



جامعة غرداية
كلية الحقوق والعلوم السياسية
قسم الحقوق



الموضوع

حماية الأشخاص من الإنتحال الرقمي

Digital identity fraud

مذكرة تخرج لنيل شهادة الماستر في الحقوق

تخصص قانون جنائي وعلوم جنائية

تحت إشراف الأستاذ الدكتور:

كيحول بوزيد

إعداد:

غريقة محمد الأمين

برقال محمد آدم

الاسم واللقب	الجامعة	الصفة
د. تشعبت محمد	جامعة غرداية	رئيسا
أ.د. كيحول بوزيد	جامعة غرداية	مشرفا
د. ماشوش مراد	جامعة غرداية	ممتحنا

السنة الجامعية: 2026/2025

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، وبتوفيقه تكتمل المساعي، نحمده سبحانه وتعالى على ما أنعم به علينا من توفيق لإتمام هذا العمل.

نتقدم بجزيل الشكر وعظيم الامتنان إلى كل من أسهم في إنجاز هذه المذكرة، وكان له أثر في مسيرتنا العلمية.

وفي مقدمة هؤلاء، نتوجه بخالص الشكر والتقدير إلى الأستاذ المشرف **كيحول بوزيد**، الذي تكرم بالإشراف على هذه المذكرة، وأفاض علينا من علمه وخبرته، وأحاط هذا العمل بمتابعة دقيقة وتوجيهات سديدة وملاحظات علمية قيمة، كان لها بالغ الأثر في إنجازها وإخراجها بالصورة المرجوة، فله منا كل التقدير والاحترام، ونسأل الله أن يجزيه خير الجزاء، وأن يبارك في علمه وعمله.

كما نتقدم بخالص الشكر والتقدير إلى السادة أعضاء لجنة المناقشة، على تفضلهم بقبول مناقشة هذه المذكرة، وعلى ما سيبدونه من ملاحظات علمية بناءة واقتراحات قيمة من شأنها أن تثري هذا العمل وتزيده جودة.

ولا يفوتنا أن نعبر عن بالغ امتناننا لجميع أساتذتنا الأفاضل الذين رافقونا طوال مسيرتنا الجامعية، وبذلوا جهودًا كبيرة في تعليمنا وتوجيهنا، وكان لهم الفضل بعد الله في تكويننا العلمي والمعرفي.

كما نتوجه بالشكر إلى كل من قدم لنا يد العون، أو أسدى لنا نصيحة، أو كان سببًا في تذليل الصعوبات التي واجهتنا خلال إعداد هذه المذكرة، سائلين الله تعالى أن يجزي الجميع خير الجزاء، وأن يوفقهم لما فيه الخير والسداد.

الاهداء

"الْحَمْدُ لِلَّهِ الَّذِي هَدَانَا لِهَذَا وَمَا كُنَّا لِنَهْتَدِيَ لَوْلَا أَنَّ هَدَانَا اللَّهُ"

الحمد لله العليّ القدير، الذي منحني القوة والبصيرة، وأعانتني بفضلِهِ وكرمه على إتمام هذا المشوار العلمي؛ فله الحمد أولاً وآخراً، وله الشكرُ ظاهراً وباطناً على نعمه التي لا تُعد ولا تُحصى، والصلاة والسلام على خير الأنام، وعلى آله وصحبه الكرام. إلى منبع العطاء وأولى الأوطان.. والديّ الكريمين:

إلى أبي العزيز:

يا من شقيتَ لأرتاح، وصبرتَ لأصل، وبذلتَ عرق الجبين لثُبتد لي طريق العلم والمعرفة. إليك يا رمز الصمود، أقدم ثمرة جهدي اعترافاً بجميلك الذي طوّق عنتي، وتضحياتك التي لا تغنيها الكلمات حقها. أدامك الله لي سنداً وتاجاً أخيراً، ورزقك الصحة والعافية وجزاك عني خير ما يجزي والداً عن ولده.

إلى أمي الغالية:

يا نبع الحنان الذي لا ينضب، ويا من كان دعاؤك في جوف الليل رفيقي وسرّ توفيقِي. إليك يا جنة الدنيا، أهدي هذا النجاح؛ فما هو إلا غرس يديك وطهر دعواتك التي كانت تفتح لي مغاليق الأبواب. حفظك الله لي، وأطال في عمرك في طاعته، وجعل الفردوس الأعلى مستقراً لك.

إلى ريحانة قلبي.. أختي "نور الهدى":

إليك يا من بوجودك تشرق الأنوار في دارنا، أهدي نجاحي لقلبك الطاهر وبراءتك التي كانت لي دافعاً وسكينة. إلى إخوتي جميعاً:

سندي وعزوتي ورفاق الدرب، شكراً لوقوفكم بجانبني ومشاركتي لحظات الجِد والتعب، أتم ذخيري التي أعتر بها. شكر خاص للأستاذ المشرف:

أتقدم بأسمى عبارات التقدير والامتنان إلى أستاذي الفاضل د. كبحول بوزيد، الذي تفضل بالإشراف على هذا البحث، فكان لنصائحهِ السديدة وتوجيهاته القيمة الأثر البالغ في إتمام هذا العمل، فجزاه الله عني خير الجزاء ونفع به وبعلمه. إلى كل من أعانتني:

أتوجه بالشكر لكل من مدّ لي يد العون بكلمة تشجيع، وإلى كافة أساتذة الكلية الذين نهلنا من علمهم طيلة سنوات الدراسة. جزى الله الجميع عني خير الجزاء، وجعل هذا العمل نافعاً ومباركاً

محمد الأمين

الاهداء

بسم الله الرحمن الرحيم

وَقُلْ رَبِّ ارْحَمْهُمَا كَمَا رَبَّيْنِي صَغِيرًا.

الحمد لله الذي بنعمته تتم الصالحات، والذي وهبنا القوة والعزيمة لإتمام هذا العمل المتواضع.

إلى من كانت ولا تزال نبع الحنان وسرّ قوتي في كل حين... إلى من سهرت الليالي من أجلي وتحملت المشاق بصبر لا يوصف... إلى التي زرعت في قلبي الأمل، وعلمتني أن النجاح لا يأتي إلا بالصبر والاجتهاد... إلى من كان دعاؤها لي طريقاً للنور، ورضاها عني أعظم غاية أرجوها...

إلى أمي الغالية، أهديك ثمرة حمدي وتعبي، أهديك هذا العمل المتواضع عرفاناً بما قدمته لي من حب وتضحية لا تُقدّر بثمن، فأنتِ النور الذي أضاء دربي، وأنتِ السند الذي لم ولن يميل، أسأل الله أن يحفظك ويطيل في عمرك، وأن يجعلني دائماً سبباً في سعادتك ورضاك.

وإلى من كانت رفيقة دربي وسندي في لحظات ضعفي.. إلى من شاركني أفراحي وأحزاني وكانت دوماً بقربي تشجعني وتدعمني إلى أختي العزيزة، أهديك هذا العمل، شاكراً لك وقوفك إلى جانبي، وكلماتك التي كانت دائماً تمنحني القوة للاستمرار. أسأل الله أن يديم محبتنا، وأن يحقق لك كل ما تتمنين.

كما لا أنسى أن أتوجه بالشكر والعرفان لكل من ساهم في دعمي ولو بكلمة طيبة أو دعاء صادق.

إلى الأستاذ المشرف الدكتور كيحول بوزيد

بكل عبارات التقدير والامتنان، نتوجه إليكم بخالص الشكر على ما أوليتموه من عناية علمية رصينة، وتوجيهات منهجية سديدة، ومتابعة دقيقة كان لها الأثر الحاسم في إتمام هذا العمل على الوجه المرجو، فلکم منا فائق الاحترام وعظيم الامتنان.

كما يسعدنا أن نتقدم بجزيل الشكر وعميق العرفان إلى كافة الأساتذة الافاضل الذين رافقونا طيلة خمس سنوات من مسارنا الجامعي، والذين لم يدخروا جهداً في سبيل تأطيرنا وتكويننا، فكانوا منارات علم وبراس هداية، أسهموا في صقل معارفنا وبلوغ هذه المرحلة

محمد آدم

قائمة المختصرات:

ص: صفحة

ج ر: جريدة رسمية

مقدمة

يشهد عصرنا الحالي تطورا تكنولوجيا متسارعا أفرز بيئة رقمية واسعة أصبحت جزءا لا يتجزأ من حياة الأفراد والمجتمعات، حيث أضحت المعاملات الإلكترونية ووسائل التواصل الحديثة من أبرز مظاهر هذا التحول الرقمي، غير أن هذا التطور رغم ما يحمله من مزايا قد أفرز في المقابل تحديات قانونية وأمنية معقدة لعل من أبرزها ظاهرة الانتحال الرقمي التي تمس بهوية الأفراد وخصوصيتهم وسمعتهم مما يجعل مسألة حماية الأشخاص في الفضاء الرقمي من القضايا الملحة التي تفرض نفسها بقوة في ظل المجتمع المعلوماتي.

ويعد الانتحال الرقمي من أخطر الجرائم المستحدثة كونه يقوم على استغلال بيانات الغير وانتحال صفاتهم أو شخصياتهم عبر الوسائط الإلكترونية بهدف تحقيق أغراض غير مشروعة سواء كانت مادية أو معنوية الأمر الذي يؤدي إلى إلحاق أضرار جسيمة بالضحايا تمس شرفهم واعتبارهم وحقوقهم الشخصية، وفي هذا السياق أصبحت الحماية القانونية للأشخاص من هذه الظاهرة ضرورة حتمية تفرضها متطلبات الأمن الرقمي وضمان الاستقرار الاجتماعي.

وتتجلى حماية الأشخاص من الانتحال الرقمي في مجموعة من الآليات المتكاملة التي تجمع بين التدابير الوقائية والعلاجية سواء على المستوى القانوني أو التقني أو التوعوي، حيث يسعى المشرع إلى سن قواعد قانونية تجرم هذا الفعل وتحدد العقوبات المناسبة له، إلى جانب وضع آليات لتعويض الضحايا وجبر الضرر اللاحق بهم فضلا عن اعتماد وسائل تقنية حديثة لحماية الهوية الرقمية وتأمين المعطيات الشخصية من الاختراق أو الاستغلال غير المشروع، وفي الجزائر أولى المشرع أهمية بالغة لموضوع حماية الأشخاص في البيئة الرقمية من خلال إدراج نصوص قانونية

ضمن التشريعات المختلفة لاسيما في قانون العقوبات وقانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي تهدف إلى تجريم أفعال الانتحال الرقمي وتوفير الحماية اللازمة للأفراد بما يواكب التطورات التكنولوجية المتسارعة ويعزز الثقة في المعاملات الإلكترونية.

أهمية الدراسة:

تكمن أهمية دراستنا لموضوع انتحال الهوية الرقمية في كونه يعالج إشكالية معاصرة تمس فئة واسعة من المجتمع خاصة في ظل الانتشار الكبير لاستخدام الإنترنت ووسائل التواصل الاجتماعي، كما تبرز أهميته في إبراز مدى فعالية التشريعات القائمة في مواجهة هذه الظاهرة، والكشف عن النقائص التي قد تعتريها، واقتراح الحلول الكفيلة بتعزيز الحماية القانونية والتقنية للأفراد.

أهداف الدراسة:

تهدف دراستنا لهذا الموضوع إلى تقديم دراسة شاملة لمختلف الآليات المعتمدة في حماية الأشخاص من الانتحال الرقمي، من خلال تحليل الإطار القانوني المنظم لهذه الجريمة، وبيان صورها وآثارها، إضافة إلى دراسة الوسائل الوقائية والتقنية المعتمدة للحد منها، وتقييم مدى نجاعتها في تحقيق الحماية المطلوبة، مع تقديم جملة من التوصيات التي من شأنها تطوير المنظومة القانونية وتعزيز الأمن الرقمي، وكذا الإفادة بقدر المستطاع بالموضوع محاولين بذلك إجلاء الغموض والفهم الخاطئ لهذا النوع من الانتحال.

أسباب اختيار الموضوع:

تتعدد الأسباب التي دفعتنا إلى اختيار هذا الموضوع والمتمثلة في الأسباب الذاتية والموضوعية، فمن الناحية الذاتية يرجع ذلك إلى الاهتمام الشخصي المتزايد بقضايا الأمن الرقمي وحماية الحقوق الفردية في البيئة الإلكترونية، والرغبة في فهم الأبعاد القانونية لهذه الظاهرة المستحدثة، أما من الناحية الموضوعية فتتمثل في الانتشار الواسع لجرائم الانتحال الرقمي وما تخلفه من آثار سلبية على الأفراد والمجتمع، الحاجة إلى تقييم فعالية النصوص القانونية الحالية ومدى قدرتها على مواكبة التطورات التكنولوجية، وبالإضافة إلى إثراء الدراسات السابقة حول الموضوع، وباختصار فإن اختيارنا لموضوع حماية الأشخاص من ظاهرة الانتحال الرقمي يعتمد على مزيج من الأسباب الذاتية والموضوعية، حيث يجمع بين الاهتمام الشخصي والمعرفة الأكاديمية.

منهج الدراسة:

وللإجابة عن هذه الإشكالية المطروحة اعتمدنا على المنهج الوصفي من خلال عرض مفهوم الانتحال الرقمي وبيان صورته وأسبابه وآثاره، مع توضيح الإطار المفاهيمي للموضوع، كما اعتمدنا على المنهج التحليلي من خلال تحليل النصوص القانونية المنظمة للانتحال الرقمي، وبيان مدى كفايتها في مواجهة هذه الظاهرة، مع تفسير الأحكام القانونية واستخلاص ما تثيره من إشكالات قانونية وعملية، كما اعتمدنا على المنهج المقارن من خلال إجراء مقارنة بين أحكام التشريع الجزائري وبعض التشريعات المقارنة فيما يتعلق بتنظيم الانتحال الرقمي وتجريمه، وذلك للوقوف على

أوجه التشابه والاختلاف، والاستفادة من التجارب القانونية المقارنة في تقييم المنظومة القانونية الجزائرية واقتراح ما من شأنه تعزيز فعاليتها.

الإشكالية:

يعد الانتحال الرقمي من أشكال الاعتداء على حقوق الملكية الفكرية هو ما جعله يثير العديد من الإشكالات القانونية والأخلاقية في البيئة الرقمية، خاصة مع سهولة الوصول للمعلومات وانتشار أدوات النسخ واللصق، وتجدر الإشارة إلى أن المشرع الجزائري لم يتقن أو لم يتطرق لهذه الظاهرة بصفة خاصة في مجمل النصوص القانونية التي أقرها وإنما تطرق لها كجزء من الجرائم الالكترونية الخاصة بالمعطيات، وانطلاقا مما سبق يمكننا طرح الإشكالية الرئيسية على النحو التالي فيما يتمثل الانتحال الرقمي؟

الدراسات السابقة:

1. دراسة خضرة شنبر، الموسومة بالآليات القانونية لمكافحة الجريمة الالكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه في كلية الحقوق، جامعة أحمد دراية أدرار، 2021/2020، والتي تحدثت عن المضامين الفكرية للجريمة الالكترونية والمجرم الالكتروني كفصل تمهيدي، ثم تطرقت للآليات الإجرائية لمكافحة الجريمة الالكترونية في الباب الأول، والآليات المؤسسية لمكافحة الجريمة الالكترونية في الباب الثاني.

