذلك إلى طبيعته التقنية والرقمية المعقدة، وإرتباطه ببيئة رقمية غير ملموسة، ما إستوجب تدخل المشرع الجزائري إلى جانب التشريعات المقارنة، لوضع قواعد ومبادئ واضحة تكفل الحماية الجزائية للمراكز القانونية المهددة بهذه الجرائم.

أهمية الموضوع:

لما كان المستند الإلكتروني أحد سمات التطور التكنولوجي الحديث ومخرجات البيئة الرقمية، حيث ظهر كبديل أو رديف للمستند التقليدي في ظل تنامي وإزدياد الإعتماد على المعاملات الإلكترونية، فقد أصبح من الضروري وضع جملة من الضوابط القانونية والفنية لضمان أمن وخصوصية المستند الإلكتروني وسرية المعطيات والمعلومات التي يتضمنها، مما جعل الحاجة ملحة إلى سن تنظيم تشريعي لهذه الظاهرة المستحدثة، إلى إجراءات قانونية توثق المعاملات القانونية عبر الإنترنت، وذلك بهدف تحقيق عنصري الثقة والأمان في المعاملات الإلكترونية.

تكمن أهمية دراستنا في أن الجرائم الماسة بالمستند الإلكتروني تعد من بين الجرائم الأكثر صعوبة من حيث الإثبات الجنائي، وذلك نظرًا للطبيعة الخاصة التي تميزها عن باقي الجرائم التقليدية، فهذا النوع المستحدث من الجرائم يتطلب أدلة ذات طبيعة فنية وتقنية خاصة،

تختلف عما اعتدناه في الجرائم التقليدية، حيث لم يعد الدليل الجنائي التقليدي مناسبًا لطبيعة الوسط الرقمي الذي ترتكب فيه هذه الجرائم، ومن ثم برزت طائفة جديدة من الأدلة تعرف بالأدلة الجنائية الإلكترونية، وهي تتماشى مع طبيعة البيئة الرقمية والمعاملات الإلكترونية، وقد إنعكست خصائص هذه البيئة على طبيعة الدليل ذاته، مما منحه طابعًا متميزًا وجعله الوسيلة الأنجع لإثبات هذا النوع من الجرائم، لما يتمتع به من حجية قانونية تستند إلى مخرجات إلكترونية ليست في صورة مادية تقليدية وإنما بصفتها الإلكترونية المحضة.

وتكمن أهمية الموضوع في أن النصوص الجزائية التقليدية بشقيها الموضوعي والإجرائي أصبحت نسبيًا غير كافية لإثبات هذا النوع من الجرائم، الذي يتطلب وسائل تقنية تتلاءم مع طبيعته الفنية والعلمية الخاصة، فهي جرائم تتسم باللامادية من حيث الأثر والدليل، مما يجعل عملية إثباتها وتحديد هوية المساهمين فيها أمرًا بالغ الصعوبة، كما أن الوصول إلى الأثر المادي للجريمة والحصول على الدليل الإلكتروني الناتج عنها، يعد تحديًا حقيقيًا أمام السلطة القضائية في التصدي لهذا النوع من الجرائم، الأمر الذي استدعى تدخلات تشريعية سريعة عاجلة تهدف إلى مواكبة التحول الذي عرفته الظاهرة الإجرامية في ظل البيئة الرقمية.

أسباب إختيار الموضوع:

يعد إختيار موضوع البحث العلمي خطوة أساسية وهامة في الإنجاز، إذ تتوقف عليها باقي المراحل، وحتى لا ينطلق أي بحث من فراغ لابد من تحديد مبررات إختياره وتوضيح دوافع الباحث، ومنه الأسباب التي دفعتني لإختيار هذا الموضوع هي:

الأسباب الذاتية:

أدى التطور التكنولوجي والإستخدام الواسع لشبكة الإنترنت إلى ظهور أشكال جديدة ومستحدثة من الجرائم، أصبحت البيئة الرقمية مجالًا خصبًا لإرتكابها، وإتسمت هذه الجرائم بصعوبة ملاحقة مرتكبيها نتيجة لطبيعتها التقنية وتعقيداتها القانونية، كل ذلك شكل دافعًا شخصيًا للتعمق في فهم السياسة الجنائية بشقيها الموضوعي والإجرائي في مجال مكافحة الجرائم الماسة بالمستند الإلكتروني، وذلك خروجًا عن إطار الجرائم التقليدية المألوفة.

الأسباب الموضوعية:

يعتبر هذا الموضوع من المواضيع المستحدثة نظرًا لإرتباطه بتطور وسائل المعاملات الإلكترونية والإنتشار المتزايد لإستخدام شبكة الإنترنت في مختلف التعاملات، كما أن طبيعة هذه الجرائم وما تطرحه من إشكالات قانونية وتقنية مستجدة خاصة في ما يتعلق بالإثبات الإلكتروني، تجعل من معالجته ضرورة ملحة ضمن الإطار القانوني.

أهداف الدراسة:

تهدف هذه الدراسة إلى التعريف بالأدلة الإلكترونية وتبسيط مفاهيمها، سعيًا إلى جعل المعرفة التقنية في متناول الباحثين، بإعتبارها الوسيلة الأساسية لإثبات الجرائم الماسة بالمستند الإلكتروني، كما تتناول كيفية إستخلاص هذه الأدلة بطرق مشروعة ومدى قابليتها للمناقشة أثناء المحاكمة الجزائية.

ونظرًا لكون المستند الإلكتروني يعد دليلًا في القضايا الجزائية كونه أحد المخرجات الإلكترونية الذي قد يقود إلى إثبات وقائع الجرائم موضوع التحقيق الجنائي، كان من الضروري الرجوع إلى مصدره القانوني في القانون المدني الذي مهد لقبوله كوسيلة إثبات، بمنحه حجية قانونية عند استيفائه لشروط معينة تعزز الثقة فيه.

كما تسعى الدراسة إلى بيان موقف أنظمة الإثبات الجنائي من اعتماد بالمخرجات الإلكترونية كأدلة إثبات في المجال الجزائي، وذلك على ضوء آراء الفقه الجنائي وموقف التشريعات المقارنة فيما يتعلق بمدى قناعة القاضي الجزائي وحريته في الأخذ بهذا النوع من الأدلة في الجرائم الماسة بالمستندات الإلكترونية.

كما أن طبيعة الجرائم الماسة بالمستند الإلكتروني والتي قد تكون ذات طابع وطني أو إقليمي أو دولي، تضفي صعوبة كبيرة على تعقب الأدلة الإلكترونية وضبطها، إذ غالبًا ما تصطدم بمشكلة حدود الإختصاص القضائي، سواء من حيث تحديد القانون الواجب التطبيق، أو الدولة المختصة بملاحقة الجناة، لذلك تهدف دراستنا إلى بيان دور التعاون الدولي في التقريب بين القوانين الجنائية ولتسهيل الإجراءات الجزائية بين الدول والتغلب على عقبة السيادة.

كما نحاول تسليط الضوء على الأجهزة المختصة التي يمكن الإستعانة بها أثناء التحقيق الجنائي، لإستخلاص الدليل الإلكتروني من الجرائم الماسة بالمستندات الإلكترونية.

كذلك تتناول الدراسة الأحكام الجزائية الموضوعية والإجرائية التي أقرها المشرع الجزائري لمكافحة هذا النوع من الجرائم، ومحاولة الوقوف على النقائص والثغرات القانونية، واستعراض البدائل الممكنة من خلال مواقف الإتفاقيات الدولية ذات الصلة والتشريعات المقارنة، بغرض تقديم مقترحات تجعل من هذا البحث مرجعًا مفيدًا للباحثين في مجال العلوم القانونية، خاصة في ظل تطور المعاملات الإلكترونية وتزايد الإعتماد عليها يومًا بعد آخر.

نطاق الدراسة:

تتناول هذه الدراسة موضوع المستند الإلكتروني بإعتباره أحد المخرجات الإلكترونية، حيث لا يمكن التطرق إلى حجية المستند الإلكتروني في المجال الجزائي دون التأكد أولًا من صحة هذا المستند، ، بحيث إمتد نطاق الدراسة إلى التطرق إلى مفهوم المستند الإلكتروني مع التركيز على الكتابة والتوقيع الإلكترونيين بإعتبارهما عنصرين أساسيين في تكوينه، وتحليل

الشروط القانونية اللازمة للإعتراف بحجيتهما في الإثبات، وكل ذلك يتم من خلال تتبع تطور النصوص القانونية المنظمة للمستند الإلكتروني بما في ذلك النصوص الملغاة وصولًا إلى النصوص القانونية المعمول بها حاليًا، وذلك بهدف إبراز كيفية تطور الإطار القانوني لهذه المخرجات الإلكترونية على المستويين الوطني والدولي.

كما تتناول هذه الدراسة مفهوم الدليل الإلكتروني بإعتباره من الأدلة المستخلصة من البيئة الرقمية، كما إمتد نطاق الدراسة ليشمل التطرق إلى حجية المخرجات الإلكترونية بإعتبارها مستندات إلكترونية يمكن الإستناد إليها في الإثبات الجزائي، في ظل مختلف أنظمة الإثبات مع عرض مواقف الفقه والنصوص التشريعية الوطنية والمقارنة والإستئناس في بعض المواضع بالإجتهاد القضائي، بما يسمح بفهم أعمق لموقع هذه المخرجات ضمن الدليل الإلكتروني.

كما يشمل نطاق الدراسة التطرق إلى الجرائم الماسة بالمستند الإلكتروني، وذلك وفقًا لأحكام التشريع الجزائري مع الإستعانة بالتشريعات المقارنة بالإضافة إلى الإتفاقيات الدولية ذات الصلة، وقد تم في هذا السياق إبراز تطور النصوص القانونية في بعض التشريعات إلى غاية وضعها الحالي، مع الوقوف في حال غياب نصوص قانونية صريحة على مدى إمكانية تطبيق بعض الأحكام التقليدية على هذا النوع من الجرائم.

كما ينصب نطاق هذه الدراسة على التحقيق الجنائي في الجرائم الماسة بالمستند الإلكتروني، وقد تم التركيز على دراسة أحكام التشريع الجزائري ذات الصلة، كما تستعين الدراسة بالتشريعات المقارنة والإتفاقيات الدولية ذات الصلة، كما تتناول الدراسة أيضًا جوانب التعاون الدولي في مكافحة الجرائم الماسة بالمستند الإلكتروني، من خلال تسليط الضوء على الآليات القانونية لتفعيل التعاون القضائي والأمني، فضلًا عن إستعراض الأجهزة المختصة التي يمكن الإستعانة بها لإستخلاص الأدلة الإلكترونية.

الدراسات السابقة:

أبرز الدراسات السابقة التي إطلعت على محتواها، فالبعض منها جاءت مختصة في جزئية لها علاقة بالمستند الإلكتروني، وبعض من الدراسات ذات العلاقة المباشرة بموضوع دراستنا الراهنة، وتلك الدراسات هي:

- بن شهرة شول، **الحماية الجنائية للتجارة الإلكترونية**، أطروحة الدكتوراه علوم تخصص: قانون جنائي، بجامعة محمد خيضر-بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، السنة الجامعية 2009-2010، تعلقت إشكالية بحثه في كيف يمكن كفالة حماية جنائية فعالة لمبادلات التجارة الإلكترونية؟، وللإجابة على الإشكالية المطروحة تطرق الباحث إلى دراسة الحماية الجنائية الموضوعية للتجارة الإلكترونية في الباب الأول، بحيث تطرق إلى الإطار التنظيمي

للتجارة الإلكترونية في الفصل الأول، أما الفصل الثاني فقد خصصه إلى الإعتداء على نظام عمل التجارة الإلكترونية، وإلى جرائم الإعتداء على مضمون نشاط التجارة الإلكترونية في الفصل الثالث، أما الباب الثاني فقد خصصه إلى الحماية الجنائية الإجرائية للتجارة الإلكترونية، بحيث تطرق فيه إلى جوانب الإجرائية لجرائم التجارة الإلكترونية في الفصل الأول، وعالج إجرئي التفتيش والضبط وإشكالات أخرى في بيئة التجارة الإلكترونية في الفصل الثاني، أما الفصل الثالث فقد خصصه إلى الحماية الإجرائية في ضوء الإتفاقيات الدولية.

تمثل نقطة التقاطع مع دراستنا فيما يتعلق بتعريف التوقيع الإلكتروني وبيان شروطه وصوره، بالإضافة إلى التطرق إلى الجرائم الماسة به، بحيث تطرقت الدراسة السابقة إلى تعريف التوقيع الإلكتروني على مستوى التشريع الجزائري بموجب التعديل الذي أجراه على القانون المدني بموجب القانون رقم: 05-10 المؤرخ في 20 جوان 2005، غير أن دراستنا إنفردت بتقديم مختلف التعريفات التي أقرها المشرع الجزائري للتوقيع الإلكتروني بدءًا من التعديل الذي أجراه على القانون المدني بموجب القانون رقم: 05-10 السالف الذكر وصولًا إلى التعريف الوارد في القانون رقم: 15-04 المؤرخ في 01 فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

تناولت الدراسة السابقة مسألة حجية التوقيع الإلكتروني من خلال التطرق لأحكام التوجيه الأوروبي رقم: 1999-93 المتعلق بشأن إرساء إطار قانوني مشترك لإستخدام التوقيع الإلكتروني الصادر بتاريخ 13 ديسمبر1999، وأيضًا وفقًا لقانون التجارة الإلكترونية المصري، في حين استندت دراستنا إلى قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وكذا التعديل الذي أجراه المشرع الجزائري على القانون المدني بموجب القانون رقم: 05-10 السالف الذكر الذي إعترف فيه بحجية التوقيع الإلكتروني وأقر بإمكانية الإعتداد به، رابطًا ذلك بتوفر نفس الشروط المتطلبة في الكتابة الإلكترونية كوسيلة إثبات، كما تم التطرق أيضًا إلى القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين الذي حدد بشكل صريح الشروط الواجب توافرها لصحة التوقيع الإلكتروني حتى يكتسي وصف الموصوف والإعتداد به في الإثبات.

كما تطرقت دراستنا إلى أحكام اللائحة رقم: 910-2014 المؤرخة في 23 جويلية 2014 الصادرة عن البرلمان الأوروبي والمجلس الأوروبي المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية، التي ألغت جميع الأحكام السابقة الواردة في التوجيه الأوروبي رقم: 1999-93 المتعلق بشأن إرساء إطار قانوني مشترك لإستخدام التوقيع الإلكتروني الصادر بتاريخ 13 ديسمبر1999، في حين إقتصرت الدراسة السابقة على تحليل التوجيه، في حين إعتمدت دراستنا على كل من التوجيه

واللائحة الذي ألغته، مما أتاح تقديم تصور أدق لتطور الإطار القانوني الأوروبي للتوقيع الإلكتروني.

كما أشارت دراستنا إلى بعض التعديلات التي طرأت على القانون المدني الفرنسي، لاسيما تلك المتعلقة بالكتابة الإلكترونية والتوقيع الإلكتروني، والتي نص عليها الأمر رقم: 2016-131 المؤرخ في 10 فيفري 2016 المتعلق بإصلاح قانون العقود والنظام العام وإثبات الإلتزامات.

وتتمثل نقطة التقاطع بين الدراستين في التطرق إلى الجرائم الماسة بنظم المعالجة الآلية للمعطيات، وجريمة السرقة المعلوماتية، بالإضافة إلى جريمة تزوير المستندات الإلكترونية.

ركزت الدراسة السابقة على الجرائم الماسة بنظم المعالجة الآلية للمعطيات بشكل عام لاسيما تلك التي تنسحب آثارها على مواقع التجارة الإلكترونية، فإن دراستنا إتخذت منحى أكثر تخصيصًا حيث إنصب التركيز على الجرائم الماسة بنظم المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني.

وتناولت دراستنا تطور النصوص القانونية المتعلقة بالجرائم الماسة بنظم المعالجة الآلية للمعطيات في التشريع الفرنسي، بدءًا من القانون رقم: 88-19 بشأن الغش المعلوماتي الذي شمل المواد من 462-2 حتى 462-4، ثم إلى القانون رقم: 1336 لسنة 1992 والذي بدأ به في الأول من مارس سنة 1994 بتضمينه أحكامًا جديدة لمواجهة ظاهرة الإجرام المعلوماتي، وكان من شأن هذا التعديل إضافة فصل ثالث ضمن الباب الثاني من القسم الثالث من قانون العقوبات، تحت عنوان: "الإعتداءات على نظم المعالجة الآلية للمعلومات" ويتكون من المواد 323-1 إلى 323-4، ثم من خلال تدخل المشرع الفرنسي سنة 2004 بتعديل بعض نصوص قانون العقوبات الفرنسي الجديد الصادر سنة 1994 فيما يتعلق بالمواد من 323-1 إلى 323-3 وذلك بتشديد العقوبة، ثم تم الإنتقال مباشرة إلى الوضع القانوني الحالي بصيغته المعدلة بوضعه الحالي.

كما أشارت دراستنا إلى العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، وفقًا لأحدث التعديلات بموجب القانون رقم: 24-06 المؤرخ في 28 أفريل 2024 المعدل والمتمم للأمر رقم: 66-156 المتضمن قانون العقوبات.

ركزت الدراسة السابقة على الجرائم الماسة بالتوقيع الإلكتروني وفقًا لما ورد في قانون التجارة الإلكترونية المصري، في حين تناولت دراستنا هذه الجرائم في ضوء ما نص عليه القانون الجزائري رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، كما تناولت في بعض الجزئيات أحكامًا واردة في قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

كما تناولت الدراسة السابقة جريمة تزوير المستندات الإلكترونية وجريمة إستعمال المستند الإلكتروني المزور من خلال التطرق إلى أحكام قانون العقوبات الجزائري وإلى مختلف التشريعات المقارنة، والإستدلال في بعض الجزئيات بموقف القضاء، ونظرًا لغياب تعريف صريح للتزوير في التشريع الجزائري آنذاك إضطرت الدراسة السابقة إلى عرض مختلف التعريفات الواردة في التشريعات المقارنة، أما دراستنا فقد إعتمدت على القانون رقم: 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير وإستعمال المزور الذي ألغى أحكام السابقة المتعلقة بهذه الجرائم المنصوص عليها في قانون العقوبات والتي كانت محل المعالجة في الدراسة السابقة، وقد تطرقت دراستنا وفقًا لهذا القانون إلى تعريف التزوير، بالإضافة إلى أحكام العقاب سواء من حيث العقوبات الأصلية أو التكميلية، فضلًا عن أحكام العقاب على الشروع والتحريض والمشاركة في إرتكاب هذه الجرائم.

كما تتمثل أيضًا نقطة تقاطع بين الدراسة السابقة ودراستنا في تناول خصائص الدليل الإلكتروني وحجيته في مجال الإثبات الجزائي، بالإضافة إلى الإجراءات المعتمدة لإستخلاص هذا الدليل، والإختصاص القضائي، وآليات التعاون والمساعدة القضائية الدولية، وتسليم المجرمين.

بلحسيني حمزة، **الحماية الجزائية للمستند الإلكتروني**، أطروحة الدكتوراه علوم تخصص: علوم قانونية، بجامعة الجيلالي اليابس، كلية الحقوق والعلوم السياسية، قسم الحقوق، السنة الجامعية 2019-2020، تعلقت إشكالية بحثه في ما مدى كفاية الآليات القانونية المقررة لحماية المستند الإلكتروني من الناحية الجزائية؟، وللإجابة على الإشكالية المطروحة تطرق الباحث إلى دراسة النظام القانوني للمستند الإلكتروني في الباب الأول بحيث تطرق فيه إلى الضوابط القانونية للمستند الإلكتروني، وإلى الضوابط الفنية لحماية المستند الإلكتروني، أما الباب الثاني فقد خصصه إلى الأحكام التنظيمية والإجرائية للمستند الإلكتروني من الناحية الجزائية، بحيث تطرق فيه إلى جرائم الإعتداء على المستند الإلكتروني سواء كانت هذه الأفعال ماسة بالمستند أو بالتوقيع الإلكتروني، وورد بعنوان الأحكام التنظيمية للمستند الإلكتروني من الناحية الجزائية وعالج فيه الأحكام الإجرائية للمستند الإلكتروني من الناحية الجزائية بين التنظيمين الداخلي والدولي.

تتمثل نقطة التقاطع مع دراستنا فيما يتعلق بتعريف المستند الإلكتروني والكتابة الإلكترونية، إضافة إلى تعريف التوقيع الإلكتروني مع بيان أبرز صوره وتطبيقاته، بالإضافة إلى التطرق إلى تعريف جهات التصديق الإلكتروني التي تناط بها مهمة التحقق من صحة التوقيع الإلكتروني ونسبته لصاحبه ومنحه القوة الثبوتية، عن طريق شهادة التصديق الإلكتروني، كما تم الإشارة إلى السلطات المكلفة بمتابعة ومراقبة نشاط هذه الجهات.

أضافت دراستنا تعريفًا الذي أورده المشرع الجزائري بموجب القانون رقم: 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير وإستعمال المزور، حيث إستخدم مصطلح محرر للدلالة على "المستند"، ووسع نطاق هذا التعريف ليشمل كلا من المحرر الورقي والمحرر الإلكتروني.

وتناولت دراستنا معالجة شاملة لتعريف التوقيع الإلكتروني على مستوى التشريع الجزائري، حيث تم التطرق إلى تطور النصوص القانونية ذات الصلة بدءًا من التعديل الذي أجراه على القانون المدني بموجب القانون رقم: 05-10 السالف الذكر، وصولًا إلى التعريف الوارد في القانون رقم: 15-04 المؤرخ في 01 فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

ميزت دراستنا بين نوعين من الجهات المكلفة بالتصديق الإلكتروني، الجهة الأولى تتمثل في الطرف الثالث الموثوق الذي يكون شخصًا معنويًا، يتولى مهمة منح شهادات التصديق الإلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي، أما الجهة الثانية التي كانت محل إهتمام الدراسة السابقة فتتمثل في مؤدي خدمات التصديق الإلكتروني والذي يكون شخصًا طبيعيًا أو معنويًا، وتتمثل مهمته في منح شهادات التصديق الإلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني لفائدة الجمهور، وقد أضافت دراستنا بيان الشروط الواجب توافرها فيه، وكذا شروط مزاولة نشاطه وفقًا لما نص عليه القانون رقم: 15-04 المؤرخ في 01 فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

كما تطرقت دراستنا إلى أحكام اللائحة رقم: 910-2014 المؤرخة في 23 جويلية 2014 الصادرة عن البرلمان الأوروبي والمجلس الأوروبي المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية، التي ألغت جميع الأحكام السابقة الواردة في التوجيه الأوروبي رقم: 1999-93 المتعلق بشأن إرساء إطار قانوني مشترك لإستخدام التوقيع الإلكتروني الصادر بتاريخ 13 ديسمبر1999، في حين إقتصرت الدراسة السابقة على تحليل التوجيه، في حين إعتمدت دراستنا على كل من التوجيه واللائحة الذي ألغته.

تطرقت الدراسة السابقة وكذا دراستنا إلى المرسوم رقم: 2001-272 المؤرخ في 30 مارس 2001 الصادر لتطبيق أحكام المادة 1316-4 من القانون المدني والمتعلق بالتوقيع الإلكتروني، في حين أشارت دراستنا أيضًا إلى المرسوم رقم: 2017-1416 المؤرخ بتاريخ 28 سبتمبر 2017 المتعلق بالتوقيع الإلكتروني الذي ألغى المرسوم السابق، وأحال تطبيق الأحكام المتعلقة بالتوقيع الإلكتروني والآلية الموصوفة لإنشاء التوقيع الإلكتروني وشهادة التوقيع الإلكتروني الموصوفة إلى أحكام اللائحة رقم: 910-2014 المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية.

كما تتمثل أيضًا نقطة تقاطع بين الدراسة السابقة ودراستنا في تناول الشروط اللازمة لإكتساب المستند الإلكتروني حجية في الإثبات وإعتباره دليلًا معتمدًا في مجال الإثبات المدني، أما فيما يتعلق بالإثبات الجزائي فقد تطرقت كل من الدراسة السابقة ودراستنا إلى مختلف أنظمة الإثبات بغرض الوقوف على مدى سلطة القاضي في تقدير الأدلة، وذلك من خلال دراسة حجية المستند الإلكتروني ضمن النظام الإثبات الحر والنظام المقيد ونظام المختلط.

أشارت الدراسة السابقة إلى خلو التشريع المصري من نصوص صريحة التي تنظم حجية المخرجات الإلكترونية بما في ذلك المستندات الإلكترونية في مجال الإثبات الجزائي، إلا أنها بينت أنه وعلى رغم من هذا الغياب، يمكن الإستناد إلى الدليل الإلكتروني وكذا المخرجات الكمبيوترية في إثبات أو نفي الجريمة، وتكون لها قوة القرائن في الإثبات، إستنادًا إلى ما تقرره المادة 303 من قانون الإجراءات الجزائية المصري، بإعتبار أن المشرع المصري يأخذ بمبدأ الإثبات الحر، أما دراستنا فقد بينت أن المشرع المصري قد تدارك الأمر وأقر صراحة بحجية المخرجات الإلكترونية بموجب المادة 15 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، الذي نص صراحة على أن للكتابة الإلكترونية وللمحررات الإلكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية، متى إستوفت الشروط المنصوص عليها في هذا القانون، ووفقًا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون، وأيضًا من خلال التطرق إلى القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات الذي عرف الدليل الإلكتروني في المادة الأولى منه وإستخدم مصطلح الدليل الرقمي للدلالة عليه، وأحال إلى اللائحة التنفيذية لتحديد الشروط الفنية الواجب توفرها لكي يكون للدليل الإلكتروني ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائي.

كما أضافت دراستنا أن إدراج عبارة "بما فيها الالكترونية" من طرف المشرع الجزائري في الفقرة الأولى من المادة 349 من القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية، يعد تأكيدًا صريحًا على شمول الأدلة الإلكترونية ضمن وسائل الإثبات، وذلك بعد أن كانت غير منصوص عليها صراحة في الفقرة الأولى من المادة 212 من الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية الجزائري الملغى، مما كان يقتضي إخضاعها آنذاك للقواعد العامة في الإثبات.

تطرقت كل من الدراسة السابقة ودراستنا إلى تناول أهم الجرائم الماسة بالمستند الإلكتروني، على وجه الخصوص جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور، والجرائم الماسة بنظم المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني، وكذا جريمة سرقة المستند الإلكتروني، بالإضافة إلى الجرائم الماسة بالتوقيع والتصديق الإلكترونيين.

تناولت الدراسة السابقة جريمتي تزوير المستند الإلكتروني وإستعمال المستند الإلكتروني المزور وذلك من خلال التطرق إلى أحكام قانون العقوبات الجزائري، حيث أشارت إلى أن جريمة التزوير تنصب في الأصل على المستندات الورقية فقط، دون أن يتوسع المشرع في مفهوم المستند ليشمل المستندات المعلوماتية ضمن المستندات محل جريمة التزوير، كما لاحظت الدراسة غياب تعريف صريح لجريمة التزوير ضمن أحكام قانون العقوبات.

أما دراستنا فقد جاءت على ضوء القانون رقم: 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير وإستعمال المزور الذي ألغى جميع الأحكام السابقة المتعلقة بهذه الجرائم المنصوص عليها في قانون العقوبات والتي كانت محل المعالجة في الدراسة السابقة، وقد تطرق هذا القانون إلى تعريف التزوير، وقام بالتوسيع من مفهوم المستند ليشمل المستندات الإلكترونية ضمن المستندات محل جريمة التزوير، وبإضافة أحكام جديدة في سبيل مواجهة هذه السلوكيات الإجرامية والتصدي لها، وتناولت دراستنا أحكام العقاب سواء من حيث العقوبات الأصلية أو التكميلية، فضلًا عن أحكام الشروع والتحريض والمشاركة في إرتكاب هذه الجرائم بموجب هذا القانون.

كما تتمثل أيضًا نقطة تقاطع بين الدراسة السابقة ودراستنا في تناول إجراءات إستخلاص الدليل الالكتروني، وآليات التعاون الدولي والمساعدة القضائية الدولية المتبادلة، وكذا تسليم المجرمين في مكافحة الجرائم الماسة بالمستند الالكتروني.

أشارت الدراسة السابقة في بعض الجزئيات وفقًا للأمر رقم: 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية الملغى، فإن دراستنا تناولت تلك المسائل ذاتها في ضوء القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية الذي ألغى الأمر السابق.

صعوبات البحث:

تتمثل الصعوبات التي يطرحها موضوع الدراسة في طابعه التقني والإجرائي، إذ لا يكفي إمتلاك خلفية قانونية لمعالجة الموضوع، بل يتطلب الأمر إلمامًا كافيًا بالجوانب التقنية بالأنظمة المعلوماتية، وهو ما يجعل الموضوع يستدعي نهجًا قانونيًا دقيقًا يراعي التداخل بين الفهم القانوني والمعرفة التقنية.

وتتمثل أبرز الصعوبات التي واجهناها في إنجاز هذا البحث أبرزها تناثر المعلومات وتوزعها بين مراجع مختلفة، وتناثر النصوص القانونية في مكافحة الجرائم الماسة بالمستند الإلكتروني في العديد من القوانين مما تطلب جهدًا مضاعفًا في جمعها وتحليلها، فضلًا عن عدم وجود قانون مستقل في الجزائر يضبط كافة الجوانب المتعلقة بحماية المعاملات الإلكترونية بصفة عامة والمستندات الإلكترونية بصفة خاصة من الناحية الجزائية، ناهيك عن عدم إمكانية

حصر القوانين المنظمة لهذا الموضوع لإرتباطه بفروع متعددة، إلى جانب المعاهدات والإتفاقيات وكذا القوانين النموذجية المنظمة للمعاملات الإلكترونية بصفة عامة والإجرام المعلوماتي بصفة خاصة، وهو ما يتطلب وضع إطار عام حاكم لمكافحة هذه الجرائم بشكل متكامل لتحقيق مواجهة فاعلة لها.

الإشكالية:

بناء على سبق ذكره نطرح الإشكالية التالية: **ما مدى كفاية وفعالية الآليات القانونية التي أقرها المشرع الجزائري للتحقيق الجنائي في الجرائم الماسة بالمستند الإلكتروني؟**

يتفرع عن إشكالية الدراسة عدة تساؤلات فرعية:

- **ما هي الطبيعة القانونية والتكوينية للدليل الإلكتروني المستمد من الجريمة الماسة بالمستند الإلكتروني؟**
- **ما مدى قناعة القاضي الجزائي بحجية المخرجات الإلكترونية في الإثبات الجنائي؟**
- **ما مدى ملاءمة النصوص القانونية الإجرائية التي أقرها المشرع الجزائري في مكافحة الجرائم الماسة بالمستند الإلكتروني ؟**

المنهج المتبع:

ارتأينا أن تكون دراستنا وفق المنهج الوصفي، كالتطرق إلى تعريف طبيعة الدليل الإلكتروني والخصائص التي تميزه عن غيره من الأدلة المادية وإلى أهم تقسيماته، بالإضافة إلى المنهج التحليلي الذي نسعى من خلاله إلى تحليل مختلف النصوص القانونية المتعلقة بالموضوع، وبآراء الفقه وأحكام القضاء وموقف الإتفاقيات الدولية، بالإضافة إلى المنهج الإستدلالي كالتطرق إلى حجية المستند الإلكتروني في المواد المدنية من خلال التركيز على حجية الكتابة الإلكترونية والتوقيع الإلكتروني بهدف تعزيز القوة الثبوتية للمستندات الإلكترونية، وكما يتم التوصل إلى إستنتاج بشأن مدى تطابق أركان بعض الجرائم المنصوص عليها في القواعد القانونية التقليدية مع بعض الجرائم المرتكبة على المستند الإلكتروني، لاسيما تلك الأفعال المشابهة لتلك التي تشكل أركان تلك الجرائم، من خلال إستنتاج مدى تطابق أركان جريمة سرقة معطيات المستند الإلكتروني مع أركان جريمة السرقة التقليدية، إلى جانب الإستعانة بالمنهج المقارن في بعض الجزئيات وذلك قصد تسليط الضوء على موقف هذه التشريعات وتدارك الإختلاف الموجود بينها، ومنه محاولة تسليط الضوء على الفراغ التشريعي الموجود عندنا وكذا الثغرات القانونية.

خطة الدراسة:

للإجابة على الإشكالية المطروحة إرتأينا تقسيم دراستنا إلى بابين، سنتطرق إلى الأحكام الموضوعية للجرائم الماسة بالمستند الإلكتروني وقواعد الإثبات الخاصة بها في الباب الأول،

والذي سوف نتطرق فيه إلى مدى إقتناع القاضي الجزائي بالدليل الإلكتروني المستمد من الجرائم في المستند الإلكتروني في (الفصل الأول)، الذي سوف نتطرق فيه إلى خصوصية الدليل الإلكتروني المستخلص من الجرائم الماسة بالمستند الإلكتروني في (المبحث الأول)، بينما سنتطرق إلى سلطة القاضي الجزائي في قبول و تقدير المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني في (المبحث الثاني)، أما (الفصل الثاني) فقد خصصناه إلى الجرائم الماسة بالمستند الإلكتروني، بحيث سنتطرق إلى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني في (المبحث الأول)، بينما إلى الجرائم الماسة بمحتوى المستند الإلكتروني في (المبحث الثاني)، وإلى الجرائم الماسة بالتوقيع والتصديق الإلكترونيين في (المبحث الثالث)، أما الباب الثاني فقد خصصناه للأحكام الإجرائية لمكافحة الجرائم الماسة بالمستند الإلكتروني، بحيث سنتطرق فيه إلى آليات مكافحة الجرائم الماسة بالمستند الإلكتروني في (الفصل الأول)، الذي سوف نتطرق فيه إلى الآليات الوطنية لمكافحة الجرائم الماسة بالمستند الإلكتروني في (المبحث الأول)، بينما سنتطرق إلى آليات التعاون الدولي لمكافحة الجرائم الماسة بالمستند الإلكتروني في (المبحث الثاني)، أما (الفصل الثاني) فقد خصصناه إلى إجراءات إستخلاص الدليل الإلكتروني في الجرائم الماسة بالمستند الإلكتروني، بحيث سنتطرق إلى الإجراءات التقليدية والتقنية لإستخلاص الدليل الإلكتروني في (المبحث الأول)، بينما إلى الإجراءات المستحدثة لإستخلاص الدليل الإلكتروني في (المبحث الثاني).

الباب الأول:

الأحكام الموضوعية للجرائم الماسة بالمستند الإلكتروني وقواعد الإثبات الخاصة بها

تمهيد:

مع تزايد إبرام المعاملات الإلكترونية وتزايد إستخدام شبكة الإنترنت، ظهرت أساليب وطرق جديدة لإرتكاب الجريمة مما أدى إلى تفشي أنواع جديدة من الجرائم والتي تسمى بالجرائم الماسة بالمستند الإلكتروني، ونظرًا للطبيعة الخاصة الذي تتميز به هذه الجرائم أصبحت مسألة إثباتها تشكل تحديًا كبيرًا، الأمر الذي إستلزم ضرورة إيجاد وسائل حديثة وجديدة تختلف عن الطرق التقليدية، مما دفع العديد من الدول إلى شرعنة الأخذ بالأدلة الجنائية الإلكترونية -الرقمية- ضمن منظومتها القانونية في عملية الإثبات الجنائي، بإعتبارها الوسيلة الفعالة والوحيدة في كثير من الأحيان لإثبات هذا النوع من الجرائم، وقد تطلب هذا التحول تطوير التشريعات العقابية بما يتناسب مع طبيعة هذه الجرائم، وضرورة إبتكار آليات جزائية جديدة قادرة على مواكبة التطور التقني والفني والتكنولوجي المتسارع في هذا المجال.

إرتأينا تقسيم الباب الأول إلى فصلين، نتطرق إلى مدى إقتناع القاضي الجزائي بالدليل الإلكتروني المستمد من الجرائم في المستند الإلكتروني في (الفصل الأول)، الذي سوف نتطرق إلى خصوصية الدليل الإلكتروني المستخلص من الجرائم الماسة بالمستند الإلكتروني في (المبحث الأول)، بينما سنتطرق إلى سلطة القاضي الجزائي في قبول و تقدير المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني في (المبحث الثاني)، أما (الفصل الثاني) فقد خصصناه إلى الجرائم الماسة بالمستند الإلكتروني، بحيث سنتطرق إلى الجرائم الماسة بنظم المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني في (المبحث الأول)، بينما إلى الجرائم الماسة بمحتوى المستند الإلكتروني في (المبحث الثاني)، وإلى الجرائم الماسة بالتوقيع والتصديق الإلكترونيين في (المبحث الثالث).

الفصل الأول:

مدى إقتناع القاضي الجزائي بالدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الإلكتروني

تمهيد:

تتمثل أهمية الأدلة الجزائية في كونها الأداة الأساسية التي يعتمد عليها القاضي الجزائي لكشف الحقيقة في الدعوى المعروضة أمامه، فدور القاضي لا يقتصر على مجرد الموازنة بين الأدلة التي يقدمها الخصوم بل يتجاوز ذلك إلى دور إيجابي يفرض عليه التحري عن الحقيقة والبحث عنها، ومن جهة أخرى فقد خول له حرية في تقدير قيمة كل دليل يعرض عليه، وله كذلك التنسيق بين الأدلة المعروضة عليه وإستخلاص نتيجة منطقية من هذه الأدلة مجتمعة سواء أكانت بالإدانة أو بالبراءة.

غير أن الأدلة المادية التقليدية لم تعد كافية لمواكبة التطورات التكنولوجية المتسارعة، وذلك بالنظر إلى الخصائص الفريدة التي تتميز بها الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، مما شكل ذلك عائقًا أمام السلطة القضائية في مواجهة هذه الجرائم والتصدي لها، ونتيجة لذلك أدى إلى صعوبة تكوين الإقتناع الشخصي للقاضي الجزائي.

الأمر الذي دفع العديد من الفقهاء ورجال القانون إلى البحث عن وسائل إثبات جديدة تتماشى مع طبيعة هذه الجرائم وتختلف عن تلك المعتمدة في الجرائم التقليدية، ويعتبر الدليل الإلكتروني أبرز هذه الوسائل إذ يعتبر أداة إثبات ضرورية وأساسية في هذا السياق لما له دور حاسم في مساعدة القاضي الجزائي على تكوين قناعته الشخصية حتى يتسنى له الفصل في القضية المعروضة عليه.

إرتأينا تقسيم دراستنا إلى مبحثين، نتطرق إلى خصوصية الدليل الإلكتروني المستخلص من الجرائم الماسة بالمستند الإلكتروني في (المبحث الأول)، أما (المبحث الثاني) فقد خصصناه إلى سلطة القاضي الجزائي في قبول و تقدير المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني.

المبحث الأول: خصوصية الدليل الإلكتروني المستخلص من الجرائم الماسة بالمستند الإلكتروني

مع تزايد إبرام المعاملات الإلكترونية أصبحت هذه الأخيرة عرضة لإنتهاكات مجرمي المعلوماتية الذين إستغلوا البيئة الرقمية لتنفيذ جرائمهم، ونظرًا لأن الدليل الإلكتروني -الرقمي- ينشأ من ذات الوسط الذي ترتكب فيه هذه الجرائم، فإنه يكتسب أهمية بالغة سواء في إثبات وقوع الجريمة ونسبتها إلى مرتكبها أو نفيها عنه.

أضفت البيئة الرقمية التي ينشأ فيها الدليل الإلكتروني عليه العديد من الخصائص والمميزات مما منحه طابعًا خاصًا يميزه عن الأدلة الجنائية التقليدية، هذا الطابع الفريد جعله الأفضل لإثبات الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، ونظرًا لأهميته في هذا السياق لا يمكن الخوض في دراسة هذا الموضوع دون التطرق إلى مفهوم الدليل الإلكتروني في عملية الإثبات في (المطلب الأول)، وإلى الدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الإلكتروني في (المطلب الثاني).

المطلب الأول: مفهوم الدليل الإلكتروني في عملية الإثبات

تعددت التعريفات المتعلقة بالدليل الإلكتروني وإختلفت من حيث نطاقها بين من يذهب إلى التوسيع في مفهومه ومن يذهب إلى التضييق، ويرجع هذا التباين إلى التخصص العلمي الذي ينتمي إليه هذا الدليل[1] وإلى درجة الإهتمام الذي يحظى به سواء على المستوى الدولي أم على صعيد الفقه الجنائي والتشريعات الوطنية (الفرع الأول)، والبيئة الرقمية التي ينشأ فيها الدليل الإلكتروني أكسبته خصائص فريدة نظرًا لكونه يتكون من مجموعة من المعطيات الإلكترونية، الأمر الذي منحه طبيعة خاصة تميزه عن الأدلة التقليدية الأخرى وتجعله يحتل مكانة مميزة كدليل جنائي في مواجهة الجرائم الماسة بالمستند الالكتروني (الفرع الثاني)، ونظرًا للتطور المستمر الذي تشهده البيئة الرقمية التي ينشأ في إطارها الدليل الإلكتروني جعلته من الأدلة المتنوعة والمستحدثة القابلة للتطور والتكيف مع مظاهر رقمية جديدة قد تظهر مع مرور الوقت، وهو ما دفع الفقه القانوني والتشريعات إلى السعي لتصنيفه وتقسيمه بما يتلاءم مع طبيعته المتغيرة والمتجددة (الفرع الثالث).

الفرع الأول: تعريف الدليل الإلكتروني

إرتأينا التمهيد لهذا الموضوع من خلال إستعراض التعريف الدولي للدليل الإلكتروني، يليه بيان أهم التعاريف الفقهية ذات الصلة، ثم التعريف التشريعي لهذا الدليل.

[1]- بلهادي حميد، **حجية الدليل الرقمي في الإثبات الجنائي**، كلية الحقوق والعلوم السياسية، جامعة بليدة 2 لونيسي علي، مجلة البحوث والدراسات القانونية والسياسية، المجلد التاسع، العدد الأول، 2019، الجزائر، ص16.

أولًا: التعريف الدولي للدليل الإلكتروني

عرفته المنظمة العالمية لدليل الكمبيوتر (IOCE) International Organization of- Computer Evidence في مارس سنة 2000 بأنه: "المعلومات المخزنة أو المنقولة والتي يمكن الإعتماد عليها أمام المحكمة"، وعرفته في أكتوبر سنة 2001 بأنه: "المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية".[1]

ويؤخذ على هذين التعريفين تجاهل التعريف الأول الصيغة التي يتم بها تخزين المعلومات على الرغم من تحديده للجهة التي سيقدم لها الدليل وخصصها بالمحكمة فقط، في حين حدد التعريف الثاني الصيغة الرقمية أو الإلكترونية التي تم تخزين المعلومات بها وتجاهل الجهة التي سيقدم إليها الدليل الإلكتروني.[2]

والتعريف الذي أخذ به التقرير الأمريكي المقدم إلى ندوة الأنتربول العلمية حول الدليل الإلكتروني سنة 2001 أعتبر الدليل الإلكتروني بأنه: "عبارة عن معطيات يمكن إعدادها وتراسلها وتخزينها رقميًا، بحيث تمكن الحاسوب من تأدية مهام ما".[3]

ثانيًا: التعريف الفقهي للدليل الإلكتروني

ومن بين أبرز التعاريف التي صاغها الفقه القانوني للدليل الإلكتروني على أنه: "الدليل المتواجد في البيئة الرقمية ويؤدي إلى إكتشاف ملابسات الجريمة، فهو ذلك الجزء المؤسس على الإستعانة بالتقنية والذي يؤدي إلى إقناع القاضي الجزائي بالإدانة، فكلما كان هناك مزج في موضوع الدليل الفكرة أو المعلومة أو الصور بالتقنية فإنه يعد دليلًا رقميًا"[4]، إلا أن هذا الإعتقاد في غير محله ذلك أن الدليل الإلكتروني لا يقتصر دوره في إثبات الجرائم المعلوماتية فحسب التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، وإنما يمتد إلى الجرائم المادية التي قد تستخدم فيها التكنولوجيا الرقمية الحديثة.

كما عرف بأنه: "تلك المعلومات التي يقبلها العقل والمنطق ويعتمدها العلم، ويتم الحصول عليها بإجراءات علمية وقانونية، وذلك بترجمة المعلومات والبيانات الحسابية المخزنة في

[1]- رفاه خضير جياد العارضي، **الدليل الإلكتروني وآثره في مجال نظرية الإثبات الجنائي دراسة مقارنة**، الطبعة الأولى، 2019، منشورات زين الحقوقية، بيروت-لبنان، ص 49.

[2]- أحمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم04/09**، رسالة الماجستير، تخصص: قانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2012-2013، ص 69.

[3]- محمد صالح جاد المولى خليفة، **الدليل الرقمي وحجيته في إثبات جرائم المعلومات دراسة مقارنة**، أطروحة الدكتوراة، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، 2018، ص 34.

[4]- رفاه خضير جياد العارضي، مرجع سابق، ص48.

الحاسوب وملحقاته وشبكات الإتصال، ويمكن إستخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة ما".[1]

كما عرف كذلك بأنه: "الدليل المأخوذ من أجهزة الحاسوب يكون في شكل مجالات أو في شكل نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها بإستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي المكون الرقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور والأصوات والأشكال والرسوم، وذلك من أجل إعتماده أمام أجهزة إنفاذ وتطبيق القانون".[2]

يلاحظ على هذا التعريف بأنه يخلط بين الدليل الإلكتروني ومسألة إستخلاصه، حيث عرف بأنه: "الدليل المأخوذ من أجهزة الحاسوب"، وهذا يعني أن هذا الدليل لا تثبت له هذه الصفة إلا إذا تم أخذه أو إستخلاصه من مصدره[3]، وبمفهوم المخالفة فإن تلك المعطيات التي لازالت لم يتم فصلها عن الحاسوب وهي في شكل مجالات أو نبضات مغناطيسية أو كهربائية لا تصلح لأن توصف بالدليل الإلكتروني وهذا إتجاه غير صحيح.[4]

كما عرف أيضًا بأنه: "كل المعطيات التي يمكن إعدادها أو تخزينها في هيئة رقمية، بحيث تمكن الحاسوب من إنجاز مهمة ما"[5]، إن هذا التعريف فقد خلط بين برامج[6] الحاسوب التي تعد ذات دور فعال في إدارة الحاسب وتشغيله، وبين الدليل الإلكتروني بوصفه دليلًا مستقلًا قائمًا بذاته[7].

ويكمن الفرق بين برامج الحاسوب والدليل الإلكتروني في الوظيفة التي يؤديها كل واحد منهما، فالبرامج لها دور فعال في تشغيل الحاسوب وتوجيهه إلى وضع الخطط المناسبة وحل المشاكل، وبدونها لا يعدو أن يكون مجرد آلة صماء كباقي الآلات، بل إنه توجد بعض من البرامج الخاصة التي تساهم في إستخلاص الدليل الإلكتروني مثل: برنامج معالجة الملفات (X-tree Pro Gold)، وبرنامج النسخ مثل (Lap Link)[8]، فالبرنامج له دور في القيام بمختلف

---

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، المؤسسة الحديثة للكتاب، الطبعة الأولى، 2022، لبنان، ص 758.

[2]- رفاه خضير جياد العارضي، مرجع سابق، ص48.

[3]- نفس المرجع، ص51.

[4]- سعيداني نعيم، مرجع سابق، ص 761.

[5]- عائشة بن قارة مصطفى، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، د.ر.ط، د.س.ن، دار الجامعة الجديدة، الإسكندرية-مصر، ص 53.

[6]- البرنامج المعلوماتي له دور في القيام بمختلف العمليات التي يحتويها الجهاز الإلكتروني، ذلك أن هذا البرنامج لا يقوم بعمله إلا عن طريق مجموعة من البرامج التي يتم إعدادها وتنص بيها مسبقًا، فتسمح هذه البرامج بالقيام بمختلف العمليات الإلكترونية عند إعطاء أوامر بذلك، وللمزيد من التفصيل، ينظر: رفاه خضير جياد العارضي، مرجع سابق، ص 50.

[7]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 35.

[8]- عائشة بن قارة مصطفى، مرجع سابق، ص 57.

العمليات التي تحتويها المنظومة المعلوماتية بواسطة مجموعة من الأوامر[1]، أما الدليل الإلكتروني له دور أساسي وأهمية كبرى في معرفة كيفية حدوث الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، بهدف إثباتها ونسبتها إلى مقترفيها لاسيما في البيئة الرقمية[2].

مما سبق نستخلص أن أغلب التعريفات حصرت مصادر الدليل الإلكتروني على ما يتم إستخراجه فقط من الحاسوب وملحقاته دون غيره من الأجهزة الرقمية الأخرى المتطورة التي لا تقل أهمية عنه ولا شك أن في ذلك تضييق لدائرة الدليل الإلكتروني، كالهواتف الذكية النقالة والتبلات وآلات التصوير الرقمي والبطاقات الذكية والتسجيلات الرقمية الصوتية، أو نظم التراسل كخوادم شبكة الإنترنت والتي تضم الكثير من المعطيات الشخصية كمعرفة المواقع الإلكترونية التي سبق زيارتها وغرف الدردشة التي تم الدخول إليها والرسائل الإلكترونية المرسلة والمستقبلة، أو من الأجهزة الملحقة بالحاسوب أو أي وسيط إلكتروني يحمل المعطيات الإلكترونية، وغيرها من الوسائل الإلكترونية الحديثة التي باتت تعتمد التقنية الرقمية في تشغيلها.[3]

ثالثًا: التعريف التشريعي للدليل الإلكتروني

لم يتطرق المشرع الجزائري إلى تعريف الدليل الإلكتروني[4]، ولذلك سنورد التعريف الذي تبناه المشرع المصري بموجب المادة الأولى من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات[5] مستخدمًا مصطلح الدليل الرقمي للدلالة عليه، وعرفه على النحو الآتي: " أي معلومات إلكترونية[6] لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها بإستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة".

يلاحظ أن المشرع المصري قد حرص عند تعريفه للدليل الإلكتروني على إبراز جوهر الدليل وهي المعلومات المستخرجة من الأجهزة الإلكترونية سواء أكانت أجهزة الحاسوب أم

[1]- سعيداني نعيم، مرجع سابق، ص-ص 759-760.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 58.

[3]- رفاه خضير جياد العارضي، مرجع سابق، ص-ص 50-51.

[4]- تم ترجيح إستعمال مصطلح "الإلكتروني" عوضًا عن "الرقمي" بإعتباره المصطلح المعتمد من طرف المشرع الجزائري، كما هو وارد في عدد من النصوص القانونية من بينها: التصديق الإلكتروني، التوقيع الإلكتروني، الكتابة في شكل الإلكتروني، وغيرها من المصطلحات ذات الصلة.

[5]- القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج)، الصادرة في 14 أوت سنة 2018.

[6]- عرفت المادة الأولى من القانون رقم: 175 لسنة 2018 السالف الذكر البيانات والمعلومات الإلكترونية كالآتي: "كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات وما في حكمها".

شبكات المعلومات وما في حكمها، وجاءت الصياغة موسعة بما تسمح إجرائيًا بالتوسع فيما يمكن إعتباره دليلًا رقميًا -إلكترونيًا-، ولم يتضمن التعريف الوارد في القانون سوى ضابطين يتعلقان بالمعلومات التي يتم جمعها أو إستخراجها بإستخدام الأجهزة الإلكترونية والشبكات، فهذين الضابطين يكمل كل منهما الآخر لذا يجب توافرهما معًا، ويجب أيضًا أن يستمر توافرهما في الدليل الإلكتروني خاصة عند مرحلة جمع وإستخراج الدليل ومرحلة توثيق وتوصيف الدليل.[1]

الفرع الثاني: خصائص الدليل الإلكتروني

يتميز الدليل الإلكتروني بمجموعة من الخصائص التي تميزه عن الدليل المادي، وهي خصائص نابعة من طبيعته الرقمية والبيئة التي يستخرج منها، وسنبين فيما يلي أبرز هذه الخصائص على النحو التالي:

أولًا: الدليل الإلكتروني ذو طبيعة علمية وتقنية

إن الدليل الإلكتروني يتميز بأنه دليل علمي إستنادًا للبيئة التي يتواجد بها والتي تم إنشاؤها من قبل مختصين فنيين على أسس علمية، مثلما هو دليل تقني إستنادًا للمصدر الذي جاء منه وهو البيئة الرقمية.

1- الدليل الإلكتروني دليل علمي:

الدليل الإلكتروني عبارة عن مجموعة من المجالات أو النبضات المغناطيسية أو الكهربائية غير الملموسة التي تكون موافقة لما وصل إليه العلم فلا يتعارض مضمونها مع القواعد العلمية الأساسية[2]، فينبغي أن تتمتع بقدرة على التجاوب مع الحقيقة تمامًا كما هو الحال بالنسبة للدليل المادي لأن العلم يسعى إلى كشف الحقيقة في حين أن القانون يسعى لتحقيق العدالة، من هنا وجب ألا يتعارض الدليل الإلكتروني مع القواعد العلمية السليمة كما مع القواعد القانونية المعمول بها، وبالتالي ينبغي ألا يخرج عن الحقائق التي توصل إليها العالم الرقمي وإلا إنعدمت قيمته كدليل علمي[3]، وإنطلاقًا من هذا فإنه إذا كان الدليل العلمي له منطقه الذي يجب أن

[1]- رامي متولي القاضي، **الدليل الجنائي الرقمي في التشريع المصري في ضوء أحكام القانون رقم: 175 لسنة 2018 ولائحته التنفيذية**، كلية القانون بالجامعة البريطانية في مصر، مجلة القانون والتكنولوجيا، المجلد الثاني، العدد الأول، أفريل 2022، مصر، ص185.

[2]- خالد ضو، **حجية الدليل الالكتروني وشروط قبوله في الإثبات الجنائي**، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو-الأغواط، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المجلد05، العدد الأول، مارس2022، الجزائر، ص205

[3]- عادل مشموشي، **جرائم المعلوماتية وتحديات مسارحها الإفتراضية، أدواتها الإلكترونية، أساليبها التقنية، مقتضياتها التشريعية**، المؤسسة الحديثة للكتاب، الطبعة الأولى، 2019، لبنان، ص 611.

لا يخرج عليه من حيث وجوب عدم تعارضه مع القواعد السليمة فإن الدليل الإلكتروني كذلك له ذات الطبيعة أي يجب أن لا يخرج عن العالم الرقمي وإلا فقد معناه[1].

وعملية البحث عن الدليل الإلكتروني تتم في البيئة الرقمية الخاضعة لقوانين المعلوماتية[2]، وعليه فإن إستخراج الدليل الإلكتروني يحتاج إلى بيئة مماثلة لتلك التي نتج عنها، لذا يتطلب الإستعانة بالأجهزة وأدوات التقنية وإستخدام برامج ملائمة، للإطلاع عليه أو إستخراجه في هيئة ملموسة أو مادية، وهي تعد أساليب علمية.[3]

2- الدليل الإلكتروني دليل تقني:

يستمد الدليل الإلكتروني طبيعته التقنية من الوسط المتواجد فيه ومن الأجهزة الإلكترونية التي يستخلص منها أو أية منظومة معلوماتية أخرى[4]، لذلك فهو ذو طبيعة تقنية يقتضي وجود خبرة قضائية متخصصة لإستخلاصه[5]، ومن هذا المنطلق يجعلنا نقرر أنه لا وجود للدليل الإلكتروني خارج بيئته التقنية، وأنه لكي يكون هناك دليلًا إلكترونيًا يجب أن يكون مستوحًا من البيئة الرقمية وهي العالم الكامن في الأجهزة الإلكترونية والشبكات التي يتم تداول الحركة عبرها[6].

وتترتب على هذه الخاصية أنه لا يمكن الوصول إلى الدليل الإلكتروني إلا من طرف الخبير التقني المتخصص الذي لديه معرفة وخبرة تقنية[7]، ومن هذا المنطلق يجعلنا نقرر أن الطبيعة التقنية تقتضي أن يكون هناك توافق بين الدليل المستخلص والبيئة المتواجد فيها[8] لأن

---

[1]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، أطروحة الدكتوراه علوم، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2014/ 2015، ص 41.

[2]- بن مالك أحمد، الخال إبراهيم، **دور الأدلة الرقمية في الإثبات الجنائي**، المركز الجامعي علي كافي تندوف، مجلة العلوم الإنسانية، المجلد 05، العدد 01، أفريل 2021، الجزائر، ص-ص 108- 109.

[3]- مسعود بن حميد المعمري، **الدليل الإلكتروني لإثبات الجريمة الإلكترونية**، كلية القانون الكويتية العالمية، مجلة كلية القانون الكويتية العالمية-أبحاث المؤتمر السنوي الدولي الخامس9-10 ماي 2018، الجزء الثاني، العدد 3، أكتوبر 2018، الكويت، ص-ص 197-198.

[4]- عميمر عبدالقادر، **التحديات القانونية لإثبات الجريمة المعلوماتية**، د.ر.ط، 2021، النشر الجامعي الجديد، تلمسان-الجزائر، ص 106.

[5]- تفيد هذه الخاصية للدليل الإلكتروني أنه لابد للضباط الشرطة القضائية وسلطات التحقيق أن يبنوا عملهم على أساس الخبرة في التقنية، فلدى بعض الدول المتقدمة يكون لسلطات التحقيق المقومات التقنية الكاملة التي تحتاجها، ويكون هناك فصل بين الخبرة وسلطة التحقيق في الجرائم التي يكون الإعتماد فيها على الدليل الإلكتروني، حيث تضم سلطة التحقيق عناصر ذات كفاءة عالية تمتلك الخبرة في التقنية كما هو الحال في الولايات المتحدة الأمريكية، أما سلطات التحقيق التي لا تمتلك ذلك فإنها تعتمد على الخبرة في تحقيق مثل هذه الجرائم المعلوماتية التي تستند على الدليل الإلكتروني لإثباتها، وبالتالي لا يتحقق الفصل بين سلطة التحقيق والخبرة، حيث إن الخبرة تقوم بدور في التحقيق لمساعدة سلطة التحقيق لإثبات الجريمة والدليل التقني، وللمزيد من التفصيل، ينظر: مسعود بن حميد المعمري، مرجع سابق، ص 198.

[6]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة الماجستير، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2012-2013، ص 123.

[7]- عميمر عبدالقادر، مرجع سابق، ص 106.

[8]- بن مالك أحمد، الخال إبراهيم، مرجع سابق، ص 109.

التقنية لا تنتج أدلة مادية ملموسة كالسلاح الأبيض الذي يتم به إكتشاف القاتل أو بصمة الإصبع أو إعترافًا مكتوبًا أو مزية غير مستحقة في جريمة الرشوة تدل على مرتكب الجريمة، وإنما ما تنتجه التقنية هو عبارة عن نبضات رقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل بين أجزاء وسائل التقنية وشبكات الإتصال متعدية حدود المكان والزمان الواحد[1]، ومن ثم فإن ترجمة الدليل الإلكتروني وإستخراجه على هيئة مادية ملموسة لا يعني أن هذا التجمع يعتبر هو الدليل بل إن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الإستناد إليها على معلومة معينة، والعلاقة في إطار بحث هذه الخاصية يجب أن تبنى على أساس الوظيفة التي يمكن أن تؤديها التقنية في كشف الدليل الإلكتروني[2]، فضلًا عن ضرورة توفر أجهزة مختصة لتجميعه وتحليل محتواه وإخضاعه لبعض البرامج للتأكد من سلامته من العبث والتلاعب[3].

نلاحظ أن مثل هذه العلاقة تلمح من ناحيتين، فمن ناحية يجب الإهتمام بتقنية البرامج التي تتعامل مع الدليل الإلكتروني من جهة تحليله وتقديمه، ومن الناحية الأخرى فإن هذه البرامج ذاتها والتي تساهم تقنيتها في الحصول على الدليل يجب أن تكون في محل قبول لدى المحكمة، ومن ثم فإن إطلاق الصفة الرقمية تعني أنه ينبغي أن يكون هناك توافق بين الدليل المرصود وبين البيئة التي يعيش فيها هذا الدليل وهي العالم الرقمي[4]، ونتيجة هذه الطبيعة التقنية نجد أن الدليل الإلكتروني يتميز بما يلي:

أ- يمتاز الدليل الإلكتروني بالسعة التخزينية العالية:

حيث لا يتطلب مساحة كبيرة لتخزين الدليل الإلكتروني إذ يكفي الإستعانة بفلاش ديسك أو أي دعامة إلكترونية لحفظ الآلاف من المعطيات سواء كانت صورًا أو مقاطع فيديو وغيرها، وحفظها لا يحتاج إلى سعة التخزين كبيرة وإنما كل ما تتطلبه أن يتم حفظها في ظروف عادية، أما سعة وسائل حفظ المعلومات الرقمية فتتسع لمكتبات بكاملها.[5]

ب-يسهم الدليل الإلكتروني في تحليل المعطيات ورصد الجاني في ذات الوقت:

حيث يمكنه من تسجيل تحركات الفرد وسلوكياته من خلال مقاطع فيديو أو تسجيلات الصوتية أو غيرها من المعطيات، كما يمكنه من كشف طبيعة شخصية الجاني من خلال ما يحتفظ به من معطيات ومعلومات وغيرها، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.[6]

---

[1]- مسعود بن حميد المعمري، مرجع سابق، ص 198.

[2]- رفاه خضير جياد العارضي، مرجع سابق، ص-ص 76-77.

[3]- عميمر عبدالقادر، مرجع سابق، ص-ص 106-107.

[4]- رفاه خضير جياد العارضي، مرجع سابق، ص 77.

[5]- عادل مشموشي، مرجع سابق، ص 612.

[6]- عائشة بن قارة مصطفى، مرجع سابق، ص 64.

ثانيًا: الدليل الإلكتروني ذو طبيعة رقمية ثنائية (0 و1)

تعني خاصية الدليل الإلكتروني ذو طبيعة رقمية ثنائية (0 و1) بأن الآثار التي يتركها مستخدم المنظومة المعلوماتية والتي تشمل الرسائل المرسلة منه أو التي إستقبلها وكافة الإتصالات التي تمت من خلال الأجهزة الإلكترونية وشبكة الإتصالات، تكون على الشكل الرقمي.[1]

وسمي البعض الدليل الرقمي بهذا الإسم -الرقمي- لأن تقنيات المعلومات الحديثة ترتكز على تقنية الترقيم، التي تعني ترجمة أو تحويل أي مستند إلكتروني مؤلف من نصوص أو صور إلى نظام ثنائي في تمثيل الأعداد يفهمه الجهاز الإلكتروني[2] قوامه تعداد غير محدود من أرقام ثنائية متمثلة في الصفر (0) والواحد (1)، حيث يمثل الرقمي (0) وضع الإغلاق (off) ويمثل الرقم (1) وضع التشغيل (On)، والتي تتميز بعدم التشابه فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه، وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة، ويختلف تكوين معطياته من حيث الحجم والموضوع.[3]

فهو إذن يشتق من أو بواسطة نظم برامجية معلوماتية أوالأجهزة الإلكترونية أو شبكات الإتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميًا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها.[4]

ثالثًا: الدليل الإلكتروني دليل غير ملموس

إن الطبيعة التكوينية للدليل الإلكتروني والوسط الرقمي المتواجد فيه جعله دليلًا غير مادي، كذلك فهو دليل ذو طبيعة غير ملموسة يتكون من معطيات ومعلومات على هيئة إلكترونية[5]، حيث أن ترجمة الدليل الإلكتروني وإستخراجه في شكل مادي ملموس لا يعني أن هذا التجميع المادي هو الدليل بل أن هذه العملية هي مجرد نقل لتلك المعطيات من طبيعتها الرقمية إلى الهيئة التي يمكن الإستدلال بها على معلومة معينة[6].

فإستخراج الدليل الإلكتروني يحتاج إلى بيئة مشابهة لتلك التي نتج عنها، لذا يتطلب الإستعانة بأجهزة وأدوات التقنية وإستخدام برامج معلوماتية ملائمة للإطلاع عليه أو إستخراجه

---

[1]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 125.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 56.

[3]- بن طالب ليندا، **الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)**، أطروحة الدكتوراه علوم، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2019، ص 43.

[4]- بهاء المري، **جرائم السوشيال ميديا فيس بوك-أنستجرام-واتس آب-فايبر-تويتر وجرائم المحمول وحجية الدليل الإلكتروني في الإثبات**، الطبعة الرابعة، 2022، دار الأهرام، مصر، ص 737.

[5]- مسعود بن حميد المعمري، مرجع سابق، ص-ص 197-198.

[6]- عميمر عبد القادر، مرجع سابق، ص 106.

في هيئة مادية وهي تعد أساليب علمية[1]، وقابلية الدليل الإلكتروني للتجسيد المادي هي ميزة إضافية تدعم حجية الدليل الإلكتروني وتزيد من موثوقيته إذا روعيت في ذلك الأصول العلمية في هذه العملية والشروط المطلوبة في الشخص القائم بها[2].

رابعًا: الدليل الإلكتروني دليل متنوع ومستحدث

في ظل التطور المتسارع الذي يشهده العصر الحالي في المجال التكنولوجي أصبح من الضروري أن يشهد الدليل الإلكتروني بدوره تطورًا من حيث تنوع أشكاله وإبتكار أنواعه، بما يواكب المستجدات التقنية ويستجيب لطبيعة الجرائم الحديثة.

خاصية التنويع تعني أن الدليل الإلكتروني يمكن أن يظهر في مختلف الأشكال، كأن يكون معطيات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الإنترنت أو خوادم الشبكات، وقد يكون معطيات مفهومة كظهور الدليل في صورة وثيقة معدة بنظام المعالجة الآلية أوصورة مخزنة بجهاز أو في البريد الإلكتروني أو في منصات التواصل، وكما قد يكون أيضًا مرتبطًا بالتشفير.[3]

أما عن كون الدليل الإلكتروني دليلًا مستحدثًا فهو مستحدث بطبيعته، إذ يمتاز بالإستحداث التلقائي تبعًا لتطور البيئة الرقمية الّتي تعتمد أساسًا على التجدد، ويرجع هذا إلى تطور الثورة التكنولوجية خاصة في مجال الإتصالات وأجهزة التواصل[4]، ما يعني عدم وجود قواعد جامدة يرتبط بها الدليل الإلكتروني من حيث طبيعته العلمية[5].

لذلك فإنه من الضروري مواكبة التطور التكنولوجي سواء من حيث الأجهزة المستحدثة أو سواء من حيث البرامج التشغيلية والمعتمدة داخل هذه الأجهزة وبرامج إستخلاص الدليل الإلكتروني، إلى جانب الإطلاع المستمر على تلك التطورات والتحديثات للبرامج والأجهزة، وهو ما يساعد على الكشف عن الأدلة الجنائية الإلكترونية وإثبات الجريمة بطريقة أسهل وأسرع.[6]

---

[1]- مسعود بن حميد المعمري، مرجع سابق، ص-ص 197-198.

[2]- عميمر عبد القادر، مرجع سابق، ص 106.

[3]- عيدة بلعابد، **الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية**، جامعة تامنغست، مجلة آفاق علمية، المجلد11، العدد01، 2019، الجزائر، ص 138.

[4]- نفس المرجع، ص 138.

[5]- بن شهرة شول، **الحماية الجنائية للتجارة الإلكترونية**، أطروحة الدكتوراه، تخصص: قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر-بسكرة، 2009-2010، ص307.

[6]- مسعود بن حميد المعمري، مرجع سابق، ص 199.

خامسًا: قابلية الدليل الإلكتروني للنسخ

قد يكون بالإمكان نسخ أو تصوير بعض الأدلة المادية إلا أن ما يستنسخ منها لا يكون له ذات الطبيعة وعادة ما لا تكون النسخ منها بذات الحالة أو القيمة بالنسبة لأصل الدليل، على خلاف الدليل الإلكتروني الذي يمكن نسخه أكثر من مرة وتكون كل نسخة منه بذات جودة الدليل الأصلي.[1]

يمكن إعتبار هذه الخاصية ميزة يتمتع بها الدليل الإلكتروني عن غيره من الأدلة المادية، حيث تعد ضمانة شديدة الفعالية للحفاظ على الدليل من مخاطر الإتلاف والفقد عن طريق نسخ طبق الأصل حيث تتطابق طريقة النسخ مع طريقة الإنشاء[2]، بالإضافة إلى إمكانية مقارنته بالأصل بإستخدام البرامج والتطبيقات الصحيحة[3] بغرض تحديد ما إذا كان الدليل الإلكتروني قد تم العبث به أو تعديله وهذا يعني أنه يصعب على الجاني إخفاء جريمته أو أدلتها، مما تشكل ضمانة لعدم نفاذ المجرم من المسؤولية الجزائية وفي نفس الوقت الحفاظ على الدليل الإلكتروني من الفقد.

سادسًا: صعوبة التخلص من الدليل الإلكتروني

لا يمكن التخلص من الدليل الإلكتروني مباشرة إن لم يتم التخلص من الوسيلة أو الجهاز الموجود فيه الدليل أو تخريبه أو إتلافه كإتلاف دعامته التي حفظ عليها، ولكن يمكن تدارك ذلك من خلال الإحتفاظ بأكثر من نسخة عنه، وذلك على خلاف الدليل المادي الذي يسهل في أحيان كثيرة التخلص منه بحرقه أو تفكيكه أو تحطيمه[4]، وكلما حدث إتصال بالعالم الرقمي عن طريق إدخال معطيات إلى ذلك العالم فإنه من الصعب التخلص منها ولو كان ذلك بإستخدام أكثر الوسائل تطورًا[5].

ويترتب على هذه الخاصية مسائل قانونية هامة أبرزها مسألة التخلص أو إخفاء الدليل، وهو يعد فعلًا آخر موضوع تجريم بمقتضى القانون، فإذا ثبت أن مرتكب الجريمة الماسة

---

[1]- عادل مشموشي، مرجع سابق، ص 611.

[2]- بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة- بجاية، المجلة الأكاديمية للبحث القانوني، المجلد 05، العدد 01، 2014، الجزائر، ص 278.

[3]- منصارة يوسف، **الدليل الإلكتروني في القانون الجزائي الطريق إلى تحول أدلة الاثبات في المادة الجزائية دراسة مقارنة**، د.ر.ط، 2018، دار الخلدونية، الجزائر، ص35.

[4]- عادل مشموشي، مرجع سابق، ص 611.

[5]- بلجراف سامية، **سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي**، مخبر القانون الخاص المقارن، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي-الشلف، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021، الجزائر، ص 682.

بالمستند الإلكتروني قد إستخدم من البرمجيات من أجل التخلص من الدليل فإنه يمكن متابعته وإدانته بالنصوص القانونية التي تجرم مثل هذه الأفعال.[1]

سابعًا: سهولة التلاعب بالدليل الإلكتروني

يمتاز الدليل الإلكتروني بسهولة التلاعب فيه سواء عن طريق التعديل أو الإتلاف أو الإدراج في مستندات أو معلومات رقمية آخرى بسرعة ودقة متناهية، ولعل ما يخفف من الآثار السلبية لهذه الخاصية في مجال التحري والتحقيق في الجريمة هو خاصية إمكانية إسترجاع الدليل الإلكتروني عن طريق البرمجيات المناسبة لذلك.[2]

ثامنًا: الدليل الإلكتروني قابل للإسترجاع

بقدر سهولة تدمير أو إخفاء الدليل الإلكتروني بقدر قيام إمكانية إسترجاع الدليل ذاته المفقود أو المخفي وهي خاصية تميزه عن غيره من الأدلة التقليدية، فالمعروف أن الأدلة في العالم المادي إذا طالها الإتلاف أو التدمير أو التصفية (أداة جريمة، شريط، مستندات، سجلات رسمية...) فإنها لا تعود إلى عالم الوجود من عالم الفناء، بعكس الدليل الإلكتروني الذي أصبحت تتوفر بخصوص الحصول عليه وإسترجاعه برمجيات متخصصة ومتطورة من ذات الطبيعة تمكن من إسترجاعه وإسترداد كافة المعطيات الموجودة التي تم محوها أو إزالتها من الدعامة التي كانت متصلة بها أو الجهاز الموجودة فيه، ولا يمكن التخلص من الدليل[3] حيث أن الملفات والمعطيات المحذوفة يمكن إستردادها[4] بعد مدة طويلة من حذفها لأن الأثر الرقمي[5] لا يمكن إخفاؤه بالكامل[6].

---

[1]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 125.

[2]- مذكور عائشة، **الحماية الجنائية للعقود الإلكترونية في التشريع الجزائري**، رسالة الماجستير، فرع قانون العقود، كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه في القانون الأساسي والعلوم السياسية، جامعة آكلي محند أولحاج البويرة، 2018، ص 137.

[3]- بن شهرة شول، مرجع سابق، ص308.

[4]- هناك العديد من البرامج الحاسوبية وظيفتها إستعادة المعطيات التي تم حذفها أو إلغائها، سواء تم هذا الإلغاء بالأمر (Delete) أو عن طريق إعادة تهيئة أو تشكيل للقرص الصلب (Hard Disk) بإستخدام الأمر (Format)، سواء كانت هذه المعطيات صوراً أو رسومات أو كتابات أو غيرها، كل ذلك يشكل صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة، طالما علم رجال البحث والتحقيق الجنائي بوقوع الجريمة، وللمزيد من التفصيل، ينظر: عائشة بن قارة مصطفى، مرجع سابق، ص 63.

[5]- يقصد بالأثر الرقمي كل ما ينتج عن تفاعل المستخدم من وسائل تقنية المعلومات والأجهزة الإلكترونية، حيث ينتج عن هذا التفاعل مجموعة كبيرة من الآثار الرقمية (يطلق عليها أحياناً البصمات الرقمية أو الأشياء الإصطناعية)، إلا أن هذا الأثر يتحول إلى دليل إلكتروني إذا نجح الخبراء التقنيون بإستخدام الأجهزة والتطبيقات التكنولوجية الخاصة في الربط بينه وبين الجريمة المرتكبة، ومن ثم إثبات الصلة بينه وبين مرتكب الجريمة، وللمزيد من التفصيل، ينظر: رامي متولي القاضي، مرجع سابق، ص188.

[6]- عميمر عبد القادر، مرجع سابق، ص 108.

وللدليل المسترجع نفس القيمة العلمية والحجية الثبوتية الأمر الذي لا يتوفر في الأدلة التقليدية، وهو ما يشكل ضمانة قوية للحفاظ على الدليل الإلكتروني من الفقدان والإتلاف والتغيير.[1]

الفرع الثالث: تقسيمات الدليل الإلكتروني

يترتب على هذه الخاصية أن أي محاولة لتقسيم الدليل الإلكتروني يمكن أن يكون محل جدل فقهي، ويرجع ذلك إلى التطور المستمر الذي يطرأ على البيئة الرقمية المتواجد فيها هذا الدليل مما تجعله من الأدلة المستحدثة والمتنوعة بطبيعتها، فتطور هذه البيئة الرقمية يكاد أن يكون تلقائيًا حيث تتسع لإمكانية شمول مظاهر رقمية جديدة خصوصًا وأن العالم الرقمي لا يزال في بداياته ولم يبلغ بعد إلى منتهاه، فالعالم الرقمي مستحدث لا ينتهي ولن يكون بسهولة إحتوائه فهو عالم متسع الأبعاد مما قد ينتجه الخيال من أفكار حول الحدود.[2]

أولًا: الجهود الفقهية لتقسيم الدليل الإلكتروني

إنقسم البعض من الفقه لتقسيم الدليل الإلكتروني إلى:

1- تقسيم الدليل الإلكتروني على أساس مصدره:

قسم الدليل الإلكتروني على أساس المصدر إلى:

أ- الأدلة الإلكترونية الخاصة بأجهزة الحاسوب وشبكاته:

سلوك غير مشروع يقع على أجهزة الحاسوب سواء وقع على المكونات المادية (Hard-Ware) أو على المكونات المعنوية (Soft Ware) أو على قواعد البيانات الرئيسية (Data-Base)، كتخريب الشاشات أو الطابعة أو وسائط التخزين الإلكترونية، وكذلك إستخدام الفيروسات أوتعديل أو محو المعطيات الرئيسية وغيرها.[3]

ب- الأدلة الإلكترونية الخاصة بالإنترنت:

وتعني الأدلة الناتجة عن النشاطات الإجرامية التي يستخدم فيها التقنية الحديثة المتمثلة بالإنترنت، وعبر عنها خبراء المنظمة الأوروبية للتعاون الإقتصادي بأنها: "كل سلوك غير مشروع أو غير مسموح به أو مناف للأخلاق، يرتبط بالمعالجة الآلية للمعطيات أو بنقلها".[4]

---

[1]- عميمر عبد القادر، مرجع سابق، ص 108.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 77.

[3]- نفس المرجع، ص 72.

[4]- بصائر علي محمد، مروى عبد الواحد حسن، **الدليل الإلكتروني في مجال الإثبات الجنائي**، كلية الأداب/ جامعة واسط، مجلة لارك للفلسفة واللسانيات والعلوم الإجتماعية، المجلد 09، العدد 05، 2019، العراق، ص 278.

ت- الأدلة الإلكترونية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات:

تستخدم هذه البروتوكولات لضمان تشغيل أنظمة الإتصال على الشبكة المعلوماتية، وهو ما يجعلها مصدر للدليل الإلكتروني نظرًا لإحتواءها على كافة النشاطات ومستخدمي الشبكة وتحديدها من حيث المكان والزمان وتحديد الأجهزة التي تم بواسطتها النشاط والأجهزة التي وقع عليها النشاط الجرمي.[1]

ث- الأدلة الإلكترونية الخاصة بالشبكة العالمية للمعلومات (الإنترنت):

هي الأدلة الناتجة عن الجرائم الماسة بأي وثيقة أو نص متاح عبر الشبكة، ومثالها إنتهاك الملكية الفكرية للأفلام والبرامج وسرقة أرقام بطاقة الإئتمان وغيرها[2]، فهذه الجرائم تتطلب إتصالًا بالإنترنت على عكس جرائم الحاسوب التي من الممكن حدوثها سواء كانت متصلة بالإنترنت أو لا.[3]

إلا أن هذه التقسيمات لا تتناسب مع مفهوم التقنيات الحديثة وإنما تم حصره في الدليل الإلكتروني المستخلص من جهاز الحاسوب وشبكاته، وميزت بين شبكات الحاسوب والإنترنت وبروتوكول تبادل المعلومات والشبكة العالمية للمعلومات التي هي في الأصل واحد فإختلاف المصطلحات لا يعني إختلافًا في المعنى.[4]

2- تقسيم الدليل الإلكتروني على أساس قيمته الثبوتية:

قسم الدليل الإلكتروني على أساس قيمته الإثباتية لقسمين رئيسيين:

أ- أدلة أعدت لتكون وسيلة إثبات:

وهذا النوع من الأدلة الإلكترونية يمكن إجماله في:

أ-1- السجلات التي تم إنشاؤها تلقائيًا بواسطة الجهاز والتي لم يساهم الإنسان في إنشاؤها كفواتير البطاقات البنكية وسجلات الهاتف.

[1]- عميمر عبدالقادر، مرجع سابق، ص 111.
[2]- بصائر علي محمد، مروى عبد الواحد حسن، مرجع سابق، ص 278.
[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 72.
[4]- نفس المرجع، ص 73.

أ-2- السجلات التي تم حفظ جزء منها بواسطة الإنسان عن طريق الإدخال والجزء الآخر تم إنشاؤه بواسطة الجهاز، ومن أمثلة على ذلك رسائل غرف المحادثة المتبادلة على الإنترنت ورسال البريد الإلكتروني.[1]

ب- الأدلة ليست معدة لتكون وسيلة إثبات:

هذا النوع من الأدلة الإلكترونية تتجسد في الآثار التي يتركها الجاني دون أن يكون راغبًا في وجودها أي تنشأ من دون إرادته، كتسجيل الرسائل المرسلة منه أو التي إستقبلها أو كافة الإتصالات التي تمت من خلال الجهاز أو شبكة المعلومات العالمية، وهو ما يسمى بالبصمة الرقمية.[2]

وتبدو أهمية التمييز بين هذين النوعين، أن النوع الأول من الأدلة الإلكترونية هو الأكثر أهمية من النوع الثاني لكونه أعد أصلًا ليكون وسيلة إثبات لبعض الوقائع، وعادة ما يعمد إلى حفظه للإحتجاج به لاحقًا، بينما النوع الثاني من الأدلة الإلكترونية لم يعد أصلًا ليكون أثرًا لمن صدر ضده.[3]

ثانيًا: الجهود التشريعية والقضائية لتقسيم الدليل الإلكتروني

التقسيم الذي قامت به وزارة العدل الأمريكية سنة 2002 والذي إعتمده القضاء الأمريكي فيما بعد، والذي قسم الدليل الإلكتروني إلى ثلاث مجموعات[4] وهي كالآتي:

1- تقسيم وزارة العدل الأمريكية:

قسمت وزارة العدل الأمريكية الدليل الإلكتروني إلى ثلاث مجموعات:

أ- السجلات المحفوظة في الحاسوب:

السجلات المحفوظة في الحاسوب تشمل الوثائق المكتوبة والمحفوظة، مثل ملفات برامج معالجة الكلمات والبريد الإلكتروني ورسائل غرف المحادثة على الإنترنت.[5]

ب- السجلات التي تم إنشاؤها بواسطة الحاسوب:

وتعد مخرجات أصلية للحاسوب حيث لم يشارك الإنسان في إعدادها مثل سجلات الهاتف وفواتير أجهزة السحب الآلي للنقود.[1]

---

[1]- خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، الطبعة الأولى، 2011، دار الثقافة للنشر والتوزيع، عمان-الأردن، ص234.

[2]- نفس المرجع، ص-ص 234-235.

[3]- حطاب كمال، **الحماية الجزائية للتجارة الإلكترونية**، أطروحة الدكتوراه، علوم تخصص: علوم قانونية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس سيدي بلعباس، 2015-2016، ص 341.

[4]- عميمر عبدالقادر، مرجع سابق، ص112.

[5]- عائشة بن قارة مصطفى، مرجع سابق، ص 74.

ت- السجلات المختلطة:

السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه عن طريق الحاسوب، ومن أمثلتها أوراق العمل المالية التي تحتوي على محتويات تم تحويلها إلى برامج أوراق العمل مثل "إكسل" ومن ثم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها.[2]

2- تقسيم الذي أخذ به القضاء الأمريكي:

يؤخذ على هذه التقسيمات أنها إقتصرت على نوع محدد من الدليل الإلكتروني وهي سجلات الحاسوب التي تحتوي على نص، رغم أن الدليل الإلكتروني يشمل على كافة المعطيات الممكن تداولها إلكترونيًا كالأصوات والصور والرسوم وغيرها، بل تستعمل حاليًا التطبيقات المعلوماتية وبروتوكولات الإتصالات في تحقيق في الجرائم الماسة بالمستند الإلكتروني، ويعتبر نظام (TCP/IP) من أبرز البروتوكولات المستخدمة في شبكة الإنترنت فهي تعد جزء أساسي منه، بحيث تدل بشكل جازم عن مصدر الجهاز الإلكتروني المستخدم في إرتكاب الجريمة وتحديد الأجهزة التي أصابها الضرر من السلوك الإجرامي وتحديد نوعية السلوك الإجرامي خلال الفترة الزمنية لإرتكاب الجريمة.[3]

أ- سجلات الحاسوب المخزنة:

ويقصد بها التخزين الإلكتروني (Computer Stored-Records) فهو ناتج عن التدخل الإنساني في تكوين الملفات عن طريق تخزينها في الحاسوب، إما يتم بواسطة إستخدام المعطيات وبناءً على ذلك تظهر القوة الإسترادادية للمعطيات على هيئة معلومات محددة، وإما يتم بواسطة تخزين المعطيات دون أن تستخدم وبناءً على ذلك لا نكون بصدد مساحة مادية في الذاكرة وإنما فقط عبارة عن مجموعة من الأرقام.[4]

ب-سجلات الحاسوب المتوالدة:

تحتوي على مخرجات برامج الحاسوب التي لم تتعرض لأي تدخل بشري فالحاسوب هو الذي يصدرها مثل سجلات الولوج على الإنترنت ومصدرها مقدم خدمة الإنترنت، فهذه السجلات لا تتضمن معطيات بشرية فهي عبارة عن مخرجات كان لابد من جود مدخلات لها ممثلة في لوغاريتمات البرمجة.[5]

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 74.

[2]- عميمر عبدالقادر، مرجع سابق، ص113.

[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 76.

[4]- لهوى رابح، **الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش**، أطروحة الدكتوراه علوم، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2020 /2021، ص57.

[5]- عائشة بن قارة مصطفى، مرجع سابق، ص 75.

ت- سجلات الحاسوب المتوالدة والمخزنة بذات وقت:

السجلات التي تجمع بين التدخل البشري ومعالجة الحاسوب كإدخال معطيات معينة وطلب من الحاسوب بمعالجتها للتوصل إلى النتائج التي يسمح بها برنامج المستخدم، وتجدر الإشارة إلى أن هذه الطبيعة خاصة بكل نوع وتنعكس على قيمته الثبوتية أمام المحاكم الأمريكية.[1]

ثالثًا: تقسيم الدليل الإلكتروني على أساس طبيعة مخرجاته

تتنوع مخرجات الأجهزة الإلكترونية بين المخرجات الورقية والمخرجات الرقمية، وهناك نوع ثالث من المخرجات يتمثل في عرض المعطيات المعالجة آليًا على الشاشة المرئية.

1- **المخرجات الورقية:**

تعتبر المخرجات الرقمية الذي تسجل فيه المعلومات على الورق أحد الأشكال الرئيسية التي تأخذها هذه المخرجات ويستخدم في ذلك الطابعات، والطابعة هي عبارة عن جهاز يقوم بإنتاج نسخ مطبوعة من المعطيات مثل التقارير والشبكات وقوائم المعطيات والبرامج التي يحتاج إليها المستخدمون، وتتنوع الطابعات الملحقة بالأجهزة الإلكترونية لإنتاج المخرجات الورقية من حيث طريقة تشغيلها وسرعة التشغيل والتطبيق المستهدف، كما يستخدم أيضًا الرسم في طباعة الرسومات بدرجات وضوح مختلفة على الورقة ومن أشهر أنواع جهاز الرسم راسم الطاولة وراسم الأسطوانات.[2]

2- **المخرجات ذات الطبيعة الرقمية:**

ويسميها البعض المخرجات اللاورقية وهي المعلومات المخزنة على أي دعامة تحمل المعطيات المعلوماتية التي تحتوي على مساحة تخزين واسعة.

3- **المخرجات المرئية:**

وتسمى أيضًا وحدة العرض المرئي، ويتمثل هذا النوع من الدليل في عرض المعطيات المعالجة آليًا بواسطة الجهاز الإلكتروني على الشاشة الخاصة به.[3]

رابعًا: تقسيم الدليل الإلكتروني على أساس وسائل تحصيله:

إضافة إلى التقسيمات السالف ذكرها فإنه من الممكن أن يتم الإعتماد على وسائل إستخلاص الدليل الإلكتروني كمعيار آخر لتقسيمه، والتي يمكن أن نوردها فيما يلي:[4]

1- الدليل الإلكتروني الناتج عن تقنية تسجيل الأصوات وتثبيتها؛

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص-ص 75-76.

[2]- أحمد يوسف الطحطاوي، **الأدلة الإلكترونية ودورها في الإثبات الجنائي (دراسة مقارنة)**، د.ر.ط، 2015، دار النهضة العربية، القاهرة-مصر، ص23.

[3]- عميمر عبدالقادر، مرجع سابق، ص 114.

[4]- نفس المرجع، ص 115.

2- الدليل الإلكتروني الناتج عن تقنية إلتقاط الصور؛

3- الدليل الإلكتروني الناتج عن تقنية مراقبة الإتصالات الإلكترونية[1]؛

4- الدليل الإلكتروني الناتج عن تقنية حفظ المعطيات المتعلقة بحركة السير؛

5- الدليل الإلكتروني الناتج عن تقنية المعطيات المتعلقة بالمشتركين[2]؛

6- الدليل الإلكتروني الناتج عن فحص مسار الإنترنت؛

7- الدليل الإلكتروني الناتج عن فحص نظام بروتكول الإنترنت (IP)؛

8- الدليل الإلكتروني الناتج عن فحص ذاكرة الأجهزة الإلكترونية؛

9- الدليل الإلكتروني الناتج عن فحص محتويات الأجهزة الإلكترونية[3].

المطلب الثاني: الدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الإلكتروني

الدليل الإلكتروني نستخدمه في حياتنا اليومية بشكل معتاد غير أننا لا نشعر بالآثار الإلكترونية التي نتركها بالأجهزة الإلكترونية، وهذه الأدلة الإلكترونية تساهم بشكل قاطع في إثبات التصرفات القانونية والتعاقدية عبر الشبكات المعلوماتية، ويتم إستخراجها في شكل مطبوع[4] فيما يعرف بالمستندات أو المحررات الإلكترونية.

ظهرت المستندات الإلكترونية وذلك عن طريق وضع المعلوماتية في صورة رقمية وتخزينها كمعطيات على دعامة إلكترونية، أو تكون مخزنة ضمن برنامج معلوماتي في جهاز إلكتروني، أو على شبكة الإنترنت في البريد الإلكتروني كنموذج لإحتواء البيانات الواردة والصادرة منه في شكل رسائل إلكترونية، تتم كتابتها وتوقيعها وإرسالها وحفظها في بيئة رقمية.[5]

لما كانت المستندات الإلكترونية تعد من بين الأدلة الجنائية التي يمكن أن تسهم في إثبات الوقائع محل الجرائم موضوع التحقيق الجنائي، فقد بات من الضروري دراسة المستند الإلكتروني كدليل في المسائل الجزائية، وتتطلب هذه الدراسة التطرق إلى مصدره القانوني والمتمثل في القانون المدني الذي أسس لظهوره وحدد شروط قبوله كوسيلة من وسائل الإثبات،

---

[1]- عميمر عبدالقادر، مرجع سابق، ص 116.

[2]- لهوى رابح، مرجع سابق، ص-ص 50-52.

[3]- الجرادات ضرغام، **أدلة الإثبات الجنائي من خلال الهواتف الذكية مفهومها وحجيتها دراسة مقارنة بين الفقه والقانون**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص-ص 16-17.

[4]- منصارة يوسف، مرجع سابق، ص 233.

[5]- بروك إلياس، عميرات عادل، **ماهية الإثبات المدني الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 166.

وهذا ما سنعرضه في دراستنا حيث نبدأ بمفهومه في (الفرع الأول)، ثم سنتطرق إلى عناصره في (الفرع الثاني)، أما (الفرع الثالث) فقد خصصناه إلى بيان الشروط اللازمة للإعتماد عليه كدليل حتى يعتد به في الإثبات الجزائي.

الفرع الأول: مفهوم المستند الإلكتروني

في ظل التزايد المطرد لحجم المعلومات وأهميتها في مختلف المجالات، أصبح من الضروري إيجاد وسائل فعالة لجمع المعلومات وحفظها وتخزينها وإسترجاعها وتداولها، إذ ظهر الجهاز الإلكتروني بصيغته الأكثر تطورًا مع شبكة الإنترنت خدمة لهذا المجال، ولما كانت المعلومات هي الشيء المتداول في الأوساط التقنية المعلوماتية فقد ظهرت الوثائق أو المستندات الإلكترونية، وهي مجموعة من المعلومات بمختلف صورها مخزونة أو معالجة بواسطة المنظومة المعلوماتية أو متداولة عن طريق شبكاتها.[1]

أولًا: تعريف المستند الإلكتروني

نظرًا لتعدد التعريفات المتعلقة بالمستند الإلكتروني وإختلافها بين الفقهاء، تبرز ضرورة إستعراض الآراء الفقهية المختلفة في تعريفه، إلى جانب التعريفات التي أقرتها المواثيق الدولية والتشريعات المقارنة، وكذا عند مكانته ضمن التشريع الجزائري.

1- التعريف الفقهي للمستند الإلكتروني:

عرف المستند الإلكتروني بأنه: "كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات، وقد سجلت عليه معلومات معينة سواء أكانت معدة للإستخدام بواسطة نظام المعالجة الآلية للمعلومات أم يكون مشتقًا من هذا النوع".[2]

كما عرف على أنه: "معلومات يتم إنشاؤها أو إرسالها أو تخزينها أو إستلامها، بوسيلة إلكترونية أو ضوئية أو رقمية أو صوتية، مادامت تتضمن إثبات واقعة أو تصرف قانوني محدد، وتتضمن توقيع إلكتروني ينسب هذه الواقعة أو التصرف لشخص محدد"، وعرف أيضًا من خلال مصطلح الوثيقة المبرمجة على أنه: "كل دعامة معلوماتية يتم الحصول عليها بوسائل معلوماتية، أي ناشئة على جهاز إلكتروني أو كهرومغناطيسي أو طبع ممغنط"، كما عرف بمصطلح الوثيقة المعلوماتية على أنه: "رسالة بيانات تتضمن معلومات تنشأ أو ترسل أو تستلم أو تخزن، بإستخدام وسائل إلكترونية".[3]

---

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص 53.

[2]- مثنى سعد السوداني، **التزوير المعلوماتي في الحاسب الآلي دراسة مقارنة**، الطبعة الأولى، 2022، دار مصر للنشر والتوزيع، القاهرة-مصر، ص 62.

[3]- بوكر رشيدة، **الحماية الجزائية للتعاملات الإلكترونية**، أطروحة الدكتوراه علوم، تخصص: قانون جزائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس - سيدي بلعباس-، 2017، ص 137.

كما ذهب البعض إلى أن المستندات لابد وأن ترتبط بالماديات حتى يمكن إضفاء وصف المستند عليها، فمثلًا لكي يمكن إضفاء وصف المستند على المعلومات فلابد من أن تكون مخزنة على الدعامة المادية، وسواء أكانت تلك المعلومات موجودة داخل المنظومة المعلوماتية أم خارجه.[1]

وإتجه البعض إلى تعريف المستند الإلكتروني على أنه: "كل دعامة مادية أو غير مادية، تصلح لأن تدون عليها الآراء أو المعلومات"، أو هو: "شيء مادي الذي يمكن أن يدون عليه شيء معنوي"، ويرى جانب آخر أن المقصود بالمستند في مجال المعلوماتية: "كل شيء مادي متميز الذي يصلح لأن يكون دعامة أو محلًا لتسجيل المعلومات المعالجة بواسطة نظام المعالجة الآلية".[2]

بينما ذهب البعض الآخر إلى أنه: "كل كتابة تدل على معنى مفهوم، ويمكن نسبتها إلى شخص معين من خلال توقيعه عليها"، ويعد الورق هو الدعامة السائدة في مجال إستعمال الكتابة وفي مختلف الميادين.[3]

2- التعريف الدولي للمستند الإلكتروني:

توصلت المجهودات الدولية عن طريق لجنة القانون التجاري الدولي لدى هيئة الأمم المتحدة إلى إصدار قانون الأونسيترال الدولي المتعلق بالتجارة الإلكترونية والتوقيع الإلكتروني وذلك بتاريخي 16 ديسمبر 1996 و05 جويلية 2001، والذي ضبط معالم التعامل الإلكتروني وإلتزامات وحقوق الأطراف بمقتضاه وإجراءات العمل بالتقنية الإلكترونية، وواكبته في هذا المجال العديد من الدول المتقدمة.[4]

عرفه قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية الذي أعدته لجنة القانون التجاري الدولي التابعة للأمم المتحدة[5] والذي أشار للمستند الإلكتروني بإستخدام مصطلح "رسالة البيانات" بمقتضى الفقرة (أ) من المادة 02 منه كالآتي: "يراد بمصطلح "رسالة بيانات": المعلومات التي يتم إنشاؤها أو إرسالها أو إستلامها أو تخزينها، بوسائل[6] إلكترونية أو

---

[1]- حبيباتني بثينة، **الجرائم المتصلة بتكنولوجيات الإعلام والإتصال**، أطروحة الدكتوراه ل.م.د، تخصص: قانون جنائي وعلم الإجرام، كلية الحقوق، جامعة الجزائر1، 2020، ص 213.

[2]- بلحسيني حمزة، **الحماية الجزائية للمستند الإلكتروني**، أطروحة الدكتوراه علوم، تخصص: علوم قانونية فرع: قانون البنوك، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، 2019-2020، ص 23.

[3]- بوكر رشيدة، مرجع سابق، ص 136.

[4]- منصارة يوسف، مرجع سابق، ص 236.

[5]- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996 مع المادة 5 مكرراً الإضافية بصيغتها المعتمدة في عام 1998، الصادر عن هيئة الأمم المتحدة في جلستها 605 المنعقدة في 16 ديسمبر 1996.

[6]- جاء في الفقرة الأولى من المادة 11 من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية السالف الذكر أن هذه الوسائل هي وسيلة تعبير عن العرض والقبول، إذ نصت على أن: "في سياق تكوين العقود، وما لم يتفق الطرفان على غير ذلك يجوز إستخدام رسائل البيانات للتعبير عن العرض وقبول العرض، وعند إستخدام رسالة بيانات في تكوين العقد لا يفقد ذلك العقد صحته أو قابليته للتنفيذ لمجرد إستخدام رسالة بيانات لذلك الغرض".

ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي"[1]، وعرف تبادل البيانات الإلكترونية في الفقرة (ب) من نفس المادة كالآتي: "يراد بمصطلح "تبادل البيانات الإلكترونية": نقل المعلومات إلكترونيًا من حاسوب إلى حاسوب آخر، بإستخدام معيار متفق عليه لتكوين المعلومات"[2].

لقد تم إعتماد مصطلح "رسالة البيانات" نظرًا لإختلاف البيئة التي يتم فيها تداول هذا المستند، حيث يتعلق الأمر ببيئة رقمية تعتمد في تعاملها على الوسائل الإلكترونية أو الضوئية أو غيرها من الوسائل المشابهة، ولم يقم بحصر هذه الوسائل إقرارًا منه بإمكانية ظهور تقنيات جديدة نتيجة التطور المستمر في المجال التكنولوجي.

3- التعريف التشريعي للمستند الإلكتروني:

سنتطرق إلى تعريف المستند الإلكتروني في مختلف التشريعات المقارنة، ثم نتطرق إلى تعريفه وفقًا لما ورد في التشريع الجزائري.

3-1- تعريف المستند الإلكتروني في التشريعات المقارنة:

يعد قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المؤرخ بتاريخ 21 أفريل 2004[3] تشريع مستقل وخاص لتنظيم المعاملات الإلكترونية في مصر، وإن كان بالإمكان إعتبار نصوصه تعديلًا للنصوص المتعلقة بالكتابة في قانون الإثبات المصري، إلا أنه فقد أضفى على المستندات الإلكترونية في نطاق المعاملات المدنية والإدارية والتجارية ذات الأهمية المقررة للكتابة التقليدية إذا ما توافرت على الشروط المنصوص عليها في القانون السالف الذكر، والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية[4] لهذا القانون الصادرة عن وزارة

[1]-Art 02 paragraphe a du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: « Le terme "message de données" désigne l'information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie ».

[2]-Art 02 paragraphe b du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: « Le terme "échange de données informatisées (EDI)" désigne le transfert électronique d'une information d'ordinateur à ordinateur mettant en œuvre une norme convenue pour structurer l'information ».

[3]- قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004، المتضمن التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المؤرخ بتاريخ 21 أفريل 2004، ج.ر.ج.م.ع العدد 17 تابع (د)، الصادر بتاريخ 22 أفريل 2004.

[4]- اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، الصادرة عن وزارة الإتصالات وتكنولوجيا المعلومات بموجب القرار رقم: 109 لسنة 2005 المؤرخ في 15 ماي 2005، جريدة الوقائع المصرية العدد 115 (تابع)، الصادر بتاريخ 25 ماي 2005، المعدلة بموجب القرار رقم: 361 لسنة 2020 المؤرخ في 19 أفريل 2020، جريدة الوقائع المصرية العدد 95 (تابع)، الصادر بتاريخ 23 أفريل 2020.

الإتصالات وتكنولوجيا المعلومات بموجب القرار رقم: 109 لسنة 2005 المؤرخ بتاريخ 15 ماي 2005، المعدلة بموجب القرار رقم: 361 لسنة 2020 المؤرخ بتاريخ 19 أفريل 2020.[1]

فقد إستخدم المشرع المصري في قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر مصطلح محرر إلكتروني للدلالة على المستند الإلكتروني، وعرفه في الفقرة (ب) من المادة الأولى منه كالآتي: "رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليًا أو جزئيًا، بوسيلة إلكترونية أو رقمية أو ضوئية أو أي وسيلة أخرى مشابهة"، وهو نفس التعريف الوارد في اللائحة التنفيذية لهذا القانون بموجب الفقرة 03 من المادة الأولى منها.

أما المشرع الفرنسي فلم ينظم مسألة المستندات الإلكترونية في القانون المدني ولم يقم بوضع تعريف خاص بها بل إكتفى بالتوسع في مفهوم الكتابة والإثبات بالكتابة سواء كان المستند رسمي أو عرفي أو إداري، بمقتضى تعديله للقانون المدني بموجب القانون رقم: 2000-230 المؤرخ في 13 مارس 2000 المتعلق بتكييف قواعد الإثبات مع تكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني[2] في المادة 1316 التي نصت على أن:" ينشأ الإثبات الخطي أو الإثبات الكتابي نتيجة من تسلسل حروف أو علامات أو أرقام أو أي رمز أو أي إشارة أخرى، ذات دلالة تعبيرية واضحة ومفهومة، أيا كانت الدعامة التي تتضمنها، أو الوسيط الذي تنتقل عبره"[3]، وبموجب التعديلات الجذرية للقانون المدني الفرنسي التي جاء بها الأمر رقم: 2016-131 المؤرخ في 10 فيفري 2016 المتعلق بإصلاح قانون العقود والنظام العام وإثبات الإلتزامات، الذي دخل حيز التنفيذ بتاريخ 01 أكتوبر 2016[4] ألغى المادة السابقة الذكر وإحتفظ بنفس المضمون في المادة 1365 من ق.م.ف[5].

ويعتبر التشريع الفرنسي الخاص بالتوقيع الإلكتروني إستجابة لتوجيهات الأمم المتحدة، حيث نبهت دول العالم المختلفة إلى ضرورة إصدار تشريعات وطنية تنظم التجارة الإلكترونية وتعترف بحجية التوقيع الإلكتروني، وقد شكلت لذلك لجنة سنة 1996 لإعداد نموذج لقانون

[1]- سحر سعد عبد السميع محمد، **الحماية الجنائية للتوقيع الإلكتروني**، د.ر.ط، 2022، دار الفكر والقانون، مصر، ص86.

[2]-Loi n°2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J.O.R.F numéro 62, 14 mars 2000.

[3]-Art 1316 du C.C.F (Modifié par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000, Abrogé par Ordonnance n°2016-131 du 10 février 2016) dispose que : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission».

[4]-Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

[5]-Art 1365 du C.C.F (Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations- art.4) dispose que: « L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support».

ينظم التجارة الإلكترونية وإنتهت هذه اللجنة من عملها سنة 1998، وأصدرت قانونًا ينظم التجارة الإلكترونية وأصدرته لجنة الأمم المتحدة للتجارة الدولية (CNUDCI).[1]

3-2- تعريف المستند الإلكتروني في التشريع الجزائري:

حذا المشرع الجزائري خطى المشرع الفرنسي بالتوسع في مفهوم الإثبات بالكتابة بدون وضع تعريف للمستند الإلكتروني، وذلك بموجب التعديل الذي أجراه على القانون المدني بموجب القانون رقم: 05-10 المؤرخ في 20 جوان 2005[2]، وأضاف المادة 323 مكرر التي نصت على أن: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز، ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها".

إلا أنه تدارك الأمر بموجب القانون رقم: 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير وإستعمال المزور[3] وإستخدم مصطلح محرر للدلالة على المستند ووسع نطاق تعريفه ليشمل كلا من المحررات الورقية والإلكترونية بموجب المادة 02 منه كالآتي: "المحرر: كل مكتوب ورقي أو إلكتروني، يسمح بمعرفة الشخص الذي صدر عنه، ويتضمن ذكر واقعة أو تعبير عن الإرادة من شأنه إنشاء مركز قانوني أو تعديله أو إنهائه أو إثباته، سواء أعد المحرر لذلك أساسًا أو ترتب عليه هذا الأثر بقوة القانون".

وفي نفس المادة ميز بين المحرر العرفي والرسمي وعرفهم كالآتي: "المحرر الرسمي: كل محرر يثبت فيه موظف أو ضابط عمومي أو شخص مكلف بخدمة عامة، ما تم لديه أو ما تلقاه من ذوي الشأن طبقًا للأشكال القانونية وفي حدود سلطته وإختصاصه، وكل محرر يعطيه القانون هذا الشكل"، أما المحرر العرفي فقد عرفه كالآتي: "كل محرر صادر ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه، وفقًا للشروط المحددة في التشريع الساري المفعول"، وهو نفس التعريف المنصوص عليه في الفقرة الأولى من المادة 327 من ق.م.ج التي تنص على أن: " يعتبر العقد العرفي صادرًا ممن كتبه أو وقعه أو وضع عليه بصمة أصبعه، ما لم ينكر صراحة ما هو منسوب إليه"، وعليه فإن المحرر العرفي الإلكتروني يعتبر حجة على من صدرمنه، وهو الشخص الذي وقعه إلكترونيًا.

لقد إتجه المشرع الجزائري إلى توسيع من نطاق تعريف المستند ليشمل كلا من المستندات الورقية والإلكترونية مع تحديد تعريف قانوني واضح لهذا الأخير، وذلك على خلاف بعض التشريعات المقارنة التي إكتفت بالإشارة إلى أن مضمون المستند الإلكتروني لا يدرك إلا

[1]- سعد عاطف عبد المطلب حسنين، **الحماية الجنائية للمصنفات الرقمية دراسة مقارنة**، الطبعة الأولى، 2018، دار الفكر الجامعي، الإسكندرية-مصر، ص 532.

[2]- القانون رقم: 05-10 المؤرخ في 20 جوان 2005، المعدل والمتمم للأمر رقم: 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، ج.ر.ج.ج.ش العدد 44، الصادرة في 26 جوان 2005.

[3]- القانون رقم: 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير وإستعمال المزور، ج.ر.ج.ج.ش العدد 15، الصادرة في 29 فيفري 2024.

بواسطة الوسائل الإلكترونية التي تتيح قراءته، دون أن تقدم تعريفًا دقيقًا أو شاملًا له مما أضفى نوعًا من الغموض على طبيعته القانونية.

ثانيًا: خصائص المستند الإلكتروني

من خلال دراسة مختلف التعاريف للمستند الإلكتروني يتضح لنا أنه يتميز بعدة خصائص وهي كما يلي:

أ- أداة للتفاهم وتبادل الأفكار بين الأفراد؛

ب- أن يكون ذو قيمة قانونية يمكن التعويل عليها عند المعاملات بين الأفراد والمؤسسات والحكومات؛

ت- يحمل هذا المستند الصفة الإلكترونية، بما يعني أن العمليات التي تتم -كتابته أو تخزينه أو إسترجاعه أو نقله أو نسخه- متصلة بتقنية تكنولوجية إلكترونية؛

ث- يمكن أن يتم تداول هذا المستند ونقله من جهاز إلكتروني لآخر؛

ج- يحمل المستند الإلكتروني ما دام مخزنًا داخل الوسيط الإلكتروني، إذ يحمل طابعًا معنويًا يسمح بإفتراض وجوده قانونًا رغم غياب الشكل المادي؛

ح- يتم إرسال هذا المستند عبر الشبكات والأجهزة الإلكترونية من جهاز لآخر، عن طريق تحويله إلى رموز أو نبضات ثم تحويله إلى كلمات مفهومة عن طريق بروتوكولات التعامل عبر الأجهزة الإلكترونية؛

خ- يمكن إرسال هذا المستند وإستقباله إلى أي مكان في العالم عبر شبكات الإنترنت.[1]

ثالثًا: التميز المستند الإلكتروني عن المستند التقليدي

رغم التشابه بين المستند الإلكتروني والمستند الورقي في إحتواء على حقيقة يريد المشرع حمايتها، وأن كل واحد منهما يتضمن على مجموعة من الرموز التي تعبر عن مجموعة مترابطة من الأفكار، ويتماثل كل واحد منهما في إنطواء على فكرة الضرر التي هي علة تجريم المساس بهما، فإن بينهما فوارق يمكن أن نستخلصها من العناصر الأساسية التي يقوم عليها المستند التقليدي، وهي: الدعامة، الكتابة، التوقيع.[2]

1- من حيث الدعامة:

المستند الورقي يعد من الأشياء المادية الملموسة، إلا أن المستند الإلكتروني ذو طابع معنوي ولا يمكن إعتباره ماديًا ما لم يتم إستخراجه من الأجهزة الإلكترونية بصورة ورقية.[3]

[1]- مثنى سعد السوداني، مرجع سابق، ص-ص 62-63.
[2]- بوكر رشيدة، مرجع سابق، ص 147.
[3]- مثنى سعد السوداني، مرجع سابق، ص 66.

فالكتابة الواردة في المستند التقليدي ترد دائمًا على دعامة تتصف بالطابع الملموس كالأوراق أو ما شابهها، كما تتميز بقدر كبير من الثبات إذ يصعب تعديلها دون ترك أثر مادي واضح لهذا التعديل، أما بالنسبة للمستند الإلكتروني فيرد على دعامة إلكترونية تمتاز في الغالب الأعم بسهولة إدخال التعديلات أو إجراء التغييرات على المعطيات المدونة عليها.[1]

وبما أن المستند موجود على الدعامة الإلكترونية ويستلزم وسيطًا إلكترونيًا لفحص محتواه ولقراءته، بناءً على ذلك فلا يمكن تحميله ونقله من جهاز إلكتروني لآخر إلا بواسطة الدعامة الإلكترونية، كما تسمح هذه الأخيرة بإرساله عبر الشبكات والأجهزة الإلكترونية عن طريق تحويله إلى نبضات أو رموز، ثم تحويله إلى كلمات مفهومة بواسطة بروتوكولات التعامل عبر الأجهزة الإلكترونية.[2]

2- من حيث الكتابة:

يمكن الإطلاع على محتوى المستند الورقي بمجرد النظر إليه، بينما يلزم للإطلاع على المستند الإلكتروني وضعه في وسيط إلكتروني لقراءته وفك رموز شفراته.[3]

فالكتابة التقليدية المتواجدة في الكيان المادي المرئي يسهل قراءتها بالعين المجردة كما أنها ترتبط بمحرر المستند وتعكس شخصيته، وبالتالي يمكن إحالتها إلى خبير مختص لمعرفة مدى صحة نسبتها إليه، في حين أن الكتابة الإلكترونية تتكون من نبضات إلكترونية لا يمكن الإطلاع على محتواها إلا بواسطة إستخدام وسيط إلكتروني، فهي كتابة قابلة للقراءة ولكنها غير ظاهرة للعين المجردة بشكل مباشر كما أنها لا تختلف في حروفها بحسب من قام بكتابتها.[4]

ويمكن تحديد شخصية من قام بتحرير المستند الورقي بمضاهاة خطه بالكتابة الموجودة في المستند، أما المستند الإلكتروني فيتم الكتابة فيه بواسطة المكونات المادية للأجهزة الإلكترونية ومن ثم لا يمكن معرفة من قام بتحريره.[5]

3- من حيث التوقيع:

لا يقتصر التوقيع الإلكتروني على بصمة الأصابع أو الإمضاء كما في التوقيع التقليدي بل يشمل على عناصر متفردة وسمات خاصة بالموقع، تتخذ شكل الحروف والأرقام والصور والأصوات والرموز والإشارات وغيرها من النماذج، بشرط أن تكون ذات طابع فردي[6] يحدد هوية صاحبه ويؤكد إرادته في إنفاذ التصرف القانوني.

---

[1]- بوكر رشيدة، مرجع سابق، ص-ص 147-148.

[2]- بلحسيني حمزة، مرجع سابق، ص 30.

[3]- مثنى سعد السوداني، مرجع سابق، ص 67.

[4]- بوكر رشيدة، مرجع سابق، ص 148.

[5]- مثنى سعد السوداني، مرجع سابق، ص 67.

[6]- بن شهرة شول، بوشارب هانية، **الضوابط القانونية لقبول الإثبات بالكتابة في الشكل الإلكتروني التوقيع الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني،=

الفرع الثاني: عناصر المستند الإلكتروني

فرض التطور التكنولوجي ضرورة إستحداث تقنيات تتلاءم مع العناصر الأساسية للمستند الإلكتروني المتمثلة في عنصري الكتابة والتوقيع، إذ لا يتصور إستمرار إعتماد الأشكال التقليدية لهذين العنصرين في البيئة الرقمية، وهو ما دفع بالمشرع الجزائري إلى التدخل لتنظيم هذه المسألة بما ينسجم مع طبيعة المستندات الإلكترونية.

أولًا: الكتابة الإلكترونية

لبيان المقصود بالكتابة الإلكترونية ارتأينا إستعراض تعريفها على المستوى الفقهي، ثم التطرق إلى التعريف الوارد في النصوص التشريعية.

1- التعريف الفقهي للكتابة الإلكترونية:

عرفت الكتابة الإلكترونية بأنها: "معلومات ذات خصائص إلكترونية، في شكل نصوص أو رسوم أو صور أو أصوات أو رموز أو برامج معلوماتية أو غيرها من قواعد البيانات"[1]، وعرفها البعض بأنها: "أية معلومة صممت أو حررت أو خزنت أو أرسلت أو إستلمت أو إسترجعت بطريقة إلكترونية، بغض النظر عن المادة المحفوظة عليها، على أن تكون ذات معنى مفهوم، وتقبل الحفظ والإسترجاع ويمكن قراءتها بأية وسيلة كانت"، وعرفها البعض الآخر: "بأنها كل حروف أو أرقام أو أي علامات أخرى، تثبت على دعامة إلكترونية أو ضوئية أو أية وسيلة مشابهة"[2]، كما عرفت على أنها: "الكتابة التي تتم عبر وسيط إلكتروني مؤتمن"[3].

2-التعريف الدولي للكتابة الإلكترونية:

لم يورد قانون الأونسيترال النموذجي المتعلق بالتجارة الإلكترونية تعريفًا صريحًا للكتابة الإلكترونية وإنما ربط تعريفها بتعريف البيانات الإلكترونية بموجب الفقرة الأولى من المادة 06 منه الذي ينص على أن: "عندما يشترط القانون أن تكون المعلومات مكتوبة، تستوفي رسالة

=الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 169.

[1]- ندى حمزة صاحب، **الحجية القانونية للمستندات الإلكترونية وطرق الطعن فيها (دراسة مقارنة)**، كلية الأداب/ جامعة واسط، مجلة لارك للفلسفة واللسانيات والعلوم الإجتماعية، المجلد 08، العدد02، 2016، العراق، ص 297.

[2]- شيخ سناء، **أدلة الإثبات المكتوبة التقليدية والإلكترونية في القانون الجزائري**، د.ر.ط، 2021، النشر الجامعي الجديد، تلمسان -الجزائر، ص 114.

[3]- زياني فيصل، زياني منير، **الحجية القانونية للإثبات بالكتابة في الشكل الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 136.

البيانات ذلك الشرط إذا تيسر الإطلاع على البيانات الواردة فيها على نحو يتيح إستخدامها بالرجوع إليه لاحقًا".[1]

وبالرجوع إلى الفقرة (أ) من المادة 02 من نفس القانون نجده يعرف رسالة بيانات بأنها:"رسالة بيانات": المعلومات التي يتم إنشاؤها أو إرسالها أو إستلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل المعطيات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي"[2]، وهو نفس التعريف الذي تبناه القانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية بموجب الفقرة (ج) من المادة 02 منه.

3-التعريف التشريعي للكتابة الإلكترونية:

سنتطرق إلى تعريف الكتابة الإلكتروني في مختلف التشريعات المقارنة، ثم نتطرق إلى تعريفها وفقًا لما ورد في التشريع الجزائري.

أ-تعريف الكتابة الإلكترونية في التشريعات المقارنة:

عرف المشرع المصري الكتابة الإلكترونية في الفقرة (أ) من المادة الأولى من قانون التوقيع الإلكتروني المصري رقم: 15 لعام 2004 المتضمن التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر كالآتي: "كل حروف أو أرقام أو رموز أو أي علامات أخرى، تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة، وتعطى دلالة قابلة للإدراك".

وعرفها المشرع الفرنسي بموجب المادة 1316 من ق.م.ف المعدلة بالقانون رقم: 2000-230 الصادر في 13 مارس 2000 المتعلق بتكييف قواعد الإثبات مع تكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني السالف الذكر كالآتي: "ينشأ الإثبات الخطي أو الإثبات الكتابي نتيجة من تسلسل حروف أو علامات أو أرقام أو أي رمز أو أي إشارة أخرى، ذات دلالة تعبيرية واضحة ومفهومة، أيا كانت الدعامة التي تتضمنها، أو الوسيط الذي تنتقل عبره"[3]، وألغيت هذه المادة بموجب الأمر رقم: 2016-131 المتعلق بإصلاح قانون العقود والنظام العام

[1]-Art 06 paragraphe 01 du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: « Lorsque la loi exige qu'une information soit sous forme écrite, un messge de données satisfait à cette exigence si l'information qu'il contient est accessible pour être consultée ultérieurement».

[2]-Art 02 paragraphe a du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: « Le terme "message de données" désigne l'information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie».

[3]-Art 1316 du C.C.F (Modifié par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000, Abrogé par Ordonnance n°2016-131 du 10 février 2016) dispose que: « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission».

وإثبات الإلتزامات السالف الذكر وعوضت بالمادة 1365 من ق.م.ف التي جاءت صياغتها كالآتي: "الكتابة هي نتيجة تسلسل من الأحرف أو علامات أو أرقام أو أي رمز أو أي إشارة أخرى، ذات دلالة تعبيرية واضحة ومفهومة، أيا كانت الدعامة التي تتضمنها"[1].

ب-تعريف الكتابة الإلكترونية في التشريع الجزائري:

أما بالنسبة لموقف المشرع الجزائري فقد عرف الكتابة الإلكترونية بموجب المادة 323 مكرر من القانون المدني المعدل والمتمم بالقانون رقم: 05-10 السالف الذكر كالآتي: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف[2] أو أرقام أو أية علامات أو رموز، ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها"، لم يكتف بالكتابة التقليدية على أنها مجموعة حروف وإنما أضاف إلى ذلك كل ما يؤدي إلى معنى متفق عليه بين الأطراف من أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، كما أضاف بأي وسيلة كانت ومهما كانت طريقة إرسالها بمعنى الوسائل والتي تتضمن المستندات الإلكترونية بمفهومها المجرد، ويقصد بها المعلومات والمعطيات التي تحتوي عليها أي دعامة أو تلك التي يتم كتابتها بواسطة الجهاز الإلكتروني وإرسالها ونشرها على شبكة الإنترنت.[3]

يتضح مما سبق أن كلا من المشرع الفرنسي والجزائري لم يركزا على الشكل التقليدي أو الإلكتروني للكتابة، بل إنصب إهتمامهما على مدى وضوحها وإمكانية قراءتها مما يعكس تبنيهما لمفهوم الواسع للكتابة، كما ترك المشرعان المجال مفتوحًا لإستخدام مختلف أنواع الدعامات تحسبًا لما قد تستحدثه التكنولوجيا من وسائل جديدة.

ثانيًا: التوقيع الإلكتروني

نتيجة للتطور المتسارع في وسائل الإتصال الحديثة والإنتشار الواسع لإستخدام شبكة الإنترنت في إبرام العقود، شهد التعامل القانوني إنتقالًا من الشكل الورقي التقليدي إلى الشكل الإلكتروني، وقد ترتب على هذا التحول بروز حاجة ملحة إلى ضرورة إيجاد بديل عن التوقيع التقليدي يحقق ذات الوظائف القانونية، ومن هنا أدى إلى تطور وظهور شكلًا جديدًا للتوقيع

[1]-Art 1365 du C.C.F (Ordonnance n°2016-131 du 10 février 2016 -art.4) dispose que: « L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support».

[2]- يأخذ البعض على المشرع الجزائري إستعماله لمصطلح أوصاف على أساس أن الوصف هو الصفة تضفى على أمر آخر فكيف يشكل تسلسل أوصاف محررًا إلكترونيًا، إلا أنه في مجال التعاقدات الإلكترونية فإن إرسال إيماءات أو إشارات تعني أحيانا القبول، وهناك إشارات على مواقع الواب في شكل وجه مستدير مبتسم تعني القبول أما غير المبتسم فتعني الرفض، ونعتقد أن مصطلح "أوصاف" هو المقابل لمصطلح "إشارات" في نص المادة 1365 من القانون الفرنسي، أما العلامات والرموز فهي الناتجة عن تحويل الكتابة العادية من قبل الإنسان إلى علامات ورموز بلغة الآلة، كالمعلومات المخزنة في الحاسوب بلغته، وللمزيد من التفصيل، ينظر: طنجاوي مراد، **مدى حجية المحررات الإلكترونية في الإثبات المدني**، أطروحة الدكتوراه علوم، قسم: القانون الخاص، كلية الحقوق، الجزائر1، 2017/2016، ص 236.

[3]- منصارة يوسف، مرجع سابق، ص 242.

الذي يتلاءم مع طبيعة المعاملات الإلكترونية، الأمر الذي دفع غالبية التشريعات إلى التدخل لتنظيمه ووضع الضواط القانونية التي تحكم إستخدامه.

1- تعريف التوقيع الإلكتروني:

إرتأينا التطرق إلى تعريف التوقيع الإلكتروني على المستوى الفقهي والدولي والتشريعي، وذلك بهدف الإلمام بمختلف التصورات التي تناولت هذا المفهوم القانوني.

أ- تعريف التوقيع الإلكتروني على المستوى الفقهي:

عرف التوقيع الإلكتروني بأنه: "بيان مكتوب في شكل إلكتروني يتمثل في حرف أو رقم أو رمز أو إشارة أو صوت أوشفرة خاصة ومميزة ينتج من إتباع وسيلة آمنة، وهذا البيان يلحق أو يرتبط منطقيًا ببيانات المستند الإلكتروني للدلالة على هوية الموقع ورضائه بمضمون المستند"[1]، وعرف أيضًا على أنه: "علامة شخصية يضعها الموقع بإسمه، ليؤكد صحة مضمون الورقة وصدق ما تم كتابته بها، وإقراره بتحمل مسؤولية ما ورد فيها"[2]، وعرف أيضًا بأنه: "بيانات مدرجة في تعامل إلكتروني أو مضافة إليه أو مرتبطة به منطقيًا، تستخدم لإثبات هوية الموقع وموافقته على التعامل الإلكتروني وإكتشاف أي تعديل يطرأ على هذا التعامل بعد التوقيع عليه"[3].

ويرى البعض الآخر بأنه: "إجراء معين يقوم به الشخص المراد توقيعه على المحرر، سواء أكان هذا الإجراء على شكل رقم أو إشارة إلكترونية معينة أو شفرة خاصة، بحيث يحتفظ بالرقم أو الشفرة في مكان آمن وسري يمنع إستعماله من قبل الغير ويعطى الثقة بأنه صدر من صاحبه حامل الرقم أو الشفرة".[4]

---

[1]- عبد الرازق وهبه سيد أحمد محمد سيد، **حجية التوقيع الإلكتروني في الإثبات"دراسة تحليلية مقارنة"**،أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 33.

[2]- بن عيسى فتيحة، المر سهام، **التوقيع الإلكتروني ومدى حجيته في العقد التجاري الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 180.

[3]- محده جلول، ورخ نور الدين، **القوة القانونية للإثبات بالتوقيع الإلكتروني في المسائل القانونية**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 258.

[4]- سحر سعد عبد السميع محمد، مرجع سابق، ص 46.

ب- تعريف التوقيع الإلكتروني على المستوى الدولي:

تعتبر لجنة القانون التجاري الدولي التابعة لهيئة الأمم المتحدة أول منظمة التي إعتمدت على التوقيع الإلكتروني كآلية في تحقيق عنصري الثقة والأمان في المعاملات الإلكترونية طبقًا للفقرة الأولى من المادة 07 من القانون النموذجي بشأن التجارة الإلكترونية سنة 1996، وذلك من خلال إعترافها به ضمنيًا وأكتفت فقط بتحديد الشروط الواجب توافرها فيه كالآتي:

1- عندما يشترط القانون وجود توقيع شخص معين، فإن هذا الشرط يعد مستوفى في حالة وجود رسالة البيانات إذا:

أ- إذا استخدمت وسيلة تهدف إلى تحديد هوية الشخص المعني، وللدلالة على موافقته على المعلومات الواردة في رسالة البيانات؛

ب- وتعد الطريقة معتمدة إذا كانت موثوقيتها كافية بالنسبة للغرض الذي أنشئت من أجله رسالة البيانات أو تم تبليغها بموجبه، مع مراعاة كل الظروف بما في ذلك أي إتفاق متعلق بذلك.[1]

إلا أن بتاريخ 05 جويلية 2001 تبنته صراحة بعد إصدارها لقانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية[2] تصدت من خلاله لتعريفه والقواعد الخاصة به وكيفية إستخدامه بمساعدة من لجنة للدول في وضع قواعد خاصة بالتوقيع الإلكتروني، وقد عرفته بموجب الفقرة (أ) من المادة 02 كالآتي: "توقيع إلكتروني: يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيًا، يجوز أن تستخدم لتعين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[3].

إهتم قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية بتعيين هوية الشخص الموقع وبيان موافقته الصريحة على المعلومات الواردة في المستند وذلك للدلالة على شخص الموقع وللتأكيد على إرادته الحرة في الإلتزام بما وقع عليه، ويلاحظ أنه لم يقم بتحديد صور التوقيع

[1]- Art 07 paragraphe 01 du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: « Signature:
1. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données :
a) Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données; et
b) Si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière».

[2]- القانون النموذجي بشأن التوقيعات الإلكترونية الصادر عن لجنة الأمم المتحدة لقانون التجارة الدولية الأونسيترال سنة 2001.

[3]-Art 02 paragraphe a du Loi type de la CNUDCI sur les signatures électroniques 2001 dispose que: «Le terme "signature électronique" désigne des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue ».

الإلكتروني تاركًا ذلك للدول في إصدار التشريعات الخاصة بها في تحديد أنواع التوقيع الإلكتروني وكيفية إستخدامه للدلالة على شخصية الموقع وإلتزامه بما وارد في المستند الإلكتروني.

وموازاة مع جهود الأمم المتحدة تولى مشرع الإتحاد الأوروبي بتبني التوقيع الإلكتروني كوسيلة إثبات بموجب التوجيه الأوروبي رقم: 1999-93 المتعلق بشأن إرساء إطار قانوني مشترك لإستخدام التوقيع الإلكتروني الصادر بتاريخ 13 ديسمبر1999[1]، لحث الدول الأعضاء على الإعتراف بالتوقيع الإلكتروني مثله مثل التوقيع التقليدي وجعله كوسيلة إثبات مقبولة لدى القضاء.[2]

عرف التوجيه الأوروبي رقم: 1999-93 المشار إليه أعلاه في المادة 02 منه التوقيع الإلكتروني، كما ميز بين نوعين من التوقيع الإلكتروني الأول التوقيع الإلكتروني البسيط عرفه بموجب الفقرة الأولى من ذات المادة كالآتي: "بيانات في شكل إلكتروني تتصل أو ترتبط إرتباطًا وثيقًا ببيانات إلكترونية أخرى، وتستخدم كوسيلة للتوثيق"[3]، أما التوقيع الإلكتروني المتقدم فلم يعرفه وإنما ذكر الشروط التي يجب توافرها فيه لكي يتصف بأنه التوقيع الإلكتروني متقدم وذلك بموجب الفقرة الثانية من نفس المادة كالآتي:

1- أن يرتبط وبشكل منفرد بصاحب التوقيع؛
2- أن يتيح كشف هوية صاحب التوقيع؛
3- أن ينشأ من خلال وسائل موضوعة تحت رقابة صاحب التوقيع؛
4- أن يكون مرتبطًا بالبيانات التي وضع عليها التوقيع، على نحو أن أي تعديل لاحق للبيانات يمكن كشفه".[4]

إلا أنه ألغي التوجيه الأوروبي رقم: 1999-93 المشار إليه أعلاه بموجب اللائحة رقم: 2014-910 المؤرخة في 23 جويلية 2014 الصادرة عن البرلمان الأوروبي والمجلس

---

[1]-Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, j.o nº l013 du 19-01-2000, Abrogé.
https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31999L0093

[2]- أزرو محمد رضا، **إشكالية إثبات العقود الالكترونية دراسة مقارنة**، أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد-تلمسان، 2015-2016، ص189.

[3]-Art 02 paragraphe 01 du La directive 1999/93/CE du PEC, op. cit, dispose que: « signature électronique ،une donnée sous forme électronique ،qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification».

[4]-Art 02 paragraphe 02 du La directive 1999/93/CE du PEC, op. cit, dispose que: « signature électronique avancée" une signature électronique qui satisfait aux exigences suivantes:
a être liée uniquement au signataire;
b permettre d'identifier le signataire;
c être créée par des moyens que le signataire puisse garder sous son contrôle exclusif
d être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable».

الأوروبي المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية[1]، وقد عرف التوقيع الإلكتروني البسيط بموجب الفقرة 10 من المادة 03 والتي جاءت صياغتها كالآتي: "البيانات في الشكل الإلكتروني مضافة أو مرتبطة منطقيًا ببيانات أخرى في شكل إلكتروني، والتي يستخدمها الموقع للتوقيع"[2]، أما التوقيع الإلكتروني الموصوف فقد أورد له تعريف وعرفه بموجب الفقرة 12 من نفس المادة كالآتي: "التوقيع الإلكتروني المتقدم الذي يتم إنشاؤه بإستخدام جهاز إنشاء توقيع الإلكتروني، وأن ينشأ على أساس شهادة تصديق إلكتروني موصوفة"[3]، وفي الفقرة 11 من نفس المادة أحالتنا إلى المادة 26 التي حددت هذه الأخيرة الشروط الواجب توافرها في التوقيع الإلكتروني حتى يكتسي وصف الموصوف[4]، وبالرجوع إلى المادة 26 نجدها حددت الشروط المتطلبة كالآتي:

أ- أن يرتبط بالموقع إرتباطًا فريدًا؛

ب-يمكن تحديد هوية الموقع؛

ت-أن يكون التوقيع قد تم إنشاؤه بإستخدام بيانات إنشاء التوقيع الإلكتروني، التي يمكن للموقع استخدامها بدرجة عالية من الثقة وتحت سيطرته الحصرية؛

ث-أن يكون مرتبطًا بالبيانات المرتبطة بهذا التوقيع، بطريقة يمكن من خلالها الكشف عن أي تغييرات لاحقة في البيانات.[5]

ألزم أن يتم إنشاء التوقيع الإلكتروني الموصوف بإستخدام جهاز إنشاء توقيع الإلكتروني وأن ينشأ على أساس شهادة تصديق إلكتروني موصوفة وأن تتوفر فيه مجموعة من الشروط

---

[1]-RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, et abrogeant la directive 1999/93/CE.
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910

[2]-Art 03 paragraphe 10 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: «signature électronique, des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer».

[3]-Art 03 paragraphe 12 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: «signature électronique qualifiée, une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique».

[4]-Art 03 paragraphe 11 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: «signature électronique avancée», une signature électronique qui satisfait aux exigences énoncées à l'article 26».

[5]-Art 26 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: « Une signature électronique avancée satisfait aux exigences suivantes:
a être liée au signataire de manière univoque;
b permettre d'identifier le signataire;
c avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif;
d être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable».

الخاصة، بهدف تحقيق المساواة القانونية بينه وبين التوقيع التقليدي، ولضمان بث الثقة والأمان في المعاملات الإلكترونية والتي لا تعتبر مطلوبة في التوقيع الإلكتروني البسيط.

وأضافت الفقرة 02 من المادة 25 منه على أن: "الأثر القانوني للتوقيع الإلكتروني الموصوف يعادل الآثر القانوني للتوقيع بخط اليد".[1]

ج- تعريف التوقيع الإلكتروني على المستوى التشريعي:

سنتطرق إلى تعريف التوقيع الإلكتروني في مختلف التشريعات المقارنة، ثم نتطرق إلى تعريفه وفقًا لما ورد في التشريع الجزائري.

ج-1- تعريف التوقيع الإلكتروني في التشريعات المقارنة:

نتيجة للتطور الحاصل في المعاملات الإلكترونية في فرنسا وإستجباتها لمقتضيات التوجيه الأوروبي بشأن التجارة الإلكترونية حتم عليها إدخال تعديلات على الأحكام الخاصة بالإثبات في القانون المدني، بإستحداث فصل جديد ضمن الباب الثالث من الكتاب الثالث من قانون المدني بعنوان: "العقود والإلتزامات في الشكل الإلكتروني" بموجب القانون رقم: 2000-230 الصادر في 13 مارس 2000 المتعلق بتكييف قواعد الإثبات مع تكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني السالف الذكر وأورد التوقيع التقليدي والتوقيع الإلكتروني في الفقرة الأولى من المادة 1316-4 منه، والتي نصت على ما يلي :" التوقيع ضروري لإتمام التصرف القانوني، وهو يحدد هوية الشخص المنسوب إليه ويعبر عن رضا الأطراف بالإلتزامات التي تترتب عن هذا التصرف، وحينما يوضع التوقيع بواسطة موظف عام فإن هذا التوقيع يضفي على المستند الطابع الرسمي"[2]، إعتمد المشرع الفرنسي في الفقرة الأولى على تعريف التوقيع العادي وركز على تحديد وظائفه والمتمثلة في تحديد شخصية الموقع والتعبير عن إرادة هذا الموقع بتحمله للإلتزامات التي يولدها التصرف القانوني.

أما التوقيع الإلكتروني فقد نصت عليه الفقرة 02 من نفس المادة على أن: "وعندما يكون إلكترونيًا فيجب أن يتم بإستخدام وسيلة موثوق بها، لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقع عليه، وتفترض الموثوقية إلى أن يثبت خلاف ذلك عند إنشاء التوقيع الإلكتروني والتأكد من هوية الموقع وضمان سلامة العقد، ضمن الشروط المحددة بمرسوم

[1]-Art 25 paragraphe 02 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: «L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite».

[2]-Art 1316-4 paragraphe 01 du C.C.F (Création Loi n°2000-230 du 13 mars 2000 -art. 1 JORF 14 mars 2000, Abrogé par Ordonnance n°2016-131 du 10 février 2016 - art.4) dispose que: « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte».

صادر عن مجلس الدولة"[1]، جاء في الفقرة 02 من نفس المادة بالشروط التي تضفي المصداقية على التوقيع الإلكتروني، وهي وجوب أن يرتكزعلى الوسيلة موثوق بها لتحديد هوية الموقع وأن تضمن إرتباطه بالعقد المتعلق به وضمان سلامة العقد.

ليأتي بعد ذلك المرسوم رقم: 2001-272 المؤرخ في 30 مارس 2001 صادر لتطبيق أحكام المادة 1316-4 من القانون المدني والمتعلق بالتوقيع الإلكتروني[2]، وقد ميز بموجب الفقرة 02 من المادة الأولى منه بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المؤمن، حيث إشترط في هذا الأخير أن يستوفي مجموعة من المتطلبات الآتية:

- أن يكون خاص بالموقع دون غيره؛
- ينشأ بإستخدام وسائل تكون تحت التحكم الحصري للموقع؛
- أن يضمن إرتبطًا بالتصرف المرفق به، من شأنه الكشف عن أي تعديل لاحق يطرأ على ذلك التصرف.[3]

وبموجب التعديلات الجذرية للقانون المدني الفرنسي التي جاء بها الأمر رقم: 2016-131 المتعلق بإصلاح قانون العقود والنظام العام وإثبات الإلتزامات السالف الذكر ألغيت المادة 1316-4 المضافة بالقانون رقم: 2000-230 المتعلق بتكييف قواعد الإثبات مع تكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني السالف الذكر واحتفظ بنفس المضمون في المادة 1367 من ق.م.ف[4].

وألغي المرسوم رقم: 2001-272 الصادر لتطبيق أحكام المادة 1316-4 من القانون المدني والمتعلق بالتوقيع الإلكتروني آنف ذكره بمقتضى المرسوم رقم: 2017-1416 المؤرخ

[1]-Art 1316-4 paragraphe 02 du C.C.F (Création Loi n°2000-230 du 13 mars 2000 -art. 1 JORF 14 mars 2000, Abrogé par Ordonnance n°2016-131 du 10 février 2016- art.4) dispose que: «Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat».

[2]-Décret n°2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, J.O. numéro 77 ,31 mars 2001, Modifié par Décret n°2016-1278 du 29 septembre 2016 - art. 1 V, Abrogé par Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique - art. 2 V.

[3]-Art 01 paragraphe 02 du Décret n°2001-272 du 30 mars 2001, Modifié par Décret n°2016-1278 du 29 septembre 2016-art. 1 V, Abrogé par Décret n°2017-1416 du 28 septembre 2017 -art. 02 V, dispose que: « Signature électronique sécurisée : une signature électronique qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable».

[4]-Art 1367 du C.C.F (Ordonnance n°2016-131 du 10 février 2016 - art. 4) dispose que: « La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat».

بتاريخ 28 سبتمبر 2017 المتعلق بالتوقيع الإلكتروني[1]، وأحال الأحكام المتعلقة بالتوقيع الإلكتروني والآلية الموصوفة لإنشاء التوقيع الإلكتروني وشهادة التوقيع الإلكتروني الموصوفة إلى أحكام اللائحة رقم: 910-2014 المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية السالفة الذكر في المادة الأولى منها والتي جاءت صياغتها كالآتي: "تفترض موثوقية في الوسيلة المستخدمة في إنشاء التوقيع الإلكتروني إلى أن يثبت خلاف ذلك، إذا كان يترتب على هذه الوسيلة إنشاء توقيع إلكتروني مؤهل. ويعد التوقيع الإلكتروني مؤهلًا اذا كان توقيعًا متقدمًا الذي يستجيب لشروط المادة 26 من اللائحة المذكورة أعلاه، والذي ينشأ بإستخدام آلية إنشاء التوقيع الإلكتروني مؤهلة يستوفي متطلبات المادة 29 من تلك اللائحة، ويعتمد على شهادة توقيع إلكتروني مؤهلة تستوفي متطلبات المادة 28 من هذه اللائحة"[2].

وعرف التوقيع الإلكتروني في القانون الفيدرالي للتوقيع الإلكتروني بأنه: "التوقيع الذي يصدر في شكل إلكتروني ويرتبط بسجل إلكتروني"، وعرف في قانون المعاملات الإلكترونية الموحد بأنه: "صوت أو رمز أو إجراء يقع في هيئة إلكترونية، يرتبط منطقيًا بعقد أو سجل آخر، ينفذ أو يصدر من شخص بقصد التوقيع على السجل".[3]

وعليه يمكن القول أن المشرع الفيدرالي قد وسع المجال أمام كل التقنيات الحديثة الموجودة أو التي ستظهر مستقبلًا التي تكون قادرة على تحقيق متطلبات التوقيع الإلكتروني، وإشترط أن يكون هذا الإجراء ملحقًا بالمستند الإلكتروني بالربط المنطقي بينهما بموجب لوغاريتمات ومعادلات وخوارزميات معينة، وعليه فإن هذا التعريف لم يركز على الوظائف المنوطة بالتوقيع عمومًا كما فعلت التشريعات اللاتينية، وإنما إعتمد على الجانب التقني أي كيفية العمل.[4]

وعرف المشرع المصري التوقيع الإلكتروني بموجب الفقرة (ج) من المادة الأولى من قانون التوقيع الإلكتروني المصري رقم: 15 لعام 2004 المتضمن التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر كالآتي: "التوقيع الإلكتروني: ما يوضع على محرر إلكتروني، ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، و يكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره"، وهو نفس التعريف الوارد في

[1]- Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique.

[2]-Art 01 du Décret n°2017-1416 du 28 septembre 2017 dispose que: «La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée. Est une signature électronique qualifiée une signature électronique avancée, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement».

[3]- منصارة يوسف، مرجع سابق، ص 259.

[4]- بن صالح سارة، **ماهية الكتابة والتوقيع الإلكترونيين كأدلة إثبات في المواد المدنية**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 18.

اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر بموجب الفقرة (أ) من المادة الأولى منها.

يلاحظ أن المشرع المصري لم يقم بتحديد الأشكال التي يمكن قد يتخدها التوقيع الإلكتروني ويستدل على ذلك من خلال عبارة "أو غيرها" الواردة في المادة آنف ذكرها، وهو ما يفسح المجال أمام الإعتراف بجميع صور التوقيع الإلكتروني الذي قد يظهر عليها مستقبلًا، كما أنه قد إتخذ بنهج النظير الوظيفي حين نص: "يسمح بتحديد شخص الموقع ويميزه عن غيره"، ولكنه قد أغفل على الوظيفة الثانية للتوقيع وهي قبول بمضمون التصرف الذي يصدر التوقيع الإلكتروني بمناسبته.[1]

ج-2- تعريف التوقيع الإلكتروني في التشريع الجزائري:

نظم المشرع الجزائري التوقيع الإلكتروني لأول مرة بمقتضى التعديل الذي أجراه على القانون المدني بموجب القانون رقم: 05-10 السالف الذكر في الفقرة 02 من المادة 327 والتي تنص على أن:" يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1 أعلاه"، وبالرجوع إلى المادة 323 مكرر1 نجدها تنص على أن: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"، يتضح لنا أنه لم يورد المشرع الجزائري تعريفًا للتوقيع الإلكتروني وإنما إكتفى بالإعتراف بحجيته رابطًا ذلك بتوفر نفس الشروط والمتطلبة في الكتابة العادية، والذي تم من خلاله الإعتراف بالكتابة الإلكترونية كوسيلة إثبات.

غير أن المشرع الجزائري تدارك الأمر وأصدر المرسوم التنفيذي رقم: 07-162 المؤرخ في 30 ماي 2007 المتعلق بنظام إستغلال الشبكات بما فيها السلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية[2]، المعدل والمتمم للمرسوم التنفيذي رقم: 01-123 المؤرخ في 09 ماي 2001 المتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية [3] والذي ألغي بموجب المرسوم التنفيذي رقم: 15-320 المؤرخ في 13 ديسمبر 2015 المحدد نظام

[1]- بوكر رشيدة، مرجع سابق، ص 177.

[2]- المرسوم التنفيذي رقم: 07-162 المؤرخ في 30 ماي 2007، المعدل والمتمم للمرسوم التنفيذي رقم: 01-123 المؤرخ في 09 ماي 2001، ج.ر.ج.ج.ش العدد 37، الصادرة بتاريخ 07 ماي 2007، الملغى.

[3]- المرسوم التنفيذي رقم: 01-123 المؤرخ في 09 ماي 2001، المتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر.ج.ج.ش العدد 27، الصادرة بتاريخ 13 ماي 2001، الملغى.

الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية[1].

ميز في المرسوم التنفيذي رقم: 07-162 المتعلق بنظام إستغلال الشبكات بما فيها السلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية السالف الذكر بين نوعين من التوقيع، التوقيع الإلكتروني العادي والتوقيع الإلكتروني المؤمن وذلك بموجب المادة 03 منه والتي جاء في مضمونها على إضافة المادة 3 مكرر إلى المرسوم التنفيذي رقم: 01-123 المتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية السالف الذكر، وجاء في مضمون المادة 3 مكرر على أن: "التوقيع الإلكتروني: هو معطى ينجم عن إستخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر1 من الأمر رقم: 75-58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني المعدل والمتمم"، وبالتالي نجد أن المشرع الجزائري لم يضع تعريفًا للتوقيع الإلكتروني وإنما إعترف بحجيته وأقر بالإعتداد به رابطًا ذلك بتوفر نفس الشروط المتطلبة في الكتابة الإلكترونية كوسيلة إثبات وذلك بعد الإحالة للمادتين 323 مكرر و323 مكرر1 من القانون المدني، أما التوقيع الإلكتروني المؤمن فوضحه في الفقرة 02 من المادة 03 مكرر من المرسوم التنفيذي رقم: 01-123 المتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية السالف الذكر بأنه هو توقيع إلكتروني الذي يفي الشروط الآتية: "بأن يكون خاصًا بالموقع، ويتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحصرية، ويضمن مع الفعل المرتبط به صلة بحيث يكون كل تعديل لاحق للفعل قابلًا للكشف عنه".

وبمقتضى صدور القانون رقم: 15-04 المؤرخ في 01 فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[2] ألغى جميع الأحكام المخالفة له[3] وميز بين نوعين من التوقيع الإلكتروني هما التوقيع الإلكتروني البسيط والتوقيع الإلكتروني الموصوف - تغيير التسمية من المؤمن إلى الموصوف- واضعًا لكل منهما تعريفًا، فالتوقيع الإلكتروني البسيط عرفه بموجب الفقرة الأولى من المادة 02 من نفس القانون على أنه: "بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيًا ببيانات إلكترونية أخرى كوسيلة توثيق"، وقد عرف هاته

[1]- المرسوم التنفيذي رقم: 15-320 المؤرخ في 13 ديسمبر 2015، المحدد نظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر.ج.ج.ش العدد 68، الصادرة بتاريخ 27 ديسمبر 2015.

[2]- القانون رقم: 15-04 المؤرخ في 01 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج.ش العدد 06، الصادرة في 10 فيفري 2015.

[3]- المادة 81 من القانون رقم: 15-04 السالف الذكر.

البيانات بموجب الفقرة 03 من نفس المادة على أنها بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني.

يتضح من المادة المشار إليها أعلاه أن المشرع الجزائري قد تبنى تعريفًا واسعًا للتوقيع الإلكتروني، إذ اعتبره عبارة عن بيانات إلكترونية مما يفتح المجال للإعتراف بأنواع جديدة من التوقيعات قد تفرزها التطورات التكنولوجية ويتيح للقانون إمكانية قبولها ضمن إطار الإثبات، إلى جانب تحديده لوظيفة هذا التوقيع وهي التوثيق أي تحديد هوية موقع المستند الإلكتروني وإلتزامه بمضمون ما ورد في المستند وموافقته على ما ورد فيه.[1]

أما التوقيع الإلكتروني الموصوف فلم يعرفه وإنما ذكر الشروط التي يجب توافرها فيه حتى يكتسي وصف الموصوف، بموجب المادة 07 من نفس القانون على أنه: "التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية:

1. أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة؛
2. أن يرتبط بالموقع دون سواه؛
3. أن يمكن من تحديد هوية الموقع؛
4. أن يكون مصممًا بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني؛
5. أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع؛
6. أن يكون مرتبطًا بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهاته البيانات".

وتضيف المادة 08 أنه يعتبر التوقيع الإلكتروني الموصوف وحده مماثلًا للتوقيع المكتوب.

يتضح من خلال ما سبق ذكره أن المشرع يهدف إلى تحقيق المساواة القانونية بين التوقيع التقليدي والتوقيع الإلكتروني الموصوف الذي تتوفر فيه الشروط الخاصة بضمان الأمان والموثوقية والتي لا تعتبر مطلوبة في التوقيع الإلكتروني البسيط.[2]

2- صور التوقيع الإلكتروني:

تجمع غالبية التعريفات المتعلقة بالتوقيع الإلكتروني على عدم حصره في شكل أو قالب معين، بل تبنت نهجًا مرنًا يتيح إستيعاب مختلف الصور التي قد تفرزها التكنولوجيا الحديثة بما يضمن قدرة التشريعات على مواكبة التحول الرقمي المستمر.

أ- التوقيع الرقمي:

التوقيع الرقمي (La Signature numirique) هو عبارة عن: " مجموعة حروف أو أرقام يختارها صاحب التوقيع، ويتم تركيبها أو ترتيبها في شكل غير مقروء، ويتم عن طريقه تحديد شخصية صاحبه بحيث لا يكون معلومًا إلا له فقط"، ويعتمد هذا التوقيع في الوصول إليه على

[1]- شيخ سناء، مرجع سابق، ص 119.
[2]- بوكر رشيدة، مرجع سابق، ص 177.

طرق حسابية معقدة ومعادلات رياضية لوغاريتمات تتحول بواسطتها المعاملة من رسالة ذات كتابة عادية مقروءة ومفهومة إلى معادلة رياضية أو رسالة رقمية غير مقروءة وغير مفهومة، ما لم يتم فك تشفيرها ممن يملك مفتاح فك الشفرة والمعادلات الخاصة بذلك.[1]

والتشفير[2] على النحو السابق لا يحقق السرية للمستند أو للبيانات بصفة عامة فحسب بل يحافظ على سلامتها ويسمح بتحديد مصدر التغييرات غير المصرح بها، كما يثبت هوية الأطراف بل أنه يضمن عدم الإنكار من الموقع على أساس أن التوقيع تم إنشاءه وفق بيانات فريدة.[3]

بحيث يستعمل الطرف الموقع على الرسالة ما يعرف بالمفتاح الخاص لوضع الترقيم الرقمي وهو مفتاح يحتفظ به الموقع ويحفظه على درجة عالية من السرية فمن الضروري أن يظل سريًا[4]، وهو عبارة عن مجموعة من الأرقام متمثلة في المعادلة الرياضية تقوم بتحويل المعلومات الموجودة في المستند الإلكتروني إلى رموز غير مفهومة مشفرة لا يمكن قراءتها ما لم يفك التشفير وذلك فقط بواسطة المفتاح العام الذي يكون متاحًا للأخرين، وقد عرفه المشرع الجزائري بموجب الفقرة 08 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر بأنه: "مفتاح التشفير الخاص هو عبارة عن سلسلة من الأعداد يحوزها حصريًا الموقع فقط وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي".

بينما يستعمل الطرف الآخر مستقبل الرسالة المفتاح العام للتحقق من صحة التوقيع الرقمي الموضوع بواسطة المفتاح الخاص[5] فيكون معروف لدى أكثر من شخص أو جهة، ويتم بواسطته فك شفرة الرسالة التي تم تشفيرها بواسطة المفتاح الخاص، كما يمكن إستخدامه

---

[1]- بن شهرة شول، بوشارب هانية، مرجع سابق، ص 169.

[2]- في الماضي كان يستخدم التشفير عن طريق النظام السيمتري "symetrique" أو ما يسمى بالتشفير المتماثل أو التشفير بإستخدام مفتاح واحد، والذي كان يتم بمقتضاه تشفير المعاملة ثم يتم إرسالها إلى المرسل إليه مع إرسال مفتاح التشفير بطريقة آمنة له حتى يتمكن من فك التشفير، ونظرًا لأن أطراف المعاملة يملكا المفتاح نفسه فكان في إمكانية المرسل إليه تعديل محتواها، وبالتالي لم يكن لها القوة الثبوتية مما عدم إمكانية الإعتداد بها في الإثبات. ثم أستبدل النظام السيمتري "symetrique" بالنظام "Asymetrique" أو ما يسمى بالتشفير المزدوج أو التشفير غير المتماثل، ويتم عن طريق إستخدام مفتاحين أحدهما للتشفير الرسالة أو المعاملة ويسمى المفتاح الخاص "Private Key"، أما المفتاح الثاني فيستعمل لفك التشفير ويسمى المفتاح العام "Public Key"، ويرتبط هذا الأخير بالمفتاح الخاص رياضيًا، وعدم إمكانية تعديل البيانات إلا عن طريق إستخدام المفتاح الخاص، ويتم منح المفتاحين للموقع عن طريق شهادة التصديق الإلكترونية التي تصدرها جهة التصديق الإلكتروني لتحديد هوية الموقع لتحقيق عنصري الثقة والأمان في المعاملات الإلكترونية، وللمزيد من التفصيل، ينظر: إبراهيم الدسوقي أبو الليل، **توثيق التعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير المتضرر**، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، المنعقد في 1-3 مايو 2003، الإمارات العربية المتحدة، ص 1857.

[3]- بوكر رشيدة، مرجع سابق، ص 181.

[4]- شيخ سناء، مرجع سابق، ص 124.

[5]- نفس المرجع، ص 124.

لتشفير رسائل مالك المفتاح الخاص[1]، وقد عرفه المشرع الجزائري بموجب الفقرة 09 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر بأنه: "سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني"، وبالتالي يتميز عنه بعدم الإحتفاظ بسريته حيث يبلغ للمرسل إليه ليتمكن عن طريقه من فك شفرة الرسالة، وميزة هذه الطريقة أنه لو عرف أحد المفتاحين فلا يمكن معرفة المفتاح الآخر حسابيًا[2].

وبالتالي فمن يرغب في التعامل إلكترونيًا يقوم بعد كتابة الرسالة بالتوقيع عليها إلكترونيًا بإستخدام مفتاحه الخاص وتمريرها من خلال برنامج خاص بالتشفير في الجهاز الإلكتروني، حيث يقوم هذا البرنامج الخاص بتشفير المعاملة بعمليات حسابية معقدة بمقتضاها تتحول الرسالة المكتوبة إلى رسالة رقمية.[3]

وهو عبارة عن أرقام مطبوعة لمحتوى المراسلة تسمى (HASH) والتي يتم التوقيع عليها بالطريقة ذاتها أي بإستخدام الأرقام، ويتم الحصول على هذا الكود بتحويل المستند المكتوب والتوقيع الوارد عليه من نمط الكتابة العادية إلى معادلة رياضية بإستخدام مفتاح سري (Token) وطرق حسابية معقدة، وذلك لتحويل المستند الإلكتروني من صورته المقروءة المفهومة إلى رسالة رقمية غير مقروءة أو غير مفهومة، ولا يمكن لأحد إعادة هذه المعادلة إلى صورتها المقروءة سوى حائز المفتاح.[4]

ولكي يتمكن من أرسلت إليه هذه الرسالة من قراءتها يتعين عليه أولًا فك شفرتها وذلك لا يتم إلا عن طريق المفتاح الآخر لمرسل الرسالة أي مفتاحه العام الذي يقوم بإرساله إلى متسلم الرسالة، وعن طريق هذا المفتاح العام وبإستخدام برنامج التشفير الخاص بالجهاز الإلكتروني يتمكن المرسل إليه من فك شفرة الرسالة وتحويلها من صورتها الرقمية إلى صورتها الأصلية المقروءة.[5]

فإذا طرأ على الرسالة أي تغيير في محتواها أو تم التلاعب في توقيع المرسل فإن الجهاز الإلكتروني يوضح ذلك على الفور، وبذلك يتوثق المتسلم من أن الرسالة التي تسلمها مرسلة بالفعل من المرسل وإن مضمونها سليم لم يتم التلاعب فيه، كما يتوثق من صحة توقيع المرسل يبقى موضوع أخير يتعلق بالكيفية التي بمقتضاها يتسنى للمرسل إليه التيقن من أن المفتاح العام الذي تسلمه يخص بالفعل المرسل الذي يرغب في التعامل معه، هنا يستلزم وجود شخص أو

---

[1]- طه عيساني، **التوقيع الإلكتروني كآلية لحماية المعاملات الإلكترونية**، كلية الحقوق والعلوم السياسية، جامعة حاج لخضر-باتنة، مجلة الباحث للدراسات الأكاديمية، المجلد 06، العدد 01، جانفي 2019، الجزائر، ص 569.

[2]- فوغالي بسمة، **إثبات العقد الإلكتروني وحجيته في ظل عالم الإنترنت**، رسالة الماجستير، تخصص: قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين-سطيف2، 2015/2014، ص-ص 68-69.

[3]- إبراهيم الدسوقي أبو الليل، مرجع سابق، ص 1857.

[4]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 722.

[5]- إبراهيم الدسوقي أبو الليل، مرجع سابق، ص-ص 1857-1858.

جهة محايدة موثوق فيها تقوم بدور الوسيط في تسليم المفتاح العام من المرسل إلى المرسل إليه، كما تقوم بإصدار شهادات إلكترونية تحدد هوية المتعاملين وصحة المعلومات التي تتضمنها رسائلهم.[1]

يؤمن هذا النوع الثقة والأمان التي يتعين توافرها لإزدهار المعاملات الإلكترونية فهو يقوم على معادلة رياضية لوغاريتمات تتشكل من أرقام سرية تعالج بطريقة رياضية، تجعل رسائل البيانات المتبادلة مشفرة غير مفهومة وغير مقروءة بشكل يضمن سرية المعلومات المتضمنة، فضلًا عن وجود جهة مختصة بالتصديق التوقيع الإلكتروني عن طريقها يتم إصدار شهادة تتضمن التصديق على التوقيع الإلكتروني للشخص المراد إثبات هويته، وصحة توقيعه ومن ثم التحقق من مضمون هذا التعامل وسلامة التوقيع الذي يحمله[2].

ولكن يعيبها إمكانية سرقة هذه الأرقام أو معرفتها من قبل الغير والتصرف فيها بشكل غير مشروع، وخاصة مع إزدياد عمليات الإحتيال والقرصنة ومحاولة بعض الأشخاص فك الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني والقيام بنسخها ومن ثم إعادة إستخدامها لأغراض غير مشروعة[3]، فضلًا عن ذلك لو كان توقيعه الإلكتروني الصادر بشأنه شهادة موثقة من الجهة المختصة قد تسرب إلى أشخاص آخرين يكون لصاحبه هو المسؤول عن ذلك طالما أنه لم يتخذ إجراءات الحيطة ويسأل عن خطئه وإهماله في الحفاظ على رقمه السري.[4]

ب- التوقيع البيومتري:

التوقيع البيومتري (La Signature biométrie) هو: "التوقيع الذي يعتمد في إنشائه على الخصائص الذاتية والسمات البيومترية سواء كانت بدنية (فيزيائية) أو سلوكية التي تميز كل فرد عن غيره وللتحقق من شخصيته"[5]، كبصمة الإصبع (Finger Printing)، التحقق من نبرة الصوت (Voice Recognition)، التعرف على الوجه البشري (Facial Recognition)، مسح قزحية وشبكية العين (Iris and Retina Scanning)، وخواص اليد البشرية (Hand-Geometry)، وغيرها من الصفات البدنية والسلوكية والتي تتغير من إنسان لآخر.

وتتم بعملية المسح الضوئي وأخذ صورة دقيقة لليد أو للوجه أو قزحية العين ثم يتم تخزينها وحفظها بصورة مشفرة داخل الجهاز الإلكتروني وإستخدامها كتوقيع في بعض

[1]- إبراهيم الدسوقي أبو الليل، مرجع سابق، ص 1858.

[2]- بوشارب هانية، مجدوب آمنة، **إلتزامات مؤدي خدمات التصديق الإلكتروني**، جامعة زيان عاشور-الجلفة، مجلة العلوم القانونية والإجتماعية، المجلد الثامن، العدد الثاني، جوان 2023، الجزائر، ص 45.

[3]- أمينة قهواجي، ليلي مطالي، **الإطار المفاهيمي والقانوني للتوقيع والتصديق الإلكترونيين في الجزائر**، كلية العلوم الإقتصادية والتجارية وعلوم التسيير، جامعة بلحاج بوشعيب عين تموشنت-الجزائر، مجلة المشكاة في الإقتصاد لتنمية والقانون، المجلد 04، العدد 08، سنة 2018، الجزائر، ص 26.

[4]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 722.

[5]- نفس المرجع، ص 723.

التصرفات القانونية[1]، وعمليًا يتم تخزين هذه الخواص على الجهاز بطريق التشفير في نظام حفظ الذاكرة، ويصادفك هذا التشفير للتحقق من صحة التوقيع وذلك بمطابقة صفات وسمات العميل المستخدم للتوقيع مع الصفات التي تم تخزينها على الجهاز[2]، فإن تمت المطابقة بين تلك الصورة مع السجل الرقمي الموجود في الجهاز فإنه يتم تنفيذ العقد وإلا ألغيت عملية التعاقد[3]، حيث تتم برمجته على أساس ألا يصدر أمرًا بفتح القفل المغلق إلا بعد أن يطابق هذه البصمة على البصمة المبرمجة في ذاكرته[4]، مما يؤدي إلى توافر الثقة في أن التوقيع بأحد تلك الخواص قد تم عن طريق الموقع ذاته مما يحدد هويته.

إلا أن الخبراء وجدوا أن إستعماله يصطدم بعقبات منها:

1. إحتمال تغير بعض خصائص الإنسان بفعل الظروف كتأكل بصمات الأصابع عبر الزمن أو بفعل بعض المهن اليدوية، أو تأثير التوتر في نبرة الصوت، أو تشابه أوجه التوائم[5]؛
2. يعيب طرق التوثيق البيومترية إمكان مهاجمتها أو نسخها من القراصنة عن طريق فك شفرتها، كما نسب إليها أنها تفتقر إلى الأمن والسرية، حيث تعمل الشركات المنتجة للطرق البيومترية على توحيد نظم عملها، هذا بالإضافة إلى أنها لا تقدم نتائج كاملة الصحة[6]؛
3. هذه الصورة من التوقيع قابلة للتزوير عن طريق خضوع الدبدبات الحاملة للصوت أو صورة بصمة الإصبع للنسخ وإعادة الإستعمال وإدخال تعديلات عليها، كذلك الشأن بالنسبة لبصمة العين فيمكن تزويرها بتقليدها عن طريق بعض أنواع العدسات اللاصقة المصنوعة من رقائق السليكون والتي تحمل نفس اللون والشكل والخصائص المخزنة على الجهاز[7]؛
4. التكلفة المعتبرة التي يتطلبها وضع نظام آمن في شبكات المعلومات بإستخدام الوسائل البيومترية، وهذا ما تسبب في محدودية إنتشاره حيث يقتصر حاليًا إستخدامه في الجانبي الأمني والمخابراتي للدول.[8]

---

[1]- بن جديد فتحي، **مدى حجية الكتابة والتوقيع الإلكترونيين في إثبات العقد المبرم عبر الإنترنت**، معهد البحوث والدراسات العربية المنظمة العربية للتربية والثقافة والعلوم، جامعة الدول العربية، مجلة البحوث والدراسات العربية، المجلد 41، العدد 62، جوان 2015، مصر، ص 113.

[2]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 723.

[3]- بن جديد فتحي، مرجع سابق، ص 113.

[4]- فوغالي بسمة، مرجع سابق، ص 71.

[5]- مثنى سعد السوداني، مرجع سابق، ص 142.

[6]- إبراهيم الدسوقي أبو الليل، مرجع سابق، ص 1855.

[7]- فارس خطابي، دليلة مباركي، **تزوير التوقيع الإلكتروني في بطاقات الإنتمان -دراسة على ضوء القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين-**، جامعة الحاج لخضر-باتنة1، المجلة الجزائرية للأمن الإنساني، المجلد 05، العدد 02، جويلية 2020، الجزائر، ص 654.

[8]- زروق يوسف، **حجية وسائل الإثبات الحديثة**، أطروحة الدكتوراه، تخصص: قانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد-تلمسان-، 2013/2012، ص 250.

ج- التوقيع بإستخدام القلم الإلكتروني:

يقصد بالتوقيع بالقلم الإلكتروني (Pen op)[1] على أن: "التوقيع الذي يستخدم فيه المعني بالأمر قلمًا إلكترونيًا ضوئيًا يكتب به توقيعه الخطي على شاشة الجهاز الإلكتروني، وفقًا لبرنامج خاص يلتقط به التوقيع من جميع خصائصه".[2]

يتم العمل بهذه الصورة من صور التوقيع من خلال الإستعانة ببرنامج خاص يتم إعداده ليتناسب مع القلم الإلكتروني من خلال الربط بالجهاز الإلكتروني [3] ذي مواصفات خاصة تمكنه من أداء مهمته في إلتقاط التوقيع من شاشته والتحقق من مطابقته للتوقيع المحفوظ بذاكرته، كما أنه يحتاج إلى جهة توثيق إضافية[4].

كما أن هذا البرنامج يقوم بإعطاء رسالة تحذير إذا وجد أي تغيير في محتويات المستند الموقع من خلال قيامه بفحص سلامة التوقيع الإلكتروني والمستند.[5]

ويقوم هذا البرنامج بوظيفتين أساسيتين لهذا النوع من التوقيعات:

ج-1- خدمة إلتقاط التوقيع:

يتلقى البرنامج أولًا معطيات العميل عن طريق بطاقته الخاصة التي يتم وضعها في الجهاز الإلكتروني وتظهر بعد ذلك التعليمات في الشاشة ويتبعها الشخص، ثم تظهر رسالة تطالب بتوقيعه بإستخدام قلم على مربع داخل الشاشة[6]، حيث يقوم الموقع بتحريك القلم على الشاشة في المكان المحدد لذلك من قبل البرنامج، ويستطيع المستخدم رؤية توقيعه على الشاشة[7].

إذ يقوم البرنامج بقياس خصائص معينة للتوقيع من حيث الحجم والشكل والنقاط والخطوط والإلتواءات[8] وغيرها من السمات الخاصة بالتوقيع، وعقب الإنتهاء من وضع التوقيع على الشاشة بهاته الصورة يظهر للموقع إختيارات تفيد إما الموافقة على شكل التوقيع الذي

---

[1]- يعتمد هذا التوقيع على إستعمال قلم حساس stylot sensible والكتابة على لوحة رقمية أو على شاشة الحاسوب، وبواسطة هذه التطبيقة المعلوماتية تمكن من إلتقاط التوقيع Signature de capture عن طريق تحريك القلم الإلكتروني signature stylo-ordinateur في أماكن محددة، وللمزيد من التفصيل، ينظر: رحمان يوسف، **الأدلة الكتابية ذات القوة القانونية**، أطروحة الدكتوراه، تخصص: قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد –تلمسان- الجزائر، 2017/2016، ص 268.

[2]- بشرى زلاسي، **المعطيات الحديثة للحاسب الإلكتروني الكمبيوتر وحجيتها في الإثبات المدني**، أطروحة الدكتوراه، قسم: القانون الخاص، كلية الحقوق، جامعة الجزائر1، 2013/2012، ص 102.

[3]- لورنس محمد عبيدات، **إثبات المحرر الإلكتروني**، الطبعة الأولى، 2009، دار الثقافة للنشر والتوزيع، عمان-الأردن، ص 148.

[4]- إبراهيم الدسوقي أبو الليل، مرجع سابق، ص 1856.

[5]- لورنس محمد عبيدات، مرجع سابق، ص 148.

[6]- فارس خطابي، دليلة مباركي، مرجع سابق، ص 654.

[7]- أزرو محمد رضا، مرجع سابق، ص 208.

[8]- مثنى سعد السوداني، مرجع سابق، ص 140.

وضعه أو إعادة المحاولة أو إلغاء التوقيع[1]، إذا تمت الموافقة تشفر تلك البيانات وتخزن عن طريق البرنامج[2].

ج-2- خدمة التحقق من موثوقية التوقيع:

عند حاجة الموقع لتوقيعه يعود إلى البرنامج الذي حفظ هذا التوقيع، ولكي تتم عملية التوثيق يطلب الجهاز الإلكتروني من الشخص كتابة توقيعه داخل مربع معين في الشاشة، ويقوم البرنامج الذي سبق ذكره بالمطابقة بين هذا التوقيع والتوقيع المحفوظ[3] بفك رموز الشفرة البيوميترية ثم تقارن المعلومات مع التوقيع المخزن وترسلها إلى البرنامج الذي يعطي الإشارة فيما إن كان التوقيع صحيحًا أم لا[4]، بعد مقارنتها مع المئات أو الآلاف من التوقيعات الموجودة في قاعدة بياناته، ثم يعطي تقريرًا مفصلًا عن الموقع وهويته[5].

وبعد التحقق من صحة التوقيع ينتقل به إلى الملف المراد توقيعه أو يعرف بما يسمى الرسالة الإلكترونية، ثم إرساله إلى الطرف المتعاقد الآخر عبر الإنترنت، هذه العملية تتم بواسطة الماسح الضوئي (Scanner) الذي يقوم بتصوير هذا التوقيع عبر أنظمة المعالجة الإلكترونية.[6]

وهذه الطريقة لا تحقق الأمان الكافي للتعامل مع المستندات التي يضاف إليها التوقيع بالقلم الإلكتروني وذلك لإمكانية إصطناع مستند إلكتروني بمواجهة صاحب التوقيع دون علمه به[7]، بحيث يمكن للمرسل إليه الإحتفاظ بنسخة من صورة التوقيع وإعادة إستعمالها في أية وثيقة من الوثائق الإلكترونية بإعتبارها صادرة من صاحب التوقيع الفعلي[8].

كما أنه قليل الإستعمال بسبب ندرة الحاسوب المزود بقلم رقمي وإرتفاع ثمنه قد يجعلان اقتناءه غير متاح للجميع بسبب ما يتطلبه من مواصفات فنية خاصة لتطبيقه[9]، كما أن مسألة التأكد من صحة التوقيع بصفة مستمرة تتطلب تدخل طرف ثالث والمتمثل في مقدمي خدمات التصديق الإلكتروني[10] بإصدار شهادات التصديق عن طريق إستعمالها لخوارزميات ووسائل التشفير تجعل القلم الإلكتروني تحت سيطرة صاحبه فقط ولا يمكن إستعماله من طرف الغير[11].

---

[1]- بلقنيشي حبيب، **إثبات التعاقد عبر الإنترنت (البريد المرئي) -دراسة مقارنة-**، أطروحة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة وهران –السانيا، 2010/ 2011، ص 120.

[2]- غنية باطلي، **الكتابة الإلكترونية كدليل إثبات**، جامعة باجي مختار-عنابة، مجلة التواصل، المجلد18، العدد02، 2012، الجزائر، ص 134.

[3]- زروق يوسف، مرجع سابق، ص-ص 251-252.

[4]- فارس خطابي، دليلة مباركي، مرجع سابق، ص 654.

[5]- طه عيساني، مرجع سابق، ص 569.

[6]- بشرى زلاسي، مرجع سابق، ص 102.

[7]- مثنى سعد السوداني، مرجع سابق، ص-ص 140-141.

[8]- شيخ سناء، مرجع سابق، ص-ص 120-121.

[9]- بشرى زلاسي، مرجع سابق، ص 103.

[10]- رحمان يوسف، مرجع سابق، ص 268.

[11]- بن حميدوش نورالدين، رحموني عبد الرزاق، **مكانة الدليل الإلكتروني في الإثبات الجزائي**، جامعة محمد بوضياف مسيلة، مجلة الدراسات والبحوث القانونية، المجلد 04، العدد 02، جانفي 2020، الجزائر، ص35.

وتجدر الإشارة إلى أن هذا النوع من التوقيع هو الذي إعتمد عليه المشرع الجزائري لتحرير الإمضاءات في عملية إستصدار جوازات السفر وبطاقات التعريف البيومترية، وذلك من خلال إصدار قرار مؤرخ في 19 جويلية 2010 والمتضمن إصدار جواز السفر وبطاقة التعريف البيومتريين، وهذا إستجابة للمنظمة العالمية للطيران والتي دعت دول العالم إلى إصدار جواز السفر البيومتري ولا يزال مستخدمًا إلى اليوم.[1]

د- التوقيع بإستخدام البطاقة الممغنطة المقترنة بالرقم السري:

التوقيع بإستخدام البطاقة الممغنطة المقترنة بالرقم السري (P.I.N) لا يتطلب العمل بها خبرة أو عناء كبيرين إذ يمكن لكل شخص إستخدامها دون ما حاجة إلى توفره على جهاز إلكتروني ودون ما حاجة كذلك إلى ربطه بشبكة الإنترنت[2]، لأنها تتمثل في المعاملات التي تجري خلال البنوك لسحب أي مبلغ من رصيد الشخص في الوقت الذي يشاء من خلال وضع البطاقة في المكان المخصص في الصراف الآلي ثم إدخال الرقم السري لصاحب البطاقة والضغط على أمر السحب بالموافقة على إتمام العملية من خلال المفاتيح الموجودة في جهاز الصراف الآلي[3]، إضافة إلى ما تقوم به هذه البطاقات من سداد لثمن بعض السلع والخدمات من خلال أجهزة مخصصة لذلك وما تقوم به أيضًا من عمليات دفع عبر الإنترنت، حيث تحتوي هاته البطاقة على رقم سري لا يعرفه إلا صاحبها والذي يخوله الدخول إلى حسابه وإجراء العمليات التي يريدها[4].

وغالبًا ما يرتبط هذا التوقيع السري بالبطاقات البلاستيكية والبطاقات الممغنطة وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة إلكترونية.[5]

وتتكون هذه البطاقة من رقم سري لا يعرفه إلا صاحبها، وذاكرة تسجيل تحتوي على جميع المعطيات الخاصة بالعميل من إسم ولقب ورقم الهوية ومكان الإقامة وتاريخ إصدار وإنتهاء صلاحية البطاقة وغيرها من المعلومات الشخصية، أما بخصوص ذاكرة البطاقة تحتوي على نظام حماية عالي الدقة ففي حالة ما إذا سرقت البطاقة وأراد الشخص إستعمالها فقد يلجأ إلى إستعمال عدة محاولات لفك الشفرة ولم يستطيع فتحها أي لا يحوز على الرقم السري، فقد يؤدي النظام الإلكتروني إلى سحب هذه البطاقة بواسطة آلة الصرف مما تفرض هذه البطاقة مكانتها وأمانها القانوني في التعاملات اليومية.[6]

وهي بطاقات بلاستيكية ذات شريط ممغنط من حيث كونه وسيلة إدخال وتخزين وتأمين للمعطيات المشفرة عليه ويتم تشفير المعطيات على هذا الشريط في مسارات أفقية ثلاثة، ويتم

---

[1]- طه عيساني، مرجع سابق، ص 570.

[2]- أمينة قهواجي، ليلي مطالي، مرجع سابق، ص 25.

[3]- مثنى سعد السوداني، مرجع سابق، ص 141.

[4]- لورنس محمد عبيدات، مرجع سابق، ص 149.

[5]- إبراهيم الدسوقي أبو الليل، مرجع سابق، ص 1853.

[6]- رحمان يوسف، مرجع سابق، ص 269.

الدفع بهذه البطاقة إعتمادًا على معطيات الشريط الممغنط من خلال قراءة المعلومات المخزنة عليه[1] وتوجد عدة صور لهذه البطاقات[2] مثل بطاقة فيزا (visa)، وأميركان إكسبرس (American- Exress)[3]، والبطاقات الممغنطة (Magnetic Stripe Cards) .

والبطاقة الممغنطة هي بطاقة يتم إصدارها من طرف المؤسسات المالية أو الإئتمانية كالبنوك، لفائدة عملائها من أجل تسهيل معاملاتهم المالية، وتجنيبهم مخاطر حمل السيولة المالية خاصة عندما يتعلق الأمر بمبلغ مالي كبير، كما أنها تساهم في توفير الوقت والجهد على العميل إذ بدلًا من ذهاب العميل إلى البنك للقيام بالمعاملات المالية فإنه يقوم بجميع عملياته المالية عن طريق الصراف الآلي في أي وقت يشاء دون أن يكون مقيد بميعاد أو مكان معين.[4]

ويعتمد نظام الحماية في هذه البطاقة على رقم سري مرتبط بصاحب البطاقة فقط، وبالتالي لو عثر أي شخص آخر على البطاقة لا يستطيع إستخدامها ما لم يكن على علم بالرقم السري، وهذا ما لا يمكن توقع حدوثه إلا في حالة الإهمال الشديد من طرف صاحب البطاقة وحتى في هذه الحالة فبإمكان صاحب البطاقة تفادي ذلك عن طريق التوجه إلى البنك ووقف العمل بهذه البطاقة.[5]

ويلاحظ أن هذا النوع من التوقيع يتميز بالسرية إلا أنه لا يصلح للإثبات لعدم وجود مستند يوضع عليه التوقيع كالمستند الكتابي أو المستند الإلكتروني المستخرج من شبكة الإنترنت، لذا يقتصر التعامل في هذا النوع من التوقيع بين البنك والعميل بموجب إتفاق خاص بينهما.[6]

---

[1]- منظور أحمد حاجي الأزهري، **بطاقة السحب النقدي**، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، المنعقد في 1-3 مايو 2003، الإمارات العربية المتحدة، ص 362.

[2]- بالرجوع إلى تاريخ نشوء بطاقة الإئتمان وتطورها نلاحظ أنها نشأت في الولايات المتحدة الأمريكية في بداية القرن العشرين، وبعد الحرب العالمية الثانية كان أول بنك يصدر البطاقة الإئتمانية هو "The Flatbush National Bank" وذلك في سنة 1947، ثم شرعت المؤسسات المالية والمصارف ببسط الخدمة للعملاء، وثم قبول هذه البطاقات من قبل التجار، وفي سنة 1951 تكونت أول شركة متخصصة في إصدار البطاقات وهي شركة "Dinners Club"، وكانت القفزة الكبرى في عالم بطاقات الإئتمان عندما سمح بنك أمريكان "American Bank" للمصارف الأخرى، ورخص لها بإصدار بطاقته الإئتمانية مما سمح بإنتشار البطاقة في بلاد العالم، كما يسر لحاملها فرصة التسوق بها ممن يقبل التعامل بها في أي بقعة من الكرة الأرضية، وللمزيد من التفصيل، ينظر: علي محمد الحسين الموسى، **البطاقات المصرفية تعريفها وأنواعها وطبيعتها**، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، المنعقد في 1-3 مايو 2003، الإمارات العربية المتحدة، ص-ص 1994-1995.

[3]- أول البنوك الأمريكية التي أصدرت بطاقات الإئتمان هو بنك فرانكلين الوطني سنة 1951، وتم تسمية البطاقة ببطاقة National Card، ثم تبعه البنك الأمريكي سنة 1958 حيث أصدر بطاقة American Card ثم ظهرت بطاقة الأمريكان إكسبريس سنة 1958، لتمكن حاملها من إستفادة الحصول على السلع والخدمات من الفنادق والشركات، على أن تحصل من عملائها ما يضمن إسترداد ما تقوم بدفعه لحساب فواتيرهم، وللمزيد من التفصيل، ينظر: أبو الوفا محمد، أبو الوفا إبراهيم، **المسئولية الجنائية عن الإستخدام غير المشروع لبطلقة الإئتمان**، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، المنعقد في 1-3 مايو 2003، الإمارات العربية المتحدة، ص 2042.

[4]- طه عيساني، مرجع سابق، ص 571.

[5]- نفس المرجع، ص 571.

[6]- مثنى سعد السوداني، مرجع سابق، ص 141.

ر- التوقيع بالماسح الضوئي:

إن أساس هذا النوع من التوقيع يقوم على فكرة نقل التوقيع اليدوي التقليدي من الدعامة الورقية إلى الدعامة الإلكترونية بواسطة الماسح الضوئي (scanner)[1]، من خلاله يقوم الشخص بالتوقيع على مستند ورقي ثم يقوم بإلتقاط صور رقمية لهذا التوقيع بواسطة جهاز الماسح الضوئي ثم نقل التوقيع الخطي كما هو على الورق إلى وثيقة موجودة في الجهاز الإلكتروني[2] حيث تتحول العلاقة الخطية إلى صورة تحفظ في شكل ملف، وهو ما يعني أن ذلك التوقيع يظهر على الجهاز في شكل صورة إلكترونية للتوقيع الخطي ثم يمكن للشخص أن ينقل هذه الصورة إلى الملف أو الرسالة المراد إضافة التوقيع إليها عبر الإنترنت كما يمكن تخزينها على أي دعامة محمولة، وفي حالة رغبة إرسال رسالة موقعة إلكترونية يتم إعطاء أمر للجهاز الإلكتروني ليعيد بنسخ صورة من التوقيع ووضعها على المستند الإلكتروني[3].

رغم سهولة إستخدام التوقيع الإلكتروني إلا أن عنصري الثقة والأمان منعدمان، إذ قد يحصل الغير على صورة ضوئية لتوقيع الشخص بأي طريقة[4] كما يستطيع الطرف الثاني إستعمال هذه النسخة والتلاعب بها، مما يثير الشكوك حول قدرة هذا التوقيع على تحديد هوية الموقع الحقيقي[5].

وأمام كل هذه المخاطر التي قد تعترض هذا النوع من التوقيع يمكننا القول أنه لا يضمن بصورة عامة تحديد هوية صاحب التوقيع، لهذا تستدعي الضرورة وضع له منظومة معلوماتية آمنة عن طريق التصديق عليه من جهات معتمدة تكون تحت رقابة الدولة وهذا ما قد يحققه التطور التقني مستقبلًا.[6]

ز- التوقيع الكودي:

يقصد بالتوقيع الكودي أو السري إستخدام مجموعة من الأرقام أو الحروف أو كليهما يختارها صاحب التوقيع لتحديد هويته وشخصيته، ويتم تركيبها وترتيبها في شكل كودي معين بحيث لا يعلمها إلا صاحب التوقيع ومن يبلغه بها.[7]

وقد كانت المعاملات البنكية هي السباقة في إستخدام هذا النوع من التوقيع من خلال البطاقات البنكية والتي تحتوي على رقم سري يقوم من خلالها صاحبها بالقيام بكل العمليات

---

[1]- شيخ سناء، مرجع سابق، ص 120.

[2]- حسان سعاد، **إثبات التعاملات الإلكترونية وفقاً للقانون الجزائري والتشريعات المقارنة**، الطبعة الأولى، 2019، مكتبة الوفاء القانونية، الإسكندرية-مصر، ص 82.

[3]- منصور داود، **القيمة القانونية للبلوك تشين في الإثبات ودوره في نطاق التوثيق الرقمي للمعاملات الإلكترونية**، جامعة زيان عاشور-الجلفة، مجلة الحقوق والعلوم الإنسانية، المجلد14، العدد02، 2021، الجزائر، ص 280.

[4]- حسان سعاد، مرجع سابق، ص 82.

[5]- زروق يوسف، مرجع سابق، ص 256.

[6]- بشرى زلاسي، مرجع سابق، ص 105.

[7]- شيخ سناء، مرجع سابق، ص 122.