2. دراسة دلال مولاي ملياني الموسومة بإشكالية الاثبات في جرائم الانترنت في التشريع الجزائري، أطروحة دكتوراه في قانون خاص بكلية الحقوق والعلوم

السياسية، جامعة أبو بكر بلقايد تلمسان، 2018/2017، والتي تطرقت لذاتية جرائم الانترنت في التشريع الجزائري في الباب الأول، ثم تطرقت لإجراءات الإثبات الجنائي في جرائم الانترنت في التشريع الجزائري في الباب الثاني.

3. دراسة أمينة ركاب الموسومة بأساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، رسالة لنيل شهادة الماجستير في القانون العام المعمق بكلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2015/2014، والتي تناولت فيها الباحثة المراقبة المادية والمراقبة الالكترونية في الفصل الأول، ثم التسرب ونظامه القانوني في الفصل الثاني.

4. دراسة ثائر خضر أحمد بني عودة الموسومة بجريمة انتحال الشخصية الالكترونية وفقا للقرار بقانون بشأن الجرائم الالكترونية الفلسطيني "دراسة تحليلية"، مذكرة مقدمة لنيل شهادة الماجستير في القانون، تخصص العلوم الجنائية بكلية الدراسات العليا، الجامعة العربية الامريكية، فلسطين، 2024، والتي تطرق فيها الباحث لأحكام القواعد الموضوعية لجريمة انتحال الشخصية الالكترونية في الفصل الأول، ثم القواعد الإجرائية لجريمة انتحال الشخصية الالكترونية في الفصل الثاني.

التعقيب على الدراسات السابقة:

من خلال استعراض الدراسات السابقة يتضح أنها شكلت مرجعية علمية مهمة في مجال الجرائم الإلكترونية، حيث أسهمت في معالجة العديد من الجوانب القانونية والإجرائية المرتبطة بهذا النوع من الجرائم، غير أنها لم تتناول موضوع الحماية من الانتحال الرقمي بشكل مباشر ومستقل وهو ما نسعى من خلاله في دراستنا.

فدراسة خضرة شنبر قدمت تحليلاً شاملاً للجريمة الإلكترونية من حيث مفاهيمها وآليات مكافحتها سواء الإجرائية أو المؤسساتية، غير أنها عالجت الموضوع بصفة عامة دون تخصيص الانتحال الرقمي كجريمة قائمة بذاتها أو إبراز آليات حماية الأشخاص منه بشكل دقيق.

أما دراسة دلال مولاي ملياني، فقد ركزت على إشكالية الإثبات في جرائم الإنترنت وهو جانب إجرائي بالغ الأهمية يتقاطع مع موضوع دراستنا خاصة فيما يتعلق بصعوبة إثبات جرائم الانتحال الرقمي، إلا أنها اقتصرت على جانب الإثبات دون التوسع في آليات الحماية القانونية والوقائية للأشخاص.

وبالنسبة لدراسة أمينة ركاب فقد تناولت أساليب التحري الخاصة في جرائم الفساد وهي وإن كانت لا تتعلق مباشرة بالجرائم الإلكترونية، إلا أنها تبرز أهمية الوسائل التقنية الحديثة في الكشف عن الجرائم، وهو ما يمكن الاستفادة منه في مجال تتبع جرائم الانتحال الرقمي، غير أنها لم تعالج خصوصية هذا النوع من الجرائم في البيئة الرقمية.

في حين تعد دراسة ثائر خضر أحمد بني عودة الأقرب إلى موضوع البحث، حيث تناولت جريمة انتحال الشخصية الإلكترونية من الجانبين الموضوعي والإجرائي، غير أنها اقتصرت على الإطار القانوني الفلسطيني، كما ركزت على انتحال الشخصية فقط دون التوسع في المفهوم الأوسع للانتحال الرقمي أو آليات الحماية الشاملة للأشخاص.

وعليه، تتميز دراستنا عن الدراسات السابقة بكونها تسعى إلى تقديم معالجة متكاملة لموضوع حماية الأشخاص من الانتحال الرقمي من خلال الجمع بين الجوانب الموضوعية والإجرائية، مع التركيز على الآليات الوقائية والقانونية في إطار التشريع الجزائري، مع الاستئناس ببعض المقارنات وهو ما يساهم في سد النقص الذي لم تتناوله الدراسات السابقة بشكل كاف.

تقسيم الدراسة:

وقد تم تقسيم هذا البحث إلى فصلين رئيسيين، حيث تناولنا في الفصل الأول الإطار المفاهيمي والقانوني للانتحال الرقمي، من خلال التعريف به وبيان خصائصه وصوره، إضافة إلى استعراض التنظيم القانوني له، أما الفصل الثاني فقد خصصناه لدراسة آليات حماية الأشخاص من الانتحال الرقمي سواء كانت وقائية أو قانونية أو تقنية، مع تحليل مدى فعاليتها في الحد من هذه الظاهرة.

وفي الختام، قمنا بعرض أهم النتائج التي توصلنا إليها مع تقديم مجموعة من التوصيات والاقتراحات التي من شأنها تعزيز الحماية القانونية للأشخاص في مواجهة الانتحال الرقمي.

الفصل الأول:

الإطار المفاهيمي والقانوني للانتقال الرقمي

تمهيد:

إن التطور المتسارع في مجال تكنولوجيا المعلومات والاتصال من أبرز السمات التي ميزت العصر الحديث، حيث أصبح الاعتماد على الوسائل الرقمية والإنترنت جزءا أساسيا من الحياة اليومية للأفراد والمؤسسات على حد سواء، فقد ساهمت هذه الثورة الرقمية في تسهيل عملية التواصل وتبادل المعلومات وإنجاز المعاملات المختلفة بسرعة وكفاءة كما فتحت آفاقا واسعة للاستفادة من الخدمات الإلكترونية في مختلف المجالات الاقتصادية والاجتماعية والإدارية، غير أن هذا التطور التكنولوجي رغم إيجابياته العديدة أفرز في المقابل مجموعة من التحديات والمخاطر التي تهدد أمن الأفراد والمجتمع ومن أبرزها الجرائم المرتبطة بالفضاء الرقمي والتي تعرف بالجرائم الإلكترونية.

ومن بين هذه الجرائم الحديثة برزت ظاهرة الانتقال الرقمي التي أصبحت تشكل خطرا متزايدا نتيجة الانتشار الواسع لمواقع التواصل الاجتماعي والمنصات الرقمية المختلفة، الذي يعتبر قيام شخص باستخدام هوية أو بيانات شخصية تعود لشخص آخر في البيئة الرقمية دون إذنه، حيث تكمن خطورة هذا الفعل في ما قد يترتب عنه من أضرار مادية أو معنوية تمس بسمعة الأفراد وحقوقهم الشخصية، وقد تمتد آثاره إلى المساس بالأمن الاجتماعي والاقتصادي، ولمواجهة هذه الظاهرة اتجهت العديد من الدول إلى سن تشريعات خاصة تهدف إلى حماية الهوية الرقمية للأفراد ومكافحة الأفعال المرتبطة بانتحالها وذلك من خلال وضع قواعد قانونية تنظم استخدام الوسائل الإلكترونية وتجرم الاعتداءات الواقعة على المعطيات الشخصية والهوية الرقمية.

وانطلاقاً من ذلك، تبرز أهمية دراسة جريمة الانتحال الرقمي من الناحية القانونية لما لها من آثار خطيرة على حقوق الأفراد وحرياتهم، إضافة إلى ما تطرحه من إشكالات قانونية تتعلق بتحديد مفهومها وبيان خصائصها وتمييزها عن الجرائم المشابهة لها، كما تقتضي هذه الدراسة الوقوف على الإطار القانوني الذي وضعه المشرع لحماية الأفراد من هذه الممارسات غير المشروعة سواء على المستوى الدستوري أو التشريعي أو الجنائي، وعليه سنتطرق في هذا الفصل إلى الإطار المفاهيمي للانتحال الرقمي من خلال بيان مفهومه وخصائصه وأشكاله المختلفة (المبحث الأول)، ثم التتبع إلى الأساس القانوني الذي يضمن حماية الأشخاص من هذه الجريمة في التشريع (المبحث الثاني).

المبحث الأول: ماهية الانتحال الرقمي:

يعد الانتحال الرقمي من الظواهر الإجرامية المستحدثة التي ظهرت نتيجة الانتشار الواسع للتكنولوجيا الرقمية والاعتماد المتزايد على الإنترنت في مختلف المعاملات اليومية، حيث يقوم هذا السلوك الإجرامي على استغلال الوسائل الإلكترونية للانتحال صفة أو هوية شخص آخر بهدف تحقيق مصلحة غير مشروعة أو الإضرار بالغير، ونظراً لخطورة هذه الظاهرة وآثارها السلبية على الأفراد والمجتمع أصبح من الضروري تحديد مفهومها بدقة (المطلب الأول)، وبيان خصائصها وأشكالها المختلفة (المطلب الثاني)، كما يقتضي الأمر التمييز بينها وبين بعض المفاهيم القانونية المشابهة التي قد تختلط بها (المطلب الثالث).

المطلب الأول: مفهوم الانتحال الرقمي:

يقصد بالانتحال الرقمي قيام شخص باستعمال هوية غيره أو بياناته الشخصية عبر الوسائل الإلكترونية كشبكة الإنترنت أو وسائل التواصل الاجتماعي بهدف خداع الغير أو تحقيق منفعة معينة، وقد أصبح هذا النوع من الجرائم من أبرز الجرائم المعلوماتية في العصر الحديث نتيجة الانتشار الواسع للتكنولوجيا الرقمية وتزايد الاعتماد على المعاملات الإلكترونية، ولتوضيح هذا المفهوم سنتطرق إلى تعريف انتحال الشخصية الإلكترونية في اللغة والاصطلاح.

الفرع الأول: تعريف الانتحال الرقمي لغة:

يقصد بالانتحال في اللغة ادعاء الشيء ونسبته إلى النفس مع أنه في الحقيقة يعود إلى غير صاحب الادعاء، فقد جاء في معاجم اللغة العربية أن الانتحال يعني الادعاء أو نسبة قول أو فعل إلى النفس وهو في الأصل لغيره.¹

وقد ورد في لسان العرب لابن منظور أن الانتحال يعني ادعاء قول أو شعر أو فعل ونسبته إلى النفس وهو لغير صاحبه، فيقال: "انتحل فلان قول فلان" أي ادعاه لنفسه ونسبه إليه وهو في الحقيقة لغيره،² كما جاء في معجم مقاييس اللغة لابن فارس

¹ - محمد بن يعقوب الفيروزآبادي، القاموس المحيط، تحقيق مكتب التراث في مؤسسة الرسالة، الطبعة الثامنة، مؤسسة الرسالة، بيروت، لبنان، 2005، ص 1061.

² - محمد بن مكرم ابن منظور، لسان العرب، الجزء 11، المطبعة الأدبية ببغداد، مصر، 1988، ص 650.

أن مادة "نحل" تدل في أحد معانيها على الادعاء، فيقال انتحل الشيء إذا ادعاه ونسبه إلى نفسه دون وجه حق.¹

أما لفظ الشخصية في اللغة فيقصد به الصفات والخصائص التي تميز الشخص عن غيره، وهي مشتقة من كلمة "شخص" التي تعني ذات الإنسان أو هيئته الظاهرة التي تميزه عن الآخرين، وبالتالي فإن الشخصية تدل على مجموع الصفات التي تجعل الفرد متميزاً عن غيره من الأشخاص.²

الفرع الثاني: تعريف الانتحال الرقمي اصطلاحاً:

يقصد بانتحال الرقمي للشخصية في مفهومه العام أن يدعي شخص لنفسه شخصية غيره أو يتمصها بقصد خداع الآخرين أو تحقيق مصلحة معينة،³ وقد عرف بعض الفقه هذا المفهوم بأنه قيام شخص بادعاء صفة أو هوية غيره بطرق خفية توهم الغير بأنها الحقيقة.⁴

¹ - ابن فارس، معجم مقاييس اللغة، تحقيق عبد السلام هارون، دار الفكر للنشر والتوزيع، بيروت، لبنان، 1979، ص 402.

² - محمد بن مكرم ابن منظور، لسان العرب، مرجع سابق، ص 650.

³ - أحمد عبد السلام علي، التعليق على جرائم التزييف والتزوير في قضاء العقوبات في ضوء الفقه والقضاء، دار الكتب القانونية، مصر، 2007، ص 121.

⁴ - ولاء البياري، انتحال الشخصية في الفقه الإسلامي، رسالة مقدمة لنيل شهادة الماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة فلسطين، 2018، ص 11.

كما عرف أيضا بأنه قيام شخص بالاستيلاء على بعض البيانات أو المعلومات الشخصية الخاصة بشخص آخر، ثم استعمال هذه المعلومات للانتحال شخصيته والتعامل مع الآخرين باسمه وذلك غالبا لتحقيق أغراض مالية أو غيرها من المصالح.¹

أما بالنسبة للانتحال الرقمي فيعد من الجرائم الحديثة التي ظهرت نتيجة التطور الكبير في تكنولوجيا المعلومات والاتصال وانتشار استخدام شبكة الإنترنت ووسائل التواصل الاجتماعي، ويقصد به أنه سلوك كاذب يقوم به شخص باستخدام هوية أو بيانات شخصية لشخص آخر عبر الوسائط الإلكترونية دون إذنه بهدف خداع الغير أو تحقيق منفعة معينة أو الإضرار بصاحب الهوية الحقيقية،² كما يقصد به السلوك غير المشروع الذي يتم من خلاله تقمص هوية شخص آخر عبر الوسائط الإلكترونية أو الشبكات المعلوماتية،³ بحيث يظهر الجاني أمام الغير بمظهر الشخص الحقيقي الذي تم انتحال شخصيته مما يؤدي إلى خداع المتعاملين معه وإيهامهم بأنهم يتعاملون مع الشخص الحقيقي.⁴

¹ - عبد العزيز الشبل، الاعتداء الإلكتروني "دراسة فقهية"، دار كنوز اشبيليا، الرياض، 2012، ص 407.

² - عبد القادر بن عبد الله بن محمد آل معبر، جريمة الانتحال الإلكتروني "دراسة مقارنة بين الفقه الإسلامي والنظام السعودي"، مجلة كلية الدراسات الإسلامية والعربية للبنات بدمنهور، المجلد الثاني، العدد التاسع، 2024، ص 1036.

³ - ثائر خضر أحمد بني عودة، جريمة انتحال الشخصية الإلكترونية وفقا للقرار بقانون بشأن الجرائم الإلكترونية الفلسطيني "دراسة تحليلية"، مذكرة مقدمة لنيل شهادة الماجستير في القانون، تخصص العلوم الجنائية، كلية الدراسات العليا، الجامعة العربية الأمريكية، فلسطين، 2024، ص 06.