المصرفية عن طريق جهاز الصراف الآلي بإدخال العميل البطاقة في الجهاز[1]، وأيضًا يستخدم هذا النوع بكثرة في المواقع الإلكترونية المشفرة التي لا تسمح بالدخول إليها إلا للمشتركين الذين لديهم كود سري يتيح لهم الدخول إلى صندوقهم البريدي[2]، ويتم إجراء عملية المطابقة عبر متصفح شبكة الإنترنت بحيث يتم توصيل الكود المشفر بين الطرفين بحيث لا يكون التوقيع معروفة إلا من صاحبه ومقدم الخدمة.[3]

3- التصديق الإلكتروني كآلية لتوثيق التوقيع الإلكتروني:

لقد أوصت أغلب التشريعات الدولية والوطنية على ضرورة تأمين التوقيع الإلكتروني، حتى يتوفر الثقة والأمان بين المتعاملين بموجبه، مما إستلزم وجود طرف محايد وهو ما أطلق عليه المشرع الجزائري بجهات التصديق الإلكتروني، تتمثل مهمته في التحقق من صحة التوقيع الإلكتروني ونسبته لموقعه ومنحه القوة الثبوتية، عن طريق شهادة التصديق الإلكتروني.[4]

أ- مفهوم الجهات المختصة بالتصديق الإلكتروني:

إرتأينا أن نتطرق إلى تعريف الجهات المختصة بالتصديق الإلكتروني، ثم إبراز الهيئات المكلفة بتقديم هذه الخدمات التصديق الإلكتروني.

أ-1- تعريف الجهات المختصة بالتصديق الإلكتروني:

لقد تتعدد التعريفات لجهات التصديق الإلكتروني على التوقيع الإلكتروني، وسنحاول فيما يلي عرض أهم هذه التعريفات.

أ-1-1- التعريف الفقهي لجهات التصديق الإلكتروني:

ظهرت عدة تعريفات لمؤدي خدمات التصديق الإلكتروني لعل أشملها أنه: " شخص طبيعي أو معنوي يستخرج الشهادات الإلكترونية، ويقدم خدمات أخرى مرتبطة بالتوقيعات الإلكترونية، ويضمن تحديد هوية الأطراف المتعاقدة، والإحتفاظ بهذه البيانات لمدة معينة، ويلتزم بإحترام القواعد المنظمة لعمله والتي يتم تحديدها بمعرفة السلطة المختصة"[5]، وعرف أيضًا بأنه: "وسيط محايد ومستقل قد يكون هذا الوسيط شخصًا طبيعيًا أو معنويًا، وقد يكون جهة عامة أو جهة خاصة، ويتدخل بناء على طلب شخص بهدف إنشاء وحفظ وإثبات الوسائل

---

[1]- حسان سعاد، مرجع سابق، ص 80.

[2]- طه عيساني، مرجع سابق، ص 568.

[3]- نفس المرجع، ص 568.

[4]- بن عيسى فتيحة، المر سهام، مرجع سابق، ص 186.

[5]- رضوان قرواش، **هيئات التصديق الإلكتروني في ظل القانون 15-04 المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين (المفهوم والإلتزامات)**، جامعة محمد لمين دباغين سطيف 2، مجلة العلوم الإجتماعية، العدد24، جوان 2017، الجزائر، ص 412.

الإلكترونية والتوقيع الإلكتروني، وتوثيقها وإصدار شهادات توثيق بذلك لإثبات صحة نسبتها لأصحابها"[1].

كما عرف أيضًا بأنه: "هيئة عامة أو خاصة، تعمل على ملء الحاجة إلى وجود طرف ثالث موثوق، يصدر شهادات تثبت صحة الحقيقة المتعلقة بموضوع التبادل الإلكتروني، بتأكيد نسبة التوقيع الإلكتروني إلى شخص معين، وتأكيد نسبة المفتاح العام المستخدم إلى صاحبه"[2]، وعرف أيضًا بأنه: "هيئة أو مؤسسة يتولى إدارتها شخصًا طبيعيًا أو معنويًا تعمل بترخيص من إحدى مؤسسات الدولة، وظيفتها إصدار شهادات التصديق الإلكتروني تربط بين شخص طبيعي أو معنوي ومفتاحه العام، أو أية مهمة أخرى[3] تتعلق بالتوقيع الإلكتروني"[4].

وعرف كذلك بأنه: "شركات أو أفراد مستقلة ومحايدة تقوم بدور الوسيط بين المتعاملين لتصديق معاملاتهم الإلكترونية وتقوم بإصدار شهادات التصديق تفيد صحة هذه المعاملات، وهي تعد كطرف ثالث محايد"[5]، كما عرف على أنه: "هوية أو بطاقة إلكترونية تصدر من جهة التوثيق مختصة، تشتمل على مجموعة من البيانات الأساسية التي تتعلق بالشهادة وهوية الشخص المرسل ومصدرها، تقوم بإثبات هوية الشخص مرسل الرسالة بواسطة ربط مفتاحه الخاص بالمفتاح العام وفقًا لضوابط معينة"[6]، وعرف أيضًا بأنه: "عبارة عن هيئات عامة أو خاصة تعمل على ترسيخ الثقة بين الأطراف المتعاملين عبر شبكة الإنترنت، وذلك من خلال إصدارها لشهادات إلكترونية لكل مشترك تشهد بموجبها بصحة البيانات والمعلومات الواردة فيها، وذلك لضمان وحماية وقبول التعامل بالمستندات الموقعة إلكترونيًا والإعتراف بحجيتها"[7].

أ-1-2- التعريف الدولي لجهات التصديق الإلكتروني:

تطرق قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 لهذه الجهة تحت مسمى مقدم خدمات التصديق، وعرفه في الفقرة (هـ) من المادة 02 بأنه: "مقدم خدمات

---

[1]- شيخ سناء، مرجع سابق، ص 141.

[2]- طه عيساني، مرجع سابق، ص 565.

[3]- يقصد بعبارة: "أية مهمة أخرى تتعلق بالتوقيع الإلكتروني" التقنيات التي تسمح بإصدار توقيع مؤرخ، وخدمات النشر والإطلاع، والخدمات المعلوماتية الأخرى كالحفظ في الأرشيف، وللمزيد من التفصيل، ينظر: بلحاج محجوبة، **القواعد العامة للتوقيع والتصديق الإلكترونيين وحمايتهما جزائياً وفقاً لقانون العقوبات والقانون رقم: 15-04**، جامعة إبن خلدون تيارت، مجلة البحوث في الحقوق والعلوم السياسية، الجزائر، المجلد 06، العدد 02، 2020، الجزائر، ص 99.

[4]- نفس المرجع، ص 99.

[5]- طه عيساني، مرجع سابق، ص 565.

[6]- طنجاوي مراد، مرجع سابق، ص 136.

[7]- بن مشري عبد الحليم، مقري صونيا، **دور جهات التصديق الإلكتروني في إثبات المعاملات الإلكترونية**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 104.

التصديق: يعني شخص يصدر الشهادات، ويجوز أن يقدم خدمات أخرى ذات الصلة بالتوقيعات الإلكترونية".[1]

كما عرف التوجيه الأوروبي رقم: 1999-93 المتعلق بشأن إرساء إطار قانوني مشترك لإستخدام التوقيع الإلكتروني السالف الذكر هذه الجهة في الفقرة 11 من المادة 02 بأنها: "أي جهة أو كل شخص طبيعي أو معنوي، يقوم بإصدار الشهادات أو تقديم خدمات أخرى تتعلق بالتوقيعات الإلكترونية"[2]، فقد ألزم هذا التوجيه على دول الأعضاء في الإتحاد الأوروبي على الترخيص بإصدار شهادات تثبت إمتثال التوقيع الإلكتروني للشروط اللازمة لكي يعتد به في الإثبات، وتضمن إرتباطه بالمستند المرفق به، مع تأمينه ضد أي تعديل أو تغيير في مضمونه.[3]

إلا أنه ألغي التوجيه الأوروبي رقم: 1999-93 بموجب اللائحة رقم: 910-2014 المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية السالفة الذكر ولم تغفل عن التطرق لتعريف مقدم التصديق الإلكتروني، حيث نصت في الفقرة 19 من المادة 03 منها على أنه: "مقدم خدمة التوثيق شخص طبيعي أو معنوي يقوم بتقديم خدمة أو أكثر من خدمات التوثيق، سواء كان مقدم خدمة التوثيق مؤهل أو غير مؤهل"[4]، وعرفت في الفقرة 20 من نفس المادة مقدم خدمة التوثيق المؤهل على أنه: "مقدم خدمة توثيق الذي يقدم خدمة أو أكثر من خدمات التوثيق المؤهلة، ومتحصل من الهيئة الإشرافية على التأهيل".[5]

أ-1-3- التعريف التشريعي لجهات التصديق الإلكتروني:

سنتطرق إلى تعريف جهات التصديق الإلكتروني في مختلف التشريعات المقارنة، ثم نتطرق إلى تعريفه وفقًا لما ورد في التشريع الجزائري.

---

[1]-Art 02 paragraphe d du Loi type de la CNUDCI sur les signatures électroniques 2001 dispose que: «Le terme "signataire" désigne une personne qui détient des données afférentes à la création de signature et qui agit soit pour son propre compte, soit pour celui de la personne qu'elle représente».

[2]-Art 02 paragraphe 11 du La directive 1999/93/CE du PEC, Abrogé par RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que : « prestataire de service de certification», toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques».

[3]- بلحسيني حمزة، مرجع سابق، ص 111.

[4]-Art 03 paragraphe 19 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: « prestataire de services de confiance, une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié».

[5]-Art 03 paragraphe 20 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: « prestataire de services de confiance qualifié, un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié».

أ-1-3-1- تعريف جهات التصديق الإلكتروني في التشريعات المقارنة:

أطلق عليه المشرع الفرنسي إسم المكلف بخدمة التوثيق الإلكتروني وعرفه بمقتضى المرسوم رقم: 2001-272 الصادر لتطبيق أحكام المادة 1316-4 من القانون المدني والمتعلق بالتوقيع الإلكتروني السالف الذكر بموجب الفقرة 11 من المادة الأولى منه: "كل شخص يصدر شهادات إلكترونية أو يقدم خدمات أخرى متعلقة بالتوقيع الإلكتروني"[1]، وألغي المرسوم السالف الذكر بمقتضى المرسوم رقم: 2017-1416 المتعلق بالتوقيع الإلكتروني السالف الذكر[2]، وأحال بموجب المادة الأولى منه تعريف المكلف بخدمة التوثيق الإلكتروني إلى الأحكام اللائحة رقم: 2014-910 المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية السالفة الذكر، وبالتالي فقد إستند إلى التعريف الوارد في هذه الأخيرة، والذي سبق أن تم التطرق إليه أعلاه.

وحسب قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر جاء خاليًا من أي تعريف لجهة التصديق على التوقيع الإلكتروني، إلا أن اللائحة التنفيذية لهذا القانون المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر عرفت جهات التصديق على التوقيع الإلكتروني في الفقرة 06 من المادة الأولى منها كالآتي: "الجهات المرخص لها بإصدار شهادة التصديق الإلكتروني، وتقديم خدمات تتعلق بالتوقيع الإلكتروني".

أ-1-3-2- تعريف جهات التصديق الإلكتروني في التشريع الجزائري:

وإعترف المشرع الجزائري بجهة التصديق وأطلق عليه إسم مؤدي خدمات التصديق الإلكتروني[3]، وعرفه بداية بموجب نص المادة 3 مكرر من المرسوم التنفيذي رقم: 07-162 المتعلق بنظام إستغلال الشبكات بما فيها السلكية الكهربائية وعلى مختلف خدمات المواصلات

---

[1]-Art 01 paragraphe 11 du Décret n°2001-272 du 30 mars 2001, Modifié par Décret n°2016-1278 du 29 septembre 2016 -art. 1 V, Abrogé par Décret n°2017-1416 du 28 septembre 2017 -art. 2 V, dispose que: « Prestataire de services de certification électronique: toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique».

[2]- Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique.

[3]- إختلفت المسميات التي أطلقت على جهات التوثيق أو مؤدي خدمات التصديق الإلكتروني وذلك بإختلاف النظم القانونية، يسمى وفقًا لقانون الأونسيترال النموذجي الخاص بالتوقيع الإلكتروني: "مؤدي خدمات التصديق"، ووفقًا للتوجيه الأوروبي رقم: 93 لسنة 1993 يسمى: "مقدمي خدمة التصديق"، وبالنسبة لقانون التجارة والمبادلات الإلكترونية التونسي يسمى: "مقدم خدمة التصديق الالكتروني"، أما بالنسبة للمشرع المغربي فقد أطلق عليهم إسم: "مؤدي خدمات التصديق الإلكتروني"، وبالنسبة للمشرع الفرنسي فقد أطلق عليه إسم: "المكلف بخدمة التوثيق الإلكتروني"، وأطلق المشرع الجزائري عليه تسمية: "مؤدي خدمات التصديق الإلكتروني"، ومن خلال ما سبق فقد إهتمت معظم التشريعات بتنظيم مؤدي خدمات التصديق الإلكتروني، ومسارة لهذا التقدم المتسارع فقد إنفرد المشرع الجزائري بفصل كامل الفصل الثالث تحت عنوان "النظام القانوني لتأدية خدمات التصديق الإلكتروني"، وللمزيد من التفصيل، ينظر: بوبكر أمال، **النظام القانوني لمؤدي خدمات التصديق الإلكتروني في الجزائر**، جامعة يحيى فارس-المدية، مجلة الدراسات القانونية، المجلد 04، العدد 01، 2018، الجزائر، ص 143.

السلكية واللاسلكية السالف الذكر بأن: "مؤدي خدمات التصديق الإلكتروني هو كل شخص في مفهوم الفقرة 08 من المادة 08 من القانون رقم: 2000-03 المؤرخ في 05 أوت سنة 2000، يسلم شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني"، وحسب الفقرة 08 من المادة 08 من القانون رقم: 2000-03 المؤرخ في 05 أوت 2000 المحدد للقواعد العامة المتعلق بالبريد والمواصلات السلكية واللاسلكية[1] نجده يعرف مؤدي الخدمات على أنه: "موفر الخدمات: كل شخص معنوي أو طبيعي يقدم خدمات، مستعملًا وسائل المواصلات السلكية واللاسلكية".

وبعد ذلك أصدر المشرع الجزائري القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر وفيه ميز بين نوعين من الجهات المكلفة بالتصديق الإلكتروني، الجهة الأولى أعطى لها تسمية الطرف الثالث الموثوق وعرفها بموجب الفقرة 11 من المادة 02 من القانون المذكور كالأتي: "شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي"، والجهة الثانية وهي التي تم إعتمادها سابقًا أعطى لها تسمية مؤدي خدمات التصديق الإلكتروني وعرفها بموجب الفقرة 12 من نفس المادة بأنه: "شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الإلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني".

ب- الجهات المكلفة بتقديم خدمات التصديق الإلكتروني:

ميز المشرع الجزائري بين نوعين من الجهات المكلفة بالتصديق الإلكتروني، الجهة الأولى أعطى لها تسمية الطرف الثالث الموثوق وعرفها بموجب الفقرة 11 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر، والجهة الثانية أعطى لها تسمية مؤدي خدمات التصديق الإلكتروني وعرفها بموجب الفقرة 12 من نفس المادة من القانون المذكور.

ب-1- الطرف الثالث الموثوق:

الطرف الثالث الموثوق والذي لا يمكن أن يكون إلا شخصًا معنويًا فقد أسندت إليه مهمة منح شهادات التصديق الإلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي[2]، ويقصد بالمتدخلين في الفرع الحكومي كل: "المؤسسات والإدارات العمومية والهيئات العمومية والمؤسسات الوطنية المستقلة وسلطات الضبط، والمتدخلون في المبادلات بين البنوك، وكل شخص أو كيان ينتمي إلى الفرع الحكومي

[1]- القانون رقم: 2000-03 المؤرخ في 05 أوت 2000، المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج.ر.ج.ج.ش العدد 48، الصادرة في 06 أوت 2000.

[2]- الفقرة 11 من المادة 02 من القانون رقم: 15-04 السالف الذكر.

بحكم طبيعته أو مهامه، هذه الجهات هي دائمًا عبارة عن شخص معنوي"،[1] ويخضع لمتابعة ومراقبة نشاطه من طرف السلطة الحكومية للتصديق الإلكتروني[2].

ب-2- مؤدي خدمات التصديق الإلكتروني:

مؤدي خدمات التصديق الإلكتروني يمكن أن يكون شخصًا طبيعيًا أو معنويًا، فقد أسندت إليه مهمة منح شهادات التصديق الإلكتروني موصوفة وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني لفائدة الجمهور[3]، ويخضع بمتابعة ومراقبة من طرف السلطة الإقتصادية للتصديق الإلكتروني[4].

وحدد القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر الشروط الواجب توافرها في مؤدي خدمات التصديق الإلكتروني، والتي تتجلى في ضرورة أن تتمتع جهة التصديق الإلكتروني سواء كان شخص طبيعي أو الشخص المعنوي بمؤهلات والخبرة اللازمة والمؤهلة في ميدان تكنولوجيات الإعلام والإتصال وخاصة للقيام بخدمات التصديق الإلكتروني، هذا إضافة إلى ضرورة تمتعه بقدرة مالية كافية، وأن يكون شخصًا طبيعيًا من جنسية جزائرية أو شخصًا معنويًا خاضعًا للقانون الجزائري، وأن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الإلكتروني.[5]

ولقد إشترط المشرع الجزائري شرط شهادة التأهيل والحصول على الترخيص، والإعتماد من الجهات المعنية التي تباشر نشاط التصديق الإلكتروني، بنصه: "يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الإقتصادية للتصديق الإلكتروني".[6]

يعد الحصول على الترخيص شرطًا ضروريًا لمزاولة هذا النشاط بغرض الحفاظ على مصالح المتعاملين إلكترونيًا، لأنه يعزز نوعًا من الثقة والآمان لديهم على عمل هذه الجهات وكذا يقلل من إحتمال تعرضهم للإحتيال من طرفها[7]، وقد تم تعريف الترخيص بموجب الفقرة 10 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر بأنه: "نظام إستغلال خدمات التصديق الإلكتروني الذي يتجسد في الوثيقة الرسمية الممنوحة لمؤدي الخدمات بطريقة شخصية، تسمح له بالبدء الفعلي في توفير خدماته".

---

[1]- الفقرة 13 من المادة 02 من القانون رقم: 15-04 السالف الذكر.

[2]- الفقرة 01 من المادة 28 من القانون رقم: 15-04 السالف الذكر.

[3]- الفقرة 12 من المادة 02 من القانون رقم: 15-04 السالف الذكر.

[4]- الفقرة 01 من المادة 30 من القانون رقم: 15-04 السالف الذكر.

[5]- المادة 34 من القانون رقم: 15-04 السالف الذكر.

[6]- المادة 33 من القانون رقم: 15-04 السالف الذكر.

[7]- صليحة مرباح، **دور التصديق الإلكتروني في إثبات المعاملات الإلكترونية وحفظها**، مخبر القانون الخاص المقارن، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي-الشلف،مجلة الدراسات القانونية المقارنة، المجلد 07، العدد01، 2021، الجزائر، ص 878.

الملاحظ أن المشرع الجزائري أشار إلى وجوب حصول مؤدي خدمات التصديق الإلكتروني -الذي يقدم خدمات التصديق لصالح الجمهور- على الترخيص لمزاولة نشاطه، تمنحه السلطة الإقتصادية للتصديق الإلكتروني بعد أن يستوفي على مجموعة من الشروط اللازمة، غير أنه لم يشر إلى وجوب حصول الطرف الثالث الموثوق على ذلك -الذي يقدم خدمات التصديق لصالح المتدخلون في الفرع الحكومي- من طرف السلطة الحكومية للتصديق.[1]

ومنه الترخيص الممنوح من السلطة الإقتصادية للتصديق الإلكتروني مرهون بالحصول على شهادة التأهيل لمدة سنة (01) واحدة قابلة للتجديد مرة واحدة لكل شخص طبيعي أو معنوي، وذلك لتهيئة كل الوسائل اللازمة لتأدية خدمات التصديق الإلكتروني، ولا يمكن لحامل شهادة التأهيل تأدية خدمات التصديق الإلكتروني إلا بعد الحصول على الترخيص.[2]

بعد أن تتم التهيئة يقدم حامل شهادة التأهيل طلب الحصول على الترخيص فتقوم السلطة الإقتصادية للتصديق الإلكتروني بنفسها أو بواسطة مكاتب تدقيق معتمدة بمطابقة طالب الترخيص مع سياسة التصديق الإلكتروني، والتأكد من توافر الشروط المتطلبة قانونًا وفي حالة المطابقة تمنحه الترخيص[3]، وتمنح شهادة التأهيل والترخيص بصفة شخصية ولا يمكن التنازل عنهما للغير[4]، وفي حالة رفضها منح شهادة التأهيل والترخيص يجب أن يكون رفضها مسببًا ويتم تبليغه للمعني بالأمر مقابل إشعار بالإستلام[5].

أما إذا منحت الترخيص فلابد أن يرفق بدفتر شروط من طرف السلطة الإقتصادية للتصديق الإلكتروني يحدد فيه شروط وكيفيات تأدية خدمات التصديق الإلكتروني وكذا توقيع شهادة التصديق الإلكتروني الخاصة بمؤدي خدمات التصديق الإلكتروني[6]، ويكون الترخيص صالحًا لمدة خمس (05) سنوات قابلة للتجديد عند إنتهاء صلاحيته وفقًا للشروط المحددة في دفتر الأعباء[7].

ج- السلطات المكلفة بمتابعة ومراقبة نشاط جهات التصديق الإلكتروني:

إستحدث المشرع الجزائري بموجب القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر في الفصل الثاني من الباب الثالث سلطات التصديق الإلكتروني، وهذه السلطات تتمثل في السلطة الوطنية والسلطة الحكومية وكذا السلطة الإقتصادية للتصديق الإلكتروني، وحدد هيكلة وتسيير ومهام كل سلطة على نحو تكمل كل

[1]- رضوان قرواش، مرجع سابق، ص 413.
[2]- المادة 35 من القانون رقم: 15-04 السالف الذكر.
[3]- شيخ سناء، مرجع السابق، ص 146.
[4]- المادة 39 من القانون رقم: 15-04 السالف الذكر.
[5]- المادة 37 من القانون رقم: 15-04 السالف الذكر.
[6]- المادة 38 من القانون رقم: 15-04 السالف الذكر.
[7]- المادة 40 من القانون رقم: 15-04 السالف الذكر.

منهما عمل الآخرى، قصد ضبط ومتابعة ومراقبة نشاط جهات التصديق الإلكتروني وتوفير عنصري الآمان والثقة لدى المتعاملين.

ج-1- السلطة الوطنية للتصديق الإلكتروني:

نص المشرع الجزائري على السلطة الوطنية للتصديق الإلكتروني في المادة 16 وما بعدها من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر، وهي عبارة عن سلطة إدارية تنشأ لدى الوزير الأول، مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي، ويتم تحديد مقرها عن طريق التنظيم[1]، وتتشكل من مجلس ومصالح تقنية وإدارية.

يتشكل مجلس السلطة من خمسة (05) أعضاء من بينهم الرئيس، يتم تعينهم من طرف رئيس الجمهورية على أساس كفاءتهم لاسيما في مجال العلوم التقنية المتعلقة بتكنولوجيات الإعلام والإتصال وفي مجال قانون تكنولوجيات الإعلام والإتصال وفي إقتصاد تكنولوجيات الإعلام والإتصال، ويتمتع المجلس بجميع الصلاحيات اللازمة لأداء مهام السلطة وبهذه الصفة يمكن المجلس أن يستعين بأي كفاءة من شأنها أن تساعده في أشغاله، وتحدد عهدة أعضاء مجلس السلطة بأربع (04) سنوات قابلة للتجديد مرة واحدة (01)[2]، بينما يسير المصالح التقنية والإدارية للسلطة مدير عام يعينه رئيس الجمهورية بناء على إقتراح من الوزير الأول، حيث يحدد تنظيم هذه المصالح وسيرها ومهامها عن طريق التنظيم[3].

تكلف السلطة الوطنية للتصديق الإلكتروني بتسجيل الإعتمادات المالية اللازمة لسير السلطة ضمن ميزانية الدولة، وكذا تكلف بترقية إستعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية إستعمالهما، وتسند لها أيضًا المهام التالية:

- إعداد سياستها للتصديق الإلكتروني والسهر على تطبيقها، بعد الحصول على الرأي الإيجابي من قبل الهيئة المكلفة بالموافقة؛

- الموافقة على سياسات التصديق الإلكتروني الصادرة عن السلطتين الحكومية والإقتصادية للتصديق الإلكتروني؛

- إبرام إتفاقيات الإعتراف المتبادل على المستوى الدولي؛

- إقتراح مشاريع تمهيدية لنصوص تشريعية أو تنظيمية تتعلق بالتوقيع الإلكتروني أو التصديق الإلكتروني على الوزير الأول؛

[1]- المرسوم التنفيذي رقم: 16- 134 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسير مهامها، ج.ر.ج.ج.ش العدد 26، الصادرة في 28 أفريل 2016.

[2]- المادة 19 من القانون رقم: 15-04 السالف الذكر.

[3]- المادة 20 من القانون رقم: 15-04 السالف الذكر.

- القيام بعمليات التدقيق على مستوى السلطتين الحكومية والإقتصادية للتصديق الإلكتروني، عن طريق الهيئة الحكومية المكلفة بالتدقيق.[1]

ج-2- السلطة الحكومية للتصديق الإلكتروني:

نص المشرع الجزائري على السلطة الحكومية للتصديق الإلكتروني في المادة 26 وما يليها من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر، والتي تنشأ لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والإتصال وتتمتع بالإستقلال المالي والشخصية المعنوية[2]، ويحدد طبيعتها وتشكيلها وتنظيمها وسيرها عن طريق التنظيم[3].

وتكلف بالمهام المتعلقة بمتابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثلاثة الموثوقة مع توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي، وتسند لها أيضًا المهام التالية:

- إعداد سياستها للتصديق الإلكتروني وعرضها على السلطة للموافقة عليها، والسهر على تطبيقها؛

- الموافقة على سياسات التصديق الصادرة عن الأطراف الثلاثة الموثوقة، والسهر على تطبيقها؛

- الإحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها والبيانات المرتبطة بمنحها من قبل الطرف الثالث الموثوق، بغرض تسليمها إلى السلطات القضائية المختصة عند الإقتضاء طبقًا للأحكام التشريعية والتنظيمية المعمول بها؛

- نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة؛

- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريًا أو بناء على طلب منها؛

- القيام بعملية التدقيق على مستوى الطرف الثالث الموثوق عن طريق الهيئة الحكومية المكلفة بالتدقيق طبقًا لسياسة التصديق.[4]

ج-3- السلطة الإقتصادية للتصديق الإلكتروني:

لم يورد المشرع الجزائري تعريفًا للسلطة الإقتصادية للتصديق الإلكتروني وإنما تطرق للجهة المكلفة بتعيينها والمتمثلة في السلطة المكلفة بضبط البريد والمواصلات السلكية

[1]- المادة 18 من القانون رقم: 15-04 السالف الذكر.

[2]- المادتين 26 و27 من القانون رقم: 15-04 السالف الذكر.

[3]- المرسوم التنفيذي رقم: 16-135 المؤرخ في 25 أفريل 2016، المحدد لطبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، ج.ر.ج.ج.ش العدد 26، الصادرة 28 أفريل 2016.

[4]- المادة 28 من القانون رقم: 15-04 السالف الذكر.

واللاسلكية[1]، وتكلف هذه السلطة بمتابعة ومراقبة مؤدي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكترونيين لصالح الجمهور، وفي هذا الإطار تتولى المهام التالية:

- إعداد سياستها للتصديق الإلكتروني وعرضها على السلطة للموافقة عليها، والسهر على تطبيقها؛

- منح التراخيص لمؤدي خدمات التصديق الإلكتروني بعد موافقة السلطة؛

- الموافقة على سياسات التصديق الصادرة عن مؤدي خدمات التصديق الإلكتروني، والسهر على تطبيقها؛

- الإحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها والبيانات المرتبطة بمنحها من طرف مؤدي خدمات التصديق الإلكتروني، بغرض تسليمها إلى السلطات القضائية المختصة عند الإقتضاء طبقًا للأحكام التشريعية والتنظيمية المعمول بها؛

- نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة؛

- إتخاذ التدابير اللازمة لضمان إستمرارية الخدمات في حالة عجز مؤدي خدمات التصديق الإلكتروني عن تقديم خدماته؛

- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة، دوريًا أو بناء على طلب منها؛

- التحقق من مدى مطابقة طالبي التراخيص مع سياسة التصديق الإلكتروني بنفسها أو عن طريق مكاتب تدقيق معتمدة؛

- السهر على وجود منافسة فعلية ونزيهة بإتخاذ التدابير اللازمة لترقية أو إستعادة المنافسة بين مؤدي خدمات التصديق الإلكتروني؛

- التحكيم في النزاعات القائمة بين مؤدي خدمات التصديق الإلكتروني فيما بينهم أو مع المستعملين طبقًا للتشريع المعمول به؛

- مطالبة مؤدي خدمات التصديق الإلكتروني أو كل شخص معين بأي وثيقة أو معلومة، تساعدها في تأدية المهام المخولة لها بموجب هذا القانون؛

- إعداد دفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني، وعرضه على السلطة للموافقة عليه؛

- إجراء كل مراقبة طبقًا لسياسة التصديق الإلكتروني ودفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني؛

[1]- المادة 29 من القانون رقم: 15-04 السالف الذكر.

- إصدار التقارير والإحصائيات العمومية وكذا تقرير سنوي يتضمن وصف نشاطاتها مع إحترام مبدأ السرية؛

- تقوم السلطة الإقتصادية للتصديق الإلكتروني بتبليغ النيابة العامة بكل فعل ذي طابع جزائي يكتشف بمناسبة تأدية مهامها.[1]

د- شهادة التصديق الإلكتروني:

تظهر أهمية شهادة التصديق الإلكتروني في كونها شهادة تؤكد فيها هيئة التصديق مدى صحة التوقيع الإلكتروني ونسبته إلى صاحبه، كما تحدد هوية الموقع ومدى إستجابة التوقيع للشروط القانونية[2]، كما تؤكد أيضًا على أن البيانات الموقع عليها والتي يتضمنها المستند الإلكتروني هي بيانات صحيحة، ولم يتم التلاعب فيها سواء بالحذف أو بالتعديل أو بالتغيير أو بالإضافة، وهو الأمر الذي من شأنه أن يؤدي إلى ترسيخ الثقة والأمان لدى المتعاملين عبر الإنترنت[3].

د-1- تعريف شهادة التصديق الإلكتروني:

سنتطرق إلى تعريف شهادة التصديق الإلكتروني في الفقه، ثم نتطرق إلى تعريفها في مختلف التشريعات المقارنة، ثم نتطرق وفقًا لما ورد في التشريع الجزائري.

د-1-1- تعريف شهادة التصديق الإلكتروني في الفقه:

عرفت شهادة التصديق الإلكتروني بأنها: "عبارة عن سجل إلكتروني صادر عن جهة توثيق معتمدة، وهذا السجل يحتوي على معلومات عن الشخص الذي يحملها والجهة المصدرة لهذا السجل وتاريخ صلاحيتها والمفتاح العام للشخص، وهذه الشهادة بمثابة هوية يصدرها شخص محايد للتعريف بالشخص الذي يحملها وللمصادقة على توقيعه الإلكتروني وعلى المعاملات الإلكترونية"[4]، وعرفت أيضًا بأنها: "الشهادات التي يصدرها مقدمو خدمات التصديق الإلكتروني المرخص لهم من قبل الجهات المسؤولة في الدولة، لتشهد بأن التوقيع الإلكتروني هو توقيع صحيح ينسب إلى من أصدره، ويستوفي الشروط والضوابط المطلوبة فيه، بإعتباره دليل إثبات يعول عليه"، كما عرفت بأنها: "مستند إلكتروني يربط بين المفتاح العام وشخص معين، ويحدد هوية ذلك الشخص"[5]، وعرفت كذلك بأنها: "صك أمان صادر عن جهة مختصة، يفيد صحة وضمان المعاملة الإلكترونية، وذلك من حيث صحة البيانات

[1]- المادة 30 من القانون رقم: 15-04 السالف الذكر.

[2]- شيخ سناء، مرجع السابق، ص 150.

[3]- بلحسيني حمزة، مرجع السابق، ص 115.

[4]- باهة فاطمة، **آثار قواعد الإثبات الإلكتروني على المراكز القانونية للخصوم "دراسة مقارنة"**، أطروحة الدكتوراه علوم، تخصص: قانون إجرائي، فرع: حقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي ليابس بسيدي بلعباس، 2017 /2018، ص 389.

[5]- بن مشري عبد الحليم، مقري صونيا، مرجع السابق، ص 108.

ومضمون المعاملة وأطرافها"، وتم تعريفها كذلك: "بأنها مستند إلكتروني يؤكد به الشخص وقائع معينة"[1].

د-1-2- التعريف الدولي لشهادة التصديق الإلكتروني:

عرفها قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 بموجب الفقرة (ب) من المادة 02 بأنها: "تعني رسالة بيانات أو سجلًا آخر، يؤكدان الإرتباط بين الموقع وبيانات إنشاء التوقيع"[2]، يستشف مما تقدم أن لم يتطرق صراحة إلى تعريف شهادة التصديق المعتمدة أو المؤهلة، وأيضًا فقد إكتفى بتحديد دور الشهادة والمتمثل في بيان الصلة التي تربط بين الشخص الموقع وبيانات إنشاء التوقيع.

وعرفها التوجيه الأوروبي رقم: 1999-93 المتعلق بشأن إرساء إطار قانوني مشترك لإستخدام التوقيع الإلكتروني السالف الذكر في الفقرة 09 من المادة 02 بأنها: "شهادة التصديق البسيطة بأنها: شهادة إلكترونية تربط بين بيانات التحقق من التوقيع وبين شخص معين تؤكد هوية هذا الشخص"[3]، وألغي بموجب اللائحة رقم: 910-2014 المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية السالفة الذكر وعرفتها هذه الأخيرة في الفقرة 14 من المادة 03 بأنها: "شهادة التوقيع الإلكتروني تعني: "الشهادة الإلكترونية التي تربط بيانات التحقق من صحة التوقيع الإلكتروني بشخص طبيعي، وتؤكد على الأقل إسم أو إسم مستعار لذلك الشخص"[4]، يتضح من خلال التعريفين السابقين أنه لم يشترط أن يكون هناك إرتباط بين الموقع وبيانات إنشاء التوقيع.

أما شهادة التصديق المؤهلة عرفها التوجيه الأوروبي رقم: 1999-93 المتعلق بشأن إرساء إطار قانوني مشترك لإستخدام التوقيع الإلكتروني السالف الذكر في الفقرة 10 من المادة 02 منه بأنها: "شهادة تستوفي المتطلبات المنصوص عليها في الملحق الأول، والتي يقدمها المكلف بخدمة التصديق الذي يستوفي للمتطلبات المنصوص عليها في الملحق الثاني"[5]، وألغي

---

[1]- باهة فاطمة، مرجع سابق، ص 389.

[2]-Art 02 paragraphe b du Loi type de la CNUDCI sur les signatures électroniques 2001 dispose que: «Le terme "certificat" désigne un message de données ou un autre enregistrement confirmant le lien entre un signataire et des données afférentes à la création de signature».

[3]-Art 02 paragraphe 09 du La directive 1999/93/CE du PEC, Abrogé par RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que : « certificat, une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne».

[4]-Art 03 paragraphe 14 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: «certificat de signature électronique, une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne».

[5]-Art 02 paragraphe 10 du La directive 1999/93/CE du PEC, Abrogé par RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: «certificat qualifié, un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II».

بموجب اللائحة رقم: 910-2014 المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية سالفة الذكر وعرفت هذه الأخيرة شهادة توقيع إلكتروني مؤهلة في الفقرة 15 من المادة 03 منها بأنها: "هي شهادة توقيع إلكتروني يتم إصدارها من قبل مقدم خدمات التوثيق المؤهل، وتستوفي المتطلبات المنصوص عليها في الملحق الأول"[1]، يتضح من خلال هذا التعريف بأنه قد إكتفى بالإشارة على تحديد المتطلبات والشروط المتعلقة بمقدم خدمة التصديق، وأغفل على النص على المتطلبات والشروط المحددة والواجب توافرها في شهادة التصديق الإلكترونية الموصوفة بعدما كان يشير لها في التوجيه الملغى.

د-1-3- تعريف شهادة التصديق الإلكتروني في التشريعات المقارنة:

عرف المشرع الفرنسي شهادة التصديق الإلكتروني بموجب المرسوم رقم: 2001-272 الصادر في 30 مارس 2001 صادر لتطبيق أحكام المادة 1316-4 من القانون المدني والمتعلق بالتوقيع الإلكتروني السالف الذكر في الفقرة 09 من المادة الأولى منه على أنها: "الشهادة الإلكترونية: وثيقة في شكل إلكتروني تأكد الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع"[2]، وألغي المرسوم السابق الذكر بمقتضى المرسوم رقم: 2017-1416 المتعلق بالتوقيع الإلكتروني السالف الذكر وأحال الأحكام المتعلقة بالشهادة التوقيع الإلكتروني الموصوفة بموجب المادة الأولى منه إلى أحكام اللائحة رقم: 910-2014 المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية سالفة الذكر، وبالتالي فقد إستند إلى التعريف الوارد في هذه الأخيرة، والذي سبق أن تم التطرق إليه أعلاه.

وعرفها المشرع المصري بموجب قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر في الفقرة (و) من المادة الأولى منه بأنها: "شهادة التصديق الإلكتروني: الشهادة التي تصدر من الجهة المرخص لها بالتصديق، وتثبت الإرتباط بين الموقع وبيانات إنشاء التوقيع" وهو نفس التعريف الوارد في اللائحة التنفيذية لهذا القانون المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر بموجب الفقرة 07 من المادة الأولى منها.

[1]-Art 03 paragraphe 15 du RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, op. cit, dispose que: «certificat qualifié de signature électronique, un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe I».

[2] -Art 01 paragraphe 09 du Décret n°- 2001 /272 du 30 mars 2001, op. cit, dispose que « Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signatair».

د-1-4- تعريف شهادة التصديق الإلكتروني في التشريع الجزائري:

أما بالنسبة لموقف المشرع الجزائري فقد أطلق عليها تسمية الشهادة الإلكترونية وذلك بموجب المرسوم التنفيذي رقم: 07-162 المتعلق بنظام إستغلال الشبكات بما فيها السلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية السالف الذكر، والذي عرفها في المادة 03 منه على أنها: "وثيقة في شكل إلكتروني، تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع"، إلا أنه قسمها إلى نوعين الأولى أطلق عليها تسمية الشهادة الإلكترونية وعرفها في الفقرة 08 من المادة 03 مكرر بأنها: "وثيقة في شكل إلكتروني، تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع"، والثانية أطلق عليها تسمية الشهادة الإلكترونية الموصوفة وعرفها في الفقرة 09 من المادة 03 مكرر بأنها: "شهادة إلكترونية تستجيب للمتطلبات المحددة".[1]

يلاحظ على التعريف الذي أورده المشرع الجزائري بأنه ركز على شكل شهادة التصديق فهي إلكترونية المصدر، وأيضًا على وظيفتها المتمثلة في الربط بين معطيات التوقيع الإلكتروني والموقع[2]، كما قد أغفل النص على المتطلبات المحددة المشار إليها في التعريف، فيكون تعريف الشهادة الإلكترونية الموصوفة مبهمًا لا يحمل دلالة واضحة لأنه أسند تفصيل التعريف إلى عنصر غير منصوص عليه وهو"المتطلبات المحددة".[3]

ثم جاء المشرع بعد ذلك في القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر وغير تسميتها وأطلق عليها تسمية "شهادة التصديق الإلكتروني" وقسمها أيضًا إلى نوعين، الأولى شهادة التصديق الإلكتروني العادية وعرفها في الفقرة 07 من المادة 02 بأنها: "وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع"، وهو تقريبًا نفس التعريف الوارد بموجب المرسوم التنفيذي رقم: 07-162 المتعلق بنظام إستغلال الشبكات بما فيها السلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية السالف الذكر، وهي الشهادة دورها إثبات صحة بيانات التوقيع الإلكتروني ومدى صلتها بالموقع ولا تتضمن بيانات محددة.

أما الثانية فهي شهادة التصديق الإلكتروني الموصوفة وعرفها في المادة 15 من ذات القانون بأنها: "شهادة تصديق إلكتروني تتوافر فيها الشروط والمتطلبات المنصوص عليها في المادة الخامسة عشر من القانون رقم: 15-04"، يبدو أن المشرع الجزائري قد تدارك إغفال النص على البيانات اللازمة لتوافرها في شهادة التصديق الإلكترونية الموصوفة وحددها بموجب المادة 15 من نفس القانون، وتعد شهادة التصديق الإلكتروني الموصوفة أكثر حجية

[1]- طه عيساني، مرجع السابق، ص 566.
[2]- باهة فاطمة، مرجع السابق، ص-ص 390-391.
[3]- طنجاوي مراد، مرجع السابق، ص 136.

مقارنة بشهادة التصديق الإلكتروني البسيطة، وهذا لإشتمالها على مجموعة من البيانات التي تؤكد نسبة التوقيع الإلكتروني إلى صاحبه.[1]

وبالرجوع إلى المادة 15 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر نجد أن المشرع الجزائري قد نص على هذه البيانات كالتالي:

- **بيانات تتعلق بالموقع:**

وتتمثل هذه البيانات فيما يلي:

- إسم الموقع أو الإسم المستعار الذي يسمح بتحديد هويته[2]؛

- إمكانية إدراج صفة خاصة للموقع عند الإقتضاء، وذلك حسب الغرض من إستعمال الشهادة التصديق الإلكتروني[3]؛

- بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني[4]؛

- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر عند الإقتضاء[5].

- **بيانات تتعلق بشهادة التصديق:**

وتتمثل هذه البيانات فيما يلي:

- الإشارة إلى أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة[6]؛

- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني[7]؛

- رمز تعريف شهادة التصديق الإلكتروني الموصوفة[8]؛

- حدود إستعمال شهادة التصديق الإلكتروني الموصوفة عند الإقتضاء[9]؛

- حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني عند الإقتضاء[10].

---

[1]- باهة فاطمة، مرجع سابق، ص 392.

[2]- المادة 3/15/ بند (ج) من القانون رقم: 15-04 السالف الذكر.

[3]- المادة 3/15/ بند (د) من القانون رقم: 15-04 السالف الذكر.

[4]- المادة 3/15/ بند (هـ) من القانون رقم: 15-04 السالف الذكر.

[5]- المادة 3/15/ بند (ك) من القانون رقم: 15-04 السالف الذكر.

[6]- المادة 3/15/ بند (أ) من القانون رقم: 15-04 السالف الذكر.

[7]- المادة 3/15/ بند (و) من القانون رقم: 15-04 السالف الذكر.

[8]- المادة 3/15/ بند (ز) من القانون رقم: 15-04 السالف الذكر.

[9]- المادة 3/15/ بند (ط) من القانون رقم: 15-04 السالف الذكر.

[10]- المادة 3/15/ بند (ي) من القانون رقم: 15-04 السالف الذكر.

- بيانات تتعلق بالجهات المكلفة بالتصديق الإلكتروني:

تتمثل البيانات في ذكر هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له بإصدار شهادة التصديق الإلكتروني الموصوفة، بالإضافة إلى تحديد البلد الذي يقيم فيه[1].

الفرع الثالث: الشروط اللازمة للإعتداد بالمستند الإلكتروني كوسيلة الإثبات

لم يكن إضفاء الحجية على المستندات الإلكترونية وجعلها أداة لإثبات المعاملات الإلكترونية أمرًا مطلقًا، بل قيدته أغلب التشريعات التي أعترفت له بالحجية في الإثبات بشروط يلزم توافرها لإكتسابه الحجية وإعتباره دليلًا في الإثبات.

أولًا: الشروط المتعلقة بالكتابة الإلكترونية على المستند الإلكتروني

لقد أقر المشرع الفرنسي بحجية الكتابة الإلكترونية في الإثبات وأخذ بنهج النظير الوظيفي، حيث نص في المادة 1316-3 من ق.م.ف المضافة بالقانون رقم: 2000-230 الصادر في 13 مارس 2000 المتعلق بتكييف قواعد الإثبات مع تكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني السالف الذكر على أن: "الكتابة على دعامة إلكترونية لها نفس القوة في الإثبات للكتابة على دعامة ورقية"[2]، وحدد الشروط الواجب توافرها حتى يمكن الإعتداد بالكتابة الإلكترونية في الإثبات في المادة 1316-1 من ق.م.ف المضافة بالقانون رقم: 2000-230 الصادر في 13 مارس 2000 المتعلق بتكييف قواعد الإثبات مع تكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني السالف الذكر التي نصت على أن: "يعتد بالكتابة المتخذة شكلًا إلكترونيًا كدليل شأنها في ذلك شأن الكتابة على دعامة ورقية، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تعد وتحفظ في ظل ظروف من شأنها أن تضمن سلامتها"[3]، إلا أنه قد تم إلغاء المادتين السابقتي الذكر بموجب الأمر رقم: 2016-131 المتعلق بإصلاح قانون العقود والنظام العام وإثبات الإلتزامات السالف الذكر وإحتفظ المشرع الفرنسي بذات مضمون المادتين في المادة 1366 من ق.م.ف[4].

[1]- المادة 3/15 بند (ب) من القانون رقم: 15-04 السالف الذكر.

[2]-Art 1316-3 du C.C.F (Création par Loi n°2000-230 du 13 mars 2000 - art. 1 JORF 14 mars 2000, Abrogé par Ordonnance n°2016-131 du 10 février 2016 - art. 3) dispose que: « L'écrit sur support électronique a la même force probante que l'écrit sur support papier».

[3]-Art 1316-1 du C.C.F (Création par Loi n°2000-230 du 13 mars 2000 - art.1 JORF 14 mars 2000, Abrogé par Ordonnance n°2016-131 du 10 février 2016 - art. 3) dispose que: « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier، sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité».

[4]-Art 1366 du C.C.F (Ordonnance n°2016-131 du 10 février 2016 - art. 4) dispose que: « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité».

وقد سار المشرع الجزائري على نفس النهج، حيث تبنى مبدأ التعادل الوظيفي بين الكتابة في الشكل التقليدي والكتابة في شكل الإلكتروني بموجب المادة 323 مكرر1 من القانون المدني المعدل والمتمم بالقانون رقم: 05-10 السالف الذكر والذي نص على أن: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالكتابة بالإثبات على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"، فقد أقر المشرع الجزائري بمبدأ التعادل الوظيفي بين كل من الكتابة الإلكترونية والكتابة التقليدية أي لهما نفس الفعالية من حيث الحجية وصحة الإثبات، وذلك بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

وتجدر بنا الإشارة إلى الجدل الفقهي الذي آثاره مضمون المادة 1316-1 من ق.م.ف - المادة 1366 من ق.م.ف الحالي- والتي تقابلها المادة 323 مكرر1 من ق.م.ج، حول مدى إعتبار الكتابة في الشكل الإلكتروني معادلة في حجيتها حجية الكتابة الرسمية على الدعامة الورقية، وتم طرح التساؤل التالي: فهل يمكن إثبات العقود التي يتطلب القانون في إثباتها الكتابة الرسمية بالكتابة في الشكل الإلكتروني؟

إنقسم الفقه حول هذه المسألة إلى فريقين، ذهب الفريق الأول إلى إعتبار أن نطاق المادة 1316 من ق.م.ف -المادة 1366 من ق.م.ف الحالي- يتسع ليشمل الكتابة التي تكون في الشكل الرسمي وهذا نظرًا لعمومية تعريف الكتابة الواردة فيها، بينما ذهب الفريق الثاني إلى القول بأن هذا التدخل التشريعي قد قصر مجال إعماله في العقود العرفية فقط، ذلك أن يشترط لصحة إثبات بعض العقود بالكتابة الرسمية حضور الضابط العمومي وتوقيعه، ويعد حضور هذا الأخير شرطًا لإكتساب المستند صفة الرسمية هو الذي يمنحها رسميتها والذي لا يمكن حضوره إذا ما تعلق الأمر بالكتابة الإلكترونية.[1]

فقد حسم الخلاف في فرنسا لمصلحة الفريق الذي نادى بضرورة التعادل الوظيفي بين الكتابة الرسمية العادية والكتابة الرسمية الإلكترونية وأصدر المشرع الفرنسي المرسوم رقم: 2005/973 الخاص بالمستندات الموثقة المؤرخ في 10 أوت 2005، حيث وضح هذا المرسوم كيفيات إنشاء وحفظ هذه المستندات التي يمكن أن تنشأ على دعامة إلكترونية بمقتضى المادة 1317 من القانون المدني وقد ساعد على إصداره وجود شبكة خاصة بالموثقين REAL، وذلك حتى يتم تداول الوثائق داخل هذه الشبكة وتتم عملية التوثيق من طرف أكثر من موثق بعد أن يوقع الأطراف على المستند بصفة رقمية عن طريق نقل التوقيع الخطي بالماسح الضوئي أو عن طريق القلم الإلكتروني، حيث يقوم الموثق بالتوقيع إلكترونيًا على المستند عن طريق الشريحة الإلكترونية REAL التي تعتبر إجراء للتوقيع الإلكتروني الآمن وضعه المجلس

[1]- سكيل رقية، **الإثبات بالمحررات الرسمية الإلكترونية في المواد المدنية والتجارية في التشريع الجزائري -دراسة مقارنة-**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص-ص 241-242.

الأعلى للموثقين، ويخص التوقيع من طرف الموثقين على المستندات الرسمية الإلكترونية ونسخها.[1]

بمعنى أن يتدخل في عملية التوثيق أكثر من موثق حيث يحضر كل من المتعاقدين أمام الموثق المتواجد في مدينته ومعه شهود وذلك بعد أن يتفقا على من يكون منهما الموثق الرئيسي، بعدها يقوم الموثق الآخر بالإلتزام بإرسال المستند الإلكتروني إلى الموثق الرئيسي ويتم الإرسال عبر شبكة داخلة للموثقين، كما يتم التوقيع من قبل المتعاقدين والشهود سواء عن طريق التوقيع بالماسح الضوئي أو بالقلم الإلكتروني، بعدها يقوم الموثق الرئيسي على المستند الإلكتروني ليضيف عليه الصفة الرسمية.[2]

أما بالنسبة لموقف المشرع المصري فقد تدارك الأمر ووسع من نطاق الكتابة الإلكترونية وجعلها في نفس مكانة الكتابة الرسمية أو العرفية في مجال المعاملات المدنية والتجارية وحتى الإدارية بموجب المادة 15 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر، الذي نص صراحة على أن: "للكتابة الإلكترونية وللمحررات الإلكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية، متى إستوفت الشروط المنصوص عليها في هذا القانون وفقًا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون".

بعد التطرق إلى مختلف التشريعات المقارنة وإستعراض موقف المشرع الجزائري، يستفاد مما سبق أن هذا الأخير كرس مبدأ التعادل الوظيفي بين الكتابة الإلكترونية والكتابة التقليدية، بما يتيح الإعتداد بالمستند الإلكتروني في الإثبات، واعتبار الكتابة الإلكترونية بمثابة الكتابة على دعامة ورقية، شريطة:

1- أن تكون الكتابة الإلكترونية مقروءة ومفهومة وواضحة:

يشترط في الكتابة تحقق خاصية القراءة والوضوح سواء كان على دعامة ورقية أو إلكترونية، أي يكون المستند بحروف أو رموز أو إشارات مفهومة ومعروفة، ويتحقق هذا الشرط في سهولة الكتابة لتقرئ مباشرة[3]، بمعنى أن يتسنى فهم وإستيعاب المستند الإلكتروني وإدراك محتواه وكذا أن يمكن إنسابه إلى صاحبه.

---

[1]- سكيل رقية، مرجع سابق، ص-ص 242-243.

[2]- سكفالي ريم، محمودي بشير، **الحجية القانونية للمحررات الإلكترونية**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 272.

[3]- حسان سعاد، مرجع السابق، ص-ص 59-60.

لم يشر المشرع الجزائري صراحة إلى هذا الشرط عند تعريفه للكتابة في المادة 323 مكرر1 المضافة بموجب القانون رقم: 05-10 المعدل والمتمم للقانون المدني السالف الذكر، وإنما نص على شرطين آخرين وهما: التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها، غير أنه ومن خلال التمعن في المادة 323 مكرر من نفس القانون يمكن إستخلاص هذا الشرط ضمنًا من خلال عبارة "ذات معنى مفهوم"، أي أنه لا يعقل أن تنتج الكتابة من تسلسل الحروف أو الأرقام أو البيانات دون إمكانية قراءتها وإدراكها، وهو نفس موقف المشرع الفرنسي من خلال عبارة "ذات دلالة تعبيرية واضحة ومفهومة" وذلك عند تعريفه للكتابة بموجب المادة 1316 من ق.م.ف الملغاة، والتي أحتفظ بمضمونها في المادة 1365 من ق.م.ف بموجب تعديله بالأمر رقم: 2016-131 المؤرخ في 10 فيفري 2016 المتعلق بإصلاح قانون العقود والنظام العام وإثبات الإلتزامات السالف الذكر.

وشرط القراءة هذا يتحقق بسهولة في الكتابة الخطية لأنها تقرأ مباشرة، ولكن يلاحظ عمليًا صعوبة تحديد هذا الشرط في الكتابة الإلكترونية لأنها مدونة على دعامة إلكترونية، وإذا رجعنا إلى المستندات الإلكترونية نجد أنها تدون على وسائط بلغة الآلة لا يمكن للإنسان قراءتها مباشرة إلا بإيصال المعلومات في الأجهزة الإلكترونية للترجمة إلى اللغة المقروءة للإنسان[1]، ويتم ذلك بواسطة برامج خاصة تقوم على تحويل لغة الآلة اللوغاريتمية المعقدة إلى اللغة التي يستطيع الإنسان فهمها، ويتم ذلك من خلال تحويل رموز الآلة إلى حروف واضحة ومقروءة، وهو ما من شأنه أن يساهم في تحقيق شرط إمكانية القراءة في المستند الإلكتروني[2].

وبالرغم من أن لا يتم قراءة المستندات الإلكترونية مباشرة وإنما تقرء عن طريق إستخدام الجهاز الإلكتروني بالنظر إلى طريقة التدوين والرموز المستخدمة فيه، إلا أن اللغة التي تظهر على شاشة الجهاز هي لغة مفهومة ومقروءة للمتعاقد وهذا يعني أنه قد تحقق شرط القراءة بها ويمكن فهمها، وهو ما يمكن إستخلاصه من المادة 323 مكرر من ق.م.ج وتحديدًا من خلال عبارة "مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها"، والمادة 1365 من ق.م.ف المعدلة بموجب الأمر رقم: 2016-131 المتعلق بإصلاح قانون العقود والنظام العام وإثبات الإلتزامات السالف الذكر من خلال عبارة "أيا كانت الدعامة التي تتضمنها" -المادة 1316 سابقًا-.

2-إمكانية التأكد من هوية مصدر المستند الإلكتروني:

ورد شرط التأكد من هوية الموقع في الفقرة 02 من المادة 09 من القانون النموذجي بشأن التجارة الإلكترونية سنة 1996[3] كالآتي: "يعطى للمعلومات التي تكون على شكل رسالة

[1]- حسان سعاد، مرجع سابق، ص 60.

[2]- زروق يوسف، مرجع سابق، ص 177.

[3]-Art 09 paragraphe 02 du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: «L'information prenant la forme d'un message de données se voit dûment accorder force probante. Cette force probante s'apprécie=

بيانات ما تستحقه من حجية في الإثبات، وفي تقدير حجية رسالة البيانات في الإثبات...الطريقة التي حددت بها هوية منشئها...".

وورد هذا الشرط بمقتضى المادة 323 مكرر1 من ق.م.ج بالنص: "شرط التأكد من هوية الشخص الذي أصدرها"، وبموجب المادة 1366 من ق.م.ف بالنص:"بشرط إمكانية التأكد من هوية الشخص الذي أصدرها" -المادة 1316-1 سابقًا-، وبمقتضى الفقرة (ب) من المادة 09 من اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر بالنص: "أن يكون متاحًا فنيًا تحديد مصدر إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية، ودرجة سيطرة منشئها على هذا المصدر وعلى الوسائط المستخدمة في إنشائها".

يهدف فرض هذا الشرط إلى إمكانية تحديد هوية الشخص محرر المستند الإلكتروني ليتمكن من تحمل الإلتزامات المترتبة عن ذلك ويكتسب الحقوق أيضًا[1]، وقد يكون من الصعب التحقق من الهوية في بعض التصرفات القانونية التي تنفذ بواسطة الكتابة الإلكترونية، إلا أن يمكن التأكد من نسبة ذلك بواسطة إستخدام تقنية التوقيع الإلكتروني عن طريق التدليل على الموقع الذي وافق أو حرر أو صدر منه المستند المدعى به عليه[2].

3- أن تكون الكتابة الإلكترونية معدة ومحفوظة في ظروف تضمن سلامتها:

ورد هذا الشرط في المادة 09 من القانون النموذجي بشأن التجارة الإلكترونية سنة 1996 لقبول رسالة البيانات ولإكتسابها الحجية في الإثبات كالآتي: "2- يعطى للمعلومات التي تكون على شكل رسالة بيانات ما تستحقه من حجية في الإثبات، وفي تقدير حجية رسالة البيانات في الإثبات...لجدارة الطريقة التي إستخدمت في المحافظة على سلامة المعلومات بالتعويل عليها..."، والمادة 323 مكرر1 من ق.م.ج نصت على أن: "... وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"، والمادة 1366 من ق.م.ف بالنص: "وأن تعد وتحفظ في ظل ظروف من شأنها أن تضمن سلامتها" -المادة 1316-1 سابقًا-، وبمقتضى اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر بموجب الفقرة (أ) من المادة 09 منها بالنص: "أن يكون متاحًا فنيًا تحديد وقت وتاريخ إنشاء الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية، وأن

=eu égard à la fiabilité du mode de création, de conservation ou de communication du message, la fiabilité du mode de préservation de l'intégrité de l'information, à la manière dont l'expéditeur a été identifiéet à toute autre considération pertinente ».

[1]- حسان سعاد، مرجع سابق، ص 62.

[2]- زروق يوسف، مرجع سابق، ص 261.

تتم هذه الإتاحة من خلال نظام حفظ إلكتروني مستقل وغير خاضع لسيطرة منشئ هذه الكتابة أو تلك المحررات أو لسيطرة المعني بها".

ويقصد بالشرط معدة ومحفوظة في ظروف تضمن سلامتها بأن يكون ذلك لغرض الدوام والإستمرار، بأن تحفظ الكتابة الإلكترونية على دعامة تؤدي إلى الثبات عليها وديمومتها تسمى الوسيط وهو وسيلة قابلة للتخزين والحفظ، بحيث يمكن الإعتداد بها بالرجوع إلى مضمونها وقت الحاجة والإحتجاج بها أمام القضاء في حال نشوء نزاع بين الأطراف[1]، وبالتالي فلا يمكن التعويل على الكتابة الإلكترونية الغير قادرة على الإستمرارية والإسترجاع عند الضرورة كدليل للإثبات والاحتجاج بها أمام القضاء[2].

وهو ما جسده البند (أ) من الفقرة الأولى من المادة 08 من القانون النموذجي بشأن التجارة الإلكترونية سنة 1996 بإشتراط المحافظة على رسالة البيانات في شكلها الأصلي كالآتي: "1- عندما يشترط القانون تقديم المعلومات أو الإحتفاظ بها في شكلها الأصلي تستوفي رسالة البيانات هذا الشرط إذا: أ- وجد ما يعول عليه لتأكيد سلامة المعلومات منذ الوقت الذي أنشئت فيه للمرة الأولى في شكلها النهائي، بوصفها رسالة البيانات أو غير ذلك"[3]، والبند (أ) من الفقرة 03 من نفس المادة كالآتي: "3-... أ- يكون معيار تقدير سلامة المعلومات هو تحديد ما إذا كانت قد بقيت مكتملة ودون تغيير، بإستثناء إضافة أي تظهير وأي تغيير يطرأ أثناء المجرى العادي للإبلاغ والتخزين والعرض"[4]، أي الإحتفاظ برسالة البيانات بالشكل الذي أنشئت أو أرسلت به مع دقة المعلومات.

ونصت المادة 10 من نفس القانون على شرط حفظ رسالة البيانات والرجوع إلى مضمونها كالآتي:"1-... أ- تيسر الإطلاع على المعلومات الواردة فيها على نحو يتيح إستخدامها في الرجوع إليها لاحقاً، ب- الإحتفاظ برسالة البيانات بالشكل الذي أنشئت أو أرسلت أو إستلمت به، أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشئت أو أرسلت أو إستلمت،

[1]- ندى حمزة صاحب، مرجع سابق، ص298.

[2]- بشرى زلاسي، مرجع سابق، ص 66.

[3]-Art 08 paragraphe 01 alinéa a du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: «1- Lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence:

a) S'il existe une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre».

[4]-Art 08 paragraphe 03 alinéa a du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: « 3- Aux fins de l'alinéa a du paragraphe 1 :

a) L'intégrité de l'information s'apprécie en déterminant si celle-ci est restée complète et n'a pas été altérée, exception faite de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition ».

ج- الإحتفاظ بالمعلومات إن وجدت التي تمكن من إستبانة منشأ رسالة البيانات، وجهة وصولها وتاريخ ووقت إرسالها وإستلامها".[1]

وهو ما كرسه المشرع الجزائري بموجب المادة 04 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي تنص على أن: "تحفظ الوثيقة الموقعة إلكترونيًا في شكلها الأصلي، ويتم تحديد الكيفيات المتعلقة بحفظ الوثيقة الموقعة إلكترونيًا عن طريق التنظيم"، وتطبيقًا لأحكام هذه المادة صدر المرسوم التنفيذي رقم: 16-142 المؤرخ في 05 ماي 2016 يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيًا[2]، وعرف بمقتضاه الوثيقة الإلكترونية في الفقرة الأولى من المادة 02 منه كالآتي: "مجموعة تتألف من محتوى وبنية منطقية وسمات العرض، تسمح بتمثيلها وإستغلالها من قبل الشخص عبر نظام إلكتروني"، والوثيقة الموقعة إلكترونيًا بموجب الفقرة 02 من نفس المادة كالآتي: "وثيقة إلكترونية مرفقة أو متصلة منطقيًا بتوقيع إلكتروني"، ودعامة الحفظ بموجب الفقرة 03 من نفس المادة كالآتي: "أي وسيلة مادية أيا كان شكلها أو خصائصها المادية، تسمح بإستلام وحفظ وإسترجاع الوثيقة الموقعة إلكترونيًا"، والحفظ بموجب الفقرة 04 من نفس المادة كالآتي: "مجموعة التدابير التقنية التي تسمح بتخزين الوثيقة الموقعة إلكترونيًا في دعامة للحفظ".

وفقًا للمرسوم السابق الذكر يجب أن يضمن حفظ الوثيقة الموقعة إلكترونيًا إسترجاع هذه الوثيقة في شكلها الأصلي لاحقًا، والتحقق من توقيعها الإلكتروني[3]، وأن تضمن كل عملية تجري عليها لدواعي الفعالية و/أو الأمن إسترجاعها في شكلها الأصلي[4].

ويجب على كل شخص طبيعي أو معنوي موقع و/أو مستلمها، أن يضمن حفظها بنفسه أو عبر طرف ثالث[5]، وإستعمال دعامات الحفظ وفق الشروط التي تضمن سلامتها وسيرها

---

[1]-Art 10 paragraphe 01 alinéa a, b, c du Loi type de la CNUDCI sur le commerce électronique 1996 dispose que: « Conservation des messages de données:

1. Lorsqu'une règle de droit exige que certains documents, enregistrements ou informations soient conservés, cette exigence est satisfaite si ce sont des messages de données qui sont conservés, sous réserve des conditions suivantes

a) L'information que contient le message de données doit être accessible pour être consultée ultérieurement;

b) Le message de données doit être conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues;

c) Les informations qui permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception, doivent être conservées si elles existent».

[2]- المرسوم التنفيذي رقم: 16-142 المؤرخ في 05 ماي 2016، يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيًا، ج.ر.ج.ج.ش العدد 28، الصادرة في 08 ماي 2016.

[3]- المادة 04 من المرسوم التنفيذي رقم: 16-142 السالف الذكر.

[4]- المادة 08 من المرسوم التنفيذي رقم: 16-142 السالف الذكر.

[5]- المادة 05 من المرسوم التنفيذي رقم: 16-142 السالف الذكر.

الحسن[1]، وأن يتم حفظها على دعامة حفظ يسمح في أي وقت بالنفاذ إلى كل محتواها وإسترجاعها بواسطة الوسائل التقنية الملائمة[2].

ويجب أن يتضمن حفظ الوثيقة الموقعة إلكترونيًا على الخصوص ما يأتي :

- الوثيقة الإلكترونية وتوقيعها الإلكتروني، أيا كان مرفقًا أو متصلًا بشكل منطقي؛
- شهادة التصديق الإلكتروني للموقع؛
- قائمة الشهادات الإلكترونية الوسيطة إلى غاية الوصول إلى السلطة الوطنية للتصديق الإلكتروني، عندما يتعلق الأمر بشهادة إلكترونية موصوفة؛
- قوائم الشهادات الملغاة أو نتائج التحقق من حالة الشهادات الإلكترونية الوسيطة إلى غاية الوصول للسلطة الوطنية للتصديق الإلكتروني؛
- تاريخ توقيع الوثيقة عند الإقتضاء.[3]

ويجب أن يشمل نقل الوثيقة الموقعة إلكترونيًا من دعامة حفظ إلى دعامة أخرى جميع العناصر الواردة أعلاه، وأن يتم التحقق من التوقيع الإلكتروني بعد نقلها إلى دعامة حفظ جديدة.[4]

إلا أن شرط الإستمرارية لا تتعلق بالكتابة الإلكترونية بذاتها على قدر ما تتعلق بالدعامة أو الوسيلة المحفوظة عليها، ويرى البعض أن إذا كان الورق بتكوينه وطبيعته يسمح بتحقيق هذا الشرط، فإن الخواص المادية والكيميائية التي تتكون منها الدعامة تتميز بحساسية عالية تجعل منها عرضة للتلف، وهو ما يتعارض مع فكرة الإستمرارية.[5]

إلا أن الورق ليس دائمًا هو الخيار الأمثل كدعامة موثوق بها في الكتابة، فقد يطرأ عليه هو الآخر على بعض من الآفات التي تجعله عرضة للفقدان أو التلف كالرطوبة والحرق والتمزيق وغيرها، ومن ناحية آخرى فإن التطور التكنولوجي يطالعنا على الوسائل المعتمدة لحفظ المعلومات بطرق مذهلة وتفي بالغرض المطلوب.[6]

4- عدم قابلية الكتابة الإلكترونية للتعديل والمحو:

لم يوضح المشرع الجزائري المقصود بالسلامة ولا الظروف والمعايير التي تكفل سلامة الكتابة الإلكترونية، وبناءً على ذلك يرى البعض أن الكتابة الإلكترونية تستمد سلامتها من سلامة المستند الإلكتروني إذا بقي على الحالة التي أنشأ عليها من دون أي تعديل أو تغيير،

[1]- المادة 2/06 من المرسوم التنفيذي رقم: 16-142 السالف الذكر.
[2]- المادة 1/06 من المرسوم التنفيذي رقم: 16-142 السالف الذكر.
[3]- المادة 07/ 1 من المرسوم التنفيذي رقم: 16-142 السالف الذكر.
[4]- المادة 07/ 2 من المرسوم التنفيذي رقم: 16-142 السالف الذكر.
[5]- طنجاوي مراد، مرجع سابق، ص 239.
[6]- نفس المرجع، ص 239.

ويتمحور مفهوم السلامة حول إمكانية الكشف عن أي تغيير أو تعديل الذي يطرأ على المستند الإلكتروني وهذا ما يضفي فيه على الحجية في الإثبات. [1]

لقد نص المشرع الجزائري إلى هذا الاجراء في العبارة الأخيرة من المادة 323 مكرر1 من ق.م.ج بالنص: "في ظروف تضمن سلامتها"، بمعنى أن تدون بتقنيات تضمن حفظها وتضمن سلامتها من أي تعديل أو تبديل في مضمونها ومحتواها، والمادة 1366 من ق.م.ف بالنص: "وأن تعد وتحفظ في ظل ظروف من شأنها أن تضمن سلامتها" -المادة 1316-1 سابقًا-، وبمقتضى اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر بموجب الفقرة (ج) من المادة 09 منها بالنص: "في حالة إنشاء وصدور الكتابة الإلكترونية أو المحررات الإلكترونية الرسمية أو العرفية بدون تدخل بشري جزئي أو كلي، فإن حجيتها تكون متحققة متى أمكن التحقق من وقت وتاريخ إنشائها ومن عدم العبث بهذه الكتابة أو تلك المحررات".

يشترط لكي تكون الكتابة دليلًا في الإثبات خلوها من العيوب التي تأثر بصحتها من كل صور التغيير والتحريف[2]، وأن يتم المحافظة عليها في الصورة التي تسهل إثبات دقة المعلومات التي وردت فيها، وأن تدل هذه المعلومات على من أنشاها أو تسلمها ووقت وتاريخ إرسالها[3].

إذ يسهل إكتشاف هذه العيوب في الكتابة التقليدية ويمكن تحديد مواطن التزوير والتغيير فيها، أما الكتابة الإلكترونية فبفضل طبيعتها الخاصة يمكن تعديل[4] التصرف الذي تتضمنه من قبل الأطراف بالإضافة أو الإلغاء دون أن تترك أثرًا ماديًا.[5]

إلا أن في الواقع التطبيقي فقد إستطاعت التقنيات المعلوماتية من التعامل مع هذا النوع من التحديات وجعل الكتابة الإلكترونية كتابة ثابتة عن طريق إبتكار تطبيقات تثبت المعطيات الموجودة على برنامج (Microsoft Word) إلى ملف ثابت لا يمكن تغيير في محتوياته أو

[1]- حميدة بن حمدين، امحمد نجيب شرافي، **الحجية القانونية للإثبات بالكتابة في الشكل الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية -بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 47.

[2]- زروق يوسف، مرجع سابق، ص 262.

[3]- ندى حمزة صاحب، مرجع سابق، ص 298.

[4]- تتميز الدعامات الإلكترونية على إختلاف أشكالها بسهولة إجراء تعديلات في المعطيات المدونة عليها، ذلك أنه بإمكان أي شخص يملك الخبرة في معالجة المعطيات إجراء أي تعديل، سواء بمسح أو بإضافة معطيات إلى المستند دون ترك أي أثر مادي، ماعدا البيان الذي يسجله الجهاز الإلكتروني والمتعلق بزمن وتاريخ التغيير، بل حتى هذا البيان قابل للتغيير إذ أن الجهاز يمكن أن نبرمجه وفق أي تاريخ نرغب فيه قبل القيام بتغيير المستند، وبالتالي يسجل التاريخ الذي وقع فيه التغيير ويكون موافقًا لتاريخ كتابة المستند، وللمزيد من التفصيل ينظر: بوكر رشيدة، مرجع سابق، ص 145.

[5]- شيخ سناء، مرجع سابق، ص 116.

العبث به بواسطة برنامج (PDF)، وبهذا تبقى المعطيات الموجودة على المستند الإلكتروني في صورتها النهائية غير قابلة للتعديل أو للتغيير إلا بإتلافها.[1]

كما أتاحت التقنيات الحديثة القدرة على إنشاء وثائق معادلة مع الوثائق الورقية في إمكانية قراءة مضمونها دون التلاعب فيها، عن طريق إستخدام برامج معدة لتحقيق هذا الغرض كنظام (Document image processing)، حيث يتم حفظ المعطيات في صناديق إلكترونية ويتعذر فتحها إلا بواسطة المفتاح الخاص، مما يترتب عليه محو أو إتلاف هذه الوثيقة المحفوظة إذا ما تم محاولة تعديلها.[2]

وأيضًا بفضل توفير التقنيات التي تعتمد على نظام التشفير، وقابليتها للحفظ بصيغتها النهائية لدى مقدمي خدمات التصديق الإلكتروني الذين يحرصون على سلامة الكتابة الإلكترونية من مخاطر التحريف أو التزوير والتعديل وبالتالي توفير الثقة فيها.[3]

وهو ما أكدت عليه اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر في المادة 12 منها بالنص: "مع عدم الإخلال بما هو منصوص عليه في المواد 2،3،5 من هذه اللائحة يتم من الناحية الفنية والتقنية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونيًا، بإستخدام تقنية شفرة المفتاحين العام والخاص وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات، أو بأي وسيلة مشابهة".

ثانيًا: الشروط المتعلقة بالتوقيع الإلكتروني على المستند الإلكتروني

لم يكن إضفاء الحجية على التوقيع الإلكتروني وجعله أداة لإثبات المعاملات الإلكترونية أمرًا مطلقًا، بل يلزم أن يستوفي على مجموعة من الشروط لإكتسابه الحجية وإعتباره دليلًا في الإثبات، فبمقتضى المادة 18 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر نص صراحة على الشروط الواجب توافرها في التوقيع الإلكتروني حتى يمكن أن تكون له حجية في الإثبات كالآتي: "يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية:

- إرتباط التوقيع بالموقع وحده دون غيره؛
- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني؛
- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني؛

[1]- رحمان يوسف، مرجع سابق، ص 253.
[2]- ندى حمزة صاحب، مرجع سابق، ص 298.
[3]- باهة فاطمة، مرجع سابق، ص 58.

وتحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك".

أما بالنسبة لموقف المشرع الجزائري فقد نص في الفقرة 02 من المادة 327 من ق.م.ج على أن يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1 من ذات القانون، وبالرجوع إلى هذه الأخيرة نجدها تنص على أن يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

ومما سبق ذكره، يتضح أن المشرع الجزائري قد اعترف بحجية التوقيع الإلكتروني وأقر بإمكانية الإعتداد به، رابطًا ذلك بتوفر نفس الشروط المتطلبة في الكتابة الإلكترونية كوسيلة إثبات المنصوص عليها في المادة 323 مكرر1 من ق.م.ج، والمتمثلة في إمكانية التأكد من هوية الشخص الذي أصدر التوقيع وأن يكون التوقيع معد ومحفوظ في ظروف تضمن سلامته.

وبمقتضى صدور القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر تدارك المشرع الجزائري الأمر وحدد صراحة الشروط الواجب توافرها لصحة التوقيع الإلكتروني حتى يكتسي وصف الموصوف بموجب المادة 07 من نفس القانون الذي نص على أن: "التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية:

1. أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة؛
2. أن يرتبط بالموقع دون سواه؛
3. أن يمكن من تحديد هوية الموقع؛
4. أن يكون مصممًا بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني؛
5. أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع؛
6. أن يكون مرتبطاً بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهاته البيانات".

يتضح مما سبق ذكره، أن المشرع الجزائري قد إشترط شروطًا إضافية إلى جانب ما ورد في نص المادة 323 مكرر 1 من ق.م.ج والتي يتعين توافرها لمنح الحجية في التوقيع الإلكتروني الموصوف والإعتداد به في الإثبات، وأعتبر بموجب المادة 08 من القانون آنف ذكره التوقيع الإلكتروني الموصوف وحده مماثلًا للتوقيع المكتوب سواء كان لشخص طبيعي أو معنوي.

وبصرف النظر عن أحكام المادة 08 المشار إليها أعلاه بإعتبار أن التوقيع الإلكتروني الموصوف هو وحده المساوي للتوقيع المكتوب في الحجية، إلا أنه في المادة 09 من نفس القانون فقد أقر المشرع الجزائري بعدم تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه

كدليل أمام القضاء، بسبب شكله الإلكتروني أو على الرغم من عدم إعتماده على شهادة تصديق إلكتروني موصوفة، أوأنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني.

حيث لا يتوفر في هذا التوقيع الشروط الواردة في المادة 08 المشار إليها أعلاه، وبالتالي لا يحظى بنفس الحجية التي يتمتع بها التوقيع الإلكتروني الموصوف، مع ذلك لا يعد منعدم الأثر القانوني أي لا يجوز تجريده من فاعليته القانونية، فإذا تمسك به أحد الأطراف فلا يمكن رفضه كدليل إثبات أمام القضاء كونه توقيعًا إلكترونيًا غير موصوف وأنه لا يعتمد على شهادة التصديق الإلكترونية الموصوفة.[1]

ولا يفرض على القاضي قبول هذا التوقيع الإلكتروني كونه لا يعتمد على شهادة التصديق، بل ينبغي أن ألا يحكم برفضه بمجرد التأكد على عدم توافر الشروط الواردة في المادة 08 حتى يتبين له أثر هذا التوقيع من عدمه، ولذلك يلزم على من قدمه كدليلًا للإثبات أن يؤكد مدى جدارة الثقة الموضوعة في الآليات المنشئة لهذا التوقيع الإلكتروني.[2]

وإستنادًا إلى ما سبق ذكره، فالإكتساب التوقيع الإلكتروني الموصوف الحجية وإعتبار المستند الالكتروني دليلًا في الإثبات لابد أن:

1- ينشأ على أساس شهادة تصديق إلكتروني موصوفة:

من أجل الحرص على سلامة والأمان في المعاملات الإلكترونية وحتى تحظى بالحجية الكاملة في الإثبات، فقد إشترط المشرع الجزائري أن ينشأ التوقيع الإلكتروني الموصوف على أساس شهادة تصديق إلكترونية موصوفة تصدر عن مقدم خدمات التصديق الإلكتروني أو من طرف ثالث موثوق، التي يشهد بمقتضاها بصحة التوقيع الإلكتروني ونسبته إلى من صدر عنه، وهذا حتى يكون له حجية في الإثبات مماثل للتوقيع المكتوب.

2- يكون التوقيع مرتبطاً بالموقع دون سواه:

أقر المشرع الجزائري بوجوبية أن يتم التوقيع الإلكتروني من طرف الموقع[3] وحده دون سواه، وبالتالي فإنه بتوافر هذا الشرط بالتوقيع الإلكتروني يؤدي إلى إتجاه نية الشخص الموقع على المستند بما يؤكد إرادته الصريحة في إبرام التصرف القانوني ورضائه بما جاء في المضمون، حتى يحوز على الحجية القانونية ويمكن الإعتداد به أمام القضاء.

ورد هذا الشرط بمقتضى المادة 323 مكرر 1 من ق.م.ج بالنص: "شرط التأكد من هوية الشخص الذي أصدرها"، وبموجب المادة 1366 من ق.م.ف بالنص: "بشرط إمكانية التأكد من

[1]- بن علي صليحة، **نطاق حجية التوقيع والتصديق الإلكترونيين**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 78.

[2]- نفس المرجع، ص 79.

[3]- عرفت الفقرة 02 من المادة 02 من القانون رقم: 15-04 السالف الذكر الموقع بأنه:" شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني، ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله".

هوية الشخص الذي أصدرها" -المادة 1316-1 سابقًا-، وبمقتضى الفقرة (أ) من المادة 18 من اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر بالنص: "إرتباط التوقيع بالموقع وحده دون غيره".

وجرى التحقق من إرتباط التوقيع الإلكتروني بالموقع بواسطة آلية تتمثل في جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق من التوقيع الإلكتروني[1]، ويشترط أن تكون موثوقة[2]، وأن تتوفر فيها المتطلبات الآتية:

- أن تتوافق البيانات المستعملة للتحقق من التوقيع الإلكتروني مع البيانات المعروضة عند التحقق من التوقيع الإلكتروني؛

- أن يتم التحقق من التوقيع الإلكتروني بصفة مؤكدة، وأن تكون نتيجة هذا التحقق معروضة عرضًا صحيحًا؛

- أن يكون مضمون البيانات الموقعة إذا إقتضى الأمر محددًا بصفة مؤكدة عند التحقق من التوقيع الإلكتروني؛

- أن يتم التحقق بصفة مؤكدة من موثوقية وصلاحية شهادة التصديق الإلكتروني المطلوبة عند التحقق من التوقيع الإلكتروني؛

- أن يتم عرض نتيجة التحقق وهوية الموقع بطريقة واضحة وصحيحة.[3]

وفي نفس السياق حددت اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر في المادة 10 منها على الضوابط الفنية والتقنية لكيفية تحقق من إرتباط التوقيع الإلكتروني بالموقع وحده دون غيره، وذلك متى إستند هذا التوقيع إلى منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة على النحو الوارد في اللائحة، وبتوافر على إحدى الحالتين الآتيتين:

- أن يكون هذا التوقيع مرتبطًا بشهادة تصديق إلكتروني معتمدة ونافذة المفعول، صادرة من جهة تصديق إلكتروني مرخص لها أو معتمدة؛
- أن يتم التحقق من صحة التوقيع الإلكتروني طبقًا للمادة 08 من اللائحة المذكورة أعلاه.

وبالرجوع إلى المادة 08 من نفس اللائحة نجدها تنص على أن: "تتحقق الهيئة من صحة التوقيع الإلكتروني بناء على طلب كل ذي شأن كالآتي: "تتحقق من سلامة شهادة التصديق

[1]- الفقرة 06 من المادة 02 من القانون رقم: 15-04 السالف الذكر.

[2]- المادة 12 من القانون رقم: 15-04 السالف الذكر.

[3]- المادة 13 من القانون رقم: 15-04 السالف الذكر.

الإلكتروني وتوافقها مع بيانات إنشاء التوقيع الإلكتروني، وإمكان تحديد مضمون المحرر الإلكتروني محل الفحص بدقة، وسهولة العلم بشخص الموقع".

3- يمكن من تحديد هوية الموقع:

حتى يعتد بالتوقيع كدليل قانوني في الإثبات يجب أن يكون عبارة عن علامة مميزة للشخص الموقع، وذلك بأن يدل التوقيع الموجود على المستند أنه ينسب لشخص معين بذاته وتميزه عن غيره فتصبح الورقة الموقعة منسوبة إليه، ونص المشرع الجزائري على هذا شرط بموجب المادة 323 مكرر1 من ق.م.ج كالآتي: "بشرط إمكانية التأكد من هوية الموقع الذي أصدرها".

تجرى المعاملات الإلكترونية غالبًا بين متعاقدين لا يجمعهم لقاء مادي مباشر بل يتم التواصل بينهم عبر بيئة رقمية، قد لا يعرف فيها أحدهم الآخر ولا تكون هناك علاقة سابقة تربطهم، وهو ما أفرز حاجة ملحة إلى توفير ضمانات قانونية وتقنية تكفل تحديد هوية الأطراف المتعاقدة، والتحقق من طبيعة التعاقد ومضمونه، وضمان أن يتم التعبير عن الإرادة بشكل صحيح يمكن نسبته إلى صاحبه، ولذلك سعى بالمشرع الجزائري إلى مواكبة هذا التطور من خلال إنشاء جهات محايدة تتولى مهام لقيام بالتصديق الإلكتروني بإصدار شهادات التصديق الإلكتروني الموصوفة تؤكد صحة التوقيع الإلكتروني وتضفي عليه الصفة الرسمية، وهو ما جسدته المادة 06 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي تنص على أن: "يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع، وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني"، وجاء في المادة 15 في فقرتها (ج) من نفس القانون على ضرورة أن تتضمن شهادة التصديق الإلكتروني الموصوفة على: "إسم الموقع أو الإسم المستعار الذي يسمح بتحديد هويته".

4- يكون مصممًا بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني:

أولى المشرع الجزائري أهمية لهذا الشرط بحيث خصص له فصلًا كاملًا الموسوم بـ "آليات إنشاء التوقيع الالكتروني الموصوف والتحقق منه"، يقع ضمن الفصل الثاني من الباب الثاني من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر، وعرف آلية إنشاء التوقيع الإلكتروني بموجب الفقرة 04 من المادة 02 من ذات القانون بأنها: "جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني"، كما إشترط أن تكون مؤمنة بموجب المادة 10 من نفس القانون بالنص: "يجب أن تكون آلية إنشاء التوقيع إلكتروني الموصوف مؤمنة"، وذلك حتى أن يتسنى ترسيخ الأمان والطمأنينة في نفوس المتعاقدين.

ليضيف المتطلبات الواجب توفرها بموجب المادة 11 من نفس القانون كالآتي:

1- يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة على الأقل ما يأتي:

أ- ألا يمكن عمليًا مصادفة البيانات المستخدمة لإنشاء التوقيع الالكتروني إلا مرة واحدة (01)، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الإعتماد؛

ب- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الإستنتاج، وأن يكون هذا التوقيع محميًا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الإعتماد؛

ج- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي إستعمال من قبل الأخرين؛

2- يجب أن لا تعدل البيانات محل التوقيع، وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع".

وهو ما كرسته اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر في المادة 02 منها، حيث أكدت على ضرورة الإلتزام بضوابط تأمين منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة كالآتي:

أ- الطابع المتفرد لبيانات إنشاء التوقيع الإلكتروني؛

ب- سرية بيانات إنشاء التوقيع الإلكتروني؛

ج- عدم قابلية الإستنتاج أو الإستنباط لبيانات إنشاء التوقيع الإلكتروني؛

د- حماية التوقيع الإلكتروني من التزوير أو التقليد أو التحريف أو الإصطناع، أو غير ذلك من صور التلاعب؛

هـ- عدم إحداث أي إتلاف بمحتوى أو مضمون المحرر الإلكتروني المراد توقيعه؛

و- ألا تحول هذه المنظومة دون علم الموقع علمًا تامًا بمضمون المحرر الإلكتروني قبل توقيعه له؛

ز- أن تربط التوقيع الإلكتروني بالمحرر الإلكتروني بطريقة متفردة تمنع إجراء أي تعديل بعد عملية التوقيع دون إكتشافه.

5- يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع:

يقصد بهذا الشرط أن يكون الموقع منفردًا بتوقيعه الإلكتروني ولا يستطيع أي شخص آخر من معرفة فك رموز التوقيع الخاصة به أو الدخول عليه سواء عند إنشاء هذا التوقيع أو عند إستعماله[1]، فبمجرد الحصول على هذه السيطرة الحصرية والمباشرة يترتب على ذلك عند

[1]- بلحاج محجوبة، مرجع سابق، ص 93.

وضع التوقيع الإلكتروني على المستند فإنه يجعل التصرف القانوني المرتبط به ثابتًا في مواجهة المنسوب إليه التوقيع[1]، أما في الحالة التي يفقد فيها الموقع السيطرة عليه لأي سبب من الأسباب فإنه يفقد الطابع السري لبيانات التوقيع ويعلمها كل شخص مما يفقد التوقيع الإلكتروني حجيته في الإثبات، لأن تمييز هويته والقدرة على تحديد شخصيته يكون مشكوكًا في صحته[2].

وهذا ما أكدت عليه اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر في المادة 11 منها على أن يتحقق من الناحية الفنية والتقنية سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني المستخدم في عملية تثبيت التوقيع الإلكتروني، عن طريق التثبت من حيازة الموقع أو تحكمه في أداة حفظ المفتاح الشفري الخاص، وعرف المفتاح الشفري الخاص بموجب الفقرة 17 من المادة الأولى منها على أنه: "أداة إلكترونية خاصة بصاحبها تنشأ بواسطة عملية حسابية خاصة، ويتم الإحتفاظ بها على أداة إنشاء التوقيع الإلكتروني، وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية".

6- إرتباط التوقيع الإلكتروني بالمستند إرتباطًا وثيقًا:

نصت الفقرة 06 من المادة 07 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر على هذا الشرط بأن يكون التوقيع الإلكتروني الموصوف مرتبطًا بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات، وكذا هو الشرط الذي أضافته اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 السالفة الذكر في المادة 02 منها في فقرتها (ز) بأن يرتبط التوقيع الإلكتروني بالمستند الإلكتروني بطريقة متفردة تمنع إجراء أي تعديل بعد عملية التوقيع دون إكتشافه.

بمعنى لا بد أن يكون التوقيع مرتبطًا إرتباطًا ماديًا مباشرًا بالمستند الإلكتروني على نحو لا يمكن فصله أو التعديل فيه إلا من صاحب المستند نفسه، حتى يكون دليلًا على إقرار الموقع على ما ورد فيه.

وأضافت اللائحة التنفيذية السالفة الذكر في المادة 12 منها على أن يتم من الناحية الفنية والتقنية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونيًا، بإستخدام

[1]- بوكر رشيدة، مرجع سابق، ص 185.

[2]- بركات عماد الدين، **حجية التوقيع الإلكتروني في إثبات المعاملات الإلكترونية -دراسة مقارنة-**، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف مسيلة، مجلة الأستاذ الباحث للدرسات القانونية والسياسية، المجلد04، العدد02، السنة 2019، الجزائر، ص-ص 1336-1337.

تقنية شفرة المفتاحين العام والخاص وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات أو بأي وسيلة مشابهة.

7- يكون التوقيع مقروءًا ومستمرًا:

مادام التوقيع الإلكتروني صورة من صور الكتابة الإلكترونية ويخضع لنفس الشروط المقررة لها لإكتساب الحجية الثبوتية فلابد أن يكون مقروءًا ومستمرًا، وهذا ما أقره المشرع الجزائري في الفقرة 02 من المادة 327 من ق.م.ج بقوله: "ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1"، وبالعودة إلى النص المادة 323 مكرر1 نجدها أنها بينت أن يكون التوقيع معدًا ومحفوظًا في ظروف تضمن سلامته حتى يتم الإعتراف بقيمته القانونية في الإثبات.

ويتحقق شرط إمكانية القراءة بشكل مباشر أو غير مباشر إذا كان التوقيع الإلكتروني مشفرًا بواسطة فك الشفرة بمفاتيح التشفير، كما يتحقق شرط الإستمرارية بقدرة إحتفاظ المستند الإلكتروني على المعلومات التي يحتويها للفترة التي يتم الرجوع فيها إليه، وبفضل التقنية الحديثة تم إستحداث وسائط وأجهزة تحقق عنصر الإستمرار والثبات للبيانات الإلكترونية والمعلومات التي تتضمنها، مع قدرتها في الإحتفاظ بها لفترة زمنية طويلة دون تعرضها للتأثيرات الخارجية التي تؤثر في المستندات الورقية.[1]

المبحث الثاني: سلطة القاضي الجزائي في قبول و تقدير المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني

إن مجرد وجود دليل جنائي يثبت إرتكاب الجريمة الماسة بالمستند الإلكتروني ونسبتها إلى شخص معين لا يكفي بذاته للإعتماد عليه لإصدار الحكم بالإدانة، بل يجب أن يخضع ذلك الدليل للقواعد التي تنظم سلطة القاضي الجزائي في قبول المخرجات الإلكترونية (المطلب الأول)، وذلك وفقًا للسلطة التي يملكها القاضي في تقدير قيمة الدليل الإلكتروني متى توافرت شروط قبوله (المطلب الثاني) إذ أن القاضي لا يملك سلطة تقدير الدليل إلا إذا كان الدليل مقبولًا قانونًا.

المطلب الأول: سلطة القاضي الجزائي في قبول المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني

سيتناول هذا المطلب حرية القاضي الجزائي في تكوين قناعته إستنادًا إلى المخرجات الإلكترونية في (الفرع الأول)، ثم يبين القيود التي قد ترد على هذه الحرية في (الفرع الثاني).

[1]- سليماني مصطفى، **وسائل الإثبات وحجيتها في عقود التجارة الإلكترونية في التشريع الجزائري والمقارن**، شهادة الدكتوراه، تخصص: القانون الخاص المعمق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية أدرار، 2020/2019، ص-ص 248-249.

الفرع الأول: حرية القاضي الجزائي في الإقتناع بالمخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني

أقر المشرع الجزائري مبدأ حرية القاضي في الإقتناع ونص عليه صراحة في الفقرة الأولى من المادة 349 من القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية [1] على أنه: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات بما فيها الالكترونية، ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعًا لإقتناعه الخاص".

ونص بموجب المادة 442 من نفس القانون على الآتي: "يتلو الرئيس قبل مغادرة المحكمة لقاعة الجلسة التعليمات الآتية التي تعلق فضلًا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة: "إن القانون لا يطلب من القضاة أن يقدموا حسابًا عن الوسائل التي بها قد وصلوا إلى تكوين إقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كافية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها، ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: "هل لديكم إقتناع شخصي"؟.

ويثار التساؤل حول ما إذا كان القاضي الجزائي الذي يحكم في الجرائم التقليدية بناءً على قناعته الشخصية، فهل يطبق المبدأ ذاته عند تعامله مع الدليل الإلكتروني؟

وللإجابة على هذا التساؤل، يستند في ذلك إلى ما نصت عليه الفقرة الأولى من المادة 349 من القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، والتي أجازت إثبات الجرائم بكافة طرق الإثبات بما في ذلك الوسائل الإلكترونية، ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعًا لإقتناعه الخاص وملزم بتسبيب حكمه وبيان الأدلة التي إستمد منها إقتناعه، وتعد إضافة عبارة "بما فيها الالكترونية" من طرف المشرع الجزائري بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر تأكيدًا صريحًا على شمول الأدلة الإلكترونية ضمن وسائل الإثبات، بعدما كانت غير منصوص عليها صراحة في الفقرة الأولى من المادة 212 من الأمر رقم: 66-المتضمن قانون الإجراءات الجزائية الجزائري الملغى، مما كان يقتضي إخضاعها آنذاك للقواعد العامة في الإثبات.

[1]- القانون رقم: 25-14 المؤرخ في 03 أوت 2025، المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج.ش العدد 54، الصادرة بتاريخ 13 أوت 2025.

وبالتالي يلتزم القاضي أن يبني إقتناعه على سبيل اليقين والجزم، والمطلوب عند الإقتناع ليس اليقين الشخصي للقاضي فحسب وإنما هو اليقين القضائي الذي يمكن أن يصل إليه الكافة لإستقامته على أدلة تحمل ذاتها معالم قوتها في الإقناع، وهو بهذا المفهوم يقوم على عنصرين أحدهما شخصي ويلخص في إرتياح ضمير القاضي وإطمئنان نفسه إلى إدانة المتهم على سبيل الجزم واليقين، والثاني موضوعي ويخلص في إرتكان هذا الإرتياح والإطمئنان على أدلة من شأنها أن تفض لذلك وفقًا لمقتضيات العقل والمنطق بحيث لا يكون عمل القاضي إبتداعًا للوقائع وإنتزاعًا من الخيال.[1]

وبالتالي تكون الأدلة الإلكترونية يقينية أي بعيدة عن الظن والتخمينات، ومفاد ذلك أن لا يكون الدليل قابلًا للشك وإذا كان كذلك فإن الشك يفسر لصالح المتهم، فهذا الشرط يوجب على القاضي الجزائي تحري الحقيقة إما بمعرفته الحسية التي يدركها بحواسه، أو بالمعرفة العقلية مستعملًا المنطق للوصول إلى التحليل والإستنتاج الصحيحين مبتعدًا عن الذاتية محكمًا عقله وضميره من أجل الوصول إلى الحقيقة.[2]

وإذا كان القاضي في الجرائم التقليدية يستطيع الوصول إلى اليقين عن طريق الحس والمعاينة والتحليل والإستنتاج، فإن الجزم بوقوع الجرائم المعلوماتية على وجه العموم والجرائم الماسة بالمستند الإلكتروني على وجه الخصوص يتطلب من القاضي نوعًا آخر من المعرفة العلمية بالأمور المعلوماتية، إذ أن الجهل بهذه الأمور يؤدي إلى التشكيك في قيمة الدليل وبالتالي يقضي بالحكم بالبراءة ويستفيد المتهم المعلوماتي من هذا الشك.[3]

خصوصًا أن القاضي الجزائي يلعب دورًا إيجابيًا في الإثبات ويؤدي الجهل في هذه الأمور إلى التشكيك في قيمة الدليل الإلكتروني، وبالتالي يفضي هذا الشك إلى الحكم بالبراءة على المتهم الذي إرتكب الجريمة من الجرائم الماسة بالمستند الإلكتروني ويستفيد من هذا الشك وبهذا يفلت من تطبيق العدالة والقانون، ومن ثمة يترتب على بلوغ الإقتناع بالإدانة درجة اليقين من طرف القاضي الجزائي لأن الإقتناع ثمرة اليقين.[4]

وتعتبر قاعدة الشك يفسر لمصلحة المتهم من أهم الضمانات الموضوعية لإقتناع القاضي، فإذا لم تتوصل الجهة القضائية من خلال الأدلة المجتمعة لديها إلى اليقين بإسناد التهمة إلى المتهم فإنه يتعين عليها أن تقضي بالبراءة.[5]

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 278.

[2]- شنتير خضرة، **الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة**، مؤسسة الكتاب القانوني إبن النديم، الطبعة الأولى، ماي 2022، الجزائر، ص 62.

[3]- بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، مرجع سابق، ص 281.

[4]- نادية ضريفي، دراج عبد الوهاب، **سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي**، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف مسيلة، مجلة الأستاذ الباحث للدرسات القانونية والسياسية، المجلد04، العدد 02، 2019، الجزائر، ص 124.

[5]- بلجراف سامية، مرجع سابق، ص 687.

الفرع الثاني: القيود الواردة على حرية القاضي الجزائي في قبول المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني

إذا كان من المسلم به أن للقاضي الجزائي حرية الإستعانة بكافة وسائل الإثبات اللازمة لإصدار حكمه بما في ذلك الدليل الإلكتروني لتكوين إقتناعه الشخصي، إلا أنه مقيد بضوابط سواء فيما يتعلق بمبدأ مشروعية الحصول على الدليل الإلكتروني أو بوجوبية مناقشة الدليل الإلكتروني.

أولًا: مبدأ مشروعية الحصول على الدليل الإلكتروني

تفيد الشرعية في قانون العقوبات الجزائري خضوع الفعل إلى النص القانوني وأن القانون هو مصدر الوحيد للتجريم والعقاب طبقًا للمادة الأولى، والتي نصت على أن: "لا جريمة ولا عقوبة أو تدابير أمن، بغير قانون".

وبالرغم من أن هذه القاعدة تمثل إحدى الركائز الأساسية التي تقوم عليها كل التشريعات الجنائية، إلا أنها لا تكفي وحدها لحماية مبادئ الشرعية والإجراءات اللازمة المتخذة في حق المتهم ومحاكمته محاكمة عادلة، وإنما من الضروري تدعيم هذه القاعدة بقاعدة ثانية تحكم تنظيم الإجراءات التي تتخذ ضد المتهم بطريقة يضمن بها إحترام كرامة وحقوق والحريات الفردية، وهذه القاعدة سميت بالشرعية الإجرائية والتي تعني ضرورة إتفاق الإجراء المتخذ مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر.[1]

والشرعية الإجرائية إذن تقتضي أن يكون القانون وحده هو مصدر كل إجراء يتخذ حيال المتهم بغرض الوصول إلى الحقيقة، مع خضوع كل هذه الإجراءات لإشراف القضاء وإفتراض براءة المتهم وإلا أعتبر الإجراء وما بني باطلًا[2]، ولما كانت هذه القاعدة عامة بالنسبة للدليل بوجه عام كان الدليل الإلكتروني كذلك شأنه في ذلك شأن باقي الأدلة، فهو خاضع لمبدأ المشروعية ومن ثم فإن القاضي لا يمكنه الإعتماد على الدليل الإلكتروني في إصدار حكمه بالإدانة أو البراءة إلا إذا كان صحيحًا ومشروعًا[3].

ومن جهة ثانية فقاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد مطابقة إجراءات الحصول عليه مع القاعدة القانونية التي نص عليها المشرع، بل تتعدى ذلك إلى

---

[1]- بن لاغة عقلية، **حجية أدلة الإثبات الجنائية الحديثة**، رسالة الماجستير، فرع: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2011-2012، ص-ص 43-44.

[2]- لهوى رابح، مرجع سابق، ص 283.

[3]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 94 .

مراعاة وإحترام لحقوق الإنسان المعترف بها دوليًا من مواثيق والإتفاقيات الدولية، بالإضافة إلى إحترام قواعد النظام العام وحسن الآداب السائدة في المجتمع.[1]

فهي تهدف إلى تقدير ضمانة أساسية وجدية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة بالتطاول عليها في غير الحالات التي رخص فيها القانون ذلك، من أجل حماية النظام الإجتماعي وبالقدر نفسه تحقيق حماية مماثلة للفرد ذاته.[2]

فإنه يتعين على القاضي أن يتأكد أولًا من مشروعية الدليل، ولا يحول دون ذلك أن يكون الدليل صارخًا في مظهره واضحًا في دلالته على إدانة المتهم ما دام مشبوهًا ملطخًا بإهدار محارم القانون[3]، ونظرًا لأهمية هذا المبدأ فقد تم تكريسه في الدستور الجمهورية الجزائرية الديمقراطية الشعبية سنة 2020[4] بموجب الفقرة الأولى من المادة 44 التي تنص على أن : "لا يتابع أحد، ولا يوقف أو يحتجز، إلا ضمن الشروط المحددة بالقانون، وطبقًا للأشكال التي نص عليها".

1- مدلول قاعدة مبدأ مشروعية الدليل الالكتروني:

قاعدة مبدأ مشروعية الدليل الإلكتروني يحكمه ضابطان يتمثلان في ما يلي:

أ- التحقق من أصالة الدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الالكتروني:

تعتمد القيمة الثبوتية للدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الإلكتروني في المقام الأول على أصالته أو مصداقيته، نظرًا لسهولة محوه أو تعديله أو تدميره والتلاعب به، وذلك بهدف إقناع المحكمة بتمتعه بالمصداقية المطلوبة.

---

[1]- هذا ما أكد عليه وأوصى به المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في "ريو دي جانيرو" بالبرازيل المنعقد في الفترة من 04 إلى 09 سبتمبر 1994 في مجال حركة إصلاح الإجراءات الجنائية بالتوصية رقم: 18 المتعلقة بالقواعد الإجرائية في بيئة جرائم الكمبيوتر، والتي نصت على أن: "كل الأدلة التي يتم الحصول عليها عن طريق إنتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة، ولا يمكن التمسك بها أو مراعاتها"، فقد أشار هذا المؤتمر إلى ضرورة إحترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الآلي والجرائم التقليدية في بيئة تكنولوجيا المعلومات، وإلا ترتب عليه بطلان الإجراء فضلًا عن تقرير المسؤولية لرجل السلطة العامة الذي إنتهك القانون، وللمزيد من التفصيل، ينظر: بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، مرجع سابق، ص 281.

أكدت على وجوب مشروعية الدليل توصيات المؤتمر الدولي الثاني عشر للجمعية الدولية لقانون العقوبات المنعقد في 22/16/ سبتمبر 1979 في هامبورج بجمهورية ألمانيا الإتحادية، على أن: "قبول الدليل في الدعاوى الجزائية، يجب أن يأخذ بعين الإعتبار كمال النظام القضائي وحقوق الدفاع، ومصالح المجني عليه، ومصالح المتهم"، وللمزيد من التفصيل، ينظر: بن لاغة عقيلة، مرجع سابق، ص 44.

[2]- رفاه خضير جياد العارضي، مرجع سابق، ص 90.

[3]- لهوى رابح، مرجع سابق، ص 284.

[4]- المرسوم الرئاسي رقم: 20-442 المؤرخ في 30 ديسمبر 2020، المتضمن التعديل الدستوري، ج.ر.ج.ج.ش العدد 82، سنة 2020.

تتمحور الجرائم الماسة بالمستند الإلكتروني ضمن البيئة الرقمية التي تعد المصدر الأساسي لأصالة الدليل الإلكتروني، وهو دليل غير مرئي لا يدرك بالحواس ولا يرقى إلى مستوى أصالة الدليل المادي في شكله الملموس، إذ لا يخلف آثارًا مادية تدل على مرتكبيه كما هو الحال في الجرائم التقليدية، فهو عبارة عن نبضات إلكترونية مكونة من تعداد غير محدود لأرقام ثنائية موحدة في الصفر (0) والواحد (1) والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه.[1]

فالكتابة مثلًا في العالم الرقمي ليس لها وجود مادي في شكل ورقي وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأي شيء في العالم الرقمي يتكون من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة وتكوين معطياته فإنها تختلف من حيث الحجم والموضوع[2]، ولقد أثارت مسألة الأصالة العديد من المشكلات من حيث مدى الإعتداد بالنسخة التي تشكل دليلًا كاملًا هنا[3].

والواقع من الأمر أن بحث موضوع الأصالة على المستوى القانوني جعل المشرع المقارن يعتمد منطق إفتراض أصالة الدليل الإلكتروني، وقد تضمن قانون الإجراءات الجنائية الفيدرالي في الولايات المتحدة الأمريكية نصًا صريحًا (القاعدة 1001 بند 03) حيث يسمح إستثناء بقبول الدليل الإلكتروني بإعتباره مستندًا أصليًا ما دام أن البيانات صادرة من الحاسب الآلي أو جهاز مماثل، وسواء أكانت هذه المعطيات مطبوعة أم مسجلة على دعامات أخرى ومقروءة للعين المجردة وتعبر عن المعطيات الأصلية بشكل دقيق، ومنه تتساوى الكتابة المادية من حيث الأصالة مع مخرجات الإلكترونية على الرغم من أن طبيعة الكتابة عبرها تجعل من المخرجات مجرد نسخ للأصل الموجود رقميًا في الأجهزة الإلكترونية أو عبر الإنترنت.[4]

ب- التحقق من صحة الإجراءات المتبعة في تحصيل الدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الإلكتروني:

طبقًا لمبدأ مشروعية الدليل الجنائي فإن الدليل لا يكون مشروعًا ومقبولًا في عملية الإثبات إلا إذا جرى التنقيب عنه أو الحصول عليه وفقًا للطرق والإجراءات التي حددها القانون، وعليه فمتى ما تم الحصول عليه خارج الشروط والضوابط التي نصت عليه القواعد القانونية فإنه لا يعتد بقيمته ولا يقبل كدليل إثبات وذلك لعدم مشروعية الحصول عليه، لأن مشروعيته تقتضي أن تكون سلطات التحري والتحقيق عن الجرائم قد إلتزمت بالشروط والضوابط التي حددت القواعد الإجرائية كيفية الحصول عليه، وإذا خالفتها فإن الدليل الإلكتروني يفرغ من قيمته

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 252.
[2]- بن طالب ليندا، مرجع سابق، ص-ص 42-43.
[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 252.
[4]- نفس المرجع، ص-ص 252-253.

القانونية وبالتالي بطلانه، أي عدم صلاحية الأخذ به والتعويل عليه في الإثبات لفقدانه القيمة القانونية مهما كانت دلالته الحقيقية.[1]

تدارك المشرع الجزائري الأمر من خلال مواكبة التطور التكنولوجي والمعلوماتي وإنتشار وسائل الإتصال الحديثة التي أدت بدورها إلى إستحداث أشكال جديدة للإجرام، فتدخل بوضع القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية[2]، من خلال إدراج إجراءات التسرب، وإعتراض المراسلات الإلكترونية وتسجيل الأصوات وإلتقاط الصور، كما وضع الضوابط اللازمة لتنفيذهما، ورغم إلغاء الأمر بموجب القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية، فقد أبقى على تلك الإجراءات.

وبموجب القانون رقم: 09-04 المؤرخ في 05 أوت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[3] نظم فيه إجراءات التفتيش وحجز المنظومة المعلوماتية، كما إستحدث المشرع إجراء مراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، وإجراء حفظ المعطيات المتعلقة بحركة السير.

ومن ثم فإن لا يجوز للقاضي الجزائي أن يقبل في إثبات إدانة المتهم أدلة إلكترونية لم تتبع بشأنها الضوابط القانونية المقررة في هذه النصوص القانونية لإستخلاصها، كالدليل الإلكتروني المستمد من تفتيش لم تأذن به السلطة القضائية، أو نتاج تفتيش جرى تنفيذه بعد إنقضاء مدة سريان الإذن، أو تفتيش مخالف للغاية منه أو لأسلوب تنفيذه.[4]

وذلك أن الخصومة الجنائية تقوم على ضمان حرية المتهم لا على مجرد إثبات سلطة الدولة في العقاب، وعليه يتعين على القاضي ألا يثبت توافر هذه السلطة تجاه المتهم إلا من خلال إجراءات مشروعة تحترم فيها الحريات وتؤمن فيها الضمانات التي رسمها القانون.[5]

فقد قضت محكمة النقض البلجيكية في هذا الصدد بأن وصف الدليل غير المشروع لا يقتصر فقط على الفعل الذي يحظره القانون صراحة، بل يشمل كل فعل يتعارض مع القواعد الجوهرية للإجراءات الجنائية أو المبادئ القانونية.[1]

---

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص-ص 806-807.

[2]- القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006، المتضمن تعديل للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية الجزائري، ج.ر.ج.ج.ش العدد 84، الصادرة في 24 ديسمبر 2006، الملغى.

[3]- القانون رقم: 09-04 المؤرخ في 05 أوت سنة 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج.ش العدد 47، الصادر في 16 أوت 2009.

[4]- لهوى رابح، مرجع سابق، ص-ص 285-286.

[5]- عميروش هنية، داعي عز الدين، **دور تكنولوجيا الإعلام والإتصال في الإثبات الجنائي**، كتاب جماعي محكم بعنوان: **أثر تكنولوجيا الإعلام والإتصال على القانون الجنائي**، د.ر.ط، مخبر البحث حول فعالية القاعدة القانونية، كلية الحقوق والعلوم السياسية، جامعة عبدالرحمان ميرة- بجاية، جوان 2021، الجزائر، ص 136.

وأشارت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 إلى المبدأ في المادة 15 بعنوان: "الشروط والضمانات" وهذا في بداية الباب الثاني المتعلق بالإجراءات، حيث أكدت المذكرة التفسيرية للإتفاقية أن على الدول تقيد إجراءات مكافحة الجرائم المعلوماتية بحماية حقوق الإنسان وحرياته الواردة في الإتفاقيات الدولية والإقليمية، كما أقرت ضمانة أخرى تتمثل في مبدأ التناسب أي أن السلطات والإجراءات يجب أن تكون متناسبة مع طبيعة وظروف الجريمة وكذا مع المبادئ المرتبطة بالقانون الداخلي للدول، كتقييد الأوامر بإنتاج معطيات معلوماتية -تقديم الدليل الإلكتروني- وتقييد سلطات التفتيش والضبط وكذا تقييد إجراءات إعتراض الإتصالات بنطاق الجرائم الخطيرة، كما أشارت الإتفاقية إلى بعض الضمانات والشروط كإشراف السلطة القضائية على هذا النوع من الإجراءات وتقديم البواعث المبررة للقيام بهذه الإجراءات وتحديد تبعتها ومدتها وإلى ضرورة حماية السر المهني، وكذلك الأخذ في الإعتبار طبائع الأشخاص والأماكن التي هي هدف لتطبيق هذه الإجراءات.[2]

فقد قضت محكمة النقض الفرنسية في حكم لها بأن: "التسجيل الهاتفي الذي يجريه أحد الأطراف بدون علم صاحب الأقوال المسجلة يشكل بطريقة غير مشروعة تؤدي إلى عدم قبوله برهانًا، وقد نقضت بذلك حكم محكمة الإستئناف بباريس الذي قد أخذ بالتسجيل" حيث ذهبت محكمة النقض الفرنسية (الغرفة التجارية) إلى أن تسجيل مكالمة هاتفية من قبل أحد الأطراف دون علم صاحب الأقوال يشكل وسيلة ماكرة مما يمنع قبول تقديمه كدليل، حيث بنت محكمة النقض حكمها بنقض محكمة إستئناف باريس الصادر في 19 جوان 2007 على مخالفة ذلك لأحكام الفقرة الأولى من المادة السادسة من الإتفاقية الأوروبية لحقوق الإنسان وحرياته الأساسية، وكانت محكمة الإستئناف بباريس قد قررت أن تسجيلات المكالمات الهاتفية المقدمة من الطرف الرافع للدعوى وليس من المحققين أو من المقرر لا يمكن رفضها بمجرد علة الحصول عليها بصورة ماكرة وبأنها تعتبر مقبولة متى خضعت للمناقضة حيث يعود للمحكمة تقدير قيمتها الثبوتية.[3]

وكذلك فإن إجراءات الحصول على الدليل الإلكتروني يجب أن يكون ضمن الإطار العام الذي حدده الدستور، وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة فيه يكون باطلًا بطلانًا مطلقًا لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به، كما أن للمحكمة أن تقضي به من تلقاء نفسها.

---

[1]- محمد أحمد المنشاوي، **سلطة القاضي الجنائي في تقدير الدليل الإلكتروني**، جامعة الكويت، مجلة الحقوق، المجلد 36، العدد02، جوان 2012، الكويت، ص 552.

[2]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 252.

[3]- رامي متولي القاضي، مرجع سابق، ص197.

والحكمة من تقرير مشروعية الحصول على الدليل عمومًا هو التوفيق بين مصلحة المجتمع في تقريره للعقاب ومصلحة الفرد في إحترام حرياته في إطار مبدأ الشرعية الإجرائية، ومن ثم تصبح هذه الضمانات الإجرائية غير ذات قيمة ما لم يتقرر الجزاء على مخالفتها لذلك فإن قانون الإجراءات الجزائية يرتب البطلان كجزاء إجرائي على الإجراء المخالف للقانون، والقاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقه له مباشرة[1] وهو الرأي الذي أخذ به المشرع الجزائري بنص المادة 287 من ق.إ.ج.ج التي نصت على أنه: "تنظر غرفة الإتهام في صحة الإجراءات المرفوعة إليها، وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به، وعند الإقتضاء ببطلان الإجراءات التالية له كلها أو بعضها".

2- قيود قبول الدليل الإلكتروني غير المشروع:

التساؤل المطروح في هذا السياق هو مدى إمكانية قبول الدليل الإلكتروني غير المشروع والإعتداد به، خاصة عندما يقدم ذلك حماية للمصلحة العامة على حساب المصلحة الخاصة للأفراد؟ الإضافة إلى التساؤل عن قيمة هذا الدليل غير المشروع في الإثبات الجنائي؟

تتمثل قيود قبول طريقة الحصول على الدليل الإلكتروني غير المشروع في ما يلي:

أ- المصلحة الأولى بالحماية والرعاية:

وهي الحالة التي يكون فيها الدليل الإلكتروني غير المشروع وسيلة إثبات لجرائم تحمل إعتداء شاملًا على مصالح المجتمع وتهدد أمن ونظام العام من جهة، وفي نفس الوقت يعد كأثر للتعدي على الحياة الخاصة وترتب على إستخدامها إعتداء على حقوق أساسية للإنسان، فأي المصلحتين أولى بالرعاية.[2]

فقد بات من الصعوبة التوفيق بين مقتضيات حماية والحفاظ على النظام العام وعدم المساس بحرمة الحياة الخاصة للفرد في إطار تنفيذ مستلزمات التحريات والتحقيقات القضائية، مما تدخل المشرع الجزائري وحسم هذا الأمر وذلك من خلال نصه في المادة 03 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر على أن: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقًا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص-ص 808-809.
[2]- عائشة بن قارة مصطفى، مرجع سابق، ص216.

وإن للمعلومة الإلكترونية صلة وثيقة بالحق في السرية والخصوصية ذلك أن هذا المستند قد يحتوي على معطيات ومعلومات لا يحق للآخرين الإطلاع عليها، وحماية المعلومة الإلكترونية في هذه الحالة تنطوي على حماية الحق في السرية والحق في الخصوصية، يدرج على سبيل المثال نص قانون التخلص من الأوراق الحكومية الأمريكي لسنة 1998 على أن الهيئات الحكومية أن تتخذ الإجراءات اللازمة لحفظ المعلومات الإلكترونية أو تسليمها أو الكشف عنها كلما كان ذلك ممكنًا كبديل للمستندات الورقية، كما نص هذا القانون كذلك على وجوب إتخاذ الإجراءات الكفيلة بإستخدام وقبول التوقيع الإلكتروني كلما كان ذلك ممكنًا، وقد حدد الشارع الأمريكي ميعادًا لإنجاز هذه الإجراءات هو الأول من أكتوبر 2003.[1]

ب- قيمة الدليل الإلكتروني غير المشروع:

سنتناول قيمة الدليل الإلكتروني غير المشروع من وجهة نظر الأنظمة الثلاثة:

ب-1- قيمة الدليل الإلكتروني غير المشروع في النظام الإثبات الحر:

نميز بين نوعين من الأدلة:

ب-1-1- قيمة الدليل الإلكتروني غير المشروع في الإدانة:

إنطلاقًا من قاعدة أن الأصل في الإنسان البراءة فإن المتهم يجب أن يعامل على أساس أنه بريء في مختلف مراحل الدعوى إلى أن يصدر بحقه حكم بات، وهذا يقتضي أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة سواء كانت أدلة تقليدية أو ناتجة عن الوسائل الإلكترونية بصفة عامة.[2]

وبالتالي فإن حكم بالإدانة يجب أن يكون مستندًا على دليل مشروع ولا يجوز أن تبنى الإدانة على دليل باطل وعدم إنتاج الإجراء الباطل للآثار التي تترتب عليه مباشرة، ومنه فهل ينطبق هذا القول على الدليل الغير المشروع في البراءة ؟

ب-1-2- قيمة الدليل الالكتروني غير المشروع في البراءة:

لقد أثار هذا التساؤل جدلًا فقهيًا واسعًا نتج عنه ثلاثة إتجاهات رئيسية:

ب-1-2-1- الإتجاه الأول:

يرى أنصار هذا الإتجاه أنه ليس للقاضي أن يحكم ببراءة المتهم بناءً على دليل جاء من طريق غير مشروع، أي لا يفرق بين ما إذا كان الدليل سوف يؤدي للبراءة أو للإدانة على حد سواء.[3]

[1]- بن طالب ليندا، مرجع سابق، ص 144.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 217.

[3]- عميروش هنية، داعي عز الدين، مرجع سابق، ص 139.

يرى أن المشروعية لازمة في كل دليل سواء أكان إدانة أو براءة، وذلك تأسيسًا على نص المادة 336 من قانون الإجراءات الجنائية المصري التي تقرر بطلان جميع الآثار المترتبة على الإجراء الباطل دون تفرقة بين دليل إدانة ودليل براءة، أضف إلى ذلك أن قصر مبدأ المشروعية على دليل الإدانة فقط دون البراءة فيه يشكل ضررًا على الفرد والمجتمع.[1]

وأضافوا أنه ليس للقضاء أن يقر قاعدة "أن الغاية تبرر الوسيلة" كمبدأ قانوني صحيح، وهو إذا أقرها في خصوص جواز إثبات البراءة بكل السبل فقد يقال فيما بعد أنه حتى التزوير وشهادة الزور حتى يعدلوا عن أقوالهم تصبح كلها أمور مشروعة لإثبات البراءة وهذا ما لا يمكن أن يقول به أحد، ولكن ينتهي إليه حتمًا منطق هذا القضاء الخاطئ.[2]

ويذهب الفقه الرأي السائد في الفقه المصري إلى تأييد موقف محكمة النقض، فيرى جانب من الفقه أن رجوع قاعدة عدم قبول الدليل المتحصل عن إجراء غير مشروع إلى إحترام حقوق الدفاع يؤدي إلى نتيجة في غاية الأهمية أدركتها محكمة النقض المصرية وهذه النتيجة هي إقتصار قيد المشروعية على دليل الإدانة لأنه هو وحده الذي يمس حق الدفاع، أما دليل البراءة فلا يخضع لهذا القيد ويؤيد بعض الفقه هذا الرأي على أساس أن الأصل في الإنسان البراءة، ولا حاجة للمحكمة أن تثبت براءته وكل ما تحتاج إليه هو أن تشكك في إدانته، فضلًا على ذلك فإن بطلان دليل الإدانة الذي تولد عن إجراء غير مشروع إنما شرع لضمان حرية المتهم.[3]

ب-1-2-2- الإتجاه الثاني:

يرى بأنه ليس هناك ما يمنع من تأسيس حكم البراءة على دليل غير مشروع إنطلاقًا من مبدأ إفتراض البراءة بإعتبارها هي الأصل، وبالتالي المحكمة ليست بحاجة لإثباتها بل كل ما تحتاجه هو التشكيك في الإدانة لكي تصدر حكمها ببراءة المتهم مما نسب إليه[4]، وهو ما يمكن الوصول إليه من خلال أي دليل ولو كان غير مشروع، أضف إلى ذلك أن للمتهم الحرية الكاملة في إختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى وما تحيط نفسه من عوامل الخوف والحذر وغيرها من العوارض الطبيعية لضعف النفوس البشرية، والإصرار على تطلب مشروعية دليل البراءة بالمثل مع دليل الإدانة قد يعرقل حق المتهم في الدفاع عن نفسه الذي يعلوا على حق المجتمع في إستيفاء العقاب.[5]

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص-ص 219-220.
[2]- عميروش هنية، داعي عز الدين، مرجع سابق، ص 139.
[3]- لهوى رابح، مرجع سابق، ص 287.
[4]- عميروش هنية، داعي عز الدين، مرجع سابق، ص 139.
[5]- عائشة بن قارة مصطفى، مرجع سابق، ص 220.

يستنتج أن مبدأ مشروعية الأدلة لا يجب أن يطغى على مبدأ إفتراض البراءة، حيث أي دليل يفيد في إثبات هذا المبدأ الأخير وجب الأخذ به دون الإلتفات لأي إعتبار آخر، لأن العدالة تضار بقدر أكبر في حالة إدانة بريء على إفلات مجرم من القضاء.[1]

ب-1-2-3- الإتجاه الثالث:

هو إتجاه توفيقي بين الإتجاهين السابقين إذ يفرق بين ما إذا كانت وسيلة الحصول على دليل البراءة تعد جريمة جنائية أم أنها مجرد مخالفة لقاعدة قانونية إجرائية، فإن كان الدليل متحصلًا من جريمة جنائية وجب إهدار الدليل وعدم الإعتداد به، لأن القول بغير ذلك مفاده الدعوى إلى إرتكاب بعض الجرائم وإخراجها من دائرة العقاب وهو ما لا يجوز وتأباه كل التشريعات الجنائية، أما إذا كان الحصول على الدليل يخالف قاعدة إجرائية فحسب، فهنا يصح الإستناد إلى هذا الدليل في تبرئة المتهم تحقيقًا للغاية من تقرير البطلان، لأن الغرض من البطلان الذي شاب وسيلة التوصل إلى الدليل إنما يرجع إلى فعل من قام بالإجراء الباطل وبالتالي لا يصح أن يضار المتهم بسبب لا دخل له فيه.[2]

وبناءً على ذلك يرى أنصار هذا الإتجاه جواز إستناد المحكمة في تبرئة المتهم إلى دليل جاء من أوراق ضبطت لدى المدافع عن المتهم على خلاف القانون، أو رسائل ضبطت لدى هيئة البريد بمعرفة النيابة العامة دون إذن من القاضي الجزائي إلى غير ذلك من الأدلة الناجمة عن تفتيش باطل، ولا يصح لها التعويل على دليل توصل إليه المتهم بطريق السرقة أو التزوير وغيرها من الجرائم.[3]

ب-2- قيمة الدليل الإلكتروني غير المشروع في نظام الإثبات المقيد:

بموجب هذه القوانين يمكن معرفة أن الأصل إذا أدى الإجراء غير القانوني إلى دليل تثبت به الجريمة فعلى القاضي أن يحكم به وليس له أن يسأل بأي طريق جاء، وإن كانت هذه هي القاعدة العامة في القوانين ذات الصياغة الأنجلوسكسونية فإن المشرع في هذه البلدان قد حاول التخفيف من وطأت هذا المبدأ فإستعمل قاعدة إستبعاد الدليل الذي يتم الحصول عليه بطريقة غير مشروعة بدلًا من بطلان الدليل والإجراءات المترتبة عليه والمعمول بها في القوانين ذات الصياغة اللاتينية.[4]

ب-2-1- بالنسبة للقانون الإنجليزي:

ففي بريطانيا نصت المادة 78 من قانون البوليس والإثبات الجنائي الصادر سنة 1984 على أن: "إذا بدا للمحكمة بعد الأخذ في الإعتبار كل الظروف وتم فهم هذه الظروف التي

[1]- بن طالب ليندا، مرجع سابق، ص 143.
[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 221.
[3]- عميروش هنية، داعي عز الدين، مرجع سابق، ص 140.
[4]- رفاه خضير جياد العارضي، مرجع سابق، ص 95.

أعطي فيها الدليل وأن تلقيه كان بسبب وقوع أضرار تتعلق بعدالة إجراءات الدعوى، فإن المحكمة لا يمكن أن تقبله".[1]

ولقد تضمن قانون الشرطة والإثبات الجنائي الإنجليزي لسنة 1984 تحديد الشروط الواجب توافرها في مخرجات الحاسوب لكي تقبل أمام القضاء، وتضمن كذلك توجيهات في كيفية تقدير قيم أو وزن البيان المستخرج عن طريق الحاسوب فأوصت المادة 11 منه بمراعاة كل الظروف عند تقييم المعطيات الصادرة عن الحاسوب المقبولة في الإثبات طبقًا للمادة 69 من القانون نفسه، وبوجه خاص مراعاة (المعاصرة) أي ما إذا كانت المعلومات المتعلقة بأمر قد تم تزويد الحاسوب بها في وقت معاصر لهذا الأمر أم لا، وكذلك مسألة ما إذا كان أي شخص من المتصلين على أي نحو بإخراج المعطيات لديه دافع لإخفاء الوقائع أو تشويهها.[2]

إن أيا من الشروط المحددة (التي تدخل في متطلبات القبول) المتعلقة بالموضوع يجب أن تخضع لتقدير المحكمة، ولقد قضت محكمة الإستئناف الجنائي في إنجلترا بذلك حيث بينت في حكمها كيفية التعامل مع الأدلة المستخرجة من الحاسوب، ويتلخص الحكم بما يلي: "أنه يبدو لهذه المحكمة أنه من الخاطئ رفض أو إنكار أية مزايا أو صلاحيات مقررة وفقًا لقانون الإثبات، يمكن بمقتضاها التوصل عن طريق التقنيات الجديدة والوسائل الحديثة التأكد من صحة وصدق التسجيل حيث يمكن التثبت من ذلك وكذلك يمكن التعرف بوضوح على الأصوات المسجلة، والمستخلص أيضًا هو أن الدليل وثيق الصلة بالموضوع من جهة أخرى يمكن قبوله، ومن ثم تؤيد المحكمة قبول هذه الأشرطة ويجب أن ينظر دائمًا بعين الإعتبار إلى مثل هذا الدليل وتقدير قيمته في ضوء جميع الظروف بالنسبة لكل قضية".[3]

ويشكك الفقه الإنجليزي في أن عدم إعطاء التفويض بصورة قانونية سليمة لإجراء التحقيق سيؤدي إلى إستبعاد دليل تم الحصول عليه من شأنه إدانة المتهم، ويستند الفقه الإنجليزي في ذلك إلى الموقف التقليدي للقضاء الإنجليزي ومفاده أن قواعد القانون العام في بريطانيا لا تحفل بكيفية تحصيل الدليل طالما كان منتجًا في الإثبات، كما أنه لا توجد قاعدة تلزم قاضي الموضوع بإستبعاد الدليل المتحصل بصورة غير مشروعة أو غير قانونية، فالقاعدة العامة تقرر أن الدليل المتحصل بطريقة غير مشروعة أو غير قانونية أو حتى بطريقة غير عادلة لا يمنع من قبوله، فهو أمرًا مألوفًا طالما كان منتجًا في الدعوى.[4]

---

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص-ص 95-96.

[2]- فهد دخين العدواني، **مشروعية الدليل الإلكتروني الصادر عن التفتيش الجنائي: دراسة مقارنة**، جامعة عين الشمس، كلية التربية، مركز تطوير التعليم الجامعي، مجلة دراسات في التعليم الجامعي، المجلد 2017، العدد السادس والثلاثون، 2017، مصر، ص 260.

[3]- نفس المرجع، ص-ص 260-261.

[4]- عميروش هنية، داعي عز الدين، مرجع سابق، ص 138.

ب-2-2- بالنسبة للقانون الأمريكي:

أما في القانون الأمريكي فالتطبيق القضائي الأمريكي لقاعدة الإستبعاد أكثر وضوحًا من التطبيق القضائي الإنجليزي، ذلك أن نظرية "فاكهة الشجرة المسمومة يجب أن لا تؤكل" تجد لها مكانًا مقبولًا في التطبيق القضائي الأمريكي دون الإنجليزي، بحيث أن الأصل في القضاء الأمريكي هو التطبيق المطلق للقاعدة والإستثناء هو التطبيق التخييري لها.[1]

وتأكيدًا على ذلك فقد خصص المشرع الأمريكي مبحثًا خاصًا وهو المبحث الخامس في المرشد الفيدرالي الأمريكي لتفتيش وضبط الحاسوب وصولًا إلى الدليل الإلكتروني يتعلق ب:"علاج إنتهاكات قانون المراقبة وقانون التسجيل والتقصي"، ويقصد به علاج بطلان الإجراءات غير المشروعة في الحصول على الدليل الإلكتروني، حيث نص في ذلك على أنه يجب على رجال الضبط القضائي والمدعين العموميين سلوك أوامر الباب الثالث -قانون المراقبة- وقانون التسجيل والتقصي عند التخطيط للمراقبة الإلكترونية، إذ يمكن أن تفسر الإنتهاكات عن غرامات وجزاءات مدنية أو جزائية.[2]

ب-2-3- بالنسبة للقانون الكندي:

وفي كندا يمكن قبول السجلات الناجمة عن الجهاز الإلكتروني إذا توافرت شروط معينة، إذ تنص المادة 29 من قانون الإثبات الكندي على عدد من الشروط التي يجب توافرها قبل عمل صورة (Copy) من السجل الذي يضاف إلى الأدلة ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي، وقد قضت محكمة إستئناف أونتاريو الكندية في قضية مكميلان بأنه يشترط لكي تكون سجلات الجهاز الإلكتروني مقبولة بوصفها نسخًا حقيقية من السجلات الإلكترونية أن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية، كما يمكن أن يتضمن ذلك وصفًا للإجراءات والعمليات المتعلقة بإدخال المعطيات وتخزينها وإسترجاعها حتى يتبين أن المستخرج المتحصل من الجهاز موثوق به بشكل كاف.[3]

ب-3- قيمة الدليل الإلكتروني غير المشروع في النظام المختلط:

يقوم نظام الإثبات المختلط بالتوفيق بين النظام الإثبات الحر ونظام الإثبات المقيد تفاديًا للنقد الذي وجه للنظامين السابقين، بحيث يعتمد على الأدلة المحددة قانونًا لإثبات بعض الوقائع دون بعضها الآخر، وفي بعض الحالات على تحديد شروط قبول الدليل وإعطاء للقاضي الحرية في تقدير الأدلة القانونية.[4]

---

[1]- بن طالب ليندا، مرجع سابق، ص 142.

[2]- نفس المرجع، ص 142.

[3]- سحر سعد عبد السميع محمد، مرجع سابق، ص 337.

[4]- خالد ضو، مرجع سابق، ص207.

فالدستور الياباني الذي يضمن حق المتهم في إلتزام الصمت يستبعد الدليل الذي يتم الحصول عليه بإعترافات مشوبة بالاكراه أو التعذيب[1]، وتهدف المادة 38 من الدستور الياباني لسنة 1947 الأخذ بقاعدة الإستبعاد المطبقة في القوانين ذات الصياغة الانجلوسكسونية، وبموجب المادة 319 من قانون الإجراءات الجنائية الياباني فإنه تستبعد عناصر الإثبات المأخوذة عن طريق الإكراه أو التعذيب أو التهديد، وقد نصت المادة 218 من ذات القانون على إستبعاد الأدلة عندما يكون الحصول عليها قد تم بالمخالفة لمتطلبات إحتوتها المادة نفسها.[2]

ثانيًا: وجوب مناقشة الدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الإلكتروني

من أهم القواعد الأساسية في الإجراءات الجزائية أن القاضي لا يجوز له أن يبني حكمه إلا على الأدلة التي طرحت أمامه في الجلسة، ولا يسمح له بالإعتماد على معلوماته الشخصية أوعلى آراء الغير.

1- مضمون مبدأ وجوب مناقشة الدليل الإلكتروني:

يقوم مبدأ وجوب مناقشة الدليل الإلكتروني على عنصريين أساسيين:

أ- إتاحة الفرصة للخصوم للإطلاع على الدليل الإلكتروني والرد عليه:

يتمثل العنصر الأول في إتاحة الفرصة للخصوم من أجل الإطلاع على الدليل الإلكتروني والرد عليه، وبهذا يحترم مبدأ حق الدفاع كما يتيح شرط مناقشة الدليل الإلكتروني تطبيقًا لمبدأ المواجهة، كما يكرس ضمانات آخرى تتمثل في لزوم إحاطة المتهم علمًا بالتهمة المنسوبة إليه ليتمكن من تحضير دفاعه، كما يسمح لكل طرف من الخصوم بتقديم ما لديه من مستندات، وسؤال الشهود والخبراء أثناء عملية المواجهة.[3]

وبالتالي فلا يصح أن يأخذ القاضي إلا بالدليل الذي يقدمه الخصوم وبعد عرضه شفويًا وعلنيًا في جلسة المحاكمة، وإتاحة الفرصة للخصوم للإطلاع عليه وإتاحة لهم فرصة مناقشته والرد عليه إن شاؤوا، أو أن يبدو رأيهم في قيمته الإثباتية.[4]

وتأسيسًا على ذلك يجب أن تبدي شفاهة وفي حضور جميع الخصوم كافة الطلبات والدفوع والمرافعات، فتطرح الأدلة عليهم للمناقشة فيها سواء كانت أدلة تقليدية أو أدلة

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص 97.

[2]- نفس المرجع، ص 97.

[3]- نادية ضريفي، دراج عبد الوهاب، مرجع سابق، ص123.

[4]- العبيدي أسامة بن غانم، **الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية**، الحقوق والعلوم السياسية، جامعة الملك سعود، مجلة جامعة الملك سعود، المجلد 25، العدد 01، جانفي 2013، السعودية، ص61.

إلكترونية، ويسمع شهود الدعوى من جديد في مواجهتهم، والخبير يجب أن يحضر ويقرأ تقريره شفويًا في الجلسة.[1]

ويترتب على إغفال الشفوية والحضورية بطلان إجراءات المحاكمة، لما يترتب على هذا الإغفال من إهدار لحق الدفاع بحرمانه من الإلمام بالأدلة المقدمة ضده، وليس هناك من دليل لا يصلح للمناقشة العلنية قبل أن يوضع موضع الإعتبار عند الإدانة أو البراءة، وبغير ذلك لا يستقيم عدل صحيح.[2]

وتطبيقًا لذلك قضت محكمة النقض الفرنسية ببطلان الحكم الذي أعتمد على معلومات قدمها أحد المستأنفين إلى المحكمة الإستئنافية مباشرة ولم تصل إلى علم بقية أطراف الدعوى، كما لا يجوز أيضًا للمحكمة أن تقضي بناء على أوراق قدمت بعد إنتهاء المرافعة وتطبيقًا لذلك قضت محكمة النقض الفرنسية بإبطال الحكم الذي أعتمد فيه القضاة في تكوين إقتناعهم على عناصر إثباتية ضمت بعد إغلاق باب المرافعة.[3]

ب-أن يكون للدليل الإلكتروني أصل في أوراق الدعوى:

إن إقتناع الشخصي للقاضي ليس مطلقًا بل هو مقيد بعدة ضوابط، بحيث لا يمكنه أن يؤسس حكمه بناءً على دليل لم يعرض للمناقشة ولو كان مقتنعًا به، ولذلك يجب أن يستند القاضي في حكمه بالإدانة إلى دليل عرض في الجلسة على الخصوم وتمت مناقشته، كما يجب أن يكون لهذا الدليل أصل في أوراق الدعوى فإذا لم يكن كذلك كان الحكم معيبًا موجبًا للنقض.[4]

أي أن يكون للدليل أصل ثابت في أوراق الدعوى ثم يطرح للمناقشة أثناء المحاكمة، وليس معنى ذلك أن تتم مناقشة ذلك الدليل علنًا، بل يكفي أن يوضع في ملف الدعوى الموضوعة تحت نظر القاضي وأن يتاح للخصوم الإطلاع عليه ومناقشته إن شاؤوا.[5]

2-موقف التشريعات المقارنة من مبدأ وجوب مناقشة الدليل الإلكتروني :

قد حرصت العديد من التشريعات الجنائية الإجرائية على النص صراحة على هذا المبدأ، ففي الدول ذات الصياغة اللاتينية فقد نص المشرع الجزائري في الفقرة 02 من المادة 349 من ق.إ.ج.ج على أنه: "لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض

[1]- ممدوح حسن مانع العدوان، **حجية الدليل الإلكتروني في الإثبات الجزائي**، الهيئة العالمية للتسويق الإسلامي، المجلة العالمية للتسويق الإسلامي، المجلد السادس، العدد الأول، 2017، لندن- المملكة المتحدة، ص 75.

[2]- عثمان محمد الحسن حاج علي، **حجية الأدلة الرقمية في إثبات جرائم الحاسب الآلي والإنترنت**، رسالة الماجستير في الفقه المقارن، قسم الفقه المقارن، كلية الشريعة والقانون الدراسات العليا، جامعة أم درمان الإسلامية،2011، ص 210.

[3]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 360.

[4]- بلجراف سامية، مرجع سابق، ص 687.

[5]- شنتير خضرة، مرجع سابق، ص 62.

المرافعات والتي حصلت المناقشة فيها حضوريًا أمامه"[1]، وهو نفس الحكم الذي أقره المشرع المصري في المادة 302 من ق.إ.ج.م والتي نصت على أنه: "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز أن يبني حكمه على أي دليل لم يطرح في الجلسة"، وكذا يتجلى موقف المشرع الفرنسي في الفقرة 02 من المادة 427من ق.إ.ج.ف والتي نصت على أنه: "لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة، ونوقشت أمامه في مواجهة الأطراف"[2].

كذلك فإن مبدأ وجوب مناقشة الدليل الجنائي من المبادئ الجوهرية التي يترتب على مخالفتها بطلان الإجراءات المتخذة في النظام الأنجلوسكسوني وخاصة في الولايات المتحدة الأمريكية، حيث أن عنصر الإثبات يجب أن يكون محلًا للمناقشة الحضورية بين الأطراف عن

[1]- وهو ما أكدته المحكمة العليا في حكم لها بتاريخ 12/ 01/ 1982 بأن: "لا يمكن لقضاة الموضوع أن يؤسسوا قرارهم إلا على الأدلة المقدمة لهم أثناء المرافعات، والتي تتم مناقشتها حضوريًا وذلك عملًا بالمادة 212 من قانون الإجراءات الجزائية"، وللمزيد من التفصيل، ينظر: بلجراف سامية، مرجع سابق، ص 687.

وفي ذلك قضت محكمة النقض المصرية بأن: "للمحكمة أن تأخذ من أدلة الدعوى بما تطمئن إليه وتطرح ما عداه ما دام له أصل ثابت بالتحقيقات"، وللمزيد من التفصيل، ينظر: نفس المرجع، ص 687.

وهذا ما يستخلص أيضًا من الأحكام القضائية مثل حكم محكمة النقض المصرية لسنة 2017 بقولها: "... وكان من المقرر أن المحكمة ليست ملزمة بالتحدث في حكمها إلا عن الأدلة ذات الأثر في تكوين عقيدتها، وكان من المقرر-أيضًا- أن الأدلة في المواد الجنائية إقناعية، وللمحكمة أن تلتفت عن دليل النفي ولو حملته أوراق رسمية -وفق المبدأ السالف سرده- ولا عليها أن تتعقبه في كل جزئية من جزئيات دفاعه، لأن مفاد إلتفاتها عنها أنها أطرحته"، وللمزيد من التفصيل، ينظر: شنتير خضرة، مرجع سابق، ص 63.

كما عبرت محكمة النقض المصرية عن ذلك في حكمها والذي ورد فيه: " إن أساس المحاكمة الجنائية هو حرية القاضي في تكوين إقتناعه من التحقيق الشفوي الذي يجريه بنفسه والذي يديره ويوجهه الوجهة التي يراها موصلة للحقيقة..."، وللمزيد من التفصيل، ينظر: بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 359.

كما أشارت إلى هذا المبدأ محكمة التمييز بدبي في حكمها الذي جاء فيه: "من الأسس الجوهرية للمحاكمات الجنائية قيامها على التحقيق الشفوي الذي تجريه المحكمة بجلسة المحاكمة في مواجهة المتهم وتسمع فيه الشهود... لأنه ليس للمحكمة أن تبدي رأيًا في دليل لم يعرض عليها لإحتمال أن يسفر هذا الدليل من إطلاعها على فحواه ومناقشته عن حقيقة قد يتغير بها وجه الرأي في الدعوى..."، وللمزيد من التفصيل، ينظر: نفس المرجع، ص 359.

وهذا ما أكد عليه المشاركون في الحلقة التمهيدية للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات التي عقدت على المستوى الدولي في"فريبورج" بألمانيا في الفترة من 8/5 أكتوبر 1992 تحت عنوان"جرائم الحاسوب وجرائم أخرى في مجال تكنولوجيا المعلومات"، فقد ذكروا أن ظهور المعلومات بكل خصائصها لا يغير شيئًا من مبدأ الإنتفاع الذاتي، فالإقتناع يجب أن يكون بناء على أثر الدليل الموجود في نفس القاضي وله أن يؤسس إقتناعه على أي من العناصر الإثباتية التي يكون للأطراف حرية الإعتراض عليها ومناقشتها، وللمزيد من التفصيل، ينظر: محمد صالح جاد المولى خليفة، مرجع سابق، ص 107.

[2]-Art 427 paragraphe 02 du C.P.P.F dispose que: « Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui».

طريق ممثليهم القانونيين، بينما يكون القاضي إلى حد مستمعًا ومصغيًا لكل ما يمكن أن يطرح في الجلسة.[1]

ولا يختلف الأمر عنه في التشريعات ذات الصياغة المختلطة فقد نص قانون الإجراءات الجنائية الياباني على وجوب مناقشة الأدلة الجنائية، حيث أن أطراف الدعوى هم الذين يتولون بدحض العناصر الإثباتية المطروحة في الجلسة تحت إشراف القاضي.[2]

3- النتائج المترتبة على مبدأ وجوب مناقشة الأدلة الإلكترونية:

تتمثل النتائج التي تترتب على مبدأ وجوب مناقشة الدليل الإلكتروني في ما يلي:

أ- عدم جواز أن يقضي القاضي بناء على معلوماته الشخصية:

من أهم النتائج المترتبة على مبدأ وجوب مناقشة الدليل الإلكتروني في الجلسة، أنه لا يسوغ للقاضي الجزائي أن يحكم بمقتضى معلوماته الشخصية في الدعوى التي يكون قد حصل عليها من محاضر قضية آخرى أو على ما رآه بنفسه أو حققه في غير الجلسة التي ينظرها والتي من الممكن أنه تؤثر في تكوين قناعته عند تقديره لأدلتها، ذلك أن هذه المعلومات لم تعرض في الجلسة ولم تتح مناقشتها وتقييمها ومن ثم يكون الإعتماد عليها مناقضًا لمبدأي الشفوية والمواجهة الذي يسود مرحلة المحاكمة العادلة.[3]

لأن القناعة المتولدة لدى القاضي هي جزء من مناقشة الأدلة والتي عن طريقها تتضح قوة أو ضعف الأدلة، فتتولد لدى القاضي قناعة من خلالها يأخذ بالدليل أو يستبعده.[4]

لكن يجوز له أن يستند في قضاءه إلى المعلومات العامة التي يفترض علم الكافة بها والتي يكتسبها القاضي من خبرته أو ثقافته العامة، مما لا تلتزم المحكمة قانونيًا ببيان الدليل عليه، فهي لا تعد من قبيل المعلومات الشخصية المحظورة على القاضي أن يبني حكمه عليها، فالقانون لم يوجب على القاضي الإستعانة بالخبراء لكشف أمور واضحة يدركها هو، كما لا يعد من قبيل القضاء بالعلم الشخصي إستناد القاضي إلى رأي علمي لا خلاف حوله.[5]

كما أنه لا يجوز له أن يكتسب صفتي الشاهد والقاضي في نفس الوقت، ذلك أن الشهادة في الأصل تخضع إلى التمحيص والتقدير من القاضي في صحتها حتى يمكن التحقق من صدقها، ولذلك إذا كان مصدر هذه الشهادة هو القاضي نفسه فإنه سيقع حينئذ في صراع مع نفسه فيتعذر عليه القيام بعملية تمحيص وتقدير تلك الشهادة.[6]

---

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص-ص 107-108.

[2]- نفس المرجع، ص108.

[3]- بلولهي مراد، **الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة**، رسالة الماجستير، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة، 2011/2010، ص116.

[4]- نادية ضريفي، دراج عبد الوهاب، مرجع سابق، ص 124.

[5]- بلولهي مراد، مرجع سابق، ص 116.

[6]- نفس المرجع، ص 116.

لأن الأمر يقتضي أن تكون المعلومات التي يدلي بعيدة عن التحيز والتأثيرات الشخصية، لذلك يجدر بالقاضي في هذه الحالة التنحي عن نظر الدعوى وإبداء أقواله كشاهد فحسب، حتى يتمكن الخصوم من مناقشتها بحرية، وينأى عن الدعوى خشية تأثره بمعلوماته ولو لم يكن لهذا التأثير من صدى ظاهر في أسباب حكمه.[1]

ب-عدم جواز أن يقضي القاضي بناء على رأي الغير:

أما فكرة عدم جواز أن يقضي القاضي في جريمة تمس بالمستند الإلكتروني بناء على رأي الغير فهي مما يتقيد به القاضي الجزائي أيضًا في تكوين إقتناعه عدم التعويل على رأي للغير بل يجب أن يستمد هذا الإقتناع من مصادر يستقيها بنفسه من التحقيق في الدعوى، وهذا نتيجة هامة من النتائج المترتبة على قاعدة وجوب مناقشة الدليل في المواد الجنائية، يستوي في ذلك أن يكون دليلًا تقليديًا أو متولدًا عن الأجهزة الإلكترونية، وأنه كان يجب أن يصدر الحكم عن عقيدة للقاضي يستقيها هو مما يجريه من التحقيقات مستقلًا في تحصيل هذه العقيدة بنفسه لا يشاركه فيها غيره.[2]

وتطبيقًا لهذا لا يجوز أن يحيل الحكم في شأن واقعة الدعوى ومستنداتها إلى دعوى آخرى غير مطروحة عليه، أو أن يعتمد على أدلة ووقائع إستقلها من محاضر قضية آخرى لم تكن مضمومة للدعوى التي ينظرها، ولا مطروحة بالجلسة التي ينظرها.[3]

كما يجب عليه أن لا يخضع لأي تأثير خارجي كتأثير رجال الصحافة مثلًا أو الفقهاء أو رجال الدين أو رأي الشخصيات البارزة، لأن الإثبات في المواد الجزائية يقوم على إقتناع القاضي نفسه بناء على ما يجري في الدعوى من تحقيق.[4]

وهذا يعني أنه للقاضي الإجتهاد في الحكم في الجرائم الماسة بالمستند الإلكتروني وعدم الإعتماد على رأي الغير، إلا إذا كان الغير من الخبراء وقد أرتاح ضميره إلى التقرير المحرر منه وقرر الإستناد إليه ضمن حكمه وبناء عليه يكون متولدًا من عقيدته وليس من تقرير الخبير[5]، ويتعين عليه في هذه الحالة أن يبين أسباب إقتناعه بهذا الرأي بإعتباره من الأدلة المقدمة إليه في الدعوى المطلوب منه أن يفصل فيها[6].

وهنا تظهر أهمية التدريب الفني الذي ينبغي أن يتلقاه القاضي في كيفية التعامل مع تقنية المعلومات وأنظمة معالجة المعطيات والأدلة الإلكترونية الناجمة عنها بشكل واف ودقيق، ومما

---

[1]- عثمان محمد الحسن حاج علي، مرجع سابق، ص-ص 212-213.

[2]- ممدوح حسن مانع العدوان، مرجع سابق، ص 76.

[3]- بلولهي مراد، مرجع سابق، ص 117.

[4]- نفس المرجع، ص 117.

[5]- نور الهدى محمودي، **مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي -دراسة تحليلية-**، أطروحة الدكتوراه علوم، تخصص:علم الاجرام وعلم العقاب، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1-الحاج لخضر-، 2018/2017، ص 199.

[6]- ممدوح حسن مانع العدوان، مرجع سابق، ص 76.

لاشك فيه أن التأهيل العلمي وعقد الدورات التدريبية المكثفة تعد من أهم الوسائل التي تضمن نجاح المهمة.[1]

المطلب الثاني: سلطة القاضي الجزائي في تقدير المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني

يعد تقدير الدليل بعد قبوله من قبل القاضي الجزائي من الخطوات الإجرائية الجوهرية في الإثبات الجنائي، إذ يناط به وحده سلطة تقدير الدليل المقبول وإستخلاص قناعته منه سواء أفضى ذلك إلى الحكم بالبراءة أو بالإدانة، والواقع أن هذه المسألة تتأثر بطبيعة نظام الإثبات المعتمد في الدولة، وعليه تختلف سلطة القاضي في تقدير أدلة الإثبات بإختلاف النظام الذي تتبناه الدولة.

وعلى هذا الأساس يصبح من الضروري التطرق إلى مختلف أنظمة الإثبات للوقوف على مدى سلطة القاضي في تقدير الأدلة، ولذلك سنتناول حجية المستند الإلكتروني في الإثبات الجنائي ضمن النظام الإثبات الحر في (الفرع الأول)، ثم في نظام الإثبات المقيد في (الفرع الثاني)، وأخيرًا في نظام الإثبات المختلط في (الفرع الثالث).

الفرع الأول: حجية المستند الإلكتروني في الإثبات الجنائي في النظام الإثبات الحر

ارتأينا أن نتطرق إلى الأسس التي يقوم عليها نظام الإثبات الحر، ثم إلى حجية الإثبات الجنائي بالدليل الإلكتروني في الفقه والتشريعات الآخذة بنظام الإثبات الحر، وإلى النتائج المترتبة على تطبيق مبدأ حرية الإثبات الجنائي بالدليل الإلكتروني.

أولًا: الأسس التي يقوم عليها نظام الإثبات الحر

تعد فرنسا من بين الدول التي تبنت نظام الإثبات الحر[2]، وقد سارت على نهجها العديد من التشريعات المقارنة وهو ما اعتمده أيضًا المشرع الجزائري، ويعرف هذا النظام بعدة تسميات

[1]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص-ص 361-362.

[2]- بداية منتصف القرن الثامن عشر تعرض نظام الأدلة القانونية والذي يحد من سلطة القاضي الجزائي في تقدير الأدلة لإنتقادات كثيرة من قبل الفلاسفة وفقهاء القانون، وكان العلامة بيكاريا beccaria أول داع للحركة في هذا المجال ونادى في مؤلفه الشهير "الجرائم والعقوبات" بأن اليقين المطلوب في المواد الجنائية لا يمكن أن يكون كامناً في قواعد الأدلة العلمية أو القانونية، ثم جاء فلانجيري filangieri مطالبًا بالقاعدة الشاملة والأساسية للإثبات في المواد الجزائية والتي توجب تأسيس كل إدانة وبصفة مطلقة على اليقين المعنوي وأن هذا اليقين لا يكمن إلا في ضمير القاضي، وللمزيد من التفصيل، ينظر: بلولهي مراد، مرجع سابق، ص-ص 10-11.

هذه الروح الجديدة أحدثت تقدمًا سريعًا وخاصة في فرنسا، حيث قام رجال القانون بمهاجمة نظام الأدلة القانونية، وكذلك القانون الجنائي الصادر عن لويس الرابع عشر سنة 1670 الذي أرسى قواعد هذا النظام، وكان من تأثير ذلك أن وافقت الجمعية التأسيسية في جلسة 18 جانفي 1791 على مشروع القانون الخاص بنظام المحلفين، وكذلك أقرت مبدأ الشفهية في المحاكمات ومبدأ حرية إقتناع القاضي، ثم تبنى المشرع الثوري في فرنسا مبدأ الإقتناع الشخصي، وصاغه في نصوص لا تعطي أي فرصة للبس، ونرى ذلك في قانون تحقيق الجنايات الصادر في 20 سبتمبر 1791، وفيما بعد في المادة 342 من قانون تحقيق الجنايات الصادر سنة 1808، والذي نقل حرفيًا تقريبًا من قانون التحقيق الجنائي الصادر سنة 1791 لكن مع=

منها نظام الإثبات الحر، أو النظام اللاتيني، أو نظام الأدلة الإقناعية، يقوم على حرية الإقتناع[1] فإقتناع الشخصي للقاضي ويقينه النابع من ضميره هو الذي يبني عليه الحكم، دون مراعاة لأي طريقة معينة يمليها عليه المشرع للوصول إلى الحقيقة[2]، بل يترك السلطة التقديرية للقاضي في تأسيس حكمه وفقًا لإقتناعه الشخصي بأي من الأدلة المطروحة أمامه[3].

والدليل الإلكتروني لا يقبل بطبيعته إخضاع القاضي لأي قيود بشأنه بل يجب أن يترك تقديره لسلطة القاضي[4]، فالقاضي الجزائي يملك حرية في الإستعانة بكل وسائل الإثبات المشروعة بناء على أي دليل يراه مقنعًا لإدانة المتهم أو تبرئته حسب ما يمليه عليه ضميره بما يتفق مع العقل والمنطق، كما يملك الحرية في تقدير الأدلة المطروحة عليه ولا يقيده المشرع بإضفاء أي قوة إثباتية لأي دليل، وضمير القاضي هو الذي يقوم بتحديد مدى قوة أي دليل في الإثبات وهذا ما أصطلح عليه بالدليل المعنوي الذي ينبع من ضمير القاضي[5]، مع تبيان الأسباب التي إستند عليها في إصدار حكمه.

وإن إعترف هذا النظام للقاضي الجزائي بسلطة الواسعة في تقدير الدليل، إلا أنه قد قيده من حيث الضوابط التي تحدد كيفية جمع الأدلة، وعدم الإلتزام بهذه الضوابط فقد تهدر من قيمة الدليل.[6]

ثانيًا: حجية المستند الإلكتروني في الإثبات الجنائي في الفقه والتشريعات الآخذة بنظام الإثبات الحر

بما أن النظام اللاتيني أو ما يعرف بالنظام الإثبات الحر يترك للقاضي أن يلتمس تكوين إقتناعه الشخصي من أي دليل يطرح أمامه في قبوله وحتى في تقديره، فإن حجية الدليل لا تثير صعوبة إنطلاقًا من حرية تقديم هذا الدليل بإعتباره من أدلة إثبات في المواد الجزائية، ويطرح في هذا الصدد تساؤل مفاده: ما مدى إمكانية الإعتداد بالمستندات الإلكترونية (مخرجات الإلكترونية) كدليل إثبات أمام القضاء؟ وما مدى حرية القاضي الجزائي في تقدير هذا النوع من الأدلة؟

=دقة وتفصيل أكثر، وأخيرًا فإنه نقل إلى المادة 427 من قانون الإجراءات الجنائية الفرنسي الحالي، وعلى ضوء هذه التطورات المتلاحقة في ميدان الإثبات الجنائي، يمكننا القول أنه منذ ذلك التاريخ تمتع القاضي بسلطة واسعة في تقدير الأدلة وفقًا لقناعته القضائية، وهو مبدأ مستقر في الفقه والقضاء، بحيث أنه يسود في معظم التشريعات المقارنة، وللمزيد من التفصيل، ينظر: بلولهي مراد، مرجع سابق، ص11.

[1]- نادية ضريفي، دراج عبد الوهاب، مرجع سابق، ص127.

[2]- عبد الرحمان خلفي، **الإجراءات الجزائية والمقارن**، الطبعة الرابعة، 2018-2019، دار بلقيس، دار البيضاء-الجزائر، ص478.

[3]- نادية ضريفي، دراج عبد الوهاب، مرجع سابق، ص127.

[4]- بلجراف سامية، مرجع سابق، ص 291.

[5]- عبد الرحمان خلفي، مرجع سابق، ص 478.

[6]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 245.

وللإجابة على التساؤل المطروح، لابد من التطرق إلى موقف الفقه وكذلك إلى مختلف التشريعات التي تبنت نظام الإثبات الحر:

1- موقف الفقه اللاتيني:

لا يشكل الدليل على الصعيد الجنائي الفرنسي أية مشكلة، حيث يرى أن الأساس هو حرية تقديم الأدلة للقاضي الجزائي وحريته في تقديرها، بمعنى آخر أن جميع أطراف الدعوى لهم الحق في تقديم أي دليل لإثبات دعواهم وبالمقابل فإن القاضي الجزائي الفرنسي له الحرية في وزن هذه الأدلة ومن ثم قبول الدليل وفقًا لما تطمئن إليه قناعته[1]، ولا يوجد خلاف في إضفاء الحجية على المخرجات الإلكترونية لأن حرية القاضي في تقدير الأدلة تدخل ضمن نطاق قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل الرادارات وأجهزة التصوير والتسجيل والتصنت، وتلك الأجهزة أخذ بها المشرع وقبلها القضاء بشروط معينة[2]، وعلى هذا الأساس حكمت محكمة النقض الفرنسية أن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي ولا يختلف الأمر بالنسبة لقبول المخرجات الإلكترونية.[3]

وفي ألمانيا فقد طرحت مسألة الأدلة الإلكترونية ومدى حجيتها في الإثبات الجنائي، ويرى هناك أن الفقرة 02 من المادة 224 من قانون الإجراءات الجنائية الألماني الإتحادي لسنة 1998 تلقي على المحكمة إلتزامًا بالوصول إلى الحقيقة والأخذ بالأدلة لكل الوقائع التي تكون هامة في إصدار الحكم، وهذا يعني أن جميع الأدلة الإلكترونية من مطبوعات ورقية أو معطيات هي أحد المصادر التي تقبلها المحكمة وتتخذها أساسًا لحكمها.[4]

2- موقف التشريعات الآخذة بنظام الإثبات الحر:

لا تثير حجية الأدلة الإلكترونية إشكالًا في الدول التي تتبنى النظام اللاتيني حيث يسود مبدأ حرية الإثبات والإقتناع، فبالنسبة للمواد الجنائية فإن السائد هو مبدأ حرية القاضي الجزائي في تكوين عقيدته لعدم تقيده بدليل معين، وعليه فإن المخرجات الإلكترونية تصلح لأن يأخذ القاضي بها في تكوين عقيدته وإستيفاء إقتناعه إذا ما إطمأن يقينه لصحة تلك المخرجات أو المستندات فإن الأساس هو حرية القاضي في تقدير هذه الأدلة.[5]

فبالرجوع إلى القواعد العامة في الإثبات الجنائي المقررة في قانون الإجراءات الجنائية الفرنسي نجده ينص في الفقرة الأولى من المادة 427 من ذات القانون على أن: "وبإستثناء

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص 194.
[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص 333.
[3]- أحمد يوسف الطحطاوي، مرجع سابق، ص 201.
[4]- رفاه خضير جياد العارضي، مرجع سابق، ص 195.
[5]- بن شهرة شول، مرجع سابق، ص311.

الحالات التي ينص فيها القانون على خلاف ذلك يجوز إثبات الجرائم بكل طرق الإثبات، ويحكم القاضي تبعًا لإقتناعه الشخصي".[1]

والمادة 353 من نفس القانون التي جاءت صياغتها كالآتي: "على رئيس محكمة الجنايات أن يعلن العبارات التالية على المحلفين قبل دخولهم المداولة، بل وأن تعلق في خط كبير في أوضح مكان في غرفة المداولة، بأن القانون لا يطلب من القضاة أن يقدموا حسابًا عن الوسائل التي قد توصلوا إلى تكوين إقتناعهم، ولا يرسم لهم قواعد يتعين لهم أن يستندوا إليها بإقتناعهم بكفاية الأدلة، بل أنه يلزمهم أن يسألوا أنفسهم في صمت وتأمل وأن يبحثوا في خلاصة ضمائرهم والإنطباع الذي أحدثته في عقولهم الأدلة المقدمة ضد المتهم ووسائل دفاعه، إن القانون لا يوجه لهم إلا السؤال الآتي الذي يحوي كل حدود واجباتهم هل لديكم إقتناع داخلي؟".[2]

ومما سبق ذكره نلاحظ أن لم يحدد المشرع الفرنسي طريقة معينة للإثبات وإنما أجاز إثبات الجرائم بجميع طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على خلاف ذلك، أي إذا كان هناك نص قانوني يحدد طريقة معينة للإثبات وجب التقيد بها، ومنه فإستخدام الأدلة الإلكترونية لا يثير أي إشكالية.

وإن كان من المفيد أن نعلم أن القانون الفرنسي رقم: 2004-575 الصادر بتاريخ 21 جوان 2004 المتعلق بالثقة في الإقتصاد الرقمي (L.C.E.N) أضاف للقانون المدني الفرنسي مادة جديدة وهي 1108-1 والتي تنص على أن القانون رقم: 2000-230 المتعلق بتكييف قواعد الإثبات مع تكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني السالف الذكر إعترف بالحجية للكتابة الإلكترونية بذات الحجية المقررة للمستندات التقليدية المدونة على دعامات مادية، هذا القانون هو متعلق أيضًا بالحجية المقرر لوسائل تكنولوجيا المعلومات.[3]

وبالرجوع إلى المادة 1316 المعدلة بموجب القانون رقم: 2000-230 المتعلق بتكييف قواعد الإثبات مع تكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني السالف الذكر بمقتضى تعديله للقانون المدني نجدها تنص على أن:" ينشأ الإثبات الخطي أو الإثبات الكتابي نتيجة من تسلسل حروف أو علامات أو أرقام أو أي رمز أو أي إشارة أخرى، ذات دلالة تعبيرية واضحة

[1]-Art 427 paragraphe 01 du C.P.P.F dispose que: « Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction».

[2]-Art 353 du C.P.P.F (Ordonnance n° 58-1296 du 23 décembre 1958) dispose que: « Avant que la cour d'assises se retire, le président donne lecture de l'instruction suivante, qui est, en outre, affichée en gros caractères, dans le lieu le plus apparent de la chambre des délibérations :

" Sous réserve de l'exigence de motivation de la décision, la loi ne demande pas compte à chacun des juges et jurés composant la cour d'assises des moyens par lesquels ils se sont convaincus, elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense. La loi ne leur fait que cette seule question, qui renferme toute la mesure de leurs devoirs :"Avez-vous une intime conviction " ?

[3]- بن شهرة شول، مرجع سابق، ص312.

ومفهومة، أيا كانت الدعامة التي تتضمنها، أو الوسيط الذي تنتقل عبره"[1]، وبموجب التعديلات الجذرية للقانون المدني الفرنسي التي جاء بها الأمر رقم: 2016-131 المتعلق بإصلاح قانون العقود والنظام العام وإثبات الإلتزامات السالف الذكر ألغى المادة السابقة الذكر وإحتفظ بنفس المضمون في المادة 1365 من ق.م.ف[2].

أما بالنسبة لموقف المشرع الجزائري فلم يختلف عن التشريعات التي تعتنق نظام الإثبات الحر كمبدأ في الإثبات الجنائي والذي يعطي للقاضي الحرية في الإقتناع، فنصت الفقرة الأولى من المادة 349 من القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية على أنه: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات بما فيها الالكترونية، ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعًا لإقتناعه الخاص"، يتضح أن المشرع الجزائري قد أقر مبدأ حرية الإثبات، حيث أجاز للقاضي الاعتماد على أي وسيلة يراها مناسبة لاثبات الجرائم بما في ذلك الوسائل الإلكترونية، إلا إذا نص القانون على خلاف ذلك فيتقيد القاضي في هذه الحالة بالوسائل وأدلة الإثبات المحددة في النص القانوني.

كما تناول المشرع الجزائري أيضًا حجية المخرجات الإلكترونية في الباب السادس المتضمن إثبات الإلتزام وبالضبط في الفصل الأول متعلق بالإثبات بالكتابة وذلك بموجب التعديل الذي أجراه على القانون المدني بموجب القانون رقم: 05-10 المؤرخ في 20 جوان 2005 السالف الذكر، وذلك في المادة 323 مكرر التي نصت على أن: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها"، ولم يكتفي المشرع الجزائري بهذه المادة وإن كانت الواضح منها إعتدادها بحجية المخرجات الإلكترونية حسب العبارة الأخيرة من المادة "مهما كانت الوسيلة التي تتضمنها" فالتفسير يحمل على التوسع في مفهوم الوسيلة، ثم إن الرموز أو العلامات أكثر إستعمالاتها وإستخداماتها تشيع في المعاملات الإلكترونية، ثم أعقب بالمادة 323 مكرر1 من ذات القانون للتأكيد على حجيتها صراحة بالقول: " يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق"، لكنه في ذات الوقت علق الإعتراف بها على شرطان حين قال: "بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تحفظ سلامتها"، مثلما نص صراحة على معادلة التوقيع الإلكتروني في القيمة القانونية والإحتجاجية بالتوقيع الخطي في الفقرة 02 من المادة 327.[3]

---

[1]-Art 1316 du C.C.F (Modifié par Loi n°2000-230 du 13 mars 2000 -art. 1 JORF 14 mars 2000, Abrogé par Ordonnance n°2016-131 du 10 février 2016) dispose que : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission».

[2]- Art 1365 du C.C.F (Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations- art.4) dispose que: « L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support».

[3]- بن شهرة شول، مرجع سابق، ص-ص 313-314.

أما بالنسبة لموقف المشرع المصري فقد جعل من مبدأ حرية الإثبات أساسًا لنظام الإثبات لديه، فقد خصص المادة 291 من ق.إ.ج.م لحرية القاضي في الإثبات ونصت على أنه: " للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازمًا لإظهار الحقيقة "، كما خصص المادة 302 من نفس القانون لحرية القاضي في الإقتناع ونصت على أنه: "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة"، وقد أكدت محكمة النقض المصرية على إتجاه القانون في الأخذ بهذا المبدأ في العديد من أحكامها فجاء في أحد أحكامها: " أن تقدير الدليل مسألة موضوعية مرجعها إقتناع المحكمة أو عدم إقتناعها، وأن مطالبة المحكمة بإتباع قاعدة ثابتة تطبقها على كل الوقائع وتتبعها مع كل الشهود هو مصادرة لحريتها الأساسية في وزن عناصر الإثبات المختلفة، وتقديرها على الوجه الذي يرتاح إليه ضميرها"[1]، كذلك نصت في حكم آخر على أنه: "من المقرر إذا كانت المحكمة قد رأت أن الفصل في الدعوى يتطلب تحقيق دليل بعينه، فواجب عليها أن تعمل على تحقيق هذا الدليل أو تضمن حكمها الأسباب التي دعتها إلى أن تعود فتقرر عدم حاجة الدعوى ذاتها إلى هذا التحقيق"[2].

إلا أن المشرع المصري تدارك الأمر وأقر بحجية المخرجات الإلكترونية بموجب المادة 15 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر الذي نص صراحة على أن للكتابة الإلكترونية وللمحررات الإلكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية، متى إستوفت الشروط المنصوص عليها في هذا القانون وفقًا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون.

وبصدور القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر عرف المشرع المصري الدليل الإلكتروني في المادة الأولى منه وإستخدم مصطلح الدليل الرقمي للدلالة عليه، وعرفه كالآتي: " الدليل الرقمي: أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها بإستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة"، وإعترف له بذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائي في المادة 11 من نفس القانون كالآتي: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص204.

[2]- نفس المرجع، ص-ص 204-205.

وأحال الشروط الفنية الواجب توفرها لكي يكون للدليل الإلكتروني ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائي بموجب اللائحة التنفيذية لهذا القانون[1] في المادة 09 منها، ونص على أن: "تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائي إذا توافرت فيها الشروط والضوابط الآتية:

1- أن تتم عملية جمع أو الحصول أو إستخراج أو إستنباط الأدلة الرقمية محل الواقعة، بإستخدام التقنيات التي تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات أو أي تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات أو أنظمة المعلومات أو البرامج أو الدعامات الإلكترونية وغيرها، ومنها على الأخص تقنية (Write Blocker, Digital Images Hash) وغيرها من التقنيات المماثلة؛
2- أن تكون الأدلة الرقمية ذات صلة بالواقعة وفي إطار الموضوع المطلوب إثباته أو نفيه، وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة؛
3- أن يتم جمع الدليل الرقمي وإستخراجه وحفظه وتحريزه بمعرفة مأموري الضبط القضائي المخول لهم التعامل مع هذه النوعية من الأدلة، أو الخبراء المتخصصين المنتدبين من جهات التحقيق أو المحاكمة، على أن يبين في محاضر الضبط أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم إستخدامها، مع توثيق كود وخوارزم (Hash) الناتج عن إستخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمي بمحضر الضبط أو تقرير الفحص الفني، مع ضمان إستمرار الحفاظ على الأصل دون عبث به؛
4- في حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية التحفظ على الأجهزة محل الفحص لأي سبب يتم فحص الأصل ويثبت ذلك كله في محضر الضبط أو تقرير الفحص والتحليل؛
5- أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له، وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته".

ثالثًا: النتائج المترتبة على تطبيق مبدأ حرية الإثبات الجنائي

وعلى ضوء ما سبق، فإن القاضي الجزائي في نظام الإثبات الحر لا يكون مقيدًا بأدلة إثبات محددة بل يتمتع بحرية تأسيس حكمه وفقًا لإقتناعه الشخصي إستنادًا إلى أي من الأدلة المعروضة أمامه، بإستثناء الحالات التي نص فيها القانون صراحة على خلاف ذلك، وهو ما منحه دورًا إيجابيًا في قبول وتقدير الدليل الإلكتروني.[2]

[1]- اللائحة التنفيذية للقانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، الصادرة عن رئيس مجلس الوزراء بموجب القرار رقم: 1699 لسنة 2020، الجريدة الرسمية العدد 35 تابع (ج)، الصادر بتاريخ 27 أوت 2020.
[2]-عائشة بن قارة مصطفى، مرجع سابق، ص189.

1- الدور الإيجابي للقاضي الجزائي في توفير الدليل الإلكتروني:

يقصد به عدم إلتزام القاضي بما يقدمه له أطراف الدعوى من أدلة، وإنما له سلطة وواجب عليه أن يبادر من تلقاء نفسه إلى إتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة الفعلية فيها، ذلك أن الحقيقة لا تظهر من تلقاء نفسها وإنما في حاجة دومًا إلى من يبحث وينقب عنها.[1]

فهذا النظام يتميز بمنح الدور الفعال للقاضي حيال الدليل الذي يوضع أمامه، فمن جهة يكون القاضي حرًا في أن يستعين بكافة طرق الإثبات للبحث عن الحقيقة والكشف عنها بإتخاذ الإجراء الذي يراه مناسبًا ويقتنع به، وهو في ذلك يختلف عن القاضي المدني الذي يكون دور هذا الأخير سلبيًا في الدعوى المنظورة أمامه، إذ يقتصر دوره على الموازنة بين أدلة الخصوم ثم يرجح أيهما الأغلب دون أن يبحث بنفسه فيما يعتقد أنه مفيد في إظهار الحقيقة، ومن جهة أخرى فقد خول للقاضي الجزائي حرية في وزن وتقدير قيمة كل دليل طرح أمامه، وبالإضافة إلى التنسيق بين الأدلة المقدمة إليه وإستخلاص نتيجة منطقية من هذه الأدلة مجتمعة إما بالإدانة أو البراءة.[2]

2- الدور الإيجابي للقاضي الجزائي في قبول الدليل الإلكتروني:

يقصد بالدور الإيجابي للقاضي الجزائي في قبول الدليل الإلكتروني أن لا يقتصر دوره مجرد قبول الأدلة الإلكترونية المطروحة أمامه لمناقشتها، بل يتعين عليه أن يتأكد من مدى مشروعيتها وذلك قبل تقديره لهذا الأدلة، لأن القاضي الجزائي لا يقدر إلا الدليل المقبول ولا يتحقق ذلك إلا إذا كان مشروعًا.[3]

الفرع الثاني: حجية المستند الإلكتروني في الإثبات الجزائي في نظام الإثبات المقيد

يعتبر نظام الإثبات المقيد (القانوني) من أقدم أنظمة الإثبات الجنائية، حيث كان الكهنة في العصور القديمة هم الذين يحددون طرق ووسائل الإثبات إلى أن وجدت الدولة بمفهومها الحديث فتولت هي بنفسها ذلك[4]، ولبيان حجية المستند الإلكتروني في نظام الإثبات المقيد وجب علينا التطرق إلى الأسس التي يقوم عليها هذا النظام، والإستثناءات الواردة على القواعد التي تحكمه.

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص-ص 189-190.
[2]- بلولهي مراد، مرجع سابق، ص 14.
[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 195.
[4]- عميروش هنية، داعي عز الدين، مرجع سابق، ص 141.

أولًا: الأسس التي يقوم عليها نظام الإثبات المقيد

يعرف هذا النظام بنظام الإثبات المحدد أو نظام الأدلة القانونية بحيث تكون فيه الأدلة محصورة ومحددة سلفًا من قبل المشرع، بحيث يقتصر دور القاضي في هذا النظام على مجرد فحص الدليل والتأكد من توافر الشروط التي حددها القانون فلا سبيل للإستناد على دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات، كما لا دور للقاضي في تقدير القيمة الإستدلالية للدليل حيث أن القانون يقيد القاضي بقائمة الأدلة التي حددت قيمتها الإثباتية.[1]

كما لا يعرف هذا النظام مبدأ إقتناع القاضي بل يحل محله إقتناع المشرع المبني على إفتراض صحة الدليل، وعملية الإثبات تتم من خلال وضع المشرع لقواعد تحدد للقاضي طريقة إقتناعه أو بمعنى آخر طريقة بناء حكمه، ويقتصر دور هذا الأخير على تطبيق القانون من حيث توافر الدليل وشروطه[2]، ففي الحالة التي يتوافر فيها شروط الدليل على النحو الذي حدده وقيده المشرع يلزم القاضي الجزائي بأن يؤسس حكمه على أساس هذا الدليل، حتى وإن لم يكن مقتنعًا به، وفي حالة ما إذا لم تتوافر الشروط المطلوبة قانونًا يكون القاضي الجزائي ملزمًا ببناء إقتناعه وتأسيس حكمه على أساس عدم قيام الدليل على الإدعاء، حتى لو كان القاضي الجزائي على قناعة بثبوت الإدعاء.[3]

وعليه فإنه في حالة توافر الدليل على شروط حددها وقيدها المشرع يكون القاضي ملزمًا بتأسيس حكمه حتى وإن كان القاضي غير مقتنع به[4]، إذ يقوم إقتناع المشرع بصحة الإسناد أو عدم صحته مقام إقتناع القاضي، وهكذا فإن اليقين القانوني يقوم أساسًا على إفتراض صحة الدليل بصرف النظر عن حقيقة الواقع أو إختلاف ظروف الدعاوى[5].

وعليه فإن في النظم التي تتبنى هذا النظام لا يمكن في ظلها الإعتراف للدليل الإلكتروني بأية قيمة إثباتية، ومهما توافرت فيه شروط اليقين فلا يجوز للقاضي أن يستند إليه لتكوين عقيدته ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، من ثم فإن خلو القانون من النص عليه سيهدر قيمته الإثباتية.[6]

ويحكم الدليل في هذا النظام قاعدتان، الأولى قاعدة إستبعاد شهادة السماع والثانية قاعدة الدليل الأفضل:

---

[1]- بلهادي حميد، مرجع سابق، ص 27.

[2]- عبد الرحمان خلفي، مرجع سابق، ص 477.

[3]- نادية ضريفي، دراج عبد الوهاب، مرجع سابق، ص 125.

[4]- بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، مرجع سابق، ص 282.

[5]- أحمد يوسف الطحطاوي، مرجع سابق، ص 206.

[6]- نفس المرجع، ص-ص 33-34.

1- قاعدة إستبعاد شهادة السماع:

المقصود بها الشهادة التي يكون الشاهد الذي أدلى بما قد سمعها ولم يشارك في وضعها بإحدى حواسه[1]، كأن يأتي شخص يحكي ما سمعه من أشخاص آخرين عن وقائع القضية أو عن المتهم ويتقدم إلى المحكمة من أجل إظهار الحقيقة، أو بعبارة أخرى من أجل إثبات أمر حدث خارج الجلسة وكان صادقًا[2].

ووفقًا لهذه القاعدة فإنه يشترط لقبول الشهادة في الإثبات أن تكون صادرة من الشخص الذي إتصل علمه مباشرة بوقائع القضية المراد إثباتها، بمعنى أن الوثيقة لا تقبل في الإثبات إلا إذا شهد محررها بمضمونها أمام المحكمة، فالشهادة التي تصدر عن شخص دراية بالأحداث والوقائع والمعلومات المراد إثباتها ويدلي بها بعد حلفه اليمين وتكون متبوعة بتحقيق حضوري، تعد كأنها الخيار الوحيد الذي يتيح للقاضي والمحلفين إختبار شهادة الشاهد من حيث مدى صدقها وتطابقها مع الواقع.[3]

إذ أن الدليل هو بيان أو قول داخل المحكمة يكرر فيه الشخص ما أدلى به خارج المحكمة، وكذلك الأدلة الواردة في الوثيقة هي مجرد قول مكتوب في وثيقة، فإذا لم تقدم هذه الوثيقة للمحكمة لإثبات أن التصريحات الواردة بها صحيحة فإن الدليل المستمد منها يستبعد، بإعتبار أن ما أحتوته هذه الوثيقة تم خارج المحكمة[4]، ويعد الدليل الإلكتروني عبارة عن شهادة سماع كونه يتضمن جمل وكلمات قام بإدخالها شخص إلى الأجهزة الإلكترونية سواء تم معالجتها أم لا، فهي في الحقيقة حدثت خارج المحكمة فمن شأن ذلك أن يثير إعتراضًا على قبول المستندات الإلكترونية المطبوعة في الإثبات أمام القضاء الجزائي وبالتالي يتم إستبعادها[5].

غير أن هناك من يرى في الفقه الأنجلوسكسوني أن قاعدة عدم جواز الشهادة السماعية هي قاعدة ليست ثابتة، بل يوجد عليها إستثناءات تلزم من خلالها الجهات القضائية الأخذ بهذه الشهادة ومن هذه الإستثناءات:

1- إذا كانت هذه الشهادة السماعية هي أفضل الأدلة المتاحة لعدم توافر الشاهد الأصلي نتيجة الأسباب الأتية:

أ- موت الشاهد الأصلي، أو مرضه مرضًا شديدًا؛

ب- تواجد الشاهد خارج حدود الدولة، وليس من المعقول علميًا ضمان حضوره؛

ت-لا يمكن العثور عليه.

---

[1]- بلجراف سامية، مرجع سابق، ص 688.

[2]- بن طالب ليندا، مرجع سابق، ص 126.

[3]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 214.

[4]- سالم محمد الأوجلي، **مقبولية الدليل الرقمي في المحاكم الجنائية**، كلية القانون، جامعة بنغازي، مجلة دراسات قانونية، المجلد 2016، العدد 19، جانفي 2016، ليبيا، ص 38.

[5]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 233.

2- تقبل الشهادة السماعية كذلك في حالة ظهور المستندات التي تم نقل الشاهد عن صاحبها كالسجلات التجارية وغيرها، ففي هذه الحالة تكون الشهادة السماعية مقبولة.[1]

يتبين مما سبق أن الدليل الإلكتروني يدخل ضمن الحالات الإستثنائية لقاعدة شهادة السماع، ليصبح هذا الدليل مقبولًا في الإثبات الجنائي.

إن معظم المحاكم الفيدرالية التي قيمت قبول سجلات الإلكترونية قامت بالتركيز على سجلات الإلكترونية كشهادة سماع (Hearsay)، حيث إعترفت المحاكم بشكل عام على إبراز أن هذه السجلات تقع داخل إستثناء سجلات الأعمال المادة 803 (06) من قانون الإثبات الفيدرالي الأمريكي.[2]

وتجدر الإشارة إلى أن قبول الدليل الإلكتروني على أساس إستثناء عن قاعدة شهادة السماع لا يمكنه أن ينطبق على جميع أنواع السجلات الإلكترونية، ذلك أنه ذكر سابقًا أن هذه الأخيرة تم تقسيمها من قبل وزارة العدل الأمريكية سنة 2002 إلى ثلاث أقسام، سجلات المحفوظة في الحاسوب، وسجلات التي تم إنشاؤها بواسطة الحاسوب، وهناك نوع ثالث من السجلات يجمع بين التدخل الإنساني ومعالجة الحاسوب المتمثل في السجلات المختلطة.[3]

ففي النوع الأول حيث تحتوي سجلات الحاسوب المخزنة على معطيات بشرية مثل المخرجات من برنامج الكتابة من الكمبيوتر (Word)، فهي تعتبر شهادة سماعية مثلها في ذلك مثل الكلمات أو التقريرات التي يسجلها الإنسان على الأجهزة المختلفة[4]، هذا النوع من السجلات يتم قبوله إستثناء من قاعدة السماع، فإذا ما تم قبول هذا النوع من السجلات فإن مزود هذه السجلات يجب أن يظهر أن الظروف التي تشير إلى المعطيات البشرية الموجودة في السجل موثوق بها ويعتمد عليها كما يجب أن تكون صحيحة[5]، فإن الذي يهدف إلى قبولها ما عليه سوى التأكد من صحة وسلامة سجلات الحاسوب وكذا سلامة برنامجه وعمله بشكل عادي، ولا يحتاج إلى إثبات أن إستثناء السماع يطبق على السجلات المطلوب قبولها في المحكمة[6].

أما النوع الثاني فإن الجهاز هو الذي يقوم بتدوين المعطيات التي تصلح أن تقدم مباشرة إلى المحكمة فهي ليست من قبيل شهادة السماع، وتتوقف قيمته الثبوتية على ما إذا كان

[1]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 215.
[2]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 234.
[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 202.
[4]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 202.
[5]- نفس المرجع، ص 234.
[6]- نفس المرجع، ص 235.

الحاسوب يعمل بطريقة أم لا[1]، فإنه يجب على من يسعى إلى جعلها مقبولة أن يثبت أن هذه المعطيات إستثناء من شهادة السماع، وبالتالي مطالب بإثبات حقيقة هذه المعطيات ويقينيتها[2].

أما بالنسبة للنوع الثالث والذي يجمع بين التدخل الإنساني ومعالجة الحاسوب وإن كان جزء منها يعد شهادة السماع وهو الصادر عن الإنسان إلا أنه لا يعد هذا النوع من السجلات شهادة السماع، حتى وإن كان يجب توافر لصحة المستند الإلكتروني شرطين، فمن ناحية يجب توافر الشرط اللازم لصحة الشهادة السماعية، كما أنه يجب التأكد من عمل الحاسوب نفسه على نحو الصحيح.[3]

ومن خلال التجارب التي مر بها القضاء الإنجليزي يلاحظ أنه حتى وإن قبل الدليل الإلكتروني في الإثبات الجنائي كإستثناء من قاعدة شهادة السماع إلا أنه قد قبل الدليل على أساس أنه شهادة مباشرة، ومن بين القضايا التي توضح لنا هذا الأمر قضية (R.V. WOOD) التي تتلخص وقائعها في أنه تم سرقة بعض المعادن وبعد ذلك تم ضبطها في حيازة أحد الأشخاص وأصبح متهمًا، وقد كانت تركيبة المواد الكيمياوية لهذه المعادن مسجلة في جهاز الحاسوب للمجني عليه وقد قدم الورقة المستخرجة من جهازه كدليل إثبات، والسؤال الذي طرح في هذه القضية هل تعتبر هذه الورقة الناتجة عن الحاسوب دليلًا سماعيًا وبالتالي لا نأخذ به؟ حيث أن المحكمة أجابت في هذا الإطار: "أن الورقة الناتجة عن الحاسوب مقبولة وفقًا للشريعة العامة وتصلح للإثبات"، وقد قبلتها على أساس أنها شهادة مباشرة.[4]

وفي نفس الإتجاه أيضًا قضت محكمة الإستئناف في إنجلترا بقبول الدليل المستخرج من الحاسوب كوسيلة إثبات مباشر وليست من الأدلة السماعية قضية (R.V. PETTIGREW)، وتدور أحداث هذه القضية حول السطو على البنك وتم إيجاد في حيازة المتهم أرقام النقود مسروقة، في أحد الأيام قام شخص بسرقة بنك وبعد مدة ألقي عليه القبض وكانت أرقام النقود مسجلة في حاسوب البنك في إنجلترا، وقد قبلت المحكمة وأخذت المحكمة من مخرجات الحاسوب الورقية كدليل إثبات مباشر وليست من الأدلة السماعية، بإعتبارها دليلًا مباشرًا وليس من الأدلة السماعية.[5]

2- قاعدة الدليل الأفضل:

تقوم فكرة الدليل الأفضل على المطالبة بالدليل الأصلي (Original Evidence) عند التعامل مع محتويات الكتابة أو التسجيلات أو الصور، لضمان أن الأحكام والقرارات التي

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 202.
[2]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 235.
[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 203.
[4]- نفس المرجع، ص 203.
[5]- نفس المرجع، ص 204.

تصدرها المحاكم تستند إلى أفضل[1] المعطيات والمعلومات والأدلة المتاحة[2]، وبمقتضى هذه القاعدة لا تكون الوثيقة مقبولة إلا إذا قدمت في شكلها الأصلي.

وعند تطبيق هذه القاعدة من حيث المبدأ على الأدلة الإلكترونية تم إستبعادها كوسيلة إثبات في هذا النظام، ويرجع السبب في ذلك أنه غالبًا ما يعرض الدليل الإلكتروني أمام القضاء في شكل مستندات مطبوعة أو كمعطيات معروضة على شاشة الأجهزة الإلكترونية[3]، والدليل الإلكتروني هو في حقيقته عبارة عن بيانات غير محددة لأرقام ثنائية، فالصورة في العالم الرقمي مثلًا ليس لها ذلك الوجود المادي المتمثل في الشكل الورقي المعروف في العالم المادي وإنما هي في أصلها مكونة من مجموعة من أرقام ثنائية، فكل ماهو موجود في العالم الرقمي في الأصل هو عبارة عن تعداد لا محدود لأرقام ثنائية، وهذه الأرقام في تكوينها الحقيقي ما هي إلا عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها ونشاطها من الطاقة[4].

مما لا يتيح للمحلفين أو للقاضي رؤية أو وضع أيديهم على الدليل الأصلي وما يقدم إليهم من مخرجات إلكترونية ليست سوى نسخ لأصول مما يجعلها دليلًا ثانويًا[5]، وهو ما أدى إلى قلق السلطة القضائية من أن مجرد مخرجات طابعة ملف إلكتروني مخزن على الأجهزة الإلكترونية لا يعد أصليًا[6].

ولذلك عادة ما يثار تساؤل حول صحة النسخة ودقتها مما يبعث الشك والريبة في هذه النسخة وإعتمادها كدليل إثبات في الدعوى، وفي هذه الحالة فإن تقديم أصل الدليل الإلكتروني غالباً ما يكون مرغوبًا، لأنه يزيل الشك أو الخطر بأن النسخة معدلة أو أن الأصل ذاته تم تغييره ونسخ منه شكل مطابق له تمامًا بعد تغييره والتلاعب فيه[7]، فعلى سبيل المثال الوثيقة المطبوعة من وثائق مايكروسوفت وورد (Microsoft Word) لا تظهر جميع التعديلات والملاحظات في حالة ما إذا تم فيها تغيير الوثيقة الأصلية، بالإضافة إلى ذلك أن الأصول في

---

[1]- لا يجوز قبول نسخة أو صورة من المستند إذا كان من الممكن الحصول على الأصل، وتطبيقًا لذلك قضت محاكم الولايات المتحدة بعدم صلاحية الصورة المقدمة من المدعي عليه أمام وجود دليل أصلي وذلك عندما قامت الشرطة الفدرالية بتفتيش أحد المتهمين بإرتكاب جناية حيازة سلاح ناري دون ترخيص، إذا قام الضباط بضبط السلاح الناري والذخيرة وأثناء التفتيش وجدوا صورة فوتوغرافية للمدعي عليه بمسدس"مسدود الفوهة" بمعنى أنه لا يسبب أذى ولا يحقق نتيجة جرمية ويبدو متطابقًا مع المسدس الذي تم ضبطه دليلًا، ولكن لم يقم أعضاء الضبط بضبط هذه الصور لعدم الحاجة إليها، دفع المدعى عليه بهذه الصور بوصفها دليلًا على أن المسدس الذي بحوزته ليس ضرر وليس هو المسدس المضبوط، لم تقبل المحكمة هذا الدفع لوجود الدليل الأفضل وهو المسدس الذي ضبطه المفتش، وأيضًا لعدم قدرة المدعى عليه من تقديم المسدس الموجود في الصورة حتى يتمكن من تقديم الدليل الأفضل، وللمزيد من التفصيل، ينظر: محمد صالح جاد المولى خليفة، مرجع سابق، ص-ص 211- 212.

[2]- سالم محمد الأوجلي، مرجع سابق، ص 37.

[3]- عثمان محمد الحسن حاج علي، مرجع السابق، ص 218.

[4]- محمد صالح جاد المولى خليفة، مرجع سابق، ص-ص 217-218.

[5]- عثمان محمد الحسن حاج علي، مرجع سابق، ص 218.

[6]- عائشة بن قارة مصطفى، مرجع سابق، ص 197.

[7]- سالم محمد الأوجلي، مرجع سابق، ص 37.

بعض العمليات التي تجرى عن طريق الأجهزة الإلكترونية قد لا تعود موجودة وربما لم يكن لها وجود أصلًا كما في حالة التحليلات أو الإسقاطات المعالجة[1].

بمعنى لا يجوز تقديم الصورة لإثبات محتوى الأصل بصفة عامة حين يقدم أحد الأطراف تأييداً لدعواه دليلًا يستند إلى عدة دعائم فإن عليه أن يقدم أفضل نموذج، وهو ما يعني أن تكون الأدلة الواجب تقديمها أولية وليست ثانوية أصلية لا بديلة، وأن يكون الدليل المقدم هو أفضل ما يتاح الحصول عليه بالنسبة لطبيعة وظروف القضية.[2]

غير أن قاعدة الدليل الأفضل ترد عليها إستثناءات وردت في القاعدة الفيدرالية للأدلة رقم: 1004، حيث تضمنت الحالات والظروف التي لا يطلب فيها من المقدمين للأدلة المتعلقة بالتسجيل أو بالصورة أو بالكتابة تقديم الأصل، بل يمكن على سبيل الإستثناء إثبات محتوياتها من خلال الأدلة الثانوية.[3]

ثانيًا: الإستثناءات الواردة على القواعد التي تحكم نظام الإثبات المقيد

على ضوء ما تقدم، تقوم قاعدة إستبعاد شهادة السماع بعدم قبول الوثيقة في الإثبات إلا إذا شهد منشئ مضمونها أمام المحكمة، أما بالنسبة لقاعدة الدليل الأفضل فلا تكون الوثيقة مقبولة إلا إذا قدمت في شكلها الأصلي، أي عدم قبول الإثبات عن طريق المخرجات الإلكترونية والتي هي في أغلبها مستندات الإلكترونية، وعلى ضوء ما جاء به هذا النظام قد يؤدي إلى إفلات الكثير من مرتكبي الجرائم الماسة بالمستند الإلكتروني من العقاب، ولذلك يثار تساؤل حول مدى إمكانية قبول الدليل الإلكتروني في الإثبات الجنائي بإعتبارة إستثناءً على القواعد التي تحكم نظام الإثبات المقيد؟

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 197.

[2]- نفس المرجع، ص-ص 204-205.

[3]- أ- وفقًا للقاعدة الفدرالية 1004 فقرة (أ) يكون الإستثناء الأول عندما تضيع الأصول الأصلية أو تدميرها، وتكون حالة فقدان الدليل في ظروف قاهرة كالحريق أو أية ظروف طبيعة أخرى، أو الإهمال الوظيفي بدون سوء نية، وتكون حالة التدمير كما في حالة التخلص الدوري من الوثائق في المؤسسات والشركات أو في حالة التطوير الدوري لبرامج وأنظمة الحواسيب، الأمر الذي يترتب عليه أحيانًا حدوث مسح كلي أو جزئي للمعطيات المخزنة في الحاسوب أو محو أشرطة التسجيل الأصلية، ففي تلك الحالات تقبل نسخة أو الصورة أو الشهادة القولية بديلًا للأصل، فقد سمحت محكمة الإستئناف الدائرة الأولى في الولايات المتحدة بقبول الشهادة حول محتويات مذكرة يزعم أنها كتبت من قبل المدعى عليه بعد أن ثبت أن هذه المذكرة قد دمرت بدون سوء نية من قبل جهات إنفاذ القانون وعد هذا الإجراء صحيحًا؛

ب- هي الحالة التي يكون فيها الدليل في حيازة شخص غير معروف للمحكمة أو لا يخضع لسلطاتها بحكم القانون، كما في الحالة بالنسبة للأشخاص الذين يتمتعون بالصفة الدبلوماسية؛

ج- حالة إستحالة تقديم الأصل، أي كان الحصول على الأصل وتقديمه للمحكمة مستحيلًا من الناحية العلمية، كما لو كان الأصل مكتوبًا أو منقوشًا على جدران مقبرة ومن خلال هذه الظروف يجوز للمحاكم أن تقبل على سبيل الإستثناء أدلة ثانوية -صور أو نسخ- تثبت صحة الدليل الأصلي وتخرج المحكمة من ثم من قاعدة أفضل دليل، وللمزيد من التفصيل، ينظر: محمد صالح جاد المولى خليفة، مرجع سابق، ص-ص 212-213.

1- خضوع المخرجات الإلكترونية لقاعدة إستبعاد شهادة سماع في الجرائم الماسة بالمستند الإلكتروني:

أصدر المشرع الإنجليزي قانون خاص بالإثبات الجنائي سنة 1956 وذلك حينما قرر مجلس اللوردات عدم قبول مخرجات الميكروفيلم كدليل في الإثبات الجنائي، غير أن المجلس المذكور سرعان ما تدارك إلى أن سوف يؤدي ذلك إلى إفلات الكثير من العقاب، لذلك أقر المجلس المذكور قانون الإثبات الجنائي في سنة 1956 الذي نص في مادته الأولى على أن: "المستند الذي يتضمن تقريرًا الذي يهدف لإثبات واقعة مادية يمكن إعتماده دليلاً عليها إذا إستوفى المستند شروطًا معينة، ومن بينها أن يكون قوام السجل المستندي معلومات يقدمها شخص لديه، أو يمكن إفتراض أن لديه معرفة شخصية بالأمور المتعلقة بالمعلومات التي يقدمها".[1]

غير أن تطبيق ما جاء في نص المادة المذكورة على الدليل الإلكتروني قد أثار صعوبات تمثلت في عدم الإعتداد بهذا الدليل في غالبية القضايا التي طرحت على المحاكم إلتزامًا بنص المادة المذكورة، مما أدى بالمشرع الإنجليزي بإصدار قانون البوليس والإثبات الجنائي في سنة 1984 والذي عمل به من الأول من جانفي 1986، ونصت المادة 68 منه على أن: "يقبل الإثبات بالمستندات التي تتعلق بأي غرض من الأغراض إذا توافرت شروط معينة[2] وهي:

أ- أن يكون المستند عبارة عن سجل، أو جزءًا من سجل، يعده الشخص بموجب واجب قانوني يقع على عاتقه، لاثبات معلومات تلقاها من شخص آخر؛

ب- يمكن قبول إفتراض توافر العلم الشخصي بالأمور المتعلقة بها المعلومات؛

ث- ألا يكون الشخص الذي استقيت منه المعلومات متاحًا، أو ممكناً تعيينه، أو تتبعه، أو من المتوقع أن يكون غير قادر على تذكر الأمور المتعلقة بتلك المعلومات.[3]

وجاءت المادة 69 منه أيضًا بحكم جديد تحدد الشروط والضوابط التي بموجبها يتم قبول الأدلة الجنائية الناتجة عن الحاسوب كأدلة إثبات في المسائل الجنائية، والتي تشترط لقبول إستكمالها لإختبارات الثقة وعدم قبولها إذا كان هناك:

- عدم وجود سبب معقول يدعو للإعتقاد بأن المعطيات المستخرجة غير سليمة تفتقر إلى الدقة، بسبب الإستخدام غير المناسب أو الخاطئ للحاسوب؛

[1]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 218.

[2]- علوي سالم، **أدلة الإثبات في التحقيق الجنائي**، رسالة الماجستير، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2016-2017، ص198.

[3]- نفس المرجع، ص198.

- أن الحاسب الناتج منه المستخرج الإلكتروني كان يعمل في جميع الأحوال بصورة سليمة، إذا لم يكن كذلك فإن أي جزء لم يعمل فيه بصورة سليمة أو كان معطلًا عن العمل لم يكن ليؤثر في إستخراج المستند أو دقة محتوياته، عليه فإن النيابة العامة إذا إستندت على مستند إلكتروني في الدعوى الجنائية تعين عليها أن تقدم الدليل على أن الجهاز يعمل بطريقة صحيحة.[1]

يتبين من الشرطين السابقين أن قبول الدليل الإلكتروني في الإثبات الجنائي متوقف على شرط عدم وجود أي سبب يدعو إلى الإعتقاد أن الحاسوب لم يستخدم بشكل صحيح أو كان لا يعمل بشكل صحيح وبالتالي أثر على الأدلة المستخرجة منه، فإذا ما طعن أحد الأطراف في صحة عمل الحاسوب أو حسن إستخدامه فإن على الطرف الذي قدم الدليل إثبات حسن إستخدام الحاسوب أثناء إستخراج الدليل منه وإنه كان يعمل بشكل صحيح، وإن أي شك في توفر الشرطين المذكورين يؤدي إلى إستبعاد هذا الدليل في الإثبات الجنائي وذلك طبقًا لقاعدة الإدانة بدون أي شك معقول.[2]

وتجدر الإشارة إلى أن قانون الشرطة والإثبات الجنائي لسنة 1984 لم يكتف بتحديد الشروط الواجب توافرها في مخرجات الحاسوب لكي تكون الأدلة مقبولة أمام القضاء، بل تضمن توجيهات لكيفية تقدير قيمة أو وزن البيان المستخرج عن طريق الحاسوب[3]، فأوصت المادة 11 من الجزء 02 من الملحق 03 من القانون المذكور بمراعاة كل الظروف عند تقييم المعطيات الصادرة عن الحاسوب المقبولة في الإثبات طبقًا للمادة 69 من القانون، وبوجه خاص مراعاة (المعاصرة) أي ما إذا كانت المعلومات المتعلقة بأمر قد تم تزويد الحاسوب بها في وقت معاصر لهذا الأمر أم لا، وكذلك مسألة ما إذا كان أي شخص من المتصلين على أي نحو بإستخراج البيان من الحاسوب لديه دافع لإخفاء الوقائع أو تشويهها[4].

وأيضًا لم يتلقى قبول ما ورد في نص المادة 69 من قانون البوليس والإثبات البريطاني لعام 1984 وطالبوا بتغيير المادة، ويرجعون ذلك لكون أن المادة السالفة الذكر قد فشلت في تسمية الأسباب الرئيسية لعدم دقة أدلة الحاسوب، ويرى أن معظم الأخطاء ناتجة عن الحاسوب يمكن إكتشافها مباشرة أو أنها ناتجة عن خطأ في المعلومات التي أدخلت إلى الجهاز، بالإضافة إلى أن التطور والتقدم التكنولوجي جعل من هذه المادة 69 السالفة الذكر غير مجدية[5]، ناهيك عن أن الصعوبات التي تواجه مستلم الوثيقة التي حصل عليها من خلال الحاسوب والمراد تقديمها كدليل في المحكمة، فهذا الشخص قد لا يكون في موقع يرضي المحكمة حول عمل الحاسوب وقد يكون هناك أفضلية للخصم حيث يكون في موقع أفضل منه، كما أنه من غير

[1]- بن طالب ليندا، مرجع سابق، ص 131.
[2]- منصارة يوسف، مرجع سابق، ص 183.
[3]- بن طالب ليندا، مرجع سابق، ص 131.
[4]- عائشة بن قارة مصطفى، مرجع سابق، ص 211.
[5]- رفاه خضير جياد العارضي، مرجع سابق، ص 197

المعقول أن تطبق المادة 69 عندما تعرض الوثيقة كدليل بينما لا تطبق تلك الفقرة عندما تستخدم من قبل الخبير ولا تطبق عندما يستخدمها الشاهد وتطبق فقط عندما تقدم من قبل الأطراف[1].

إن أهم الإعتراضات على حجية الدليل الإلكتروني هي أن تلك الأدلة تعد أدلة سماعية وأن القاعدة السائدة في القانون الإنجليزي هو قاعدة إستبعاد شهادة سماع، ولكن بعد صدور قانون إساءة إستخدام الحاسب سنة 1990 تكاثفت الجهود المبذولة من قبل اللجنة القانونية البريطانية بتعديل أحكام الشهادة السماعية في الدعاوى المدنية والجنائية، مما ساعدت في تخفيف الإعتراضات على قبول الدليل الإلكتروني في الإثبات المدني والجنائي.[2]

وفي سنة 1997 إقترحت هذه اللجنة مجموعة من التعديلات التي سعت من خلالها إلى التخفيف من الأحكام المتعلقة بقبول الشهادة السماعية، وكذلك إهتمت اللجنة بعين الإعتبار بحجية الدليل الإلكتروني في الإثبات الجنائي في الحالات التي تكون المعطيات متوالدة تلقائيًا دون تدخل الإنسان في إدخالها بل متحصلة من الأجهزة التي تقوم تلقائيًا بتسجيلها في حادثة أو واقعة، وإعتبرت اللجنة القانونية أن مثل هذه المعطيات لا تعتبر شهادة سماعية وإنما تعتبر دليلًا أصليًا لأنه تم الحصول عليها دون تدخل الإنسان، وأما المعطيات التي تم إدخالها من قبل الإنسان في الحاسوب فقد كانت محل إثارة الجدل، ومن ثم سعت اللجنة القانونية إلى تخفيف من متطلبات قبول الشهادة السماعية من خلال إقتراح إلغاء المادة 69 السالفة الذكر ولكن لم تضع لها بديلًا مناسبًا.[3]

كما أقترح البعض أنه في حالة ما إذا كان الحاسوب موضوعًا للإستخدام غير المصرح به فإن أي أدلة مستندية ناتجة عنه بخصوص أصل ومدة هذا الإستخدام لن يكون مقبولًا، لأن سوء إستخدام للحاسوب في حد ذاته أدى إلى عدم عمل الجهاز كما ينبغي.[4]

وخلاصة ما سبق، يتضح أن هناك طلبًا ملحًا بإلغاء المادة 69 من قانون البوليس والإثبات الجنائي البريطاني، كما أكدت على ذلك اللجنة القانونية وإقترحت بالإلغاء في سنة 1997، ولكنها لم تضع له البديل المناسب أسوة بما قررته اللجنة القانونية الإسكتلندية بخصوص الدليل الإلكتروني التي توصلت إلى عدم ضرورة وحاجة إلى المادة 69 السالفة الذكر في القضايا في المسائل الجزائية في إسكتلندا.[5]

وبناءً عليه فإن بمطالبة إلغاء المادة 69 وعدم تقديم بديل لها يؤدي إلى فراغ تشريعي في هذا الخصوص، وإن كنا نسايرهم في هذا الطرح لأنه بمجرد الطعن في صحة عمل الحاسوب من قبل الطرف الآخر، فإنه يقع على عاتق الطرف الذي قدم الدليل إثبات أن الحاسوب كان

[1]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 220.
[2]- رفاه خضير جياد العارضي، مرجع سابق، ص 197.
[3]- محمد صالح جاد المولى خليفة، مرجع سابق، ص- ص 220-221.
[4]- رفاه خضير جياد العارضي، مرجع سابق، ص- ص 197-198.
[5]- أحمد يوسف الطحطاوي، مرجع سابق، ص 210.

يعمل بصورة صحيحة أثناء إستخراج الدليل منه أو أن عمله غير الصحيح لم يؤثر على دقة الأدلة المتحصل عليه، وكان الأصح أن يقع عبء الإثبات في عدم صحة عمل الحاسوب على الطرف الذي قدم الطعن وليس من قدم الدليل، حيث يكون الأصل هو صحة عمل الحاسوب وقيامه بعمله بشكل صحيح والإستثناء أن عمله غير صحيح.[1]

وبدورنا نثمن الجهود التي أرساها المشرع الإنجليزي، ولكن يجب أن نبين كما ذكرنا سابقًا في تعريف الدليل الإلكتروني بأن ليس من الأجدر حصر الدليل على ذلك الدليل الذي يتم إستخراجه فقط من الحاسوب وملحقاته دون غيره من الأجهزة الرقمية الأخرى المتطورة، بل يقتضي الأمر عدم تضييق نطاق التجريم ليتسع لمصادر إستخلاص الدليل الإلكتروني المستحدثة وما قد تتيحه التكنولوجيا من وسائل إثبات مستقبلًا.

2- خضوع المخرجات الإلكترونية كإستثناء لقاعدة الدليل الأفضل في الجرائم الماسة بالمستند الإلكتروني:

تقررت هذه القاعدة في القانون الإثبات الفيدرالي الأمريكي بموجب المادة 1002 بنصها: "بإستثناء ما هو مقرر في هذا القانون أو بقانون خاص يصدر عن الكونجرس فإنه عند إثبات مضمون الكتابة والتسجيل والصورة، فإنه يلزم توافر أصل الكتابة والتسجيل والصورة"[2]، ومن ثم فإن إثبات مضمون الكتابة أو التسجيل أو الصورة يبقى مرهونًا بتقديم الأصل لإثبات محتواها، ما لم يرد نص يجيز خلاف ذلك.

وعليه فإن الصورة أو النسخة المطابقة للأصل غير مقبولة لإثبات محتوى الأصل، وهذا يعني أن مخرجات طابعة لملف إلكتروني مخزن على الجهاز الإلكتروني لا يعد أصليًا، كون أن

[1]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 221.

- نأخذ قضية الآنسة ماكوين كنموذج لهذه التطبيقات وتتلخص وقائع هذه القضية في أنه في ساعة متأخرة في 21 جويلية 1992 لاحظت الشرطة أن الآنسة ماكوين تقوم بقيادة السيارة بصورة شاذة في أحد شوارع ليفربول، وعلى إثر ذلك تم إعتقالها من قبل الشرطة للشك في أنها تقود السيارة وهي مخمورة وتم إقتيادها إلى مركز الشرطة، حيث طلب منها عينتان من التنفس للتحليل بإستخدام جهاز قياس درجة السكر وهو عبارة عن حاسوب يقوم بعملية قياس نسبة الكحول عن طريق جهاز التنفس، وقد أدانت المحكمة الآنسة ماكوين بتهمة قيادة السيارة وهي في حالة سكر بالإعتماد على الدليل المقدم وهو نسبة الكحول التي سجلها الحاسوب وقد إعترضت على التقرير المقدم من قبل الشرطة حيث إدعت أن الجهاز لم يكن يعمل بصورة دقيقة أثناء أخذ العينة وأثناء صدور النتيجة، لكن المحكمة إستدعت مدير المختبر التي زودت مركز الشرطة بذلك النوع من الحاسوب الخاص بقياس نسبة الكحول، حيث قدم شهادته وأوضح أن دقة عمل ساعة الحاسوب وبالتالي لا تؤثر على صحة المعطيات التي يقدمها الحاسوب بخصوص نسبة الكحول، وعلى هذا الأساس قررت المحكمة أن متطلبات الفقرة الأولى من المادة 69 من قانون لشرطة والإثبات الجزائي البريطاني قد تم الإيفاء بها وبالتالي قبلت هذا الدليل المتحصل من الحاسوب وأدانت المتهمة على أساسها، وللمزيد من التفصيل، منصارة يوسف، مرجع سابق، ص- ص 208-209.

[2] -Rule 1002 of federal rules of Evidence : «To prove the content of a writing, recording, or photograph, the Original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of congress ».

الملف الأصلي عبارة عن أرقام غير مفهومة، أما مخرجات الطابعة فهي نتيجة معالجة الملف من خلال سلسلة معقدة من العمليات الإلكترونية والآلية.[1]

ومع ظهور المستندات الإلكترونية إستدعى الأمر إلى تغيير قاعدة الدليل الأفضل لكي تتلائم مع عصر المعلومات، وقد إستجابت بعض التشريعات كالقانون الأمريكي والإنجليزي لهذه المستجدات، وقام بحسم هذه المسألة لصالح الدليل الإلكتروني وذلك من خلال تعديل قانون الإثبات الفيدرالي الأمريكي.[2]

ففي البند 01 من المادة 1001 من قانون الإثبات الأمريكي سمح الإعتراف بالأدلة الإلكترونية كي تحظى بذات الإهتمام الذي تحظى به الأدلة الأخرى[3]، فتعرف الكتابة والتسجيلات بأنها حروف أو أرقام أو كلمات أو ما يعادلها، مكتوبة على اليد أو منسوخة على الآلة الكاتبة أو مطبوعة أو تم تصويرها أو إتخذت شكل نبضات مغناطيسية بتسجيل ميكانيكي أو إلكتروني أو أي شكل آخر من تجميع المعلومات[4].

ولقد ذهبت نصوص قانون الإثبات الفيدرالي الأمريكي أبعد من ذلك، فقد نص البند 03 من المادة 1001 على أن: "إذا كانت المعطيات مخزنة في الحاسوب أو جهاز مماثل، فإن مخرجات الطابعة أو أية مخرجات آخرى، يمكن قراءتها بالنظر إلى ما تم إظهارها وتبرز إنعكاسًا دقيقًا للمعطيات، تعد معطيات أصلية"[5]، فقد أوردت هذه القاعدة إستثناء بقبول الدليل الإلكتروني بإعتباره مستندًا أصليًا، ما دام أن المعطيات صادرة من الحاسوب أو جهاز مماثل وسواء أكانت هذه المعطيات مطبوعة أم مسجلة على دعامات أخرى ومقروءة للعين المجردة وتعبر عن المعطيات الأصلية بشكل دقيق[6].

وقد توسع القانون الأمريكي أكثر حيث قام بإعتماد مقياس القانون العام، وذلك في إطار الإعتراف بالنسخة طبق الأصل[7] الفورية الصادرة عن الجهاز الإلكتروني[8]، وبالتالي قام

---

[1]- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 236.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص-ص 205-206.

[3]- بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، مرجع سابق، ص 282.

[4]- شيماء عبد الغني محمد عطاالله، **الحماية الجنائية للتعاملات الإلكترونية**، د.ر.ط، 2007، دار الجامعة الجديدة، الإسكندرية- مصر، ص 388.

[5]-Rule 1001/3 of federal rule evidence, provides that : « if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original».

[6]- بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، مرجع سابق، ص 282.

[7]-Rule 1001e of Federal rules of Evidence, provides that: «A duplicate is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques. Which accurately reproduces the original».

حيث تعرف المادة e 1001 من القانون الإثبات الأمريكي النسخة طبق الأصل بأنها : "النسخة الطبق الأصل المنتجة لذات الأثر للنسخة الأصلية.... عن طريق إعادة تسجيلها ميكانيكيًا أو إلكترونيًا...أو عن طريق وسيلة تقنية أخرى مساوية التي تعيد إنتاجها بدقة كالأصل"، وللمزيد من التفصيل، ينظر: بن طالب ليندا، مرجع سابق، ص 134.

[8]- نفس المرجع، ص 134.

المشرع بإستخدام مدلول موسع للكتابة والتسجيلات، ليشمل كل من الحروف والكلمات والأرقام، أو ما يعادلها مكتوبة على اليد أو منسوخة على الآلة الكاتبة أو مطبوعة، أو تم تصويرها أو إتخذت شكل نبضات مغناطيسية بتسجيل ميكانيكي أو إلكتروني أو أي شكل آخر، من تجميع المعلومات[1]، بما يسمح بقبول المخرجات الإلكترونية في الإثبات، والغالب الأعم في القضاء الأمريكي أنه يعول على قبول دليل السجلات المحتفظ بها على الجهاز[2]، لذلك يتم إعتبار الكتابة الموجودة داخل الجهاز في صورة كهرومغناطيسية من قبيل النسخة الأصلية، وبالتالي لا تصطدم مع قاعدة الدليل الأفضل.

هذا وقد أقر القانون الأمريكي في المادة 1003 من قانون الإثبات الأمريكي: "أن النسخة المطابقة للأصل تقبل كالأصل، إلا إذا:

- أثير حولها تساؤل جدي يتعلق بجديتها وأصالتها؛
- إذا كانت الظروف لا تسمح بقبول النسخة المطابقة للأصل، لكي تحل محل الأصل".[3]

وبناءً عليه فإنه وفقًا لهذه القاعدة من القواعد الإتحادية تعد المعلومات المخزنة في الجهاز الإلكتروني أو الموجودة عبر فضاء الإنترنت التي يتم رؤيتها عن طريق البصر من خلال شاشة الجهاز أو عن طريق مخرجات الإلكترونية، صالحة لأن تكون دليلًا أصليًا تنطبق عليه قاعدة الدليل الأفضل.[4]

هذا بالنسبة للتشريعات على المستوى الفيدرالي، أما على مستوى الولايات فقد صدرت عدة قوانين تحوي نصوصًا تعالج على نحو خاص مشكلات قبول الدليل الإلكتروني أمام المحاكم، فإن تطور الذي حصل في مجال التشريع لا يقتصر فقط على القواعد الفيدرالية للإثبات الأمريكي بل يشمل ذلك القوانين الخاصة بالولايات المتحدة كذلك القائمة في ولاية كاليفورنيا وولاية أيوا، لكي تشمل الدليل الإلكتروني بشكل موسع فسمحت بالإعتراف بالمواد المكتوبة والمسجلة والإلكترونية لكي تحظى بذات الإهتمام الذي تحظى به الأدلة الأخرى في المحاكم[5]، من ذلك ما نص عليه قانون الحاسوب لسنة 1984 الصادر في ولاية أيوا حيث تنص المادة 16/716 منه على أن: "في أحوال الإتهام بمقتضى هذا الفصل تكون مخرجات الحاسوب مقبولة، كدليل على الكيان المنطقي أو البرنامج أو المعطيات التي يحتويها حاسوب أو المعطيات التي تؤخذ منه، بغض النظر عن تطبيق قاعدة إثبات تقضى بخلاف ذلك"، وفي ولاية كاليفورنيا تنص المادة 5/1500 من قانون الإثبات الصادر في سنة 1983 على أن: "المعلومات المسجلة

[1]- بن فردية محمد، **الاثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، مرجع سابق، ص 236.
[2]- فهد دخين العدواني، مرجع سابق، ص- ص 268- 269.
[3]- بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، مرجع سابق، ص 282.
[4]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 228.
[5]- بن طالب ليندا، مرجع سابق، ص 134.

بواسطة الحاسوب أو برامج الحاسوب أو نسخ أيهما لا يجب وصفها أو معاملتها على أنها غير مقبولة بمقتضى قاعدة أفضل دليل.[1]

أما بالنسبة للقانون الإنجليزي بمقتضى المادة 27 من قانون العدالة الجنائية لسنة 1988 قد تم قبول صور المستندات أو جزء منها.[2]

الفرع الثالث: حجية المستند الإلكتروني في الإثبات الجنائي في النظام المختلط

يقصد بالنظام المختلط النظام الذي يجمع بين النظامين السابقين النظام اللاتيني والنظام الأنجلوسكسوني، إذ تتبع قوانينه منهجًا وسطًا بين نظام الإثبات الحر ونظام الإثبات المقيد، وفي هذا الصدد سنتطرق إلى بيان حجية المستند الإلكتروني فيه.

أولًا: الأسس التي يقوم عليها النظام المختلط

يمثل النظام المختلط الإتجاه التوفيقي الذي يجمع بين المزايا الإيجابية في النظام الإثبات الحر والأخرى في النظام الإثبات المقيد، إذ يعتمد على تحديد أدلة معينة التي من الضروري أن يأخذ بها القاضي في إثبات بعض الوقائع دون بعضها الآخر، وأيضًا يشترط أن تتوفر في بعض الحالات شروط معينة في الدليل، كما يعطي للقاضي الجزائي الحرية في تقدير هذه الأدلة، وتتفاوت الأنظمة القانونية في تطبيق هذا النظام بين دول تقلل في الشروط وآخرى توسع منها[3]، وأخذ هذا النظام صورتين:

الصورة الأولى: تتمثل في التوفيق بين القناعة الشخصية للقاضي والتأكيد المطروح من طرف المشرع سواء كانت في حالة الإدانة أو البراءة، أما إذا لم يتطابق إقتناع القاضي وقناعة المشرع فإن القاضي لا يستطيع أن يحكم لا بالإدانة ولا بالبراءة، ولذلك تم التوصل إلى إقتراح حلًا وسطًا ومؤقتًا بأن يصدر القاضي الجزائي قرارًا بأن التهمة غير ثابتة ووقف سير الدعوى مؤقتًا مع تمتع المتهم بحريته الشخصية.[4]

الصورة الثانية: أن يتم التوفيق بين النظامين السابقين في حالة إدانة المتهم فقط، بمعنى التوفيق بين الإقتناع القانوني والإقتناع الشخصي للقاضي، فإذا لم يقتنع القاضي بالأدلة القانونية المطروحة أمامه حكم بالبراءة.[5]

[1]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 229.
[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 208.
[3]- التوجي محمد، **الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال**، شهادة الدكتوراه، تخصص: القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية أدرار، 2019/2018، ص 204.
[4]- بلولهي مراد، مرجع سابق، ص 15.
[5]- سحر سعد عبد السميع محمد، مرجع سابق، ص 337.

ثانيًا: موقف الفقه والتشريعات الآخذة بالنظام المختلط

القانون الإجرائي الياباني حدد وسائل الإثبات ومن ناحية أخرى أخذ بقاعدة الإقتناع الذاتي للقاضي، فأدلة الإثبات إذًا ليست حرة فالسجلات الإلكترونية لا تقبل كدليل في المحكمة إلا إذا تم تحويلها إلى صور مرئية ومقروءة عن طريق مخرجات الطباعة، ففي هذه الحالة يتم قبول الأدلة الناتجة عن الأجهزة الإلكترونية سواء كانت هي الأصل أم كانت نسخة من هذا الأصل.[1]

وقد إستبعد قانون الإجراءات الجنائية الياباني الشهادة السماعية كقاعدة عامة طبقًا للمادة 320 من ق.إ.ج إلا أنه أورد على هذه القاعدة بعض الإستثناءات وفقًا للمواد 321-328 من ق.إ.ج ويدخل في هذه الإستثناءات الأدلة المتولدة عن الأجهزة الإلكترونية، فطبقًا لنص المادة 323 من ق.إ.ج التي قرر قبول فيها ثلاثة أنواع من السجلات كأدلة في المواد الجنائية وهي:

1. نسخة من السجل العائلي للفرد أو نسخة من صك موثق، أو أي مستندات رسمية تشهد على الوقائع التي يكون من واجب الموظف العام بما في ذلك موظفي الحكومات الأجنبية التصديق عليها؛
2. دفتر الحساب وسجل السفر، المستندات الأخرى التي تعد لتنظيم السير المعتاد للأعمال التجارية؛
3. أية مستندات أخرى غير مذكورة في البندين السابقين، إذا تم إعدادها تحت ظروف تضفي مصداقية خاصة على تأكيد الحقيقة المتضمنة في مسألة معينة؛
4. وبالإضافة إلى هذا الإستثناء السابق المنصوص عليه في المادة 323 من ق.إ.ج، يمكن طباعة المخرجات الإلكترونية وقبولها أثناء فترة المحاكمة من خلال شهادات الخبراء.[2]

أما الفقه التشيلي فيرى أن الدليل الإلكتروني المتولد من جهاز الحاسوب أو أي وسيلة إلكترونية أخرى، يمكن أن يكون مقبولًا في المحكمة دليلًا كتابيًا أو مستنديًا كالنظم الحديثة الأخرى لجمع وتسجيل المعلومات، مثل التصوير الفوتوغرافي والتصوير بالأقمار الإصطناعية والتصوير بالأشعة والهاتف اللاسلكي وتسجيلات الصوت، فهذه الوسائل العلمية جميعًا يمكن إعتبارها مستندات بالمعنى الواسع لهذا المصطلح، وذلك لأن التقدم الفني قد تجاوز المفهوم التقليدي للمستند الذي يعرفه على أنه مجرد ورقة مكتوبة، ويرى الفقه التشيلي أن إعتبار الوسائل العلمية الحديثة من قبل المستندات يجعلها تندرج ضمن مفهوم المادة 457 من قانون الاجراءات الجنائية التشيلي التي تعد المستندات العامة والخاصة أدلة إثبات قانونية.[3]

فقد عمد المشرع التشيلي بحصر طرق الإثبات بموجب المادة 457 من قانون الإجراءات الجنائية والتي تشمل كل من: شهادة الشهود، تقرير الخبراء، المعاينة الشخصية للقاضي،

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 337.
[2]- أحمد يوسف الطحطاوي، مرجع سابق، ص 218.
[3]- رفاه خضير جياد العارضي، مرجع سابق، ص 200.

المستندات العامة والخاصة، الإعتراف، والقرائن، ونص أيضًا في المادة 456 مكرر من نفس القانون على عدم جواز إدانة أي شخص بجريمة إذا لم تصل المحكمة المختصة عن طريق الآليات القانونية للإثبات إلى الإقتناع بأن السلوك الجرمي قد أرتكب، وأن الشخص المدان قد ساهم في إرتكاب هذا السلوك وأن مساهمته معاقب عليها قانونًا.[1]

وعلى ذلك لا يمكن للمحكمة أن تقتنع بالجريمة وبأن الفعل المعاقب عليه قد تم إرتكابه بالفعل وأن شخصًا معينًا قد إقترف أو ساهم في إقترافه إلا من خلال وسائل الإثبات القانونية السالفة الذكر التي ينبغي أن تستمد منها إقتناعها بالإدانة 456 مكرر من ق.إ.ج، ونظرًا للتطورات العلمية الحديثة فقد صدر مشروع قانون الإجراءات الجنائية التشيلي وذلك بغرض إدخال وسائل إثبات جديدة وثيقة الصلة وملائمة كي تستمد منها المحكمة إقتناعها، فالمادة 113 من المشروع المقترح مثلًا تنص على أن: "الأفلام السينمائية والنظم الأخرى الخاصة بإنتاج الصورة والصوت والإختزال وبصفة عامة أي وسائل أخرى قد تكون ملائمة ووثيقة الصلة، وتفضي إلى إستخلاص المصداقية، يمكن أن تكون مقبولة كدليل إثبات".[2]

ومما سبق ذكره، فقد تمسك القانون الإجرائي التشيلي بنظام التحديد الحصري لوسائل الإثبات في المواد الجزائية على نحو تكون فيه الوسائل التي تم تحديدها وتنظيمها قانونيًا وسائل مشروعة يمكن إستخلاص الحقيقة من خلالها، وفي ضوء هذا التحديد يمكن أن يكون الدليل الناشئ عن الجهاز الإلكتروني بما فيه المستند الإلكتروني مقبولًا في الإثبات الجنائي إستنادًا إلى تقرير الخبير المقدم بشأن المعطيات المعنية المعالجة آليًا، فاللقاضي طبقًا للمادة 221 من قانون الإجراءات أن يطلب تقريرًا من الخبير عند حدوث أي من الحالات المحددة قانونًا في مجالات العلم أو التجارة أو الفن، وأيضًا في حال وجود حالة ضرورية أو لازمة لتقييم واقعة أو ظرف مؤثر في الدعوى، وكذا في حالة المعطيات والعناصر الأخرى التي يقدمها أو يوفرها الجهاز الإلكتروني، ويكون رأي الخبير التقني المتخصص مهمًا لمساعدة القاضي في كشف الحقيقة.[3]

وتجدر الإشارة إلى أن المشرع الجزائري قد أخذ بالنظام المختلط أيضًا إلى جانب النظام الحر في قبول الدليل في بعض الجرائم، وذلك بالأخذ بحرية الإثبات كقاعدة عامة بموجب المادة 349 من ق.إ.ج والتي أشرنا إليها سابقًا، وإستثناء بنص القانون أخذ بمبدأ الأدلة القانونية وذلك من خلال عبارة: "ما عدا الأحوال التي ينص فيها القانون على غير ذلك".[4]

---

[1]- بلحسيني حمزة، مرجع سابق، ص 187.

[2]- أحمد يوسف الطحطاوي، مرجع سابق، ص 219 .

[3]- بلحسيني حمزة، مرجع سابق، ص 187.

[4]- تجدر الإشارة إلى بعض الجرائم التي قيد المشرع الجزائري إثباتها بنصوص خاصة كجريمة المعاقب عليها في نص المادة 339 من ق.ع.ج، والتي لا يمكن إثباتها إلا بالطرق التي أوردها المشرع الجزائري على سبيل الحصر في نص المادة 341 من نفس القانون، والتي نصت على أن: "الدليل الذي يقبل عن إرتكاب الجريمة المعاقب عليها بالمادة 339 يقوم إما على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة تلبس، وإما بإقرار وارد في رسائل أو مستندات صادرة من المتهم، وإما بإقرار قضائي".

خلاصة:

لا يمكن النظر في حجية المستند الإلكتروني في المجال الجزائي دون التأكد أولًا من صحة هذا المستند وإعتراف القانون المدني به كوسيلة الإثبات، فالقانون المدني هو من وضع الأساس القانوني لظهور المستندات الإلكترونية ومنحها القوة الثبوتية، بشرط أن تتضمن الكتابة والتوقيع الإلكترونيين، وأن تستوفي الشروط الفنية والتقنية المطلوبة، وبناءً على هذا الإعتراف المدني يمكن الإعتماد على المستند الإلكتروني كدليل في القضايا الجزائية.

وقد منح المشرع الجزائري لهذه المستندات ذات القوة الثبوتية التي يتمتع بها المستند الورقي التقليدي، متى توافرت فيها عنصرا الكتابة والتوقيع الإلكترونيين اللذان يعدان معادلين في حجيتهما للكتابة والتوقيع التقليديين، طالما إستوفت المستندات الإلكترونية الشروط الفنية والتقنية المنصوص عليها في مختلف التشريعات.

وفي هذا الإطار فإن القاضي الجزائي ملزم بعدة ضوابط، أهمها التحقق من مشروعية الحصول على الدليل الإلكتروني، فلا يجوز له أن يستند إلى الدليل في إصدار حكم بالإدانة أو البراءة ما لم يكن هذا الدليل صحيحًا ومشروعًا، كما يجب عليه مناقشة هذا الدليل بشكل علني داخل المحاكمة، بما يضمن قوق الدفاع وتحقيق العدالة.

وقد إختلف الفقه الجنائي والتشريعات المقارنة بشأن حجية المستند الإلكتروني في المواد الجزائية ومدى قوته في الإثبات، فقد تباينت هذه التشريعات في مدى قبول المخرجات الإلكترونية كأدلة في الإثبات الجزائي، فبعضها تبنى نظام الإثبات الحر والذي يخول القاضي الجزائي سلطة تقديرية واسعة في تكوين إقتناعه وتقدير قيمة الدليل، دون التقيد بنوع معين من الأدلة ما لم ينص القانون على خلاف ذلك، بينما إعتمدت تشريعات أخرى نظام الإثبات المقيد الذي يحدد الأدلة المقبولة قانونًا ويلزم القاضي بعدم الخروج عنها، إلا أن هذا النظام أورد إستثناءات لقبول الإثبات عن طريق خضوع المخرجات الإلكترونية والتي هي في أغلبها مستندات إلكترونية إلى قاعدة إستبعاد شهادة سماع وقاعدة الدليل الأفضل، كما ظهرت بعض الأنظمة التي جمعت بين هذين الإتجاهين فتبنت ما يعرف بالنظام المختلط الذي يمنح القاضي حرية نسبية في تقدير الأدلة ضمن حدود معينة، وعليه تختلف سلطة القاضي في تقدير الأدلة حسب طبيعة نظام الإثبات الذي تعتمده الدولة.

الفصل الثاني:
الجرائم الماسة بالمستند الإلكتروني

تمهيد:

أدى التوسع في إستخدام التقنيات الحديثة إلى تحول جذري في طريقة إبرام المعاملات، حيث أصبحت تبرم في بيئة رقمية تعتمد على تبادل المعطيات والمعلومات بصيغة رقمية تتجسد في نبضات إلكترونية غير مرئية، وقد أسفر عن هذا التحول بروز نوع جديد من الجرائم يعرف بالجرائم الماسة بالمستند الإلكتروني، والتي تتم ضمن بيئة رقمية لا تخلف في الكثير من الأحيان أثرًا ماديًا ملموسًا، ونتيجة لذلك تتسم هذه الجرائم بصعوبة كشفها وإثباتها مما يثير العديد من التحديات القانونية.

وقد أدى هذا التطور إلى قصور وعدم كفاية النصوص التقليدية في تجريم هذا النوع من الأفعال، إذ أن تلك النصوص وضعت أساسًا لحماية الكيانات المادية من صور الإعتداء المعروفة والتقليدية، أما الجرائم الماسة بالمستند الإلكتروني فهي جرائم مستحدثة تتسم بالتطور المستمر وتفرز أشكالًا متعددة من الجرائم يصعب حصرها ضمن الأطر التقليدية، ولذلك بات من الضروري تدخل المشرع الجزائري لوضع قواعد ومبادئ للحماية الجزائية لهذا النوع من الجرائم، وذلك إلتزامًا بمبدأ الشرعية الذي يقضي بأن: "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون" بما يضمن أن تكون كل جريمة محددة بنص قانوني يبين أركانها والعقوبة المقررة لها.

إرتأينا تقسيم دراستنا إلى ثلاث مباحث، نتطرق إلى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني في (المبحث الأول)، أما (المبحث الثاني) فقد خصصناه إلى الجرائم الماسة بمحتوى المستند الإلكتروني، وإلى الجرائم الماسة بالتوقيع والتصديق الإلكترونيين في (المبحث الثالث).

المبحث الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني

سعى المشرع الجزائري من خلال تعديل قانون العقوبات[1] بموجب القانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004[2] إلى إضافة قسم سابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث منه، وخصصه لجرائم المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في إطار مواكبة الحماية الفعالة لأنظمة المعالجة الآلية للمعطيات، ورغبة منه في مواكبة متطلبات العصرنة والسير نحو تطوير المنظومة التشريعية بما يتماشى مع التحولات الرقمية المتسارعة، تأسيسًا بذلك على ما إنتهجته العديد من التشريعات المقارنة.

المطلب الأول: صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني

إرتأينا التطرق في هذا المطلب إلى جريمتي الدخول والبقاء غير المصرح بهما داخل نظام المعالجة الآلية للمعطيات الذي يحتوي على مستندات إلكترونية ضمن (الفرع الأول)، بينما سنتطرق لجريمة المساس بسلامة معطيات المستند الإلكتروني في (الفرع الثاني)، ولجريمة إتلاف المستند الإلكتروني في (الفرع الثالث)، أما (الفرع الرابع) سنتطرق لجريمة إستخدام المعطيات كوسيلة للإعتداء على المستند الإلكتروني، وجريمة التعامل بالمعطيات الواردة في المستند الإلكتروني في (الفرع الخامس).

الفرع الأول: جريمتي الدخول والبقاء غير المصرح بهما داخل نظام المعالجة الآلية للمعطيات الذي يحتوي على مستندات إلكترونية

نظرًا لخطورة وجسامة الجريمة محل الدراسة إتجه المشرع الجزائري على غرار العديد من التشريعات المقارنة إلى تجريم فعل الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات، لما يتيحه هذا الفعل من إمكانية الوصول غير المصرح به إلى المعطيات الإلكترونية الخاصة بالمستند الإلكتروني، كما أدرج المشرع الجزائري أيضًا فعل البقاء غير المصرح به داخل النظام ضمن الأفعال المعاقب عليها.

وهي الجريمة المنصوص عليها في المادة 02 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بعنوان: "الولوج غير القانوني"[3]، والفقرة الأولى

---

[1]- الأمر رقم: 66-156 المؤرخ في 08 جوان 1966، المتضمن القانون العقوبات الجزائري، ج.ر.ج.ج.ش العدد 49، الصادرة في في تاريخ 11 جوان 1966، المعدل والمتمم.

[2]- القانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم: 66-156 المتضمن قانون العقوبات، ج.ر.ج.ج.ش العدد 71، الصادرة في 10 نوفمبر 2004.

[3]-Art 02 du convention sur la cybercriminalité dispose que : « Accès illégal: Chaque Partie adopte les mesures législatives et autres qui se révélent nécessaires pour ériger en infraction pénale, conformément à son droit interne l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commiseen violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une=

من المادة 06 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[1] بعنوان:"جريمة الدخول غير المشروع"[2]، والفقرة الأولى من المادة 394 مكرر من قانون العقوبات الجزائري[3]، والفقرة الأولى من المادة 323-1 من قانون العقوبات الفرنسي[4]، والفقرة الأولى من المادة 14 من القانون المصري رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات[5].

أولًا: الركن المادي لجريمتي الدخول والبقاء غير المصرح بهما داخل نظام المعالجة الآلية للمعطيات الذي يحتوي على مستندات إلكترونية

تنص الفقرة الأولى من المادة 394 مكرر من ق.ع.ج على أنه يعاقب كل من يدخل بطريق الغش أو يحاول ذلك في كل أو جزء من نظام المعالجة الآلية للمعطيات، ويسرت عليه الوصول إلى المعطيات الخاصة بالمستندات الإلكترونية، كما وجرم فعل البقاء وعدم الخروج من ذلك النظام على الرغم من علم الجاني بعدم مشروعية فعله، فيستمر في البقاء داخل النظام بعد دخوله إليه وعدم قطع الإتصال به، أو إذا كان الغرض منه العبث أو الإطلاع على المعطيات الخاصة بالمستندات الإلكترونية.

=autre intention délictueuse, ou soit en relation avec un systéme informatique connecté á un autre systéme informatique».

ترجمتها:
تنص المادة 02 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 على أن: " الولوج غير القانوني: يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل إعتبارها جريمة جنائية، وفقًا لقانونه الداخلي، للولوج العمدي لكل أو لجزء من جهاز الحاسب بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال إنتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلًا عن بعد بحاسب آخر".

[1]- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تم اعتمادها من قبل مجلس وزراء العرب والداخلية بتاريخ 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم: 14-252 المؤرخ في 08 سبتمبر 2014، ج.ر.د.ش، العدد 54، سنة 2014.

[2]- تنص الفقرة الأولى من المادة 06 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "جريمة الدخول غير المشروع : الدخول أو البقاء وكل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار به".

[3]- تنص الفقرة الأولى من المادة 394 مكرر من ق.ع.ج على أن: "يعاقب بالحبس من ستة (06) أشهر إلى سنتين (02) وبغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

[4]-Art 323-1 du C.P.F (Modifié par Loi n°2023-22 du 24 janvier 2023 - art. 6) dispose que: « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100.000 € d'amende».

ترجمتها:
تنص الفقرة الأولى من المادة 323-1 من ق.ع.ف على أن: "يعاقب على الدخول أو البقاء عن طريق الغش داخل كل أو جزء من نظام المعالجة الآلية للمعطيات، بالحبس لمدة ثلاث (03) سنوات وغرامة مقدارها 100.000 يورو".

[5]- تنص الفقرة الأولى من المادة 14 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات على أن: "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف 50.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه".

ويتحقق هذا الدخول غير المصرح به متى دخل الجاني إلى نظام المعالجة الآلية للمعطيات كله أو إلى جزء منه دون وجه حق أي دون موافقة صاحب النظام أو من له حق السيطرة عليه، أما فعل البقاء غير المصرح به داخل النظام فقد جرمه المشرع لكونه يمثل إستمرارًا في التواجد داخل النظام دون وجه حق وتنصرف إرادته لذلك.[1]

يتمثل محل الجريمة في نظام المعالجة الآلية للمعطيات، وهو المصطلح المعتمد في قانون العقوبات الجزائري، بينما إستخدم المشرع الجزائري مصطلح "المنظومة المعلوماتية" في القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر، وعرفها بموجب الفقرة (ب) من المادة 02 منه بأنها: "المنظومة المعلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج معين".

على غرار المشرع المصري الذي وسع من محل الجريمة وجعلها تشمل كل من النظم المعلوماتية والمواقع الإلكترونية والحسابات الخاصة، وإستخدم مصطلح "النظام المعلوماتي" للدلالة على "نظام المعالجة الآلية للمعطيات"، وعرفه بمقتضى المادة الأولى من القانون المصري رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر بأنه: " النظام المعلوماتي: مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية"، كما عرف الموقع في نفس المادة بأنه: "مجال أو مكان إفتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة"، بينما عرف الحساب الخاص في نفس المادة بأنه: "مجموعة من المعلومات الخاصة بشخص طبيعي أو إعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة، أو إستخدامها من خلال موقع أو نظام معلوماتي".

1- جريمة الدخول غير المصرح به داخل نظام المعالجة الآلية للمعطيات الذي يحتوي على مستندات إلكترونية:

يعد الولوج أو الدخول غير المصرح به -عن طريق الغش- داخل نظام المعالجة الآلية للمعطيات الذي يحتوي على المستندات الإلكترونية المرحلة الأولى والسابقة على إرتكاب الجرائم الماسة بالمستند الإلكتروني الأخرى وضرورية لها، وهو سلوك يشكل تهديدًا للأمن المعلوماتي من حيث المساس بالسرية وسلامة وتوافر الأنظمة والمعطيات المعلوماتية، نتيجة لهذا الدخول قد يترتب عليه بعد ذلك الوصول إلى المعطيات الواردة بالمستند الإلكتروني

[1]- محمود سعد عبد المجيد، **الجرائم السيبرانية وإنعكاسات ثورة تكنولوجيا المعلومات والإتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية دراسة تحليلة وصفية مقارنة**، د.ر.ط، 2023، دار المطبوعات الجامعية، الإسكندرية-مصر، ص 414.

المخزنة في النظام، والإضرار بها أو إستخدامها لغير الغرض الذي توجد من أجل تحقيقه في نظام المعالجة الآلية للمعطيات.[1]

ولا يقصد بالدخول إلى المكان الذي يوجد فيه الجهاز الإلكتروني ونظامه وإنما يقصد بالدخول إستخدام الوسائل الفنية والتقنية إلى نظام المعالجة الآلية للمعطيات [2]، لذلك فقد أنتقدت البعض من التشريعات المقارنة إستخدام مصطلح "الدخول" وفضلت إستخدام مصطلح "الإتصال بالنظام المعلوماتي"، وذلك لأن مصطلح الدخول يعبر عن المدلول المادي على عكس مصطلح الإتصال الذي يعبر عن المدلول المعنوي[3].

وإنما يجب أن ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات[4]، ولا يتغير من طريقة الدخول شيئًا سواء تم ذلك بطريقة مباشرة إلى المعلومات، أو عن طريق الإعتراض غير المشروع لعمليات الإتصال بهدف الدخول إلى النظام[5].

ونظرًا لكون التشريعات المقارنة لم تبين بشكل واضح المقصود بمصطلح الدخول[6] في المجال المعلوماتي، فقد عرفه البعض من الفقه بأنه عملية الولوج غير الشرعي إلى نظام

---

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 685.

[2]- نفس المرجع، ص 685.

[3]- باهة فاطمة، مرجع السابق، ص 365.

[4]- حسين محمد الغول، **جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها دراسة مقارنة**، الطبعة الأولى،2017، مكتبة بدران الحقوقية، لبنان، ص 454.

[5]- حمزة بن عقون، **السلوك الاجرامي للمجرم المعلوماتي**، د.ر.ط، جوان 2019، دار تديكلت، الجزائر، ص 119.

[6]- يلاحظ أن هناك بعض التفسيرات لكلمة الدخول قد ساوت بين الدخول المادي في مكان مادي والدخول الإفتراضي إلى شبكة الإنترنت، ويلاحظ أن مقاييس العالم المادي وتلك التي تتعلق بالعالم الإفتراضي تختلف كلا منهما عن الأخرى، ويلاحظ أن أغلب تشريعات الإنترنت والحاسوب لم تتعرض لمفهوم الدخول، ولذلك توجد بعض الأحكام القضائية في الولايات المتحدة الأمريكية التي قامت بتفسير معنى الدخول إلى الحاسوب، وقد برز ذلك عام 1996 أمام محكمة كانساس العليا في قضية الولاية ضد Allen، التي تخلص وقائعها في قيام Allen بإستخدام الحاسب الشخصي له بشكل مستمر بنظام الإتصال الهاتفي بالشبكة dial up، وذلك للإتصال بحاسب شركة الهاتف الجنوبية الغربية التي تتحكم في تحويلات الإتصالات البعيدة المدى وتلاعب بها، بحيث تسمح للمستخدم بالقيام بالمكالمات بعيدة المدى مجانًا، وعندما إتصل Allen بالحواسيب للشركة المشار إليها ظهرت له شاشة تطلب منه إسم المستخدم وكلمة العبور، وتبين أن Allen قد خمن كلمة عبور وقام بإزالة الدليل على نشاطه، وتمت إدانة Allen بتهمة دخوله إلى حواسيب الشركة المذكورة بدون تصريح منتهكًا بذلك تشريع جرائم الحاسوب بولاية كانساس، وقد دفع Allen أمام المحكمة بأنه لا يوجد دليل على دخوله إلى حاسوب شركة Bell، إلا أن الولاية دفعت بمسؤولية المذكور إعتمادًا على التعريف التشريعي الواسع لعبارة الدخول بأنها تعني "الإقتراب أو إصدار أمر أو الإتصال بـ... أو تخزين معطيات في... أو إسترداد معطيات من... أو أية شئ آخر يؤدي إلى إستخدام مصادر الحاسوب"، إلا أن المحكمة قررت بأن هذا التعريف كان واسعًا وإذا أخذ به فإنه يؤدي إلى القول بعدم دستورية التشريع لغموضه، ورفضت المحكمة الأخذ بهذا التعريف وفسرت معنى الدخول بقولها بأن قاموس Webster يعرف الدخول Access كحرية أو قابلية للحصول أو الإستخدام، وهذا مشابه للبناء الذي أعدته محكمة الموضوع للوصول إلى عدم وجود دليل ظاهر يقرر أن Allen تحصل على دخول إلى حواسيب شركة Bell، فحتى مرحلة ما قبل قيام Allen بوضع إسمه وكلمة عبور على المكان المقرر في موقع الشركة فلن نستطيع القول بأن لديه القابلية لإستخدام الحواسيب شركة Bell أو الحصول على أي شي، لذا فإنه لا يستطيع القول بأن دخوله إلى نظم حواسيب شركة Bell هو أمر معروف بشكل عام، ومعنى الدخول هنا يبرز كما لو كان مبنيًا على حقيقة الإفتراض وبحيث أن الإسم الصحيح وكلمة العبور تسمح للمستخدم بالدخول إلى الملفات المتواجدة في الداخل ولكن الإسم الخاطئ وكلمة العبور غير الصحيحة تمنع المستخدم من الدخول، وبغياب الدليل بأن Allen قد دخل عبر بحث كلمة العبور للوصول إلى المعلومات بالداخل يؤدي إلى القول بأنه لم يدخل إلى حواسيب شركة Bell، وللمزيد من التفصيل، ينظر: سعد عاطف عبد المطلب حسنين، مرجع سابق، ص-ص 341-342.

التشغيل في الجهاز الإلكتروني من قبل شخص لا يملك حق الدخول بهدف القيام بأفعال غير مشروعة، أو أنه إساءة إستخدام الجهاز ونظامه بواسطة شخص ليس مصرحًا له بإستخدامه، والولوج إليه للوصول إلى المعطيات المخزنة بداخله بغرض الإطلاع عليها[1].

يتحقق فعل الدخول أو الولوج إلى النظام المعلوماتي متى دخل الجاني إلى النظام كله أو جزء منه، وتضيف المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 شرطًا مفاده وجوب بأن يحدث فعل الولوج بدون حق، وذلك يعني أنه لا عقاب للولوج المصرح به من قبل مالك النظام أو صاحب الحق على النظام أو جزء منه مثلًا لأغراض الإختبار المرخص أو حماية النظام للمعني، فضلًا عن ذلك لا يكون هناك تجريم للولوج إلى النظام يتيح للجمهور الولوج المجاني والمفتوح، ففي مثل هذه الحالة الولوج إلى النظام حقًا من الحقوق.[2]

ومنه فإن مجرد الدخول إلى نظام المعالجة الآلية للمعطيات لا يشكل سلوكًا غير مشروعًا وإنما يستمد عدم مشروعيته من كونه قد تم عن طريق الغش، ويكون كذلك أيضًا إذا ما كان بدون تصريح من المسؤول عن النظام[3]، ومنه فإن عدم مشروعية الدخول يرتبط أساسًا بعلم من له السلطة أو الحق في الدخول إلى النظام أو بالتصريح له بالدخول إليه، وبناءً على ذلك فإن عدم المشروعية هو إنعدام السلطة في الدخول إلى هذا النظام[4].

ولذلك فقد حرصت بعض التشريعات مثل القانون الكندي على تجريم إستعمال نظام المعالجة الآلية للمعطيات بدون رضا صاحبه، فينص التشريع الكندي على عقاب: "كل من بسوء نية وبدون وجه حق"، ووفقًا للقانون الأمريكي الخاص بالغش بالكمبيوتر لسنة 1986 فإن الدخول في النظام دون موافقة صاحبه كالدخول في نظم البنوك والمصارف المالية أمر مجرم ومعاقب عليه إذا تم ذلك بنية الغش[5]، والمشرع الجزائري من خلال عبارة: "كل من يدخل أو يبقى عن طريق الغش"، والمشرع الفرنسي من خلال عبارة: "الدخول أو البقاء عن طريق الغش"، والمشرع المصري من خلال عبارة: "كل من دخل عمدًا، أو دخل بخطأ غيرعمدي وبقى بدون وجه حق".

وذلك على أساس أن هذه الأفعال يمكن أن تخلق عقبات أمام المستخدمين الشرعيين للأنظمة المعلوماتية، كما يمكن أن تؤدي إلى إتلاف أو تدمير باهظ التكلفة في حالة إعادة البناء، كما أن هذا التدخل يمكن أن يترتب عليه الوصول إلى معطيات سرية مثال ذلك كلمات المرور

---

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 685.

[2]- هلالي عبد اللاه أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست الموقعة في 23 نوفمبر 2001**، د.ر.ط، 2006، دار النهضة العربية، القاهرة، ص-ص 72-73.

[3]- بوكر رشيدة، مرجع سابق، ص 35.

[4]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص-ص 685-686.

[5]- خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، الطبعة الأولى، 2009، دار الفكر الجامعي، الإسكندرية-مصر، ص 251.

أو معلومات عن النظام الهدف وأسرار تسمح بإستخدام النظام مجانًا، بل وتشجع القراصنة على إرتكاب جرائم أكثر خطورة.[1]

وكذلك يتحقق الدخول غير المشروع متى كان مسموحًا للجاني بالدخول إلى جزء معين من البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه[2]، وقد تدارك المشرع الأمريكي ذلك من خلال توسعه في جريمة الدخول غير المصرح به بحيث مكن أيضًا مساءلة العاملين داخل المؤسسة والمستخدمين المصرح لهم[3]، بموجب قانون التحكم في العنف الإجرامي وتنفيذ القانون الذي أصدره الرئيس الأمريكي بتاريخ 13 سبتمبر 1994[1].

---

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص 70.

[2]- عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)**، الطبعة الأولى، 2006، دار الفكر الجامعي، الإسكندرية-مصر، ص 357.

[3]- يرجع الغموض فى عبارة بدون تصريح إلى عدم تحديد التشريعات المقارنة تعريف لها، وقد واجهت المحاكم الأمريكية صعوبات كبيرة في محاولة التوصل إلى تفسير لمعنى عبارة "بدون تصريح"، ومن أهم القضايا التي حاولت فيها المحاكم إيجاد تفسير لذلك فى قضية US, V.Morris وهي قضية الولايات المتحدة ضد Morris والتي عرفت بقضية دودة الإنترنت، وتخلص وقائعها في قيام أحد الطلاب بالدراسات العليا في جامعة كورنيل Cornell ويدعي Robert Morris في نهاية الثمانينات بتصميم برنامج حاسوب عرف بالدودة Worm وصممت هذه الدودة لكشف ثغرات في أمن الشبكات وبخاصة شبكة الإنترنت، وهي عبارة عن جرثومة أطلقها موريس من حاسوب في 02 نوفمبر سنة 1988 وإنتشرت هذه الدودة إنتشارًا سريعًا وأعادت طبع نفسها وخرجت عن نطاق التحكم، وتم إتهام موريس بإنتهاك القسم 18، U.S.C، 1030 (A) (O) (A) الذي كان يحظر الدخول العمدي إلى حاسوب فيدرالي بدون تصريح إذا حدث ضرر ما، وتم إدانة Morris بمعرفة هيئة المحلفين، وقام موريس بالإستئناف ودفع بأن الدخول إلى الحاسوب لم يكن بدون تصريح لأنه له الحق في الدخول إلى بعض الحواسيب المصابة بالدودة ومنها الحواسيب في جامعات Cornell, Berkeley, Harvard، وأسس دفاعه على أساس التمييز بين نوعين من إساءة التصريح وهما الدخول "بدون تصريح" والدخول بناء على تجاوز الحق في الدخول، حيث إن بعض التشريعات تحظر الدخول بدون تصريح، والبعض الآخر تحظر الدخول غير المصرح به وتجاوز الصلاحية في الدخول وقد كافحت المحاكم كثيرًا من أجل التمييز بين العبارتين، وللمزيد من التفصيل، ينظر: سعد عاطف عبد المطلب حسنين، مرجع سابق، ص427.

وقد دعم Morris دفاعه إستنادًا إلى تقرير مجلس الشيوخ الصادر سنة 1986 بشأن التعديلات التي تمت على القسم 1030 U.S.C. Sec. 18 نظرًا لأن هذا التقرير قد إقترح التمييز بين "الدخول بدون تصريح" و"تجاوز الصلاحية في الدخول"، وهذا التمييز يجد أساسه في الإختلاف بين طائفتين وهما طائفة الدخلاء Outsiders الذين لا يملكون أي حقوق للدخول إلى الحواسيب مثل الهاكرز Hackers، والطائفة الثانية وهي طائفة المطلعين Insiders وهم الأشخاص الذين لديهم حقوق في الدخول إلى الحاسوب مثل الموظفين في إحدى الجهات الذين يدخلون إلى حاسوب جهة العمل، وإستند أيضًا إلى إقتراح التقرير بأنه في الحالات التي يحظر فيها الكونجرس الدخول إلى الحواسيب بدون تصريح ولكن لم يحظر تجاوز الصلاحية في الدخول فإنه يعد لحظر أفعال الدخلاء وليس المطلعين، ودفع موريس بأنه لديه حواسيب إنترنت مشروعة وبالتالي فإنه يدخل ضمن الطائفة المطلعة، وبالتالي لا يمكن إدانته على جريمة الدخول إلى حواسيب شبكة الإنترنت بدون تصريح، وقد رفضت الدائرة الثانية دفع Morris بالرغم من أن دفعه يتفق مع التشريعات التي تحظر فقط الدخول بدون تصريح والذي يستهدف الدخلاء، وأسست حكمها على أن الكونجرس لم يرسم خطًا واضحًا بين الذين يملكون دخولًا ما إلى أية حواسيب فيدرالية، وأولئك الذين لا يملكون ذلك حيث كان قصد الكونجرس أن الأفراد الذين يملكون الدخول إلى بعض الحواسيب الفيدرالية يعدون موضوعًا للمسؤولية وفق نصوص الإحتيال الحاسوبي والقيام بالدخول بدون تصريح إلى الحواسيب الفيدرالية الأخرى، وللمزيد من التفصيل، ينظر: نفس المرجع، ص-ص 427-428.

وفي قضية الولاية ضد Olsen، والتي تخلص وقائعها في أن شخصًا يدعي Laurence Olsen كان يعمل رجل شرطة قام بإستخدام معطيات الحاسوب للشرطة للدخول والحصول على مخرجات طابعة لرخصة مصورة لطالبات جامعيات مقيمات بجوار جامعة واشنطن، وأدين Olsen بتهمة الدخول إلى حاسوب حكومي بدون تصريح إنتهاكًا لتشريع واشنطن بشأن إنتهاك الحاسوب، وفي الإستئناف نازع Olsen بأن دخوله لم يكن غير مصرحًا به مباشرة، وأخذت المحكمة إدعاء Olsen مأخذ=

وبالنسبة للمشرع المصري فإن جريمة تجاوز حدود الحق في الدخول جعلها جريمة مستقلة بموجب المادة 15 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر، والتي جاءت صياغتها كالآتي: "يعاقب بالحبس مدة لا تقل عن ستة (06) أشهر وبغرامة لا تقل عن ثلاثين ألف 30.000 جنيه ولا تجاوز خمسين ألف 50.000 جنيه أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي، مستخدمًا حقًا مخولًا له فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول"، تفترض هذه الجريمة أن الجاني مخول بالدخول للموقع الإلكتروني أو الحساب الخاص أو النظام المعلوماتي، ولكنه قد خالف القواعد أو القيود التي تنظم هذا الدخول، سواء أكانت هذه القيود زمانية أم مكانية أم موضوعية بأن تجاوز مستوى الدخول المصرح له به، ويستوي لدى القانون أن يكون التصريح للجاني بالدخول للموقع الإلكتروني أو الحساب الخاص أو النظام المعلوماتي بسبب وظيفته أم غير ذلك.[2]

أما الوسائل التي يمكن الإعتماد عليها في عملية الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات فقد جاءت المادة 394 مكرر من ق.ع.ج شاملة ولم تحدد طريقة معينة لطرق الدخول، فمدلول مصطلح الدخول الواردة في هذه المادة تشير إلى كافة الأفعال التي تسمح بالولوج إلى النظام والسيطرة والإحاطة على المعطيات التي يتكون منها[3]، وعليه يجوز الدخول إليه بأي وسيلة كانت، ولذلك تقع الجريمة بأية وسيلة كانت أو بأي طريقة، ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر.

وعليه يمكن تصور اللجوء إلى كافة الوسائل المتاحة للدخول إلى نظام المعالجة الآلية للمعطيات، أحيانًا قد لا يتطلب هذا السلوك سوى تشغيل الجهاز، وأحيانًا يتطلب أمورًا أكثر تعقيدًا كمحاولة الحصول على الرقم السري حتى يمكن الدخول إلى النظام، وقد يتم عن طريق إستعمال برامج خبيثة يتم دمجها في أحد البرامج الأصلية للجهاز حيث تعمل كجزء منه، وتقوم هذه البرامج بتسجيل الشيفرات التي يتعامل بها المستخدمون الشرعيون، كما توجد وسائل تعتمد على ضعف الأنظمة ذاتها[4] أو على إثر بعض الأخطاء المترتبة عن عملية البرمجة، وغالبًا ما

=الفحص وذلك بفحص قواعد العمل التي تنظم سلوك Olsen، وإنتهت المحكمة إلى أن محضر الجلسة لم يبين أن رخصة الدخول إلى الحاسوب كانت مشروطة لإستخدام هذه المعطيات ونقضت حكم الإدانة، ويستخلص من ذلك أن Olsen كان مصرحًا له بالدخول إلى الحاسوب داخل جهة العمل، ولكن لم يحدد له حدودًا معينة من أجل الدخول إلى الحاسوب، ولذلك فإن المتهم كان يملك الحق في الدخول إلى نظام الحاسوب وأن إستخدام هذا الحق في غرض غير مشروع لا ينفي أن الدخول مصرح به، وللمزيد من التفصيل، ينظر: سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 430.

[1]- نفس المرجع، ص-ص 425-426.

[2]- رامي متولي القاضي، عمر سالم، **شرح قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 مقارناً بالتشريعات المقارنة والمواثيق الدولية**، الطبعة الأولى، 2020، مركز الدراسات العربية للنشر والتوزيع، مصر، ص 104.

[3]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص-ص 687-688.

[4]- حمزة بن عقون، مرجع سابق، ص 119.

تتم جميع محاولات إختراق الأنظمة المعلوماتية بواسطة برامج متوفرة على الإنترنت يمكن لمن له خبرة تقنية أن يستخدمها لتنفيذ هجماته على أجهزة الغير[1].

وفي النهاية فإن الجريمة تقوم بفعل الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات ولو لم يترتب عليه أي نتيجة أخرى، فلا يشترط لقيامها إلتقاط المتدخل للمعطيات التي يتضمنها المستند الإلكتروني أو بعضها أو إستعمالها، بل إن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام.[2]

ومنه تعد جريمة الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات من الجرائم الشكلية التي لا يتطلب لقيام الركن المادي فيها تحقق نتيجة ما، وبالرغم من إمكانية حدوث أضرار معينة بالمعطيات بمحوها أو تعديلها أو إفساد نظام التشغيل نتيجة لهذا السلوك، إلا أن ذلك لا يغير من طبيعة الجريمة بإعتبارها جريمة شكلية.[3]

2- جريمة البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات الذي يحتوي على مستندات إلكترونية:

يعرف فعل البقاء غير المصرح به بأنه: "التواجد داخل نظام المعالجة الآلية للمعطيات تحتوي على مستندات إلكترونية، رغمًا عن إرادة من له الحق في السيطرة على هذا النظام".[4]

ويكفي لتحقق عنصر البقاء مجرد التواجد داخل كل أو جزء من النظام المعالجة الآلية للمعطيات، فمجرد التجول يكفي لقيام هذا السلوك المجرم دونما أن يشترط لذلك المحو أو الإتلاف أو التعديل للمعلومات المتواجدة في النظام، ويرى البعض أن الإستعمال التعسفي لنظام المعالجة الآلية للمعطيات لا يعد من قبيل الدخول أو البقاء، إذ أن المتهم ليس له الحق في الدخول أو البقاء في حين أن المستعمل المتعسف له الحق في الدخول والبقاء غير أنه يستعمل النظام في غير الغرض المخصص له، كأن يقوم بتشغيل برنامج خاص بالألعاب أو التسوق.[5]

وقد يتحقق السلوك الإجرامي لجريمة البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات في الحالة التي يجد فيها الشخص نفسه داخل النظام عن طريق الخطأ أو الصدفة، غير أنه يقرر البقاء داخل النظام وعدم قطع الإتصال به[6] وهو ما أشار إليه المشرع المصري

---

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص-ص 687-688.

[2]- آمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، الطبعة الثانية، 2007، دار هومة للطباعة النشر والتوزيع، الجزائر، ص-ص 109-110.

[3]- حمزة بن عقون، مرجع سابق، ص 120.

[4]- بلحسيني حمزة، مرجع سابق، ص 268.

[5]- ملياني عبد الوهاب، **أمن المعلومات في بيئة الأعمال الإلكترونية**، أطروحة الدكتوراه في القانون العام، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد- تلمسان-، 2016-2017، ص 184.

[6]- حمزة بن عقون، مرجع سابق، ص 122.

من خلال عبارة: "دخل بخطأ غير عمدي، وبقى بدون وجه حق"، أو حينما يستمر في البقاء بداخل النظام بعد المدة المسموح له بالبقاء بداخله من قبل المسؤول عن النظام[1].

وقامت البعض من التشريعات المقارنة بتقنين جريمة البقاء بجوار جريمة الدخول على الرغم من أن البقاء هو نتيجة طبيعية لفعل الدخول، وبمعنى آخر نجد أن البعض من التشريعات المقارنة قد أكدت على أن الجريمتين منفصلتين وأن الدخول غير المصرح به يحدث بمجرد الولوج داخل النظام دون إنتظار لحدوث نتيجة إجرامية من جراء ذلك، وبالمثل جريمة البقاء تحدث بمجرد التواجد داخل النظام بصفة غير مشروعة دونما حدوث نتيجة معينة من جراء ذلك.[2]

ذلك أن هناك تعددًا ماديًا سببه أن الدخول غير المصرح به هو سلوكًا إجراميًا مختلفًا تمامًا عن فعل البقاء غير المشروع وكل منهما غير مرتبط بالآخر، ذلك أن عندما يستخدم المشرع مصطلحين مختلفين يجب أن تكون دلالة ومعنى كل مصطلح مختلف عن المصطلح الآخر، فمصطلح البقاء لا يشمل مصطلح الدخول والعكس صحيح، كما أن صفة الغش لا تقتصر التطبيق على فعل الدخول فقط وإنما تنطبق على فعل البقاء أيضًا.[3]

وتعد هذه الجريمة من الجرائم المستمرة لإستمرار الإعتداء على المصلحة المحمية قانونًا ما دام إستمر البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات، كما تعد أيضًا من الجرائم الوقتية نظرًا لأن هذه الجريمة تتم بمجرد تحقق فعل الدخول غير المصرح به، وما تجدر الإشارة إليه أنه في الحالة التي يتم فيها الدخول غير المصرح به إلى النظام ومن ثم البقاء فيه لفترة زمنية يتحقق الإجتماع المادي للجرائم.[4]

فيستهدف الإعتداء على المعطيات المخزنة فيه أو يستهدف المعدات المتصلة به، وواضح أن المشرع الجزائري لم يكتف بتجريم الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات، بل تجاوز ذلك إلى تجريم مجرد المحاولة وذلك حسب العبارة الواردة في الفقرة الأولى من المادة 394 مكرر بالنص على "أو يحاول ذلك"، غير أن ما يمكن إثارته هنا هو ما يتعلق بفكرة الإثبات، وما من شأنه إعطاء تصور يفيد بأن هناك شروع أو محاولة طالما أن الجريمة في حد ذاتها تطرح إشكالًا في الإثبات[5]، حيث يزعم المتهم في حالة القبض عليه أنه كان على وشك الإنفصال عن النظام المعتدى عليه[6].

---

[1]- حبيباتني بثينة، مرجع سابق، ص- ص 35-36.

[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 343.

[3]- حبيباتني بثينة، مرجع سابق، ص 36.

[4]- حمزة بن عقون، مرجع سابق، ص-ص 122-123.

[5]- زيبحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، د.ر.ط، 2011، دار الهدى، عين ميلة- الجزائر، ص 51.

[6]- بن مكي نجاة، **السياسة الجنائية لمكافحة جرائم المعلوماتية**، د.ر.ط، 2017، دار الخلدونية، القبة القديمة- الجزائر، ص 184.

ووصف جريمة البقاء يتغير إلى وصف جريمة أخرى إذا قام الجاني بإرتكاب ما من شأنه أن يغير في وصف هذه الجريمة، كما لو قام بإنتهاك الحق في الخصوصية أو وضع فيروسات أو أحدث تخريب في النظام أثناء البقاء.[1]

كما تعد هذه الجريمة من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة إجرامية معينة، فيكفي البقاء غير المصرح به داخل النظام ليقوم الركن المادي لهذه الجريمة.[2]

ولكن التساؤل المطروح متى تنتهي جريمة الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات، ومتى تبدأ جريمة البقاء فيه؟

ذهب البعض إلى أن جريمة الدخول تقوم منذ اللحظة التي يدخل فيها إلى نظام المعالجة الآلية للمعطيات ويبقى مدة قصيرة من الزمن داخله وتكتمل، وبعد إكتمال تلك اللحظة تبدأ جريمة البقاء داخل النظام وتنتهي بإنتهاء حالة البقاء، ويؤخذ على هذا الرأي أنه لا يحدد لحظة بداية جريمة البقاء بطريقة حاسمة وبدقة[3]، وذهب رأي آخر إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع، وأصبح غير مشروع فإذا لم ينسحب يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام[4]، لأنه يتجول في نظام يعلم مسبقًا أن مبدأ دخوله وإستمراره فيه غير مشروع، ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام[5].

لكنه ومع ذلك يظل الغموض قائمًا حول مدة البقاء داخل نظام المعالجة الآلية للمعطيات ويطرح صعوبة حول تحديد زمن البقاء، ويجب التفرقة هنا بين البقاء الحاصل عن جريمة الدخول غير المصرح به وبين البقاء الناتج عن الدخول المسموح به لكون الجاني رفض الخروج بعد إستيفاء الوقت المسموح له بالدخول فيه للنظام، وفي كل الحالات يتضح أن المشرع ربط البقاء كتصرف إرادي من قبل الجاني بسوء النية أي عن طريق الغش، ويستوي في ذلك أن يكون الدخول أو البقاء في النظام كله أو حتى في جزء منه ذلك أن الإعتداء قد يستهدف الجهاز نفسه بكيانه المنطقي.[6]

وإنطلاقًا مما تقدم، يتضح أن الركن المادي لجريمة البقاء غير المصرح به يبدأ من اللحظة التي يدرك فيها الفاعل حقيقة الإتصال الذي تم، وبقاءه ضمن نظام المعالجة الآلية للمعطيات دون حق يتيح إجراء الإتصال أو الإبقاء عليه، ومن الجدير بالذكر أنه لا يشترط لتحقيق الركن المادي في هذه الجريمة أن يقدم الجاني على إرتكاب جريمة أخرى ولكن يكفي لتحقيقها إستمرار الجاني بالبقاء في النظام من دون أن يقوم بأي نشاط، والبقاء داخل النظام لا يعني القيام

---

[1]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 344.

[2]- بن مكي نجاة، مرجع سابق، ص 184.

[3]- خثير مسعود، **الحماية الجنائية لبرامج الكومبيوتر أساليب وثغرات**، د.ر.ط، 2010، دار الهدى، عين ميلة- الجزائر، ص117.

[4]- آمال قارة، مرجع سابق، ص 112.

[5]- خثير مسعود، مرجع سابق، ص 117.

[6]- زيبحة زيدان، مرجع سابق، ص 50.

بالإتلاف أو التعديل أو التخريب في النظام وما يحتويه من المستندات الإلكترونية بل يعني إمكانية التحكم في النظام، ومن هنا يتبين أن وصف البقاء قد يتغير إلى وصف جريمة أخرى إذا أقدم الجاني على إرتكاب ما من شأنه أن يغير وصف هذه الجريمة، كما لو قام بالمساس بسرية المعطيات وبإنتهاك الحق في الخصوصية[1]، ويرى البعض بأن النشاط الإجرامي في هذه الجريمة لا يتطلب أن ينجح الفاعل في الوصول إلى معطيات المستند الإلكتروني داخل النظام، ذلك أنه وإن كانت العلة من تجريم الدخول غير المصرح به هي حماية المعلومات والبرامج من الوصول إليها والتلاعب بها، إلا أن هذه الجريمة هي من الجرائم التي تشكل عدوانًا محتملًا على الحق، وليست من الجرائم التي تتمثل في تحقق العدوان على الحق الذي يحميه القانون[2].

ثانيًا: الركن المعنوي لجريمتي الدخول والبقاء غير المصرح بهما داخل نظام المعالجة الآلية للمعطيات الذي يحتوي على مستندات إلكترونية

جريمة الدخول غير المصرح به داخل نظام المعالجة الآلية للمعطيات يحتوي على مستندات إلكترونية أوالبقاء فيه من الجرائم العمدية الذي يستلزم لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، حيث يجب أن يكون الجاني عالمًا بأنه يقوم بفعل الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات أو البقاء فيه دون إذن أو تصريح أي بصورة غير مشروعة، حتى وإن كان له الحق في الدخول فإن هذا الحق قد يكون مقيدًا من حيث الزمن أو من حيث النطاق، كما يجب أن تتجه إرادته إلى البقاء في النظام وعدم قطع الإتصال به رغم علمه بعدم مشروعية هذا الفعل.

ينتفي القصد الجنائي إذا كان الجاني يعتقد أن له تصريح بالدخول أو البقاء، أو أن الموقع متاحًا ومفتوحًا للجمهور، وكذلك إذا كان الدخول تم عن طريق الصدفة أو الخطأ أو السهو، لكن في المقابل يتعين عليه أن يخرج فورًا من نظام المعالجة الآلية للمعطيات عند علمه بأن دخوله أو بقاءه غير مصرح بهما، في حال عدم قيامه بذلك توافر لديه القصد الجنائي منذ اللحظة التي تحقق فيها العلم وأعتبر مرتكبًا لجريمة الدخول أو البقاء غير المصرح بهما.[3]

فالدخول الذي يتم عن طريق الصدفة أو السهو أو الخطأ لا يعد في رأي البعض دخولًا غير مشروع، وعلى الشخص أن يخرج فور إدراكه أنه دخل إليه دون وجه حق، فإذا بقى ولم يخرج تحقق القصد الجنائي لديه ويكون قد تم عن طريق الغش، أما إذا كان الدخول أو البقاء مسموحًا به أو وقع في خطأ بشأن حقه في الدخول أو البقاء سواء من حيث النطاق أو الزمان فلا يعد القصد الجنائي متوفرًا في هذه الحالة .[4]

[1]- بلحسيني حمزة، مرجع سابق، ص- ص 269- 270.
[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 347.
[3]- حبيباتني بثينة، مرجع سابق، ص-ص 48-49.
[4]- ملياني عبد الوهاب، مرجع سابق، ص 185.

وأن يكون القصد الجنائي معاصرًا للسلوك الإجرامي وأن تتجه إرادته لإرتكابه، فإن تخلف القصد الجنائي في لحظة بدء فعل الدخول غير المصرح به ينفي الصفة الإجرامية عن هذا السلوك.[1]

وقد عبر المشرع الجزائري في الفقرة الأولى من المادة 394 مكرر من ق.ع.ج عن القصد العام من خلال إستعماله عبارة " كل من يدخل أو يبقى عن طريق الغش"، فإستخدام هذه العبارة يدل على سوء نية الجاني ومع علمه، يعني بأن دخوله إلى نظام المعالجة الآلية للمعطيات والبقاء فيه غير مصرح به وغير مشروع.

ويلاحظ أن جميع النصوص القانونية في مختلف الدول التي تناولت جريمة الدخول والبقاء بدون تصريح إلى نظام المعالجة الآلية للمعطيات قد عبرت عن القصد العام في هذه الجريمة، كتشريع الدنماركي الذي أشار إلى أن الفاعل يقوم بالدخول غير المصرح به إلى النظام على نحو مخالف للقانون، وفي فرنسا قررت المادة 323-1 من ق.ع.ف أن يكون الدخول إلى النظام قد تم عن طريق الغش والخداع، ومن بين هذه التشريعات أيضًا قوانين لبعض الولايات الأمريكية كولاية كاليفورنيا التي تعاقب بوصف الجنحة كل شخص يدخل عمدًا في النظام أو الشبكة أو في البيانات المبرمجة مع علمه بعدم رضاء صاحب النظام عن ذلك[2]، وقد تطلب القانون الإنجليزي أن يتم الدخول إلى النظام على نحو غير مصرح به مع العلم بذلك، وفي فنلندا وسويسرا والبرتغال إشترط أن يتم الدخول إلى النظام بدون تصريح، وفي السويد واليونان أن يتم الدخول إلى النظام بدون وجه حق، وفي هولندا وأستراليا أن يتم الدخول عمدًا وعلى نحو غير مشروع أو بدون وجه حق[3].

وهناك البعض من التشريعات التي تتطلب قصدًا خاصًا بالإضافة إلى القصد العام في أركان هذه الجريمة وتشدد العقوبة بناءً عليه، وهو قصد التأثير في المعطيات أو التأثير في نظام المعالجة الآلية للمعطيات نفسه للعقاب على هذا الدخول، ومن هذه القوانين القانون الأسترالي والقانون الألماني والقانون الكندي والقانون النمساوي والقانون اليوناني والقانون الإنجليزي، ففي أستراليا تشدد العقوبة متى إرتكب فعل الدخول غير المصرح به إلى النظام بنية الإضرار بالغير، وفي الدنمارك تم تشديد العقوبة متى إرتكب فعل الدخول بنية الإحاطة بمعلومات تتعلق بالأسرار المتعلقة بعمل إحدى الشركات.[4]

ومن هذه التشريعات أيضًا القانون السعودي بشأن مكافحة جرائم المعلوماتية لسنة 2008 حيث جرم هذا القانون الدخول غير المشروع بطريقة متعمدة إلى الكمبيوتر أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها، فقد جاء

[1]- حمزة بن عقون، مرجع سابق، ص 121.
[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 350.
[3]- خالد ممدوح إبراهيم، مرجع سابق، ص 260.
[4]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص-ص 350-351.

نص المادة 05 على أنه: "يعاقب بالسجن مدة لا تزيد على أربع (04) سنوات وبغرامة لا تزيد على ثلاثة ملايين 3.000.000 ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1- الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها؛

2- إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها، أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها، أو حذفها أو تسريبها أو إتلافها أو تعديلها؛

3- إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت".[1]

وعلى الرغم من أن النظام السعودي المشار إليه قد جرم الدخول غير المشروع في نظام حاسب آلي أو موقع إلكتروني أو شبكة، فإنه لم يجرم مجرد الدخول بل إشترط أن يكون ذلك الدخول بقصد تحقيق غاية معينة، أي إستلزم توافر نية معينة وهو ما يسمى بالقصد الخاص.[2]

الفرع الثاني: جريمة المساس بسلامة معطيات المستند الإلكتروني

تكمن الفكرة الأساسية للجريمة محل الدراسة في وجود معطيات يتضمنها المستند الإلكتروني داخل نظام المعالجة الآلية للمعطيات، حيث تكون هذه المعطيات معدة للمعالجة ثم يتم التدخل فيها بصورة غير مشروعة، إما عن طريق إدخال معطيات أخرى لم تكن موجودة أصلًا وذلك بقصد التشويش على المعطيات الموجودة سابقًا مما قد يؤثر على صحتها، أو كل فعل قد يؤدي إلى إزالة المعطيات بطريقة غير مشروعة، أو عن طريق تعديل وتغيير في مضمونها إما بالشطب أو الإضافة ويؤثر ذلك بالنتيجة على سلامتها[3]، وهي الجريمة المنصوص عليها في المادة 394 مكرر1 من قانون العقوبات الجزائري[4]، وتقابلها المادة 323-3 من قانون العقوبات الفرنسي[5].

---

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص-ص 278-279.

[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص 131.

[3]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 696.

[4]- تنص المادة 394 مكرر1 من ق.ع.ج على أن: "يعاقب بالحبس من سنة (01) إلى ثلاث (03) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

[5]-Art 323-3 du C.P.F (Modifié par Loi n°2015-912 du 24 juillet 2015 - art. 4) dispose que: « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende».

ترجمتها:

نصت المادة 323-3 من ق.ع.ف على أن: "يعاقب على الإدخال للمعطيات بطريق الغش في نظام المعالجة الآلية للمعطيات أو محوها أو التعديل بطريق الغش للمعطيات التي يحتويها، بعقوبة الحبس لمدة خمس (05) سنوات وغرامة قدرها=

أولًا: أركان جريمة المساس بسلامة معطيات المستند الإلكتروني

لقيام جريمة المساس بسلامة معطيات المستند الإلكتروني، لابد من توافر أركانها القانونية المتمثلة في:

1- الركن المادي لجريمة الإعتداء على سلامة المعطيات الإلكترونية الواردة في المستند الإلكتروني:

لتحقق الركن المادي في الجريمة المراد دراستها، لابد من توافر عنصريين:

أ- السلوك الاجرامي:

الأفعال المتمثلة في الإدخال والإزالة والتعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها، حتى ولو تضمن إعتداء على المعطيات الواردة في المستند الإلكتروني داخل نظام المعالجة الآلية للمعطيات، فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهم، لأن كل تلك الأفعال لا تنطوي لا على إدخال ولا على تعديل.[1]

ومنه يتحقق السلوك الإجرامي إما في إدخال معطيات ضمن محتوى المستند الإلكتروني بطريق الغش أو إزالتها أو تعديلها، ويكفي لقيام الجريمة أن يصدر عن الجاني إحداها فقط فلا يشترط أن تقع هذه الأفعال مجتمعة، والتي تتمثل في:

أ-1- فعل الإدخال:

يعرف فعل الإدخال على أنه: "إدخال المعطيات في نظام المعالجة الآلية للمعطيات لم تكن موجودة أصلًا، وذلك بهدف التشويش على المعطيات الموجودة، مما قد يؤثر على صحتها"، أو أنه: "إدخال خصائص ممغنطة جديدة في الدعامة الموجودة، سواء كانت فارغة أو كانت تحتوي على خصائص ممغنطة قبل هذا الإدخال".[2]

وهي مرحلة إدخال المعطيات في المستند الإلكتروني بمعطيات زائفة أو مغلوطة لم تكن موجودة فيه من قبل، ويتم فعل الإدخال عن طريق إستخدام برامج خبيثة بهدف التعديل في المعطيات مما يؤثر على صحتها أو قيمتها أو نسبتها، كما أنه يكون بهدف تشويهها أو إتلافها أو تدميرها، مما يؤثر ذلك سلبًا على المعطيات الموجودة فيه من حيث قيمتها وسلامتها.[3]

=150.000 يورو. وإذا إرتكبت هذه الجريمة ضد نظام المعالجة الآلية للمعطيات الشخصية التي تنفذها الدولة، فإن العقوبة تزيد إلى الحبس سبع (07) سنوات وغرامة قدرها 300 ألف يورو".

[1]- آمال قارة، مرجع سابق، ص-ص 122-123.

[2]- حبيباتني بثينة، مرجع سابق، ص 54.

[3]- ملياني عبد الوهاب، مرجع سابق، ص-ص 192-193.

أ-2- فعل الإزالة:

يقصد بفعل الإزالة: " المحو الجزئي أو الكلي للمعطيات المتواجدة على الدعامة، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات في منطقة خاصة بالذاكرة".[1]

ويلاحظ أن النص المادة 394 مكرر1 من ق.ع.ج لم يستثني بأن تكون الإزالة للمعطيات التي يتضمنها المستند الإلكتروني جزئيًا أو كليًا، والأرجح أن يشمل المعنيين معًا طالما أن كليهما يشكل فعلًا ينطوي على خطورة كبيرة من شأنها إلحاق الأذى بالغير[2].

وقد أوصى التقرير الصادر عن المجلس الأوروبي بخصوص الجرائم المعلوماتية بتجريم الأفعال التي تؤدي إلى تدمير المعلومات، ولقد ميزت التوصية الصادرة عنه بين شكلين من أشكال التدمير الذي يلحق بالمعلومات، الأول يتعلق بمحو المعلومات تمامًا، والثاني بإخفاء المعلومات بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محوها تمامًا[3]، فيذهب البعض إلى أن إخفاء المعلومات دون محوها لا يمكن أن يشكل تدميرًا لها، ومؤدى ذلك أن إخفاء أحد الملفات على سبيل المثال لا يترتب عليه محو المعلومات التي يحتوي عليها من ذاكرة نظام المعالجة الآلية للمعطيات وإنما يؤدي فقط إلى تعديل في قائمة الملفات، وهو ما يعني أن إخفاء المعلومات في هذه الحالة لا يعدو أن يكون تعديلًا وليس تدميرًا[4].

أ-3- فعل التعديل:

يقصد بفعل التعديل تغيير في المعطيات التي يتضمنها المستند الإلكتروني وإستبدالها بالمعطيات الآخرى، عن طريق برامج تلاعب في المعطيات سواء بمحوها كليًا أو جزئيًا أو بتعديلها[5]، وكذا عن طريق إمدادها بالمعطيات المغايرة تؤدي إلى نتائج غير تلك التي صممت لأجلها[6].

ويتحقق فعل التعديل بكل سلوك من شأنه أن يؤدي إلى تحقيق غاية الجاني في ذلك، فإذا ما كانت الغاية من التعديل الحصول على مستند مخالف للمستند الأصلي المحفوظ في ذاكرة نظام المعالجة الآلية للمعطيات فقد يتم تحقيق ذلك بواسطة حذف المعطيات أو الإضافة أو إدخال معطيات جديدة.[7]

---

[1]- بن شهرة شول، مرجع سابق، ص102.

[2]- زيبحة زيدان، مرجع سابق، ص 55.

[3]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، الطبعة الأولى، 2009، دار الفكر الجامعي، الإسكندرية- مصر، ص 419.

[4]- نفس المرجع، ص 419.

[5]- حسين محمد الغول، مرجع سابق، ص 466.

[6]- ملياني عبد الوهاب، مرجع سابق، ص 195.

[7]- حبيباتني بثينة، مرجع سابق، 59.

وقد فرقت التوصية الصادرة عن المجلس الأوروبي المتعلقة بالجرائم المعلوماتية بين التعديلات التي تؤدي إلى نتائج سلبية تتعلق بحالة المعلومات والبرامج، وبين التعديلات غير المصرح بها والتي لا تؤدي إلى إحداث هذه النتائج بل قد تساعد على تحسين أي من المكونات المنطقية للجهاز الإلكتروني ونظامه، وقد تضمنت التوصية بندًا يطالب إدراج التعديلات الأولى ضمن القائمة الأساسية لجرائم المعلوماتية ولكنه إكتفى في خصوص الثانية بإدراجها ضمن القائمة الإختيارية، إلا أن الدول التي جرمت إتلاف المعلومات لم تعتد بهذه التفرقة حيث تم تجريم كافة أشكال التعديل، وإن إختلفت النصوص فيما بينها في تحديد هذا التعديل، فبينما إستخدمت كثير من القوانين تعبير تعديل المعلومات بشكل مباشر، إستخدمت قوانين أخرى تعبيرات مختلفة وإن كانت تدل على نفس المعنى.[1]

ب- محل التجريم:

أفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يتضمنها المستند الإلكتروني، سواء بإضافة معطيات جديدة غير صحيحة أو إزالة أو تعديل معطيات موجودة من قبل، وهذا يعني أن النشاط الإجرامي في هذه الجريمة يرد على محل أو موضوع محدد وهو المعطيات الخاصة بالمستند الإلكتروني والمخزنة داخل نظام المعالجة الآلية للمعطيات أي التي يحتويها النظام وتشكل جزءًا منه[2]، وقد عرف المشرع الجزائري المعطيات المعلوماتية بموجب الفقرة (ج) من المادة 02 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر كالآتي: "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

ويترتب على ذلك أن الجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها وحتى ولو لفترة قصيرة كما لو كانت مفرغة على دعامة إلكترونية خارج النظام، فتنصرف الحماية الجزائية إلى المعطيات المعلوماتية المتواجدة داخل نظام المعالجة الآلية للمعطيات أو تلك التي تكون في طور المعالجة أو الإرسال ضمن نطاق النظام، ولا يشترط أن تقع أفعال الإدخال والإزالة وتعديل المعطيات بطريق مباشر بل يمكن أن يتحقق ذلك بطريق غير مباشر سواء من بعد أم بواسطة شخص ثالث[3]، أما المعطيات غير المعالجة التي لم تدخل بعد داخل النظام فهي خارج نطاق الحماية المشمولة بهذا النص وإن كان يجوز حمايتها وفقًا لنصوص جنائية أخرى[4].

---

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص-ص 418-419.

[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص-ص 120-121.

[3]- حسين محمد الغول، مرجع سابق، ص 465.

[4]- خثير مسعود، مرجع سابق، ص-ص 123-124.

2- الركن المعنوي لجريمة المساس بسلامة معطيات المستند الإلكتروني:

جريمة محل الدراسة من الجرائم العمدية التي يشترط لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، فيجب أن يكون الجاني عالمًا بأن فعل الإدخال والإزالة والتعديل سلوكات غير مشروعة وأنه يعتدي على صاحب الحق في المعطيات، ومع ذلك تتجه إرادته الحرة إلى إرتكاب السلوكات الإجرامية السابقة الذكر.

وبالرغم من إشتراط المشرع الجزائري توفر نية الغش لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير، بل تتوفر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو الإزالة أو التعديل مع العلم بذلك وإتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرًا في الجريمة.[1]

وقد طبقت محكمة النقض الفرنسية المادة 323-3 من ق.ع.ف على قيام أحد الأشخاص بتعديل وإلغاء لمعلومات تتعلق باللوائح المطبقة بإحدى الشركات بطريق العمد، وقد أقرت المحكمة بأنه ليس من اللازم أن تكون هذه التعديلات أو الإلغاءات تم إرتكابها بواسطة شخص ليس له حق الدخول في نظام المعالجة الآلية للمعطيات، ولا يشترط أن يتوافر لدى الجاني نية الإضرار، وبناء على ذلك أيدت حكم محكمة الإستئناف الذي أدان المتهم عن هذه الجريمة بعدما إستخلصت أركانها من قيام الشخص بتعديل المعطيات والتي سبق وأن قام بتسجيلها بطريقة نهائية على النظام للمحاسبة كأن يقوم بالإشراف عليه.[2]

الفرع الثالث: جريمة إتلاف المستند الإلكتروني

قد لا يكتفي المجرم المعلوماتي بالدخول غير المصرح به والبقاء في الأنظمة المعالجة الآلية للمعطيات، بل قد يتجاوز فعله الغرض الإجرامي بإتلافه المستندات والمعطيات المسجلة إلكترونيًا والمخزنة بداخل هذه الأنظمة.[3]

أولًا: جريمة إتلاف المستند الإلكتروني بحذف أو تغيير معطياته

نص المشرع الجزائري على هذه الجريمة بموجب الفقرة 02 من المادة 394 مكرر من ق.ع.ج[4]، ونص المشرع الفرنسي على هذه الجريمة بموجب الفقرة 02 من المادة 323-1 من ق.ع.ف[5] كظرف تشديد لجريمة الدخول أو البقاء غير المصرح بهما داخل نظام المعالجة الآلية

[1]- بن مكي نجاة، مرجع سابق، ص 190.

[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 373.

[3]- بلحسيني حمزة، مرجع سابق، ص-ص 215-216.

[4]- تنص الفقرة 02 من المادة 394 من ق.ع.ج على أن: "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

[5]-Art 323-1 paragraphe 02 du C.P.F (LOI n°2023-22 du 24 janvier 2023 - art. 6) dispose que: «Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende».=

للمعطيات، ونجد المشرع المصري قد تناول جريمة الإتلاف المعلوماتي في المادة 17 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر[1].

وهي الجريمة المنصوص عليها في المادة 04 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بعنوان: "الإعتداء على سلامة البيانات"[2] والمادة 08 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بعنوان: "الإعتداء على سلامة البيانات"[3].

لقيام الجريمة محل الدراسة يشترط أن يقوم الجاني بإتلاف المستندات الإلكترونية، وذلك من خلال فعل الحذف أو التعديل بإستخدام وسيلة إلكترونية معينة.

1- الركن المادي:

تتحقق الصورة المشددة لهذه الجريمة متى ترتب على الدخول أو البقاء غير المصرح بهما داخل نظام المعالجة الآلية للمعطيات حذف أو تغيير لمعطيات مستندات الإلكترونية التي يتضمنها، ويكفي لتحقق هذا الظرف المشدد أن تتوفر علاقة سببية بين فعل الدخول أو البقاء غير المصرح بهما وبين النتيجة التي تحققت المتمثلة في تغيير أو حذف المعطيات، ولعل فعل

=ترجمتها:

تنص الفقرة 02 من المادة 323-1 من ق.ع.ف على أن: "إذا ترتب على ذلك حذف أو تغيير لمعطيات النظام أو تخريب لنظام تشغيل النظام، تكون العقوبة الحبس خمس (05) سنوات وغرامة قدرها 150.000 يورو".

[1]- تنص المادة 17 من القانون رقم: 175 لسنة 2018 السالف الذكر على أن: "يعاقب بالحبس مدة لا تقل عن سنتين (02) وبغرامة لا تقل عن مائة ألف 100.000 جنيه ولا تجاوز خمسمائة ألف 500.000 جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا متعمدًا وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي إستخدمت في الجريمة".

[2] -Art 04 du convention sur la cybercriminalité dispose que : «Atteinte à l'intégrité des données:

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'alterer ou de supprimer des données informatiques.

2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux».

ترجمتها:

تنص المادة 04 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 على أن: "الإعتداء على سلامة البيانات:

1- تعتمد كل دولة ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما إرتكبت عمدًا: إتلاف بيانات حاسوبية حذفها إفسادها، تعديلها أو تدميرها.

2- يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة 01 في ضرر جسيم".

[3]- تنص المادة 08 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "الإعتداء على سلامة البيانات:

1- تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدًا وبدون وجه حق.

2- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم".

التغيير أو الحذف يرد على المعلومات الإلكترونية سواء بإعتبارها أموالًا معنوية ذات طبيعة إلكترونية أو بإعتبارها مستندًا إلكترونيًا ذات طابع خاص ناتج عن معالجتها إلكترونيًا.[1]

وتتمثل الصور التي أشار إليها المشرع الجزائري من خلال نص الفقرة 02 من المادة 394 مكرر من ق.ع.ج[2] والمشرع الفرنسي وفقًا للفقرة 02 من المادة 323-1 من ق.ع. ف، في حذف المعطيات الواردة في المستند الإلكتروني سواء عن طريق إتلافها أو تدميرها جزئيًا أو كليًا، كما يشمل ذلك أيضًا حذف المعطيات من داخل نظام المعالجة الآلية للمعطيات وهو ما يعد من أخطر صور الضرر التي تلحق بالمستند الإلكتروني[3]، وأوضحت المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بأن حذف المعطيات مطابقًا لتدمير الشيء المادي حيث يتم تدميرها وجعلها غير قابلة للتعرف[4].

ويتمثل التغيير في الجريمة محل الدراسة في تغيير حالة المعطيات الواردة في المستند الإلكتروني المخزن داخل نظام المعالجة الآلية للمعطيات وذلك من خلال تبديل هذه المعطيات وإستبدالها بأي طريقة كانت، مما يترتب على ذلك تخريب وإتلاف المعطيات كما يفقدها قيمتها وجديتها[5]، بحيث تبقى موجودة ولكن دون أن تحمل أي معنى ولا أي فائدة بعد أن تم التلاعب فيها بصورة تؤثر في قيمتها، ويصبح من غير ممكن إستغلالها ومعالجتها وتحقيق الغرض الذي جمعت لأجله حتى يتحقق معنى الإتلاف عليها، لأنها سوف تعطي معلومات غير صحيحة عن الشخص، لأن الجهاز الإلكتروني بوصفه مجرد آلة لا يمتلك القدرة على التمييز بين المعطيات الصحيحة وغير الصحيحة[6].

وأشارت المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 إلى أن المقصود بمصطلح "التغيير" هو تعديل المعطيات القائمة، وبالتالي فإن إدخال رموز خبيثة مثل الفيروسات وأحصنة طروادة مشمولة في هذه الفقرة كما هو الحال بالنسبة للتعديل الناجم عن المعطيات، وأوضحت بأن المقصود بإتلاف المعطيات الإلكترونية أي عمل يمنع أو ينهي توافر المعطيات للشخص الذي لديه حق الولوج إلى الجهاز الإلكتروني أو لوسيلة الحفظ التي تم تخزين المعطيات عليها.[7]

وإتلاف المعلومات يتم بوسائل ذات طبيعة تقنية ترتبط ببرمجة المعلومات كالبرامج التخريبية، وتتعدد وسائل تخريب وإتلاف المعلومات ومنها على سبيل المثال حذف المعطيات

---

[1]- بوكر رشيدة، مرجع سابق، ص 151.

[2]- تنص الفقرة 02 من المادة 394 من ق.ع.ج على أن: "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

[3]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 690.

[4]- هلالي عبد اللاه أحمد، مرجع سابق، ص87.

[5]- بلحسيني حمزة، مرجع سابق، ص 224.

[6]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 690.

[7]- التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مجلس أوروبا سلسلة المعاهدات الأوروبية رقم: 185، معتمد في 01 نوفمبر 2001، ص11.

عن طريق تعريض قطع التيار أثناء معالجة المعطيات، أو بوضع شريحة أو دائرة مطبوعة في غير مكانها الصحيح، أو التلاعب في المعطيات بتغييرها بحيث تفقد قيمتها وحقيقتها التي كانت عليها[1]، ويمكن أن يتحقق فعل إتلاف معطيات المستند الإلكتروني بوسائل أخرى كإجراء بعض التعديلات على المعلومات الموجودة في النظام بصورة مباشرة، أو من خلال إستخدام الشبكة المعلوماتية كوسيلة للوصول إلى الجهاز والعبث بما يحويه من معطيات ومستندات إلكترونية[2].

وقد أشارت المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 إلى أن يتلخص الهدف من هذا الحكم في توفير حماية لمعطيات الجهاز الإلكتروني وبرامجه، تكون مماثلة لتلك التي تتمتع بها الأشياء المادية ضد إلحاق الضرر المتعمد، وتتمثل المصلحة القانونية المحمية هنا في سلامة المعطيات أو برامج معلوماتية المخزنة وفي حسن تشغيلها أوإستخدامها.[3]

ونجد المشرع المصري قد تناول جريمة الإعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية في المادة 17 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر، تفترض هذه الجريمة قيام الجاني بأي سلوك من شأنه الإضرار بسلامة البيانات والمعلومات والنظم المعلوماتية، ويستوي لدى القانون الوسيلة المستخدمة في إحداث الإضرار بالبيانات والمعلومات فقد تكون أداة مادية أو برنامج ضار كالفيروس أو خلافه، ومن أبرز صور الضرر التي تلحق بالبيانات والمعلومات والنظم المعلوماتية والتي أشار إليها القانون هي الإتلاف والتخريب والتعطيل وتعديل المسار والإلغاء.[4]

وورد أيضًا في قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر بموجب البند (ب) من الفقرة الأولى من المادة 23، عقاب كل من أتلف أو عيب توقيعًا أو وسيطًا أو محررًا إلكترونيًا أو زور شيئًا، من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر.

2- الركن المعنوي:

الجريمة محل الدراسة جريمة عمدية يتعين لقيامها توافر القصد الجنائي العام لدى الجاني بعنصريه العلم والإرادة، فإذا أثبت الجاني إنتفاء العلاقة السببية بين السلوك الإجرامي-الدخول أو البقاء غير المصرح بهما- والنتيجة الإجرامية التي هي ذات الظرف المشدد في الجريمة، كأن يثبت أن الحذف أو تغيير المعطيات، أو أن عدم صلاحية نظام المعالجة الآلية للمعطيات

[1]- بهاء المري، مرجع سابق، ص- ص 119- 120.
[2]- بلحسيني حمزة، مرجع سابق، ص 224.
[3]- التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مرجع سابق، ص11.
[4]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 113.

للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ، إنتفى السلوك الإجرامي وإنتفى بذلك معه القصد الجنائي.[1]

وبالإضافة إلى علم الجاني بالعناصر المكونة للجريمة، يشترط المشرع أن تتجه إرادته إلى إرتكاب السلوك الإجرامي، وإذا إنتفت الإرادة إنتفى الركن المعنوي لإنعدام الإرادة.

وتطلب قانون المصري رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر بموجب المادة 17 منه لتحقق الجريمة أن يكون الإضرار بسلامة البيانات بدون وجه حق، أي أن يكون غير مشروع وهو أمر بديهي، ويكون الإتلاف غير مشروع إذا كان غير مطابقًا للقوانين أو اللوائح والتعليمات، ويرجع تقدير هذه الأمور لسلطة قاضي الموضوع يقدرها في ضوء ظروف وملابسات الجريمة.[2]

ثانيًا: جريمة إتلاف المستند الإلكتروني من خلال تخريب نظام المعالجة الآلية للمعطيات الذي يتضمنه

لقيام الجريمة محل الدراسة يشترط أن يتم إتلاف المستندات الإلكترونية من خلال تخريب نظام المعالجة الآلية للمعطيات الذي تخزن فيه تلك المستندات.

1- الركن المادي:

وهي الجريمة المنصوص عليها في المادة 05 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بعنوان: "الإعتداء على سلامة النظام" والتي نصت على أن: "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما إرتكب عمدًا وبغير حق: الإعاقة الخطيرة لإشتغال النظم المعلوماتية عن طريق إدخال بيانات معلوماتية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها"[3].

تشير المذكرة التفسيرية للإتفاقية إلى أن الهدف من النص المذكور هو تجريم الإعاقة العمدية للإستخدام الشرعي للنظم المعلوماتية بما في ذلك نظم الإتصالات السلكية واللاسلكية من خلال إستخدام معطيات معلوماتية أو التأثير عليها، وقد تمت صياغة النص بطريقة محايدة بحيث يمكن حماية جميع أنواع الوظائف بموجبه، وتتمثل المصلحة القانونية المحمية في

[1]- خثير مسعود، مرجع سابق، ص 119.

[2]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 116.

[3]-Art 05 du convention sur la cybercriminalité dispose que : « Atteinte à l'intégrité du système: Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un systéme informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques".

مصلحة مشغلي ومستخدمي النظم المعلوماتية أوالإتصالات حتى يكونوا قادرين على تشغيلها بشكل سليم.[1]

ونص المشرع الجزائري بموجب الفقرة 03 من المادة 394 مكرر من ق.ع.ج[2] على ظرف مشدد مستقل وهو مجرم لذاته وذلك إذا ترتب عن الأفعال المذكورة في الفقرتين الأولى والثانية من نفس المادة تخريب تشغيل نظام المعالجة الآلية للمعطيات، والمراد بالتخريب في الجريمة محل الدراسة إتلاف النظام وبالتالي تعطيله عن أداء مهامه، ويتضمن مصطلح التخريب كافة الأوصاف المؤدية لإفساد أو عرقلة وظائف النظام والذي يتم من خلال العبث في المعطيات التي تتعلق بنظام سيره، وبناءً على ذلك فإن التخريب أشد ضررًا من فعل التغيير، غير أن المشرع الجزائري ربط بينه وبين نتيجته المتمثلة في تعطيل النظام.[3]

والجريمة محل الدراسة من الجرائم المادية التي يتطلب لقيامها تحقق النتيجة وإلا بغيابها سينعدم الظرف المشدد، وتكون محل المتابعة فيها بموجب الدخول أو البقاء غير المصرح بهما إلى نظام المعالجة الآلية للمعطيات.[4]

وقد نص المشرع الفرنسي على هذه الجريمة بموجب الفقرة 02 من المادة 323-1 من ق.ع.ف[5] كظرف تشديد لجريمة الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، ثم نص تقريبًا على نفس الجريمة بصفة مستقلة في المادة 323-2 من نفس القانون، ويكمن الإختلاف بين الحالتين في التشريع الفرنسي في أن تعطيل نظام المعالجة الآلية للمعطيات المقترن بجريمة الدخول أو البقاء يكون من غير قصد أما جريمة تعطيله المنصوص عليها بصفة مستقلة في المادة 323-2 من ق.ع.ف هي جريمة عمدية، وعليه فإن معيار التفرقة بينهما يكمن في القصد.[6]

وفي هذا الاطار تنص المادة 323-2 من ق.ع.ف على أن :"يعاقب كل من يقوم بتعطيل أو إفساد تشغيل نظام المعالجة الآلية للمعطيات، بالسجن لمدة خمس (05) سنوات وغرامة

---

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص92.

[2]- تنص الفقرة 03 من المادة 394 من ق.ع.ج على أن: "وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة، تكون العقوبة الحبس من سنة (01) إلى ثلاثة (03) سنوات والغرامة من 100.000دج إلى 300.000 دج".

[3]- ملياني عبد الوهاب، مرجع سابق، ص 188.

[4]- نفس المرجع، ص 188.

[5]-Art 323-1 paragraphe 02 du C.P.F (LOI n°2023-22 du 24 janvier 2023 - art. 6) dispose que: «Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende».

ترجمتها:

تنص الفقرة 02 من المادة 323-1 من ق.ع.ف على أن: "إذا ترتب على ذلك حذف أو تغيير لمعطيات النظام أو تخريب لنظام تشغيل النظام، تكون العقوبة الحبس خمس (05) سنوات وغرامة قدرها 150.000 يورو".

[6]- ملياني عبد الوهاب، مرجع سابق، ص-ص 186-187.

قدرها 150 ألف يورو"[1]، ويتضح من خلال المصطلحات المستخدمة بنص المادة المذكورة أنها تشمل كل فعل من شأنه إرباك عمل نظام المعالجة الآلية للمعطيات، ويستوي أن يكون من شأن نشاط الجاني إعاقة أو إفساد نظام التشغيل أو الإرسال، ويستوي أن يؤدي نشاط الجاني إلى توقف نظام العمل بصورة دائمة أو مؤقتة، أو أن يستخدم الجاني في إرتكاب الجريمة أي وسيلة من شأنها أن تعوق سير النظام، كالإعتداء المادي على النظام أو نشر فيروسات[2] فيه[3].

ونجد المشرع المصري قد تناول جريمة الإتلاف المعلوماتي في الفقرة 02 من المادة 14 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر[4] إذا نتج عن الدخول غير المشروع وأسفر عنه أي ضرر مادي وقع على النظام المعلوماتي محظور الدخول عليه، أو الموقع الإلكتروني أو الحساب الشخصي، من خلال تغيير في محتواه أو إتلافه أو محوه أو من خلال الإضرار بمستخدم هذه المواقع أو الأنظمة من خلال نسخ محتواه أو إعادة نشر المعطيات الموجودة عليه.[5]

وورد النص على هذه الجريمة أيضًا في البند (هـ) من الفقرة الأولى من المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر، وعليه فإن السلوك الإجرامي يتحقق لكل من إخترق نظام معالجة المعطيات التي يحتوي عليها التوقيع أو الوسيط الإلكتروني أو المستند الإلكتروني، أو إعترضه أو عطله عن أداء وظيفته.

فتعطيل نظام المعالجة الآلية للمعطيات عن أداء نشاطه الذي صمم لأجله[6] لا يشترط فيه طريقة معينة لحصول الإعاقة فقد تكون بطريقة مادية أو معنوية، ومن أمثلة إعاقة النظام بطريق مادي أعمال العنف المادية على الأجهزة الإلكترونية وشبكة الإتصالات وذلك عن طريق تخريبها بكسرها أو سكب سائل عليها أو أي مادة أخرى أو حتى منع العاملين من الوصول إلى النظام، أما الإعاقة أو التعطيل بوسيلة معنوية فقد يتمثل في إدخال فيروس على

---

[1]-Art 323-2 du C.P.F (LOI n°2015-912 du 24 juillet 2015 - art. 4) dispose que: «Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende».

[2]- الفيروس عبارة عن برنامج يتراوح طوله بين 200-400 بايت، وينتقل عن طريق الأقراص والشبكات، وعندما يصل إلى حاسوب سليم فإنه يقوم بالبحث عن البرامج التي ينتهي إسمها بالإمتداد EXE- COM ثم يقوم بنسخ نفسه على هذه البرامج، وعند الإستعانة بأحد البرامج المصابة بالفيروس يبدأ الفيروس في أعماله التخريبية وفي بعض الأحيان يؤخر الفيروس عمله التخريبي إلى وقت محدد ليقوم بذلك، وللمزيد من التفصيل، ينظر: حنان ريحان مبارك المضحكي، **الجرائم المعلوماتية دراسة مقارنة**، الطبعة الأولى، 2014، منشورات الحلبي الحقوقية بيروت- لبنان، ص 128.

[3]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 373.

[4]- تنص الفقرة 02 من المادة 14 من القانون رقم: 175 لسنة 2018 السالف الذكر على أنه:" يعاقب بالحبس مدة لا تقل عن سنتين (02)، وغرامة لا تقل عن مائة ألف 100.000 جنيه ولا تجاوز مائتي ألف 200.000 جنيه أو بإحدى هاتين العقوبتين، إذا نتج عن الدخول غير المشروع على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه، إتلاف أو محو أو تغير للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي".

[5]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 99.

[6]- بن شهرة شول، مرجع سابق، ص98.

البرنامج، أو تعديل كلمة السر أو كيفية أداء النظام لوظيفته بوسيلة تؤدي على سبيل المثال لأن يتباطأ النظام عن أداء وظيفته المعلوماتية.[1]

ويقصد بالإفساد أو التعييب كل فعل وإن لم ينجم عنه التعطيل لكنه يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للإستعمال، وذلك من خلال تقديم نتائج غير تلك التي ينبغي الحصول عليها.[2]

أما بخصوص تقنيات الإفساد والتعييب فهي متعددة منها القنبلة المعلوماتية بحيث يدخل بواسطتها مجموعة من المعطيات تتكاثر داخل نظام المعالجة الآلية للمعطيات وتجعله غير صالح للإستعمال، فوظيفة الفيروس هو القيام بتغيير غير محسوس في البرنامج أو المعطيات حيث تجعل مخرجات النظام غير تلك التي كان من المفترض أن يصورها.[3]

وعليه فإن الإخلال المتعلق نظام المعالجة الآلية للمعطيات بالمفهوم السابق يختلف عن العرقلة أو التعطيل، فهو لا يتسبب إلى توقف نظام عن عمله أو إتلافه لكن يجعله غير قادر على الإستعمال الصحيح والسليم، وتتأثر به الأجهزة الإلكترونية وكذا البرامج والأنظمة على حد سواء، ويتم تنفيذ هذا النوع من التعطيل بعدة تقنيات وأساليب الإعاقة أو العرقلة إلا أن النتيجة تختلف بإختلاف السلوك الجرمي.[4]

ويستوي في هذه الجريمة أن يكون من شأن نشاط الجاني أن يؤدي إلى توقف نظام المعالجة الآلية للمعطيات عن العمل بصورة دائمة أو مؤقتة، كما يستوي أن تكون الإعاقة أو الإفساد كلية أو جزئية.[5]

2- الركن المعنوي:

تعد الجريمة محل الدراسة من الجرائم العمدية التي تتطلب توافر القصد الجنائي العام لدى الجاني والمتمثل في عنصري العلم والإرادة، ويقتضي ذلك أن يكون الجاني عالمًا بالعناصر المكونة للجريمة، بأن يعلم بأنه يقوم بتخريب تشغيل نظام المعالجة الآلية للمعطيات أو بإعاقة أو إفساد النظام، وأن تتجه إرادته إلى إرتكاب السلوك الإجرامي.

ولا تتطلب هذه الجريمة قصدًا جنائيًا خاصًا مثل قصد الإضرار بالغير، ولذلك إذا قام الشخص الذي يتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد نظام المعالجة الآلية

[1]- بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، أطروحة الدكتوراه علوم، كلية الحقوق، جامعة الجزائر 01 – بن يوسف بن خدة-، 2018/2017، ص 170.

[2]- نفس المرجع، ص 171.

[3]- بن شهرة شول، مرجع سابق، ص99.

[4]- ملياني عبد الوهاب، مرجع سابق، ص 190.

[5]- سحر سعد عبد السميع محمد، مرجع سابق، ص 202.

للمعطيات نتيجة لخطأ في التشغيل أو التعامل مع المعطيات، ينتفي القصد الجنائي لديه ولا يسأل عن هذه الجريمة. [1]

والجريمة وفقًا للمادة 323-2 من ق.ع.ف بوضعها الحالي تتحقق بتوافر قصد الجنائي العام بعكس ما كان عليه الحال في نص القانون رقم: 88-19 بشأن الغش المعلوماتي، حيث كانت تتطلب توافر قصد خاص وهو نية الإضرار بالغير والذي عبر عنها المشرع بأن يكون الفعل الإجرامي وقع من الجاني دون مراعاة لحقوق الغير، وهو الأمر الذي إنتقده الفقه وإستجاب المشرع الفرنسي وعدل عن تطلب هذا القصد الخاص، وقد إرتبطت جريمة الإتلاف وإعاقة نظام المعالجة الآلية للمعطيات غير العمدية بالدخول أو البقاء بطريق الغش في النظام وتشدد متى نتج عنه محو أو تعديل المعلومات أو إفساد للنظام. [2]

الفرع الرابع: جريمة إستخدام المعطيات كوسيلة للإعتداء على المستند الإلكتروني

في إطار حماية سرية المعطيات الإلكترونية ولغرض توفير الثقة لدى المتعاملين في البيئة الرقمية وسع المشرع الحماية الجنائية لأنظمة المعالجة الآلية للمعطيات، بحيث امتدت هذه الحماية لتشمل أيضًا المعطيات أو المعلومات المرتبطة بهذه الأنظمة[3]، وهي الجريمة المنصوص عليها في المادة 06 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بعنوان: "إساءة إستخدام الأجهزة"[4]، والفقرة الأولى من المادة 09 من

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 204.

[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 375.

[3]- بلحسيني حمزة، مرجع سابق، ص 288.

[4] -Art 06 du convention sur la cybercriminalité dispose que : « Abus de dispositifs:

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a. la production, la Vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition.

i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2-5 ci-dessus;

ii. d'un mot de passe, d'un code d'accés ou des données informatiques similaires permettant d'accéder à tout ou partie d'un systéme informatique.

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2-5; et.

b. la possession d'un élément visé aux paragraphes a 1 ou 2 ci-dessus dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2-5. Une Partie peu exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2. Le présent article ne saurait être interpréter comme imposant une responsabilité pénale lorsque la production, la vente, L'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe I du présent article n'a pas pour but de commettre une infraction établie conformément à l'Article 2 à 5 de la présente Convention, comme en cas d'essais autorisés ou de protection d'un systéme informatique .

3. Chaque partie peut se réserver le droit de ne pas appliquer le paragraphe I du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1 a 2».=

الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بعنوان: "جريمة إساءة إستخدام وسائل تقنية المعلومات"[1]، وفي البند 01 من الفقرة الأولى من المادة 394 مكرر2 من قانون العقوبات الجزائري[2]، والتي تقابلها المادة 323-3-1 من قانون العقوبات الفرنسي[3].

=ترجمتها:

تنص المادة 06 من الإتفاقية الأوروبية الخاصة بالجرائم المعلوماتية الموقعة في بودابست عام 2001 على أن: "إساءة إستخدام الأجهزة:

1- يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات يرى أنها ضرورية لتجريم، تبعًا لقانونه الداخلي، القيام عمدًا، ودون حق بما يلي:

أ - إنتاج أو بيع، أو الحصول من أجل الإستخدام، أو إستيراد، أو نشر، أو أي أشكال أخرى للوضع تحت التصرف.

1- أي جهاز، يحتوي على برنامج معلوماتي، مصمم أو موفق بشكل أساسي لغرض إرتكاب إحدى الجرائم المنصوص عليها وفقاً للمواد من 2 - 5 السابق الإشارة إليها.

2- كلمة المرور، أو شفرة الدخول، أو أي بيانات مماثلة تسمح بالولوج إلى كل أو إلى جزء من نظام الحاسوب.

بنية إستخدامها لغرض إرتكاب جريمة من الجرائم المشار إليها في المواد من 2-5.

ب - حيازة أي عنصر من العناصر المشار إليها في البندين أ- 1، أ - 2 بنية إستخدامه في إرتكاب أي جريمة من الجرائم الواردة في المواد 2 - 5.

ويمكن لأي طرف أن يشترط في قانونه الداخلي وجود بعض هذه العناصر من أجل تقرير المسؤولية الجنائية.

2- هذه المادة لا يجب أن تفسر على أنها تفرض مسؤولية جنائية، حينما يكون إنتاج، أو بيع، أو الحصول من أجل الإستخدام، أو الإستيراد، أو النشر، أو الأشكال الأخرى للوضع تحت التصرف المشار إليها في الفقرة الأولى من هذه المادة، ليس بهدف إرتكاب جريمة، وفقًا للمواد 2 - 5 من هذه الإتفاقية، مثال ذلك حالة الإختبار المصرح به أو حماية نظام الحاسوب.

3- كل طرف يمكن أن يحتفظ بحقه في تطبيق الفقرة الأولى من هذه المادة، بشرط ألا يحمل هذا التحفظ بيع أو توزيع أو وضع تحت التصرف، لأي عنصر من العناصر المشار إليها في البندين أ- 1، أ- 2".

[1]- تنص الفقرة الأولى من المادة 09 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن:"جريمة إساءة إستخدام وسائل تقنية المعلومات: إنتاج أو بيع أو شراء أو إستيراد أو توزيع أو توفير:
أ- أية أدوات أو برامج مصممة أو مكيفة لغايات إرتكاب الجرائم المبينة في المادة 06 إلى المادة 08.
ب- كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة، يتم بواسطتها دخول نظام معلومات ما، بقصد إستخدامها لأية من الجرائم المبينة في المادة 06 إلى المادة 08".

[2]- تنص الفقرة الأولى من المادة 394 مكرر2 من ق.ع.ج على أن: "يعاقب بالحبس من سنة (01) إلى خمس (05) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدًا وعن طريق الغش بما يأتي:
1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة، عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم".

[3]-Art 323-3-1 du C.P.F (LOI n°2013-1168 du 18 décembre 2013 - art. 25) dispose que: « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée».

ترجمتها:

تنص المادة 323-3-1 من ق.ع.ف على أن:"يعاقب على الأفعال التي ترتكب -بدون وجه حق- الإستيراد أو الحيازة أو العرض أو البيع أو توفير أي معدات أو أدوات أو برامج معلوماتية أو أي معطيات مصممة أو مخصصة، لإرتكاب واحدة أو أكثر من الجرائم المنصوص عليها في المواد 323-1 إلى 323-3 بالعقوبات المقررة للجريمة نفسها، أو للجريمة الأشد في عقوبتها".

أولًا: الركن المادي لجريمة إستخدام المعطيات كوسيلة للإعتداء على المستند الإلكتروني

إن الأفعال التي جاء بها البند 01 من الفقرة الأولى من المادة 394 مكرر2 من ق.ع.ج من شأنها أن تجعل من المعطيات قابلة للإستعمال في إرتكاب الجريمة الماسة بالمستند الإلكتروني، وكأن الأمر يتعلق بتهيئة المعطيات من خلال مراحل تبدأ بتصميم هذه المعطيات والبحث فيها ثم تجميعها، وصولًا إلى جعلها في متناول وتحت تصرف الغير من خلال نشرها أو الإتجار بها أو توفيرها.[1]

لا يشترط أن تقع هذه الأفعال مجتمعة لكي يقوم الركن المادي للجريمة، بل يكفي لتحقق النشاط الإجرامي قيام الجاني بإحدى هاته الأفعال والتي تتمثل في:

1- التصميم:

وهو عملية إعداد معطيات صالحة لإستخدامها في إرتكاب الجريمة وذلك عن طريق إصطناعها وإخراجها للوجود أو إنتاجها، ويعد هذا الفعل أي عملية في سلسلة التعامل في المعطيات التي تدخل ضمن لائحة الوسائل التقنية والمعلوماتية المستخدمة في جرائم الإعتداء على الأنظمة المعالجة الآلية للمعطيات وما تحتويه من المستندات الإلكترونية، وغالبًا ما يقوم المختص في مجال التقنية بعملية التصميم كالمبرمج ومصمم البرامج، فعلى سبيل المثال برنامج القنبلة المعلوماتية الذي يعد برنامج يصمم ويثبت بداخل نظام المعالجة الآلية للمعطيات وتكون غايته بعد ذلك محو وتدمير المعطيات التي يتضمنها المستند الإلكتروني.[2]

2- البحث:

يقصد البحث في كيفية تصميم المعطيات وإعدادها وليس مجرد البحث عن هذه المعطيات المتعلقة بالمستند الإلكتروني، ولهذا جاءت عبارة البحث بعد عبارة التصميم مباشرة وإن كان النص قد جاء عامًا.[3]

3- التجميع:

وهي عملية تستند إلى جمع أكبر قدر ممكن من المعطيات المخزنة أو المعالجة في أنظمة المعالجة الآلية للمعطيات أوالمرسلة منه، لكي يتمكن الجاني بعد ذلك من إستخدامها في إرتكاب إحدى الجرائم الأخرى مثل التلاعب في المعطيات أو إتلافها.[4]

وتعدد المعطيات قد يؤدي إلى رفع درجة الخطورة التي تشكلها، ولا شك أن من يحوز المعطيات لا يعد خطرًا بقدر ما يسببه من يقوم بتجميع هذه المعطيات، إذ إن التجميع يعبر عن

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 706.
[2]- نفس المرجع، ص 707.
[3]- بن مكي نجاة، مرجع سابق، ص 194.
[4]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 708.

خطورة الفاعل ويشير إلى إمكانية إرتكابه أو تسهيله لإرتكاب الجرائم محل الدراسة[1]، ومن الأدوات والتقنيات الحديثة التي تم تصميمها لتجميع المعطيات نجد ملفات التجسس فيما يتعلق بالمعطيات المخزنة، أو برامج الإعتراض فيما يتعلق بالمعطيات المرسلة[2].

والملاحظ أن المشرع الفرنسي فقد إصطلح عليها بمصطلح الحيازة (Détenir) بينما الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 فضلت مصطلح "الحصول من أجل الإستخدام"، إلا أن المصطلح الذي إعتمده المشرع الجزائري يعتبر أكثر دقة على أساس أن التجميع يقتضي وجود حيازة لعدد كبير من المعلومات دون وجود نية إستخدامها، فمجرد توافرها لدى الجاني يكون قد إرتكب الجريمة المعاقب عليها في الفقرة الأولى من المادة 394 مكرر من ق.ع.ج.[3]

4- التوفير:

يقصد بهذا السلوك جعل المعطيات في متناول الغير ووضعها تحت تصرفه، وجعلها متاحة لمن يرغب في إستخدامها لإرتكاب الجرائم الماسة بالمستند الإلكتروني، وكذا عرضها عليه وتقديمها له، ولا تقتصر هذه العملية على من قام بتجميعها بل تتعدى إلى أشخاص آخرين، وبناءً على ذلك تزداد خطورة هذه العملية بإزدياد هؤلاء.[4]

وقد إستعملت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 عبارة: "أي أشكال أخرى للوضع تحت التصرف"، ومن قبيل ذلك إتاحة شفرة الولوج أو كلمة المرور التي تسمح بالدخول إلى نظام المعالجة الآلية للمعطيات غير المصرح به، وقد توسع القضاء الفرنسي في تفسير معنى "التوفير" ليشمل الإفشاء أو الكشف العلني للثغرات الأمنية في النظام، وأيضًا إفشاء المعطيات إلى الغير لما تكون تحت سيطرته بإعتباره المسؤول عن النظام، ليتم بعد ذلك إستخدامها في إرتكاب إحدى الجرائم الماسة بالمستند الإلكتروني.[5]

5- النشر:

يقصد بعملية النشر إذاعة المعطيات الإلكترونية التي من الممكن إستخدامها في إرتكاب الجريمة وتمكين الغير من الإطلاع عليها، وتتم عملية النشر بأي وسيلة كانت لتشمل كل نشاط الذي من شأنه أن يؤدي إلى نقل المعطيات إلى الغير، وهو سلوك ينطوي على درجة عالية من الخطورة كونه قادرًا على نقل المعطيات إلى علم أكبر عدد ممكن من الأشخاص ممن ليس لهم الحق في الإطلاع عليها[6]، مما يجعل إحتمال إستعمال هذه المعطيات في العديد من الجرائم الماسة بالمستند الإلكتروني، وهو الأمر الذي يحاول المشرع علاجه من خلال تجريمه لهذه

---

[1]- بن مكي نجاة، مرجع سابق، ص-ص 194-195.

[2]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 708.

[3]- ملياني عبد الوهاب، مرجع سابق، ص 198.

[4]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 709.

[5]- نفس المرجع، ص 709.

[6]- نفس المرجع، ص-ص 709- 710.

التعاملات، وذلك للتضييق ما أمكن من دائرة الأشخاص الذين يحصلون على هذه المعطيات بمقابل[1].

6- الإتجار:

الإتجار هو تقديم المعطيات للغير بمقابل، ويشمل كل أنواع التعاملات التي تقع على المعطيات الصالحة لإرتكاب الجرائم محل الدراسة وتقدم وفقها المعطيات نظير مقابل معين، والفرق بين هذا السلوك وسلوك التوفير أن هذا الأخير يفهم منه أنه تقديم للمعطيات قد يكون دون مقابل معين بينما يفهم من الإتجار تقديم المعطيات بمقابل دائمًا، والمشرع أراد بالنص على كليهما أن يشمل كل أنواع التعاملات التي تقع على المعطيات سواء كانت بمقابل أم بغير مقابل.[2]

ويستوي في ذلك أن يحقق الجاني هدفًا شخصيًا أو مصلحة للغير والذي قد يكون مالك أو صاحب المعالجة الآلية للمعطيات نفسه أو أي شخص مستأجر أو منتفع به وفي الخلاصة كل من له مصلحة في تلك المعطيات، والملاحظ أن لم يشترط المشرع الجزائري في البند 01 من الفقرة الأولى من المادة 394 مكرر2 من ق.ع.ج بأن تكون المعطيات مخزنة داخل النظام نفسه، مما يعني أن الحماية القانونية تشمل كذلك المعطيات المعالجة آليًا المخزنة بواسطة أي دعامة، ويستوي في ذلك أن يتم إلتقاط المعلومات والوصول إليها عن طريق التجسس المعلوماتي أو بطرق الإحتيال، وتكتسي عمليات التجسس خطورة كبيرة سيما حال إستهدافها معطيات سرية تجارية أو عسكرية أو غيرها والتي تعتبر ظرفًا مشددًا في نظر المشرع الجزائري.[3]

إلا أننا نجد المشرع الفرنسي قد إستعمل مصطلحًا آخر وهو الإستيراد (D'importer)، فهو يعد تقديم المعلومات سلوك جرمي سواء كان مقابل أجر أو بدونه، في حين الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 تضمن البيع والإستيراد بينما يتصور وقوع الإتجار بالبيع والإستيراد وكذا الشراء، لهذا إتجه المشرع الجزائري نحو التوسع في تجريم التعامل في المعلومات التي يمكن أن ترتكب بها الجرائم محل الدراسة، وذلك بناءً على رغبته في الوقاية المسبقة للحد من هذه الجرائم وضمان لغياب النص التشريعي الذي يؤدي إلى إفلات الجاني من العقاب.[4]

ثانيًا: الركن المعنوي لجريمة إستخدام المعطيات كوسيلة للإعتداء على المستند الإلكتروني

الجريمة محل الدراسة من الجرائم العمدية التي تتطلب لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة لدى مرتكبها، بقيام العلم لدى الجاني بعناصر المكونة للجريمة، بأن يعلم بأنه يقوم بإحدى السلوكات المنصوص عليها على سبيل الحصر في البند 01 من الفقرة

[1]- بن مكي نجاة، مرجع سابق، ص 195.
[2]- نفس المرجع، ص 196.
[3]- زيبحة زيدان، مرجع سابق، ص 63.
[4]- ملياني عبد الوهاب، مرجع سابق، ص 199.

الأولى من المادة 394 مكرر2 من ق.ع.ج من تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار بالمعطيات المخزنة أو المعالجة آليًا أو المرسلة عن طريق نظام المعالجة الآلية للمعطيات، وأن فعله يشكل جرمًا معاقبًا عليه، ثم على الرغم من علم الجاني بذلك تنصرف إرادته لإتيان فعل أو أكثر من أفعال المنصوص عليها سابقًا.

وتطلبت البعض من التشريعات المقارنة لقيام الركن المعنوي لابد من توافر القصد الخاص وهو ما عبرت عنه بمصطلح "نية الغش" أو بمصطلح "عن طريق الغش"، وعليه لا يكفي أن يكون الجاني قد تصرف بطريقة عمدية بل يجب أن تتوفر لديه نية الغش لكي تعد إحدى السلوكيات المذكورة من صميم الإجرام المعلوماتي[1]، ولم ينص المشرع الجزائري صراحة على إشتراط القصد الجنائي الخاص لقيام الركن المعنوي لهذه الجريمة إذ يكفي لقيامها توفر القصد الجنائي على النحو السابق بيانه، لكن بالرجوع إلى المادة 06 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 نجد إنها إشترطت صراحة لتوقيع العقوبة على التعامل في المعطيات أو البرامج الصالحة لإرتكاب جريمة أن يكون هذا التعامل بنية إستخدامها لهدف إرتكاب إحدى الجرائم الواردة في المواد 02،05 من الإتفاقية[2].

الفرع الخامس: جريمة التعامل بالمعطيات الواردة في المستند الإلكتروني

جريمة التعامل بالمعطيات الواردة في المستند الإلكتروني هي الجريمة المنصوص عليها في البند 02 من الفقرة 02 من المادة 394 مكرر2 من قانون العقوبات الجزائري التي تنص على أن: "يعاقب بالحبس من شهرين (02) إلى ثلاث (03) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدًا وعن طريق الغش بما يأتي: ...2- حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

أولًا: الركن المادي لجريمة التعامل بالمعطيات الواردة في المستند الإلكتروني

لا يشترط لقيام الجريمة أن تقع هذه الأفعال مجتمعة معًا، بل يكفي لتحقق النشاط الإجرامي قيام الجاني بإحدى هاته الأفعال والتي تتمثل في:

1- الحيازة:

يتمثل فعل الحيازة[3] في السيطرة الإرادية للشخص على الشيء تمكنه من الإنتفاع بالمعلومات أو إستعمالها أو تعديلها أو نقلها أو توجيهها أو إتلافها مع توفر لديه نية إحتباسها مع

[1]- بلحسيني حمزة، مرجع سابق، ص 292.

[2]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص-ص 710-711.

[3]- أشارت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على فعل الحيازة في الفقرة 02 من المادة 09 منها على أن: "حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد إستخدامها لغايات إرتكاب أي من الجرائم المذكورة في المادة 06 إلى المادة 08".

علمه بذلك بصفة مؤقتة أو دائمة، وهي أيضًا رابطة واقعية بين الشخص والمال المنقول تتيح السيطرة على مال منقول سيطرة مستقلة مقترنة بنية التملك والإحتباس[1]، أي أن يمارس الشخص عمل مادي يمس المال من دون رقابة من شخص آخر له سلطة قانونية أعلى على المال بمقتضى حق من الحقوق، وعليه فالحيازة وفقًا للقانون الجنائي لا تعد حقًا أو مركزًا قانونيًا، بل هي مركز واقعي قد تكون مشروعة مستندة لسبب صحيح كما قد تكون غير مشروعة[2].

غير أن لا يعني حيازة الجاني للمعطيات الواردة في المستند الإلكتروني المتحصلة من جريمة ما أنها تخرج عن سيطرة المجني عليه مالك لهذه المعطيات بصورة كلية، وكل ما في الأمر أن هذا الأخير يفقد ميزة الإستئثار بها كونها ليست منقولًا ماديًا، وأن تكون الحيازة لهذه المعطيات دائمًا غير مشروعة ذلك لأن عدم مشروعيتها مستندة إلى كونها تم الحصول عليها بطريقة غير مشروعة، أي بدون علم ورضا صاحبها الشرعي[3] أو بعلمه وبدون رضاه.

2- الإفشاء:

إستخدم المشرع الجزائري مصطلح "الإفشاء" للدلالة على إطلاع الغير على المعلومة الواردة بالمستند، وذلك بأي طريقة كانت سواء شفاهة أو بالكتابة أو بالإشارة[4]، وبناءً على ذلك يفترض الإفشاء إنتقال المعلومة من حيازة الجاني إلى الغير وهذا هو الفرق بين الإفشاء والحيازة، حيث أن الحيازة ينحصر وجود المعلومات لدى الحائز دون تقديمها إلى الغير، في حين أن الإفشاء يتم نقل المعلومات من الحائز لها إلى الغير، ولا يشترط أن ينتمي هذا الأخير إلى فئة معينة[5].

وتجدر الإشارة إلى أن المشرع الجزائري إستخدم في المادة 394 مكرر2 من ق.ع.ج مصطلح "المعطيات" المتحصل عليها ولم يستخدم مصطلح "السر" الواردة في المادة 301 من نفس القانون[6]، ذلك لأنه يعتبر كل المعطيات التي يتم الحصول عليها نتيجة الدخول أو البقاء غير المصرح بهما في نظم المعالجة الآلية للمعطيات أن المتحصل عليها غير مصرح له بالدخول إلى النظام.[7]

---

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 713.

[2]- ملياني عبد الوهاب، مرجع سابق، ص 200.

[3]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 713.

[4]- بلحسيني حمزة، مرجع سابق، ص 282.

[5]- ملياني عبد الوهاب، مرجع سابق، ص-ص 200-201.

[6]- الأطباء، والجراحون، والصيادلة، والقابلات، وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة، سواء كانت دائمة أو مؤقتة، على أسرار أدلي بها إليهم، إذا أفشوا تلك الأسرار في غير الحالات التي يوجب عليهم فيها القانون إفشاءها أو يصرح لهم بذلك.

[7]- بلحسيني حمزة، مرجع سابق، ص 282.

3- النشر:

تتحقق الجريمة محل الدراسة بهذا السلوك عندما يتم الحصول على المعطيات الواردة في المستند الإلكتروني بطريقة غير مشروعة بواسطة الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات المتضمن لهذه المعطيات، ويقوم الجاني بإذاعتها وتمكين الغير من العلم بها والإطلاع عليها بأي وسيلة تحقق هذه الغاية.[1]

ولم يحدد المشرع الجزائري وسيلة معينة للنشر، وبناءً على ذلك يستوي أن يتم النشر بواسطة أي دعامة تحمل هذه المعطيات أو عن طريق المخرجات الإلكترونية أو على أي وسيلة آخرى، خصوصًا أن الوسائل التقنية الحديثة ساهمت على السرعة في النشر وبكفاءة عالية للمعلومات المتحصل عليها من جرائم الإعتداء على نظام المعالجة الآلية للمعطيات.[2]

4- الإستعمال:

يتحقق السلوك الإجرامي للجريمة محل الدراسة في إستعمال المعطيات الواردة بالمستند الإلكتروني والمخزنة فيه لأي غرض كان ومهما كان الهدف منه ونوعه، ويتحقق هذا السلوك في إختراق نظام المعالجة الآلية للمعطيات والولوج إليه بطريقة غير مشروعة والحصول على هذه المعطيات، بإستعمالها أي الإنتفاع بها وإستغلالها بطريقة غير مشروعة.[3]

ثانيًا: الركن المعنوي لجريمة التعامل بالمعطيات الواردة في المستند الإلكتروني

ورد المشرع الجزائري في الجريمة محل الدراسة مصطلحي "عمدًا" و"عن طريق الغش" مما تقتضي أنها من الجرائم العمدية التي تتطلب لقيامها توافر لدى مرتكبها القصد الجنائي العام بعنصريه العلم والإرادة، بقيام العلم لدى الجاني بعناصر المكونة للجريمة بأن يعلم بأنه يقوم بإحدى السلوكات المنصوص عليها في البند 02 من الفقرة 02 من المادة 394 مكرر2 من ق.ع.ج من حيازة أو إفشاء أو نشر أو إستعمال المعطيات الواردة بالمستند الإلكتروني لأي غرض كان من شأنه أن يشكل جرمًا معاقبًا عليه، وأن سلوكه يكون وسيلة لإرتكاب جرائم التعامل بالمعطيات الواردة في المستند الإلكتروني، ثم تنصرف إرادته الحرة للتعامل في هذه المعطيات رغم علمه هذا.

المطلب الثاني: العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني

نصت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في المادة 11 منها على القواعد العامة المتعلقة بالمساهمة الجنائية والعقوبات بشأن الجرائم المشار إليها في المواد من 02 إلى 10، وقد أوجبت الإتفاقية على الدول الأعضاء إتخاذ تدابير تشريعية

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 715.
[2]- ملياني عبد الوهاب، مرجع سابق، ص 201.
[3]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 715.

للنص على المسؤولية عن الشروع والتدخل والتحريض في إرتكاب هذه الجرائم أو ما تختاره الدولة منها، وذلك بغرض وجود رادع عام لما لهذه الجرائم من تأثير شديد على إقتصاديات الدول، وكذلك النص على مسؤولية الأشخاص المعنوية عن الأفعال التي ترتكب لمصلحة الشخص المعنوي من قبل أي شخص الذي يتصرف لمصلحته، سواء كان إستنادًا إلى تمثيل قانوني أو بإعتباره مناطًا به إتخاذ القرار عن الشخص القانوني أو لأنه خاضع لسلطته بما في ذلك أفعال التحريض والتدخل والمساعدة الجنائية، وكذلك مسؤولية الرؤساء عن غياب أو تخلف الرقابة والإشراف والتحكم بتصرفات الأشخاص المعنيين بالعمل.[1]

فقد خصصنا المطلب الثاني إلى العقوبات الأصلية والتكميلية المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني في (الفرع الأول)، بينما إلى أحكام العقاب على الإتفاق الجنائي والشروع فيها في (الفرع الثاني).

الفرع الأول: العقوبات الأصلية والتكميلية المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني

سنتطرق إلى العقوبات الأصلية ثم إلى العقوبات التكميلية المقررة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني.

أولًا: العقوبات الأصلية المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني

يقصد بالعقوبات الأصلية هي تلك التي يجوز الحكم بها دون أن تقترن بها أي عقوبة أخرى، ومن هذه العقوبات ماهو مقرر للشخص الطبيعي ومنها ماهو مقرر للشخص المعنوي.

1- العقوبات الأصلية المقررة للشخص الطبيعي:

سنتناول أولًا موقف مختلف التشريعات المقارنة، ثم ننتقل إلى بيان موقف المشرع الجزائري.

أ- موقف المشرع الفرنسي:

كانت اللبنة الأولى لتنظيم وحماية نظام المعلوماتية في فرنسا سنة 1978 حيث صدر القانون رقم: 78-17 الصادر في 06 جانفي 1978 الذي يتعلق بالحريات والمعلوماتية، وقد عالج هذا التشريع مسألة تخزين المعطيات في الحاسوب وأنواع هذه المعطيات ومدتها وتلك التي لا يجوز تخزينها وكذلك الجهة المختصة بالرقابة على تنفيذ هذا القانون، وقد أنشأ بموجب هذا القانون لجنة تسمى "اللجنة القومية للمعلوماتية والحريات" وهي تختص بإجراء رقابتين سابقة ولاحقة للتأكد من الحماية الكاملة للحريات في ظل النظم المعلوماتية.[2]

[1]- محمود سعد عبد المجيد، مرجع سابق، ص 411.

[2]- مثنى سعد السوداني، مرجع سابق، ص 146.

وعمل هذه اللجنة يقوم على تطبيق أحكام قانون المعلوماتية وإبلاغ ذوي الشأن بحقوقهم وواجباتهم والتحقق من إحترام نظام المعلومات لأحكام القانون وإصدار الإذن (الترخيص) السابق للإدارة من أجل إنشاء نظم المعلومات أو تلقي الإخطارات من الأفراد في هذا الخصوص، وهذه اللجنة مستقلة في عملها تعد تقريرًا سنويًا عن أعمالها يقدم لرئيس الدولة وللبرلمان وأعضاء اللجنة الذين لا يخضعون لأي تعليمات أو توجيهات في ممارسة أعمالهم، لذلك يطلق عليها أنها سلطة إدارية مستقلة.[1]

ولكنه إقتصر قانون 06 جانفي 1978 المتعلق بالمعلوماتية والحريات على المعلومات الإسمية والحريات ولهذا فإن جميع مواده إقتصرت على حماية الحياة الشخصية للأفراد، كما توسع القضاء الفرنسي في حماية حرية التعبير على حماية المعطيات ذات الخاصية الشخصية.[2]

ودعا رئيس الوزراء الفرنسي سنة 1984 إلى تشكيل لجنة لإقتراح الحلول المناسبة لمواجهة الجرائم الناشئة عن الحواسيب الإلكترونية وخطورتها على الحياة الخاصة والحريات العامة والحريات الفردية، كما طلب رئيس الجمهورية من الحكومة أن تقدم إقتراحًا بمشروع قانون خلال ستة (06) أشهر لمواجهة هذه الظاهرة، وفي 27 جوان 1985 شكلت لجنة برئاسة الأمين العام لمجلس الدولة الفرنسي لبحث آثار خطورة الحواسيب الإلكترونية على الحياة الخاصة، كما أجريت مناقشات مستفيضة في الجمعية الوطنية الفرنسية إنتهت بإصدار هذا القانون، وقد أقر هذا القانون المسؤولية الجنائية والمدنية للشخص المتعسف في المعالجة الآلية للبيانات الإسمية لو سببت معالجته الخطأ ضررًا لشخص آخر، وأكدت المادة الأولى من هذا القانون الأهداف المرجوة من وراء إصداره بقولها: "إن المعلوماتية لابد وأن تكون في خدمة المواطن، ولا ينبغي لها أن تستخدم كوسيلة للإعتداء على الشخصية الإنسانية ولا على حقوق الإنسان ولا الحياة الخاصة ولا على الحريات الفردية أو العامة".[3]

وفي سنة 1985 تقدم وزير العدل وقتئذ بمشروع قانون جديد للعقوبات أضاف إلى الكتاب الثالث منه بابًا رابعًا بعنوان جرائم المعلوماتية مكونًا من ثماني مواد وهي من 307-1 إلى 307-8، والتي كانت تجرم إلتقاط البرامج أو المعطيات أو أي شيء آخر من المنظومة المعلوماتية عمدًا، وإستخدام أو نقل أو إنتاج برامج أو معطيات أو أي عنصر من عناصر المنظومة دون موافقة من لهم الحق عليه، وتخريب أو إتلاف أي جزء من نظام المعالجة الآلية للمعطيات، وكذلك إعاقته عن أداء وظيفته، والحصول على فائدة غير مشروعة عن طريق الإستخدام غير المشروع لنظام المعالجة الآلية للمعطيات، ومنها بالتأكيد حماية التوقيع الإلكتروني والمستند الإلكتروني والمعاملات الإلكترونية من التزوير الذي يمكن أن يقع عليها،

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 158.

[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 311.

[3]- نفس المرجع، ص 312.

إلا أن هذا المشروع على الرغم من أنه قد بذل فيه جهد كبير إلا أنه لم ير النور إذ أنه لم يتم إقراره.[1]

وفي 05 أوت 1986 تقدم إلى الجمعية الوطنية الفرنسية النائب Jacque codfrain مع بعض النواب من أعضاء حزب التجمع من أجل الجمهورية بإقتراح مشروع قانون فى الغش المعلوماتي، وكان هذا الإقتراح مجرد تعديل وتطويع بعض الجرائم التقليدية فى نطاق الأموال مثل السرقة والنصب وخيانة الأمانة والإخفاء والتخريب والإتلاف والتزوير وإستعمال المستندات المزورة، ولكن عند نظر البرلمان الفرنسي لهذا الإقتراح دارت حوله مناقشات طويلة ومعمقة وأدخلت عليه تعديلات جوهرية، وتم إقراره في شكل جديد يختلف عن شكله الأول الذي قدم به بحيث إقترب من الإقترح الذي سبق الإشارة إليه في مشروع قانون العقوبات لسنة 1985 وكان ذلك في 22 ديسمبر1987، وأصبح قانونًا منذ 05 جانفي 1988 وحمل رقم: 88-19 بشأن الغش المعلوماتي وأدمج هذا القانون في قانون العقوبات الفرنسي وأصبح يشكل بابًا جديدًا هو الباب الثالث من الكتاب الثالث من القسم الثاني من قانون العقوبات والمتعلق بالجنايات والجنح المتعلقة بآحاد الناس، حيث يعالج الباب الأول: "الجنايات والجنح ضد الأشخاص" ويعالج الباب الثاني:"الجنايات والجنح ضد الملكية".[2]

وقد شمل المواد من 462-2 حتى 462-4 كما يلي:

المادة 462-2 من ق.ع.ف تنص على أن: "يعاقب بالحبس من شهرين (02) إلى سنة (01) وبغرامة تتراوح من ألفين 2.000 فرنك إلى خمسون ألف 50.000 فرنك أو بإحدى هاتين العقوبتين، كل من قام بالدخول أو البقاء كليًا أو جزئيًا داخل نظام المعالجة الآلية للمعطيات بدون تصريح، وإذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل في المعطيات المخزنة في النظام سواء بالإتلاف تكون العقوبة الحبس لمدة تتراوح ما بين شهرين (02) إلى سنتين (02) والغرامة التي تتراوح ما بين عشرة ألاف 10.000 فرنك إلى مائة ألف 100.000 فرنك".[3]

ونصت المادة 462-3 من ذات القانون على أن: "يعاقب بالحبس لمدة تتراوح من ثلاثة (03) أشهر إلى ثلاثة (03) أعوام وبالغرامة من عشرة آلاف 10.000 فرنك إلى مائة ألف

[1]- مثنى سعد السوداني، مرجع سابق، ص-ص 148-149.

[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص 159.

[3]-Art 462-2 du Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dispose que: « Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois a un an et d'une amende de 2 000 F a 50 000 F ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans les systèmes, soit une altération du fonctionnement de ce système, l'emprisonnement sera de 2 mois a 2 ans et l'amende de 10 000 F a 100 000 F».

100.000 فرنك أو بإحدى هاتين العقوبتين، كل من أضر أو زيف بطريقة عمدية تترتب عليه أضرارًا بحقوق الغير في نظام المعالجة الآلية للمعطيات".[1]

المادة 442-4 من نفس القانون تنص على أن: "يعاقب بالحبس لمدة تتراوح من ثلاثة (03) أشهر إلى ثلاثة (03) سنوات وبالغرامة من ألفين 2.000 فرنك إلى خمسمائة ألف 500.000 فرنك أو بإحدى هاتين العقوبتين، كل من قام بإدخال معطيات إلى نظام المعالجة الآلية معين أو تعديل أو إلغاء بث المعلومات التي يحتويها بطريقة مباشرة أو غير مباشرة وأضر بحقوق الغير".[2]

ثم قام المشرع الفرنسي بإصدار قانون العقوبات الفرنسي الجديد رقم: 1336 لسنة 1992 والذي بدأ به في الأول من مارس سنة 1994 بتضمينه أحكامًا جديدة لمواجهة ظاهرة الإجرام المعلوماتي، وكان من شأن هذا التعديل إضافة فصل ثالث للباب الثاني من القسم الثالث من قانون العقوبات، ويقع الفصل المضاف تحت عنوان: "الإعتداءات على نظم المعالجة الآلية للمعطيات" ويتكون من المواد 323-1 إلى 323-4.[3]

المادة 323-1 منه تعالج الدخول غير المشروع أو البقاء غير المصرح بهما إلى نظام المعالجة الآلية للمعطيات وهذه المادة تعد ترديدًا للمادة 462-2 المضافة بقانون 05 جانفي 1988 إلى قانون العقوبات القديم السابق الإشارة إليه، إلا أنها إختلفت في مقدار العقوبة فهي تعاقب على الدخول والبقاء غير المصرح بهما في أحد نظم المعالجة الآلية للمعطيات بعقوبة تتمثل في الحبس لمدة سنة (01) وبغرامة لا تزيد عن مائة ألف 100.000 فرنك، وفي حالة لو ترتب على واقعة الدخول والبقاء غير المصرح بهما تعديل أو إلغاء أو إتلاف البرامج أو النظم المعالجة فإن العقوبة تتضاعف إلى الحبس سنتين (02) والغرامة التي تصل إلى مائتي ألف 200.000 فرنك".[4]

والمادة 323-2 منه هي ترديد أيضًا لنص المادة 462-3 وتعالج الإعتداءات الإرادية على سير نظم المعالجة الآلية للبيانات بحيث يترتب على ذلك تعطيل سير النظام أو إعاقته، وقد نصت هذه المادة على أن العقوبة تكون الحبس لمدة ثلاث (03) سنوات والغرامة التي تصل إلى خمس وأربعون ألف 45.000 فرنك.[5]

---

[1]-Art 462-32 du Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dispose que: « Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à 3 ans et d'une amende de 10 000 F a 100 000 F ou de l'un de ces deux peines».

[2]-Art 462-4 du Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dispose que :« Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission sera puni d'un emprisonnement de 3 mois a 3 ans et d'une amende de 2000 F a 500 000 F ou de l'une de ces deux peines».

[3]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 320.

[4]- نفس المرجع، ص-ص 320-321.

[5]- نفس المرجع، ص 321.

والمادة 323-3 منه تعالج الإعتداءات الموجودة داخل نظام المعالجة الآلية على المعطيات والمعلومات، والعقوبات المقررة فيها هي نفس العقوبات المقررة في المادة 323-2 .[1]

والمادة 323-4 منه تعالج الأفعال الصادرة عن عصابات الإجرام المعلوماتي التي تشكل واحدة أو أكثر من الجرائم المنصوص عليها في المواد من 323-1 إلى 323-3 سالفة الذكر، والعقوبة المنصوص عليها في هذه المادة هي نفس العقوبة أو أشد العقوبات المقررة للفعل ذاته في المواد السابقة.[2]

وأخيرًا فقد تدخل المشرع الفرنسي سنة 2004 بتعديل بعض نصوص قانون العقوبات الفرنسي الجديد الصادر سنة 1994 فيما يتعلق بالمواد من 323-1 إلى 323-3 المنوه عنها سابقًا وذلك بتشديد العقوبة، وقد تم تعديل المادة 323-1 حيث أصبحت تنص على أن: "يعاقب على الدخول أو البقاء بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية للمعطيات، بالحبس لمدة سنتين (02) وغرامة مقدارها ثلاثون ألف 30.000 يورو، وإذا ترتب على ذلك محو أو تعديل لمعطيات النظام أو إتلاف لنظام تشغيل هذا النظام تكون العقوبة الحبس ثلاث (03) سنوات وغرامة قدرها خمس وأربعون ألف 45.000 يورو".[3]

أما المادة 323-2 من نفس القانون تنص على أن: "يعاقب على تعطيل أو إفساد نظام المعالجة الآلية للمعطيات بعقوبة الحبس لمدة خمس (05) سنوات وغرامة قدرها خمس وسبعون ألف 75.000 يورو".[4]

أما المادة 323-3 من نفس القانون تنص على أن: "يعاقب على الإدخال للمعطيات بطريق الغش في نظام المعالجة الآلية أو محوها أو التعديل بطريق الغش للمعطيات التي يحتويها، بعقوبة الحبس لمدة خمس (05) سنوات وغرامة قدرها خمس وسبعون ألف 75.000 يورو".[5]

وقد تلت ذلك عدة تعديلات جاءت في إطار سياسة تشديد العقوبات، وصولًا إلى الصيغة الحالية لقانون العقوبات الفرنسي:

---

[1]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 321.

[2]- نفس المرجع، ص 321.

[3]-Art 323-1 du C.P.F (Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004) dispose que :« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende».

[4]- Art 323-2 du C.P.F (Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004) dispose que: « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende».

[5]- Art 323-3 du C.P.F (Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004) dispose que: «Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou demodifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende».

تنص المادة 323-1 من ق.ع.ف على أن: "يعاقب على الدخول أو البقاء عن طريق الغش داخل كل أو جزء من نظام المعالجة الآلية للمعطيات بالحبس لمدة ثلاث (03) سنوات وغرامة مقدارها مائة ألف 100.000 يورو، إذا ترتب على ذلك حذف أو تغيير لمعطيات النظام أو تخريب لنظام تشغيل النظام تكون العقوبة الحبس خمس (05) سنوات وغرامة قدرها مائة وخمسون ألف 150.000 يورو. وإذا إرتكبت الجرائم المشار إليها في الفقرتين السابقتين ضد نظام المعالجة الآلية للمعطيات الشخصية التي تنفذها الدولة فإن العقوبة تزيد إلى الحبس لمدة سبعة (07) سنوات وغرامة قدرها ثلاثمائة ألف 300.000 يورو".[1]

تنص المادة 323-2 من ق.ع.ف على أن: "يعاقب كل من يقوم بتعطيل أو إفساد تشغيل نظام المعالجة الآلية للمعطيات بالحبس لمدة خمس (05) سنوات وغرامة قدرها مائة وخمسون ألف 150.000 يورو".[2]

تنص المادة 323-3 من ق.ع.ف على أن: "يعاقب على الإدخال للمعطيات بطريق الغش في نظام المعالجة الآلية للمعطيات أو محوها، أو التعديل بطريق الغش للمعطيات التي يحتويها، بعقوبة الحبس لمدة خمس (05) سنوات وغرامة قدرها مائة وخمسون ألف 150.000 يورو. وإذا إرتكبت هذه الجريمة ضد نظام المعالجة الآلية للمعطيات الشخصية التي تنفذها الدولة فإن العقوبة تزيد إلى الحبس سبع (07) سنوات وغرامة قدرها ثلاثمائة ألف 300.000 يورو".[3]

تنص المادة 323-3-1 من ق.ع.ف على أن: "يعاقب على الأفعال التي ترتكب بدون وجه حق الإستيراد أو الحيازة أو العرض أو البيع أو توفير أي معدات أو أدوات أو برامج معلوماتية أو أي معطيات مصممة أو مخصصة، لإرتكاب واحدة أو أكثر من الجرائم المنصوص عليها في المواد من 323-1 إلى 323-3 بالعقوبات المقررة للجريمة نفسها أو للجريمة الأشد في عقوبتها".[4]

---

[1]-Art 323-1 du C.P.F (Modifié par Loi n°2023-22 du 24 janvier 2023 - art. 6) dispose que: « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100.000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende .Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. ».

[2]-Art 323-2 du C.P.F (LOI n°2015-912 du 24 juillet 2015 - art. 4) dispose que: «Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende».

[3]-Art 323-3 du C.P.F (Modifié par Loi n°2015-912 du 24 juillet 2015 - art. 4) dispose que: « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende».

[4]-Art 323-3-1 du C.P.F (LOI n°2013-1168 du 18 décembre 2013 - art. 25) dispose que: « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement=

ب- موقف المشرع المصري:

تعاقب الفقرة الأولى من المادة 14 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر بالحبس مدة لا تقل عن سنة (01) وبغرامة لا تقل عن خمسون ألف 50.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، كل من دخل عمدًا أو دخل بخطأ غير عمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.

وإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين (02) وغرامة لا تقل عن مائة ألف 100.000 جنيه ولا تجاوز مائتي ألف 200.000 جنيه أو بإحدى هاتين العقوبتين، طبقًا للفقرة 02 من نفس المادة، وورد النص على هذه الجريمة أيضًا في البند (هـ) من الفقرة الأولى من المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر ويتحقق السلوك الإجرامي لكل من إخترق النظام التي يحتوي عليها التوقيع أو الوسيط الإلكتروني أو المستند الإلكتروني أو إعترضه أو عطله عن أداء وظيفته، بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر.

وتعاقب المادة 17 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر على جريمة الإعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية بالحبس مدة لا تقل عن سنتين (02) وبغرامة لا تقل عن مائة ألف 100.000 جنيه ولا تجاوز خمسمائة ألف 500.000 جنيه أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا متعمدًا وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي إستخدمت في الجريمة، وورد النص على هذه الجريمة أيضًا في البند (ب) من الفقرة الأولى من المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر التي تعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، كل من: أتلف أو عيب توقيعًا أو وسيطًا أو محررًا إلكترونيًا أو زور شيئًا من ذلك، بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر.

=adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée».

ج- موقف المشرع الجزائري:

تتمثل العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني وفقًا للقانون رقم: 24-06 المؤرخ في 28 أفريل 2024 المعدل والمتمم للأمر رقم: 66-156 المتضمن قانون العقوبات[1] السالف الذكر، في ما يلي:

تعاقب الفقرة الأولى من المادة 394 مكرر من ق.ع.ج بالحبس من ستة (06) أشهر إلى سنتين (02) وبغرامة من ستون ألف 60.000 دج إلى مائتي ألف 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة طبقًا للفقرة 02 من المادة 394 مكرر من نفس القانون، وبالرجوع إلى العقوبة المقررة لجريمة الدخول والبقاء غير المصرح بهما داخل نظام للمعالجة الآلية للمعطيات يحتوي على مستندات إلكترونية هي الحبس من ستة (06) أشهر إلى سنتين (02) وبالغرامة من ستون ألف 60.000 دج إلى مائتي ألف 200.000 دج، وعليه بمضاعفة الحدين الأدنى والأقصى للعقوبتين السالبة للحرية والغرامة تكون العقوبة في جريمة المساس بسلامة معطيات المستند الإلكتروني بالحبس من سنة (01) إلى أربعة (04) سنوات وغرامة من مائة وعشرون ألف 120.000 دج إلى أربعمائة ألف 400.000 دج.

وإذا ترتب على الأفعال المنصوص عليهما في الفقرتين 01 و02 من المادة 394 مكرر تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من سنة (01) إلى ثلاث (03) والغرامة من مائة ألف 100.000 دج إلى ثلاثمائة ألف 300.000 دج طبقًا للفقرة 03 من نفس المادة.

وتعاقب المادة 394 مكرر1 من القانون السالف الذكر بالحبس من سنة (01) إلى ثلاث (03) سنوات وبالغرامة من خمسمائة ألف 500.000 دج إلى مليوني 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

وتعاقب الفقرة الأولى من المادة 394 مكرر2 من نفس القانون بالحبس من سنة (01) إلى خمس (05) سنوات وبالغرامة من مليون 1.000.000 دج إلى خمس ملايين 5.000.000 دج، كل من يقوم عمدًا وعن طريق الغش بما يأتي: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية التي يمكن أن ترتكب بها الجرائم محل الدراسة.

والفقرة 02 من المادة 394 مكرر2 من نفس القانون تعاقب بالحبس من شهرين (02) إلى ثلاث (03) سنوات وبغرامة من مليون 1.000.000 دج إلى خمس ملايين 5.000.000 دج،

[1]- القانون رقم: 24-06 المؤرخ في 28 أفريل 2024، المعدل والمتمم للأمر رقم: 66-156 والمتضمن قانون العقوبات، ج.ر.ج.ج.ش العدد 30، الصادرة بتاريخ 30 أفريل سنة 2024.

كل من يقوم عمدًا وعن طريق الغش بما يأتي: حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم محل الدراسة.

كما تضاعف العقوبات المقررة وفقًا المادة 394 مكرر3 من نفس القانون بالحبس من سنتين (02) إلى عشر (10) سنوات وبالغرامة من سبعمائة ألف 700.000 دج إلى مليوني 2.000.000 دج، متى إستهدفت الجرائم التي سبق التطرق لها الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وذلك دون الإخلال بتطبيق العقوبات الأشد.

2- العقوبات الأصلية المقررة للشخص المعنوي:

نصت المادة 12 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 على مسؤولية الأشخاص المعنوية بحيث نصت الفقرة الأولى منها على أن: "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير، لضمان مساءلة الأشخاص المعنويين عن الجرائم المنصوص عليها في هذه الإتفاقية التي ترتكب لمصلحتها من قبل أي شخص طبيعي، سواء قام بذلك بمفرده أو بإعتباره عضوًا في هيئة تابعة للشخص المعنوي يتقلد منصبًا قياديًا داخلها، وذلك بناء على:

أ- سلطة تمثيل الشخص المعنوي؛

ب- سلطة إتخاذ القرارات نيابة عن الشخص المعنوي؛

ج- سلطة ممارسة الرقابة لدى الشخص المعنوي".[1]

تشير المذكرة التفسيرية للإتفاقية بأن الغرض من المادة هي فرض المسؤولية على الشركات والمؤسسات والأشخاص المعنوية بالنسبة للأفعال الإجرامية المرتكبة لصالحها عن طريق شخص يمارس سلطة القيادة داخلها، وكذا فرض المسؤولية في حال عدم قيام ذلك الشخص بالإشراف على موظف أو عامل أو مراقبته حيث يؤدي هذا الإخفاق إلى إرتكاب ذلك الموظف أوالعامل لأحد الجرائم المنصوص عليها في الإتفاقية.[2]

وبمقتضى الفقرة الأولى من المادة 12 يجب توافر أربعة شروط لتقرير مسؤولية الشخص المعنوي، وهي:

[1]-Art 12 paragraphe 01 du convention sur la cybercriminalité dispose que: «Responsabilité des personnes morales:

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, sur les bases suivantes:

a. un pouvoir de représentation de la personne morale;

b. une autorité pour prendre des décisions au nom de la personne morale;

c. une autorité pour exercer un contrôle au sein de la personne morale».

[2]- التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مرجع سابق، ص 19.

أولًا: يجب أن تكون الجريمة المرتكبة في إحدى الجرائم المنصوص عليها في الإتفاقية؛

ثانيًا: يجب أن تكون الجريمة قد إرتكبت لمصلحة الشخص المعنوي؛

ثالثًا: يجب أن ترتكب الجريمة بواسطة شخصًا يشغل منصبًا قياديًا بما في ذلك الشريك والمحرض أي شخصًا يمارس سلطة القيادة، والذي يعني شخصًا طبيعيًا الذي لديه منصب رفيع في المؤسسة مثال ذلك المدير؛

رابعًا: يجب أن يكون الشخص الذي يشغل منصبًا قياديًا أن يتصرف إستنادًا على سلطة من سلطاته -سلطة تمثيلية أو سلطة تقريرية أو سلطة رقابية-، والتي تبرهن على أن هذا الشخص الطبيعي قد تصرف في نطاق سلطته من أجل تحميل الشخص المعنوي المسؤولية.[1]

وبالإضافة إلى ما تقدم تنص الفقرة 02 من نفس المادة على أن: " بالإضافة إلى الحالات المنصوص عليها سابقًا في الفقرة الأولى من هذه المادة يجب على كل طرف أن يتخذ الإجراءات الضرورية لضمان مساءلة الشخص المعنوي، إذا تخلف الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة الأولى في إرتكاب جريمة مشار إليها في الفقرة الأولى لفائدة الشخص المعنوي من قبل شخص طبيعي يتصرف تحت سلطته".[2]

تضيف المذكرة التفسيرية للإتفاقية على أن الفقرة 02 تلزم الأطراف بأن تكون لديهم القدرة على فرض المسؤولية على الشخص المعنوي، عندما لا ترتكب الجريمة من قبل الشخص الذي يمارس سلطة القيادة -الشخص القائد- المشار إليه في الفقرة الأولى، ولكن بواسطة شخص آخر يتصرف تحت سلطة الشخص المعنوي القانونية، بمعنى أحد موظفيه أو عملائه ضمن نطاق سلطتهم.[3]

وبالنسبة للشروط الواجب إستيفائها قبل إلحاق مسؤولية الشخص المعنوي، فيمكن إجمالها فيما يلي:

1. جريمة يتم إرتكابها من قبل موظف أو عامل الشخص المعنوي؛
2. أن ترتكب الجريمة لفائدة الشخص المعنوي؛
3. أن يكون إرتكاب الجريمة أصبح ممكنًا، بسبب فشل الشخص القائد في الإشراف على الموظف أو العامل.[4]

---

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 151-152.

[2]-Art 12 paragraphe 02 du convention sur la cybercriminalité dispose que : « Outre les cas déjá prévus au paragraphe 1, chaque partie adopte les mesures nécessaires pour s'assurer qu'une personne morale puisse être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions visées au paragraphe 1 pour le compte de ladite personne morale par une personne physique agissant sous son autorité».

[3]- التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مرجع سابق، ص19.

[4]- نفس المرجع، ص20.

وفي هذا السياق، فإن تخلف الإشراف يجب ألا يفسر على أنه يشمل عدم إتخاذ التدابير المناسبة والمعقولة لمنع الموظفين أو العملاء من إرتكاب الأنشطة الإجرامية نيابة عن الشخص المعنوي.[1]

وجدير بالذكر أن شكل هذه الإجراءات الملائمة والمنطقية يمكن أن يشتمل على عدة عوامل مثال ذلك طبيعة المنشأة والحجم والمعايير المطبقة أو الممارسة الجيدة...إلخ، ويجب ألا يفسر ذلك على أنه يستوجب فرض نظام عام للمراقبة على إتصالات المستخدمين.[2]

ومن هذا المنطلق فإن مقدم الخدمات لا يمكن أن يكون مسؤولًا عن جريمة ترتكب عبر جهازه عن طريق زبون أو مستخدم أو شخص ثالث، وذلك لأن مصطلح شخص طبيعي يعمل تحت سلطته لا ينطبق إلا على المستخدمين والعملاء الذين ينصرفون في إطار سلطاتهم.[3]

وتضيف الفقرة 03 من نفس المادة على أن: "وتبعًا للمبادئ القانونية للدولة الطرف يمكن أن تكون المسؤولية القانونية للشخص المعنوي جنائية أو مدنية أو إدارية"[4]، بموجب هذه الفقرة يمكن لكل طرف أن يقرر نصًا على أي من هذه الأشكال للمسؤولية أوتجميعها معًا وفقًا للمبادئ القانونية السائدة في القوانين الداخلية، طالما أنه يستوفي بالمعايير المشار إليها في الفقرة 02 من المادة 13 والتي وفقًا لها بأن تكون العقوبة أوالإجراءات فعالة وملائمة ورادعة وأن تشمل العقوبات المالية[5].

وتنص الفقرة 04 من نفس المادة على أن: "لا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين إرتكبوا الجريمة"[6]، أي أن مسؤولية الأشخاص المعنوية لا تستبعد مسؤولية الأشخاص الطبيعية[7].

أما بالنسبة للإتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد نصت في المادة 20 منها على المسؤولية الجنائية للأشخاص الطبيعية والمعنوية، على أن تلتزم كل دولة طرف مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص المعنوية عن الجرائم التي يرتكبوها ممثلوها بإسمها أو لصالحها، دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيًا.

---

[1]- التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مرجع سابق، ص20.

[2]- هلالي عبد اللاه أحمد، مرجع سابق، ص153.

[3]- نفس المرجع، ص153.

[4]-Art 12 paragraphe 03 du convention sur la cybercriminalité dispose que : «Selon les principes juridiques de la Partie la responsabilité d'une personne morale peut être pénale, civile ou administrative».

[5]- هلالي عبد اللاه أحمد، مرجع سابق، ص153.

[6]-Art 12 paragraphe 04 du convention sur la cybercriminalité dispose que : «Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction».

[7]- هلالي عبد اللاه أحمد، مرجع سابق، ص153.

أما على مستوى التشريعات فبالنسبة للمسؤولية الجزائية للشخص المعنوي في التشريع الفرنسي فطبقًا للمادة 323-6 من ق.ع.ف تتحمل الأشخاص المعنوية المسؤولية الجزائية كالآتي:

في إطار الشروط المنصوص عليها في المادة 121-2 بالنسبة للجرائم المنصوص عليها في الفصل الخاص بالإعتداءات على أنظمة المعالجة الآلية للمعطيات والمتمثلة في:

- الأشخاص المعنوية بإستثناء الدولة تعد مسؤولة جنائيًا، وفقًا لما هو منصوص عليه في المواد من 121-4 إلى 121-7، عن الجرائم المرتكبة لحسابها بواسطة أجهزتها أو ممثليها؛

- ومع ذلك فإن السلطات المحلية وهيئاتها مسؤولة جنائيًا إلا عن الجرائم المرتكبة أثناء ممارستها لأنشطة، قد تكون محل إتفاقيات تفويض المرفق العام؛

- ولا يترتب على قيام المسؤولية الجنائية للأشخاص المعنوية إستبعاد مسؤولية الأشخاص الطبيعيين، سواء بصفتهم فاعلين أو شركاء في نفس الجريمة، مالم ينص على خلاف ذلك في الفقرة الرابعة من المادة 121-3.[1]

بالإضافة إلى الغرامة وفقًا لأحكام المادة 131-38:

-الغرامة التي تعادل خمس (05) أضعاف الحد الأقصى للعقوبة المقررة للشخص الطبيعي، بموجب القانون الذي يعاقب على الجريمة؛

- إذا تعلق الأمر بجناية لا ينص فيها القانون على عقوبة الغرامة على الأشخاص الطبيعيين، تكون الغرامة التي يجوز الحكم بها على الأشخاص المعنوية قدرها 1.000.000 يورو".[2]

والعقوبات المنصوص عليها في المادة 131-39:

- الحل، إذا ثبت أن الشخص المعنوي قد تم إنشاؤه، أو تم تحويل هدفه، بغرض إرتكاب الأفعال الإجرامية، وذلك إذا كانت الجريمة المعنية جناية أو جنحة يعاقب عليها الشخص الطبيعي بعقوبة سالبة للحرية تساوي أو تفوق ثلاث (03) سنوات؛

- المنع النهائي أو المؤقت لمدة لا تتجاوز خمس (05) سنوات، من مزاولة نشاط أو عدة أنشطة مهنية أو إجتماعية بصورة مباشرة أو غير مباشرة؛

[1]-Art 121-2 du C.P.F (Loi n°2004-204 du 9 mars 2004 - art. 54 JORF 10 mars 2004 en vigueur le 31 décembre 2005) dispose que: « Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants. Toutefois, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public. La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3».