⁴ - زيد بني خالد، التنظيم القانوني لجريمة انتحال الشخصية الإلكترونية وفقا لقانون الجرائم الإلكترونية الأردني، رسالة مقدمة لنيل شهادة الماجستير، كلية الحقوق، جامعة جرش، 2021، ص 15.

كما يتم الانتحال الرقمي من خلال قيام المجرم الإلكتروني بانتحال شخصية الضحية أو المجني عليه عبر الوسائل الإلكترونية، وذلك بهدف الاستفادة من سمعته أو سلطته أو مكانته الاجتماعية أو حتى من أمواله، وقد يتم هذا الانتحال من خلال استخدام بياناته الشخصية أو إنشاء حسابات إلكترونية باسمه أو التظاهر بالتعامل باسمه أمام الغير، كما قد يمتد الأمر إلى انتحال شخصية بعض المواقع أو الجهات الإلكترونية الموثوقة بهدف خداع المستخدمين واستغلال ثقتهم لتحقيق مكاسب غير مشروعة، حيث يكثر استخدام هذا النوع من الانتحال خاصة في المجال التجاري، إذ يستغل الجاني ثقة المتعاملين بالضحية أو بالموقع المنتحل من أجل الحصول على معلومات أو أموال بطرق احتيالية.¹

وبذلك يمكننا تعريف الانتحال الرقمي بأنه قيام شخص باستخدام بيانات أو هوية شخص آخر عبر شبكة الإنترنت أو الأنظمة المعلوماتية، بقصد خداع الغير أو تحقيق منفعة معينة وهو سلوك يجرمه القانون لما ينطوي عليه من اعتداء على الخصوصية والحقوق الشخصية للأفراد.

المطلب الثاني: خصائص وأشكال الانتحال الرقمي:

إن دراسة الانتحال الرقمي لا يكفي فقط التطرق لتعريفها بل لا بد من التطرق لكل من خصائصه وأشكاله المتنوعة وهي على النحو التالي:

الفرع الأول: خصائص الانتحال الرقمي:

¹ - عمرو موسى، الجرائم المعلوماتية "جرائم الحاسب الآلي في مصر وفي الدول العربية"، المكتب الجامعي، الإسكندرية، مصر، 2006، ص 102.

تتميز الجرائم الإلكترونية، ومن بينها جريمة الانتحال الرقمي بجملة من الخصائص التي تميزها عن الجرائم التقليدية، ويرجع ذلك أساسا إلى ارتباطها بالتطور التكنولوجي واستخدام وسائل الاتصال الحديثة، ويمكن إبراز أهم هذه الخصائص فيما يلي:

1. صعوبة اكتشاف الانتحال الرقمي:

يتسم الانتحال الرقمي بكونه خفيا ومستترا في أغلب الأحيان، إذ قد تقع الجريمة دون أن يشعر بها الضحية حتى أثناء وجوده على شبكة الإنترنت، ويعود ذلك إلى امتلاك الجاني مهارات تقنية تمكنه من تنفيذ الجريمة بدقة عالية، كإرسال الفيروسات، أو سرقة البيانات والمعلومات الخاصة، أو إتلافها، أو التجسس على الاتصالات وغيرها من الأفعال الإجرامية،¹ كما أن هذه الجرائم غالبا لا تترك أثارا مادية واضحة بعد ارتكابها الأمر الذي يصعب من مهمة اكتشافها أو إثباتها، ولذلك فإن التعامل مع هذا النوع من الجرائم يتطلب خبرة فنية متخصصة وقدرات تقنية عالية من قبل جهات التحقيق.²

2. الانتحال الرقمي عابر للحدود:

¹ - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، 2009، ص 31.

² - محمد رحموني، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، المجلد 16، العدد الثالث، الجزائر، سبتمبر 2017، ص 441.

يعد الانتحال الرقمي من الجرائم الإلكترونية العابرة للحدود الجغرافية، حيث لا تعترف بحدود الدول أو القارات، فمع انتشار شبكة الإنترنت والاتصالات الحديثة أصبح من الممكن ربط ملايين أجهزة الحاسوب عبر مختلف دول العالم مما يسمح بارتكاب الجريمة من أي مكان، فقد يكون الجاني موجودا في دولة معينة بينما يكون المجني عليه في دولة أخرى،¹ وقد تتواجد البيانات محل الاعتداء في دولة ثالثة، وبهذا أصبح مسرح الجريمة المعلوماتية ذا طابع عالمي، إذ يمكن للجاني ارتكاب فعله الإجرامي عن بعد دون الحاجة إلى التواجد المادي في مكان وقوع الجريمة.²

3. المنتحل الرقمي شخص ذكي ومتخصص:

غالبا ما يتمتع المنتحل الرقمي بدرجة عالية من الذكاء والمهارة التقنية، حيث يمتلك معرفة متخصصة في مجال الحاسوب وتقنيات المعلومات تمكنه من اختراق الأنظمة الإلكترونية والتلاعب بها، كما يستطيع تطوير أساليب جديدة للتحايل على الأنظمة الأمنية وتجاوز وسائل الحماية، وعادة ما يقوم هذا النوع من المجرمين بدراسة البيئة المعلوماتية المستهدفة بعناية قبل تنفيذ الجريمة بهدف تقادي اكتشافه أو تتبع نشاطه عبر الشبكات أو داخل أجهزة الحاسوب.³

¹ - عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية، القاهرة، مصر، 2005، ص 42.

² - نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، ص 52.

³ - طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني لحماية المعلوماتي"، دار الجامعة الجديدة، القاهرة، مصر، 2009، ص 177.

4. جريمة هادئة لا تعتمد على المجهود العضلي:

تختلف جريمة الانتحال الرقمي عن الانتحال التقليدي التي تعتمد غالبا على القوة أو المجهود العضلي كالسرقة أو الاعتداء الجسدي... الخ، فالانتحال الرقمي يعتمد أساسا على الجهد الذهني والمعرفة التقنية، حيث يقوم الجاني باستخدام مهاراته في مجال الحاسوب والبرمجيات لاخترق الأنظمة المعلوماتية أو التلاعب بالبيانات،¹ ويعود ذلك إلى أن هذه الجرائم تتعلق بمعطيات ومعلومات رقمية يمكن تعديلها أو حذفها أو نقلها داخل أنظمة الحاسوب دون الحاجة إلى استخدام القوة المادية.²

5. صعوبة اثبات جريمة الانتحال الرقمي:

يعد إثبات هذه الجريمة من المسائل المعقدة نظرا لعدم وجود أدلة مادية تقليدية كالتي توجد في الجرائم العادية مثل البصمات أو الآثار المادية، فهي غالبا ما تتم في شكل بيانات أو أرقام رقمية داخل أنظمة الحاسوب، وقد يتم اكتشافها بعد فترة طويلة من ارتكابها أو عن طريق الصدفة،³ كما أن تعقب مرتكبيها يتطلب خبرة تقنية متقدمة، خاصة وأن الجناة غالبا ما يستخدمون أساليب التمويه والتضليل لإخفاء هويتهم وعدم الكشف عن أفعالهم الإجرامية.⁴

¹ - عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، مرجع سابق، ص 46.

² - محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها، مرجع سابق، ص 442.

³ - رستم هشام، الجرائم المعلوماتية "أصول التحقيق الجنائي الفني"، مجلة الأمن والقانون، العدد الثاني، 1999، ص 11.

⁴ - محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها، مرجع سابق، ص 443.

الفرع الثاني: أشكال الانتحال الرقمي:

تتخذ جريمة الانتحال الرقمي عدة صور وأساليب تختلف باختلاف الوسائل التقنية التي يستخدمها الجناة، ومن بين أبرز هذه الأشكال ما يلي:

1. التصيد الاحتيالي: يعد التصيد الاحتيالي من أكثر صور الانتحال الرقمي

انتشاراً، وهو أسلوب من أساليب الهندسة الاجتماعية يقوم فيه المجرم الإلكتروني بانتحال صفة جهة موثوقة أو كيان معروف كالمؤسسات المالية أو المواقع الإلكترونية الرسمية، بهدف خداع الضحية وإقناعه بالكشف عن معلوماته الشخصية أو اتخاذ إجراء معين يؤدي إلى اختراق أمنه المعلوماتي، ويعتمد مرتكبو التصيد الاحتيالي على عدة وسائل لارتكاب جرائمهم من بينها إرسال رسائل عبر البريد الإلكتروني أو الرسائل النصية القصيرة عبر الهاتف المحمول، أو نشر روابط ومنشورات عبر مواقع التواصل الاجتماعي، أو حتى إجراء مكالمات هاتفية مباشرة مع الضحايا، وغالباً ما تتضمن هذه الرسائل أو المنشورات روابط لمواقع إلكترونية مزيفة صممها الجناة لتبدو مشابهة للمواقع الأصلية وذلك بغرض خداع الضحية ودفعه إلى إدخال بياناته الحساسة.¹

2. تزوير الهوية الرقمية: يقصد بتزوير الهوية الرقمية قيام شخص باستخدام

بيانات أو معلومات تعريفية تعود لشخص آخر دون إذنه، وذلك بقصد الظهور أمام الغير بمظهر ذلك الشخص الحقيقي، ويتم ذلك من خلال الاستيلاء على

¹ - حسام نبيل الشنراقي، التصيد الاحتيالي في ظل التطور التقني "أنماطه، تحديات المكافحة، الحلول"-دراسة تحليلية-، مجلة الدراسات القانونية والاقتصادية، المجلد العاشر، العدد الثالث، سبتمبر 2024، ص 2417.

بعض عناصر الهوية الرقمية للضحية كالاسم أو الصورة الشخصية أو عنوان البريد الإلكتروني أو الحسابات على مواقع التواصل الاجتماعي، ثم استعمالها لإنشاء حسابات مزيفة أو التعامل مع الآخرين باسمه.¹

3. الانتحال الصوتي: يعد الانتحال الصوتي من الصور الحديثة للانتحال الرقمي، ويعتمد على استخدام تقنيات الذكاء الاصطناعي في تقليد أو توليد أصوات مشابهة للأصوات البشرية، حيث تستعمل هذه التقنية في العديد من المجالات المشروعة كالأنظمة الصوتية التفاعلية وصناعة الترفيه، إلا أنها قد تستغل أيضاً لأغراض غير مشروعة كخداع الأفراد أو المؤسسات من خلال تقليد صوت شخص معين والتحدث باسمه، ويعرف التقليد الصوتي الرقمي بأنه عملية تقنية تعتمد على الذكاء الاصطناعي لتحليل الخصائص الصوتية لشخص معين وإعادة إنتاجها بشكل يجعل الصوت الناتج يبدو وكأنه صادر عن الشخص الحقيقي.²

4. الانتحال العلمي: يقصد بالانتحال العلمي استخدام أفكار أو أعمال الآخرين دون الإشارة إلى مصدرها الحقيقي أو نسبتها إلى أصحابها سواء كان ذلك بقصد أو دون قصد، ويعد هذا السلوك من أخطر الانتهاكات الأكاديمية لأنه يمس بمبدأ الأمانة العلمية والنزاهة في البحث العلمي، ولا يقتصر الانتحال

¹ - فتحة سويس، انتحال الهوية الرقمية، المجلة الجزائرية للقانون والعدالة، المجلد 11، العدد الأول، جوان 2025، ص 90.

² - هند سفر حمدان العتيبي، التقليد الصوتي الرقمي والاحتيال المالي من منظور خبراء الأمن السيبراني، بحوث ودراسات، العدد 166، 2025، ص 182.

العلمي على سرقة النصوص المكتوبة فقط، بل يشمل أيضا الاستيلاء على الأفكار والآراء والرسوم والبرامج الحاسوبية وغيرها من أشكال الإبداع الفكري، وبناء على ذلك يمكن تعريف الانتحال أو السرقة العلمية بأنها قيام شخص باقتباس كتابات أو أفكار الغير كلياً أو جزئياً، ونسبتها إلى نفسه دون الإشارة إلى صاحبها الأصلي وهو ما يشكل مخالفة للأعراف الأكاديمية وانتهاكا لحقوق الملكية الفكرية.¹

5. الاحتيال التجاري: يقصد بالاحتيال التجاري كل فعل يقوم به الفاعل بهدف الإيقاع بالآخرين أو تحقيق مكاسب غير مشروعة، وذلك من خلال الاستفادة من طبيعة أو خصائص المواد أو الفوائد التي تدخل عليها أعماله، وقد يتم الغش عبر استبدال مواد أقل قيمة بأخرى أعلى، أو تقليل كمية المادة أو إضافة مواد أخرى تزيد من حجمها بينما تقلل من جودتها أو فعاليتها، وكل ذلك بغرض تحقيق أرباح طائلة بطرق غير مشروعة.²

المطلب الثالث: تمييز الانتحال الرقمي عن المفاهيم المشابهة:

يمكن تمييز الانتحال الرقمي عن مجموعة من المفاهيم المشابهة والمتمثلة في التزوير الإلكتروني والابتزاز الإلكتروني.

¹ - سعاد أجمود، السرقة العلمية وطرق مكافحتها، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الثاني، العدد الثامن، ديسمبر 2017، ص 567.

² - عبد الفتاح بيومي الحجازي، حماية المستهلك عبر شبكة الانترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص 53.

الفرع الأول: تمييز الانتحال الرقمي عن التزوير الإلكتروني:

يتشابه الانتحال الرقمي والتزوير الإلكتروني في جوانب عدة، حيث يعتمد كلاهما على الوسائل التقنية كالحاسوب كأداة رئيسية في ارتكاب الأفعال المجرمة، بالإضافة لكونهما جريمتان عابرتان لا تحتاجان لجهد عضلي بل هما جريمتان هادئتان، بالإضافة إلى كونهما عابرتان للحدود ويصعب اكتشافهما، مع ذلك تبرز الفروق بوضوح بينهما، إذ يتم الانتحال الرقمي من خلال استغلال اسم الشخص، صورته، أو صفته الوظيفية وذلك عن طريق إنشاء حسابات مزيفة على وسائل التواصل الاجتماعي أو استخدام البريد الإلكتروني الخاص بالغير للظهور بمظهرهم، أما التزوير الإلكتروني فهو يقوم على تغيير الحقيقة أو البيانات سواء بالشهادة أو القول أو الكتابة أو العمل، أو تحريف الوثائق الرقمية، بهدف حرمان المستحق من حقه أو الاستيلاء على حقوق الآخرين أو الحصول على مكاسب غير مشروعة.¹

الفرع الثاني: تمييز الانتحال الرقمي عن الابتزاز الإلكتروني:

يختلف الانتحال الرقمي عن الابتزاز الإلكتروني من خلال أن الانتحال الرقمي كما سبق ذكره يركز على استخدام هوية شخص آخر أو بياناته لإيهام الغير وتحقيق منفعة، دون أن يقتضي ذلك الضغط المباشر على الضحية، أما الابتزاز الإلكتروني فيقوم على استخدام أساليب الضغط المادي أو المعنوي لدفع الضحية إلى القيام بسلوك معين يجلب منفعة للمبتز، مع العلم المسبق بعدم قدرة الضحية المطلقة على مقاومة

¹ - أحمد محمد محروس عبد العال، التزوير الإلكتروني بين التشريع التقليدي وآليات المواجهة الحديثة، المجلة

الأكاديمية للأبحاث والنشر العلمي، العدد 70، فيفري 2025، ص 48.

هذا الضغط، وقد يكون المبتز شخصا أو منظمة، ويهدف من وراء هذه الأفعال إلى الحصول على منفعة مباشرة أو إجبار الضحية على تقديم خدمة محددة سواء كانت مالية أو معلوماتية أو غيرها.¹

المبحث الثاني: الأساس القانوني لحماية الأشخاص من الانتحال الرقمي:

تسعى التشريعات الحديثة إلى توفير الحماية القانونية للأفراد في مواجهة الجرائم المرتكبة عبر الفضاء الإلكتروني ومن بينها جريمة الانتحال الرقمي التي تمس بالحقوق الشخصية والهوية الرقمية للأفراد، وقد تجلت هذه الحماية في العديد من النصوص الدستورية والتشريعية التي تكفل حماية الحياة الخاصة والمعطيات الشخصية للأشخاص، كما أقر المشرع عقوبات جنائية تهدف إلى ردع الأفعال المرتبطة بانتحال الهوية الرقمية، وتبرز أهمية هذه الحماية في ظل تزايد استخدام الوسائل الرقمية وما يترتب عنه من مخاطر تهدد أمن الأفراد والمجتمع، لذلك أصبح من الضروري لنا دراسة الإطار القانوني الذي ينظم حماية الأشخاص من هذه الجريمة في مختلف النصوص القانونية من خلال الحماية الدستورية والتشريعية (المطلب الأول)، ثم

¹ - فاطمة العرفي، حجية الدليل الرقمي في اثبات جريمة الابتزاز الإلكتروني في القانون الجزائري، مجلة صوت

القانون، المجلد الثامن، العدد الثاني، أكتوبر 2022، ص 495-496.

الحماية الجنائية للهوية الرقمية (المطلب الثاني)، وأخيرا موقف المشرع الجزائري من الانتحال الرقمي (المطلب الثالث).

المطلب الأول: الحماية الدستورية والتشريعية:

لم يتطرق المؤسس الدستوري في الجزائر إلى مسألة الانتحال الرقمي بصفة صريحة ومباشرة، إلا أنه أقر مجموعة من المبادئ العامة التي تكفل حماية الأشخاص وحقوقهم الأساسية، والتي يمكن الاستناد إليها في مواجهة هذه الظاهرة، فالدستور الجزائري يولي أهمية كبيرة لحماية كرامة الإنسان وخصوصيته وصون حياته الخاصة، وهي حقوق قد تتعرض للانتهاك نتيجة ممارسات الانتحال الرقمي، وفي هذا الإطار نصت المادة 81 من التعديل الدستوري لسنة 2020 على أن كل شخص يمارس حرياته في إطار احترام الحقوق المعترف بها للغير في الدستور، خاصة ما يتعلق باحترام الحق في الشرف والحياة الخاصة وحماية الأسرة والطفولة والشباب،¹ ويستفاد من خلال استقراءنا لنص المادة سالف الذكر أن المشرع الدستوري حرص على إيجاد توازن بين ممارسة الحريات الفردية وعدم الاعتداء على حقوق الآخرين، وهو ما يشكل أساسا قانونيا لحماية الأفراد من أي اعتداء على شخصيتهم أو سمعتهم بما في ذلك الانتحال الرقمي.

كما عزز الدستور هذه الحماية من خلال المادة 47 التي نصت على أن حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي تعد حقا أساسيا، وأن القانون

¹ - انظر المادة 81 من المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج ر العدد 82 المؤرخة في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020.

يعاقب على كل انتهاك لهذه الحقوق، حيث تعد هاته المادة مواكبة واضحة للتطورات التكنولوجية وانتشار استخدام الوسائل الرقمية، حيث أصبح تداول البيانات الشخصية عبر الأنظمة المعلوماتية يشكل أحد أهم المجالات التي قد يستغلها الجناة في ارتكاب جرائم الانتحال الرقمي،¹ ومن الملاحظ أن المشرع الجزائري من خلال التعديل الدستوري لسنة 2020 قد وسع من نطاق الحماية الدستورية للأشخاص، مقارنة بالتعديل الدستوري لسنة 2016 الذي ركز بشكل أساسي على حماية الأشخاص الطبيعيين فقط، بينما جاء التعديل الجديد ليؤكد على حماية أوسع للحقوق المرتبطة بالشخصية والبيانات الشخصية في البيئة الرقمية.

كما حاول المشرع الجزائري مواجهة هذه الظاهرة من خلال مجموعة من النصوص القانونية التي تتعلق بالجرائم المعلوماتية والاعتداء على الأنظمة المعلوماتية والبيانات الشخصية، ومن بين أهم هذه النصوص القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، والذي جاء لمواكبة التطور التكنولوجي وانتشار استعمال الوسائل الرقمية في مختلف المجالات،² كما تدخل المشرع الجزائري لاحقا من خلال القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي والذي يهدف إلى ضمان حماية البيانات الشخصية للأفراد ومنع استعمالها أو معالجتها بطريقة غير مشروعة، وهو ما يشكل إحدى الوسائل القانونية المهمة

¹ - انظر المادة 47 من المرسوم الرئاسي رقم 20-442، مصدر سابق.

² - انظر أحكام القانون رقم 09-04 المؤرخ في 05 غشت 2009، القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر العدد 47 الصادرة بتاريخ 06 غشت 2009.

لمواجهة جرائم الانتحال الرقمي التي تعتمد أساسا على استغلال البيانات الشخصية للغير.¹

وعليه، فإن النصوص الدستورية والتشريعية وإن لم تتناول الانتحال الرقمي بشكل مباشر، إلا أنها توفر إطارا عاما للحماية يمكن من خلاله مواجهة هذه الجريمة، خاصة عندما تمس الشرف أو السمعة أو الحياة الخاصة للأفراد أو عند الاعتداء على بياناتهم الشخصية.

المطلب الثاني: الحماية الجنائية للهوية الرقمية:

يمكن مواجهة بعض صور الانتحال الرقمي من خلال نصوص قانون العقوبات الجزائي التي تجرم أفعالا مرتبطة بالجرائم المعلوماتية كالاعتداء على الأنظمة المعلوماتية أو الدخول غير المشروع إليها، أو استغلال البيانات والمعلومات دون وجه حق، ومن بين هذه النصوص المواد المتعلقة بالدخول غير المشروع إلى الأنظمة المعلوماتية وتخريب البيانات أو تعديلها، والتي يمكن تطبيقها في بعض الحالات المرتبطة بالانتحال الرقمي.

الفرع الأول: العقوبات الأصلية:

من خلال استقراء النصوص القانونية المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية في التشريع الجزائي، يتضح أن المشرع قد أقر نظاما عقابيا متدرجا

¹ - انظر احكام القانون رقم 18-07 المؤرخ في 10 يونيو 2018، لمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر العدد 34 لسنة 2018، المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 يوليو 2025، ج ر العدد 48 الصادرة بتاريخ 24 يوليو 2025.

يتناسب مع خطورة الفعل الإجرامي المرتكب، ويظهر هذا التدرج في تحديد العقوبات وفقاً لدرجة الاعتداء على الأنظمة المعلوماتية أو المعطيات الرقمية، حيث يمكن التمييز بين ثلاث درجات أساسية من الجرائم، تتمثل الدرجة الأولى في جريمة الدخول أو البقاء بالغش داخل النظام المعلوماتي وهي الصورة البسيطة للجريمة، وقد حدد المشرع لها عقوبة تتمثل في الحبس من ثلاثة أشهر إلى سنة، وغرامة مالية تتراوح بين 50.000 دج و 100.000 دج، وذلك وفقاً لما نصت عليه المادة 394 مكرر من قانون العقوبات والتي تعتبر كنص يتم تطبيقه على الجرائم المعلوماتية.¹

أما الدرجة الثانية فتتعلق بجريمة الدخول أو البقاء المشدد داخل النظام المعلوماتي حيث تتشدد العقوبة إذا ترتب عن هذا الفعل حذف أو تغيير المعطيات الموجودة داخل المنظومة المعلوماتية، وفي هذه الحالة تكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50.000 دج إلى 150.000 دج، خاصة إذا نتج عن الدخول أو البقاء غير المشروع تخريب في نظام تشغيل المنظومة المعلوماتية، وذلك طبقاً لما ورد في المادة 394 مكرر/02 و 03 من القانون سالف الذكر.²

أما الدرجة الثالثة فتتعلق بجريمة الاعتداء العمدي على المعطيات المعلوماتية والتي تعد من أخطر الجرائم المعلوماتية، حيث نصت المادة 394 مكرر 01 على أن العقوبة المقررة لهذا الفعل هي الحبس من ستة أشهر إلى ثلاث سنوات، وغرامة مالية

¹ - انظر المادة 394 مكرر من الأمر رقم 66-156 المؤرخ في مؤرخ في 8 جوان سنة 1966، المتضمن قانون العقوبات، ج ر ع 49، الصادرة في 11 جوان 1966. (المعدل والمتمم)

² - انظر الفقرتين 02 و 03 من المادة 394 مكرر من الأمر رقم 66-156، مصدر سابق.

تتراوح بين 500.000 دج و 2.000.000 دج، وذلك عندما يتعلق الأمر بتخريب أو تعديل أو إتلاف المعطيات الموجودة داخل النظام المعلوماتي.¹

الفرع الثاني: العقوبات التكميلية:

إضافة إلى العقوبات الأصلية، نص المشرع الجزائري في المادة 394 مكرر 03 على مجموعة من العقوبات التكميلية التي يمكن للقاضي الحكم بها في الجرائم الماسة بالأنظمة المعلوماتية، ومن أهمها:

1. المصادرة: وتشمل الأجهزة والبرامج والوسائل المستعملة في ارتكاب الجريمة، مع مراعاة حقوق الغير حسن النية.

2. إغلاق المواقع الإلكترونية: ويقصد بها المواقع التي تستعمل كوسيلة لارتكاب الجرائم المعلوماتية.

3. إغلاق المحل أو مكان الاستغلال: وذلك في حال ارتكبت الجريمة بعلم صاحب المكان كالمقاهي الإلكترونية التي يتم من خلالها ارتكاب هذه الجرائم.²

الفرع الثالث: العقوبات المقررة للشخص المعنوي:

أقر المشرع الجزائري مبدأ المسؤولية الجزائية للشخص المعنوي في قانون العقوبات، وذلك بموجب التعديل الوارد في تعديل قانون العقوبات لسنة 2004، وقد

¹ - انظر المادة 394 مكرر 01 من الأمر رقم 66-156، مصدر سابق.

² - انظر المادة 394 مكرر 03 من الأمر رقم 66-156، مصدر سابق.

نصت المادة 51 مكرر على إمكانية مساءلة الشخص المعنوي جزائيا عن الجرائم المرتكبة لحسابه أو باسمه، كما أكدت المادة 18 مكرر من نفس القانون على العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح،¹ وبالنسبة للغرامة المطبقة على الشخص المعنوي عند ارتكابه إحدى الجرائم الماسة بالأنظمة المعلوماتية، فإنها تعادل خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وذلك وفقا لما نصت عليه المادة 394 مكرر 2.04².

المطلب الثالث: موقف المشرع الجزائري من الانتحال الرقمي:

تبنى المشرع الجزائري موقفا صارما في مواجهة ظاهرة الانتحال الرقمي ولكن ليس بصفة مباشرة والجرائم المرتبطة باستعمال تكنولوجيا الإعلام والاتصال، وذلك من خلال إدخال تعديلات متتالية على قانون العقوبات بهدف مواكبة التطورات التكنولوجية والحد من الجرائم التي قد ترتكب عبر الفضاء الرقمي، وقد تجسد هذا التوجه أساسا من خلال التعديل الذي جاء به القانون رقم 04-15 المعدل والمتمم لقانون العقوبات رقم 66-156 والذي أدخل مجموعة من النصوص الجديدة التي تعاقب على بعض الأفعال المرتبطة بالمساس بالحياة الخاصة واستعمال الوسائط التكنولوجية في الاعتداء على الغير،³ كما تعزز هذا الاتجاه لاحقا من خلال القانون رقم 09-04 الذي أدرج أحكاما خاصة بحماية أنظمة المعالجة الآلية للمعطيات وتجريم الاعتداء عليها بحيث

¹ - انظر المادتين 51 مكرر و18 مكرر من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل لقانون العقوبات رقم 66-156، ج ر العدد 71 الصادرة بتاريخ 10 نوفمبر 2004.

² - انظر المادة 394 مكرر 04 من الأمر رقم 66-156، مصدر سابق.

³ - انظر أحكام القانون رقم 04-15، مصدر سابق.

يعد هذا القانون مكملًا لقانون العقوبات،¹ ثم جاء القانون رقم 20-06 ليشدد العقوبات ويوسع نطاق التجريم ليشمل بعض الأفعال المرتكبة عبر مواقع التواصل الاجتماعي، وهو ما يعكس توجه المشرع نحو إرساء حماية جنائية فعالة لمواجهة ظاهرة الانتحال الرقمي.²

ويتجلى موقف المشرع الجزائري كذلك من خلال نصوص المواد 394 مكرر إلى 394 مكرر 07 على تجريم الدخول أو البقاء في نظام معلوماتي أو جزء منه دون وجه حق، أو عن طريق الغش، كما جرم المشرع الأفعال التي تتمثل في حذف أو تعديل أو إدخال معطيات بطريقة غير مشروعة داخل هذه الأنظمة لما قد يترتب عنها من أضرار جسيمة تمس بسلامة المعلومات المخزنة أو بسير الأنظمة المعلوماتية، كما اتجه المشرع الجزائري إلى تشديد العقوبات بموجب التعديلات اللاحقة لقانون العقوبات حيث تم تعزيز الحماية الجنائية للأنظمة المعلوماتية من خلال تشديد العقوبات في الحالات التي يترتب فيها عن الاعتداء على النظام المعلوماتي حذف أو تغيير المعطيات أو تعطيل عمل النظام، وفي هذا السياق نصت المواد 394 مكرر وما بعدها على مضاعفة العقوبات عندما يكون الفعل موجهاً ضد أنظمة معلوماتية تابعة للدولة أو للمؤسسات العمومية أو الهيئات الحساسة، كما عاقب المشرع حتى على

¹ - انظر أحكام القانون رقم 09-04، مصدر سابق.

² - انظر أحكام القانون رقم 20-06 المؤرخ في 28 أبريل سنة 2020، يعدل ويتم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر العدد 25 الصادرة في 29 أبريل 2020.