[2]-Art 131-38 du C.P.F (Loi n°2004-204 du 9 mars 2004 - art. 55 JORF 10 mars 2004) dispose que: « Le taux maximum de l'amende applicable aux personnes morales est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction. Lorsqu'il s'agit d'un crime pour lequel aucune peine d'amende n'est prévue à l'encontre des personnes physiques, l'amende encourue par les personnes morales est de 1 000 000 euros».

- الوضع تحت الرقابة القضائية لمدة لا تتجاوز خمس (05) سنوات؛
- الغلق النهائي أو المؤقت، لمدة لا تتجاوز خمس (05) سنوات، لمؤسسة أو أكثر من المؤسسات التابعة للشخص المعنوي والتي إستعملت في إرتكاب الأفعال المجرمة؛
- الإقصاء النهائي أو المؤقت، لمدة لا تتجاوز خمس (05) سنوات من الصفقات العمومية؛
- مصادرة الأشياء التي إستخدمت أو كان من شأنها أن تستخدم في إرتكاب الجريمة؛
- نشر أو تعليق حكم الادانة.[1]

بالإضافة إلى الحظر المنصوص عليه في البند 02 من المادة 131-39 الذي ينطبق على النشاط المهني الذي بمناسبته إرتكبت الجريمة.[2]

وقد نص المشرع المصري على المسؤولية الجزائية للشخص المعنوي بموجب القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر ضمن المواد 35 و36 و37، وبإستعراضنا لنصوص هذه المواد نجدها تنص على:

- المسؤولية الجزائية للأشخاص الطبيعية من المسؤولين عن الإدارة الفعلية لأي شخص معنوي عن عدم إبلاغ الجهات الرسمية المختصة عن وقت علمه بالجرائم التي تتعرض لها المواقع والحسابات والبريد الإلكتروني المخصص للكيان الذي يديره، يعاقب بالحبس مدة لا تقل عن ثلاثة (03) أشهر وبغرامة لا تقل عن ثلاثين ألف 30.000 جنيه ولا تزيد على مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، طبقًا للمادة 35 من ذات القانون؛
- يعاقب المسؤول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل إرتكابها، تحقيقًا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي، طبقًا للمادة 2/36 من ذات القانون؛

---

[1]-Art 131-39 du C.P.F (LOI n°2014-790 du 10 juillet 2014 - art. 12) dispose que: «Lorsque la loi le prévoit à l'encontre d'une personne morale, un crime ou un délit peut être sanctionné d'une ou de plusieurs des peines suivantes :
1° La dissolution, lorsque la personne morale a été crée ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure ou égale à trois ans, détournée de son objet pour commettre les faits incriminés ;
2° L'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
3° Le placement, pour une durée de cinq ans au plus, sous surveillance judiciaire ;
4° La fermeture définitive ou pour une durée de cinq ans au plus des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus ;
8° La peine de confiscation, dans les conditions et selon les modalités prévues à l'article 131-21».

[2]-Art 323-6 du C.P.F (Loi n°2009-526 du 12 mai 2009 - art. 124) dispose que: « Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise».

- للمحكمة أن تقضي بإيقاف ترخيص مزاولة الشخص المعنوي للنشاط مدة لا تزيد على سنة (01)، ولها في حالة العود أن تحكم بإلغاء الترخيص، أو حل الشخص المعنوي بحسب الأحول، وأن يتم نشر الحكم في جريدتين يوميتين واسعتي الإنتشار على نفقة الشخص المعنوي، طبقًا للمادة 2/36 من ذات القانون؛
- تقرير مسؤولية الإدارة الفعلية للشخص المعنوي إستبعاد المسؤولية الجزائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التي تقوم بها الجريمة، طبقًا للمادة 37 من ذات القانون.

وبموجب المادة 24 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر يعاقب المسؤول عن الإدارة الفعلية للشخص المعنوي المخالف بذات العقوبات المقررة في المادة 23 عن الأفعال التي ترتكب بالمخالفة لأحكام المادة 21 من هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك، ويكون الشخص المعنوي مسؤولًا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد إرتكبت من أحد العاملين به بإسم ولصالح الشخص المعنوي.[1]

[1]- ومؤدى ذلك أنه إذا كان الجانى فى الجرائم السابقة هو الشخص المعنوي، فإن المدير المسؤول عن الإدارة الفعلية لذلك الشخص يسأل جنائيًا ويعاقب بالعقوبات المقررة للجرائم السابقة، والمتمثلة في الحبس والغرامة أو أيهما، وبالغرامة فقط إن كانت هي العقوبة الجنائية الوحيدة لهذه الجريمة، وذلك بشرط أن تكون الجريمة قد وقعت، لأن المدير المسؤول لم يراع الواجبات المفروضه عليه والتي تقتضيها تلك الإدارة. ومن ناحية أخرى فإن المشرع قد ألزم الشخص المعنوي متضامنًا بالغرامة والتعويضات التي قد يقضي بها متى كانت الجريمة قد إرتكبها شخص طبيعي بإسم ولصالح ذلك الشخص المعنوي، والحقيقة أن العقوبات المالية وكذلك التعويضات المقضى بها هي أمور تتفق وطبيعة الشخص المعنوي، وللمزيد من التفصيل، ينظر: سحر سعد عبد السميع محمد، مرجع سابق، ص-ص 220-221.

لا سيما وأن الجريمة قد إرتكبت بإسم ولصالح ذلك الشخص المعنوي، وحسب هذا النص فإن الأشخاص المعنوية العامة أو الخاصة قد ينسب إليها مخالفتها لأي حكم من أحكام هذا القانون أو اللوائح التي صدرت بناءً عليه، ويتعين أن تكون هذه المخالفة والتي تمثل جريمة جنائية، قد وقعت بناء على تصرف أو إهمال أو موافقة عضو مجلس إدارة أو مدير أو أي موظف آخر لدى ذلك الشخص المعنوي. ويكون التصرف بأن يصدر أحدهم قرارًا ما ترتب عليه مخالفة ذلك القانون، أو يوافق على تصرف أتاه أحدهم مؤدى إلى مخالفة ذلك القانون أو يهمل في إتخاذ إجراء إحترازي يكون من شأنه وقوع مخالفة لأحكام هذا القانون، أو يتستر عضو مجلس الإدارة أو الموظف لدى الشخص المعنوي على تصرف يشكل مخالفة الأحكام ذلك القانون ولوائحه التنفيذية، وللمزيد من التفصيل، ينظر: نفس المرجع، ص221.

ويستوى أن يصدر الفعل الذى يشكل مخالفة من عضو مجلس إدارة أو موظف لدى الشخص المعنوي أو شخص آخر يتصرف بهذه الصفة، وهذه الجريمة في حال ثبوتها يعاقب عنها الشخص الطبيعي الذي صدرت منه وكذلك الشخص المعنوي، شرط أن تكون هناك عقوبات تتفق وطبيعة ذلك الشخص المعنوي كالإغلاق أو الغرامة. ولذلك فنص المادة 02 لا يذكر جريمة محددة، لكنه يذكر مخالفات لنصوص هذا القانون شرط أن تمثل جريمة جنائية، ولهذا فإن شكلت المخالفة جريمة جنائية تطبق العقوبات على الشخص الطبيعي الذي إقترف هذه الجريمة ثم الشخص المعنوي الذي ينسب إليه فعل الجاني، شرط أن تتفق طبيعة هذه العقوبات مع طبيعة الشخص المعنوي، وسواء كان شخصًا معنويًا عامًا أم من الأشخاص. وقد سايرت محكمة النقض هذا الإتجاه فقضت بوجوب معاقبة مدير المصنع أو المنشأة إذا لم يحرر عقود العمل كتابة ومن نسختين بينه وبين عمال المصنع كما حكمت في مقام آخر بوقوع المسؤولية الجنائية على ممثلي الشخص المعنوي لما يقترفونه من جرائم أثناء قيامهم بالعمل لحسابه، وللمزيد من التفصيل، ينظر: نفس المرجع، ص- ص 221-222.

أما بالنسبة لموقف المشرع الجزائري فيعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني بغرامة تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي طبقًا للمادة 394 مكرر04 من ق.ع.ج.

ومنه تعاقب الفقرة الأولى من المادة 394 مكرر من ق.ع.ج الشخص المعنوي الذي يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، أو يحاول ذلك، طبقًا لنص المادة 394 مكرر4 من نفس القانون بغرامة تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وعليه تكون العقوبة الأصلية للشخص المعنوي المدان غرامة تقدر مليون 1.000.000 دج.

وإذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة طبقًا للفقرة 02 من المادة 394 مكرر من نفس القانون، تكون العقوبة للشخص المعنوي الغرامة التي تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وعليه تكون العقوبة غرامة تقدر بمليوني 2.000.000 دج.

وإذا ترتب على الأفعال المنصوص عليهما في الفقرتين 02 و03 من المادة 394 مكرر من نفس القانون تخريب نظام إشتغال المنظومة تكون العقوبة للشخص المعنوي الغرامة التي تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وعليه تكون العقوبة غرامة تقدر بمليون وخمسمائة ألف 1.500.000 دج.

وتعاقب المادة 394 مكرر1 من القانون السالف الذكر كل شخص معنوي أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها الغرامة التي تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وعليه تكون العقوبة الغرامة المقدرة بعشرة ملايين 10.000.000 دج.

وتعاقب الفقرة الأولى من المادة 394 مكرر2 من نفس القانون كل من يقوم عمدًا وعن طريق الغش بما يأتي: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية التي يمكن أن ترتكب بها الجرائم محل دراستنا، الغرامة التي تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وعليه تكون العقوبة الغرامة المقدرة بخمس وعشرون مليون 25.000.000 دج.

والفقرة 02 من المادة 394 مكرر2 من نفس القانون كل من يقوم عمدًا وعن طريق الغش بما يأتي: حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم محل دراستنا، الغرامة التي تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وعليه تكون العقوبة الغرامة المقدرة بخمس وعشرون مليون 25.000.000 دج.

كما تضاعف العقوبات المقررة وفقًا المادة 394 مكرر3 من نفس القانون متى إستهدفت الجرائم التي سبق التطرق لها الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، الغرامة التي تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وعليه تكون العقوبة الغرامة المقدرة بعشرة ملايين 10.000.000 دج.

ثانيًا: العقوبات التكميلية المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني

إلى جانب العقوبات الأصلية فإنه يجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة بنص المادة 09 من ق.ع.ج على حسب ظروف الوقائع بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من ذات القانون بالنسبة للشخص المعنوي.

ومنه تنص المادة 09 من ق.ع.ج على أن : العقوبات التكميلية هي:

1. الحجر القانوني؛
2. الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية؛
3. تحديد الإقامة؛
4. المنع من الإقامة؛
5. المصادرة الجزئية للأموال؛
6. المنع المؤقت من ممارسة مهنة أو نشاط؛
7. إغلاق المؤسسة؛
8. الإقصاء من الصفقات العمومية؛
9. الحظر من إصدار الشيكات و/أو إستعمال بطاقات الدفع؛
10. تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من إستصدار رخصة جديدة؛
11. سحب جواز السفر؛
12. نشر أو تعليق حكم أو قرار الإدانة؛
13. المنع من الإتصال بالضحية".

وتنص المادة 18 مكرر من نفس القانون على أن :...واحدة أو أكثر من العقوبات التكميلية الأتية:

1. حل الشخص المعنوي؛
2. غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (05) سنوات؛
3. الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (05) سنوات؛
4. المنع من مزاولة نشاط أو عدة أنشطة مهنية أو إجتماعية بشكل مباشر أو غير مباشر، نهائيًا أو لمدة لا تتجاوز خمس (05) سنوات؛
5. مصادرة الشيء الذي استعمل في إرتكاب الجريمة أو نتج عنها؛
6. نشر وتعليق حكم الإدانة؛

7. الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (05) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي إرتكبت الجريمة بمناسبته".

فضلًا عن ذلك، رصد المشرع الجزائري عقوبات تكميلية وجوبية بموجب المادة 394 مكرر6 من ق.ع.ج، والتي تشمل المصادرة للأجهزة والبرامج والوسائل المستخدمة، وكذا عقوبة الغلق للمواقع المستعملة في الجريمة وغلق المحل أو المكان المستغل في إرتكابها، وتشترك فيها جميع الجرائم محل الدراسة.

فبالنسبة للمصادرة فإنه وبعد إدانة الجاني بالعقوبات الأصلية يخضع هذا الأخير لعقوبة تكميلية تقتضي مصادرة الأجهزة والبرامج والوسائل المستخدمة في إرتكاب الجريمة مع مراعاة الحقوق الغير حسن النية[1]، وهو ما نصت عليه المادة 394 مكرر6 من ذات القانون صراحة عندما قضت بأنه: "مع الإحتفاظ بالحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة".

وهذا الإتجاه الذي ذهب إليه المشرع الجزائري هو ما سبقه إليه المشرع الفرنسي حين أقر عقوبة المصادرة بموجب البند 03 من المادة 323-5 من ق.ع.ف والتي جاءت صياغتها كالآتي: "مصادرة الأشياء التي إستخدمت أو كان ينوي إستخدامها في إرتكاب الجريمة أو تلك التي نجمت عنها، مع إستثناء المواد الخاضعة للتعويض".[2]

أما بالنسبة لموقف المشرع المصري فقد نصت الفقرة الأولى من المادة 38 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكرعلى أن: "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونًا أو غيرها، مما يكون قد إستخدم في إرتكاب الجريمة أو سهل أو ساهم في إرتكابها"[3]، ويقصد بالأدوات الأشياء التي إستعملت في إرتكاب الجريمة، بينما يقصد بالآلات والمعدات والأجهزة كل وسيلة مصنعة أو تقنية تستخدم في إرتكاب الجرائم المنصوص عليها في القانون، ولم يشترط المشرع المصري لوجوب المصادرة إلا أن تكون هذه الأدوات أو الآلات أو المعدات أو الأجهزة قد إستخدمت في إرتكاب الجريمة أو سهلت أو

[1]- نصت المادة 15 مكرر2 من ق.ع.ج على أن : "يعتبر من الغير حسن النية الأشخاص الذين لم يكونوا شخصيًا محل متابعة أو إدانة من أجل الوقائع التي أدت إلى المصادرة، ولديهم سند ملكية أو حيازة صحيح ومشروع على الأشياء القابلة للمصادرة".

[2]-Art 323-5 du C.P.F (Loi n° 92-685 du 22 juillet 1992) dispose que: « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution».

[3]- المصادرة هي من العقوبات التكميلية التي أخذ بها المشرع المصري بموجب المادة 30 من قانون العقوبات المصري، والتي جعلت مصادرة الأشياء المضبوطة المتحصلة من جناية أو جنحة، وكذلك الأسلحة والآلات المضبوطة التي إستعلمت أو التي من شأنها أن تستعمل فيها، وهذا كله بدون إخلال بحقوق الغير الحسن النية جوازية للقاضي، إلا أن خروجًا على القاعدة العامة فقد جعل المشرع المصري المصادرة وجوبية في قانون مكافحة جرائم تقنية المعلومات.

ساهمت في إرتكابها، وأن تكون حيازتها غير مشروعة أي أن حيازتها أو إحرازها أو التعامل فيها يشكل جريمة.[1]

أما بالنسبة للغلق فيتم إغلاق المواقع التي تكون محل الجريمة، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد إرتكبت بعلم مالكها، ومنه فهي تتعلق بمحلين:

الأول: المواقع الإلكترونية التي تستعمل في إرتكاب الجريمة، أو ساهمت في إرتكابها.

الثاني: إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد إرتكبت بعلم مالكها، وهو المكان الذي كان يستغله الجاني في إرتكاب الجريمة والذي قد يحتوي على الوسائل الإلكترونية التي إستعملت في تنفيذ الجريمة.[2]

ويقوم ذلك في الحالة التي يكون صاحب المحل مشاركًا في الجريمة، وذلك إذا تمت الجريمة وهو عالم بها ولم يتصد لها بالإخبار عنها أو بمنع مرتكبيها من إرتياد محله لإرتكاب مثل هذه الجرائم.[3]

وأما بالنسبة لمدة الغلق فإن المادة 394 مكرر6 من ق.ع.ج لم تحدد ذلك، وبالرجوع إلى القواعد العامة في تحديدها نجد المادة 16 مكرر1 من ذات القانون تنص على أن يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي إرتكبت الجريمة بمناسبته، ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة لا تزيد عن عشر (10) سنوات في حالة الإدانة لإرتكاب جناية وخمس (05) سنوات في حالة الإدانة لإرتكاب جنحة، وبإعتبار الجرائم محل الدراسة جنحة فإن مدة الغلق إما أن تكون بصفة نهائية أو مؤقتة بمدة لا تزيد عن (05) سنوات.

ونجد المشرع الفرنسي بدوره فقد نص على عقوبة الغلق طبقًا للبند 04 من المادة 323-5 من ق.ع.ف كالآتي: "الغلق لمدة لا تتجاوز خمس (05) سنوات لمؤسسة أو أكثر من المؤسسات التابعة للشخص المعني، والتي استعملت في إرتكاب الأفعال الإجرامية"[4]، ونجد المشرع الفرنسي نص أيضًا على غيرها من العقوبات التكميلية الوجوبية وذلك بموجب المادة 323-5 من ق.ع.ف كالآتي: "يتحمل الأشخاص الطبيعيون المدانون بإرتكاب الجرائم المنصوص عليها في هذا الفصل أيضًا بالعقوبات التكميلية التالية:

1- المنع لمدة لا تتجاوز خمس (05) سنوات من مباشرة الحقوق المدنية والمدنية المتصلة بالعائلة، وفقًا لأحكام المادة 131-26؛

---

[1]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 231.

[2]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص693.

[3]- خثير مسعود، مرجع سابق، ص 131.

[4]-Art 323-5 paragraphe 04 du C.P.F (Loi n° 92-685 du 22 juillet 1992) dispose que: «4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés».

2 - المنع لمدة لا تتجاوز خمس (05) سنوات من ممارسة الوظائف العامة أو مزاولة النشاط المهني أو الإجتماعي، الذي ارتكبت الجريمة بمناسبته أو أثناء ممارسته؛

3 - مصادرة الأشياء التي إستعملت أو كانت معدة لإرتكاب الجريمة، أو تلك التي نجمت عنها، بإستثناء الأشياء القابلة للرد؛

4 - الغلق لمدة لا تتجاوز خمس (05) سنوات لمؤسسة أو أكثر من المؤسسات التابعة للشخص المعني، والتي استعملت في إرتكاب الأفعال الإجرامية؛

5 - الإقصاء لمدة لا تتجاوز خمس (05) سنوات من الصفقات العمومية؛

6 - المنع لمدة لا تتجاوز خمس (05) سنوات من إصدار الشيكات، بإستثناء الشيكات التي تستخدم لسحب الأموال من الجهة المسحوب عليها أو الشيكات المصدق عليها؛

7- نشر أو إذاعة الحكم القضائي الصادر، وفقًا للشروط المنصوص عليها في مادة 131-35".[1]

أما بالنسبة للتشريع المصري فقد نص على ذلك في الفقرة 02 من المادة 38 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر على أن: "وفي الحالات التي يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الإعتباري المدان بأي جريمة منصوص عليها في هذا القانون لم يحصل على الترخيص فيحكم فضلًا عن العقوبات المقررة بالغلق"، يتضح أن المشرع المصري أجاز الحكم بغلق المحل الخاص بالشخص المعنوي إذا لم يكن حاصلًا على ترخيص بمزاولة النشاط من إحدى الجهات الحكومية، وترجع الحكمة في النص على غلق المحل أو الموقع في أن هذا الموقع أو المحل كان وسيلة سهلت للجاني لإرتكاب الجريمة فيه، ومن ثم تحكم المحكمة بإغلاق المحل أو الموقع إذا كانت الجريمة قد إرتكبت بعلم مالكها وذلك إغلاقًا كليًا أو للمدة التي تقدرها المحكمة[2].

[1]-Art 323-5 du C.P.F (Loi n° 92-685 du 22 juillet 1992) dispose que: « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35».

[2]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص-ص 232-233.

وأضاف المشرع المصري عقوبة العزل من الوظيفة المؤقت والوجوبي إذا قضت المحكمة بالإدانة على أحد الموظفين العموميين لإرتكابه جريمة من الجرائم محل الدراسة أثناء وبسبب تأديته لوظيفته، فتنص المادة 39 من ذات القانون على أن: "للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين لإرتكابه جريمة من الجرائم المنصوص عليها في هذا القانون أثناء وبسبب تأديته لوظيفته، أن تقضي بعزله من وظيفته مؤقتًا، إلا في الحالات المشار إليها في المادة 34 من هذا القانون[1] فيكون العزل وجوبيًا".

الفرع الثاني: أحكام العقاب على الإتفاق الجنائي والشروع في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني

سنتطرق إلى عقوبة الإتفاق الجنائي والشروع في ما يلي:

أولًا: الإتفاق الجنائي

لأجل تقرير حماية متقدمة ووقائية للنظم المعلوماتية خرج المشرع الفرنسي عن القواعد العامة في العقاب على الجرائم، إذ نقض هذه القواعد بأن العقاب لا يقع ولا يقرر إلا على الجرائم التامة أو تلك التي تقف عند الشروع أو المحاولة أما الأعمال التحضيرية التي تسبق البدء في التنفيذ فلا عقاب عليها كقاعدة عامة، ونص المادة 323-4 يعد إستثناءًا من القاعدة العامة أو هو النص الخاص الذي يقيد العام فقد عاقبت على مساهمة أكثر من شخص في إرتكاب أفعال مادية تحضيرية تهدف إلى إرتكاب إحدى الجرائم المنصوص عليها في المواد 323-1 إلى 323-3.[2]

ونص المشرع الجزائري في المادة 394 مكرر5 من ق.ع.ج على أن: "كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدًا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"، نلاحظ أن المشرع الجزائري رصد لها نفس عقوبة الجريمة التامة ذلك أن جرائم الإعتداء على نظم المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني قد تتم في شكل جماعات وإن كان لم يسبق إتفاق بين هاته المجموعة على إرتكاب هذه الجريمة، ولكن النتيجة الجرمية تبين إتفاق ضمني بين أفراد المجموعة، إذ أن هذه الجرائم لا تتطلب إجتماع حقيقي فيما بين شخصين أو أكثر وإنما يتصور الإتفاق الجنائي بمجرد إنتقال كلمة السر من شخص إلى آخر وإن لم يكن بينهما معرفة سابقة.[3]

---

[1]- الحالات التي أشارت إليها المادة 34 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر: "إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون، بغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الإقتصادي، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الإجتماعي، تكون العقوبة السجن المشدد".

[2]- بن شهرة شول، مرجع سابق، ص109.

[3]- خثير مسعود، مرجع سابق، ص 129.

ثانيًا: عقوبة الشروع

تمر الجريمة في أغلب الأحيان قبل إرتكابها بعدة مراحل، مرحلة التفكير والعزم والتخطيط هي أول مرحلة التي تتبادر فيها فكرة الجريمة في ذهن المرتكب، ولا يعاقب فيها على ما يأتيه من الأفعال إلا إذا نص المشرع على خلاف ذلك.

ثم مرحلة التحضير للجريمة التي يتم فيها إعداد فيها الوسائل التي تستعمل أو تسهل في إرتكاب الجريمة، هذه المرحلة غير معاقب عليها إذ ترك المشرع فرصة للجاني للعدول عن جريمته، لكن إذا إرتقت هذه الأفعال إلى درجة الخطورة التي تمس المصالح المحمية إعتبرها المشرع جريمة مستقلة بذاتها.

وفي نطاق الجرائم محل الدراسة راعى المشرع عند صياغته للمواد المتعلقة بالإعتداءات للنظام المعالجة الآلية للمعطيات بالعقاب على بعض الأعمال التحضيرية بوصفها جرائم مستقلة، ومن قبيل ذلك ما جاءت به المادة 394 مكرر2 من ق.ع.ج من الأفعال بوصفها جرائم مستقلة كالبحث والتصميم، كذلك المادة 394 مكرر5 من نفس القانون التي تعاقب على مجرد الأعمال التحضيرية في الصورة الإتفاق الجنائي.[1]

ثم تأتي مرحلة الشروع وهي المرحلة التي تنصرف فيها إرادة الجاني إلى تنفيذ الجريمة فعلًا، فيبدأ في تنفيذ الركن المادي ولكنها لا تتم لأسباب لا دخل لإرادته فيها[2] وهذه المرحلة معاقب عليها في القانون، وفي هذا الصدد تنص المادة 30 من القانون السالف الذكر على أن: كل محاولات لإرتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى إرتكابها تعتبر كالجناية نفسها، إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"، وتنص المادة 31 من نفس القانون على أن: "المحاولة في الجنحة لا يعاقب عليها إلا بناءً على نص صريح في القانون".

بالرجوع إلى القواعد العامة نجد أن تجريم الشروع في الجنايات لا يحتاج إلى نص تجريمي، أما في مواد الجنح كقاعدة لا يعاقب عليه إلا بنص وبذلك نجد أن المشرع الجزائري قد تبنى فكرة العقوبة على الشروع في إرتكاب الجنح الماسة بنظم المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني وذلك رغبة منه في توفير حماية فعالة لهذا النظام، وذلك من خلال المادة 394 مكرر7 من ذات القانون التي تنص على أن: "يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"، وهو ما قضي به المشرع الفرنسي بموجب المادة 323-7 من ق.ع.ف والتي تنص على أن: "يعاقب على الشروع في الجرائم المنصوص عليها في المواد 323-1 إلى 323-3-1 بذات العقوبة المقررة

[1]- مليايني عبد الوهاب، مرجع سابق، ص 209.

[2]- أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص**، الجزء الثاني، الطبعة السابع عشرة، 2018، دار هومة للطباعة والنشر والتوزيع، الجزائر، ص 126.

تلك الجرائم"[1]، بينما المشرع المصري قرر عقوبة أقل من العقوبة المقررة للجريمة التامة بموجب المادة 40 من القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر بنصه: "كل من شرع في إرتكاب الجنح المنصوص عليها في هذا القانون، يعاقب بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة".

والمشرع في الجرائم محل الدراسة ليس له بد من تجريم الشروع، وذلك لأنه جرم مرحلة الإتفاق الجنائي في الأعمال التحضيرية بصفتها مرحلة من مراحل الجريمة تسبق الشروع وعليه لزامًا أن يجرم الشروع بوصفه مرحلة لاحقة عليها، ولا يعقل أن يجرم المشرع مرحلة ويبيح أخرى لاحقة عليها[2]، ومن خلال إستقراء نص المادة 394 مكرر5 من ق.ع.ج نجد أنها مشمولة بهذا النص أي أن المشرع الجزائري قد تبنى فكرة الشروع في الإتفاق الجنائي.

وقد أخرجت بعض التشريعات المقارنة بما في ذلك التشريع الفرنسي جنحة الإتفاق الجنائي لتحضير جرائم الماسة بالأنظمة المعالجة الآلية للمعطيات من نطاق الشروع لأنها تعتبر أن في ذلك مساس بالنظرية العامة في القانون الجنائي، لأن التحضير للجرائم الذي يتم في إطار إتفاق أو مجموعة تشكل في حد ذاتها محاولة أو عمل تحضيري مما يؤدي إلى تبني فكرة الشروع في الشروع.[3]

المبحث الثاني: الجرائم الماسة بمحتوى المستند الإلكتروني

تعد المستندات الإلكترونية بما تتضمنه من معطيات ومعلومات من الأهداف المتزايدة للإعتداءات الإلكترونية، سواء كانت هذه المستندات مخزنة داخل الأنظمة المعلوماتية أو محفوظة على وسائط خارجية، وتشهد جرائم الإعتداء عليها تزايدًا مستمرًا إذ لا يتوانى محترفو النظم المعلوماتية عن إبتكار وسائل وتقنيات متطورة لإختراق هذه المعطيات وتمتد هذه الإعتداءات لتشمل المعطيات الإلكترونية التي يتم إنشاؤها تلقائيًا، فضلًا عن التوقيعات الإلكترونية المدرجة ضمن تلك المستندات، مما قد يسبب خسائر كبيرة للمتعاملين، ويهدد عنصري الثقة والخصوصية في المعاملات الإلكترونية.[4]

ومنه سنتناول في هذا المبحث جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور في (المطلب الأول)، وجريمة سرقة معطيات المستند الإلكتروني في (المطلب الثاني).

[1]- Art 323-7 du C.P.F (Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004) dispose que: « La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines».

[2]- بن مكي نجاة، مرجع سابق، ص 209.

[3]- آمال قارة، مرجع سابق، ص 133.

[4]- بلحسيني حمزة، مرجع سابق، ص 192.

المطلب الأول: جريمة تزوير المستند الإلكتروني و جريمة إستعمال المستند الإلكتروني المزور

إذا كانت المستندات الإلكترونية تنطوي على إثبات وقائع قانونية لها حجيتها في الإثبات، فإن التغيير فى محتواها من شأنه أن ينطوي على مساس بحجية ما تضمنته من وقائع، لذلك فقد نصت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في مادتها 07 بأنه: "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم وفقًا لقانونه الداخلي، الإدخال، الإتلاف، المحو، أو الطمس العمدي، وبدون حق للمعطيات الإلكترونية الذي يتوالد عنه معطيات غير صحيحة، بقصد أخذها في الحسبان أو إستخدامها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت سهلة القراءة مباشرة وواضحة أم لا، ويمكن لأي طرف أن يشترط في قانونه الداخلي نية الغش أو نية إجرامية مشابهة من أجل تقرير المسؤولية الجنائية".[1]

تحصر المذكرة التفسيرية للإتفاقية الغرض من هذه المادة فى إنشاء جريمة موازية لجريمة تزوير المستندات الورقية، وتهدف هذه الجريمة إلى سد ثغرات قانون العقوبات المتعلقة بالتزوير التقليدي التي تتطلب سهولة القراءة المرئية للمعطيات المتضمنة في المستند والتي لا تنطبق على المعطيات المسجلة على دعامة إلكترونية، وقد يكون للتلاعب بمثل هذه المعطيات ذات القيمة الإثباتية يمكن أن تكون لها نفس النتائج الوخيمة التي تترتب عن الأفعال التقليدية للتزوير إذا تم إيقاع الطرف الثالث في الغلط.[2]

أما عن موقف المشرع الجزائري فقد تضمنت النصوص القانونية المتعلقة بجرائم تزوير المستندات وإستعمالها في قانون العقوبات الجزائري بموجب المواد من 197 إلى غاية المادة 231، وقسمها إلى ستة أقسام وهي: تزوير النقود وما يتصل بها، تقليد أختام الدولة والدمغات والطوابع والعلامات، التزوير في المحررات العمومية أو الرسمية، التزوير في المحررات العرفية أو التجارية أو المصرفية، والتزوير في بعض الوثائق الإدارية والشهادات، كما تطرق إلى الأحكام المشتركة المتعلقة بإستخدام ما سبق ذكره، غير أن جميع هذه الأحكام تنطبق أساسًا على المستندات العادية فقط ولم يتخذ أي موقف لسد الفراغ التشريعي أو التوسيع من مفهوم المستند ليشمل المستندات الإلكترونية ضمن المستندات محل جريمة التزوير.

---

[1]-Art 07 du convention sur la cybercriminalité dispose que : «Falsification informatique: Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées a des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée».

[2]- هلالي عبداللاه أحمد، مرجع سابق، ص108.

وظل المشرع الجزائري على موقفه إلى غاية سنة 2014 حين أصدر القانون رقم: 14-03 المؤرخ في 24 فيفري 2014 المتعلق بسندات ووثائق السفر[1]، كتمهيدًا لمصادقته على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب المرسوم الرئاسي رقم: 14-252 المؤرخ في 08 سبتمبر 2014[2]، وعرفت هذه الإتفاقية جريمة التزوير المعلوماتي بالمادة 10 منها كالآتي: "إستخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات، تغييرًا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة".

ونص المشرع الجزائري على تجريم تزوير سندات ووثائق السفر وإستعمالها بموجب المادة 17 من القانون رقم: 14-03 المتعلق بسندات ووثائق السفر السالف الذكر، والذي نص على أن: "كل شخص يزور أو يقلد، أو يحرض على أي تحريف، أو يتلف عمدًا سندًا أو وثيقة سفر، أو يستعمل عمدًا سندًا أو وثيقة سفر مزورة أو مقلدة أو محرفة، يتعرض إلى العقوبات المنصوص عليها في قانون العقوبات، وإذا مست الأفعال المذكورة أعلاه البيانات المخزنة في النظام البيومتري الإلكتروني فتطبق العقوبات المنصوص عليها في قانون العقوبات، لا سيما تلك المنصوص عليها في المواد 394 مكرر إلى 394 مكرر7"، بإعتبار أن النظام البيومتري الإلكتروني ما هو إلا نظام من أنظمة المعالجة الآلية للمعطيات، وبهذا يكون المشرع قد أحال إلى تطبيق العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، وقد سبق وأن تطرقنا إليها في المبحث الأول من هذا الفصل.

وفي سنة 2015 أصدر القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر وتناول فيه فصلًا كاملًا للأحكام الجزائية المتعلقة بالجرائم الماسة بالتوقيع والتصديق الإلكترونيين، إلا أنه جاء خاليًا على أي نص يعالج فيه تزوير التوقيع الإلكتروني أو المستند الإلكتروني، على غرار المشرع المصري الذي نص بصورة صريحة على جريمة تزوير التوقيع الإلكتروني والمحرر الإلكتروني والوسيط الإلكتروني بمقتضى قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر.

إلا أنه في سنة 2024 تدارك الأمر وأصدر قانون خاص ومستقل متعلق بمكافحة التزوير وإستعمال المزور بمقتضى القانون رقم: 24-02 المؤرخ في 26 فيفري 2024 السالف الذكر وألغى جميع الأحكام المخالفة له والمنصوص عليها في قانون العقوبات الجزائري، وقام بالتوسيع من مفهوم المستند ليشمل المستندات الإلكترونية ضمن المستندات محل جريمة التزوير، وبإضافة أحكام جديدة في سبيل مواجهة هذه السلوكيات الإجرامية والتصدي لها،

[1]- القانون رقم: 14-03 المؤرخ في 24 فيفري 2014، المتعلق بسندات ووثائق السفر، ج.ر.ج.ج.ش العدد 16، الصادرة في 23 مارس 2014.

[2]- المرسوم الرئاسي رقم: 14-252 المؤرخ في 08 سبتمبر 2014، ج.ر.ج.ج.ش العدد 57، الصادرة بتاريخ 28 سبتمبر 2014.

وعرف التزوير بموجب المادة 03 منه كالآتي: "التزوير : كل تغيير للحقيقة عن طريق الغش في أحد المحررات أو الوثائق أو الدعائم المنصوص عليها في هذا القانون، بأي وسيلة من شأنه إحداث ضرر، ويهدف أو من شأنه أن يترتب عليه إقرار حق أو صفة أو واقعة ترتب آثارًا قانونية، ويشمل التزوير التقليد والتزييف المنصوص عليهما في هذا القانون"

الفرع الأول: جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور

ارتأينا تناول جريمة تزوير المستند الإلكتروني، ثم التطرق إلى جريمة إستعمال المستند الإلكتروني المزور.

أولًا: جريمة تزوير المستند الإلكتروني

التزوير بشكل عام هو: "تغيير الحقيقة أيا كانت وسيلته وأيا كان موضوعه"، أما التزوير في المستندات فهو حسب تعريفه المستقر هو: "تغيير الحقيقة في مستند بإحدى الطرق التي نص عليها القانون، تغييرًا من شأنه إحداث ضرر مقترن بنية إستعمال المستند المزور فيما أعد له".[1]

وتنشأ جريمة تزوير المستند الإلكتروني بتوافر ركنين أساسيين، ركن المادي وهو السلوك الإجرامي المتمثل في فعل تغيير الحقيقة وأن ينصب هذا تغيير على مستند إلكتروني وأن يكون قد حدث بإحدى الطرق التي حددها القانون على سبيل الحصر، والركن المعنوي المتمثل في القصد الجنائي العام والخاص بعلم وإتجاه إراداة الجاني إلى إرتكاب الفعل المعاقب عليه قانونًا قصد إحداث ضرر للغير.

1- الركن المادي لجريمة تزوير المستند الالكتروني:

يتجسد الركن المادي لجريمة تزوير المستندات الإلكترونية في كل فعل يؤدي إلى تغيير الحقيقة في مستند إلكتروني، ويتم هذا التزوير بإحدى الطرق التي نص عليها القانون، وأن يكون من شأن هذا التغيير إحداث ضرر أو إحتماله، وتبعًا لذلك يمكن تقسيم الركن المادي إلى أربعة عناصر كالآتي:

أ- وجود المستند كمحل التجريم:

يتمثل محل الجريمة في وجود الوثيقة أو المستند بمعنى الشيء الذي ينصب ويقع عليه فعل التزوير، وأن يكون المستند الإلكتروني هو الذي تأثر بالتغيير الذي أحدث عليه سواء بالإضافة أو الحذف أو التعديل أو أي فعل من شأنه تغيير حقيقة المعطيات الواردة في هذا المستند على نحو يسبب به ضررًا لصاحبه الأصلي، بمعنى أن النشاط الإجرامي في هذا النوع من الجرائم يرد على محل أو موضوع محدد هو المستند الإلكتروني وما يتضمنه من معطيات

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 183.

ومعلومات تمت معالجتها آليًا[1]، ومن هذا المنطلق لا تقوم جريمة التزوير إذا كان تغيير الحقيقة قد تم بقول أو بفعل، كما لا تقوم لو حصل تغيير الحقيقة في وثيقة لا يمكن الإستناد إليها لممارسة حق أو عمل.[2]

ب- السلوك الإجرامي:

يتمثل السلوك الجرمي المكون للجريمة محل الدراسة في فعل تغيير الحقيقة ويعني إستبدالها بما يخالفها، وإذا إنتفى هذا التغيير إنتفى التزوير وبالتالي فلا يعتبر تغييرًا للحقيقة إذ ظل مضمون المستند في حالته الأصلية.[3]

ويكفي لتغيير الحقيقة الذي تتطلبه جريمة التزوير أن يكون هناك مساس بحقوق الغير أو مراكزهم القانونية الثابتة في تلك المستندات[4]، ولا يتطلب القانون أن تغيير الحقيقة برمتها وإنما تقوم الجريمة بأقل قدر من التغيير، فيستوي أن يقع التغيير في مضمون المستند بكامله أو ينصب التغيير على واحد فقط من معطياته[5].

ولذلك يتصور وقوع التزوير في النطاق المعلوماتية عن طريق تغيير الحقيقة على المستندات التي تمثل المخرجات الإلكترونية، طالما أن التغيير ذاته قد طال المعطيات الموجودة في الجهاز الإلكتروني، شرط حصول الضرر والذي يتمثل في إهتزاز الثقة المفترضة في المستندات الرسمية حال التزوير المعلوماتي في المستند الرسمي، أو المساس بحق لأحد الأفراد وذلك حال التزوير المعلوماتي في المستند العرفي.[6]

ج- طرق التزوير:

لا يتحقق الركن المادي للتزوير بمجرد تغيير الحقيقة بأية طريقة من الطرق، وإنما يجب أن يكون هذا التغيير قد حدث بإحدى الطرق المنصوص عليها في القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر، والتي جاءت على سبيل الحصر في التزوير المعنوي والتزوير المادي.

---

[1]- بلحسيني حمزة، مرجع سابق، ص 199.

[2]- أحسن بوسقيعة، مرجع سابق، ص 452

[3]- آمال قارة، مرجع سابق، ص 139.

[4]- نفس المرجع، ص 139.

[5]- أحسن بوسقيعة، مرجع سابق، ص 456.

[6]- عبدالفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، د.ر.ط، 2005، دار الكتب القانونية، مصر، ص 140.

ج-1- التزوير المعنوي: يعرف بأنه كل تغيير لحقيقة المستند أثناء إنشاؤه لا بعده، وعلى هذا الأساس يقع من الشخص المكلف بكتابة المستند، كما أن لا يترك أثرًا ماديًا مما يصعب إكتشافه.[1]

وفقًا لما سبق ذكره، يثار التساؤل حول مدى إمكانية تزوير الكتابة والتوقيع الإلكترونيين من خلال طرق التزوير المعنوي؟

يرى البعض إمكانية حدوث تزوير الكتابة والتوقيع الإلكترونيين بطرق التزوير المعنوي، في ظل ما نشهده من توغل الوسائل التقنية والتكنولوجية الحديثة في حياتنا اليومية المعاصرة، وذلك في عمليات دفع الفواتير والشراء عن بعد وعمليات البنوك والمؤسسات والشركات بإختلاف أنواعها.[2]

ويكون ذلك بتغيير إقرارات أولى الشأن بالتدخل من خلال المنظومة المعلوماتية لتسجيل معطيات لم تصدر من المتعاقدين أو أولى الشأن، أي تدوين إتفاقات أو أقوال غير التي صدرت من المتعاقدين أو أملوها[3]، حيث يتصور قيام الموظف العام المختص بتحرير العقود والكتابات الرسمية بتغيير الحقيقة، وذلك بتغيير إقرارات أولى الشأن عند مرحلة إدخال المعطيات المتلقاة وتحريره لكتابة رسمية في شكل إلكتروني ووضعه للتوقيعات الإلكترونية لأطرافها[4]، عندما يكلف مثلًا بكتابة مستند وفقًا للمعطيات والشروط التي طلب صاحب الشأن إثباتها بالمستند، فيكتب معطيات وشروطًا آخرى مغايرة لما طلبه[5]، أو أن يقوم في وثيقة بنكية التي يحصل على بياناتها من ذوي الشأن أو فاتورة الهاتف فيثبت سداد جزء منها على حين أن صاحبها سددها كاملة، أو يثبت التسوية المالية لمعاملات أحد العملاء دون أن يكون ذلك حقيقيًا[6].

أو جعل واقعة مزورة فى صورة واقعة صحيحة عن طريق إثبات وقائع كاذبة أو غير معترف بها، ومن ذلك مثلًا يلجأ الجاني إلى جعل واقعة غير صحيحة في صورة واقعة صحيحة أو غير معترف بها في صورة واقعة معترف بها، كوقائع الميلاد والوفاة والولاية والوصاية وغيرها من الأمور التي يختص بها الموظف الموكل إليه هذا الأمر إذا ما كان من مستخدمي المنظومة المعلوماتية في نشاطه الوظيفي.[7]

---

[1]- راضية مشري، **جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري**، جامعة 08 ماي 1945 قالمة، حوليات جامعة قالمة للعلوم الإجتماعية والإنسانية، المجلد11، العدد20، جوان 2017، الجزائر، ص131.

[2]- باهة فاطمة، مرجع سابق، ص 339.

[3]- رمزي بن الصديق، **تزوير المحررات الإلكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية**، كلية الحقوق والعلوم السياسية، جامعة تامنغست، مجلة الإجتهاد للدراسات القانونية والإقتصادية، المجلد 07، العدد02، 2018، الجزائر، ص 208.

[4]- باهة فاطمة، مرجع سابق، ص 339.

[5]- حبيباتني بثينة، مرجع السابق، ص 208.

[6]- باهة فاطمة، مرجع سابق، ص 339.

[7]- فؤاد حسين العزيزي، **الجرائم المعلوماتية دراسة مقارنة**، د.ر.ط، 2014، دار الفكر الجامعي، الإسكندرية-مصر، ص 356.

كما يمكن وقوع التزوير المعنوي بإنتحال شخصية الغير، وذلك بإستيلاء الجاني مثلًا على البطاقات الشخصية للغير بالحصول عليها بعد فقدها أو بسرقتها والإدعاء بأنها تخصه، ومن ثمة إستعمالها في العمليات التي أنشأت من أجلها كالسحب أو الدفع أو غير ذلك.[1]

فالتزوير في المعلوماتية لا يتصور وقوعه بإحدى الطرق المعنوية للتزوير والتي لا تتحقق إلا أثناء التعبير عن الأفكار، والفرض أن تلك الأفكار قد تم التعبير عنها من قبل، بينما يقع التزوير في هذا المجال عن طريق الإستعانة بطرق التزوير المادية اللاحقة، وهي التقليد والتوقيع، والحذف، والإضافة، والتغيير.[2]

ج-2- التزوير المادي: التزوير المادي يعرف بأنه كل تغيير للحقيقة ينصب على مصدر المستند بأن ينسب المستند إلى غير منشئه، أو يتناول بالتعديل صلب المستند بعد إنشائه من المستند الحقيقي، ويتم من خلال وضع توقيع مزور، حذف أو إضافة أو تغيير مضمون المستند، وإصطناع المستند.[3]

وفقًا لما سبق ذكره، يثار التساؤل حول مدى إمكانية تزوير الكتابة والتوقيع الإلكترونيين من خلال طرق التزوير المادي ؟

إمكانية وقوع تزوير الكتابة والتوقيع الإلكترونيين بهذه الطرق فهو أمر وارد، ذلك أنه بالإمكان التلاعب في معطيات الكتابة والتوقيع الإلكترونيين وتغيير الحقيقة فيها بالإضافة أو الحذف أو التعديل، كلما كانت المعالجة الآلية لهذه المعطيات تسمح بإدخال وإضافة معطيات جديدة أو محو جزء منها أو كلها أو تعديلها وإستبدالها بآخرى.[4]

فالتزويرالمادي يتم من خلال الدخول غير المصرح به خفية إلى المنظومة المعلوماتية، ويمكن أن يتم عن طريق الحذف بإزالة كلمة أو رقم أو رمز معين[5]، وقد يتحقق بفعل الإدخال مؤداه قيام الجاني بإضافة معطيات جديدة لم تكن موجودة إلى معطيات المستند الأصلي على نحو يغير من مضمونه ويترتب عليه آثارًا قانونية، كقيام الجاني وهو الموظف المختص أو مأمور الضرائب بإضافة أرقام أو كلمات أو حروف إلى المعطيات الخاصة بالعملاء، على نحو يؤدي إلى زيادة التكاليف الإنتاجية والتي تخصم من الضريبة المستحقة مما يقلل من المبلغ الضريبي المستحق[6]، ويمكن أن يتم عن طريق الإبدال بحذف شيء من المستندات وإثبات غيره بدلًا منه[7].

---

[1]- باهة فاطمة، مرجع سابق، ص-ص 339-340.

[2]- خثير مسعود، مرجع سابق، ص 137.

[3]- راضية مشري، مرجع سابق، ص 131.

[4]- باهة فاطمة، مرجع سابق، ص 338.

[5]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 396.

[6]- فؤاد حسين العزيزي، مرجع سابق، ص 355.

[7]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 396.

كما يمكن أن يقوم الجاني بإستخدام إمكانيات النظم المعلوماتية من خلال السحب الإلكتروني لإمضاء أو خاتم أو بصمة لشخص ما، من خلال وحدة إدخال النصوص والصور المسماة بالماسح الضوئي، فيتمكن من خلال ذلك بوضع الإمضاء أو الختم الذي تم سحبه بواسطة وحدة معالجة المدخلات للمنظومة المعلوماتية، ووضعها على المستند الذي يهدف الجاني إلى تغيير الحقيقة في محتواه بإستخدام تلك الطريقة، حيث يكون المستند بمعلوماته متواجد داخل المنظومة، ويخرج بعد ذلك في صورة مخرجات ورقية يتم الإعتماد عليها في تقرير أثر قانوني يتم البناء عليه.[1]

كما يمكن كذلك وضع الإمضاءات المزورة على المستندات المعالجة آلياً عن طريق الإستخدام الغير المشروع للأرقام الشخصية السرية للدخول بعد الحصول عليها أو من خلال سرقة منظومة التوقيع بها[2]، عند إستخدام مثلًا بطاقة الإئتمان داخل ماكينة السحب الآلي للنقود فإن الماكينة تطلب من مستخدم البطاقة إدخال الرقم السري الخاص بالبطاقة، فإذا كان المتعامل مع بطاقة الإئتمان سواء كانت صحيحة أو مزورة غير حاملها الشرعي وبغير رضاه فإنه بإدخال الرقم السري هذا يكون قد وضع إمضاء مزورًا لا يعرب عن إرادة صاحب البطاقة في سحب النقود، بإعتبار أن النقر على لوحة مفاتيح ماكينة السحب الآلي يعتبر توقيعًا إلكترونيًا من صاحب الحق في ذلك[3].

د- الضرر:

لا يكفي لقيام جريمة تزوير المستند الإلكتروني تحقق الركن المادي في تغيير الحقيقة في المستند الإلكتروني فحسب، وأن يتم هذا التغيير بإستخدام إحدى الطرق التي نص عليها القانون، وإنما يجب أن يكون من شأن ذلك إحداث ضرر للغير، فالضرر عنصر جوهري في قيام جريمة التزوير فهو التهديد أو الإعتداء على كل مصلحة يحميها القانون، كما يعرف بأنه فقد أو نقص أو مساس بحال أو مصلحة يحميها القانون، ولا يميز في الضرر الذي يمس بالحقوق أو مصالح محمية بين الضرر المادي أو الأدبي، كما يستوي أن يكون مساسًا بمصلحة عامة أو خاصة[4]، ولا يشترط لقيام الجريمة أن يكون الضرر محققًا بالفعل، وإنما أيضًا يعد الضرر متوافرًا حتى ولو كان محتمل الوقوع والذي يكفي فيه الشروع في إستعمال المستند، فتقدير وجود الضرر هي مسألة موضوعية تخضع فى تقديرها لمحكمة الموضوع حسب ظروف كل دعوى[5].

---

[1]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص-ص 206-207.

[2]- باهة فاطمة، مرجع سابق، ص 338.

[3]- إيهاب فوزي السقا، **جريمة التزوير في المحررات الإلكترونية**، د.ر.ط، 2008، دار الجامعة الجديدة للنشر، الإسكندرية- مصر، ص 63.

[4]- بن شهرة شول، مرجع سابق، ص 180.

[5]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص397.

2- الركن المعنوي لجريمة تزوير المستند الإلكتروني:

جريمة تزوير المستند الإلكتروني من الجرائم العمدية التي يتطلب لقيامها توفر القصد الجنائي العام لدى المزور، الذي يتمثل في علم الجاني على وجه اليقين بأن ما حصل من تغيير فيه يعتبر مستندًا في نظر القانون وأنه لا يجوز أن يقع عليه أي تغيير للحقيقة، ضف إلى ذلك ضرورة علم الجاني بأن الطريقة التي حصل بها التزوير هي بإحدى الطرق المنصوص عليها قانونًا، ومن شأن هذا التغيير إلحاق ضرر فعلي أو إحتمالي للغير، ويجب أن تتجه إرادته السليمة إلى إتيان بهذا الفعل.

وقد تطلبت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 ضرورة توافر القصد الجنائي الخاص في جرائم التزوير المعلوماتي بموجب المادة 07 منها التي نصت على أن: "ويمكن لأي طرف أن يشترط في قانونه الداخلي نية الغش أو نية إجرامية مشابهة من أجل تقرير المسؤولية الجنائية"[1]، وتشير المذكرة التفسيرية للإتفاقية إلى ضرورة السماح للأطراف عند وضع الجريمة موضع التنفيذ في القانون الداخلي إمكانية إضافة شرط نية الغش أو نية إجرامية مماثلة أو مشابهة قبل تقرير المسؤولية الجزائية[2]، وهو ما أشار إليه المشرع الجزائري بإستعماله لمصطلح "عن طريق الغش" في تعريفه لمصطلح "التزوير" بموجب المادة 03 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر.

وقد ثار خلاف حول تحديد هذا القصد، فقد ذهب البعض إلى أن المقصود بالسوء النية في جريمة التزوير هي أن تتجه نية الجاني وقت إرتكاب فعل تغيير الحقيقة إلى إستعمال المستند الإلكتروني المزور فيما زور من أجله أي الإحتجاج به على إعتبار أنه صحيح، أو دفع مضرة عنه أو عن غيره.[3]

ومع ذلك يجب التنبيه إلى أن إستعمال المستند الإلكتروني المزور ليس ركنًا في جريمة التزوير، فقد لا يستخدم المستند قط ومع ذلك تقوم الجريمة إذا توفرت لدى الجاني نية إستعمال المستند كمسألة نفسانية محضة.[4]

وعلاوة على ذلك لابد من أن يتوافر في التزوير قصدًا خاصًا، والذي قد يكون نية إستعمال المستند الإلكتروني المزور فيما زورمن أجله أو نية الغش أو نية الإضرار بالغير وهو

[1]-Art 07 du convention sur la cybercriminalité dispose que : « ...Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée».

[2]- هلالي عبداللاه أحمد، مرجع سابق، ص110.

[3]- بلحسيني حمزة، مرجع سابق، ص201.

[4]- أحسن بوسقيعة، مرجع سابق، ص 460.

المجني عليه أو أي نية إجرامية أخرى تعد ضرورية لإستكمال البنيان القانوني لجريمة التزوير.[1]

ويرجع لقاضي الموضوع تقدير توافر القصد العام والخاص، وهو غير ملزم بذكره في الحكم صراحة إذا ما ورد في أسباب الحكم ما يدل عليه.[2]

ثانيًا: جريمة إستعمال المستند الإلكتروني المزور

إذا كان التزوير في مدلوله العام يعني تغيير الحقيقة أيا كانت وسيلته، فإن هذا التغيير يمكن أن يقترن بنية إستعمال ما زور لتحقيق أغراض غير مشروعة وإلحاق ضرر بالغير، ومن ثم فإن إستعمال المستندات المزورة يعد قانونًا جريمة مستقلة عن جريمة التزوير.[3]

ولقيام جريمة إستعمال المستند الإلكتروني المزور لابد من توافر ركنين أساسيين: الركن المادي ويتمثل في السلوك الإجرامي المتمثل في فعل الإستعمال، شريطة أن ينصب هذا الفعل على مستند إلكتروني تم تزويره، والركن المعنوي وهو القصد الجنائي والذي يقتضي علم الجاني بأن المستند الذي يستعمله مزور، ومع ذلك يقدم على استعماله بإرادته الحرة.

1- الركن المادي لجريمة إستعمال المستند الإلكتروني المزور:

يتحقق الركن المادي في جريمة إستعمال المستند الإلكتروني المزور بإرتكاب الجاني لفعل الإستعمال والذي ينصب على مستند مزور مع علمه بذلك.

أ- فعل الإستعمال:

يعد إستعمال المستند الإلكتروني المزور هو السلوك الإجرامي والقاعدة الأساسية التي تقوم عليها الجريمة محل الدراسة، وفي هذا يعرف الإستعمال بأنه إبراز المستند المزور والتمسك به على إعتبار أنه صحيح[4]، وعرفت محكمة النقض المصرية الإستعمال بأنه: "معنى عامًا يندرج فيه كل فعل إيجابي يستخدم به المستند المزور والإستناد إلى ما دون فيه، ويستوي في ذلك أن يكون هذا الإستعمال قد بوشر على جهة رسمية أو على موظف عام، أو كان حاصلًا في معاملات الأفراد"[5].

وبالنظر إلى موقف الفقه الفرنسي نجد تحديد معنى الإستعمال أخذ إتجاهين، فالإتجاه الأول أخذ بالمفهوم الضيق حيث يرى بوجوب أن تكون هناك علاقة تزامن بين فعل التزوير وفعل الإستعمال أي فلابد أن يكون هناك إرتباط بينهما، أما المفهوم الموسع فيرى أن مجرد

[1]- فؤاد حسين العزيزي، مرجع سابق، ص-ص 364-365.
[2]- أحسن بوسقيعة، مرجع سابق، ص 460.
[3]- بلحسيني حمزة، مرجع سابق، ص 209.
[4]- نفس المرجع، ص 210.
[5]- إيهاب فوزي السقا، مرجع سابق، ص79.

إستعمال أو إستخدام المستند المزور يشكل جريمة الإستعمال دون إشتراط أن يستخدم المستند فيما زور من أجله، إلا أنه لا يمكن الأخذ بهذا الإتجاه الأخير فيما يتعلق بالمستندات الإلكترونية لا يتطابق وذاتية المعلومات، الأمر الذي يدفعنا إلى بيان ذاتية الإستعمال فيما يتعلق بحالة إستعمال المستندات الإلكترونية المزورة[1]، وهي تتميز بعدد من الخصائص، من أبرزها ما يلي:

- إختلاف مفهوم الإستعمال عن مفهوم التزوير ذاته، فبالرغم من وجود علاقة بين النصين القانونيين بوجود التزوير إلا أنه يتبقى لمفهوم الإستعمال ذاتية تختلف عن مفهوم التزوير نابعة من وجود نصين قانونيين، أحدهما يتعلق بالتزوير والآخر يتعلق بالإستعمال، ويترتب على هذا المفهوم نتائج عديدة أهمها أن الفاعل في جريمة الإستعمال قد يختلف عن الفاعل في جريمة التزوير، كما أن الفاعل فى جريمة الإستعمال لا تطبق عليه عقوبة الإشتراك في جريمة التزوير، كما قد يكون الفاعل فاعلًا لكل من جريمتي التزوير والإستعمال، فإنه من الممكن أن يبرأ عن أحد الجريمتين دون أن يتم تبرئته عن الجريمة الأخرى[2]؛
- يعد الإستعمال تامًا ومكتملًا فى حالة تقديم وإبراز أو نقل المستند المزور، وفي هذه الحالة فلا يشترط أن يؤدي هذا الإستعمال إلى تحقيق النتيجة المطلوبة، ويعد العدول اللاحق على الإستعمال نتيجة الندم أو التوبة غير مؤثر فى قيام المسؤولية الجنائية[3]؛
- اختلف حول طبيعة جريمة إستعمال المستند المزور، فهناك من يرى أن جريمة إستعمال مستند مزور جريمة وقتية تقع بمجرد التمسك بالمستند المزور، وهناك من يرى أن جريمة الإستعمال جريمة مستمرة وليست جريمة وقتية إذ تظل الجريمة قائمة طالما بقى الفاعل محتج بالمستند المزور ولا تنتهي حالة الإستمرار إلا إذا تنازل الفاعل عن التمسك بالمستند المزور أو أن يصدر حكم نهائي بتزوير المستند، وهناك من يرى أن جريمة الإستعمال تعد جريمة وقتية إلا أنها قابلة للتجديد، فهي ليست جريمة مستمرة تبقى موجودة بدون مساهمة جديدة بل لابد وأن تكون هناك مساهمة جديدة، وفي هذه الحالة فإن هذا الفعل فقط هو الذي يؤدي إلى قيام هذه الجريمة، يترتب على ذلك إمكانية أن يتم معاقبة أكثر من شخص بجريمة الإستعمال، وذلك كما لو قام شخصان كل على حدة بإستعمال المستند المزور، ففي هذه الحالة سيعاقب كل شخص منهما بجريمة إستعمال مستقلة عن الجريمة الأخرى[4].

ولقيام جريمة إستعمال المستند المزور، يشترط أن يقدم هذا المستند للإحتجاج به والإستناد إليه في إثبات حق أو مصلحة أو مركز قانوني أو صفة أو شخصية أو للحصول على تصريح ما، من الجهات المختصة بإصدار التصاريح أو التراخيص.[5]

---

[1]- أحمد خليفة الملط، **الجرائم المعلوماتية**، الطبعة الثانية، 2006، دار الفكر الجامعي، الإسكندرية-مصر، ص 480.

[2]- نفس المرجع، ص 480.

[3]- نفس المرجع، ص 480.

[4]- محمد أمين الرومي، **جرائم الكمبيوتر والإنترنت**، د.ر.ط، 2004، دار المطبوعات الجامعية، الإسكندرية-مصر، ص-ص 116-117.

[5]- فؤاد حسين العزيزى، مرجع سابق، ص 365.

فالإستعمال يقتضي توافر أمرين تقديم المستند المزور والإحتجاج به، وبالتالي فإن مجرد تقديم المستند المزور أو إبرازه لا يعد إستعمالًا له إن لم يقترن ذلك بالتمسك بالمستند أو الإحتجاج به على إعتبار أنه صحيح[1]، ولذلك لو تخلفت إرادة الإستفادة من المستند المزور أو لم تكن مصحوبة بسلوك إحتجاجي يهدف إلى ترتيب آثار المستند الصحيح لم تقم جريمة الإستعمال، ولهذا لا تقر حيازة المستند المزور إستعمالًا له ولو أقر الشخص بوجوده عنده أو تم ضبطه لديه، بل إن الفعل لا يشكل جريمة أصلًا ما لم يثبت أن الحائز هو الذي قام بالتزوير[2].

كذلك فإن إيداع المستند المزور لدى الغير لحفظه لا يعد إستعمالًا له سواء أنبيء الغير بأن المستند مزور أو صحيح، وإذا أمر القضاء شخصًا بأن يقدم مستندًا يحوزه فقدمه مختارًا ولم يحتج به فذلك ليس إستعمالًا للمستند المزور ولو كان عالمًا بتزويره وذلك لأن لم يزوره ولم يقدمه للإستعمال، أن يقوم الجاني بإستعمال الوثيقة المعلوماتية المزورة أو المستند المزور أو الدعامة المزورة ويقدمها للإحتجاج بهما مع علمه أنها مزورة بمعنى أن تنصرف إرادته لهذا الإستعمال مع علمه بالطبع بتزويرها، وذلك لأن جريمة الإستعمال جريمة عمدية سواء كان الإستعمال لمستند مزور تقليديًا أو معلوماتيًا وهو ما أكده القضاء الفرنسي في شأن إستعمال الوثيقة المعلوماتية المزورة.[3]

ب- محل الجريمة (المستند المزور) :

إلى جانب فعل الإستعمال كشرط جوهري في الجريمة محل الدراسة فإنه يشترط كذلك أن ينصب الإستعمال على مستند إلكتروني مزور، حيث أن هذه الجريمة لا تقوم إلا إذا كان نشاطها الإجرامي منصبًا على مستند إلكتروني ثبت تزويره، ومن ثم فلا يجوز الإستناد في إدانة المتهم من أجل إستعمال مستند إلكتروني مزور على جريمة تزوير لم تثبت قانونًا.[4]

ويشترط أن يكون المستند المزور حجة في الإثبات، ويتطلب ذلك أن يكون المستند منسوب صدوره إلى جهة أو هيئة أو شخص آخر غير من يقدم مستند المعلومات المزور لإستعماله أمام الغير.[5]

2- الركن المعنوي لجريمة إستعمال المستند الإلكتروني المزور:

جريمة إستعمال المستندات الإلكترونية المزورة جريمة عمدية يتطلب لقيامها توفر عنصري العلم والإرادة لدى الجاني، فيتحقق القصد الجنائي العام فيها بإتجاه إرادة الجاني إلى

[1]- أحمد خليفة الملط، مرجع سابق، ص 479.

[2]- إيهاب فوزي السقا، مرجع سابق، ص 80.

[3]-عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع السابق، ص 263.

[4]- بلحسيني حمزة، مرجع سابق، ص 211.

[5]- محمد أمين الرومي، مرجع سابق، ص 117.

إستعمال المستند والتمسك به على أنه صحيح مع العلم بتزويره، لذلك يجب أن يثبت علم الجاني اليقيني بتزوير المستند فإذا إنتفى العلم لديه إنتفى القصد الجنائي.

كذلك يشترط أن يقوم العلم وقت إستعمال الجاني للمستند المزور وليس بعد الإستعمال بأن المستند الذي بين يديه مزور، ويشترط أن تبين المحكمة ما يثبت توافر العلم اليقيني لدى الجاني بكون المستند مزورًا عند استعماله، فمجرد التدليل على أن المتهم تمسكه بمستند مزور لا يكفي في ثبوت العلم لديه بأن المستند مزور خاصة إذا كان المتهم ليس هو من قام بتزوير المستند أو إشترك في تزويره.[1]

الفرع الثاني: العقوبات المقررة لجريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور

نخصص الفرع الثاني لدراسة العقوبات المقررة لكل من جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور، حيث نتناول أولًا العقوبات التي أقرتها التشريعات المقارنة، ثم ننتقل إلى موقف المشرع الجزائري.

أولًا: موقف التشريعات المقارنة

سنتناول في البداية موقف المشرع الفرنسي، ثم ننتقل إلى موقف المشرع المصري.

1- موقف المشرع الفرنسي:

إعترف المشرع الفرنسي بجريمة التزوير المعلوماتي بما فيها تزوير وإستعمال المستند الإلكتروني المزور منذ سنة 1988، وذلك بموجب القانون رقم: 88-19 الصادر بتاريخ 05 جانفي 1988 المتعلق بالغش المعلوماتي، وأفرد لهذه الجريمة نصًا مستقلًا وعاقب فيه على تزوير الوثائق المعالجة آليًا بموجب المادة 462-5 منه كالآتي :"يعاقب بالسجن من سنة (01) إلى خمسة (05) سنوات وبغرامة من عشرون ألف 20.000 فرنك إلى مليوني 2.000.000 فرنك، من قام بتزييف الوثائق المعلوماتية مهما كان شكلها أو طبيعتها وذلك للإضرار بالغير".[2]

وكذا تجريم إستعمال الوثائق المعالجة آليًا المزورة وجعل عقوبتها مساوية لعقوبة التزوير بموجب المادة 462-6 منه كالآتي: "يعاقب بالحبس من سنة (01) إلى خمسة (05) سنوات وبغرامة يتراوح مقدارها من عشرون ألف 20.000 فرنك إلى مليوني 2.000.000 فرنك أو

[1]- محمد أمين الرومي، مرجع سابق، ص 118.

[2]- Art 462-5 du C.P.F (créé par Loi 88-19 du 5 janvier 1988 art.1 JORF 6 janvier 1988, Abrogé par Loi n°92-1336 du 16 décembre 1992-art .372 V JORF 23 décembre 1992 en vigueur le 1er mars1994) disposse que : «Quiconque aura procédé la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000 F à 2.000.000 F»

بإحدي هاتين العقوبتين، كل من قام عمدًا بإستعمال الوثائق المعلوماتية المشار إليها في المادة 462-5.[1]

وسع المشرع الفرنسي بموجب هذا التعديل من محل التزوير -وسع من مفهوم المستند-، بحيث لم يعد يقتصر على ما يمكن تصنيفه تحت وصف المكتوب فقط وإنما أصبح يمتد ليشمل أي دعامة أخرى للتعبير عن الأفكار، وهذا لا ينطبق فقط على المستندات المعالجة آليًا بل يشمل أيضًا البرامج أيا كان نوعها والمعلومات المسجلة على وسائط إلكترونية ولو لم يتم معالجتها بعد، أو لم يتم إدخالها بعد إلى الجهاز الإلكتروني، والتعليمات المتعلقة بكيفية تشغيل البرامج وكذلك تذاكر المترو والبطاقات البنكية وبطاقات السحب وبطاقات الائتمان أو الدفع حتى ولو لم تدخل الخدمة.[2]

إلا أنه وبعد صدور القانون الفرنسي الجديد في 16 ديسمبر 1992 والذي بدأ به في الأول من مارس 1994، قرر المشرع الفرنسي بإلغاء النص الخاص بتزوير المستندات المعالجة آليًا وإستعمالها والإكتفاء بإضافته إلى النصوص التقليدية الخاصة بالتزوير، بعد تطويع نصوصها بما يتلاءم وتلك المستندات والذي يشمل المستندات الإلكترونية والتقليدية بذات الحماية الجنائية.[3]

وأصبح ينص على هذه الجريمة في المادة 441-1 في شأن تزوير المحررات العرفية والرسمية المعدلة بالأمر رقم: 2000-916 المؤرخ في 19 سبتمبر 2000 كالآتي: "يعد تزويرًا كل تغيير أو تحريف في الحقيقة، من شأنه أن يحدث ضررًا ويتم بأي وسيلة كانت، وينصب على محرر أو على أي دعامة للتعبير عن الأفكار يكون موضوعها أو يمكن أن يترتب عليه إقامة الدليل على ثبوت حق أو واقعة ذات آثار قانونية".[4]

أما المادة 441-2 فقد تناولت التزوير في المحررات الرسمية وجاء فيها: "يعاقب على التزوير الذي يرتكب في وثيقة مسلمة بواسطة الإدارة العامة بهدف إثبات الإعتراف أو إثبات حق أو هوية أو منح تصريح، بالسجن لمدة ثلاثة (03) سنوات وغرامة قدرها خمس وسبعون ألف 75000 يورو .ويعاقب على إستعمال التزوير المذكور في الفقرة السابقة بذات العقوبة.

---

[1]- Art 462-6 du C.P.F (créé par Loi 88-19 du 5 janvier 1988 - art .1 JORF 6 janvier 1988, Abrogé par Loi n°92-1336 du 16 décembre 1992 – art .372 V JORF 23 Décembre 1992 en vigueur le 1er mars 1994) dispose que: «quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000 F à 2.000.000 F ou de l'une de ces deux peines».

[2]- بلحسيني حمزة، مرجع سابق، ص 204.

[3]- سحر سعد عبد السميع محمد، مرجع سابق، ص161.

[4]-Art 441-1 du C.P.F (modifié par Ordonnance n°2000-916 du 19 septembre 2000-art.3 v JORF 22 septembre 2000 en vigueur le 1 er janvier 2002) dispose que:«Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45 000 euros d'amende».

وتشدد العقوبة إلى السجن سبع (07) سنوات وغرامة قدرها مائة ألف 100.000 يورو عند إرتكاب التزوير أو إستعمال التزوير:

1- إما بواسطة شخص مؤتمن على السلطة أو مكلف بمهمة في الخدمة العامة، وتصرف أثناء ممارسته لوظائفه؛

2- وإما بطريقة إعتيادية؛

3- بقصد تسهيل إرتكاب جريمة، أو لتزوير مستند يساعد الإفلات من العقاب لمرتكبيها".[1]

وكان السبب الذي أدى إلى إلغاء النص الخاص بالتزوير المعلوماتي هو أن إفراد جرائم التزوير الواقعة على المستندات الإلكترونية سوف يكون من غير جدوى ما دام مفهوم التزوير نفسه غير واضح المعنى، وهو ما دفع بالمشرع الفرنسي إلى إدراج تعريف للتزوير في نص المادة 441 من قانون العقوبات الجديد التي أصبحت تشمل كل صور التزوير الحديثة التي تنشأ عن إستخدام الأجهزة الإلكترونية.[2]

2- موقف المشرع المصري:

نظم المشرع المصري جرائم التزوير في قانون العقوبات ضمن الباب السادس عشر من الكتاب الثاني تحت عنوان "التزوير" من خلال المواد من 206 إلى 225، التي تحدد العقوبات تبعًا لنوع المستند محل التزوير، وتختلف هذه العقوبات عن تلك المقررة لجرائم إستعمال المستندات المزورة، مع العلم أن جميع هذه الأحكام تنصب على المستندات العادية.

وجرم المشرع المصري تزوير السجلات الإلكترونية الخاصة بالأحوال المدنية، ويتضح جليًا أنه قد ساوى في قانون الأحوال المدنية رقم: 143 لسنة 1994 بين السجلات الورقية والإلكترونة في تطبيق أحكامه، وقد إعتبر البيانات المسجلة إلكترونيًا بمراكز الأحوال المدنية بيانات تطبيق أحكام هذا القانون، وقانون العقوبات تعتبر البيانات المسجلة إلكترونيًا وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في المستندات الرسمية، فإذا وقع تزوير في المستندات السابقة أو غيرها من المستندات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس (05) سنوات، وقد نصت المادة 74 من قانون الأحوال المدنية

[1]- Art 441-2 du C.P.F (Modifié par Ordonnance n°2000-916 du 19 septembre 2000-art .3 V JORF 22 septembre 2000 en vigueur le 1er janvier 2002) dispose que: « Le faux commis dans un document délivré par une administration publique aux fins de constater un droit, une identité ou une qualité ou d'accorder une autorisation est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. L'usage du faux mentionné à l'alinéa précédent est puni des mêmes peines. Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsque le faux ou l'usage de faux est commis :

1° Soit par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions;

2° Soit de manière habituelle;

3° Soit dans le dessein de faciliter la commission d'un crime ou de procurer l'impunité à son auteur».

[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص-ص 161-162.

رقم: 143 لسنة 1994 على أنه مع القوانين يعاقب بالحبس مدة لا تجاوز ستة (06) أشهر وبغرامة لا تزيد عن خمسمائة 500 جنيه أو بإحدى هاتين العقوبتين، كل من أطلع أو شرع في الإطلاع أو حصل أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الأجهزة الإلكترونية أو وسائط التخزين الملحقة بها، أو قام بتغييرها بالإضافة أو الحذف أو بالإلغاء أو بالتدمير أو بالمساس بها، بأي صورة من الصور أو إذاعها أو إفشاها في غير الأحوال التي نص عليها القانون وفقًا للإجراءات المنصوص عليها فيه، فإذا وقعت الجريمة على البيانات أو المعلومات أو الإحصاءات المجمعة تكون العقوبة السجن.[1]

وبصدور قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر قام بتجريم تزوير التوقيع الإلكتروني والوسيط الإلكتروني والمحرر الإلكتروني بموجب الفقرة الأولى من المادة 23 بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، كل من أتلف أو عيب توقيعًا أو وسيطًا أو محررًا إلكترونيًا أو زور شيئًا من ذلك، بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر، وإستعمل توقيعًا أو وسيطًا أو محررًا إلكترونيًا معيبًا أو مزورًا مع علمه بذلك.

وفي حالة العود تزاد بمقدار المثل العقوبة المقررة لهذه الجريمة في حديها الأدنى والأقصى، وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الإنتشار، وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه.[2]

ونص القانون السابق الذكر صراحة على مسؤولية الجزائية للشخص المعنوي عن الجرائم التي ترتكب بالمخالفة لأحكام هذا القانون حيث نصت المادة 24 منه على أن: "يعاقب المسؤول عن الإدارة الفعلية للشخص الإعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك. ويكون الشخص الإعتباري مسؤولًا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد إرتكبت من أحد العاملين به بإسم ولصالح الشخص الإعتباري".

ثانيًا: موقف المشرع الجزائري

سنتطرق إلى العقوبات المقررة لجريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور، وبالإضافة إلى أحكام العقاب على المشاركة والتحريض والشروع فيها.

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 174.

[2]- الفقرتين 03 و04 من المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 السالف الذكر.

1- العقوبات المقررة لجريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور:

سنتطرق إلى العقوبات التي تسري على الشخص الطبيعي، ثم تلك على الشخص المعنوي.

أ- العقوبات الأصلية المقررة لجريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور:

يقصد بالعقوبات الأصلية تلك العقوبات التي يجوز الحكم بها دون أن تقترن بها أي عقوبة أخرى، ومن هذه العقوبات ما هو مقرر للشخص الطبيعي ومنها ما هو مقرر للشخص المعنوي.

أ-1- العقوبات الأصلية المقررة للشخص الطبيعي:

تتمثل العقوبات الأصلية للشخص الطبيعي في ما يلي:

أ-1-1- العقوبات البسيطة:

تنص المادة 31 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر على أن: "يعاقب بالحبس من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من مليون 1.000.000 دج إلى مليوني 2.000.000 دج، كل شخص عدا من حددتهم المادة 32 إرتكب تزويرًا في محررات عمومية أو رسمية:

1) إما بتقليد أو تزييف الكتابة أو التوقيع،
2) إما بإصطناع إتفاقات أو نصوص أو إلتزامات أو مخالصات أو بإدراجها في هذه المحررات لاحقًا،
3) إما بإضافة أو بإسقاط أو بتزييف شروط أو إقرارات أو وقائع أعدت هذه المحررات لتلقيها أو لإثباتها،
4) إما بإنتحال شخصية الغير أو الحلول محلها".

وتنص المادة 32 من نفس القانون على أن: "يعاقب بالسجن المؤقت من عشرين (20) سنة إلى ثلاثين (30) سنة، كل قاض أو موظف أو ضابط عمومي، إرتكب عن قصد تزويرًا في محررات عمومية أو رسمية أثناء تأدية وظيفته:

1) إما بوضع توقيعات مزورة،
2) إما بإحداث تغييرفي محررات أو خطوط أو توقيعات،
3) إما بإنتحال شخصية الغير أو الحلول محلها،
4) وإما بالكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير بعد إتمامها أو قفلها.

ويعاقب بنفس العقوبة كل قاض أو موظف أو ضابط عمومي قام عن قصد أثناء تحريره محررات من أعمال وظيفته بتزييف جوهرها أوظروفها بطريق الغش، وذلك إما بكتابة إتفاقات خلاف التي دونت أوأمليت أمامه من الأطراف أو بتقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو بالشهادة كذبًا بأن وقائع قد إعترف بها أو وقعت في حضوره أو بإسقاطه أو بتغييره عمدًا الإقرارات التي تلقاها".

وتنص المادة 33 من نفس القانون على أن: "يعاقب بالحبس من سنة (01) إلى خمس (05) سنوات وبغرامة من مائة ألف 100.000 دج إلى خمسمائة ألف 500.000 دج كل شخص ليس طرفًا في المحرر أدلى أمام ضابط عمومي أو موظف بتصريح يعلم أنه غير مطابق للحقيقة، ومع ذلك فإنه يستفيد من العذر المعفي بالشروط المنصوص عليها في قانون العقوبات كل من أدلى بوصفه شاهدًا أمام ضابط عمومي أو موظف بتصريح غير مطابق للحقيقة ثم عدل عنه قبل أن يترتب على إستعمال المحرر أي ضرر للغير، وقبل أن يكون هو نفسه محل متابعة".

وتنص المادة 34 من نفس القانون على أن: "في الحالات المنصوص عليها في هذا الفرع يعاقب بالحبس من خمس (05) سنوات إلى عشر (10) سنوات وبغرامة من خمسمائة ألف 500.000 دج إلى مليون 1.000.000 دج، كل من يستعمل المحرر مع علمه بأنه مزور".

وتنص المادة 36 من نفس القانون على أن: "يعاقب بالحبس من سنة (01) إلى خمس (05) سنوات وبغرامة من مائة ألف 100.000 دج إلى خمسمائة ألف 500.000 دج، كل من إرتكب تزويرًا بإحدى الطرق المنصوص عليها في المادة 31 أعلاه في محررات عرفية".

أ-1-2- العقوبة المشددة:

يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات وبغرامة من ستون ألف 60.000 دج إلى ثلاثمائة ألف 300.000 دج كل من ثبت علمه بوقوع الجريمة من الجرائم المنصوص عليها في القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر بما في ذلك جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور، ولم يبلغ عنها فورًا السلطات العمومية المختصة، وتشدد العقوبة المقررة لتصبح الحبس من سنتين (02) إلى خمس (05) سنوات والغرامة من مائتي ألف 200.000 دج إلى خمسمائة ألف 500.000 دج إذا كان الشخص ممن توصل إلى معرفة هذه الأفعال بحكم وظيفته أو مهنته.[1]

[1]- المادة 73 من القانون رقم: 24-02 السالف الذكر.

في حالة العود تضاعف العقوبات المنصوص عليها في جريمة تزوير المستند الإلكتروني ولجريمة إستعمال المستند الإلكتروني المزور.[1]

أ-1-3- الإعفاء من العقوبة أو تخفيضها:

أقر المشرع الجزائري الإعفاء من العقوبة بموجب الفقرة الأولى من المادة 75 من القانون آنف ذكره والتي تنص على أن: "يستفيد من الأعذار المعفية من العقوبة المنصوص عليها في قانون العقوبات كل من إرتكب أو شارك في جريمة أو أكثر من الجرائم المنصوص عليها في هذا القانون، وقام قبل أي متابعة بإبلاغ السلطات الإدارية و/أو القضائية عنها و/أو كشف هوية مرتكبيها و/أو القبض عليهم أو مكن من حجز محل الجريمة"، ويترتب على ذلك أن يستفيد الفاعل أو الشريك في جريمة تزوير المستند الإلكتروني أو جريمة إستعمال المستند الإلكتروني المزور من العذر المعفي من العقوبة إذا قام بإبلاغ الجهات المختصة السلطات الإدارية أو القضائية عن الجريمة، وساعد على معرفة هوية مرتكبيها أو القبض عليهم، أو مكن من حجز محل الجريمة، وذلك قبل مباشرة إجراءات المتابعة.

ويستفيد من العذر المعفي من العقوبة كل من أدلى بوصفه شاهدًا أمام ضابط عمومي أو موظف بتصريح غير مطابق للحقيقة ثم عدل عنه قبل أن يترتب على إستعمال المستند أي ضرر للغير، وقبل أن يكون هو نفسه محل متابعة.[2]

وأقر المشرع الجزائري التخفيض من العقوبة بموجب الفقرة 02 من المادة 75 من ذات القانون والتي تنص على أن: "تخفض العقوبة المقررة إلى النصف بالنسبة لكل شخص إرتكب أو شارك في إحدى الجرائم المنصوص عليها في هذا القانون، وساعد بعد مباشرة إجراءات المتابعة في القبض على شخص أو أكثر من الأشخاص الضالعين في إرتكابها و/أو كشف هوية من ساهم في إرتكابها"، ويترتب على ذلك أن يستفيد الفاعل أو الشريك في جريمة تزوير المستند الإلكتروني أو جريمة إستعمال المستند الإلكتروني المزور من التخفيض من العقوبة المقررة إلى النصف متى ساعد في القبض على شخص أو أكثر من الأشخاص الضالعين في إرتكابها، أو كشف عن هوية من ساهم فيها، وهذا بعد مباشرة إجراءات المتابعة.

أ-2- العقوبات الأصلية المقررة للشخص المعنوي:

يكون الشخص المعنوي مسؤولًا جزائيًا عن جريمة تزوير المستند الإلكتروني أو في جريمة إستعمال المستند الإلكتروني المزور وفقًا للقواعد المقررة في قانون العقوبات الجزائري[3]، وبالرجوع إلى الأحكام العامة المنصوص عليها في هذا القانون نجد المادة 18 مكرر منها تنص على أن: "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات

[1]- المادة 81 من القانون رقم: 24-02 السالف الذكر.
[2]- المادة 2/33 من القانون رقم: 24-02 السالف الذكر.
[3]- المادة 80 من القانون رقم: 24-02 السالف الذكر.

والجنح هي: الغرامة التي تساوي مرة (01) إلى خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة"، وعليه تكون العقوبة الأصلية للشخص المعنوي المدان:

يعاقب الشخص المعنوي من إرتكب تزويرًا في محررات عمومية أو رسمية بموجب المادة 31 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر بالغرامة من مليوني 2.000.000 دج (وهو الحد الأقصى للغرامة المقررة قانونًا للجريمة) إلى عشرة ملايين 10.000.000 دج (وهو ما يعادل خمس (05) مرات الحد الأقصى).

يعاقب كل شخص معنوي ليس طرفًا في المستند أدلى أمام ضابط عمومي أو موظف بتصريح يعلم أنه غير مطابق للحقيقة بموجب المادة 33 من نفس القانون بالغرامة من خمسمائة ألف 500.000 دج إلى مليوني وخمسمائة ألف 2.500.000 دج.

يعاقب كل من يستعمل المستند مع علمه بأنه مزور بموجب المادة 34 من نفس القانون بالغرامة قدرها من مليون 1.000.000 دج إلى خمس ملايين 5.000.000 دج.

ويعاقب كل من إرتكب تزويرًا بإحدى الطرق المنصوص عليها في المادة 31 في المستندات العرفية بموجب المادة 36 من نفس القانون بالغرامة من خمسمائة ألف 500.000دج إلى مليوني وخمسمائة ألف 2.500.000 دج.

ب- العقوبات التكميلية المقررة لجريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور:

يقصد بالعقوبات التكميلية وفقًا للمادة 3/04 من ق.ع.ج: "تلك العقوبات التي لا يجوز الحكم بها مستقلة عن عقوبة أصلية فيما عدا الحالات التي ينص عليها القانون صراحة، وهي إما إجبارية أو إختيارية".

رصد المشرع الجزائري عقوبات تكميلية إختيارية للشخص الطبيعي وللشخص المعنوي كما يلي:

ب-1- العقوبات التكميلية المقررة في قانون العقوبات الجزائري:

أجاز المشرع الجزائري الحكم على الجاني المدان بجريمة أو أكثر من الجرائم المنصوص عليها في القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر بما في ذلك جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور بالعقوبات التكميلية، وهذا ما أكدته المادة 78 من نفس القانون التي نصت على أن: "يمكن الجهة القضائية المختصة أن تطبق على الشخص الطبيعي المحكوم عليه بإرتكاب إحدى الجرائم المنصوص عليها في هذا القانون، عقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات".

وبالتالي فقد أحالت المادة السالفة الذكر إلى قانون العقوبات الجزائري لتوقيع العقوبات التكميلية على الجاني، وبالتالي فإنه يجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة بنص المادة 09 من قانون العقوبات بالنسبة للشخص الطبيعي، والعقوبات التكميلية المحددة فى نص المادة 18 مكرر من قانون العقوبات بالنسبة للشخص المعنوي.[1]

ب-2- العقوبات التكميلية المستحدثة بموجب القانون الجزائري رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور:

رأى المشرع الجزائري أن من الأنسب لمكافحة الجرائم المنصوص عليها في القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر بما في ذلك جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور، إستحداث جزاءات جديدة تكميلية تتمثل في ما يلي:

- تبطل بقوة القانون الوثائق والمستندات والشهادات التـي ثبت تزويرها، وما ترتب عنها من حقوق وآثار[2]؛

---

[1]- تنص المادة 09 من ق.ع.ج على أن : العقوبات التكميلية هي:
1. الحجر القانوني؛
2. الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية؛
3. تحديد الإقامة؛
4. المنع من الإقامة؛
5. المصادرة الجزئية للأموال؛
6. المنع المؤقت من ممارسة مهنة أو نشاط؛
7. إغلاق المؤسسة؛
8. الإقصاء من الصفقات العمومية؛
9. الحظر من إصدار الشيكات و/أو إستعمال بطاقات الدفع؛
10. تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من إستصدار رخصة جديدة؛
11. سحب جواز السفر؛
12. نشر أو تعليق حكم أو قرار الإدانة؛
13. المنع من الإتصال بالضحية".

وتنص المادة 18 مكرر من نفس القانون على أن :...واحدة أو أكثر من العقوبات التكميلية الأتية:
1. حل الشخص المعنوي؛
2. غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (05) سنوات؛
3. الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (05) سنوات؛
4. المنع من مزاولة نشاط أو عدة أنشطة مهنية أو إجتماعية بشكل مباشر أو غير مباشر، نهائياً أو لمدة لا تتجاوز خمس (05) سنوات؛
5. مصادرة الشيء الذي استعمل في إرتكاب الجريمة أو نتج عنها؛
6. نشر وتعليق حكم الإدانة؛
7. الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (05) سنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي إرتكبت الجريمة بمناسبته".

[2]- المادة 1/74 من القانون رقم: 24-02 السالف الذكر.

- تأمر الجهة القضائية في حالة الإدانة وجوبًا بمصادرة الوسائل المستعملة في إرتكاب الجرائم محل الدراسة والأموال المتحصل عليها، مع مراعاة حقوق الغير حسن النية[1]؛
- تأمر الجهة القضائية بإتلاف الوثائق والمستندات والشهادات والنقود والأختام والدمغات والطوابع والعلامات محل التزوير[2]؛
- تقضي الجهة القضائية المختصة بمنع أي أجنبي حكم عليه بسبب الجرائم محل الدراسة، من الإقامة في التراب الوطني نهائيًا أو لمدة لا تتجاوز عشر (10) سنوات[3]؛
- يجب حجز الوثائق والمستندات موضوع الجرائم محل الدراسة، غير أنه يمكن للجهة القضائية المختصة ولضرورات حسن سير المرفق العمومي المعني أن تأمر بتحييد الورقة المعنية بالتزوير إذا كانت تشكل جزءًا من سجل عمومي ومنع إستعمالها إلى حين صدور حكمها في القضية، ويتم إدراج هذا الأمر ضمن السجل المعني[4].

2- أحكام العقاب على الشروع والمشاركة والتحريض في جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور:

تتمثل عقوبة الشروع والإشتراك والتحريض في ما يلي:

أ- عقوبة الشروع في جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور:

نصت المادة 30 من ق.ع.ج على أن: "كل محاولات لإرتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى إرتكابها تعتبر كالجناية نفسها، إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"، وتنص المادة 31 من نفس القانون على أن: "المحاولة في الجنحة لا يعاقب عليها إلا بناءً على نص صريح في القانون"، وبالرجوع إلى القواعد العامة نجد أن الشروع في الجنح لا يعاقب عليه إلا بناءً على نص صريح في القانون، ومن خلال إستقرائنا للفقرة الأولى من المادة 76 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر نجد أنها مشمولة بهذا النص والتي تنص على أن: "يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القانون بنفس العقوبة المقررة للجريمة التامة"، وبذلك فقد تبنى المشرع الجزائري فكرة العقوبة على الشروع في جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور.

[1]- المادة 2/74 من القانون رقم: 24-02 السالف الذكر.
[2]- المادة 3/74 من القانون رقم: 24-02 السالف الذكر.
[3]- المادة 79 من القانون رقم: 24-02 السالف الذكر.
[4]- المادة 18 من القانون رقم: 24-02 السالف الذكر.

ب- عقوبة الشريك في جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور:

عرفت المادة 42 من ق.ع.ج الشريك على أنه: "يعتبر شريكًا في الجريمة من لم يشترك إشتراكًا مباشرًا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على إرتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك".

وقد يتخذ الشريك صورة الشريك الحكمي بموجب المادة 43 من نفس القانون على أنه: "يأخذ حكم الشريك من يقدم مسكنًا أو ملجًأ أو مكانًا، للإجتماع لواحد أو أكثر من الأشرار الذين يمارسون اللصوصية أو العنف ضد أمن الدولة أو الأمن العام أو ضد الأشخاص أو الأموال، مع علمه بسلوكهم الإجرامي".

أما فيما يخص العقوبة المقررة للشريك، فقد نصت الفقرة الأولى من المادة 44 من ذات القانون على أن: "يعاقب الشريك في جناية أو جنحة بالعقوبة المقررة للجناية أو الجنحة"، وبالرجوع إلى القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر نجده ينص بموجب الفقرة 02 من المادة 76 على أن: "يعاقب الشريك والمحرض في الجرائم المنصوص عليها في هذا القانون بنفس العقوبة المقررة للجريمة التامة"، وعليه فإن الشريك يخضع للعقوبة المقررة في جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور وقد سبق وأن تطرقنا إليها أعلاه سواء فيما يتعلق بالشخص الطبيعي أو الشخص المعنوي.

وتنص الفقرتان 02 و03 من المادة 44 من ق.ع.ج على أن: "لا تؤثر الظروف الشخصية التي ينتج عنها تشديد أو تخفيف العقوبة أو الإعفاء منها إلا بالنسبة للفاعل أو الشريك الذي تتصل به هذه الظروف. والظروف الموضوعية اللصيقة بالجريمة التي تؤدي إلى تشديد أو تخفيف العقوبة التي توقع على من ساهم فيها يترتب عليها تشديدها أو تخفيفها، بحسب ما إذا كان يعلم أو لا يعلم بهذه الظروف".

يفهم مما سبق، أن ظروف تشديد العقوبة وظروف تخفيف العقوبة أو الإعفاء منها والتي سبق وأن فصلنا فيها أعلاه، لا تؤثر إلا بالنسبة للفاعل أو الشريك التي تتصل به هذه الظروف، أما بالنسبة للظروف الموضوعية اللصيقة بالجريمة فتسري وتؤثر على الشريك إلا إذا كان يعلم بها، فإذا لم يعلم بها فلا تؤثر عليه.

ج- عقوبة المحرض في جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور:

المحرض هو الشخص الذي يخلق فكرة إرتكاب الجريمة لدى الغير الذي يكون أهلًا لتحمل المسؤولية الجزائية بالتأثير على إرادته، عن طريق إستعمال لإحدى الأساليب المذكورة في المادة 41 من ق.ع.ج على سبيل الحصر والمتمثلة في: الهبة، أو الوعد، أو تهديد، أو إساءة إستعمال السلطة أو الولاية، أو التحايل أو التدليس الإجرامي.

وتنص الفقرة 02 من المادة 76 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر على أن: "يعاقب الشريك والمحرض في الجرائم المنصوص عليها في هذا القانون بنفس العقوبة المقررة للجريمة التامة"، وعليه يخضع المحرض على إرتكاب جريمة تزوير المستند الإلكتروني أو جريمة إستعمال المستند الإلكتروني المزور بنفس العقوبة المقررة فيها، وذلك عن طريق إستعماله لإحدى الأساليب المذكورة في المادة 41 من ق.ع.ج على سبيل الحصر للتحريض على إرتكاب الجرائم السابقة الذكر.

المطلب الثاني: جريمة سرقة بيانات المستند الإلكتروني

تتحقق جريمة سرقة معطيات المستندات الإلكترونية من خلال كل فعل يؤدي إلى الإستيلاء على المستندات أو المعلومات أو المعطيات مملوكة للغير دون وجه حق، فقد عرفت المادة 350 من ق.ع.ج السرقة كمايلي: "كل من إختلس شيئًا غير مملوك له يعد سارقًا"، والمادة 311-1 من ق.ع.ف التي تنص على أن: "السرقة هي الإستيلاء الإحتيالي على ممتلكات الغير"[1]، والمادة 311 من ق.ع.م التي نصت على أن: "كل من إختلس منقولًا مملوكًا لغيره فهو سارق"، يتضح أنه لكي نكون أمام جريمة السرقة يجب أن ينصب فعل إختلاس على مال منقول مملوك للغير بنية تملكه والإستيلاء عليه بدون رضاء صاحبه، وبإتجاه إرادته المعتبرة قانونًا إلى تحقيق النتيجة المرجوة بنية التملك، غير أنه يتضح مما سبق ذكره أن المواد المشار إليها لم تتطرق صراحة إلى جريمة السرقة الواقعة في نطاق المعلوماتية.

وبالرجوع إلى قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر بموجب المادة 23 نجدها تنص على أن: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين كل من: ....هـ - لكل من توصل بأية طريقة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني..."، ويتمثل السلوك الإجرامي في قيام الجاني بالحصول على التوقيع الإلكتروني أو المحرر الإلكتروني أو الوسيط الإلكترونى بطريقة غير شرعية، وأهم صور عدم الشرعية في هذه الجريمة أن يتم الحصول على واحدة مما سبق عن طريق النصب أو الإحتيال أو السرقة أو خيانة الأمانة، ولذلك فعدم المشروعية في هذه الجريمة قد يتمثل في سرقة المنظومة المعلوماتية أو البرنامج الخاص بالتوقيع الإلكتروني أو المحرر الإلكتروني أو سرقة الوسيط الإلكتروني.[2]

ومما سبق، يثور التساؤل حول مدى إمكانية خضوع سرقة معطيات المستند الإلكتروني للنص المشار إليه سابقًا في قانون العقوبات الجزائري؟ وما هو موقف كل من المشرع والفقه من هذه الظاهرة الإجرامية الخطيرة ؟

[1]-Art 311-1 du C.P.F dispose que: « Le vol est la soustraction frauduleuse de la chose d'autrui».

[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص-ص 191-192.

الفرع الأول: أركان جريمة سرقة معطيات المستند الإلكتروني

لقيام أركان جريمة سرقة معطيات المستند الإلكتروني يجب توافر الركن المادي والذي يشمل محل الجريمة أو موضوعها، والسلوك الإجرامي المتمثل في فعل الإختلاس، بالإضافة إلى الركن المعنوي والمتمثل في القصد الجنائي بنوعيه العام والخاص.

أولًا: الركن المادي لجريمة سرقة معطيات المستند الإلكتروني

لقيام الركن المادي لابد من توافر العناصر التالية:

1- محل التجريم:

لتحقق جريمة السرقة فإنه لا بد أن يتحقق السلوك الإجرامي على مال أو شيء مادي، أي شيء ملموس يمكن نقله وتحويله بدون تلف أو بتلف بسيط، ويصلح في نظر القانون لأن يكون محلًا للتملك[1]، وفي هذا الصدد لابد من توضيح مدى إنطباق وصف المال في مجال النظم المعلوماتية، وذلك بتحديد طبيعة المال وطبيعة المنقول فيها.

أ- طبيعة المال في مجال النظم المعلوماتية:

بالنسبة لطبيعة وصف المال على النظم المعلوماتية، فيمكن تعريف المال المعلوماتي على أنه مجموعة من الكيانات التي تتيح إدخال المعلومات والمعطيات ومعالجتها وتخزينها وإسترجاعها عند الطلب، وهو يتكون من كيانين أساسيين: كيان مادي وكيان معنوي.

أ-1- المال المعلوماتي المادي:

المال المعلوماتي المادي يتمثل في العناصر المادية المكونة للمنظومة المعلوماتية وهي التي تحتوي على المعلومات أو تسهم في معالجتها وتكون لها كيان مادي ملموس، مثل وحدات العرض والتسجيل والشاشة والملحقات التي به من أجهزة إدخال وإخراج وكذلك وسائط التخزين، وبشأن هذا النوع يجمع الفقه على أن المال المعلوماتي الطبيعي فإنه يصلح أن يكون محلًا لجريمة السرقة بإعتباره مالًا ماديًاً ملموسًاً، ويمكن نقله وحيازته بنية التملك والإستيلاء عليه.[2]

---

[1]- حنان ريحان مبارك المضحكي، مرجع سابق، ص 152.

[2]- غوالم توفيق، **السرقة المعلوماتية (دراسة تأصيلية-تحليلية- مقارنة)**، رسالة الماجستير، فرع: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2013/2012، ص 74.

أ-2- المال المعلوماتي المعنوي (المنطقي):

الكيان المعنوي أو ما يعرف بالمال المعلوماتي المعنوي (المنطقي)، يقصد به المكونات غير المادية للمنظومة المعلوماتية، مثل البرامج والمعطيات المعالجة آلياً والمخزنة على الجهاز الإلكتروني.[1]

وعليه يثار تساؤل حول مدى إمكانية إعتبار الكيان المعنوي (المنطقي) للجهاز الإلكتروني مالًا؟ وللإجابة على هذا التساؤل ، انقسمت الآراء إلى:

أ-2-1- الرأي المعارض لإضفاء وصف المال:

البعض يرى عدم صلاحية المعلومات لأن تكون محلًا للإعتداء عليها، حيث أن المعلومة في حالتها المجردة والفكرة في حد ذاتها لا تقبل التملك والإستئثار، وأن تداولها والإنتفاع بها من حق الكافة دون تمييز ومن ثم لا يمكن أن تكون محلًا للملكية الفكرية.[2]

ويفرق البعض الآخر من هذا الإتجاه بين المعطيات التي لم تتم معالجتها إلكترونيًا والتي تمت معالجتها لتتحول إلى معلومات، فيرى أن الأولى بإعتبار أن عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها فإنه لا يمكن إختلاسها لعدم توافر المادية فيها، بخلاف المعطيات التي تمت معالجتها إلكترونيًا فتتحدد في كيان مادي يتمثل في نبضات أو إشارات إلكترونية ممغنطة يمكن تخزينها على وسائط معينة ونقلها وإستغلالها وإعادة إنتاجها، فضلًا عن إمكانية تقديرها كمًا وقياسها فهي إذن ليست شيئًا معنوياً كالحقوق والأفكار بل هي شيء له في العالم الخارجي وجود مادي.[3]

كون أن مصطلح "المادة" في العلوم الطبيعية هي كل ما يشغل حيزًا ماديًا، ولما كان البرنامج يشغل حيزًا ماديًا في فراغ معين هو ذاكرة الجهاز الإلكتروني، كما يمكن قياس هذا الحيز بمقاييس معينة هي البايت والكيلوبايت والميجابايت، ومما يعضد الطبيعة المادية للمعطيات الإلكترونية أن هذه المعطيات تأخذ شكل نبضات إلكترونية مثل التيار الكهربائي الذي يعد من قبيل الأشياء المادية، علاوة على أن البرنامج أو المعلومة وإن لم يكونا شيئًا ملموسًا إلا أن لهما كيان مادي يمكن رؤيته على الشاشة مترجمًا إلى أفكار، وأن المعلومات المتنقلة عبر الأسلاك عن طريق إنتقال نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل ومصدر تتولد عنه يمكن سرقته وبالتالي لها كيان مادي، ناهيك عن أنه يمكن الإستحواذ

[1]- غوالم توفيق، مرجع سابق، ص 74.
[2]- آمال قارة، مرجع سابق، ص-ص 18-19.
[3]- خثير مسعود، مرجع سابق، ص 42.

على هذه البرامج والمعلومات عن طريق تشغيلها، أي وضعها في الجهاز وتشغيله عن طريق مفتاح السر ومعرفة الكود اللازم للتشغيل.[1]

وفقًا لهذا الرأي فإن المعطيات إذا لم تعالج آليًا بواسطة الجهاز الإلكتروني لا تعتبر من قبيل الأموال الخاضعة للحماية الجنائية، بإعتبار أن هذه المعالجة تتم في صورة نبضات إلكترونية مما يمكن القول معه بأنه بعملية المعالجة تلك تتحول من أموال معنوية إلى أموال مادية الأمر الذي يخضعها للنصوص التقليدية لجرائم الأموال، ويأخذ نفس حكمها المعطيات المخزونة سواء في البرامج أو في ذاكرته، وبالتالي تأخذ برامج ومعطيات الإلكترونية حكم الأموال عليه وبالتالي تتمتع بالحماية الجنائية المقررة لها.[2]

أ-2-2- الرأي المؤيد لإضفاء وصف المال:

يعترف للمعلوماتية بأنها مال أي لها قيمة مالية ويمكن من خلال ذلك أن تخضع للسرقة، على إعتبار أنها ترتبط بشخص صاحبها فهو الذي فكر فيها وبالتالي فهي لصيقة بشخصيته، كما أنها تكتسب ميزة أساسية ألا وهي ميزة الإنتقال فهي قابلة للإنتقال من طرف لآخر، وهذا يعني أن هناك طرفًا مستقبلًا لهاته المعلومات.[3]

ومن هنا تنشأ علاقة محورها المعلومات إما بينها وبين صاحبها وإما بين صاحبها والغير، وعليه فالمعلومات بإعتبارها نتاجًا ذهنيًا لمن يعطيها شكل المعلومة ينشأ عنها علاقة مثل تلك التي تنشأ بين المالك وبين ما يملك فيكون له نقلها وإيداعها وحفظها وتأجيرها وبيعها كما تتولد وتتغير وتنتهي حقوقًا عليها، ومن بين هاته المعلومات البرامج الرقمية.[4]

ذلك أن المستندات الإلكترونية وما تتضمنه من معلومات مالًا يمكن أن يكون محلًا للسرقة، والحجة في ذلك أن المعلومات المعالجة بوصفها كيانات منطقية أصبحت من القيم الإقتصادية المستحدثة نتيجة للتطور الذي حدث في مجال تقنية المعلومات الذي أعطى الأموال المعنوية قيمة إقتصادية قد تفوق قيمة الأموال المادية[5]، وعليه تعتبر المعلومات أموالًا لأنها قيمة إقتصادية تطرح للتداول شأنها شأن أي سلعة آخرى، كما وأن لها سوقًا تجاريًا يخضع لقوانين السوق الإقتصادية[6].

وبما أن البرامج تعد في جوهرها معلومات معالجة إلكترونيًا ولها قيمة إقتصادية فإنه يجب معاملتها على أنها مال، ما يؤكد هذا المعنى أن المشرع الحديث يعترف لصاحب هذه المعلومات بما يطلق عليه الحق في الملكية الفكرية، ولولا أن المعلومات مالًا ما كان المشرع ليستطيع

[1]- محمود سعد عبد المجيد، مرجع سابق، ص 344.
[2]- آمال قارة، مرجع سابق، ص 19.
[3]- خثير مسعود، مرجع سابق، ص 40.
[4]- نفس المرجع، ص 40.
[5]- بلحسيني حمزة، مرجع سابق، ص 238.
[6]- نفس المرجع، ص 238.

التسليم لها بهذا الحق، وإن كانت طبيعة هذه الملكية محل جدل فإنها على حال نوع من الملكية أو الحق الذي لصاحبه في القليل الحق في إحتكار إستغلال هذا المال غير المادي أي المعلومات والتي منها البرامج الرقمية.[1]

وهو ما نص به البند (هـ) من الفقرة الأولى من المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر صراحة، وعلى ذلك فالبرنامج المعلوماتي في شأن التوقيع الإلكتروني أو المستند الإلكتروني يصلح لأن يكون محلًا للسرقة المعلوماتية، ولا خلاف في سرقة الوسيط الإلكتروني بوصفه من الأدوات أو الأشياء التي تؤدي وظيفة إلكترونية، ومع ذلك وإزاء صراحة نص المادة في العقاب على هذا السلوك الإجرامي فإن مظلته تمتد إلى سرقة البرنامج المعلوماتي الخاص بالتوقيع الإلكترونى وكذلك المستند الإلكتروني ويمتد كذلك للعقاب على سرقة الوسيط المعلوماتي شرط توافر أركان جريمة السرقة الأخرى.[2]

ب- طبيعة المنقول في مجال النظم المعلوماتية:

أما بالنسبة لطبيعة المنقول في مجال النظم المعلوماتية فقد أعتبر البعض أن المعلومات المخزنة في الأجهزة الإلكترونية لا تعتبر في حد ذاتها منقولًا ماديًا ولا يتصور إنتزاع حيازتها ومن ثم لا يمكن أن تكون محلًا للسرقة، ولكن الوسيلة المثبتة عليها المعلومات هي التي تصلح لأن تكون محلًا وموضوعًا للسرقة لأن ذلك يتطابق مع نصوص القانون الجنائي التي تتطلب في محل السرقة أن يكون له كيانًا ماديًا، وبالتالي فإن المعلومات المخزنة في الأجهزة الإلكترونية على ركيزة سواء ملف أو فلاش ديسك تصلح لأن تكون محلًا للسرقة بسبب دعامتها المادية، والسرقة هنا تشمل الإطار المادي وما تتضمنه من معلومات.[3]

ووفقًا لنصوص القانون المصري نجد أن الأموال المعنوية كالأفكار والآراء والإبتكارات والحقوق الشخصية أو العينية أو المنافع لا تصلح لأن تكون محلًا للسرقة، ولكن الحقوق إذا إتخذت مظهرًا ماديًا يتمثل في وثيقة أو مستند فإنها تدخل في عداد المنقولات المادية التي يصح أن يرد عليها الإختلاس في جريمة السرقة، وتطبيقًا لذلك فإن السرقة تقع بالنسبة للإستيلاء على الأصول التي دونت فيها المؤلفات والألحان والإختراعات، وكذلك العقود والإيصالات والمخالصات والسندات والكمبيالات والأسهم والحوالات.[4]

ولكن أنتقد هذا التوجه بأن الدعامات التي تثبت عليها البرامج أو المعلومات أو المعطيات في حقيقة الأمر ذات قيمة تافهة، وبالتالي يصعب القول بإمكان تجريم الفعل على النحو الذي

[1]- آمال قارة، مرجع سابق، ص 18.
[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص 192.
[3]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 379.
[4]- نفس المرجع، ص 377.

يحمي هذه المحتويات التي تتضمنها الدعامة، مما يجعل السارق في هذه الحالة معاقبًا على جريمة السرقة ولكنه قد يعفى من العقاب أو تكون تفاهة قيمة الدعامة سببًا مخففًا للعقاب.[1]

فإذا كانت الأجهزة الإلكترونية المادية لا تحتاج إلى نصوص خاصة لحمايتها جزائيًا إذ تشملها نصوص الجرائم التقليدية، فالأمر يختلف بصدد الكيان المعنوي لتلك الأجهزة لأن جرائم الإعتداء على الأموال يشترط بشأنها عادة أن يكون موضوعها شيئًا ماديًا وطبيعة الكيان المعنوي ليس كذلك.[2]

فمثلًا مصطلح "شيء" الوارد بالنص العقابي الفرنسي والجزائري ومصطلح "المنقول" الواردة بالنص المصري وردت بالعموم بحيث تسمح بإدراج الأشياء أو المنقولات المادية وغير المادية أي المعنوية كالمستندات الإلكترونية وما تضمنه من معلومات، وهو الأمر الذي أخذ به بصلاحية الأموال المعنوية للسرقة كالمستندات الإلكترونية لأن تكون محلًا للسرقة.[3]

زيادة على ذلك فإن الإستيلاء على المعلومة يمكن أن يتحقق عن طريق السمع أوالمشاهدة، ومن ثم فإن المعلومة يمكن أن تنتقل من عقل إلى آخر، وفي هذه الحالة يمكن صب المعلومة في إطار مادي عن طريق تحييزها داخل إطار والإستئثار به، وينتج ذلك عن قيام الشخص الذي إلتقط المعلومة عن طريق السمع أو المشاهدة بتدوينها أو تسجيلها على دعامة ثم يعرضها للبيع، مثلًا ففي هذه الحالة تنتقل المعلومة من ذمة شخص إلى ذمة آخر.[4]

السبب الذي أدى إلى الجدل أن فمن غير المنطقي أن يهتم المشرع ويقر حماية للدعامات ويغفل أو يسكت عن تجريم سرقة المعلومات الموجودة بداخلها أو التي يمكن أن تحويها، فالعبرة بالقيمة المالية والإقتصادية والتجارية والنقدية لتلك المعلومات المخزنة في الدعامة المادية، والواقع الميداني يشهد أن القاضي لا يلتزم بحرفية النص كمنهج للتفسير، فمنطق العدالة وأسس التقاضي يقضيان بأن يتعدى التفسير إلى غاية النص وروحه ومنطقه في هذا المقام مسايرة التطور التقني، حيث مقتضيات حماية المجتمع تمنع أن تجرم سرقة الأسطوانة أو الدعامة ذات القيمة تافهة وفقًا لجرمية النص ويسكت عن غايته وروحه بعدم تجريم محتوى الدعامة (معلومة، معطيات، مال...) الذي يجب حمايته فهو المقصود إبتداء من أحكام السرقة.[5]

---

[1]- حنان ريحان مبارك المضحكي، مرجع سابق، ص 154.

[2]- آمال قارة، مرجع سابق، ص 15.

[3]- بلحسيني حمزة، مرجع سابق، ص 239.

[4]- أحمد خليفة الملط، مرجع سابق، ص-ص 243-244.

[5]- بن شهرة شول، مرجع سابق، ص-ص 143-144.

2- السلوك الإجرامي:

يقتضي فعل الإختلاس بنقل الشيء أو نزعه من حيازة المجني عليه وإدخاله في حيازة الجاني بنية التملك، بدون علم المجني عليه وبغير رضاه وقد يكون بعلمه ولكن بغير رضاه.[1]

وعليه يشترط لتحقق فعل الإختلاس في جريمة السرقة ضرورة توافر عنصرين أحدهما موضوعي والثاني معنوي أو ما يسمى بالشخصي، حيث يتمثل العنصر الموضوعي للإختلاس في الإستيلاء على الحيازة على نحو يشكل إخراج الشيء من حيازة المجني عليه وإدخاله في حيازة الجاني، في حين يتمثل العنصر الشخصي للإختلاس في نية الجاني في تملك الشيء وحيازته وعدم رضاء المجني عليه أي المالك أو الحائز للشيء عن فعل الإختلاس الذي إرتكبه الجاني.[2]

ومنه فلا يكفي لقيام الجريمة أن يختلس الشخص مالًا غير مملوكًا له، وإنما يشترط أن يقع الإختلاس على مال مملوك للغير حتى ولو لم يكن مالك هذا المال معروفًا، وقد قضي بأنه لا يؤثر في قيام جريمة السرقة عدم الإهتداء إلى معرفة شخص المالك للمسروقات، كما قضي أيضًا بأن خطأ الحكم في ذكر إسم مالك الشيء المسروق لا يعيب.[3]

وبما أننا بصدد الحديث عن فعل الإختلاس وعناصره ضمن نطاق المعلوماتية، يثار التساؤل حول مدى إنطباق التعريف السابق بعنصريه على المستندات الإلكترونية وما تتضمنه من معطيات ومعلومات؟

يرى البعض أن تطبيق نصوص السرقة في ظل تشريعنا الحالي على إقتناء المعطيات أو المعلومات يصطدم بعقبات، حيث قرر إن إقتناء المعلومة لا يعني أخذها وإن نسخ المعلومات بدون أخذ مصدرها الأصلي يعني تقاسم الإطلاع على المعلومات مع صاحبها الشرعي مع عدم وجود نية لحرمان صاحب المعلومات من هذه المعلومات سواء بصفة مؤقتة أو دائمة، وأن النية تتجه أساسًا إلى الإطلاع عليها فقط.[4]

عكس ما تم إتخاذه من قبل محكمة النقض الفرنسية والذي أعتبر موقفها متقدمًا عندما قضى الحكم الإستئنافي الصادر في فرنسا بتاريخ 29 سبتمبر 1977 الذي أيد حكم محكمة الدرجة الأولى الذي رفض وجود أركان جريمة السرقة ولم يحصل إختلاس مستندات تحتوي على المعلومات بل ظلت المستندات بحيازة المؤسسة على أساس أنه لم يحصل إختلاس لشيء مملوك في هذه القضية، فالمستند الذي تم تصويره إنما يطال المحتوى الفكري وليس المستند ذاته وبالتالي لا يعتبر إختلاسًا يبرر العقاب، في حين أن محكمة النقض رفضت هذا القول

[1]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 381.
[2]- بلحسيني حمزة، مرجع سابق، ص-ص 241-242.
[3]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 378.
[4]- نفس المرجع، ص 383.

وإعتبرت أن تصوير المستندات لأغراض شخصية دون موافقة مالكها يشكل جريمة سرقة خاصة وأن هذه المستندات لم تكن بحوزته.[1]

كما يرى هذا الإتجاه أنه يوجد إختلاف بين المال محل السرقة والقيم الذهنية، أن المعلومات ذات القيمة الإقتصادية الضخمة مثل المتعلقة بالأسرار التجارية والصناعية يجب حمايتها جنائيًا عن طريق تدخل المشرع بنص خاص للعقاب على أفعال الإستيلاء عليها.[2]

ويرى البعض أن هذه المبادئ العامة تطبق على السرقة المعلوماتية وذلك لأن الإختلاس للمال المعلوماتي يتحقق على إثر قيام الجاني بتشغيل الجهاز الإلكتروني والحصول على المعطيات أو المعلومات أو حيازتها، وهو ليس في حاجة لإستعمال العنف كما في السرقة التقليدية كي ينقل المعلومة ويستحوذ عليها، فكل ذلك من الممكن الحصول عليه عن طريق الشبكة وبسهولة دون أن يكون مضطرًا لإتيان السلوك المادي المنصوص عليه في مواد السرقة بما فيها فعل الإختلاس للمنقول، ولذلك فمجرد حيازته للمعلومة عن طريق إستحواذها أو الحصول عليها بطريق غير مشروع يتحقق الإختلاس المعلوماتي بعناصره الثلاث من سلوك إجرامي ونتيجة إجرامية وعلاقة سببية.[3]

ويمكن القول أيضًا أنه وبعد أن إتضح أن الإتجاه الراجح يؤكد أن المستندات المعالجة آليًا يمكن أن تكون محلًا للإختلاس إذا ما تم وضعها والتعامل بها عن طريق نسخها والإطلاع عليها بالبصر أو ما يطلق عليه الإلتقاط الذهني، وذلك بسبب أن فعل الإختلاس يضر بالقيمة الإقتصادية لها، فإنه ينبغي الذكر أن فكرة الإستيلاء التي تعتبر العنصر الموضوعي المكون للركن المادي محققة الوجود.[4]

ومن التطبيقات الحديثة ما قضت به محكمة النقض الفرنسية في إحدى القضايا بأن: "المعطيات المعلوماتية من الأشياء القابلة للسرقة، حيث قضت بتأييد إدانة عاملين بإحدى ورش التأليف الضوئي بمطبعة (Bourquin) بجريمة السرقة، لقيامهما داخل مطبعة بنسخ 47 أسطوانة معلوماتية تحتوي على ملفات للعملاء على قدر كبير من الأهمية من ناحية قيمتها التجارية، وكذلك نسخ 71 أسطوانة أخرى مسجل عليها كل عمليات المطبعة، واستوليا عليها من رب العمل بهدف تأسيس مشروع منافس"، وبالتالي نجد أن محكمة النقض الفرنسية قضت بتوافر عناصر جريمة السرقة بالرغم من أنه تم نسخ الأسطوانات ولم يتم نقل الأصول من مكانها.[5]

وبهذا يمكن القول أن المعلومات الواردة في المستندات الإلكترونية يمكن أن تكون محلًا لفعل الإختلاس، ويتحقق هذا الأمر بإستيلاء الجاني على المستند الإلكتروني المخزن على

[1]- حسين محمد الغول، مرجع سابق، ص 433.
[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 383.
[3]- حسين محمد الغول، مرجع سابق، ص 441.
[4]- بلحسيني حمزة، مرجع سابق، ص 242.
[5]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص-ص 381-382.

الجهاز الإلكتروني لغيره وإخراجه من حيازة صاحبه لإدخاله في حيازته، وذلك عن طريق نقله خلسة إلى جهازه الشخصي أو إلى أي وسيط مادي له سيطرة مادية عليه، على أن يتم هذا كله بغير رضاء صاحب المستند الإلكتروني.[1]

ثانيًا: الركن المعنوي لجريمة سرقة بيانات المستند الإلكتروني

جريمة سرقة معطيات المستند الإلكتروني جريمة عمدية يتطلب لقيامها توفر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يكون الجاني عالمًا بأن سلوكه ينطوي على فعل الإختلاس، بحيث يجب أن تتجه إلى الإستيلاء على المعلومات المسجلة إلكترونياً، وهي المعلومات الواردة في المستند الإلكتروني التي خضعت لعملية المعالجة الآلية، أو المعلومات الواردة في المستند الإلكتروني المخزن داخل المنظومة المعلوماتية، أو المعلومات الواردة في المستند الإلكتروني المسجلة إلكترونياً والمخزنة على وسائط تخزين خارجية، مع علمه بأن المعلومات محل السرقة ليست ملكًا له.[2]

وأن تتجه إرادة الجاني إلى فعل الإستيلاء على هذا المنقول، وذلك عن طريق تبديل الحيازة من حيازة المجني عليه وإدخاله في حيازة الجاني وإخضاعه لسيطرته المادية التي تمكنه من الظهور عليه بمظهر المالك[3]، وعدم توافر عنصر الإرادة في الفعل ينفي القصد الجنائي فمن يقوم يأخذ الدعامة الإلكترونية من صاحبها بدون علمه لمعرفة المستند الإلكتروني المسجل عليها ثم يعيدها إلى صاحبها فلا يتوافر لديه نية الإختلاس[4].

ولا يكتمل القصد الجنائي في جريمة السرقة إلا بتوافر القصد الخاص بجانب القصد العام، والقصد الخاص يقصد به أن تتصرف نية الجاني إلـى إمتلاك الشيء محل الإختلاس، أي أن تنصرف نية الجاني إلى الظهور على الشيء بمظهر المالك له وحرمان المالك من سلطاته على الشيء، ويرى القضاء الفرنسي أن سرقة جهد المنظومة المعلوماتية فى أوقات فراغه سرقة منفعة، مستندًا إلى أحكام محكمة النقض الفرنسية التي إكتفت بتوافر نية التملك الوقتية التي تتوافر بمجرد إرتكاب الشخص عمل من أعمال التصرف التي تتم عن كونه مالك للشيء.[5]

وهناك رأي يرى أن القصد الخاص "نية التملك" لا تتوافر في حالة قراءة المعلومات التي يتضمنها المستند الإلكتروني من خلال الشاشة أو سماعها من خلال سماعات أو حالة الإلتقاط للإشعاعات، فالجاني لم يقصد حرمان صاحبها منها بصفة دائمة أو مؤقتة وإنما شاركه الإنتفاع

[1]- بلحسيني حمزة، مرجع سابق، ص 243.
[2]- نفس المرجع، ص-ص 243-244.
[3]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 384.
[4]- أحمد خليفة الملط، مرجع سابق، ص 273.
[5]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 384.

بها بالإطلاع عليها، ويرى أنه في حالة ما إذا كان هناك ثمة حالات يخشى منها الإفلات من العقاب لخطورتها الإجرامية فيمكن مواجهتها بنصوص خاصة.[1]

الفرع الثاني: العقوبة المقررة لجريمة سرقة معطيات المستند الإلكتروني

ورد نص التجريم على هذه الجريمة بموجب المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر التي تعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، لكل من توصل بأية طريقة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني، وفي حالة العود تزاد بمقدار المثل العقوبة المقررة لهذه الجريمة في حديها الأدنى والأقصى، وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الإنتشار وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه.

وتنص المادة 24 من نفس القانون على عقاب المسؤول عن الإدارة الفعلية للشخص المعنوي المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع عمله بذلك، ويكون الشخص المعنوي مسؤولًا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات إذا كانت المخالفة قد إرتكبت من أحد العاملين به بإسم ولصالح الشخص المعنوي.

وفيما يتعلق بموقف المشرع الجزائري فقد نصت المادة 350 من ق.ع.ج على عقاب كل من إختلس شيئًا غير مملوك له بالحبس من سنة (01) إلى خمس (05) سنوات وبغرامة من مائة ألف 100.000 دج إلى خمسمائة ألف 500.000 دج، يتضح أن المشرع الجزائري لم يشترط لتطبيق أحكام هذه المادة أن يكون المال محل السرقة ماديًا، وهو الأمر الذي دفع الرأي الراجح إلى التأكيد على أن وقوع جريمة السرقة على مال معنوي لا يصطدم بمبدأ شرعية الجريمة والعقوبة، ولكن مع ذلك يمكن القول أن عدم إيراد المشرع الجزائري بشكل صريح لفظ المعطيات والمستندات الإلكترونية المخزنة داخل المنظومة المعلوماتية في المادة 350 من نفس القانون.[2]

وعليه لا يمكن تطبيق نص المادة 350 من ق.ع.ج على أفعال سرقة معطيات المستندات الإلكترونية، لأنها لم تتضمن أي عبارة صريحة تتعلق بالبيانات أو المعطيات الإلكترونية ضمن

[1]- أحمد خليفة الملط، مرجع سابق، ص 376.
[2]- بلحسيني حمزة، مرجع سابق، ص 248.

نطاق التجريم، وهو ما يحدث فراغًا تشريعيًا في تجريم هذا النوع من الأفعال الأمر الذي يستوجب من المشرع الجزائري التدخل لتدارك هذا القصور وسد الفراغ التشريعي.

المبحث الثالث: الجرائم الماسة بالتوقيع والتصديق الإلكترونيين

ساهم التطور التكنولوجي المتسارع في وسائل الإتصال الحديثة وتزايد إستخدام شبكة الإنترنت في إنجاز العقود، في الإنتقال من التعامل الورقي إلى التعامل الإلكتروني من خلال إبرام معاملات إلكترونية بين متعاقدين لا يتقابلون ماديًا وإنما يتم التواصل بينهم بشكل إفتراضي قد يجهل بعضهم البعض فضلًا عن عدم وجود علاقات سابقة بينهم، وقد استدعى هذا الواقع الجديد توفير الثقة والأمان بينهما مما تطلب وضع مجموعة من الضمانات القانونية الكفيلة بتحقيق ذلك، كضمان تحديد هوية المتعاقدين والتأكد من طبيعة التعاقد ومضمونه وضمان التعبير عن الإرادة على نحو يمكن نسبة التصرف إلى صاحبه، مما حذا بالمشرع الجزائري إلى مواكبة هذا التطور إنشاء جهات محايدة للقيام بالتصديق الإلكتروني تتولى إصدار شهادات التصديق الإلكتروني الموصوفة أو تقديم خدمات أخرى في مجال التصديق الإلكتروني، وألزمها بجملة من الإلتزامات القانونية التي تقع على عاتقها لضمان خلق بيئة إلكترونية آمنة للتعامل عبر شبكة الإنترنت وإلا تكون محلًا للمساءلة الجزائية بموجب القانون رقم: 15-04 المؤرخ في الأول من فيفري سنة 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر[1]، ولم يقف المشرع الجزائري عند هذا الحد بل رتب المسؤولية الجزائية عن الأضرار التي قد تلحق بالمستفيد من طالب الخدمة، وكذا الأضرار التي قد تنشأ عن الغير.

المطلب الأول: الجرائم المرتكبة من طرف مؤدي خدمات التصديق الإلكتروني

حذا المشرع الجزائري خطى التشريعات المقارنة في سعيه لمواكبة التطور الحاصل في مجال إبرام المعاملات الإلكترونية، وذلك من خلال إنشاء جهات مختصة بالتصديق الإلكتروني تتولى إصدار شهادات تؤتمن التصديق على التوقيع الإلكتروني، بهدف إثبات هوية الشخص المبرم وصحة توقيعه، ومن ثم التحقق من مضمون التعامل وسلامة التوقيع المرفق به، وقد ألزم المشرع الجزائري هذه الجهات بجملة من الإلتزامات القانونية التي تقع على عاتقها لضمان الثقة والأمان اللازمين لإزدهار البيئة الرقمية وتوسع المعاملات الإلكترونية بموجب القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر، ونظرًا لما تكتسبه البيانات والمعلومات المتعلقة بشهادة التصديق الإلكتروني من أهمية وحساسية، أقر المشرع الجزائري مجموعة من الجزاءات التي تطبق على جهات التصديق الإلكتروني في حال مخالفتها ما يقع على عاتقها.

[1]- بوشارب هانية، مجدوب آمنة، مرجع سابق، ص 32.

الفرع الأول: جريمة الإخلال بالإلتزام إعلام السلطة الإقتصادية عن التوقف عن ممارسة النشاط

يلزم القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر مؤدي خدمات التصديق الإلكتروني الذي يرغب في وقف نشاطه المتعلق بتأدية خدمات التصديق الإلكتروني أو بأي فعل قد يؤدي إلى ذلك، بإعلام السلطة الإقتصادية للتصديق الإلكتروني في الآجال المحدد في سياستها، وإلتزامه بأحكام سياسة التصديق[1] لهذه السلطة المتعلقة بإستمرارية الخدمة، ويترتب على وقف النشاط سحب الترخيص[2]، بإعتبار هذه السلطة مكلفة بمتابعة ومراقبة عمله[3] ولكونها المكلفة بمنح الترخيص له لمزاولة النشاط.

وإذا أوقف نشاطه لأسباب خارجة عن إرادته فعليه أن يعلم السلطة الإقتصادية للتصديق الإلكتروني بذلك فورًا، وتقوم هذه الأخيرة بإلغاء شهادته للتصديق الإلكتروني الموصوفة بعد تقدير الأسباب المقدمة، ويجب على مؤدي خدمات التصديق إتخاذ التدابير اللازمة والمنصوص عليها في سياسة التصديق الإلكتروني للسلطة الإقتصادية، من أجل حفظ البيانات المرتبطة بشهادة التصديق الموصوفة الممنوحة وتبليغ أصحابها بذلك.[4]

ويتعرض كل مؤدي خدمات التصديق الإلكتروني يخالف ما تم ذكره للمساءلة الجزائية بتهمة إرتكاب الجريمة المنصوص عليها في المادة 67 من نفس القانون، التي تجرم كل إخلال بالإلتزام المتعلق بإعلام السلطة الإقتصادية بالتوقف عن ممارسة النشاط .[5]

وورد النص على هذه الجريمة في الفقرة 02 من المادة 19 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة

---

[1]- عرفت الفقرة 15 من المادة 02 من القانون رقم: 15-04 السالف الذكر سياسة التصديق الإلكتروني كالآتي: "مجموع القواعد والإجراءات التنظيمية والتقنية، المتعلقة بالتوقيع والتصديق الإلكترونيين".

[2]- المادة 3/58 من القانون رقم: 15-04 السالف الذكر.

[3]- المادة 1/30 من القانون رقم: 15-04 السالف الذكر.

[4]- تنص المادة 58 من القانون رقم: 15-04 السالف الذكر على أن: "يجب على مؤدي خدمات التصديق الإلكتروني إعلام السلطة الإقتصادية للتصديق الإلكتروني، في الآجال المحددة في سياسة التصديق لهذه السلطة، برغبته في وقف نشاطاته المتعلقة بتأدية خدمات التصديق الإلكتروني أو بأي فعل قد يؤدي إلى ذلك. وفي هذه الحالة يلتزم مؤدي خدمات التصديق الإلكتروني بأحكام سياسة التصديق للسلطة الإقتصادية للتصديق الإلكتروني المتعلقة بإستمرارية الخدمة. ويترتب على وقف النشاط سحب الترخيص".

وتنص المادة 59 من القانون رقم: 15-04 السالف الذكر على أن: "يجب على مؤدي خدمات التصديق الإلكتروني الذي يوقف نشاطه لأسباب خارجة عن إرادته، أن يعلم السلطة الإقتصادية للتصديق الإلكتروني بذلك فورًا، وتقوم هذه الأخيرة بإلغاء شهادته للتصديق الإلكتروني الموصوفة بعد تقدير الأسباب المقدمة. وفي هذه الحالة يتخذ مؤدي خدمات التدابير اللازمة، والمنصوص عليها في سياسة التصديق الإلكتروني للسلطة الإقتصادية من أجل حفظ المعلومات المرتبطة بشهادة التصديق الإلكتروني الموصوفة الممنوحة له".

[5]- تنص المادة 67 من القانون رقم: 15-04 السالف الذكر على أن: "يعاقب بالحبس من شهرين (02) إلى سنة (01) واحدة وبغرامة من مائتي ألف 200.000 دج إلى مليون 1.000.000 دج أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بإلتزام إعلام السلطة الإقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و59 من هذا القانون".

تكنولوجيا المعلومات السالف الذكر التي تنص على أن: ولا يجوز التوقف عن مزاولة النشاط المرخص به أو الإندماج في جهة أخرى أو التنازل عن الترخيص للغير، إلا بعد الحصول على موافقة كتابية مسبقة من الهيئة"، ويعاقب كل من يخالف ما ورد في الفقرة السابقة بالعقوبة المقررة في المادة 23 من نفس القانون[1].

أولًا: أركان جريمة إخلال بإلتزام إعلام السلطة الاقتصادية عن التوقف عن ممارسة النشاط

لقيام هذه الجريمة، لابد من توافر ثلاث أركان:

1- الركن المفترض:

إشترط المشرع الجزائري لقيام جريمة إخلال بإلتزام إعلام السلطة الإقتصادية عن التوقف عن ممارسة النشاط أن تتوفر صفة معينة في الجاني بأن يكون مؤديًا لخدمات التصديق الإلكتروني، وقد عرفته الفقرة 12 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر على أنه: "يعد كل شخص طبيعي أو معنوي يقوم بمنح شهادات التصديق الإلكتروني، أو تقديم خدمات أخرى في مجال التصديق الإلكتروني"، وحسب قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر جاء خاليًا من أي تعريف لجهة التصديق على التوقيع الإلكتروني، إلا أن اللائحة التنفيذية لهذا القانون المعدلة بموجب القرار رقم: 361 لسنة 2020 سالفة الذكر عرفت جهات التصديق على التوقيع الإلكتروني بموجب الفقرة 06 من المادة الأولى منها كالآتي:" جهات التصديق الإلكتروني: الجهات المرخص لها بإصدار شهادة التصديق الإلكتروني، وتقديم خدمات تتعلق بالتوقيع الإلكتروني".

لقيام هذه الجريمة لابد من توافر في الجاني صفة العمل لدى الجهة المختصة بإصدار شهادات التصديق الإلكترونية، وبالمقابل لا تتحقق هذه الجريمة في من تنتفي فيه تلك الصفة، وعلة التجريم تكمن في أن الجاني قد أؤتمن على البيانات أو المعلومات بسبب وظيفته أو عمله، فمناط العقاب يكمن في الإخلال بإلتزام ناشئ عن المهنة وما يترتب على عاتقه من واجبات التي تضمن سير الحسن للمهنة.[2]

كما إشترط المشرع الجزائري لقيام الجريمة محل الدراسة أن يتم الإخلال بإلتزام إعلام السلطة الإقتصادية عن التوقف عن ممارسة النشاط، ولم يعرف هذه السلطة بل إكتفى فقط

[1]- تنص المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لعام 2004 السالف الذكر على أن: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين كل من ... د- خالف أحكام المادة 19".

[2]- عزيزة لرقط، **الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري**، كلية الحقوق والعلوم السياسية، جامعة تامنغست، مجلة الإجتهاد للدراسات القانونية والإقتصادية، المجلد 06 ، العدد 01، جانفي 2017، الجزائر، ص 120.

بالتطرق للجهة المكلفة بتعيينها المتمثلة في السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية.[1]

وتكلف السلطة الإقتصادية للتصديق الإلكتروني بمتابعة ومراقبة مؤدي خدمات التصديق الذين يقدمون خدمات التوقيع والتصديق الإلكترونيين لصالح الجمهور، وكذا تتولى بالمهام المنصوص عليها في المادة 30 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر.[2]

2- الركن المادي:

يتحقق السلوك الإجرامي عندما يخل مؤدي خدمة التصديق الإلكتروني بإلتزام إعلام السلطة الإقتصادية للتصديق الإلكتروني في الآجال المحددة في سياسة التصديق لهذه السلطة، عن رغبته في التوقف عن ممارسة نشاطه المتعلق بتأدية خدمات التصديق الإلكتروني أو بأي

[1]- المادة 29 من القانون رقم: 15-04 السالف الذكر.

[2]- تنص المادة 30 من القانون رقم: 15-04 السالف الذكر على أن: "تكلف السلطة الإقتصادية للتصديق الإلكتروني بمتابعة ومراقبة مؤدي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكترونيين لصالح الجمهور، وفي هذا الإطار تتولى المهام التالية:

- إعداد سياستها للتصديق الإلكتروني وعرضها على السلطة للموافقة عليها، والسهر على تطبيقها؛

- منح التراخيص لمؤدي خدمات التصديق الإلكتروني بعد موافقة السلطة؛

- الموافقة على سياسات التصديق الصادرة عن مؤدي خدمات التصديق الإلكتروني، والسهر على تطبيقها؛

- الإحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها، والبيانات المرتبطة بمنحها من طرف مؤدي خدمات التصديق الإلكتروني بغرض تسليمها إلى السلطات القضائية المختصة، عند الإقتضاء، طبقًا للأحكام التشريعية والتنظيمية المعمول بها؛

- نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة؛

- إتخاذ التدابير اللازمة لضمان إستمرارية الخدمات في حالة عجز مؤدي خدمات التصديق الإلكتروني عن تقديم خدماته؛

- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريًا أو بناء على طلب منها؛

- التحقق من مدى مطابقة طالبي التراخيص مع سياسة التصديق الإلكتروني بنفسها أو عن طريق مكاتب تدقيق معتمدة؛

- السهر على وجود منافسة فعلية ونزيهة بإتخاذ التدابير اللازمة لترقية أو إستعادة المنافسة بين مؤدي خدمات التصديق الإلكتروني؛

- التحكيم في النزاعات القائمة بين مؤدي خدمات التصديق الإلكتروني فيما بينهم أو مع المستعملين طبقًا للتشريع المعمول به؛

- مطالبة مؤدي خدمات التصديق الإلكتروني أو كل شخص معين بأي وثيقة أو معلومة، تساعدها في تأدية المهام المخولة لها بموجب هذا القانون؛

- إعداد دفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني، وعرضه على السلطة للموافقة عليه؛

- إجراء كل مراقبة طبقًا لسياسة التصديق الإلكتروني، ودفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني؛

- إصدار التقارير والإحصائيات العمومية، وكذا تقرير سنوي يتضمن وصف نشاطاتها مع إحترام مبدأ السرية.

- وتقوم السلطة الإقتصادية للتصديق الإلكتروني بتبليغ النيابة العامة بكل فعل ذي طابع جزائي يكتشف بمناسبة تأدية مهامها".

فعل قد يؤدي إلى ذلك، وكل من توقف عن ممارسة نشاطه لأسباب خارجة عن إرادته وأخل بإعلام السلطة الإقتصادية بذلك.[1]

3-الركن المعنوي:

تعد الجريمة محل الدراسة من الجرائم العمدية التي يتطلب لقيامها توفر القصد الجنائي العام بعنصريه العلم والإرادة، إذ ينبغي أن يكون الجاني عالمًا بكافة الأركان المكونة للجريمة، ومنها ضرورة علمه بأنه يحمل صفة مقدمي خدمات التصديق الإلكتروني وفقًا للفقرة 12 من المادة 02 من نفس القانون، وأن يكون عالمًا أن توقفه يقتضي إبلاغه للسلطة الإقتصادية ضمن الآجال المحدد في سياستها ورغم ذلك أخل بإلتزامه، أما إذا إنتفى العلم بأحد العناصر السابقة فإنه ينتفي معه القصد الجنائي العام.

ولا يكفي لقيام الركن المعنوي أن يكون الجاني عالمًا بإرتكابه الجريمة، بل يجب أن تتجه إرادته إلى إقتراف السلوك الإجرامي بأن تكون إرادته حرة سليمة، فإذا ثبت أن الجاني قام بمزاولة نشاطه خارج الآجال المحددة تحت تأثير الإكراه أو أي سبب آخر يؤثر على طبيعة إرادته، ينتفي القصد الجنائي العام.

ثانيًا: العقوبة المقررة لجريمة الإخلال بالإلتزام إعلام السلطة الاقتصادية عن التوقف عن ممارسة النشاط

يعاقب مؤدي خدمة التصديق الإلكتروني الذي أخل بإلتزام إعلام السلطة الإقتصادية بالتوقف عن نشاطه ضمن الآجال المحدد بالحبس من شهرين (02) إلى سنة (01) واحدة، وبغرامة من مائتي ألف 200.000 دج إلى مليون 1.000.000 دج، أو بإحدى هاتين العقوبتين.[2]

يتضح مما سبق أن المشرع الجزائري منح السلطة التقديرية لقاضي الموضوع فيما يتعلق بالعقوبة المقررة للشخص الطبيعي، فقد أعطى له الخيار بين عقوبة الحبس وعقوبة الغرامة.

أما إذا كان مرتكب الجريمة شخصًا معنويًا فطبقًا لنص المادة 75 من نفس القانون يعاقب بغرامة تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وعليه تكون العقوبة الأصلية للشخص المعنوي الغرامة مقدرة بخمسة ملايين 5.000.000 دج.

فضلًا عن ذلك يجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة بنص المادة 09 من قانون العقوبات الجزائري بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من نفس القانون بالنسبة للشخص المعنوي.

[1]- المادة 67 من القانون رقم: 15-04 السالف الذكر.

[2]- المادة 67 من القانون رقم: 15-04 السالف الذكر.

أما موقف المشرع المصري فيعاقب بموجب المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر لكل من خالف أحكام المادة 19 التي تنص على عدم جواز التوقف عن مزاولة النشاط المرخص به أو الإندماج في جهة أخرى أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة كتابية مسبقة من الهيئة[1]، بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، وفي حالة العود تزاد بمقدار المثل العقوبة المقررة لهذه الجريمة في حديها الأدنى والأقصى، وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الإنتشار وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه.

ونص القانون آنف ذكره صراحة على مسؤولية الجزائية للشخص المعنوي عن الجرائم التي ترتكب بالمخالفة لأحكام هذا القانون حيث نصت الفقرة الأولى من المادة 24 منه على أن: "يعاقب المسؤول عن الإدارة الفعلية للشخص الإعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك".

والفقرة 02 من نفس المادة على أن: "ويكون الشخص الإعتباري مسؤولًا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد إرتكبت من أحد العاملين به بإسم ولصالح الشخص الإعتباري ".

الفرع الثاني: جريمة جمع البيانات الشخصية للمعني دون موافقته الصريحة وإستعمالها إستعمالًا غير مشروع

لتوفير أقصى درجات الأمان والثقة للعملاء فقد ألزم المشرع الجزائري جهة التصديق الإلكتروني بالحفاظ على سرية البيانات المتعلقة بشهادات التصديق الإلكتروني وفقًا لمقتضيات المادة 42 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي جاء نصها كالآتي: "يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة"، وأضاف بموجب المادة 43 من نفس القانون بضرورة أخذ الموافقة الصريحة للمعني قبل جمع بياناته الشخصية، ولا يمكن لمؤدي خدمات التصديق الإلكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن إستعمال هذه

[1]- يقصد بالهيئة طبقًا للفقرة 26 من المادة الأولى من اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المعدلة بموجب القرار رقم: 361 لسنة 2020 سالفة الذكر كالآتي: "الهيئة: هيئة تنمية صناعة تكنولوجيا المعلومات".

البيانات لأغراض أخرى، وفي حال الإخلال بأحكام المادة السابقة يتعرض مؤدي خدمات التصديق الإلكتروني للمسؤولية الجزائية بموجب المادة 71 من ذات القانون.[1]

وفي نفس السياق أشارت المادة 21 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر إلى الجريمة محل الدراسة كالآتي: "بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو إتصل بها بحكم عمله إفشاؤها للغير أو إستخدامها في غير الغرض الذي قدمت من أجله"، وكل من يخالف أحكام المادة السابقة الذكر يعاقب بالعقوبة المنصوص عليها في الفقرة (د) من المادة 23 من نفس القانون.

أولًا: أركان جريمة جمع البيانات الشخصية للمعني دون موافقته الصريحة وإستعمالها إستعمالاً غير مشروع

لقيام الجريمة محل الدراسة لابد من توافر ثلاث أركان:

1-الركن المفترض:

إشترط المشرع الجزائري أن تتوافر صفة معينة في الجاني حتى تقوم هذه الجريمة، وهي أن يكون من مؤدي خدمات التصديق الإلكتروني حسب ما جاء به التعريف الفقرة 12 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر.

2-الركن المادي:

لتحقق الركن المادي في الجريمة محل الدرسة، يشترط توافر:

أ- السلوك الإجرامي:

ألزم المشرع الجزائري مؤدي خدمات التصديق الإلكتروني بموجب المادة 43 من القانون آنف ذكره بضرورة أخذ الموافقة الصريحة من المعني قبل جمع بياناته الشخصية، ولا يمكن أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن إستعمال هذه البيانات لأغراض أخرى، ومن ثم يفترض لقيام السلوك الإجرامي بإتيان مؤدي خدمة التصديق الإلكتروني فعلًا إيجابيًا يتمثل في جمع البيانات ذات طابع الشخصي للمعني

[1]- تنص المادة 43 من القانون رقم: 15-04 السالف الذكر على أن: "لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني، إلا بعد موافقته الصريحة، ولا يمكن مؤدي خدمات التصديق الإلكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن إستعمال هذه البيانات لأغراض أخرى".

تنص المادة 71 من القانون رقم: 15-04 السالف الذكر على أن: "يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات، وبغرامة من مائتي ألف 200.000 دج إلى مليون 1.000.000 دج أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون".

دون رضاه، أي دون الحصول على موافقته التي يجب أن تكون صريحة، وأن يستعمل هذه البيانات التي قام بجمعها في غير الغرض التي جمعت من أجله.

ونلاحظ في هذا الصدد أن المشرع المصري في المادة 21 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر المذكورة أعلاه قد إكتفى بتجريم إستعمال البيانات التي قام بجمعها في غير الغرض التي جمعت من أجله من خلال عبارة: "ولا يجوز... إستخدامها في غير الغرض الذي قدمت من أجله"، بدون تطرق إلى تجريم جمع هذه البيانات بعد أخذ الموافقة الصريحة للمعني

ب- محل التجريم:

يقصد بالسرية الحفاظ على المعلومات ذات الطابع الشخصي المقدمة من العميل لجهة التصديق بهدف حفظها أو تبادلها أو إستخدامها في إنشاء مفاتيح التشفير الإلكتروني وإصدار شهادة المصادقة الإلكترونية، وبالتالي تنحصر سلطة مؤدي خدمات التصديق الإلكتروني في هذا المجال فقط ولا تتعداه إلى إستخدام تلك المعلومات لأغراض أخرى.[1]

البيانات الشخصية التي يحظر على مؤدي خدمة التصديق الإلكتروني جمعها بدون موافقة المسبقة للشخص المعني، هي كل معلومة من شأنها أن تجعل هذا الأخير قابلًا للتعريف أو معرفًا مثل عناصر هويته[2] كهوية الشخصية وجواز السفر وغير ذلك من الأوراق الثبوتية.

وإن كان المشرع الجزائري لم يحدد طبيعة البيانات التي يتوجب المحافظة على سريتها، غير أنه وبالرجوع إلى المادة 15 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر نجده قد نص على البيانات التي تتعلق بشخص الموقع التي تستوجبها شهادة التصديق الإلكتروني كالآتي:

- إسم الموقع أو الإسم المستعار الذي يسمح بتحديد هويته؛

- إمكانية إدراج صفة خاصة للموقع عند الإقتضاء، وذلك حسب الغرض من إستعمال الشهادة التصديق الإلكتروني؛

- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر عند الإقتضاء".

وتنص المادة 22 من اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 سالفة الذكرعلى البيانات التي تتعلق بشخص الموقع كالتالي:

[1]- شيخ سناء، مرجع سابق، ص 156.

[2]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص-ص 730-731.

- إسم الموقع الأصلي أو إسمه المستعار أو إسم شهرته، وذلك في حالة إستخدامه لأحدهما؛
- صفة الموقع؛
- المفتاح الشفري العام لحائز الشهادة المناظر للمفتاح الشفري الخاص به؛
- ما يفيد إختصاص الموقع، والغرض الذي تستخدم فيه الشهادة".

3-الركن المعنوي:

تعد الجريمة محل الدراسة من الجرائم العمدية التي يتطلب لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، وذلك من خلال علم الجاني بكافة العناصر المكونة للجريمة، أن يكون الجاني عالمًا بأنه من مؤدي خدمات التصديق الإلكتروني، وأنه يقوم بجمع البيانات الشخصية للمعني دون أن تكون لديه موافقة صريحة منه، أو علمه بأنه يقوم بإستعمال هذه البيانات التي جمعها في غير الغرض الذي خصصت من أجله، وأن يكون عالمًا بأن لا يمكن إستعمال هذه البيانات لأغراض الأخرى، وبالتالي ينتفي القصد الجنائي في الحالة التي يكون جمع هذه البيانات الشخصية بموافقة الصريحة من المعني، وكذلك إستعمالها في الغرض الذي خصص لها لأغراض منح وحفظ الشهادات التصديق الإلكتروني، ويجب أن تتجه إرادته السليمة إلى إتيان أحد السلوكات الإجرامية.

ثانياً: العقوبة المقررة لجريمة جمع البيانات الشخصية للمعني دون موافقته الصريحة وإستعمالها إستعمالاً غير مشروع

يترتب على قيام جريمة جمع البيانات الشخصية للمعني دون موافقته الصريحة وإستعمالها إستعمالاً غير مشروع، عقاب الجاني إذا كان شخصًا طبيعيًا بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات وبغرامة من مائتي ألف 200.000 دج إلى مليون 1.000.000 دج أو بإحدى هاتين العقوبتين فقط[1]، وتكون العقوبة الأصلية للشخص المعنوي هي الغرامة المقدرة بخمس ملايين 5.000.000 دج حسب المادة 75 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي تقضي برفع الحد الأقصى للغرامة المقررة للشخص الطبيعي إلى خمس (05) مرات.

ويجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة المادة 09 من ق.ع.ج بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من ق.ع.ج بالنسبة للشخص المعنوي.

ويعاقب بموجب المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر لكل من خالف أحكام المادة 21 التي تنص على عدم جواز إستخدام بيانات التوقيع

[1]- المادة 71 من القانون رقم: 15-04 السالف الذكر.

الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني في غير الغرض الذي قدمت من أجله، بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، وفي حالة العود تزداد بمقدار المثل العقوبة المقررة لهذه الجريمة في حديها الأدنى والأقصى، وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الإنتشار وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه.

وبموجب المادة 24 من القانون آنف ذكره يعاقب المسؤول عن الإدارة الفعلية للشخص المعنوي المخالف بذات العقوبات المقررة في المادة 23 عن الأفعال التي ترتكب بالمخالفة لأحكام المادة 21 من هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك، ويكون الشخص المعنوي مسؤولًا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد إرتكبت من أحد العاملين به بإسم ولصالح الشخص المعنوي.

الفرع الثالث: جريمة إفشاء البيانات الشخصية لشهادة التصديق الإلكتروني

أقر المشرع الجزائري تجريم فعل إفشاء المعلومات والبيانات المتعلقة بالشهادة التصديق الإلكترونية بموجب المادة 70[1] من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي أحالتنا إلى المادة 42[2] من نفس القانون، التي تلزم هذه الأخيرة كل مؤدي خدمات التصديق الإلكتروني بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة، وبالإضافة إلى تجريم فعل الإفشاء الذي يقوم به القائم بالتدقيق بموجب المادة 73 التي تعاقب كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية إطلع عليها أثناء قيامه بالتدقيق[3].

وورد النص على هذه الجريمة في المادة 21 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر التي نصت على أن بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية ولا

[1]- تنص المادة 70 من القانون رقم: 15-04 السالف الذكر على أن: "يعاقب بالحبس من ثلاثة (03) أشهر إلى سنتين (02) وبغرامة من مائتي ألف دينار 200.000 دج إلى مليون 1.000.000 دج أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخل بأحكام 42 من هذا القانون".

[2]- تنص المادة 42 من القانون رقم: 15-04 السالف الذكر على أن: "يجب على كل مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة".

[3]- تنص المادة 73 من القانون رقم: 15-04 السالف الذكر على أن: "يعاقب بالحبس من ثلاثة (03) أشهر إلى سنتين (02) وبغرامة من عشرين ألف 20.000 دج إلى مائتي ألف 200.000 دج أو بإحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية أطلع عليها أثناء قيامه بالتدقيق".

يجوز لمن قدمت إليه أو أتصل بها بحكم عمله إفشاؤها لغير، وكل من يخالف أحكام المادة سابقة الذكر يعاقب بالعقوبة المنصوص عليها في الفقرة (د) من المادة 23 من نفس القانون.[1]

أولًا: أركان جريمة إفشاء بيانات الشخصية لشهادة التصديق الإلكتروني

إفشاء هذه المعلومات أو الأسرار يعنى إذاعتها أو نقلها وإطلاع الغير عليها وخروجها من حيز الكتمان أو السرية، بعد أن كان العلم بها قاصرًا على أصحابها أو الذين ائتمنوا عليها بحكم وظيفتهم، وهم من هذه الجريمة مقدمي خدمة التصديق الإلكتروني ومعاونوهم، والذين يقومون بدون علم ورضاء صاحبها بإفشاء سرها[2]، ولقيام جريمة إفشاء بيانات الشخصية لشهادة التصديق الإلكتروني لابد من توافر ثلاث أركان:

1-الركن المفترض:

فقد تتداخل الحماية المقررة للتوقيع الإلكتروني والحماية الجنائية للأسرار، ذلك أن المستند الإلكتروني قد يحتوي سرًا يرغب الفرد في الإحتفاظ به بعيدًا عن تدخل الآخرين، غير أنه مع ذلك فإن التفرقة بين جرائم الماسة بالتوقيع الإلكتروني وجرائم إفشاء الأسرار ممكنة، ذلك أن فعل إفشاء السر يجب أن يتم من شخص مؤتمن على الحفاظ على هذا السر وهو ما يعبر عنه بشرط الصفة، وذلك بخلاف الإعتداء على التوقيع الإلكتروني إذ يجوز أن يقع من أي شخص.[3]

إشترط المشرع الجزائري لقيام جريمة إفشاء بيانات الشخصية لشهادة التصديق الإلكتروني أن تتوفر صفة معينة في الجاني بأن يكون مؤديًا لخدمات التصديق الإلكتروني وفقًا للتعريف الوارد في الفقرة 12 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر.

وكل شخص مكلف بالتدقيق الذي يقوم بكشف المعلومات السرية التي إطلع عليها أثناء قيامه بالتدقيق، ويقصد بالتدقيق طبقًا للفقرة 16 من المادة 02 من نفس القانون على أن: "التحقق من مدى المطابقة وفقًا لمرجعية ما".

والسلطات التي يمكنها إجراء التدقيق تتمثل في السلطة الوطنية من خلال البند 05 من الفقرة الأولى من المادة 18 ويكون ذلك على مستوى السلطتين الحكومية والإقتصادية للتصديق الإلكتروني عن طريق الهيئة الحكومية المكلفة بالتدقيق، كما خول هذه الصلاحية أيضًا للسلطة الحكومية من خلال البند 06 من المادة 28 من نفس القانون ويكون ذلك على مستوى الطرف الثالث الموثوق عن طريق الهيئة الحكومية المكلفة بالتدقيق طبقًا لسياسة التصديق، أما السلطة

[1]- تنص المادة 23 من قانون التوقيع الإلكتروني رقم: 15 لعام 2004 السالف الذكر على أن: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين كل من .... د- خالف أيا من أحكام المادتين 19، 21 من هذا القانون".

[2]- سحر سعد عبد السميع محمد، مرجع السابق، ص 139.

[3]- نفس المرجع، ص 113.

الإقتصادية فهي الأخرى خول لها القانون صلاحية التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الالكتروني بنفسها أو عن طريق مكاتب معتمدة وفقًا للبند 08 من الفقرة الأولى من المادة 30 من ذات القانون.

2-الركن المادي:

لتحقق الركن المادي في الجريمة محل الدرسة، يشترط توافر:

أ-السلوك الإجرامي:

لقيام السلوك الإجرامي لابد أن يكون الجاني قد إطلع أو تحصل على بيانات شخصية بحكم عمله المتمثل في إنشاء شهادات التصديق الإلكترونية بالنسبة لمؤدي خدمات التصديق الإلكتروني أو أثناء قيامه بعملية التدقيق بالنسبة للشخص المكلف بالتدقيق، ثم يقوم بإفشاءها وإطلاع الغير عليها ممن ليس له الحق بذلك وإخراجها بسبب ذلك من حيز السرية والكتمان، بعد أن كان العلم بها قاصرًا على أصحابها أو الذين إئتمنوا عليها بحكم وظيفتهم دون علم أو رضا صاحبها.[1]

ويتحقق هذا السلوك الإجرامي إما بصورة إيجابية حين يتعمد الجاني للغير بالإطلاع على هذه البيانات أو المعلومات، أو بصورة سلبية حين يسمح الجاني للغير بالإطلاع على بيانات الموقع دون مبرر وسند قانوني، وفي حالة عدم تأمين بيانات التوقيع الإلكتروني كما هو منصوص عليه في البند 04 من المادة 07 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي إشترطت أن يكون التوقيع الإلكتروني مصممًا بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني[2]، وذلك لضمان ترسيخ الأمان والطمأنينة في نفوس المتعاقدين.[3]

---

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 728.

[2]- عرف المشرع الجزائري آلية إنشاء التوقيع الإلكتروني بموجب الفقرة 04 من المادة 02 من القانون رقم: 15-04 السالف الذكر بأنها: "جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني"، وإشترط في المادة 10 من نفس القانون بضرورة أن تكون آلية إنشاء التوقيع الإلكتروني الموصوف مؤمنة، وحدد المتطلبات التي يلزم أن تتوفر فيها بموجب المادة 11 من نفس القانون كالآتي:"

يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة، على الأقل ما يأتي:

أ- ألا يمكن عمليًا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الإعتماد؛

ب- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الإستنتاج، وأن يكون هذا التوقيع محميًا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الإعتماد؛

ج- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي إستعمال من قبل الآخرين؛

يجب أن لا تعدل البيانات محل التوقيع، وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع".

[3]- عزيزة لرقط، مرجع سابق، ص-ص 120-121.

ويتحقق الركن المادي للجريمة بمجرد إنتهاك سرية البيانات وخصوصيتها حتى ولو لم يترتب على الفعل أي نتيجة، فالجريمة من الجرائم الشكلية يكتفي المشرع فيها بتحقق السلوك الإجرامي دون إشتراط تحقق النتيجة، لأن الغرض من التجريم هو الحفاظ على سرية وخصوصية البيانات وليس تحقق نتيجة إجرامية، ويستوي في المعلومات التى يتم إنشاؤها أن تكون مكتوبة في أوراق أو مسجلة على دعامة إلكترونية أو تكون مخزنة ضمن برنامج معلوماتي في جهاز إلكتروني.[1]

ب- محل التجريم:

وهي المعطيات الشخصية التي يطلع عليها مؤدي خدمة التصديق الإلكتروني أو المكلفون بالتدقيق أثناء قيامهم بمهامهم، والممنوحة لهم من طرف أصحابها في سبيل عمليات التصديق الإلكتروني، وبالرجوع إلى المادة 15 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر نجد المشرع الجزائري قد نص على البيانات التي تستوجبها شهادة التصديق الإلكتروني كالآتي:

- الإشارة إلى أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة؛
- تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له المصدر لشهادة التصديق الإلكتروني، وكذا البلد الذي يقيم فيه؛
- إسم الموقع أو الإسم المستعار الذي يسمح بتحديد هويته؛
- إمكانية إدراج صفة خاصة للموقع عند الإقتضاء، وذلك حسب الغرض من إستعمال الشهادة التصديق الإلكتروني؛
- بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات إنشاء التوقيع الإلكتروني؛
- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني؛
- رمز تعريف شهادة التصديق الإلكتروني؛
- التوقيع الإلكتروني الموصوف لمؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني؛
- حدود إستعمال شهادة التصديق الإلكتروني الموصوفة، عند الإقتضاء؛
- حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني، عند الإقتضاء؛
- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر، عند الإقتضاء".

وتنص المادة 22 من اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المعدلة بموجب القرار رقم: 361 لسنة 2020 سالفة الذكر على البيانات التي تستوجبها شهادة التصديق الإلكتروني كالآتي: "يجب أن تشتمل نماذج شهادات التصديق الإلكتروني التي

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 138.

يصدرها المرخص له على البيانات الآتية، وذلك على نحو متوافق مع المعايير المحددة في الفقرة (أ) من الملحق الفني والتقني المرفق بهذه اللائحة:

- ما يفيد صلاحية هذه الشهادة للإستخدام في التوقيع الإلكتروني؛
- موضوع الترخيص الصادر للمرخص له، موضحًا فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه؛
- إسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسي وكيانها القانوني، والدولة التابعة لها إن وجدت؛
- إسم الموقع الأصلي أو إسمه المستعار أو إسم شهرته، وذلك في حالة إستخدامه لأحدهما؛
- صفة الموقع؛
- المفتاح الشفري العام لحائز الشهادة المناظر للمفتاح الشفري الخاص به؛
- تاريخ بدء صلاحية الشهادة، وتاريخ إنتهائها؛
- رقم مسلسل للشهادة؛
- التوقيع الإلكتروني لجهة إصدار الشهادة؛
- عنوان الموقع الإلكتروني Web Site المخصص لقائمة الشهادات الموقوفة أو الملغاة؛

ويجوز أن تشتمل الشهادة على أي من البيانات الآتية عند الحاجة:

- ما يفيد إختصاص الموقع والغرض الذي تستخدم فيه الشهادة؛
- حد قيمة التعاملات المسموح بها بالشهادة؛
- مجالات إستخدام الشهادة".

3-الركن المعنوي:

جريمة إفشاء بيانات الشخصية لشهادة التصديق الإلكتروني هي جريمة عمدية تتطلب وجود القصد الجنائي العام والذي يقوم أساسًا على عنصري العلم والإرادة، بقيام العلم لدى الجاني بعناصر الجريمة، إذ ينبغي أن يعلم الجاني بأنه من مؤدي خدمات التصديق الإلكتروني أو أنه مكلف بالتدقيق أثناء قيامه بمهامه، وكذا إنصراف علمه بأنه ملزم بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة التي قد تحصل عليها بحكم وظيفته، وأنه لا يجوز له إطلاع الغير عليها، ورغم ذلك تنصرف إرادته السليمة بالإتيان بهذا السلوك الإجرامي بمخالفة المحافظة على هذا الإلتزام والقيام بإفشائها إلى الغير.

ثانيًا: العقوبة المقررة لجريمة إفشاء البيانات الشخصية لشهادة التصديق الإلكتروني

يعاقب مؤدي خدمة التصديق الإلكتروني الذي يفشي البيانات الشخصية المتعلقة بالشهادة التصديق الإلكتروني الممنوحة بالحبس من ثلاثة (03) أشهر إلى سنتين (02) وبغرامة من مائتي ألف 200.000 دج إلى مليون 1.000.000 دج أو بإحدى هاتين العقوبتين فقط.[1]

[1]- تنص المادة 70 من القانون رقم: 15-04 السالف الذكر.

وإذا كان مقترف الفعل من المكلفين بالتدقيق فإن العقوبة هي الحبس من ثلاث (03) أشهر إلى سنتين (02) وبغرامة من عشرين ألف 20.000 دج إلى مائتين ألف 200.000 دج أو بإحدى هاتين العقوبتين فقط.[1]

أما إذا كان المدان هو شخصًا معنويًا فإن العقوبة تتمثل حسب المادة 75 من القانون آنف الذكر في الغرامة المقدرة بخمس (05) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي، وعليه تكون العقوبة لمؤدي خدمة التصديق الإلكتروني الغرامة المقدرة خمسة ملايين 5.000.000 دج، في حين تكون العقوبة للمكلفين بالتدقيق الغرامة المقدرة مليون 1.000.000 دج.

ويجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة المادة 09 من ق.ع.ج بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من ق.ع.ج بالنسبة للشخص المعنوي.

وورد نص التجريم على هذه الجريمة بموجب المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر التي تعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، لكل من يخالف أحكام المادة 21 من هذا القانون، وفي حالة العود تزداد بمقدار المثل العقوبة المقررة لهذه الجريمة في حديها الأدنى والأقصى، وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الإنتشار وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه.

وبموجب المادة 24 من القانون آنف ذكره يعاقب المسؤول عن الإدارة الفعلية للشخص المعنوي المخالف بذات العقوبات المقررة في المادة 23 عن الأفعال التي ترتكب بالمخالفة لأحكام المادة 21 من هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك، ويكون الشخص المعنوي مسؤولًا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد إرتكبت من أحد العاملين به بإسم ولصالح الشخص المعنوي.

الفرع الرابع: جريمة إصدار شهادة التصديق الإلكتروني دون ترخيص أو مزاولة النشاط رغم سحب الترخيص منه

ورد النص على هذه الجريمة في المادة 72 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر لكل مؤدي خدمات التصديق

[1]- تنص المادة 73 من القانون رقم: 15-04 السالف الذكر.

الإلكتروني الذي يستأنف أو يواصل نشاطه بالرغم من سحب الترخيص منه، أو كل من يؤدي خدمات التصديق الإلكتروني دون ترخيص[1]، وقد تم تعريف الترخيص بموجب الفقرة 10 من المادة 02 من نفس القانون بأنه: "نظام إستغلال خدمات التصديق الإلكتروني الذي يتجسد في الوثيقة الرسمية الممنوحة لمؤدي الخدمات، بطريقة شخصية تسمح له بالبدء الفعلي في توفير خدماته".

وورد النص على هذه الجريمة في البند (أ) من الفقرة الأولى من المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر لكل من أصدر شهادة التصديق الإلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة، وبالإضافة إلى البند (د) من نفس الفقرة لكل من خالف أحكام المادة 19 التي تنص في فقرتها الأولى على عدم جواز مزاولة نشاط إصدار شهادات التصديق الإلكتروني إلا بترخيص من الهيئة، وكذا إلى ضرورة التقيد بمجموعة من الإلتزامات التي تقع على عاتق من يرغب في الحصول على ترخيص بغرض ممارسة نشاط إصدار شهادات التصديق الإلكتروني.[2]

أولًا: أركان جريمة إصدار شهادة التصديق الإلكتروني دون ترخيص ومزاولة النشاط رغم سحب الترخيص منه

لقيام الجريمة محل الدراسة لابد من توافر ثلاث أركان:

1-الركن المفترض:

إشترط المشرع الجزائري أن تتوافر صفة معينة في الجاني حتى تقوم هذه الجريمة، وهي أن يكون من مؤدي خدمات التصديق الإلكتروني حسب ما جاء به التعريف الفقرة 12 من المادة

[1]- تنص المادة 72 من القانون رقم: 15-04 السالف الذكر على أن: "يعاقب بالحبس من سنة (01) واحدة إلى ثلاث (03) سنوات وبغرامة من مائتين ألف 200.000 دج إلى مليوني 2.000.000 دج أو بإحدى هاتين العقوبتين فقط، كل ما يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص، أو كل مؤدي خدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه. تصادر التجهيزات التي إستعملت لإرتكاب الجريمة طبقًا للتشريع المعمول به".

[2]- تنص المادة 23 من قانون التوقيع الإلكتروني رقم: 15 لعام 2004 السالف الذكر على أن: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه أو بإحدى هاتين العقوبتين كل من: أ- أصدر شهادة التصديق الإلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة... د- خالف أحكام المادة 19".

وبالرجوع إلى المادة 19 من نفس القانون نجدها تنص في الفقرة الأولى منها على أن: لا تجوز مزوالة نشاط إصدار شهادات التصديق الإلكتروني إلا بترخيص من الهيئة، وذلك نظير مقابل يحدده مجلس إدارتها وفقًا للإجراءات والقواعد والضمانات التي تقررها اللائحة التنفيذية لهذا القانون ودون التقيد بأحكام القانون رقم: 129 لسنة 1947 بإلتزامات المرافق العامة، مع مراعاة ما يأتي:

أ- أن يتم إختيار المرخص له في إطار المنافسة والعلانية؛

ب- أن يحدد مجلس إدارة الهيئة مدة الترخيص بحيث لا تزيد على تسعة وتسعين عامًا؛

ج- أن تحدد وسائل الإشراف والمتابعة الفنية والمالية التي تكفل حسن سير المرفق بإنتظام وإطراد".

02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر.

2-الركن المادي:

لتحقق الركن المادي في الجريمة محل الدرسة، يشترط توافر:

أ-السلوك الإجرامي:

يتحقق السلوك الإجرامي في قيام الجاني بإستمرار إصدار شهادات التصديق الإلكتروني رغم سحب الترخيص منه، وأيضًا قد يتخذ صورة إنتحال صفة مؤدي خدمات التصديق الإلكتروني فيقوم بإصدار شهادة تصديق الإلكتروني دون الحصول على ترخيص ممارسة النشاط من طرف السلطة الإقتصادية للتصديق الإلكتروني.

ومن ثم يستلزم في هذا السلوك مزاولة الإصدار فعلًا، إذ لا تتحقق الجريمة بمجرد إتجاه إرادة الشخص في إصدار شهادة التصديق الإلكتروني وإنما يلزم أن تصدر حقًا من الجاني، ذلك أنها الدليل على مباشرة إصداره لشهادة تصديق الإلكتروني دون الحصول على ترخيص.[1]

ويعتبر شرط الحصول على الترخيص لمزاولة هذا النشاط أمرًا ضروريًا للحفاظ على مصلحة المتعاملين إلكترونيًا، لأنه يضفي نوعًا من الثقة والأمان لدى المتعاملين ويقلل من إمكانية تعرضهم للإحتيال في عمل هذه الجهات.[2]

وترتيبًا على ذلك، فإن الجريمة محل الدراسة من الجرائم الشكلية التي يتطلب لقيامها توافر السلوك الإجرامي فقط، والذي يتمثل في قيام الجهة قبل حصولها على الترخيص وفق الإجراءات والشروط التي حددها القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر خاصة المواد 33 وما يليها منه، في إصدار شهادات التصديق الإلكتروني أو إستمرارها في منح شهادات التصديق بالرغم من سحب الرخصة منها في الحالات التي حددها ذات القانون.[3]

ب-محل التجريم:

يتمثل محل الجريمة وفقاً للمادة 72 من القانون آنف ذكره في شهادة التصديق الإلكتروني الموصوفة، وهي شهادة تصدر من طرف الجهة المختصة بإصدار شهادات التصديق الإلكتروني، الغرض منها تأكيد صحة بيانات التوقيع ونسبته إلى صاحبه، وتتضمن العديد من البيانات التي تجعل منها أكثر أمانًا للمتعاقدين، وتوصف قانونيًا بصفة موصوف في حالة ما إذا

[1]- بلحسيني حمزة، مرجع سابق، ص 302.
[2]- صليحة مرباح، مرجع سابق، ص 878.
[3]- عزيزة لرقط، مرجع سابق، ص 123.

توفرت على البيانات المحددة قانونيًا[1]، وقد سبق وأن تطرقنا إليها في المبحث الأول من الفصل الأول ضمن الباب الأول.

3-الركن المعنوي:

تعد الجريمة محل الدراسة من الجرائم العمدية التي تقتضي توافر لدى مرتكبها القصد الجنائي العام بعنصريه العلم والإرادة، إذ ينبغي أن يعلم الجاني بأنه إنتحل صفة مؤدي خدمات التصديق الإلكتروني، وإنصراف علمه بأن سلوكه المتمثل في إصدار شهادة التصديق الإلكتروني الموصوفة دون الحصول على ترخيص وفقًا للقانون، أو أن يعلم بأنه إستأنف أو واصل نشاطه بالرغم من سحب ترخيصه، وتتجه إرادته السليمة إلى إرتكاب هذا السلوك الإجرامي.

ثانيًا: العقوبة المقررة لجريمة إصدار شهادة التصديق الالكتروني دون ترخيص ومزاولة النشاط رغم سحب الترخيص منه

يترتب على قيام جريمة إصدار شهادة التصديق الالكتروني دون ترخيص ومزاولة النشاط رغم سحب الترخيص منه، عقاب الجاني إذا كان شخصًاً طبيعيًاً بالحبس من سنة (01) واحدة إلى ثلاث 03 سنوات وبغرامة من مائتي ألف 200.000 دج إلى مليوني 2.000.000 دج أو بإحدى هاتين العقوبتين فقط.[2]

أما إذا كان مرتكب السلوك الإجرامي شخصًا معنويًا فإن العقوبة تقدر بعشرة ملايين 10.000.000 دج، حسب المادة 75 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي تقضي برفع الحد الأقصى للغرامة المقررة للشخص الطبيعي إلى خمس (05) مرات.

ويجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة المادة 09 من ق.ع.ج بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من ق.ع.ج بالنسبة للشخص المعنوي.

ويعاقب بموجب الفقرة الأولى من المادة 23 من قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات السالف الذكر كل من أصدر شهادة التصديق الإلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة، كل من خالف أحكام المادة 19 التي تنص في فقرتها الأولى على عدم جواز مزاولة نشاط إصدار شهادات التصديق الإلكتروني إلا بترخيص من الهيئة، ولكل من لم يتقيد بالإلتزامات التي تقع على عاتق من يرغب في ممارسة نشاط إصدار شهادات التصديق الإلكتروني، بالحبس وبغرامة لا تقل عن عشرة آلاف 10.000 جنيه ولا تجاوز مائة

[1]- بلحاج محجوبة، مرجع سابق، ص 109.
[2]- المادة 72 من القانون رقم: 15-04 السالف الذكر.

ألف 100.000 جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، وفي حالة العود تزداد بمقدار المثل العقوبة المقررة لهذه الجريمة في حديها الأدنى والأقصى، وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الإنتشار وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه.

ونص القانون السالف الذكر صراحة على مسؤولية الشخص المعنوي عن الجرائم التي ترتكب بالمخالفة لأحكام هذا القانون بموجب المادة 24 منه على أن يعاقب المسؤول عن الإدارة الفعلية للشخص المعنوي المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك، ويكون الشخص المعنوي مسؤولًا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد إرتكبت من أحد العاملين به بإسم ولصالح الشخص المعنوي.

الفرع الخامس: جريمة الإخلال بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني

يلزم مؤدي خدمات التصديق الإلكتروني قبل منح شهادة التصديق الإلكتروني أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع، وكذا منح شهادة أو أكثر لكل شخص يقدم طلبًا وذلك إلا بعد التحقق من هوية الشخص الموقع، وعند الإقتضاء التحقق من صفاته الخاصة، أما فيما يخص الأشخاص المعنوية فإنه يجب الإحتفاظ بسجل يدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع المتعلق بشهادة التصديق الإلكتروني الموصوفة، حتى يتمكن من تحديد هوية الشخص الطبيعي عند كل إستعمال لهذا التوقيع الإلكتروني[1]، وإلا يعرض كل من أخل عمدًا بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني الموصوفة بالمسؤولية الجزائية بموجب المادة 69 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر.[2]

أولًا: أركان جريمة الإخلال بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني

لقيام الجريمة محل الدراسة لابد من توافر ثلاث أركان:

1-الركن المفترض:

إشترط المشرع الجزائري لقيام جريمة الإخلال بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني، أن تتوفر صفة معينة في الجاني بأن يكون من مؤدي خدمات التصديق الإلكتروني

[1]- المادة 44 من القانون رقم: 15-04 السالف الذكر.

[2]- تنص المادة 69 من القانون رقم: 15-04 السالف الذكر على أن: "يعاقب بالحبس من شهرين (02) إلى ثلاث (03) سنوات بغرامة من عشرين ألف 20.000 دج إلى مائتي ألف 200.000 دج أو بإحدى هاتين العقوبتين فقط، كل من يخل عمدًا بإلتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة".

حسب ما جاء به التعريف الفقرة 12 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر.

2-الركن المادي:

يتمثل الركن المادي في إخلال مؤدي خدمة التصديق الإلكتروني بإلتزامه المتمثل في تحديد هوية طالب شهادة التصديق الإلكتروني الموصوفة، كون أنه ملتزم بالتحقق من البيانات التي تتضمنها الشهادة[1]، والمتمثل في عدم التأكد المسبق من هوية الشخص الذي يتقدم بطلب الحصول على شهادة التصديق الإلكتروني الموصوفة عن طريق أي وثيقة ثبوتية إذا كان شخصًا طبيعيًا، أما إذا كانت الشهادة لصالح الشخص المعنوي فإنه ملزم بالتحقق من الهوية بواسطة التفويض الممنوح له لهذا الغرض[2].

على إعتبار أن شهادة التصديق الإلكتروني تعد بمثابة وثيقة إلكترونية تربط بين الشخص وتوقيعه الإلكتروني، لذلك تعتبر مسألة تحديد هوية صاحب الشهادة من المسائل الجوهرية التي تستقصي حقيقتها الجهات الممارسة لهذا النشاط.[3]

إن التحقق من هوية الموقع وإصدار شهادة التصديق الإلكتروني له تمنح الثقة لدى الغير بأن البيانات التي تحتويها الشهادة صحيحة وبالخصوص هوية الموقع ونسبة التوقيع إليه، مما يحث من يطلع على هذه الشهادة التعامل معه بكل ثقة وإطمئنان، على أن جهة التصديق الإلكتروني تختص بتوفير الوسائل التي تثبت أن الشخص الذي تم تحديد هويته في الشهادة يمتلك السيطرة على أداة التوقيع، ويلتزم بسرية بيانات شهادة التصديق وعلى سرية المفاتيح وعدم إتاحتها للغير، وأن يلتزم على عدم إستعمالها إستعمالًا غير مشروع أو أن يستخدمها لغير الأغراض التي أصدرت بشأنها وأنها كانت سارية المفعول وقت إجراء التوقيع.[4]

3-الركن المعنوي:

تعد جريمة الإخلال بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني من الجرائم العمدية التي تستلزم لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، إذ ينبغي أن يعلم الجاني بأنه من مقدمي خدمات التصديق الإلكتروني، وأن يعلم بأنه ملزم بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني، ومع ذلك يقوم بمنح الشهادة له دون التأكد من هويته، وتتجه إرادته السليمة إلى إتيان السلوك الإجرامي.

---

[1]- بلحسيني حمزة، مرجع سابق، ص 298.

[2]- بلحاج محجوبة، مرجع سابق، ص 124.

[3]- نفس المرجع، ص 124.

[4]- خنافيف محمد، شايبي العيد، **الآليات الفنية التي إعتمدها المشرع الجزائري في القانون 04/15 لضمان أمن التوقيع الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية -بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر، ص 126.

ثانياً: العقوبة المقررة لجريمة الإخلال بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني

يترتب على قيام الجريمة محل الدراسة توقيع العقوبة على الجاني إذا كان شخصًا طبيعيًا بالحبس من شهرين (02) إلى ثلاث (03) سنوات وغرامة من عشرين ألف 20.000 دج إلى مائتي ألف 200.000 دج أو إحدى هاتين العقوبتين فقط.[1]

أما إن كان شخصًا معنويًا تكون العقوبة التي تعادل (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي حسب المادة 75 من القانون آنف ذكره، ومنه تتمثل في غرامة المقدرة بمليون 1.000.000 دج.

ويجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة المادة 09 من ق.ع.ج بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من ق.ع.ج بالنسبة للشخص المعنوي.

المطلب الثاني: جرائم طالبي خدمات التصديق الإلكتروني

ألزم المشرع الجزائري الأشخاص الذين يقدمون بياناتهم الشخصية إلى جهات التصديق الإلكتروني بغرض الحصول على شهادة تصديق إلكتروني، بضرورة تقديم تلك البيانات بشكل صحيح، وبإستعمال الشهادة فقط في الأغراض التي منحت لأجلها.

الفرع الأول: جريمة الإدلاء بتصاريح وإقرارات كاذبة

أقر المشرع الجزائري تجريم كل تصريح أو إقرار كاذب من المعني بالأمر لمقدم خدمة التصديق الإلكتروني للحصول على شهادة التصديق الإلكتروني الموصوفة[2]، نظرًا لأن البيانات الشخصية المتعلقة بالمعاملات الإلكترونية تتوقف على ما تقدمه الأطراف المتعاقدة، وطبقًا لأحكام نص المادة 45 من نفس القانون فإنه يلغى شهادة التصديق الإلكتروني الموصوفة عندما يتبين أنه قد تم منحها بناء على معلومات خاطئة أو مزورة[3].

أولًا: أركان جريمة الإدلاء بتصاريح وإقرارات كاذبة

لقيام الجريمة محل الدراسة لابد من توافر ثلاث أركان:

---

[1]- المادة 69 من القانون رقم: 15-04 السالف الذكر.

[2]- تنص المادة 66 من القانون رقم: 15-04 السالف الذكر على أن: "يعاقب بالحبس من ثلاث (03) أشهر إلى ثلاث (03) سنوات وبغرامة من عشرين ألف 20.000 دج إلى مائتي ألف 200,000 دج أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة".

[3]- المعلومات الخاطئة هي معلومات صحيحة ولكن تخص شخص آخر يحمل نفس الإسم لصاحب الشهادة الأصلي، أما المعلومات المزورة فهي معلومات غير صحيحة تصدر الشهادة بناء عليها، وللمزيد من التفصيل، ينظر: صليحة مرباح، مرجع سابق، ص 881 .

1- الركن المفترض:

إشترط المشرع الجزائري صفة الشخص الموقع طالب إنشاء التوقيع في الجاني لقيام جريمة الإدلاء بتصاريح وإقرارات كاذبة، والذي عرفه بموجب الفقرة 02 من المادة 02 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر على أنه: "الموقع: شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني، ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله".

2-الركن المادي:

تتوقف موثوقية التوقيع الإلكتروني على صحة البيانات المدلى بها من المعني بالشهادة الإلكترونية، ذلك أن هذه البيانات هي بيانات التحقق والتي تسمح لجهات التصديق الإلكتروني على إثبات الصلة بين التوقيع الإلكتروني والموقع، لذلك فإنه يتطلب على مؤدي خدمة التصديق الإلكتروني عند إصدار الشهادة جمع البيانات الشخصية وطلبها مباشرة من الشخص المعني، كما يمكن الحصول عليها من الغير بعد الموافقة الخطية أو الإلكترونية للشخص المعني، وعلى هذا الأخير أن يحرص على الإدلاء بهذه البيانات على نحو صحيح وغير مغلوط تفاديًا للتأثير السلبي على مصداقية الشهادة الإلكترونية التي يصدرها مؤدي الخدمة.[1]

يتحقق السلوك الإجرامي في هذه الجريمة بقيام الجاني بالإدلاء بإقرارات كاذبة تتمثل في التصريحات المغلوطة والمخالفة للحقيقة ذات علاقة بإنشاء شهادة التوقيع، سواء لمؤدي الخدمات التصديق الإلكتروني أو للطرف الثالث الموثوق، بغرض إصدار شهادة التصديق الإلكتروني الموصوفة.

ونلاحظ أن المشرع الجزائري قد إستعمل مصطلح "إقرارات" للتعبير على ما يصرح به الموقع لطلب إنشاء التوقيع، في حين أن التشريعات المقارنة قد إستعملت مصطلح "معطيات إنشاء التوقيع"، ونعتقد أن مصطلح إقرارات الأشمل ويستغرق كل المعلومات الأخرى[2]، كما أنه قد أغفل عن تحديد موضوع هذه الإقرارات.

والغرض من التجريم هو حماية المتعاملين في المعاملات الإلكترونية التي تعتمد على المنظومة المعلوماتية، والتي تعد المعلومات أو البيانات فيها عنصرًا جوهريًا، ويستوي بشأن هذه المعلومات أن تكون معالجة أو غير معالجة، بمعنى أن تكون مخزنة أو غير مخزنة داخل المنظومة المعلوماتية، وكذا تعزيز الثقة لدى المتعاملين ويحافظ على حقوقهم.[3]

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 724.