مجرد محاولة الدخول غير المشروع إلى هذه الأنظمة، وهو ما يعكس الطابع الوقائي للتشريع الجزائري في مجال مكافحة الجرائم المعلوماتية.¹

ومن جهة أخرى، عمل المشرع الجزائري على مكافحة الاحتيال والانتحال الرقمي من خلال التعديل الذي مس بعض أحكام قانون العقوبات بموجب القانون رقم 06-20 سالف الذكر، حيث تم توسيع نطاق التجريم ليشمل بعض الأفعال المرتكبة عبر شبكة الإنترنت ومواقع التواصل الاجتماعي، فقد نصت المادة 372 من القانون رقم 06-20 على معاقبة انتحال اسم الغير أو صفته في ظروف قد تؤدي إلى تسجيل حكم في صحيفة السوابق القضائية، وهو ما يمكن تطبيقه على حالات انتحال الهوية الرقمية أو إنشاء حسابات مزيفة لاستغلال اسم أو صفة شخص آخر بهدف الاحتيال أو الإضرار به،² كما نصت المادة 196 مكرر على معاقبة نشر أو ترويج الأخبار الكاذبة عبر مختلف الوسائل بما فيها الوسائط الإلكترونية، إذا كان من شأن ذلك المساس بالنظام العام أو الأمن العمومي.³

كما أولى أيضا المشرع الجزائري عناية خاصة بحماية الحياة الخاصة للأفراد في البيئة الرقمية من خلال التعديلات التي جاء بها القانون رقم 04-15 والتي أدخلت نصوصا تجرم الاعتداء على الحياة الخاصة باستعمال الوسائل التكنولوجية، فقد نصت المواد 303 مكرر وما بعدها من قانون العقوبات على معاقبة كل من يقوم بالنقاط أو

¹ - انظر المواد من 394 مكرر 01 إلى 394 مكرر 07 من القانون رقم 06-20، مصدر سابق.

² - انظر المادة 372 من القانون رقم 06-20، مصدر سابق.

³ - انظر المادة 196 مكرر من القانون رقم 06-20، مصدر سابق.

تسجيل أو نقل صورة أو كلام لشخص في مكان خاص دون رضاه سواء تم ذلك
باستعمال أجهزة تقليدية أو وسائل إلكترونية حديثة.¹

¹ - انظر المواد من 303 مكرر وما بعدها من القانون رقم 04-15، مصدر سابق.

الفصل الثاني:

الآليات الوقائية لحماية الأشخاص
من الانتحال الرقمي

في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصال وما صاحبه من توسع في استخدام الوسائط الرقمية في مختلف مناحي الحياة، برزت تحديات جديدة تتعلق بحماية الأفراد من الجرائم الإلكترونية وعلى رأسها ظاهرة الانتحال الرقمي التي أصبحت تمثل تهديدا حقيقيا للهوية الشخصية والحقوق الفردية، فقد أتاح الفضاء الرقمي فرصا واسعة للتواصل والتفاعل لكنه في المقابل سهل ارتكاب ممارسات غير مشروعة من بينها انتحال صفة الغير واستغلال بياناتهم الشخصية لأغراض احتيالية أو تشهيرية أو إجرامية.

وأمام تنامي هذه الظاهرة، أصبح من الضروري تبني آليات متعددة لمواجهةها لا تقتصر فقط على الجانب القانوني الزجري بل تشمل أيضا التدابير الوقائية التي تهدف إلى الحد من وقوع الجريمة قبل حدوثها، إذ تلعب التوعية الرقمية دورا مهما في تمكين الأفراد من حماية بياناتهم الشخصية والتعامل الآمن مع الوسائط الإلكترونية، إضافة إلى ذلك تبرز أهمية التدابير التقنية التي تعتمد على وسائل تكنولوجية متطورة لحماية الهوية الرقمية من الاختراق أو الاستغلال غير المشروع، وفي المقابل أيضا تظل الآليات القانونية والقضائية ضرورية لمكافحة الانتحال الرقمي من خلال تجريم الأفعال المرتبطة به وفرض العقوبات المناسبة على مرتكبيها.

ومن هذا المنطلق، سنتطرق في هذا الفصل إلى دراسة مختلف الآليات المعتمدة لحماية الأشخاص من الانتحال الرقمي، سواء كانت وقائية (المبحث الأول)، أو قانونية وقضائية (المبحث الثاني).

المبحث الأول: الآليات الوقائية:

تعد الوقاية من الجرائم الإلكترونية ومن بينها الانتحال الرقمي من أهم الوسائل التي تساهم في الحد من انتشارها وتقليل آثارها السلبية على الأفراد والمجتمع، فبدل الاكتفاء بملاحقة الجريمة بعد وقوعها تسعى الآليات الوقائية إلى منع حدوثها من خلال تعزيز الوعي الرقمي لدى الأفراد وتوفير بيئة رقمية آمنة، وتتحقق هذه الوقاية من خلال مجموعة من الوسائل من أبرزها نشر ثقافة الاستخدام الآمن للإنترنت، وتدخل المؤسسات المختصة في تنظيم المجال الرقمي، إضافة إلى اعتماد تدابير تقنية حديثة تهدف إلى حماية البيانات الشخصية والهوية الرقمية، وعليه سنتناول في هذا المبحث دور التوعية والوقاية الرقمية في **المطلب الأول**، ثم دور المؤسسات والهيئات المختصة في **المطلب الثاني**، وأخيرا التدابير التقنية لحماية الهوية الرقمية في **المطلب الثالث**.

المطلب الأول: دور التوعية والوقاية الرقمية:

تعرف التوعية الرقمية بأنها مجموعة من الأنشطة التربوية والإعلامية التي تهدف إلى تعديل سلوك الأفراد في البيئة الرقمية، وتعزيز إدراكهم بمخاطر التهديدات الإلكترونية وتمكينهم من تبني ممارسات آمنة أثناء استخدامهم للتكنولوجيا في حياتهم اليومية، فالمعرفة وحدها لا تكفي بل يجب أن تتحول إلى سلوك عملي راسخ وهو ما يمثل جوهر التثقيف الرقمي، وتبدأ التوعية الرقمية من أبسط الممارسات مثل اختيار كلمات مرور قوية والتعرف على رسائل البريد الإلكتروني المشبوهة، ثم تتطور لتشمل فهما أعمق لمفاهيم أمن المعلومات، وحماية البيانات الشخصية والمؤسساتية، وكيفية التصرف السليم عند التعرض لمحاولات اختراق أو تسريب، وفي هذا الإطار تلعب

التنشئة التربوية سواء داخل المؤسسات التعليمية أو في بيئات العمل دورا محوريا في ترسيخ هذا الوعي.¹

ويعد الأفراد خط الدفاع الأول في مواجهة الجرائم الرقمية بما فيها الانتحال الرقمي، إذ إن أي خطأ بشري بسيط ناتج عن الجهل أو الإهمال قد يفتح المجال أمام اختراقات خطيرة حتى وإن كانت الأنظمة التقنية متطورة، فقد يؤدي النقر على رابط خبيث أو تحميل ملف مجهول المصدر إلى اختراق كامل للنظام، وهو ما يبرز أهمية تمكين الأفراد من مهارات الحماية الذاتية، ومن ثم فإن التوعية الرقمية يجب أن تكون شاملة ومستمرة وموجهة لكافة فئات المجتمع مع مراعاة اختلاف مستوياتهم المعرفية.²

وقد أصبح من الواضح أن أحد أبرز التحديات التي تواجه الأمن الرقمي هو إهمال العامل البشري، حيث يتم التركيز غالبا على الجانب التقني دون الاهتمام بسلوك المستخدم، غير أن التقنية لا تحمي نفسها بل تحتاج إلى مستخدم واع ومدرب مما يجعل الوقاية من الجرائم الرقمية وعلى رأسها الانتحال الرقمي رهينة بمدى وعي الأفراد.³

¹ - أحمد خالد الزبيدي، مدخل إلى الأمن السيبراني: المبادئ والتطبيقات، دار صفاء للنشر والتوزيع، الأردن، 2021، ص 65.

² - أحمد إسماعيل، زويبري عبد الحليم، دور التكنولوجيا الحديثة في ارتكاب الجرائم الالكترونية وسبل مكافحتها، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025/2024، ص 67.

³ - توفيق محمود محمد القزاز، الأمن السيبراني لمصادر المعلومات، مؤسسة طيبة للنشر والتوزيع، مصر، 2022، ص 87.

كما تبرز أهمية التوعية الرقمية على المستوى المؤسسي خاصة مع تعقيد البنى التكنولوجية واعتماد المؤسسات على قواعد بيانات ضخمة تتضمن معلومات حساسة، فاختراق هذه البيانات لا يقتصر أثره على الخسائر المادية بل يمتد إلى الإضرار بسمعة المؤسسة وفقدان ثقة العملاء، وقد يترتب عليه مسؤوليات قانونية، لذلك يتعين على المؤسسات إدماج برامج التوعية الرقمية ضمن سياساتها الإدارية من خلال تنظيم دورات تدريبية دورية، وإجراء محاكاة لهجمات افتراضية، وتوفير إرشادات واضحة حول كيفية التعامل مع التهديدات.¹

وفي السياق ذاته، تلعب المؤسسات التعليمية دوراً مهماً في نشر ثقافة الوعي الرقمي من خلال إدماج مفاهيم الأمن الرقمي ضمن المناهج الدراسية، واعتماد أساليب تعليمية تفاعلية تجمع بين الجانب النظري والتطبيقي، فلا تكتمل فعالية التوعية الرقمية دون الاستعانة بوسائل الإعلام والمنصات الرقمية التي تتيح نشر رسائل توعوية مبسطة عبر الفيديوهات القصيرة والمواد التفاعلية مما يضمن وصولها إلى أكبر شريحة ممكنة من المجتمع.²

وأخيراً، فإن نجاح استراتيجيات التوعية الرقمية يتطلب الاعتماد على أساليب حديثة تقوم على التفاعل والمشاركة مثل المحاكاة والتدريب العملي بدل الاكتفاء بالتلقين النظري، كما ينبغي تصميم البرامج التوعوية بما يتناسب مع خصوصية كل

¹ - أحمد إسماعيل، زوبيري عبد الحليم، دور التكنولوجيا الحديثة في ارتكاب الجرائم الالكترونية وسبل مكافحتها، مرجع سابق، ص 68.

² - دلال صالح أنديجاني، فدوى ياسين نور الدين فلمبان، ممارسات تعزيز الوعي بثقافة الأمن السيبراني في المؤسسات التعليمية، مجلة العلوم التربوية والنفسية، المجلد السادس، العدد الرابع، الخليج العربي، السعودية، 2022، ص 47.

فئة مستهدفة سواء كانوا طلبة أو موظفين أو مستخدمين عاديين لضمان تحقيق الأثر المطلوب في الحد من ظاهرة الانتحال الرقمي.¹

المطلب الثاني: دور المؤسسات والهيئات المختصة:

في ظل التحولات الرقمية المتسارعة والانفجار المعلوماتي الكبير أصبح الفضاء الرقمي مجالا خصبا لظهور الجرائم المستحدثة وعلى رأسها الانتحال الرقمي الذي يهدد أمن الأفراد والمؤسسات والدولة، الأمر الذي استدعى تدخل هيئات متخصصة للتصدي لهذه الظاهرة.

الفرع الأول: الهيئات الأمنية المختصة:

تضطلع الهيئات الأمنية بدور محوري في مكافحة الانتحال الرقمي من خلال الكشف عنه وتتبع مرتكبيه اعتمادا على الوسائل التقنية الحديثة، ويعد المركز الوطني للأدلة الرقمية (CNED) من أبرز هذه الهيئات، حيث يتولى جمع وتحليل الأدلة الرقمية المستخرجة من مختلف الوسائط الإلكترونية كالحواسيب والهواتف ووسائط التخزين وذلك بفضل كفاءات متخصصة في مجالات الإعلام الآلي والأمن المعلوماتي والجنايات الرقمية، ويساهم هذا المركز في كشف جرائم الانتحال الرقمي من خلال تتبع الآثار الرقمية وربطها بالأفعال الإجرامية،² كما تلعب فرق مكافحة الجرائم

¹ - ماريا بادة، أنجيلا إم ساس، جيسون آر سي نيرس، حملات التوعية بالأمن السيبراني: لماذا تفشل في تغيير السلوك؟ أرشيف arXiv، الولايات المتحدة الأمريكية، 2019، ص 05.

² - كريمة لعروسي، الجرائم الإلكترونية في الجزائر ودور الشرطة العلمية في مكافحتها، دار الخلدونية، الجزائر، 2021، ص 136.

المعلوماتية دورا تكميليا من خلال القيام بالتحريات التقنية والتدخل الميداني مما يعزز من فعالية الأجهزة الأمنية في مواجهة هذا النوع من الجرائم.

الفرع الثاني: الهيئات الإدارية والمؤسسات الرسمية:

إلى جانب الهيئات الأمنية، تساهم الهيئات الإدارية والمؤسسات الرسمية في الوقاية من الانتحال الرقمي والحد منه، ففي مقدمتها الهيئة الوطنية لحماية المعطيات الشخصية التي أنشئت بموجب القانون رقم 18-07¹ والتي تعمل على مراقبة مدى التزام الجهات المختلفة بحماية البيانات الشخصية ومنع استغلالها بطرق غير مشروعة، وهو ما يشكل أحد أهم مصادر جرائم الانتحال الرقمي²، كما يبرز دور مركز الاستجابة لطوارئ الحاسوب (Algeria-CERT) الذي يتولى رصد الهجمات الرقمية وتحليلها وإصدار التحذيرات الأمنية والتنسيق بين الجهات المعنية للتصدي لها إضافة إلى تقديم الدعم التقني للمؤسسات³، ومن جهة أخرى تمثل الوكالة الوطنية للأمن السيبراني الإطار الاستراتيجي الأعلى في هذا المجال، والتي تعمل على وضع وتنفيذ السياسات الوطنية للأمن السيبراني من خلال إعداد خطط لمواجهة التهديدات الرقمية، وإطلاق منصات للإبلاغ عن الحوادث، وتنظيم تدريبات ومحاكاة بالتعاون مع

¹ - انظر القانون رقم 18-07، مصدر سابق، ص 12.

² - عبد الكريم بوكاف، حماية المعطيات الشخصية في القانون الجزائري، دار الفضيحة، الجزائر، 2019، ص 84.

³ - سفيان مزياني، الأمن السيبراني في الجزائر: تحديات وآفاق، دار هومة، الجزائر، 2020، ص 112.

شركاء دوليين، وهو ما يساهم في تعزيز الحماية الرقمية وبناء بيئة آمنة تقل فيها فرص وقوع جرائم الانتحال الرقمي.¹

المطلب الثالث: التدابير التقنية لحماية الهوية الرقمية:

إن التدابير التقنية من أهم الوسائل المعتمدة لحماية الهوية الرقمية، حيث تهدف إلى تأمين الأنظمة المعلوماتية والبيانات من مختلف التهديدات الإلكترونية خاصة في ظل تزايد جرائم الانتحال الرقمي، وتتمثل هذه التدابير في مجموعة من الآليات التي تسعى إلى ضمان سرية المعلومات وسلامتها واستمرارية الوصول إليها.