[2]- نفس المرجع، ص-ص 725-726

[3]- بلحاج محجوبة، مرجع سابق، ص 125.

وتعد الجريمة محل الدراسة من الجرائم الشكلية، وبالتالي لا يشترط المشرع لقيام ركنها المادي حلول ضرر أو تحقق نتيجة معينة، وإنما يكفي لقيامها تحقق السلوك الإجرامي وهو تقديم معلومات خاطئة أو كاذبة.

3-الركن المعنوي:

تعد الجريمة محل الدراسة من الجرائم العمدية التي تتطلب لقيامها تحقق القصد الجنائي العام بعنصريه العلم والإرادة، أي أن يعلم الجاني بأنه شخص الموقع طالب إنشاء التوقيع، ويعلم بأنه يقدم إقرارات ومعلومات كاذبة وعدم صحتها، ومع ذلك تنصرف إرادته السليمة الصريحة بإتيان السلوك الإجرامي بغية الحصول على شهادة التصديق الإلكتروني الموصوفة لتوقيعه.

ثانيًا: العقوبة المقررة لجريمة الإدلاء بتصاريح وإقرارات كاذبة

يترتب على قيام جريمة الإدلاء بتصاريح وإقرارات كاذبة توقيع العقوبة على الجاني إذا كان شخصًا طبيعيًا بالحبس من ثلاث (03) أشهر إلى ثلاث (03) سنوات وبغرامة من عشرين ألف 20.000 دج إلى مائتي ألف 200,000 دج، أو بإحدى هاتين العقوبتين فقط.[1]

أما إذا كان مقترف السلوك الإجرامي شخصًا معنويًا فإن العقوبة تكون الغرامة المقدرة مليون 1.000.000 دج حسب المادة 75 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي تقضي برفع الحد الأقصى للغرامة المقررة للشخص الطبيعي إلى خمس (05) مرات.

ويجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة المادة 09 من ق.ع.ج بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من ق.ع.ج بالنسبة للشخص المعنوي.

الفرع الثاني: جريمة إستعمال شهادة التصديق الإلكتروني الموصوفة لغير الغرض الذي منحت من أجله

شهادة التصديق الإلكتروني الموصوفة تصدر بناء على إرادة العميل الذي قدم طلب إصدارها، وملزم أن يستعملها فقط في الأغراض التي منحت من أجلها، وإلا يتابع بالجريمة المنصوص عليها في المادة 74 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر.[2]

[1]- المادة 66 من القانون رقم: 15-04 السالف الذكر.

[2]- تنص المادة 74 من القانون رقم: 15-04 السالف الذكر على أنه: "يعاقب بغرامة من ألفي 2.000 دج إلى مائتي ألف 200.000 دج، كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها".

أولًا: أركان جريمة إستعمال شهادة التصديق الإلكتروني الموصوفة لغير الغرض الذي منحت من أجله

لقيام الجريمة محل الدراسة لابد من توافر ثلاث أركان:

1- الركن المفترض:

يشترط المشرع الجزائري لقيام الجريمة محل الدراسة أن يحمل الجاني صفة صاحب الشهادة التصديق الإلكتروني الموصوفة، فبمجرد أن يستعمل شهادته لغير الأغراض التي منحت من أجلها تتحقق الجريمة.

2-الركن المادي:

لتحقق الركن المادي في الجريمة محل الدرسة، يشترط توافر:

أ-السلوك الإجرامي:

لقيام الجريمة محل الدراسة يقتضي إستعمال شهادة التصديق الإلكتروني الموصوفة من طرف صاحبها لغير الغرض الذي منحت لأجله وفقًا للمادة 74 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر، وعليه يتضح جليًا أنه لا يتحقق السلوك الإجرامي في حالة ما إذا تم إستعمال الشهادة من غير صاحبها، كما أنها من الجرائم السلوك أو الجرائم الشكلية فلا تحتاج إلى تحقيق نتيجة فيكفي لقيامها توفر النشاط الإجرامي.

وقد بينت المادة 15 من ذات القانون بأن هناك حدود لإستعمال شهادة التصديق الإلكتروني، غير أنها لم توضح هذه الحدود ذلك أن هذه الأخيرة تختلف بإختلاف نوع الشهادة، بحيث تتمثل حدود شهادة توثيق التاريخ في توثيق تاريخ ووقت إصدار التوقيع الإلكتروني، أما شهادة الإذن تتمثل في تقديم بيانات الموقع كمحل إقامته ومؤهلاته، في حين تتمثل حدود شهادة البيان في تأكيد صحة واقعة معينة ووقت وقوعها.[1]

ب-محل التجريم:

يتمثل محل الجريمة وفقًا لنص المادة 74 من ذات القانون، في شهادة التصديق الإلكتروني الموصوفة، وقد سبق وأن تطرقنا إليها في المبحث الأول من الفصل الأول ضمن الباب الأول.

3-الركن المعنوي:

جريمة إستعمال شهادة التصديق إلكتروني الموصوفة لغير الغرض الذي منحت لأجله هي جريمة عمدية تتطلب وجود القصد الجنائي العام والذي يقوم أساسًا على عنصري العلم والإرادة، وعليه لقيام هذه الجريمة لابد أن يعلم الجاني بأنه يستعمل شهادة التصديق الإلكتروني

[1]- بلحسيني حمزة، مرجع سابق، ص-ص 305- 306.

الموصوفة الممنوحة له في غير الغرض المخصص له وأن هذا الفعل مجرم قانونًا، ومع ذلك تنصرف إرادته السليمة إلى الإتيان بهذا السلوك الإجرامي.

ثانيًا: العقوبة المقررة لجريمة إستعمال شهادة التصديق إلكتروني الموصوفة لغير الغرض الذي منحت من أجله

يترتب على قيام جريمة إستعمال شهادة التصديق الإلكتروني لغير الغرض الذي منحت لأجله توقيع العقوبة على الجاني إذا كان شخصًا طبيعيًا، وذلك بالغرامة من ألفي 2.000 دج إلى مائتي ألف 200.000 دج[1]، أما إذا كان مقترفها شخصًا معنويًا فإن العقوبة تكون الغرامة المقدرة مليون 1.000.000 دج حسب المادة 75 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي تقضي برفع الحد الأقصى للغرامة المقررة للشخص الطبيعي إلى خمس (05) مرات.

ويجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة المادة 09 من ق.ع.ج بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من ق.ع.ج بالنسبة للشخص المعنوي.

المطلب الثالث: الجريمة المرتكبة من قبل الغير

يتطلب لإبرام المعاملات الإلكترونية توفير الثقة والأمان، لذلك كان لابد من إيجاد وسيلة للمحافظة على سرية البيانات وحمايتها لكي تمنع غير المتعاقدين -أو من يصرح له قانونًا بذلك- من الإطلاع عليها، لذلك إستخدمت وسيلة التشفير بكتابة أرقام أو رموز معينة بدلًا من الكتابة العادية، بحيث يكون المفتاح الخاص (Private Key) بالشفرة لا يعرفه إلا أطراف العملية التجارية.[2]

إلا أن المشرع الجزائري تدارك إمكانية حيازة أو إفشاء أو إستعمال هذه البيانات من الغير، وذلك بتجريمها بموجب المادة 68 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر.[3]

الفرع الأول: أركان جريمة حيازة أو إفشاء أو إستعمال بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير

يشتمل نص المادة 68 من القانون آنف الذكر على عدة أفعال وهي الحيازة والإفشاء والإستعمال بيانات إنشاء التوقيع الإلكتروني الخاصة بالغير، وبالتالي يعد أحد هذه الأفعال كاف لقيام الجريمة وتوقيع العقوبة على مقترفيها.

---

[1]- المادة 74 من القانون رقم: 15-04 السالف الذكر.

[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص 142.

[3]- تنص المادة 68 من القانون رقم: 15-04 السالف الذكر على أن: "يعاقب بالحبس من ثلاثة (03) أشهر إلى ثلاث (03) سنوات وبغرامة من مليون 1.000.000 دج إلى خمسة ملايين 5.000.000 دج، أو بإحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير".

أولًا: الركن المفترض

نظرًا لإمكانية إطلاع أكثر من شخص على المستند الإلكتروني لم يشترط المشرع الجزائري توفر صفة محددة في الجاني بالنسبة للجريمة محل دراستنا، ويتجلى ذلك من خلال إستعماله لمصطلح "كل من"، وبناءً عليه يعاقب كل من يقوم بحيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع موصوفة خاصة بالغير.

ومدلول الشخص لا ينصرف للموقع لأن المادة واضحة وصريحة حيث إستخدمت مصطلح بيانات إنشاء التوقيع الإلكتروني الخاصة بالغير، سيما وأن الفقرة الثانية من المادة 02 من نفس القانون تمنح للموقع أي لكل شخص طبيعي حق حيازة بيانات إنشاء التوقيع الإلكتروني، سواء كان هذا الشخص يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله.[1]

ثانيًا: الركن المادي:

لتحقق الركن المادي في الجريمة محل الدرسة، يشترط توافر:

1-السلوك الإجرامي:

يتحقق السلوك الإجرامي إما بحيازة بيانات التوقيع الإلكتروني الخاصة بالغير، وتكفي الحيازة المادية ولا يشترط الحيازة القانونية، وأيضًا تقوم الجريمة في الحالة التي يقوم فيها الجاني بإفشاء بيانات إنشاء التوقيع الإلكتروني[2]، والعلة في التجريم أن من وضعت لديه هذه البيانات يكون قد أؤتمن عليها لما تتمتع بها أو الإستعمال[3]، وقد تتحقق أيضًا الجريمة في إستعمال بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير، كإستخدام الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني، أي التي يستخدمها الشخص الطبيعي الذي يحوز بيانات إنشاء التوقيع الإلكتروني سواء كان هذا الأخير يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله.[4]

وتعتبر هذه الجريمة من الجرائم الشكلية التي تتحقق بمجرد قيام السلوك الإجرامي، ولا ضرورة حدوث ضررًا أو نتيجة عنها.

2-محل التجريم:

يتمثل محل السلوك الإجرامي في بيانات إنشاء التوقيع الإلكتروني الخاصة بالغير، وقد عرفها المشرع الجزائري بموجب الفقرة 05 من المادة 02 من القانون رقم: 15-04 المحدد

[1]- بلحسيني حمزة، مرجع سابق، ص 308.

[2]- يقصد بإفشاء بيانات إنشاء التوقيع الإلكتروني أي إطلاع الغير على البيانات الفريدة، كالرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني، وللمزيد من التفصيل، ينظر: نفس المرجع، ص 308.

[3]- عزيزة لرقط، مرجع سابق، ص 124.

[4]- بلحسيني حمزة، مرجع سابق، ص 309.

للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر على النحو الآتي: "بيانات إنشاء توقيع إلكتروني: بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الإلكتروني".

ثالثًا: الركن المعنوي:

جريمة حيازة أو إفشاء أو إستعمال بيانات إنشاء التوقيع الإلكتروني الموصوفة الخاصة بالغير جريمة عمدية يتطلب لقيامها توفر القصد الجنائي العام بعنصريه العلم والإرادة، أي أن يعلم الجاني بأنه يحوز أو يفشي أو يستعمل بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير، ويجب أن تتجه إرادة الجاني إلى إتيان أحد الأفعال المذكورة سلفاً.

الفرع الثاني: العقوبة المقررة لجريمة حيازة أو إفشاء أو إستعمال بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير

يترتب على قيام جريمة حيازة أو إفشاء أو إستعمال بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير، توقيع العقوبة على الجاني إذا كان شخصًا طبيعيًا بالحبس من ثلاثة (03) أشهر إلى ثلاث (03) سنوات وبغرامة من مليون 1.000.000 دج إلى خمسة ملايين 5.000.000 دج أو بإحدى هاتين العقوبتين فقط[1]، أما إذا كان مقترف السلوك الإجرامي شخصًا معنويًا فإن العقوبة تقدر خمس وعشرون مليون 25.000.000 دج حسب المادة 75 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر التي تقضي برفع الحد الأقصى للغرامة المقررة للشخص الطبيعي إلى خمس (05) مرات.

ويجوز الحكم بواحدة أو أكثر من العقوبات التكميلية الإختيارية المحددة المادة 09 من ق.ع.ج بالنسبة للشخص الطبيعي، وإلى العقوبات التكميلية المحددة فى نص المادة 18 مكرر من ق.ع.ج بالنسبة للشخص المعنوي.

[1]- المادة 68 من القانون رقم: 15-04 السالف الذكر.

خلاصة:

أصبحت النصوص القانونية الموضوعية التقليدية غير قادرة على مواجهة الجرائم الماسة بالمستندات الإلكترونية، مما دفع العديد من التشريعات المقارنة إلى سد الفراغ التشريعي إما من خلال إصدار قوانين جديدة أو تعديل القوانين القائمة وذلك عن طريق إضافة أحكام جديدة إلى قانون العقوبات أو إصدار تشريعات مستقلة تتعلق بالمعاملات الإلكترونية، وقد تناول الفقه الجنائي مسألة مدى تطابق أركان الجرائم المنصوص عليها في القواعد القانونية التقليدية مع بعض الجرائم المرتكبة على المستندات الإلكترونية، لاسيما الأفعال المشابهة لتلك التي تشكل أركان الجرائم التقليدية، والتي وضعت لتطبق وفق معايير ومعطيات معينة.

لذلك فقد تدارك المشرع الجزائري الوضع وتدخل لتحديد قواعد ومبادئ الحماية الجزائية لهذه الجرائم، من خلال القانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، حيث تم تجريم كافة الإعتداءات التي تستهدف المستند الإلكتروني وذلك في إطار الحماية الجزائية للأنظمة المعلوماتية، وقد وردت هذه الأحكام في القسم السابع مكرر من قانون العقوبات تحت عنوان:" المساس بأنظمة المعالج الآلية للمعطيات"، كما أصدر المشرع الجزائري القانون رقم: 15-04 المؤرخ في الأول من فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، بهدف سد الفراغ التشريعي وذلك لضمان خلق بيئة إلكترونية آمنة للتعامل عبر شبكة الإنترنت، إضافة إلى ذلك أصدر قانونًا مستقلًا يتعلق بمكافحة التزوير وإستعمال المزور بمقتضى القانون رقم: 24-02 المؤرخ في 26 فيفري 2024، وألغى جميع الأحكام المخالفة له في قانون العقوبات الجزائري.

خلاصة :

يتضح أن الدليل الإلكتروني المستخلص من الجرائم التي تمس بالمستندات الإلكترونية يخضع لنفس القواعد التي تحكم الأدلة المادية، سواء من حيث سلطة القاضي الجزائي في قبول هذا الدليل أو تقديره له، والقاضي الجزائي مقيدًا بضوابط قانونية معينة سواء ما كان متعلق بمبدأ مشروعية الحصول على الدليل الإلكتروني، وبوجوبية مناقشة هذا الدليل أثناء المحاكمة.

إختلف الفقه الجنائي والتشريعات المقارنة حول حجية المستند الإلكتروني في المواد الجزائية ومدى قوته في الإثبات، وذلك تبعًا للنظام القانوني المعتمد في كل الدولة، وقد تباينت أنظمة الإثبات الجنائي بشأن موقفها من إعتماد المخرجات الإلكترونية كدليل في الإثبات الجزائي.

وأصبحت النصوص القانونية الموضوعية التقليدية غير قادرة على مواجهة الجرائم الماسة بالمستند الإلكتروني، مما دفع العديد من التشريعات المقارنة إلى سد هذا الفراغ التشريعي من خلال إصدار قوانين جديدة، وفي هذا السياق فقد تدخل المشرع الجزائري لتحديد قواعد ومبادئ الحماية الجزائية لهذه الجرائم، حيث أصدر القانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004، كما أصدر أصدر القانون رقم: 15-04 المؤرخ في 01 فيفري 2015 الذي يحدد القواعد العامة للتوقيع والتصديق الإلكترونيين وذلك لضمان خلق بيئة إلكترونية آمنة للتعامل عبر شبكة الإنترنت، كما أصدر المشرع القانون رقم: 24-02 المؤرخ في 26 فيفري الذي يتناول مكافحة التزوير وإستعمال المستندات المزورة.

الباب الثاني:
الأحكام الإجرائية لمكافحة الجرائم الماسة بالمستند الإلكتروني

تمهيد :

رغم الجهود المبذولة في مكافحة الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص من الناحية العقابية الموضوعية، سواء من خلال سن تشريعات خاصة أو تعديل القوانين القائمة بإدماج نصوص جديدة ضمن قانون العقوبات أو عبر قوانين مستقلة، إلا أن القصور ظل يشكل عائقًا أمام فعالية هذه المكافحة منذ ظهور هذا النوع من الجرائم.

إذ لم تعد القواعد الإجرائية التقليدية كافية لملاحقة مرتكبيها، لكونها ترتكب غالبًا في الخفاء وعن بعد، مما يصعب إكتشافها وتحديد هوية المساهمين فيها والوصول إلى أثرها المادي، كما أن المجني عليه قد لا يلاحظ وقوع الجريمة أصلًا، وفي ظل نقص تدريب السلطات القضائية على التعامل مع هذا النوع من الأدلة، وما قد يستخدمه المجرم المعلوماتي من تدابير الحماية الفنية التي تحول دون كشف أمره مما يعيق الوصول إلى الدليل الذي يدينه، الأمر الذي إستوجب التدخل التشريعي لسد الفراغ التشريعي، ومواكبة هذا النوع المستحدث من الإجرام المرتبط بالتطور التكنولوجي.

إرتأينا تقسيم دراستنا إلى فصلين، نتطرق إلى الآليات لمكافحة الجرائم الماسة بالمستند الإلكتروني في (الفصل الأول)، الذي سوف نتطرق فيه إلى الآليات الوطنية لمكافحة الجرائم الماسة بالمستند الإلكتروني في (المبحث الأول)، بينما سنتطرق إلى آليات التعاون الدولي في مكافحة الجرائم الماسة بالمستند الإلكتروني في (المبحث الثاني)، أما (الفصل الثاني) فقد خصصناه إلى إجراءات إستخلاص الدليل الإلكتروني في الجرائم الماسة بالمستند الإلكتروني، بحيث سنتطرق إلى الإجراءات التقليدية والتقنية لإستخلاص الدليل الإلكتروني في (المبحث الأول)، بينما إلى الإجراءات المستحدثة لإستخلاص الدليل الإلكتروني في (المبحث الثاني).

الفصل الأول:

آليات مكافحة الجرائم الماسة بالمستند الالكتروني

تمهيد :

تتصف الجرائم الماسة بالمستند الإلكتروني بكونها جرائم عابرة للحدود تتم غالبًا في الخفاء وغير مرئية في كثير من حالاتها، وهو ما يجعل إثباتها وتحديد هوية مرتكبيها أمرًا بالغ الصعوبة، مما فرض ضرورة البحث عن آليات المساعدة أكثر ملاءمة لطبيعتها التقنية بما يستوجب إيجاد وسائل حديثة ومتطورة، دون إغفال دور الآليات التقليدية المعتمدة في المسائل الجنائية متى ثبت فعاليتها، كإستعانة بالأجهزة الوطنية المختصة في حال إرتكاب الجريمة في دولة أخرى، والإستماع إلى شهادة الشهود، أو اللجوء إلى الخبرة التقنية، وغيرها من الوسائل التي كرستها القوانين الجنائية لتسهيل عمل سلطات التحري والتحقيق في إطار مكافحة هذا النوع من الجرائم.

لم تكن الآليات المخصصة لها على المستوى الوطني كافية وحدها لمكافحة هذا النوع من الجرائم، بل إستلزم الأمر وضع آليات تنسيق وتعاون على المستويين الإقليمي والدولي، تتكاثف فيها الجهود وتتوحد من أجل إيجاد وسائل فعالة وناجعة للتصدي لهذه الظاهرة الإجرامية المستحدثة، التي باتت ترتكب من خلالها أخطر الجرائم وأكثرها تعقيدًا.

إرتأينا تقسيم دراستنا إلى مبحثين، نتطرق إلى الآليات الوطنية لمكافحة الجرائم الماسة بالمستند الإلكتروني في (المبحث الأول)، أما (المبحث الثاني) فقد خصصناه إلى آليات التعاون الدولي في مجال الجرائم الماسة بالمستند الإلكتروني.

المبحث الأول: الآليات الوطنية لمكافحة الجرائم الماسة بالمستند الإلكتروني

سنتطرق إلى الشهادة الإلكترونية والخبرة التقنية ودورهما في إثبات الجرائم الماسة بالمستند الإلكتروني في (المطلب الأول)، أما (المطلب الثاني) فقد خصصناه إلى الأجهزة المختصة وطنيًا في التحقيق الجنائي في الجرائم الماسة بالمستند الإلكتروني.

المطلب الأول: الشهادة الإلكترونية والخبرة التقنية ودورهما في إثبات الجرائم الماسة بالمستند الإلكتروني

يميز بين كل من الخبرة والشهادة من حيث أن الأولى ترتكز على الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها التدليلية في الإثبات على خلاف الثانية، ومن ثم كانت الخبرة وفقًا على رأي الأخصائيين من أهل العلم والتكنولوجيا لا بناء على مجرد مشاهدتهم أو سماعهم، فالشاهد يدلي بأقواله عن الواقعة كما حدثت، أما الخبير فشهادته فنية أي تنصرف إلى تقييمه الفني للواقعة محل الخبرة، ونتيجة لذلك أجاز الفقه إستبدال الخبير في الدعوى بغيره من الخبراء وهو أمر غير متصور بالنسبة للشاهد لأن دوره في الدعوى قاصر عليه وحده.[1]

الفرع الأول: الشهادة الإلكترونية وعلاقتها بالجرائم الماسة بالمستند الإلكتروني

الشهادة هي التصريحات التي يدلى بها الأطراف غير الخصوم أمام السلطة القضائية المختصة بشأن جريمة، سواء كانت تتعلق بثبوت إدانة المتهم وظروف إرتكابها وإسنادها إليه أو براءته منها، وللشهادة أهمية بالغة في مجال الإجراءات الجزائية لأن الجريمة ليست تصرفًا قانونيًا ولكنها سلوك غير مشروع، يجتهد الجاني في التكتم عن سلوكه الجرمي ويحرص على إخفائه عن أعين الناس.[2]

وكثيرًا ما يكون للشهادة أثناء إجراءات التحري والتحقيق أثر في القضاء بالإدانة أو بالبراءة، لأن الشهادة قد يدلى بها فور وقوع الحادث وقبل أن تمتد يد العبث وقبل أن يطول عليها الوقت فتضعف معالم الوقائع التي تنصب عليها.[3]

والشهادة في الجرائم الماسة بالمستند الإلكتروني لا تختلف من حيث ماهيتها عن تلك في الجرائم التقليدية، وللتعمق أكثر في الدراسة سنتطرق إلى مفهوم الشهادة في مجال الجرائم الماسة بالمستند الإلكتروني في (المطلب الأول)، بينما سنتطرق في (المطلب الثاني) إلى الشاهد المعلوماتي وجزاء تخلفه عن إلتزاماته.

---

[1]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 316.

[2]- علي عدنان فيل، **إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)**، د.ر.ط، 2012، دار الكتب والوثائق القومية، الإسكندرية-مصر، ص 61.

[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 125.

أولًا: مفهوم الشهادة في مجال الجرائم الماسة بالمستند الإلكتروني

سنتناول تعريف الشهادة في مجال الجرائم الماسة بالمستند الإلكتروني، مع التطرق إلى مدلول الشاهد المعلوماتي.

1- تعريف الشهادة في مجال الجرائم الماسة بالمستند الإلكتروني:

سنتطرق إلى تعريف الشهادة وأنواعها، وإلى المحادثة المرئية عن بعد:

أ- تعريف الشهادة:

عرفت الشهادة بصفة عامة بأنها: "التصريحات التي يدلى بها الأطراف غير الخصوم أمام السلطة القضائية المختصة بشأن جريمة وقعت، سواء كانت تتعلق بثبوت إدانة المتهم وظروف إرتكابها وإسنادها إليه أو براءته منها"[1]، كما عرفتها محكمة النقض المصرية بقولها: "الشهادة في الأصل هي تقرير شخص لما يكون قد رآه، أو قد سمعه بنفسه، أو قد أدركه على وجه العموم بحواسه"[2].

إستنادًا إلى ما تقدم، يمكن تعريف الشهادة الإلكترونية على أنها : "إثبات واقعة معينة من خلال ما يصرح به أحد الأشخاص لما يكون قد شاهده بحواسه عن هذه الواقعة بطريقة مباشرة، عن طريق الإدلاء بأقواله بواسطة وسيط معلوماتي أو منظومة إلكترونية" أو هي: "تقرير الشخص لما يكون قد أدركه أو سمعه أو رآه على وجه العموم بحواسه، على أن يتم هذا التقرير عبر الوسائط الإلكترونية أو النظم المعلوماتية".[3]

وتنقسم الشهادة إلى نوعين كما يلي:

أ-1- الشهادة المباشرة:

يقصد بالشهادة المباشرة أن المعلومات التي يدلي بها الشخص ليست محل رأي أو معتقد شخصي لديه وإنما وصلت إلى حواسه مباشرة ودون وساطة شخص آخر، فقد تأتي الشهادة نتيجة سماع الشخص لأقوال صدرت عن شخص آخر، وقد تكون ناتجة عن حاسة البصر كأن يشاهد الشخص الواقعة التي يدلي عنها الشهادة، وقد تكون كذلك ناتجة عن حاسة الشم كأن تصل رائحة معينة إلى حاسة الشم لديه مثل شم الضابط أحيانًا لرائحة المخدرات في مكان ما.[4]

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 125.

[2]- بلولهي مراد، مرجع سابق، ص 50.

[3]- عادل بوزيدة، **دور الشهادة الإلكترونية في الإثبات الجزائي على ضوء قانون الإجراءات الجزائية الجزائري**، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي-تبسة، مجلة النبراس للدراسات القانونية، المجلد الأول، العدد الأول، سبتمبر 2016، الجزائر، ص 137.

[4]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 257.

فهنا تكون المعلومة في هذا النوع هي الشهادة ذات الوضع الذي يمكن الوثوق به قانونًا، أو بعبارة أدق وضع نوع معين من الثقة يخضع للسلطة التقديرية لقاضي الموضوع بإعتبارها إحدى الأدلة التي يستند إليها في نظرية الإثبات الجنائي في نطاق المواد الجنائية.[1]

أ-2- الشهادة غير المباشرة (الشهادة السماعية):

هناك أيضًا ما يسمى بالشهادة غير المباشرة أي الشهادة السماعية[2]، وذلك حينما لا يشهد الشخص بما رآه أو سمعه مباشرة فهو لم يعاين واقعة محل الإثبات بنفسه وإنما سمع غيره يذكر معلومات بشأنها.

ولا شك أن هذه الشهادة الواقعة بالإستماع تعبر عن إشاعات قد تصدق وقد تكذب، من أجل ذلك فإنها تسمع عن سبيل الإستئناس حيث أنها تمثل أضعف أنواع الشهادة، وذلك لأن النقل من الغير من شأنه أن يلحق بالمعلومات بالعديد من التغييرات، فمن سمع من الغير قد يبالغ في عواطفه ووصفه للأمور أو قد يقلل من أهميتها فهو لم يعش الموقف نفسه الذي عاشه الشخص الوسيط بظروفه وأحداثه، وهو أمر يمكنه من النقل شبه الحقيقي إن لم نقل الموقف ذاته ولكن النقل إلى الغير وشهادة هذا الغير لا تتطابق مع الواقع، وهو ما دفع بالعديد من التشريعات إلى منع شهادة الإستماع أو قبولها بشروط محددة على سبيل الحصر.[3]

ومن القواعد العامة المستقرة في القانون الجنائي عدم قبول البينة السماعية أمام المحاكم الجنائية إلا في حالات إستثنائية حصرها القانون بشروط مشددة، وينسب عدم قبول البينة السماعية إلى إستحالة إستجواب ومناقشة حجية الأدلة الجنائية الإلكترونية، على سبيل المثال لقد تضمنت القواعد الفيدرالية الأمريكية نصًا يعتبر السجلات والمعطيات المنظمة بدقة بينة مقبولة أمام المحاكم الجنائية إستثناء للبينة السماعية، وبناء على تلك القواعد تعد التقارير والمعلومات والمعطيات المحفوظة في أي شكل وكذلك الوقائع والأحداث والأراء ونتائج التحاليل المنقولة بواسطة أصحاب المعرفة والخبرة فى نطاق الأنشطة والممارسات المنظمة بينة مقبولة أمام المحاكم الجنائية، لكونها معطيات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من

---

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 259.

[2]- من التطبيقات على ذلك التساؤل في الفقه الأمريكي حول ما إذا كانت المخرجات الإلكترونية يمكن القبول بها وفقًا لقواعد السماع الواردة في المادة 803، حيث إنتهت محكمة black burn إلى أن المخرجات الإلكترونية لا تصلح لتطبيق قواعد السماع، حيث إعتبرت المحكمة المستند الإلكتروني الناتج عن الجهاز الإلكتروني فى تلك الحالة غير معترف به وفقًا لتلك المادة، غير أن محكمة إستئناف black burn خالفت ذلك النهج وإعتبرت أن مخرجات طابعة الجهاز الإلكتروني يعتمد عليها بشكل كاف، ويمكن قبولها وفقًا لإستثناء السماع في المادة 24/806 من قانون الإثبات الفيدرالي، ومؤدى ذلك أن سجلات الإلكترونية المخزنة التى تحتوي على بيانات سماعية أو بصرية تخضع لإستثناء قاعدة السماع، متى قدمت للتدليل على إرتكاب جريمة إعتداء على المستند الإلكتروني، غير أنه وحتى تقبل المحكمة فى تلك الحالة بالمستند الإلكترونى كدليل إثبات، ويجب أن تتحقق من أن معطيات المستند الإلكتروني قد إستوفت الشروط المشروعية والثقة، كما أن المحاكم بصفة عامة تسمح بقبول سجلات الإلكترونية المخزنة كسجلات أعمال وفقًا للمادة 803/ 6 من قانون الإثبات الفيدرالي، ولقد قرر القضاء أن سجلات الإلكترونية المتعلقة بالأعمال يعترف بها إذا تم حفظها طبقاً لإجراء تقني مصمم لضمان دقتها أو تم إبتكارها لأجل دوافع تهدف إلى ضمان دقتها، وللمزيد من التفصيل، ينظر: سحر سعد عبد السميع محمد، مرجع سابق، ص-ص 315-316.

[3]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 260.

الأدلة السماعية، والأدلة الجنائية الإلكترونية من هذا القبيل لكونها معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آليًا بأسلوب علمي.[1]

ب- المحادثة المرئية عن بعد:

أخذ المشرع الإنجليزي بتقنية المحادثة المرئية عن بعد (vidéo conférence) بمقتضى قانون العدالة الجنائية لسنة 1988 ودخل حيز التنفيذ في سنة 1989 بموجب المادة 32 منه، الذي يجيز إستخدام دائرة تليفزيونية مغلقة تتيح للطفل الإدلاء بشهادته من قاعة مجاورة أثناء المحاكمة[2]، وإذا كان عمره أقل من 16 سنة ويجرى إستجوابه في إحدى جرائم الإعتداء البدني على الأشخاص أو إلحاق الأذى به أو تهديده، أو إذا كان الطفل مجني عليه ويجرى إستجوابه في جريمة إرتكاب الفاحشة أو في جريمة تنطوي على إستعمال قسوة، وكذا يجيز الإستماع لإدلاء الشاهد بشهادته في حالة ما إذا كان خارج الإقليم الوطني لبريطانيا، ومن ثم يقتصر إستعمال تقنية المحادثة المرئية عن بعد على سماع الشهود دون أن يمتد ذلك لسماع المتهمين، ولا يجوز الإدلاء بالشهادة دون الحصول على الإذن من المحكمة المختصة.[3]

وقد أجازت عدة ولايات في الولايات المتحدة الأمريكية على إستعمال تقنية المحادثة المرئية عن بعد في المحاكمات الجزائية إلا أنها إقتصرت ذلك في سماع الأطفال القصر، ففي قضية ولاية ماريلاند في مواجهة المسمى كريغ من أبرز القضايا التي قررت فيها المحكمة العليا الأمريكية على عدم تعارض بند المواجهة مع إستعمال تقنية المحادثة المرئية عن بعد من أجل الاستماع إلى أقوال الشهود في مواجهتهم بالمتهمين، وقد تم إستعمال التقنية للسماح لضحية الإعتداء الجنسي يبلغ من العمر ست (06) سنوات الإدلاء بشهادته، طبقًا لقانون هذه الولاية الذي يجيز بذلك في الحالة التي قد ينتج عن الإدلاء بها داخل قاعة المحكمة إلى تعرض الطفل بالإصابة بإضطراب نفسي حاد كأن يفقد القدرة على التواصل.[4]

وقد أشارت بعض التقارير إلى موافقة المحكمة العليا الأمريكية في 03 ماي 2020 على إنعقاد لجلسات الإستماع في عشر (10) دعاوى منظورة أمامها عبر تقنية المحادثة المرئية عن بعد، وكذا قبولها بتغطية المسموعة لهذه الجلسات كتدبير من التدابير الإحترازية لمواجهة وباء كوفيد-19، بالرغم من أن كانت المحكمة دائمًا ترفض لهذه التقنيات نتيجة لتمسكها الحازم

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 259.

[2]- رامي متولي القاضي، **إجراءات التحقيق والمحاكمة عن بعد- دراسة تحليلية مقارنة**، جامعة الشارقة، مجلة جامعة الشارقة للعلوم القانونية، المجلد19، العدد 02، جوان 2022، الإمارات العربية المتحدة، ص 386.

[3]- نفس المرجع، ص 387.

[4]- بوخلوط الزين، **آلية المحاكمة عن بعد ومبادئ المحاكمة العادلة**، كلية الحقوق، جامعة عين تموشنت، مجلة البصائر للدراسات القانونية والإقتصادية، المجلد 01، العدد 03، ديسمبر 2021، الجزائر، ص- ص 86-87.

بتقاليدها التاريخية وهو ما إعتبره البعض بالتحسن الإيجابي الذي يعزز من مبدأ شفافية القضاء.[1]

وبالنسبة للمشرع الفرنسي فقد أجاز بموجب المادة 706-61 من ق.إ.ج.ف أن يطلب المتهم في مرحلة التحقيق الإبتدائي أو المحاكمة أن يواجه مع الشاهد تطبيقًا لأحكام المادة 706-58 من نفس القانون من خلال جهاز فني يسمح بإجراء جلسة سماع للشاهد عن بعد أو أن يطلب إستجواب هذا الشاهد من قبل محاميه بالوسيلة نفسها، وأن يتم عرض صوت الشاهد بطريقة لا تسمح بالتعرف على هويته بواسطة العمليات التقنية المناسبة، وإذا أمرت المحكمة بتقديم معلومات إضافية لغرض سماع الشاهد فإن هذا الأخير يتم سماعه إما من قبل قاضي التحقيق المكلف بتنفيذ ذلك أو عن طريق أحد أعضاء المحكمة يطلب إختياره لذلك بإستخدام وسائل التقنية المقدمة.[2]

كما قد تبنى المشرع الفرنسي إمكانية إستخدام تقنية المحادثة المرئية عن بعد لتسيير إجراءات التحقيق والمحاكمة بموجب المادة 706-71 من قانون الإجراءات الجزائية، والتي طرأ عليها عدة تعديلات ليشمل هذا الإستخدام تقريبًا كل مراحل الدعوى العمومية بمقتضى عدة قوانين ساهمت في توسيع من نطاق إستخدام إجراء تقنية المحادثة المرئية عن بعد كإجراء الإستجواب والسماع في مرحلة التحري والتحقيق، وأيضًا فيما يخص إجراء التقديم أمام وكيل الجمهورية أو قاضي التحقيق بهدف تمديد في فترة التوقيف للنظر، وأيضًا فيما يخص إجراء المناقشة الوجاهية سواء بهدف وضع المتهم رهن الحبس المؤقت أو فيما يتعلق بتمديده أو إستئنافه.[3]

وأصدرت محكمة النقض الفرنسية بتاريخ 02 مارس 2011 قرارًا مفاده أن الإستعانة بالتقنيات المنصوص عليها في المادة 706-71 من ق.إ.ج.ف لا يتطلب تسبيبًا خاصًا من قبل المحاكم كما أن ضمانات المحاكمة العادلة مرتبطة أساسًا بالتقنيات المستعملة لذلك، وهو القرار

---

[1]- رامي متولي القاضي، **إجراءات التحقيق والمحاكمة عن بعد- دراسة تحليلية مقارنة**، المرجع السابق، ص- ص 385-386.

[2]-Art 706-61 du C.P.P.F (Loi n°2004-204 du 9 mars 2004 - art. 141 JORF 10 mars 2004) dispose que: « La personne mise en examen ou renvoyée devant la juridiction de jugement peut demander à être confrontée avec un témoin entendu en application des dispositions de l'article 706-58 par l'intermédiaire d'un dispositif technique permettant l'audition du témoin à distance ou à faire interroger ce témoin par son avocat par ce même moyen. La voix du témoin est alors rendue non identifiable par des procédés techniques appropriés. Si la juridiction ordonne un supplément d'information aux fins d'audition du témoin, ce dernier est entendu soit par un juge d'instruction désigné pour exécuter ce supplément d'information, soit, si l'un des membres de la juridiction a été désigné pour exécuter cette audition, en utilisant le dispositif technique prévu par l'alinéa précédent».

[3]- بن عزة محمد حمزة، **تطور تجربة القضاء الفرنسي في إستعمال تقنية المحادثة المرئية من إجراء إستثنائي إلى سياسة قضائية**، الملتقى الوطني حول إستخدام تقنية المحادثة المرئية عن بعد في القضاء الوطني والدولي بين متطلبات العصرنة ومقتضيات حماية حقوق الأشخاص، كلية الحقوق، جامعة الجزائر-1- بن يوسف بن خدة، المنعقد يوم 12 مارس 2023، الجزائر، ص 255.

الذي تلاه عدة قرارات مؤيدة لإستعمال تقنية المحادثة المرئية عن بعد مؤكدة فيها أن الحضور الشخصي للمتهم ليس ضروريًا ويتحقق حتى ولو تمت المحاكمة عن بعد.[1]

وبسبب إنتشار جائحة كوفيد-19 وحالة الطوارئ المعلنة والمفروضة في البلاد أصدرت الحكومة الفرنسية عدة قرارات لتتحكم في الوضع منها الأمر رقم: 2020-1401 المؤرخ في 18 نوفمبر 2020 المتعلق بتيسير الإجراءات القانونية والإقتصادية، بحيث أدخل تعديلات تسمح بإستعمال آلية المحاكمة المرئية عن بعد في كافة المحاكمات الجزائية بما فى ذلك الجنايات، كما ألغى شرط الموافقة المسبقة للمتهم ليتم محاكمته عبر هذه التقنية، وبناءً على ذلك أصبح إستعمال هذه الآلية كأصل عام بعدما كان إستثناءًا، وهو القرار الذي أثار جدلًا من رجال القانون وهيئات الدفاع عن حقوق الإنسان خاصة نقابة القضاة الفرنسيين وكذا نقابة المحامين بحجة أن العمل بهذه الآلية بهذه الطريقة يترتب عليه مساس وإنتهاك لضمانات المحاكمة العادلة[2]، ثم أصدر مجلس الدولة الفرنسي قرارًا بتاريخ 04 أوت 2021 ألغى القرار السابق ذكره معتبرًا إياه أنه يمثل إنتهاكًا خطيرًا وواضحًا لحقوق الدفاع لا يمكن تبريره بمقتضيات الوضع الصحي الناتج عن وباء كوفيد-19، كما أصدر المجلس الدستوري الفرنسي بتاريخ 15 جانفي 2021 قرارًا تحت رقم: 2020-872 قضى بعدم دستورية المحاكمة عبر تقنية المحادثة المرئية عن بعد التي تجري دون الموافقة المسبقة للمتهم[3].

وسلك المشرع الجزائري في ذلك مسلك أقرانه من التشريعات المقارنة من خلال تبنيه تقنية المحادثة المرئية عن بعد بمقتضى تعديل الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية بموجب الأمر رقم: 15-02 المؤرخ في 23 جويلية 2015[4] فيما يتعلق بحماية الشهود والخبراء والضحايا، ونص صراحة على جواز أمر جهة الحكم تلقائيًا أو بطلب من الأطراف بسماع الشاهد مخفي الهوية عن طريق وضع وسائل تقنية تسمح بكتمان هويته بما في ذلك السماع عن طريق المحادثة المرئية عن بعد وإستعمال الأساليب التي لا تسمح بمعرفة صورة الشخص وصوته[5]، وذلك كتدبير من التدابير الحماية إذا كانت حياتهم أو سلامتهم الجسدية أو حياة أو سلامة أفراد عائلاتهم أو أقاربهم أو مصالحهم الأساسية معرضة لتهديد خطير، بسبب المعلومات التي يمكنهم تقديمها للقضاء والتي تكون ضرورية لإظهار الحقيقة في قضايا الجريمة المنظمة أو الإرهاب أو الفساد[6].

---

[1]- بوخلوط الزين، مرجع سابق، ص 87.

[2]- نفس المرجع، ص 83.

[3]- نفس المرجع، ص 88.

[4]- الأمر رقم: 15-02 المؤرخ في 23 جويلية 2015، المعدل والمتمم للأمر رقم: 66-155 المورخ في 08 جوان 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج.ش العدد 40، الصادرة بتاريخ 23 جويلية 2015، الملغى.

[5]- الفقرة الأولى من المادة 65 مكرر27 من الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم السالف الذكر، الملغى.

[6]- المادة 65 مكرر19 من الأمر رقم: 66-155 السالف الذكر، الملغى.

كما أجاز المشرع الجزائري إستعمال تقنية المحادثة المرئية عن بعد بموجب القانون رقم: 15-03 المؤرخ في 01 فيفري 2015 المتعلق بعصرنة العدالة[1] إذا إستدعى بعد المسافة أو تطلب ذلك حسن سير العدالة، وتحديدًا في المادة الأولى منه والتي نصت على أن: "يهدف هذا القانون إلى عصرنة سير قطاع العدالة من خلال...- إستخدام تقنية المحادثة المرئية عن بعد في الإجراءات القضائية"، وذلك من خلال وضع منظومة معلوماتية مركزية تابعة لوزارة العدل تسمح بإستعمال تقنية المحادثة المرئية عن بعد في الإجراءات القضائية، وجاء هذا في الفصل الرابع تحت عنوان: "إستعمال المحادثة المرئية عن بعد أثناء الإجراءات القضائية" حيث نظم إجراءاتها وشروطها في المواد 14،15 و16 من نفس القانون، وهو القانون الذي أعتمد فيه المشرع تقنية المحادثة المرئية عن بعد كآلية تكرس التقاضي الإلكتروني وتسيير الإجراءات القضائية، فالمحاكمة المرئية وفقًا لهذا القانون تقنية تمكن القاضي سواء قاضي التحقيق أو قاضي الحكم من سماع المتهمين أو الشهود أو الخبراء عن بعد.

فقد نص المشرع الجزائري على تقنية المحادثة المرئية عن بعد بموجب القانون رقم: 15-03 المتعلق بعصرنة العدالة السالف الذكر ولكن لم يقوم بتطبيقها وبقي على نظام المحاكم التقليدية القائم على الوثائق الورقية، فقد كانت فترة جمود النص من حيث التطبيق ولم تفعل المحاكم الإلكترونية إلى غاية تدهور الوضع الصحي في ظل جائحة وباء كوفيد-19، مما جعلها تبادر بتنفيذ تقنيات التكنولوجيا وإدخالها حيز التنفيذ على مستوى السلطات القضائية تفاديًا لتفشي وباء كوفيد-19 على مستوى قطاع العدالة، حيث أصدر تعديلًا لقانون الإجراءات الجزائية وطبقت تقنية المحاكم الإلكترونية فعليًا في سنة 2020[2] وذلك قصد مواجهة الظروف الإستثنائية التي فرضها تفشي وباء كوفيد-19 وتداعياته على مختلف القطاعات وإحداثه لعزلة، بموجب الأمر رقم: 20-04 المؤرخ في 20 أوت 2020 المعدل والمتمم للأمر رقم: 66-155 والمتضمن قانون الإجراءات الجزائية[3] وإستحدث بموجبه الكتاب الثاني مكرر بعنوان: "إستعمال وسائل الإتصال المسموعة والمرئية أثناء الإجراءات"، وقسمه إلى ثلاثة أبواب تضمنت على التوالي الأحكام العامة وإستعمال المحادثة المرئية عن بعد في التحقيق القضائي وإستعمال المحادثة المرئية عن بعد في مرحلة المحاكمة من خلال تنظيمهم في المواد من 441 مكرر إلى 441 مكرر 11 وألغى جميع الأحكام المخالفة له.

---

[1]- القانون رقم: 15-03 المؤرخ في 01 فيفري 2015، المتعلق بعصرنة العدالة، ج.ر.ج.ج.ش العدد 06، الصادرة بتاريخ 10 فيفري 2015.

[2]- سامية غراب، ماجدة شهيناز بودوح، **متطلبات تجسيد المحاكم الإلكترونية في ظل البيئة الرقمية على ضوء التشريع الجزائري**، كتاب جماعي دولي بعنوان: **المحكمة الإلكترونية كوسيلة لتقريب مرفق القضاء من المواطن**، الطبعة الأولى، سبتمبر2022، المركز المغاربي- شرق أدنى للدراسات الإستراتيجية، المملكة المتحدة – بريطانيا-، ص 158.

[3]- الأمر رقم: 20-04 المؤرخ في 30 أوت سنة 2020، المعدل والمتمم للأمر رقم: 66- 155 المؤرخ في 08 جوان سنة 1996 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج.ش العدد 51، الصادرة في 31 أوت سنة 2020، الملغى.

وبموجب إلغاء الأمر رقم: 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية السالف الذكر بموجب القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية السالف الذكر، إلا أن هذا الأخير أعاد إدراج تقنية المحادثة المرئية عن بعد ضمن المواد من 128 إلى 138 ضمن الفصل السادس من الباب الثاني من الكتاب الثاني، وقد وسع من نطاق الحماية التي كانت مقتصرة في السابق على حماية الشهود والخبراء والضحايا فقط، جعلها تشمل أيضًا حماية المدعين المدنيين والأطراف المدنية والمبلغين، كما توسع في مجال الجرائم التي تطبق فيها هذه الحماية بعد أن كانت مقتصرة فقط في قضايا الجريمة المنظمة أو الإرهاب أو الفساد بسبب المعلومات التي يمكنهم تقديمها للقضاء والتي تكون ضرورية لإظهار الحقيقة، لتشمل الجرائم ضد أمن الدولة، والمتاجرة بالمخدرات والمؤثرات العقلية، وتبييض الأموال، وجرائم الإتجار بالبشر وجرائم الإتجار بالأعضاء، وجرائم تهريب المهاجرين، كما أجاز بإمكانية تمديد الحماية إلى جرائم أخرى إذا كانت حالة المعني تستوجب ذلك[1].

ويلاحظ كذلك أن المشرع الجزائري قد شدد العقوبات ضد كل من يكشف عن هوية أو عنوان الأشخاص المستفدين من الحماية، كما يتعرض المبلغ الذي يقوم بتبليغ عن وقائع غير صحيحة للعقوبات المقررة للوشاية الكاذبة المنصوص عليها في قانون العقوبات الجزائري، كما أدرج في المقابل إعفاء هذا الأخير من المتابعة التأديبية أو الجزائية بإفشاء السر المهني لتبليغه عن جرائم أطلع عليها أثناء أو بمناسبة أداء مهامه[2].

وتم إلغاء الأمر رقم: 20-04 المؤرخ في 20 أوت 2020 المعدل والمتمم للأمر رقم: 66-155 والمتضمن قانون الإجراءات الجزائية السالف الذكر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، غير أن هذا الأخير أعاد تنظيم الأحكام المتعلقة بإستعمال وسائل الإتصال المسموعة والمرئية أثناء الإجراءات بإدراجها في المواد من 639 إلى 650 ضمن الكتاب الخامس، ومكن الجهات القضائية لمقتضيات حسن سير العدالة أو حماية المتهم أو الحفاظ على الأمن والنظام العام أو الصحة العمومية أو أثناء الكوارث الطبيعية أو لدواعي إحترام مبدأ الآجال المعقولة، إستعمال المحادثة المرئية عن بعد في الإجراءات القضائية مع إحترام الحقوق والقواعد المنصوص عليها في هذا القانون.[3]

[1]- المادة 128 من القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر.

[2]- المادة 137 من القانون رقم: 25-14 السالف الذكر.

شدد القانون رقم: 25-14 السالف الذكر العقوبات المنصوص عليها في المادة 138، ضد كل من يكشف عن هوية أو عنوان الأشخاص المستفدين من الحماية، حيث تم رفع الحد الأدنى لعقوبة الحبس من ستة (06) أشهر إلى سنة (01) مع الإبقاء على الحد الأقصى بخمس (05) سنوات، كما رفع الحد الأدنى للغرامة المالية من 50.000 دج إلى 100.000 دج مع الإبقاء على الحد الأقصى البالغ 500.000 دج، وأضاف عبارة "دون الإخلال العقوبات الأشد المنصوص عليها في التشريع المفعول".

[3]- المادة 1/639 من القانون رقم: 25-14 السالف الذكر.

3- مدلول الشاهد المعلوماتي في الجرائم الماسة بالمستند الإلكتروني:

سنتناول تعريف الشاهد المعلوماتي مع بيان فئاته:

أ- تعريف الشاهد المعلوماتي:

يمكن تعريف الشاهد بأنه: "الشخص الذي لا تقوم ضده أسباب معقولة لقيام شبهة مساهمته في الجريمة، أو لا تتوافر في حقه دلائل قوية ومتوافقة على إتهامه بإرتكاب الجريمة أو مشاركته فيها يكون قد شاهد الواقعة موضوع البحث أو له معلومات عنها"[1]، ويمكن تعريفه أيضًا بأنه: "كل شخص الذي عاين معلومات عن الواقعة عن طريق حاسة من حواسه"، أو هو: "كل شخص الذي تكون له معلومات التي تثبت الواقعة أو تنفيها".

والشاهد في الجريمة الماسة بالمستند الإلكتروني هو الشخص الفني والمتخصص وصاحب الخبرة في علوم التقنية الرقمية والمعلوماتية وشبكات الإتصال والذي يعتمد عليه في التحقيق الجنائي، وقد أطلق البعض عليه مصطلح الشاهد المعلوماتي تمييزًا له عن الشاهد في الجرائم التقليدية.[2]

ولا يقصد أن يكون الشاهد خبيرًا تقنيًا، فالشاهد يدلي بأقواله عن الواقعة كما حدثت في مادياتها، أما الخبير فشهادته فنية أي تنصرف إلى تقييمه الفني للواقعة محل الخبرة، ونتيجة لذلك أجاز الفقه إستبدال الخبير في الدعوى بغيره من الخبراء، وهو أمر غير متصور بالنسبة للشاهد لأن دوره في الدعوى قاصر عليه وحده.[3]

ونظرًا إلى الإختلاف الموجود بين الشاهد المعلوماتي والشاهد العادي فهذا الأخير قد يساهم بدور فعال في إتمام العملية الإثباتية في الجرائم الماسة بالمستند الإلكتروني عندما يتعلق الأمر بالسلوك المادي في العالم الواقعي للمجرم المعلوماتي، كأن يحدد من طرف السلطة القضائية المختصة مصدر السلوك الجرمي عبر الإنترنت عن طريق عنوان الجهاز الإلكتروني المتصل (IP) الذي قد يكون في مقهى الإنترنت، أما الشاهد فهو صاحب أو مساعد صاحب المحل أو غيره من الذين يشهدون على ما وقع كالتردد المنتظم للمشتبه فيه وعلى نفس الجهاز الإلكتروني مما قد يساعد ذلك في متابعته.[4]

---

[1]- عبدالله أوهايبية، **شرح قانون الإجراءات الجزائية الجزائري**، الجزء الأول، الطبعة الثانية 2018، دار هومة، الجزائر، ص 577.

[2]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، أطروحة الدكتوراه علوم في القانون العام، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1 (بن يوسف بن خدة)، 2020/2019، ص- ص 251- 252.

[3]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 316.

[4]- مولاي ملياني دلال، **إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري**، أطروحة الدكتوراه في القانون الخاص، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد- تلمسان، 2017-2018، ص- ص 139-140.

ب- فئات الشاهد المعلوماتي:

فإذا كانت الشهادة تقبل وفقًا للشروط المنصوص عليها في قانون الإجراءات الجزائية من طرف أي شخص بغض النظر عن مستواه العلمي أو الإجتماعي فهي ليست كذلك في الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، يرجع ذلك إلى إختلاف مسرح الجريمة الرقمي والدليل الناتج عنه الذي ينبغي أن يكون من قبل أشخاص مختصون في تقنيات الإعلام والإتصال، ونظرًا لوجود إختلاف بين الشهادة العادية والشهادة في الجرائم الواقعة على المستند الإلكتروني هذا حتمًا يؤدي إلى إختلاف أصناف الشهود فيها وكذا إختلاف في طرق أدائها.[1]

ب-1- الأشخاص الذين لهم صلة بالمنظومة المعلوماتية:

عرف المشرع الجزائري المنظومة المعلوماتية وفقًا الفقرة (ب) من المادة 02 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر كما يلي: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج معين"، وبهذا التعريف يمكن أن يشمل الأشخاص الذين لهم صلة بالمنظومة المعلوماتية إلى عدة فئات من أهمها:

ب-1-1- القائم على تشغيل المنظومة المعلوماتية:

الشخص المسؤول عن تشغيل المنظومة المعلوماتية والأجهزة والملحقات والأدوات المرتبطة بها، ويجب أن يكون على دراية تامة ويتمتع بخبرة واسعة في إستخدامهما[2]، وهو يقوم على نقل المعطيات من الوثائق إلى وسائط التخزين التي تتم معالجتها بواسطة المنظومة المعلوماتية[3]، وأن تكون لديه معلومات عن قواعد تطوير البرامج[4].

ب-1-2- المبرمج:

وهم الشخص المتخصص في كتابة أوامر البرامج، وينقسم إلى فئتين:

الفئة الأولى: مخطط برامج التطبيقات

يقوم مخطط برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ومن ثم تحويلها إلى برامج دقيقة وموثقة تحقق جميع هذه المواصفات.[5]

---

[1]- مولاي ملياني دلال، مرجع سابق، ص 137.
[2]- نفس المرجع، ص139.
[3]- حبيباتني بثينة، مرجع سابق، ص 350.
[4]- سحر سعد عبد السميع محمد، مرجع سابق، ص317.
[5]- مولاي ملياني دلال، مرجع سابق، ص 139.

الفئة الثانية: مخطط برامج النظم

يقوم مخطط برامج النظم بإختبار وتصحيح وتعديل برامج المنظومة المعلوماتية الداخلية، أي أنه يقوم بالوظائف الخاصة بتجهيز النظام بالبرامج والأجزاء الداخلية المسؤولة عن التحكم في وحدات الإدخال والإخراج ووسائط التخزين، بالإضافة إلى إدخال أي إضافات أو تعديلات لهذه البرامج.[1]

ب-1-3- المحلل:

يقوم المحلل بتحليل الخطوات وتتبع المعطيات داخل المنظومة بواسطة ما يسمى بمخطط تدفق البيانات، وإستنتاج الأماكن التي يمكن تحويلها إلى أنظمة آلية بواسطة الجهاز الإلكتروني[2]، ويقوم أيضًا بجمع معطيات نظام الفحص ودراستها ثم تحليل النظام إلى وحدات منفصلة، وإستنتاج العلاقة الوظيفية التي من الممكن أن تجمع بين هذه الوحدات[3].

ب-1-4- مهندس الصيانة والإتصالات:

مهندس الصيانة والإتصالات هو المسؤول عن أعمال الصيانة الخاصة بتقنيات الأجهزة الإلكترونية بمكوناتها والشبكات المتصلة بها.[4]

ب-1-5- مدير النظم:

مدير النظم هو الشخص الذي يوكل له مهمة أعمال الإدارة في المنظومة المعلوماتية.[5]

ب-2- الأشخاص لهم صلة بالإنترنت:

هناك أشخاص آخرون يعدون بمثابة شهود في هذه الجرائم وهم مقدمي الخدمات الوسيطة في مجال تقنية المعلومات والإنترنت، فهم جميعًا يعتبرون شهودًا بحكم لهم دور كبير في توصيل طالب الخدمة إلى شبكة الإنترنت.[6]

ب-3- الشاهد المعلوماتي وفقًا لقانون الدليل الخاص بولاية كاليفورنيا الأمريكية:

يحصر قانون الدليل الخاص بولاية كاليفورنيا الأمريكية شهود الجريمة المعلوماتية في الآتي:

. محلل النظم الذي صمم وحدد برنامج الجهاز الإلكتروني الذي أنتج الدليل؛

. المبرمج الذي قام بتحرير البرنامج وإختباره؛

. المشغل الذي يقوم بتشغيل البرنامج؛

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 127.

[2]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص252.

[3]- مولاي ملياني دلال، مرجع سابق، ص 139.

[4]- حبيباتني بثينة، مرجع سابق، ص 351.

[5]- مولاي ملياني دلال، مرجع سابق، ص 139.

[6]- عثمان محمد الحسن حاج علي، مرجع سابق، ص 139.

. طاقم عمليات المعطيات الذي يعد المعطيات بالصورة التي يستطيع الجهاز الإلكتروني قراءتها؛

. أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة والأسطوانات التي تشتمل على المعطيات والمعلومات المصدرية الصحيحة؛

. مهندس الصيانة الإلكترونية الذي يقوم على صيانة الجهاز الأصلي، والتأكد من عمله بصورة صحيحة؛

. موظفو المدخلات والمخرجات، والمسؤولون عن معالجة المدخلات والمخرجات المستخدم في تنفيذ برامجه؛

. مبرمجو صيانة النظام، والمسؤولون عن سرية عمل الجهاز الإلكتروني في تنفيذ برامجه؛

. المستخدم النهائي الذي يمد بالمعلومات المدخلة، ويصرح بتنفيذ برامج الأجهزة الإلكترونية ويستخدم نواتجها.[1]

ثانيًا: جزاء تخلف الشاهد المعلوماتي عن أداء إلتزاماته في الجرائم الماسة بالمستند الإلكتروني

نظم المشرع الجزائري مجموعة من الإلتزامات التي تقع على عاتق الشاهد الذي له دورًا فعالًا في إثبات الجرائم الماسة بالمستند الإلكتروني، مع إبراز الخصائص التي تميز الشاهد المعلوماتي عن الشاهد العادي أثناء إدلائه بشهادته في هذا النوع من الجرائم، بالإضافة إلى ما يترتب على الإخلال بهذه الإلتزامات.

1- إلتزامات الشاهد في الجرائم الماسة بالمستند الإلكتروني:

من أهم الإلتزامات المفروضة على الشاهد: الإلتزام بالحضور، وأداء اليمين القانونية، والإدلاء بشهادته.

أ- إلتزام الشاهد بالحضور:

يلزم الشاهد الذي تم إستدعاؤه للإدلاء بشهادته بالحضور وأداء اليمين عند الإقتضاء وإدلاء بشهادته حول الجريمة موضوع التحقيق مع مراعاة الأحكام القانونية المتعلقة بالسر المهني بموجب الفقرة الأولى من المادة 172 من ق.إ.ج.ج التي تنص على أن: "كل شخص إستدعى لسماع شهادته ملزم بالحضور وحلف اليمين وأداء الشهادة، مع مراعاة الأحكام القانونية المتعلقة بسير المهنة"، وطبقًا للفقرة الأولى من المادة 236 من نفس القانون في إطار تنفيذ الإنابة القضائية والتي تنص على أن: "يتعين على كل شاهد إستدعى لسماع شهادته أثناء تنفيذ إنابة قضائية الحضور وحلف اليمين والإدلاء بشهادته"، وتكون بصفة رضائية طواعية ويتم إستدعائه طبقًا لأحكام المادة 163 من نفس القانون والتي تنص على أن: "يستدعي قاضي

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص-ص 264-265.

التحقيق أمامه بصفته شاهدًا كل شخص يرى فائدة من سماع شهادته، ويتم إستدعاء الشهود برسالة عادية أو برسالة موصى عليها أو بالطريق الإلكتروني، كما يمكنهم المثول طواعية، كما يمكن قاضي التحقيق إستدعاء الشاهد بواسطة أحد أعوان القوة العمومية وتسلم نسخة من الإستدعاء إلى الشخص المطلوب حضوره".

ويؤدي الشهود أقوالهم أمام قاضي التحقيق سريًا وعلى إنفراد بموجب أحكام نص المادة 165 من نفس القانون التي تنص على أن: "يؤدي الشهود شهادتهم فرادى أمام قاضي التحقيق ويعاونه أمين ضبط دون حضور المتهم، ويحرر محضرا بأقوالهم".

وإذا تعذر على الشاهد الحضور إنتقل إليه قاضي التحقيق برفقة أمين الضبط وبعد إخطار وكيل الجمهورية، لسماع شهادته أو إتخذ لهذا الغرض طريق الإنابة القضائية، وإذا تحقق قاضي التحقيق أن الشاهد قد إدعى كذبًا بعدم إستطاعته الحضور جاز له أن يتخذ ضده الاجراءات القانونية طبقًا لأحكام المادة 172 من نفس القانون.[1]

ويجوز للمحكمة أن تستدعي الشاهد للحضور في الجلسة المحددة للإدلاء بشهادته بموجب المادة 359 من نفس القانون التي تنص على أن: "كل شخص مكلف بالحضور أمام المحكمة لسماع أقواله كشاهد ملزم بالحضور وحلف اليمين وأداء الشهادة"، ويكون التكليف بالحضور تبعًا لما هو منصوص عليه في المادة 609 وما يليها من نفس القانون.

ولقد أجاز القانون رقم: 15-03 المتعلق بعصرنة العدالة السالف الذكر إذا إستدعى بعد المسافة أو تطلب ذلك حسن سير العدالة، بإستجواب وسماع الأطراف عن طريق المحادثة المرئية عن بعد وفقًا للأحكام المنصوص عليها في نفس القانون، ومع مراعاة إحترام الحقوق والقواعد المنصوص عليها في قانون الإجراءات الجزائية السابق التطرق لها.[2]

إذ مكن المشرع الجزائري قاضي التحقيق من إستعمال تقنية المحادثة المرئية عن بعد عند إستجواب المتهم أو سماع الشاهد والخبراء والأطراف المدنية وفي إجراء المواجهة بينهما، ولم يغفل إستفادة جهات الحكم من إستغلال هذه التقنية في سماع الشهود والأطراف المدنية والخبراء، ويمكن لها أيضًا من خلال نظرها في قضايا الجنح أن تلجأ إلى نفس الآلية لتلقي تصريحات متهم محبوس لكنه قيدها بشرطين هما موافقة المتهم المحبوس وموافقة النيابة العامة.[3]

ويتم الإستجواب أو السماع أو المواجهة بإستعمال آلية المحادثة المرئية عن بعد بمقر المحكمة الأقرب من مكان إقامة الشخص المطلوب تلقي تصريحاته بحضور وكيل الجمهورية المختص إقليميًا وأمين الضبط، ويتحقق وكيل الجمهورية من هوية الشخص الذي يتم سماعه

[1]- المادة 174 من القانون رقم: 25-14 السالف الذكر.
[2]- المادة 1/14 من القانون رقم: 15-03 السالف الذكر، الملغاة.
[3]- المادة 15 من القانون رقم: 15-03 السالف الذكر، الملغاة.

ويحرر محضرًا عن ذلك، وإذا كان الشخص المسموع محبوسًا تتم المحادثة المرئية عن بعد من المؤسسة العقابية التي يوجد فيها المحبوس وفقًا للكيفيات المحددة في الفقرة السابقة.[1]

ويجب أن تضمن الوسيلة المستعملة سرية الإرسال وأمانته، ويجب أن يتم تسجيل التصريحات على دعامة تضمن سلامتها وترفق بملف الإجراءات، وتدون التصريحات كاملة وحرفيًا على محضر يوقع من طرف القاضي المكلف بالملف وأمين الضبط.[2]

وبالموازاة مع ذلك وقصد مواجهة الظروف الإستثنائية التي فرضها تفشي وباء كوفيد-19 صدر الأمر رقم: 20-04 المعدل والمتمم للأمر رقم: 66-155 والمتضمن قانون الإجراءات الجزائية السالف الذكر، وألغى جميع الأحكام المخالفة للأحكام الواردة بخصوص إستعمال المحادثة المرئية عن بعد في مرحلة المحاكمة بموجب المادة 441 مكرر11، ومكن الجهات القضائية لمقتضيات حسن سير العدالة أو الحفاظ على الأمن أو الصحة العمومية أو أثناء الكوارث الطبيعية أو لدواعي إحترام مبدأ الآجال المعقولة، إستعمال تقنية المحادثة المرئية عن بعد في الإجراءات القضائية مع إحترام الحقوق والقواعد المنصوص عليها في قانون الإجراءات الجزائية[3].

وتم إلغاء الأمر رقم: 20-04 المعدل والمتمم للأمر رقم: 66-155 والمتضمن قانون الإجراءات الجزائية السالف الذكر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، غير أن هذا الأخير أعاد تنظيم الأحكام المتعلقة بإستعمال وسائل الإتصال المسموعة والمرئية أثناء الإجراءات بإدراجها ضمن الكتاب الخامس ضمن المواد من 639 إلى 650.

ومكن جهات التحقيق -قاضي التحقيق وغرفة الإتهام وجهة الحكم- أن تستعمل المحادثة المرئية عن بعد من أجل إستجواب أو سماع شخص، أو في إجراء المواجهة بين الأشخاص، وفي التبليغات التي يستوجب قانون الإجراءات الجزائية تحرير محاضر بشأنها، مع إلزام التقيد بسرية التحقيق.[4]

وبإمكان لجهات الحكم أن تلجأ لإستعمال المحادثة المرئية عن بعد من تلقاء نفسها أو بناء على طلب النيابة العامة أو أحد الخصوم أو دفاعهم في إستجواب أو سماع شخص أو في إجراء المواجهة بين الأشخاص[5]، وتجدر الإشارة إلى أن هذه الإمكانية قد أعيد تنظيمها وتوسيع نطاقها لأول مرة بموجب الأمر رقم: 66-155 والمتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم: 20-04 السالف الذكر في المادة 441 مكرر7 منه، وهذا بعدما كان الأمر يقتصر

[1]- المادة 16 من القانون رقم: 15-03 السالف الذكر، الملغاة.
[2]- المادة 14 من القانون رقم: 15-03 السالف الذكر، الملغاة.
[3]- المادة 441 مكرر من الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم: 20-04 السالف الذكر، الملغاة.
[4]- المادة 641 من القانون رقم: 25-14 السالف الذكر.
[5]- المادة 646 من القانون رقم: 25-14 السالف الذكر.

فقط على قضايا الجنح وبعد موافقة المعني والنيابة العامة في ظل المادة 15 من القانون رقم: 15-03 المتعلق بعصرنة العدالة السالف الذكر.

كما تم إلغاء شرط الموافقة المسبقة للمتهم للسماح بمحاكمته عن بعد بموجب المادة 441 مكرر8 من الأمر رقم: 66-155 والمتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم: 20-04 السالف الذكر، وهو الشرط الذي كانت تنص عليه المادة 14 من القانون رقم: 15-03 المتعلق بعصرنة العدالة السالف الذكر.

بحيث أصبحت جهة الحكم وحدها صاحبة السلطة التقديرية في تقرير إستعمال هذه الآلية لسير إجراءات المحاكمة أو التحقيق، وإذا رأت جهة الحكم اللجوء إلى إستعمال تقنية المحادثة المرئية عن بعد من تلقاء نفسها فإنها تستطلع رأي النيابة العامة وتحيط باقي الخصوم علمًا بذلك، فإذا إعترضت النيابة العامة أو قدم أحد الخصوم أو محاميه أو المتهم أو محاميه دفوعًا لتبرير رفضه الإمتثال لهذا الإجراء ورأت جهة الحكم عدم جدية هذا الإعتراض أو هذه الدفوع فإنها تصدر قرارًا غير قابل لأي طعن بإستمرار المحاكمة وفق هذا الإجراء.[1]

تجري المحاكمة أو التحقيق القضائي بإستعمال هذه التقنية الحديثة بمقر المحكمة الأقرب من مكان إقامة الشخص المطلوب تلقي تصريحاته، وبحضور أمين الضبط وبعد تحقق وكيل الجمهورية المختص إقليميًا من هويته.[2]

يحرر أمين الضبط محضرًا عن سير عملية إستعمال المحادثة المرئية عن بعد، ويوقعه ثم يرسله بمعرفة وكيل الجمهورية إلى الجهة القضائية المختصة لإلحاقه بملف الإجراءات.[3]

يحرر أمين ضبط المؤسسة العقابية محضرًا عن سير عملية إستعمال هذه التقنية ويوقعه، ثم يرسله بمعرفة رئيس المؤسسة العقابية إلى الجهة القضائية المختصة لإلحاقه بملف الإجراءات.[4]

إذا طلب أحد الأطراف أو محاميه من الجهة القضائية إستخدام تقنية المحادثة المرئية عن بعد تبت هذه الجهة في الطلب بالقبول أو بالرفض بعد إستطلاع رأي باقي الأطراف أو محاميهم والنيابة العامة، غير أنه يجوز لها مراجعة قرارها إذا ظهرت ظروف جديدة بعد تقديم الطلب.[5]

ب- الإلتزام بأداء اليمين القانونية:

يتعين أداء اليمين قبل الإدلاء بالشهادة مما يجعل الشاهد حريصًا على قول الحق، والتكييف القانوني لليمين هو أنه يمثل ضمانة تضفي الثقة على الشهادة التي يتعين أن تتوافر لكي تكون

[1]- المادة 1/647 من القانون رقم: 25-14 السالف الذكر.
[2]- المادة 1/640 من القانون رقم: 25-14 السالف الذكر.
[3]- المادة 2/640 من القانون رقم: 25-14 السالف الذكر.
[4]- المادة 2/647 من القانون رقم: 25-14 السالف الذكر.
[5]- المادة 648 من القانون رقم: 25-14 السالف الذكر.

دليلًا يعتمد عليه القاضي في تكوين إقتناعه[1]، وفي هذا الصدد نصت الفقرة الأولى من المادة 172 من ق.إ.ج.ج على أن: "كل شخص استدعي لسماع شهادته ملزم بالحضور وحلف اليمين وأداء الشهادة، مع مراعاة الأحكام القانونية المتعلقة بسر المهنة"، ونصت المادة 359 من نفس القانون على أن: كل شخص مكلف بالحضور أمام المحكمة لسماع أقواله كشاهد، ملزم بالحضور وحلف اليمين وأداء الشهادة".

ونصت المادة 364 من نفس القانون على أن يؤدي الشاهد اليمين القانونية قبل أداء شهادته حسب الصيغة القانونية المنصوص عليها في المادة 168 من نفس القانون بحيث يؤديها ويده اليمنى مرفوعة اليمين بالصيغة الأتية: "أقسم بالله العظيم أن أتكلم بغير حقد ولا خوف وأن أقول كل الحق ولا شيء غير الحق".

وذلك بخلاف المشرع المصري فلم يبين صيغة اليمين ولكن إكتفى بأن الشاهد "يشهد بالحق ولا يقول إلا الحق" وهو ما يتضح من خلال المادة 283 من ق.إ.ج.م التي تنص على أن: "يجب على الشهود الذين بلغت سنهم أربع عشرة (14) سنة أن يحلفوا يمينًا قبل أداء الشهادة، على أنهم يشهدون بالحق ولا يقولون إلا الحق"، أما بالنسبة للمشرع الفرنسي فإن صيغة اليمين حتمية وجزاء مخالفتها البطلان وتختلف بإختلاف المحاكم، فهي أمام محكمة الجنايات كالتالي: "أتكلم بدون حقد وبدون خوف وأقول كل الحق ولا شيء غير الحق" طبقًا للفقرة 03 من المادة 331 من ق.إ.ج.ف[2]، وقد إستقرت المحاكم الفرنسية بالحكم ببطلان الشهادة إذا حلف الشاهد بأن "يقول الحق" بدلًا من "كل الحق" لأنه قد يتكتم على جزء من الحقيقة، أو إذا حلف بأن يقول "كل الحق" بدلًا من "لا شيء غير الحق" لأنه قد يصرح بالحقيقة ويضيف إليها شيء غير صحيح[3].

والصيغة أمام محاكم الجنح والمخالفات وقضاة التحقيق طبقًا للمواد 103 و446 من ذات القانون كالآتي: "إن الشاهد يقول كل الحق ولا شيء غير الحق".[4]

والملاحظ أنه الإدلاء بالشهادة دون حلف اليمين ممن لا يلزمه القانون بأدائها جائز فحددت المادة 365 من ق.إ.ج.ج على سبيل الحصر الأشخاص المعفيين من أداء اليمين القانونية، فتسمع شهادة القصر الذين لم يكملوا السادسة عشرة (16) من العمر بغير حلف اليمين، وكذلك الشأن بالنسبة للأشخاص المحكوم عليهم بالحرمان من الحقوق الوطنية، ويعفى كذلك من حلف اليمين أصول الأطراف وفروعهم وأزواجهم وإخوتهم وأخواتهم وأصهارهم على درجتهم من

[1]- بوكر رشيدة، مرجع سابق، ص 368.

[2]-Art 331 paragraphe 03 du C.P.P.F (Ordonnance n°58-1296 du 23 décembre 1958) dispose que: «Avant de commencer leur déposition, les témoins prêtent le serment " de parler sans haine et sans crainte, de dire toute la vérité, rien que la vérité"».

[3]- بن طالب ليندا، مرجع سابق، ص 72.

[4]-Art 103 du C.P.P.F (Loi n°2000-516 du 15 juin 2000 - art. 31 JORF 16 juin 2000 en vigueur le 1er janvier 2001) dispose que: « Les témoins prêtent serment de dire toute la vérité, rien que la vérité». Et Art 446 du C.P.P (Loi 93-1013 1993-08-24 art. 28 JORF 25 août 1993 en vigueur le 2 septembre 1993) dispose que: « Avant de commencer leur déposition, les témoins prêtent le serment de dire toute la vérité, rien que la vérité»

عمود النسب، غير أن الأشخاص المشار إليهم يجوز أن يسمعوا بعد حلف اليمين إذا لم تعارض في ذلك النيابة العامة أو أحد أطراف الدعوى، وتنص المادة 366 من نفس القانون على أن: " إن أداء اليمين من شخص غير أهل للحلف أو محروم أو معفى منها لا يعد سببًا للبطلان".

ج- الإلتزام بالإدلاء بالشهادة:

يعد الإلتزام بالإدلاء بالشهادة من أهم الإلتزامات المفروضة على الشاهد فهو جوهر مهمته، ينطوي هذا الإلتزام على واجبين إثنين يتحملهما الشاهد، الإلتزام بالتكلم وواجب قول الحقيقة:

الواجب الأول: كل شخص إستدعى لسماع شهادته ملزم بإدلاء بشهادته بعد حلفه لليمين، مع مراعاة الأحكام القانونية المتعلقة بالسر المهني كالأطباء والمحامين وغيرهم ممن لهم مبرر قانوني لذلك.[1]

وقبل إدلاء الشاهد بشهادته يطلب منه ذكر إسمه ولقبه وعمره وحالته ومهنته وسكنه، وتقرير ما إذا كانت تربطه صلة نسب أو قرابة مع الخصوم أو ملحق بخدمتهم أو كان فاقدًا للأهلية، فينوه عن هذه الأسئلة والأجوبة في المحضر[2]، والأصل في الشهادة أن يدلي الشاهد بشهادته شفاهة عملًا بحكم المادة 165 من نفس القانون التي تنص على أن: "يؤدي الشهود شهادتهم فرادى أمام قاضي التحقيق ويعاونه أمين الضبط دون حضور المتهم، ويحرر محضرًا بأقوالهم".

ويجوز لقاضي التحقيق أن يستعين بمترجم عند سماع الشاهد شريطة ألا يكون المترجم هو بدوره شاهدًا في القضية أو هو أمين ضبط التحقيق، كما لا يجوز أن يكون المترجم هو أحد أطراف الدعوى وذلك لضمان حياد الترجمة.[3]

إلا أنه يجوز أن تكون الشهادة كتابية إذا تعذر على الشاهد أن يدلى بها شفاهة كالأصم والأبكم فتنص المادة 167 من القانون السالف الذكر على أن: "إذا كان الشاهد أصمًا أو أبكمًا توضع الأسئلة وتكون الإجابات بالكتابة، وإذا لم يكن يعرف الكتابة يندب له قاضي التحقيق من تلقاء نفسه مترجمًا قادرًا على التحدث معه، ويذكر في المحضر إسم المترجم المنتدب ولقبه ومهنته وموطنه وينوه عن حلفه اليمين، ثم يوقع على المحضر".

أما جهة الحكم تقتضي أن يؤدي الشاهد شهادته شفويًا وبالإعتماد أساسًا على ذاكرته حتى ولو كانت شهادته مكتوبة في محضر سماعه أمام قاضي التحقيق، ولا يجوز له أن يتلو شهادة مكتوبة ولا أن تتلى شهادته المدونة في محضر إلا بعد فراغه من الإدلاء بشهادته شفويًا ويكون ذلك من باب الإستجواب والتمحيص فقط، ويسمح له القانون بصفة إستثنائية أن يستعين

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 135.

[2]- المادة 1/168 من القانون رقم: 25-14 السالف الذكر.

[3]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، الطبعة الرابعة، 2018، دار هومة، الجزائر، ص 261.

بمستندات بتصريح من الرئيس إذا كانت هناك بيانات حسابية أو علمية يتعذر أن تحفظها الذاكرة، وليس مطلوبًا منه أن يبدي رأيه في الأحداث بل عليه أن يصرح بما يعلم فقط.[1]

الواجب الثاني: فلا يمكن للشاهد أن يساهم في إظهار الحقيقة إلا إذا كانت شهادته نزيهة غير كاذبة، ومن هنا لا يكفي أن يمتثل ويحلف اليمين بل إنه ملتزم بقول الحقيقة.[2]

يجب على الشاهد قبل الإدلاء لشهادته أن يحلف على أن يقول كل الحق وألا ينطق بسواه، فالأصل في الشاهد أن يتحلى بالصدق في أقواله، فالإلتزام بقول الحقيقة تعد من بين أهم الإلتزامات المفروضة على الشاهد الذي يتعين عليه عند الإدلاء بشهادته أن يتأكد من قوله للحقيقة، وذلك لتمكين القاضي الإستناد عليها وأن يبني على أساسها حكمه، وبذلك نجد أن المشرع الجزائري قد رتب المسؤولية الجزائية من خلال تجريمه لشهادة الزور[3] بإعتبارها تعيق حسن السير العدالة وتهدر من مصداقيتها وتبعد القاضي إلى تحقيق الإنصاف والعدل.[4]

وبناءً على ما تقدم، فإن من بين أهم النقاط الجوهرية التي قد تثار فيما يتعلق بالشهادة في الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص قصور أحكام الشهادة في الحصول على الدليل الإلكتروني، الأمر الذي إستلزم البحث عن وسيلة قانونية جديدة تحقق ما لم تستطيع فكرة الإلتزام بأداء الشهادة أن تؤديه، وهذه الوسيلة هي: "الإلتزام بالإعلام في الجريمة المعلوماتية"[5]، والذي يقصد به إلتزام الشاهد

---

[1]- نجيمي جمال، مرجع السابق، ص-ص 464-465.

تنص المادة 370 من القانون رقم: 25-14 السالف الذكر على أن: "يؤدي الشهود شهادتهم شفويًا. غير أنه يجوز لهم بصفة إستثنائية الإستعانة بمستندات بترخيص من الرئيس. ويقوم الرئيس بعد أداء كل شاهد لشهادته بتوجيه ما يراه لازمًا من أسئلة على الشاهد وما يطرحه عليه أطراف الدعوى من الأسئلة إن كان ثمة محل لذلك. وللنيابة العامة حرية توجيه ما تراه من الأسئلة مباشرة إلى المتهمين وإلى الشهود والى الضحايا والأطراف المدنية. ويجوز لدفاع كل من المتهم أو الضحية أو الطرف المدني توجيه الأسئلة مباشرة إلى كل شخص يتم سماعه في الجلسة، بعد إذن الرئيس وتحت رقابته والذي له أن يأمر بعدم الإجابة عن السؤال. ويجوز للشاهد أن ينسحب من قاعة الجلسة بعد أداء شهادته مالم يقرر الرئيس غير ذلك. ويجوز للنيابة العامة وكذلك للضحية وللمدعي المدني وللمتهم أن يطلبوا إنسحاب الشاهد موقتًا من قاعة الجلسة بعد أداء شهادته، لكي يتسنى إعادة إدخاله إليها وسماعه من جديد إذا كان ثمة محل لذلك، مع إجراء مواجهات بين الشهود أو عدم إجرائها، وللرئيس من تلقاء نفسه أن يأمر بهذا الإجراء".

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 136.

[3]- تنص المادة 374 من القانون رقم: 25-14 السالف الذكر على أن: "إذا تبين من المناقشات شهادة الزور في أقوال الشاهد فللرئيس أن يأمر إما من تلقاء نفسه أو بناء على طلب النيابة العامة أو أحد الأطراف، هذا الشاهد على وجه الخصوص بأن يلزم مكانه ويحضر المناقشات، وأن لا يبرح مكانه لحين النطق بالحكم، وفي حالة مخالفة هذا الأمر يأمر الرئيس بالقبض على هذا الشاهد. ويوجه الرئيس قبل النطق بإقفال باب المناقشة إلى من يظن فيه شهادة الزور دعوة أخيرة ليقول الحق، ويحذره بعد ذلك من أن أقواله سيعتد بها منذ الآن من أجل تطبيق العقوبات المقررة لشهادة الزورعند الإقتضاء. ويكلف الرئيس أمين ضبط الجلسة بتحرير محضر بالإضافات والتبديلات والمفارقات التي قد توجد بين شهادة الشاهد وأقواله السابقة. وبعد صدور الحكم في موضوع الدعوى أو في حالة تأجيل القضية يأمر الرئيس بأن يقتاد الشاهد بواسطة القوة العمومية بغير تمهل إلى وكيل الجمهورية الذي يطلب إفتتاح التحقيق معه. ويرسل أمين الضبط إلى وكيل الجمهورية نسخة من المحضر الذي حرره تطبيقًا للفقرة الثالثة من هذه المادة".

[4]- علوي سالم، **أدلة الإثبات في التحقيق الجنائي**، رسالة الماجستير، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر01- بن يوسف بن خدة، 2016-2017، ص 56.

[5]- عائشة بن قارة مصطفى، مرجع سابق، ص137.

المعلوماتي الحائز على المعلومات الجوهرية اللازمة المتصلة بالمنظومة المعلوماتية، بأن يعلم بها السلطات القضائية المختصة لمقتضيات التحريات والتحقيقات القضائية، التي تقتضي مصلحة هذه الأخيرة في الحصول على تلك المعلومات الجوهرية.

وعليه فإن إلتزام الشاهد بالإعلام فى الجرائم الماسة بالمستند الإلكتروني يقتضي منه تقديم إلى جهة التحري أوالتحقيق أوالمحاكمة ما يحوزه من معلومات الجوهرية والضرورية للولوج إلى المنظومة المعلوماتية تنقيبًا عن أدلة الجريمة داخلها، كما يجب أن يراعي الشاهد المعلوماتي في شهادته أن تكون بسيطة ومفهومة، محددة، ودقيقة[1]، ولا ينشأ إلتزام الشاهد بالإعلام في الجرائم الماسة بالمستند الإلكتروني إلا إذا توافرت ثلاثة شروط أساسية تتمثل فيما يلي:

الشرط الأول: لكي يلتزم الشاهد المعلوماتي بواجب الإعلام في أي جريمة من الجرائم الماسة بالمستند الإلكتروني لابد أن تكون هذه الجريمة قد إرتكبت بالفعل، ولا يصح هذا الإلتزام لضبط جريمة مستقبلية حتى لو دلت التحريات والتحقيقات الجدية تثبت أن الجريمة على أنها ستقع بالفعل، كما أنه لا يكفي مجرد وقوع جريمة من الجرائم الماسة بالمستند الإلكتروني لقيام هذا الإلتزام بل لابد أن تكون من بين الجرائم التي يعتبرها القانون جناية أو جنحة.[2]

الشرط الثاني: أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات الجوهرية المتصلة بالمنظومة المعلوماتية محل الواقعة، ويتمثل مضمون هذه المعلومات الجوهرية في ثلاث عناصر متمثلة في:

1- طبع ملفات المعطيات المخزنة في ذاكرة الجهاز الإلكتروني أو وسائط تخزين المعطيات الثانوية، ويعلم بها سلطات التحري والتحقيق؛

2- الإفصاح عن كلمة المرور السرية للسلطات التحري والتحقيق؛

3- الكشف عن الشفرات المسجلة بها الأوامر الخاصة بتنفيد البرامج المختلفة، حيث أن الرسائل المكتوبة بالشفرة أو الأوامر تحتاج لفهمها إلى ترجمة لحل هذه الشفرة.[3]

الشرط الثالث: فلا يكفي لإلتزام الشاهد المعلوماتي بالإعلام فى الجرائم الماسة بالمستند الإلكتروني أن نكون بصدد جريمة قد وقعت بالفعل، وأنها تعد جنحة أو جناية، وأن يكون الشاهد على علم ومعرفة بالمعلومات الجوهرية المتصلة بالمنظومة المعلوماتية محل الواقعة، بل ينبغي إلى جانب ذلك أن تقتضي مصلحة التحقيق الحصول على تلك المعلومات الجوهرية، وخاصة إذا كان الأمر يتطلب لإختراق المنظومة لأجل البحث عن أدلة جنائية الموجودة بداخلها والتي تفيد فى كشف الجريمة.[4]

---

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص-ص 321-322.

[2]- نفس المرجع، ص322.

[3]- بوكر رشيدة، مرجع سابق، ص-ص 370-371.

[4]- سحر سعد عبد السميع محمد، مرجع سابق، ص323.

ومن أجل الحصول على هذه المعلومات الضرورية لحسن سير إجراءات التحقيق والوصول إلى كشف الحقيقة وإدانة فاعليها، يجيز القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر في الفقرة الأخيرة من المادة 05 منه للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكافة المعلومات الضرورية لإنجاح هذه المهمة.

وقد تلجأ بعض الدول إلى إستخدام وسائل الضغط على الشهود من أجل حملهم على التعاون الإيجابي مع سلطات التحري والتحقيق، حيث يسأل الشاهد الذي أخفى كلمة السر أو الشفرة أو الذي أعطى أوامر خاطئة بجريمة شهادة الزور لأنه يعوق حسن سير العدالة، أو يسأل جزائيًا بإعتباره شريكًا في الجريمة موضوع المحاكمة.[1]

ومما سبق ذكره، فإذا كان يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحري والتحقيق ما يحوزه من معلومات جوهرية وهامة اللازمة للولوج إلى المنظومة المعلوماتية بحثًا عن أدلة محل الجريمة بداخله، فالتساؤل الذي يثار في هذا الصدد هو مدى جواز إجبار الشاهد المعلوماتي على الإفصاح بالرقم السري الخاص بالدخول إلى المنظومة المراد تفتيشها والعائدة له، أو الكشف عن الشفرات المدون بها الأوامر الخاصة بتنفيذ البرامج أو طبع ملفات معطيات المختزنة قصد التعاون مع سلطات التحقيق؟

وللإجابة على التساؤل المطروح أهمية بالغة، حيث إن الخبير المنتدب من الجهة القضائية قد لا يكون قادرًا على معرفة الأساليب الفنية التي يمكن إتباعها للكشف عن أدلة تفيد في كشف الحقيقة، وقد لا يعلمها إلا هذا الشاهد مثل كلمة المرور والبرامج المستخدمة التي إستعان بها المتهم في إرتكاب الجرائم الواقعة على المستند الإلكتروني[2]، وقد ذهب الفقه في الإجابة على هذا التساؤل إلى إتجاهين رئيسيين:

الإتجاه الأول: يرى أنصار هذا الإتجاه أنه لا يجوز إكراه الشاهد وفقًا للقواعد العامة في أداء الشهادة، بأن يقوم بطباعة ملفات المعطيات المخزنة في المنظومة المعلوماتية أو إلزامه بالإفصاح عن كلمات المرور السرية أو الكشف عن الشفرات الخاصة بالبرامج المختلفة، ففي إتفاقية تريس تنص المادة 39 من القسم السابع على أن المعطيات المحتفظ بها لدى الغير والمقدمة لجهات حكومية تتمتع بالسرية ولا يحق لأي شخص طبيعي أو معنوي أن يفصح عن محتوى تلك المعطيات، ومن ثم فإن لهم الحق بموجب تلك المادة في الإمتناع عن الإدلاء بالشهادة بشأن معطيات المستند الإلكتروني حتى ولو كانت محلًا للإعتداء.[3]

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 137.

[2]- نفس المرجع، ص 129.

[3]- سحر سعد عبد السميع محمد، مرجع سابق، ص320.

وفي ألمانيا يذهب أغلبية الفقه الجنائي الألماني إلى عدم إلتزام الشاهد بطبع المعطيات المخزنة في ذاكرة الجهاز الإلكتروني على أساس أن الإلتزام بأداء الشهادة لا يتضمن هذا الواجب، كما هو مقرر في تركيا فلا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات الخاصة بتشغيل البرامج المختلفة.[1]

ويوجد بعض الفئات في فرنسا ممنوعة بنص القانون من الإفصاح عن بعض المعطيات التي تكون بحوزتها مثل المحامين والأطباء متى تعلقت بأسرار مهنتهم، ومن ثم فمتى كان تحت يد أيا من هؤلاء مستندًا يحمل توقيعًا مزورًا متعلقًا بسر من أسرار مهنته أو كان محلًا للتلاعب فلا يجوز إلزامه بتقديمه أو الشهادة بشأنه.[2]

الإتجاه الثاني: على عكس الإتجاه الأول يرى أنصار هذا الإتجاه أن من بين الإلتزامات التي تقع على عاتق الشاهد المعلوماتي القيام بطباعة ملفات المعطيات المخزنة داخل الجهاز الإلكتروني، أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة[3]، وهذا الإتجاه يؤكد ضرورة الإلتزام بالإعلام ويحتجون بالأسباب التالية:

- العمل على إدراج هذا المبدأ ضمن المواد القانونية المنظمة لهذا الشأن، وذلك حتى يسهل على رجال التحري والتحقيق من أداء مهامهم، وفي نفس الوقت حماية للشاهد من خرق سر المهنة؛
- الإلتزام بالإعلام مبدأ وقائي[4]، بحيث يرى البعض من أنصار هذا الإتجاه أن الإلتزام بالإعلام يشكل وقاية، ويحول دون ضبط الجهاز بأكمله أو الأجهزة الممتدة التابعة له في التفتيش والمعاينة.[5]

ومن التشريعات التي تفرض واجب التعاون على الشاهد في مجال الجريمة المعلوماتية القانون الإنجليزي الصادر سنة 1984 بشأن البوليس والأدلة الجنائية، حيث يعطي للمحققين الحق في أن يطلبوا من الغير تمكينهم من الدخول إلى المعلومات المخزنة في الجهاز الإلكتروني أو الإطلاع عليها أو قراءتها.[6]

وفي هولندا يتيح مشروع قانون الحاسب الآلي طبقًا للمادة 125-k لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل المنظومة المعلوماتية بتقديم المعلومات اللازمة لإختراقها والولوج إلى داخلها كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج

---

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص320.

[2]- نفس المرجع، ص-ص 320-321.

[3]- علي عدنان الفيل، مرجع سابق، ص-ص 64-65.

[4]- بمعنى أن المعطيات والمعلومات المجرمة يمكن أن تكون مخزنة في وحدة معالجة مركزية في الجهاز الإلكتروني ضمن شبكة معلومات ممتدة، هنا يلعب الدور الوقائي للشهادة المعلوماتية دوره في بيان مكان تلك المعطيات التي تثير الريبة والشكوك وعدم التحفظ على المنظومة المعلوماتية بأكملها، وللمزيد من التفصيل، ينظر: حبيباتني بثينة، مرجع سابق، ص- ص 357-358.

[5]- التوجي محمد، مرجع سابق، ص 180.

[6]- عائشة بن قارة مصطفى، مرجع سابق، ص 130.

المختلفة، وإذا وجدت معطيات مشفرة داخل ذاكرة الجهاز الإلكتروني وكانت مصلحة التحقيق تستلزم الحصول عليها يتم تكليف القائم على تشغيل المنظومة المعلوماتية بحل رموز هذه المعطيات، وفي اليونان طبقًا للفقرة الأولى من المادة 223 من قانون الإجراءات الجنائية اليوناني فإنه يمكن الحصول من القائم على تشغيل المنظومة المعلوماتية على كلمة المرور السرية للولوج في المنظومة، كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني، لكن ليس على الشاهد أي إلتزامات بالنسبة لطباعة ملفات معطيات مخزنة في ذاكرة الجهاز الإلكتروني وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل وليس الكشف عن معلومات جديدة.[1]

ويؤيد إتجاه من الفقه الجنائي الفرنسي هذا الإتجاه ويبررون موقفهم على أساس أن المشرع الفرنسي طالما أنه لم ينظم هذه المسألة فلا مناص من تطبيق القواعد العامة في الشهادة، ومن ثم فإن الشهود الذين يقع عليهم إلتزام قانوني بالإلتزام بأداء الشهادة يكونون مكلفين بالإفصاح عن كلمات المرور السرية التي يعرفوها أو شفرات تشغيل البرامج، بإستثناء حالات المحافظة على سر المهنة فإنهم لا يعفيهم من هذا الإلتزام إلا التمسك بإحترام السر المهني.[2]

وقد تجاوزت المادة 18 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 ذلك المدى عندما ألزمت الغير ليس فقط بتقديم ما عساه يكون تحت يده، وإنما أيضًا بالتحفظ والإفصاح عن معطيات المستندات الإلكترونية التي يعتقد أنها محلًا للتلاعب أو المحو والتي من شأنها الكشف عن الجريمة وتحديد هوية مرتكبيها[3]، والذي ينص البند (أ) من الفقرة الأولى من نفس المادة على أن: "يجب على كل طرف أن يتبنى الإجراءات التشريعية والإجراءات التي يرى أنها ضرورية من أجل تأهيل سلطاته المختصة أن تأمر:

أ- شخصًا ما على أرضه بإرسال بيانات معلوماتية معينة في حوزة أو تحت سيطرة هذا الشخص، والمخزنة في نظام معلوماتي أو في دعامة تخزين معلوماتية".[4]

وعلى ذلك نرى أنه وفقًا للقواعد السابقة الذكر أن الشاهد لا يلتزم إلا بذكر ما يعلمه عن الجريمة ولا يجوز إجباره على القيام بعمل معين، ونلاحظ أن المادة 284 من ق.إ.ج.م تنص على أن: "إذا إمتنع الشاهد عن أداء اليمين أو الإجابة في غير الأحوال التي يجيز له القانون فيها ذلك، حكم عليه..."، ومعنى ذلك أن الشاهد يلتزم بالإجابة عن أسئلة توجهها المحكمة له وليس للمحكمة أن تلزمه بالقيام بعمل معين، وفي ذلك تقول محكمة النقض المصرية أن الشهادة هي

[1]- علي عدنان الفيل، مرجع سابق، ص65.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 131.

[3]- سحر سعد عبد السميع محمد، مرجع سابق، ص 259.

[4]-Art 18 paragraphe 01 du convention sur la cybercriminalité dispose que : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession oú sous le contrôle de cette personne, et stockées dans un systéme informatique où un support de stockage informatique».

تقرير شخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه، وبالمثل فإن المادة 331 من ق.إ.ج.ف تحدد واجبات الشاهد في الشهادة بخصوص الوقائع المسندة إلى المتهم أو بخصوص شخصية هذا الأخير أو أخلاقياته، لذلك ليس من واجب الشاهد في جريمة تمس بالمستند الإلكتروني طبع ملفات المعطيات المخزنة في ذاكرة الجهاز الإلكتروني أو الإفصاح عن كلمات المرور السرية أو الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج، إذ أن هذا الإلتزام يزيد عن نطاق الشهادة لذلك ينبغي أن يكون هناك تدخل تشريعي عن طريق وضع نصوص قانونية خاصة لكي تفرض على الشاهد واجب التعاون مع الجهة القضائية في أثناء التحقيقات والمحاكمة.[1]

2- جزاء تخلف الشاهد المعلوماتي عن إلتزاماته:

في حالة إمتناع الشاهد عن الحضور فبموجب الفقرة الأولى من المادة 164 من ق.إ.ج.ج تجيز لقاضي التحقيق بناء على طلب وكيل الجمهورية إحضاره عن طريق القوة العمومية جبرًا ويعاقب وفقًا للأحكام المنصوص عليها في المادة 172 من نفس القانون والتي تنص على أن: "يتعين على كل شخص استدعي بواسطة أحد أعوان القوة العمومية لسماع شهادته، أن يحضر ويؤدي اليمين عند الإقتضاء ويدلي بشهادته، وإلا عوقب بمقتضى نص المادة 172"، وهي الصلاحية المخولة له بموجب الفقرة 02 من المادة 69 من ذات القانون التي تنص على أن: " وفي سبيل مباشرة مهام وظيفته أن يستعين مباشرة بالقوة العمومية"، وفي إطار تنفيذ الإنابة القضائية جاء نفس الحكم وفقًا للفقرة 02 من المادة 236 من نفس القانون التي تنص على أن: "فإذا تخلف عن القيام بهذه الواجبات أخطر القاضي المنيب الذي يسوغ له أن يجبر الشاهد على الحضور بواسطة القوة العمومية، وأن يطبق في حقه العقوبات المنصوص عليها في الفقرة 02 من المادة 172 من هذا القانون".

وبالرجوع إلى الفقرة 02 من أحكام المادة 172 من نفس القانون نجد أنها تنص على توقيع عقوبة على الشاهد الذي ثبت أن تم إستدعاءه بواسطة القوة العمومية وتخلف عن الحضور بالغرامة تقدر من عشرة ألاف 10.000 دج إلى عشرون ألفًا 20.000 دج والتي تنص على أن: "وإذا لم يحضر الشاهد فيجوز لقاضي التحقيق بناء على طلب وكيل الجمهورية إستحضاره جبرًا بواسطة القوة العمومية والحكم عليه بغرامة من 10.000 دج الى 20.000 دج".

وتنص نفس الفقرة على أن إذا حضر الشاهد فيما بعد وأبدى أعذارًا محقة ومدعمة بما يؤيد صحتها تبرر تخلفه عن الحضور، جاز لقاضي التحقيق بعد سماع طلبات وكيل الجمهورية أن يعفيه من الغرامة كلها أو جزء منها.

ويجوز توقيع غرامة مالية على الشاهد الذي يمتنع عن أداء اليمين أو الإدلاء بشهادته رغم حضوره بالغرامة من عشرة ألاف 10.000 دج إلى عشرون ألفًا 20.000 دج وذلك بناء على

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص-ص 136-137.

طلب من وكيل الجمهورية بموجب المادة الفقرة 03 من نفس المادة، أما في حالة إعلان الشاهد بأنه يعرف مرتكبي جناية أو جنحة ومعرفته لمعلومات عن الجريمة موضوع التحقيق أو تفيد في كشف ملابساتها ثم يرفض الإجابة على الأسئلة الموجهة إليه في هذا الشأن بمعرفة قاضي التحقيق، يجوز إحالته على المحكمة المختصة والحكم عليه بالحبس من شهرين (02) إلى سنة (01) وبغرامة من عشرون ألفًا 20.000 إلى مئة ألف 100.000 دج أو بإحدى هاتين العقوبتين طبقًا للمادة 173 من ذات القانون.

أما في حالة التخلف عن الحضور أثناء المحاكمة وكانت الشهادة تنصب على مخالفة أو جنحة فيجوز للجهة القضائية بناء على طلب النيابة العامة عقاب كل شاهد يتخلف عن الحضور أو يمتنع عن حلف اليمين أو أداء الشهادة بالعقوبة المنصوص عليها في المادة 172 السالفة الذكر والمتمثلة في الغرامة من عشرة ألاف 10.000 دج إلى عشرون ألفًا 20.000 دج، كما يجوز من تلقاء نفسها أو بناء على طلب النيابة العامة اللجوء إلى إستعمال القوة العمومية لإحضار الشاهد عند تخلفه عن الحضور بغير عذر تراه مقبولًا ومشروعًا لسماع أقواله أو تأجيل القضية لأقرب جلسة ممكنة، ويتحمل الشاهد المتخلف عن الحضور كل مصاريف التكليف بالحضور والإجراءات والإنتقال وغيرها، ويجوز لهذا الأخير أن يرفع المعارضة أمام نفس الجهة القضائية.[1]

وإذا كان قد تم إستدعاء الشاهد أمام محكمة الجنايات وتخلف عن الحضور بدون عذر مقبول، جاز لمحكمة الجنايات أن تأمر بإستحضار الشاهد المتخلف بواسطة القوة العمومية عند الإقتضاء سواء من تلقاء نفسها أو بناء على طلبات النيابة العامة أو باقي أطراف الدعوى، أو الإكتفاء بتلاوة محضر سماعه أمام قاضي التحقيق[2] أو تأجيل القضية لتاريخ لاحق، وفي هذه الحالة يتعين عليها أن تحكم على الشاهد الذي تخلف عن الحضور أو رفض أن يحلف أو يؤدي شهادته بغرامة من خمسة ألاف 5.000 دج إلى عشرة ألاف 10.000 دج أو بالحبس من عشرة (10) أيام إلى شهرين (02)، ويتحمل الشاهد في هذه الحالة مصاريف الحضور للشهادة والإجراءات والإنتقال وغيرها، مع حقه في رفع معارضة في حكم الإدانة في غضون ثلاثة (03) أيام من تبليغه إلى شخصه، وعلى المحكمة أن تفصل فيها إما في نفس الجلسة التي تمت فيها المرافعات وإما في تاريخ لاحق.[3]

وهذا بخلاف حالة الشاهد الذي لم يسبق إستدعاؤه وسماعه أمام قاضي التحقيق فتطبق بشأنه أحكام الفقرة 03 من المادة 422 من نفس القانون والتي تنص: "وله بصفة خاصة أن يأمر

---

[1]- المادة 360 من القانون رقم: 25-14 السالف الذكر.

[2]- الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم: 17-07 المؤرخ في 27 مارس 2017 الملغى، أضاف إلى النص أن طلب إستحضار الشاهد المتخلف يمكن أن يتقدم به كل أطراف الدعوى، كما يمكن للمحكمة الإكتفاء بتلاوة محضر سماع الشاهد أمام قاضي التحقيق، وهو ما كان يجري به العمل سابقًا دون نص، وإنما بناء على السلطة التقديرية لرئيس المحكمة، وللمزيد من التفصيل، ينظر: نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الثاني، الطبعة الرابعة، 2018، دار الهومة، الجزائر، ص 63.

[3]- المادة 434 من القانون رقم: 25-14 السالف الذكر.

بحضور الشهود الذين لم يسبق إستدعاؤهم ويتبين من خلال المناقشة أن سماعهم ضروري لإظهار الحقيقة، وإذا إقتضى الأمر بإستعمال القوة العمومية لهذا الغرض".

الفرع الثاني: الخبرة التقنية في الجرائم الماسة بالمستند الإلكتروني

قد يقوم القاضي بإتخاذ عدة إجراءات لازمة للكشف عن ملابسات الجريمة وتحديد مرتكبيها، إلا أن قد يواجهه مسائل تقنية يصعب عليه الفصل فيها أو التغلب عليها وحده، لأن يستدعي إلى إمتلاك قدرات خاصة ومهارات قد لا تتوفر فيه، وهو ما يدفعه إلى الإستعانة بخبير أو أكثر لتوضيح مسألة معينة أو أكثر قد تواجهه.[1]

أولًا: مفهوم الخبرة التقنية

سنتناول تعريف الخبرة، ثم نتطرق إلى تعريف الخبير التقني.

1- تعريف الخبرة التقنية:

يقصد بالخبرة بصفة عامة المهارة المكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة، أو نتيجة دراسات خاصة تلقاها، أو نتيجة الإثنين معًا أي العمل والدراسة، ومن هنا يطلق على ذوي هذه المهارات "بالخبراء".[2]

والخبرة القضائية عمومًا هي إبداء رأي فني من شخص مختص فنيًا في شأن واقعة ذات أهمية في الدعوى، فهي وسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالإستعانة بالمعلومات العلمية، وهي في حقيقتها ليست دليلًا مستقلًا عن الدليل القولي أو المادي وإنما هي تقييم فني لهذا الدليل.[3]

وهو ليس حكم قضائي وليس له قيمة أكثر من شهادة الشهود، ولا يمنع القاضي من حقه الكامل في تقدير الوقائع التي تعرض عليه حق قدرها، والمحكمة ليست ملزمة برأي الخبير فيما يتعلق بمعرفة التلازم بين الفعل والنتيجة ونوعية الأدلة المستخدمة، حتى ولو تعلق الأمر بالجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، فللمحكمة أن تختار ما تراه مناسب للأخذ به كما أن لها الحق في تفضيل تقرير على تقرير آخر، ولها أن تبحث في مسألة وتفصل فيها بدون أخذ رأي الفني للخبراء.[4]

وتبرز أهمية الإستعانة بالخبير الفني في إثبات الجرائم الماسة بالمستند الإلكتروني بشكل أكبر عند غيابه، فقد تعجز سلطات التحري والتحقيق في الكشف عن الجريمة وجمع الأدلة بخصوصها لنقص الكفاءة والتخصص اللازمين للتعامل في الجوانب التقنية والفنية التي إرتكبت

[1]- بلحسيني حمزة، مرجع سابق، ص 364.
[2]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 283.
[3]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 315.
[4]- مولاي ملياني دلال، مرجع سابق، ص 162.

بواسطتها الجريمة، وهو ما قد يؤدي إلى محو الدليل أو تدميره عند التعامل معه[1]، نظرًا لأن الأجهزة الإلكترونية وشبكات الإتصال متعددة الأنواع والنماذج، والمجالات العلمية والتقنية المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة، كما أن التطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب معها على المتخصص تتبعها وإستيعابها، وكل هذه الأمور تشكل عقبة أمام المختصين في مجال القانون بحيث لا تمكنهم معرفتهم القانونية وحدها من فك لغز الجريمة[2].

فإنتداب الخبراء ذوي المعرفة بتقنيات المنظومة المعلوماتية ومناقشتهم في كيفية وقوع الجريمة، ومواجهة المتهم بتقرير الخبرة وما ورد فيه قد ينهي التحقيق إما بثبوت واقعة الجريمة من قبل المتهم وإحالته إلى المحكمة المختصة أو بصدور أمر بألا وجه للمتابعة، ويمكن للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم، ولا يرفض طلب الخصوم إلا إذا كان عديم الفائدة لأنه أمر يعود لتقدير القاضي لذا عليه تسبيبه عند الرفض.[3]

ولعل إدراك بعض التشريعات المقارنة لهذه الأهمية جعلها لا تكتفي بالنصوص التقليدية التي تنظم الخبرة الفنية وإنما أسرعت إلى تدعيمها بنصوص قانونية جديدة خاصة بالخبرة في مجال الجرائم المعلوماتية، ونذكر في مقدمتها القانون البلجيكي الصادر في 23 نوفمبر 2000 المتعلق بالإجرام المعلوماتي حيث نصت المادة 88 منه على أن: "يجوز لقاضي التحقيق والشرطة القضائية الإستعانة بخبير مختص ليقدم بطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه، أو الدخول إلى البيانات المخزونة أو المعالجة أو المنقولة بواسطته"، وتضيف نفس المادة: "لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق، وعلى الخبير الإستجابة لطلب هيئات التحقيق والقضاء وإلا تعرض لعقوبات جزائية".[4]

ووفقًا للقانون المشار إليه فإن الإلتزام بتشغيل المنظومة وإستخراج المعطيات المطلوبة منها يرجع إلى قاضي التحقيق بصفة أصلية، ويجوز كذلك للنيابة العامة على سبيل الإستثناء في حالة التلبس بالجريمة أو عند الرضا بعملية التفتيش، فمهمة الخبير وفقًا للنص السابق تتمثل من ناحية في تشغيل المنظومة ومن ناحية أخرى في تقديم المعطيات المطلوبة حسب الطريقة التي

[1]- براهيمي جمال، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة الدكتوراه علوم، تخصص: القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري- تيزي وزو، 2018، ص 70.

[2]- بلحسيني حمزة، مرجع سابق، ص 365.

[3]- شنتير خضرة، مرجع سابق، ص 123.

[4]- عائشة بن قارة مصطفى، مرجع سابق، ص140.

تريدها جهة التحقيق، كأن تسجل وتسلم تلك المعطيات على الفلاش ديسك أو على أي وسيط إلكتروني يحمل المعطيات الإلكترونية أو على ورق.[1]

وهو ما تداركه المشرع الجزائري بموجب القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر في الفقرة 04 من المادة 05 منه، والفقرة 03 من المادة 16 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر على إمكانية للسلطات المكلفة بتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

كما مكن للجهات القضائية اللجوء إلى الخبرة لإثبات الجرائم المنصوص عليها في القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر بما في ذلك جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور، ما لم يكن التزوير ثابتًا من طبيعة الوثيقة المزورة أو من تصريحات الجهة المصدرة لها بموجب المادة 17 من ذات القانون.

2- تعريف الخبير التقني:

الخبير هو شخص مختص فنيًا في مجال من المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى، ويستطيع بما له من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية والتي تحتاج إلي خبرة فنية خاصة.[2]

وتقتضي فاعلية الخبرة ضرورة الجمع بين التعمق في كل من الدراسة العلمية والنظرية والممارسة العملية للتخصص العلمي والنظري، وكذا متابعة مستمرة للتطورات التي تلحق بفروع التخصص، غير أن ذلك ليس شرطًا لازمًا في بعض الأحيان فقد يقتصر الخبير على مجرد الخبرة العملية في فرع التخصص دون أن يكون هناك رصيد من الدراسة العلمية والنظرية وهو الأمر الذي نلاحظه في مجالات الخبرة في الفروع المهنية المختلفة[3]، إلا أنه يؤخذ عليه بأنه يتعارض مع الواقع القانوني ذلك أنه عادة ما يحرر الخبير في نهاية أعمال الخبرة تقريرًا ويلزم في هذا الأخير أن يتوافر على جميع العناصر الشكلية والموضوعية، وبالتالي لا يمكن للخبير التقني فحسب أن يعد هذا التقرير، فضلًا على أن هذا الرأي من شأنه

[1]- محمود سعد عبد المجيد، مرجع سابق، ص 501.

[2]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 285.

[3]- محمود سعد عبد المجيد، مرجع سابق، ص 498

جعل جميع أفراد المجتمع بمختلف أعمار خبراء التقنية نتيجة الإنتشار الواسع لمعرفة التقنيات الرقمية والشبكية[1].

ولدى بعض الدول المتقدمة كالولايات المتحدة الأمريكية المقومات التقنية الكاملة وذات كفاءة عالية للسلطات التحقيق، ويكون هناك فصل بين الخبرة وسلطة التحقيق في الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، أما سلطات التحقيق التي لا تمتلك ذلك فإنها تعتمد على الخبرة التقنية وبالتالي لا يتحقق الفصل بين سلطة التحقيق والخبرة، حيث إن الخبرة تقوم بدور في التحقيق لمساعدة سلطة التحقيق لإثبات الجريمة والدليل الإلكتروني.[2]

إستنادًا الى ما سبق ذكره، يمكن تقسيم الخبراء إلى نوعين وذلك على النحو التالي:

الطائفة الأولى: وهم الخبراء من خريجي الكليات العملية[3]، ويتم تدريب هؤلاء وتلقينهم بعض المواد القانونية والشرطية بما يتفق وإحتياجتهم في مجال التخصص.[4]

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 143.

[2]- مسعود بن حميد المعمري، مرجع سابق، ص 198.

[3]- تتنوع المجالات التي تقتضي الخبرة بحيث أنها قد تشمل الموظفين التابعين للدولة أو غيرهم، فهي تشمل مثلًا الأطباء الشرعيين الذين يتلقون بالإضافة إلى علم الطب دراسات تخصصية في الإصابات الجنائية بأنواعها المختلفة، ويقدم هؤلاء خبراتهم في مجال الفحص الطبي والتشريح لتوضيح أسباب الإصابة أو الوفاة وكيفية حدوثها ونوع الأداة المستخدمة في إرتكاب الجريمة ووقت الحدوث والنتائج المترتبة عليها، كذلك يوجد ما يسمى بخبراء البصمات والذين يقومون بالكشف عن آثار البصمات التي قد يكون الجاني تركها في مكان إرتكاب الجريمة ومقارنتها مع بصمات أخرى من المشتبه بهم ومعتادي الإجرام، ويوجد أيضًا ما يسمى بخبراء التصوير الجنائي الذي يقع على عاتقهم الإختصاص بتصوير مسرح الجريمة بالمحتويات التي قد يتضمنها وتوضيح بعض الآثار والمخلفات التي وجدت، فكأنما يقوم بتسجيل المكان بأكمله عن طريق الصور الفوتوغرافية، حيث يتمكن المحققون والمحكمة من الإطلاع عليها وبيان مسرح الجريمة بكل محتوياته، بالإضافة إلى هؤلاء يوجد أيضًا من يسمون بالخبراء الجنائيين والذين ينقسمون إلى عدة طوائف كالخبراء بالفحوص البيولوجية، وهناك أيضًا من يسمون بخبراء الفحوص الكيميائية والذين يتخصصون في تحليل المواد سواء كانت عضوية أو غيرها لتحديد نوعها والمواد التي تتركب منها وعناصرها أو أية مواد أخرى قد توجد في مسرح الجريمة ولا يعرف محتواها، ويوجد أيضًا خبراء الأسلحة الذين يتولون فحص الأسلحة وتحديد نوعها ونوع الأظرف المستخدمة في إطلاق النار وفيما إذا كانت تعود للسلاح الذي تم ضبطه أم لا، وزاوية إطلاق النار أو الوضعية التي كان عليها كل من المتهم والمجني عليه، ويوجد أيضًا خبراء بالحرائق حيث يختصون في كشف المكان وبيان المواد المستخدمة في إشعال الحريق وهل كان متعمدًا أم كان نتيجة لإلتماس كهربائي وأيضًا بتحديد منطقة بدء الحريق والأسباب التي أدت إليه والزمن الذي تطلبه إشتعال المواد المستخدمة أو الوقت الذي إستغرقه الحريق، كذلك يوجد الخبراء يكون إختصاصهم كشف التزييف والتزوير في المستندات التي قد يطعن أحد الخصوم بالدعوى أنها مزورة فتقوم هنا السلطة القضائية المختصة بإحالتها إلى خبير يختص بدراسة هذا المستند وبيانات التغيير أو العبث الذي تم في الفصل فيما إذا كان هذا المستند نسخة أصلية أو أنها نسخة مقلدة منها ولا شك أن هذا الأمر يحتاج إلى إستخدام العديد من الطرق الفنية والحديثة للمضاهاة وتقرير ما إذا كان هناك تزييف أو تزوير، وهناك أيضًا طوائف قد لا تتبع الجهاز الحكومي أو ما يسمى بخبراء الجدول ولكن يعتبرون من أهل الخبرة الجائز اللجوء إليهم لأخذ رأيهم في الأمور التي قد تحتاج إلى مثل ذلك الرأي بحسب تقدير المحقق والتي يعجز عن تقويمها هو بنفسه، كما هو الحال في أصحاب الهوايات الذين أصبحوا أصحاب معرفة وإضطلاع في تربية بعض الحيوانات كالأغنام والإبل والحمام خاصة فيما يتعلق بتقدير قيمتها عند إصابتها أو نفوقها من قبل فعل المتهم غير المشروع، وللمزيد من التفصيل، ينظر: خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص-ص 289- 291.

[4]- نفس المرجع، ص 287.

الطائفة الثانية: وهم الخبراء من ضباط الشرطة الذين يعملون في مجال المعمل الجنائي والأدلة الجنائية، يقتضي تخصصهم تلقينهم وتدربهم تدريبًا خاصًا ودراسة بعض العلوم وذلك لمعاونتهم في التحليل العلمي في مجال التخصص، وهذه الطائفة تتخصص في مجال فحص الأسلحة النارية والكشف عن التزوير والتزييف ومضاهاة الخطوط وفحص قضايا الحريق وغيرها.[1]

ثانيًا: الضوابط التي تحكم الخبرة التقنية

تخضع الخبرة التقنية لمجموعة من الضوابط القانونية والفنية، فالضوابط القانونية تنحصر في تلك الضوابط المنصوص عليها في قانون الإجراءات الجزائية، أما الضوابط الفنية فتشمل خطوات إستخلاص الدليل الإلكتروني.

1- الضوابط القانونية:

تتمثل الضوابط القانونية التي تحكم الخبرة التقنية في ما يلي:

أ- الإستعانة بالخبير التقني:

أجاز المشرع الجزائري للنيابة العامة الإستعانة بالخبرة التقنية بمقتضى القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر في الفقرة الأولى من المادة 46 منه التي تنص على أن: "يمكن النيابة العامة الإستعانة في المسائل الفنية بأشخاص مؤهلين مساعدين متخصصين، يتم إختيارهم من بين الأشخاص ذوي الإختصاص، وإذا تعذر ذلك يمكن إختيارهم من جدول الخبراء القضائيين"، ونصت الفقرة الأخيرة من نفس المادة على أن يحدد شروط وكيفيات إختيار الأشخاص المؤهلين ونظامهم التعويضي عن طريق التنظيم.

وتجدر الإشارة إلى أن المادة المذكورة أعلاه جاءت لتحل محل المادة 35 مكرر من الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية الملغى، والتي كانت تنص على أن: "يمكن النيابة العامة الإستعانة في مسائل فنية بمساعدين متخصصين"، وقد تم تنظيم تطبيق أحكام هذه المادة من خلال المرسوم التنفيذي رقم: 17-324 المؤرخ في 08 نوفمبر 2017 الذي يحدد شروط وكيفيات تعيين المساعدين المتخصصين لدى النيابة العامة وقانونهم الأساسي ونظام تعويضاتهم[2]، وتلاه قرار وزير العدل المؤرخ في 07 مارس 2018 الذي يهدف إلى تحديد قائمة التخصصات التي يعين فيها المساعدون المتخصصون والجهات القضائية المعنية[3].

ويلاحظ أن المادة 46 من القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر لم تقتصر فقط على إعادة ترقيم المادة من 35 مكرر إلى 46، بل جاءت بإضافة

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 287.

[2]- المرسوم التنفيذي رقم: 17-324 المؤرخ في 08 نوفمبر 2017، يحدد شروط وكيفيات تعيين المساعدين المتخصصين لدى النيابة العامة وقانونهم الأساسي ونظام تعويضاتهم، ج.ر.ج.ج.ش العدد 67، الصادرة في 15 نوفمبر2017.

[3]- قرار وزير العدل المؤرخ في 07 مارس 2018، يحدد قائمة التخصصات التي يعين فيها المساعدون المتخصصون والجهات القضائية المعنية، ج.ر.ج.ج.ش العدد22، الصادرة 18 أفريل 2018.

تمثلت في النص على أن في حالة تعذر على النيابة العامة الإستعانة بأشخاص مؤهلين مساعدين متخصصين من بين الأشخاص ذوي الإختصاص، يمكن أن يتم إختيارهم من جدول الخبراء القضائيين.

وفي هذا الإطار سيتم التطرق إلى أهم ما جاء به المرسوم التنفيذي وقرار وزير العدل اللذين نظمت بموجبهما كيفيات إختيار مساعدين متخصصين، حيث يتم إنتداب المساعدين المتخصصين لدى الجهات القضائية ذات الإختصاص الموسع[1] في تخصصات التالية: المحاسبة والمالية، الصفقات العمومية، التقنيات والعمليات المالية والمصرفية، التقنيات الجمركية، أنظمة المعالجة الآلية للمعطيات، التجارة الدولية، المناجم والمعادن النفيسة، لنيابات العامة للمجالس القضائية بالجزائر ووهران وقسنطينة وورقلة[2]، ويقوم النائب العام بتوزيعهم على نيابات الجمهورية التابعة لمجلسه القضائي حسب إحتياجات كل منها[3]، وكذا يمكن للجهات القضائية التي لا تملك مساعدين في إختصاص معين الإستعانة بالمساعدين المتخصصين للجهات القضائية الأخرى بناء على طلب النائب العام[4].

يتابع المساعدون قبل مباشرة مهامهم تكوينًا مدته ثلاثة (03) أشهر، يتضمن على الخصوص التعرف على العمل القضائي وإختصاصات الجهات القضائية وسيرها وكيفيات ممارسة مهامهم[5]، يقوم المساعدون بتكليف من النيابة العامة وتحت مسؤوليتها بالمشاركة في كل الإجراءات المتعلقة بالدعوى العمومية لاسيما:

- إبداء الرأي في المسائل الفنية؛
- إستغلال الوثائق والمستندات ذات العلاقة بمهامهم؛
- مساعدة ضباط الشرطة القضائية في المسائل الفنية؛
- يقدم المساعدون أعمالهم في شكل تقارير تلخيصية أو تحليلية.[6]

يؤدي المساعدون مهامهم بموضوعية وإستقلالية وحياد، ويخضعون إلى السلطة المباشرة لقضاة النيابة لدى الجهة القضائية التي يمارسون مهامهم أمامها، ولا يخضعون في ممارسة مهامهم إلى تعليمات إدارتهم الأصلية.[7]

كما يمكن للضباط الشرطة القضائية الإستعانة بالمساعدين متخصصين المكلفين من النيابة العامة وتحت مسؤوليتها لمساعدتهم في المسائل الفنية طبقًا للفقرة 04 من المادة 09 من

[1]- المادة 02 من قرار وزير العدل السالف الذكر.
[2]- المادة 03 من قرار وزير العدل السالف الذكر.
[3]- المادة 2/02 من المرسوم التنفيذي رقم: 17-324 السالف الذكر.
[4]- المادة 17 من المرسوم التنفيذي رقم: 17-324 السالف الذكر.
[5]- المادة 08 من المرسوم التنفيذي رقم: 17-324 السالف الذكر.
[6]- المادة 09 من المرسوم التنفيذي رقم: 17-324 السالف الذكر.
[7]- المادة 10 من المرسوم التنفيذي رقم: 17-324 السالف الذكر.

المرسوم التنفيذي رقم: 17-324 الذي يحدد شروط وكيفيات تعيين المساعدين المتخصصين لدى النيابة العامة وقانونهم الأساسي ونظام تعويضاتهم.

كما يجيز المشرع الجزائري لضباط الشرطة القضائية بندب خبير في الحالتين:

حالة التلبس: قيام حالة التلبس يعطي للضبطية القضائية صلاحيات قانونية أوسع من صلاحياتها العادية للبحث والتحري، إذ أجاز المشرع الجزائري الإستعانة بالخبراء في حالة الجرم المشهود بموجب المادة 81 من ق.إ.ج.ج التي تنص على أن: "إذا إقتضى الأمر إجراء معاينات لا يمكن تأخيرها فلضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك، وعلى هؤلاء الأشخاص الذين يستدعيهم لهذا الإجراء أن يؤدوا اليمين كتابة على إبداء رأيهم بما يمليه عليهم الشرف والضمير".

لم يوضح النص ما إذا كان بإستطاعة ضابط الشرطة القضائية إستغلال ما يتوصل إليه الخبير ومناقشة المشتبه فيهم بشأنه، ولكن يبدو أن ذلك شيء منطقي وضروري لمعالجة حالة التلبس.[1]

الإنابة القضائية: أجاز المشرع الجزائري لقاضي التحقيق أن يندب أحد ضباط الشرطة القضائية للقيام ببعض إجراءات التحقيق بموجب الفقرة الأولى من المادة 234 من ق.إ.ج.ج التي تنص على أن: "يجوز لقاضي التحقيق أن يكلف بطريق الانابة القضائية أي قاضي من قضاة محكمته أو أي ضابط من ضباط الشرطة القضائية المختص بالعمل في تلك الدائرة أو أي قاضي من قضاة التحقيق، بالقيام بما يراه لازمًا من إجراءات التحقيق في الأماكن الخاضعة للجهة القضائية التي يتبعها كل منهم"، وتنص الفقرة 02 من المادة 235 من نفس القانون على أن: "ولا يجوز لضباط الشرطة القضائية إستجواب المتهم أو القيام بمواجهته أو سماع أقوال المدعي المدني"، ومنه فإنه يجوز لضباط الشرطة القضائية المنتدبون بإتخاذ أي إجراء من إجراءات التحقيق الإبتدائي بما فيها الإستعانة بالخبراء ضمن حدود الإنابة القضائية، ماعدا ما تعلق بإستجواب المتهم أو القيام بمواجهته أو سماع أقوال المدعي المدني.

كما أجاز المشرع الجزائري بموجب المادة 239 من ق.إ.ج.ج لجهات التحقيق أو الحكم عندما تعرض عليها مسألة ذات طابع فني أن تأمر بندب خبير، إما من تلقاء نفسها أو بناء على طلب النيابة العامة أو بناء على طلب الخصوم أو محاميهم.

وإن رأى قاضي التحقيق أنه لا موجب للإستجابة لطلب إجراء الخبرة فعليه أن يصدر في ذلك أمرًا معللًا بالرفض في أجل عشرة (10) أيام يبدأ سريانه من تاريخ إستلامه الطلب[2]، ويكون قابلًا للإستئناف من طرف وكيل الجمهورية في أجل ثلاث (03) أيام من صدوره[3]،

---

[1]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 138.

[2]- المادة 2/239 من القانون رقم: 25-14 السالف الذكر.

[3]- المادة 2/266 من القانون رقم: 25-14 السالف الذكر.

ومن طرف المتهم أو محاميه في أجل ثلاث (03) أيام كذلك تسري من تاريخ تبليغ أمر الرفض إليه[1].

وإذا لم يبت قاضي التحقيق في الأجل المذكور، يمكن الطرف المعني إخطار غرفة الإتهام مباشرة خلال عشرة (10) أيام، ويتعين على هذه الأخيرة أن تفصل في ذلك الطلب في أجل عشرين (20) يومًا تسري من تاريخ إخطارها ويكون قرارها غير قابل لأي طعن.[2]

كما يجوز أن يختار الخبير من الجدول الذي تعده المجالس القضائية[3] بعد إستطلاع رأي النيابة العامة، وتحدد كيفيات قيد الخبراء أو شطب أسماءهم بقرار من وزير العدل[4]، كما يجوز بصفة إستثنائية أن يختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول[5]، كحالة الإستعجال وغياب الخبير المختص المقيد بالجدول أو التخصص الدقيق للخبير في فرع من الفروع العلمية ذات الصلة بمسألة البحث، ويثار البطلان أمام غرفة الإتهام أو كدفع أولي قبل الخوض في الموضوع أمام جهة الحكم.[6]

ويجوز لقاضي التحقيق ندب خبير أو عدة خبراء[7] حسب مقتضيات التحقيق، وهذا التعدد ضروري في مجال الخبرة التقنية ذلك أنه من الصعوبة وجود مختص ذو معرفة شاملة بالتقنيات الرقمية ونظمها، حتى وإن كان يملك القدرات على الظهور بمظهر المتفرد في مجال الخبرة القضائية[8].

---

[1]- المادة 2/268 من القانون رقم: 25-14 السالف الذكر.

[2]- المادة 239/ 3 من القانون رقم: 25-14 السالف الذكر.

[3]- نظم المشرع الجزائري شروط التعيين في وظيفة الخبراء القضائيين في المرسوم التنفيذي رقم: 95-310 المؤرخ في 10 أكتوبر 1995، إذ حدد شروط التسجيل في قوائم الخبراء القضائيين وكيفياته، كما حدد حقوقهم وواجباتهم، في الفصل الثاني تحت عنوان: "الشروط العامة للتسجيل"، وفرق بين الشروط المتطلبة في الشخص الطبيعي وتلك المتعلقة بالشخص المعنوي. فيما يتعلق بالشروط المتطلبة في الشخص الطبيعي فبإستقراء المادة 04 في الفقرة 08 منها يمكن إجمال هذه الشروط فيما يلي: "شرط الجنسية الجزائرية، شرط الكفاءة العلمية، شرط حسن السيرة"، أما فيما يتعلق بالشخص المعنوي فبموجب المادة 05 من المرسوم المذكور نجد أن هذه الشروط تتمثل فيما يلي: "أن تتوفر في المسيرين الإجتماعيين الشروط المنصوص عليها في الفقرات 3 و4 و5 من المادة 04، أي نفس الشروط المطلوبة في الشخص الطبيعي، أن يكون الشخص المعنوي قد مارس نشاطًا لا تقل مدته عن خمس (05) سنوات لإكتساب تأهيل كاف في التخصص الذي يطلب التسجيل فيه، أن يكون له مقر رئيسي أو مؤسسة تقنية تتماشى مع تخصصه في دائرة إختصاص المجلس القضائي".
لم يحدد المشرع طبيعة شخص الخبير سواء كان شخصًا طبيعيًا أو شخصًا معنويًا كمؤسسة متخصصة تعمل في مجال المحاسبة مثلًا، وإن كان الواقع العملي للخبرة الإستعانة بالشخص الطبيعي، إلا أنه في مجال الجريمة الإلكترونية يتعين الإستعانة بشركات ومنظمات أو مؤسسات متخصصة، حيث تملك موارد مادية من برامج وأجهزة حديثة، وموارد بشرية من مهندسين متخصصين في الحاسوب والإنترنت، ومن أمثلة هذه الشركات مختبر الخبرة والبحث عن البصمات الآثار المعلوماتية في فرنسا Lerti، وللمزيد من التفصيل، ينظر: عائشة بن قارة مصطفى، مرجع سابق، ص 142.

[4]- المادة 1/240 و2 من القانون رقم: 25-14 السالف الذكر.

[5]- المادة 3/240 من القانون رقم: 25-14 السالف الذكر.

[6]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 334.

[7]- المادة 243 من القانون رقم: 25-14 السالف الذكر.

[8]- عائشة بن قارة مصطفى، مرجع سابق، ص 142.

وأن يحدد دائمًا في الأمر بندب خبير المهمة المطلوبة منه والأسئلة الفنية أو العملية التي يطلب الإستفسار فيها، وأن هذه المهمة لا يجوز أن تتعلق إلا بفحص مسائل ذات طابع فني، ولا يفوض فيها أي جزء من جوانب إختصاصه لأن ذلك قد يعرض أمره للبطلان.[1]

ب- سير الخبرة:

تتم الخبرة وفق القواعد المحددة في قانون الإجراءات الجزائية الجزائري فيما يلي:

ب-1- أداء اليمين القانونية:

يلزم على الخبير حلف اليمين قبل أداء مهمته تحت طائلة البطلان، فهو يعد إجراء جوهري لجعل الخبير يلتزم بالصدق والأمانة في مهمته وبث الطمأنينة في الآراء التي يقدمها، سواء ما تعلق بتقدير القاضي أو لثقة أطراف الدعوى.[2]

يؤدي الخبير اليمين بمجرد قيده لأول مرة بالجدول الخاص بالمجلس القضائي أمام القاضي وبحضور أمين الضبط يمينًا أمام ذلك المجلس بالصيغة المنصوص عليها في المادة 241 من ق.إ.ج.ج وهي كالآتي: "أقسم بالله العظيم وأتعهد بأن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص، وأن أبدي رأيي بكل نزاهة وإستقلال"، ولا يجدد هذا القسم بعد ذلك عند تعيينه لإجراء أي خبرة ما دام الخبير مقيدًا في الجدول.[3]

وفي حالة ندب خبير من خارج الجدول، يتعين على الخبير المختار تأدية اليمين حسب الصيغة المنصوص عليها أعلاه أمام قاضي التحقيق وذلك قبل مباشرته للمهمة المطلوبة منه، وأن يتم تحرير محضر بأداء اليمين يوقع من قبل قاضي التحقيق والخبير وأمين الضبط، وفي حالة قيام مانع من حلف اليمين لأسباب معينة يتعين ذكرها بالتحديد ويؤدي حينئذ أداء اليمين بالكتابة ويرفق الكتاب المتضمن ذلك بملف التحقيق[4]، وغياب محضر أداء اليمين أو الكتاب المتضمن من ملف الدعوى لا تعوضه الإشارة إلى أداء اليمين في تقرير الخبرة ويؤدي ذلك إلى بطلانه[5].

ويؤدي الشخص المؤهل اليمين أمام المجلس القضائي الذين يعينون بدائرة إختصاصه عند تعيينهم وقبل مباشرة مهامهم وفق الصيغة المنصوص عليها في الفقرة 02 من المادة 46 من نفس القانون وهي كالآتي: "أقسم بالله العظيم بأن أقوم بأداء مهامي على أحسن وجه، وأن أحافظ على سرية المعلومات التي أطلع عليها بمناسبة أداء أعمالي" ويحرر محضر بذلك[6]، وبموجب

---

[1]- محمد حزيط، **أصول الإجراءات الجزائية في القانون الجزائري على ضوء آخر التعديلات لقانون الإجراءات الجزائية والإجتهاد القضائي**، الطبعة الثانية، 2019، دار هومة، الجزائر، ص 296.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص-ص 143-144.

[3]- المادة 1/241 و2 من القانون رقم: 25-14 السالف الذكر.

[4]- المادة 3/241 و4 و5 من القانون رقم: 25-14 السالف الذكر.

[5]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 335.

[6]- المادة 07 من المرسوم التنفيذي رقم: 17-324 السالف الذكر.

المادة 81 من نفس القانون إذا إقتضى الأمر إجراء معاينات لا يمكن تأخيرها فالضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك، وأن يؤدوا اليمين كتابة على إبداء رأيهم بما يمليه عليهم الشرف والضمير.

ب-2- مراقبة مراحل الخبرة:

يقوم الخبير بأداء مهمته تحت مراقبة قاضي التحقيق أو القاضي الذي تعينه الجهة القضائية التي أمرت بإجراء الخبرة[1]، ويجب عليه أثناء قيامه بمهمته أن يكون على إتصال بقاضي التحقيق أو القاضي المنتدب، وأن يحيطوه علمًا بتطورات الأعمال التي يقومون بها، ويمكنه من كل ما يجعله في كل حين قادرًا على إتخاذ الإجراءات اللازمة[2].

وإذا تعلق الأمر بالأحراز المختومة التي لم تكن قد فضت ولم يتم جردها، يتعين على قاضي التحقيق أو القاضي الذي تعينه الجهة القضائية أن يعرضها على المتهم قبل إرسالها للخبير[3]، وأن يعدد هذه الأحراز في المحضر الذي يحرر خصيصًا لإثبات تسليم هذه الأشياء[4]، كما يتعين على الخبراء أن ينوهوا في تقريرهم عن كل فض أو إعادة فض للأحراز التي يقومون بجردها[5]، أما إذا كانت الأحراز قد سبق جردها أو فضها فلا داعي لعرضها مرة أخرى على المتهم ويكفي جردها في محضر التسليم[6].

وتطبيقًا لنفس النص السالف الذكر، أكدت محكمة النقض الفرنسية على واجب الخبير إعلام قاضي التحقيق بالوقائع التي تبدو له مشبوهة والتي تظهر له عند دراسة الوثائق التي تكون قد سلمت له لأغراض الخبرة، وأنه إذا كانت تلك الوقائع من شأنها أن تكون جرائم أخرى غير الجرائم المحددة في الأمر بندب الخبير فالقاضي التحقيق أن يتخذ كل الإجراءات اللازمة.[7]

وإذا ظهرت للخبير في إطار أداء مهمته مسألة تقنية خارجة عن دائرة إختصاصه فإنه طبقًا للمادة 149 من ق.إ.ج يجوز له أن يطلب من قاضي التحقيق الترخيص له بضم فنيين يعينون بأسمائهم ويكونون على الخصوص مختارين لتخصصهم، وإذا تم ذلك يؤدي الفنيون المعينون اليمين بنفس الصيغة التي يؤدي بها الخبراء يمينهم ضمن الشروط المنصوص عليها في المادة 145 من نفس القانون ويحرر محضرًا عنها، وعند أداءهم للمهمة يحرر هؤلاء التقنيون تقريرًا يرفقونه بتقرير الخبراء.

---

[1]- المادة 5/239 من القانون رقم: 25-14 السالف الذكر.

[2]- المادة 2/244 من القانون رقم: 25-14 السالف الذكر.

[3]- المادة 160 /3 من القانون رقم: 25-14 السالف الذكر.

[4]- المادة 1/246 من القانون رقم: 25-14 السالف الذكر.

[5]- المادة 2/246 من القانون رقم: 25-14 السالف الذكر.

[6]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 338.

[7]- محمد حزيط، مرجع سابق، ص-ص 297-298.

ويجوز للخبير على سبيل المعلومات وفي الحدود اللازمة لأداء مهمته تلقي تصريحات أشخاص غير المتهم[1]، ولكنه لا يملك أي سلطة للبحث عن الشهود لإجبارهم على الإدلاء بشهادتهم إلا إذا رأى فائدة في ذلك، حينئذ يمكن للخبير إطلاع قاضي التحقيق بذلك وفي هذه الحالة يتم سماع الشهود من قبل قاضي التحقيق بنفسه، كما يتعين على الخبير أن يخطر الخصوم بأن لهم الحق في إبداء ملاحظاتهم المكتوبة في موضوع المهمة المنوط به أداءها[2].

وإذا إضطر الخبير إلى إستجواب المتهم لا يمكنه القيام بذلك بنفسه، وإنما يقوم به قاضي التحقيق أو القاضي المعين من المحكمة بحضور الخبير وبحضور محامي المتهم بعد إستدعاءه قانونًا وفقًا للأوضاع والشروط المنصوص عليها في المادتين 180 و181 من ذات القانون[3]، اللتين تنصان على أن يتم إستجواب المتهم إلا بحضور محاميه أو بعد دعوته قانونًا ما لم يتنازل صراحة عن ذلك، وأن يتم إستدعاء المحامي بكتاب موصى عليه يرسل إليه بيومين على الأقل قبل إستجواب المتهم، وأن يوضع ملف الإجراءات تحت طلبه قبل كل إستجواب بأربع وعشرين (24) ساعة على الأقل، وجواز حضور وكيل الجمهورية هذا الإستجواب وتوجيه مباشرة ما يراه لازمًا من الأسئلة.

غير أنه يجوز للمتهم أن يتنازل عن الضمانات المذكورة أعلاه بتقرير صريح منه أمام قاضي التحقيق أو القاضي المعين من المحكمة، وأن يمد الخبير بحضور محاميه أو بعد إستدعائه قانونًا بالإيضاحات اللازمة لتنفيذ مهمته، كما يجوز له أيضًا بإقرار كتابي يقدمه للخبير ليرفقه بتقريره أن يتنازل عن مساعدة محاميه له في جلسة أو أكثر من جلسات سماع أقواله.[4]

وإذا تعلقت الخبرة بفحص المتهم كحالة ما إذا تعلق الأمر بإجراء خبرة عقلية للمتهم من طرف طبيب متخصص في الأمراض النفسية والعقلية، فإنه طبقًا للفقرة 05 من المادة 247 من

---

[1]- المادة 1/247 من القانون رقم: 25-14 السالف الذكر.

[2]- المادة 247/ 2 من القانون رقم: 25-14 السالف الذكر.

[3]- المادة 247/ 3 من القانون رقم: 25-14 السالف الذكر.

تنص المادة 180 من القانون رقم: 25-14 السالف الذكر على أن: "لا يجوز سماع المتهم أو الضحية أو المدعي المدني أو إجراء مواجهة بينهما، إلا بحضور محاميه أو بعد دعوته قانونًا ما لم يتنازل صراحة عن ذلك، وينوه عن هذا التنازل في المحضر. يستدعي المحامي برسالة موصى عليها ترسل إليه بيومين (02) على الأقل، قبل إستجواب المتهم أو سماع الضحية أو الطرف المدني حسب الحالة. يمكن أيضًا إستدعاء محامي الأطراف بأي وسيلة إلكترونية أخرى ويثبت ذلك بمحضر. ويجب أن يوضع ملف الإجراءات تحت طلب محامي المتهم قبل كل إستجواب بأربع وعشرين (24) ساعة على الأقل، كما يجب أن يوضع تحت طلب محامي الضحية أو المدعي المدني قبل سماع أقواله بأربع وعشرين ساعة (24) على الأقل".

وتنص المادة 181 من نفس القانون على أن: "يجوز لوكيل الجمهورية حضور إستجواب المتهمين ومواجهتهم وسماع أقوال المدعي المدني. ويجوز له أن يوجه له أن يوجه مباشرة ما يراه لازمًا من الأسئلة. ويتعين على أمين ضبط التحقيق في كل مرة يبدي فيها وكيل الجمهورية لقاضي التحقيق رغبته في حضور الإستجواب أن يخطره بمذكرة بسيطة قبل الإستجواب بيومين (02) على الأقل".

[4]- المادة 247/ 4 من القانون رقم: 25-14 السالف الذكر.

ذات القانون يجوز للخبراء الأطباء أن يوجهوا للمتهم الأسئلة اللازمة لأداء مهمتهم بغير حضور القاضي ولا حضور المحامي.[1]

ومن جهة أخرى يجوز لأطراف الخصومة أثناء إجراء أعمال الخبرة أن يطلبوا إلى الجهة القضائية التي أمرت بها، أن تكلف خبير بإجراء أبحاث معينة أو سماع أي شخص معين بإسمه الذي قد يكون قادرًا على مدهم بالمعلومات ذات طابع فني.[2]

ب-3- مدة الخبرة:

كل قرار يصدر بندب خبير يجب أن تحدد فيه مهلة لإنجاز مهمته، وإذا كانت هذه المهلة غير كافية إذا إقتضت ذلك أسباب خاصة يجوز أن تمد هذه المهلة من طرف قاضي التحقيق أو الجهة التي ندبته بأمر مسببًا بناءً على طلب من الخبير، وإذا لم يودع الخبير تقريره في الميعاد المحدد له فإنه يجوز إستبداله بغيره في الحين مع إلزامه أن يقدم نتائج ما قام به من أبحاث، كما عليه أن يرد جميع الأشياء والأوراق والوثائق التي تكون قد عهد بها إليه على ذمة إنجاز مهمته في ظرف ثمان وأربعين (48) ساعة، وعلاوة على ذلك فمن الجائز أن تترتب عليه المسؤولية المدنية، وقد يتخذ ضده تدابير تأديبية قد تصل إلى شطبه من جدول الخبراء المنصوص عليه في المادة 240 من نفس القانون.[3]

ب-4- إعداد تقرير الخبرة وإيداعه:

يحرر الخبير عند إنتهاء الأجل المحدد له تقريرًا موقعًا مشتملًا على وصف كافة الأعمال التي قام بها أثناء تأديته لأعماله التي عهد إليه بإتخاذها ويوقع على تقريره، وأن يشهد بقيامه شخصيًا لها.[4]

وعلى الخبير المعين بإسمه في الأمر القضائي أن يقوم بالمهمة بنفسه حتى ولو يرأس عددًا من الخبراء فلا يجوز له تكليف أي منهم للقيام بالمهمة بدلًا عنه، وذلك لا يمنع مجرد المساعدة المادية من مساعديه أو من خبراء آخرين إذا كانت تحت إشرافه.[5]

ويتضمن التقرير أيضًا على النتائج التي توصل إليها الخبير بنفسه من عمله والتي يبدي فيها رأيه حول النتيجة التي توصل إليها حسب خبرته والتي تجيب أساسًا على الأسئلة التي يكون قاضي التحقيق قد طرحها عليه ويوقع على تقرير الخبرة ويودعه، وكذا الأحراز أو ما تبقى منها لدى أمين ضبط الجهة القضائية التي أمرت بالخبرة ويثبت هذا الإيداع بمحضر، وإن تعدد الخبراء وإختلفوا في الرأي أو كانت لهم تحفظات في شأن النتائج المشتركة فعلى كل خبير

[1]- محمد حزيط، مرجع سابق، ص 299.
[2]- المادة 248 من القانون رقم: 25-14 السالف الذكر.
[3]- المادة 1/244 من القانون رقم: 25-14 السالف الذكر.
[4]- المادة 1/249 من القانون رقم: 25-14 السالف الذكر.
[5]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 340.

منهم أن يبدي رأيه أو تحفظاته بصورة مستقلة مع التعليل وجهة نظره وأن يوقع تقريره ويؤرخه.[1]

وينجز المساعدين المتخصصين أعمالهم في شكل تقارير تلخيصية أو تحليلية[2]، ويخضعون إلى السلطة المباشرة لقضاة النيابة لدى الجهة القضائية التي يمارسون مهامهم أمامها[3].

ب-5- تبليغ تقرير الخبرة إلى الأطراف وإبداء ملاحظاتهم حوله:

تفاديًا لمناقشة نقائص الخبرة أمام جهات الحكم في جلسة علانية حاول المشرع حصر الإنتقادات التي قد توجه إلى عمل الخبراء في مرحلة التحقيق[4]، ولهذا الغرض نصت الفقرة الأولى من المادة 250 من ق.إ.ج.ج على أنه إثر إيداع تقرير الخبرة يقوم قاضي التحقيق بإستدعاء من يعنيهم الأمر من أطراف الدعوى ويحيطهم علمًا بما إنتهى إليه الخبراء من نتائج، وذلك مع مراعاة أحكام المادتين 180 و181 من نفس القانون.

فيتلقى قاضي التحقيق أقوالهم ويحدد لهم أجلًا لإبداء ملاحظاتهم بشأن الخبرة أو تقديم طلبات خلالها، ولاسيما فيما يخص إجراء أعمال خبرة تكميلية أو القيام بخبرة مضادة إذا تطلب الأمر ذلك، وإذا لم يبت قاضي التحقيق في أجل ثلاثين (30) يومًا من تاريخ إستلامه الطلب يمكن للطرف المعني إخطار غرفة الإتهام مباشرة خلال عشرة (10) أيام، ولهذه الأخيرة أجل ثلاثين (30) يومًا للفصل في الطلب تسري من تاريخ إخطارها ويكون قرارها غير قابل لأي طعن، وإذا رفض قاضي التحقيق هذه الطلبات يتعين عليه أن يصدر أمرًا مسببًا في أجل ثلاثين (30) يومًا من تاريخ إستلامه الطلب.[5]

فإن كان طلب إجراء الخبرة التكميلية أو المضادة قد قدم من طرف المتهم أو محاميه وصدر بشأنه أمرًا برفض الطلب، جاز للمتهم أو محاميه بمقتضى المادة 268 من نفس القانون إستئناف الأمر المذكور في أجل ثلاثة (03) أيام من تاريخ تبليغه، أما الطرف المدني أو محاميه فلم يخولهم القانون هذا الحق.[6]

وبناءً على ذلك فلا يمكن للمحكمة أن تستند على تقرير الخبير الذي لم يقدم الملاحظات عليه سواء من أطراف الخصوم أو بواسطة محاميهم، فلهم الحق في إظهار الخطأ في البيانات أو المعلومات التي أوردها الخبير، ولهم أيضًا الحق في نفي أسانيده وحججه لإثبات عدم صحة ما توصل إليه الخبير.[7]

---

[1]- المادة 249 من القانون رقم: 25-14 السالف الذكر.

[2]- المادة 2/09 من المرسوم التنفيذي رقم: 17-324 السالف الذكر.

[3]- المادة 1/10 من المرسوم التنفيذي رقم: 17-324 السالف الذكر.

[4]- أحسن بوسقيعة، **التحقيق القضائي**، الطبعة الثالثة عشرة، 2021، دار هومة، الجزائر، ص 128.

[5]- المادة 1/250 و2 و3 من القانون رقم: 25-14 السالف الذكر.

[6]- محمد حزيط، مرجع سابق، ص 300.

[7]- بلولهي مراد، مرجع سابق، ص 74.

ج- مدى حجية تقرير الخبير التقني:

يتعين على الخبير بعد الإنتهاء من مهمته أن يعد تقريرًا يضمن فيه نتائج ما توصل إليه بعد الإستناد إلى الأسس والقواعد العلمية والفنية في معالجة المسائل المطروحة، ويخضع هذا التقرير لتقدير القاضي فالقانون لم يعترف له بأي قوة ثبوتية فله أن يأخذ أو يستبعد نتائج الخبرة كما يشاء، ويمكنه كذلك أن يأمر بإجراء الخبرة التكميلية[1] أو القيام بالخبرة المضادة أو المقابلة خصوصًا في حالة تعارض النتائج التي توصل إليها الخبير في سياق نفس الموضوع أو تعارض التقرير مع شهادة الشهود[2].

ويجوز للرئيس الجلسة من تلقاء نفسه أو بناء على طلب النيابة العامة أو الخصوم أو محاميهم أن تأمر بإستدعاء الخبير إذا تطلب الأمر ذلك لمناقشته حول التقرير الذي تقدم به، بتوجيه للخبراء أسئلة تدخل في نطاق المهمة التي عهد إليهم بها.[3]

حيث يتم سماع شهادة الخبراء الذين قاموا بفحص الحاسوب أو الهواتف المحمولة أو الموقع أو الحساب الخاص بالمتهم أو بريده الإلكتروني، ومناقشتهم فيما أعدوه من تقارير بشأن أدلة الجريمة وكيفية وصولهم إلى النتائج التي بلغوها، حتى تطمئن المحكمة إلى التقرير الفني المقدم منهم من عدمه، لاسيما أن أعمالهم تتصل بمسائل مادية أو فنية بحتة يصعب على القضاء إستيعابها دون متخصص يوضح دورها في الكشف عن الجريمة ومرتكبها.[4]

ومن الجدير بالذكر أن القاضي يمتلك السلطة التقديرية لتقدير الخبير الذي يرد إليه، غير أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز له نفيها إلا بالأسانيد الفنية.[5]

إلا أن هناك من يرى أن الوسائل التقنية العلمية في معظم الأحيان ليست دليلًا مستقلًا في ذاتها وإنما هي عبارة عن قرائن يتم دراستها وإستخلاص دلالتها، ومؤدى ذلك أنها لا تصلح في ذاتها كدليل وحيد في الإثبات الجزائي، وهناك رأي آخر يرى أن الدليل العلمي أصبح يقيد من حرية القاضي في تقدير الدليل ويلزمه على الفصل بمقتضاه، لكن هامش تطبيق السلطة التقديرية فيه ضئيل أي لم يعد القاضي مطلقًا في وزن الدليل العلمي الذي بات يأخذ دور

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص-ص 145-146.

[2]- نفس المرجع، ص 146.

[3]- المادة 2/251 من القانون رقم: 25-14 السالف الذكر.

قرار الغرفة الجنائية بالمحكمة العليا الفاصل في الطعن رقم: 679593 بتاريخ 2010/07/22 (منشور على موقع المحكمة العليا وبمجلة المحكمة العليا، العدد 02 لعام 2011، الصفحة 361) وأهم ما جاء فيه: " يمكن لمحكمة الجنايات طلب مثول الخبراء في جلسة الحكم قصد مناقشة أعمالهم الفنية بحضور جميع الأطراف، يستحسن بالنسبة لغرفة الإتهام في حالة خبرات طبية متناقضة ترك مسألة تقديرها لجهة الحكم"، وللمزيد من التفصيل، ينظر: نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 345.

[4]- بهاء المري، مرجع سابق، ص 836.

[5]- عائشة بن قارة مصطفى، مرجع سابق، ص 146.

الصدارة في الإثبات الجزائي، خاصة بعد ظهور الأدلة الإلكترونية وإنشاء المخابر العلمية المتخصصة لفحص الأدلة وتقييم عمليات الإثبات الجنائي.[1]

وفي التطبيق العملي غالبًا ما يسلم القاضي بما توصل إليه الخبير في تقريره ويستند حكمه على أساسه، ويتسم هذا التصرف بالمنطق ذلك أن رأي الخبير ورد في موضوع تقني لا إختصاص للقاضي به وليس في شأن خبرته القضائية أن تمكنه الفصل فيه، فضلًا عن ذلك هو الذي إنتدب الخبير وإعتمد عليه وإعتبره مناسب لمهمته.[2]

2- الضوابط الفنية:

الجرائم الماسة بالمستند الإلكتروني تتسم بطابع فني في غاية التعقيد حيث يكون محل الجريمة فيها غير ملموس، وتتميز أساليب إرتكابها بالتطور السريع والمتلاحق، لذلك لا يمكن كشف غموضها إلا من قبل متخصصين يمتلكون مستوى متقدم من الكفاءة في مجال تخصصهم.[3]

أ- جمع الدليل الإلكتروني:

تتم عملية جمع الأدلة الإلكترونية عبر ثلاث مراحل كالآتي:

المرحلة الأولى: ويتم فيها جمع المعلومات المخزنة لدى مقدم خدمة الإنترنت، من حيث تتبع أنظمة الخوادم التي دخل فيها المجرم المعلوماتي ومحاولة إيجاد أي أثر له من خلالها.[4]

المرحلة الثانية: وهي مرحلة مراقبة المجرم المعلوماتي فمن المحتمل عودته إلى مسرح الجريمة، وتتم بواسطة عدة طرق:

- إستخدام برامج المراقبة للبحث عن المعلومات المشتبه فيها، وحصر وتسجيل معطيات كل دخول وخروج بالموقع؛
- إستخدام ما يعرف بالحشرات (bugs)، وهي أجزاء توضع في الجهاز لمراقبته؛
- إستخدام كاميرات مراقبة لشاشة الجهاز الإلكتروني المعدة للإستخدام التجاري، وأبسط الطرق لمراقبة الجهاز الإلكتروني هي الدخول لمكان وجوده وزرعه؛
- هناك وسيلة آخرى وهي أصعب قليلًا تتمثل في زرع فيروس أو دودة من نوع حصان طروادة، وهذه الوسيلة لها ميزة بأنها تستطيع مراقبة أكثر من جهاز واحد، ولكن يجب عدم السماح للفيروس بالإنتشار وإلا سوف يصبح هدفًا لبرامج الدفاع ضد الفيروسات[5]؛

[1]- منصارة يوسف، مرجع سابق، ص-ص 332-333.
[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 147.
[3]- علي عدنان فيل، مرجع سابق، ص-ص 27-28.
[4]- أحمد يوسف الطحطاوي، مرجع سابق، ص 325.
[5]- نفس المرجع، ص 325.

المرحلة الثالثة: يتم فحص الجهاز الإلكتروني بعد ضبطه من قبل السلطات القضائية المختصة بمكوناته المادية والمعنوية، لإشتقاق الدليل منه.[1]

ويحتاج الخبراء لتأدية أعمالهم التقنية إلى الإستعانة بالأجهزة والأنظمة والبرمجيات، لتحري الحقيقة وجمع الأدلة الإلكترونية وإكتشاف المعلومات التي يحتويها كل دليل، والتي تتمثل في ما يلي:

- أجهزة بقدرة عالية على التحليل وتخزين المعطيات؛
- نسخ من مختلف أنظمة التشغيل المستعملة لدى الأفراد والمؤسسات؛
- نسخ من برامج حذف وكسر كلمات المرور لمختلف الأجهزة الإلكترونية، برامج الضغط وفك الضغط، برامج التشفير وفك التشفير، برامج حماية الأنظمة والشبكات من الإختراق، برامج كشف الأجهزة المخفية من الأقراص الصلبة، برامج إستعادة الملفات المحذوفة وبرامج البحث عن الإنترنت.[2]

ولقد وضعت وزارة العدل الأمريكية إطار عملي نموذجي يحدد التقنيات الأساسية التي يلزم على الخبير التقني إتباعها لجمع الأدلة الإلكترونية وفحصها وتحليلها، وبالتالي كتابة النتائج المتوصل إليها في التقرير[3]، هذا النموذج يتميز بأنه يوضح أنواع الأدلة والمعلومات المستخلصة منها وأماكن وجود هذه المعلومات في الأجهزة وأنظمة المعلومات المختلفة، كما أنه يربط كل مجموعة من المعلومات بنوع محدد من الجرائم الماسة بالمستند الإلكتروني، فمثلًا يحدد هذا النموذج قائمة بالأماكن المعتادة التي يمكن العثور فيها على الملفات المخفية والملغاة، وأيضًا يحدد أنواع المعلومات الأخرى مثل الصور وكلمات السر أو أرقام بطاقات الهوية مثل رقم الضمان الآلي، وهي معلومات مفيدة في عمليات التحري في بعض الأنواع من الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، فالتعرف على أنواع المعلومات المفيدة وأماكن إخفائها يعتبر خطوة إيجابية تساعد على تقديم أدلة قانونية يعتد بها عند تقديم الجناة للمحكمة أمام القضاء.[4]

ب- أدوات جمع الدليل الإلكتروني:

يقوم الخبير التقني في سبيل تحري الحقيقة الإستعانة بكل ما يمكنه من التوصل إلى الدليل الإلكتروني، ومن بين هذه البرمجيات ما يلي:

ب-1- برنامج اذن التفتيش:

برنامج اذن التفتيش (Computer Scorch Warrant Program) هو برنامج قاعدة بيانات يسمح بإدخال كافة المعلومات الأساسية اللازمة لترقيم الأدلة وتسجيل المعطيات منها،

[1]- محمود سعد عبد المجيد، مرجع سابق، ص 503.
[2]- نفس المرجع، ص 504.
[3]- براهيمي جمال، مرجع سابق، ص 76.
[4]- أحمد يوسف الطحطاوي، مرجع سابق، ص 326.

ويمكن لهذا البرنامج إصدار إيصالات لتسليم الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد موضع دليل معين أو تحديد ظروف ضبط هذا الدليل.[1]

ب-2- قرص بدء تشغيل الحاسوب:

يجب تأمين قرص بدء تشغيل الحاسوب (Bootable Diskette) ليتمكن تشغيل الحاسوب، حيث يعتبر هذا القرص ضروريًا لعملية بدء تشغيل الحاسوب إذا كان نظام التشغيل فيه محميًا بكلمة مرور، ويجب أن يكون القرص مزودًا ببرنامج مضاعفة المساحة (Double space) فربما كان المتهم قد إستخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.[2]

ب-3- برنامج معالجة الملفات:

برنامج معالجة الملفات مثل برنامج (X tree Pro Gold)، يمكن من العثور على الملفات الرقمية في أي مكان على الشبكة، ويستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن إستخدمه للبحث عن كلمات معينة أو عن أسماء ملفات أو غيرها مما له صلة بالأمر.[3]

ب-4- برنامج النسخ:

برنامج النسخ مثل برنامج (Lap Link) هو برنامج يسمح بنسخ المعطيات من الجهاز الإلكتروني الخاص بالمتهم ونقلها إلى جهاز آخر من خلال المنفذ المتتالي (Serial Port) أو سواء على المنفذ المتوازي (Parallel Port)، وهذا البرنامج مفيد جدًا للحصول على نسخة من المعلومات قبل أي محاولة محوها أو تدميرها من جانب المجرم المعلوماتي.[4]

ب-5- برامج كشف الديسك:

برامج كشف الديسك مثل برنامج (AMA Disk, View disk)، يمكن من خلال هذا البرنامج الحصول على محتويات أجهزة التخزين مهما كان أسلوب تهيئته، وهذا البرنامج توجد منه نسخة عادية تصلح للأفراد العاديين ونسخة خاصة للسلطة القضائية المختصة ويمكن الحصول عليه من شركة (Sydex Software).[5]

ب-6- برنامج الدمج وفك الدمج:

برنامج الدمج وفك الدمج (pkzip)، يستخدم هذا البرنامج في دمج الملفات أو تفكيكها، فقد يكون المجرم المعلوماتي قد قام بدمج برامجه فلا يمكن الإطلاع عليها إلا بعد فك الدمج.[6]

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 150.

[2]- نفس المرجع، ص-ص 150-151.

[3]- أحمد يوسف الطحطاوي، مرجع سابق، ص323.

[4]- نفس المرجع، ص323.

[5]- محمد حسن السراء، **الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية**، القيادة العامة لشرطة الشارقة مركز بحوث الشرطة، الفكر الشرطي، المجلد 21، العدد 02، 2012، الإمارات العربية المتحدة، ص- ص 45-46.

[6]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 173.

ب-7- برنامج إلتقاط فحص ضد الشبكة:

برنامج (Visual route5.2a) عبارة عن برنامج يكشف عن الهجمات أو برامج مراقبة الشبكة، فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها المسح والمناطق التي تم فيها الهجوم، وبعد معرفة عنوان (IP) إسم الجهة يرسم البرنامج خطًا يوضح من خلاله مسار الهجوم بين مصدره والجهة التي إستهدفها الهجوم.[1]

ب-8- برامج إتصالات:

برامج إتصالات مثل برامج (LANtastic)، يستطيع ربط جهاز الخبير أو جهات التحري والتحقيق بجهاز المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات، ثم يحفظ في دعامة إلكترونية.[2]

ج- خطوات إشتقاق الدليل الإلكتروني:

لما كانت عملية جمع الأدلة الإلكترونية تعد من أهم وأصعب الأمور التي تواجه الخبير التقني، كان لزامًا عليه أن يتبع عدة خطوات من أجل إشتقاق هذا النوع المستحدث من الأدلة، وتتمثل هذه الخطوات في ما يلي:

ج-1- خطوات ما قبل التشغيل والفحص:

- التحقق من مطابقة محتويات المضبوطات وفقًا لما هو مدون عليها؛
- التأكد من صلاحية مكونات نظام الأجهزة الإلكترونية المتعلقة بالجريمة للتشغيل؛
- توثيق وتسجيل معطيات المكونات المضبوطة، كالنوع والطراز والرقم التسلسلي.[3]

ج-2- خطوات التشغيل والفحص:

- إستكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز؛
- عمل نسخة على وسائط التخزين المضبوطة لإجراء عملية الفحص المبدئي على هذه النسخة، لحماية النسخة الأصلية من أي فقد أو تلف أو تدمير، سواء من سوء الإستخدام أو لوجود قنابل برامجية أو فيروسات[4]؛
- تحديد أنواع وأسماء المجموعات البرمجية، وبرامج النظام برامج التشغيل، وبرامج التطبيقات، وبرامج الإتصالات، أو ما إذا كان هناك نوع معين من البرامج ذات دلالة بموضوع الجريمة الماسة بالمستند الإلكتروني[5]؛

---

[1]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 173.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 152.

[3]- براهيمي جمال، مرجع سابق، ص- ص 76-77.

[4]- عائشة بن قارة مصطفى، مرجع سابق، ص 148.

[5]- أحمد يوسف الطحطاوي، مرجع سابق، ص 327.

- تحديد ما إذا كان هناك برامج أو ملفات رقمية أو معلومات أو معطيات، ذات صلة وثيقة بموضوع الجريمة الماسة بالمستند الإلكتروني[1]؛
- إظهار الملفات المخبأة والنصوص المخفية داخل الصور[2]؛

- يتم إعداد قائمة يجد فيها الخبير كل الأدلة الإلكترونية التي تم الحصول عليها في الدعامة الإلكترونية الخاصة به، مع إجراء مراجعة لكل صورة محتفظ بها في جهاز إلكتروني آخر للتأكد من سلامة القائمة[3]؛

- تحويل الدليل الإلكتروني إلى هيئة مادية[4]، وذلك عن طريق تصوير محتواها إذا كانت صور أو نصوص أو طباعة الملفات الرقمية أو وضعها في أي دعامة إلكترونية حسب نوع المعطيات والمعلومات المكونة للدليل[5].

كل ما تم ذكره سابقًا، يمكن أن يتم بنجاح على النسخ طبق الأصل، لكن عند إسترجاع الملفات التي تم محوها من على الأصل وذلك بإستخدام أحد برامج إستعادة المعطيات، وكذلك بالنسبة للملفات المعطلة أو التالفة مثل برنامج (Easy Recover 4 all Professional)، ولكن الجهات المتخصصة دائمًا تحرص على إستخدام أحدث البرامج وقد تطور لنفسها برامج خصيصًا لذلك، وبعد ذلك يتم تخزين هذه الملفات أو المعطيات ويعمل لها نسخ طبق الأصل أخرى من الأسطوانة أو القرص المحتوى لها لفحصها عن طريق تطبيق الخطوات السالفة الذكر التي تتم على النسخ طبق الأصل.[6]

ج-3- تحديد مدى الترابط بين الدليل المادي والدليل الإلكتروني:

يتم فحص كلا من الدليل المادي المضبوط والدليل الإلكتروني في صورته الملموسة الموجود في الملفات التي تم ضبطها وبذلك يكون تم الربط بينهما، مما يكسب الدليل المصداقية والموثوقية واليقينية اللتان تؤديان إلى قبوله لدى السلطة القضائية المختصة.[7]

---

[1]- أحمد يوسف الطحطاوي، مرجع سابق، ص 327.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 149.

[3]- نفس المرجع، ص 149.

[4]- أن أغلب المعطيات المخزنة التي تتداول عبر الأجهزة الإلكترونية تكون على هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة، بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الأجهزة الإلكترونية، لذا يتطلب الإستعانة بأجهزة وأدوات التقنية وإستخدام برامج معلوماتية ملائمة للإطلاع عليه أو إستخراجه في هيئة ملموسة أو مادية، وهي تعد أساليب علمية، إلا أن ترجمته وإخراجه في شكل مادي ملموس لا يعني أن هذا التجميع المادي هو الدليل، بل أن هذه العملية ليست سوى عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الإستدلال بها على معلومة معينة، وللمزيد من التفصيل، ينظر: بوشارب هانية، بن شهرة شول، **صعوبة عملية إستخلاص الدليل الإلكتروني**، جامعة عمار ثليجي-الأغواط، مجلة الدراسات القانونية والسياسية، المجلد09، العدد01، جانفي 2023، الجزائر، ص 69.

[5]- عائشة بن قارة مصطفى، مرجع سابق، ص 149.

[6]- أحمد يوسف الطحطاوي، مرجع سابق، ص 328.

[7]- عائشة بن قارة مصطفى، مرجع سابق، ص 149.

ج-4- مرحلة تدوين النتائج وإعداد التقرير:

يتم إعداد تقرير لجميع الخطوات والإجراءات المتبعة لإستخلاص الدليل الإلكتروني، ويرفق به في الغالب الملاحق الإيضاحية لإعتمادها ثم تصديرها إلى السلطة القضائية المختصة.[1]

ثالثًا: وسائل الخبير التقني في إكتشاف الدليل الإلكتروني

توجد وسائل يمكن أن تساعد الخبير في جمع الأدلة التي تساهم في كشف كيفية وقوع الجرائم الماسة بالمستند الإلكتروني وتحديد المجرم المعلوماتي، وهي كما يأتي:

1-الوسائل المادية:

هي الأدوات الفنية التي يستخدمها الخبير عادة في بنية نظام المعلومات، والتي يمكن بإستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة التي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها[2]، ومن أهم هذه الوسائل:

أ- عنوان بروتوكول الإنترنت (IP):

تستعين السلطات القضائية المختصة عادة بنظام فحص الإلكتروني لتحديد موقع جهاز مصدر السلوك الإجرامي، الذي يتم بواسطته تتبع الحركة العكسية لمسار الإنترنت أو الحركة التراسلية للسلوك الممارس عبر الإنترنت إلى غاية الوصول إلى العنوان الرقمي للجهاز يسمى ((adresse internet protocole (IP)، وهذا الأخير هو عبارة عن بروتوكول لتحديد المعطيات والمواقع على شبكة الإنترنت والذي يتم التعرف بمقتضاه على الجهاز المتصل بشبكة الإنترنت من خلال عناوين عددية، ولكل الجهاز الإلكتروني عنوان خاص به يسمى (IP adresse).[3]

بروتوكول الإنترنت (IP)[4] هو المسؤول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها وهو يشبه إلى حد كبير عنوان البريد العادي حيث يتيح للموجهات

---

[1]-عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة**، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، 12-14 نوفمبر 2008، الرياض- المملكة العربية السعودية، ص 36.

[2]- خالد ممدوح إبراهيم، **الخبرة القضائية الرقمية في الجرائم المعلوماتية دراسة مقارنة في القانون المصري والإماراتي والأمريكي**، مرجع سابق، ص173.

[3]- براهيمي جمال، مرجع سابق، ص- ص 201-202.

[4]- أشير في المؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلو في الفترة ما بين 29 و31 ماي 2000 موضوع عدم إمكانية البنية التحتية للإنترنت من التوصل إلى تحديد شخصية مرتكب الجريمة أو المصدر الحقيقي لها، وإن كانت توفر إمكانية التعرف على عنوان ورقم الجهاز الإلكتروني فقط المرتبط بالإنترنت والمستعمل كوسيلة لإرتكاب الجريمة عن طريق عنوان IP، الذي يشير إلى رقم يعين الجهاز الإلكتروني الموصول على الأنترنت. لكن في مقابل ذلك فإن هذا الرقم ليس موحدًا على المستوى العالمي، بالإضافة إلى أن مصداقية الهوية عبر الإنترنت IP تتقلص كثيرًا في بعض الدول، إذا علمنا أن كل خط هوية على الإنترنت يصادفه عدد من الهويات التي يمكن أن تكون محلًا للتغاير بين أعضاء الإنترنت المشتركين في مزود خدمة واحد، ذلك أن أي شخص يملك هوية رقمية محددة حقًا حال وجوده على الإنترنت، إلا أنه إذا حدث وإنقطع الإرسال فإن=

والشبكات المعنية نقل الرسالة وهو يوجد بكل جهاز مرتبط بالإنترنت[1]، ويتكون من أربعة أجزاء وكل جزء يتكون من أربع خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية والجزء الثاني لمقدم الخدمة والثالث لمجموعة الأجهزة الإلكترونية المرتبطة والرابع يحدد الجهاز الذي تم الإتصال منه[2].

ويعمل بروتوكول (IP) بشكل متزامن مع بروتوكول التحكم بالنقل ((TCP) -Trams Commission Protocol)، وهذان البروتوكولان (TCP/IP) هما من عائلة بروتوكولات الإتصال بين عدة أجهزة طورت أساسًا لنقل المعطيات بين أنظمة (UNIX) ثم أصبحت المقياس المستخدم لنقل المعطيات الرقمية عبر شبكة الإنترنت، ويرتكز البروتوكولان معًا (TCP/IP) على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Pachet) بين مختلف الوصلات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها، وحزمة المعلومات تمثل جزء من ملف معلوماتي ذات حجم مصغر ثابت تحمل كل منها رقمًا خاصًا ومعلومات تعريفية بكل من الجهاز المرسل والمرسل إليه، وعند كل وصلة تتم قراءة جهة المرسل إليه ثم تتم إعادة إرسال الحزمة المارة عبرهما نحو الوصلات التالية الأقرب إلى جهة المقصد أو المرسل إليها النهائية[3].

وفي حالة وقوع الجريمة الماسة بالمستند الإلكتروني فيمكن للخبير إتباع المسار التراسلي للبروتوكول (IP) للبحث عن رقم الجهاز المستعمل في إرتكاب الجريمة ومن ثم تحديد موقعه[4]

=الشخص نفسه إذا عاد من جديد إلى الإنترنت، فإن الهوية السابقة لن تكون له وإنما لغيره ومن الممكن جدًا أن يتواجد بهوية IP أخرى، وللمزيد من التفصيل، ينظر: سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص-ص 193-194.

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص 175.

[2]- خالد ممدوح إبراهيم ، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 304.

[3]- براهيمي جمال، مرجع سابق، ص 202.

[4]- من التدابير الأمنية التي من الممكن أن يستخدمها الجناة لإعاقة الوصول إليهم وبالتالي نزع كل صلة بينهم وبين فعلهم الإجرامي، إخفاء هوية المستخدم بإستخدام مختلف أدوات الإتصال أمرًا متاحًا، ومن بين الأدوات التي تستخدم لهذا الغرض برنامج بسيفون (pasiphon) وشبكة تور (Tor)، والهدف من هذا الإجراء هو عرقلة تتبع عنوان بروتوكول الإنترنت (IP) لهذا المستخدم، ويزداد الأمر صعوبة حينما تكون المعلومات المحملة في عناوين (IP) غير حقيقية أو زائفة وهذا ممكن حين إستخدام الحزم المعلوماتية (Packet) عنوان (IP) زائف، بحيث يظهر أن المعلومات جاءت من نظام معالجة محدد بينما في الحقيقة جاءت من جهاز آخر، ومثال ذلك عندما يقوم برنامج خبيث بإدخال معلومات كاذبة أو غير حقيقية عن عنوان (IP) في حزم الإرسال وقبل الولوج في الشبكة المعلوماتية أو نتيجة إستخدام الجاني جهازًا آخر غير جهازه الشخصي، كإستخدام الأجهزة الموجودة بالأماكن العامة أو اللجوء إلى مقاهي الإنترنت، على إعتبار أن جل هذه المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هوياتهم، أو نتيجة تردد عدد كبير من الأشخاص على المكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط بين زمن إرتكابها وبين حدوث النتيجة الإجرامية كما هو الحال بالنسبة لمقاهي الإنترنت، مما يفسح المجال لحدوث تغيرات أو عبث في الآثار المادية للجريمة أو زوال بعضها، وهو ما يلقي ظلالًا من الغموض على الدليل، وهو ما أستغله مرتكبوا الجرائم المعلوماتية لطمس هوياتهم، وإرتكاب جرائمهم دون إمكانية التعرف عليهم بسهولة، وهو ما جعل إخفاء الهوية من أهم العوائق التي تواجه العاملين في مجال التحري والتحقيق عن هذه الجرائم، بحيث يصب تحديد مرتكب الجريمة أو موقعه، وللمزيد من التفصيل، ينظر: بوشارب هانية، بن شهرة شول، **صعوبة عملية إستخلاص الدليل الإلكتروني**، مرجع سابق، ص 73.=

ومنه معرفة الجاني[1]، ويمكن لمقدم خدمة الإنترنت أن يراقب المشترك كما يمكن للشبكة التي تقدم خدمة الإتصال الهاتفي أن تراقبه أيضًا إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك[2].

وتوجد أكثر من طريقة يمكن من خلالها معرفة العنوان الخاص بالجهاز الإلكتروني في حالة الإتصال المباشر، منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل (WINDOWS) حيث يتم كتابة (WINPCFG) في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP)، مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل إتصال بشبكة الإنترنت.[3]

ومن هذه الوسائل أيضًا البريد الإلكتروني وبرامج المحادثة كما في حالة إستعمال أحد البرامج التحادثية كأداة للجريمة فإنه يتطلب تحديد هوية المتصل وتحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى ولو لم يدون معلوماته في خانة المرسل، شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة.[4]

ب- برنامج البروكسي:

يشتغل برنامج البروكسي (PROXY) كوسيط بين المستخدم والإنترنت، بحيث يضمن مقدمي خدمات الإنترنت على ضمان الأمن وتوفير خدمات الذاكرة الجاهزة[5] وذلك إختصارًا للوقت اللازم للوصول إلى موقع معين على شبكة الإنترنت عند تكرار الولوج إليه، وهو وسيط يسمح بالربط بين الشبكات لتعزيز قدرتها على إدارة الشبكة[6].

وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبًا من المستخدم للبحث عن صفحة ما ضمن الذاكرة (Cache) المحلية المتوفرة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل ليقوم بإرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية وفي هذه الحالة يستخدم البروكسي كمزود للعميل ويستخدم أحد عناوين بروتوكول الإنترنت (IP)، ومن أهم مزايا هذا النظام أن الذاكرة (Cache) المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت

=برتوكول الإنترنت (TCP/IP) الذي يكشف عن الجهاز المرتكب بواسطته الجريمة المعلوماتية ليس موحدًا على المستوى العالمي وليس لصيقًا به بصفة دائمة، بل هو قابل للتغير مع كل إتصال بشبكة الإنترنت. لأن كل خط هوية على الإنترنت (IP) يصادفه عدد من الهويات التي يمكن أن تكون محلًا للتغير بين أعضاء الإنترنت المشتركين في مزود إنترنت واحد، فمثلًا عندما يتصل شخص من الجزائر بالإنترنت تمنح له فورًا هوية رقمية خاصة به، ولكن إذا حدث إنقطاع في الإرسال وقام بعدها هذا الشخص بإعادة الإتصال بالإنترنت مرة ثانية، فإن ذلك يفقده هويته السابقة ليجد نفسه بهوية (IP) أخرى، وللمزيد من التفصيل، ينظر: براهيمي جمال، مرجع سابق، ص-ص 203-204.

[1]- بوشارب هانية، بن شهرة شول، **صعوبة عملية إستخلاص الدليل الإلكتروني**، مرجع سابق، ص 78.

[2]- رفاه خضير جياد العارضي، مرجع سابق، ص 175.

[3]- خالد ممدوح إبراهيم ، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 304.

[4]- رفاه خضير جياد العارضي، مرجع سابق، ص-ص 175-176.

[5]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 173.

[6]- بلحسيني حمزة، مرجع سابق، ص 370.

عليها، مما يجعل دوره قوي وفعال في الإثبات عن طريق فحص تلك العمليات المحفوظ بها والتي تخص المتهم والموجودة عند مقدم الخدمة.[1]

وقد طبقت دولة الإمارات العربية المتحدة هذا النظام الذي يقوم بمراجعة نوعية الخدمات المقدمة عبر شبكة الإنترنت، فعندما يطلب المشترك موقعًا ما على الشبكة تصل الإشارة إلى الرقيب الذي يقوم بدوره بعرض الموضوع على قائمة كبيرة جدًا من المواقع الممنوعة، فإذ تبين له أن الموقع المطلوب يدخل ضمن هذه القائمة المحظورة فلا يستطيع المشترك الحصول على هذا الموقع، ومن أهم مزاياه أن ذاكرة (Cache) المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل أثرها قويًا في الإثبات عن طريق فحص تلك العمليات المحفوظة بها التي تخص المتهم والموجودة عند مقدم الخدمة.[2]

ج- نظام (Honey pot):

وهو نظام حاسوبي مصمم خصيصًا لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية معطيات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه إنطباعًا خاطئًا بسهولة الإعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الإعتداء على أي جهاز آخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الإعتداء وتحليلها وبالتالي إتخاذ تدابير وقائية فعالة، وهذه المعلومات التي تم جمعها تفيد في تحليل أبعاد الجريمة في حال وقوعها وتعطي فريق التحقيق بالعديد من المعطيات التي توضح معالم الجريمة.[3]

د- برامج تتبع الإختراق:

يستطيع الخبير التقني أن يتتبع أثر مخترقي المنظومة المعلوماتية عن طريق برامج تمكن من التعرف على أي محاولات الإختراق التي تمت وتقدم بيانًا شاملًا لمستخدم الجهاز الإلكتروني الذي تم إختراقه، ويحتوي هذا البيان على إسم الحدث وتاريخه وعنوان بروتوكول الإنترنت (IP) الذي تمت من خلاله عمليات الإختراق، وكذا إسم الشركة المزودة لخدمة الإنترنت والمستضيفة للمخترق وأرقام مداخلها ومخارجها على شبكة الإنترنت بالإضافة إلى معلومات أخرى.[4]

---

[1]- خالد ممدوح إبراهيم، **الخبرة القضائية الرقمية في الجرائم المعلوماتية دراسة مقارنة في القانون المصري والإماراتي والأمريكي**، مرجع سابق، ص175.

[2]- رفاه خضير جياد العارضي، مرجع سابق، ص 176.

[3]- علي عدنان فيل، مرجع سابق، ص 72.

[4]- بلحسيني حمزة، مرجع سابق، ص 370.

ر- نظام كشف الإختراق:

نظام كشف الإختراق (intrusion Detection System) ويرمز له إختصارًا بالأحرف (IDS)، وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على الأجهزة الإلكترونية أو الشبكة مع تحليلها، بحثًا عن أية إشارة قد تدل على وجود مشكلة قد تهدد من الجهاز أو الشبكة.[1]

ويتم ذلك من خلال تحليل رزم البيانات أثناء إنتقالها عبر الشبكة ومن ببعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها في الجهاز الإلكتروني أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للإعتداءات على الأنظمة المعلوماتية والتي يطلق عليها أهل الإختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبعدة طرق ويسجل المعطيات الخاصة بهذا الإعتداء في سجلات إلكترونية خاصة.[2]

ح- أدوات تدقيق ومراجعة العمليات الحاسوبية:

أدوات تدقيق ومراجعة العمليات الحاسوبية (Auditing Tools) هي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسبة إلكترونية معينة وتسجيلها في ملفات خاصة يطلق عليها (Logs)، والكثير من هذه الأدوات تأتي مضمنة في أنظمة التشغيل المختلفة، وبعضها يأتي كبرامج مستقلة يتم تركيبها على أنظمة التشغيل بعد إعدادها للعمل، وكل ما يحتاجه الأمر هو قيام مدير الشبكة أو النظام بتفعيلها وإعدادها للعمل في وقت مبكر وسابق لإرتكاب الجريمة، حتى يمكن أن تقوم بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة ربما ساعدت في كشف أسلوب الجريمة وشخصية مرتكبها، ومن الأمثلة على هذه الأدوات أداة (Event Viewer) لبيئة النوافذ وأداة (Syslogd) لبيئة يونيكس.[3]

خ- أدوات الضبط:

تتمثل في برامج الحماية وأدوات المراجعة وأدوات مراقبة المستخدمين للشبكة وبرامج التنصت على الشبكة والتقارير التي تنتجها نظم أمن البيانات ومراجعة قاعدة البيانات وبرامج النسخ الإحتياطي[4] التي تستخدم لعمل نسخة مطابقة تمامًا للأقراص الصلبة الموجودة في الحاسبات الإلكترونية محل التحقيق وعلى مستوى (Bit stream Backup)، بغرض عمل الفحوصات الجنائية عليها دون تعريض الأقراص الأصلية لأي تغير في البيانات الموجودة[5]،

---

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 306.

[2]- نفس المرجع، ص-ص 306-307.

[3]- علي عدنان فيل، مرجع سابق، ص 73.