الفرع الأول: تأمين الدخول إلى الأنظمة المعلوماتية:

يقصد بتأمين الدخول إلى الأنظمة المعلوماتية مجموعة الآليات والتدابير التقنية التي تهدف إلى حماية المعلومات من مختلف المخاطر التي قد تتعرض لها وعلى رأسها الكشف غير المشروع أو الاطلاع عليها من قبل أشخاص غير مرخص لهم خاصة في الحالات التي يرغب فيها مالكو المعلومات في الحفاظ على سريتها، ويعد هذا الجانب من أهم عناصر الأمن المعلوماتي إذ يتطلب تحقيق درجة عالية من الوثوقية من خلال اتخاذ التدابير اللازمة لحماية سرية المعلومات الحساسة، وضمان إمكانية الوصول إليها حصريا من قبل المستخدمين المصرح لهم دون غيرهم، كما يشمل ذلك أيضا حماية سلامة المعلومات ليس فقط من حيث منع تعديلها بل كذلك

¹ - مروان زواوي، الحوكمة الرقمية والأمن السيبراني في الجزائر، دار الكتاب الحديث، الجزائر، 2021، ص

حمايتها من أي استعمال غير مشروع قد يؤدي إلى انتهاك محتواها سواء عن طريق التعديل أو المحو أو التدمير.¹

ولا تقتصر السلامة المعلوماتية على حماية المحتوى فقط بل تمتد لتشمل ضمان استمرارية الوصول إلى المعلومات واستمرار عمل النظام المعلوماتي دون انقطاع، وذلك من خلال التصدي للهجمات الإلكترونية التي قد تهدف إلى حرمان المستخدمين من الاستفادة من هذه المعلومات، ومن جهة أخرى يقتضي تأمين الدخول كذلك ضمان عدم إنكار التصرفات الإلكترونية وهو ما يتحقق من خلال اعتماد آليات التصديق الإلكتروني التي تسمح بإثبات هوية الأطراف المتعاملة ومنع أي طرف من إنكار قيامه بعمل معين كإرسال رسالة أو تنفيذ معاملة إلكترونية، وفي حالة نشوء نزاع بين الأطراف يتم اللجوء إلى جهة موثوقة ومحايدة للفصل فيه وهو ما تجسده هيئات التصديق الإلكتروني من خلال تفعيل دور التوقيع الإلكتروني كوسيلة قانونية وتقنية لإثبات التصرفات الرقمية.²

الفرع الثاني: الحماية بواسطة الجدران النارية:

نظرا للانتشار الواسع لظاهرة قرصنة المعلومات والتجسس المعلوماتي نتيجة توفر برامج الاختراق وسهولة الحصول عليها عبر مختلف المواقع الإلكترونية، أصبح من الممكن اختراق الأجهزة والأنظمة المعلوماتية دون عناء يذكر خاصة في ظل وجود ثغرات أمنية في البرمجيات أو أنظمة التشغيل، وقد ترتب عن هذه التهديدات العديد

¹ - فتية حزام، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية "قراءة في أحكام المرسوم الرئاسي رقم 20-05"، مجلة الحقوق والعلوم الإنسانية، المجلد 13، العدد الثالث، أكتوبر 2020، ص 174.

² - دلال صادق الجواد، أمن المعلومات دار اليازوري العلمية للنشر والتوزيع، الأردن، 2008، ص 41 وما يليها.

من المخاطر من بينها الانتحال والسرقة والاحتياز من خلال التلاعب بالبيانات المدخلة أو المخرجات، إضافة إلى التجسس الصناعي عبر سرقة المعلومات الحساسة ونقلها إلى جهات منافسة عبر البريد الإلكتروني، وأمام هذه المخاطر برزت الحاجة إلى اعتماد آليات تقنية فعالة لمواجهةها من أهمها الجدران النارية والتي يقصد بها ذلك النظام أو البرنامج (وقد يكون جهازاً أو تطبيقاً) الذي يثبت على مستوى الخادم أو عند نقاط الاتصال بالشبكة، ويعمل على فرض سياسات أمنية بين الشبكة الداخلية والإنترنت.¹

الفرع الثالث: الحماية باستخدام البرامج الأمنية:

تعد الأجهزة والأنظمة المعلوماتية عرضة لمخاطر متعددة من أبرزها الفيروسات والبرمجيات الخبيثة التي تصيب الأنظمة الإلكترونية وتؤدي إلى إتلاف البيانات أو سرقتها أو تعطيل عمل النظام، ونظراً لخطورة هذه التهديدات كان من الضروري تطوير آليات تقنية فعالة للحد منها تمثلت في إنشاء برامج أمنية متخصصة في الكشف عن الفيروسات ومكافحتها، وقد تم تصميم هذه البرامج من قبل مختصين في مجال الإعلام الآلي من مهندسين ومحلي نظم ومبرمجين، حيث تعمل على كشف الفيروسات والبرمجيات الضارة قبل تفعيلها داخل النظام، ومن ثم القضاء عليها أو عزلها بما يضمن حماية الجهاز والمعلومات المخزنة فيه، غير أنه ورغم فعالية هذه

¹ - فتحة حزام، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية "قراءة في أحكام المرسوم الرئاسي رقم 05-20"، مرجع سابق، ص 174-175.

البرامج إلا أنها لا توفر حماية مطلقة إذ قد تعجز أحيانا عن اكتشاف بعض البرمجيات المتطورة أو ملفات التجسس الحديثة.¹

الفرع الرابع: استخدام تقنية التشفير الإلكتروني:

إن التشفير الإلكتروني من أهم الوسائل التقنية الحديثة لحماية الهوية الرقمية، حيث يهدف إلى تأمين البيانات والمعلومات المتداولة عبر الوسائط الإلكترونية ومنع الوصول غير المشروع إليها أو التلاعب بمحتواها، ويقصد بالتشفير تحويل البيانات من شكلها العادي المقروء إلى رموز أو إشارات غير مفهومة بحيث لا يمكن الاطلاع عليها إلا من قبل الأشخاص المصرح لهم،² وتجدر الإشارة إلى أن المشرع الجزائري لم يعرف التشفير لكنه تطرق إلى مفاتيح التشفير العمومي والخاص من خلال المادة 02 من القانون رقم 15-04 المتعلق بالتوقيع والمصادقة الإلكترونيين.³

ويتميز نظام التشفير بعدة خصائص، من أبرزها تشفير البيانات والمعلومات المتداولة عبر الوسائط الإلكترونية بما يضمن حمايتها، احترام سرية البيانات المشفرة مع الاعتراف بحق أصحابها في حماية خصوصيتهم وتجريم الاعتداء عليها، ارتباط التشفير بالتوقيع الإلكتروني حيث يستخدم لإثبات هوية الأطراف وضمان صحة المعاملات، كما يعتبر التشفير وسيلة فعالة لتعزيز الثقة في المعاملات الإلكترونية، إذ

¹ - عبد الرحمان بن عبد الله السند، الأحكام الفقهية للمعاملات الإلكترونية، 2004، ص 400.

² - فتيحة حزام، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية "قراءة في أحكام المرسوم الرئاسي رقم 20-05"، مرجع سابق، ص 175.

³ - انظر المادة 02 من القانون رقم 15-04 المؤرخ في 01 فيفري 2015، يحدد القواعد المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر العدد 06 لسنة 2015.

يضمن أن المعلومات التي يتلقاها المرسل إليه هي ذاتها التي أرسلها صاحبها دون أي تعديل أو تحريف.¹

المبحث الثاني: الآليات القانونية والقضائية:

إلى جانب التدابير الوقائية تمثل الآليات القانونية والقضائية الإطار الأساسي لمكافحة جرائم الانتحال الرقمي، حيث تتدخل القواعد القانونية لتجريم هذه الأفعال وتحديد العقوبات المقررة لها، كما تنظم الإجراءات المتعلقة بمتابعة مرتكبي هذه الجرائم والتحقيق معهم بما يضمن تحقيق العدالة وحماية حقوق الضحايا، ولا يقتصر دور هذه الآليات على الجانب الردعي فقط بل يمتد ليشمل جبر الضرر الذي يلحق بالمتضررين من خلال التعويض، لذلك يعد هذا الإطار القانوني والقضائي ضروريا لضمان مواجهة فعالة لظاهرة الانتحال الرقمي، وعليه سنتناول في هذا المبحث التجريم والعقوبات المقررة للانتحال الرقمي في **المطلب الأول**، ثم إجراءات المتابعة والتحقيق في **المطلب الثاني**، وأخيرا التعويض عن الضرر الناجم عن الانتحال الرقمي في **المطلب الثالث**.

المطلب الأول: التجريم والعقوبات المقررة للانتحال الرقمي:

شهدت الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال تطورا ملحوظا في ظل الثورة الرقمية، الأمر الذي دفع المشرع الجزائري إلى التدخل من خلال وضع إطار قانوني خاص لمواجهتها وذلك عبر جملة من النصوص التشريعية، من بينها القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

¹ - عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، لبنان، 2010، ص 236.

ومكافحتها، وكذا القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.¹

ورغم هذه الجهود، فإن جريمة الانتحال الرقمي لا تزال تطرح إشكالات على مستوى التأطير القانوني، إذ لم يتم تنظيمها بشكل صريح ومستقل وإنما يتم التعامل معها من خلال تطبيق نصوص متفرقة في قانون العقوبات وبعض القوانين الخاصة، وهو ما يعكس وجود نوع من القصور التشريعي في مواجهة هذه الجريمة المستحدثة، وفي هذا السياق يمكن إدراج الانتحال الرقمي ضمن عدة أوصاف قانونية قائمة من بينها:

- جريمة النصب.
- جريمة الدخول أو البقاء بغش في نظام معالجة آلية للمعطيات.²
- جريمة جمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة.³
- جريمة التقليد عبر الأنترنت.⁴

كما نجد أن بعض النصوص القانونية مثل المواد المتعلقة بحماية المعطيات الشخصية أو الجرائم المعلوماتية، توفر أساسا قانونيا غير مباشر لتجريم هذا الفعل إلا

¹ - فتية سويسري، انتحال الهوية الرقمية، مرجع سابق، ص 113-114.

² - انظر المادتين 387 و394 مكرر من الأمر رقم 66-156، مصدر سابق.

³ - انظر المادة 59 من القانون رقم 18-07، مصر سابق.

⁴ - انظر المادة 151 من الأمر رقم 03-05 المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر العدد 44 الصادرة بتاريخ 23 يوليو 2003.

أنها لا تغطي جميع صورته الحديثة، ومن هنا برزت الحاجة إلى تدخل تشريعي صريح يجرم الانتحال الرقمي بشكل مستقل بالنظر إلى خطورته على الأفراد والمجتمع لما ينطوي عليه من مساس بالهوية الرقمية والسمعة والخصوصية، وفي هذا الإطار يمكن اقتراح نص قانوني خاص يدرج ضمن قانون العقوبات، ينص على ما يلي: "يعاقب بالحبس من (...) إلى (...) وبغرامة من (...) إلى (...) أو بإحدى هاتين العقوبتين، كل من قام بانتحال الهوية الرقمية للغير، أو استعمل معطيات أو بيانات، مهما كانت طبيعتها، من شأنها التعريف بشخص معين، وذلك باستخدام تكنولوجيات الإعلام والاتصال لغرض غير مشروع، بما يؤدي إلى الإضرار بالغير أو المساس بسمعته أو طمأنينته".¹

المطلب الثاني: إجراءات المتابعة والتحقيق:

يعد التشريع الإطار الأساسي الذي تقوم عليه مكافحة الجرائم بمختلف صورها، حيث يكرس مبدأ الشرعية القاضي بأنه لا جريمة ولا عقوبة إلا بنص قانوني، ويعتبر قاضي التحقيق صاحب الاختصاص الأصيل في مباشرة إجراءات التحقيق، غير أن هذا المبدأ يرد عليه استثناء في مجال الجرائم المرتبطة بالإنترنت، إذ منح المشرع الجزائري صلاحيات خاصة لجهات مختصة نظرا لطبيعة هذه الجرائم وتعقدها، ورغم الجهود التشريعية المبذولة فإن النصوص القانونية وحدها لا تكفي لمواجهة الجرائم

¹ - فتية سويس، انتحال الهوية الرقمية، مرجع سابق، ص 114-115.

الإلكترونية ما لم تدعم بقواعد إجرائية ومؤسسية فعالة تضمن التطبيق العملي للقانون،
وتمكن من كشف الجرائم وضبط مرتكبيها.¹

الفرع الأول: الإجراءات التقليدية:

تتمثل الإجراءات التقليدية في الأساليب التي تطرق لها المشرع الجزائري في
ظل القانون رقم 04-09 والتمثلة في التفتيش والحجز، بالإضافة للمعاينة والمراقبة
الإلكترونية.

1. التفتيش والحجز:

يقصد بالتفتيش ذلك الإجراء القانوني الذي يهدف إلى البحث عن أدلة مادية
تفيد في كشف الحقيقة بشأن جريمة وقعت ونسبتها إلى مرتكبيها، ويتم ذلك وفق
ضوابط قانونية محددة خاصة عندما يتعلق الأمر بأماكن تتمتع بالحرمة كالمساكن،²
وفي مجال الجرائم الإلكترونية يكتسي التفتيش طابعا خاصا إذ يمتد ليشمل مكونات
النظام المعلوماتي بمختلف أنواعها سواء كانت مادية (كأجهزة الحاسوب والوسائط

¹ - خضرة شنبر، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق،
جامعة أحمد دراية أدرار، 2021/2020، ص 42.

² - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر،
2009، ص 182.

الإلكترونية) أو معنوية (كالبيانات والبرمجيات)،¹ كما قد يشمل شبكات الاتصال التي تحتوي على أدلة رقمية يمكن الاستناد إليها في الإثبات.²

كما تنقسم شروط التفتيش إلى شروط موضوعية كوقوع جريمة معلوماتية، ووجود قرائن قوية، وتحديد محل التفتيش، وشروط شكلية كصدور إذن مسبب، وإنجاز التفتيش بواسطة مختصين، واعتماد وسائل تقنية مناسبة.³

أما بالنسبة للحجز فيعد إجراء مكملًا للتفتيش والذي يهدف إلى وضع اليد على الأدلة الرقمية المستخرجة من النظام المعلوماتي،⁴ وقد نظم المشرع هذا الإجراء في القانون رقم 04-09 سالف الذكر من خلال نص المادة 06⁵ منه حيث سمح بنسخ البيانات محل البحث أو حجزها مع ضمان سلامتها ومنع الوصول إليها أو التلاعب بها.⁶

2. المعاينة والمراقبة الإلكترونية:

¹ - انظر المادة 16 من القانون رقم 04-09، مصدر سابق.

² - دلال مولاي ملياني، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، أطروحة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2018/2017، ص 215.

³ - خالد حياض الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص 154-155.

⁴ - دلال مولاي ملياني، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، مرجع سابق، ص 228.

⁵ - انظر المادة 06 من القانون رقم 04-09، مصدر سابق.

⁶ - خضرة شنبر، الآليات القانونية لمكافحة الجريمة الإلكترونية، مرجع سابق، ص 101.

المعاينة هي إجراء يقوم فيه المحقق بفحص مسرح الجريمة لجمع الأدلة وكشف الحقيقة،¹ وفي الجرائم الإلكترونية لا يقتصر مسرح الجريمة على المكان المادي بل يشمل البيئة الرقمية،² أما المراقبة فتعد وسيلة فعالة للكشف عن الجرائم قبل وقوعها أو أثناء ارتكابها،³ وتشمل تتبع الاتصالات الإلكترونية بمختلف أنواعها، إذ أنها مستمدة من اتفاقية بودابست والتي استخدمت مصطلح معطيات المحتوى.⁴

الفرع الثاني: الإجراءات الحديثة:

تتمثل الإجراءات الحديثة التي تطرق لها المشرع الجزائري في كل من اعتراض المراسلات، تسجيل الأصوات، التقاط الصور، إضافة إلى تقنية التسرب أو الاختراق.

1. اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

اعتمد المشرع الجزائري هذه الوسائل كآليات حديثة للتحري نظرا لكون الجرائم الإلكترونية (الانتحال الرقمي) ترتكب غالبا في الخفاء، مما يتطلب وسائل تقنية متطورة لكشفها بما يتماشى مع التطور التكنولوجي في مجال الاتصالات،⁵ فيقصد باعتراض المراسلات كل عملية تهدف إلى تسجيل أو نسخ أو مراقبة الاتصالات التي تتم عبر

¹ - خضرة شنبر، نفس المرجع، ص 64.

² - منير محمد الجنبهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات، دار الفكر الجامعي، الإسكندرية، مصر، 2018، ص 63.

³ - انظر المادة 02 من القانون رقم 09-04، مصدر سابق.

⁴ - دلال مولاي ملياني، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، مرجع سابق، ص 209.

⁵ - بومدين كعبيش، أساليب التحري الخاصة في جرائم الفساد، مجلة القانون، المجلد الخامس، العدد الثاني، ديسمبر 2016، ص 304.

الوسائل السلوكية أو اللاسلوكية مثل المكالمات الهاتفية،¹ وقد نظم المشرع هذا الإجراء ضمن المواد من 65 مكرر إلى 65 مكرر 10 من قانون الإجراءات الجزائية.²

أما التسجيل الصوتي فيقصد به تسجيل الأحاديث أو الأصوات في وسائط تقنية بهدف الاحتفاظ بها واستعمالها كدليل، ويشمل ذلك تسجيل المحادثات الخاصة التي قد تفيد في كشف الجريمة،³ أما بالنسبة لالتقاط الصور فهو إجراء يتم من خلال تثبيت صور أشخاص أو أماكن باستخدام وسائل تقنية دون علمهم بهدف توثيق حالة معينة مرتبطة بالجريمة.⁴

2. التسرب أو الاختراق:

يعد التسرب من أخطر وأدق أساليب التحري الحديثة، فهو تقنية تحقيق خاصة تسمح لضابط أو عون الشرطة القضائية بالتظاهر بأنه مشارك في النشاط الإجرامي بهدف كسب ثقة المشتبه فيهم وجمع الأدلة من داخل الجماعة الإجرامية،⁵ وقد عرفه

¹ - نعيم سعيدي، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013/2012، ص 177-178.

² - انظر القانون رقم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، (المعدل) بالقانون رقم 06-22 مؤرخ في 20 ديسمبر 2006، ج ر العدد 84 المؤرخة في 24 ديسمبر 2006، (المعدل والمتمم) بالقانون رقم 25-14 المؤرخ في 03 غشت 2025، يتضمن قانون الإجراءات الجزائية، ج ر العدد 54 الصادرة بتاريخ 13 غشت 2025.

³ - دلال مولاي ملياني، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، مرجع سابق، ص 183.

⁴ - أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، رسالة لنيل شهادة الماجستير، تخصص قانون عام معمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، ص 66.

⁵ - عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، 2012، ص 74-75.

المشرع الجزائري بأنه قيام ضابط أو عون شرطة قضائية، تحت إشراف مسؤول بمراقبة أشخاص مشتبه فيهم بإيهاهم أنه شريك أو فاعل معهم.¹

المطلب الثالث: التعويض عن الضرر الناجم عن الانتحال الرقمي:

يعد التعويض عن الانتحال الرقمي أحد أهم الآليات القانونية الكفيلة بجبر الأضرار التي تلحق بالأفراد نتيجة الاعتداء على حقوقهم الرقمية، ولا سيما في ظل الطبيعة غير المادية للضرر الناشئ عن هذا النوع من الانتهاكات، فمع اتساع نطاق استخدام الوسائط الإلكترونية وتزايد الاعتماد على المنصات الرقمية في مختلف مناحي الحياة لم تعد الأضرار المترتبة على الانتحال الرقمي مقتصرة على الخسائر المادية فحسب بل أصبحت تمتد لتشمل الأضرار المعنوية كالمساس بالسمعة، وانتهاك الحياة الخاصة، والتأثير النفسي الذي قد يصيب الضحية، ومن ثم يكتسي التعويض أهمية بالغة باعتباره وسيلة قانونية تهدف إلى إعادة التوازن المختل وجبر الضرر سواء من خلال التعويض المالي أو غيره من صور التعويض بما يتلاءم مع طبيعة الضرر الرقمي وخصوصياته.²

الفرع الأول: وجود أساس قانوني عام للتعويض:

يعد الضرر الركن الجوهري الذي تقوم عليه المسؤولية المدنية، بحيث لا يمكن تصور قيام الحق في التعويض بدونه مهما بلغت جسامة الفعل غير المشروع، وفي مجال الانتحال الرقمي يكتسب الضرر طابعا خاصا يميزه عن الضرر التقليدي نظرا لطبيعة البيئة الرقمية والحق المعتدى عليه، فالانتحال الرقمي يمس حقوقا شخصية

¹ - انظر المادة 65 مكرر 12 من الأمر رقم 66-155، مصدر سابق.

² - أحمد محمد حسان، نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدولة والأفراد: دراسة مقارنة، دار النهضة العربية، مصر، 2001، ص 45.

ويؤدي غالبا إلى أضرار غير مادية تتجاوز المفهوم الكلاسيكي للضرر القابل للتعويض.¹

ما يمكن ملاحظته هو أن المشرع الجزائري لم ينص صراحة على أحكام خاصة بالتعويض عن الضرر الناجم عن الانتحال الرقمي رغم تجريمه لبعض صورته في إطار القوانين الجزائية الحديثة، غير أن ذلك لا يعني حرمان الضحية من الحق في التعويض، إذ يمكن تأسيس هذا الحق على القواعد العامة للمسؤولية التقصيرية المنصوص عليها في القانون المدني لاسيما المادة 124 التي تقضي بأن كل فعل يرتكبه الشخص ويسبب ضررا للغير يلزم مرتكبه بالتعويض،² ويشمل هذا التعويض مختلف الأضرار التي قد تنجم عن الانتحال الرقمي سواء كانت مادية كتتحقيق خسارة مالية، أو معنوية كالمساس بالسمعة والاعتبار والتسبب في أضرار نفسية، خاصة وأن المشرع الجزائري اعترف بالتعويض عن الضرر المعنوي بموجب المادة 182 مكرر من القانون المدني سالف الذكر، وعليه فإن ضحية الانتحال الرقمي يمكنه اللجوء إلى القضاء للمطالبة بالتعويض متى توافرت أركان المسؤولية من خطأ وضرر وعلاقة سببية مع بقاء تقدير قيمة التعويض خاضعا للسلطة التقديرية للقاضي وفقا لظروف كل حالة.³

¹ - سلمان علي حمادي، التعويض عن الضرر الناجم عن انتهاك الخصوصية الرقمية "دراسة مقارنة بين اللائحة العامة لحماية البيانات الأوروبية لحماية البيانات والقانون المدني العراقي"، مجلة المدارات العلمية للعلوم الإنسانية والاجتماعية، المجلد الرابع، العدد الأول، مارس 2026، ص 179.

² - انظر المادة 124 من الأمر رقم 75-58 مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني الجزائري، ج ر العدد 78 لسنة 1975.

³ - انظر المادة 182 من الأمر رقم 75-58، مصدر سابق.

الفرع الثاني: معايير تقدير التعويض عن الضرر الناتج عن الانتحال الرقمي:

إن تقدير التعويض عن الضرر الناجم عن الانتحال الرقمي من أدق المسائل التي تواجه القضاء نظرا للطبيعة غير المادية لمعظم هذه الأضرار وصعوبة قياسها بمعايير حسابية دقيقة، وقد استقر الفقه على أن التعويض في هذا المجال يجب أن يكون جابرا للضرر بقدر الإمكان دون أن يؤدي إلى إثراء غير مشروع للمضرور أو إلى إفلات المسؤول من الجزاء المدني.¹

ويعتمد القضاء في تقدير التعويض على مجموعة من المعايير في مقدمتها جسامة الاعتداء وطبيعته وما إذا كان الانتحال قد وقع عمدا أو نتيجة إهمال إذ كلما كان السلوك أكثر خطورة وتعهدا، ارتفع مقدار التعويض المقرر للمضرور، كما يراعى نطاق انتشار البيانات المنتحلة ومدى صعوبة محوها أو السيطرة عليها بعد نشرها باعتبار ذلك عنصرا مؤثرا في تقدير حجم الضرر.²

ويضاف إلى ذلك معيار الآثار المترتبة على الانتحال في الحياة الشخصية والاجتماعية والمهنية للمضرور، حيث يؤخذ بعين الاعتبار ما قد يلحقه من أذى نفسي

¹ - أحمد محمد حسان، نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدولة والأفراد: دراسة مقارنة، مرجع سابق، ص 56.

² - علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي "دراسة مقارنة"، المؤسسة الحديثة للكتاب، ليبيا، 2006، ص 85.

أو اجتماعي أو مهني وهو ما يدفع إلى ضرورة منح القاضي سلطة تقديرية واسعة نظراً لتفاوت ظروف كل حالة.¹

كما يعتد بسلوك المسؤول بعد وقوع الانتحال كالمبادرة إلى إزالة المحتوى المنتحل، أو تقديم الاعتذار، أو اتخاذ تدابير تصحيحية، إذ قد يخفف ذلك من جسامة الضرر ويؤثر في مقدار التعويض، وفي المقابل فإن الاستمرار في الانتحال أو الامتناع عن معالجته يعد ظرفاً مشدداً،² وتتسجم مرونة التقدير القضائي مع التوجهات المقارنة التي تعطي وزناً لعناصر مثل نطاق التداول، وإمكانية استرجاع البيانات، ومدة بقاء الأثر الرقمي بوصفها عوامل مضاعفة للضرر.³

¹ - سلمان علي حمادي، التعويض عن الضرر الناجم عن انتهاك الخصوصية الرقمية "دراسة مقارنة بين اللائحة العامة لحماية البيانات الأوروبية لحماية البيانات والقانون المدني العراقي"، مرجع سابق، ص 182.

² - عبد الله يوسف محمود، الحق في حماية البيانات الشخصية في البيئة الرقمية، دار المسيرة للنشر والتوزيع، عمان، الأردن، 2022، ص 90.

³ - سلمان علي حمادي، التعويض عن الضرر الناجم عن انتهاك الخصوصية الرقمية "دراسة مقارنة بين اللائحة العامة لحماية البيانات الأوروبية لحماية البيانات والقانون المدني العراقي"، مرجع سابق، ص 183.

خاتمة

بعد دراستنا لموضوع انتحال الهوية الرقمية والذي يعد من أبرز التحديات التي أفرزها التطور التكنولوجي وانتشار استخدام الوسائط الرقمية، توصلنا إلى مجموعة من النتائج من أهمها:

1. أن الانتحال الرقمي يمثل اعتداء خطيرا على الهوية الشخصية والاعتبار المعنوي للأفراد لما ينطوي عليه من استخدام غير مشروع للبيانات والمعلومات الشخصية.
2. يتميز الانتحال الرقمي بتعدد صوره وأشكاله سواء عبر شبكات التواصل الاجتماعي أو البريد الإلكتروني أو غيرها من الوسائط الرقمية مما يزيد من صعوبة كشفه وإثباته.
3. وجود تقارب بين الانتحال الرقمي وبعض الجرائم المشابهة كالتروير والاحتيال المعلوماتي، غير أنه يتميز بخصوصية تتعلق بالبيئة الرقمية وطبيعة الوسائل المستعملة.
4. كرس المشرع الجزائري حماية قانونية للهوية الرقمية من خلال نصوص دستورية وتشريعية، إضافة إلى تجريم الأفعال المرتبطة بالانتحال الرقمي ضمن قوانين العقوبات والجرائم المعلوماتية.
5. تعتمد حماية الأشخاص من الانتحال الرقمي على مزيج من الآليات الوقائية، كالنوعية الرقمية والتدابير التقنية، إلى جانب الآليات القانونية والقضائية التي تضمن المتابعة والعقاب والتعويض.
6. تلعب المؤسسات والهيئات المختصة دورا محوريا في الوقاية من هذه الجرائم ومكافحتها، رغم التحديات المرتبطة بالتطور المستمر للتقنيات الحديثة.

7. يشكل الانتحال الرقمي تهديدا مباشرا للثقة في المعاملات الإلكترونية خاصة في ظل توسع الخدمات الرقمية واعتماد الأفراد والمؤسسات على الفضاء الافتراضي في تبادل المعلومات.

8. يساهم التطور التكنولوجي السريع في تسهيل ارتكاب الانتحال الرقمي من خلال أدوات متقدمة لإخفاء الهوية وتزوير البيانات وصعوبة تتبع الجناة.

9. تعاني عملية إثبات الانتحال الرقمي من إشكالات قانونية وفنية نظرا لاعتمادها على أدلة رقمية قابلة للتعديل أو الإخفاء.

10. يؤدي الانتحال الرقمي إلى آثار سلبية على الحقوق الفكرية والأدبية من خلال المساس بحقوق المؤلفين وإضعاف قيمة الإنتاج الفكري والإبداعي .

11. يتطلب التصدي للانتحال الرقمي تعزيز التعاون الدولي نظرا لطبيعته العابرة للحدود.

التوصيات والاقتراحات:

وبالرغم من الجهود المبذولة في هذا المجال، إلا أن الانتحال الرقمي لا يزال يشكل تهديدا متزايدا للأفراد والمجتمع وهو ما يدفع إلى ضرورة تعزيز الإطار القانوني والعملية لمواجهته، الأمر الذي جعلنا نقدم بعض التوصيات والاقتراحات التي نأمل أن تؤخذ بعين الاعتبار، من بينها:

- ضرورة تحديث التشريعات الوطنية بشكل مستمر لمواكبة التطورات التكنولوجية والأنماط المستحدثة للانتحال الرقمي.
- تعزيز الوعي الرقمي لدى الأفراد من خلال إدراج برامج توعوية وتكوينية حول مخاطر الانتحال وسبل الوقاية منه.