[4]- ناني لحسن، **التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية**، د.ر.ط، 2018، النشر الجامعي الجديد، تلمسان-الجزائر، ص 75.

[5]- علي عدنان فيل، مرجع سابق، ص 73.

ومن أشهر هذه البرمجيات برنامج (Safe back) وبرنامج (Encase) وتعمل في بيئة وندوز وكذلك أداة (DD) لبيئة يونيكس والتسجيل وغيرها من الأدوات مثل (IDS).[1]

ج- الوسائل المساعدة للتحقيق:

من بين هذه الوسائل الأدوات المستخدمة في إسترجاع المعلومات من الأقراص التالفة وبرامج كسر كلمات المرور وبرامج الضغط وفك الضغط وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسوب وبرامج نسخ المعطيات، وأيضًا من الأدوات المهمة والتي تساعد جدًا في عملية التحقيق برامج منع الكتابة على القرص الصلب وذلك بعد إرتكاب الجريمة مما يساعد في المحافظة على مسرح الجريمة.[2]

البرامج التي تساعد على إسترجاع الملفات والمعلومات التي قد يلجأ الجاني إلى حذفها نهائيًا من الجهاز الإلكتروني فمن أشهرها على سبيل المثال برنامج (Get Free) لبيئة النوافذ وبرنامج (Extractor) لبيئة يونيكس، وهناك أيضًا برمجيات تحرير الملفات الست عشرية (Hexadecimal Editors) وهي برامج تمكن من الإطلاع على محتوى كل ملف حاسوبي بشكله الثنائي تمنح مزيدًا من القدرة على تحليل الملف والتعرف على طبيعة المعطيات التي يحتويها[3]، وهناك برمجيات البحث عن المفردات النصية والتي تستخدم في البحث عبر البيانات عن تلك الملفات التي تحتوي على مفردات معينة عادة ما يكون لها علاقة بالقضية ومن الأمثلة عليها برنامج (Et search) وبرنامج (String Search).[4]

و- أدوات فحص ومراقبة الشبكات:

هذه الأدوات تستخدم في فحص بروتوكول (TCP/IP) وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها مثل أداة (ARP)، ووظيفتها تحديد مكان الجهاز فيزيائيًا على الشبكة برنامج (Visual Route 5.2a) وهو أداة للتتبع، أما برنامج (NET STAT) فهو أداة لفحص حالة الإتصال الحالي للبروتوكول (TCP/IP).[5]

2- الوسائل الإجرائية:

يقصد بالوسائل الإجرائية الإجراءات التي تستخدم في تنفيذ طرق التحقيق الثابتة والمتغيرة والمحددة وغير المحددة التي تثبت وقوع الجريمة وتحديد شخصية مرتكبيها[6]، وتتمثل في ما يلي:

---

[1]- علي عدنان فيل، مرجع سابق، ص 74.
[2]- ناني لحسن، مرجع سابق، ص 74.
[3]- علي عدنان فيل، مرجع سابق، ص 74.
[4]- نفس المرجع، ص 75.
[5]- ناني لحسن، مرجع سابق، ص 74.
[6]- خالد ممدوح إبراهيم، **الخبرة القضائية الرقمية في الجرائم المعلوماتية دراسة مقارنة في القانون المصري والإماراتي والأمريكي**، مرجع سابق، ص177.

أ- إقتفاء الأثر:

هناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل في طياتها العديد من النصائح أولاها نصيحة "قم بمسح آثارك (Cover Your Tracks)"، ذلك أنه لو لم يقم المخترق بمسح آثاره فإنه من المؤكد أنه سوف يتم التوصل إليه والقبض عليه حتى وإن كانت عملية الإختراق قد تمت بشكل سليم، هذا ويمكن للخبير التقني تقصي الأثر بعدة طرق سواء عن طريق بريد الإلكتروني الذي تم إستقباله أو عن طريق تتبع أثر الجهاز الذي تم إستخدامه للقيام بعملية الإختراق.[1]

أي عن طريق الآثار المعلوماتية التي يتركها مستخدم الإنترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الإتصالات التي تمت من أي جهاز من الأجهزة الإلكترونية، ويلاحظ أن الآثار المستخلصة من الجهاز الإلكتروني يمكن أن تكون مفيدة لما تحتويه من معلومات مثل صفحات المواقع المختلفة والبريد الإلكتروني والفيديو الرقمي وغرف الدردشة والمحادثة والملفات المخزنة في الجهاز الشخصي والصور المرئية وكذا الدخول للخدمة والإتصال بالإنترنت عن طريق مقدم الخدمات وغيرها، لذلك فإن هذه الآثار تشمل رؤية لمسرح الجريمة المادي ومسرح الرقمي نفسه فإذا كانت هناك جريمة حدثت فعلًا في العالم الحقيقي، وإستخدام الجهاز الإلكتروني بطريقة ما في أحد أفعالها فإن السلطة القضائية المختصة أو مقتفي الأثر الجنائي يجب عليهم أن يبحثوا في كلا المسرحين المادي والرقمي للعثور على الدليل[2].

ب- الإطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته:

ينبغي الإطلاع على المنظومة المعلوماتية ومكوناتها من شبكات وتطبيقات وخدمات تقدم للعملاء، كما ينبغي الإطلاع على عمليات المنظومة المعلوماتية كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة، ومدى مزامنة الأجهزة ومدى تخصيص وقت معين في اليوم يسمح بإستخدام كلمات المرور ومدى توزيع الصلاحيات للمستفيدين وإجراءات أمن العاملين وأسلوب النسخ الإحتياطي، والإستعانة ببرامج الحماية كمراقبة المستفيدين والموارد والبرامج التي تعالج المعطيات وتسجيل الوقائع وحالات فشل الدخول إلى المنظومة[3]، بالإضافة إلى معرفة نوعية برامج الحماية وأسلوب عملها والإستفادة من التقارير التي تنتجها نظم أمن البيانات وتقارير جدران الحماية[4].

---

[1]- خالد ممدوح إبراهيم، **الخبرة القضائية الرقمية في الجرائم المعلوماتية دراسة مقارنة في القانون المصري والإماراتي والأمريكي**، مرجع سابق، ص-ص 177-178.

[2]- رفاه خضير جياد العارضي، مرجع السابق، ص 177.

[3]- خالد ممدوح إبراهيم ، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع السابق، ص 308.

[4]- علي عدنان فيل، مرجع السابق، ص 77.

ج- الإستعانة بالذكاء الإصطناعي:

أثبتت تجارب إستخدام التقنيات المعلوماتية نجاحها في جمع الأدلة الجنائية وتحليلها وإستخلاص الحقائق منها، وعليه يمكن للخبير الإستعانة بالذكاء الإصطناعي في حصر الفرضيات والإحتمالات والأسباب والحقائق ومن ثم يتم الوصول إلى نتائج معينة على ضوء معاملات حسابية يتم تحليلها بالجهاز الإلكتروني وفق برامج تم تصميمها خصيصًا من أجل هذا الغرض.[1]

الأنظمة الخبيرة (Expert Systems)[2] هي نوع من أنظمة الذكاء الإصطناعي، هي تقنية تبحث في كيفية نقل خبرة الفرد والمعارف السابقة في برامج معلوماتية قد تحل محل الخبير البشري أو تساعد في إتخاذ القرار كأقل تقدير، وتعرف كذلك بإسم الأنظمة ذات الأساس المعرفي (Knowledge Based systems) وهي الشكل الأكثر بروزًا في مجال الأنظمة الخبيرة، وهي برامج معلوماتية تتضمن معارف وقدرات تحليلية للخبير في تخصص معين بغية إستخلاص معارفه وتجاربه السابقة في ميدان معين ونقلها للجهاز الإلكتروني بطريقة تجعلها متاحة للمستخدمين الأقل خبرة.[3]

المطلب الثاني: الأجهزة المختصة وطنيًا في التحقيق الجنائي في جرائم المستند الإلكتروني

تعد الجرائم الماسة بالمستند الإلكتروني من القضايا ذات الطبيعة الفنية في غاية التعقيد نظرًا لكونها غالبًا ما تكون جرائم غير مرئية، مما يستدعي إسناد مهام التحري والتحقيق فيها إلى أجهزة تتمتع بالكفاءة والتكوين المتخصص والمعرفة التقنية الدقيقة ما يؤهلها لقدرة التعامل مع هذا النوع المستحدث من الإجرام، مما سوف نحاول أن نلقي الضوء على هذه الأجهزة في ما يلي:

---

[1]- بلحسيني حمزة، مرجع السابق، ص 371.

[2]- الأنظمة الخبيرة نظام مبني على المعرفة مصمم لنمذجة قدرة الخبير الإنساني على حل المشكلات، وشكلًا متطورًا من أشكال الذكاء الإصطناعي والتي إستندت في بناء النظم على مبدأ شبيه بمنطق التفكير الإنساني، وطرق ذات مواصفات ذكية تعتمد على الجهاز الإلكتروني، تفاعلية وموثوقة يمكنها إتخاذ القرارات في أي وقت، وتتميز بقدرتها على حل جميع المشكلات المعقدة، فمرحلة إتخاذ القرار هي المستوى الأكثر أهمية للذكاء والخبرة البشرية مع هذه الأنظمة، حيث يحاكي الذكاء الإصطناعي هذه العمليات بأسلوب حديث ومتقدم، وعندما نتحدث عن أنظمة خبيرة فإننا نعني حل المشكلات الأكثر تعقيدًا في مجال معين، أي يتضمن برنامج الذكاء الإصطناعي ما يكفي من المعرفة المخزنة لحل المشكلات المعقدة التي لا يستطيع البشر حلها، وبالتالي يأتي دورالخبير البشري في تحقيقها، وللمزيد من التفصيل، ينظر: محمد سحنوني، رياض بن غبريد، **الذكاء الإصطناعي والتطورات المستقبلية**، كتاب جماعي دولي بعنوان: **الجوانب القانونية للتكنولوجيا الحديثة والذكاء الإصطناعي**، الطبعة الأولى، أوت 2023، المركز المغاربي-شرق أدنى للدراسات الإستراتيجية، المملكة المتحدة- بريطانيا-، ص-ص 17-18.

[3]- روابح عبلة، **المفاهيم الأساسية للذكاء الإصطناعي وتطبيقاته المختلفة**، كتاب جماعي دولي بعنوان: **الجوانب القانونية للتكنولوجيا الحديثة والذكاء الإصطناعي**، الطبعة الأولى، أوت 2023، المركز المغاربي-شرق أدنى للدراسات الإستراتيجية، المملكة المتحدة - بريطانيا-، ص 7.

الفرع الأول: الوحدات التابعة للأمن الوطني

إن من بين الأهداف الإستراتيجية التي يسعى إلى تحقيقها كشف الجريمة والقبض على مرتكبيها والوقاية والحد منها وحماية الحريات وصون الحقوق والإستعداد لمواجهة الأزمات والكوارث بفعالية، من أجل الضبط الجيد للأمن وحفظ النظام العام وأداء جميع المهام المسندة للأمن الوطني كما حددها التشريع والتنظيم المعمول بهما.[1]

أولًا: المعهد الوطني للبحث في علم التحقيق الجنائي

تم إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي بموجب المرسوم الرئاسي رقم: 04-432 المؤرخ في 29 ديسمبر 2004 المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي[2]، وتم تنظيم المصالح والأقسام والمخابر الجهوية للمعهد بموجب قرار وزاري مشترك المؤرخ في 14 أفريل 2007[3]، والذي يضم مصلحة الخبرات الخاصة بالدلائل التكنولوجية التابعة للقسم التقني للمعهد[4]، وكذلك مخبر الأدلة المعلوماتية، وجرائم الكمبيوتر، ومخبر إستغلال الهواتف المحمولة التابع للمصلحة التقنية للمخبر الجهوي[5].

المعهد الوطني للبحث في علم التحقيق الجنائي هو عبارة عن مؤسسة عمومية ذات طابع إداري يتمتع بالشخصية المعنوية والإستقلال المالي[6]، ويوضع تحت وصاية الوزير المكلف بالداخلية ويتبع المديرية العامة للأمن الوطني[7]، ويتولى المهام الآتية:

- تحليل المؤشرات المادية التي يتم جمعها بمناسبة معاينة المخالفات والتحريات التي تتطلب مشاركة مختلف التخصصات التقنية والعلمية بناء على طلب من السلطات القضائية المختصة؛
- إعداد تقارير الخبرة بناء على طلب من السلطات المختصة المؤهلة قانونًا؛
- القيام بأعمال التكوين وتجديد المعارف وتحسين المستوى والتكوين ما بعد التدرج في ميداني علم التحقيق الجنائي والإجرام؛
- المساهمة في وضع مراجع أساسية في مجال علم التحقيق الجنائي؛

---

[1]- شنتير خضرة، مرجع سابق، ص-ص 202-203.

[2]- المرسوم الرئاسي رقم: 04-432 المؤرخ في 29 ديسمبر 2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، ج.ر.ج.ج.ش العدد 84، الصادرة بتاريخ 29 ديسمبر 2004.

[3]- القرار الوزاري المشترك المؤرخ في 14 أفريل 2007، المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، ج.ر.ج.ج.ش العدد 36، الصادرة في 03 جوان 2007.

[4]- تنص المادة 05 من القرار الوزاري المشترك السالف الذكر على ما يلي: "...مصلحة الخبرات الخاصة بالدلائل التكنولوجية تكلف بما يأتي: "تحليل بطلب من السلطات القضائية المختصة الدلائل المادية التي تم جمعها إثر معاينة المخالفات والتحريات، في ميادين الدلائل المعلوماتية، وجرائم الكمبيوتر، والبصمات الصوتية، ومعالجة الصورة والإشارة، وإستغلال الهواتف المحمولة، وإعداد تقارير الخبرة...".

[5]- المادة 10 من المرسوم الرئاسي رقم: 04-432 السالف الذكر.

[6]- المادة 02 من المرسوم الرئاسي رقم: 04-432 السالف الذكر.

[7]- المادة 03 من المرسوم الرئاسي رقم: 04-432 السالف الذكر.

- إعداد بنك معطيات في مجال التحقيق الجنائي، يوضع تحت تصرف الهيئات والأجهزة الوطنية والدولية في إطار الإجراءات والإتفاقات المقررة؛
- القيام بالتسيير الممركز لوثائق الإثبات وللعينات المرجعية ذات العلاقة ببنوك المعطيات، وكذا الحفاظ على الوثائق التي تكتسي طابعًا تعليميًا أو علميًا؛
- تطوير وتحسين وتوحيد نمط بروتوكولات الخبرة الخاصة بالأدلة المتعلقة بعلم التحقيق الجنائي المطبقة في المخابر المتخصصة؛
- القيام بناء على طلب من السلطات المؤهلة بكل دراسة أو بحث في علم التحقيق الجنائي أو الإحصائي أو القانوني ذي العلاقة مع الشرطة الجنائية، والقيام عند الإقتضاء بتقديم التوصيات المرتبطة بها؛
- القيام بنشر الوثائق وأعمال الدراسات والبحث ذات الصلة بالنشاطات العلمية والتقنية؛
- القيام بالشراكة العلمية والتعاون مع المعاهد والجامعات المتخصصة، سواء على الصعيد الوطني أو على الصعيد الدولي في ميدان متابعة البحث في علم التحقيق الجنائي؛
- التحيين الدائم عن طريق متابعة: النشاطات التقنية والعلمية، الدراسات والمنشورات في هذا الميدان، المستجدات في مجال البحث والتجهيزات التقنية والعلمية.[1]

ثانيًا: المصلحة المركزية لمكافحة الجرائم السيبرانية

أنشئت المصلحة المركزية لمكافحة الجرائم السيبرانية سنة 2011، وهي الجرائم المعروفة أيضًا بالجرائم المعلوماتية، وقد كانت في بدايتها عبارة عن فصيلة شكلت الإنطلاقة الأولى لتأسيس تشكيل أمني متخصص في محاربة هذا النوع من الجرائم التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها على مستوى المديرية العامة للأمن الوطني، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بناءً على قرار السيد اللواء المدير العام للأمن الوطني وأضيفت للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي سنة 2015[2]، لتحول فيما بعد إلى مصلحة عملياتية مجهزة بالمورد البشري المتخصص والوسائل التقنية ذات مستوى عالي لمواجهة التحديات المتزايدة في مجال الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، وتضم الهيكلة الحالية للمصلحة المركزية لمكافحة الجرائم السيبرانية هياكل متخصصة ومكاتب للدعم والتسيير والتحليل[3].

[1]- المادة 05 من المرسوم الرئاسي رقم: 04-432 السالف الذكر.

[2]- حسين جيجة، سحواد نسيمة، **جهود إستباقية للأمن الوطني لتحقيق الأمن المعلوماتي والإمتياز في الأداء**، الشرطة المديرية العامة للأمن الوطني، **روبورتاج منشور في** مجلة الشرطة المديرية العامة للأمن الوطني، العدد 129، ديسمبر 2015، الجزائر، ص 142.

[3]- غنية حساني، **العصب الرقمي لصد الجرائم المعلوماتية**، الشرطة المديرية العامة للأمن الوطني، مجلة الشرطة المديرية العامة للأمن الوطني، العدد 158، ماي 2024، الجزائر، ص 18.

وقد تم تدشين المقر الجديد للمصلحة المركزية لمكافحة الجرائم السيبرانية التابع لمديرية الشرطة القضائية يوم الأربعاء بتاريخ 25 أكتوبر 2023 في الجزائر العاصمة، وذلك في إطار تنفيذ المخطط السنوي للمديرية العامة للأمن الوطني حسب ما أورده بيان للمديرية مجهز بالمورد البشري المتخصص وبكافة الوسائل التقنية العالية المستوى المتصلة بالتكنولوجيات الحديثة، وتندرج هذه العملية ضمن مساعي عصرنة المصالح العملياتية للشرطة للإرتقاء بالعمل الأمني في مواجهة التحديات المرتبطة بكل أشكال الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص والتهديدات السيبرانية.[1]

ويتم إنتقاء الكفاءات المتخصصة التي تعمل في مجال مكافحة هذا النوع من الجرائم من مدارس الشرطة أو من المصالح العملياتية، ممن تتوفر فيهم شروط المهارة والتحكم بالتقنيات الحديثة وشبكات التواصل الإلكترونية، ليتم بعدها تكوينهم على مستوى المصلحة المركزية لمكافحة الجرائم السيبرانية، وتنقسم البرامج التكوينية إلى ثلاث فئات على النحو التالي:

- تكوين المحققين المختصين في الجرائم المعلوماتية لاسيما تلك المتعلقة بالجرائم الماسة بالمستند الإلكتروني؛
- تكوين متدخلين أوليين في مجال الجرائم المعلوماتية بما يشمل الجرائم الماسة بالمستند الإلكتروني؛
- تكوين متخصص في مجال التفتيش الإلكتروني.[2]

ويشارك عناصر المصلحة المركزية بصورة دورية في دورات تكوينية منظمة من طرف المؤسسات والمنظمات الدولية التي تندرج في إطار التعاون الدولي والتعاون الشرطي الثنائي مع العديد من الدول في مجال مكافحة الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، بالإضافة إلى تنظيم دورات من طرف المنظمة الدولية للشرطة الجنائية (الأنتربول) ومكتب الأمم المتحدة المعني بالمخدرات ومكافحة الجريمة الدولية.[3]

وتتولى المصلحة المركزية لمكافحة الجرائم السيبرانية المهام الآتية:

- تسخير الموارد البشرية والمادية، لضمان تنسيق محكم أساسه صون وحماية أمن الوطن والمواطن؛
- تباشر مهامها تحت إشراف السلطات القضائية، فهي مختصة في تنفيذ تعليمات وإنابات الجهات القضائية على المستوى الوطني؛

[1]- الموقع الرسمي الإذاعة الجزائرية، تاريخ التصفح: 2024/05/09، الساعة 19:34، رابط الموقع:
https://news.radioalgerie.dz/ar/node/34199

[2]- غنية حساني، مرجع سابق، ص-ص 18-19.

[3]- نفس المرجع، ص 19.

- تقوم عن طريق أخصائيها بتأطير تكوين تقني أساسي لطلبة القضاة، وفقًا لإتفاقية مبرمة بين وزارة العدل والمديرية العامة للأمن الوطني؛
- تم تطوير نظام أمني إلكتروني محمي خاص لتبادل المعلومات والمعطيات على مستوى مصالح المديرية العامة للأمن الوطني، يسمح بتنسيق فعال بين المصلحة المركزية لمكافحة الجرائم السيبرانية ومختلف فرق مكافحة هذا النوع من الجرائم المتواجدة على الإقليم الوطني، لضمان الإشراف العملياتي الدائم والمستمر لهذه الفرق المحلية؛
- تنسيق مع مختلف المصالح الأمنية على غرار الدرك الوطني على تنظيم حملات توعية حول الجرائم المعلوماتية التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها.[1]

وفي سياق ذي صلة تنسق المصلحة المركزية لمكافحة الجرائم السيبرانية مع المنظمة الدولية للشرطة الجنائية (الأنتربول) حول تورط أشخاص في قضايا تخص:

- المساس بالقصر بإستخدام تكنولوجيات الإعلام والإتصال؛
- تبليغ عن محاولات الإنتحار؛
- المساس بالسلامة الجسدية للأشخاص؛
- سرقة المعطيات الخاصة بالبطاقات البنكية.[2]

ثالثًا: المخابر التابعة للمديرية الفرعية للشرطة العلمية والتقنية

إستحدثت المديرية العامة للأمن الوطني هيكلها التنظيمي بهدف خلق وحدات متخصصة تساهم كل منها على مكافحة نوع معين من الجرائم دون سواها، ولذلك قامت المديرية العامة للأمن الوطني بإستحداث أربع (04) مصالح مختصة في شكل نيابة مديرية، وهي

- نيابة القضايا الجنائية؛
- نيابة مديرية الإقتصادية والمالية؛
- نيابة مديرية الشرطة العلمية والتقنية؛
- مصلحة البحث والتحليل.[3]

وأسندت مهمة مكافحة الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص إلى نيابة مديرية الشرطة العلمية والتقنية التي تضع لخدمة هذا الهدف مصالح عملية مختصة بذلك التي تتولى البحث والتحري والتحقيق، وهذه الوحدات هي: المخبر المركزي للشرطة العلمية والتقنية (الجزائر العاصمة)، المخبر الجهوي

[1]- غنية حساني، مرجع سابق، ص- ص 19-20.

[2]- نفس المرجع، ص20.

[3]- ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة الدكتوراه علوم، تخصص: قانون العقوبات والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2015-2016، ص177.

للشرطة العلمية (وهران)، المخبر الجهوي للشرطة العلمية (قسنطينة)، المخبر الجهوي للشرطة العلمية (بشار)، المخبر الجهوي للشرطة العلمية (تمنراست)[1].

تتولى مخابر الشرطة العلمية والتقنية سواء المركزي أو الجهوي فروعًا متخصصة في إطار قسمين أساسيين، الدائرة العلمية التي تتولى تحليل الأدلة الجنائية المتعلقة بالمجال البيولوجي والطب الشرعي والكيميائي والمخدرات وكذلك تلك المتعلقة بمجال التسميم والمتفجرات والحريق، كل منها على مستوى مخبر خاص، والدائرة التقنية التي تتولى تحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها القذائف والأسلحة بمختلف أنواعها وكذا جرائم التزوير، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الآخرى.[2]

ويضم المخبر الجهوي للشرطة العلمية على مستوى ولاية قسنطينة كما هو الحال بالنسبة لمخبر ولاية وهران، مخبرًا خاصًا يتولى إجراءات البحث والتحقيق بشأن الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، وذلك تحت تسمية دائرة الأدلة الرقمية والأثار التكنولوجية والتي لم تكن عند إستحداثها سنة 2004 سوى قسم، غير أن الإرتفاع الملحوظ لعدد القضايا في البيئة الرقمية عجل بترقيتها إلى دائرة تضم ثلاث (03) أقسام فرعية[3]، وهي:

1- قسم إستغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات:

يتم من خلاله إستغلال الحاسوب من جميع الأنواع وبمختلف مكوناته، بالإضافة إلى كاميرات الرقمية وآلات التصوير وإستخراج محتوى الدعامات الرقمية، كما يتوفر في القسم على أدوات ومعدات حديثة وخبرة إستخراج الكلمات السرية وإسترجاع الملفات المحذوفة[4]، كما يوفر دعمًا لفرق الشرطة الميدانية في مجال إصلاح جميع الدعامات التالفة لتجهيزات الحاسوب وإسترجاع جميع المعطيات غير المعالجة الموجودة في شرائط الفيديو الرقمية والهواتف النقالة والذاكرات الخارجية[5].

2- قسم إستغلال الأدلة الناتجة عن الهواتف النقالة:

هذا القسم يسمح في حالة توقيف المشتبه فيه وكان قد إستعمل تكنولوجيا الهاتف النقال بإستخراج جميع المعطيات الظاهرة والمحذوفة منها ومعرفة مختلف شرائح "سيم" التي تم وصلها أو إستعمالها وكذا بطاقات الذاكرة بالإضافة إلى تشخيص المعطيات التي على علاقة مع

[1]- ربيعي حسين، مرجع سابق، ص177.
[2]- نفس المرجع، ص 178.
[3]- نفس المرجع، ص 179.
[4]- دائرة الأدلة الرقمية للأمن الوطني، الشرطة المديرية العامة للأمن الوطني، روبورتاج منشور في مجلة الشرطة المديرية العامة للأمن الوطني، العدد 149، جويلية 2021، الجزائر، ص 37.
[5]- نفس المرجع، ص 37.

القضايا المعالجة، كما يوفر القسم دعمًا في تحليل المعطيات والملتيميديا وقائمة الإتصالات وسجل المكالمات الهاتفية والإيمايلات والرسائل النصية والرسائل المرئية والتصفح عبر الإنترنت وإنجاز مخططات علاقات الإتصالات لكشف إرتباطات الجرمية وأبعادها وشركائها.[1]

3- قسم معالجة الصور والفيديوهات:

يختص هذا القسم في معالجة وتحسين نوعية الفيديوهات والصور المخزنة في الدعائم الإلكترونية كالمسجلات الرقمية ومنصات التواصل وشرائط الفيديو الرقمية ودعامات التخزين، لتصبح بذلك دلائل وقرائن في إثبات تورط المشتبه فيهم.[2]

تضم الدائرة في صفوفها ثمانية (08) أعضاء، أربع (04) منهم أعوان شرطيون رسميون يتمتعون بصفة ضابط الشرطة القضائية والبقية هم أعوان شبيهون، يحمل كل واحد منهم شهادة جامعية في تخصص الإعلام الآلي إضافة إلى إحاطتهم بالجانب القانوني، ومما يزيد من فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث والتحقيق في الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص هو إمتثالهم بصفة دورية لدورات تكوينية لغرض الإطلاع على كل المستجدات القانونية والتقنية في مجال الإجرام المعلوماتي.[3]

رابعًا: الفصائل التابعة للمصالح الولائية للشرطة القضائية

أوجدت المديرية العامة للأمن الوطني سنة 2010 ما يقارب 23 خلية لمكافحة الجرائم المعلوماتية التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، موزعة على النحو التالي:

- 08 خلايا على مستوى ولايات الوسط؛
- 06 خلايا على مستوى ولايات الغرب؛
- 08 خلايا على مستوى ولايات الشرق؛
- خلية على مستوى الجنوب.

لتقوم بعدها المديرية العامة للأمن الوطني بتعميم هذه الخلايا على مستوى جميع مصالح أمن ولايات الوطن.[4]

ومع إزدياد نسبة إرتكاب الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص أدى إلى ضرورة توسيع في التشكيل الأمني عن

---

[1]- دائرة الأدلة الرقمية للأمن الوطني، مرجع سابق، ص 37.

[2]- نفس المرجع، ص 37.

[3]- ربيعي حسين، مرجع سابق، ص 179.

[4]- حملاوي عبد الرحمان، **دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة محمد خيضر- بسكرة، المنعقد بتاريخ 16و 17 نوفمبر 2015، الجزائر، ص 8.

طريق تكوين الفصائل على مستوى أمن 48 ولاية[1]، حيث تم إنتقاء مائة 100 عنصر شرطة الذين تتوفر فيهم شروط الكفاءة والإطلاع المستمر على التقنيات الحديثة للإنترنت وشبكات الإتصال، أسفرت عن ذلك إستحداث 48 فصيلة تابعة للمصالح الولائية للشرطة القضائية لأمن الولايات.[2]

في سنة 2013 تم إنشاء هذه الفصائل المكونة من عناصر الشرطة ذات كفاءة، تلقوا تكوينًا على مستوى معهد الشرطة الجنائية في سحاولة بغرب ولاية الجزائر العاصمة وباشروا في أداء مهامهم مباشرة بعد الإنتهاء من التربص وتم تزويدهم بالمعدات التقنية اللازمة لذلك، ويتمثل دور هذه الفصائل في رصد ومراقبة شبكات التواصل الإجتماعي والتكفل بشكاوي وبلاغات المواطنين ومباشرة التحقيقات الجنائية في القضايا التي تكون في متناولهم أو يتواصلون مع المصلحة المركزية للمساعدة التقنية وكذا معاينة مسرح الجريمة والبحث عن الأدلة الإلكترونية وإستغلالها لتحديد الفاعلين، ويتم بعدها إعداد ملفات قضائية بشأن الفعل المرتكب.[3]

وتقوم هذه الفصائل أيضًا بمهام وقائية بالمشاركة في ندوات والحملات التوعوية على المستوى المحلي، كما تم إعطائهم تعليمات صارمة على مراقبة مقاهي الإنترنت وإحصاءها دوريًا، بغرض تحفيز هذه العناصر على التعرف والإندماج في الميدان وتكوين علاقات مع المسيرين خاصة في ظل إستغلال هذه الفضاءات من طرف المشتبه فيهم في قضايا إرهابية.[4]

الفرع الثاني: الوحدات التابعة للدرك الوطني

الدرك الوطني قوة عسكرية منوطة بها مهام الأمن العمومي، وتحكمه القوانين والتنظيمات الجاري بها العمل في وزارة الدفاع الوطني والقوانين والتنظيمات المتعلقة بمهمة الأمن العمومي وكذا أحكام المرسوم الرئاسي رقم: 09-143 المؤرخ في 27 أفريل 2009[5]، وفي سبيل تنفيذ الدرك الوطني لمهامه يتضمن ما يأتي: قيادة الدرك الوطني، القيادات الجهوية للدرك الوطني، الوحدات الإقليمية، الوحدات المشكلة، الوحدات المتخصصة، الوحدات الجوية، وحدات الإسناد، هياكل التكوين، الهياكل العلمية والتقنية.[6]

---

[1]- في سنة 2019 تم إنشاء ولايات جديدة وأصبحت الجزائر تقسم إلى 58 ولاية.

[2]- حسين جيجة، سحواد نسيمة، مرجع سابق، ص 142.

[3]- حبيباتني بثينة، مرجع سابق، ص 231.

[4]- حسين جيجة، سحواد نسيمة، مرجع سابق، ص 149.

[5]- المادة 02 من المرسوم الرئاسي رقم: 09-143 المؤرخ في 27 أفريل سنة 2009، المتضمن مهام الدرك الوطني وتنظيمه، ج.ر.ج.ج.ش العدد 26، الصادرة في 03 ماي سنة 2009، المعدل والمتمم.

[6]- المادة 03 من المرسوم الرئاسي رقم: 23-313 المؤرخ في 03 سبتمبر سنة 2023، المعدل والمتمم للمرسوم الرئاسي رقم: 09-143 المؤرخ في 27 أفريل سنة 2009، المتضمن مهام الدرك الوطني وتنظيمه، ج.ر.ج.ج.ش العدد 59، الصادرة بتاريخ 10 سبتمبر 2023.

يكافح الدرك الوطني في مجال الشرطة القضائية الإجرام والجريمة المنظمة، ويستعمل لهذا الغرض وسائل تحريات الشرطة العلمية والتقنية وخبرة الأدلة الجنائية وذلك طبقًا للتشريع والتنظيم الساري المفعول، وفي هذا الصدد يكلف الدرك الوطني لاسيما بما يأتي:

- تلقي الشكاوي والبلاغات وجمع الإستدلالات والقيام بالتحقيقات الأولية؛
- البحث والتحري ومعاينة جميع الجرائم المنصوص عليها في قانون العقوبات والقوانين الخاصة، وجمع الأدلة عنها والبحث عن مرتكبيها والمساهمين فيها؛
- تنفيذ الإنابات القضائية الصادرة عن الجهات القضائية، وتلبية أوامرها وتسخيراتها؛
- تنفيذ السياسة الجزائية في مجال إختصاصه؛
- إعداد الدراسات والتحاليل المرتبطة بمجال الشرطة القضائية، وإقتراح الحلول على السلطات المؤهلة لإتخاذ القرار؛
- تحديد وتحليل كل التهديدات المرتبطة بمختلف الجرائم لاسيما الجريمة المنظمة والجرائم الإقتصادية والمالية؛
- تقديم الإقتراحات وإبداء الرأي بمناسبة إعداد النصوص المتعلقة بالشرطة القضائية.[1]

تعمل مصالح الدرك الوطني على مكافحة الجرائم الماسة بالمستند الإلكتروني من خلال هيئاتها المركزية التالية:

أولًا: المعهد الوطني للأدلة الجنائية وعلم الإجرام

تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب المرسوم الرئاسي رقم: 04-183 المؤرخ في 26 جوان 2004[2]، فهو عبارة عن مؤسسة عمومية ذات طابع إداري ويتمتع بالشخصية المعنوية والإستقلال المالي[3]، ويوضع تحت وصاية وزير الدفاع الوطني ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه، وبهذه الصفة فإنه يخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية.[4]

ومعتمد في مجال الأدلة الجنائية من خلال إعتماد 56 طريقة تحليلية وفق المعيارين الدوليين إيزو 17020 وإيزو 17025 من قبل هيئة الإعتماد الجزائرية ALGERAC[5]، ويتكون من إحدى عشر (11) دائرة متخصصة في مختلف المجالات تضمن إنجاز:[1]

---

[1]- المادة 08 من المرسوم الرئاسي رقم: 09-143 السالف الذكر.

[2]- المرسوم الرئاسي رقم: 04-183 المؤرخ في 26 جوان 2004، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر.ج.ج.ش العدد 41، الصادرة في 27 جوان 2004، المعدل والمتمم.

[3]- المادة 1/02 من المرسوم الرئاسي رقم: 04-183 السالف الذكر.

[4]- المادة 2/02 من المرسوم الرئاسي رقم: 04-183 السالف الذكر.

[5]- الموقع الرسمي للدرك الوطني، تاريخ التصفح: 2024/05/06، الساعة 10:04، رابط الموقع:
https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php

- إجراء بناء على طلب من القضاة والمحققين أو السلطات المؤهلة الخبرات والفحوص العلمية، التي تخضع لإختصاص كل طرف في إطار التحريات الأولية والتحقيقات القضائية، بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح؛
- تقديم مساعدة علمية أثناء القيام بالتحريات المعقدة، بإستخدام مناهج الشرطة العلمية والتقنية، الرامية إلى تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة؛
- المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام؛
- تصميم بنوك معطيات وإنجازها طبقًا للقانون بما في ذلك تلك الخاصة بالبصمات الجينية التي ستكون في متناول المحققين والقضاة، بغرض وضع المقاربات وإستخلاص الروابط المحتملة بين المجرمين وأساليب النشاط الإجرامي؛
- المشاركة بصفته هيئة تضمن الفحوص والخبرات في مجال علم الإجرام، في تحديد سياسة جنائية مثلى لمكافحة الإجرام؛
- المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة؛
- العمل على ترقية البحث التطبيقي وأساليب التحريات التي ثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي؛
- المشاركة في كل الملتقيات والمحاضرات أو الندوات على الصعيدين الوطني والدولي الضرورية في تطوير مستخدمي المعهد؛
- المشاركة في تنظيم دورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية؛
- تصور الأبحاث الموكلة إلى الغير، وضمان متابعتها وتقديرها.[2]

ومن بين هذه الدوائر توجد دائرة الإعلام الآلي والإلكترونيك مهمتها تقديم المساعدة التقنية في التحقيقات أكثر تعقيدًا، وكذا مكلفة بتحليل ومعالجة وتقديم الدليل الإلكتروني للسلطة القضائية المختصة، كما يحرص أفرادها على تأمين اليقظة التكنولوجية من أجل تعزيز معارف التقنيات والأساليب المعتمدة في مختلف التجارب العلمية لإنجاز المهام الموكلة إليها، وتنقسم إلى ثلاثة (03) مخابر وذلك وفقًا لنوع المعلومات وكل مخبر مزود بفصيلة تقتني المعطيات من وسائط المعلومات وتحرص على ضمان شرعية ونزاهة الدليل[3]:

1- **مخبر الإعلام الآلي**: يحتوي على 07 قاعات تتمثل في: مكتب التوجيه، قاعة موزع، قاعة تخزين، فصيلة تحليل المعطيات، فصيلة الأنظمة المشحونة، فصيلة إقتناء المعطيات، فصيلة الهواتف، وتتمثل مهامه في:

---

[1]- قيادة الدرك الوطني، **مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة محمد خيضر- بسكرة، المنعقد بتاريخ 16و 17 نوفمبر 2015، الجزائر، ص 03.

[2]- المادة 04 من المرسوم الرئاسي رقم: 04-183 السالف الذكر.

[3]- قيادة الدرك الوطني، مرجع سابق، ص- ص 4-5.

- تحليل ومعالجة وسائط المعطيات الرقمية عبر الهاتف والشريحة وذاكرة الفلاش وقرص الصلب؛
- تحديد التزوير الإلكتروني للبطاقات البنكية؛

ولقيام مخبر الإعلام الآلي بمهامه فقد تم تجهيزه ب:

- محطة محمولة وثابتة لإجراء تجارب الإعلام الآلي؛
- جهاز إقتناء معلومات الهاتف والحاسوب؛
- محطة تصليح وترميم الأجهزة والوسائط المعطلة؛
- خبرات الإعلام الآلي والحبكات الإعلامية والتجهيزات البيانية.[1]

2- **مخبر الفيديو**: يحتوي على 04 قاعات، قاعة تخزين، قاعة موزع، قاعتان لتحليل، وتتمثل مهامه في:

- إعادة تشكيل مسرح الجريمة بواسطة ثلاثي الأبعاد؛
- تحسين نوعية الصورة (فيديو، صورة) بمختلف التقنيات؛
- مقارنة الأوجه وشرعية الفيديو والصور.

ولقيام مخبر الفيديو بمهامه فقد تم تجهيزه ب:

- الأجهزة لقراءة مختلف وسائط الفيديو الرقمية أو الممغنطة؛
- جهاز فيديوبوكس؛
- حبكات إعلامية (3D Studio Max، برنامج ثلاثي الأبعاد)؛
- موزع لحفظ شرائح الفيديو.[2]

3- **مخبر الصوت**: يحتوي على 05 قاعات، قاعة موزع، قاعة تخزين، 03 قاعات للتحليل، وتتمثل مهامه في:

- تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة؛
- تحديد ومعرفة المتكلم؛
- تحديد شرعية التسجيلات الصوتية.

ولقيام مخبر الصوت بمهامه فقد تم تجهيزه ب:

- أجهزة الإزدواجية والسماع؛
- حبكات إعلامية (تحسين ومعالجة التسجيلات الصوتية ونسخ الأقراص المضغوطة)؛

---

[1]- قيادة الدرك الوطني، مرجع سابق، ص 6 .

[2]- نفس المرجع، ص 7.

- أجهزة التصليح والتعبير.[1]

ثانيًا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها في سنة 2008 وعمل على تأمين المنظومة المعلوماتية لخدمة الأمن العمومي، حيث يهدف ضباط وأعوان الشرطة القضائية المؤهلين في الدرك الوطني على تنفيذ القوانين وجمع الأدلة وتحليل المعطيات المتعلقة بالجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص والبحث عن مرتكبيها وتحديد هويتهم، ويعمل المركز على مساعدة بقية الأجهزة الأمنية في أداء مهامها لهذا الغرض.[2]

ويهدف المركز على تزويد الدرك الوطني بأداة يقظة في المجال المعلوماتي على الصعيد الوطني، ويقدم المساعدة التقنية وتوفير السند والدعم إلى السلطات القضائية ومصالح الشرطة القضائية، ويعد أداة للوقاية من خطر الأنظمة المعلوماتية وقواعد وبنوك المعلومات على الشبكات المعلوماتية.[3]

ويقوم مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها بالمهام التالية:

- ضمان المراقبة المستمرة على شبكة الإنترنت؛
- مراقبة الإتصالات الإلكترونية في حدود ما يسمح به القانون لصالح وحدات الدرك الوطني والسلطات القضائية؛
- مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، والبحث عن الأدلة في شبكة الإنترنت؛
- المشاركة في عمليات التحري والتسرب عبر شبكة الإنترنت لصالح وحدات الدرك الوطني والسلطات القضائية؛
- المشاركة في قمع الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، من خلال التعاون مع الهيئات الوطنية ومختلف مصالح الأمن.[4]

ثالثًا: مديرية الأمن العمومي والإستعلام

مديرية الأمن العمومي والإستعلام هي عبارة عن هيئة تعمل على التنسيق بين المركز التقني العلمي ومختلف الوحدات الإقليمية، في مجال إجراءات البحث والتحري في الجرائم

[1]- قيادة الدرك الوطني، مرجع سابق، ص 8.
[2]- شنتير خضرة، مرجع سابق، ص 213.
[3]- حبيباتني بثينة، مرجع سابق، ص 236.
[4]- ربيعي حسين، مرجع سابق، ص 185.

المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص.[1]

رابعًا: المصلحة المركزية للتحريات الجنائية

المصلحة المركزية للتحريات الجنائية هي عبارة عن هيئة ذات إختصاص وطني، مهمتها مكافحة الجرائم المعلوماتية التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها.[2]

الفرع الثالث: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته

خصص المشرع الجزائري الفصل الخامس لجهاز يسمى بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته بموجب القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر، وتم الإحالة على التنظيم لتحديد كيفيات سير هذه الهيئة.

سنتطرق إلى نشأتها وتشكيلتها وكذا إبراز أهم مهامها المرتبطة بالجرائم الماسة بالمستند الإلكتروني.

أولًا: نشأة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته

تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته بموجب المادة 13 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر التي نصت على أن: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم".

وأحالت الفقرة 02 من نفس المادة إلى التنظيم لتحديد تشكيلة الهيئة وتنظيمها وكيفيات سيرها، وهو الأمر الذي تقرر فعلًا بصدور المرسوم الرئاسي رقم: 15-261 المؤرخ في 08 أكتوبر 2015 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[3]، بحيث تم تشكيل السلطة وأكدت المادة 02 منه على أن تعد هذه الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي، توضع لدى الوزير المكلف بالعدل، ويحدد مقرها بمدينة الجزائر.

---

[1]- ربيعي حسين، مرجع سابق، ص 183.

[2]- نفس المرجع، ص 183.

[3]- المرسوم الرئاسي رقم: 15-261 المؤرخ في 08 أكتوبر 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج.ش العدد 53، الصادرة بتاريخ 08 أكتوبر 2015، الملغى.

هذا وقد تم تعديل هذا المرسوم بمقتضى المرسوم الرئاسي رقم: 19-172 المؤرخ في 06 جوان 2019[1]، الذي تم بموجبه إلغاء أحكام المرسوم الرئاسي رقم: 15-261 السالف الذكر بموجب المادة 24 منه، وذلك نتيجة للظروف الأمنية والسياسية التي شهدها البلد في تلك الفترة، مما نتج عنه إلى ظهور المخاطر الفعلية لتعرض المؤسسات الدستورية وكذا الأمن العمومي للخطر، ومنه فقد تم تحويل صلاحية هذه الهيئة من الوزير المكلف بالعدل إلى وزير الدفاع الوطني مما حولها إلى هيئة ذات الطابع الأمني.[2]

وبالتالي، أصبحت تعد هذه الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلال المالي، توضع تحت سلطة وزارة الدفاع الوطني، ومقرها بالجزائر العاصمة مع إمكانية نقلها إلى أي مكان آخر بموجب قرار من وزير الدفاع الوطني.[3]

ثم قام المشرع الجزائري بإصدار مرسوم رئاسي رقم: 20-183 المؤرخ في 13 جويلية 2020[4] الذي قام بإعادة تنظيم الهيئة، الذي تم بموجبه إلغاء أحكام المرسوم الرئاسي رقم: 19-172 السالف الذكر بموجب المادة 37 منه، وأصبحت الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي، وتوضع تحت سلطة رئيس الجمهورية، ومقرها بالجزائر العاصمة مع إمكانية نقلها إلى أي مكان آخر بموجب المرسوم الرئاسي[5].

ثم صدر المرسوم الرئاسي رقم: 21-439 المؤرخ في 07 نوفمبر 2021[6] الذي يهدف إلى إعادة تنظيم الهيئة، الذي تم بموجبه إلغاء أحكام المرسوم الرئاسي رقم: 20-183 السالف الذكر بموجب المادة 41 منه، وبالتالي تعد الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، وتوضع لدى رئيس الجمهورية، ومقرها بالجزائر العاصمة مع إمكانية نقلها إلى أي مكان آخر بموجب المرسوم الرئاسي[7].

---

[1]- المرسوم الرئاسي رقم: 19-172 المؤرخ في 06 جوان 2019، المحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر.ج.ج.ش العدد 37، الصادرة بتاريخ 09 جوان 2019، الملغى.

[2]- حكيمة بوكحيل، سامية بن عديد، **الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الإتصال ودورها في تفتيش نظم المعلوماتية**، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي-الشلف، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021، الجزائر، ص 1544.

[3]- المادة 02 و 03 من المرسوم الرئاسي رقم: 19-172 السالف الذكر.

[4]- المرسوم الرئاسي رقم: 20-183 المؤرخ في 13 جويلية 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج.ش العدد 40، صادرة بتاريخ 18 جويلية 2020، الملغى.

[5]- المادة 02 و 03 من المرسوم الرئاسي رقم: 20-183 السالف الذكر.

[6]- المرسوم الرئاسي رقم: 21-439 المؤرخ في 07 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج.ش العدد 86، الصادرة في 11 نوفمبر 2021.

[7]-المادة 02 و 03 من المرسوم الرئاسي رقم: رقم: 21-439 السالف الذكر.

ثانيًا: تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته

تتكون الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته من مجلس توجيه ومديرية عامة، يوضعان تحت سلطة رئيس الجمهورية، ويقدمان له عرضًا عن نشاطاتهما.

1- مجلس التوجيه:

يتولى الأمين العام لرئاسة الجمهورية رئاسة مجلس التوجيه الذي يتشكل من الأعضاء الآتي ذكرهم : الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج، الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية، الأمين العام لوزارة العدل، الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية، قائد الدرك الوطني، المدير العام للأمن الداخلي، المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي، المدير العام للأمن الوطني، رئيس مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي، ممثل عن رئاسة الجمهورية يعينه رئيس الجمهورية.[1]

يجتمع مجلس التوجيه في دورة عادية مرة واحدة (01) في السنة بناء على إستدعاء من رئيسه، ويمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضروريًا بناء على إستدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة، ويعد مجلس التوجيه تقريرًا بعد كل دورة.[2]

2- المديرية العامة:

تضم المديرية العامة: مديرية المراقبة الوقائية واليقظة الإلكترونية، مديرية الإدارة والوسائل، مصلحة للدراسات والتلخيص، مصلحة للتعاون واليقظة التكنولوجية، ملحقات جهوية.[3]

يديرها مدير عام يعين بموجب المرسوم الرئاسي وتنهي مهامه حسب الأشكال نفسها وتعد وظيفته وظيفة عليا في الدولة[4]، وتعد كل من وظائف مديري المديريات ونوابهم ورؤساء المصالح والملحقات الجهوية في المديرية العامة وظائف عليا في الدولة، يتم التعيين في هذه الوظائف بموجب مرسوم رئاسي بناء على إقتراح من المدير العام للهيئة وتنهي المهام فيها حسب الأشكال نفسها.[5]

[1]- المادة 06 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[2]- المادة 08 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[3]- المادة 11 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[4]- المادة 09 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[5]- المادة 12 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.

لسير الهيئة يلحق بها قضاة وفقًا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول، وأيضًا ضباط وأعوان الشرطة القضائية مؤهلون من المصالح العسكرية للأمن والدرك الوطني والأمن الوطني الذين يحدد عددهم بموجب قرارات مشتركة بين وزير الدفاع الوطني والوزير المكلف بالداخلية والأمين العام لرئاسة الجمهورية، وكذا مستخدمو الدعم التقني والإداري للمصالح العسكرية للأمن المختصة والدرك الوطني والأمن الوطني[1]، ويمكن للهيئة أن توظف فئات أخرى من المستخدمين حسب الحاجة.[2]

وفي إطار التعاون يمكن للهيئة أن تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضروريتين لإنجاز المهام المسندة إليها.[3]

ثالثًا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته

تتولى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها المهام الآتية :

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته؛

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في إجراء التحريات المتعلقة بالجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال ومن بينها الأفعال الماسة بالمستندات الإلكترونية، وذلك من خلال جمع المعلومات اللازمة وإنجاز الخبرات القضائية؛

- تبادل المعلومات مع نظيراتها في الخارج بغرض جمع المعطيات المفيدة للتعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وعلى وجه الخصوص الجرائم الماسة بالمستند الإلكتروني، وتحديد مكان تواجدهم[4].

وتكلف الهيئة على الخصوص ما يلي :

- تحديد الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بما في ذلك الجرائم الماسة بالمستند الإلكتروني، ووضعها حيز التنفيذ، وتنشيط وتنسيق عمليات الوقاية منها؛

- ضمان المراقبة الوقائية للإتصالات الإلكترونية تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة؛

[1]- المادة 20 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[2]- المادة 21 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[3]- المادة 24 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[4]- المادة 14 من القانون رقم: 09-04 السالف الذكر.

- كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني المراقبة الإلكترونية عندما يتعلق الأمر بأمن الجيش، وفقًا لنفس الشروط المنصوص عليها في التشريع الساري المفعول؛
- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل إستعمالها في الإجراءات القضائية؛
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والإتصال؛
- المساهمة في تحيين المعايير القانونية في مجال إختصاصها؛
- تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بما في ذلك الجرائم الماسة بالمستند الإلكتروني، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحتها عن طريق جمع المعلومات والتزويد بها وإنجاز الخبرات القضائية؛
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية، وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال إختصاصها.[1]

كما أسندت إلى مديرية المراقبة الوقائية واليقظة الإلكترونية مهام المرتبطة بالشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بما في ذلك الجرائم الماسة بالمستند الإلكتروني كالآتي:

- تنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية من أجل الكشف عن هذه الجرائم، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقًا للتشريع الساري المفعول؛
- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة، وجمع المعطيات المفيدة لتحديد مكان تواجد مرتكبيها والتعرف عليهم؛
- جمع ومركزة وإستغلال كل المعلومات التي تسمح بالكشف عن هذه الأفعال الإجرامية وحفظها؛
- تزويد السلطات القضائية ومصالح الشرطة القضائية بالمعلومات والمعطيات المتعلقة بالجرائم محل الدراسة، سواء بصفة تلقائية أو بطلب منها.[2]

كما تكلف مصلحة الدراسات والتلخيص على الخصوص مركزة ومراقبة الإجراءات المتعلقة بالطلبات القضائية طبقًا للقواعد المنصوص عليها في قانون الإجراءات الجزائية.[3]

[1]- المادة 04 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[2]- المادة 14 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.
[3]- المادة 17 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.

كما تكلف الملحقة الجهوية بتنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بما في ذلك الجرائم الماسة بالمستند الإلكتروني، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقًا للتشريع الساري المفعول.[1]

الفرع الرابع: الإستعانة بمقدمي الخدمات وتسخيرهم

نظرًا لما تتطلبه عملية التحري والتحقيق عن الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص من إلمام بتقنيات متخصصة خاصة في مجال عمل المنظومة المعلوماتية، فقد سمح القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر بالإستعانة بمقدمي خدمات الإنترنت ومساعدة السلطات القضائية المختصة في مواجهة هذا النوع من الجرائم والكشف عن مرتكبيها.

وينحصر دورهم في تمكين المستخدم من الولوج على شبكة الإنترنت والتجول فيها والإطلاع على ما يريد، لذلك فمنهم من يسهل للمستخدم الإنترنت من الولوج إلى الموقع ومنهم من ينقل الخدمة ومنهم من يخزن المعلومات أو ينقلها[2]، مما سنتطرق إلى تعريفهم وتصنيفهم في ما يلي:

أولًا: تعريف وأصناف مقدمي الخدمات

مقدمو الخدمات قد يكونون أشخاصًا طبيعيين أو معنويين، ويتسم عملهم بالطابع التقني كما تتعدد المسميات التي يعرفون بها[3]، وسنتناول تعريفهم وأصنافهم في ما يلي:

1- تعريف مقدمي الخدمات:

عرفت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 مقدم الخدمة في الفقرة (ج) من المادة الأولى منها كالآتي: "مقدم الخدمة يشير إلى:

1- كل جهة عامة أو خاصة تقدم لمستخدمي خدماتها إمكانية الإتصال عن طريق النظام المعلوماتي؛

2- كل جهة أخرى تعالج أو تخزن المعطيات المعلوماتية بدلًا من خدمة الإتصال أو نيابة عن مستخدمي هذه الخدمة".[4]

---

[1]- المادة 1/19 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.

[2]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص- ص 482-483.

[3]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص 338.

[4]-Art 01 paragraphe c du convention sur la cybercriminalité dispose que : « c. « fournisseur de service» désigne :=

وعرفت الإتفاقية العربية لجرائم تقنية المعلومات في الفقرة 02 من المادة 02 كالآتي: "مزود الخدمة: أي شخص طبيعي أو معنوي عام أو خاص، يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الإتصالات أو مستخدميها".

وقد عرف المشرع الجزائري مقدمي الخدمات في الفقرة (د) من المادة 02 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر كالآتي: "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها".

الملاحظ في هذا التعريف أنه تضمن الجوانب التقنية لمقدمي الخدمات فقط، فهو معالج ومخزن المعطيات وكذلك هو مقدم خدمة الإتصال بواسطة منظومة معلوماتية أو نظام للإتصالات وهي خدمات تقنية، في حين أن دور مقدمي الخدمات لا يقتصر على الدور التقني فقط بل هناك جهات تقوم بتوريد خدمات المحتوى المعلوماتي في شبكة الإنترنت إلى الجمهور وهي أهم مصدر للتدفق المعلوماتي، كما أن هناك جهات أخرى تقوم بتخزين التطبيقات والسجلات المعلوماتية لعملائها وتمدهم بالوسائل التقنية والمعلوماتية التي تمكنهم من الوصول إلى ذلك المخزون عبر شبكة الإنترنت.[1]

وإن عملية إيصال خدمة الإنترنت بمفهومها الواسع تمر بعدة وسطاء من أجل وصول الخدمة للمستخدم، فمقدم خدمة الإنترنت هو من يضع تحت تصرف المستخدم الوسائل التقنية من أجل الولوج إلى شبكة الإنترنت، ومن الملاحظ وفق تعريف الفقرة (د) من المادة 02 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر أن المشرع الجزائري لم يفرق بين هؤلاء المتدخلين في عملية إيصال خدمة الإنترنت، والأصل أنه لا يمكن الحصول على خدمة الإنترنت والدخول وإستغلال هذه الشبكة دون أن يتم ذلك عن طريق مقدميها أو ما يعرف بالوسطاء، ورغم تعدد طرق الوصول إلى الإنترنت مثلًا (ISDN/ADSL) لكن العامل المشترك لكل هذا هو وجود مقدمي الخدمات كل حسب الدور الذي يؤديه في إيصال الخدمة.[2]

=i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique;

ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs».

[1]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص-ص 339-340.

[2]- مولاي ملياني دلال، مرجع سابق، ص- ص 116-117.

2-أصناف مقدمي الخدمات:

المتدخلين في تقديم خدمات الإنترنت هم:

أ- متعهد الوصول (مقدمي خدمة التوصيل):

أي شخص طبيعي أو معنوي يقوم بدور فني لتوصيل المستخدم أو الجمهور إلى شبكة الإنترنت، وذلك بمقتضى عقود الإشتراك يضمن توصيل العميل إلى المواقع التي يريدها[1] أو البريد الإلكتروني للأشخاص الذين يريد مخاطبتهم في أي مكان من العالم، فهو لا يقدم المعلومة أو محتوى المواقع الإلكترونية بل تقتصر مهمته على إيصال المستخدم إلى الإنترنت عن طريق أجهزته الخاصة، فهو ليس منتجًا للمصنف ولكنه يضطلع بتقديم خدمات ذات طبيعة فنية تمكن مشتركيه من إستخدام شبكة الإنترنت ومن ثم ليس له الإطلاع أو التعرف على مضمون الرسائل والمعلومات المتبادلة عبر الشبكة التي تمر من خلاله.[2]

وعليه يتضح لنا أن الدور الذي يقوم به متعهد الوصول فني بحث لا يتعدى توصيل المستخدم بشبكة الإنترنت ولا علاقة له بالمحتوى الإلكتروني الذي يمر عبر شبكته، حيث يمكنه من الولوج إلى المواقع التي يريدها والحصول على حاجاته من المعلومات والخدمات.[3]

ب- متعهد الإيواء (مقدمي خدمة الإيواء):

إن مصطلح الإيواء (hébergement) بمعناه الإلكتروني الواسع يشمل وضع الوسائل التقنية والمعلوماتية بمقابل أو بالمجان تحت تصرف العملاء ليتمكنوا من الدخول إلى شبكة الإنترنت في أية لحظة، بغية بث مضمون معلوماتي معين نصوص أو صور أو أصوات للجمهور، ويتولى هذه المهمة متعهد للإيواء (fournisseur d'hébergement) يعمل على تخزين المعطيات والمعلومات التي يبثها أصحاب المواقع الإلكترونية على جهازه الإلكتروني المرتبط على الدوام بشبكة الإنترنت، بحيث يتمكن أصحاب هذه المواقع من إطلاع الجمهور على مضمونها المعلوماتي على مدار الساعة.[4]

فخدمة الإيواء كما عرفتها المادة 14 من التوجيه الأوروبي حول التجارة الإلكترونية والمادة 6-1/2 من القانون الفرنسي حول الثقة في الإقتصاد الرقمي عبارة عن نشاط يمارسه شخص طبيعي أو معنوي يهدف إلى تخزين مواقع إلكترونية وصفحات ويب (web pages) على جهازه الإلكتروني الخادم بشكل مباشر ودائم مقابل أجر أو بالمجان، ويضع من خلاله تحت تصرف عملائه الوسائل التقنية والمعلوماتية التي تمكنهم في أي وقت من بث ما يريدون على شبكة الإنترنت من نصوص وصور وأصوات وتنظيم المؤتمرات والحلقات النقاشية

[1]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 486.

[2]- نفس المرجع، ص 487.

[3]- حدة بوخالفة، **مقدمو خدمات الإنترنت ومسؤوليتهم الجزائية**، أطروحة الدكتوراه علوم في القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي-تبسة-، 2016-2017، ص 30.

[4]- حسين محمد الغول، مرجع سابق، ص-ص 540-541.

وإنشاء روابط معلوماتية مع المواقع الإلكترونية الآخرى (liens hypertexts)، ومن الوسائل التي يقدمها متعهد الإيواء لعملائه تخصيص مساحة قرص أو شريط مرور لبث المعلومات التي يرغبون بنشرها على شبكة الإنترنت، وتزويد العميل بحساب خاص يمكنه من الإتصال بمتعهد الإيواء وإضافة أو حذف أو تغيير ما يريد من معلومات.[1]

وقد عرف المشرع الجزائري مقدم خدمة الإيواء في الفقرة (د) من المادة 02 القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر بأنه: "أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها"، وهو التعريف الذي جاء مشابهًا إلى درجة كبيرة للتعريف الذي جاءت به الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 حينما عرفت بدورها متعهد الإيواء بأنه أي كيان آخر يقوم بمعالجة بيانات الكمبيوتر أو تخزينها نيابة عن مزود خدمة الإتصالات أو مستخدمي هذه الخدمة.

أي أن وظيفته إيواء كل ما هو معلوماتي بداية من المعطيات التي تأخذ إما شكل صور أو رسوم أو فيديوهات وغيرها، ويقوم بهذه العملية إما شخص طبيعي أو معنوي فهو بمثابة المؤجر لمساحة معينة من العالم الرقمي، ومن ذلك يمكن للمستأجر أن يحوي مكانه المؤجر كل ما يرغب به دون أي رقابة ويستخدم في ذلك الجهاز المضيف[2]، فالجهاز المركزي الرئيسي يقوم بإستضافة أجهزة أخرى من خلال الإتصال به مباشرة ويسمى بذلك المضيف باستضافة المعطيات وبثها وإسترجاعها والإستفادة من الخدمات الأخرى من خلال البرامج المتعددة الموجودة على الجهاز المضيف.[3]

ج- مقدمي المضمون (الناشرين):

إعتمد الفقه في تعريف مقدمي المضمون على عدة معايير متباينة فمنهم من يعتمد على معيار القيام بنشر صفحات للجمهور عبر مواقع الإنترنت أو معيار تحقيق المنفعة الإقتصادية أو معيار إنشاء وتنظيم المحتويات عبر موقع الإنترنت، وبناء على ذلك تم تعريفه على أنه: "الشخص الطبيعي أو الشركة التي تنشر للجمهور صفحات عبر مواقع الإنترنت".[4]

ويتمثل الإلتزام الرئيسي لمقدمي المضمون في مراقبة المحتوى على الموقع بحيث هو من يحدد المحتوى الذي يجب إتاحته للجمهور على الخدمة التي أنشأها أو المسؤول عنها، وهو المسؤول عن جميع المحتويات الموجودة على موقعه، وبالتالي فهو ليس مسؤولًا فقط عما يكتبه على موقعه بل مسؤولًا على كل ما ينشر على الموقع.[5]

---

[1]- حسين محمد الغول، مرجع سابق، ص 541.

[2]- مولاي ملياني دلال، مرجع سابق، ص 122.

[3]- نفس المرجع، ص 123.

[4]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص 341.

[5]- نفس المرجع، ص 341.

د- ناقل المعلومات:

يعرف الناقل المادي للمعلومة بعامل الإتصالات، وهو ذلك الشخص الذي يساعد فنيًا في تحويل المعلومات ونقلها عبر الشبكة الإنترنت، فهو وسيط بين متلقي المعلومة مستخدم الخدمة ومورد المعلومة أو منتجها.[1]

فهو الذي يتولى النقل المادي لها بوسائله الفنية بالقيام بالربط بين الشبكات تنفيذ لعقد نقل المعلومات بين الأجهزة المرتبطة بمواقع الإنترنت أو بمستخدمي الشبكة، حيث ينحصر دوره من خلال هذا التعريف في الربط بين مختلف الشبكات أي كقاعدة عامة عدم مراقبته أو علمه بالمعلومات التي تعبر الشبكة بواسطته.[2]

و- منتج المعلومة أو مؤلفها:

يعتبر منتج المعلومة أو مؤلفها شخصًا طبيعيًا أو شخصًا معنويًا، يعمل بواسطة وسائل التقنية على بث معلومات معينة بشأن موضوع محدد على إحدى مواقع شبكة الإنترنت وفقًا لأحكام والشروط والضوابط.[3]

ي- ناشر المعلومة:

إن لناشر المعلومة مفاهيم كثيرة حسب الدور الذي يقوم به على شبكة الإنترنت، فقد يكون الشخص الذي قام بإنشاء صفحة التواصل وسمح للأشخاص بالدخول إليها والتعرف فيما بينهم عن طريقها، أو قام بتأليف المحتوى المعلوماتي، أو قد يكون الشخص الذي وضع المعلومات على المواقع أو أرسلها عبر الشبكة.[4]

ثانيًا: إلتزامات مقدمي الخدمات في مكافحة الجرائم الماسة بالمستند الإلكتروني

- يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتفتيش لجمع و/أو تسجيل المعطيات المتعلقة بالجرائم المنصوص عليها في القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر ووضع المعطيات المعنية تحت تصرفها[5]، ويتعين عليهم كتمان سرية العمليات التي ينجزونها والمعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[6]؛
- يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها، وبوضع المعطيات المتعلقة

[1]- حدة بوخالفة، مرجع سابق، ص 32.
[2]- مولاي ملياني دلال، مرجع سابق، ص 123.
[3]- نفس المرجع، ص 123.
[4]- حدة بوخلفة، **المسؤولية الجنائية لمقدمي خدمات الإنترنت**، د.ر.ط، 2019، دار هومة، الجزائر، ص 126.
[5]- المادة 4/16 من القانون رقم: 24-02 السالف الذكر.
[6]- المادة 5/16 من القانون رقم: 24-02 السالف الذكر.

بحركة السير التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة[1]، ويتعين عليهم كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[2]؛

- التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها، بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن[3]؛
- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة، وإخبار المشتركين لديهم بوجودها[4].

المبحث الثاني: آليات التعاون الدولي لمكافحة الجرائم الماسة بالمستند الإلكتروني

تتجاوز آثار الجرائم الماسة بالمستند الإلكتروني في كثير من الحالات حدود الدولة الوطنية وتمتد إلى دول أخرى، إذ غالبًا ما ينتشر مرتكبوها عبر عدة دول، ولهذا أصبح التعاون الدولي في مكافحتها أمرًا حتميًا، مما يستدعي توفير الوسائل المناسبة التي تعزز من فعالية هذا التعاون، بهدف التصدي لها بشكل ناجع ومتكامل.

المطلب الأول: آليات التعاون القضائي لمكافحة جرائم المستند الإلكتروني

سنتطرق إلى التعاون والمساعدة القضائية الدولية في (الفرع الأول)، أما (الفرع الثاني) فقد خصصناه لآلية تسليم المجرمين في مكافحة الجرائم الماسة بالمستند الالكتروني.

الفرع الأول: التعاون والمساعدة القضائية الدولية

أجاز المشرع الجزائري بموجب الفصل السادس من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر التعاون والمساعدة القضائية الدولية، في إتخاذ الإجراءات القانونية اللازمة التي تسهل التبادل الدولي لمكافحة الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص في إطار ما تسمح به الأطر القانونية المعمول بها.

أولًا: الإختصاص القضائي

يقوم الإختصاص القضائي للدولة التي إرتكبت الجريمة الماسة بالمستند الإلكتروني على إقليمها بإستبعاد تطبيق لأي قانون أجنبي داخلها عملًا بمبدأ الإقليمية، كما يقوم الإختصاص القضائي للدولة على الشخص الذي يحمل جنسيتها طبقًا لمبدأ الشخصية ولو كانت الجريمة قد وقعت خارج إقليمها، وعلى كل جريمة يكون المجني عليه يحمل جنسيتها حتى ولو كان الجاني

[1]- المادة 1/10 من القانون رقم: 09-04 السالف الذكر.
[2]- المادة 2/10 من القانون رقم: 09-04 السالف الذكر.
[3]- المادة 1/12 من القانون رقم: 09-04 السالف الذكر.
[4]- المادة 2/12 من القانون رقم: 09-04 السالف الذكر.

أجنبيًا، وكذا يقوم الإختصاص القضائي للدولة على كل شخص يحمل جنسية أجنبية إرتكب في الخارج جريمة تمس بمصالحها الأساسية تطبيقًا لمبدأ العينية.

فضلًا عما سبق ذكره، تختص المحاكم الجزائرية بالنظر في الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيًا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني بموجب المادة 15 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر، وهو ما نصت عليه المادة 12 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر بإختصاص الجهات القضائية الجزائرية بالنظر في هذا النوع من الجرائم التي ترتكب خارج الإقليم الوطني وتؤدي بإضرار الجزائر و/أو بمؤسساتها و/أو بمواطنيها.

وسنسلط الضوء على الإختصاص المحلي على النحو الآتي:

1- الإختصاص المحلي لضباط الشرطة القضائية:

كقاعدة عامة، يمارس ضباط الشرطة القضائية إختصاصهم المحلي في حدود الدائرة التي يباشرون ضمنها وظائفهم المعتادة[1]، وفي كل مجموعة سكنية في المناطق العمرانية المقسمة إلى دوائر للشرطة، فإن إختصاص محافظي وضباط الشرطة الذين يمارسون وظائفهم في إحداها يشمل كافة المجموعة السكنية أي المدينة كلها[2].

---

[1]- أحكام الإختصاص المحلي لا تمنع الضبطية القضائية من الحصول على أية معلوماتٍ خارج دائرة إختصاصها عن طريق الهاتف أو غيره من وسائل الإتصال، وهو ما ذهبت إليه محكمة النقض الفرنسية في قرارها الصادر بتاريخ 1995/01/10 تحت رقم 94-84- 687 :

Cour de cassation; Chambre criminelle, 10 janvier 1995, n° 94-84.687 Bulletin criminel 1995 N° 13 p. 31

Sommaire : Si, selon l'article 18, alinéa ler, du Code de procédure pénale, les officiers de police judiciaire n'ont, en principe, compétence que dans les limites territoriales où ils exercent leurs fonctions, rien ne leur interdit de recueillir des renseignements en dehors de leur circonscription par téléphone, télécopie ou tout autre mode de communication, la valeur des renseignements ainsi recueillis étant soumise à la discussion contradictoire des parties et à l'appréciation des juges.

وترجمة هذا المبدأ :

{إذا لم يكن لضباط الشرطة القضائية وفقًا للمادة 18 فقرة 1 من قانون الإجراءات الجزائية إختصاص إلا ضمن الحدود الإقليمية التي يباشرون فيها وظائفهم، من حيث المبدأ فإنه لا يوجد ما يمنعهم من الحصول على معلومات من خارج دائرتهم عن طريق الهاتف أو الفاكس أو غيرها من طرق الإتصالات، وتبقى قيمة المعلومات التي تم جمعها على هذا النحو خاضعة للمناقشة للأطراف ولتقدير القضاة، وللمزيد من التفصيل، ينظر: نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص-ص 81-82.

[2]- المادة 24/ 1 و5 من القانون رقم: 25-14 السالف الذكر.

إلا أنه ورد على هذه القاعدة إستثناء وهو تمديد إختصاص ضباط الشرطة القضائية إلى دائرة إختصاص المجلس القضائي الملحقون به إذا بررت حالة الإستعجال ذلك[1]، وكما يمكن أن يمتد هذا الإختصاص أيضًا في حالة الإستعجال على كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونيًا، ويجب أن يساعدهم في ذلك أحد ضباط الشرطة القضائية الذي يمارس وظائفه في إختصاص المجموعة السكنية المعنية[2]، على أنه في كلا الحالتين يتعين عليهم أن يخبروا مسبقًا وكيل الجمهورية الذي يباشرون مهمتهم في دائرة إختصاصه[3]، ولا تطبق شروط تمديد الإختصاص وضوابطه على ضباط الشرطة القضائية التابعين للمصالح العسكرية للأمن أو للمصالح المركزية للشرطة القضائية، فإن إختصاصهم وطني أي يمارسون إختصاصهم على مستوى كافة الإقليم الوطني[4].

وتم توسيع من إختصاص ضباط الشرطة القضائية وجعلته يشمل كامل الإقليم الوطني في إطار البحث ومعاينة في إحدى الجرائم[5] المنصوص عليها على سبيل الحصر بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، وفي هذه الحالة يعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميًا ويعلم وكيل الجمهورية المختص إقليمياً بذلك في جميع الحالات[6].

وقد منح المشرع الجزائري من خلال المادة المادة 25 من ق.إ.ج.ج لضباط الشرطة القضائية وتحت سلطتهم أعوان الشرطة القضائية ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره، أن يمددوا عبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الإشتباه فيهم بإرتكاب الجرائم المحددة في المادة 24 بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة

---

[1]- يذهب جانب من الفقه الجنائي إلى أن حالة الإستعجال التي تكون سندًا للتوسع في الإختصاص المكاني يجب حصرها في نطاق الحالات التي يخشى معها ضياع الدليل، إذا لم يسارع ضابط الشرطة القضائية لإتخاذ إجراءات معينة كحالات التلبس مثلًا، ويوسع جانب آخر في مدلول الإستعجال ليشمل ضرورة البحث والتحري أي الضرورة الإجرائية التي تقتضي التوسع في الإختصاص المحلي. إلا أن إعتماد حالة الإستعجال في تمكين ضابط الشرطة القضائية من الخروج على نطاق إختصاصه المحلي لم يسلم من النقد، إذ أن مثل هذه الحالة قد تستغل من طرف الضابط ليوسع في إختصاصه المحلي فيما ليس فيه داع، مما قد يعرض الحريات والحقوق الفردية للخطر ويضيع على الجماعة الوصول للحقيقة بطريق مشروع، إلا أن ما يخفف من هذا النقد أن ضابط الشرطة القضائية يعمل تحت إدارة وإشراف النيابة العامة -وكيل الجمهورية والنائب العام- ومراقبة غرفة الإتهام، بالإضافة لرقابة قضاء الموضوع حول مدى تطبيق القانون تطبيقًا صحيحًا، وللمزيد من التفصيل، ينظر:عبدالله أوهايبية، مرجع سابق، ص 327.

[2]- المادة 2/24 و3 من القانون رقم: 25-14 السالف الذكر.

[3]- المادة 4/24 من القانون رقم: 25-14 السالف الذكر.

[4]- المادة 6/24 من القانون رقم: 25-14 السالف الذكر.

[5]- يمتد إختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني إذا تعلقت الأبحاث والمعاينات بجرائم القتل العمدي، جرائم المخدرات والمؤثرات العقلية، والجريمة المنظمة عبر الحدود الوطنية، والجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، وجرائم الفساد، وجرائم التهريب، وجرائم الإتجار بالبشر، وجرائم الإتجار بالأعضاء، وجرائم تهريب المهاجرين، وجرائم إختطاف الأشخاص، طبقًا للفقرة 07 من المادة 24 من قانون الإجراءات الجزائية.

[6]- المادة 24 /8/7 من القانون رقم: 25-14 السالف الذكر.

بالمستند الإلكتروني جزءًا منها، أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من إرتكاب هذه الجرائم أو قد تستعمل في إرتكابها.

2- الإختصاص المحلي لوكيل الجمهورية:

حددت المادة 58 من ق.إ.ج الإختصاص المحلي لوكيل الجمهورية بصفة واضحة وموضوعية والتي تنص على أن: "يتحدد الإختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، أو بمحل إقامة أحد الأشخاص المشتبه فيهم إرتكابها أو المساهمة في إرتكابها، أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر، ما لم يحدد القانون إختصاصًا آخر".

وعليه فإن الإختصاص المحلي لوكيل الجمهورية يتحدد بتوافر أحد العناصر الثلاثة التالية:

أ- مكان وقوع الجريمة بدائرة إختصاص المحكمة المعين بها؛

ب- أن يكون محل إقامة المشتبه فيه أو أحد المساهمين بصفة عامة في إرتكاب الجريمة موجود بدائرة إختصاص المحكمة التي يعمل فيها؛

ج- محل القبض على أحد هؤلاء الأشخاص، حتى ولو كان هذا القبض قد حصل لسبب آخر في دائرة إختصاص المحكمة التي يعمل فيها، ما لم يحدد القانون إختصاصًا آخر.

3- الإختصاص المحلي لقاضي التحقيق:

وفيما يخص الإختصاص المحلي لقاضي التحقيق فقد نظمته المادة 70 من ق.إ.ج، والذي يتحدد بمكان وقوع الجريمة أو محل إقامة أحد المتهمين أو المشتبه فيهم إرتكابها أو المساهمة في إرتكابها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر، ما لم ينص القانون على إختصاص آخر والتي أخذت بنفس المعايير المنصوص عليها في المادة 58 من نفس القانون المذكورة آعلاه.

كما يمكن لقاضي التحقيق أن يقوم بأية عملية التفتيش أو الحجز ليلًا أو نهارًا، في أي مكان على إمتداد التراب الوطني، أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك.[1]

وفي حالة الضرورة يجوز لقاضي التحقيق أن ينتقل رفقة أمين الضبط بعد إخطار وكيل الجمهورية بمحكمته، إلى دوائر إختصاص المحاكم المجاورة للدائرة التي يباشر فيها وظيفته، للقيام بجميع إجراءات التحقيق إذا ما إستلزمت ضرورات التحقيق أن يقوم بذلك، على أن يخطر مقدمًا وكيل الجمهورية بالمحكمة التي سينتقل إلى دائرتها وينوه في محضره عن الأسباب التي دعت إلى إنتقاله.[2]

[1]- الفقرة 04 من المادة 78 من القانون رقم: 25-14 السالف الذكر.
[2]- المادة 156 من القانون رقم: 25-14 السالف الذكر.

4- المحكمة المختصة في مجال الجرائم الماسة بالمستند الإلكتروني:

حددت الفقرة الأولى من المادة 468 من ق.إ.ج.ج الإختصاص المحلي بالنظر في الجنحة محكمة مكان وقوع الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان هذا القبض قد وقع لسبب آخر.

وينشأ على مستوى محكمة مقر مجلس قضاء الجزائر قطب جزائي وطني[1] متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[2] والجرائم المرتبطة بها، كما يختص بالحكم في الجرائم المنصوص عليها في الفصل إذا كانت تشكل جنحًا[3] بما في ذلك جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.

يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وكذا قاضي التحقيق ورئيس ذات القطب، صلاحياتهم في كامل الإقليم الوطني.[4]

كما يختص وكيل الجمهورية وقاضي التحقيق ورئيس ذات القطب لدى القطب المستحدث حصريًا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الأكثر تعقيداً[5] والجرائم المرتبطة بها، والتي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها [6].

يجب إرسال التقارير الإخبارية وإجراءات التحقيق مباشرة من قبل مصالح الضبطية القضائية إلى وكيل الجمهورية لدى محكمة مقر مجلس قضاء الجزائر، ويتلقى ضباط الشرطة

---

[1]- تم إنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بموجب الأمر رقم: 21-11 المؤرخ في 25 أوت 2021 المتمم للكتاب الأول بباب سادس عنوانه "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال" من الأمر رقم: 66-155 المؤرخ في 08 جوان 1966 والمتضمن قانون الإجراءات الجزائية وتضمن المواد من 211 مكرر22 إلى 211 مكرر29، إلا أنه وبعد إلغاء الأمر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، أصبح ضمن الفصل الثالث من الباب الرابع من الكتاب الثاني ضمن المواد من 335 إلى 342.

[2]- المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال وفقًا للفقرة 03 من المادة 335 من القانون رقم: 25-14 السالف الذكر بأنها: "أي جريمة ترتكب أو يسهل إرتكابها إستعمال منظومة معلوماتية أو نظام للإتصالات الإلكترونية أو أي وسيلة أخرى، أو آلية ذات صلة بتكنولوجيات الإعلام والإتصال".

[3]- المادة 335/1و2 من القانون رقم: 25-14 السالف الذكر.

[4]- المادة 336 من القانون رقم: 25-14 السالف الذكر.

[5]- عرفت الفقرة 02 من المادة 338 من القانون رقم: 25-14 السالف الذكر الجريمة المتصلة بتكنولوجيات الإعلام والإتصال الأكثر تعقيدًا بأنها: "الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين بها، أو بسبب إتساع الرقعة الجغرافية لمكان إرتكاب الجريمة أو جسامة أثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب إستعمال وسائل تحري خاصة، أو خبرة فنية متخصصة، أو اللجوء إلى تعاون قضائي دولي".

[6]- المادة 338 من القانون رقم: 25-14 السالف الذكر.

القضائية حينئذ التعليمات منه مباشرة، وفي حالة فتح تحقيق قضائي فإنهم يتلقون الإنابات القضائية مباشرة من قاضي التحقيق المخطر بالملف.[1]

إذا تبين لوكيل الجمهورية أن الوقائع المبلغة له عملًا بأحكام المادة 345 لا تدخل ضمن إختصاصه، فإنه يصدر مقررًا بالتخلي عن الملف لصالح وكيل الجمهورية المختص إقليميًا[2]، وذات الأمر بالنسبة لقاضي التحقيق فإذا ما تبين له أن الوقائع المخطر بها لا تدخل ضمن إختصاصه يصدر أمرًا بعدم الإختصاص، إما تلقائيًا بعد أخذ رأي وكيل الجمهورية وإما بناء على إلتماسات هذا الأخير، يحول ملف الإجراءات بسعي من وكيل الجمهورية إلى النيابة العامة المختصة إقليميًا متى أصبح أمر قاضي التحقيق نهائيًا، مع بقاء الأوامر بالقبض والإيداع الصادرة عن قاضي التحقيق سارية المفعول، ولا تجدد إجراءات المتابعة والتحقيق وكذا الإجراءات الشكلية المتخذة قبل صدور الأمر بعدم الإختصاص[3].

يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وكذا قاضي التحقيق ورئيس ذات القطب، إختصاصًا مشتركًا مع الإختصاص الناتج عن تطبيق المواد 58 و70 و468 من ذات القانون بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها.[4]

يرسل وكلاء الجمهورية لدى الجهات القضائية المختصة إقليميًا وفقًا لأحكام المادة 58 من نفس القانون فورًا وبكل الطرق، نسخًا من التقارير الإخبارية وإجراءات التحقيق المنجزة من قبل الشرطة القضائية إلى وكيل الجمهورية المختص لدى القطب.[5]

كما يمكن أن يطالب وكيل الجمهورية لدى القطب الجزائي بعد أخذ رأي النائب العام لدى مجلس قضاء الجزائر بملف الإجراءات إذا اعتبر أن الجريمة تدخل ضمن إختصاصه[6]، كما يمكن له المطالبة بملف الإجراءات خلال التحريات الأولية والمتابعة والتحقيق القضائي[7]، وفي هذه الحالة يصدر وكيل الجمهورية المختص إقليميًا خلال مرحلتي التحريات الأولية والمتابعة، عند توصله بإلتماسات وكيل الجمهورية لدى القطب الجزائي المتضمنة المطالبة بملف الإجراءات مقرراً بالتخلي لصالح هذا الأخير.[8]

[1]- المادة 346 من القانون رقم: 25-14 السالف الذكر.
[2]- المادة 347 من القانون رقم: 25-14 السالف الذكر.
[3]- المادة 348 من القانون رقم: 25-14 السالف الذكر.
[4]- المادة 1/340 من القانون رقم: 25-14 السالف الذكر.
[5]- المادة 1/321 من القانون رقم: 25-14 السالف الذكر.
[6]- المادة 322 من القانون رقم: 25-14 السالف الذكر.
[7]- المادة 323 من القانون رقم: 25-14 السالف الذكر.
[8]- المادة 324 من القانون رقم: 25-14 السالف الذكر.

وفي حالة فتح تحقيق قضائي تحال إلتماسات وكيل الجمهورية لدى القطب الجزائي المتضمنة المطالبة بملف الإجراءات من قبل وكيل الجمهورية على قاضي التحقيق المخطر بالملف، ويصدر قاضي التحقيق أمرًا بالتخلي عن الملف لصالح قاضي التحقيق بالقطب الجزائي.[1]

ثانيًا: المساعدة القضائية الدولية المتبادلة

أجازت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بموجب الفقرة الأولى من المادة 25 منها للدول الأطراف أن توفر المساعدة المتبادلة لبعضها البعض على أوسع نطاق ممكن، لأغراض التحقيقات أو الإجراءات المتابعة المتعلقة بالجرائم الجنائية المتصلة بنظم ومعطيات الجهاز الإلكتروني أو بجمع الأدلة الإلكترونية[2]، وهو ما أجازت به الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات للدول الأطراف بمقتضى المادة 32 منها على تبادل المساعدة القضائية فيما بينها، بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات في البيئة الرقمية أو لجمع الأدلة الإلكترونية.

وهو ما أقره المشرع الجزائري بموجب القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر في الفقرة الأولى من المادة 16 منه، بحيث خول للسلطات المختصة تبادل المساعدة القضائية الدولية في جمع الأدلة الإلكترونية وكشف مرتكبيها، في إطار التحريات أو التحقيقات الجارية لمعاينة الجرائم الماسة بالمستند الإلكتروني.

وتتخذ المساعدة القضائية الدولية عدة صور كما يلي:

1- تبادل المعلومات:

إن من أهم غايات التعاون بين الدول، تبادل والحصول على المعلومات والمعطيات المتعلقة بالجريمة والمجرمين، مما يلزم أن يكون هناك نظام إتصال يسمح للجهات القائمة على التحقيق بجهات أجنبية، لجمع أدلة معينة أو معلومات مهمة التي غالبًا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين.

وتتم هذه المساعدة القضائية الدولية من خلال تبادل المعلومات بين الأجهزة القضائية والأمنية في مختلف الدول حول الأنشطة الإجرامية التي يباشرها مجرمو المعلوماتية بهدف تحقيق تعاون أمني فعال في مواجهتها، ويشمل ذلك تقديم المعلومات والوثائق والمواد الإستدلالية والسوابق القضائية للجناة وغيرها، التي تطلبها سلطة أجنبية وهي بصدد النظر في

[1]- المادة 325 من القانون رقم: 25-14 السالف الذكر.

[2]-Art 25 paragraphe 01 du convention sur la cybercriminalité dispose que: « Principes généraux relatifs à l'entraide 1- Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir les preuves sous forme électronique d'une infraction pénale».

جريمة ما، عن الإتهامات التي وجهت إلى شخص لا يتواجد تحت سلطتها.[1]

وفي هذا السياق أشارت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في الفقرة الأولى من المادة 26 منها، أنه يجوز لدولة طرف وبمراعاة قانونها الوطني ودون طلب مسبق، أن ترسل إلى طرف آخر معلومات يتم الحصول عليها في حال إذا ما ارتأت أن الإفصاح عن هذه المعلومات قد يساعدها في إطار التحقيقات التي تنجزها، وذلك بغرض التعاون ومساعدتها في القيام بتحقيقاتها حول الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص.[2]

وأوضحت المذكرة التفسيرية للإتفاقية أن الطرف الذي يملك معلومات قيمة ويعتقد بأنها قد تساعد طرفًا آخر في تحقيق جنائي أو إجراء جنائي، والتي لا يدرك الطرف الذي يجري التحقيق أو الإجراء بوجودها، في مثل هذه الحالات لن يتم تقديم أي طلب للمساعدة المتبادلة، لذلك تمكن الفقرة الأولى الدولة التي تتوفر لديها المعلومات من إحالتها إلى الدولة الأخرى دون طلب مسبق، وأعتبر هذا الحكم مفيدًا لأنه ثمة حاجة بموجب قوانين بعض الدول إلى هذا التقديم الإيجابي للسلطة القانونية من أجل تقديم المساعدة في حال إنعدام الطلب، ولا يكون الطرف ملزمًا بتقديم المعلومات تلقائيًا إلى طرف آخر، ويجوز له أن يمارس سلطته التقديرية في ضوء ظروف القضية قيد النظر، فضلًا عن ذلك لا يحول الكشف التلقائي للمعلومات دون قيام الطرف المفصح إذا كانت له الإختصاص القضائي بالتحقيق أو إقامة إجراءات تتعلق بالوقائع التي تم الكشف عنه.[3]

وهو ما أجازت به الفقرة الأولى من المادة 33 من الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات لأي دولة طرف ضمن حدود قانونها الداخلي وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها، إذا إعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات

---

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص377.

[2]-Art 26 paragraphe 01 du convention sur la cybercriminalité dispose que : « Information spontanée :Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propre enquetes lorsqu'elle estime que cela pourrait ader la Partie destinataire à engager ou à mener à bien des enquétes ou des procédures au sujet d'infractions pénales établies conformément à la présente convention, ou lorsque ces informations pourraient aboutir à une demande formulée par cette Partie au titre du présent chapitre».

ترجمتها:

تنص الفقرة الأولى من المادة 26 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 على أن: "المعلومات التلقائية:

1- يجوز لدولة طرف في حدود قانونها الوطني ودون طلب مسبق، أن ترسل إلى طرف آخر معلومات يتم الحصول عليها في إطار التحقيقات التي تنجزها، في حال إذا ما إرتأت أن الإفصاح عن هذه المعلومات قد يساعد الطرف المتلقي لهذه المعلومات في الشروع أو القيام بتحقيقات أو متابعات بشأن جرائم جنائية مقررة طبقًا لهذه الاتفاقية، أو أن ذلك قد يؤدي إلى تقديم طلب للتعاون من جانب تلك الدولة الطرف بموجب هذا الباب".

[3]- التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مرجع السابق، ص 43.

في الجرائم المنصوص عليها في الإتفاقية، أو قد تؤدي إلى طلب التعاون من قبل تلك الدولة الطرف.

فقد حرصت الفقرة الأولى من المادة 26 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001، والفقرة الأولى من المادة 33 من الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات، على التأكيد على إلتزام الدولة الطرف التي في حوزتها معلومات مهمة في تقديم المساعدة لدولة أخرى خلال التحقيقات الجنائية، أو تداول الدعوى العمومية في الحالة التي لا تدرك فيها السلطة القضائية في الدولة التي تجري التحقيقات الجنائية أو الملاحقة بوجود هذه المعلومات، دون الحاجة إلى تقديم طلب للمساعدة المتبادلة في تلك الحالة.[1]

وبالرجوع إلى أحكام القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر نجد المادة 17 منه تنص على أن: "تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو إتخاذ أي إجراءات تحفظية، وفقًا للإتفاقيات الدولية ذات الصلة والإتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل"، ووفقاً للمادة السابقة، يتم تبادل المعلومات في إطار مبدأ المعاملة بالمثل وإستجابة للإتفاقيات الدولية وكذا الإتفاقيات الثنائية التي صادقت عليها الجزائر، ويشمل ذلك تقديم المعلومات والوثائق التي تطلبها السلطة القضائية الجزائرية أو تلك التي تطلبها دولة أجنبية.

كما أجاز المشرع الجزائري للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته إنجاز الخبرات القضائية وتجميع المعلومات التي تحتاج إليها السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، بالإضافة إلى تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبيها وتحديد مكان تواجدهم، وهو ما تم النص عليه في المادة 14 من نفس القانون.

وقد إشترطت الفقرة 02 من المادة 18 من نفس القانون على أن تكون الإستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة، وكذا بشرط عدم إستعمالها في غير ما هو موضح في الطلب، وهو ما أكدت عليه الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في الفقرة 02 من المادة 26 منها على وجوب المحافظة على سرية تلك المعلومات أو إستخدامها وفقًا لشروط معينة تطلبها الدولة مقدمة المعلومات، وفي حال قبول الدولة الطرف المتلقية لهذه المعلومات الخاضعة للشروط وجب عليها الإلتزام بها

[1]- بوكر رشيدة، مرجع سابق، ص 409.

وإحترامه، وإذا لم يكن بإمكانها الإمتثال لهذا الطلب وجب عليها إشعار الدولة المقدمة للمعلومات بذلك والذي يبقى لها بعد ذلك خيار عدم تقديم المعلومات[1].

تشير المذكرة التفسيرية للإتفاقية مسألة قيام الطرف في بعض الظروف بإرسال المعلومات تلقائيًا فقط إذا كانت المعلومات الحساسة ستظل سرية أو إذا أمكن فرض شروط أخرى على إستخدام المعلومات، وتكون السرية على وجه الخصوص من الإعتبارات الهامة في الحالات التي قد تتعرض فيها المصالح الهامة للدولة مقدمة المعلومات للخطر إذا ما أتيحت تلك المعلومات للعموم، مثلًا حيثما تكون هناك حاجة لحماية هوية الوسيلة المستعملة لجمع المعلومات أو لإخفاء التحقيق الجاري بشأن جماعة إجرامية، وإذا كشف التحقيق المسبق أن الطرف المتلقي لا يستطيع الإمتثال لشروط يسعى إليها الطرف مقدم المعلومات، مثلًا عندما لا يستطيع الإمتثال لشروط السرية لأن المعلومات مطلوبة كدليل في محاكمة علنية يقوم الطرف المتلقي بإبلاغ الطرف المقدم الذي يبقى له بعد ذلك خيار عدم تقديم المعلومات، أما إذا وافق الطرف المتلقي مع ذلك على هذا الشرط فيجب عليه إحترامه، ومن المتوقع أن تكون الشروط المفروضة بموجب هذه المادة متوافقة مع الشروط التي يمكن أن يفرضها الطرف مقدم المعلومات، عملًا بطلب المساعدة المتبادلة من الطرف المتلقي.[2]

وهو الشرط الذي نصت عليه الفقرة 02 من المادة 33 من الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات، على أن قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، فإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين، وإذا لم تستطيع الإلتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك، والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات.

ونظرًا لعامل السرعة الذي يعتبر عامل من العوامل الرئيسية والهامة في مكافحة الجرائم الماسة بالمستند الإلكتروني، كون القدرة العالية التي يمتاز بها المجرم المعلوماتي على إخفاء

---

[1]-Art 26 paragraphe 02 du convention sur la cybercriminalité dispose que: « Information spontanée: Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou ne soient utilisées que sous certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins étre fourni. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières».

ترجمتها:

تنص الفقرة 02 من المادة 26 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 على أن: "المعلومات التلقائية:

2- يجوز للطرف الذي يقدم هذه المعلومات قبل تقديمها، أن يطلب الحفاظ على سرية تلك المعلومات أو استخدامها فقط وفقًا لشروط معينة، وإذا لم يكن بإمكان الدولة الطرف المتلقية لهذه المعلومات الإمتثال لهذا الطلب، وجب عليها إشعار الطرف المقدم للمعلومات بذلك، والذي يقرر عندئذ إذا ما كان يتعين عليه مع ذلك تقديم تلك المعلومات. في حال قبول الدولة الطرف المتلقية بالمعلومات الخاضعة للشروط، وجب عليها الإلتزام بها".

[2]- التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مرجع السابق، ص 44.

ومحو كل آثار الجريمة والتستر عنها في فترة وجيزة، تطبيقًا لذلك أبرمت إتفاقات جديدة[1] لتقليص الوقت وإختصار الإجراءات عن طريق الإتصال المباشر بين السلطات المعنية بالتحقيق، مثل الإتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويًا في حالة الإستعجال على أن يتم تأكيد هذا التبادل كتابة بعد ذلك، كما حث المجلس الأوروبي الدول الأعضاء على تيسير إتخاذ الإجراءات وإنشاء نظام الربط بين السلطة القضائية والسلطات الأجنبية، بهدف الحصول على الأدلة على وجه السرعة.[2]

وهو ما أجازت به الفقرة 03 من المادة 25 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 لكل دولة طرف في الحالات العاجلة بطلب المساعدة المتبادلة أو بوثائق عن طريق وسائل الإتصال العاجلة بما في ذلك الفاكس أو البريد الإلكتروني، بقدر ما توفره تلك الوسائل من مستويات ملائمة للأمن والتحقق من صحة البيانات بما في ذلك إستخدام التشفير عند الضرورة، مع التأكيد الرسمي بتطبيق تلك الوسائل عندما تطالب بذلك الدولة الطرف المطلوب منه تقديم المساعدة، وتقبل الدولة الطرف المطلوب منها تقديم المساعدة وتستجيب للطلب بأي من وسائل الإتصال العاجلة.[3]

وهو نفس المنحى الذي سارت عليه الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات بموجب الفقرة 03 من المادة 32 منها، إذ أجازت على ضرورة تقديم طلب المساعدة الثنائية والإتصالات المتعلقة بها بشكل خطي، ويجوز في الحالات الطارئة أن يقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الإلكتروني، على أن تضمن هذه الإتصالات القدر المعقول من الأمن والمرجعية بما في ذلك إستخدام التشفير وتأكيد الإرسال حسبما تطلب الدولة الطرف، ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الإتصالات.

فقد حثت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في الفقرة 03 من المادة 25 منها، والفقرة 03 من المادة 32 من الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات، الدول الأطراف على طلب المساعدة المتبادلة بوسائل سريعة

---

[1]- أيضًا في البند الثاني من المادة 30 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999، والمادة 15 من إتفاقية الرياض العربية للتعاون القضائي 1983، والمادة 53 من إتفاقية شينجن 1990 والخاصة بإستخدام الإتصالات المباشرة بين السلطات القضائية في الدول الأطراف، والفقرة 13 من المادة 46 من إتفاقية الأمم المتحدة لمكافحة الفساد، وللمزيد من التفصيل، ينظر: حسام محمد نبيل عبد الرؤوف مرسي، **التعاون الدولي في مكافحة الجرائم المرتكبة عبر الإنترنت (الآليات- الصعوبات- الحلول)**، أكاديمية العلوم الشرطية- الشارقة، مجلة العلوم الشرطية والقانونية، المجلد الخامس، العدد الثاني، جويلية 2014، الإمارات العربية المتحدة، ص 59.

[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص 382.

[3]-Art 25 paragraphe 03 du convention sur la cybercriminalité dispose que : « Principes généraux relatifs à l'entraide: Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification y compris le cryptage si nécessaire, avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication».

في حالات الإستعجال بما في ذلك الفاكس أو البريد الإلكتروني، على أن تضمن هذه الإتصالات سلامة المعلومات المتبادلة بين الطرفين بما في ذلك إستعمال وسائل التشفير عند الضرورة، وتعزيز ذلك بطلب رسمي لاحقًا.

وهو ما إعتمده المشرع الجزائري بموجب الفقرة 02 من المادة 16 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر الذي نص على أن: "يمكن في حالة الإستعجال ومع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية، إذا وردت عن طريق وسائل الإتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها".

2- نقل الإجراءات الجزائية:

نصت إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة الدولية العابرة للحدود لسنة 2000 في المادة 21 منها على أن: "يتعين على الدول الأطراف أن تنظر في إمكانية أن تنقل إحداها إلى الأخرى إجراءات الملاحقة المتعلقة بجرم مشمول بهذه الإتفاقية، في الحالات التي يعتبر فيها ذلك النقل في صالح التسيير السليم للعدالة، وخصوصًا عندما يتعلق الأمر بعدة ولايات قضائية، وذلك بهدف تركيز الملاحقة".[1]

يقصد بنقل الإجراءات الجزائية قيام دولة ما بمقتضى إتفاقية أو معاهدة بإتخاذ إجراءات جنائية بصدد جريمة إرتكبت في إقليم دولة أخرى بناء على طلب هذه الأخيرة متى ما توافرت شروط معينة، ويطلق على الدولة التي تطلب إتخاذ الإجراءات "الدولة الطالبة" بينما تسمى الدولة القائمة بالإجراءات "الدولة المطلوب إليها"، ومقابل ذلك تتعهد الدولة الطالبة إتخاذ الإجراءات بالمعاملة بالمثل، وإحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القضائية، ومن الشروط الواجب توافرها أن يكون اللجوء لهذا الإجراء دورًا هامًا في الوصول إلى الحقيقة المنشودة، بالإضافة إلى شرعية الإجراءات المطلوب إتخاذها، بمعنى أن تكون مقررة ومشروعة في قانون الدولة المطلوب إليها عن ذات الجريمة.[2]

ويجب أن تكون هناك إجراءات سريعة ومناسبة ونظام إتصال يسمح للجهات القائمة على التحقيق بالإتصال بجهات أجنبية لجمع أدلة معينة، ويتعين عندئذ أن تسمح الأخيرة بإجراء التحقيقات اللازمة.[3]

---

[1]- معزيز أمينة، **خصوصيات إجراءات قمع الجريمة المنظمة**، رسالة الماجستير، فرع: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2011-2012، ص-ص 98-99.

[2]- شنتير خضرة، مرجع سابق، ص 230.

[3]- سحر سعد عبد السميع محمد، مرجع سابق، ص 381.

3- الإنابة القضائية الدولية:

قد تواجه السلطة القضائية المختصة صعوبة في الحصول على دليل متعلق بالجريمة الماسة بالمستند الإلكتروني خاصة عندما يكون هذا الدليل محفوظًا على جهاز إلكتروني موجود في دولة أخرى، ولذا تعد إتفاقيات الإنابة القضائية هي السبيل الوحيد لتحصيله[1]، فالإنابة بهذا الشكل تهدف إلى تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى كسماع الشهود أو إجراء التفتيش وغيرها[2]، ومنه يتمثل هذا الإجراء في طلب تتقدم به الدولة الطالبة إلى الدولة المطلوب منها في إتخاذ إجراء من إجراءات الدعوى العمومية، من أجل الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة التي تقدمت بطلب لتعذر قيامها بهذا الإجراء بنفسها.

ومما سبق ذكره، تساعد الإنابة القضائية الدولية على عدم ضياع الأدلة والآثار المتعلقة بالجريمة المرتكبة وإلى تسهيل الإجراءات الجزائية بين الدول بصدد جريمة من الجرائم الماسة بالمستند الإلكتروني، بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية والتي تمنع الدول الأجنبية من مباشرة بعض الأعمال القضائية داخل إقليم دولة الأخرى.

ثالثًا: إتخاذ الإجراءات التحفظية

غالبًا ما يحيط المجرم المعلوماتي أفعاله غير المشروعة بسياج من الحماية الأمنية، مما يزيد من صعوبة تطبيق القواعد الإجرائية اللازمة للوصول إلى الأدلة التقنية التي قد تدينه، كما يحرص بعد إرتكاب جريمته على طمس الآثار التي قد تكشف عن وقوعها، الأمر الذي إستدعى الإتفاق على ضرورة وضع آلية تضمن الحفاظ على هذه المعطيات إلى حين تنفيذ طلب المساعدة المتبادلة والذي قد يستغرق وقتًا أطول، وهو ما أقر به المشرع الجزائري طبقًا للمادة 17 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر التي تنص على أن:"...إتخاذ أي إجراءات تحفظية وفقًا للإتفاقيات الدولية ذات الصلة والإتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل".

وهو ما أقرت به المادة 29 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001[3]، والمادة 37 من الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية

[1]- أومدور رجاء، **خصوصية التحقيق في مواجهة الجرائم المعلوماتية**، أطروحة الدكتوراه الطور الثالث ل.م.د، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي -برج بوعريريج، 2020-2021، ص 222.

[2]- عبدالله سيف الكيتوب، **الأحكام الإجرائية لجريمة الإحتيال المعلوماتي**، د.ر.ط، 2013، دار النهضة العربية، القاهرة-مصر، ص 205.

[3]-Art 29 paragraphe 01 du convention sur la cybercriminalité dispose que : «Conservation rapide de données informatiques stockées: Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la=

المعلومات[1]، حيث بمقتضى هذه الآلية يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى أن تحصل على التحفظ العاجل على المعطيات المخزنة بواسطة المنظومة المعلوماتية الذي يقع ضمن إقليم الدولة المطلوب منها، والتي تنوي أن تقدم بشأنه طلبًا بالمساعدة المتبادلة من أجل البحث عن معطيات أو النفاذ إليها أو مصادرتها أو تأمينها أو كشفها.

وعند إستلام الطلب من الطرف الآخر يقوم الطرف المطلوب منه المساعدة بإتخاذ كافة الإجراءات المناسبة، وذلك لتعجيل حفظ المعطيات المحددة وفقًا لقانونها الوطني، ولغايات الإستجابة للطلب فلا يجوز تقييد توفير هذا الحفظ بشرط إزدواجية التجريم.[2]

ويجوز لأي دولة الطرف أن تحتفظ بحقها بالرفض طلب الحفظ بشرط إزدواجية التجريم بالنسبة للجرائم غير تلك المنصوص عليها في الإتفاقيتين، في الحالات التي يتوافر لديها فيها أسباب للإعتقاد بأنه يتعذر في وقت الكشف أو الإفصاح عن هذه المعلومات إستيفاء الشرط الخاص بإزدواجية التجريم.[3]

على خلاف ذلك لا يجوز للطرف متلقي الطلب أن يرفض طلبًا للحفظ إلا إذا كان تنفيذه يمس بسيادته أو أمنه أو نظامه العام أو مصالحه الأساسية الأخرى، أو عندما يعتبر الجريمة جريمة سياسية أو جريمة ذات الصلة بجريمة سياسية، أو حينما تدرك الدولة الطرف المطلوب منها المساعدة بأن الحفظ لن يضمن توافر المعطيات مستقبلًا أو أنه سيهدد السرية أو يلحق الضرر بالتحقيقات التي تنجزها الدولة الطرف مقدمة الطلب، مما يستوجب إشعار الطرف مقدم

=conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données ».

[1]- تنص الفقرة الأولى من المادة 37 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات: لأي دولة طرف أن تطلب من دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات تقع ضمن إقليمها، بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلبًا بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات".

[2]-Art 29 paragraphe 03 du convention sur la cybercriminalité dispose que : «Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation ».

تنص الفقرة 03 من المادة 37 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "عند إستلام إحدى الدول الأطراف الطلب من دولة طرف أخرى، فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل عاجل بحسب قانونها الداخلي، ولغايات الإستجابة إلى الطلب فلا يشترط وجود إزدواجية التجريم للقيام بالحفظ".

[3]-Art 29 paragraphe 04 du convention sur la cybercriminalité dispose que : «Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser qu'au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie ».

تنص الفقرة 04 من المادة 37 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: " أي دولة طرف تشترط وجود إزدواجية التجريم للإستجابة لطلب المساعدة، يجوز لها في حالات الجرائم عدا المنصوص عليها في الفصل الثاني من هذه الإتفاقية، أن تحتفظ بحقها برفض طلب الحفظ حسب هذه المادة، إذا كان هناك سبب للإعتقاد بأنه لن يتم تلبية شرط إزدواجية التجريم في وقت الكشف".

الطلب على وجه السرعة لتحدد بعدها مدى إمكانية تنفيذ الطلب.[1]

وألزمت كل من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 والإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات ضمان الإحتفاظ بالمعطيات المحفوظة لمدة لا تقل عن ستين (60) يومًا، ريثما تمكن الدولة الطرف الطالبة من تسليم طلب يسعى للبحث في المعطيات والنفاذ إليها ومصادرتها وتأمينها أو الكشف عنها، وبعد إستلام مثل هذا الطلب يجب إستمرار بالإحتفاظ بالمعطيات في إنتظار صدور قرار بشأن ذلك الطلب.[2]

كما أجازت المادة 30 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001[3]، والمادة 38 من الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية

---

[1]-Art 29 paragraphe 05, 06 du convention sur la cybercriminalité dispose que: « 5. En outre, une demande de conservation peut être refusée uniquement :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

a. si la Partie requise estime que le fait d'accéder de la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels

6. Lorsque la Partie requise estime que la conservation simple ne suffira pas pour garantir la disponibilité future des données, compromettra la confidentialité de l'enquête de la Partie requérante ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande ».

- تنص الفقرتين 05 و06 من المادة 37 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "بالإضافة لذلك، يمكن رفض طلب الحفظ إذا:

أ- تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية؛

ب-إعتبار الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها.

حيثما تعتقد الدولة الطرف المطلوب منها المساعدة بأن الحفظ لن يضمن التوفر المستقبلي للمعلومات أو سيهدد سرية تحقيقات الدولة الطرف الطالبة لها أو سلامتها، فيجب عليها إعلام الدولة الطرف الطالبة لها لتحدد بعدها مدى إمكانية تنفيذ الطلب".

[2] -Art 29 paragraphe 07 du convention sur la cybercriminalité dispose que : «Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins 60 jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande ».

- تنص الفقرة 07 من المادة 37 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "أي حفظ ناجم عن الإستجابة للطلب المذكور في الفقرة (1) يجب أن يكون لفترة لا تقل عن 60 يومًا، من أجل تمكين الدولة الطرف الطالبة من تسليم طلب البحث أو الوصول أو الضبط أو التأمين أو الكشف للمعلومات، وبعد إستلام مثل هذا الطلب يجب الإستمرار بحفظ المعلومات حسب القرار الخاص بالطلب".

[3]-Art 30 du convention sur la cybercriminalité dispose que : «Divulgation rapide de données conservées:

1. Lorsqu'en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de service et la voie par laquelle la communication a été transmise.

2. La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b. si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels ».

المعلومات[1]، في حال إكتشفت الدولة الطرف المطلوب منها المساعدة أثناء تنفيذ طلب المساعدة من أجل التحفظ على المعطيات المتعلقة بحركة سير والمتعلقة بإتصال محدد بأن أحد مقدمي الخدمات في دولة أخرى مشتركًا في نقل الإتصال، تقوم الدولة الطرف المطلوب منها المساعدة على الفور بالكشف عن القدر الكافي من حركة السير للمعطيات لتحديد هوية مقدم الخدمة والمسار الذي تم من خلاله ذلك الإتصال، فضلًا عن إمكانية الإمتناع عن الكشف المعطيات المتعلقة بحركة سير إذا تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها المساعدة أنها تشكل جريمة سياسية، أو إذا كان تنفيذ الطلب يمثل إنتهاكًا لسيادة الدولة أو أمنها أو نظامها أو مصالحها.

الفرع الثاني: آلية تسليم المجرمين في مكافحة الجرائم الماسة بالمستند الالكتروني

نظرًا لأهمية آلية تسليم المجرمين، فقد تم تكريسها دستوريًا بموجب أحكام المادة 50 من الدستور الجزائري سنة 2020[2]، التي تنص على أن: "يتمتع كل أجنبي يتواجد فوق التراب الوطني بشكل قانوني بحماية القانون لشخصه وأملاكه. لا يمكن تسليم أحد إلا بمقتضى إتفاقية دولية مصادق عليها أو بموجب قانون. لا يمكن في أي حال تسليم أو إبعاد أي لاجئ سياسي إستفاد قانونًا من حق اللجوء".

وتتمثل آلية تسليم المجرمين في مجموعة من القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عملية التسليم وفقًا لقوانينها الوطنية وتعهداتها لأجل إتمام عملية التسليم، بهدف التوفيق بين المحافظة على حقوق الإنسان وحريته وبين تأمين الصالح العام الناشئ عن ضرورات التعاون الدولي في مكافحة الجريمة بحيث لا يفلت أي مجرم من العقاب، وهذه الإجراءات تتقاسمها الدولتان الطالبة والمطالبة، كما وأنها ليست مطلقة بل مقيدة ببعض الإلتزامات الدولية.[3]

ويقصد بآلية تسليم المجرمين إعادة الشخص المطلوب إلى الدولة صاحبة الإختصاص بمحاكمته، فهو إجراء تطلب بمقتضاه دولة من دولة أخرى تسليم شخص موجود على إقليمها لتحاكمه أو لتنفذ عقوبة محكوم بها عليه، ولكي يتم ذلك يشترط أن يكون الشخص المطلوب

---

[1]- تنص المادة 38 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة:

1- حيثما تكتشف الدولة الطرف المطلوب منها -في سياق تنفيذ الطلب حسب المادة السابعة والثلاثين لحفظ معلومات تتبع المستخدمين الخاصة بإتصالات معينة- بأن مزود خدمة في دولة أخرى قد إشترك في بث الإتصال، فيجب على الدولة الطرف المطلوب منها أن تكشف للدولة الطرف الطالبة قدرًا كافيًا من معلومات تتبع المستخدمين من أجل تحديد مزود الخدمة ومسار بث الإتصالات.

2- يمكن تعليق كشف المعلومات تتبع المستخدمين حسب الفقرة (1) إذا:

أ- تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية؛

ب- إعتبرت الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سلامتها أو أمنها أو نظامها أو مصالحها".

[2]- المرسوم الرئاسي رقم: 20-442 المؤرخ في 30 ديسمبر 2020 ، ج.ر.ج.ج.ش العدد 82، سنة 2020.

[3]- سحر سعد عبد السميع محمد، مرجع سابق، ص 416.

تسليمه قد إرتكب جريمة وصدر ضده حكم بالإدانة، وقبل أن يبدأ في تنفيذ العقوبة يفر خارج إقليم الدولة التي أصدرت الحكم فترسل في طلبه لتنفيذ الحكم الصادر عليه، أو أن يكون الشخص المطلوب تسليمه قد إرتكب جريمة وقبل أن يكتشف أو يضبط يفر خارج إقليم الدولة التي إرتكب فيها الجريمة، فتقدم هذه الأخيرة طلب تسليم إلى الدولة التي فر إليها من أجل محاكمته بها وفقًا لقانونها وأمام قضائها.[1]

نصت المادة 24 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001[2] على تطبيق آلية التسليم إلا في حالة إذا ما كانت الجرائم المنصوص عليها في هذه الإتفاقية معاقب عليها بموجب قوانين كلا من الطرفين المعنيين بعقوبة سالبة للحرية لمدة أقصاها سنة واحدة (01) على الأقل أو بعقوبة أشد، وتطبق العقوبة الأقل في حالة وجود إتفاقية

[1]- لعوارم وهيبة، **نظام تسليم المجرمين دراسة تحليلية مقارنة بين المواثيق الدولية التشريع الجزائري والتشريعات المقارنة**، كلية الحقوق والعلوم السياسية، جامعة برج بوعريريج، مجلة البيبان للدراسات القانونية والسياسية، المجلد 01، العدد الأول، جوان 2016، الجزائر، ص 111.

[2] -Art 24 du convention sur la cybercriminalité dispose que: «Extradition:

1. a. Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b. Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, c'est la peine minimum prévue par ce traité ou cet arrangement qui s'applique.

2. Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3. Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4. Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5. L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6. Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte en temps utile de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable conformément à la législation de cette Partie.

7. a. Chaque Partie communique au Secrétaire général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b. Le Secrétaire général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre ».

بشأن تسليم المجرمين أو إذا ما كان توجد تشريعات موحدة أو ذي صلة بالمعاملة بالمثل، وقد إعتبرت الإتفاقية الجرائم المنصوص عليها في المواد من 2 إلى 11 الجرائم التي يجب تسليم المجرمين فيها إذا ما وجدت إتفاقية لتسليم المجرمين بين الأطراف[1]، وتدمج هذه الجرائم على وجه الإلزام بوصفها جرائم تستوجب تسليم المجرمين في كل إتفاق يعقد بينهم أو من خلالهم لتسليم المجرمين[2].

وفي حالة عدم وجود إتفاقية تسليم المجرمين بين الأطراف يجوز إعتبار هذه الإتفاقية الأساس القانوني لعملية التسليم، وبالنسبة للدول التي لا تجعل تسليم المجرمين مشروط على إتفاقية تسليم فإنهم بإنضمامهم لهذه الإتفاقية يعتمدون الجرائم المنصوص عليها في الإتفاقية كجرائم يجوز فيها تسليم المجرمين، ويخضع تسليم المجرمين لقانون الدولة المطلوب منها التسليم أو إتفاقية تسليم المجرمين واجبة التطبيق، وفي حالة الرفض بسبب الجنسية أو الإختصاص القضائي فإن الدولة المراد التسليم منها أن تحيل الدعوى لسلطاتها المختصة وإبلاغ النتيجة للطرف للدولة الطالبة، وعلى الدول عند التوقيع أن تخطر السكرتير العام لمجلس أوروبا بإسم السلطة المسؤولة عن طلبات التسليم.[3]

ونصت الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات على إجراء تسليم المجرمين، وقد أشارت المادة 31 منها إلى جواز الإعتداد بالإتفاقية كأساس قانوني بين الدول الأطراف في مسألة تسليم المجرمين، وحددت شروط التسليم بألا تكون الجريمة المطلوب فيها التسليم أن لا تقل عقوبتها عن عقوبة سالبة للحرية لمدة سنة (01) أو بعقوبة أشد، فضلًا عن خضوع التسليم للشروط المنصوص عليها في الدولة التي يقدم إليها طلب التسليم، مع تقرير حق الدول الأطراف في رفض طلب التسليم مع التعهد بتوجيه الإتهام للجناة الذين يرتكبون جرائم معاقب عليها وفقًا لقانون الدولتين لا تقل عن سنة (01) أو بعقوبة أشد لدى أي من الدولتين.[4]

المطلب الثاني: آليات التعاون الأمني في مجال الجرائم الماسة بالمستند الإلكتروني

يعد الطابع العابر للحدود الوطنية من أبرز السمات التي تميز الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، ويقصد بذلك أن آثار هذه الجرائم لا تقتصر على النطاق الإقليمي للدولة بل قد تمتد إلى دول أخرى مما يترتب عليه صعوبة في جمع الأدلة اللازمة لإثباتها وتعقب مرتكبيها، مما شكل ذلك تحديًا كبيرًا أمام السلطات القضائية في التصدي لها رغم الجهود المبذولة في مكافحتها، وهو ما يجعل من التعاون الدولي ضرورة حتمية لمواجهة هذا النوع من الجرائم والتصدي لها بفعالية.

[1]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 81.
[2]- بن شهرة شول، مرجع سابق، ص364.
[3]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 81.
[4]- نفس المرجع، ص 82.

الفرع الأول: المنظمة الدولية للشرطة الجنائية (الأنتربول)

تعد المنظمة الدولية للشرطة الجنائية (الأنتربول) الآلية الفعالة والإطار الأنسب في مكافحة الجرائم المعلوماتية التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، نظرًا لما تقدمه من إمكانية تعقب وضبط لمقترفي الجرائم على إختلاف أنواعها عبر مختلف دول العالم، وتسليمهم إلى السلطات القضائية المختصة بغية محاكمتهم وتوقيع العقوبة عليهم.

انضمت الجزائر إلى المنظمة الدولية للشرطة الجنائية (الأنتربول) في أوت سنة 1963، ممثلة بالمكتب المركزي الوطني (BCN) تحت وصاية مباشرة لمديرية العامة للأمن الوطني، ويباشر مهامه طبقًا لنصوص التشريع الوطني ملتزمًا بالإطار القانوني المسير للمنظمة الدولية للشرطة الجنائية (الأنتربول).[1]

وتتمثل أهداف المنظمة الدولية للشرطة الجنائية (الأنتربول) في:

- تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان؛
- إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام وفي مكافحتها.[2]

وتستعمل وظيفتين رئيسيتين لتحقيق أهدافها:

- التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم، وتسليمهم للدول التي تطلبهم[3]؛

- يجمع الإنتربول المعلومات عن الجرائم الماسة بالمستندات الإلكترونية ويحفظها ويحللها، ويتبادلها مع جميع بلدانه الأعضاء عبر منظومة الإنتربول العالمية للإتصالات، ويتم ذلك التعاون من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة[4]، وذلك عن طريق ما يلي:

- زيادة تبادل المعلومات بين الدول الأعضاء بشأن الأساليب الإجرامية المتبعة في الجرائم الماسة بالمستندات الإلكترونية عن طريق الفرق العاملة الإقليمية وحلقات العمل التدريبية، وقد تم إنشاء نقاط إتصال مستمرة ويمكنها تلقي أو تقديم المعلومات وطلبات المساعدة، وتعتبر شبكة

---

[1]- **الجزائر في المنظمة الدولية للشرطة الجنائية –انتربول منذ 1963**، الشرطة المديرية العامة للأمن الوطني، مجلة الشرطة المديرية العامة للأمن الوطني، العدد 119، جويلية/أوت 2013، الجزائر، ص 52.

[2]- المادة 02 من القانون الأساسي للمنظمة الدولية للشرطة الجنائية الانتربول المعتمد أثناء الدورة 25 للجمعية العامة للأمم المتحدة بفيينا سنة 1956، الموجود على الرابط:

file:///C:/Users/SAM/Downloads/01%20A%20Constitution_2023.pdf

[3]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 150.

[4]- سحر سعد عبد السميع محمد، مرجع سابق، ص 394.

النقاط المرجعية المركزية الوطنية شرطًا أساسيًا لإستحداث منظومة إنذار مبكر، وقد بادر أكثر من 120 مكتبًا مركزيًا إلى تعيين نقاط مرجعية مركزية وطنية[1]؛

- تعمل المنظمة الدولية للشرطة الجنائية (الأنتربول) بوضع قائمة إسمية لضباط متخصصين يمكن الإستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية بما في ذلك الجرائم الماسة بالمستند الإلكتروني، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال هذا النوع من الجرائم من خلال خلق فرق عمل وورشات تكوين، ولقد أنشأت هذه المنظمة خلال سنة 2004 وحدة خاصة لمكافحة جرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته.[2]

الفرع الثاني: على المستوى الإقليمي

لقد ساهمت العديد من الأجهزة على المستوى الإقليمي في محاولة الدعم والتنسيق وتطوير آساليب التعاون لمكافحة الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص على المستوى الإقليمي، من خلال الدراسات وتقديم المساعدات وتطوير التعاون بين الدول الأعضاء في هذه المنظمات، بما يحقق المواجهة الفعالة لهذه الظاهرة الإجرامية المستجدة.

أولًا: الشرطة الأوروبية (اليوروبول)

تعتبر الشرطة الأوروبية (Europol) وليد ونتاج سيطرة المنظمة الدولية للشرطة الجنائية (الأنتربول) على الساحة الأوروبية لفترة زمنية طويلة، وقد أقترح إنشاءه من قبل ألمانيا أمام المجلس الأوروبي سنة 1991 بمناسبة إنعقاد مؤتمر لوكسمبورج، غير أنه تجسد فعليًا سنة 1995 وذلك بعد مصادقة دول المجلس الأوروبي على إتفاقية ماستريخت في 29 جويلية 1995 ليتخذ لاهاي مقرًا له.[3]

هو أحد أجهزة مكافحة الجرائم الماسة بالمستندات الإلكترونية عن طريق معالجة المعلومات المرتبطة بها على مستوى الإتحاد الأوروبي، وكذا بتسهيل تبادل تلك المعلومات عن طريق تزويد المحققين ومدعم بمساعداته التقنية[4]، وأيضًا قام بإنشاء وحدات ومراكز تابعة له بغرض توفير منصة لمديري قسم التحقيقات والملاحقات القضائية، وكذا تطوير وتعزيز

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 395.
[2]- محمود سعد عبد المجيد، مرجع سابق، ص 470.
[3]- ربيعي حسين، مرجع سابق، ص 152.
[4]- سحر سعد عبد السميع محمد، مرجع سابق، ص 395.

إستراتيجية منسقة داخل الإتحاد الأوروبي لجعل الفضاء الرقمي مكانًا آمنًا للمواطنين في الإتحاد الأوروبي وحكوماته ومؤسساته.[1]

كما يقوم اليوروبول بتقديم المساندة والدعم للدول الأعضاء ومساعدتها في حل القضايا الجنائية بشكل سريع، من خلال إرساله فرق من الخبراء والمحللين الجنائيين التابعين له للمشاركة في التحقيقات التي تجريها الدولة، ويشرف على اليوروبول مجلس الوزراء لشؤون العدل والداخلية الذي يتألف من وزراء العدل والشؤون الداخلية من جميع الدول الأعضاء في الإتحاد الأوروبي.[2]

ثانيًا: وحدة التعاون القضائي الأوروبية (الأوروجيست)

وحدة التعاون القضائي الأوروبية المعروفة بإسم الأوروجيست (Eurojust)، هو جهاز أنشئ في 28 فيفري 2002 ويعمل على مستوى أوروبا إلى جانب اليوروبول في مجال مكافحة جميع أنواع الجرائم، وينعقد إختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الإتحاد الأوروبي أو دولة أخرى من العالم الثالث أو دولة عضو من الرابطة الأوروبية.[3]

وفي جوان سنة 2013 قدمت المفوضية الأوروبية إقتراح إلى البرلمان والمجلس الأوروبيين بخصوص اللائحة الجديدة توفر الإطار القانوني الجديد للأوروجيست بديلًا للقانون السابق لسنة 2002 والذي مسته عدة تعديلات، وبعد مفاوضات مكثفة إعتمد البرلمان والمجلس الأوروبيين اللائحة الجديدة للأوروجيست في نوفمبر سنة 2018 والتي أصبحت قابلة للتطبيق في 12 ديسمبر 2019، وبذلك أصبح بإمكان مكافحة مستويات المتصاعدة من الجرائم بالغة الخطورة العابرة للحدود والتي تعد الجرائم الماسة بالمستند الإلكتروني إحداها.[4]

ويعد الأوروجيست وحدة للتعاون القضائي والشرطي في مكافحة الجرائم الخطيرة، ومهمته الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات، وله من الصلاحيات ما يؤهله لفتح تحقيقات ومباشرة متابعات جنائية، ويعد بمثابة الدعامة الفعالة في مجال التحقيقات والمطاردات التي تقوم بها السلطات القضائية الوطنية وخصوصًا فيما يتعلق بالإجرام المعلوماتي.[5]

---

[1]- شنتير خضرة، مرجع سابق، ص 262.

[2]- محمد كمال محمود الدسوقي، **الحماية الجنائية لسرية المعلومات الإلكترونية دراسة مقارنة**، الطبعة الأولى، 2015، دار الفكر والقانون، مصر، ص138.

[3]- محمود سعد عبد المجيد، مرجع سابق، ص-ص 473-474

[4]- شنتير خضرة، مرجع سابق، ص-ص 265-266.

[5]- محمود سعد عبد المجيد، مرجع سابق، ص 474.

كما يقوم بتسهيل تنفيذ طلبات التعاون القضائي والقرارات في هذا المجال، كما يجوز أن يطلب على أساس مسبب إلى السلطات المختصة في الدول الأعضاء المعنية إتخاذ تدابير تحقيق خاصة أو أي إجراء آخر يبرره التحقيق أو الإدعاء، وتشكيل فريق تحقيق مشترك وفقًا لأدوات التعاون ذات الصلة وتزويدها بجميع المعلومات اللازمة لممارسة مهامه، ويقوم الأوروجيست أيضًا بتقديم آراء في حدود صلاحياته إلى اليوروبول بعد دراسة التحليلات التي أجراها بمبادرة منه أو بناء على طلب مكتب المدعي العام الأوروبي.[1]

ثالثًا: شنجن

تم إنشاء منطقة شنجن بموجب معاهدة (SCENGEN) وتم توقيعها في 14 جوان 1985 والتوقيع على إتفاقية تطبيق لتلك المعاهدة في 19 جوان 1990، وقد إستحدثت هذه الإتفاقية وسيلتين جديدتين تتمثل في مراقبة المشتبه فيهم عبر الحدود وملاحقة المجرمين، وذلك بهدف تعزيز التعاون الأمني الأوروبي لمواجهة التحديات الأمنية التي تفرضها الظروف المستجدة منها الجرائم الماسة بالمستند الإلكتروني.[2]

يتكون نظام معلومات شنجن من قسم مركزي مقره مدينة ستراسبورغ وأقسام وطنية في كل دولة من الدول المنظمة، كذلك به بنك معلومات كبير تسجل فيه المعلومات التي ترسلها إليه قوات الشرطة والسلطات القضائية في كل دولة، ومن بين هذه المعلومات عناوين الأفراد سواء أولئك المطلوب تسليمهم من قبل دول أخرى أو من دخول أراضي دولة ما أو المعلن إختفاؤهم أو المطلوب تقديمهم للعدالة بأمر قضائي لأي سبب كان.[3]

رابعًا: المنظمة الإفريقية للشرطة الجنائية (الأفريبول)

تهدف منظمة الأفريبول (Afripol) المعروفة رسميًا بإسم المنظمة الإفريقية للشرطة الجنائية إلى تنسيق التعاون الشرطي بين الدول الإفريقية الأعضاء، وكذا العمل على تشجيع وتكوين خبراء ومتخصصين بإنشاء مراكز إفريقية لتدريبهم وفقًا لنص المادة الثالثة من النظام الأساسي لآلية الإتحاد الإفريقي للتعاون الشرطي، وهي تقوم بعدة مهام من بينها مكافحة الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص من خلال تبادل المعلومات والإستخبارات وفقًا لما ورد في الفقرة (د) من المادة الرابعة من النظام الأساسي للأفريبول والتي تنص على أن: "تيسير تبادل أو تقاسم المعلومات أو الإستخبارات، لمنع ومكافحة الجرائم المنظمة عبر الوطنية والإرهاب والجريمة السيبرانية".[4]

[1]- شنتير خضرة، مرجع سابق، ص 267.
[2]- عائشة بن قارة مصطفي، مرجع سابق، ص-ص 260-261.
[3]- سحر سعد عبد السميع محمد، مرجع سابق، ص-ص 396-397.
[4]- محمود سعد عبد المجيد، مرجع سابق، ص 475.

والإهتمام بتطوير قدرات ضباط الشرطة في الدول الإفريقية الأعضاء عن طريق برامج متطورة لتدريبهم من خلال تأسيس مراكز إمتياز إفريقية، وأيضًا تعزيز التنسيق مع الهياكل المماثلة في مكافحة ومنع الجريمة، وكذا تشجيع المساعدة التقنية المتبادلة ذات الكفاءة والخبرة الواسعة وتحسين الكفاءة وفاعلية ضباط الشرطة وتسهيل المساعدة القضائية المتبادلة بالتنسيق والتعاون مع الآليات العملياتية الآخرى على مستوى الإقليمي أو الدولي، بهدف دعم إستراتيجية التعاون والتنسيق بين مختلف تلك الآليات وكذا تطوير الآليات القارية لمنع الجريمة ووضع إستراتيجية إفريقية منسقة لمنع ومكافحة مختلف أنواع الجرائم البالغة الخطورة كالجرائم الماسة بالمستند الإلكتروني.[1]

ومن أجل تعزيز قدرات ضباط الشرطة في الدول الإفريقية الأعضاء أقامت تعاونًا مع المنظمات الدولية بما في ذلك المنظمة الدولية للشرطة الجنائية (الأنتربول)، من خلال برنامج دعم الإنتربول للإتحاد الأفريقي (ISPA) ومع منظمات الشرطة كالشرطة الفيدرالية الألمانية وكذا المنظمات الوطنية والإقليمية، وكذا المساعدة في تحقيق العديد من المشاريع (Africa-Cyber Surg) وشراء أجهزة الفرز الرقمي (SPEKTOR) وتدريب سبع دول وشراء العديد من التراخيص (CHAINALYSIS) وشراء تراخيص أدوات (CYBERBELT) وتدريب البلدان المستفيدة.[2]

خامسًا: مجلس وزراء الداخلية العرب

أنشأ مجلس وزراء الداخلية العرب المكتب العربي للشرطة الجنائية في سنة 1965 بناء على الإتفاقية الخاصة بإنشاء المنظمة العربية للدفاع الإجتماعي ضد الجريمة، حيث كان مكتب الشرطة الجنائية في دمشق أحد مكاتبها المتخصصة ويمارس هذا المكتب نشاطه من خلال ثلاث وزارات الداخلية والعدل والشؤون الإجتماعية على مستوى الدول العربية.[3]

بهدف تعزيز وتوسيع التعاون بين أجهزة الشرطة في الدول الأعضاء في مكافحة الجرائم وملاحقة مقترفيها طبقًا للقوانين والأنظمة المعمول بها في كل دولة[4]، بالإضافة إلى تقديم المعونة التي تطلبها الدول الأعضاء من أجل دعم وتطوير أجهزة الشرطة[5].

---

[1]- شنتير خضرة، مرجع سابق، ص 260.

[2]- الموقع الرسمي المنظمة الإفريقية للشرطة الجنائية الأفريبول، تاريخ التصفح: 2024/05/01، الساعة 15:48، رابط الموقع:

https://afripol.africa-union.org/ar /

[3]- محمد كمال محمود الدسوقي، مرجع سابق، ص 140.

[4]- عائشة بن قارة مصطفى، مرجع سابق، ص 261.

[5]- محمد كمال محمود الدسوقي، مرجع سابق، ص- ص 140-141.

خلاصة:

إن الطبيعة الخاصة للأدلة الإلكترونية وقابليتها السريعة للمحو أو التعديل أو الإتلاف، تستلزم ضرورة إتخاذ وسائل ملائمة لتشجيع التعاون سواء على المستوى الوطني أو الدولي لمكافحة الجرائم محل دراستنا.

ويتطلب ذلك إستقطاب الخبراء المتخصصين في الجرائم الماسة بالمستند الإلكتروني، لأن في كثير من الأحيان تواجه عملية إستخلاص الدليل الإلكتروني نقص في الخبرة الفنية والتقنية لدى سلطات التحري والتحقيق، كما يعتمد التحقيق الجنائي على شهادة الشهود، فغالبًا ما يكون للشهادة أثناء التحقيق الجنائي دور حاسم، حيث يمكن أن تؤثر في إصدار الحكم بالإدانة أو بالبراءة، لأن يسعى الجاني جاهدًا لإخفاء أفعاله فور إرتكاب الجريمة، كما يحرص على إخفاء الأدلة عن الأنظار، ولأن الشاهد يدلي بأقواله مباشرة بعد وقوع الحادث، مما يساهم في الحفاظ على دقة المعلومات قبل أن يتم العبث بالأدلة، أو يتأثر الزمن على وضوح التفاصيل المتعلقة بالواقعة.

ونظرًا للطابع العابر للحدود للجرائم الماسة بالمستند الإلكتروني، لم تكن الآليات الوطنية وحدها قادرة على مواجهة هذا النوع من الإجرام، لذلك إستدعى الأمر إستحداث نصوص قانونية تتعلق بالتعاون والمساعدة القضائية الدولية المتبادلة لمكافحة هذه الجرائم والتصدي لها، وهو ما سيسهم بشكل كبير في الكشف عن مرتكبي هذه الجرائم الخطيرة، كما إستلزم الأمر أيضًا تطوير آليات تنسيق وتعاون دولي وإقليمي، تتكاثف فيه كل الجهود وتتحد من أجله كل القوى لإيجاد آليات مكافحة فعالة وناجعة لهذه الظاهرة الإجرامية.

الفصل الثاني:

إجراءات إستخلاص الدليل الإلكتروني في الجرائم الماسة بالمستند الإلكتروني

تمهيد:

تعد الطبيعة غير المرئية للأدلة الإلكترونية من أبرز الإشكالات التي تواجه سلطات التحري والتحقيق، إذ إن هذا النوع من الجرائم لا يخلف آثارًا مادية ملموسة تدل على مرتكبيها كما هو الحال في الجرائم التقليدية، فالجرائم الماسة بالمستند الإلكتروني غالبًا ما تقع في بيئة رقمية إفتراضية خارج إطار الواقع الملموس مما يجعل من الصعب تتبع مرتكبيها إعتمادًا على الوسائل التقليدية، خلافًا للجريمة التقليدية التي لها مسرح تجري عليه الأحداث تخلف أثارًا مادية تقوم عليها الأدلة، وهذا المسرح يعطي المجال أمام سلطات التحري والتحقيق في الكشف عن الجريمة، الأمر الذي إستلزم ضرورة ظهور نوع من التحدي في تصدي لهذا النوع من الجرائم.

نظرًا لكون القواعد الإجرائية التقليدية لم تعد قادرة على إثبات هذا النوع من الجرائم، وأصبحت عاجزة عن ملاحقة مرتكبيها خاصة أنها ترتكب في الخفاء وعن بعد، ما يجعل كشفها وإثباتها وتحديد هوية المساهمين فيها أمرًا بالغ الصعوبة، كما أن الوصول إلى الأثر المادي للجريمة يعد تحديًا نظرًا للخصائص التي تميز الأدلة المستخلصة منها، كل ذلك شكل عائقًا أمام السلطة القضائية في مواجهتها والتصدي لها، بالتالي أدت هاته العوائق إلى صعوبة تكوين إقتناع الشخصي للقاضي الجزائي، الأمر الذي إستلزم بضرورة إيجاد وسائل حديثة وجديدة تختلف عن الطرق التقليدية لمكافحتها.

بالإضافة إلى ما يستخدمه المجرم المعلوماتي من أساليب أمنية وتدابير حماية فنية تحول دون كشف أمره، فإنه غالبًا ما يحيط أفعاله غير المشروعة بسياج من الحماية قبل إرتكابه لها، مما يزيد من صعوبة تطبيق القواعد الإجرائية المتاحة للبحث عن الأدلة الإلكترونية التي يمكن أن تدينه، كما يحرص بعد إرتكاب الجريمة على محو آثارها التي تدل على وقوعها الأمر الذي يحول دون إثباتها ويعيق إدانته، مما يشكل عائقًا كبيرًا أمام سلطات البحث والتحقيق أثناء محاولتها تطبيق للقواعد الإجرائية المقررة لإستخلاص الأدلة.

وفضلاً عما سبق ذكره إرتأينا تقسيم دراستنا إلى مبحثين، نتطرق إلى الإجراءات التقليدية والتقنية لإستخلاص الدليل الإلكتروني في (المبحث الأول)، أما (المبحث الثاني) فقد خصصناه إلى الإجراءات المستحدثة لإستخلاص الدليل الإلكتروني.

المبحث الأول: الإجراءات التقليدية والتقنية لإستخلاص الدليل الإلكتروني

يسهم الإنتقال للمعاينة في جمع الأدلة المرتبطة بالجريمة محل التحقيق وضبط كل ما يلزم لكشف الحقيقة، قبل أن تمتد إليه يد العبث أو تزول معالمه (المطلب الأول)، ويقتضي التفتيش أو الولوج في الجرائم الماسة بالمستند الإلكتروني البحث عن الأشياء ذات صلة بالجريمة، وذلك من خلال ضبط الأدوات التي إستخدمت في إرتكابها أو أي شي آخر من شأنه أن يفيد في كشف الحقيقة (المطلب الثاني)، ويعد الضبط الغاية المباشرة للتفتيش، وهو الوسيلة القانونية التي تمكن السلطة المختصة من وضع يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو إستعملت في إقترافها (المطلب الثالث).

المطلب الأول: معاينة مسرح الجريمة الماسة بالمستند الإلكتروني

المعاينة تكتسي طبيعة خاصة في هذا المجال لكونها تقوم على فحص حسي مباشر لمكان أو شخص أو أي شيء له علاقة بالجريمة لإثبات حالته والتحفظ على كل ما يفيد من الأشياء في كشف الحقيقة، وللتعمق في الدراسة سنتطرق إلى تعريف إجراء المعاينة في (الفرع الأول)، بينما سنتطرق في (الفرع الثاني) إلى مدى صلاحية معاينة مسرح الجريمة الماسة بالمستند الإلكتروني، ومع ضرورة مراعاة لمجموعة من الضوابط قبل وأثناء إجراء المعاينة في (الفرع الثالث).

الفرع الأول: تعريف إجراء المعاينة

لم يعرف المشرع المقصود بالمعاينة مما دعا الفقه للتصدي لتعريفها، حيث عرفت بأنها: "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"[1]، وجاء في تعريف آخر أن المعاينة هي: "إجراء بمقتضاه يتم الإنتقال إلى مكان إرتكاب الجريمة والتحقق منه، وجمع كل الآثار المتعلقة بالجريمة، وكيفية وقوعها، وكذلك جمع كل الأشياء التي تفيد في إكتشاف الحقيقة"[2].

وتكمن أهمية المعاينة في الجرائم المادية بأنها تتيح جمع الأدلة بغرض المحافظة عليها من يد العبث أو إخفائها أو تشويهها، كما تتيح إتخاذ الإجراءات الفورية اللازمة لم تكن متاحة ما لم يتم الإنتقال إلى مكان إرتكاب الجريمة فورًا كسماع شهادة الشهود الحاضرين ومواجهتهم ببعضهم البعض وغير ذلك من الإجراءات المتخذة[3]، كما تساعد في تصور كيفية إرتكاب الجريمة وظروف ملابساتها[4]، فيما عدا بعض الجرائم التي لا تصلح بطبيعتها بأن تكون محلًا

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 259.
[2]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص 231.
[3]- بدري فيصل، مرجع سابق، ص 106.
[4]- بن طالب ليندا، مرجع سابق، ص 47.

لإجراء المعاينة كجريمة الرشوة وجريمة السب التي تتم بالقول في غير علانية وغيرها من الجرائم[1].

والجدير بالذكر أن ليس كل إنتقال للسلطات القضائية المختصة هو بغرض إجراء المعاينة، فقد ينتقل قاضي التحقيق لأجل تفتيش مكان الواقعة، أو حتى سماع شهادة الشهود، أو أي جريمة تقبل المعاينة بطبيعتها.[2]

أما معاينة مسرح الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، فيقصد بها الآثار الرقمية التي يتركها مستخدم شبكة الإنترنت كالرسائل المرسلة منه أو التي إستقبلها وكافة الإتصالات التي قام بها من خلال الأجهزة الإلكترونية والشبكة العالمية وغيرها، مع ضرورة البحث في المحتوى إلا ضمن نطاق السلطات الممنوحة لجهات التحري والتحقيق مراعاة لمبدأ المشروعية وصون الخصوصية المعلوماتية للأفراد.[3]

فالمعاينة لا تهدف إلى مجرد جمع الأدلة الجنائية، بل تعني المشاهدة وإثبات الحالة في مكان وقوع الجريمة والمحافظة على آثارها في مسرحها، مما قد يتيح الإطلاع على الدليل وإثباته للمحافظة عليه من العبث به أو إخفائه[4]، وفك غموض الجريمة وحل شفراتها، فهي ذات أهمية في التحقيق الجنائي لأنها تترجم ما قام به الجاني من الأفعال الإجرامية، وتأكد من وقوع الجريمة ونفيها، وصدق أقوال أطراف الواقعة، وبيان العمد أو الخطأ في الواقعة، وتعتبر أيضًا ذات أهمية في التكييف القانوني للواقعة، وتساعد القاضي الجزائي في تكوين إقتناعه الشخصي، ولابد أن تتم وفقًا لمبدأ المشروعية لضمان تحقيق نتائجها[5].

وتجدر الإشارة هنا إلى أن المعاينة قد تكون إجراء تحقيق أو تحري، ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد وحرياتهم.[6]

والمعاينة التي ينفذها ضابط الشرطة القضائية أثناء مباشرة وظيفته أثناء التحريات الأولية نصت عليها الفقرة 03 من المادة 20 من ق.إ.ج.ج التي تنص على أن: "ويناط بالشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في التشريع الجزائي وجمع الأدلة عنها والبحث عن مرتكبيها والمساهمين فيها، ما دام لم يبدأ فيها تحقيق قضائي"، وذلك بصفة تلقائية

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص81.
[2]- مولاي ملياني دلال، مرجع سابق، ص 154.
[3]- أومدور رجاء، مرجع سابق، ص 153.
[4]- عبدالله أوهايبية، مرجع سابق، ص 563.
[5]- شنتير خضرة، مرجع سابق، ص 78.
[6]- محمود سعد عبد المجيد، مرجع سابق، ص-ص 486-487.

أو بناء على شكوى أو بلاغ، أو بناء على تعليمات النيابة، وهذه الصلاحيات واسعة وغير محدودة تسمح بالقيام بكل التحريات التي تفيد في الوصول للحقيقة[1].

وبديهي أن التحري عن الجرائم لا يتأتى إلا بمعاينة آثارها والتحري عن ملابسات إرتكابها والمحافظة على تلك الآثار ورفعها ليمكن إستغلالها[2]، وفي هذا الإطار تنص الفقرات 02، 03، 04 من المادة 73 من ق.إ.ج.ج على أن ضابط الشرطة القضائية يسهر على المحافظة على الآثار التي يخشى أن تختفي، وأن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة، وأن يعرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في الجناية للتعرف عليها وتقديم المعلومات بها، كما نصت المادة 81 من نفس القانون في حالة ما إذا إقتضى الأمر بإجراء معاينات ذات طابع علمي أو تقني لا يمكن تأخيرها فلضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك.

فالمحافظة على الآثار في مسرح الجريمة أو ضبط بعض الأشياء وعرضها على المشتبه فيه يقوم به ضابط الشرطة القضائية تلقائيًا في حالة التلبس، بينما في غير حالة التلبس لا يمكنه ذلك إلا بموافقة المعنيين بالأمر، وعدم عرض المحجوزات للتعرف عليها لا يؤثر في صحة الإجراءات.[3]

وبالرجوع إلى نص المادة 97 من القانون آنف ذكره نجدها تنص على أنه لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة، إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يجيد الكتابة فبإمكانه الإستعانة بشخص يختاره بنفسه، مع ذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه، مع ضرورة تطبيق الأحكام المنصوص عليها في المواد من 75 إلى 78 من ذات القانون، إلا أنه إستثنى هذا الإجراء عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المنصوص عليها على سبيل الحصر في الفقرة 03 من المادة 78 من القانون السالف الذكر بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، حينها تطبق الأحكام الواردة في المادة 78 وكذا المادة 79 من نفس القانون.

وعلاوة على ضباط وأعوان الشرطة القضائية يؤهل لمعاينة جرائم تزوير المستند الإلكتروني وجرائم إستعمال المستند الإلكتروني المزور، الموظفون وأعوان الإدارات

---

[1]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 74.

[2]- أحمد غاي، **ضمانات المشتبه فيه أثناء التحريات الأولية دراسة مقارنة للضمانات النظرية التطبيقية المقررة للمشتبه فيه في التشريع الجزائري والتشريعات الأجنبية والشريعة الاسلامية**، الطبعة الثالثة، 2017، دار هومة، الجزائر، ص 208.

[3]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص-ص 125-126.

والمصالح العمومية المكلفون ببعض مهام الضبط القضائي المنوطة بهم، بموجب قوانين خاصة وفق الأوضاع وفي الحدود المبينة بتلك القوانين وفي قانون الإجراءات الجزائية.[1]

أما المعاينة التي ينفذها قاضي التحقيق أثناء مباشرة وظيفته أثناء التحقيق الإبتدائي نصت عليها المادة 155 من ق.إ.ج.ج على أن: "يجوز لقاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائمًا بأمين ضبط التحقيق، ويحرر محضرًا بما يقوم به من إجراءات".

وتجدر الإشارة إلى أن مجال تنقل قاضي التحقيق غير محصور في دائرة إختصاصه الإقليمي، بل يمتد ليشمل أيضًا دوائر إختصاص المحاكم المجاورة للدائرة التي يباشر فيها وظيفته، على أن يخطر مقدمًا وكيل الجمهورية بمحكمته وكذا وكيل الجمهورية بالمحكمة التي سينتقل إلى دائرتها، وينوه في محضره عن الأسباب التي دعت إلى إنتقاله.[2]

الفرع الثاني: مدى صلاحية معاينة مسرح الجريمة الماسة بالمستند الإلكتروني

تتم معاينة مسرح الجرائم الماسة بالمستند الإلكتروني من خلال الإنتقال إلى مكان وقوع الجريمة، إلا أن هذا الإنتقال لا يقتصر على العالم المادي فحسب بل يشمل أيضًا العالم الرقمي، ويرى البعض بأنه ينبغي التعامل مع هذا المسرح على أنه مسرحان، المسرح التقليدي الذي يقع خارج البيئة الرقمية ويتكون بشكل أساسي من المكونات المحسوسة المادية للمكان الذي تم فيه إرتكاب الجريمة، وهو المسرح الذي قد يترك فيه الجاني آثارًا مادية كالبصمات أو وسائط التخزين الرقمية، والمسرح الإفتراضي الذي يقع داخل البيئة الرقمية ويتكون من المعطيات المعلوماتية التي توجد داخل الجهاز الإلكتروني وأيضًا تلك المتداولة عبر شبكة الإنترنت.[3]

وما سبق طرحه يثير تساؤلًا حول مدى صلاحية مسرح إرتكاب الجرائم الماسة بالمستند الإلكتروني للمعاينة؟ وللإجابة عن هذا التساؤل يتعين علينا أن نميز بين:

أولًا: الجرائم الواقعة على المكونات المادية للأجهزة الإلكترونية

لا يستدعي أدنى صعوبة لإثبات صلاحية هذه المكونات لمعاينتها، بإعتبار أنها تتم في المسرح التقليدي وهو المسرح الذي يقع عادة خارج البيئة الرقمية ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو قريب من مسرح الجريمة التقليدية[4]، وذلك بالإنتقال بسرعة إلى مسرح الجريمة للحفاظ على المكونات المادية كالأجهزة الإلكترونية ومستلزماتها وملحقاتها (كالطابعة، جهاز الماسح الضوئي...) وجميع الأشياء التي من الممكن أن تكون أدلة

[1]- المادة 13 من القانون رقم: 24-02 السالف الذكر.
[2]- المادة 156 من القانون رقم: 25-14 السالف الذكر.
[3]- بلحسيني حمزة، مرجع سابق، ص 318.
[4]- محمود سعد عبد المجيد، مرجع سابق، ص 489.

إلكترونية كشرائط الفيديو الرقمية (Dvd، Cd، Flash) وغيرها، وذلك قبل العبث بمضمونها أو إتلافها أو التخلص منها[1].

ثانيًا: الجرائم الواقعة على المكونات المعنوية للأجهزة الإلكترونية أو بواسطتها

أما في الحالة الثانية، تتم المعاينة في المسرح الإفتراضي أي الذي يقع داخل البيئة الرقمية، ويتكون أساسًا من المعطيات المعلوماتية المثبتة في ذاكرة الجهاز الإلكتروني، وتأتي في مقدمة هذه الجرائم تلك التي تستهدف البرامج المعلوماتية وبياناتها أو ترتكب من خلالها، بالإضافة إلى الجرائم الماسة بالمستند الإلكتروني.[2]

وهناك عدة طرق تمكن سلطة التحري والتحقيق من الإنتقال إلى العالم الرقمي لإجراء المعاينة، ومن ذلك على سبيل المثال:

1- بواسطة الجهاز الإلكتروني المتواجد في المكتب؛

2- اللجوء إلى مقهى الإنترنت (Cyber Café)؛

3- اللجوء إلى مقر عمل مقدمي خدمة الإنترنت (Internet Server Provider)، الذي يعد أنسب مكان يمكن إجراء المعاينة فيه؛

4- الإنتقال إلى مقر مكتب الخبير التقني المختص بغرض الولوج إلى العالم الرقمي لإجراء المعاينة، إذا توفر له في القانون ما يبيح ذلك، ولعل هذا متوفر في مصر من خلال إدارة مكافحة الجريمة الإلكترونية التابعة لوزارة الداخلية.[3]

وقد تتخذ معاينة مسرح الجرائم الماسة بالمستند الإلكتروني عدة صور، كتحميل نسخة من المستند المعتدى عليه أو التحفظ على نسخة منه، أو إستخراجه عن طريق الطابعة، أو عن طريق حفظ موقع الإنترنت بإستخدام خاصية الحفظ المتوفرة في نظام التشغيل، أو من خلال تصوير شاشة الجهاز الإلكتروني بواسطة آلة تصويرية، أو عن طريق إستخدام برمجية إلكترونية متخصصة في إلتقاط صور للشاشة وهو ما يعرف بتجميد مخرجات الشاشة.[4]

وما سبق ذكره، المسرح الافتراضي الذي تجري عليه معاينة الجرائم الواقعة على المكونات المعنوية للأجهزة الإلكترونية تعترضه عدة صعوبات، من أهمها:

1- يتمحور نشاط الجرائم الماسة بالمستند الإلكتروني داخل البيئة الرقمية، ولا تخلف في الغالب آثارًا مادية تدل على مرتكبيها بخلاف الجرائم التقليدية التي تترك عادةً أدلة مادية[5]؛

---

[1]- أومدور رجاء، مرجع سابق، ص 155.

[2]- محمود سعد عبد المجيد، مرجع سابق، ص-ص 489-490.

[3]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 156.

[4]- بلحسيني حمزة، مرجع سابق، ص 317.

[5]- يتميز الدليل فيها بأنه دليل غير مرئي، فهو عبارة عن نبضات إلكترونية مكونة من سلسلة طويلة من الأرقام الثنائية 0،1، والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه، فالكتابة مثلًا في العالم الرقمي ليس لها وجود مادي في شكل ورقي وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأي شيء=

غالبًا ما يكون للجريمة التقليدية مسرح تجري عليه الأحداث التي تخلف آثارًا مادية تترتب عليها الأدلة، وهذا المسرح يعطى المجال أمام سلطة التحري والتحقيق في الكشف عن الجريمة والأدلة وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة الماسة بالمستند الإلكتروني يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة.[1]

2- نتيجة تردد العديد من الأشخاص إلى مكان أو مسرح الجريمة -كمقاهي الإنترنت-، خلال الفترة الزمنية الفاصلة بين زمن إرتكاب الجريمة ووقوع النتيجة الإجرامية، مما يفسح مجال العبث أو حدوث تغيرات أو زوال الآثار المادية للجريمة، وهو ما يخلق نوعًا من الغموض حول الدليل[2]؛

3- سهولة محو آثار الدليل الإلكتروني أو تعديله أو إتلافه أو التلاعب في معطياته[3].

لذلك حبذا على المشرع أن يقرر عقوبات جزائية على كل من يقوم بتغيير أو بتعديل في المعلومات المسجلة في ذاكرة الجهاز الإلكتروني، أو في وسائط التخزين، أو في قاعدة البيانات

=في العالم الإفتراضي يتكون من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة، وأما تكوين معطياته فإنها تختلف من حيث الحجم والموضوع، فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة، مما يستحيل معه الإطلاع عليها بوسائل غير تقنية تعالج هذه الذبذبات في صورة مفهومة للبشر، وبالتالي أن أغلب المعطيات المخزنة التي تتداول عبر الأجهزة الإلكترونية تكون على هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الأجهزة، لذا يتطلب الإستعانة بأجهزة وأدوات التقنية وإستخدام برامج معلوماتية ملائمة للإطلاع عليه أو إستخراجه في هيئة ملموسة أو مادية وهي تعد أساليب علمية، إلا أن ترجمته وإخراجه في شكل مادي ملموس لا يعني أن هذا التجميع المادي هو الدليل بل أن هذه العملية ليست سوى عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الإستدلال بها على معلومة معينة، وللمزيد من التفصيل، ينظر: بوشارب هانية، بن شهرة شول، **صعوبة عملية إستخلاص الدليل الإلكتروني**، مرجع سابق، ص 69.

[1]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 60.

[2]- براهيمي جمال، مرجع سابق، ص 198.

[3]- يستعمل المجرم المعلوماتي عدة أساليب وتقنيات تسمح له بإخفاء كل آثار الجريمة والتستر عنها بسهولة كبيرة، وذلك من خلال التوصل بتقنيات معدة لهذا الغرض مع الأخذ بعين الإعتبار سهولة وسرعة إمكانية محو وتعديل المعطيات الإلكترونية التي يمكن القيام بها في أزمان قياسية متناهية القصر تقاس باللحظات والثواني، فمن خلال إدخاله لبعض التعليمات في المنظومة المعلوماتية يتم محو المعطيات بالكامل في لمح البصر، كما يمكنه وبمجرد كبسة زر خاطفة على لوحة المفاتيح أن يقوم بإلغاء الأوامر الصادرة للجهاز، على إعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما أن يحس الجاني بأن أمره سينكشف حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبها أمرًا في غاية الصعوبة، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم إستطاعة هذه السلطات إقامة الدليل ضده، فضلًا عن سهولة تنصله من مسؤولية هذا العمل بإرجاعه حسبما تشهد بذلك وقائع عديدة، على خطأ في المنظومة المعلوماتية أو الشبكة أو في الأجهزة، وإلى جانب هذا الأسلوب يستعمل الجناة أسلوب التغليط والتضليل الذي يتم إما عن طريق التلاعب بقواعد البيانات والبرامج أو إدخال معطيات مختلقة مزيفة أو محرفة في المنظومة، أو تغيير مسار المعطيات الصحيحة المدخلة دون أن يحس المجني عليه بذلك، ويجتهد المهندسون في مجال تقنية المعلومات في إبتكار برامج معينة لهذا الغرض، وتكمن آلية عملها في أنه بمجرد محاولة شخص غير مصرح له ولوج المنظومة أو إستخدام جهاز المزود بهذا البرنامج، فإن هذا الأخير يصدر أمرًا للجهاز بحيث يتم إتلاف المعطيات المخزنة به ومحوها بصورة تلقائية، وللمزيد من التفصيل، بوشارب هانية، بن شهرة شول، **صعوبة عملية إستخلاص الدليل الإلكتروني**، مرجع سابق، ص-ص 71-72.

أو بنك المعلومات، بغرض الحرص على محافظة على مسرح الجريمة قبل القيام بأي إجراءات التمهيدية للتحقيق الجنائي[1]، وإن تم تدارك الأمر بمقتضى المادة 74 من ق.إ.ج.ج[2]، إلا أن هذا النص القانوني ينصرف إلى أغلب الجرائم المادية، ويمكن تطبيقه عند معاينة المكونات المادية للجهاز الإلكتروني[3] على عكس المكونات المعنوية التي تتطلب إجراءات خاصة[4].

الفرع الثالث: ضوابط إجراء معاينة مسرح الجريمة الماسة بالمستند الإلكتروني

يتميز مسرح الجريمة في الجرائم الماسة بالمستند الإلكترونى عن غيره من الجرائم التقليدية بوجود أدلة ذات طبيعة غير مرئية، لذلك فلابد من مراعاة عدة قواعد فنية قبل وأثناء إجراء المعاينة، حتى يكون لإجراء المعاينة في هذا النوع من الجرائم فائدة في كشف الحقيقة عنها وعن مرتكبيها، كالآتي:

أولاً: الضوابط الواجب إتخاذها قبل إجراء المعاينة

يجب قبل الإنتقال لإجراء معاينة مسرح الجريمة الماسة بالمستند الإلكتروني، ضرورة إتباع الإجراءات التالية:

1- توفير معلومات مسبقة عن مكان الجريمة، ومن المالك لهذا المكان، ونوع وعدد الأجهزة المتوقع مداهمتها وشبكات الإتصال الخاصة بها[5]، لتحديد كيفيات التعامل معها فنيًا من حيث الضبط والتأمين وحفظ المعلومات والمستندات[6]؛

2- إعداد خريطة توضح الموقع الذي سوف يتم الإغارة عليه وتفاصيل المبنى أو الطابق من المبنى موضع البلاغ، وتحديد مواقع وعدد الأجهزة والخزائن والملفات، ويحدد ذلك من خلال مصادر المعلومات السرية[7]؛

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 82.

[2]- تنص المادة 74 من القانون رقم: 25-14 السالف الذكر على أن: "يحظر، في مكان إرتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، وإلا عوقب بغرامة من 20.000 دج إلى 100.000 دج. غير أنه يستثنى من هذا الحظر حالة ما إذا كانت التغييرات أو نزع الأشياء ضرورية للسلامة والصحة العمومية أو تستلزمها معالجة الضحايا. وإذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة عوقب على هذا الفعل بالحبس من ثلاثة (03) أشهر إلى ثلاثة (03) سنوات وبغرامة من 50.000 دج إلى 150.000 دج.

- Art 55 paragraphe 01 du C.P.P.F (Modifie par loi n°92-1336 du 16 décembre 1992, art 11, JORF 23 décembre 1992 en vigueur le 1er mars 1994) dispose que: « Dans les lieux où un crime a été commis, il est interdit, sous peine de l'amende prévue pour les contraventions de la quatrième classe, à toute personne non habilitée, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélèvements quelconques».

[3]- بن طالب ليندا، مرجع سابق، ص 48.

[4]- بوكر رشيدة، مرجع سابق، ص 271.

[5]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 598.

[6]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 62.

[7]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص598.

3- الحصول على المعدات الضرورية للإستعانة بها في الفحص والتشغيل، مثل برنامج النسخ وبرنامج معالجة الملفات والبرنامج الذي يقوم بإنشاء صورة قرص الصلب، ويستخدم تحديدًا لأغراض التحقيق الجنائي في المباحث الفيدرالية الأمريكية، ويسميها الخبراء بحقيبة الأدلة الرقمية[1]؛

4- إعداد قائمة دائمة بالإحتياجات العامة لجميع الغارات مسبقًا، ومراجعة توفر إحتياجات كل حالة على حدة[2]؛

5- إعداد فريق متخصص من الخبراء الذي يتولى معاينة مسرح الجريمة، على أن يكون هذا الفريق مرفقًا بالإذن للقيام بالتفتيش، لأن أغلب الجرائم المعلوماتية بما في ذلك الجرائم الماسة بالمستند الإلكتروني غالبًا ما تكون داخل أماكن لها خصوصياتها[3]؛

6- إخطار أعضاء الفريق الذى سيتولى المعاينة للتحرك لمسرح الجريمة قبل بوقت كاف حتى يستعد من الناحية الفنية والعملية، ولتمكينهم من إعداد الخطة المناسبة لضبط أدلة الجريمة حال معاينتها[4]، وتحديد المعطيات والإختصاصات والمهام المطلوبة من كل عضو في فريق المعاينة على حده لضمان الإنجاز مع عدم التداخل[5]؛

7- إعداد خطة الهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على أن تكون الخطة موضحة بالرسومات وتتم مراجعتها من أعضاء الفريق قبل بدء التحرك مع الأخذ في الإعتبار قاعدة العسكرية والتي تعني الحالة والرسالة والتنفيذ والمداخل والمخارج والإتصالات، وهي ملائمة للأجهزة الأمنية وأجهزة إنفاذ القوانين، فالحالة أو الوضع يعني معرفة حجم القضية التي تقوم بالتحقيق فيها وعدد المتورطين فيها، أما الرسالة فهي تحديد الهدف من الإجراء، والتنفيذ يعني كيفية أداء المهمة، أما المداخل والمخارج فإن معرفتها ضرورية وهي تختلف من جريمة إلى أخرى وتحسب وفقًا لمكونات طريق التحقيق، بينما يأتي عنصر الإتصالات لضمان السرية وسلامة التعامل وتبادل المعلومات أثناء تنفيذ الإجراء[6]؛

8- تأمين التيار الكهربائي من الإنقطاع المفاجئ، لأن إنقطاعه يسبب العديد من المخاطر تتمثل في التوقف المفاجئ للأجهزة الإلكترونية، مما قد يسبب في محو المعلومات من الذاكرة، وبالتالي فقدان كافة العمليات التي كان يتم تشغيلها، وإتصالات الشبكة، وأنظمة الملفات الثابتة[7]؛

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 85.

[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 598.

[3]- عائشة بن قارة مصطفى، مرجع سابق، ص85.

[4]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص62.

[5]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 599.

[6]- نفس المرجع، ص 599.

[7]- عائشة بن قارة مصطفى، مرجع سابق، ص 86.

9- الإحتفاظ بسرية حتى نهاية التفتيش، إذ أن المعلومات التي يتم البحث عنها يمكن إتلافها بسهولة من قبل المتهمين أو المتورطين في الجريمة[1]؛

10- السعي أن تتم كل هذه الإجراءات وفقًا لمبدأ المشروعية، وفي إطار ما تنص عليه القوانين الجنائية[2].

ثانيًا: الضوابط الواجب إتخاذها أثناء إجراء المعاينة

بعد وصول الفريق إلى مسرح الجريمة يتم التأمين والسيطرة على المكان والبدء في التفتيش، على النحو التالي:

1- وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة، بل ورصد الإتصالات الهاتفية من وإلى مكان مسرح الجريمة مع إبطال مفعول أجهزة الهاتف المتحرك التى قد تساعد -عن طريق تقنية معينة- في تدمير أدلة الجرائم الواقعة على المستند الإلكتروني متى تم توصيلها بالأجهزة محل المعاينة وذلك ممكن عمليًا[3]، وإبعاد الموظفين عن الأجهزة الإلكترونية وكذلك عن الأماكن الأخرى التي توجد بها الأجهزة[4]؛

2- عند العثور على حواسيب أو أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها، وتدوين الحالة التي هي عليها إذا كانت منطفئة أو في حالة تشغيل موصولة بالكهرباء أو بجهاز لاحق آخر، كما ينبغي ترقيم لواحقها بشكل متسلسل[5]؛

3- تحديد الأجهزة الإلكترونية الموجودة في مكان المعاينة، وتحديد مواقعها بأسرع فرصة ممكنة، وفي حالة وجود شبكة إتصالات يجب البحث عن خادم الملف (File Server)، وذلك لتعطيل الإتصالات لمنع تخريب الأدلة الموجودة أو محوها[6]؛

4- مراعاة تصوير الجهاز الإلكتروني المضبط بمحل وقوع الجريمة، والأجهزة الطرفية الموصولة به، والمحتويات، وأوضاع المكان الذي يوجد فيه بصفة عامة، مع الحرص على تصوير أجزاءه الخلفية وملحقاته الأخرى، وكذا مراعاة أن يتم تسجيل تاريخ ووقت ومكان إلتقاط كل صورة[7]؛

وهنا تواجه القائمين بالمعاينة عدة تحديات يجب الإنتباه لها، يتمثل التحدي الأول في أن التصوير يجب أن يكون للجهاز الذي من خلاله تمت ممارسة السلوك المادي المرتب للنتيجة، وكذلك كل ما يتصل بهذا الجهاز من ملحقات وأجهزة أخرى، والتحدي الثاني هو أنه يجب

---

[1]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 599.

[2]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 62.

[3]- نفس المرجع، ص 63.

[4]- علي عدنان فيل، مرجع سابق، ص 34.

[5]- محمود سعد عبد المجيد، مرجع سابق، ص 491.

[6]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 63.

[7]- عائشة بن قارة مصطفى، مرجع سابق، ص 86.

الإنتباه والتركيز عند تسجيل التاريخ والوقت، بحيث يمكن أن يكون الجهاز مضبوطًا بتوقيت معين يظهر على الصورة فقط، والكاميرا بها توقيت آخر وهو ما يحتاج إلى خبير فني فيما بعد للمقارنة بينهما بفحص الجهاز والتأكد من ذلك، والتحدي الثالث هو تحديد مكان التصوير بدقة.[1]

5- العناية البالغة بملاحظة الطريقة التي تم بها إعداد المنظومة المعلوماتية، والآثار الإلكترونية التي يخلفها ولوج المنظومة أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الإتصال ونوع الجهاز الذي تم عن طريقه الولوج[2]؛

6- يتم وضع المخطط تفصيلي للمنشأة التي أرتكب بها الجريمة، مع كشف التفصيلي بالمسؤولين بها ودور كل واحد منهم[3]؛

7- قطع التيار الكهربائي عن موقع المعاينة، لشل فاعلية الجاني في القيام بأي فعل من شأنه محو أو التأثير على آثار الجريمة[4]؛

8- مراعاة عدم نقل أي مستندات إلكترونية أو أية مادة معلوماتية من مسرح الجريمة قبل إجراء إختبارات، إلا بعد التأكد من خلو المحيط الخارجي لموقع الأجهزة الإلكترونية من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو أو إتلاف المعطيات المخزنة.[5]

ولن يتأتى ذلك إلا عن طريق خبراء التقنيين، ويرتبط بذلك أن الفريق الذي يتولى المعاينة ومن ثم ضبط وتحريز الأدلة -إن وجدت- لابد وأن يضم إثنين أو أكثر من الخبراء يتولون ضبط وإدخال المعلومات المضبوطة في الجهاز الإلكتروني، وتصنيف الأدلة وتحريزها في صناديق، ووضع العلامات الدالة عليها، ويقوم هذا الفريق كذلك بنقل الأجهزة الإلكترونية المضبوطة بعد تكملة إجراءات الرسم والتصوير، على أن يراعى تنوع خبراء التقنيين ما بين محققين وآخرين مدربين على التعامل مع الأدلة وطرق تقييمها.[6]

9- القيام بالتحفظ على المستندات الخاصة بالإدخال والمخرجات الورقية للأجهزة الإلكترونية ذات الصلة بالمستندات الإلكترونية محل الجريمة، وذلك لرفع ومضاهاة ما قد يوجد عليها من بصمات أو آثار مادية[7]؛

10- ربط الأقراص التي ربما تحمل الأدلة، مع جهاز الذي يمنع التسجيل أو الكتابة عليها، مما يتيح للسلطة القضائية المختصة من قراءة معطياتها من دون تغييرها[8]؛

---

[1]- عميمر عبد القادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص 237.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 86.

[3]- علي عدنان فيل، مرجع سابق، ص 34.

[4]- نفس المرجع، ص 34.

[5]- عائشة بن قارة مصطفى، مرجع سابق، ص87.

[6]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 65.

[7]- عائشة بن قارة مصطفى، مرجع سابق، ص 87.

[8]- نفس المرجع، ص 87.

11- التحفظ على ما يمكن العثور عليه من المحتويات بسلة المهملات، وتصوير المحتوى لإثبات ذلك رقميًا، لأن من المحتمل أن لم يتمكن الجاني من التخلص منها فلهذا يجب التحفظ عليها[1]، كالمخرجات المتحصلة من الوسائل الإلكترونية كالأوراق الملقاة أو الممزقة، وكذا جميع الأشياء التي من الممكن أن تكون أدلة إلكترونية كشرائط الفيديو الرقمية غير السليمة أو المحطمة المتواجدة فيها، التي يتم فحصها وترفع من عليها البصمات التي قد تكون لها صلة بالجريمة المرتكبة[2]؛

12- الملاحظة وإثبات حالة التوصيلات والكابلات والتي تكون متصلة بكل مكونات المنظومة، وذلك حتى يسهل تحليل المعطيات ومقارنتها والوصول إلى دليل فيما بعد[3]؛

حصر مباشرة المعاينة على فئة معينة من الخبراء والسلطة القضائية الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في تقنيات الإلكترونية والشبكات ونظم المعلومات وإسترجاع المعلومات، والذين اخضعوا لتدريب الكافي على التعامل مع هذه النوعية من الأدلة، والآثار التي يحويها مسرح الجريمة الماسة بالمستند الإلكتروني[4]، ويضم كذلك آخرين للرسم والتصوير، وذلك لرسم كروكي المسرح الجريمة، وتحديد مواقع الأجهزة والملفات والأشخاص، وأيضًا أشخاصًا للتفتيش العملي -في مسرح الجريمة-، شرط أن يتم ذلك وفقًا للتشريع المعمول به، ثم أفرادًا هدفهم تأمين مسرح الجريمة وضبط مخارجها ومنافذها[5].

13- تحريز الدليل الإلكتروني المتحصل عليه عن طريق ضبط وتحريز الدعائم الأصلية للمعطيات وعدم الإكتفاء بضبط النسخ، ومراعاة لظروف الحرارة والرطوبة لكي يتم تخزينها، والتقيد بالضوابط الفنية المتعلقة بنقلها، مع تأمين البرامج المضبوطة قبل تشغيلها فنيًا، وقيام بالنسخ الإحتياطية السليمة والكاملة، وتمييز كل الدليل الإلكتروني عن غيره بواسطة وضع علامة مادية الخاصة به.[6]

فضلًا عن الضوابط الفنية الواجب مراعاتها، فإن الإنتقال بسرعة وإجراء المعاينة يعد شرطًا أساسيًا، كما يجب الحفاظ على الأماكن التي يجرى فيها المعاينة قدر المستطاع، والسعي لإستغلالها على أكمل وجه وفقًا للطرق العلمية الحديثة، وهو ما حرص عليه المشرع الجزائري حين وضع نصوصًا[7] تكفل ضمانات للتحري والتحقيق في هذه المرحلة، وذلك من خلال توقيع عقوبات قد تصل إلى حد الحبس في حالة عرقلة حسن سير العدالة[1].

---

[1]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص 238.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 87.

[3]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص164.

[4]- بلحسيني حمزة، مرجع سابق، ص 321.

[5]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 66.

[6]- أومدور رجاء، مرجع سابق، ص 158.

[7]- تنص المادة 43 من القانون رقم: 25-14 السالف الذكر على أن : "يحظر في مكان إرتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة، أو ينزع أي شيء منها قبل الإجراءات الأولية=

المطلب الثاني: التفتيش في الجرائم الماسة بالمستند الإلكتروني

لم يقدم المشرع الجزائري تعريفًا خاصًا أو دقيقًا للتفتيش بل اعتبره من إجراءات التحقيق وأحاطه بجملة من الضوابط الصارمة، بهدف توفير الحد الأدنى من الضمانات الكفيلة بالحفاظ على حقوق الفرد وحريته، نظرًا لأهميته في كشف الأدلة وخطورته لما قد يترتب عليه من مساس بحرية الأشخاص وكرامتهم، ذلك أن إقرار هذه الضمانات يمثل صونًا لهذه الحقوق من الهدر والتعسف، فهو التعبير الحي عن قوة القانون في مدى إلزام السلطة القضائية بإحترام حدود إختصاصها ومهامها، وبين ضرورة التصدي للإجرام بدون تعسف، وهو ما جسدته المادة 48 من الدستور الجزائري سنة 2020 والتي تنص على أن: "تضمن الدولة عدم إنتهاك حرمة المسكن، لا تفتيش إلا بمقتضى القانون وفي إطار إحترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

يمكن تعريف التفتيش بأنه: "البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون"، وبأنه: "البحث عن الحقيقة في مستودع سرها حيثما تكون مع الشخص أو في منزل، الحقيقة التي تتمثل في ثبوت أو إنتفاء إرتكاب شخص معين لجريمة معينة وقعت بالفعل، وأتهم هذا الشخص بإرتكابها على أساس من الجدية التي تؤيدها إمارات قوية"[2]، كما عرف بأنه عبارة عن: "إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات إرتكابها أو نسبتها إلى المتهم وفقًا لإجراءات قانونية محددة"[3]، ويقصد به أيضًا بأنه: "الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، والبحث عن المعطيات غير المادية المخزنة في الجهاز الإلكتروني، بهدف إثبات الجريمة المعلوماتية ونسبتها إلى مرتكبها"[4].

بناءً على ما سبق ذكره، يطرح التساؤل الآتي: ما مدى فعالية التفتيش كآلية إجرائية للتحقيق والكشف عن الجرائم الماسة بالمستند الإلكتروني؟ وللإجابة على هذا التساؤل، سنتطرق إلى ما يلي:

=للتحقيق القضائي، وإلا عوقب بغرامة من 200 إلى 1.000دج. غير أنه يستثنى من هذا الحظر حالة ما إذا كانت التغييرات أو نزع الأشياء للسلامة والصحة العمومية، أو تستلزمها معالجة المجني عليهم. وإذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة، عوقب على هذا الفعل بالحبس من ثلاثة 03 أشهر إلى ثلاثة 03 سنوات وبغرامة من 1.000 إلى 10.000 دج.".

[1]- بلحسيني حمزة، مرجع سابق، ص 322.

[2]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 182.

[3]- نفس المرجع، ص 182.

[4]- محمود سعد عبد المجيد، مرجع سابق، ص 478.

الفرع الأول: مدى قابلية تفتيش مكونات الأجهزة الإلكترونية

التفتيش ليس غاية في حد ذاته وإنما هو الوسيلة لغاية تتمثل في إمكانية الوصول من خلاله إلى أدلة مادية تساهم في بيان وظهور الحقيقة، وللوقوف على ما مدى صلاحية الجرائم الماسة بالمستند الإلكتروني للتفتيش عن أدلتها، يجب التمييز في هذا الصدد بين الحالتين الآتيتين:

أولًا: مدى قابلية تفتيش المكونات المادية للأجهزة الإلكترونية

يتفق البعض على قابلية خضوع المكونات المادية للأجهزة الإلكترونية للتفتيش في مجال الجرائم الماسة بالمستندات الإلكترونية متى تم ذلك وفقًا للإجراءات القانونية، بحيث لا يثير تفتيش هذه المكونات أي مشاكل متى تم هذا الإجراء وفقًا للقواعد التقليدية، وعليه يمكن ولوج المكونات المادية للأجهزة الإلكترونية بأوعيتها المختلفة للبحث عن الجرائم الماسة بالمستندات الإلكترونية، والتنقيب عن أي شيء من الممكن أن يفيد في كشف حقيقتها، وكذا تحديد مقترفيها.[1]

إلا أن حكم هذه المكونات متوقف على طبيعة المكان الموجودة فيه إذا ما كان من الأماكن العامة (Les lieux publics) أم الأماكن الخاصة (Les lieux privés)، إذ لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص أو عام كان لها حكم هذا المكان، فيجب أن يتم التفتيش في الحالات التي يجوز فيها ذلك وبنفس الضمانات المقررة قانونًا للتفتيش في هذه الأماكن، وعليه فإن وقوع جريمة الماسة بالمستند الإلكتروني يعطي صاحب الإختصاص صلاحية التفتيش في كل مكان يمكن أن يعثر فيه على أدلة تثبت وقوع الجريمة ونسبتها إلى فاعل معين[2]، وهنا يجب التفريق بين الأماكن العامة والخاصة:

1- تفتيش الأماكن العامة:

وهي الأماكن التي يتسني لكل إنسان أن يمر بها في كل وقت ولا تتمتع بحرمة المنزل سواء كانت من الأماكن العامة بطبيعتها (les lieux publics par nature) وهي الأماكن التي يرتدها العامة في كل وقت مثل الشوارع والحدائق العامة والمتنزهات العامة والمواصلات وغيرها، أم كانت من الأماكن العامة بالتخصيص (les lieux publics par destination) وهي تلك الأماكن التي يرتادها العامة في أوقات معينة كالمقاهي والمطاعم والمحلات وغيرها، حيث يباح دخولها إما لفئة معينة من الأفراد أو بلا تفرقة، وقد تكون بمقابل أو مجانًا، ويمكن دخولها خلاف للأماكن الخاصة وتفتيشها إذا ما تم غلقها لإنتهاء فترة العمل وإنصراف العامة فهذه الحالة تأخذ طابع الخصوصية، كذلك الشأن فيما يحتويه من مكاتب أو غرف خاصة لصاحبها،

[1]- بلحسيني حمزة، مرجع سابق، ص 326.
[2]- رفاه خضير جياد العارضي، مرجع سابق، ص129.

ومن الواضح أن التفتيش الذي ينصب على المكونات المادية للأجهزة الإلكترونية تبدو عادية نظرًا لإمكانية ضبط وحجز تلك المكونات وإتلافها جزئيًا أو كليًا.[1]

ويستوي الأمر بالنسبة للمكونات التي بحيازة شخص ما، بغض النظر عن صفته سواء كان عامل الصيانة أو مبرمج أو موظف في شركة تنتج برامج معلوماتية، فإن تفتيشها تخضع لأحكام تفتيش الأشخاص، وفقًا للشروط والضمانات المحددة قانونًا.[2]

2- تفتيش الأماكن الخاصة:

فإذا كانت موجودة في مكان خاص (un lieu privé) كمسكن المتهم أو أحد ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونًا في التشريعات المختلفة[3]، مع مراعاة التمييز بين ما إذا كانت المكونات المراد تفتيشها:

- منعزلة عن غيرها من الأجهزة الأخرى؛
- متصلة بجهاز آخر، أو الطرفية النهائية (Terminal endpoint) في مكان آخر كمسكن غير المتهم مثلًا.[4]

وبالرجوع إلى القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر نجده قد أورد قاعدة عامة بموجب المادة 157 منه، الذي يجيز التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدًا لإظهار الحقيقة، إلا أن المادة 97 منه نصت صراحة على أن لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة، إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يجيد الكتابة فبإمكانه الإستعانة بشخص يختاره بنفسه، مع ذكر ذلك في المحضر، وتطبق فضلًا على ذلك أحكام المواد من 75 إلى 78 من نفس القانون.

إلا أنه إستثنى المشرع الجزائري تطبيق هذه الضمانة بموجب الفقرة 03 من المادة 97 من القانون آنف ذكره على طائفة من الجرائم المذكورة في الفقرة 03 من المادة 78 من نفس القانون بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، حيث أجاز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناءً على إذن مسبق من وكيل الجمهورية المختص.

---

[1]- زيبحة زيدان، مرجع سابق، ص 134.

[2]- براهيمي جمال، مرجع سابق، ص-ص 16-17.

[3]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 564.

[4]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص-ص 195-196.

ويلاحظ أن المشرع الجزائري قد غلب مصلحة المجتمع في سبيل تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن بإعتباره مستودع أسرارهم، فالظاهر من النص أنه يشير إلى التعدي المشروع لخصوصية الشخصية للفرد إلا أن ما يبيحه ويقلل من خطورته الطابع الخاص للجريمة الماسة بالمستند الإلكتروني، فهي جريمة قابلة للتعديل وللمحو في ثوان معدودة وقد تزداد الصعوبة إذا كان الدليل الإلكتروني الوحيد لإثباتها، ولتحقيق الموازنة في الحد الأدنى من الضمانات في المحافظة على الحقوق وحريات الأفراد وبين ضرورة التصدي للإجرام بدون تعسف، أجاز المشرع الجزائري بإجراء تفتيش المنزل إلا في حالة صدور الإذن من وكيل الجمهورية المختص.[1]

ثانيًا: مدى قابلية تفتيش المكونات المعنوية للأجهزة الإلكترونية

مما سبق، نخلص إلى نتيجة مفادها أنه لا خلاف حول إمكانية إخضاع المكونات المادية للأجهزة الإلكترونية للتفتيش، من أجل البحث عن الأدلة التي تفيد في كشف الحقيقة وعن مرتكبيها ونسبة الجريمة إليهم، كونها ذو طبيعة مادية سهل الحصول عليها وينطبق عليها ذات الإجراءات القانونية التقليدية المقررة للتفتيش دون أدنى صعوبة أو عائق، لكن الخلاف يحتدم بالنسبة إلى تفتيش المكونات المعنوية للأجهزة الإلكترونية، كون الدليل في هذه الحالة غير محسوس يشمل المعطيات والملفات المخزنة.

وهي عبارة عن مجموعة من البرامج والملفات المتعلقة بتشغيل وحدة معالجة المعطيات، وتنقسم إلى كيانات أساسية تضم البرامج الضرورية التي يتم من خلالها تشغيل وإستخدام الجهاز الإلكتروني، وكيانات تطبيقية تضم برامج تمكن المستخدم من أن ينفذ بواسطتها عملًا معينًا بإستخدام الجهاز.[2]

وقد ثار خلاف حول مدى صلاحية تفتيش المكونات المعنوية للأجهزة الإلكترونية كتمهيد لضبط الأدلة الإلكترونية المتعلقة بجرائم الماسة بالمستندات الإلكترونية، مما أدى إلى إنقسام الآراء إلى عدة إتجاهات:

1- الإتجاه الأول:

ذهب الرأي الأول إلى إمكانية تفتيش المكونات المعنوية للجهاز الإلكتروني، وضبط المعطيات المعلوماتية بمختلف أشكالها، مستندين في ذلك من القوانين الإجرائية التي أوردت مصطلح "ضبط أي شيء" عند تنظيمها لأحكام إصدار الإذن بالضبط، وذلك من خلال توسيع

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 90.
[2]- محمود سعد عبد المجيد، مرجع سابق، ص 480.

تفسير عبارة "ضبط أي شيء"، فإن ذلك تم تفسيره بحيث يشمل جميع المعلومات والمعطيات سواء كانت مادية أو معنوية.[1]

ويحاول البعض التغلب على هذه الصعوبة باللجوء إلى حيلة التميز بين المعلومات والمعطيات سواء التي تمت معالجتها إلكترونيًا أو التي لم تتم معالجتها بعد، فينفى الطابع المادي عن أولها ويؤكد للثانية طابعًا ماديًا على أساس أنها نبضات أو ذبذبات إلكترونية أو إشارات أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط معينة ويمكن قياسها[2]، وبالتالي ينفون الطابع المعنوي لهذه المعطيات المعالجة آليًا مؤكدين أنها شيء يمكن لمسه في المحيط الخارجي وأنها كيان مادي لا يمكن جحده، مستندين في ذلك إلى حكم محكمة جنح بروكسل الذي أكد على كون هذه المعطيات أشياء مادية محسوسة، وإنتهوا إلى إمكانية خضوع هذه المعطيات لقواعد التفتيش التقليدية وبالتالي إمكانية ضبطها[3].

ومن التطبيقات التشريعية التي تجيز تفتيش مكونات الجهاز الإلكتروني من خلال ما تخوله بعض التقنيات الإجرائية لسلطة التحقيق من إتخاذ أي إجراء أو أي شي لازم لجمع أدلة الجريمة والحفاظ عليها[4]، المادة 126 من قانون الإجراءات الجنائية الفرنسي التي أعطت سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريًا لجمع الدليل وحمايته، ويفسر الفقه الفرنسي عبارة "ضبط أي شيء" بأنها تشمل جميع المعطيات سواء كانت مادية أو معنوية، سواء أكانت هذه المعطيات مخزنة في حاملتها أم معالجة آليًا في الذاكرة الداخلية، أي أن أنصار هذا الإتجاه قد اخضعوا الكيانات المعنوية للجهاز الإلكتروني للإجراءات نفسها المتبعة في تفتيش الكيان المادي[5].

ونصت المادة 251 من قانون الإجراءات الجزائية اليوناني على تمكين سلطات التحقيق القيام بأي شيء يعتبر ضروريًا لجمع الدليل وحمايته، ويفسر "أي شيء" بأنها تمتد لتشمل ضبط المعطيات المعالجة آليًا أو تلك التي تم تخزينها، وبناءً على ذلك فإن ضبط المعطيات المخزنة في الذاكرة الداخلية للجهاز الإلكتروني لا تشكل أي إشكال في القانون اليوناني.[6]

كذلك هناك بعض القوانين التي تقدم قواعد تفصيلية للتفتيش تطبق على مكونات الجهاز الإلكتروني ومعطياته في حالات معينة، ومن ذلك على سبيل المثال القسم الفرعي رقم: 1/16 من قانون المنافسة (The competition act) في كندا، فهذا القسم يزود الشخص الذي يحمل إذنًا للتفتيش إمكانية أن يستخدم أو يعمل على إستخدام أي منظومة معلوماتية خاصة بالجهاز

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص91.
[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص 308.
[3]- نفس المرجع، ص 308.
[4]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 565.
[5]- رفاه خضير جياد العارضي، مرجع سابق، ص 130.
[6]- بن طالب ليندا، مرجع سابق، ص 52.

الإلكتروني، لتفتيش أي معطيات تحتويها أو تكون متاحة لهذه المنظومة، كما يمكنه أن يسجل أو يعمل على إستخدام أي منظومة للجهاز الإلكتروني لتفتيش أي معطيات تحتويها أو تكون متاحة لهذه المنظومة، كما يمكنه أن يسجل أو يعمل على تسجيل تلك المعطيات في شكل مطبوعات أو أي مخرجات أخرى[1]، ووسع الفقه الجنائي في كندا من تفسير نص المادة 487 من قانون العقوبات الكندي على تمكين إصدار الأمر القضائي لتفتيش وضبط أي شيء تتوفر في شأنه أسس أو مبررات معقولة تدعو بأن الجريمة قد وقعت أو يشتبه في وقوعها، أو أن هناك نية لإستخدامها في إرتكاب جريمة، أو أنه سوف يتيح دليلًا على إرتكاب هذه الجريمة.[2]

2- الإتجاه الثاني:

بينما ذهب رأي آخر إلى عدم إعتبار الكيان المعنوي للجهاز الإلكتروني - كالمعطيات غير المرئية أو غير الملموسة- "شيئًا"، لأن المقصود بلفظ الشيء هو ما كان ماديًا أي ملموسًا، أما المعطيات غير المرئية أو غير الملموسة لا يمكن إعتبارها شيئًا، وكذا على الأدلة الإلكترونية غير المادية كالمستندات الإلكترونية، ذلك أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء الملموسة، ونظرًا لأنها لا تعد شيئًا ماديًا بالمعنى المألوف للكلمة فإنه لا يمكن ضبطها.[3]

ولذلك يقترح هذا الإتجاه إزاء هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش إمكانية البحث وضبط المعطيات المعالجة آليًا، وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة المادية أو أية مادة معالجة بواسطة الجهاز الإلكتروني.[4]

ولمواكبة هذه التغيرات قام المشرع الفرنسي بتعديل نصوص التفتيش وأضاف عبارة المعطيات المعلوماتية في المادة 94 من قانون الإجراءات الجزائية بموجب المادة 42 من القانون رقم: 2004-575 المؤرخ في 21 جوان 2004 المتعلق بالثقة في الإقتصاد الرقمي لتصبح هذه المادة على النحو التالي: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على الأشياء أو المعطيات المعلوماتية، يكون كشفها مفيدًا لإظهار الحقيقة..."[5].

[1]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 565.

[2]- حبيباتني بثينة، مرجع سابق، ص 318.

[3]- بلحسيني حمزة، مرجع سابق، ص 328.

[4]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 566.

[5]-Art 94 du C.P.P.F (Modifié par LOI n°2010-768 du 9 juillet 2010 - art. 1) dispose que: « Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité...».

3- الإتجاه الثالث:

وفي مقابل هذين الرأيين يوجد رأي آخر نأي بنفسه عن البحث عما إذا كانت كلمة "شيء" تشمل المعطيات المعنوية لمكونات الجهاز الإلكتروني أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على معطيات الجهاز الإلكتروني إذا إتخذت شكلًا ماديًا.[1]

ويخلص أصحاب المسار إلى أن البرامج المعلوماتية يمكن أن تنطبق عليها خصائص وسمات المادة وبالتالي تدخل في نطاق الأشياء المادية، ويستوي في ذلك أن تكون برامج المنظومة أو برامج تطبيقات، مستندين في ذلك إلى أن المادة هي كل ما يشغل حيزًا ماديًا في فراغ معين وأن هذا الحيز يمكن قياسه والتحكم فيه، وبناءً عليه فإن الكيان المعنوي (المنطقي) للجهاز الإلكتروني أو البرنامج يشغل حيزًا ماديًا في الذاكرة ويمكن قياسه بمقياس معين هو البايت (Byte) والكيلوبايت (KB) والميغابايت (MB)، وهكذا تقاس سعة أو حجم الذاكرة الداخلية بعد الحروف التي يمكن خزنها فيها.[2]

فالمعطيات تكون في شكل نبضات إلكترونية ممثلة بالرقمين الصفر والواحد وهي تشبه التيار الكهربائي الذي إعتبرته الكثير من التشريعات من الأشياء المنقولة، وبالتالي فإن المعلومات يمكن أن تدخل في نطاق الأشياء المادية[3] لأنها قابلة لأن تسجل أو تخزن على وسائط إلكترونية يمكن قياسها، وبهذا يثبت الطابع المادي لها إذ يمكن لمسه في المحيط المعنوي الخارجي، وبالتالي يمكن خضوعها لقواعد التفتيش التقليدية[4].

وبالتالي فإن تفتيش الوسط الرقمي يكون صحيحًا إذا أسفر عن وجود معطيات إتخذت فيما بعد شكلًا ماديًا، وهذا الإتجاه أخذ به قانون الإجراءات الألماني في القسم 94 منه حينما نص على أن الأدلة المضبوطة يجب أن تكون ملموسة، ولذلك فإن المعطيات إذا تمت طباعتها تعد أشياء ملموسة يمكن ضبطها.[5]

ولذلك فإن الجرائم التي ترتكب على الكيانات المادية يسهل إكتشاف أمرها وضبطها، وأما الجرائم التي تقع على الكيانات المعنوية فإنه يصعب إكتشافها إذا ظلت على صورتها المعنوية

---

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 198.
[2]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص-ص 146-147.
[3]- بوكر رشيدة، مرجع سابق، ص 277.
[4]- حبيباتني بثينة، مرجع سابق، ص 319.
[5]- أومدور رجاء، مرجع سابق، ص 140.

في شكل نبضات أو ذبذبات، وأما إذا تحولت إلى مستخرجات أو مستندات أو سجلات فإنه يسهل الوصول إلى الجرائم التي ترتكب عليها.[1]

ثالثًا: موقف المشرع الجزائري

قبل التطرق إلى موقف المشرع الجزائري سنعرض أهم الإتفاقيات ذات الصلة، إبتداءً بإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 التي حثت دول الأعضاء على تجسيد أحكام خاصة بالتفتيش النظم المعلوماتية في قوانينها الإجرائية لتفادي أي إشكال يمكن أن يثار حول الموضوع، وذلك بتخويل سلطاتها المكلفة بمكافحة الإجرام صلاحيات التفتيش والولوج للمعطيات المعلوماتية التي تم إحتواؤها سواء في داخل النظام المعلوماتي[2] -المصطلح الذي تقابله عبارة "المنظومة المعلوماتية" في التشريع الجزائري والمعتمد في دراستنا- أو في جزء منه، أو على دعامة تخزين مستقلة[3]، وذلك من خلال الفقرة الأولى من المادة 19 منها التي تنص على أن: "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير، بغية تمكين سلطاتها المختصة سلطة التفتيش أو الولوج بطريقة مشابهة[4]:

---

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 200.

[2]- عرفت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 النظام المعلوماتي في الفقرة (أ) من المادة الأولى منها كالآتي: "يعني كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى، تنفيذًا لبرنامج معين، بأداء معالجة آلية للبيانات".
النظام المعلوماتي (Le systéme informatique) عبارة عن جهاز يتكون من مكونات مادية ومكونات منطقية، وذلك بغرض المعالجة الآلية للمعطيات، والتي تعني مجموعة من العمليات التي تطبق على المعطيات من خلال برنامج معلوماتي، والذي يعني بدوره مجموعة من الأوامر التي يمكن أن تنفذ من خلال الجهاز. ويشتمل النظام المعلوماتي على وسائل أو وحدات لإدخال وإخراج وتخزين المعطيات، وهو قد يكون منفردًا أو منفصلًا بمجموعة من الأجهزة المماثلة عن طريق شبكة وهي عبارة عن أداة ربط بين جهازين أو أكثر، وهذه الرابطة يمكن أن تكون أرضية كالسلك أو الكابل، كما يمكن أن تكون لاسلكية مثل الراديو أو الأشعة تحت الحمراء أو القمر الصناعي أو كليتهما معًا، أي سلكية ولاسلكية. كما يمكن أن تكون الشبكة مقتصرة جغرافيًا على منطقة صغيرة فتسمى شبكة محلية، أو أن تغطى منطقة كبيرة فتسمى شبكة واسعة أو ممتدة. وتعد شبكة الإنترنت شبكة عالمية لأنها تتكون من العديد من الشبكات المتصلة معًا والتي تعرف بإسم (TCP/IP) أي بروتوكول إتصالات الإنترنت، وهو البروتوكول الذي يجمع بين بروتوكولي (TCP) و(IP) للإتصالات والذي أصبح البروتوكول المعتمد لهذه الشبكة، وللمزيد من التفصيل، هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 276-277.

[3]-عملية تفتيش وضبط دعامة تخزين معلوماتية التي تسمح بتخزين المعطيات المعلوماتية المنصوص عليها في بند (ب) من الفقرة الأولى من المادة 19، يمكن أن يتم إجراؤها بالإستفادة من سلطات التفتيش التقليدية بيد أن تطبيق إجراء التفتيش المعلوماتي يستلزم غالبًا ليس فقط تفتيش النظام بل أيضًا كل دعامة تخزين مشتركة كالأقراص تكون مجاورة مباشرة لهذا النظام المعلوماتي، ولذلك وبسبب هذه العلاقة بين الإثنين فإن الفقرة الأولى تقرر تأهيل سلطة كلية تغطى الموقفين، وللمزيد من التفصيل، نفس المرجع، ص 234.

[4]- مصطلح التفتيش لا يثير أية صعوبة، إذ يقصد به البحث والتنقيب عن أدلة الجريمة بفحص المعطيات ومحاولة معرفة محتواها أو خط سيرها، أما مصطلح الدخول وما يعبر عنه أحيانًا بالولوج فهو مصطلح خاص بنظم التكنولوجيا والإتصال يحقق الوصول إلى المعطيات المخزنة ويقتضيه بطبيعة الحال إجراء التفتيش والحصول على الأدلة، ولهذا ثمة فرق بين الإثنين، فالدخول إجراء للتفتيش والتفتيش وسيلة لجمع الأدلة، ورغم هذه التفرقة فإنهما يعتبران من إجراءات التحقيق الماسة=

أ- لنظام معلوماتي أو أي جزء منه، وكذا المعطيات المعلوماتية[1] المخزنة فيه، على أراضي الدولة الطرف؛

ب- لدعامة تخزين المعلوماتية، تسمح بتخزين المعطيات المعلوماتية".[2]

تهدف هذه المادة إلى تحديث وتناغم التشريعات الداخلية المتعلقة بالتفتيش وبضبط المعطيات المعلوماتية المخزنة، بهدف تجميع أدلة تتصل بتنقيبات أو إجراءات جنائية معينة، كل تشريع داخلي يتعلق بالإجراءات الجنائية يقرر السلطات المختصة بالتفتيش وضبط الأشياء المادية، ومع ذلك ففي غالبية الدول فإن المعطيات المعلوماتية المخزنة لا تعتبر في حد ذاتها كأشياء مادية، وبالتالي لا يمكن الحصول عليها أو ضبطها لأغراض التحري والتحقيق بنفس طريقة الأشياء المادية، لكن على الأقل يمكن ضبط حاملة المعطيات أي الدعامة التي تم تخزين المعطيات عليها، وبالتالي إن الهدف من هذه المادة هو إقامة سلطة مساوية أو معادلة خاصة بالمعطيات المخزنة.[3]

وقد تبنت الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات ذات المبدأ في الفقرة الأولى من المادة 26 منها، إلى تمكين الدول الأعضاء سلطاتها المختصة من التفتيش أو الوصول إلى تقنية معلومات[4] -المصطلح الذي تقابله عبارة "المنظومة المعلوماتية" في التشريع

=بحقوق الأفراد، لذا يجب أن يستند إتخاذها إلى نص قانوني وهذا ما نصت عليه المادة 2/19 من الإتفاقية، وللمزيد من التفصيل، ينظر: رامي متولي القاضي، عمر سالم، مرجع سابق، ص-ص 284-285.

[1]-عرفت الفقرة (ب) من المادة الأولى من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 البيانات المعلوماتية (Les données informatiques) بأنها: "تعني كل تمثيل للوقائع، أو المعلومات، أو المفاهيم تحت أي شكل، وتكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة، يجعل الحاسب يؤدي المهمة".

تشير المذكرة التفسيرية للإتفاقية إلى أن تعريف البيانات المعلوماتية الوارد بالفقرة (ب) من المادة الأولى من هذه الإتفاقية مأخوذ عن هيئة التوصيف العالمية الإيزو (ISO). وأن هذا التعريف يتضمن ضمن ما يتضمنه عبارة "التي تكون مهيأة للمعالجة الآلية"، وهذا يعني أن البيانات لابد أن توضع في شكل يسمح بمعالجتها مباشرة عن طريق الحاسوب. ومن أجل توضيح أكثر لمعنى "البيانات" في الإتفاقية يجب أن يتم فهمها على أنها: "بيانات تأخذ شكلًا إلكترونيًا أو أي شكل آخر يسمح بمعالجتها مباشرة، وفقًا لبرنامج معين يجعل الحاسوب يؤدي المهمة المنوطة به"، وللمزيد من التفصيل، هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 46-47.

[2]- Art 19 paragraphe 01 du convention sur la cybercriminalité dispose que : « Perquisition et saisie de données informatiques stokées:

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquistionner ou à accéder d'une façon similaire:

a. à un systéme informatique ou à une partie de celui-ci ainsi qu'au données informatiques qui y sont stockées; et

b. á un support du stockage informatique permettant de stocker des données informatiques sur son territoire».

[3]- هلالي عبد اللاه أحمد، مرجع سابق، ص 229.

[4]- عرفت الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات "تقنية المعلومات" في الفقرة الأولى من المادة 02 منها بأنها: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها وإسترجاعها ومعالجتها وتطويرها وتبادلها، وفقًا للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيًا ولاسلكيًا في نظام أو شبكة".

الجزائري المعتمد في دراستنا- أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها، وبيئة أو وسيط لتخزين المعلومات التقنية والتي قد تكون مخزنة فيه أو عليه.

أما بالنسبة لموقف المشرع الجزائري، فقد أجاز تفتيش المنظومة المعلوماتية[1] بموجب المادة 05 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر، والتي نصت على أن: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04، الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها؛
ب-منظومة تخزين معلوماتية".

وكذا الفقرة الأولى من المادة 16 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور التي تجيز للسلطات القضائية المختصة تلقائيًا أو بناء على طلب ضابط الشرطة القضائية، الأمر بالتفتيش الإلكتروني ولو عن بعد لمنظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية[2] المخزنة فيها أو منظومة تخزين معلوماتية، قصد معاينة الجرائم المنصوص عليها في هذا القانون بما في ذلك جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور.

الفرع الثاني: تفتيش المنظومة المعلوماتية عن بعد

بسبب ترابط النظم المعلوماتية وإتصال بعضها ببعض، فإن المعطيات محل البحث قد لا تكون مخزنة فعليًا في الجهاز الإلكتروني بل قد تكون محفوظة في منظومة معلوماتية أخرى، إلا أنه يمكن الوصول إليها بسهولة عن طريق المنظومة المرتبطة بالجهاز محل التفتيش، كما يمكن أن تكون المعطيات مخزنة في أداة تخزين تشترك مباشرة بالجهاز أو مرتبطة بطريقة غير مباشرة عبر نظم الإتصالات كالإنترنت.[3]

يثير هذا الفرض تساؤلًا هامًا يتعلق بإمكانية إمتداد حق التفتيش في حال تبين أن الجهاز الإلكتروني أو الطرفية النهائية (Terminal endpoint) الموجودة في منزل المتهم متصلة

[1]- عرفت الفقرة (ب) من المادة 02 من القانون رقم: 09-04 السالف الذكر المنظومة المعلوماتية بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج معين".

[2]- عرفت الفقرة (ج) من المادة 02 من القانون رقم: 09-04 السالف الذكر المعطيات المعلوماتية بأنها: "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

[3]- هلالي عبد اللاه أحمد، مرجع سابق، ص 232.

بجهاز أو طرفية في مكان آخر مملوك لشخص أخر خلاف المتهم؟ وللإجابة على هذا التساؤل المطروح لابد من التمييز بين الفرضين التاليين:

أولًا: إتصال جهاز المتهم بجهاز أو الطرفية النهائية موجودة في مكان آخر داخل الدولة

تتحقق هذه الفرضية عندما يقوم الجاني بتحويل معلومات أو معطيات مرتبطة بجريمة تمس مستندًا إلكترونيًا، من جهازه الخاص إلى جهاز أو منظومة معلوماتية مملوكة لشخص آخر وموجودة في مكان آخر، ليتم تخزينها هناك.[1]

تسمح الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 للدول الأطراف أن تمد نطاق التفتيش إلى نظام معلوماتي، إذا كان هناك إعتقاد بأن المعطيات المطلوبة مخزنة في نظام معلوماتي آخر أو في جزء منه على أرضها، إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش[2]، كما أجازت الإتفاقية العربية لجرائم تقنية المعلومات من خلال الفقرة 02 من المادة 26 على كل دولة طرف على توسيع نطاق التفتيش أوالوصول إلى تقنية معلومات معينة أو جزء منها، إذا كان هناك إعتقادًا بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها، وكانت هذه المعلومات قابلة للوصول قانونًا أو متوفرة في التقنية الأولى، فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.

ويرى البعض في ألمانيا بشأن إمكانية إمتداد الحق في التفتيش، أنه إذا تبين أن الطرفية النهائية للجهاز في منزل المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم، ففي هذه الحالة يمكن أن يمتد التفتيش إلى السجلات والمعطيات الموجودة في مكان آخر إستنادًا إلى مقتضيات القسم 103 من قانون الإجراءات الجنائية الألماني[3]، والتي تجيز هذه الأخيرة على إمكانية التمديد بدون الحاجة إلى الإذن القضائي يخص هذا التمديد، كلما دعت ضرورات التحقيق إلى ذلك[4].

كما حسمت بعض التشريعات هذه المسألة، فنجد الفقرة 03 من المادة 02 من القانون البلجيكي الصادر بتاريخ 25 ديسمبر 2016 المتعلق بتحسين أساليب التفتيش، وبعض تدابير التحقيق المتعلقة بالإنترنت والإتصالات الإلكترونية، وإنشاء قاعدة بيانات للبصمات الصوتية،

---

[1]- براهيمي جمال، مرجع سابق، ص 22.

[2]-Art 19 paragraphe 02 du convention sur la cybercriminalité dispose que : « Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe1a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir de système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou d'un accés d'une façon similaire à l'autre système».

[3]- خالد عياد الحلبي، مرجع سابق، ص-ص 164- 165.

[4]- براهيمي جمال، مرجع سابق، ص 22.

والمعدلة للمادة 39 مكرر من قانون التحقيق الجنائي، تجيز تمديد التفتيش إلى المنظومة المعلوماتية أخرى، توجد في مكان آخر غير مكان التفتيش الأصلي، بناءً على الإذن من وكيل الجمهورية وذلك كالآتي: "إذا كان ضروريًا لكشف الحقيقة بشأن الجريمة محل البحث، إذا كانت الإجراءات الأخرى غير مناسبة، أو وجدت مخاطر تتعلق بضياع عناصر الإثبات".[1]

ونجد المشرع الفرنسي قد حسم هذا الإشكال بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون رقم: 2003- 239 الصادر في 18 مارس 2003 بشأن الأمن الداخلي في فرنسا، حيث أضاف المادة 57-1 في قانون الإجراءات الجزائية بموجب المادة 17-1 منه والذي نص على أنه: "يجوز لضباط الشرطة القضائية أو تحت مسؤولياتهم ولأعوان الشرطة القضائية أثناء عملية التفتيش تمت وفقًا للشروط المنصوص عليها في هذا القانون، بالدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يجرى فيها التفتيش إلى المعطيات التي تهم التحقيق المخزنة في هذا النظام أو في أي نظام معلوماتي آخر، ما دام أن هذه المعطيات متاح الدخول إليها من النظام الرئيسي أو من نظام مرتبط بالنظام الرئيسي، كما يجوز لهم أيضًا في إطار شروط التفتيش المنصوص عليه في هذا القانون الولوج عن طريق الأنظمة المعلوماتية المثبتة في أماكن الخدمة أو وحدات الشرطة أو الدرك إلى المعطيات التي تهم التحقيق الجاري والمخزنة في نظام معلوماتي آخر، إذا كانت هذه المعطيات يمكن الوصول إليها من النظام الرئيسي".[2]

أما فيما يتعلق بموقف المشرع الجزائري، فإن الفقرة 02 من المادة 05 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر تنص على أن: "في الحالة المنصوص عليها في الفقرة (أ)[3] من هذه المادة، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها إنطلاقًا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقًا بذلك"، بحيث يسمح للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من نفس القانون، تمديد التفتيش عن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى بسرعة إلى

[1]- لهوى رابح، مرجع سابق، ص-ص 215-216.

[2]-Art 57-1 paragraphe 01,02 du C.P.P.F (créé par loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure, art 17) dispose que: « Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. Ils peuvent également, dans les conditions de perquisition prévues au présent code, accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial».

[3]- منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها.

هذه المنظومة أو جزء منها داخل الإقليم الوطني، مع إعلام السلطة القضائية المختصة بذلك مسبقًا.

ثانيًا: إتصال جهاز المتهم بجهاز آخر أو الطرفية النهائية موجودة في مكان آخر خارج الدولة

قد يتبين أحيانًا أثناء التحقيق الجنائي في بعض الحالات أنه من الضروري تفتيش جهاز إلكتروني موجود خارج إقليم الدولة، وذلك عندما يقدم الجاني على تخزين المعطيات في الأنظمة المعلوماتية تقع خارج الدولة، مستخدمًا في ذلك شبكة الإتصالات بهدف إعاقة عملية جمع الأدلة، وهو ما يقتضي تمديد الإذن بالتفتيش إلى خارج إقليم الدولة ويدخل بذلك في النطاق الجغرافي للدولة الأخرى، وهو ما يطلق عليه بالتفتيش عبر الحدود.[1]

هذه الطبيعة التي تتميز بها الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص كونها جريمة عابرة للحدود، خلقت العديد من الإشكاليات حول تحديد الدولة صاحبة الإختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه، بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وبالتالي فإن الوصول للحقيقة بشأنها يستوجب الإستعانة بخبرة فنية عالية المستوى.[2]

إذ يتشكك البعض في ألمانيا في مسألة الولوج إلى الأنظمة المعلوماتية الأجنبية لضبط المعطيات المخزنة فيها، بقولهم: أن السماح بإسترجاع المعطيات التي تم تخزينها بالخارج، وخاصة عندما يكون ذلك الإسترجاع مرتبطًا بالوضع القائم لحساب في بنك أمر مشكوك فيه، وأنه في ظل غياب الإتفاق الخاص بين الدول المعنية، قد يعتبر ذلك خرقًا لحقوق السيادة لدولة أخرى، وخرقًا للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائية.[3]

ويؤيد هذا الرأي التطبيق القضائي في ألمانيا، ففي إحدى قضايا الغش المعلوماتي أثناء إجراءات التحقيق عن جريمة غش وقت وقعت في معطيات الحاسوب، فقد تبين وجود إتصال بين الجهاز المتواجد في ألمانيا وبين شبكة إتصالات في سويسرا، حيث تخزن من خلالها معطيات المشروعات فيها، وعندما أرادت سلطات التحقيق الألمانية ضبط هذه المعطيات، فلم تتمكن من ذلك إلا عن طريق إلتماس المساعدة الذي تم بالتبادل بين الدولتين.[4]

وفي سبيل تجنب هذه العقبات الإجرائية وحتى لا يفسح المجال أمام المجرمين للإفلات من العقاب، سعى المجلس الأوروبي من خلال توصيته رقم: 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات على أنه : "يجوز لسلطة التحقيق والإستدلال بمناسبة التفتيش الإلكتروني، بسط مجال تفتيش جهاز إلكتروني معين يدخل في

---

[1]- بوكر رشيدة، مرجع سابق، ص 283.

[2]- علي جعفر، **جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة**، الطبعة الأولى، 2013، منشورات زين الحقوقية، بيروت-لبنان، ص 99.

[3]- طارق إبراهيم الدسوقى عطية، **الأمن المعلوماتي النظام القانوني للحماية المعلوماتية**، د.ر.ط، 2009، دار الجامعة الجديدة للنشر، الإسكندرية-مصر، ص- ص 388-389.

[4]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 206.

دائرة إختصاصها إلى غيرها من الأجهزة الإلكترونية المرتبطه به، بواسطة شبكة الإنترنت بما فيها المتواجدة خارج الإختصاص الوطني وضبط المعطيات المتواجدة فيها، كلما كان التدخل الفوري للقيام بذلك ضروريًا"[1]، بمعنى أن يمتد تفتيش الإلكتروني للجهاز إلى الشبكة المتصلة به، ولو كانت تلك الشبكة تقع داخل إقليم دولة أخرى.

وأجاز المجلس الأوروبي في التوصية رقم: 17 لسنة 1995 إلى التأكيد على إمكانية إمتداد نطاق تفتيش الإلكتروني إلى المنظومة المتواجدة في الخارج، متى كانت هناك ضرورة لإتخاذ إجراءات عاجلة في هذا الأمر، ولكن يجب أن يتم الحصول على موافقة الدولة التي يمتد التفتيش إلى الأجهزة أو المنظومة المتواجدة في إقليمها، وذلك حتى يكون هذا التفتيش ذو أساس قانوني، وكي لا يمثل إنتهاكًا لسيادة تلك الدولة[2]، بنصه على أن: "يمكن أن يمتد نطاق تفتيش الجهاز إلى المنظومة المتواجدة في الخارج، إذا كان من الضروري إتخاذ إجراءات عاجلة في هذا الشأن، ويتعين أن يوجد أساس قانوني لإمتداد بحال هذا النوع من التفتيش، حتى لا يشكل ذلك الإجراء مخالفة لسيادة دولة أجنبية، لذلك فإنه من الضروري الحصول على موافقة الدولة التي يمتد التفتيش إلى منظومة تتواجد على إقليمها".[3]

وبناءً على ذلك، ففي هولندا فإن مشروع قانون جريمة الحاسب يصرح لجهات التحقيق بإجراء التفتيش داخل الأماكن بما يتضمن تفتيش الأنظمة المعلوماتية المرتبطة حتى إذا كانت موجودة في دول أخرى، وذلك بشرط أن يكون هذا التدخل مؤقتًا وأن تكون المعطيات التي يتم التفتيش عنها لازمة لإظهار الحقيقة (المادة j/125).[4]

ويتحفظ البعض في هولندا على نص المادة j/125 ، بالقول إنه قد يكون من الأفضل لأسباب عملية السماح بالتفتيش لمنظومة معلوماتية الموجودة في بلد أجنبي بغرض ضبط المعطيات المخزنة فيها، بيد أن هذا الإختراق المباشر وفقًا لتقرير المجلس الأوروبي يعتبر إنتهاكًا لسيادة دولة أخرى، ولذا فإنه مع عدم وجود إتفاقية دولية فإن هذا الإختراق المباشر الذي تتضمنه المادة J/125 يفضل عدم تطبيقه.[5]

ونصت المادة 88 من قانون تحقيق الجنايات البلجيكي الصادر في 23 نوفمبر 2000 على أنه: "إذا أمر قاضي التحقيق بالتفتيش في منظومة معلوماتية أو في جزء منها، فإن هذا البحث يمكن أن يمتد إلى منظومة معلوماتية أخرى توجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الإمتداد وفقًا لضابطين:

1- إذا كان ضروريًا لكشف الحقيقة بشأن الجريمة محل البحث؛

[1]- براهيمي جمال، مرجع سابق، ص 27.
[2]- بلحسيني حمزة، مرجع سابق، ص 336.
[3]- عائشة بن قارة مصطفى، مرجع سابق، ص 98.
[4]- طارق إبراهيم الدسوقى عطية، مرجع سابق، ص 388.
[5]- نفس المرجع، ص 388.

2- إذا وجدت مخاطر تتعلق بضياع بعض الأدلة، نظرًا لسهولة عملية محو أو إتلاف، أو تحريف أو نقل المعطيات محل البحث.[1]

ويبرر البعض على هذا النص بالقول بأن سلطة التحقيق يمكنها الدخول إلى المنظومة المعلوماتية والإطلاع على المعطيات المطلوبة دون أن تدرك أن هذه المعطيات توجد من الناحية المادية خارج إقليم بلجيكا، والبديل لهذا النص هو إرسال لجنة قضائية إلى الدولة المعنية وتطلب من السلطة المختصة بها أن تتحفظ على المعطيات المكونة لمحل الجريمة وتعطيها نسخة منها، غير أن هذا الإجراء قد يستغرق وقتًا مما قد يمنح للمتهم فرصة لتدمير هذه المعطيات، ومع ذلك يعترف الفقه بأن هذا النص يمثل إعتداء على سيادة الدولة.[2]

لذا فإن البعض يرى أن التفتيش الإلكتروني العابر للحدود لابد وأن يتم في إطار إتفاقيات تعاون خاصة ثنائية أو دولية تجيز هذا الإمتداد تعقد بين الدول المعنية، وبالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في ظل غياب تلك الإتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى، وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني.[3]

وفي نفس السياق أوصت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 للدول من خلال مادتها 25، على جميع دول الأطراف فيها بضرورة توفير المساعدة المتبادلة لبعضها البعض على أوسع نطاق، لغايات التحقيقات أو الإجراءات المتعلقة بالجرائم ذات الصلة بالنظم والمعطيات المعلوماتية أو لجمع الأدلة الإلكترونية، وكذا تكون المساعدة المتبادلة خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة، أو في معاهدات المساعدة المتبادلة، بما في ذلك الأسباب التي يجوز للدولة الطرف المطلوب منها المساعدة أن ترفض التعاون على أساسها.[4]

وقد تصدى المشرع الفرنسي لهذا الإشكال في قانون الإجراءات الجزائية وذلك بموجب الفقرة 03 من المادة 57-1 المضافة بموجب المادة 17 من القانون الأمن الداخلي رقم: 2003-239، والتي تنص على أن: "إذا تبين مسبقًا أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليم الوطني، وأنه يمكن الدخول إليها أو أنها متاحة إنطلاقًا من النظام الرئيسي، فإنه يمكن الحصول عليها من طرف ضباط الشرطة القضائية وفقًا للشروط

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص-ص 203-204.

[2]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 275.

[3]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص-ص 205-206.

[4]-Art 25 paragraphe 01, 04 du convention sur la cybercriminalité dispose que: «Principes généraux relatifs à l'entraide:

1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

4....l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération....».

المنصوص عليها في المعاهدات الدولية"[1] بحيث أجاز لضباط الشرطة القضائية القيام بتفتيش الأنظمة المعلوماتية ولو كانت متواجدة خارج الإقليم الوطني، شريطة أن يتم مراعاة الشروط المنصوص عليها في المعاهدات الدولية.

وهو نفس الموقف الذي عبر عنه المشرع الجزائري من خلال الفقرة 03 من المادة 05 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر على النحو التالي: "إذا تبين مسبقًا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقًا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة، طبقًا للإتفاقيات الدولية ذات صلة ووفقًا لمبدأ المعاملة بالمثل"، بحيث لم يسمح المشرع الجزائري التفتيش عن بعد لأنظمة معلوماتية المتواجدة خارج الإقليم الوطني، إلا في إطار المساعدة المتبادلة مع السلطات الأجنبية المختصة طبقًا للإتفاقيات الدولية ذات الصلة ووفقًا لمبدأ المعاملة بالمثل.

لم ينص المشرع الجزائري الضوابط التي ينبغي إعتمادها عند تمديد التفتيش، وإنما إكتفى فقط بذكر الأسباب للقيام بذلك، والمتمثلة في الإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، ولم يبين على أن هذا التمديد لابد أن يكون ضروريًا للكشف عن الحقيقة.[2]

فتحسبًا لطابع السرعة الفائقة الذي يجري عليه نقل المعلومات الإجرامية وتهريبها للخارج بقصد تخزينها وإخفائها، وما يستدعيه من الإستعجال في تعقب آثارها وضبطها لإستعمالها كدليل إثبات، وسعت بعض التشريعات المقارنة من صلاحيات سلطات التحقيق للقيام بتفتيش الأنظمة المتصلة حتى لو كانت متواجدة خارج إقليمها الوطني، وقرنت ذلك بحالة الضرورة.[3]

فقد نصت المادة 41 من إتفاقية تريس (TRIES) على إلزام الأعضاء أن يتخذوا إجراءات الإنقاذ التي تتيح إتخاذ تدابير فعالة ضد أفعال التعدي، بما في ذلك التدابير السريعة للحيلولة دون التعديات والتدابير التي تشكل رادعًا لأي تعديات أخرى، ومن بين التدابير الرئيسية المطلوبة لإستحداث معدلات ردع أكثر فعالية ضد أفعال النسخ الرقمية غير المرخص بها، إتخاذ

[1] -Art 57-1 paragraphe 03 du C.P.P.F (créé par loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure, art 17, Modifié par LOI n°2023-22 du 24 janvier 2023 -art. 24) dispose que: « s'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur».

[2]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص 300.

[3]- محمود سعد عبد المجيد، مرجع سابق، ص 484.

إجراءات سريعة بالتفتيش دون علم الطرف الآخر وهو أمر ضروري للإحتفاظ بأدلة النسخ غير المشروعة للأعمال المخزنة إلكترونيًا في وسائط إلكترونية يمكن سحبها بسهولة.[1]

وهو ما أجازت به المادة 32 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 للدول الأطراف على إمكانية الدخول في أجهزة أو منظومة معلوماتية تابعة لدولة أخرى بغرض التفتيش والضبط بدون الحصول على إذنها، في حالتين:

أ- عندما تكون المعطيات المعلوماتية التي تم الوصول إليها متاحة للجمهور، بغض النظر عن موقعها الجغرافي؛

ب-عندما يتم الوصول إلى هذه المعطيات المخزنة الموجودة لدى دولة طرف أخرى أو تلقيها من خلال نظام معلوماتي داخل إقليمها، بناء حصول تلك الدولة طرف على الموافقة القانونية والإرادية من الشخص الذي يملك السلطة القانونية للكشف عن المعطيات لتلك الدولة الطرف عبر نظام معلوماتي المذكور".[2]

وتجدر الإشارة إلى أن الحصول على موافقة الشخص الذي يملك سلطة الكشف عن المعطيات المطلوبة، يتطلب ضرورة وجود إتفاقية بين الدولتين، أو طلب الإذن من الدولة التي تتواجد على إقليمها تلك المعطيات.[3]

وقد إقترحت لجنة الدول أطراف هذه الإتفاقية على إثر المناقشات التي أجرتها في سنة 2009 إضافة حالات أخرى إلى الحالتين المشار إليهما في المادة 32 من الإتفاقية، وهي:

1- حالة التفتيش عن بعد بحسن نية؛
2- حالات الإستعجال القصوى أو الحالات الإستثنائية؛
3- حالة التفتيش عن بعد وفقًا لمعيار مشروعية التفتيش "سلطة الإستعمال".[4]

إلا أن قد لقي ذلك إعتراض من قبل الفقه والقضاء في معظم الدول، نظرًا لما يتضمنه من إنتهاك لسيادة الدول وخرق لإختصاصها الوطني، وعليه يفضل أن يتم التفتيش العابر للحدود في إطار التعاون القضائي الدولي وفقًا لآليات الإتصال سريعة وميسرة يتم تحديدها في إتفاقيات الدولية الثنائية أو متعددة الأطراف.[5]

---

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 311.

[2] -Art 32 du convention sur la cybercriminalité dispose que: « Une partie peut, sans l'autorisation d'une autre partie:
a: accéder à des données informatiques, stockées accessibles au public source ouverte,
quelle que soit la localisation géographique de ces données,
b: accéder à, ou recevoir au moyen d'un système informatique situé sur un territoire, des données informatiques stockées situées dans un autre état, si la partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique».

[3]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص 298.

[4]- محمود سعد عبد المجيد، مرجع سابق، ص 485.

[5]- براهيمي جمال، مرجع سابق، ص-ص 30-31.

الفرع الثالث: شروط التفتيش الإلكتروني

إذا كان التفتيش بمفهومه التقليدي يستوجب توافر مجموعة من الشروط أو الضوابط فيما يتعلق بعملية البحث عن الدليل الإلكتروني، فإن كثيرًا من هذه الشروط تبقى مستمرة في البيئة الرقمية وتنطبق عليها، ولكن يبقى الإختلاف في الأسلوب المتبع في التفتيش، ذلك أن التفتيش في مجال التقنيات الحديثة إجراء معقد وصعب، ولما كان التفتيش إجراء خطيرًا يمس حرية وخصوصية الإنسان، فقد حرصت القوانين المقارنة على إحاطته بضمانات وضوابط أساسية لكي تسبغ عليه نوع من المشروعية عند مباشرته، لذلك وجب وضع جملة من الضوابط التي تحكم إجرائه[1]، ومن هذه الضوابط ما يلي :

أولًا: الشروط الشكلية لتفتيش الإلكتروني

الضوابط الشكلية لا تهدف إلى مجرد تحقيق مصلحة العدالة في ضمان مشروعية الإجراءات المتخذة فحسب، بل سياجًا يحمي حقوق وحريات الإنسان وحرمة مسكنه وحياته وممتلكاته الخاصة، وتتمثل في ما يلي:

1- قاعدة الحضور أثناء التفتيش الإلكتروني:

تنص القاعدة العامة على أن عملية إجراء التفتيش يتم في المسكن بحضور شخص المشتبه فيه، فإذا تعذر عليه الحضور وقت ذلك الإجراء يلزم على الضابط الشرطة القضائية المكلف بالتفتيش أن يكلفه بتعيين ممثل له، وإذا إمتنع عن ذلك أو كان هاربًا إستدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.[2]

وإذا جرى التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقًا أو أشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش، وإن تعذر ذلك إتبع الإجراء المنصوص عليه في الفقرة السابقة.[3]

وإذا حدث أثناء التحري في جريمة متلبس بها أو تحقيق متعلق بإحدى الجرائم المذكورة في الفقرة 03 من المادة 78 من ذات القانون بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، وكان الشخص الذي يتم تفتيش مسكنه موقوفًا للنظر أو محبوسًا في مكان آخر، وأن الحال يقتضي عدم نقله إلى ذلك المكان لإحتمال فراره أو إختفاء الأدلة خلال المدة اللازمة لنقله أو بسبب مخاطر جسيمة قد تمس بالنظام العام، يمكن أن يجرى التفتيش بعد الموافقة المكتوبة المسبقة من وكيل الجمهورية

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص 118.
[2]- المادة 1/76/ البند 1 من القانون رقم: 25-14 السالف الذكر.
[3]- المادة 1/76/ البند 2 من القانون رقم: 25-14 السالف الذكر.

أو قاضي التحقيق وبحضور شاهدين مسخرين وفقًا للإجراء المنصوص عليه في المادة 76 من نفس القانون، أو بحضور ممثل يعينه صاحب المسكن محل التفتيش.[1]

وإذا كان القائم بالتفتيش قاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه في مسكن المتهم فعليه أن يلتزم بما سبق ذكره بوجوب حضور المتهم أو ممثله أو شاهدين، ويجوز للقاضي التحقيق في مواد الجنايات أن يقوم بتفتيش مسكن المتهم بنفسه وأن يكون ذلك بحضور وكيل الجمهورية[2].

وإذا حصل التفتيش في مسكن غير مسكن المتهم، يستدعى صاحب المنزل الذي يجري تفتيشه ليكون حاضرًا وقت التفتيش، فإذا كان ذلك الشخص غائبًا أو رفض الحضور أجري التفتيش بحضور إثنين من أقاربه أو أصهاره الحاضرين بمكان التفتيش، فإن لم يوجد أحد منهم فبحضور شاهدين لا تكون ثمة بينهم وبين سلطات القضاء أو الشرطة تبعية[3].

ويعد ما سبق ذكره ضمانة حقيقة للشخص -المشتبه فيه أو للمتهم- من خطر تعسف القائم بالتفتيش، وفي الوقت نفسه يعد ضمانة بالنسبة للقائم بالتفتيش من إتهامه بإختلاق الأدلة أو تسببه في ضياع بعض الأشياء.[4]

ولضابط الشرطة القضائية وحده مع الأشخاص السابق ذكرهم الحق في الإطلاع على الأوراق أو المستندات قبل حجزها، وأيضًا إذا إقتضى الأمر أثناء إجراء التحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها مع مراعاة ما تقتضيه، كما يجب إتخاذ كل التدابير اللازمة لضمان إحترام السر في الأماكن التي تم تفتيشها يشغلها شخص ملزم قانونًا بكتمان السر المهني.[5]

رغم أن المشرع الجزائري قد أجرى تعديلًا على الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية بموجب القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006 السالف الذكر، حيث أضاف فقرة في المادة 45 تتضمن إستثناءً عن ضمانة حضور بعض الأشخاص، حيث إستغنى بموجب هذا التعديل حضور الشخص -المشتبه فيه أو المتهم- ولا رضاه أثناء عملية التفتيش، ولا حضور من يمثله أو حضور شاهدين مسخرين، إذا تعلق الأمر في إحدى الجرائم المنصوص عليها على سبيل الحصر بما في ذلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، دون الإخلال بقواعد ضمان إحترام السر المهني، وكذا جرد الأشياء وحجز المستندات التي يجب مراعاتها.

---

[1]- المادة 79 من القانون رقم: 25-14 السالف الذكر.

[2]- المادة 158 من القانون رقم: 25-14 السالف الذكر.

[3]- المادة 1/159 من القانون رقم: 25-14 السالف الذكر.

[4]- رفاه خضير جياد العارضي، مرجع سابق، ص 125.

[5]- المادة 2/76 و3، والمادة 2/97 من القانون رقم: 25-14 السالف الذكر.

إلا أنه وبعد إلغاء الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية السالف الذكر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، تم الإبقاء على نفس الضمانة، مع إعادة ترقيم المادة لتصبح المادة 76.

كما يلاحظ توسع في نطاق الجرائم التي تشملها هذه الضمانة[1]، ومن جهة أخرى قام المشرع بتغيير تسمية الجرائم التي كانت تعرف سابقًا في المادة 45 بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بتسمية جديدة "الجرائم المتصلة بتكنولوجيات الإعلام والإتصال"، وهو المصطلح الذي يشمل نطاقًا أوسع من الأفعال الإجرامية ذات الصلة بتكنولوجيا، ويعد هذا المصطلح هو المعتمد في القانون رقم: 09-04 المؤرخ في 05 أوت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.[2]

2- الميقات الزمني لإجراء التفتيش الإلكتروني:

يقصد بالميقات الزمني في التفتيش، تنظيم وقت إجراء التفتيش من قبل القائم به خلال فترة زمنية عادة ما يحددها المشرع، وذلك حرصًا على تضييق نطاق الإعتداء على الحرية الفردية وحرمة المسكن، فطبقًا للقاعدة العامة المكرسة في قانون الإجراءات الجزائية بموجب المادة 78 منه فإنه يحظر تفتيش المساكن ومعاينتها سواء من طرف ضابط الشرطة القضائية أو من طرف قاضي التحقيق قبل الساعة الخامسة (5) صباحًا وبعد الثامنة (8) مساءً، إلا أنه وكإستثناء فيمكن إذن إجراء التفتيش خارج الفترة الزمنية المسموح فيها بالتفتيش بطلب من صاحب المسكن أو بناءً على نداءات موجهة من الداخل[3] أو في الحالات الإستثنائية المقررة قانونًا، ما لم ينص القانون على خلاف ذلك.

---

[1]- الجرائم المشار إليها سابقًا في الفقرة 06 من المادة 45 من الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم السالف الذكر، تمثلت في سبعة فئات وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بجرائم الصرف، وبعد إلغاء الأمر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، أصبحت الجرائم المشمولة بهذه الضمانة منصوصًا عليها في الفقرة 06 من المادة 76 وأصبحت تشمل: جرائم القتل العمدي، جرائم المخدرات والمؤثرات العقلية، والجريمة المنظمة عبر الحدود الوطنية، والجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، وجرائم الفساد، وجرائم التهريب، وجرائم الإتجار بالبشر، وجرائم الإتجار بالأعضاء، وجرائم تهريب المهاجرين، وجرائم إختطاف الأشخاص.

[2]- المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال وفقًا للفقرة 03 من المادة 335 من القانون رقم: 25-14 السالف الذكر بأنها: "أي جريمة ترتكب أو يسهل إرتكابها إستعمال منظومة معلوماتية أو نظام للإتصالات الإلكترونية أو أي وسيلة أخرى، أو آلية ذات صلة بتكنولوجيات الإعلام والإتصال".

- وبموجب البند (أ) من المادة 02 من القانون رقم: 09-04 السالف الذكر بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية".

[3]- يبقى السؤال مطروحًا في حالة موافقة صاحب المسكن أو صدور طلب النجدة من داخل المسكن، وهي حالات نعتقد أنها تسمح منطقيًا بعدم إشتراط الإذن القضائي المسبق -قانون الإجراءات الجزائية الفرنسي لا يشترط الإذن القضائي في هذه الحالة (المادة 56 منه)-، وهو ما أكدته المحكمة العليا في قرارها الصادر عن غرفة الجنح والمخالفات بتاريخ 1997/07/30 فصلًا في الطعن رقم: 165609 منشور بالمجلة القضائية، العدد 1997/2، الصفحة 213 (الأب قدم شكوى ضد إبنه الذي كان=

غير أنه يجوز إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات النهار أو الليل قصد التحقيق في جميع الجرائم المعاقب عليها في المواد من 339 إلى 345 من ق.ع.ج، وذلك في داخل كل فندق، أو منزل مفروش، أو فندق عائلي، أو محل لبيع المشروبات، أو ناد أو منتدى أو مرقص، أو أماكن المشاهدة العامة وملحقاتها وفي أي مكان مفتوح للعموم أو يرتاده الجمهور، إذا تحقق أن أشخاصًا يستقبلون فيه عادة لممارسة الدعارة[1]؛

ويجوز للقاضي التحقيق في مواد الجنايات أن يقوم بتفتيش مسكن المتهم في غير الساعات المحددة في المادة 78 من ق.إ.ج.ج، بشرط أن يباشر التفتيش بنفسه وأن يكون ذلك بحضور وكيل الجمهورية.[2]

ويجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، عندما يتعلق الأمر بإحدى الجرائم المذكورة في الفقرة 03 من المادة 78 من ذات القانون بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، وذلك بناءً على إذن مكتوب مسبق من وكيل الجمهورية المختص، كما يمكن لقاضي التحقيق في الجرائم المذكورة سابقًا أن يقوم بعملية التفتيش أو الحجز ليلًا أو نهارًا وفي أي مكان على إمتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك، كما يمكنه أن يأمر بأية تدابير تحفظية تلقائيًا أو بناءً على تسخير من النيابة العامة أو بناءً على طلب من ضابط الشرطة القضائية، كما يمكنه إتخاذ التدابير الأخرى المنصوص عليها في التشريع المعمول به[3].

يلاحظ أن قد أدرك المشرع الجزائري ميزة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها عندما إستثناها من حظر التفتيش ليلًا، من حيث قابلية دليلها الإلكتروني للتدمير والمحو في فترة زمنية وجيزة، نظرًا لتأجيل التفتيش في الموعد القانوني قد يعرقل سير مجريات التحقيق[4]، لذلك كلما كان إجراء التفتيش في وقت قريب بعد إرتكاب الجريمة كانت فرصة الحصول على الأدلة أكبر، لأن الحصول على الدليل في الجرائم الماسة بالمستند الإلكتروني يتطلب السرعة في إجراء التفتيش

=مخمورًا ويهدد أفراد العائلة بمسدس) بقولها أنه "ولما ثبت- في قضية الحال- أن الجنحة المتابع بها هي جنحة متلبس بها الأمر الذي أدى بمأموري الضبطية القضائية إلى تفتيش المنزل، مكان وقوع الجريمة، ليلًا وخارج الوقت القانوني، دون التمكن من الحصول على إذن مسبق، لكن برضا وخط مكتوب من الشاكي صاحب المنزل وهي الصفة التي لا ينافسه فيها إبنه المتهم. ومن ثم فإن قرار غرفة الإتهام القاضي بصحة إجراءات التفتيش في محله، مما يستوجب رفض الطعن"، وللمزيد من التفصيل، ينظر: نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 129.

[1]- المادة 2/78 من القانون رقم: 25-14 السالف الذكر.

[2]- المادة 158 من القانون رقم: 25-14 السالف الذكر.

[3]- المادة 3/78 و4 و5 من القانون رقم: 25-14 السالف الذكر.

[4]- عائشة بن قارة مصطفى، مرجع سابق، ص 112.

في أي وقت ليلًا كان أم نهارًا[1]، فإنه ومن الضروري عدم تحديد ميقات محدد للتفتيش وأن يتم ذلك ليلًا أو نهارًا على حد سواء متى كانت المصلحة تقتضي ذلك.

ومن خلال ما سبق، يتضح أن المشرع الجزائري لم يتطرق إلى تحديد مدة التفتيش في الإذن، وإنما إكتفى فقط بتحديد أوقات التفتيش والإستثناءات الواردة عليها، مما قد يؤدي إلى إمكانية بقاء المأذون بتفتيشه مهددًا في حريته وحرمة مسكنه لمدة طويلة، ولذلك فمن الأنسب تدارك هذا الأمر بتحديد المدة الزمنية لإجراء التفتيش مع جواز تمديد المدة المحددة في الإذن عند إنقضائها في حالة عدم إنتهاء المهمة المنوطة لإجرائها.

3- محضر التفتيش الإلكتروني:

عند القيام بإجراء التفتيش ينبغي وجوبيًا تحرير محضر يثبت فيه كل ما تم من إجراءات وما أسفر عنه من الأدلة، ويشترط لصحته ما تستوجبه القواعد العامة في المحاضر عمومًا، والتي تقتضي بأن يكون مكتوبًا باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره، وأن يحتوي في طياته كافة الإجراءات التي أتخذها بشأن الوقائع التي يثبتها.[2]

---

[1]- رفاه خضير جياد العارضي، مرجع سابق، ص 124.

[2]- يحرر ضابط الشرطة القضائية محضر التفتيش في عين المكان، وهو محرر له خصوصيته يحمل في مضمونه كل ما قام به من إجراءات من بداية التفتيش إلى نهايته، يتضمن محضر التفتيش ما يلي:

- الإشارة إلى المستندات القانونية التي سمحت له بالتفتيش، فإذا كان يباشر التحقيق في إطار التلبس فعليه إستظهار إذن وكيل الجمهورية أو قاضي التحقيق الذي يسمح له بدخول مساكن الأشخاص أو أي مكان خاص حسب نص المادة 75 من من القانون رقم: 25-14 السالف الذكر، بينما إذا تعلق الأمر بتفتيش مكان عام فضابط الشرطة القضائية لا يحتاج إلى الإذن ولا ينوه عنه في المحضر، في حين إذا كان يمارس صلاحيات التحقيق الإبتدائي فعليه بالإضافة إلى الإذن القضائي أن يتحصل على الإذن الصريح والمكتوب بخط يد صاحب المنزل أو من ينوب عنه في الكتابة إذا كان لا يعرفها ويختاره بنفسه، ويذكر ذلك في المحضر صراحة تطبيقًا لنص المادة 97 من نفس القانون؛

- ذكر في المحضر كل من حضر التفتيش من شهود أو من ناب عن المتهم إذا كان يتعذر عليه الحضور حسب نص المادة 76 من نفس القانون؛

- يجب أن يكون محضر التفتيش مكتوبًا؛

- تطبق عليه السرية؛

- يجب أن يحتوي محضر التفتيش على إسم ضابط الشرطة القضائية الذي قام به ومساعديه؛

- أن يكون مؤرخ بالساعة واليوم والشهر والسنة، والأسباب التي أدت إلى التفتيش؛

- أن تكون هناك مصلحة من إجراء التفتيش، فلا يلجأ ضابط الشرطة القضائية لطلب إذن التفتيش لمجرد علمه بوقوع الجريمة بل لأسباب جدية؛

- يجب ذكر كل مراحل السلبية والإيجابية، فقد نكون أمام محضر تفتيش سلبي أو محضر تفتيش إيجابي؛

- في حالة حجز أشياء أو مستندات أو أية مادة لها علاقة بالجريمة وجدت في محل التفتيش، التنويه عنها في المحضر بهذه الطريقة: "....وقد حجزنا....ووضعت في حرز مختوم، مرقم، موقع"، ويؤشر في المحضر بأن المتهم أو من ينوب عنه قد إطلعوا على المحجوزات كالآتي :

" وقد واجهناه بالشيء المحجوز وبعد عملية التفتيش أقفلنا المحضر نحن ض ش ق.....ومساعدونا.....على الساعة....": ويوقعون عليه مع إظهار المضبوطات في محضر الجرد؛

- يجب ذكر في المحضر المكان الذي يتم فيه التفتيش لأن هناك بعض الأماكن تتطلب إجراءات خاصة فلا يمكن إجراء التفتيش في الحرم الجامعي إلا بعد الحصول على إذن مدير المعهد أو الجامعة، كما يتطلب تفتيش مكاتب المحامين حضور نقيب=

ونفس الأمر بالنسبة لمحضر تفتيش المنظومة المعلوماتية، فضلًا عن الشكليات الضرورية فلا بد من إحاطة سلطات التحري والتحقيق بتقنية المعلومات، والإستعانة بالخبير التقني في مجال الخبرة التقنية الضرورية، وأثناء صياغة مسودة محضر التفتيش.[1]

4- صدور الإذن بإجراء عملية التفتيش الإلكتروني:

يجب أن يتم إجراء عملية التفتيش بناءً على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق المختص إقليميًا وأن يصدر إلى ضباط الشرطة القضائية لإجرائه، كما يجب أن تتم هذه العملية تحت الإشراف المباشر للقاضي الذي أذن به، وهو ما جسدته الفقرة 03 من المادة 48 من الدستور الجزائري سنة 2020 والتي تنص على أن: "لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

وأيضًا أن يكون هذا الإذن مبنيًا على سبب يبرر إصداره كونه أكثر خطورة على حريات الأفراد وحياتهم الخاصة، ويعد إذن التفتيش من الشروط المهمة التي يجب توافرها لصحة هذا الإجراء، وبدون هذا الإذن يبطل إجراء التفتيش، لأنه من الإجراءات المهمة التي تمس حرمة الحياة الخاصة للأفراد، ولا تجوز مباشرته إلا بعد توافر المبرر لذلك.[2]

تتمثل الشروط الواجب توافرها لصحة الإذن بالتفتيش تحت طائلة البطلان، في ما يلي:

- أن يكون الإذن مكتوبًا ومؤرخًا وموقعًا عليه ممن أصدره، ويذكر فيه إسم ووظيفة من أصدره؛

- أن يكون صريحًا وواضحًا في الدلالة على التفويض، وأن يتضمن الوظيفة وصفة المأذون له بالتفتيش؛

- تحديد نوع الجريمة، والأشياء التي ينفذ من أجل تحقيقها، أي موضوع التفتيش؛

- تحديد محل التفتيش، أي تحديد الشخص والمسكن المراد تفتيشه، تحديدًا دقيقًا.[3]

ولا يجوز لضباط الشرطة القضائية عند الإنتقال للتفتيش في مسكن أي شخص الذي يظهر أنه ساهم في الجناية أو يحوز أوراقًا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة، إلا بعد

=المحامين... إلخ، وينوه على ذلك في المحضر مع توقيعه، وللمزيد من التفصيل، ينظر: إلهام حورية ساعد، **المحاضر في المادة الجزائية**، د.ر.ط، 2023، دار بلقيس للنشر، دار البيضاء- الجزائر، ص-ص 37-38.

- يتضمن محضر التفتيش كل البيانات المتعلقة بالقائم بالتفتيش، إسم قاضي التحقيق المختص والدائرة الإدارية التابع إليها المحكمة، وإسم كاتب الضبط، وكل ما يتعلق بالواقعة الإجرامية وبأطراف القضية والمكان المراد تفتيشه، نفس البيانات الواجب توفرها في المحضر الإستدلالي مع التغيير في الترويسة وأسماء وألقاب وصفة محرر المحضر، وللمزيد من التفصيل، ينظر: نفس المرجع، ص 58.

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 113.

[2]- رفاه خضير جياد العارضي، مرجع سابق، ص-ص 123-124.

[3]- ناني لحسن، مرجع سابق، ص-ص 104- 105.

إستظهار الإذن المكتوب الصادر من وكيل الجمهورية أو قاضي التحقيق الذي أذن به، وذلك قبل الدخول إلى المنزل والشروع في التفتيش.[1]

ويلاحظ أن الأمر يختلف من حيث إصدار الإذن بالتفتيش في المنظومة المعلوماتية عن الإذن بالتفتيش في الجرائم التقليدية الأخرى، لأن قد يصدر الإذن في حق الشخص قامت قرائن قوية على إرتكابه للجريمة، وعند القيام بتنفيذ الإذن بالتفتيش فقد يستدعي الأمر إلى إمتداد حق التفتيش إلى منظومة معلوماتية أخرى، إما أن تكون تابعة للمتهم أو أن له عدة أجهزة في أماكن متفرقة كأن يكون مالكًا لجهاز في منزله وجهاز في مكان آخر أو أن يكون له شريكًا في الأجهزة، مما يستدعي الحصول على إذن آخر، ويتم ذلك من خلال تحديد نطاق هذا التفتيش وما يستتبعه بالضرورة من تتبع الشبكات المعلومات، ويخضع ذلك للسلطة التقديرية للقاضي من حيث توفر حالة الضرورة أو عدم توافرها، وهذا التوجه إتبعته البعض من الدول مثل كندا والولايات المتحدة الأمريكية، على أن يكون إذن التفتيش متضمنًا ما يلي:

- البحث عن الأدلة المحصلة من الكيان المنطقي، والتي يدخل فيها نظم التشغيل وبرامج التطبيق؛
- المعطيات المستخدمة بواسطة برنامج معلوماتي أو كيانه المنطقي؛
- السجلات التي تثبت إستخدام نظام المعالجة الآلية للمعطيات؛
- السجلات المستخدمة في عملية الولوج في المنظومة المعلوماتية لمعالجة المعطيات.[2]

ثانياً: الشروط الموضوعية للتفتيش الإلكتروني

يقصد بالشروط الموضوعية الضوابط القانونية اللازمة لإجراء تفتيش صحيح، والتي تكون غالبًا سابقة على تنفيذه، ويمكن حصرها في ثلاث شروط أساسية هي: السبب، المحل، السلطة المختصة بالقيام به، وفيما يلي سنفصل كل شرط على حده:

1- وجود سبب للتفتيش الإلكتروني:

يتحقق سبب التفتيش من خلال وقوع جريمة من الجرائم الماسة بالمستند الإلكتروني التي يتم بموجبها توجيه الإتهام إلى الشخص المراد تفتيشه، وذلك بناءً على توافر قرائن قوية ودلائل كافية تفيد تورطه بها، ومنه يتحقق سبب التفتيش بوقوع جريمة من الجرائم الماسة بالمستند الإلكتروني بالفعل سواء كانت جنحة أو جناية ، وإتهام شخص أو أشخاص معينين بإرتكاب هذه الجريمة أو المشاركة فيها، وتوافر قرائن على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره.

[1]- المادة 1/75 من القانون رقم: 25-14 السالف الذكر.

[2]- عز الدين عثماني، **إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية**، المركز الجامعي مرسلي عبدالله-تيبازة، مجلة دائرة البحوث والدراسات القانونية والسياسية، المجلد 02، العدد 04، جانفي 2018، الجزائر، ص 62.

أ- وقوع جريمة من الجرائم الماسة بالمستند الإلكتروني بالفعل سواء كانت جنحة أو جناية:

التفتيش هو إجراء من إجراءات التحري والتحقيق ولا يتخذ إلا حيال جريمة تكون قد إرتكبت بالفعل، سواء تم تكييفها بأنها جنحة أو جناية ومن ثم تستبعد المخالفات من نطاق هذا الإجراء لضآلة خطورتها[1]، ولا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة تقع في المستقبل ولو كانت هناك مؤشرات على جدية إحتمال وقوعها، ذلك أن إجراء التفتيش الذي يقع من أجل فعل لا يشكل جريمة يعتبر باطلًا، ومن ثم لا يجوز إصداره[2].

إلا أنه بمقتضى المادة 05 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر نجد أن المشرع الجزائري قد أجاز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من نفس القانون[3]، إمكانية اللجوء إلى إجراء تفتيش منظومة معلوماتية، إما للوقاية من حدوث جرائم أو في حالة توفر معلومات عن إحتمال وقوع جرائم معينة.

ب- إتهام شخص أو أشخاص معينين بإرتكاب الجريمة الماسة بالمستند الإلكتروني أو المشاركة فيها:

لا يكفي لمباشرة إجراء التفتيش مجرد وقوع جريمة من الجرائم الماسة بالمستند الإلكتروني، بل يتعين توافر في الشخص المطلوب تفتيشه دلائل كافية تؤدي إلى الإعتقاد بأنه قد ساهم في إرتكابها بوصفه فاعلًا أو شريكًا فيها، أو بحيازة أشياء تتعلق بها.

أما إذا كان الهدف من التفتيش هو لغرض الإساءة إلى الشخص المشتكى عليه أو الإنتقام منه أو غير ذلك، فإن التفتيش يكون باطلًا وغير مشروع، ونفس الأمر ينطبق على التفتيش الذي يقع على مختلف الوسائل الإلكترونية من أجل الحصول على الدليل الإلكتروني.[4]

ج- توافر قرائن تفيد في كشف الحقيقة:

ينبغي أن يتوافر في المكان أو لدى الشخص المراد تفتيشه -شخصه أو مسكنه- دلائل وأسباب كافية تدعو للإعتقاد بأنه قد ساهم في إرتكاب الجريمة الماسة بالمستند الإلكتروني سواء بوصفه فاعلًا أو شريكًا، مما يستوجب إتهامه بها.

---

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 100.

[2]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص154.

[3]- توفر معلومات كافية تنذر بإحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني، أو للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولة المتبادلة.

[4]- رفاه خضير جياد العارضي، مرجع سابق، ص 121.

ويمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعينة التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة، وكذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة الماسة بالمستند الإلكتروني إلى شخص معين سواء بوصفه فاعلًا أم شريكًا، وهذا الشرط ذاته متطلب في حال التفتيش بصدد جريمة تقليدية ذلك أنه لا يمكن تفتيش شخص أو تفتيش مسكنه ما لم تكن هناك دلائل على إرتكاب الشخص إحدى الجرائم.[1]

ومن الدلائل المستمدة من التطبيق العملي والقرائن التي تنبئ عن إرتكاب الشخص للجريمة الماسة بالمستند الإلكتروني، وترجح إمكانية نسبتها له وفق السياق العقلاني والمنطقي، أن يتم تحديد هوية الجهاز الإلكتروني (IP) الذي تم إرتكاب الجريمة بواسطته، وكان ذلك الجهاز يخص شخصًا بعينه[2]، ونجد هذا الشرط يعد متطلبًا بحد ذاته في حال التفتيش الجرائم التقليدية، لأن لا يمكن تفتيش شخصًا أو تفتيش منزله ما لم تتوفر دلائل على إرتكابه للجريمة[3]، ويمكن الإستدلال على ذلك بما نصت عليه الفقرة الأولى من المادة 75 من ق.إ.ج.ج والتي تنص على أن:" لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية، أو أنهم يحوزون أوراقًا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش".

وهكذا فالتفتيش لا يجري إلا إذا توافرت أسباب كافية على أن يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات إستعملت في الجريمة أو أشياء متحصلة منها أو أي أشياء أو مستندات إلكترونية يحتمل أن يكون لها فائدة في إستجلاء الحقيقة لدى المجرم المعلوماتي[4]، وبالتالي فإن مجرد وقوع جريمة وإتهام شخص معين بإرتكابها أو المشاركة فيها لا يكفي لحث سلطة التحقيق إلى إصدار الإذن بالتفتيش ومباشرتها[5]، لذا يجب أن تكون هذه الدلائل والأمارات كافية والشبهات مقبولة ضد شخص معين بقدر يبرر تعرض التفتيش لحريته أو لحرمة مسكنه في سبيل كشف إتصاله بالجريمة الماسة بالمستند الإلكتروني بصفة خاصة[6].

ولا يقتصر الأمر على مجرد تجميع القرائن والأدلة التي تفيد وقوع الجريمة ونسبتها إلى فاعلها، بل يجب أن تتضمن كذلك المعلومات والقرائن التي تعزز موقف المشتبه فيه وتنفي عنه إرتكابه الجريمة.[7]

---

[1]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص-ص 576-577.

[2]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 155.

[3]- بن مكي نجاة، مرجع سابق، ص 219.

[4]- نفس المرجع، ص 219.

[5]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 213.

[6]- بن مكي نجاة، مرجع سابق، ص 219.

[7]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص 212.

2- محل التفتيش الإلكتروني:

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة[1] خاصة كالمسكن، أو على الشخص ذاته أو رسائله بالنسبة للجرائم التقليدية، وأما محل التفتيش في الجرائم الماسة بالمستند الإلكتروني فهو الجهاز الإلكتروني بمكوناته المادية (Hardware) والمعنوية (Software) وشبكات الإتصال الخاصة به (Network)، وذلك يستلزم مراعاة أن يتم الإشارة إلى محل التفتيش في الإذن المقرر له.[2]

أ- نظم المعلوماتية كمحل للتفتيش الإلكتروني:

يتمثل محل تفتيش النظم المعلوماتية في كل المكونات المادية والمعنوية وشبكات الإتصال الخاصة به، والتي قد توجد في حوزة شخص، أو تكون موضوعة في مكان له حرمة السكن، بحيث يصح الإستناد إليها كدليل على إرتكاب الجريمة.[3]

وتثير مسألة محل التفتيش مشكلة خاصة بكيفية تنفيذ إذن التفتيش، والذي يشترط فيه أن يكون محددًا فيه نطاق وحدود تنفيذ الإذن بالتفتيش، ويشار إلى أن محل التفتيش الإلكتروني ينبغي أن يشمل البرامج أو الكيانات المنطقية، المعطيات المسجلة في ذاكرة الجهاز أو في مخرجاته، السجلات المثبتة لإستخدام نظام المعالجة الآلية للمعطيات، السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للمعطيات، وما يتعلق بها من سجلات كلمات السر ومفاتيح الدخول، ومفاتيح فك الشفرة.[4]

وأخذت الشرطة الكندية بذات الرأي السابق، إذا إعتمدت الشرطة التابعة لمركز المعلوماتية الكندي نموذجًا للإذن بالتفتيش، يتضمن التصريح بالبحث عن ضبط البرنامج أو كيان المنطقي، والتي يدخل فيها برنامج التطبيق، ونظم التشغيل وما يتفرغ عنها من نظم، والمعطيات المستخدمة بواسطة برنامج معلوماتي، وأيضًا السجلات التي تثبت إستخدام الأنظمة الآلية المعالجة للمعطيات، والسجلات المستخدمة في عملية الولوج في المنظومة المعلوماتية لمعالجة المعطيات.[5]

ب- الشخص كمحل للتفتيش الإلكتروني:

الجهاز الإلكتروني بمكوناته وشبكات إتصاله يستلزم مجموعة من الأشخاص أصحاب الخبرة والتخصص في تقنية ومعلومات هذا الجهاز، فالشخص بوصفه محلًا لتفتيش المنظومة

[1]- عائشة بن قارة مصطفى، مرجع سابق، ص 103.
[2]- رفاه خضير جياد العارضي، مرجع سابق، ص 122.
[3]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص580.
[4]- علي عدنان الفيل، مرجع سابق، ص40.
[5]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 272.

المعلوماتية قد يكون من مشغلو النظم المعلوماتية، وخبراء البرمجة سواء كانو مخططي برامج تطبيقات، أم كانوا مخططي برامج نظم، وقد يكون من المحللين، أو من مهندسي الصيانة والإتصالات، أو من مديري النظم المعلوماتية، أو من أي آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة الحاسب المحمولة أو تلفونات متصلة بجهاز المودم أو مستندات.[1]

ج- المسكن وما في حكمه كمحل للتفتيش الإلكتروني:

حكم تفتيش المكونات المادية والمعنوية يتوقف على طبيعة المكان الموجودة فيه، فإذا كانت موجودة في مكان خاص لها حكم تفتيش المسكن ولا يجوز تفتيشها إلا وفقًا للضمانات المقررة في المادة 75 وما بعدها من ق.إ.ج.ج، أما تفتيش مكونات المادية والمعنوية للأجهزة الإلكترونية الموجودة في مكان عام فإن أغلب الشريعات المقارنة تجيز الدخول إلى المحال العامة المفتوحة للجمهور بكل سهولة دون الحاجة لإذن بالتفتيش.[2]

ويقصد بالمسكن وما في حكمه كمحل للتفتيش هو المكان الذي يأوي إليه الإنسان ويتخذه مقرًا له والمتمثل في المستودع الذي يحتفظ فيه الشخص بالأشياء المادية محل البحث، ولقد عرفته المادة 355 من ق.ع.ج كما يلي: "يعد منزلًا مسكونًا كل مبنى أو دار أو غرفة أو خيمة أو كشك، ولو متنقل متى كان معدًا للسكن وإن لم يكن مسكونًا وقتذاك، وكافة توابعه مثل الأحواش وحظائر الدواجن ومخازن الغلال والإسطبلات والمباني التي توجد بداخلها، مهما كان إستعمالها حتى ولو كانت محاطة بسياج خاص داخل السياج أو السور العمومي".

يعني كل مكان للإقامة بالمفهوم الواسع سواء كان الموطن العادي أو أي مكان آخر للإقامة كغرفة في فندق أو حجرة في مكتب، مهما كان السند المعتمد عليه كالملكية أو الإيجار أو الإحتلال المادي دون سند، فإذا لم تتوفر صفة مكان الإقامة (كمداخل السيارة، أو ورشة عمل، أو زاوية في الشارع، أو في الساحة العمومية) فإن الضمانات المنصوص عليها لا تقوم.[3]

3- السلطة المختصة بإجراء عملية التفتيش الإلكتروني:

نظرًا لخطورة إجراء التفتيش على الحرية الشخصية وإنتهاك حرمة الحياة الخاصة للأفراد، فقد تم إسنادها لسلطة قضائية المخول لها قانونًا صلاحيات إجرائه، تكفل تلك الحريات والحقوق من الهدر.

خول المشرع الجزائري بموجب المادة 75 من ق.إ.ج.ج سلطة إصدار الأمر بإجراء التفتيش لوكيل الجمهورية أو لقاضي التحقيق، وأن ينجز تحت إشراف المباشر للقاضي الذي أذن به، والذي يمكنه عند الإقتضاء أن ينتقل إلى عين المكان للسهر على إحترام أحكام القانون،

[1]- خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، مرجع سابق، ص-ص 214-215.
[2]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 155.
[3]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص-ص 128-129.

ولقد أشارت نفس المادة على أن الإذن بالتفتيش تفويض تصدره سلطة قضائية إلى أحد ضباط الشرطة القضائية للقيام بالتفتيش، يستشف ذلك من خلال عبارة: "لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص... لإجراء تفتيش إلا بإذن مكتوب...".

وفي هذه الحالة يجب أن يحدد في إذن الندب بالتفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها، والهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الإستكشافي، بحيث لا يترك شيء للسلطة التقديرية لرجل الشرطة الذي سيقوم بتنفيذ الأمر.[1]

المطلب الثالث: ضبط الدليل الإلكتروني المستخلص من الجرائم الماسة بالمستند الإلكتروني

إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه فهو بذلك غاية التفتيش القريبة والأثر المباشر الذي يسفر عنه هذا الإجراء[2]، لذلك فإنه يقصد بالضبط بمعناه التقليدي هو: "وضع اليد على الأوراق أو الأسلحة أو الأدوات المتعلقة بالجريمة، التي تفيد في كشف الحقيقة"، والضبط لا يرد إلا على الأشياء فليس محله الأشخاص، أما الضبط في المجال المعلوماتي فهو: "وضع اليد على الدعائم المادية والمعنوية التي تحتوي على المعطيات المعلوماتية التي تتصل بالجريمة الواقعة على المستند الإلكتروني، وتفيد في كشف الحقيقة عنها وعن مرتكبها"[3].

وعلى ذلك فإن الضبط كإجراء من إجراءات التحقيق هو وضع اليد على الشيء وحبسه والمحافظة عليه لمصلحة التحقيق، والضبط الذي يقصده هنا هو الضبط القضائي أي الذي يهدف إلى الحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة.[4]

وبالتالي الغاية من التفتيش هو ضبط أي شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها، سواء أكان هذا الشيء أدوات استعملت في إرتكاب الجريمة أو شيئًا نتج عنها وكل ما يفيد في كشف الحقيقة[5]، وعلى ذلك فإن ضبط الأشياء المتعلقة بالجريمة هو الأثر المباشر للتفتيش[6].

لكن ليس معنى ذلك أن الضبط لا يقع إلا نتيجة للتفتيش إذ من الممكن أن يكون الضبط نتيجة لمعاينة، كما أنه يجوز أن تضبط أشياء قدمها الشهود أو المتهمون بإختيارهم، كذلك يجوز أن يطلب من أحد الأفراد بتقديم شيء موجود في حيازته إليه ويلزمه بذلك.[7]

---

[1]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 584.

[2]- سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، مرجع سابق، ص 797.

[3]- رفاه خضير جياد العارضي، مرجع سابق، ص-ص 157-158.

[4]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 636.

[5]- ناني لحسن، مرجع سابق، ص 119.

[6]- طارق إبراهيم الدسوقى عطية، مرجع سابق، ص 441.

[7]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 636.

الفرع الأول: مدى صلاحية ضبط مكونات الأجهزة الإلكترونية كدليل في الجرائم الماسة بالمستند الإلكتروني

قد يتساءل المرء عن الأشياء التي يمكن أن تضبط أو تحرز في الجريمة الواقعة على المستند الإلكتروني، خاصة وأن أكثر الأدلة التي قد نتحصل عليها هي عبارة عن نبضات كهربائية، فإذا كان التفتيش ينتهي بتحديد موضع ومكان المعطيات كانت موضوع التفتيش، فإن المعالجة التي تجرى عليها لجعلها مرئية للإطلاع عليها وإثباتها أو إستخراجها من الأجهزة الإلكترونية في صورة مستندات مطبوعة لا تعد تفتيشًا عن أدلة الجريمة ولكنها تمثل وصلًا إلى هذه الأدلة ومن ثم ضبطًا لها، فتلك الكيانات المعنوية تكون بذلك قد تحولت إلى أشياء مرئية مقروءة تكتسب كيانًا ماديًا يمكن بواسطته ضبطها ونقلها من مكان لآخر، فالضبط ينصب على الأشياء المادية وغير المادية والتوغل داخل المنظومة المعلوماتية والعثور على المعطيات المخزنة في المنظومة أو النظم المرتبطة بالمنظومة محل الإشتباه، هدفه ضبط ما يعد ذو فائدة من معطيات ليكون دليل يتحدد بها الركن المادي للجريمة.[1]

ومنه سنتطرق في هذا الفرع إلى ضبط المكونات المادية للجهاز الإلكتروني، ثم إلى ضبط المكونات المعنوية للجهاز الإلكتروني.

أولًا: ضبط المكونات المادية للجهاز الإلكتروني

لا يوجد خلاف حول ضبط المكونات المادية للأجهزة الإلكترونية ومواجهتها إجرائيًا بالنصوص التقليدية كغيرها من الأشياء المادية التي تساعد في إظهار الحقيقة[2]، وعلى هذا الأساس فإن ضبط المكونات المادية للأجهزة الإلكترونية لا يثير مشاكل في الفقه المقارن، ولا يوجد خلاف بين فقهاء القانون في إمكانية ضبط هذه المكونات بل حتى إمكانية ضبطها بشكل كامل لتأكيد الإحتفاظ بالدليل إذا كان مشغل الجهاز غير متعاون مع جهات التحري والتحقيق[3].

وسنعرض المكونات المادية للحاسوب على سبيل المثال[4]، والتي يمكن تقسيمها إلى:

1- وحدات الإدخال:

وحدات الإدخال (Input Units) هي مجموعة من الوحدات المسؤولة عن إدخال الأوامر أو المعطيات إلى الحاسوب وإيصالها إلى وحدة الذاكرة للتخزين، وبمعنى آخر لا يمكن للمجرم المعلوماتي إرتكاب جريمته عن طريق الحاسوب إلا بإستعمال هذه الأدوات، والتي يمكنه بمقتضاها تغذية الحاسوب بالبيان أو المعلومة التي يريد تزويدها أو تخزينها أو يعدل في تلك

---

[1]- شنتير خضرة، مرجع سابق، ص-ص 116-117.

[2]- حبيباتني بثينة، مرجع سابق، ص 332.

[3]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 159.

[4]- مصادر الدليل الإلكتروني عديدة لا تقل أهمية عن الحاسوب وملحقاته، والتي يمكن أن يعتمد عليها لإرتكاب هذا النوع من الجرائم وتكون مصدرًا للدليل الإلكتروني، وذلك لسهولة نقلها وإستخدامها في أي مكان وأكثر فعالية، كالهواتف الذكية النقالة والتبلات وآلات التصوير الرقمي، وغيرها من الوسائل الإلكترونية الحديثة التي باتت تعتمد التقنية الرقمية في تشغيلها.

المعلومات والمعطيات المحفوظة على الجهاز أو المسجلة لدى شبكة المعلومات الدولية، وهذه الوحدات هي[1]:

لوحة المفاتيح (Key Board)، وشاشات اللمس (Touch screen)، الإدخال المرئي (Machine vision)، الإدخال الصوتي (Voice Input)، الفأرة (Mouse)، القلم الضوئي (Light pen)، القراءة الضوئية للحروف (Recognition Optical Character) ، نظام قراءة الحروف المغناطيسية (Magnetic ink characher readr system)، الماسح الضوئي (Scanner)، مشغل الأسطوانات (CD-ROOM)، مشغل الأقراص الممغنطة (Floppy disk-drive FDD)، جهاز التعرف على الأصوات (The System Of Recogntion On The-Sounds)[2].

2- وحدات الإخراج:

وحدة الإخراج (Out Put Unit) هي الوحدة التي يمكن من خلالها تحويل المعلومات غير المقروءة وغير المرئية إلى معلومات مقروءة أو مرئية أو الإثنين معًا، فهي وسائل إستخراج نتائج الإتصال بين الأفراد ونظام الحاسوب، حيث تقوم هذه الوحدة بإستقبال النتائج من وحدة التخزين الذاكرة، وإخراجها على أوساط الإخراج المختلفة، وذلك لإستخدامها بواسطة المستفيدين من المنظومة ووسائلها في ذلك، بالإضافة إلى ماهو معلوم من وسائل يتم من خلالها قراءة المعلومات عن طريق وحدات العرض المرئي أي عن طريق الشاشات بأنواعها الثلاثة الشاشة العارضة الأحادية بلونين فقط، وشاشة التلفزيون، وأيضًا هناك وسائل آخرى إلى جانب ذلك يتم بها تحويل البرامج والمعلومات إلى مستندات ورقية مقروءة كالطابعات على مختلف أنواعها العادية منها أو الليزرية، وأيضًا وحدات رسم المنحنيات البيانية، والوحدات الطرفية.[3]

3-وحدة المعالجة المركزية :

وحدة المعالجة المركزية ((Central Processin Unit (CPU) تقوم هذه الوحدة بتلقي الأوامر عن طريق وحدات الإدخال وتقوم بمعالجتها وبإخراجها بالكيفية التي يرغب بها مشغل الجهاز[4]، فهي التي تقوم بالإشراف على كل العمليات الحسابية والتحكم ومعالجة المعطيات وتخزينها، وكذلك التنسيق بين مكونات الجهاز المادية مع بعضها البعض من جهة وبينها وبين البرمجيات من جهة أخرى، وتقسم إلى وحدة التحكم ووحدة الحساب والمنطق والذاكرة[5].

---

[1]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 18.

[2]- طارق إبراهيم الدسوقى عطية، مرجع سابق، ص449.

[3]- محمد حماد مرهج الهيتي، **جرائم الحاسوب ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها**، الطبعة الأولى، 2006، دار المناهج للنشر والتوزيع، عمان-الأردن، ص 42.

[4]- حنان ريحان مبارك المضحكي، مرجع سابق، ص 65.

[5]- فؤاد حسين العزيزي، مرجع سابق، ص 23.

أ- وحدة الحساب والمنطق:

وحدة الحساب والمنطق ((Arithmetic and Logical Unit (ALU) هي جزء من وحدة المعالجة المركزية (CPU) والمسؤولة عن معالجة المعطيات حسابيًا ومنطقيًا، وتتكون من مجموعة من الدوائر المنطقية التي يتم توظيفها لأداء العمليات ومجموعة من المسجلات، وهي ذاكرة سريعة تستخدمها هذه الوحدة لإستيعاب المعطيات التي يجرى معالجتها.[1]

ومن أهم وظائف وحدة الحساب والمنطق إنجاز العمليات الحسابية (Arithmetic-operation) بواسطة دوائر حسابية مثل الجمع والطرح والضرب والقسمة، وتنفيذ تلك العلميات وفق ترتيب محدد مسبقًا وتحت إشراف وحدة التحكم، وأيضًا إنجاز العمليات المنطقية (operations- Logical) وذلك عن طريق مقارنة القيمة الرقمية وفقًا لتعليمات.[2]

ب- وحدة التحكم:

وحدة التحكم ((Control Unit (CU تقوم هذه الوحدة بوظيفة التحكم والرقابة الآلية والتنظيم والتنسيق بين وظائف الوحدات المختلفة في الحاسوب، وإلى جانب ذلك تقوم بتفسير العمليات الموجودة في البرنامج وتنفيذها، ومن ثم توجيه وتحديد العمليات اللازمة لجميع وحدات الحاسوب، فلذلك هي تهيمن على كافة العمليات التي تجري داخل وحدة التشغيل المركزية، كما تراقب كافة الإجراءات التي تتم داخل الحاسوب، وكذلك تنظم العلاقة بين وسائل الإدخال ووسائل الإخراج.[3]

ج- وحدة الذاكرة:

وحدة الذاكرة (Memory Unit) هي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز، أو تخزين النتائج الآتية من وحدة المعالجة المركزية، وهناك نوعان من وحدات الذاكرة هما:

- وحدة الذاكرة الرئيسية (Main Memory)؛
- وحدة الذاكرة المساعدة (Auxiliary Memory).[4]

4-وحدة الذاكرة الرئيسية:

وحدة الذاكرة الرئيسية (Main Memory) دورها الجوهري يتمثل في حفظ المعطيات المعلوماتية المطلوب الإحتفاظ بها، وتحويلها إلى معلومات وتحليلها وإستخراجها بصور مختلفة، إذ من دونها لا يمكن تحليل المعطيات، فهي بمثابة مسرح العمليات في الحاسوب حيث تحتفظ بداخلها بالمعطيات من أرقام وصور وأصوات وخلافه، ويقوم المعالج بتخزين المعطيات

[1]- أحمد خليفة الملط، مرجع سابق، ص 35.
[2]- طارق إبراهيم الدسوقى عطية، مرجع سابق، ص 94.
[3]- محمد حماد مرهج الهيتي، مرجع سابق، ص 41.
[4]- علي جعفر، مرجع سابق، ص 42.

في الذاكرة، ليتم بعد ذلك معالجتها من قبل المعالج بواسطة تطبيقات أو برامج معدة مسبقًا، وهي كناية عن خطوات منطقية متتالية، ويمكن تشبيه لوحة الذاكرة برفوف متلاصقة أو حقائب متراصة لكل منها عنوان محدد، يتم تخزين المعطيات فيها مع حفظ مكان أو عنوان أو رمز التخزين، وذلك لكي يتمكن المعالج من العودة إليها من خلال الرمز الخاص بكل منها وتنقسم الذاكرة الرئيسية بدورها إلى قسمين[1]:

أ- ذاكرة المؤقتة:

ذاكرة المؤقتة ((Random Access Memory (RAM) وتسمى كذلك ذاكرة القراءة والكتابة وتستخدم لتخزين البرامج والمعطيات التي تقع تحت المعالجة، أي أن محتويات هذه الذاكرة قابلة للتعديل والحذف والإضافة والتغيير، كما أنها تفقد محتوياتها بإنقطاع التيار الكهربائي[2]، وهذه الذاكرة تخزن فيها المعطيات بصورة مؤقتة إستعدادًا لمعالجتها أو لتخزينها في وسائط التخزين الدائمة[3].

ب- ذاكرة القراءة فقط:

ذاكرة القراءة فقط ((Read Only Memory (ROM تتيح هذه الذاكرة للمستخدم إمكانية قراءة المعلومات المخزنة فيها فقط، كما لا يمكن الكتابة عليها أو تعديل محتواها، وتتسم بأن التخزين فيها يتصف بالدوام، كما تحتفظ بمحتواها ولو إنقطع التيار الكهربائي عنها، لهذه الأسباب تعتمد هذه الذاكرة في تخزين البرامج المشغلة للحاسوب، والتي يحتاج إليها بصورة دائمة من ذلك برامج الإقلاع والمترجمات.[4]

5-وحدات التخزين:

تعد وحدات التخزين من أهم أجزاء الحاسوب، لأنها تحتوي على المعلومات والبرامج التي يستخدمها المستخدم في عمله، ومن خلال أجزائها يمكن لمستخدم الجهاز تخزين الملفات التي يقوم بعملها وذلك على برامج التشغيل المختلفة، ويعد هذا الجزء هامًا لإرتكاب الجريمة الماسة بالمستند الإلكتروني، إذ بإقتحام الملفات المخزنة يمكنه الحصول على ما يريد من معطيات أو معلومات التي يتضمنها المستند الإلكتروني، أو تخريب هذه المعلومات أو تدميرها أو تزييفها وتزويرها.[5]

---

[1]- عادل مشموشي، مرجع سابق، ص 37.

[2]-علي جبار الحسيناوي، **جرائم الحاسوب والإنترنت**، د.ر.ط، 2009، دار اليازوري العلمية للنشر والتوزيع، عمان- الأردن، ص 24.

[3]- علي جعفر، مرجع سابق، ص 42.

[4]- عادل مشموشي، مرجع سابق، ص 38.

[5]-عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 21.

قد تكون كمية المعلومات المراد تخزينها كبيرة بدرجة لا يمكن خزنها في وحدة التخزين الرئيسية أي الذاكرة الرئيسية، لذا فإن الأمر يتطلب وحدات تخزين ثانوية أو إضافية، بقصد التوسع في طاقة وحدة التخزين الداخلية، وتنقسم وحدات التخزين إلى نوعين[1]:

أ- وحدات التخزين المباشرة:

بمعنى أن أي بيان مسجل على هذه الوسائط يمكن الوصول إليه مباشرة دون الحاجة إلى قراءة المعطيات المسجلة عليه من البداية حتى البيان المطلوب، ويتمثل هذا النوع في الأقراص المغناطيسية.[2]

ومن أهم خصائصها إمكانية القراءة أو التسجيل على أي قطاع بها، وتغيير أو تعديل أي ملف مسجل عليها دون الحاجة إلى إنشاء ملف جديد، إذ يمكن تعديل السجل في موضعه.[3]

ب-وحدات التخزين التتابعية:

من أجل الوصول إلى أي بيان مسجل على هذه الوسائط يجب قراءة الشريط من بدايته إلى المكان الذي يوجد عليه البيان المطلوب، ويتمثل هذا النوع في الأشرطة المغناطيسية.[4]

5-أجهزة الإتصال:

أجهزة الإتصال تنقسم إلى:

أ- المودم:

المودم (Modem) جهاز الذي يمكن أجهزة الحاسوب أو الأجهزة الإلكترونية من الإتصال ببعضها البعض عبر خطوط الهاتف، وقد تستخدم في إستقبال وإرسال الفاكس والمكالمات الهاتفية.[5]

ب- الكروت أو البطاقات:

الكروت أو البطاقات (PCMCIA Cards) وهذه البطاقات تستعمل في أجهزة الحاسوب الصغيرة، وهي تشبه البطاقات الإئتمانية، ومن أنواعها: النوت بوك (Notebook)، واللاب توب (Laptop).[6]

---

[1]- طارق إبراهيم الدسوقى عطية، مرجع سابق، ص 96.

[2]- نفس المرجع، ص 96.

[3]- أحمد خليفة الملط، مرجع سابق، ص 39.

[4]- طارق إبراهيم الدسوقى عطية، مرجع سابق، ص 96.

[5]- حنان ريحان مبارك المضحكي، مرجع سابق، ص 68.

[6]- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، مرجع سابق، ص 22.

ثانيًا: ضبط المكونات المعنوية للجهاز الإلكتروني

إن الهدف الأساسي لعملية التفتيش هو وضع اليد على الأدلة المادية التي تساعد على كشف الحقيقة، لكن من البديهي القول بأن ضبط الأشياء المادية كالمعدات والأوراق والمستندات يعد شيئًا سهلًا وغير مثير لأية إشكالات في نظر القانون، غير أنه ليس من السهل أبدًا توقيع الضبط على المكونات المعنوية[1]، مما يثير التساؤل حول مدى إمكانية خضوع المكونات المعنوية للجهاز الإلكتروني لعملية الضبط؟

إنقسم الفقه إلى إتجاهين عند الإجابة على هذا التساؤل:

1- الإتجاه الأول:

يرى هذا الإتجاه بأنه لا يتصور أن يرد الضبط إلا على المكونات المادية، أما المكونات المعنوية من برامج ومعطيات ينتفي فيها الكيان المادي وبالتالي لا تصلح أن تكون محلًا للضبط[2]، وبالتالي عدم صلاحية المعطيات المخزنة آليًا لأن تكون محلًا للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية، لإنتفاء الطابع المادي عن هذه المعطيات في حال تجردها على الدعامة المادية.[3]

ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة مادية أو غيرها من الوسائل المادية، ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة.[4]

2- الإتجاه الثاني:

على النقيض من الرأي السابق، يرى جانب آخر إلى أن إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في الكشف عن الجريمة، فإن هذا المفهوم يمتد ليشمل المعطيات المعلوماتية أو قاعدة بيانات بكافة مشتملاتها[5]، فالمعطيات المعالجة إلكترونيًا ما هي إلا ذبذبات إلكترونية أو موجات كهرومغناطيسية تقبل التسجيل والحفظ والتخزين على وسائط مادية وبالإمكان نقلها وبثها وإستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره[6]، وإن كانت المكونات المعنوية غير ملموسة إلا أنها ببعض المعالجات الداخلية في الجهاز يمكن أن تصبح مادية يرد عليها الضبط، مثل المعطيات التي بواسطة الطابعة مثلًا تصبح سهل إخراجها على أوراق أو أقراص الليزر، وبالتالي يمكن أن تكون محلًا للضبط[7].

---

[1]- زيبحة زيدان، مرجع سابق، ص 148.

[2]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 640.

[3]- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مرجع سابق، ص 159.

[4]- خالد عياد الحلبي، مرجع سابق، ص 171.

[5]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 640.

[6]- خالد عياد الحلبي، مرجع سابق، ص 171.

[7]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 640.

وإستند هذا الإتجاه إلى المادة 7/29 من قانون الإثبات الكندي التي تقرر أن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية يقتصر على تفتيش المكان، بغرض تفقده وأخذ نسخة من المواد المكتوبة يستوي في ذلك أن تكون السجلات مكتوبة أم في شكل إلكتروني.[1]

ولقد حسمت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 صراحة بصلاحية المكونات المعنوية والوسائل الإلكترونية لأن تكون محلًا للضبط، وذلك من خلال الفقرة 03 من المادة 19 منها التي نصت على أن: "يجب على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تخويل سلطاته المختصة سلطة ضبط أو الحصول بطريقة مشابهة على المعطيات المعلوماتية وفقًا للفقرتين 01 و02...".[2]

وتدخلت عدة دول لتعديل قوانينها لسد الفراغ التشريعي المتعلق بالضبط الأدلة الإلكترونية وقواعد تحريزها، في مقدمتها المشرع البلجيكي الذي قام بمقتضى قانون 28 نوفمبر 2000 بتعديل قانون التحقيق الجزائي بإضافة المادة 39 bis التي سمحت بضبط الأدلة الإلكترونية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للمعطيات بقصد عرضها على السلطات القضائية.[3]

والمشرع الفرنسي الذي قام بإدخال تعديل على قانون الإجراءات الجزائية الفرنسي لسد هذا الفراغ التشريعي، وذلك بموجب قانون الأمن الداخلي رقم: 239 لسنة 2003 حيث إستحدث الفقرة 04 من المادة 57-1 التي نص فيها على أن: "يجوز نسخ المعطيات التي تم السماح بالوصول إليها من جراء تفتيش النظام المعلوماتي في ظل الشروط المنصوص عليها في هذه المادة، ودعامات التخزين هذه يتعين تحريزها وفقًا للشروط المنصوص عليها في هذا القانون".[4]

وتدخل المشرع الجزائري بدوره لمواجهة القصور الموجود في قانون الإجراءات الجزائية فيما يخص ضبط المكونات المعنوية للجهاز الإلكتروني بموجب القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر تحت عنوان "حجز المعطيات المعلوماتية".

---

[1]- حبيباتني بثينة، مرجع سابق، ص 334.

[2]-Art 19 paragraphe 03 du convention sur la cybercriminalité dispose que : « Chaque Partie adople les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accés a été réalisé en application des paragraphes 1 ou 2...».

[3]- بن طالب ليندا، مرجع سابق، ص 66.

[4]-Art 57-1 paragraphe 04 du C.P.P.F (créé par loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure, art 17) dispose que: « les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent êtres copiées sur tout supports. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code».

الفرع الثاني: إجراءات ضبط الدليل الإلكتروني

يعد الضبط الأثر المباشر للتفتيش، فهو وضع اليد على الدعائم المادية المخزنة فيها المعطيات المعلوماتية التي تم بموجبها إرتكاب الجريمة، والتي من شأنها تسهيل إثبات واقعة معينة، وقد تأخذ هذه المضبوطات الصورة المادية في الحالة التي يتعلق الأمر فيها بضبط المكونات المادية للجهاز الإلكتروني وملحقاته، كما قد تأخذ الصورة المعنوية والمتمثلة في المكونات المعنوية (المنطقية).

نصت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في الفقرة 03 من المادة 19 منها على أن: "يجب على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تخويل سلطاته المختصة سلطة ضبط، أو الحصول بطريقة مشابهة على المعطيات المعلوماتية وفقًا للفقرتين 01 و02، وهذه الإجراءات تشمل السلطات التالية:

أ- ضبط أو الوصول بطريقة مشابهة إلى نظام معلوماتي أو جزء منه، أو إلى دعامة تخزين معلوماتية؛

ب- التحقق والتحفظ على نسخة من هذه المعطيات المعلوماتية؛

ج- المحافظة على سلامة المعطيات المخزنة؛

د- منع الوصول إلى هذه المعطيات أو رفعها من النظام المعلوماتي".[1]

صلاحيات الضبط أو الحصول بوسيلة مشابهة على المعطيات المعلوماتية التي كونت موضوع التفتيش أو الولوج بطريقة مشابهة، فقد ناقشتها الفقرة 03 من المادة 19 ونصت على أن يشمل نطاق الضبط الأجزاء المادية للجهاز الإلكتروني ودعامات التخزين المعلوماتية، خاصة في الحالات التي لا يمكن فيها الحصول على نسخة من المعطيات أو المعلومات، وكذلك ضبط البرامج الضرورية من أجل الولوج إلى المعطيات وضبطها، وبالإضافة إلى إستخدام المصطلح التقليدي الضبط فقد تم إستخدام مصطلح الحصول بطريقة مشابهة مماثلة وذلك من أجل الأخذ في الإعتبار طرقًا أخرى، كرفع المعطيات غير المادية أي جعلها غير قابلة للوصول إليها إما عن طريق ترميزها (Leur Codage) أو تقييدها (Le blocage) عن طريق أية وسيلة

[1]-Art 19 paragraphe 03 du convention sur la cybercriminalité dispose que : « Chaque Partie adople les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accés a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les préogatives suivantes:

a. saisir ou obtenir d'une façon similaire un systéme informatique ou une partie de celui-ci ou un support de stockage informatique;

b. réaliser et conserver une copie de ces données informatiques;

c. préserver i'intégrité des données informatiques stockées pertinentes;

d. rendre inaccessibles ou enlever ces données informatiques du systéme informatique consulté».

إلكترونية أخرى تمنع الدخول إلى هذه المعطيات، لكن ذلك لا يعني تدميرها فالضبط ليس معناه المحو النهائي للمعطيات المضبوطة بل تستمر في الوجود مع حرمان المشتبه فيه من الولوج إليها.[1]

وعليه يمكن تقسيم الإجراءات التي نصت عليها المادة 3/19 إلى نوعين:

- إجراءات تحفظية: تهدف إلى الحفاظ على المعطيات المخزنة التي ترى الجهة المختصة أهميتها في التحقيق ببقائها في أمكنتها في النظام المعلوماتي للجهاز أو في دعامة التخزين، ومنع الوصول إليها أو إلغاؤها أو التصرف فيها؛
- إجراءات الضبط: وهي إجراءات لاحقة للتفتيش والدخول، ويقصد بها جمع المعطيات سواء بأخذ دعامة تخزين المعلومات ذاتها، أو بعمل نسخة من المعطيات المخزنة بها أو بالنظام المعلوماتي للجهاز في ورق أو شرائط الفيديو الرقمية.[2]

ولقد أخذت الإتفاقية العربية لجرائم تقنية المعلومات بنفس المعنى بموجب الفقرة الأولى من المادة 27 منها للدول الأعضاء بتمكين سلطاتها المختصة من ضبط وتأمين تقنية المعلومات التي يتم الوصول إليها عن طريق تفتيش المعلومات المخزنة، هذه الإجراءات تشمل صلاحيات:

أ- ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات؛

ب- عمل نسخة من معلومات تقنية المعلومات والإحتفاظ بها؛

ج- الحفاظ على سلامة معلومات تقنية المعلومات المخزنة؛

د- إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

وسار المشرع الجزائري على نفس النهج بموجب الفقرة الأولى من المادة 06 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر التي تنص على أن: "عندما تكتشف السلطات التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقًا للقواعد المقررة في قانون الإجراءات الجزائية"، وفيما يخص الحجز عن طريق منع الوصول إلى المعطيات فقد نصت المادة 07 من نفس القانون على أن: "إذا إستحال إجراء الحجز وفقًا لما هو منصوص عليه في المادة 06 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة".

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص- ص 300-301.

[2]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 285.

وإستنادًا للمادتين 06 و07 من ذات القانون، نجد أن المشرع الجزائري قد خول طريقتين لضبط المعطيات المعلوماتية التي كانت موضوع التفتيش:

الطريقة الأولى: عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة وتكون مفيدة في الكشف عن الجرائم الماسة بالمستند الإلكتروني أو مرتكبيها، ففي هذه الحالة يمكن أن تحجز المنظومة برمتها، كما يمكن أن يحجز جزء منها عن طريق نسخ المعطيات[1] محل البحث على دعامة تخزين إلكترونية، تكون هذه الأخيرة قابلة للحجز ووضعها في أحراز وفقًا لما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية[2].

وبالتالي تتحقق الأولى عن طريق نسخ وتحميل المعطيات محل البحث على دعامة تخزين مادية، وتكون هذه الأخيرة قابلة للضبط والوضع في أحراز مختومة حسب ما هو مقرر في قواعد تحريز الدليل التقليدية المنصوص عليها في قوانين الإجراءات الجزائية، وهي الطريقة المقصودة في المادة أعلاه بمصطلح -الضبط saisir-.[3]

كما ترك المجال مفتوحًا أمام ظهور تقنيات تخزين جديدة بناء على التطورات التقنية المذهلة في مجال صناعة الأجهزة الإلكترونية وملحقاتها، إذ أنه لا يمكن التعامل مع تلك المعطيات في شكلها الأولي المعنوي وهي عبارة عن نبضات أو ذبذبات إلكترونية أو إشارة ممغنطة إلا بعد نسخها على هذه الدعامات.[4]

الطريقة الثانية: إذا إستحال إجراء الحجز وفقًا للطريقة الأولى ولما هو مقرر في المادة 06 من نفس القانون لأسباب تقنية، يتعين على السلطة المختصة بالتفتيش والحجز أن تستعمل التقنيات

---

[1]- إن المعطيات تتوافر في شكل غير مادي أو غير ملموس مثل الشكل الكهرومغناطيسي يمكن قراءتها بإستخدام جهاز الإلكتروني، لكن لا يمكن ضبطها وأخذها بنفس طريقة ضبط وأخذ مستند ورقي، يجب أن يتم ضبطها وأخذها أو عمل نسخة من هذه المعطيات تأخذ شكلًا ماديًا كأن تكون نسخة ورقية أو شكلًا غير مادي على دعامة مادية مثال ذلك قرص مغناطيسي، وذلك قبل ضبط وأخذ الدعامة المادية المحتوية على هذه النسخة، في هاتين الحالتين الأخيرتين اللتين تم فيهما عمل نسخة من المعطيات، فإن المعطيات الأصلية تظل باقية في المنظومة المعلوماتية أو في أداة التخزين، وللمزيد من التفصيل، ينظر: هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 231-232.

[2]- تغلق الأشياء أو المستندات المحجوزة ويتم الختم عليها إذا أمكن ذلك، وإذا تعذرت الكتابة عليها فإنها توضع في وعاء أو كيس يضع عليه ضابط الشرطة القضائية شريطًا من الورق ويختم عليه بختمه، ويحرر محضر جرد الأشياء والمستندات المحجوزة التي وجدها في مكان التفتيش وفقًا للمادة 4/76و5 من ق.إ.ج.ج، وأثناء إجراء التحقيق يجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة، ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبًا بمحاميه أو بعد إستدعائهما قانونًا، كما يستدعي أيضًا كل من ضبطت لديه هذه الأشياء لحضور هذا الإجراء، ولا يجوز لقاضي التحقيق أن يضبط غير الأشياء والوثائق النافعة في إظهار الحقيقة أو التي قد يضر إفشاؤها بسير التحقيق، ويجوز لمن يعنيهم الأمر الحصول على نفقتهم وفي أقصر وقت على نسخة أو صورة فوتوغرافية لهذه الوثائق التي بقيت مضبوطة إذا لم تحل دون ذلك مقتضيات التحقيق، وإذا إشتمل الضبط على نقود أو سبائك أو أوراق تجارية أو أوراق ذات قيمة مالية ولم يكن من الضرورة لإظهار الحقيقة أو المحافظة على حقوق أطراف الدعوى الإحتفاظ بها عينًا فإنه يسوغ لقاضي التحقيق أن يصرح لأمين الضبط بإيداعها بالخزينة العمومية طبقًا المادة 2/160و3و4 من ق.إ.ج.ج.

[3]- براهيمي جمال، مرجع سابق، ص 48.

[4]- يزيد بوحليط، **تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري**، جامعة باجي مختار-عنابة، التواصل في الإقتصاد والإدارة والقانون، المجلد 22، العدد04، ديسمبر2016، الجزائر، ص- ص 90-91.

المناسبة من أجل منع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو القيام بنسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة، هو ما نصت عليه المادة 07 من ذات القانون.

والتي تكون بإستعمال تقنيات وتدابير الحماية الفنية كتقنيات التشفير والترميز وبرامج منع الكتابة وإستخدام خوارزميات -تجزئة- للملفات المشفرة، من أجل منع الأشخاص المرخص لهم بإستخدام المنظومة المعلوماتية والوصول إلى المعطيات الأصلية التي تحتويها هذه المنظومة أو القيام بنسخها، ويكون ذلك في حالة ما إذا إستحال لأسباب تقنية حجز هذه المعطيات وفقًا للطريقة الأولى.[1]

الملاحظ في هذه المسألة هو غياب تحديد المشرع للأسباب التقنية التي تمنع الحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كإستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب إختراقه، أو ما تعلق بعملية نسخ المعطيات بسبب التطور الدائم في هذه التقنيات وما يتطلبه ذلك من توفير الوسائل التقنية اللازمة، إضافة إلى ضمان تكوين دوري بقصد إكتساب أعضاء الأجهزة القضائية المختصة في مجال التحقيق والكشف عن الجرائم الماسة بالمستند الإلكتروني المهارات المتطلبة لمكافحتها.[2]

أما بخصوص المعطيات المحجوزة ذات المحتوى المجرم فنصت المادة 08 من نفس القانون على أنه: "يمكن للسلطة التي تباشر التفتيش أن تأمر بإتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل بإستعمال الوسائل التقنية المناسبة لذلك".

الفرع الثالث: قواعد تحريز المضبوطات المعلوماتية وتأمينها

لقد أشارت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في البندين (ج)، (د) من الفقرة 03 من المادة 19 منها على مجموعة من التدابير الخاصة لضمان تحريز الأدلة وتأمينها فنيًا وصيانتها من أي تغيير أو إتلاف أو عبث يمكن أن يصيبها، بغرض المحافظة على سلامة المعطيات المخزنة، والمنع من الوصول إلى هذه المعطيات[3] أو رفعها[4] من النظام المعلوماتي"[1]، ولقد أخذت الإتفاقية العربية لجرائم تقنية المعلومات بنفس

---

[1]- براهيمي جمال، مرجع سابق، ص 48.

[2]- يزيد بوحليط، مرجع سابق، ص 91.

[3]- بمنع الأشخاص غير المرخص لهم من الوصول إلى المعطيات التي تم ضبطها داخل دعامة مادية للتخزين، من خلال إحاطتها بتدابير الحماية الفنية كالترميز والتشفير أو بأية وسيلة إلكترونية أخرى تمنع الدخول إليها، وصيانتها ببرامج منع التحريف والتغيير في المعطيات مثل برامج منع الكتابة، وللمزيد من التفصيل، ينظر: براهيمي جمال، مرجع سابق، ص-ص 49-50.

[4]- يتم اللجوء إلى هذا الإجراء في حالة ما إذا كانت المعطيات تتضمن خطرًا أو ضررًا بالمجتمع ومثال ذلك: البرامج التي تحتوي على فيروسات أو تقدم نموذجًا لعمل فيروسات أو قنابل، أو في الحالات التي تكون فيها محتوى المعطيات غير مشروع كما في حالة المواد الإباحية الطفولية. ولا يقصد بهذه العبارة "الرفع" (enlèvement) تدمير المعطيات بل تستمر في الوجود، إلا أنه يتم حرمان المشتبه فيه من الولوج إليها، لكن يمكن إعادتها إليه بعد التحقيق الجنائي. ومن التشريعات التي أخذت بهذا=

المعنى بموجب البندين (ج)، (د) من الفقرة الأولى من المادة 27 منها للدول الأعضاء على إلزام سلطاتها المختصة من الحفاظ على سلامة معلومات تقنية المعلومات المخزنة، وإزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

وهو ما أكدته الفقرة 02 من المادة 06 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر على أن: " يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز، السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية".

بالإضافة النص على بعض الإجراءات المسهلة والمساعدة لها، في منح صلاحيات بالإستعانة بأي شخص لديه خبرة ومعرفة فنية في تشغيل المنظومة المعلوماتية محل البحث والإجراءات المطبقة، من أجل حماية المعطيات التي تتضمنها هذه المنظومة، وإلزامه بالتعاون معها بتقديم المساعدة اللازمة والضرورية لتسهيل عملية تفتيش وضبط هذه المعطيات، وجعلهما أكثر فعالية وأقل تكلفة، بشرط أن تقتصر هذه المساعدة على تقديم المعلومات الضرورية فحسب دون الإخلال بحرمة الحياة الخاصة للأفراد ولا تتعارض مع قواعد السر المهني.[2]

وهو ما جسدته الفقرة 04 من المادة 19 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 والتي نصت على أن: "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام، أو الإجراءات المطبقة من أجل حماية المعطيات المعلوماتية التي تضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات المشار إليها فى الفقرتين 01 و02"[3]، وهو ما تبنته الإتفاقية العربية لجرائم تقنية المعلومات في الفقرة 02 من المادة 27 منها، على النص على تمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات، من أجل تقديم المعلومات الضرورية لإتمام إجراءات التفتيش والوصول إلى معلومات تقنية المعلومات.

=الإجراء قانون تحقيق الجنايات البلجيكي وذلك من خلال المادة 29 مكرر/ 3 حيث أعطى للنيابة العامة سلطة الأمر بغلق هذه المعطيات (Blocage de données) لمنع الوصول إليها، أو إلى النسخة المستخرجة منها الموجودة لدى من يستعملون المنظومة، وللمزيد من التفصيل، ينظر: عائشة بن قارة مصطفى، مرجع سابق، ص- ص 117- 118.

[1]-Art 19 paragraphe 03 du convention sur la cybercriminalité dispose que : « ...:

c. préserver i'intégrité des données informatiques stockées pertinentes;

d. rendre inaccessibles ou enlever ces données informatiques du systéme informatique consulté».

[2] - براهيمي جمال، مرجع سابق، ص-ص 50-51.

[3]-Art 19 paragraphe 04 du convention sur la cybercriminalité dispose que : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du systéme informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2».

وهو ما أكدته الفقرة 04 من المادة 05 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر على أن: "يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

فضلًا عن ما سبق ذكره، يمكن إتخاذ أيضًا بعض الإجراءات الخاصة للحفاظ على الدليل الإلكتروني من أي عبث، وذلك على النحو التالي:

1- إستخراج النسخ الإحتياطية من دعائم المعطيات المضبوطة، والعمل عليها لتجنب المساس بالدليل الأصلي[1]، والتعامل مع المنظومة من قبل خبراء تقنيين[2]؛

2- تأمين البرامج المعلوماتية المضبوطة فنيًا، وذلك قبل تشغيلها[3]؛

3- الإحتفاظ على المعطيات المرفوعة أو المنسوخة على الوضع الذي وجدت عليه لحظة الضبط، وعدم تغييرها خلال فترة الإجراءات الجزائية[4]؛

4- مراعاة ظروف الحرارة والرطوبة المناسبة عند التخزين، مع تجنب تعرض الدعامة للأضواء أو لأي سائل من السوائل، علمًا أنه في مثل هذه الظروف قد تصل مدة صلاحية التخزين إلى ثلاث (03) سنوات دون أن يصيبها تعديل أو تلف أو تحول[5]؛

5- تخزين الدليل الإلكتروني في أماكن آمنة غير معرضة للمجالات الكهرومغناطيسية والغبار[6]؛

وذلك بعدم تعريض القرص للأتربة وذرات الغبار والدخان، لأن ذلك يؤثر على السطح المغناطيسي مما يجعله غير قابل للقراءة أو الكتابة، ولذا يجب وضعه في غلافه الورقي الذي يغطي الأجزاء المكشوفة بعد الإستعمال[7]، وعدم تعريض الأقراص للمجالات المغناطيسية وذلك بعدم وضعها على الأجهزة أو السطوح المعدنية حتى لا يفقد ما عليها لأن التسجيل على الأسطوانة أو القرص يتم مغناطيسيًا[8]، وعدم الضغط عليه بوضع أشياء ثقيلة، وعدم كتابة بيانات اللاصقة الورقية المخصصة للمستخدم بعد لصقها على القرص لأن الضغط عليها بالقلم قد يفسد سطح القرص[9]، وعدم ثني الأقراص الممغنطة لأن ذلك قد يتسبب إلى إتلافها وفقدان

---

[1]- براهيمي جمال، مرجع سابق، ص 49

[2]- خالد عياد الحلبي، مرجع سابق، ص 177.

[3]- براهيمي جمال، مرجع سابق، ص 49.

[4]- حبيباتني بثينة، مرجع سابق، ص 338.

[5]- براهيمي جمال، مرجع سابق، ص 49.

[6]- خالد عياد الحلبي، مرجع سابق، ص 178.

[7]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 655.

[8]- نفس المرجع، ص 655.

[9]- نفس المرجع، ص 655.

كافة المعلومات المسجلة عليها، وعدم تعرضها للصدمات أو لمجالات مغناطيسية، أو المرور بها أو تخزينها على مقربة من محطة الإرسال اللاسلكي[1].

الفرع الرابع: الصعوبات التي تعترض إجراءات ضبط الدليل الإلكتروني

تعترض عملية ضبط الدليل الإلكتروني عدة صعوبات وعقبات، نذكر منها:

1. الصعوبات التي قد تواجه السلطة القضائية المختصة أن لا تصل إلى علمها هذه الجرائم، وذلك راجع إما لصعوبة إكتشافها من طرف الأشخاص العاديين أو حتى من قبل الشركات التي وقعت ضحية لها، وكذا الإحجام عن الإبلاغ خوفًا من إهتزاز ثقة عملائها خاصة على مستوى المؤسسات التجارية والبنوك، فذاتية الجريمة الماسة بالمستند الإلكتروني من حيث كونها مجهولة ومستترة تتم في بيئة رقمية قد لا تترك وراءها أي أثر خارجي تحول دون إكتشافها من طرف المجني عليه، وإذا ما تصادف وإكتشفها فإنه يعمد في أغلب الأحيان إلى التستر عليها والصمت بدل إبلاغ الشرطة للتحقيق بشأنها ومعرفة مرتكبها، وففي بعض الأحيان عدم علمه بوقوعه ضحية، وبالإضافة على ذلك قد يرجع إلى عدم إدراكه بأن مثل هذه الأفعال والهجمات تدخل ضمن الأفعال المعاقب عليها قانونًا، وهو ما يزيد من صعوبة كشف هذا النوع من الجرائم والوصول إلى الأدلة التي تثبت صلتها بفاعليها[2]؛
2. قد يكون محل الأدلة الإلكترونية جزء لا يمكن عزله عن المنظومة المعلوماتية أو الشبكة المعلوماتية، مما يتعين إلى إحتجاز المنظومة أو تعطيل شبكاتها بسبب إجراءات التحقيق لتحصيل الدليل، مما يؤدي بالضرورة إلى عزل المنظومة بالكامل عن دائرتها لمدة زمنية قد تطول أو تقصر، وهو الأمر الذي قد يؤثر على وتيرة سير أعمال جهة المستخدمة للمنظومة ويتسبب لها أضرارًا، ففي هذه الحالة تضطر إعمال مبدأ التناسب والذي يقتضي على ضبط الأدلة الضرورية فقط التي لها علاقة بالجريمة والتي تفيد في كشف الحقيقة.[3]

قد تحتوي على عناصر لا يمكن فصلها لأنها تتضمن عناصر مهمة لإثبات الجريمة، لذا يتعين تطبيق مبدأ التناسب من أجل إقامة التوازن بين مصلحة الدولة في كشف الحقيقة ومصلحة صاحب المنظومة في تسيير أعماله وعدم ضياع فرص الربح خاصة في المشاريع الإقتصادية، ومبدأ التناسب يرمي إلى إقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة دون أن يؤدي ذلك إلى تعطيل كل العمل في المنظومة والشبكات المتصلة بها، ومن التطبيقات القضائية ما قضت به المحكمة الفيدرالية الألمانية بإلغاء قرار الضبط الذي ورد على 220 دسك بالإضافة إلى الوحدة المركزية لمخالفته مبدأ التناسب.[4]

---

[1]- حبيباتني بثينة، مرجع سابق، ص 338.

[2]- بوشارب هانية، بن شهرة شول، **معوقات التحقيق الجنائي في البيئة الإفتراضية**، جامعة عمار ثليجي-الأغواط، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السابع، العدد الثاني، 2023، الجزائر، ص-ص 2008-2009.

[3]- براهيمي جمال، مرجع سابق، ص 54.

[4]- شنتير خضرة، مرجع سابق، ص-ص 118- 119.

3. عدم إبداء مستخدمي الأنظمة المعلوماتية الإستعداد للتعاون الكامل والفعال مع سلطات التحري والتحقيق، مما يعني أن الضبط بالنسبة لهم قد يمثل مساسًا بحقوق الغير[1]، وقد يرفضون التعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة، وقد يسعون بدلًا من ذلك إلى محاولة تجاوز آثارها حتى ولو كانت الوسيلة هي مكافأة المجرم، تجنبًا للأضرار بسمعتها أو خوفًا من أن الكشف عن أسلوب إرتكاب الجريمة قد يؤدي إلى تكرار وقوعها بتقليدها من طرف الآخرين، وقد تكون الخشية بسبب أن التبليغ قد يكون فرصة ذهبية أمام المجرم المعلوماتي لمعرفة ثغرات المنظومة المعلوماتية للمؤسسة، ومختلف نقاط الضعف فيها[2]؛

4. إن أكثر عائق يواجه السلطة القضائية المختصة هو عدم وجود دليل مرئي يمكن فهمه بالقراءة وقابليته للإدراك الحسي[3]، وتأتي من هنا مشكلة ضبط هذه المعطيات وإحرازها في شكل إلكتروني وحجزها ووضعها في خاتم قانوني لإستغلالها في البحث، وإذا كانت بعض التجهيزات والتقنيات تسمح للباحثين بالوصول إلى هذه المعطيات التي تبقى في ذاكرة الجهاز الإلكتروني المستعمل، إلا أنها تتطلب خبرة عالية وإمكانيات قد لا تتوافر عادة لدى السلطات القضائية المختصة[4]؛

5. قد لا تتمكن السلطات التحري والتحقيق من كشف الجريمة إذا علمت بها، وذلك بسبب قدرة الجاني على محو أو تدمير أدلة الإدانة خلال فترة زمنية وجيزة، وفي هذه الحالة يهدف المحو السريع إلى منع السلطات من إقامة الدليل ضده، فضلًا عن سهولة تنصله من هذا العمل بإرجاعه إلى خطأ في المنظومة المعلوماتية أو الشبكة، وإلى جانب هذا الأسلوب يستعمل الجناة أسلوب التغليط والتضليل الذي يتم إما عن طريق التلاعب بقواعد البيانات

---

[1]- خالد عياد الحلبي، مرجع سابق، ص 174.

[2]- بوشارب هانية، بن شهرة شول، **معوقات التحقيق الجنائي في البيئة الإفتراضية**، مرجع سابق، ص-ص 2009- 2010.

[3]- يتميز الدليل فيها بأنه دليل غير مرئي فهو عبارة عن نبضات إلكترونية مكونة من سلسلة طويلة من الأرقام الثنائية 0،1، والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه، فالكتابة مثلًا في العالم الرقمي ليس لها وجود مادي في شكل ورقي وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأي شيء في العالم الإفتراضي يتكون من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة، وأما تكوين معطياته فإنها تختلف من حيث الحجم والموضوع، فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة، مما يستحيل معه الإطلاع عليها بوسائل غير تقنية تعالج هذه الذبذبات في صورة مفهومة للبشر، وبالتالي أن أغلب المعطيات المخزنة التي تتداول عبر الحواسيب تكون على هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحواسيب، لذا يتطلب الإستعانة بأجهزة وأدوات التقنية وإستخدام برامج حاسوبية ملائمة للإطلاع عليه أو إستخراجه في هيئة ملموسة أو مادية وهي تعد أساليب علمية، إلا أن ترجمته وإخراجه في شكل مادي ملموس لا يعني أن هذا التجميع المادي هو الدليل، بل أن هذه العملية ليست سوى عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الإستدلال بها على معلومة معينة، وللمزيد من التفصيل، ينظر: بوشارب هانية، بن شهرة شول، **صعوبة عملية إستخلاص الدليل الإلكتروني**، مرجع سابق، ص 69.

[4]- صغير يوسف، **الجريمة المرتكبة عبر الإنترنت**، رسالة الماجستير، تخصص: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013، ص 118.

والبرامج أو إدخال معطيات مختلقة مزيفة أو محرفة في المنظومة، أو تغيير مسار المعطيات الصحيحة المدخلة دون أن يحس المجني عليه بذلك[1]؛

6. إن ضخامة كمية المعطيات والمعلومات المعالجة إلكترونيًا في الشبكة المعلوماتية التي يجب فحصها، بهدف الوصول إلى إستخلاص المعطيات التي تصلح كأدلة جنائية والمطلوب ضبطها لإستخلاص الدليل الإلكتروني منها، فضلًا عن تطلب قدرة من الخبرة الفنية لتحديد المعطيات التي تصلح كأداة جنائية من عدمه، هي من أكبر العقبات التي تواجه السلطة القضائية المختصة في الجريمة الماسة بالمستند الإلكتروني[2]؛

7. ضعف خبرة السلطة القضائية المختصة في هذه الجرائم، حيث قد ينقصهم التدريب الكافي على التعامل مع الأدلة التي قد يتركها الجناة في بعض الأحيان، الأمر الذي يؤدي إلى تدمير هذا الدليل أو الإقلال من قيمته[3]؛

8. قد تكون هذه الأدلة عبارة عن معطيات معلوماتية متداولة عبر الشبكات أو محفوظة في أجهزة مملوكة لشخص خارج الإقليم الوطني، مما يعيق الجهة القضائية المختصة من الوصول إليها وضبطها دون تعاون ومساعدة أجهزة التحقيق التابعة لتلك الدولة[4]؛

9. مدى قبول القاضي للنسخة المأخوذة عن تلك المعطيات كدليل إثبات في حالة صعوبة ضبط النسخة الأصلية، لأن القضاء في عدة دول خاصة الدول الأنجلوسكسونية يشكك في حجيتها ولا يعتبرها كالنسخة الأصلية لإحتمال التلاعب.[5]

المبحث الثاني: الإجراءات المستحدثة لإستخلاص الدليل الإلكتروني

نظرًا لعجز أساليب التحري والتحقيق التقليدية والتي لم تعد كافية أو فعالة في الكشف عن الجرائم المعلوماتية التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، إستحدث المشرع

---

[1]- بوشارب هانية، بن شهرة شول، **الصعوبات التي تواجهها الجهات التي تتولى التحري والتحقيق في الجرائم الإلكترونية**، ملتقى وطني حول التجارب التشريعية في مواجهة الجريمة الإلكترونية، معهد الحقوق والعلوم السياسية، المركز الجامعي نور البشير البيض، يوم 04 ديسمبر 2023، الجزائر، غير منشور، ص 3.

[2]- إذا كانت السلطة القضائية المختصة في الجرائم التقليدية يواجهون صعوبة في التدقيق ببعض السجلات والمعطيات المكتوبة الممسوكة في شركة أو مؤسسة، فماذا سيكون الوضع عليه في الحالات التي يتطلب التحقيق في جريمة ما الإطلاع على آلاف من السجلات والمعطيات الرقمية من نصوص وصور فوتوغرافية ومقاطع فديو، والبحث عنها بين عدد من آلاف الصفحات، كما أن الإطلاع عليها وتحليلها يستوجب الكثير من الوقت، والتي يلزم فرزها من قبل الجهات المختصة وتصنيفها إلى معطيات مجرمة وأخرى غير مجرمة مما قد يتبين من الفحص أن عددًا كبيرًا من المعطيات ربما يكون غير ذي فائدة، ونتيجة لعدم إمكانية وجود فرز في إطار التخزين الرقمي في العالم الرقمي، فإن فحص هذه المعطيات يحتاج إلى وقت وجهد ونفقات ضخمة فمثل هذه الأمور تشكل عقبة أمام سلطات البحث، ويصبح الأمر أكثر تعقيدًا فيما لو عمد المجرم إلى تشتيت المعلومات والمعطيات التي دخل إليها بهدف تضليل المحققين وإجهادهم، لكي يكفوا عن متابعة البحث عن الأدلة الجرمية، وللمزيد من التفصيل، ينظر: بوشارب هانية، بن شهرة شول، **معوقات التحقيق الجنائي في البيئة الإفتراضية**، مرجع سابق، ص-ص 2004-2005.

[3]- سعد عاطف عبد المطلب حسنين، مرجع سابق، ص 643.

[4]- براهيمي جمال، مرجع سابق، ص 55.

[5]- نفس المرجع، ص 55.

الجزائري نصوصًا خاصة لمواجهة هذا النوع الخطير من الإجرام، محاطًا إياها بمجموعة من الضوابط الصارمة، ويهدف ذلك إلى تحقيق التوازن بين متطلبات كشف الجرائم ومشروعية إجراءات الملاحقة من جهة وبين حماية الأفراد وخصوصياتهم الشخصية من جهة أخرى.

ذلك أن تقرير هذه الضمانات يعد وسيلة لصيانة تلك الحقوق من الهدر أو التعسف أو الإخلال بها، وهو في ذات الوقت التعبير الحي عن قوة القانون من حيث مدى إلتزام السلطات القضائية بحدود مهمتها، مع ضرورة التصدي للإجرام دون تعسف.

المطلب الأول: التسرب الإلكتروني

أدرج المشرع الجزائري إجراء التسرب بمقتضى القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية، حيث أفرد له الفصل الخامس تحت عنوان "في التسرب" من الباب الثاني من الكتاب الأول، والذي تضمن ثمانية مواد تمتد من المادة 65 مكرر11 إلى المادة 65 مكرر18، ورغم إلغاء الأمر رقم: 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، بموجب القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية، فقد أبقى المشرع الجزائري على هذا الإجراء، وأعاد تنظيمه ضمن المواد من 120 إلى 127 المدرجة في الفصل الخامس من الباب الثاني من الكتاب الثاني.

سنتطرق إلى تعريف التسرب الإلكتروني وصوره في (الفرع الأول)، وسنتطرق إلى شروط صحة التسرب الإلكتروني في (الفرع الثاني)، بينما (الفرع الثالث) فقد خصصناه إلى الحماية القانونية المقررة للمتسرب.

الفرع الأول: تعريف التسرب الإلكتروني وصوره

ارتأينا أن نتطرق إلى تعريف التسرب الإلكتروني، ثم إلى صوره.

أولاً: تعريف التسرب الإلكتروني

عرف المشرع الجزائري عملية التسرب طبقًا لأحكام الفقرة الأولى من المادة 121 من ق.إ.ج.ج كالآتي: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

نلاحظ من خلال الفقرة آنف الذكر، أن المشرع الجزائري قد أجاز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية عن طريق ضابط أو عون الشرطة القضائية، القيام بعملية التوغل والإختراق داخل جماعة إجرامية ومراقبتهم، وذلك بإيهامهم بأنه فاعل

أصلي أو شريك أو مخفيًا لمحصلات الجريمة، حتى يحظى بثقتهم بغرض الكشف عن ملابسات الجريمة، والتعرف على هوية مرتكبيها.[1]

فالتسرب على هذا النحو هو عملية أمنية تفيد قيام أحد عناصر الشرطة القضائية بالتسلل إلى جماعة إجرامية، أو التوغل داخل مكان أو تنظيم داخل مكان أو تنظيم يصعب الدخول إليه، تجعله يتقرب إليهم ويشعرهم بالإنتماء إليهم بصفته شريكًا أو خاف أو وسيط، بغرض مراقبة تحركات أفراد هذه الجماعة قبل أو خلال قيامهم بالعمل الإجرامي، ومن ثمة تحقيق حالة التلبس بالجريمة.[2]

ويحكم التسرب مبدأ المشروعية فلا يجوز أن ترقى الحيلة إلى درجة العمل غير المشروع أو التحريض على الجريمة، لأن البحث عن الحقيقة لا يتأتى إلا بإجراء مشروع، فلا يجوز البحث عن الحقيقة بطرق غير مشروعة.[3]

أما التعريف الذي أقره المشرع الفرنسي بموجب الفقرة 02 من المادة 706-81 من ق.إ.ج.ف المعدلة بموجب القانون رقم: 2025-532 المؤرخ في 13 جوان 2025 الرامي إلى تخليص فرنسا من فخ الإتجار غير المشروع بالمخدرات، والذي عرف التسرب بأنه: "الإجراء الذي يقوم به الضابط أو عون الشرطة القضائية مخول بشكل خاص وفقًا لشروط يحددها مرسوم، ويتصرف تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، وذلك من خلال مراقبة أشخاص يشتبه في إرتكابهم جناية أو جنحة، عبر التظاهر أمام هؤلاء الأشخاص بأنه فاعلًا أصليًا معهم أو شريكًا لهم أو مخفيًا لمتحصلات الجريمة، أو في صورة ضحية أو طرف ثالث مفوض من هذه الأخيرة، أو أي شخص له مصلحة في إرتكاب الجريمة".[4]

بمقتضى التعديل الذي أدخل على قانون الإجراءات الجزائية الفرنسي بموجب القانون رقم: 2025-532 السالف الذكر، يلاحظ أن المشرع الفرنسي قد وسع من نطاق صور التسرب، بحيث أتاح لضابط أو عون المتسرب وتحت مسؤولية ضابط الشرطة القضائية المنسق للعملية بإمكانية التسلل إلى الجماعة الإجرامية، مع التظاهر بعدة صفات كأن يتقمص صفة الضحية أو طرف ثالث مفوض من هذه الأخيرة، أو أي شخص له مصلحة في إرتكاب الجريمة.

وعرف المشرع البلجيكي عملية التسرب بموجب المادة 1/octies 47 من قانون التحقيقات الجنائية على أنه: "العملية التي يقوم فيها موظف الشرطة يسمى المتسرب بهوية وهمية، بإنشاء

---

[1]- بوكر رشيدة، مرجع سابق، ص 308.

[2]- عبد الرحمان خلفي، مرجع سابق، ص 104.

[3]- عبدالله أوهايبية، مرجع سابق، ص 362.

[4]-Art 706-81 paragraphe 02 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que: « L'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, a surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprés de ces personnes, comme un de leurs coauteurs, complices ou receleurs ou comme une victime, un tiers mandaté par cette dernière ou toute personne intéressée à la commission de l'infraction».

علاقات مستمرة مع شخص أو عدة أشخاص، تتوفر بشأنهم قرائن جدية حول إرتكابهم أو أنهم سيرتكبون جرائم في إطار جماعة إجرامية منظمة حسب المادة 324 مكرر من قانون العقوبات أو الجنايات والجنح المحددة بالمادة 2/90-4 من قانون التحقيقات الجنائية"[1]، يلاحظ أن المشرع البلجيكي قد أجاز للضابط أو العون المتسرب بإقامة علاقات توصف بأنها مستمرة أو دائمة مع شخص أو عدة أشخاص المشتبه فيهم في إرتكاب الجرائم المنصوص عليها على سبيل الحصر، وإن كانت العلاقة معزولة أو منقطعة فلا تدخل في إطار القانون 06 جانفي 2003 المتعلق بالأساليب الخاصة للبحث والتحري.[2]

من خلال تعريف إجراء التسرب، يتبين أنه لا يتناسب مع طبيعة البيئة التي ترتكب فيها الجريمة الماسة بالمستند الإلكتروني، مما يثير التساؤل حول مدى إمكانية اللجوء إلى هذا الإجراء للتوغل داخل الجماعة الإجرامية بهدف إستخلاص الدليل الإلكتروني ؟

بالرجوع إلى نص المادة 120 من ق.إ.ج.ج نجد أنها حصرت الجرائم التي يجوز فيها تنفيذ عملية التسرب بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وبالتالي فإن هذا إجراء لا يقتصر على العالم المادي فحسب بل يمكن تفعيله أيضًا في البيئة الرقمية، وبما أن الجرائم الماسة بالمستند الإلكتروني تندرج ضمن هذا النطاق فإن اللجوء إلى إجراء التسرب يصبح أمرًا ضروريًا بإعتباره من إجراءات التحري الخاصة بها.

يمكن تصور تنفيذ عملية التسرب في الجرائم الماسة بالمستند الإلكتروني، من خلال قيام الضابط أو عون المتسرب بإقامة حلقات إتصال مباشر مع المشتبه فيهم سواء عن طريق البريد الإلكتروني أو من خلال الإشتراك في محادثات غرف الدردشة ومواقع التواصل الإجتماعي، مع الظهور بمظهر يوهم بأنه أحد الفاعلين مثلهم مستعملًا في ذلك أسماء وصفات وهيئات مستعارة ووهمية، كما قد يلجأ إلى إختراق بعض المواقع أو فتح ثغرات إلكترونية فيها سعيًا منه للإستفادة من معلوماتهم حول طرق الإقتحام التي يعتمدها الهاكر للموقع، أو لمسايرتهم بنية رصد المعلومات المتعلقة بأفعالهم الإجرامية وما ينوون إرتكابه من الجرائم لاحقًا.[3]

ثانيًا: صور التسرب الإلكتروني

يعد التسرب عملية إختراق يقوم بها ضابط أو عون الشرطة القضائية وتحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بهدف التوغل في منظمة إجرامية موهمًا أعضاءها أنه شريك لهم أو فاعل في إرتكاب جناية أو جنحة أو مخفيًا لمحصلات تلك الجريمة، بغرض كشف ملابسات الجريمة والتعرف على هوية مرتكبيها[4]، طبقًا لأحكام الفقرة الأولى من

[1]- روابح فريد، **الأساليب الإجرائية الخاصة للتحري والتحقيق في الجريمة المنظمة**، أطروحة الدكتوراه في القانون العام، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1 بن يوسف بن خدة، 18 فيفري 2016، ص 150.

[2]- نفس المرجع، ص 151.

[3]- نسيغة فيصل، عبير بعقيقي، **الإثبات في الجرائم المعلوماتية على ضوء القانون 04/09**، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر-الوادي، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 02، جوان 2018، الجزائر، ص43.

[4]- أحمد غاي، مرجع سابق، ص 197.

المادة 121 من ق.إ.ج.ج التي تنص على أن: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

1- المتسرب كفاعل الأصلي:

لمعرفة معنى الفاعل الأصلي يجب الرجوع إلى القواعد العامة المنصوص عليها في قانون العقوبات الجزائري في المادة 41 منه، والتي تنص على أن: "يعتبر فاعلًا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة، أو حرض على إرتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة إستعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي".

الفاعل الأصلي أو المباشر هو الذي يساهم مساهمة مباشرة، فهو من يقدم أعمالًا مباشرة لتنفيذ الجريمة، سواء إرتكبت الجريمة من شخص أو عدة أشخاص يقومون بأدوار رئيسية في تنفيذ الجريمة، إذا ظهروا على مسرح الجريمة وعاصر نشاطهم زمن وقوع الجريمة، من خلال إرتكاب الأفعال الإجرامية المذكورة في المادة 123 من ق.إ.ج.ج، وذلك لغرض كسب ثقة أعضاء المنظمة الإجرامية والحصول على الأدلة المادية للكشف عن هوية المشتبه فيهم، غير أن المشرع الجزائري يمنع من التحريض على إرتكاب الجريمة[1]، طبقًا للفقرة 02 من المادة 121 من ق.إ.ج.ج التي تنص على أن: "...لا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضًا على إرتكاب الجرائم"، بمعنى أن الضابط أو العون المتسرب بإمكانه أن يقوم بالأفعال المذكورة في المادة 123 من نفس القانون بصفته فاعل أصلي بدون أن يكون محرضًا[2] عليها، فتحريضه على إقتراف الجريمة يتعارض مع إلتزامه في الحرص على تطبيق أحكام القانون وإضفاء الشرعية الإجرائية، وكذا على حسن كفالة الحرية الشخصية للفرد[3].

ومما سبق ذكره، فإن الضابط أو العون المتسرب يكون مقيدًا بعدم القيام بأعمال خارجة عن تلك المحددة على سبيل الحصر وإلا تعرض للمساءلة الجزائية، وهذا من شأنه أن يؤثر عليه ذلك أين يجد نفسه مخيرًا بين الإمتناع عن إرتكاب الأفعال التي لم يأذن بها القانون مما قد يؤدي إلى فشل العملية، أو الإقدام على إرتكابها لكسب ثقة الجماعة الإجرامية المتسرب فيها وإنجاح العملية مع تحمله للمسؤولية الجزائية المترتبة على ذلك.

---

[1]- نبيلة قيشاح، **الإجراءات المستحدثة لمكافحة الجريمة المنظمة في التشريع الجزائري**، أطروحة الدكتوراه علوم، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي –تبسة-، 2020/2019، ص-ص 183-184.

[2]- المحرض هو خلق فكرة الجريمة لدى الغير، عن طريق إستعمال الآساليب المذكورة في المادة 41 من ق.ع.ج على سبيل الحصر والمتمثلة في: تحريض على إرتكاب الفعل بالهبة، أو الوعد، أو التهديد، أو إساءة إستعمال السلطة أو الولاية، أو التحايل، أو التدليس الإجرامي.

[3]- بولمكاحل أحمد، ليطوش دليلة، **التسرب والشرعية الإجرائية**، كلية الحقوق والعلوم السياسية، جامعة باتنة1-الحاج لخضر، مجلة الباحث للدراسات الأكاديمية، المجلد07، العدد02، 2020، الجزائر، ص 1115.

2- المتسرب كشريك:

إستنادًا إلى الأحكام العامة، نجد أن المادة 42 من ق.ع.ج تعرف الشريك على أنه: "يعتبر شريكًا في الجريمة من لم يشترك إشتراكًا مباشرًا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على إرتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها، مع علمه بذلك"، لم يحدد المشرع الجزائري الطرق التي تتم بها مساعدة أو معاونة الفاعل الأصلي، مما يعني أن جميع الطرق صالحة لأن تكون مساعدة سواء كانت مادية أو معنوية، وقد تكون قبل إرتكاب الجريمة أو أثناءها أو قرب الإنتهاء منها، كما يلي:

- الأفعال التحضيرية، وهي الأفعال التي يقوم بها قبل إرتكاب الجريمة؛
- الأفعال المسهلة، وهي التي تكون أثناء إرتكاب الجريمة، وهنا يحاول الشريك تسهيل عمل الفاعل الأصلي بشرط أن لا يكون متواجد في مسرح الجريمة فيعتبر فاعلًا أصليًا؛
- الأفعال المنفذة، وهي التي يرتكبها الشريك عند قرب الإنتهاء من الجريمة لكن بعيدًا عن مسرح الجريمة.

وهناك صورة ثانية للشريك يسمى بالشريك الحكمي طبقًا للمادة 43 من نفس القانون والتي تنص على أن: "يأخذ حكم الشريك من يقدم مسكنًا أو ملجًأ أو مكانًا للإجتماع لواحد أو أكثر من الأشرار، الذين يمارسون اللصوصية أو العنف ضد أمن الدولة أو الأمن العام أو ضد الأشخاص أو الأموال، مع علمه بسلوكهم الإجرامي".

لم يشترط المشرع الجزائري وجود إتفاق سابق بين هؤلاء الأشرار على إرتكاب الجرائم، كما كان يشترط في السابق تكرار الفعل لقيام الجريمة، وذلك من خلال الإعتياد على تقديم المسكن أو الملجأ أو المكان للإجتماع لواحد أو أكثر منهم، إلا أنه تدارك الأمر بمقتضى تعديله لقانون العقوبات بموجب القانون رقم: 24-06 المؤرخ في 28 أفريل 2024 السالف الذكر وجعل السلوك الإجرامي يتحقق بمجرد قيام الشريك بالفعل الإجرامي لأول مرة، متى كان عالمًا بالطبيعة الإجرامية لسلوك الأشرار.

وعليه فالضابط أو عون المتسرب الذي يأخذ صورة الشريك كل من لم يشترك إشتراكًا مباشرًا مع الفاعل أو الفاعلين الأصليين، ولكن يقوم بإيهامهم من خلال مساعدتهم بشتى الطرق أو المعاونة على إرتكابهم الأفعال التحضيرية أو المسهلة أو المنفذة للجريمة، أما الإشتراك الحكمي فيعتبر المتسرب مشتركًا إشتراكًا حكميًا إذا قام بالأفعال المساعدة كتقديم المسكن أوالملجأ أو مكان للإجتماع لواحد أو أكثر من المجرمين، مع علمه بسلوكهم الإجرامي.

3- المتسرب كخاف:

فقد يكون الضابط أو عون المتسرب خافي، بأن يلجأ لإخفاء متحصلات الجريمة التي ترتكبها الجماعات الإجرامية دون أن يكون مسؤولًا جزائيًا.[1]

الخافي هو من يقوم بإخفاء متحصلات الجريمة، وبعبارة أكثر وضوحًا فإن التسرب هو عملية إختراق أحد أعضاء أجهزة الأمن (ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية) لمنظمة إجرامية، موهمًا أعضاءها أنه شريك لهم أو فاعل في إرتكاب جناية أو جنحة أو مخفيًا لمحصلات تلك الجريمة، بغرض كشف ملابسات الجريمة والتعرف على هوية مرتكبيها.[2]

الفرع الثاني: شروط صحة التسرب الإلكتروني

أحاط المشرع الجزائري إجراء التسرب بمجموعة من الشروط التي تهدف إلى توفير الحد الأدنى من الضمانات، نظرًا لما ينطوي عليه هذا الإجراء من خطورة وما يشكله من إنتهاك لحرمة الحياة الخاصة للأفراد، فهو يعد التعبير الحي عن قوة القانون في مدى كفالة إلتزام السلطات القضائية بحدود إختصاصها.

أولًا: الشروط الموضوعية لعملية التسرب الإلكتروني

تتمثل الشروط الموضوعية لعملية التسرب في ما يلي:

1- شرط الضرورة:

المقصود بشرط الضرورة (principe de nécessité) وجود ضرورة قصوى تستدعي للقيام بهذا الإجراء نظرًا لعدم كفاية كل إجراءات التحري أو التحقيق، بغرض الحصول على الأدلة القانونية التي تسمح بالوصول إلى المجرمين الحقيقين، ولقد أشارت المادة 120 من ق.إ.ج.ج على شرط الضرورة بعبارة: "عندما تقتضي ضرورات التحري أو التحقيق".

أي إستدعى الأمر اللجوء إلى إجراء التسرب، وذلك بإعتباره الإجراء الوحيد والأنسب الذي يمكن بواسطته من إظهار الحقيقة بعد أن ثبت عدم نجاعة إجراءات البحث العادية، أو أن

[1]- نص المشرع الجزائري في المادة 387 من ق.ع.ج بأنه: "كل من أخفى عمدًا أشياء مختلسة أو مبددة أو متحصلة من جناية أو جنحة في مجموعها أو في جزء منها، يعاقب بالحبس من سنة (01) على الأقل إلى خمس (05) سنوات على الأكثر، وبغرامة من عشرون ألف 20.000 دج إلى مائة ألف 100.000 دج. ويجوز أن تتجاوز الغرامة عشرون ألف 20.000 دج حتى تصل إلى ضعف قيمة الأشياء المخفاة. ويجوز علاوة على ذلك أن يحكم على الجاني بالحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 من هذا القانون لمدة سنة (01) على الأقل وخمس (05) سنوات على الأكثر، وكل ذلك مع عدم الإخلال بأية عقوبات أشد إذا إقتضى الأمر في حالة الإشتراك في الجناية طبقًا للمواد 42 و43 و44".

[2]- أحمد غاي، مرجع سابق، ص 197.

الإستمرار فيها في تحقيق الغرض قد أضحى بعيد الإحتمال، أو عجزها عن كشف ملابسات الجريمة وجمع الأدلة عنها.[1]

وشرط الضرورة مقيد بنوع محدد من الجرائم المشار إليها في المادة 114 من ق.إ.ج.ج وهي: جرائم القتل العمدي، جرائم المخدرات والمؤثرات العقلية، والجريمة المنظمة عبر الحدود الوطنية، والجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، وجرائم الفساد، وجرائم التهريب، وجرائم الإتجار بالبشر، وجرائم الإتجار بالأعضاء، وجرائم تهريب المهاجرين، وجرائم إختطاف الأشخاص.

2- شرط الإحتياطية:

شرط الإحتياطية (principe de subsidiarité) يفيد في عدم اللجوء إلى إستعمال إجراء التسرب إلا على وجه الإحتياط، عندما تكون الوسائل العادية غير كافية درءًا للوقوع في المساس بالحريات الفردية، وتشير إليه دائمًا المادة 120 من ق.إ.ج.ج بالنص: "عندما تقتضي ضرورات التحري أو التحقيق"، أي لا يتم اللجوء إليه إلا إستثناء، وبشروط دقيقة، مع إحاطته بضمانات كبيرة.[2]

3- شرط الملاءمة:

شرط الملاءمة (principe de proportionnalité) يفيد في قيام الإشتباه ضد أشخاص معينين بأنهم إرتكبوا جناية أو جنحة أو ربما هم بصدد القيام بذلك وفقًا لأحكام المادة 121 من ق.إ.ج.ج، مع ضرورة التقيد بالجرائم المشار إليها على سبيل الحصر بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، أي لا بد من قيام قرائن قوية وجدية تشير على الغالب بوقوع جريمة في الوقت القريب أو أن الفاعلين بصدد التحضير.[3]

ثانيًا: الشروط الشكلية لعملية التسرب الإلكتروني

تتمثل الشروط الشكلية لإجراء التسرب في ما يلي:

1- تحرير تقرير مسبق لإجراء التسرب الإلكتروني:

كأصل عام وبمقتضى المادة 27 من ق.إ.ج.ج يلزم كل ضابط الشرطة القضائية أثناء قيامه بعمله تحرير محضرًا مفصلًا يشمل جميع جوانب الإجراء وموافة وكيل الجمهورية به،

[1]- عنتر أسماء، **إجراءات التحقيق القضائي الخاصة -دراسة مقارنة-**، أطروحة الدكتوراه، تخصص: قانون قضائي خاص، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس -مستغانم، 2020-2021، ص 244.

[2]- عبد الرحمان خلفي، مرجع سابق، ص 105.

[3]- نفس المرجع، ص 106.

وتختلف تسميات أنواع المحاضر بحسب الإجراء المنجز، وفي إطار إجراء التسرب تحديدًا يلاحظ أن المادة 122 من نفس القانون نصت صراحة على أنه قبل البدء في إجراء التسرب يقع على عاتق ضابط الشرطة المكلف بتنسيق العملية تحرير تقريرًا كتابيًا، يتضمن جميع العناصر الضرورية المتعلقة بالعملية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب وكذا الأشخاص المسخرين.

ويجب مراعاة في إعداد هذا التقرير إحترام جميع مراحل عملية التسرب من بدايتها إلى نهايتها، بذكر جميع المعلومات المتعلقة بالجريمة، وتحديد هوية المشتبه في تورطهم في إرتكاب الجريمة، وتحديد الوسائل المستعملة ونوعيتها، وتحديد الأماكن التي تم إستخدامها، وبناءً على ذلك يتعين على الضابط المنسق أن يجمع أكبر قدر ممكن من المعلومات حول الجريمة محل التحري والتحقيق وكذا أهمية القيام بإجراء عملية التسرب، حتى يتسنى لوكيل الجمهورية أو قاضي التحقيق أن يأمر بإجرائها، مع الأخذ في الإعتبار العناصر اللازمة لمعاينة الجرائم.[1]

2- إصدار الإذن من السلطة القضائية المختصة ومراقبتها لعملية التسرب الإلكتروني وتنفيذه:

وسنحاول تفصيل ذلك من خلال النقاط التالية:

أ- إصدار ترخيص من السلطة القضائية المختصة:

نصت المادة 120 من ق.إ.ج.ج على أنه: "عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 114، يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه"، وهو ما يتطابق مع الفقرة الأولى من المادة 706-81 من ق.إ.ج.ف[2].

وعليه لمباشرة هذا الإجراء فلا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه، بل ألزم المشرع الجزائري أن يصدر إذنًا للقيام به وأن يكون قانونيًا وحاملًا لصفة الوثيقة الرسمية، وهو ذلك الأمر القضائي الصادر من طرف وكيل الجمهورية المختص إقليميًا أو من طرف قاضي التحقيق بعد إخطار وكيل الجمهورية.

---

[1]- عنتر أسماء، مرجع سابق، ص 251.

[2]-Art 706-81 paragraphe 01 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que: « l'orsque les nécessités de l'enquête ou de l'instruction concernant l'un des crimes ou délits entrant dans le champs d'application des articles 706-73 et 706-73-1 le justifient, le procureur de la République ou après avis de ce magistrat, le juge d'instruction saisi peuvent autoriser qu'il soit procédé, sous leur contrôle respectif à une opération d'infiltration dans les conditions prévues par la présente section».

ترجمتها:

تنص الفقرة الأولى من المادة 706-81 من ق.إ.ج.ف على أن: "عندما تبرر ضرورة التحري أو التحقيق في أي جريمة أو جريمة تدخل في نطاق المادتين 706-73 و706-73-1 تبرر ذلك، يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، أن يأذن بإجراء عملية التسرب تحت إشرافه وفقًا للشروط المنصوص عليها في هذه المادة".

ولهذا فقد منحت المادة 120 من ق.إ.ج.ج صلاحية الإذن بهذا الإجراء لوكيل الجمهورية وذلك إذا إقتضته ضرورات البحث والتحري، كما يمكنه إتخاذ هذا الإجراء في حالة التلبس في إحدى الجرائم المذكورة سابقًا على سبيل الحصر في المادة 114 من ذات القانون، كما منح الحق بإصداره لقاضي التحقيق بعد إخطار وكيل الجمهورية إذا إقتضته ضرورات التحقيق الإبتدائي في هذه الجرائم بتكليف ضباط الشرطة القضائية عن طريق الإنابة القضائية بموجب المادة 234 من نفس القانون.

ب- أن يكون الإذن مسببًا:

لا يكفي أن يتم إصدار الإذن بالتسرب من طرف الجهة القضائية المختصة فحسب، بل يجب أن يتضمن على الشروط المبينة في المادة 124 من ق.إ.ج.ج، وذلك بأن يكون مكتوبًا ومسببًا وذلك تحت طائلة البطلان، ونجد المشرع الفرنسي هو بدوره ورد هذا الشرط بموجب الفقرة الأولى من المادة 706-83 من ق.إ.ج.ف[1]، أما في بلجيكا فيصدر الإذن بالتسلل من قاضي التحقيق أو ممثل المقاطعة، ويجوز إعطاء الإذن شفويًا وتأكيده في أقرب وقت كتابيًا إذا كان الوضع ملحًا ويستلزم السرعة في الفقرتين 03 و04 من المادة 56[2].

فالتسبيب هو التبرير وإيضاح السبب الذي يؤدي إلى القيام بعملية التسرب، بمعنى بيان الأسانيد القانونية والواقعية التي أدت إلى إصدار الإذن من خلال تبيان القرائن والدلائل ومدى كفايتها والفائدة المرجوة من التسرب[3]، وبالتالي على السلطة القضائية الآذنة بعملية التسرب أن تتأكد من مدى جدية وكفاية المبررات التي يستنبط منها على إرتكاب الجريمة ونسبتها إلى مرتكبيها، فإذا إطمئنت إليها أصدرت الإذن بناء عليها، وإن لم تطمئن إليها رفضت إصدار الإذن[4].

ويتم تحديد طبيعة الجريمة التي تبرر اللجوء للقيام بهذا الإجراء وهي الجرائم التي حددت في المادة 114 من ق.إ.ج.ج بما في ذلك الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، ومع ضرورة أن يشتمل الإذن تحديد هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وأن تحدد فيه مدة التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر، قابلة للتجديد أربعة (04) أشهر أخرى حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية[5]، وهو ما يتطابق مع الفقرتين 02

---

[1]-Art 706-83 paragraphe 01 du C.P.P.F (Loi n° 2004-204 du 09 mars 2004) dispose que : « a peine de nullité, l'autorisation donnée en application de l'article 706-81 est délivrée par écrit et doit être spécialement motivée».

ترجمتها :

تنص الفقرة الأولى من المادة 706-83 من ق.إ.ج.ف على أن: "تحت طائلة البطلان، الإذن الممنوح بموجب المادة 706-81 يصدر كتابيًا وأن يكون مسببًا".

[2]- محمد صالح جاد المولى خليفة، مرجع سابق، ص 138.

[3]- عنتر أسماء، مرجع سابق، ص-ص 252- 253.

[4]- نفس المرجع، ص 253.

[5]- المادة 124 /2 و3و4 من القانون رقم: 25-14 السالف الذكر.

و03 من المادة 706-83 من ق.إ.ج.ف التي إشترطت أن يبين في الإذن طبيعة الجريمة وهوية ضابط الشرطة القضائية المكلف بإجرائه ومدة التسرب التي لا يمكن أن تتجاوز مدة أربعة (04) أشهر والتي تكون قابلة للتجديد ضمن نفس الشروط الشكلية والزمنية[1].

ويضيف قانون التحقيقات الجنائية البلجيكي أن يتضمن الإذن بالتسرب أيضًا ذكر طريقة تنفيذ التسرب وبدون تحديد طريقة معينة، كتطبيق تقنيات التحري البوليسي أو الإستعانة بخبرة أحد المدنيين، وكذا إستراتيجيات وسيناريوهات التنفيذ وغيرها.[2]

وإنطلاقًا مما سبق ذكره، يعتبر تسبيب الإذن بالتسرب في أنه يعد ضمان أساسي لعدم تعسف السلطة القضائية الآذنة بعملية التسرب، وتقييد سلطتها في إصدار الإذن دون التيقن أو دون التحقق من المبررات التي يستند إليها لإتخاذ هذا الإجراء الخطير، فضلًا على أنه يتيح للقضاء من بسط رقابته على المبررات التي إستند إليها وكيل الجمهورية أو قاضي التحقيق في إصداره الإذن، فيقر ويعتد بما ترتب على هذا الإجراء من آثار، أو إذا لم يقر فيهدر الإجراء ولا يعتمد على ما أسفر عنه من الأدلة إذا ثبت أنه من دون هدف أو غاية إلى تحقيق غرض آخر غير ما حدده القانون، وبناءً على ذلك فإشتراط التسبيب يدفع بالسلطة القضائية المختصة إصدار إذن التسرب الإلتزام غالبًا بالتأني والتفكير في مدى إتخاذ هذا الإجراء الخطير.[3]

ويلاحظ أن المشرع الجزائري رتب البطلان إلا في حالة عدم مراعاة كتابة الإذن وتسبيبه، في حين أنه لم يقتضيه في حالة عدم ذكر هوية ضابط الشرطة القضائية المسؤول عن عملية التسرب والجريمة والمدة التي تستغرقها، وهو ما يدل على أن لا يترتب بطلان الإذن بالتسرب عند عدم مراعاة الشكليات المنصوص عليها في الفقرتين 02 و03 من المادة 124 من ق.إ.ج.ج.[4]

وقد أغفل المشرع الجزائري شرطًا لازمًا لمشروعية عملية التسرب المتمثل في تحديد الأشخاص الخاضعين لعملية التسرب[5]، فإغفال على هذه الضمانة يعد فراغًا تشريعيًا ينبغي معالجته، لأن المباشرة في تنفيذ عملية التسرب يعد إجراء خطيرًا على الحرية الشخصية للفرد، والإستثناء لا يقاس عليه ولا يتوسع في تفسيره[6].

---

[1]-Art 706-83 paragraphe 02 et 03 du C.P.P.F (Loi n°2004-204 du 9 mars 2004) dispose que : « Elle mentionne la ou les infractions qui justifient le recours à cette procédure et l'identité de de l'officier de police judiciaire sous la responsabilité duquel se déroule l'opération. Cette autorisation fixe la durée de l'opération d'infiltration, qui ne peut pas excéder quatre mois. L'operation peut être renouvelée dans les mêmes conditions de forme et de durée. Le magistrat qui a autorisé l'opération peut, à tout moment, ordonner son interruption avant l'expiration de la durée fixée».

[2]- روابح فريد، مرجع سابق، ص 158.

[3]- ركاب أمينة، **أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري**، رسالة الماجستير، تخصص: قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد-تلمسان-، 2014-2015، ص-ص 110-111.

[4]- عنتر أسماء، مرجع سابق، ص 257.

[5]- نفس المرجع، ص 256.

[6]- نفس المرجع، ص 256.

ولضمان نجاح عملية التسرب أوجب المشرع الجزائري أن تضم رخصة الإذن بالقيام بها في ملف الإجراءات بعد الإنتهاء من العملية وليس وقت إصدارها أو أثناء تنفيذها، وذلك للحفاظ على السرية الضرورية بين القاضي الآمر بالقيام بها وضابط الشرطة القضائية المنسق والمشرف عليها وكذا الضابط أو العون المتسرب.[1]

ج- مراقبة عملية التسرب الإلكتروني:

تنفيذ عملية التسرب تكون تحت إشراف ورقابة القاضي الآمر بها الذي يكون بحوزته ملف القضية منذ إصداره الإذن بإجرائها إلى نهايتها، فهو من يتابع الأحداث والمستجدات والتطورات التي قد تطرأ عليها، ويكون على علم بسيرها بالتتابع حتى لا تحدث إنتهاكات قانونية[2]، ويمكنه أن يأمر في أي وقت بوقفها قبل إنقضاء المدة المحددة قانونًا[3] إذا إستدعى الوضع ذلك، ويقوم بالرقابة المباشرة عليها ضابط الشرطة القضائية المكلف بتنسيق العملية، فينظر في كافة وقائع الميدان ومدى صحتها وعدم تجاوزها للضوابط القانونية والإجرائية، ويلزم على المتسرب بأن ينسق معه ويحيطه علمًا بكل جديد[4].

وقد جاءت هذه الأحكام مطابقة تمامًا لما أقره المشرع الفرنسي، ففي الفقرة الأولى من المادة 706-81 من ق.إ.ج.ف أوكل من خلالها مهمة منح الإذن بالتسرب لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، كما تكون أعمال الضبطية القضائية المكلفة بالتنسيق في العملية تحت رقابتها[5]، وكذا يجوز للقاضي الذي أذن بالعملية أن يأمر في أي وقت بوقفها قبل إنتهاء المدة المحددة بموجب الفقرة 03 من المادة 706-83 من ق.إ.ج.ف[6].

وعليه إن توقف دور السلطة القضائية المختصة على المتابعة ومراقبة مراحل عملية التسرب عن بعد يعود إلى طبيعة التسرب في حد ذاته، لأنه يصعب تصور وكيل الجمهورية أو قاضي التحقيق خارج مكتبه متخفيًا بزي مجرم يبحث عن مرتكب الجريمة لمدة تفوق أربعة (04) أشهر، كما أنه لا يمكن لضابط الشرطة القضائية أن يكون مراقبًا للعملية وإنما مسؤولًا ومنسقًا فقط عليها، فهذا الأخير يعد بمثابة همزة وصل بين الضابط أو العون المتسرب الذي كلفه الضابط بالعملية والسلطة القضائية المختصة، كما أنه في الواقع التطبيقي البحث عن

---

[1]- سوماتي شريفة، **المتابعة الجزائية في جرائم الفساد في التشريع الجزائري**، رسالة ماجستير، فرع: القانون الجنائي، كلية الحقوق، جامعة الجزائر1، 2011/2010، ص-ص 78- 79.

[2]- عنتر أسماء، مرجع سابق، ص 248.

[3]- المادة 124/ 5 من القانون رقم: 25-14 السالف الذكر.

[4]- بولمكاحل أحمد، ليطوش دليلة، مرجع سابق، ص 1116.

[5]-Art 706-81 paragraphe 01 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que: « l'orsque les nécessités de l'enquête ou de l'instruction concernant l'un des crimes ou délits entrant dans le champs d'application des articles 706-73 et 706-73-1 le justifient, le procureur de la République ou après avis de ce magistrat, le juge d'instruction saisi peuvent autoriser qu'il soit procédé, sous leur contrôle respectif à une opération d'infiltration dans les conditions prévues par la présente section».

[6]-Art 706-83 paragraphe 03 du C.P.P.F (Loi n°2004-204 du 9 mars 2004) dispose que :«...Le magistrat qui a autorisé l'opération peut à tout moment ordonner son interruption avant l'expiration de la durée fixée».

الجاني يعد من مهام الشرطة القضائية، وعمليًا يستثنى رؤساء المجالس الشعبية البلدية ويرجع ذلك إلى كونهم شخصيات معروفة وهذا يتعارض مع الطابع السري للعملية.[1]

3- الجهات المختصة المخولة لها بتنفيذ إجراء التسرب:

أوكل المشرع الجزائري مهمة تنفيذ إجراء التسرب إلى ضباط أو أعوان الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب بموجب الفقرة الأولى من المادة 121 من ق.إ.ج، وقد جاءت هذه الأحكام مطابقة تقريبًا لما أقرته الفقرة 02 من المادة 706-81 من ق.إ.ج.ف[2].

وبناءً على ذلك فإن إجراء التسرب يتم تحت إشراف ومتابعة ضابط الشرطة القضائية الذي يتولى على التنسيق بين الضابط أو العون المتسرب والسلطة القضائية التي أمرت بهذا الإجراء -وكيل الجمهورية أو قاضي التحقيق- من جهة، وتوجيه سلوك المتسرب وحمايته من أي خطر جسدي قد يتعرض له من جهة أخرى، وبصفته المسؤول عن عملية التسرب فإنه يقوم بتحضير المهمة وتنظيمها، والوحيد الذي تظهر هويته في الملف الإجرائي على الرغم من عدم قيامه بعملية التسرب، كما يمكن سماعه بوصفه كشاهد عن العملية.[3]

ويتمتع بصفة المتسرب حسب ما ورد في المادة 121 من ق.إ.ج، ضباط الشرطة القضائية الذين ورد ذكرهم في المادة 23 من ق.إج.ج[4]، ويستثنى من هؤلاء لإعتبارات ميدانية

---

[1]- عنتر أسماء، مرجع سابق، ص 249.

[2]-Art 706-81 paragraphe 02 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que: « L'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, a surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprés de ces personnes, comme un de leurs coauteurs, complices ou receleurs ou comme une victime, un tiers mandaté par cette dernière ou toute personne intéressée à la commission de l'infraction».

ترجمتها:

تنص الفقرة 02 من المادة 706-81 من ق.إ.ج.ف على أن: "الإجراء الذي يقوم به الضابط أو عون الشرطة القضائية مخول بشكل خاص وفقًا لشروط يحددها مرسوم، ويتصرف تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، وذلك من خلال مراقبة أشخاص يشتبه في إرتكابهم جناية أو جنحة، عبر التظاهر أمام هؤلاء الأشخاص بأنه فاعلًا أصليًا معهم أو شريكًا لهم أو مخفيًا لمتحصلات الجريمة، أو في صورة ضحية أو طرف ثالث مفوض من هذه الأخيرة، أو أي شخص له مصلحة في إرتكاب الجريمة".

[3]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، مرجع سابق، ص 271.

[4]- تنص المادة 23 من القانون رقم: 25-14 السالف الذكر على أن: "يتمتع بصفة ضابط الشرطة القضائية:

1- رؤساء المجالس الشعبية البلدية؛

2- ضباط الدرك الوطني؛

3- الموظفون التابعون للأسلاك الخاصة للمراقبين، ومحافظي، وضباط الشرطة للأمن الوطني؛

4- ضباط الصف الذين أمضوا في سلك الدرك الوطني ثلاث (03) سنوات على الأقل وتم تعيينهم بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل، بعد موافقة لجنة خاصة؛=

رؤساء المجالس الشعبية البلدية، بالإضافة إلى أعوان ضباط الشرطة القضائية الذين ورد ذكرهم في المادة 29 من نفس القانون[1].

كما أشار المشرع الجزائري وفقًا للمادتين 122 و123 من ق.إ.ج.ج[2] على إمكانية تسخير أشخاص آخرين للمساعدة في هذه العملية والذين يعتبرون متسربين، وهو كل شخص يراه ضابط الشرطة القضائية القائم بتنسيق عملية التسرب مفيدًا وضروريًا للإستعانة به في تنفيذ المهمة المنوطة به، وهذا دائمًا تحت الرقابة القضائية.

ولم يشترط صفة معينة في الشخص المساعد، فيمكن أن يكون من عامة الناس الذي بوسعه الإندماج والإختلاط بمختلف فئات المجتمع، وهو ما قد لا يكون متاحًا بسهولة للعاملين في أجهزة الأمن لإعتبارات المتعلقة بوظائفهم، ولا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية المتسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات وذلك تحت طائلة العقوبات الجزائية التي حددتها المادة 125 من من ق.إ.ج.ج[3]، وقد يكون الشخص المسخر لعملية التسرب من التقنيين أو الفنيين أو المخبريين الذي يستعين بهم الضابط أو العون المتسرب لمساعدته في عمله[4].

= 5- الموظفون التابعون للأسلاك الخاصة للمفتشين ومحققي وحفاظ وأعوان الشرطة للأمن الوطني الذين أمضوا ثلاث (03) سنوات على الأقل بهذه الصفة والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية، بعد موافقة لجنة خاصة؛

6- ضباط وضباط الصف التابعون للمصالح العسكرية للأمن الذين تم تعيينهم خصيصًا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل؛

7- المتصرفون الإداريون في الشؤون البحرية وقادة الوحدات العائمة التابعون للمصلحة الوطنية لحرس السواحل، في حدود صلاحياتهم المنصوص عليها في التشريع والتنظيم الساريي المفعول؛

8- مفتشو الملاحة والعمل البحري وأعوان حرس السواحل التابعون للمصلحة الوطنية لحرس السواحل، الذين قضوا في الخدمة بهذه الصفة ثلاث (03) سنوات على الأقل، وعينوا بموجب قرار مشترك بين وزير الدفاع الوطني ووزير العدل، بعد رأي اللجنة الخاصة المذكورة في هذه المادة، في حدود صلاحياتهم المنصوص عليها في التشريع والتنظيم الساريي المفعول.

تحدد تشكيلة اللجنة المنصوص عليها في هذه المادة وتسييرها عن طريق التنظيم".

[1]- تنص المادة 29 من القانون رقم: 25-14 السالف الذكر على أن:" يعد من أعوان الضبط القضائي موظفو مصالح الشرطة، وذوو الرتب في الدرك الوطني، والدركيون، ومستخدمو المصالح العسكرية للأمن، ومفتشو الملاحة والعمل البحري، وكذا أعوان حرس السواحل التابعون للمصلحة الوطنية لحرس السواحل، الذين ليست لهم صفة ضابط الشرطة القضائية".

[2]- تنص المادة 122 من القانون رقم: 25-14 السالف الذكر على أن: "يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريرًا مسبقًا، يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب وكذا الأشخاص المسخرين طبقًا للمادة 123 أدناه".

تنص المادة 123 من القانون رقم: 25-14 السالف الذكر على أن: "يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض، دون أن يكونوا مسؤولين جزائيًا".

[3]- عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**،مرجع سابق، ص-ص 270-271.

[4]- وداعي عزالدين، **التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن**، كلية الحقوق والعلوم السياسية، جامعة عبدالرحمن ميرة-بجاية، المجلة الأكاديمية للبحث القانوني، مجلد16، عدد02، 2017، الجزائر، ص 212.

الفرع الثالث: الحماية القانونية المقررة للمتسرب

سنتناول الحماية الجزائية لهوية المتسرب، وإعفائه من المسؤولية الجزائية، بالإضافة إلى ضرورة وقف العملية في ظروف تضمن سلامته، مع إبقاء إذن التسرب خارج الملف، وعدم جواز الإستماع إليه كشاهد.

أولًا: الحماية الجزائية لهوية المتسرب

تتمثل الحماية الجزائية لهوية المتسرب، في إستعماله لهوية مستعارة مع توقيع العقوبة على كل من يكشف عن هويته الحقيقية كما يلي:

1- إستعمال الهوية المستعارة للمتسرب:

عملية التسرب ينبغي أن تتم بكل سرية نظرًا للخطر الذي يمكن أن يتعرض له الضابط أو العون المتسرب، وتجسيدًا لهذه السرية أقر المشرع الجزائري له حماية خاصة ما يسمح بالحفاظ على أمنه وسلامته طبقًا للفقرة 02 من المادة 121 من ق.إ.ج.ج[1]، ويتحقق ذلك من خلال تمكين الضابط أو العون المتسرب من إستعمال هوية مستعارة بدلًا من هويته الحقيقية، وذلك لضمان حمايته من إنكشاف أمره من قبل الجماعة الإجرامية التي تمكن من التوغل داخلها، وذلك حماية له من كل إنتقام أو تعدي على حياته أو سلامته الجسدية.

ويمنع على الضابط أو العون المتسرب الكشف عن هويته الحقيقية لأي شخص طيلة عملية التسرب، حتى ولو كان هذا الشخص من ضباط أو أعوان الشرطة القضائية، ماعدا ضابط الشرطة القضائية المنسق للعملية والقاضي الذي رخص بإجرائها، في أي مرحلة من مراحل الإجراءات[2]، لأن الكشف عن الهوية سيتسبب في إفشال عملية التسرب التي تسعى إلى إلقاء القبض على الجناة، كما أن سيعرض الضابط أو العون المتسرب مكشوف الهوية إلى الخطر[3].

---

[1]- تنص المادة 2/121 من القانون رقم: 25-14 السالف الذكر على أن: "يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة..."

[2]- تنص 1/125 من القانون رقم: 25-14 السالف الذكر على أن: "لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة، في أي مرحلة من مراحل الإجراءات"، وهذه الأحكام جاءت مطابقة لما قررته الفقرة الأولى من المادة 706-84 من ق.إ.ج.ف كالآتي:

Art 706-84 paragraphe 01 du C.P.P. F (Loi n°2004-204 du 9 mars 2004 - art. 1 JORF 10 mars 2004 en vigueur le 1er octobre 2004) dispose que: « L'identité réelle des officiers ou agents de police judiciaire ayant effectué l'infiltration sous une identité d'emprunt ne doit apparaître à aucun stade de la procédure».

[3]- حاحة عبد العالي، **الآليات القانونية لمكافحة الفساد الإداري في الجزائر**، أطروحة الدكتوراه علوم، تخصص قانون عام، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر-بسكرة، 2013/2012، ص 274.

إلا أن المشرع الجزائري لم يحدد كيفية الحصول على الهوية المستعارة للضابط أو العون المتسرب، وهل بإمكان أن تكون مدعمة بوثائق تثبتها، فعدم تنظيم هذه العملية سيستصعب من إثبات المتسرب لهويته بموجب وثائق إدارية، لبعث الإطمئنان في نفوس المنظمة الإجرامية.[1]

كان هذا الفراغ التشريعي قائمًا في ظل الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم السالف الذكر، الذي يتمثل في غياب تنظيم قانوني واضح لكيفية الحصول على الهوية المستعارة والوثائق التي تثبتها، غير أن هذا الفراغ ظل قائمًا حتى بعد إلغاء الأمر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، ما يدل على أن المشرع الجزائري لم يتدارك هذا النقص، وفي المقابل يلاحظ أن المشرع الفرنسي من خلال تعديله لقانون الإجراءات الجزائية بموجب القانون رقم 2025-532 السالف الذكر قام بتعديل المادة 706-81 بتعزيز الحماية القانونية للضابط أو للعون المتسرب من خلال الإقرار بإمكانية إستخدام وسائل تقنية تسمح له بتغيير صوته أو مظهره الجسدي[2] عند إستعمال الهوية المستعارة.

2- تجريم الكشف عن الهوية الحقيقية للمتسرب:

أقر المشرع الجزائري العقوبات الجزائية لكل من كشف عن الهوية الحقيقية للضابط أو للعون المتسرب بموجب المادة 125 من ق.إ.ج.ج، وذلك ضمانًا لحماية سلامة وأمن المتسرب وعدم تعريضه للخطر، إذ يعاقب بالحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة من مائتي ألف 200.000 دج إلى خمسمائة ألف 500.000 دج، لكل من يكشف هوية ضابط أو عون الشرطة القضائية المتسرب، حتى ولو لم يترتب عن هذا الكشف أية أضرار للمتسرب، وأقر المشرع الفرنسي بموجب الفقرة 02 من المادة 706-84 من ق.إ.ج.ف عقوبات تصل إلى السجن لمدة خمسة (05) سنوات وغرامة تقدر بخمس وسبعون ألف 75.000 يورو[3].

وقد يؤدي الكشف عن الهوية الحقيقية للضابط أو للعون المتسرب إلى الإعتداءات جسدية في أعمال العنف أو الضرب أو الجرح على هؤلاء المتسربين أو أزواجهم أو أبنائهم أو أصولهم المباشرين، كما قد يؤدي إلى وفاة أحد هؤلاء الأشخاص، أقر المشرع الجزائري عقوبات مشددة لكل حالة على النحو الآتي:

[1]- أومدور رجاء، مرجع سابق، ص180.

[2] - Art 706-81 paragraphe 02 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que: « … L'officier ou l'agent de police judiciaire est à cette fin autorisé à faire usage d'une identité d'emprunt, y compris en faisant usage d'un dispositif permettant d'altérer ou de transformer sa voix ou son apparence physique …»

[3]-Art 706-84 paragraphe 02 du C.P.P.F (Loi n°2004-204 du 9 mars 2004 - art. 1 JORF 10 mars 2004 en vigueur le 1er octobre 2004) dispose que: « La révélation de l'identité de ces officiers ou agents de police judiciaire est punie de cinq ans d'emprisonnement et de 75 000 € d'amende»

الحالة الأولى: إذا تسبب الكشف عن هوية الضابط أو العون المتسرب في أعمال العنف أو الضرب أو الجرح على هؤلاء المتسربين أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس (05) سنوات إلى عشر (10) سنوات والغرامة من خمسمائة ألف 500.000 دج إلى مليون 1.000.000 دج، ويعاقب المشرع الفرنسي على مثل هذه الحالة بعقوبة قد تصل إلى السجن لمدة سبع (07) سنوات وغرامة قدرها مائة ألف 100.000 يورو[1].

الحالة الثانية: إذا أدى الكشف عن هوية الضابط أو العون المتسرب في وفاة أحد هؤلاء الأشخاص، فقد أقر المشرع الجزائري العقوبة تتمثل في الحبس من عشر (10) سنوات إلى عشرين (20) سنة والغرامة من مليون 1.000.000 دج إلى مليوني 2.000.000 دج، دون الإخلال عند الإقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات الجزائري، أما المشرع الفرنسي يعاقب على هذه الحالة بالسجن لمدة عشر (10) سنوات وغرامة تقدر بمائة وخمسون ألف 150.000 يورو، دون الإخلال عند الإقتضاء بتطبيق أحكام الإعتداءات على حياة الفرد في الفصل الأول من الباب الثاني من الكتاب الثاني[2].

يتعلق الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات الجزائري المشار إليه بتطبيق أحكام الجنايات والجنح المرتكبة ضد الأشخاص، وهو ما يعني البحث في قصد الذي يكشف هوية ضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب، فإذا كان يهدف من وراء فعله إلى إلحاق الأذى بالشخص المتسرب فإنه يعتبر أيضًا شريكًا في تلك الجريمة سواء كانت عنفًا أو قتلًا إلى جانب جنحة الكشف عن هوية المتسرب، وأما إذا كان فعل الكشف ناجمًا عن تهاون ودون قصد فإنه في حالة وقوع أعمال العنف أو القتل فإنه يعتبر مرتكبًا لجريمة الضرب أو الجرح غير العمد أو القتل غير العمد، وهو ما لا يمنع من متابعة الفاعل الأصلي بالجرم العمد الذي إرتكبه سواء كان ضربًا أو قتلًا.[3]

لم يقتصر المشرع الجزائري في توفير الحماية القانونية على ضباط أو أعوان الشرطة القضائية المباشرين لعملية التسرب، بل وسع نطاق هذه الحماية لتشمل أفراد عائلة المتسرب، فتتضاعف العقوبات إذا تسبب الكشف في حدوث أي ضرر له أو لزوجه أو أبنائه أو أصوله المباشرين، وإذا كان الضحايا من أقارب الشخص المتسرب غير المذكورين صراحة في نص

[1]-Art 706-84 paragraphe 03 du C.P.P.F (Loi n°2004-204 du 9 mars 2004 - art. 1 JORF 10 mars 2004 en vigueur le 1er octobre 2004) dispose que: « Lorsque cette révélation a causé des violences, coups et blessures à l'encontre de ces personnes ou de leurs conjoints, enfants et ascendants directs, les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende».

[2]-Art 706-84 paragraphe 04 du C.P.P.F (Loi n°2004-204 du 9 mars 2004 - art. 1 JORF 10 mars 2004 en vigueur le 1er octobre 2004) dispose que: « Lorsque cette révélation a causé la mort de ces personnes ou de leurs conjoints, enfants et ascendants directs, les peines sont portées à dix ans d'emprisonnement et à 150.000 euros d'amende, sans préjudice, le cas échéant, de l'application des dispositions du chapitre Ier du titre II du livre II du code pénal».

[3]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 200.

المادة 125 من ق.إ.ج.ج، فيمكن الإستناد إلى نفس الوصف الجزائي الوارد في قانون العقوبات، متى توفرت الشروط الموضوعية.

ومن خلال ما سبق، يلاحظ أن المشرع الجزائري لم يوسع من مجال الحماية إلى الأشخاص الذين يتم تسخيرهم في عملية التسرب، على الرغم من كون هؤلاء قد أفادهم بالإعفاء من المتابعة الجزائية مثلهم مثل الضابط أو العون المتسرب.[1]

ويلاحظ أيضًا أن المشرع إكتفى بتشديد العقوبة المقررة للشخص الذي يكشف عن هوية منفذي عملية التسرب وفقاً لجسامة الضرر الناتج، ولم يدرج العقوبة المخصصة للشخص المسخر بغرض إتمام عملية التسرب، لأن الشخص المسخر قد يعرف ضابط أو عون الشرطة القضائية المتسرب معرفة جيدة كما قد يعرف أسرته وأصوله وفروعه، مما يلزم إدراج العقوبة وتشديدها على هذا الشخص.[2]

وكان هذا الفراغ التشريعي قائمًا في ظل الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم السالف الذكر، إلا أنه إستمر رغم إلغاء هذا الأمر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، لذا حبذا لو يتداركه المشرع الجزائري من خلال تدخلات تشريعية كفيلة بمعالجة هذا القصور.

ثانيًا: الإعفاء من المسؤولية الجزائية

تماشيًا مع خصوصية عملية التسرب، أجاز المشرع الجزائري لضباط وأعوان الشرطة القضائية المرخص لهم بتنفيذ العملية وكذا الأشخاص المسخرين لذلك إرتكاب أفعال مخالفة للقانون تدل على أنهم منخرطين في إرتكاب الجريمة طبقًا للفقرة الأولى من المادة 123 من ق.إ.ج.ج، وعليه فإن هذه الأفعال هي في الأصل أفعال معاقب عليها ولكن أضفى عليها المشرع صفة الشرعية إذا دعت ضرورات التحري أو التحقيق في ذلك[3]، ومن خلال نص المادة 706-82 من ق.إ.ج.ف[4] نجد المشرع الفرنسي هو الآخر أعفى ضباط وأعوان الشرطة القضائية

[1]- ركاب أمينة، مرجع سابق، ص 139.

[2]- وداعي عزالدين، مرجع سابق، ص 215.

[3]- ركاب أمينة، مرجع سابق، ص 133.

[4]-Art 706-82 du C.P.P.F (Loi n°2004-204 du 9 mars 2004 - art. 1 JORF 10 mars 2004 en vigueur le 1er octobre 2004) dispose que: « les officiers ou agents de police judiciaire autorisés a procéder a une opération d'infiltration peuvent, sur l'ensemble du territoire national, sans être pénalement responsables de ces actes:

1° Acquérir, détenir, transporter, livrer ou délivrer des substances, biens, produits, documents ou informations tirés de la commission des infractions ou servant à la commission de ces infractions,

2° Utiliser ou mettre à disposition des personnes se livrant à ces infractions des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication.

L'exonération de responsabilité prévue au premier alinéa est également applicable, pour les actes commis à seule fin de procéder à l'opération d'infiltration, aux personnes requises par les officiers ou agents de police judiciaire pour permettre la réalisation de cette opération».

المرخص لهم بعملية التسرب وكذا الأشخاص الذين يتم إستدعاؤهم من طرف الضباط أو أعوان الشرطة القضائية للمساعدة في إنجاز هذه العملية من المسؤولية الجزائية.

وتتمثل الأفعال التي يجوز القيام بها في إقتناء أو حيازة أو نقل أو تسليم أو إعطاء، مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من إرتكاب الجرائم أو مستعملة في إرتكابها، وأيضًا إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الإتصال.[1]

ويتضح لنا من خلال طبيعة هذه الأفعال أنها تستوجب المشاركة الإيجابية كحيازة متحصلات الجريمة أو وسائل إرتكابها، وهذه الأفعال لها تأثير على المسؤولية الجزائية إلا أن المشرع الجزائري أعفى القائمين على عملية التسرب من هذه المسؤولية وذلك بنصه الصريح في المادة 123 من ق.إ.ج.ج على أن: "دون أن يكونوا مسؤولين جزائيًا"، ويمتد هذا الإعفاء لظروف أمنية للمتسرب حتى بعد إنقضاء المهلة المحددة في رخصة التسرب، وفي حالة عدم تمديدها أو في حالة تقرير وقف العملية، بشرط ألا يتجاوز ذلك مدة أربعة (04) أشهر سواء من تاريخ إنقضاء المدة المحددة في الإذن أو من تاريخ صدور قرار وقفها من قبل القاضي الذي رخص بإجرائها.[2]

والهدف من إعطاء للمتسرب لهاته الصلاحيات التي يقوم بموجبها بتقديم العون والدعم للجماعة الإجرامية المعنية بعملية التسرب، هو بهدف كسب ثقتهم وإزالة كافة الشكوك وراء الغاية الحقيقية والهوية الحقيقية للضابط أو للعون المتسرب أو للشخص المسخر، لكن في حدود ما تستوجه العملية.[3]

أما الجرائم التي يرتكبها خارج الأفعال المنصوص عليها على سبيل الحصر في المادة 123 من ق.إ.ج.ج، فإنه يعاقب عليها طبقًا للنصوص القانونية السارية المفعول، ونفس المبدأ منصوص عليه في المادة 706-81 من ق.إ.ج.ف الذي لا يسمح للعون أو الضابط المتسرب أثناء العملية التحريض على إرتكاب الجرائم[4].

لذا حبذا لو يتدخل المشرع الجزائري لتحديد الجرائم التي يجوز للمتسرب إرتكابها في إطار عملية التسرب وفقاً للضوابط، مع إعفاءه من المسؤولية الجزائية عن الأفعال التي لم يأذن

---

[1]- المادة 123 من القانون رقم: 25-14 السالف الذكر.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 123.

[3]- ركاب أمينة، مرجع سابق، ص 136.

[4]-Art 706-81 paragraphe 02 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que : «...et à commettre si nécessaire les actes mentionnés à l'article 706-82. A peine de nullité, ces actes ne peuvent constituer une incitation ayant déterminé la commission d'infractions».

ترجمتها:

تنص الفقرة الثانية من المادة 706-81 من ق.إ.ج.ف على أن:"...القيام عند الإقتضاء بإرتكاب الأفعال المشار إليها في المادة 706-82. ولا يجوز أن تشكل هذه الأفعال تحريضًا على إرتكاب الجرائم".

له بإرتكابها في إطار عملية التسرب، متى ثبت أنه إضطر إلى إرتكابها لضمان نجاح عملية التسرب، بالنظر إلى الأهداف الهامة التي قد تتحقق من نجاحها.[1]

ثالثًا: توقيف العملية في ظروف تضمن سلامة المتسرب

إذا تقرر وقف عملية التسرب بموجب أمر من السلطة المختصة بمنح الإذن بمباشرتها متى رأت أنه لا جدوى من إستمرارها، أو عند إنقضاء المهلة المحددة قانونًا أو في حالة عدم تمديدها، ولم يتمكن الضابط أو العون المتسرب من الإنسحاب بشكل آمن فلا يحول له من مواصلة نشاطاته المذكورة في المادة 123 من ق.إ.ج للوقت الضروري الكافي، حتى يتمكن من توقيف نشاطه والإنسحاب في ظروف تضمن أمنه دون أن يكون مسؤولًا جزائيًا، على ألا يتجاوز ذلك مدة أربعة (04) أشهر، ولكن بشرط إخطار القاضي المرخص بإجراء عملية التسرب في أقرب الآجال، وإذا إنقضت مهلة أربعة (04) أشهر ولم يتمكن الضابط أو العون المتسرب من توقيف نشاطه بشكل آمن، يمكن لهذا القاضي إصدار ترخيص آخر لتمديد له بمواصلة عملية التسرب لمدة أربعة (04) أشهر على الأكثر.[2]

غير أن التساؤلات التي تطرح في هذا السياق، هل تعد مهلة ثمانية (08) أشهر كافية دائمًا لضمان أمن المتسرب وسلامته؟ وما الموقف القانوني في حال تعذر عليه توقيف نشاطه في ظروف تضمن له سلامته، لما قد يشكله هذا التوقف من خطر على حياته؟ وهل تترتب مسؤوليته الجزائية في حال إستمر في نشاطه بعد إنقضاء مهلة ثمانية (08) أشهر؟

يمكن القول أنه إذا كان المشرع قد أعطى للقاضي مصدر الإذن بعملية التسرب الحق في تمديد عملية التسرب إلى عدد غير محدود من المرات وفقًا للمادة 124 من ق.إ.ج.ج، كان عليه أن لا يقيده في العامل الزمني فيما يتعلق بتأمين سلامة وأمن المتسرب، لأن في ذلك خطورة على حياة المتسرب الذي وهب نفسه لتنفيذ مهمة أذن بها القانون.[3]

يعد من الأنسب أن يتدارك المشرع الجزائري هذا القصور التشريعي من خلال إعادة النظر في المادة 126 من ق.إ.ج.ج، بفتح إمكانية تمديد المدة الزمنية لإجراء التسرب بما يتيح للمتسرب مواصلة نشاطه متى إقتضت الضرورة ذلك شريطة أن يتم هذا التمديد في ظروف تضمن أمنه وسلامته وتحت رقابة الجهة القضائية المختصة التي أصدرت الإذن بالتسرب، ويلاحظ أن هذا الفراغ التشريعي لم يطرأ حديثًا بل كان قائمًا في ظل الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم السالف الذكر، إلا أنه إستمر رغم إلغاء هذا الأمر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، مما يبرز الحاجة الملحة لتدخل تشريعي يعالج هذا القصور.

---

[1]- ركاب أمينة، مرجع سابق، ص 135.

[2]- المادة 126 من القانون رقم: 25-14 السالف الذكر.

[3]- عنتر أسماء، مرجع سابق، ص 273.

رابعًا: إبقاء الإذن بالتسرب خارج الملف

تنص الفقرة الأخيرة من المادة 124 من ق.إ.ج.ج على أن: "تودع الرخصة في ملف الإجراءات بعد الإنتهاء من عملية التسرب"، وهكذا فقد حرص المشرع الجزائري على ضرورة إبقاء الإذن بإجراء عملية التسرب خارج ملف الإجراءات، أي لا يتم إدراجه في ملف القضية وقت تحريره أو أثناء تنفيذ العملية إلى حين الإنتهاء من العملية ثم يضاف إلى الملف، وذلك حفاظًا على حياة وأمن الضابط أو العون المتسرب وعائلته وعدم تمكين الغير من معرفة هويته الحقيقية، وبهذا يكون المشرع الجزائري قد سار على نهج المشرع الفرنسي الذي أخذ بنفس التدبير في الفقرة 04 من المادة 706-83 من ق.إ.ج.ف[1].

خامسًا: عدم جواز سماع المتسرب كشاهد

من بين صور الحماية التي أقرها المشرع الجزائري عدم إلزام الضابط أو العون المتسرب بالإدلاء بشهادته، بل يجوز فقط سماع ضابط الشرطة القضائية الذي تجرى العملية تحت مسؤوليته دون سواه بوصفه شاهدًا عن العملية، وبمفهوم المخالفة لا يجوز سماع ضابط أو عون الشرطة القضائية المتسرب كشاهد فهؤلاء تظل هويتهم الحقيقية سرية بالنسبة للجميع حفاظًا على حياتهم وحياة أسرتهم، طبقًا للمادة 127 من ق.إ.ج.ج التي تنص على أن: "يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدًا عن العملية"، وهذا ما يتطابق مع الفقرة الأولى من المادة 706-86 من ق.إ.ج.ف[2].

وما يلاحظ في هذا الصدد، أجاز سماع ضابط الشرطة القضائية المكلف بتنسيق العملية بوصفه شاهد على العملية، في حين أنه مجرد ناقل لشهادة المتسرب بناء على التقرير الذي تلقاه منه، لذلك فما الجدوى من الشهادة وفي المواجهة بينه وبين المتهمين إن لم يعاين أي فعل هو بنفسه، فقد تخفى عليه بعض الأمور التي قد تلعب دورًا مهما في التحري والتحقيق، حتى لو كان المبرر هو الحماية القانونية المقررة للمتسرب، فهذا الأخير هو الأدرى بكامل تفاصيل ومجريات وقائع العملية.

---

[1]- Art 706-83 paragraphe 04 du C.P.P.F (Loi n°2004-204 du 9 mars 2004 - art. 1 JORF 10 mars 2004 en vigueur le 1er octobre 2004) dispose que: « L'autorisation est versée au dossier de la procédure après achèvement de l'opération d'infiltration».

ترجمتها:

تنص الفقرة 04 من المادة 706-83 من ق.إ.ج.ف على أن :"يضاف الإذن إلى ملف الإجراءات بعد الإنتهاء من عملية التسرب".

[2]-Art 706-86 paragraphe 01 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que: « l'officier de police judiciaire sous la responsabilité duquel se déroule l'opération d'infiltration peut seul être entendu en qualité de témoin sur l'opération».

ترجمتها:

تنص الفقرة الأولى من المادة 706-86 من ق.إ.ج.ف على أن: "يعد ضابط الشرطة القضائية الذي تنفذ العملية تحت مسؤوليته، الشخص الوحيد الذي يمكن سماعه كشاهد بشأن هذه العملية".

أما المشرع الفرنسي فقد توصل إلى الحل حينما أجاز مواجهة الضابط أو العون المتسرب أثناء مجريات التحقيق الجنائي بوقائع القضية وعناصر الوسط المتسرب فيه وذلك عن طريق إستعمال وسائل التقنية[1]، توفر له الحماية من خلال عدم التعرف على هويته، وقد يكون إدلاء لشهادته داخل غرفة مهيأة ومخصصة لهذا الغرض.[2]

وبموجب التعديل الذي أدخل على قانون الإجراءات الجزائية الفرنسي بموجب القانون رقم: 2025-532 السالف الذكر، يلاحظ أن المشرع الفرنسي بعدما كان يجيز سماع الشاهد عن بعد بإستخدام تقنية تتيح ذلك أو إستجوابه من قبل محاميه عبر الوسيلة نفسها، قد أضاف من خلال التعديل بإلزام الحفاظ على هوية الشاهد مجهولة بكافة الوسائل الممكنة، بما في ذلك إستخدام وسيلة تقنية تتيح من تغيير صوته أو مظهره الجسدي.[3]

---

[1]- إعتمد المشرع الفرنسي تقنية المواجهة عن طريق الصوت، حيث لا يمكن التعرف على الصوت ولا هوية الشاهد، ويتم إستعمال وسائل تقنية توفر له الحماية مثل إستعمال أجهزة وبرامج تغير نبرات الصوت أو إستعمال الشاشة الإلكترونية، وهذا أفضل إجراء إتخذه المشرع الفرنسي في سماع شهادة المتسرب، لأن ضابط الشرطة القضائية المنسق لم يباشر عملية التسرب بنفسه، وبالتالي قد تخفى عليه بعض الأمور التي قد تلعب دورًا مهما في التحقيق القضائي ويكون الضابط أو العون المتسرب أكثر علمًا بها. إلى جانب هذه التقنية فإن المشرع الفرنسي لا يجيز الحكم بالإدانة بالإعتماد على الدليل المستمد من شهادة المتسرب، لأن هويته تبقى مجهولة، وهذا تماشيًا مع ما جاءت به المحكمة الأوربية لحقوق الإنسان في مادتها الثامنة، وللمزيد من التفصيل، ينظر: نبيلة قيشاح، مرجع سابق، ص-ص 196-197.

[2]- لواتي فوزي، **التحقيق في جرائم المخدرات على ضوء أساليب التحري الخاصة**، رسالة الماجستير، فرع القانون الجنائي، كلية الحقوق، جامعة الجزائر1، 2015/2014، ص 81.

[3] - Art 706-86 paragraphe 02 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que: « Toutefois, s'il ressort du rapport mentionné au troisième alinéa de l'article 706-81 que la personne mise en examen ou comparaissant devant la juridiction de jugement est directement mise en cause par des constatations effectuées par un agent ayant personnellement réalisé les opérations d'infiltration, cette personne peut demander à être confrontée avec cet agent en faisant usage du dispositif technique prévu à l'article 706-61 ou d'un dispositif permettant d'altérer ou de transformer sa voix ou son apparence physique. Les questions posées à l'agent infiltré à l'occasion de cette confrontation ne doivent pas avoir pour objet ni pour effet de révéler, directement ou indirectement, sa véritable identité ».

- Art 706-61 du C.P.P.F (Modifié par Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic) dispose que: « La personne mise en examen ou renvoyée devant la juridiction de jugement peut demander à être confrontée avec un témoin entendu en application des dispositions de l'article 706-58 par l'intermédiaire d'un dispositif technique permettant l'audition du témoin à distance ou à faire interroger ce témoin par son avocat par ce même moyen. L'anonymat du témoin est préservé par tout moyen, y compris par l'utilisation d'un dispositif technique permettant d'altérer ou de transformer sa voix ou son apparence physique.Si la juridiction ordonne un supplément d'information aux fins d'audition du témoin, ce dernier est entendu soit par un juge d'instruction désigné pour exécuter ce supplément d'information, soit, si l'un des membres de la juridiction a été désigné pour exécuter cette audition, en utilisant le dispositif technique prévu par l'alinéa précédent ».

ترجمة المادتين:

تنص الفقرة 02 من المادة 706-86 من ق.إ.ج.ف على أن: " غير أنه إذا تبين من التقرير المشار إليه في الفقرة الثالثة من المادة 706-81، أن الشخص المتابع قضائيًا أو الماثل أمام جهة الحكم قد وجهت إليه إتهامات مباشرة إستنادًا إلى معاينات قام بها عون نفذ شخصيًا عمليات التسلل، فإنه يمكن لهذا الشخص أن يطلب مواجهته مع ذلك العون، بإستخدام الوسيلة التقنية المنصوص عليها في المادة 706-61، أو بإستخدام وسيلة تتيح تغيير صوته أو مظهره الجسدي.=

لذا حبذا لو سار المشرع الجزائري على النهج ذاته، لاسيما بعد إلغائه للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية السالف الذكر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، حيث أعاد من خلال هذا الأخير إدراج تقنية المحادثة المرئية عن بعد، ووسع من نطاق الحماية بعدما كانت مقتصرة في السابق على حماية الشهود والخبراء والضحايا فقط، جعلها تشمل أيضًا حماية المدعين المدنيين والأطراف المدنية والمبلغين، كما شمل هذا التوسيع الجرائم التي تطبق فيها هذه الحماية، لذلك فمن المستحسن أن يعتمد المشرع الجزائري نفس التوجه فيما يتعلق بسماع شهادة المتسرب بمنحه مستوى مماثلًا من الحماية، وأن لا يقتصر الأمر على الضابط المنسق للعملية.

المطلب الثاني: الإجراءات ذات الطابع الشخصي في مواجهة الجرائم الماسة بالمستند الإلكتروني

يعتبر إعتراض المراسلات الإلكترونية وتسجيل الأصوات وإلتقاط الصور، ومراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، من أفضل الإجراءات التقنية الضرورية لتعقب الأدلة في هذه الجرائم والحفاظ عليها، وإلى جانب ذلك فإن المحافظة على المستند الإلكتروني تقتضي منح السلطة القضائية المختصة صلاحية التحفظ الفوري على ما قد يتضمنه الجهاز الإلكتروني من معطيات يمكن أن تشكل دليلًا وكذلك الأمر بتقديم المعطيات المعلوماتية المتعلقة بالمشترك، ويشترط لقبول الدليل لإثبات الجرائم أن تتوفر فيه شروط المشروعية والصحة، وأن يكون من الممكن الإعتماد عليه بوصفه حجة فيما يتضمنه من قوة إثباتية تؤكد إرتكاب الجريمة من قبل المتهم.[1]

الفرع الأول: الإجراءات المتعلقة بالمعطيات المتحركة

أدرج المشرع الجزائري إجراء إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور بمقتضى القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية، حيث أفرد فصلًا رابعًا تحت عنوان "في إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور" من الباب الثاني من الكتاب الأول، والذي

=ويشترط ألا يكون من أهداف أو نتائج الأسئلة الموجهة إلى العون المتسلل أثناء هذه المواجهة، الكشف عن هويته الحقيقية، سواء بشكل مباشر أو غير مباشر".

تنص الفقرة الأولى من المادة 706-86 من ق.إ.ج.ف على أن: " يجوز للشخص المتابع قضائيًا أو المحال أمام جهة الحكم أن يطلب مواجهته مع شاهد تم الإستماع إليه تطبيقًا لأحكام المادة 706-58، وذلك من خلال وسيلة تقنية تتيح سماع الشاهد عن بُعد، أو أن يطلب من محاميه إستجواب هذا الشاهد عبر الوسيلة نفسها. ويحافظ على سرية هوية الشاهد بكافة الوسائل، بما في ذلك إستخدام وسيلة تقنية تتيح تغيير صوته أو مظهره الجسدي. وفي حال قررت الجهة القضائية إجراء تحقيق تكميلي بغرض سماع الشاهد، يتم سماعه إما من قبل قاضي تحقيق يعين لتنفيذ هذا التحقيق التكميلي، أو إذا تم تعيين أحد أعضاء الجهة القضائية للقيام بهذه المهمة، بإستخدام الوسيلة التقنية المشار إليها في الفقرة السابقة".

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 267.

تضمن مواد تمتد من المادة 65 مكرر5 إلى المادة 65 مكرر10، ورغم إلغاء الأمر رقم: 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، بموجب القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية، فقد أبقى المشرع الجزائري على هذا الإجراء، وأعاد تنظيمه ضمن المواد من 114 إلى 119 المدرجة في الفصل الرابع من الباب الثاني من الكتاب الثاني.

1- تعريف إعتراض المراسلات الإلكترونية وتسجيل الأصوات وإلتقاط الصور:

أشار المشرع الجزائري إلى هذا الإجراء ضمن أساليب التحري الخاصة في قانون الإجراءات الجزائية بعنوان "في إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور"، دون تحديد مفهومه بدقة.

إلا أن يمكن تعريف إعتراض المراسلات بأنها: "عملية مراقبة سرية المراسلات السلكية واللاسلكية، في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات، حول الأشخاص المشتبه فيهم في إرتكابهم أو في مشاركتهم في إرتكاب الجريمة"[1]، والمقصود بالمراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية بموجب المادة 08 من القانون رقم: 2000-03 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية السالف الذكر بأنها: "كل تراسل أو إرسال أو إستقبال، لعلامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة، عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية"، فقد حدد المشرع الجزائري مفهوم المراسلات بموجب المادة 114 من ق.إ.ج.ج في الحالات التي تتم من خلال إستخدام وسائل الإتصال السلكية واللاسلكية فقط، وبذلك يكون قد تم إستبعاد المراسلات الورقية العادية والخطابات الخطية التي تتم عن طريق البريد.[2]

ويقصد بالتسجيل الصوتي: "تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص، في أماكن خاصة أو عمومية"[3]، أو "مراقبة المحادثة الهاتفية وتسجيلها، وكافة الإتصالات التي تتم بواسطة سلكي أو لاسلكي[4]"، ويقصد بإلتقاط الصور: "إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص"[5].

[1]- عبد الرحمان خلفي، مرجع سابق، ص 100.
[2]- حاحة عبد العالي، مرجع سابق، ص 260
[3]- الفقرة الأولى من المادة 114 من القانون رقم: 25-14 السالف الذكر.
[4]- حاحة عبد العالي، مرجع سابق، ص 261.
[5]- الفقرة الأولى من المادة 114 من القانون رقم: 25-14 السالف الذكر.

2- ضوابط إعتراض المراسلات الإلكترونية وتسجيل الأصوات وإلتقاط الصور:

إذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو بمناسبة التحقيق الإبتدائي بالخصوص في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، يسمح لضباط الشرطة القضائية إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية، ووضع الترتيبات التقنية دون موافقة المعنيين بغرض تسجيل الأصوات وإلتقاط الصور، بناءً على إذن مكتوب من طرف وكيل الجمهورية المختص إقليميًا، وفي حالة فتح تحقيق قضائي تتم بناء على إذن من قاضي التحقيق، وتحت المراقبة المباشرة للقاضي الآمر بها.[1]

ويسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو كان ذلك خارج المواعيد القانونية، وبغير علم أو رضا الأشخاص الذين لهم الحق على تلك الأماكن.[2]

ويجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب إلتقاطها والأماكن المقصودة السكنية أو غيرها، والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، ويجب أن يكون الإذن محدد لمدة أقصاها أربعة (04) أشهر قابلة للتجديد ضمن نفس الشروط الشكلية والزمنية إلى غاية إنتهاء مقتضيات التحري أو التحقيق القضائي.[3]

ونظرًا لأن العملية تقنية محضة، فقد أجاز القانون لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه، تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية، للتكفل بالجوانب التقنية للعمليات المذكورة أعلاه.[4]

وخول لضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص تحرير محضرًا عن كل عملية إعتراض وتسجيل للمراسلات، وكذا عن عمليات وضع الترتيبات التقنية وعملية الإلتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، وينبغي أن يذكر في المحضر المحرر تاريخ وساعة بدء العملية والإنتهاء منها.[5]

يصف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف، وترفق به الدعامة

[1]- المادة 1/114 و3 و4 من القانون رقم: 25-14 السالف الذكر.
[2]- المادة 2/114 من القانون رقم: 25-14 السالف الذكر.
[3]- المادة 116 من القانون رقم: 25-14 السالف الذكر.
[4]- المادة 117 من القانون رقم: 25-14 السالف الذكر.
[5]- المادة 118 من القانون رقم: 25-14 السالف الذكر.

الإلكترونية إذا طلبها وكيل الجمهورية، وتنسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الإقتضاء بمساعدة مترجم يسخر لهذا الغرض.[1]

يدرج مضمون المراسلات أو الصور أو المحادثات المعترضة والمفيدة في إظهار الحقيقة، وهذا إلى جانب الإحتفاظ بالتسجيل برمته وجعله في حرز مختوم لضمان سلامته، ولم يمنع القانون من أخذ النسخ الإحتياطية لذلك التسجيل تبقى مرفقة به من باب الإحتياط، إلا أن لم ينص القانون الجزائري على مصير السند المادي للتسجيل بخلاف قانون الإجراءات الجزائية الفرنسي الذي نص على تحطيمه بعد إنقضاء الدعوى العمومية نهائيًا، بينما المحاضر تبقى مدرجة بملف الدعوى.[2]

تتم جميع العمليات سابقة الذكر بدون المساس بالسر المهني، وإذا إكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببًا لبطلان الإجراءات العارضة.[3]

ثانيًا: مراقبة الإتصالات الإلكترونية

إستحدث المشرع الجزائري بموجب المادة 03 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر إجراء مراقبة الإتصالات الإلكترونية، واعتبرها إجراء يهدف إلى وضع الترتيبات التقنية وجمع وتسجيل محتوى الإتصالات الإلكترونية في حينها، وتطرق إلى ضوابط إجرائها في المادة 04 من نفس القانون.

1- المقصود بإجراء مراقبة الإتصالات الإلكترونية:

المراقبة الإلكترونية هو العمل الذي يقوم به المراقب بإستخدام التقنية الإلكترونية لجمع المعطيات والمعلومات عن المشتبه فيه، سواء أكان شخصًا أو مكانًا أو شيئًا حسب طبيعته مرتبط بالزمن التاريخ أو الوقت، لتحقيق غرض أمني أو لأي غرض آخر[4]، وقد عرفها المشرع الأمريكي في المادة 2510-4 من قانون الإتصالات الفيدرالي لسنة 1968 بأنها: "عملية الإستماع لمحتويات أسلاك أو أي إتصالات شفوية، عن طريق إستخدام جهاز إلكتروني أو أي جهاز آخر"[5]، وقد أغفل المشرع الجزائري عن تعريف المراقبة ولكنه عرف الإتصالات الإلكترونية بموجب الفقرة (و) من المادة 02 من القانون رقم: 09-04 المتضمن للقواعد

[1]- المادة 119 من القانون رقم: 25-14 السالف الذكر.

[2]- نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، مرجع سابق، ص 196.

[3]- المادة 115 من القانون رقم: 25-14 السالف الذكر.

[4]- محمود سعد عبد المجيد، مرجع سابق، ص 514.

[5]- نفس المرجع، ص 514.

الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر بأنها: "أي تراسل أو إرسال أو إستقبال، علامات أو إشارات، أو كتابات، أو صور، أو أصوات، أو معلومات مختلفة، بواسطة أي وسيلة إلكترونية".

إذا كان يقصد بالمراقبة والتجميع والتسجيل وضع الشيء تحت الملاحظة، وتسجيل ما يحدث في ظل جو من السرية والحذر بحيث يستحيل الإحساس بوجود المراقبة، فإن هذا المفهوم لا يختلف في نطاق الإتصالات الإلكترونية، كل ما في الأمر أنها تتم بواسطة إستخدام وسائل وأجهزة إلكترونية لتحقيق الغرض المحدد، وإفراغ النتيجة في ملف إلكتروني، وتحرير تقارير بناءً على هذه النتيجة.[1]

وما ينبغي الإشارة إليه أن المراقبة السرية الإلكترونية للإتصالات الإلكترونية ومن ضمنها المحادثات الهاتفية لا يمكن إعتبارها نوعًا من أنواع التفتيش، وذلك لأن المراقبة الإلكترونية ترد عن معطيات المرور -المعطيات المتعلقة بحركة السير- التي تتجسد هنا بالإتصالات الإلكترونية حال إجرائها دون تلك التي إنتهت وخزنت، في حين التفتيش إنما يرد فقط على المعطيات المعلوماتية المخزنة التي تتجسد هنا بالإتصالات الإلكترونية التي تمت وخزنت[2]، وقد أكد ذلك المجلس الأوروبي من خلال توصياته التي طالبت بالتفرقة بين مراقبة معطيات المتعلقة بالمرور وبين تفتيش وضبط المعطيات المعلوماتية المخزنة، وعليه لا تعد المراقبة الإلكترونية تفتيشًا بل هي إجراء خاص يبدأ من لحظة إلتقاط الإتصال الإلكتروني من خلال الأجهزة والتقنيات المعدة لهذا الغرض، وتنتهي بمجرد وصول المحادثة أو المراقبة إلى حيازة الجهة المراقبة[3].

وميزت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بين نوعين من المعطيات المعلوماتية التي يتم تجميعها محل الإعتراض، بين المعطيات المتعلقة بالمرور والمعطيات المتعلقة بالمحتوى، بالنسبة للنوع الأول فإن المادة الأولى من الإتفاقية قد عرفتها بأنها: "كل المعطيات التي تعالج الإتصالات التي تمر عن طريق النظام المعلوماتي، والتي يتم إنتاجها بواسطة هذا النظام بوصفه عنصرًا في سلسلة الإتصال، مع تعيين المعلومات التالية: أصل الإتصال، مقصد الإتصال أو الجهة المقصودة بالإتصال، خط السير، ساعة وتاريخ، حجم وفترة الإتصال، أو نوع الخدمة"، أما بالنسبة للنوع الثاني المتمثل في المعطيات المتعلقة بالمحتوى فإنه لم يأت تعريف لها في الإتفاقية لكنها تشير إلى المحتوى الإخباري للإتصال، بمعنى مضمون الإتصال أو الرسالة أو المعلومات المنقولة عن طريق الإتصال، فيما عدا المعطيات المتعلقة بالمرور.[4]

---

[1]- بوكر رشيدة، مرجع سابق، ص 337.

[2]- بن مكي نجاة، مرجع سابق، ص 231.

[3]- بلحسيني حمزة، مرجع سابق، ص 401.

[4]- هلالي عبد اللاه أحمد، مرجع سابق، ص- ص 249-250.

حيث أدرجت كل إجراء على حدة تحت عنوان خاص، فخصت تجميع حركة المعطيات بعنوان "التجميع في الوقت الفعلي لمعطيات المرور" في المادة 20 منها، والتي أجازت في فقرتها الأولى للدول الأطراف بتبني الإجراءات التشريعية وأي إجراءات أخرى تراها ضرورية تخول سلطاتها المختصة القيام بجمع أو تسجيل من خلال تطبيق الوسائل الفنية الموجودة على أرضها، أو إلزام مقدم الخدمة في حدود قدرته الفنية المتوافرة على جمع أو تسجيل من خلال تطبيق الوسائل الفنية في إقليم الدولة الطرف، أو التعاون مع السلطات المختصة ومساعدتها في جمع أو تسجيل بشكل فوري حركة سير المعطيات المرتبطة بإتصالات معينة في إقليم ذلك الطرف التي تم نقلها بواسطة المنظومة المعلوماتية.[1]

ويهدف هذا الإجراء الخاص بالتجميع في الوقت الفعلي للمعطيات المتعلقة بحركة السير الذي قد تقوم به السلطة المختصة في الدولة، أو ينفذه مقدمو الخدمة بناء على أوامر صادرة إليهم من السلطة المختصة بهذا الإجراء إلى تسهيل مهمة الجهات القائمة بجمع الأدلة.[2]

ويختلف إجراء التجميع في الوقت الفعلي للمعطيات المتعلقة بحركة السير عن إجراء التحفظ السريع على المعطيات المتعلقة بحركة السير الذي نصت عليه المادة 16 من الإتفاقية، في أن المعطيات في حالة التحفظ موجودة لدى مقدم الخدمة أي مخزنة بالمنظومة المعلوماتية أو في دعامة التخزين، بينما في حالة التجميع أو التسجيل فالمعطيات ليست مخزنة ويهدف هذا الإجراء إلى جمعها أو تسجيلها وقت مباشرة الإتصال وهذا ما عبرت عنه الإتفاقية بالوقت الفعلي أو الحقيقي، ولهذا فهو يحتاج إلى وسائل تقنية حديثة قد لا تتوفر لدى السلطة المختصة أو قد لا يكون بمقدورها القيام به، وعلى ذلك أسندت الإتفاقية القيام بإجراء التجميع أو التسجيل للسلطة المختصة في الدول لتقوم به بنفسها أو تنفذه من خلال مقدم الخدمة أو بمساعدته.[3]

ولا تعد الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 الإتفاقية الوحيدة التي نظمت هذا الإجراء، بل تطرقت له كذلك الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات في المادة 28 منها بعنوان "الجمع الفوري لمعلومات تتبع المستخدمين"، بحيث أوردت أحكامًا مماثلة لسابقتها، فألزمت كل دولة طرف تمكين سلطات التحقيق المختصة

---

[1]-Art 20 paragraphe 01 du convention sur la cybercriminalité dispose que: «Collecte en temps réel des données relatives au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique ».

[2]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 286.

[3]- نفس المرجع، ص 286.

من الجمع أو التسجيل بواسطة الوسائل الفنية على إقليم الدولة الطرف، فضلًا عن إلزام مقدم الخدمة ضمن إختصاصه الفني على جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف، أوالتعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للإتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

أما تجميع محتوى المعطيات فجاء تحت عنوان "إعتراض المعطيات الخاصة بالمحتوى" في الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بموجب المادة 21 منها، بحيث أجازت الفقرة الأولى منها على كل دولة طرف في الإتفاقية بتبني الإجراءات التشريعية وأي إجراءات أخرى تراها ضرورية لتخويل سلطاتها المختصة بتطبيق الوسائل الفنية الموجودة على إقليمها لغرض الجمع أو التسجيل المعطيات المتعلقة بالمحتويات، فضلًا عن إلزام مقدم الخدمة في نطاق قدرته الفنية المتوافرة بأن يجمع أو يسجل بواسطة الوسائل الفنية على إقليم الدولة الطرف، أو يتعاون مع السلطات المختصة ومساعدتها في جمع وتسجيل في الوقت الفعلي المعطيات المتعلقة بحركة السير المرتبطة بإتصالات معينة المنقولة في إقليم ذلك الطرف بواسطة المنظومة المعلوماتية.[1]

الأصل أن إجراء إعتراض مضمون المعطيات تباشره سلطة معينة بالدولة، إلا أن الإتفاقية أجازت إلزام مقدم الخدمة للقيام به على أساس أنه قد تتوافر لديه الإمكانيات الفنية اللازمة لذلك، ويلاحظ بأن هذا الإجراء يختلف عن إجراء التحفظ السريع على مضمون المعطيات الذي نصت عليه المادة 16 من الإتفاقية في أن المعطيات المطلوب التعرف على مضمونها مخزنة ويلتزم مقدم الخدمة بالتحفظ عليها، بينما يعد الإعتراض على مضمون المعطيات نوعًا من المراقبة المعاصرة للإتصال وجمع وتسجيل مضمون أية إتصالات تتعلق بمسائل غير مشروعة.[2]

وفي نفس السياق فقد أوردت الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات في المادة 29 منها أحكامًا مماثلة لسابقتها، فألزمت كل دولة طرف بتبني الإجراءات التشريعية

---

[1]-Art 21 paragraphe 01 du convention sur la cybercriminalité dispose que : « Interception de données relatives au contenu:

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne, à:

a collecter or à enregistrer par l'application de moyens techniques existant sur son territoire: et

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, á:

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique».

[2]- رامي متولي القاضي، عمر سالم، مرجع سابق، ص 287.

والضرورية فيما يخص الجرائم المنصوص عليها في القانون الداخلي للدولة الطرف فيها، لتمكين سلطاتها المختصة من الجمع أو التسجيل المعلومات المتعلقة بالمحتوى بواسطة الوسائل الفنية المتوافرة على إقليمها، كما ألزمت مقدمي الخدمات بالتعاون ومساعدة السلطات المختصة في جمع أو تسجيل المعلومات المتعلقة بالمحتوى بشكل فوري مع الإتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

فضلًا عما سبق ذكره، فإن التشريعات الحالية لا تقيم أية تفرقة بين تجميع المعطيات المتعلقة بحركة السير وإعتراض المعطيات المتعلقة بالمحتوى، سواء لعدم تقرير أية تفرقة في القانون الداخلي بالنسبة للفروق المتعلقة بالمصالح ذات الطبيعة الخاصة، وسواء لأن تقنيات التجميع المتعلقة بالإجراءين تتماثل إلى حد كبير، وهكذا فإن الشروط القانونية الواجب توافرها لتطبيق الإجراءين والجرائم التي يتم إستخدام هذين الإجراءين بصددها تكون متماثلة، وقد أقرت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 هذا الوضع بعمل نفس الإستخدام التشغيلي لمصطلح "يجمع أو يسجل" في نص المادتين 20 و21.[1]

2- ضوابط إجراء مراقبة الإتصالات الإلكترونية:

إن من بين دواعي اللجوء إلى مراقبة الإتصالات الإلكترونية توفر معلومات كافية تنذر بإحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني، أو للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولة المتبادلة.[2]

وفي هذا السياق، يلاحظ أن المشرع الجزائري قد حدد الحالات التي يسمح فيها باللجوء إلى مراقبة الإتصالات الإلكترونية في الجرائم الخطيرة دون سواها، وهو ما أكدت عليه الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 عندما نصت في الفقرة الأولى من المادة 21 على أن: "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأي إجراءات أخرى يرى أنها ضرورية، من أجل تخويل سلطاته المختصة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي".[3]

وقد قيد المشرع الجزائري اللجوء إلى عملية مراقبة الإتصالات الإلكترونية بشرط الحصول المسبق على إذن مكتوب من السلطة القضائية المختصة لمباشرة هذا الإجراء بموجب

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 250-251.

[2]- الفقرة الأولى من المادة 04 من القانون رقم: 09-04 السالف الذكر.

[3]-Art 21 paragraphe 01 du convention sur la cybercriminalité dispose que : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne...».

الفقرة 02 من المادة 04 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر التي تنص على أن: "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه، إلا بإذن مكتوب من السلطة القضائية المختصة".[1]

[1]- الأصل أن يتم إعتراض الإتصالات الإلكترونية إلا بإذن قضائي مسبق، ولكن هناك حالات في بعض التشريعات المقارنة يكون فيه الإعتراض مشروعًا دون صدور هذا الإذن، ويكون ذلك إما في إطار المراقبة المعتادة لمقدم الخدمة لمتابعة عمل الشبكة أو تكون بناء على شكوى المشترك، وسنحاول دراسة ذلك بالتفصيل في التالي:

المراقبة المعتادة لمقدم الخدمة لعمل الشبكة: تقرر بعض التشريعات -كالقانون الأمريكي- إستثناء خاصًا بمقدمي الخدمات يستطيعون بمقتضاه أن يقوموا بمراقبة المشتركين في خدماتهم، وذلك من خلال معرفة ما يقوم هؤلاء المشتركون به من نشاط التداخل فى أجهزة الآخرين أو تخزين مواد مخالفة للقانون، وتسجيل هذه التداخلات والتبليغ عنها لرجال الضبط القضائي (مادة 18 U.S.C. § 2511 2ai)، وللمزيد من التفصيل، ينظر: بوكر رشيدة، مرجع سابق، ص343.

ومن الجدير بالذكر أن المشرع الأمريكي لم يطلق سلطة مقدمي ممارسة تلك الرقابة، بل إشترط عدة شروط ينبغي توافرها لصحة هذه الرقابة وتتمثل فيما يلي:

- أن يكون مقدم الخدمات مجنيًا عليه في جريمة؛

- أن يقوم بالمراقبة وبالتبليغ عما يعلمه من جرائم إلى الجهات القضائية حماية لحقوقه، وليس قيامًا بدور المساعد للمباحث في التحريات التي يقومون بها؛

- ألا يشارك رجل الشرطة أو يشرف على مقدم الخدمات في قيامه بأعمال المراقبة؛

- ألا يطلب رجل الشرطة من مقدم الخدمات القيام بتلك المراقبة عونًا له، أي أن المبادرة بالتبليغ يجب أن تأتي من جانب مقدم الخدمات، وللمزيد من التفصيل، ينظر: عائشة بن قارة مصطفى، مرجع سابق، ص172.

ولا يجوز لرجال الضبط القضائي أن يبادروا إلى تلك المراقبة دون تبليغ من مقدمي الخدمات أو سبق حصولهم على إذن بذلك، وهذا ما قضى به في قضية تتلخص وقائعها في أن رجال الضبط القضائي كانوا يتبعون متهمًا في جريمة إختطاف وقد عمد هذا المختطف إلى إستخدام خط تليفوني مقلد، لذا لجأ رجال الضبط إلى مقدم خدمات الإتصالات السلكية (التليفونات) لمراقبة هذا الخط، إستنادًا إلى أن القانون يسمح لهم بتلك الرقابة في حالة الإعتداء على حقوق هؤلاء المقدمين لتلك الخدمات، ومن هذه الإعتداءات سرقة الخطوط. ولاحظت المحكمة -بحق- أن المبادرة بالرقابة للخطوط يجب أن تبدأ من مقدمي الخدمات في أثناء قيامهم بأعمالهم، فلهم عندئذ أن يقوموا بتبليغ رجال الضبط. والعكس من ذلك غير جائز قانونًا كما هو الحال في هذه الدعوى، وللمزيد من التفصيل، ينظر: شيماء عبد الغني محمد عطاالله، مرجع سابق، ص221.

وبالإضافة إلى حق مقدمي الخدمات في مراقبة الإتصالات التي تصل إلى أجهزتهم إذا كانت تشكل مساسًا بحق من حقوقهم كسرقة الخطوط، فإن القانون الأمريكي أجاز لهم تلك المراقبة إذا كانت ضرورية لقيامهم بأعمالهم مثل أعمال إصلاح الخطوط والصيانة (المادة 2511 2 a i§)، ويجب أن تمارس تلك المراقبة في حدود ضيقة بالقدر اللازم لذلك الإصلاح أو تلك الصيانة، وللمزيد من التفصيل، ينظر: نفس المرجع، ص 224.

2 - المراقبة بناء على شكوى المشترك: إختلفت التشريعات المقارنة حول مدى إمكانية السماح للسلطات بمراقبة الإتصالات الإلكترونية بناء على الطلب الصادر من صاحب الجهاز محل الإعتداء بوضع جهازه تحت المراقبة من قبل رجال الضبط القضائي بذلك (ويقاس هذا الإستثناء على مقدم الخدمات)، وكان الأمر يدور بين موقفين: أحدهما مؤيد والثاني معارض لهذه المراقبة، وللمزيد من التفصيل، ينظر: عائشة بن قارة مصطفى، مرجع سابق، ص172.

بالنسبة للموقف المعارض يجسده رأي في كندا ويعتبر فيه أن مقدم الخدمات متماثل في عمله مع رجال السلطة العامة، وبالتالي فإنه ليس من حقه القيام بتلك الرقابة وتلك التسجيلات بدون إذن، فإذا قام بذلك فإنه يخالف حكم (الفقرة 02 من المادة 24) من ميثاق الحقوق والحريات الكندي، وللمزيد من التفصيل، ينظر: نفس المرجع، ص172.

أما بالنسبة للموقف المؤيد لهذا النوع من المراقبة، فإنه إذا كان الأصل أنه لا يجوز مراقبة الإتصالات الإلكترونية -مثلها في ذلك مثل الإتصالات السلكية- إلا بأمر قضائي، فإن القانون الأمريكي يسمح بالخروج على هذا الإستثناء في حالة الطلب=

إلا أنه عندما يتعلق الأمر بالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فقد خول للنائب العام لدى مجلس قضاء الجزائر صلاحية منح الإذن لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها لمباشرة إجراء مراقبة الإتصالات الإلكترونية لمدة ستة (06) أشهر قابلة للتجديد، على أن يكون ذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.[1]

يتضح مما سبق، أن المشرع الجزائري خول صلاحية إصدار الإذن إلى النائب العام لدى مجلس قضاء الجزائر في الحالات المحددة على سبيل الحصر، وحدد مدتها بستة (06) أشهر قابلة للتجديد، أما في بقية الحالات المنصوص عليها في الفقرة الأولى من المادة 04 من القانون آنف ذكره فقد أحالنا بصفة غير مباشرة إلى القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية فيما يتعلق بمنح الإذن ومدته.

وبالرجوع إلى المرسوم الرئاسي رقم: 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر، نجده قد خول للهيئة ضمان المراقبة الوقائية للإتصالات الإلكترونية تحت سلطة القاضي المختص، قصد الكشف عن الجرائم الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.[2]

وإمكانية وضع وحدة مراقبة واحدة أو أكثر تزود بالوسائل والتجهيزات التقنية الضرورية، على أن يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة لصالح ضباط الشرطة القضائية الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية، تحت إدارة ومراقبة قاضي لدى الهيئة يساعده واحد أو أكثر من ضباط الشرطة القضائية المنتمون للهيئة، وتحرر أشغالها في محاضر طبقًا لأحكام قانون الإجراءات الجزائية.[3]

=الصادر من صاحب الجهاز محل الإعتداء بوضع جهازه تحت المراقبة من قبل رجال الضبط القضائي، وبالتالي فإن الإستثناء يسمح لمقدم الخدمات بأن يقوم بذلك، وللمزيد من التفصيل، ينظر: شيماء عبد الغني محمد عطاالله، مرجع سابق، ص 225.

ويلزم لتوافر هذا الإستثناء إجتماع أربعة شروط وهي:

الشرط الأول: أن يسمح المالك - أو صاحب الحق- لرجال الضبط بوضع الجهاز الخاص به تحت المراقبة؛

الشرط الثاني: أن يتم ذلك في إطار تحقيق جنائي قائم؛

الشرط الثالث: أن تتوافر دلائل كافية على أن تسجيل الإتصالات القادمة من الجهاز الصادر منه الإعتداء يفيد في كشف الحقيقة؛

الشرط الرابع: أن يقتصر رجال الضبط على إعتراض الإتصالات الصادرة من وإلى الأجهزة محل التحقيق، وللمزيد من التفصيل، ينظر: عائشة بن قارة مصطفى، مرجع سابق، ص173.

[1]- الفقرة 03 من المادة 04 من القانون رقم: 09-04 السالف الذكر.

[2]- المادة 04 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.

[3]- المادة 26 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.

وتكون الترتيبات التقنية موجهة حصريًا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والإعتداءات على أمن الدولة ومكافحتهما في حينها داخل منظومة معلوماتية وتحت سلطة قاضي لدى الهيئة، ويترتب على إستخدامها لغير الأغراض المخصص لها توقيع العقوبات المنصوص عليها في قانون العقوبات الجزائري المقررة للمساس بالحياة الخاصة للغير.[1]

وقد يتم التعاون والإستعانة بمقدمي الخدمات في حدود جمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها[2]، وهو ما أجازت به الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في المادة 21 منها للدول الأطراف على تخويل سلطاتها المختصة إلزام مقدم الخدمة في نطاق قدرته الفنية المتوافرة بأن يجمع أو يسجل بواسطة الوسائل الفنية على إقليم الدولة الطرف، أو يتعاون مع السلطات المختصة ومساعدتها في جمع وتسجيل في الوقت الفعلي المعطيات المتعلقة بالمرور المرتبطة بإتصالات معينة المنقولة في إقليم ذلك الطرف بواسطة المنظومة المعلوماتية، وهو ما أجازت به أيضًا الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات في المادة 29 منها[3].

يلاحظ أن هذا الإلتزام المفروض على مقدمي الخدمات لا يتم تطبيقه إلا في حدود عملية التجميع أو التسجيل أو التعاون والمساعدة، وأن يكون ذلك في نطاق الإمكانيات الفنية المتوفرة لدى مقدم الخدمات، بيد أن النصوص الحالية لا تلزم مقدمي الخدمات بضمان أن يكون بحوزتهم إمكانات فنية لمباشرة عملية التجميع أو التسجيل أو منح العون والمساعدة، كما أنها لا تفرض عليهم حيازة تجهيزات جديدة أو أن يكلفوا خبراء لمساعدتهم أو أن يتم مباشرة هذا الإجراء بشكل باهظ لنظمهم المعلوماتية، أما إذا كان لدى نظمهم المعلوماتية وموظيفهم الذين يعملون فيها الإمكانات الفنية اللازمة لمباشرة هذا التجميع أو التسجيل أو منح العون والمساعدة، فإن هذه النصوص تلزمهم بإتخاذ الإجراءات الضرورية من أجل تطبيق هذه الإمكانات الفنية.[4]

---

[1]- الفقرة 03 من المادة 04 من القانون رقم: 09-04 السالف الذكر، والمادة 25 من المرسوم الرئاسي رقم: 21-439 السالف الذكر.

[2]- الفقرة الأولى من المادة 10 من القانون رقم: 09-04 السالف الذكر.

[3]- تنص الفقرة الأولى من المادة 29 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "إعتراض معلومات المحتوى:

1- تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من:

أ- الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف، أو؛

ب- التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للإتصالات المعنية في إقليمها، والتي تبث بواسطة تقنية معلومات".

[4]- هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 304-305.

على هذا الأساس إذا لم يكن لدى مقدم الخدمات إمكانات فنية لمباشرة هذه العملية، فإن السلطات المكلفة بتطبيق قانون الطرف صاحب الشأن تأخذ على عاتقها القيام بهذه المهمة.[1]

فضلًا عن إلزام مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وأية معلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[2]، وهو ما أكدت عليه الفقرة 03 من المادة 21 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 على إلتزام كل دولة طرف بإتخاذ الإجراءات التشريعية الضرورية لإلزام مزود الخدمة بالإحتفاظ على سرية الوقائع، وذلك عند تنفيذه للصلاحيات المنصوص عليها في هذه المادة وأية معلومات تتعلق بها[3]، كما نصت على ذات المعنى الفقرة 03 من المادة 29 من الإتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات[4].

ويتضح مما سبق، أن المشرع الجزائري لم ينظم كافة المسائل التي تتعلق بإجراء مراقبة الإتصالات الإلكترونية، على خلاف المشرع الفرنسي الذي إستوجب تحرير محضر من الهيئات المعنية بعد الإنتهاء من مباشرة عملية المراقبة، ووضع تسجيلات خاصة بالمراقبة في أحراز مغلقة مع ختمها بالأختام الرسمية المغلقة، كما أجاز بإمكانية إتلاف تلك التسجيلات بعد الإنتهاء من التحقيق والمحاكمة، على أن يتم ذلك بناءً على طلب المدعي العام في المقاطعة أو النيابة العامة.[5]

الفرع الثاني: الإجراءات المتعلقة بالمعطيات الساكنة

ارتأينا التطرق أولًا إلى حفظ المعطيات المتعلقة بحركة السير، ثم بعد ذلك إلى الأمر بتقديم المعطيات المعلوماتية المتعلقة بالمشترك.

أولًا: حفظ المعطيات المتعلقة بحركة السير

يعد هذا الإجراء أداة تحقيق مستحدثة ويقصد به توجيه السلطة المختصة لمقدمي الخدمات الأمر بالتحفظ على المعطيات المخزنة في حوزته وتحت سيطرته في إنتظار إتخاذ

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص 264.

[2]- الفقرة 02 من المادة 10 من القانون رقم: 09-04 السالف الذكر.

[3] -Art 21 paragraphe 03 du convention sur la cybercriminalité dispose que : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet».

[4]- تنص الفقرة 03 من المادة 29 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "تلتزم كل دولة طرف إتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالإحتفاظ بسرية أية معلومة، عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة".

[5]- بلحسيني حمزة، مرجع سابق، ص 408.

إجراءات القانونية أخرى كالتفتيش، ويتضح أن التحفظ العاجل هو إجراء أولي تمهيدي الهدف منه هو محاولة الإحتفاظ بالمعطيات قبل فقدانها[1].

أقرت ذلك الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 من خلال أحكام المادتين 16 و17 منها، وتقابلها المواد 23 و24 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقد أكده المشرع الجزائري بموجب المادة 10 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر وألزم مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية وبوضع المعطيات التي يتعين عليهم حفظها وفقًا للمادة 11 من نفس القانون تحت تصرف السلطات المذكورة.

وتطبيقًا لذلك، نصت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 في الفقرة الأولى من المادة 16 منها[2]، والإتفاقية العربية لمكافحة جرائم تقنية المعلومات في الفقرة الأولى من المادة 23 منها[3]، على ضرورة إلتزام كل دولة طرف فيها على تمكين سلطاتها المختصة أن تأمر أو تفرض بطريقة أخرى مقدم الخدمة على التحفظ العاجل للمعطيات المخزنة، وأن يكون لجهة التحقيق أن تأمر أو تصل فورًا على المعطيات بما فى ذلك حركة سير المعطيات التى يتم تخزينها بواسطة منظومة المعلوماتية، خاصة في حال وجود أسباب تدعو للإعتقاد بأن تلك المعطيات على وجه الخصوص معرضة للفقد أو التعديل.

وينبغي التنويه في هذا الإطار إلى أن عملية الحفظ هنا لا تخص كل المعطيات المعلوماتية بمختلف نماذجها، إنما تخص المعطيات المتعلقة بحركة السير، التي عرفتها الفقرة (د) من المادة الأولى من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بأنها: "تعني كل المعطيات التي تتعامل مع الإتصال والتي تمر من خلال النظام المعلوماتي أو يتم إعدادها بواسطة هذا الأخير، والذي يعد عنصرًا في سلسلة الإتصال بالإشارة إلى مصدر الإتصال، مكان الوصول، خط السير، الساعة التاريخ الحجم مدة الإتصال، أو نوع

[1]- بن مكي نجاة، مرجع سابق، ص 230.

[2]-Art 16 paragraphe 01 du convention sur la cybercriminalité dispose que: « Conservation rapide de données informatiques stockées: Chaque Partie adopte les mesres législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre maniére la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'ily a des raisons de penser que celles-ci sont particuliérement susceptibles de perte ou de modification».

[3]- تنص الفقرة الأولى من المادة 23 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات، وخصوصًا إذا كان هناك إعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل".

الخدمة المؤداة"[1]، وهو تقريبًا نفس التعريف الذي تبناه المشرع الجزائري بموجب الفقرة (هـ) من المادة 02 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر على أنها: "أي معطيات متعلقة بالإتصالات عن طريق منظومة معلوماتية تنتجها هذه الأخيرة، بإعتبارها جزءًا في حلقة الإتصالات توضح مصدر الإتصال، والوجهة المرسلة إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة".

وتشير المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 إلى أن الإجراءات الواردة في المادة 16 منها تنطبق على المعطيات المخزنة التي سبق الإحتفاظ بها من طرف حائزي المعطيات كمقدمي الخدمات، كما وتشير إلى شمولية المعطيات المعلوماتية المخزنة التي تكون محلًا للتحفظ، بحيث يمكن أن تشتمل على أي نوع من المعطيات المحددة في الأمر بالتحفظ، وقد تكون تلك المعطيات واردة في مستندات تجارية طبية أو شخصية[2]، ويمكن أن يشمل ذلك أيضًا على سبيل المثال المعطيات التي لا يتم الإحتفاظ بها إلا لفترة وجيزة وكما هو الحال عند تبني شركة سياسة محو المعطيات بعد كل فترة معينة، أو أن المعطيات يتم محوها منهجيًا عندما يكون وسط التخزين مطلوبًا من أجل تسجيل معطيات أخرى[3].

وقد حدد المشرع الجزائري المعطيات المتعلقة بحركة السير التي يتعين على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية المختصة لأغراض التحقيق، في المادة 11 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر على النحو التالي:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة؛
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال؛
- الخصائص التقنية، وكذا تاريخ ووقت ومدة كل إتصال؛
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة، أو المستعملة، ومقدميها؛
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال، وكذا عناوين المواقع المطلع عليها؛

[1]- يشير مصطلح مصدر الإتصال يمكن معرفته عن طريق رقم التليفون وعنوان بروتوكول الإنترنت une adress IP أو بطريقة مماثلة تحديد هوية جهاز الإتصال الذي يقوم مقدم الخدمة بتقديم خدماته من خلاله، ومكان الإتصال يمكن معرفته عن طريق الجهاز الذي تتجه إليه الإتصالات المرسلة، كما يستدل على نوع الخدمة المؤداة بنوع الخدمة المستخدمة داخل الشبكة كأن تكون نقل ملفات أو بريد إلكتروني أو بريد آني أو لحظي، وللمزيد من التفصيل، ينظر: هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 278-279.

[2]- بلحسيني حمزة، مرجع سابق، ص 381.

[3]- هلالي عبد اللاه أحمد، مرجع سابق، ص 200.

وبالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وكذا تلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه".

وتقدير ما إذا كان التحفظ على المعطيات المعلوماتية المخزنة ضروريًا من عدمه يتوقف على مدى جدية المبررات التي ترتكن إليها سلطات القضائية لإصدار الأمر بالتحفظ عليها، وقد حددت المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 الأسباب التي تدعو إلى إتخاذ مثل هذا الإجراء، وذلك للمبررات التالية:

- قابلية المعطيات المعلوماتية للتلاشي، بالإضافة إلى أنها لا تبقى داخل المنظومة المعلوماتية إلا لفترة قصيرة فإنه من السهل أن تخضع للتلاعب أو التغيير، وهكذا يسهل فقدان عناصر إثبات الجريمة من خلال الإهمال وممارسات التخزين غير الدقيقة أو التغيير العمدي لها أو محوها من أجل تدمير كل عنصر للإثبات، أو محو هذا العنصر في إطار العمليات العادية أو الروتينية لمحو المعطيات التي لم تعد في حاجة إليها، وإحدى وسائل المحافظة على سلامة المعطيات وسريتها هو قيام السلطات المختلفة بالتحفظ عليها لدى حائزها خاصة إذا كان حارس المعطيات جدير بالثقة، كما في حالة شركة تجارية ذات سمعة طيبة فإن سلامة المعطيات يمكن ضمانها بطريقة أسرع عن طريق إصدار أمر بالتحفظ على المعطيات لديها، وبهذا يمكن أن يكون الأمر بالتحفظ على المعطيات أقل قلقًا أو إخلالًا بالمنظومة بالنسبة للأنشطة وأقل ضررًا على سمعة الشركة الأمنية من عملية تفتيش الأوعية المعلوماتية بغرض الضبط[1]؛

- غالبًا ما يتم إرتكاب الجريمة الماسة بالمستند الإلكتروني عن طريق نقل الإتصالات التي يتم من خلالها تبادل المعطيات والمعلومات عبر المنظومة المعلوماتية، حيث يمكن أن تتضمن هذه الإتصالات محتويات غير مشروعة مثل مواد الإباحية للأطفال أو فيروسات المعلوماتية، أو أي تعليمات أخرى تحمل إعتداء على المعطيات أو تعوق حسن أداء المنظومة، كما يمكن أن تشتمل على عناصر يمكن من خلالها إثبات أن جرائم أخرى قد تم إرتكابها أو الدليل على إرتكاب جرائم أخرى مثل الإتجار بالمخدرات أو النصب، فتحديد مصدر إرسال هذه الإتصالات يمكن أن يساعد في تحديد هوية مرتكبي الجريمة[2]؛
- تأمين الدليل الإلكتروني من الضياع والإتلاف، عندما تحتوي هذه الإتصالات على محتوى غير مشروع أو دليل على نشاط إجرامي، فإن نسخ من هذه الإتصالات يتم الإحتفاظ بها بواسطة مقدمي الخدمات من أجل عدم فقد عناصر الإثبات الجوهرية، مثل المراسلة الإلكترونية المخزنة التي تم إرسالها أو إستقبالها، ومن شأنه أن يكشف عن أدلة على الإجرام.[3]

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 289-290.
[2]- نفس المرجع، ص290.
[3]- نفس المرجع، ص290.

وتنص الفقرة 02 من المادة 16 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001[1]، والفقرة 02 من المادة 23 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[2]، على أنه حينما يقوم الطرف بتطبيق إجراء التحفظ من خلال الأمر بالتحفظ، فإن هذا الأخير يتصل بالمعطيات المخزنة ومتواجدة إما في حوزة أو تحت إشراف الشخص الذي أرسل إليه الأمر، وهكذا فإن المعطيات المخزنة يمكن أن تكون بالفعل في حوزة الشخص المعني كما يمكن أن تكون مخزنة في مكان آخر ولكنها خاضعة لإشرافه، ولتحقيق هذه المسألة فإنه يجب على الدولة الطرف في الإتفاقية إتخاذ الإجراءات التشريعية والإجراءات الأخرى التي تراها ضرورية من أجل إلزام هذا الشخص الذي يتلقى الأمر على التحفظ على المعطيات المعلوماتية المخزنة من أجل الحفاظ وحماية سلامة تلك المعطيات لمدة لا تزيد عن تسعين (90) يومًا، على أن تكون تلك المدة قابلة للتجديد بغرض السماح للسلطات المختصة من القيام بمهمتها في البحث والتقصي.

وقد حدد المشرع الجزائري مدة حفظ تلك المعطيات بسنة واحدة (01) إبتداءً من تاريخ التسجيل[3]، وأقر المسؤولية الإدارية لمقدمي الخدمات لعدم إحترامهم للإلتزامات الملقاة على عاتقهم، إلى جانب المسؤولية الجزائية في حال ما ترتب على أعمالهم عرقلة حسن سير التحريات القضائية[4].

ولما كان التحفظ على معطيات المستند الإلكتروني في جرائم الإعتداء عليه، ينطوي حتمًا على مساس بسرية المعلومات وحرمة الحياة الخاصة لما يتضمنه ذلك الإجراء من تحفظ على جميع معطيات الجهاز الإلكتروني، فقد كان ضروريًا تقييد السلطة القضائية بهذا الإجراء بقيود تضمن التوازن بين حق المجتمع فى إنزال العقاب على المتهم، وحق هذا الأخير في عدم

[1]-Art 16 paragraphe 02 du convention sur la cybercriminalité dispose que : « Lorsqu'une partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiés se trouvant en sa possession ou sous son contrôle, cette partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'á maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite».

[2]- تنص الفقرة 02 من المادة 23 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة 01 بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته، ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يومًا قابلة للتجديد من أجل السلطات المختصة من البحث والتقصي".

[3]- الفقرة 03 من المادة 11 من القانون رقم: 09-04 السالف الذكر.

[4]- أقر المشرع الجزائري المسؤولية الإدارية على عاتق مقدمي الخدمات في حال إخلالهم بإلتزاماتهم بوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المكلفة بالتحريات القضائية، إلى جانب المسؤولية الجزائية التي تترتب عندما تؤدي أعمالهم إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (06) أشهر إلى خمس (05) سنوات، وبغرامة من خمسون ألف 50.000 دج إلى خمسمائة ألف 500.000 دج، بينما تطبق على الشخص المعنوي الغرامة تقدر وفقًا للقواعد المنصوص عليها في قانون العقوبات أي بما تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وبالتالي فإن العقوبة المالية تقدر بمليوني وخمسمائة ألف 2.500.000 دج، بموجب الفقرتين 04 و05 من المادة 11 من القانون رقم: 09-04 السالف الذكر.

المساس بسرية المعلومات المخزنة على الجهاز الخاص به[1]، وتطبيقًا لذلك نصت الفقرة 03 من المادة 16 من الإتفاقية الأوروبية الخاصة بالجرائم المعلوماتية المبرمة في بودابست عام 2001[2] والفقرة 03 من المادة 23 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[3]، على إلزام الدول الأطراف فيها بتبني الإجراءات الضرورية لإلتزام السرية بالنسبة لتطبيق إجراءات التحفظ على الشخص الملزم بالتحفظ على المعطيات في غضون المدة المحددة في قانونه الداخلي.

وفي السياق نفسه، نص المشرع الجزائري من خلال الفقرة 02 من المادة 10 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر على إلزام مقدمي الخدمات بكتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

وأجازت الفقرة الأولى من المادة 17 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001[4] والمادة 24 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[5] من أجل ضمان التحفظ على المعطيات المتعلقة بحركة السير المطلوب حفظها، بأن

---

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص 269.

2-Art 16 paragraphe 03 du convention sur la cybercriminalité dispose que: « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci á garder le secret sur la mise en oeuvre desdites procédures pendant la durée prévue par son droit interne».

[3]- تنص الفقرة 03 من المادة 23 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات، للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي".

[4]-Art 17 paragraphe 01 du convention sur la cybercriminalité dispose que : « Conservation et divulgation rapides de données relatives au trafic:

1. Afin d'assurer la conservation des données relatives au trafic en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour:

a. veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de service aient participé à la transmission de cette communication; et

b. assurer la divulgation rapide à l'autorité compétente de la partie, ou à une personne désignée par cette autorité, d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise».

[5]- تنص المادة 24 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين:

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل:

2- ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين، بغض النظر عن إشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الإتصالات.

3- ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين، لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الإتصالات".

تلزم الدولة الطرف إتخاذ الإجراءات التشريعية وأي الإجراءات الأخرى التي تراها ضرورية من أجل أن تتأكد من أن التحفظ لهذه المعطيات المتعلقة بحركة السير متوافر، بغض النظر عن إشتراك واحد أو أكثر من مقدمي خدمة في بث تلك الإتصالات[1]، فضلًا عن ضمان إمكانية الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو شخص تعينه تلك السلطات لمقدر كافي من حركة السير للمعطيات، لتمكين الدولة الطرف من تحديد هوية مقدمي الخدمة ومسار بث الإتصالات.

وتشير المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 أن المادة 17 منها تفرض على كل مقدم خدمة الذي يتلقى الأمر بالتحفظ الإفشاء السريع للسلطات المختصة، أو أي شخص آخر معين من قبل هذه السلطات، عن مقدار كاف من معطيات حركة السير لتمكين تلك السلطات المختصة تحديد هوية كل مقدمي الخدمة الأخرين والطريق الذي بمقتضاه تم نقل الإتصال، وينبغي على السلطات المختصة أن تحدد بوضوح نوع معطيات حركة السير الهامة المطلوب الكشف عنها، ولعل في الحصول على هذه المعلومات من شأنه أن يسمح للسلطات المختصة بتحديد ما إذا كان يجب عليها إتخاذ إجراءات التحفظ فيما يتعلق بمقدمي خدمات الأخرين، وبهذه الطريقة يمكن للسلطة القضائية المختصة أن تعقب مصدر ووجهة الإتصال، وكذا تحديد هوية مرتكب أو مرتكبي الجريمة المحددة التي تخضع للتحقيق.[2]

ثانيًا: الأمر بتقديم المعطيات المعلوماتية المتعلقة بالمشترك

ألزمت الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 بمقتضى الفقرة الأولى من المادة 18 منها على كل دولة طرف فيها أن تتبنى الإجراءات التشريعية والإجراءات التي تراها أنها ضرورية، من أجل تمكين سلطاتها المختصة بأن تأمر شخصًا ما داخل أراضيها بتقديم معطيات معلوماتية معينة مخزنة في المنظومة المعلوماتية أو في دعامة تخزين معلوماتية والتي تكون في حوزته أو تحت سيطرته، أو أن تلزم مقدم خدمات

[1]- يحدث في الغالب أن يكون عدة مقدمي خدمات قد ساهموا في نقل الإتصال وأن يكون بحوزة كل منهم بعض البيانات المرور المتعلقة بنقل إتصال معين، والتي نتجت وتم الإحتفاظ بها بواسطة مقدم الخدمة بمناسبة مرور الإتصال عن طريق نظامه أو عن طريق مقدمي خدمة آخرين، وقد يحدث أيضًا أن تكون بيانات المرور أو بعض نماذج من بيانات المرور مشتركة بين مقدمي الخدمات الذين ساهموا في نقل الإتصال لأغراض تجارية أو أمنية أو تقنية في مثل هذه الحالة، فإن أيا من مقدمي الخدمات يمكن أن يكون بحوزته بيانات مرور جوهرية من أجل تحديد المصدر والخط النهائي للإتصال. ومع ذلك ففي الغالب أن مقدم خدمة بمفرده لا يكون بحوزته من بيانات المرور ما يكفي للتحديد بإتقان لمصدر أو نهاية الإتصال، إذ إن كل مقدم خدمة من هؤلاء يكون لديه بعض أجزاء اللغز، وبالتالي فإنه من جماع هذه الأجزاء التي يجب إختبارها يمكن التعرف على مصدر ومنتهى هذه الإتصالات، وللمزيد من التفصيل، ينظر: هلالي عبد اللاه أحمد، مرجع سابق، ص 207.

[2]- نفس المرجع، ص 209.

موجود على أراضيها بأن يرسل لها معطيات المشترك ذات الصلة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته.[1]

ومنه فقد حددت الجهات التى يجوز إلزامها بتنفيذ الأمر بالتحفظ، وهي:

أ- أحد الأشخاص يحوز ويسيطر على معطيات المستند الإلكتروني المخزنة على جهازه أو دعامة مادية، متى كانت متصلة بالمستند الإلكتروني محل التجريم؛

ت-أجهزة الخدمة المتصلة بإرسال ما تحوزه أو تسيطر عليه من معطيات المشتركين.[2]

وقد حددت هذه الإتفاقية أيضًا بموجب الفقرة 03 من المادة 18 منها[3] المقصود بمصطلح المعطيات المتعلقة بالمشتركين والتي يعني به أية معلومات موجودة في صورة معطيات بالجهاز الإلكتروني أو أية صورة أخرى، يتم حفظها بأحد أجهزة تقديم الخدمة المعلوماتية والتي تتعلق بالمشتركين في الخدمات الخاصة به خلاف خط سير المعطيات أو مضمونها، والتي بموجبها يمكن التوصل إلى:

أ- نوعية خدمة الإتصال أو المراسلة المستخدمة، والشروط الفنية التي يتم إتخاذها في ذلك، والفترة الزمنية للخدمة؛

ب - المعطيات الشخصية للمشترك، وعنوانه البريدي أو الجغرافي ورقم هاتفه وغير ذلك من أرقام الدخول الأخرى الخاصة به، والمعطيات الخاصة بالفواتير والدفع والتي تكون متوافرة بموجب الإتفاق على الخدمة أو الترتيبات الخاصة بذلك؛

---

[1]-Art 18 paragraphe 01 du convention sur la cybercriminalité dispose que : « Injonction de produire:

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession oú sous le contrôle de cette personne, et stockées dans un systéme informatique où un support de stockage informatique; et.

b. à un fournisseur de services offrant des prestations sur le territoire de la partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services».

[2]- سحر سعد عبد السميع محمد، مرجع سابق، ص 272.

[3]-Art 18 paragraphe 03 du convention sur la cybercriminalité dispose que : « Aux fins du présent article, l'expression "données relatives au abonnés" désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accés, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service,

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service».

ج- أية معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات الإتصالات، والتي تتوافر بموجب الإتفاق على الخدمة أو الترتيبات الخاصة بذلك.[1]

وبالنسبة للتشريع الأمريكي ففي قانون خصوصية الإتصالات الإلكترونية المعروف بـ (ECPA) فقد أجاز لرجال الضبط القضائي في إطار ما يقومون به من جمع الإستدلالات، الإطلاع على المعطيات الموجودة في حوزة مقدمي الخدمات والتي تخص مستخدمي شبكة الإنترنت، وهذه المعلومات تتمثل في ثلاث طوائف وهي:

1- المعلومات الشخصية الخاصة بالمشترك، مثل إسمه ورقم تلفونه وعنوانه؛

2- المعلومات الشخصية الخاصة بالمتعامل مع المشترك، أي كل من يتصل به أو يدخل معه في صفقة؛

3- المعلومات المتعلقة بمحتوى المعطيات، أي مضمون المحادثات ومضمون الملفات؛

وبناءً عليه فإن المشترك في خدمات مقدمي الخدمات لا يتمتع بالحق في الخصوصية بالنسبة لهذه الأنواع الثلاثة من المعلومات سابقة.[2]

وتشير المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 على أنه في إطار التحقيق الجنائي قد تكون المعلومات المتعلقة بالمشترك ضرورية في حالتين محددتين:

أولًا: أن هذه المعلومات عن المشترك ضرورية لتحديد نوع الخدمات أو التدابير التقنية ذات الصلة التي إستخدمها أو يستخدمها المشترك، مثل نوع الخدمة الهاتفية المستخدمة مثلًا الهاتف النقال، ونوع الخدمات الأخرى المرتبطة مثل إعادة توجيه المكالمات والبريد الصوتي ورقم الهاتف أو عنوان البريد الإلكتروني؛

ثانيًا: عندما يكون العنوان التقني معروفًا، تكون هنالك حاجة إلى حيازة المعلومات عن المشترك من أجل المساعدة في تحديد هوية الشخص المطلوب، ويمكن أن تكون معلومات أخرى متعلقة بالمشترك مثل المعلومات التجارية المتعلقة بسجلات الفواتير والدفع الإشتراك، وأيضًا يمكن أن تكون مفيدة في التحقيقات الجنائية خاصة عندما تنطوي الجريمة قيد التحقيق على إحتيال على الجهاز الإلكتروني أو جرائم إقتصادية أخرى.[3]

وبهذا فإن إصدار الأمر بتقديم معطيات معلوماتية أو معلومات متعلقة بالمشترك توجد في حوزة أو تحت سيطرة شخص أو مقدم الخدمات، والإجراء لا ينطبق حتى من أجل هذا إلا على

[1]- سحر سعد عبد السميع محمد، مرجع سابق، ص-ص 272- 273.
[2]- شيماء عبد الغني محمد عطاالله، مرجع سابق، ص 216.
[3]- التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مرجع سابق، ص 29.

عاتق الشخص أو مقدم الخدمات الذي يحتفظ بهذه المعلومات، فعلى سبيل المثال إن بعض مقدمي الخدمات لا يحتفظون بأي أثر للمستخدمين بالنسبة لخدماتهم.[1]

ويشير تعبير "في حيازة أو تحت السيطرة" إلى الحيازة المادية للمعطيات المعنية داخل حدود هذا الطرف، ويشير كذلك إلى الحالات التي تكون فيها المعطيات المراد إظهارها خارج الحيازة المادية للشخص ولكن بمقدوره السيطرة عليها من خلال مرورها داخل حدود هذا الطرف، ومثال ذلك الشخص الذي يتلقى أمر تقديم المعلومات المخزنة لحسابه عن طريق الخدمة الفورية للتخزين عن بعد، فإنه يتعين عليه الإمتثال للأمر ويقوم بإظهار هذه المعطيات.[2]

كما أشارت المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 على أنه يجوز للدولة الطرف في تلك الإتفاقية تمكين السلطات المختصة صلاحية الأمر بأن تلزم مقدمي الخدمات تقديم المعطيات المتعلقة بالمشترك، والتي تكون في حيازته المادية أو تحت سيطرته حيث تكون هذه المعطيات مخزنة بعيدًا عن الحيازة المادية لمزود الخدمة ولكن يمكن السيطرة عليها، ومثال ذلك أن تكون المعطيات مخزنة في وحدة تخزين عن بعد ويتم تقديمها عن طريق شركة أخرى.[3]

ولا تعد الإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 الإتفاقية الوحيدة التي تناولت الأمر بإصدار المعطيات المعلوماتية بل تناولته كذلك الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في مادتها 25، حيث ألزمت هذه الأخيرة كل دولة طرف فيها على تبني الإجراءات الضرورية لتمكين سلطاتها المختصة من إصدار أمر لأي شخص في إقليمها، لتسليم لها معلومات معينة موجودة في حيازته والمخزنة على تقنية معلومات أو وسيط تخزين معلومات، وكذا إصدار الأمر لأي مقدم خدمة يقدم خدماته في إقليم الدولة الطرف في الإتفاقية لتسليم معلومات المشترك المتعلقة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته[4].

ويتجه المجلس الأوروبي هذا الإتجاه بالنسبة للمعلومات المتواجدة داخل الأنظمة المعلوماتية والتي تتواجد في حيازة أو تحت سيطرة مقدمي الخدمات، فتدعو لجنة الوزراء لهذا المجلس في توصيتها رقم: 13 في سنة 1995 إلى أن تتضمن قوانين الإجراءات الجنائية في

---

[1]- هلالي عبد اللاه أحمد، مرجع سابق، ص 215.

[2]- نفس المرجع، ص 216.

[3]- نفس المرجع، ص 217.

[4]- تنص المادة 25 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى :

1- أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص، والمخزنة على تقنية معلومات أو وسيط تخزين معلومات؛

2- أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات، في حوزة مقدم الخدمة أو تحت سيطرته".

الدول الأعضاء منح رجال الضبط القضائي السلطة التي تسمح لهم بطلب المعلومات المتواجدة لدى مقدمي الخدمات والتي تفيد في الكشف عن الحقيقة.[1]

وفي هذا الصدد، تنص المادة 06 من القانون المصري رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات السالف الذكر على أن: "يجوز لجهة التحقيق المختصة بحسب الأحوال أن تصدر أمرًا مسببًا لمأموري الضبط القضائي المختصين لمدة لا تزيد على ثلاثين (30) يومًا قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على إرتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يأتي: "...3- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الإتصالات التي تمت على ذلك النظام أو النظام التقني"، وتنص المادة 32 من نفس القانون على أن: "يعاقب بالحبس مدة لا تقل عن ستة (06) أشهر، وبغرامة لا تقل عن عشرين ألف 20.000 جنيه ولا تجاوز مائة ألف 100.000 جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة إمتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها في المادة 06 من هذا القانون".

أما المشرع الفرنسي فقد تناول هذا الجانب من خلال المادة 60-1 من ق.إ.ج.ف المعدلة بالقانون رقم: 2023-22 التي تنص على أن: "يجوز لوكيل الجمهورية أو لضابط الشرطة القضائية أو تحت إشراف هذا الأخير أو لعون الشرطة القضائية، أو في الحالة المنصوص عليها في البند °3 من الفقرة الثانية من المادة 21-3، أو مساعد التحقيق، بأن يطلب بأي وسيلة كانت، من أي شخص أو مؤسسة أو هيئة خاصة أو عمومية أو من أي إدارة عمومية، التي يحتمل أن تكون بحيازتهم معلومات ذات صلة بالتحقيق، بما في ذلك مراعاة أحكام المادة 60-1-2 المعلومات المتعلقة بنظام المعلوماتي أو تلك المتعلقة بمعالجة المعطيات الشخصية، أن يسلمه هذه المعلومات لاسيما في شكل رقمي، وعند الإقتضاء وفقًا للمعايير التي تحدد بموجب نص تنظيمي، دون أن يكون لهؤلاء أن يتمسكوا من دون مبرر مشروع بالإلتزام بسر المهنة لرفض الإمتثال لهذا الطلب، وعندما يتعلق هذا الطلب بالأشخاص المشار إليهم في المواد 56-1 إلى 56-6 فإن تسليم هذه المعلومات لا يمكن أن يتم إلا بموافقتهم بإستثناء الأشخاص المذكورين في المواد 56-1 إلى 56-5، ويعاقب بغرامة قدرها 3750 يورو كل من إمتنع عن الإستجابة لهذا الطلب في أقرب الآجال، وعند الإقتضاء وفقًا للمعايير المطلوبة".[2]

[1]- شيماء عبد الغني محمد عطاالله، مرجع سابق، ص 215.

[2]-Art 60-1 du C.P.P.F (Modifié par LOI n°2023-22 du 24 janvier 2023 - art. 18 V) dispose que: « Le procureur de la République ou l'officier de police judiciaire ou, sous le contrôle de ce dernier, l'agent de police judiciaire ou, dans le cas prévu au 3° de l'article 21-3, l'assistant d'enquête peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris, sous réserve de l'article 60-1-2, celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme=

وألزم المشرع الجزائري بموجب المادة 10 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية وبوضع المعطيات التي يتعين عليهم حفظها وفقًا للمادة 11 من نفس القانون تحت تصرف السلطات المذكورة، بما في ذلك المعطيات التي تسمح بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، والمعطيات المتعلقة بنشاطات الهاتف التي تسمح بالتعرف على مستعملي الخدمة.

وبموجب الفقرتين 04 و05 من المادة 11 من نفس القانون أقر المسؤولية الإدارية على عاتق مقدمي الخدمات في حال إخلالهم بإلتزاماتهم بوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المكلفة بالتحريات القضائية، إلى جانب المسؤولية الجزائية التي تترتب عندما تؤدي أعمالهم إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (06) أشهر إلى خمس (05) سنوات، وبغرامة من خمسون ألف 50.000 دج إلى خمسمائة ألف 500.000 دج، بينما تطبق على الشخص المعنوي الغرامة تقدر وفقًا للقواعد المنصوص عليها في قانون العقوبات أي بما تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وبالتالي فإن العقوبة المالية تقدر بمليوني وخمسمائة ألف 2.500.000 دج.

وأشارت المذكرة التفسيرية للإتفاقية الأوروبية بشأن الجرائم المعلوماتية الموقعة في بودابست عام 2001 أن يمكن أن يستثنى الشروط والضمانات المشار إليها في الفقرة 02 من المادة 18[1] وفقًا للقانون الداخلي لكل دولة طرف فيها بأن تستبعد معطيات أو معلومات سرية، ويمكن لأي طرف أن تحدد الشروط والسلطات المختصة والضمانات المختلفة فيما يتعلق بتقديم أنواع معينة من المعطيات المعلوماتية أو المعلومات عن المشتركين التي تم حيازتها عن طريق فئات معينة من الأشخاص أو مقدمي الخدمات، فعلى سبيل المثال يمكن لكل دولة أن تخول لرجال السلطة العامة صلاحية إصدار أمر تقديم المعطيات على أن تكون صلاحياتهم مقتصرة على بعض أنواع معينة من المعطيات مثل المعطيات المتعلقة بالمشترك المعروفة للكافة، إذ في حين إذا خرج الأمر عن تلك المعطيات فإن الأمر يقتضي إصدار هذا الأمر من المحكمة، ويمكن في بعض الحالات للدولة المعنية أن تتطلب أو تفرض بمقتضى ضمانات حقوق الإنسان إن هذا الأمر لا يصدر إلا عن طريق سلطة قضائية وذلك من أجل الحصول على أنواع معينة من المعطيات، مع مراعاة مبدأ التناسب الذي يستوجب إستبعاد تطبيق هذا الإجراء بالنسبة للقضايا عديمة الخطورة.[2]

=numérique, le cas échéant selon des normes fixées par voie réglementaire, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. Lorsque les réquisitions concernent des personnes mentionnées aux articles 56-1 à 56-5, la remise des informations ne peut intervenir qu'avec leur accord. A l'exception des personnes mentionnées aux articles 56-1 à 56-5, le fait de s'abstenir de répondre à cette réquisition dans les meilleurs délais et s'il y a lieu selon les normes exigées est puni d'une amende de 3 750 euros».

[1]-Art 18 paragraphe 02 du convention sur la cybercriminalité dispose que : « Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15».

[2]- هلالي عبد اللاه أحمد، مرجع سابق، ص-ص 217-218.

خلاصة:

لا تقتصر صعوبة إثبات الجرائم الماسة بالمستند الإلكتروني على مسألة تعذر الوصول إلى الأدلة الكافية لإثباتها، بل تمتد هذه الصعوبة لتشمل أيضًا الإجراءات المتعلقة بالحصول على تلك الأدلة، ولهذا تدخل المشرع الجزائري من خلال إستحدث نصوص قانونية خاصة تنظم القواعد الإجرائية بهدف مكافحة هذا النوع من الجرائم، سواء عبر تعديل أحكام قانون الإجراءات الجزائية بما يتلائم مع البيئة الرقمية التي ترتكب فيها هذه الجرائم، أو ضمن القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

كما عمل المشرع على تأهيل سلطات التحري والتحقيق للتعامل مع هذا النوع من الجرائم وإستخلاص الأدلة الإلكترونية منها، بالإضافة إلى إستحداث وحدات متخصصة في مكافحة هذا النوع من الإجرام، بما يواكب التطورات الحاصلة في هذا المجال والتغيرات التكنولوجية في ميدان المعلوماتية.

وقد حسم مسألة الإختصاص القضائي في الجرائم المعلوماتية والتي تعد الجرائم الماسة بالمستند الإلكتروني جزءًا منها، من خلال منح القضاء الجزائري صلاحية النظر في الجرائم المرتكبة داخل الإقليم الجزائري بغض النظر عن هوية مرتكب الجريمة أو نوعها أو مكان إرتكابها، كما منح بموجب القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها للمحاكم الجزائرية صلاحية النظر في الجرائم المرتكبة خارج الإقليم الوطني، إذا كان مرتكبها أجنبيًا أو إذا كانت تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني.

خلاصة:

إن الطبيعة الخاصة التي يتميز بها الدليل الإلكتروني المستخلص من الجرائم الماسة بالمستند الإلكتروني، قد إستدعت تدخلات تشريعية تشمل تنظيم إجراءات الحصول عليه، وتعزيز التعاون سواء على المستوى الوطني أو الدولي، بهدف التصدي للجرائم موضوع دراستنا، كما أصبح من الضروري تأهيل سلطات التحري والتحقيق للتعامل مع هذه الجرائم وإستخلاص الأدلة الإلكترونية المرتبطة بها، وإستحداث وحدات متخصصة في مكافحة هذا النوع من الإجرام، وذلك لأن عملية إستخلاص الدليل الإلكتروني غالبًا ما تواجه نقصًا في الخبرة الفنية والتقنية لدى سلطات التحري والتحقيق، مما تظهر الحاجة الملحة إلى تعاون ومساعدة قضائية دولية لمكافحة هذه الجرائم والتصدي لها، ومواجهة الإشكالات المتعلقة بمكان وقوعها وإختصاص المحاكم بها، وجمع المعلومات والتحريات بشأنها مع تعزيز التنسيق بين الدول ووضع قواعد للتسليم فيها.

الخاتمة

أصبحث الجهود المبذولة في مكافحة الجرائم الماسة بالمستند الإلكتروني تواجه عدة عراقيل، إذ لم تعد النصوص الجزائية سواء في شقها الموضوعي أو الإجرائي قادرة على إثبات هذا النوع من الجرائم أو ملاحقة مرتكبيها، وذلك بسبب الطبيعة الخفية التي ترتكب بها، ما يصعب كشفها وإثباتها وتحديد هوية المتورطين فيها، كما يعد الوصول إلى الأثر المادي للجريمة أمرًا معقدًا بالنظر إلى الخصائص المميزة للأدلة المستخلصة منها، وقد شكل ذلك عائقًا أمام السلطة القضائية في مواجهة هذه الجرائم والتصدي لها، مما إستدعى تدخلات تشريعية عاجلة لمواكبة التطور الذي شهدته الظاهرة الإجرامية؛ ومن خلال ذلك توصلنا إلى جملة من النتائج نذكرها فيما يلي:

- تعد الجرائم الماسة بالمستند الإلكتروني من الجرائم التي تتسم بالصعوبة في الإثبات الجنائي، وذلك بالنظر إلى طبيعتها الخاصة التي تميزها عن الجرائم التقليدية، فهذا النوع المستحدث من الجرائم يتطلب أدلة ذات طبيعة خاصة ومختلفة تمامًا عن تلك المعهودة في الجرائم التقليدية، إذ لم يعد الدليل الجنائي التقليدي ملائمًا لطبيعة البيئة التي ترتكب فيها هذه الجرائم، ونظرًا لهذه الخصوصية ظهرت فئة جديدة من الأدلة تتماشى مع طبيعة الوسط الرقمي وهي الأدلة الإلكترونية وقد تعددت التعريفات المتعلقة بها، وتباينت المفاهيم بين من أخذ بمنهج موسع ومن إقتصر على تفسير ضيق، ويعزى هذا التباين إلى موضع العلم الذي تنتمي إليه هذه الأدلة وإلى درجة الإهتمام التي تحظى به، سواء على المستوى الدولي أو ضمن الفقه الجنائي؛
- يتميز الدليل الإلكتروني بمجموعة من الخصائص التي تميزه عن الدليل المادي، وهي خصائص نابعة من طبيعته الرقمية والبيئة التي يستخرج منها، الأمر الذي منحه طبيعة خاصة تميزه عن الأدلة التقليدية الأخرى وتجعله يحتل مكانة مميزة كدليل جنائي في مواجهة الجرائم الماسة بالمستند الالكتروني، ونظرًا للتطور المستمر الذي تشهده البيئة الرقمية التي ينشأ في إطارها الدليل الإلكتروني جعلته من الأدلة المتنوعة والمستحدثة القابلة للتطور والتكيف مع مظاهر رقمية جديدة قد تظهر مع مرور الوقت، وهو ما دفع الفقه القانوني والتشريعات إلى السعي لتصنيفه وتقسيمه بما يتلاءم مع طبيعته المتغيرة والمتجددة؛
- في نظام الإثبات الحر، يتمتع القاضي الجزائي بحرية الإستعانة بجميع وسائل الإثبات التي يراها ضرورية لإصدار حكمه، فإقتناع الشخصي للقاضي ويقينه النابع من ضميره هما الأساسان اللذان يبنى عليهما الحكم بما يتفق مع العقل والمنطق، حيث أنه في هذا النظام لا يفرض المشرع أدلة الإثبات معينة، بل ترك الحرية للقاضي في تأسيس حكمه وفقًا لإقتناعه الشخصي من أي دليل يطرح أمامه في قبوله وحتى في تقديره، إلا أنه ملزم بتسبيب حكمه وبيان الأدلة التي إستند إليها في تكوين قناعته، كما أنه مقيد بجملة من الضوابط سواء ما كان متعلقًا بمبدأ مشروعية الحصول على الدليل، أو بوجوب مناقشة الدليل أثناء المحاكمة؛

- في نظام الإثبات المقيد، يلزم القاضي الجزائي بإتباع وسائل محددة في التعامل مع الأدلة كما يكون مقيدًا بالشروط القانونية الواجب توافرها في كل دليل ليعتد به، ويحكم الدليل في هذا النظام قاعدتان قاعدة إستبعاد شهادة السماع التي تقوم بعدم قبول الوثيقة في الإثبات إلا إذا شهد منشئ مضمونها أمام المحكمة، والثانية قاعدة الدليل الأفضل والتي يقصد بها أن الوثيقة لا تقبل إلا إذا قدمت في شكلها الأصلي، إلا أن هذا النظام أورد إستثناءات لقبول الإثبات عن طريق خضوع مخرجات الإلكترونية والتي هي في أغلبها مستندات إلكترونية إلى قاعدة إستبعاد شهادة سماع وقاعدة الدليل الأفضل؛
- النظام المختلط، يتبع نظامًا وسطًا بين الإثبات الحر والإثبات المقيد، إذ يعتمد القانون على تحديد لأدلة معينة التي يتوجب على القاضي أن يأخذ بها في إثبات بعض الوقائع دون بعضها الآخر، وأيضًا يشترط في الدليل شروطًا معينة في بعض الحالات، كما يعطي للقاضي الحرية في تقدير الأدلة القانونية، وتتفاوت الأنظمة القانونية في العمل بهذا النظام بين دول توسع في الشروط وآخرى تقلل منها؛
- لقد أخذ المشرع الجزائري بنظام الإثبات الحر، يستند في ذلك إلى ما نصت عليه الفقرة الأولى من المادة 349 من القانون رقم: 25-14 المؤرخ في 03 أوت 2025 والمتضمن قانون الإجراءات الجزائية، والتي أجازت إثبات الجرائم بكافة طرق الإثبات بما في ذلك الوسائل الإلكترونية، ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وبذلك فاللقاضي الجزائي حرية الإستعانة بكافة وسائل الإثبات اللازمة لإصدار حكمه بما في ذلك الدليل الإلكتروني لتكوين إقتناعه الشخصي، إلا أنه ملزم بتسبيب حكمه وبيان الأدلة التي إستمد منها إقتناعه، ومقيد بضوابط سواء ما كان متعلق بمبدأ مشروعية الحصول على الدليل الإلكتروني، ووجوبية مناقشة الدليل الإلكتروني؛
- تعد إضافة عبارة "بما فيها الإلكترونية" في الفقرة الأولى من المادة 349 من القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر تأكيدًا صريحًا على شمول الأدلة الإلكترونية ضمن وسائل الإثبات، بعدما كانت غير منصوص عليها صراحة في الفقرة الأولى من المادة 212 من الأمر رقم: 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم والملغى، مما كان يقتضي إخضاعها آنذاك للقواعد العامة في الإثبات؛
- لم ينظم المشرع الجزائري مسألة المستندات الإلكترونية في القانون المدني ولم يقم بوضع تعريف خاص بها، بل إكتفى بالتوسع في مفهوم الكتابة والإثبات بالكتابة في المادة 323 مكرر منه وذلك بموجب التعديل الذي أجراه على القانون المدني بموجب القانون رقم: 05-10 المؤرخ في 20 جوان سنة 2005، إلا أنه تدارك الأمر بموجب القانون رقم: 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير وإستعمال المزور، وإستخدم مصطلح المحرر للدلالة على المستند، ووسع من تعريفه ليشمل كلا من المحرر الورقي والمحرر الإلكتروني بموجب المادة 02 منه؛

- منح المشرع الجزائري للمستند الإلكتروني نفس القوة الثبوتية التي يتمتع بها المستند الورقي التقليدي، وذلك بشرط إستيفائه لمتطلبات محددة أبرزها توافر الشروط الفنية والتقنية اللازمة، لاسيما في عنصري الكتابة والتوقيع الإلكترونيين اللذان يعدان مكافئين في حجيتهما للكتابة والتوقيع التقليديين، ما دامت هذه المستندات الإلكترونية قد إستوفت المتطلبات الفنية والتقنية المنصوص عليها في التشريع الجزائري؛
- أقر المشرع الجزائري بمبدأ التعادل الوظيفي بصيغة واضحة وصريحة بين الكتابة في الشكل التقليدي والكتابة في شكل الإلكتروني بموجب المادة 323 مكرر1 من القانون المدني المعدل والمتمم بالقانون رقم: 05-10 السالف الذكر، فقد إعتبر الكتابة الإلكترونية مقبولة كدليل في الإثبات مثل الكتابة الورقية أي لهما نفس الفعالية من حيث الحجية وصحة الإثبات للإعتداد بالمستند الإلكتروني في الإثبات، حيث أنه ترتبط الكتابة الإلكترونية بالمستند الإلكتروني مثلما ترتبط الكتابة التقليدية بالمستند الورقي وحتى يعتد به قانونًا، وذلك بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها؛
- نص المشرع الجزائري في الفقرة 02 من المادة 327 من القانون المدني المعدل والمتمم بالقانون رقم: 05-10 السالف الذكر على أن يمكن أن يعتد بالتوقيع الإلكتروني ومنحه الحجية القانونية إذا إستوفى الشروط المنصوص عليها في المادة 323 مكرر1 من ذات القانون، وبالتالي فقد ساوى بين التوقيع الإلكتروني والتوقيع الكتابي فى الحماية الجنائية، مما يتضح لنا أن قد إعترف المشرع الجزائري بحجية التوقيع الإلكتروني والإعتداد به رابطًا ذلك بتوفر نفس الشروط المتطلبة في الكتابة الإلكترونية كوسيلة إثبات المنصوص عليها في المادة 323 مكرر1 سالفة الذكر، والمتمثلة في إمكانية التأكد من هوية الشخص الذي أصدر التوقيع، وأن يكون التوقيع معد ومحفوظ في ظروف تضمن سلامته؛
- بمقتضى صدور القانون رقم: 15-04 المؤرخ في 01 فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين أضاف بموجب المادة 07 منه شروطًا إضافية عن تلك المذكوره بنص المادة 323 مكرر1 من القانون المدني والمذكورة أعلاه، وهذه الشروط لابد من توافرها لإضفاء الحجية في التوقيع الإلكتروني الموصوف وليعتد به في الإثبات، تتمثل هذه الشروط في: أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة، وأن يرتبط بالموقع دون سواه، وأن يمكن من تحديد هوية الموقع، وأن يكون مصممًا بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني، وأن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع، وأن يكون مرتبطًا بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهاته البيانات؛
- أضافت المادة 08 من القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر أن التوقيع الإلكتروني الموصوف وحده مماثلًا للتوقيع المكتوب، بإعتبار أن التوقيع الإلكتروني البسيط لا يتوفر على الشروط الواردة في

المادة 07 المذكورة أعلاه وبالتالي لا يتمتع بالحجية التي يحظى بها التوقيع الإلكتروني الموصوف، إلا أن نصت المادة 09 من نفس القانون بعدم تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء، بسبب شكله الإلكتروني أو على الرغم من عدم إعتماده على شهادة تصديق إلكتروني موصوفة، أو أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني، فعلى القاضي ألا يرفضه إذا تمسك به أحد الأطراف أمام القضاء، ولذلك يمنح لمن قدمه كدليل إثبات أن يؤكد مدى جدارة الثقة الموضوعة في الوسائل المنشئة لهذا التوقيع الإلكتروني؛

- سعى المشرع الجزائري من خلال تعديل قانون العقوبات بموجب القانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004 إلى إضافة قسم سابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث منه، وخصصه لجرائم المساس بأنظمة المعالجة الآلية للمعطيات بما في ذلك المعطيات الخاصة بالمستند الإلكتروني، وذلك في إطار مواكبة الحماية الفعالة لأنظمة المعالجة الآلية للمعطيات، ورغبة منه في مواكبة متطلبات العصرنة والسير نحو تطوير المنظومة التشريعية بما يتماشى مع التحولات الرقمية المتسارعة، تأسيسًا بذلك على ما إنتهجته العديد من التشريعات المقارنة؛

- تدارك المشرع الجزائري أهمية مواكبة التطورات المتسارعة خاصة في مجال المعاملات الإلكترونية، وهو ما دفعه إلى التدخل لسد الفراغ التشريعي بهدف إرساء بيئة رقمية آمنة للتعامل عبر شبكة الإنترنت، وقد تم سن القانون رقم: 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين السالف الذكر الذي ساهم في تعزيز الثقة لتعميم التعاملات الإلكترونية، كما خصص ضمن هذا القانون فصلًا كاملًا للأحكام الجزائية المتعلقة بالجرائم الماسة بالتوقيع والتصديق الإلكترونيين وذلك في الفصل الثاني من الباب الرابع، ولم يقتصر هذا القانون على التجريم والعقاب، بل تضمن أيضًا مجموعة من الإلتزامات التي تقع على عاتق الهيئات المكلفة بالتصديق الإلكتروني، بهدف تكريس الثقة والأمان بإعتبارهما عنصرين أساسيين لإزدهار بيئة المعاملات الإلكترونية؛

- إذا كانت المستندات الإلكترونية تنطوي على إثبات وقائع قانونية لها حجيتها في الإثبات، فإن التغيير فى محتواها من شأنه أن ينطوي على مساس بحجية ما تضمنته من وقائع، وهو ما تداركه المشرع الجزائري من خلال إصدار قانون مستقل وخاص بمكافحة التزوير وإستعمال المزور بمقتضى القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر، وألغى جميع الأحكام المخالفة له والمنصوص عليها في قانون العقوبات الجزائري، وقام بالتوسيع من مفهوم المستند ليشمل المستندات الإلكترونية ضمن المستندات محل جريمة التزوير وإستعمالها، وبإضافة أحكام جديدة في سبيل مواجهة هذه السلوكيات الإجرامية والتصدي لها؛

- من خلال دراسة جريمة سرقة معطيات المستند الإلكتروني تبين وإن كان البعض قد إستبعد المعلومات من طائفة الأموال على أساس أنها غير مادية، إلا أن رأيًا آخر يخالفه إذ يرى أن معيار المال لا يحدد بوجود كيان مادي وإنما بالنظر إلى قيمته الإقتصادية، وبناءً عليه يرى هذا الإتجاه أن صلاحية الأموال المعنوية للسرقة كالمستندات الإلكترونية تصلح لأن تكون محلًا للسرقة متى ثبت لها قيمة مالية، ومع ذلك فإن المشرع الجزائري لم ينص على هذه الجريمة بصورة صريحة ضمن نصوصه العقابية، مما يؤدي إلى وجود فراغ تشريعي ويفتح المجال أمام تأويلات بخصوص عبارات المادة 350 من قانون العقوبات، خاصة وأنها لم تشترط صراحة أن يكون المال موضوع السرقة ذا طبيعة مادية؛
- الإستعانة بخبير أو أكثر لتوضيح مسألة معينة قد تواجه أثناء التحريات والتحقيقات، ويعهد بذلك إلى خبراء يتمتعون بدرجة عالية من الكفاءة والتدريب والمعرفة والتمييز في مجال تخصصهم ويتحكمون جيدًا في تقنياتها، ما يؤهلها للتعامل مع هذا النوع المستحدث من الإجرام؛
- تطرق المشرع الجزائري إلى إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بموجب المادة 13 من القانون رقم: 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، وجعل من مهامها وفقًا للمادة 14 من نفس القانون إنجاز الخبرات القضائية وتجميع المعلومات التي تحتاج إليها السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال، بالإضافة إلى تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وتحديد مكان تواجدهم، وقد تمت الإحالة على التنظيم لتحديد كيفيات سير هذه الهيئة؛
- بموجب إلغاء الأمر رقم: 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية بموجب القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية، أعاد هذا الأخير إدراج تقنية المحادثة المرئية عن بعد ضمن المواد من 128 إلى 138 ضمن الفصل السادس من الباب الثاني من الكتاب الثاني، وقد وسع من نطاق الحماية التي كانت مقتصرة في السابق على حماية الشهود والخبراء والضحايا فقط، جعلها تشمل أيضًا حماية المدعين المدنيين والأطراف المدنية والمبلغين، كما توسع في مجال الجرائم التي تطبق فيها هذه الحماية بعد أن كانت مقتصرة فقط في قضايا الجريمة المنظمة أو الإرهاب أو الفساد بسبب المعلومات التي يمكنهم تقديمها للقضاء والتي تكون ضرورية لإظهار الحقيقة، كما أجاز بإمكانية تمديد الحماية إلى جرائم أخرى إذا كانت حالة المعني تستوجب ذلك؛

- شدد المشرع الجزائري العقوبات على كل من يكشف عن هوية أو عنوان الأشخاص المستفدين من الحماية، كما يتعرض المبلغ الذي يقوم بتبليغ عن وقائع غير صحيحة للعقوبات المقررة للوشاية الكاذبة المنصوص عليها في قانون العقوبات الجزائري، كما أدرج في المقابل إعفاء هذا الأخير من المتابعة التأديبية أو الجزائية بإفشاء السر المهني لتبليغه عن جرائم أطلع عليها أثناء أو بمناسبة أداء مهامه؛
- تم إلغاء الأمر رقم: 20-04 المؤرخ في 20 أوت 2020 المعدل والمتمم للأمر رقم: 66-155 والمتضمن قانون الإجراءات الجزائية بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية، غير أن هذا الأخير أعاد تنظيم الأحكام المتعلقة بإستعمال وسائل الإتصال المسموعة والمرئية أثناء الإجراءات بإدراجها في المواد من 639 إلى 650 ضمن الكتاب الخامس، ومكن الجهات القضائية لمقتضيات حسن سير العدالة أو حماية المتهم أو الحفاظ على الأمن والنظام العام أو الصحة العمومية أو أثناء الكوارث الطبيعية أو لدواعي إحترام مبدأ الآجال المعقولة، إستعمال المحادثة المرئية عن بعد في الإجراءات القضائية مع إحترام الحقوق والقواعد المنصوص عليها في هذا القانون؛
- أدرج المشرع الجزائري إجراء التسرب بمقتضى القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية، حيث أفرد له الفصل الخامس تحت عنوان "في التسرب" من الباب الثاني من الكتاب الأول، والذي تضمن ثمانية مواد تمتد من المادة 65 مكرر11 إلى المادة 65 مكرر18، ورغم إلغاء الأمر رقم: 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، بموجب القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية، فقد أبقى المشرع الجزائري على هذا الإجراء، وأعاد تنظيمه ضمن المواد من 120 إلى 127 المدرجة في الفصل الخامس من الباب الثاني من الكتاب الثاني؛
- أدرج المشرع الجزائري إجراء إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور بمقتضى القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية، حيث أفرد فصلًا رابعًا تحت عنوان "في إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور" من الباب الثاني من الكتاب الأول، والذي تضمن مواد تمتد من المادة 65 مكرر5 إلى المادة 65 مكرر10، ورغم إلغاء الأمر رقم: 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، بموجب القانون رقم: 25-14 المؤرخ في 03 أوت 2025 المتضمن قانون الإجراءات الجزائية، فقد أبقى المشرع الجزائري على هذا الإجراء، وأعاد تنظيمه ضمن المواد من 114 إلى 119 المدرجة في الفصل الرابع من الباب الثاني من الكتاب الثاني؛
- أجاز المشرع الجزائري الدخول بغرض التفتيش ولو عن بعد، إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها، أو منظومة تخزين معلوماتية، بموجب الفقرة الأولى من المادة 05 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم

المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر، وأيضًا في الفقرة الأولى من المادة 16 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر قصد معاينة الجرائم المنصوص عليها في هذا القانون بما في ذلك جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور؛

- أجاز المشرع الجزائري للسلطات القضائية المكلفة بالتفتيش تمديد التفتيش، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى أو جزء منها في إقليمها، وأن هذه المعطيات يمكن الدخول إليها إنطلاقًا من المنظومة الأولى، بعد إعلام السلطة القضائية المختصة بذلك مسبقًا، طبقًا للفقرة 02 من المادة 05 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر؛

- إذا تبين مسبقًا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقًا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطـني، فـإن الحصول عليها لا يتم إلا في إطار المساعدة المتبادلة مع السلطات الأجنبية المختصة طبقًا للإتفاقيات الدولية ذات الصلة ووفقاً لمبدأ المعاملة بالمثل، طبقًا للفقرة 03 من المادة 05 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر؛

- أجاز المشرع الجزائري صراحة ضبط المكونات المعنوية، بإعتبارها صالحة لأن تكون محلًا للضبط، تحت عنوان "حجز المعطيات المعلوماتية" بموجب القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر، وقد خول للسلطات القضائية المكلفة بالتفتيش طريقتين لضبط المعطيات المعلوماتية التي كانت موضوع التفتيش، إما بحجز المنظومة برمتها، أو يحجز جزء منها عن طريق نسخ المعطيات محل البحث على دعامة تخزين إلكترونية، تكون هذه الأخيرة قابلة للحجز والوضع في أحراز مختومة وفقًا لما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية، وفي حالة إذا إستحال إجراء الحجز وفقًا للطريقة الأولى لأسباب تقنية، يتعين على السلطة المختصة بالتفتيش والحجز أن تستعمل التقنيات المناسبة من أجل منع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو القيام بنسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة؛

- إستحدث المشرع الجزائري بموجب المادة 03 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر إجراء مراقبة الإتصالات الإلكترونية، وهو إجراء يهدف إلى وضع الترتيبات التقنية للإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، إذا إستدعت ذلك مقتضيات حماية النظام العام من إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو

الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني، أو للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولة المتبادلة، وقد تطرق المشرع إلى الضوابط لهذا الإجراء في المادة 04 من نفس القانون؛

- ألزم المشرع الجزائري مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة بموجب المادة 10 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر، وحدد المعطيات المتعلقة بحركة السير التي يتعين عليهم التحفظ عليها في المادة 11 من نفس القانون، وحدد مدة حفظ لتلك المعطيات بسنة واحدة (01) إبتداءً من تاريخ التسجيل؛

- أقر المشرع الجزائري المسؤولية الإدارية على عاتق مقدمي الخدمات في حال إخلالهم بإلتزاماتهم بوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المكلفة بالتحريات القضائية، إلى جانب المسؤولية الجزائية التي تترتب عندما تؤدي أعمالهم إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (06) أشهر إلى خمس (05) سنوات، وبغرامة من خمسون ألف 50.000 دج إلى خمسمائة ألف 500.000 دج، بينما تطبق على الشخص المعنوي الغرامة تقدر وفقًا للقواعد المنصوص عليها في قانون العقوبات أي بما تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وبالتالي فإن العقوبة المالية تقدر بمليوني وخمسمائة ألف 2.500.000 دج، بموجب الفقرتين 04 و05 من المادة 11 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر؛

- إن الطبيعة العابرة للحدود التي تتسم بها الجرائم الماسة بالمستند الإلكتروني قد أفرزت العديد من الإشكالات حول تحديد الدولة صاحبة الإختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه، بالإضافة إلى إشكالات تتعلق بإجراءات الملاحقة القضائية، لذلك فقد حسم المشرع الجزائري مسألة الإختصاص القضائي في هذا النوع من الجرائم، ومنح للقضاء الجزائري صلاحية النظر فيها بغض النظر عن مرتكب الجريمة أو نوعها أو مكان الإعتداء، كما منح بموجب المادة 15 من القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر للمحاكم الجزائرية سلطة النظر في هذه الجرائم المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيًا أو تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني، وهو ما نصت عليه المادة 12 من القانون رقم: 24-02 المتعلق بمكافحة التزوير وإستعمال المزور السالف الذكر بإختصاص

الجهات القضائية الجزائرية بالنظر في الجرائم المنصوص عليها في هذا القانون بما في ذلك جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور التي ترتكب خارج الإقليم الوطني وتؤدي بإضرار الجزائر و/أو بمؤسساتها و/أو بمواطنيها؛

- نص المشرع الجزائري في القانون رقم: 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السالف الذكر على تمكين السلطات المختصة من تبادل المساعدة القضائية الدولية في جمع الأدلة الإلكترونية وكشف مرتكبيها، وذلك في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم الماسة بالمستند الإلكتروني، ويمكن في حالة الإستعجال ومع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية، إذا وردت عن طريق وسائل الإتصال السريعة بما في ذلك أجهزة الفاكس أوالبريد الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها، بالإضافة إلى أن تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات، أو إتخاذ أي إجراءات تحفظية وفقًا للإتفاقيات الدولية ذات الصلة والإتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل، وقد إشترط على أن تكون الإستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة، وكذا بشرط عدم إستعمالها في غير ما هو موضح في الطلب، وأن ترفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

مقترحات البحث:

وتجدر بنا الإشارة إلى أنه من خلال هذه الدراسة توصلنا إلى مجموعة من الإقتراحات نذكرها كما يلي:

- ضرورة الإلتزام بالإعلام في الجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، وذلك بأن يتدخل المشرع الجزائري لإقرار إلزام الشاهد المعلوماتي بأن يدلي ما يحوزه من المعلومات الجوهرية هامة واللازمة للولوج إلى منظومة المعلوماتية، أو الكشف عن الشفرات المدون بها الأوامر الخاصة بتنفيذ البرامج، أو بأن يقوم بطباعة ملفات المعطيات المخزنة في ذاكرة الجهاز، قصد التعاون مع سلطات التحقيق، بإستثناء حالات المحافظة على سر المهنة فإنهم لا يعفيهم من هذا الإلتزام إلا التمسك بإحترام السر المهني؛
- من الأنسب أن يتدخل المشرع الجزائري لإقرار عقوبات على الشاهد المعلوماتي في حالة إمتناعه عن الإدلاء بشهادته، وذلك في غير الأحوال التي يجيز له القانون فيها ذلك، وأن يسأل الشاهد الذي يخفي الشفرة أو كلمة السر أو الذي يعطي أوامر خاطئة عن جريمة شهادة الزور لأنه يعوق سير العدالة، أو يسأل بإعتباره شريكًا في الجريمة موضوع المحاكمة؛
- تشجيع المجني عليه بالإبلاغ عن أية جريمة معلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص فور ملاحظتها، وحبذا لو ينص المشرع الجزائري على جزاء عدم الإبلاغ عما يصل الأشخاص بحكم مهنتهم أو وظيفتهم من أخبار

عن وقوع تلك الجرائم، وإلزامية التعاون مع السلطات المختصة مع تقدير الجزاء عن الإخلال بهذا الإلتزام؛

- من الأنسب على المشرع الجزائري أن يتدارك القصور التشريعي من خلال التدخل بإعادة النظر في المادة 126 من ق.إ.ج.ج، بترك مجال تمديد المدة الزمنية لإجراء التسرب بفتح إمكانية تمديد المدة الزمنية لإجراء التسرب بما يتيح للمتسرب مواصلة نشاطه متى إقتضت الضرورة ذلك، شريطة أن يتم هذا التمديد في ظروف تضمن أمنه وسلامته وتحت رقابة الجهة القضائية المختصة التي أصدرت الإذن بالتسرب، لأن مهلة ثمانية (08) أشهر غير كافية دائمًا لتأمين أمن المتسرب وسلامته لما قد يشكله هذا التوقف من خطر على حياته، ويلاحظ أن هذا الفراغ التشريعي لم يطرأ حديثًا بل كان قائمًا في ظل الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم السالف الذكر، إلا أنه إستمر رغم إلغاء هذا الأمر بموجب القانون رقم: 25-14 المتضمن قانون الإجراءات الجزائية السالف الذكر، مما يبرز الحاجة الملحة لتدخل تشريعي يعالج هذا القصور؛
- من الأنسب أن يتدخل المشرع الجزائري لإقرار إمكانية الإعتماد على شهادة الضابط أو العون المتسرب وأن لا يقتصر الأمر على الضابط المنسق للعملية، وذلك عن طريق وضع وسائل تقنية توفر له الحماية تسمح بكتمان هويته بما في ذلك السماع عن طريق المحادثة المرئية عن بعد وإستعمال الأساليب التي لا تسمح بمعرفة صورته وصوته، وذلك كتدبير من التدابير الحماية لحياته أو سلامته الجسدية أو حياة أو سلامة أفراد عائلاته أو أقاربه؛
- من الأنسب أن يتدخل المشرع الجزائري وينظم كل المسائل المتعلقة بإجراء مراقبة الإتصالات الإلكترونية، بأن يستوجب من السلطات القضائية المختصة بعد الإنتهاء من مباشرة عملية المراقبة تحرير محضر، ووضع التسجيلات الخاصة بالمراقبة في أحراز مغلقة مع ختمها بالأختام الرسمية المغلقة، وأن يجيز إمكانية إتلاف تلك التسجيلات بعد إنتهاء التحقيق والمحاكمة؛
- من الأنسب أن يتدخل المشرع الجزائري ويحدد مصير مضمون إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور وذلك بعد إنقضاء الدعوى العمومية، من حيث تحديد ما إذا كان يجب تحطيمها أو إتلافها أو الإحتفاظ بها ضمن المحاضر التي تبقى مدرجة في ملف الدعوى، وهو ما يستدعي تدخلًا تشريعيًا صريحًا لحسم هذا الإشكال؛
- من الأنسب الإهتمام أكثر بالتأهيل التقني والفني لسلطات التحري والتحقيق في مجال إستخلاص الأدلة الإلكترونية، وإخضاعهم لتدريبات ودورات تعليمية تقنية متخصصة ومكثفة، وإمدادهم بأفضل وسائل التقنية الحديثة ونظم المعلومات التي تمكنهم من الحصول عليها؛
- من الأنسب أن يتدخل المشرع الجزائري لتدارك القصور التشريعي وذلك بإيراد نص صريح وواضح يجرم فيه السرقة المعلوماتية، سواء من خلال سن تشريعات جديدة تضيف

أحكامًا جديدة وإلحاقها بقانون العقوبات، أو عبر تعديل نص المادة 350 من قانون العقوبات بحيث يجعلها تشمل إلى جانب السرقة التقليدية السرقة المعلوماتية، وهو ما لا يتقرر إلا بجعل فعل الإختلاس ينصب على الأشياء المادية وغير المادية؛

- ضرورة سن قانون مستقل خاص بالجرائم المعلوماتية على وجه العموم ولاسيما الجرائم الماسة بالمستند الإلكتروني على وجه الخصوص، وإقرار المزيد من الجزاءات الرادعة على هذا النوع المستحدث من السلوكيات الإجرامية، وضرورة التصدي لها إزاء الفراغ التشريعي لمكافحة هذه الظاهرة الإجرامية الجديدة المرتبطة بالتطور التكنولوجي، وتطوير المنظومة التشريعية في مجال الإثبات الإلكتروني بمواكبة التطور الذي يطرأ على الجرائم بصورة عامة؛
- التركيز على الجانب الوقائي بنشر الوعي والثقافة القانونية بين أفراد المجتمع، بواسطة أجهزة المجتمع بما فيها وسائل الإعلام من أجل إدراكهم بخطورة هذه الجرائم وما تسببه من أضرار والإستخدام السيء لها، وأهمية التبليغ عن مرتكبيها حتى تسهل السيطرة عليها.

أفاق البحث:

تعد المنظومة المعلوماتية جزءًا لا غنى عنها في جميع مجالات الأنشطة، بحيث أصبحت جزءًا أساسيًا من الحياة اليومية، لكن بقدر ما وفرت هذه المنظومة العديد من الإيجابيات ومجموعة خيارات، بقدر ما تهدد للمراكز القانونية القائمة والناشئة، مما إستدعى التصدي لها، ورغم أن التصدي لهذه التحديات قد يبدو سهلًا من الناحية النظرية في سن القوانين، إلا أن يعد أمرًا صعبًا من الناحية الإجرائية، ومن هذا المنطلق يمكننا أن نبحث أيضًا في كيفية تأمين المستندات الإلكترونية، وكفاءة الأجهزة القضائية في تصدي لهذه الظاهرة.

قائمة المصادر والمراجع

I. قائمة المصادر:

أولًا: الدستور

المرسوم الرئاسي رقم: 20-442 المؤرخ في 30 ديسمبر 2020، المتضمن التعديل الدستوري، ج.ر.ج.ج.ش العدد 82، سنة 2020.

ثانيًا: المواثيق الدولية

1. الإتفاقية الأوروبية الخاصة بالجرائم المعلوماتية الموقعة في بودابست في 23 نوفمبر 2001.
2. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تم اعتمادها من قبل مجلس وزراء العرب والداخلية بتاريخ 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم: 14-252 المؤرخ في 08 سبتمبر 2014، ج.ر.د.ش ،العدد 54، سنة 2014.

ثالثًا: النصوص التشريعية

أ- النصوص القانونية الدولية:

1. قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996 مع المادة 5 مكررا الإضافية بصيغتها المعتمدة في عام 1998، الصادر عن هيئة الأمم المتحدة في جلستها 605 المنعقدة في 1996/12/16.
2. القانون النموذجي بشأن التوقيعات الإلكترونية الصادر عن لجنة الأمم المتحدة لقانون التجارة الدولية الأونسيترال سنة 2001.
3. التوجه الأوروبي رقم: 1999-93 بشأن الإطار المشترك للتواقيع الإلكترونية الصادر بتاريخ 13 ديسمبر 1999.

ب- النصوص القانونية في التشريع الجزائري:

ب-1- القوانين:

1. القانون رقم: 2000-03 المؤرخ في 05 أوت 2000، المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج.ر.ج.ج.ش العدد 48، الصادرة في 06 أوت 2000.
2. القانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم: 66-156 المتضمن قانون العقوبات، ج.ر.ج.ج.ش العدد 71، الصادرة في 10 نوفمبر 2004.
3. القانون رقم: 05-10 المؤرخ في 20 جوان 2005، المعدل والمتمم للأمر رقم: 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، ج.ر.ج.ج.ش العدد 44، الصادرة في 26 جوان 2005.

4. القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006، المتضمن تعديل للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية الجزائري، ج.ر.ج.ج.ش العدد 84، الصادرة في 24 ديسمبر 2006، ملغى.
5. القانون رقم: 09-04 المؤرخ في 05 أوت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج.ش العدد 47، الصادر بتاريخ 16 أوت 2009.
6. القانون رقم: 14-03 المؤرخ في 24 فيفري 2014، المتعلق بسندات ووثائق السفر، ج.ر.ج.ج.ش العدد 16، الصادرة في 23 مارس 2014.
7. القانون رقم: 15-03 المؤرخ في 01 فيفري 2015، المتعلق بعصرنة العدالة، ج.ر.ج.ج.ش العدد 06، الصادرة بتاريخ 10 فيفري 2015.
8. القانون رقم: 15-04 المؤرخ في 01 فيفري 2015، المحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج.ش العدد 06، الصادرة في 10 فيفري 2015.
9. القانون رقم: 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير وإستعمال المزور، ج.ر.ج.ج.ش العدد 15، الصادرة في 29 فيفري 2024.
10. القانون رقم: 24-06 المؤرخ في 28 أفريل 2024، المعدل والمتمم للأمر رقم: 66-156 والمتضمن قانون العقوبات، ج.ر.ج.ج.ش العدد 30، الصادرة بتاريخ 30 أفريل سنة 2024.

ب-2- الأوامر:

1. الأمر رقم: 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية الجزائري، ج.ر.ج.ج.ش العدد 48، الصادرة في 10 جوان 1966، المعدل والمتمم.
2. الأمر رقم: 66-156 المؤرخ في 08 جوان 1966، المتضمن القانون العقوبات الجزائري، ج.ر.ج.ج.ش العدد 49، الصادرة في في تاريخ 11 جوان 1966، المعدل والمتمم.
3. الأمر رقم: 15-02 المؤرخ في 23 جويلية 2015، المعدل والمتمم للأمر رقم: 66-155 المورخ في 08 جوان 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج.ش العدد 40، الصادرة بتاريخ 23 جويلية 2015.
4. الأمر رقم: 20-04 المؤرخ في 30 أوت سنة 2020، المعدل والمتمم للأمر رقم: 66- 155 المؤرخ في 08 جوان سنة 1996 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج.ش العدد 51، الصادرة في 31 أوت سنة 2020.
5. الأمر رقم: 21-11 المؤرخ في 25 أوت 2021، المتمم للأمر رقم: 66-155 المؤرخ في 08 جوان 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج.ش العدد 65، الصادرة بتاريخ 26 أوت 2021.

رابعًا: النصوص التنظيمية

أ- المراسيم الرئاسية:

1. المرسوم الرئاسي رقم: 04-183 المؤرخ في 26 جوان 2004، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر.ج.ج.ش العدد 41، الصادرة في 27 جوان 2004، المعدل والمتمم.
2. المرسوم الرئاسي رقم: 04-432 المؤرخ في 29 ديسمبر 2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، ج.ر.ج.ج.ش العدد 84، الصادرة بتاريخ 29 ديسمبر 2004.
3. المرسوم الرئاسي رقم: 09-143 المؤرخ في 27 أفريل سنة 2009، المتضمن مهام الدرك الوطني وتنظيمه، ج.ر.ج.ج.ش العدد 26، الصادرة في 03 ماي سنة 2009، المعدل والمتمم.
4. المرسوم الرئاسي رقم: 14-252 المؤرخ في 08 سبتمبر 2014، ج.ر.ج.ج.ش العدد 57، الصادرة بتاريخ 28 سبتمبر 2014.
5. المرسوم الرئاسي رقم: 15-261 المؤرخ في 08 أكتوبر 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج.ش العدد 53، الصادرة بتاريخ 08 أكتوبر 2015، ملغى.
6. المرسوم الرئاسي رقم: 19-172 المؤرخ في 06 جوان 2019، المحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر.ج.ج.ش العدد 37، الصادرة بتاريخ 09 جوان 2019، ملغى.
7. المرسوم الرئاسي رقم: 20-183 المؤرخ في 13 جويلية 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج.ش العدد 40، صادرة بتاريخ 18 جويلية 2020، ملغى.
8. المرسوم الرئاسي رقم: 21-439 المؤرخ في 07 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج.ش العدد 86، الصادرة في 11 نوفمبر.
9. المرسوم الرئاسي رقم: 23-313 المؤرخ في 03 سبتمبر سنة 2023، المعدل والمتمم للمرسوم الرئاسي رقم: 09-143 المؤرخ في 27 أفريل سنة 2009، المتضمن مهام الدرك الوطني وتنظيمه، ج.ر.ج.ج.ش العدد 59، الصادرة بتاريخ 10 سبتمبر 2023.

ب- المراسيم التنفيذية:

1. المرسوم التنفيذي رقم: 01-123 المؤرخ في 09 ماي 2001، المتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات

المواصلات السلكية واللاسلكية، ج.ر.ج.ج.ش العدد 27، الصادرة بتاريخ 13 ماي 2001، ملغى.
2. المرسوم التنفيذي رقم: 07-162 المؤرخ في 30 ماي 2007، المعدل والمتمم للمرسوم التنفيذي رقم: 01-123 المؤرخ في 09 ماي 2001، ج.ر.ج.ج.ش العدد 37، الصادرة بتاريخ 07 ماي 2007، ملغى.
3. المرسوم التنفيذي رقم: 15-320 المؤرخ في 13 ديسمبر 2015، المحدد نظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر.ج.ج.ش العدد 68، الصادرة بتاريخ 27 ديسمبر 2015.
4. المرسوم التنفيذي رقم: 16- 134 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسير مهامها، ج.ر.ج.ج.ش العدد 26، الصادرة في 28 أفريل 2016.
5. المرسوم التنفيذي رقم: 16-135 المؤرخ في 25 أفريل 2016، المحدد لطبيعة السلطة الحكومية للتصديق الإلكتروني وتشكيلها وتنظيمها وسيرها، ج.ر.ج.ج.ش العدد 26، الصادرة 28 أفريل 2016.
6. المرسوم التنفيذي رقم: 16-142 المؤرخ في 05 ماي سنة 2016، يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيًا، ج.ر.ج.ج.ش العدد 28، الصادرة في 08 ماي 2016.
7. المرسوم التنفيذي رقم: 17-324 المؤرخ في 08 نوفمبر 2017، يحدد شروط وكيفيات تعيين المساعدين المتخصصين لدى النيابة العامة وقانونهم الأساسي ونظام تعويضاتهم، ج.ر.ج.ج.ش العدد 67، الصادرة في 15 نوفمبر2017.

ج- القرارات:

1. قرار وزاري مشترك المؤرخ في 14 أفريل 2007، المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، ج.ر.ج.ج.ش العدد 36، الصادرة في 03 جوان 2007.
2. قرار وزير العدل المؤرخ في 07 مارس 2018، يحدد قائمة التخصصات التي يعين فيها المساعدون المتخصصون والجهات القضائية المعنية، ج.ر.ج.ج.ش العدد22، الصادرة 18 أفريل 2018.

II. قائمة المراجع:

أولًا: الكتب

أ- الكتب المتخصصة:

1. أحمد خليفة الملط، **الجرائم المعلوماتية**، الطبعة الثانية، 2006، دار الفكر الجامعي، الإسكندرية-مصر.

2. أحمد يوسف الطحطاوي، **الأدلة الإلكترونية ودورها في الإثبات الجنائي (دراسة مقارنة)**، د.ر.ط، 2015، دار النهضة العربية، القاهرة-مصر.

3. آمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري**، الطبعة الثانية، 2007، دار هومة للطباعة النشر والتوزيع الجزائر.

4. إيهاب فوزي السقا، **جريمة التزوير في المحررات الإلكترونية**، د.ر.ط، 2008، دار الجامعة الجديدة للنشر، الإسكندرية-مصر.

5. بن مكي نجاة، **السياسة الجنائية لمكافحة جرائم المعلوماتية**، د.ر.ط، 2017، دار الخلدونية، القبة القديمة- الجزائر.

6. بهاء المري، **جرائم السوشيال ميديا فيس بوك-أنستجرام-واتس آب-فايبر-تويتر وجرائم المحمول وحجية الدليل الإلكتروني في الإثبات**، الطبعة الرابعة، 2022، دار الأهرام، مصر.

7. علي جعفر، **جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة**، الطبعة الأولى، 2013، منشورات زين الحقوقية، بيروت-لبنان.

8. حدة بوخلفة، **المسؤولية الجنائية لمقدمي خدمات الإنترنت**، د.ر.ط، 2019، دار هومة، الجزائر.

9. حسان سعاد، **إثبات التعاملات الإلكترونية وفقاً للقانون الجزائري والتشريعات المقارنة**، الطبعة الأولى، 2019، مكتبة الوفاء القانونية، الإسكندرية-مصر.

10. حسين محمد الغول، **جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها دراسة مقارنة**، الطبعة الأولى،2017، مكتبة بدران الحقوقية، لبنان.

11. حمزة بن عقون، **السلوك الاجرامي للمجرم المعلوماتي**، د.ر.ط، جوان 2019، دار تديكلت، الجزائر.

12. حنان ريحان مبارك المضحكي، **الجرائم المعلوماتية دراسة مقارنة**، الطبعة الأولى، 2014، منشورات الحلبي الحقوقية بيروت- لبنان.

13. خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، الطبعة الأولى، 2011، دار الثقافة للنشر والتوزيع، عمان-الأردن.

14. خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، الطبعة الأولى، 2009، دار الفكر الجامعي، الإسكندرية-مصر.

15. خالد ممدوح إبراهيم، **الخبرة القضائية الرقمية في الجرائم المعلوماتية دراسة مقارنة في القانون المصري والإماراتي والأمريكي**، الطبعة الأولى، 2023، دار الفكر الجامعي، الإسكندرية-مصر.

16. خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، الطبعة الأولى، 2009، دار الفكر الجامعي، الإسكندرية-مصر.

17. خثير مسعود، **الحماية الجنائية لبرامج الكومبيوتر أساليب وثغرات**، د.ر.ط، 2010، دار الهدى، عين ميلة- الجزائر.

18. رامي متولي القاضي، عمر سالم، **شرح قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 مقارناً بالتشريعات المقارنة والمواثيق الدولية**، الطبعة الأولى، 2020، مركز الدراسات العربية للنشر والتوزيع، مصر.

19. رفاه خضير جياد العارضي، **الدليل الإلكتروني وآثره في مجال نظرية الإثبات الجنائي دراسة مقارنة**، الطبعة الأولى، 2019، منشورات زين الحقوقية، بيروت-لبنان.

20. زيبحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، د.ر.ط، 2011، دار الهدى، عين ميلة- الجزائر.

21. سحر سعد عبد السميع محمد، **الحماية الجنائية للتوقيع الإلكتروني**، د.ر.ط، 2022، دار الفكر والقانون، مصر.

22. سعد عاطف عبد المطلب حسنين، **الحماية الجنائية للمصنفات الرقمية دراسة مقارنة**، الطبعة الأولى، 2018، دار الفكر الجامعي، الإسكندرية-مصر.

23. سعيداني نعيم، **الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)**، المؤسسة الحديثة للكتاب، الطبعة الأولى، 2022، لبنان.

24. شنتير خضرة، **الآليات القانونية لمكافحة الجريمة الإلكترونية دراسة مقارنة**، مؤسسة الكتاب القانوني إبن النديم، الطبعة الأولى، ماي 2022، الجزائر.

25. شيخ سناء، **أدلة الإثبات المكتوبة التقليدية والإلكترونية في القانون الجزائري**، د.ر.ط، 2021، النشر الجامعي الجديد، تلمسان –الجزائر.

26. شيماء عبد الغني محمد عطاالله، **الحماية الجنائية للتعاملات الإلكترونية**، د.ر.ط، 2007، دار الجامعة الجديدة، الإسكندرية-مصر.

27. طارق إبراهيم الدسوقى عطية، **الأمن المعلوماتي النظام القانوني للحماية المعلوماتية**، دون ذكر رقم الطبعة، 2009، دار الجامعة الجديدة للنشر، الإسكندرية-مصر.

28. عادل مشموشي، **جرائم المعلوماتية وتحديات مسارحها الإفتراضية، أدواتها الإلكترونية، أساليبها التقنية، مقتضياتها التشريعية**، المؤسسة الحديثة للكتاب، الطبعة الأولى، 2019، لبنان.

29. عائشة بن قارة مصطفى، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، د.ر.ط، د.س.ن، دار الجامعة الجديدة، الإسكندرية-مصر.

30. عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)**، الطبعة الأولى، 2006، دار الفكر الجامعي، الإسكندرية-مصر.

31. عبدالفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، د.ر.ط، 2005، دار الكتب القانونية، مصر.

32. عبدالله سيف الكيتوب، **الأحكام الإجرائية لجريمة الإحتيال المعلوماتي**، د.ر.ط، 2013، دار النهضة العربية، القاهرة-مصر.

33. علي جبار الحسيناوي، **جرائم الحاسوب والإنترنت**، د.ر.ط، 2009، دار اليازوري العلمية للنشر والتوزيع، عمان- الأردن.

34. علي جعفر، **جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة**، الطبعة الأولى، 2013، منشورات زين الحقوقية.

35. علي عدنان فيل، **إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)**، د.ر.ط، 2012، دار الكتب والوثائق القومية، الإسكندرية-مصر.

36. عميمر عبدالقادر، **التحديات القانونية لإثبات الجريمة المعلوماتية**، د.ر.ط، 2021، النشر الجامعي الجديد، تلمسان-الجزائر.

37. فؤاد حسين العزيزي، **الجرائم المعلوماتية دراسة مقارنة**، د.ر.ط، 2014، دار الفكر الجامعي، الإسكندرية-مصر.

38. لورنس محمد عبيدات، **إثبات المحرر الإلكتروني**، الطبعة الأولى، 2009، دار الثقافة للنشر والتوزيع، عمان-الأردن.

39. مثنى سعد السوداني، **التزوير المعلوماتي في الحاسب الآلي دراسة مقارنة**، الطبعة الأولى، 2022، دار مصر للنشر والتوزيع، القاهرة-مصر.

40. محمد أمين الرومي، **جرائم الكمبيوتر والإنترنت**، د.ر.ط، 2004، دار المطبوعات الجامعية، الإسكندرية-مصر.

41. محمد حماد مرهج الهيتي، **جرائم الحاسوب ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها**، الطبعة الأولى، 2006، دار المناهج للنشر والتوزيع، عمان-الأردن.

42. محمد كمال محمود الدسوقي، **الحماية الجنائية لسرية المعلومات الإلكترونية دراسة مقارنة**، الطبعة الأولى، 2015، دار الفكر والقانون، مصر.

43. محمود سعد عبد المجيد، **الجرائم السيبرانية وإنعكاسات ثورة تكنولوجيا المعلومات والإتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية دراسة تحليلة وصفية مقارنة**، د.ر.ط، 2023، دار المطبوعات الجامعية، الإسكندرية-مصر.

44. منصارة يوسف، **الدليل الإلكتروني في القانون الجزائي الطريق إلى تحول أدلة الاثبات في المادة الجزائية دراسة مقارنة**، د.ر.ط، 2018، دار الخلدونية، الجزائر.

45. ناني لحسن، **التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية**، د.ر.ط، 2018، النشر الجامعي الجديد، تلمسان-الجزائر.

46. هلالي عبد اللاه أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست الموقعة في 23 نوفمبر 2001**، د.ر.ط، 2006، دار النهضة العربية، القاهرة.

ب- الكتب العامة:

1. أحسن بوسقيعة، **التحقيق القضائي**، الطبعة الثالثة عشرة، 2021، دار هومة، الجزائر.
2. أحسن بوسقيعة، **الوجيز في القانون الجزائي الخاص**، الجزء الثاني، الطبعة السابع عشرة، 2018، دار هومة للطباعة والنشر والتوزيع، الجزائر.
3. أحمد غاي، **ضمانات المشتبه فيه أثناء التحريات الأولية دراسة مقارنة للضمانات النظرية التطبيقية المقررة للمشتبه فيه في التشريع الجزائري والتشريعات الأجنبية والشريعة الاسلامية**، الطبعة الثالثة، 2017، دار هومة، الجزائر.
4. إلهام حورية ساعد، **المحاضر في المادة الجزائية**، د.ر.ط، 2023، دار بلقيس للنشر، دار البيضاء- الجزائر.
5. عبدالرحمان خلفي، **الإجراءات الجزائية والمقارن**، الطبعة الرابعة، 2018-2019، دار بلقيس، دار البيضاء-الجزائر.
6. عبدالله أوهايبية، **شرح قانون الإجراءات الجزائية الجزائري**، الجزء الأول، الطبعة الثانية 2018، دار هومة، الجزائر.
7. محمد حزيط، **أصول الإجراءات الجزائية في القانون الجزائري على ضوء آخر التعديلات لقانون الإجراءات الجزائية والإجتهاد القضائي**، الطبعة الثانية، 2019، دار هومة، الجزائر.
8. نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الأول، الطبعة الرابعة، 2018، دار هومة، الجزائر.
9. نجيمي جمال، **قانون الإجراءات الجزائية الجزائري على ضوء الإجتهاد القضائي (مادة بمادة)**، الجزء الثاني، الطبعة الرابعة، 2018، دار الهومة، الجزائر.

ثانيًا: الرسائل الجامعية

أ- أطروحات الدكتوراه:

1. أزرو محمد رضا، **إشكالية إثبات العقود الالكترونية دراسة مقارنة**، أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد-تلمسان، 2015-2016.
2. أومدور رجاء، **خصوصية التحقيق في مواجهة الجرائم المعلوماتية**، أطروحة الدكتوراه الطور الثالث ل.م.د، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي -برج بوعريريج، 2020-2021.

3. باهة فاطمة، **آثار قواعد الإثبات الإلكتروني على المراكز القانونية للخصوم "دراسة مقارنة"**، أطروحة الدكتوراه علوم، تخصص: قانون إجرائي، فرع: حقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي ليابس بسيدي بلعباس، 2017 /2018.
4. بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، أطروحة الدكتوراه علوم، كلية الحقوق، جامعة الجزائر 01 – بن يوسف بن خدة-، 2018/2017.
5. براهيمي جمال، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة الدكتوراه علوم، تخصص: القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري- تيزي وزو، 2018.
6. بشرى زلاسي، **المعطيات الحديثة للحاسب الإلكتروني الكمبيوتر وحجيتها في الإثبات المدني**، أطروحة الدكتوراه، قسم: القانون الخاص، كلية الحقوق، جامعة الجزائر1، 2013/2012.
7. بلحسيني حمزة، **الحماية الجزائية للمستند الإلكتروني**، أطروحة الدكتوراه علوم، تخصص: علوم قانونية فرع: قانون البنوك، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، 2019-2020.
8. بلقنيشي حبيب، **إثبات التعاقد عبر الإنترنت (البريد المرئي) -دراسة مقارنة-**، أطروحة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة وهران –السانيا، 2010/ 2011.
9. بن شهرة شول، **الحماية الجنائية للتجارة الإلكترونية**، أطروحة الدكتوراه، تخصص: قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر-بسكرة، 2009-2010.
10. بن طالب ليندا، **الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)**، أطروحة الدكتوراه علوم، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2019.
11. بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، أطروحة الدكتوراه علوم، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2014/ 2015.
12. بوكر رشيدة، **الحماية الجزائية للتعاملات الإلكترونية**، أطروحة الدكتوراه علوم، تخصص: قانون جزائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس - سيدي بلعباس-، 2017.
13. التوجي محمد، **الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال**، شهادة الدكتوراه، تخصص: القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية أدرار، 2019/2018.

14. حاحة عبد العالي، **الآليات القانونية لمكافحة الفساد الإداري في الجزائر**، أطروحة الدكتوراه علوم، تخصص قانون عام، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر-بسكرة، 2013/2012.
15. حبيباتني بثينة، **الجرائم المتصلة بتكنولوجيات الإعلام والإتصال**، أطروحة الدكتوراه ل.م.د، تخصص: قانون جنائي وعلم الإجرام، كلية الحقوق، جامعة الجزائر1، 2020.
16. حدة بوخالفة، **مقدمو خدمات الإنترنت ومسؤوليتهم الجزائية**، أطروحة الدكتوراه علوم في القانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي-تبسة-، 2016-2017.
17. حطاب كمال، **الحماية الجزائية للتجارة الإلكترونية**، أطروحة الدكتوراه، علوم تخصص: علوم قانونية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس سيدي بلعباس، 2015-2016.
18. ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة الدكتوراه علوم، تخصص: قانون العقوبات والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2015-2016.
19. رحمان يوسف، **الأدلة الكتابية ذات القوة القانونية**، أطروحة الدكتوراه، تخصص: قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد –تلمسان- الجزائر، 2017/2016.
20. روابح فريد، **الأساليب الإجرائية الخاصة للتحري والتحقيق في الجريمة المنظمة**، أطروحة الدكتوراه في القانون العام، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1 بن يوسف بن خدة، 18 فيفري 2016.
21. زروق يوسف، **حجية وسائل الإثبات الحديثة**، أطروحة الدكتوراه، تخصص: قانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد-تلمسان-، 2013/2012.
22. سليماني مصطفى، **وسائل الإثبات وحجيتها في عقود التجارة الإلكترونية في التشريع الجزائري والمقارن**، شهادة الدكتوراه، تخصص: القانون الخاص المعمق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية أدرار، 2020/2019.
23. طنجاوي مراد، **مدى حجية المحررات الإلكترونية في الإثبات المدني**، أطروحة الدكتوراه علوم، قسم: القانون الخاص، كلية الحقوق، الجزائر1، 2017/2016.
24. عميمر عبدالقادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)**، أطروحة الدكتوراه علوم في القانون العام، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1 (بن يوسف بن خدة)، 2020/2019.
25. عنتر أسماء، **إجراءات التحقيق القضائي الخاصة -دراسة مقارنة-**، أطروحة الدكتوراه، تخصص: قانون قضائي خاص، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس -مستغانم، 2020-2021.

26. لهوى رابح، **الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش**، أطروحة الدكتوراه علوم، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2020 /2021.
27. محمد صالح جاد المولى خليفة، **الدليل الرقمي وحجيته في إثبات جرائم المعلومات دراسة مقارنة**، أطروحة الدكتوراة، قسم القانون الجنائي، كلية الحقوق، جامعة طنطا، 2018.
28. ملياني عبد الوهاب، **أمن المعلومات في بيئة الأعمال الإلكترونية**، أطروحة الدكتوراه في القانون العام، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد- تلمسان-، 2016-2017.
29. مولاي ملياني دلال، **إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري**، أطروحة الدكتوراه في القانون الخاص، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد- تلمسان، 2017-2018.
30. نبيلة قيشاح، **الإجراءات المستحدثة لمكافحة الجريمة المنظمة في التشريع الجزائري**، أطروحة الدكتوراه علوم، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي –تبسة-، 2020/2019.
31. نور الهدى محمودي، **مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي -دراسة تحليلية-**، أطروحة الدكتوراه علوم، تخصص:علم الاجرام وعلم العقاب، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1-الحاج لخضر-، 2018/2017.

ب- رسائل الماجستير:

1. أحمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم04/09**، رسالة الماجستير، تخصص: قانون الجنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2012-2013.
2. بلولهي مراد، **الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة**، رسالة الماجستير، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر- باتنة، 2011/2010.
3. بن لاغة عقلية، **حجية أدلة الإثبات الجنائية الحديثة**، رسالة الماجستير، فرع: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2011-2012.
4. ركاب أمينة، **أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري**، رسالة الماجستير، تخصص: قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد-تلمسان-، 2014-2015.
5. سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة الماجستير علوم، تخصص: علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2012-2013.

6. سوماتي شريفة، **المتابعة الجزائية في جرائم الفساد في التشريع الجزائري**، رسالة ماجستير، فرع: القانون الجنائي، كلية الحقوق، جامعة الجزائر1، 2011/2010.

7. صغير يوسف، **الجريمة المرتكبة عبر الإنترنت**، رسالة الماجستير، تخصص: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013.

8. عثمان محمد الحسن حاج علي، **حجية الأدلة الرقمية في إثبات جرائم الحاسب الآلي والإنترنت**، رسالة الماجستير في الفقه المقارن، قسم الفقه المقارن، كلية الشريعة والقانون الدراسات العليا، جامعة أم درمان الإسلامية،2011.

9. علوي سالم، **أدلة الإثبات في التحقيق الجنائي**، رسالة الماجستير، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر01- بن يوسف بن خدة، 2016-2017.

11. غوالم توفيق، **السرقة المعلوماتية (دراسة تأصيلية–تحليلية- مقارنة)**، رسالة الماجستير، فرع: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2013/2012.

12. فوغالي بسمة، **إثبات العقد الإلكتروني وحجيته في ظل عالم الإنترنت**، رسالة الماجستير، تخصص: قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين-سطيف2، 2015/2014.

13. لواتي فوزي، **التحقيق في جرائم المخدرات على ضوء أساليب التحري الخاصة**، رسالة الماجستير، فرع القانون الجنائي، كلية الحقوق، جامعة الجزائر1، 2015/2014.

14. مذكور عائشة، **الحماية الجنائية للعقود الإلكترونية في التشريع الجزائري**، رسالة الماجستير، فرع قانون العقود، كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه في القانون الأساسي والعلوم السياسية، جامعة آكلي محند أولحاج البويرة، 2018.

15. معزيز أمينة، **خصوصيات إجراءات قمع الجريمة المنظمة**، رسالة الماجستير، فرع: القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2011-2012.

ثالثًا: المقالات

1. أمينة قهواجي، ليلي مطالي، **الإطار المفاهيمي والقانوني للتوقيع والتصديق الإلكترونيين في الجزائر**، كلية العلوم الإقتصادية والتجارية وعلوم التسيير، جامعة بلحاج بوشعيب عين تموشنت-الجزائر، مجلة المشكاة في الإقتصاد لتنمية والقانون، المجلد 04، العدد 08، سنة 2018، الجزائر.

2. بركات عماد الدين، **حجية التوقيع الإلكتروني في إثبات المعاملات الإلكترونية -دراسة مقارنة-**، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف مسيلة، مجلة الأستاذ الباحث للدرسات القانونية والسياسية، المجلد04، العدد02، السنة 2019، الجزائر.

3. بصائر علي محمد، مروى عبد الواحد حسن، **الدليل الإلكتروني في مجال الإثبات الجنائي**، كلية الأداب/ جامعة واسط، مجلة لارك للفلسفة واللسانيات والعلوم الإجتماعية، المجلد 09، العدد 05، 2019، العراق.
4. بلجراف سامية، **سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي**، مخبر القانون الخاص المقارن، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي-الشلف، مجلة الدراسات القانونية المقارنة، المجلد 7، العدد 01، 2021، الجزائر.
5. بلحاج محجوبة، **القواعد العامة للتوقيع والتصديق الإلكترونيين وحمايتهما جزائياً وفقاً لقانون العقوبات والقانون رقم: 15-04**، جامعة إبن خلدون تيارت، مجلة البحوث في الحقوق والعلوم السياسية، الجزائر، المجلد 06، العدد 02، 2020، الجزائر.
6. بلهادي حميد، **حجية الدليل الرقمي في الإثبات الجنائي**، كلية الحقوق والعلوم السياسية، جامعة بليدة 2 لونيسي علي، مجلة البحوث والدراسات القانونية والسياسية، المجلد التاسع، العدد الأول، 2019، الجزائر.
7. بن جديد فتحي، **مدى حجية الكتابة والتوقيع الإلكترونيين في إثبات العقد المبرم عبر الإنترنت**، معهد البحوث والدراسات العربية المنظمة العربية للتربية والثقافة والعلوم، جامعة الدول العربية، مجلة البحوث والدراسات العربية، المجلد 41، العدد 62، جوان 2015، مصر.
8. بن حميدوش نورالدين، رحموني عبد الرزاق، **مكانة الدليل الإلكتروني في الإثبات الجزائي**، جامعة محمد بوضياف مسيلة، مجلة الدراسات والبحوث القانونية، المجلد 04، العدد 02، جانفي 2020، الجزائر.
9. بن فردية محمد، **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)**، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة- بجاية، المجلة الأكاديمية للبحث القانوني، المجلد 05، العدد 01، 2014، الجزائر.
10. بن مالك أحمد، الخال إبراهيم، **دور الأدلة الرقمية في الإثبات الجنائي**، المركز الجامعي علي كافي تندوف، مجلة العلوم الإنسانية، المجلد 05، العدد 01، أفريل 2021، الجزائر.
11. بوبكر أمال، **النظام القانوني لمؤدي خدمات التصديق الإلكتروني في الجزائر**، جامعة يحيى فارس-المدية، مجلة الدراسات القانونية، المجلد 04، العدد 01، 2018، الجزائر.
12. بوخلوط الزين، **آلية المحاكمة عن بعد ومبادئ المحاكمة العادلة**، كلية الحقوق، جامعة عين تموشنت، مجلة البصائر للدراسات القانونية والإقتصادية، المجلد 01، العدد 03، ديسمبر 2021، الجزائر.
13. بوشارب هانية، بن شهرة شول، **صعوبة عملية إستخلاص الدليل الإلكتروني**، جامعة عمار ثليجي-الأغواط، مجلة الدراسات القانونية والسياسية، المجلد09، العدد01، جانفي 2023، الجزائر.

14. بوشارب هانية، بن شهرة شول، **معوقات التحقيق الجنائي في البيئة الإفتراضية**، جامعة عمار ثليجي-الأغواط، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السابع، العدد الثاني، 2023، الجزائر.
15. بوشارب هانية، مجدوب آمنة، **إلتزامات مؤدي خدمات التصديق الإلكتروني**، جامعة زيان عاشور-الجلفة، مجلة العلوم القانونية والإجتماعية، المجلد الثامن، العدد الثاني، جوان 2023، الجزائر.
16. بولمكاحل أحمد، ليطوش دليلة، **التسرب والشرعية الإجرائية**، كلية الحقوق والعلوم السياسية، جامعة باتنة1-الحاج لخضر، مجلة الباحث للدراسات الأكاديمية، المجلد07، العدد02، 2020، الجزائر.
17. حسام محمد نبيل عبد الرؤوف مرسي، **التعاون الدولي في مكافحة الجرائم المرتكبة عبر الإنترنت (الآليات- الصعوبات- الحلول)**، أكاديمية العلوم الشرطية- الشارقة، مجلة العلوم الشرطية والقانونية، المجلد الخامس، العدد الثاني، جويلية 2014، الإمارات العربية المتحدة.
18. حكيمة بوكحيل، سامية بن عديد، **الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الإتصال ودورها في تفتيش نظم المعلوماتية**، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي-الشلف، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021، الجزائر.
19. خالد ضو، **حجية الدليل الالكتروني وشروط قبوله في الإثبات الجنائي**، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو-الأغواط، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المجلد05، العدد الأول، مارس2022، الجزائر.
20. راضية مشري، **جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري**، جامعة 08 ماي 1945 قالمة، حوليات جامعة قالمة للعلوم الإجتماعية والإنسانية، المجلد11، العدد20، جوان 2017، الجزائر.
21. رامي متولي القاضي، **إجراءات التحقيق والمحاكمة عن بعد- دراسة تحليلية مقارنة**، جامعة الشارقة، مجلة جامعة الشارقة للعلوم القانونية، المجلد19، العدد 02، جوان 2022، الإمارات العربية المتحدة.
22. رامي متولي القاضي، **الدليل الجنائي الرقمي في التشريع المصري في ضوء أحكام القانون رقم: 175 لسنة 2018 ولائحته التنفيذية**، كلية القانون بالجامعة البريطانية في مصر، مجلة القانون والتكنولوجيا، المجلد الثاني، العدد الأول، أفريل 2022، مصر.
23. رضوان قرواش، **هيئات التصديق الإلكتروني في ظل القانون 15-04 المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين (المفهوم والإلتزامات)**، جامعة محمد لمين دباغين سطيف2، مجلة العلوم الإجتماعية، العدد24، جوان 2017، الجزائر.

24. رمزي بن الصديق، **تزوير المحررات الإلكترونية بين قابلية الخضوع للقواعد التقليدية وضرورة مراعاة الخصوصية**، كلية الحقوق والعلوم السياسية، جامعة تامنغست، مجلة الإجتهاد للدراسات القانونية والإقتصادية، المجلد 07، العدد02، 2018، الجزائر.
25. سالم محمد الأوجلي، **مقبولية الدليل الرقمي في المحاكم الجنائية**، كلية القانون، جامعة بنغازي، مجلة دراسات قانونية، المجلد 2016، العدد 19، جانفي 2016، ليبيا.
26. صليحة مرباح، **دور التصديق الإلكتروني في إثبات المعاملات الإلكترونية وحفظها**، مخبر القانون الخاص المقارن، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي-الشلف، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021، الجزائر.
27. طه عيساني، **التوقيع الإلكتروني كآلية لحماية المعاملات الإلكترونية**، كلية الحقوق والعلوم السياسية، جامعة حاج لخضر-باتنة، مجلة الباحث للدراسات الأكاديمية، المجلد 06، العدد 01، جانفي 2019، الجزائر.
28. عادل بوزيدة، **دور الشهادة الإلكترونية في الإثبات الجزائي على ضوء قانون الإجراءات الجزائية الجزائري**، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي-تبسة، مجلة النبراس للدراسات القانونية، المجلد الأول، العدد الأول، سبتمبر 2016، الجزائر.
29. العبيدي أسامة بن غانم، **الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية**، الحقوق والعلوم السياسية، جامعة الملك سعود، مجلة جامعة الملك سعود، المجلد 25، العدد 01، جانفي 2013، السعودية.
30. عز الدين عثماني، **إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية**، المركز الجامعي مرسلي عبدالله-تيبازة، مجلة دائرة البحوث والدراسات القانونية والسياسية، المجلد 02، العدد 04، جانفي 2018، الجزائر.
31. عزيزة لرقط، **الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري**، كلية الحقوق والعلوم السياسية، جامعة تامنغست، مجلة الإجتهاد للدراسات القانونية والإقتصادية، المجلد 06 ، العدد 01، جانفي 2017، الجزائر.
32. عيدة بلعابد، **الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية**، جامعة تامنغست، مجلة آفاق علمية، المجلد11، العدد01، 2019، الجزائر.
33. غنية باطلي، **الكتابة الإلكترونية كدليل إثبات**، جامعة باجي مختار-عنابة، مجلة التواصل، المجلد18، العدد02، 2012، الجزائر.
34. فارس خطابي، دليلة مباركي، **تزوير التوقيع الإلكتروني في بطاقات الإئتمان -دراسة على ضوء القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين-**، جامعة الحاج لخضر-باتنة1، المجلة الجزائرية للأمن الإنساني، المجلد05، العدد02، جويلية 2020، الجزائر.

35. فهد دخين العدواني، **مشروعية الدليل الإلكتروني الصادر عن التفتيش الجنائي: دراسة مقارنة**، جامعة عين الشمس، كلية التربية، مركز تطوير التعليم الجامعي، مجلة دراسات في التعليم الجامعي، المجلد 2017، العدد السادس والثلاثون، 2017، مصر.
36. لعوارم وهيبة، **نظام تسليم المجرمين دراسة تحليلية مقارنة بين المواثيق الدولية التشريع الجزائري والتشريعات المقارنة**، كلية الحقوق والعلوم السياسية، جامعة برج بوعريريج، مجلة البيبان للدراسات القانونية والسياسية، المجلد 01، العدد الأول، جوان 2016، الجزائر.
37. محمد أحمد المنشاوي، **سلطة القاضي الجنائي في تقدير الدليل الإلكتروني**، جامعة الكويت، مجلة الحقوق، المجلد 36، العدد02، جوان 2012، الكويت.
38. محمد حسن السراء، **الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية**، القيادة العامة لشرطة الشارقة مركز بحوث الشرطة، الفكر الشرطي، المجلد 21، العدد 02، 2012، الإمارات العربية المتحدة.
39. مسعود بن حميد المعمري، **الدليل الإلكتروني لإثبات الجريمة الإلكترونية**، كلية القانون الكويتية العالمية، مجلة كلية القانون الكويتية العالمية-أبحاث المؤتمر السنوي الدولي الخامس9-10 ماي 2018، الجزء الثاني، العدد 3، أكتوبر 2018، الكويت.
40. ممدوح حسن مانع العدوان، **حجية الدليل الإلكتروني في الإثبات الجزائي**، الهيئة العالمية للتسويق الإسلامي، المجلة العالمية للتسويق الإسلامي، المجلد السادس، العدد الأول، 2017، لندن- المملكة المتحدة.
41. منصور داود، **القيمة القانونية للبلوك تشين في الإثبات ودوره في نطاق التوثيق الرقمي للمعاملات الإلكترونية**، جامعة زيان عاشور-الجلفة، مجلة الحقوق والعلوم الإنسانية، المجلد14، العدد02، 2021، الجزائر.
42. نادية ضريفي، دراج عبد الوهاب، **سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي**، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف مسيلة، مجلة الأستاذ الباحث للدرسات القانونية والسياسية، المجلد04، العدد 02، 2019، الجزائر.
43. ندى حمزة صاحب، **الحجية القانونية للمستندات الإلكترونية وطرق الطعن فيها (دراسة مقارنة)**، كلية الأداب/ جامعة واسط، مجلة لارك للفلسفة واللسانيات والعلوم الإجتماعية، المجلد 08، العدد02، 2016، العراق.
44. نسيغة فيصل، عبير بعقيقي، **الإثبات في الجرائم المعلوماتية على ضوء القانون 04/09**، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر-الوادي، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 02، جوان 2018، الجزائر.
45. وداعي عز الدين، **التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن**، كلية الحقوق والعلوم السياسية، جامعة

عبدالرحمن ميرة-بجاية، المجلة الأكاديمية للبحث القانوني، مجلد16، عدد02، 2017، الجزائر.

46. يزيد بوحليط، **تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري**، جامعة باجي مختار-عنابة، التواصل في الإقتصاد والإدارة والقانون، المجلد 22، العدد04، ديسمبر2016، الجزائر.

رابعًا: الملتقيات

1. بروك إلياس، عميرات عادل، **ماهية الإثبات المدني الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية -بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
2. بن شهرة شول، بوشارب هانية، **الضوابط القانونية لقبول الإثبات بالكتابة في الشكل الإلكتروني التوقيع الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
3. بن صالح سارة، **ماهية الكتابة والتوقيع الإلكترونيين كأدلة إثبات في المواد المدنية**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
4. بن عزة محمد حمزة، **تطور تجربة القضاء الفرنسي في إستعمال تقنية المحادثة المرئية من إجراء إستثنائي إلى سياسة قضائية**، الملتقى الوطني حول إستخدام تقنية المحادثة المرئية عن بعد في القضاء الوطني والدولي بين متطلبات العصرنة ومقتضيات حماية حقوق الأشخاص، كلية الحقوق، جامعة الجزائر-1- بن يوسف بن خدة، المنعقد يوم 12 مارس 2023، الجزائر.
5. بن علي صليحة، **نطاق حجية التوقيع والتصديق الإلكترونيين**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
6. بن عيسى فتيحة، المر سهام، **التوقيع الإلكتروني ومدى حجيته في العقد التجاري الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق

والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.

7. بن مشري عبد الحليم، مقري صونيا، **دور جهات التصديق الإلكتروني في إثبات المعاملات الإلكترونية**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
8. بوشارب هانية، بن شهرة شول، **الصعوبات التي تواجهها الجهات التي تتولى التحري والتحقيق في الجرائم الإلكترونية**، ملتقى وطني حول التجارب التشريعية في مواجهة الجريمة الإلكترونية، معهد الحقوق والعلوم السياسية، المركز الجامعي نور البشير البيض، يوم 04 ديسمبر 2023، الجزائر، غير منشور.
9. الجرادات ضرغام، **أدلة الإثبات الجنائي من خلال الهواتف الذكية مفهومها وحجيتها دراسة مقارنة بين الفقه والقانون**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
10. حملاوي عبد الرحمان، **دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة محمد خيضر- بسكرة، المنعقد بتاريخ 16 و 17 نوفمبر 2015، الجزائر.
11. حميدة بن حمدين، امحمد نجيب شرافي، **الحجية القانونية للإثبات بالكتابة في الشكل الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية -بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
12. خنافيف محمد، شايبي العيد، **الآليات الفنية التي إعتمدها المشرع الجزائري في القانون 04/15 لضمان أمن التوقيع الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية -بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2022، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
13. زياني فيصل، زياني منير، **الحجية القانونية للإثبات بالكتابة في الشكل الإلكتروني**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الثاني، الطبعة 2021، كلية الحقوق والعلوم

السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.

14. سكفالي ريم، محمودي بشير، **الحجية القانونية للمحررات الإلكترونية**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
15. سكيل رقية، **الإثبات بالمحررات الرسمية الإلكترونية في المواد المدنية والتجارية في التشريع الجزائري -دراسة مقارنة-**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
16. عبد الرازق وهبه سيد أحمد محمد سيد، **حجية التوقيع الإلكتروني في الإثبات"دراسة تحليلية مقارنة"**،أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.
17. قيادة الدرك الوطني، **مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة محمد خيضر- بسكرة، المنعقد بتاريخ 16 و 17 نوفمبر 2015، الجزائر.
18. محده جلول، ورخ نور الدين، **القوة القانونية للإثبات بالتوقيع الإلكتروني في المسائل القانونية**، أعمال الملتقى الدولي السادس عشر بعنوان: الإثبات الإلكتروني في المواد المدنية والجزائية - بين الإطلاق والتقييد-، الجزء الأول، الطبعة 2021، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، المنعقد يوم 09 ديسمبر 2021 عبر تقنية التحاضر المرئي عن بعد، الجزائر.

خامسًا: المؤتمرات

1. إبراهيم الدسوقي أبو الليل، **توثيق التعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير المتضرر**، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، المنعقد في 1-3 مايو 2003، الإمارات العربية المتحدة.
2. أبو الوفا محمد، أبو الوفا إبراهيم، **المسئولية الجنائية عن الإستخدام غير المشروع لبطلقة الإئتمان**، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد

الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة ، المنعقد في 1-3 مايو 2003، الإمارات العربية المتحدة.

3. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة**، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، 12-14 نوفمبر 2008، الرياض- المملكة العربية السعودية.
4. علي محمد الحسين الموسى، **البطاقات المصرفية تعريفعها وأنواعها وطبيعتها**، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، المنعقد في 1-3 مايو 2003، الإمارات العربية المتحدة.
5. منظور أحمد حاجي الأزهري، **بطاقة السحب النقدي**، بحوث مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الأول، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، جامعة الإمارات العربية المتحدة، المنعقد في 1-3 مايو 2003، الإمارات العربية المتحدة.

سادسًا: المنشورات

1. روابح عبلة، **المفاهيم الأساسية للذكاء الإصطناعي وتطبيقاته المختلفة**، كتاب جماعي دولي بعنوان: **الجوانب القانونية للتكنولوجيا الحديثة والذكاء الإصطناعي**، الطبعة الأولى، أوت 2023، المركز المغاربي-شرق أدنى للدراسات الإستراتيجية، المملكة المتحدة- بريطانيا.
2. سامية غراب، ماجدة شهيناز بودوح، **متطلبات تجسيد المحاكم الإلكترونية في ظل البيئة الرقمية على ضوء التشريع الجزائري**، كتاب جماعي دولي بعنوان: **المحكمة الإلكترونية كوسيلة لتقريب مرفق القضاء من المواطن**، الطبعة الأولى، سبتمبر 2022، المركز المغاربي- شرق أدنى للدراسات الإستراتيجية، المملكة المتحدة - بريطانيا-.
3. عميروش هنية، داعي عز الدين، **دور تكنولوجيا الإعلام والإتصال في الإثبات الجنائي**، كتاب جماعي محكم بعنوان: **أثر تكنولوجيا الإعلام والإتصال على القانون الجنائي**، د.ر.ط، جوان 2021، مخبر البحث حول فعالية القاعدة القانونية، كلية الحقوق والعلوم السياسية، جامعة عبدالرحمان ميرة- بجاية، الجزائر.
4. محمد سحنوني، رياض بن غبريد، **الذكاء الإصطناعي والتطورات المستقبلية**، كتاب جماعي دولي بعنوان: **الجوانب القانونية للتكنولوجيا الحديثة والذكاء الإصطناعي**، الطبعة الأولى، أوت 2023، المركز المغاربي-شرق أدنى للدراسات الإستراتيجية، المملكة المتحدة- بريطانيا.

سابعًا: المجلات

1. **الجزائر في المنظمة الدولية للشرطة الجنائية –انتربول منذ 1963**، الشرطة المديرية العامة للأمن الوطني، مجلة الشرطة المديرية العامة للأمن الوطني، العدد 119، جويلية/أوت 2013، الجزائر.
2. حسين جيجة، سحواد نسيمة، **جهود إستباقية للأمن الوطني لتحقيق الأمن المعلوماتي والإمتياز في الأداء**، الشرطة المديرية العامة للأمن الوطني، روبورتاج منشور في مجلة الشرطة المديرية العامة للأمن الوطني، العدد 129، ديسمبر 2015، الجزائر.
3. **دائرة الأدلة الرقمية للأمن الوطني**، الشرطة المديرية العامة للأمن الوطني، روبورتاج منشور في مجلة الشرطة المديرية العامة للأمن الوطني، العدد 149، جويلية 2021، الجزائر.
4. غنية حساني، **العصب الرقمي لصد الجرائم المعلوماتية**، الشرطة المديرية العامة للأمن الوطني، مجلة الشرطة المديرية العامة للأمن الوطني، العدد 158، ماي 2024، الجزائر.

ثامنًا: المواقع الإلكترونية

1. قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996 مع المادة 5 مكررا الإضافية بصيغتها المعتمدة في عام 1998، الصادر عن هيئة الأمم المتحدة في جلستها 605 المنعقدة في 1996/12/16، الموجود على الرابط التالي:
   https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-ecomm-a_ebook.pdf
2. لائحة الإتحاد الأوروبي رقم: 910-2014 المؤرخة في 23 جويلية 2014 الصادرة عن البرلمان الأوروبي والمجلس الأوروبي المتعلقة بتحديد التعريف الإلكتروني وخدمات الثقة في المعاملات الإلكترونية داخل السوق الأوروبية الموحدة وإلغاء التوجيه EC/93/1999، الموجود على الرابط التالي:
   https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910
3. الموقع الرسمي المنظمة الدولية للشرطة الجنائية الأنتربول، الموجود على الرابط التالي:
https://www.interpol.int/ar/3/12/3
4. القانون الأساسي للمنظمة الدولية للشرطة الجنائية الانتربول المعتمد أثناء الدورة 25 للجمعية العامة للأمم المتحدة بفيينا سنة 1956، الموجود على الرابط التالي:
file:///C:/Users/SAM/Downloads/01%20A%20Constitution_2023.pdf
5. الموقع الرسمي المنظمة الإفريقية للشرطة الجنائية الأفريبول، الموجود على الرابط التالي:
   https://afripol.africa-union.org/ar /

6. الموقع الرسمي للدرك الوطني، الموجود على الرابط التالي:

https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php

7. الموقع الرسمي الإذاعة الجزائرية، الموجود على الرابط التالي:

https://news.radioalgerie.dz/ar/node/34199

تاسعًا: النصوص التشريعية الأجنبية

أ- النصوص القانونية في التشريع المصري:

1. قانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004، المتضمن التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المؤرخ بتاريخ 21 أفريل 2004، ج.ر.ج.م.ع العدد 17 تابع (د)، الصادر بتاريخ 22 أفريل 2004.
2. القانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج)، الصادرة في 14 أوت سنة 2018.
3. اللائحة التنفيذية للقانون التوقيع الإلكتروني المصري رقم: 15 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، الصادرة عن وزارة الإتصالات وتكنولوجيا المعلومات بموجب القرار رقم: 109 لسنة 2005 المؤرخ في 15 ماي 2005، جريدة الوقائع المصرية العدد 115 (تابع)، الصادر بتاريخ 25 ماي 2005، المعدلة بموجب القرار رقم: 361 لسنة 2020 المؤرخ في 19 أفريل 2020، جريدة الوقائع المصرية العدد 95 (تابع)، الصادر بتاريخ 23 أفريل 2020.
4. اللائحة التنفيذية للقانون رقم: 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، الصادرة عن رئيس مجلس الوزراء بموجب القرار رقم: 1699 لسنة 2020، الجريدة الرسمية العدد 35 تابع (ج)، الصادر بتاريخ 27 أوت 2020.

B- Les textes juridiques internationaux en français:

1. Loi Type de la commission des Nations Unies pour le droit commercial international sur le commerce électronique 1996.
2. Loi Type de la Commission des Nations Unies pour le droit commercial international sur les signatures électroniques 2001.
3. Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, j.o n° l013 du 19-01-2000, Abrogé.
4. - Directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché

intérieur directive sur le commerce électronique, J.O.C.E , L.178 du 17/07/2000.

5. RÈGLEMENT UE N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, et abrogeant la directive 1999/93/CE.
6. La convention sur la Cybercriminalité et son Rapport explicatif ont été adopté par le Comité des Ministres du conseil de l'Europe à l'occasion de sa 109e session, le 8 novembre 2001. La Convention a été ouvert à la signature à Budapest, le 23 novembre 2001, à l'occasion de la Conférence Internationale sur la Cybercriminalité, et elle est entrée en vigueur le 1er juillet 2004.

A- Les textes juridiques dans la législation française:

1. Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique.
2. Loi n° 92-685 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les biens.
3. Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur.
4. Loi n°2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J.O.R.F numéro 62, 14 mars 2000, Abrogé.
5. Loi n° 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes.
6. Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure en France, modifiée par loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
7. Loi n°2004-204 du 9 mars 2004 - art. 54 JORF 10 mars 2004 en vigueur le 31 décembre 2005 portant adaptation de la justice aux évolutions de la criminalité.
8. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

9. Loi n°2009-526 du 12 mai 2009 - art. 124 de simplification et de clarification du droit et d'allègement des procédures.

10. Loi n° 2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale.

11. Loi n°2013-1168 du 18 décembre 2013 - art. 25 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

12. Code de Pénale Modifié par LOI n°2014-790 du 10 juillet 2014 visant à lutter contre la concurrence sociale déloyale.

13. Loi n°2015-912 du 24 juillet 2015 relative au renseignement.

14. Loi n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne.

15. Loi n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur.

16. Loi n°2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic.

17. Ordonnance n° 58-1296 du 23 décembre 1958 modifiant et complétant le Code de procédure pénale.

18. Ordonnance n°2000-916 du 19 septembre 2000 portant adaptation de la valeur en euros de certains montants exprimés en francs dans les textes législatifs.

19. Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n° 0035 du 11 février 2016.

B- Les textes réglementaires:

1. Décret n°2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, J.O. numéro 77 ,31 mars 2001, Modifié par Décret n°2016-1278 du 29 septembre 2016 - art. 1 V , Abrogé par Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique - art. 2 V.
2. Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique.

الفهرس

مقدمة ---------- 7

الباب الأول: ----------

الأحكام الموضوعية للجرائم الماسة بالمستند الإلكتروني وقواعد الإثبات الخاصة بها ----------14

الفصل الأول: ----------16

مدى إقتناع القاضي الجزائي بالدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الإلكتروني ----------16

المبحث الأول: خصوصية الدليل الإلكتروني المستخلص من الجرائم الماسة بالمستند الإلكتروني ----------18
المطلب الأول: مفهوم الدليل الإلكتروني في عملية الإثبات ----------18
الفرع الأول: تعريف الدليل الإلكتروني----------18
الفرع الثاني: خصائص الدليل الإلكتروني ----------22
الفرع الثالث: تقسيمات الدليل الإلكتروني ----------29
المطلب الثاني: الدليل الإلكتروني المستمد من الجرائم الماسة بالمستند الإلكتروني---------34
الفرع الأول: مفهوم المستند الإلكتروني ----------35
الفرع الثاني: عناصر المستند الإلكتروني----------42
الفرع الثالث: الشروط اللازمة للإعتداد بالمستند الإلكتروني كوسيلة الإثبات----------79
المبحث الثاني: سلطة القاضي الجزائي في قبول و تقدير المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني ----------95
المطلب الأول: سلطة القاضي الجزائي في قبول المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني----------95
الفرع الأول: حرية القاضي الجزائي في الإقتناع بالمخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني----------96
الفرع الثاني: القيود الواردة على حرية القاضي الجزائي في قبول المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني ----------98
المطلب الثاني: سلطة القاضي الجزائي في تقدير المخرجات الإلكترونية بإعتبارها دليلًا مستمدًا من الجرائم الماسة بالمستند الالكتروني---------- 114
الفرع الأول: حجية المستند الإلكتروني في الإثبات الجنائي في النظام الإثبات الحر ------ 114
الفرع الثاني: حجية المستند الإلكتروني في الإثبات الجزائي في نظام الإثبات المقيد ------ 121

الفرع الثالث: حجية المستند الإلكتروني في الإثبات الجنائي في النظام المختلط---------- 134
خلاصة: ---------- 137
الفصل الثاني: ---------- 138
الجرائم الماسة بالمستند الإلكتروني ---------- 138
المبحث الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني ---------- 140
المطلب الأول: صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني---------- 140
الفرع الأول: جريمتي الدخول والبقاء غير المصرح بهما داخل نظام المعالجة الآلية للمعطيات الذي يحتوي على مستندات إلكترونية---------- 140
الفرع الثاني: جريمة المساس بسلامة معطيات المستند الإلكتروني ---------- 152
الفرع الثالث: جريمة إتلاف المستند الإلكتروني ---------- 156
الفرع الرابع: جريمة إستخدام المعطيات كوسيلة للإعتداء على المستند الإلكتروني ------- 164
الفرع الخامس: جريمة التعامل بالمعطيات الواردة في المستند الإلكتروني ---------- 169
المطلب الثاني: العقوبات المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني---------- 171
الفرع الأول: العقوبات الأصلية والتكميلية المقررة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني---------- 172
الفرع الثاني: أحكام العقاب على الإتفاق الجنائي والشروع في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالمستند الإلكتروني ---------- 191
المبحث الثاني: الجرائم الماسة بمحتوى المستند الإلكتروني ---------- 193
المطلب الأول: جريمة تزوير المستند الإلكتروني و جريمة إستعمال المستند الإلكتروني المزور ---------- 194
الفرع الأول: جريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور ---------- 196
الفرع الثاني: العقوبات المقررة لجريمة تزوير المستند الإلكتروني وجريمة إستعمال المستند الإلكتروني المزور ---------- 205
المطلب الثاني: جريمة سرقة بيانات المستند الإلكتروني---------- 216
الفرع الأول: أركان جريمة سرقة معطيات المستند الإلكتروني ---------- 217
الفرع الثاني: العقوبة المقررة لجريمة سرقة معطيات المستند الإلكتروني---------- 225
المبحث الثالث: الجرائم الماسة بالتوقيع والتصديق الإلكترونيين---------- 226
المطلب الأول: الجرائم المرتكبة من طرف مؤدي خدمات التصديق الإلكتروني---------- 226

الفرع الأول: جريمة الإخلال بالإلتزام إعلام السلطة الإقتصادية عن التوقف عن ممارسة النشاط---------- 227
الفرع الثاني: جريمة جمع البيانات الشخصية للمعني دون موافقته الصريحة وإستعمالها إستعمالًا غير مشروع---------- 231
الفرع الثالث: جريمة إفشاء البيانات الشخصية لشهادة التصديق الإلكتروني ---------- 235
الفرع الرابع: جريمة إصدار شهادة التصديق الإلكتروني دون ترخيص أو مزاولة النشاط رغم سحب الترخيص منه---------- 240
الفرع الخامس: جريمة الإخلال بإلتزام تحديد هوية طالب شهادة التصديق الإلكتروني ---- 244
المطلب الثاني: جرائم طالبي خدمات التصديق الإلكتروني ---------- 246
الفرع الأول: جريمة الإدلاء بتصاريح وإقرارات كاذبة ---------- 246
الفرع الثاني: جريمة إستعمال شهادة التصديق الإلكتروني الموصوفة لغير الغرض الذي منحت من أجله ---------- 248
المطلب الثالث: الجريمة المرتكبة من قبل الغير ---------- 250
الفرع الأول: أركان جريمة حيازة أو إفشاء أو إستعمال بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير---------- 250
الفرع الثاني: العقوبة المقررة لجريمة حيازة أو إفشاء أو إستعمال بيانات إنشاء التوقيع الإلكتروني الموصوف الخاصة بالغير---------- 252
خلاصة:---------- 253

خلاصة : ---------- 254

الباب الثاني: ---------- 255

الأحكام الإجرائية لمكافحة الجرائم الماسة بالمستند الإلكتروني ---------- 255

الفصل الأول: ---------- 257
آليات مكافحة الجرائم الماسة بالمستند الالكتروني ---------- 257
المبحث الأول: الآليات الوطنية لمكافحة الجرائم الماسة بالمستند الإلكتروني ---------- 259
المطلب الأول: الشهادة الإلكترونية والخبرة التقنية ودورهما في إثبات الجرائم الماسة بالمستند الإلكتروني---------- 259
الفرع الأول: الشهادة الإلكترونية وعلاقتها بالجرائم الماسة بالمستند الإلكتروني---------- 259
الفرع الثاني: الخبرة التقنية في الجرائم الماسة بالمستند الإلكتروني ---------- 283
المطلب الثاني: الأجهزة المختصة وطنيًا في التحقيق الجنائي في جرائم المستند الإلكتروني309
الفرع الأول: الوحدات التابعة للأمن الوطني ---------- 310

الفرع الثاني: الوحدات التابعة للدرك الوطني---------- 316
الفرع الثالث: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته ---------- 321
الفرع الرابع: الإستعانة بمقدمي الخدمات وتسخيرهم---------- 326
المبحث الثاني: آليات التعاون الدولي لمكافحة الجرائم الماسة بالمستند الإلكتروني --------- 331
المطلب الأول: آليات التعاون القضائي لمكافحة جرائم المستند الإلكتروني---------- 331
الفرع الأول: التعاون والمساعدة القضائية الدولية---------- 331
الفرع الثاني: آلية تسليم المجرمين في مكافحة الجرائم الماسة بالمستند الالكتروني-------- 346
المطلب الثاني: آليات التعاون الأمني في مجال الجرائم الماسة بالمستند الإلكتروني------- 348
الفرع الأول: المنظمة الدولية للشرطة الجنائية (الأنتربول)---------- 349
الفرع الثاني: على المستوى الإقليمي ---------- 350
خلاصة: ---------- 354
الفصل الثاني: ---------- 355
إجراءات إستخلاص الدليل الإلكتروني في الجرائم الماسة بالمستند الإلكتروني---------- 355
المبحث الأول: الإجراءات التقليدية والتقنية لإستخلاص الدليل الإلكتروني---------- 357
المطلب الأول: معاينة مسرح الجريمة الماسة بالمستند الإلكتروني ---------- 357
الفرع الأول: تعريف إجراء المعاينة---------- 357
الفرع الثاني: مدى صلاحية معاينة مسرح الجريمة الماسة بالمستند الإلكتروني ---------- 360
الفرع الثالث: ضوابط إجراء معاينة مسرح الجريمة الماسة بالمستند الإلكتروني --------- 363
المطلب الثاني: التفتيش في الجرائم الماسة بالمستند الإلكتروني---------- 368
الفرع الأول: مدى قابلية تفتيش مكونات الأجهزة الإلكترونية ---------- 369
الفرع الثاني: تفتيش المنظومة المعلوماتية عن بعد---------- 377
الفرع الثالث: شروط التفتيش الإلكتروني ---------- 385
الفرع الأول: مدى صلاحية ضبط مكونات الأجهزة الإلكترونية كدليل في الجرائم الماسة بالمستند الإلكتروني---------- 397
الفرع الثاني: إجراءات ضبط الدليل الإلكتروني ---------- 404
الفرع الثالث: قواعد تحريز المضبوطات المعلوماتية وتأمينها ---------- 407
الفرع الرابع: الصعوبات التي تعترض إجراءات ضبط الدليل الإلكتروني ---------- 410
المبحث الثاني: الإجراءات المستحدثة لإستخلاص الدليل الإلكتروني---------- 412
المطلب الأول: التسرب الإلكتروني ---------- 413
الفرع الأول: تعريف التسرب الإلكتروني وصوره ---------- 413
الفرع الثاني: شروط صحة التسرب الإلكتروني ---------- 418
الفرع الثالث: الحماية القانونية المقررة للمتسرب ---------- 426

المطلب الثاني: الإجراءات ذات الطابع الشخصي في مواجهة الجرائم الماسة بالمستند الإلكتروني---------- 434
الفرع الأول: الإجراءات المتعلقة بالمعطيات المتحركة---------- 434
الفرع الثاني: الإجراءات المتعلقة بالمعطيات الساكنة ---------- 445
خلاصة: ---------- 457

الخاتمة ---------- 459

قائمة المصادر والمراجع---------- 471

الفهرس---------- 496

ملخص:

أدى التزايد الملحوظ في إبرام المعاملات الإلكترونية إلى جانب الإستخدام الواسع لشبكة الإنترنت، إلى تطور ملحوظ في أساليب وطرق إرتكاب الجريمة، وهو ما أسهم في تفشي الجرائم الواقعة على المستند الإلكتروني، ونظرًا للطابع الخاص الذي تتميز به هذه الجرائم فقد أحيطت عملية إثباتها بجملة من الصعوبات أثرت بشكل مباشر على فعالية الإثبات الجنائي، وترتبط هذه الصعوبات أولًا بطبيعة الدليل الإلكتروني الناشئ عنها، والذي يعتبر إحدى الآثار المهمة في الربط بين الجريمة ومرتكبها، كما تعود أيضًا إلى التحديات التي تواجه السلطات المكلفة بالتحري والتحقيق، وقد إستوجب هذا الوضع ضرورة تطوير الجانب التشريعي العقابي لمواجهة هذه الإنتهاكات، بما يواكب التطورالسريع الذي تعرفه الظاهرة الإجرامية، والسعي إلى إيجاد آليات جزائية مستحدثة تساير المستجدات التقنية والفنية والتكنولوجية، لاسيما مع بروز نوع جديد من التحديات أمام هذه السلطات في التصدي لهذا النوع من الجرائم وإستخلاص الدليل الإلكتروني منها.

الكلمات المفتاحية: الدليل الإلكتروني، حجية المستند الإلكتروني، شهادة التصديق الإلكتروني، مراقبة الإتصالات الإلكترونية، التفتيش الإلكتروني، جريمة تزوير المستند الإلكتروني، الجرائم الماسة بالمعالجة الآلية للمعطيات.

The Abstract :

The significant increase in electronic transactions, along with the widespread use of the Internet, has led to a noticeable evolution in the methods and techniques used to commit crimes, which has contributed to the spread of offenses targeting electronic documents. Due to the particular nature of these crimes, the process of proving them has been surrounded by a number of difficulties that have directly affected the effectiveness of criminal evidence. these difficulties stem primarily from the inherent nature of the electronic evidence, resulting from such crimes, which is considered one of the key elements in establishing a link between the offense and its perpetrator. They also arise from the practical challenges faced by the authorities responsible for investigation and inquiry. This situation has necessitated the development of the punitive legislative framework to address such violations, in a manner that keeps pace with the rapid evolution of criminal phenomena and the need to establish innovative criminal mechanisms that are aligned with technological and scientiic advancements particularly in light of the emergence of new challenges facing these authorities in combating this category of crimes and in extracting relevant electronic evidence.

Keywords: Electronic Evidence, Authentic Electronic Signature, Electronic certification certificate, Interception of Electronic communications, Electronic Search, The Crime of Forgery of an Electronic Document, Crimes Affecting Automated Data Processing.