- دعم التعاون بين مختلف الجهات الأمنية والقضائية والتقنية من أجل تحسين فعالية الكشف عن هذه الجرائم ومكافحتها.
- تطوير وسائل الإثبات الإلكتروني وتبسيط إجراءات التقاضي في القضايا المرتبطة بالجرائم الرقمية.
- تشجيع استخدام وسائل الحماية التقنية، كالتشفير والمصادقة الثنائية، لضمان أمن المعطيات الشخصية.
- تفعيل دور القضاء في حماية الضحايا من خلال تسريع إجراءات الفصل في القضايا ومنح تعويضات عادلة عن الأضرار الناتجة.
- تعزيز التعاون الدولي في مجال مكافحة الجرائم المعلوماتية نظرا للطابع العابر للحدود الذي يميز الانتحال الرقمي.
- إنشاء هيئات متخصصة أو دعم الهياكل القائمة لمرافقة الضحايا وتقديم الدعم القانوني والتقني لهم.

وفي الأخير، يبقى تحقيق حماية فعالة للأشخاص من الانتحال الرقمي رهين تضافر الجهود بين المشرع، والمؤسسات، والأفراد بما يضمن بيئة رقمية آمنة قائمة على الثقة والاحترام المتبادل للحقوق والحريات.

قائمة المصادر والمراجع

1. النصوص القانونية:

1. المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج ر العدد 82 المؤرخة في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020.
2. الأمر رقم 66-156 المؤرخ في مؤرخ في 8 جوان سنة 1966، المتضمن قانون العقوبات، ج ر ع 49، الصادرة في 11 جوان 1966. (المعدل والمتمم)
3. الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، (المعدل) بالقانون رقم 06-22 مؤرخ في 20 ديسمبر 2006، ج ر العدد 84 المؤرخة في 24 ديسمبر 2006، (المعدل والمتمم) بالقانون رقم 25-14 المؤرخ في 03 غشت 2025، يتضمن قانون الإجراءات الجزائية، ج ر العدد 54 الصادرة بتاريخ 13 غشت 2025.
4. الأمر رقم 75-58 مؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني الجزائري، ج ر العدد 78 لسنة 1975.
5. الأمر رقم 03-05 المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر العدد 44 الصادرة بتاريخ 23 يوليو 2003.
6. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل لقانون العقوبات رقم 66-156، ج ر العدد 71 الصادرة بتاريخ 10 نوفمبر 2004.
7. القانون رقم 18-07 المؤرخ في 10 يونيو 2018، لمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر العدد 34

- لسنة 2018، المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 يوليو 2025، ج ر العدد 48 الصادرة بتاريخ 24 يوليو 2025.
8. القانون رقم 09-04 المؤرخ في 05 غشت 2009، القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر العدد 47 الصادرة بتاريخ 06 غشت 2009.
9. القانون رقم 15-04 المؤرخ في 01 فيفري 2015، يحدد القواعد المتعلقة بالتوقيع والتصديق الالكترونيين، ج ر العدد 06 لسنة 2015.
10. القانون رقم 20-06 المؤرخ في 28 أبريل سنة 2020، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر العدد 25 الصادرة في 29 أبريل 2020.

II. القواميس:

1. ابن فارس، معجم مقاييس اللغة، تحقيق عبد السلام هارون، دار الفكر للنشر والتوزيع، بيروت، لبنان، 1979.
2. محمد بن مكرم ابن منظور، لسان العرب، الجزء 11، المطبعة الأدبية ببولاق، مصر، 1988.
3. محمد بن يعقوب الفيروزابادي، القاموس المحيط، تحقيق مكتب التراث في مؤسسة الرسالة، الطبعة الثامنة، مؤسسة الرسالة، بيروت، لبنان، 2005.

III. الكتب:

4. أحمد خالد الزبيدي، مدخل إلى الأمن السيبراني: المبادئ والتطبيقات، دار صفاء للنشر والتوزيع، الأردن، 2021.
5. أحمد عبد السلام علي، التعليق على جرائم التزيف والتزوير في قضاء

- العقوبات في ضوء الفقه والقضاء، دار الكتب القانونية، مصر، 2007.
6. أحمد محمد حسان، نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدولة والأفراد: دراسة مقارنة، دار النهضة العربية، مصر، 2001.
7. توفيق محمود محمد القزاز، الأمن السيبراني لمصادر المعلومات، مؤسسة طيبة للنشر والتوزيع، مصر، 2022.
8. خالد حياض الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.
9. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2009.
10. دلال صادق الجواد، أمن المعلومات دار اليازوري العلمية للنشر والتوزيع، الأردن، 2008.
11. سفيان مزياني، الأمن السيبراني في الجزائر: تحديات وآفاق، دار هومة، الجزائر، 2020.
12. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني لحماية المعلومات"، دار الجامعة الجديدة، القاهرة، مصر، 2009.
13. عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، لبنان، 2010.
14. عبد الرحمان بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية، 2004.
15. عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، 2012.
16. عبد العزيز الشبل، الاعتداء الالكتروني "دراسة فقهية"، دار كنوز

- اشبيليا، الرياض، 2012.
17. عبد الفتاح بيومي الحجازي، حماية المستهلك عبر شبكة الانترنت، دار الفكر الجامعي، الإسكندرية، 2007.
18. عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية، القاهرة، مصر، 2005.
19. عبد الكريم بوكاف، حماية المعطيات الشخصية في القانون الجزائري، دار الفضيلة، الجزائر، 2019.
20. عبد الله يوسف محمود، الحق في حماية البيانات الشخصية في البيئة الرقمية، دار المسيرة للنشر والتوزيع، عمان، الأردن، 2022.
21. علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي "دراسة مقارنة"، المؤسسة الحديثة للكتاب، ليبيا، 2006.
22. عمرو موسى، الجرائم المعلوماتية "جرائم الحاسب الآلي في مصر وفي الدول العربية"، المكتب الجامعي، الإسكندرية، مصر، 2006.
23. كريمة لعروسي، الجرائم الالكترونية في الجزائر ودور الشرطة العلمية في مكافحتها، دار الخلدونية، الجزائر، 2021.
24. ماريا بادة، أنجيلا إم ساس، جيسون آر سي نيرس، حملات التوعية بالأمن السيبراني: لماذا تفشل في تغيير السلوك؟ أرشيف arXiv، الولايات المتحدة الأمريكية، 2019.
25. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، 2009.
26. مروان زواوي، الحوكمة الرقمية والأمن السيبراني في الجزائر، دار الكتاب الحديث، الجزائر، 2021.

27. منير محمد الجنيهي، صعوبات التحقيق واستخراج الأدلة في جرائم

المعلومات، دار الفكر الجامعي، الإسكندرية، مصر، 2018.

28. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات

الحلبي الحقوقية، بيروت، لبنان، 2005.

IV. الرسائل والمذكرات:

✓ رسائل الدكتوراه:

1. خضرة شنبر، الآليات القانونية لمكافحة الجريمة الالكترونية، أطروحة مقدمة

لنيل شهادة الدكتوراه، كلية الحقوق، جامعة أحمد دراية أدرار، 2021/2020.

2. دلال مولاي ملياني، إشكالية الاثبات في جرائم الانترنت في التشريع الجزائري،

أطروحة دكتوراه، تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة

أبو بكر بلقايد تلمسان، 2018/2017.

✓ مذكرات الماجستير:

1. أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري،

رسالة لنيل شهادة الماجستير، تخصص قانون عام معمق، كلية الحقوق والعلوم

السياسية، جامعة أبو بكر بلقايد تلمسان.

2. ثائر خضر أحمد بني عودة، جريمة انتحال الشخصية الالكترونية وفقا للقرار

بقانون بشأن الجرائم الالكترونية الفلسطيني "دراسة تحليلية"، مذكرة مقدمة لنيل

شهادة الماجستير في القانون، تخصص العلوم الجنائية، كلية الدراسات العليا،

الجامعة العربية الامريكية، فلسطين، 2024.

3. زيد بني خالد، التنظيم القانوني لجريمة انتحال الشخصية الالكترونية وفقا

لقانون الجرائم الالكترونية الأردني، رسالة مقدمة لنيل شهادة الماجستير، كلية

الحقوق، جامعة جرش، 2021.

4. ولاء البياري، انتحال الشخصية في الفقه الإسلامي، رسالة مقدمة لنيل شهادة الماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة فلسطين، 2018.

✓ مذكرات الماستر:

1. أمحمد إسماعيل، زوبيري عبد الحليم، دور التكنولوجيا الحديثة في ارتكاب الجرائم الالكترونية وسبل مكافحتها، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2025/2024.

2. نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2013/2012.

v. المقالات:

1. أحمد محمد محروس عبد العال، التزوير الالكتروني بين التشريع التقليدي وآليات المواجهة الحديثة، المجلة الاكاديمية للأبحاث والنشر العلمي، العدد 70، فيفري 2025.

2. بومدين كعيبش، أساليب التحري الخاصة في جرائم الفساد، مجلة القانون، المجلد الخامس، العدد الثاني، ديسمبر 2016.

3. حسام نبيل الشنراقي، التصيد الاحتيالي في ظل التطور التقني "أنماطه، تحديات المكافحة، الحلول"-دراسة تحليلية-، مجلة الدراسات القانونية والاقتصادية، المجلد العاشر، العدد الثالث، سبتمبر 2024.

4. دلال صالح أنديجاني، فدوى ياسين نور الدين فلمبان، ممارسات تعزيز الوعي

- بثقافة الأمن السيبراني في المؤسسات التعليمية، مجلة العلوم التربوية والنفسية، المجلد السادس، العدد الرابع، الخليج العربي، 2022.
5. رستم هشام، الجرائم المعلوماتية "أصول التحقيق الجنائي الفني"، مجلة الأمن والقانون، العدد الثاني، 1999.
6. سعاد أجدود، السرقة العلمية وطرق مكافحتها، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الثاني، العدد الثامن، ديسمبر 2017.
7. سلمان علي حمادي، التعويض عن الضرر الناجم عن انتهاك الخصوصية الرقمية "دراسة مقارنة بين اللائحة العامة لحماية البيانات الأوروبية لحماية البيانات والقانون المدني العراقي"، مجلة المدارات العلمية للعلوم الإنسانية والاجتماعية، المجلد الرابع، العدد الأول، مارس 2026.
8. عبد القادر بن عبد الله بن محمد آل معبر، جريمة الانتحال الالكتروني "دراسة مقارنة بين الفقه الإسلامي والنظام السعودي"، مجلة كلية الدراسات الإسلامية والعربية للبنات بدمنهور، المجلد الثاني، العدد التاسع، 2024.
9. فاطمة العرفي، حجية الدليل الرقمي في اثبات جريمة الابتزاز الالكتروني في القانون الجزائري، مجلة صوت القانون، المجلد الثامن، العدد الثاني، أكتوبر 2022.
10. فتحة حزام، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية "قراءة في أحكام المرسوم الرئاسي رقم 20-05"، مجلة الحقوق والعلوم الإنسانية، المجلد 13، العدد الثالث، أكتوبر 2020.
11. فتحة سويسي، انتحال الهوية الرقمية، المجلة الجزائرية للقانون والعدالة، المجلد 11، العدد الأول، جوان 2025.
12. محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها،

مجلة الحقيقة، المجلد 16، العدد الثالث، سبتمبر 2017.

13. هند سفر حمدان العتيبي، التقليد الصوتي الرقمي والاحتيال المالي من

منظور خبراء الأمن السيبراني، بحوث ودراسات، العدد 166، 2025.

الفهرس

الموضوع	الصفحة
شكر وتقدير	–
إهداء	–
مقدمة	02
الفصل الأول: الإطار المفاهيمي والقانوني للانتحال الرقمي	
تمهيد	10
المبحث الأول: ماهية الانتحال الرقمي	11
المطلب الأول: مفهوم الانتحال الرقمي	12
الفرع الأول: تعريف الانتحال الرقمي لغة	12
الفرع الثاني: تعريف الانتحال الرقمي اصطلاحاً	13
المطلب الثاني: خصائص وأشكال الانتحال الرقمي	15
الفرع الأول: خصائص الانتحال الرقمي	16
الفرع الثاني: أشكال الانتحال الرقمي	19
المطلب الثالث: تمييز الانتحال الرقمي عن المفاهيم المشابهة	22
الفرع الأول: تمييز الانتحال الرقمي عن التزوير الإلكتروني	22
الفرع الثاني: تمييز الانتحال الرقمي عن الابتزاز الإلكتروني	22

24	المبحث الثاني: الأساس القانوني لحماية الأشخاص من الانتحال الرقمي
24	المطلب الأول: الحماية الدستورية والتشريعية
27	المطلب الثاني: الحماية الجنائية للهوية الرقمية
27	الفرع الأول: العقوبات الأصلية
28	الفرع الثاني: العقوبات التكميلية
29	الفرع الثالث: العقوبات المقررة للشخص المعنوي
30	المطلب الثالث: موقف المشرع الجزائري من الانتحال الرقمي
الفصل الثاني: آليات حماية الأشخاص من الانتحال الرقمي	
34	تمهيد
35	المبحث الأول: الآليات الوقائية
35	المطلب الأول: دور التوعية والوقاية الرقمية
38	المطلب الثاني: دور المؤسسات والهيئات المختصة
38	الفرع الأول: الهيئات الأمنية المتخصصة
39	الثاني: الهيئات الإدارية والمؤسسات الرسمية
40	المطلب الثالث: التدابير التقنية لحماية الهوية الرقمية
40	الفرع الأول: تأمين الدخول إلى الأنظمة المعلوماتية

41	الفرع الثاني: الحماية بواسطة الجدران النارية
42	الفرع الثالث: الحماية باستخدام البرامج الأمنية
43	الفرع الرابع: استخدام تقنية التشفير الالكتروني
44	المبحث الثاني: الآليات القانونية والقضائية
44	المطلب الأول: التجريم والعقوبات المقررة للانتحال الرقمي
46	المطلب الثاني: إجراءات المتابعة والتحقيق
47	الفرع الأول: الإجراءات التقليدية
49	الفرع الثاني: الإجراءات الحديثة
51	المطلب الثالث: التعويض عن الضرر الناجم عن الانتحال الرقمي
51	الفرع الأول: وجود أساس قانوني عام للتعويض
53	الفرع الثاني: معايير تقدير التعويض عن الضرر الناتج عن الانتحال الرقمي
56	خاتمة
60	قائمة المراجع
69	الفهرس
73	الملخص

الملخص:

تتناول هذه المذكرة موضوع حماية الأشخاص من الانتحال الرقمي من خلال معالجة شاملة تجمع بين الجانب المفاهيمي والقانوني والعملي، فقد تم في الفصل الأول التطرق إلى الإطار المفاهيمي والقانوني للانتحال الرقمي، حيث تم توضيح ماهيته من خلال تعريفه وبيان خصائصه وأشكاله المختلفة، مع تمييزه عن المفاهيم المشابهة، كما تم إبراز الأساس القانوني لحماية الأشخاص منه عبر استعراض الحماية الدستورية والتشريعية، والحماية الجنائية للهوية الرقمية، إضافة إلى تحليل موقف المشرع الجزائري في تنظيم هذه الظاهرة، أما في الفصل الثاني فقد تم التركيز على آليات الحماية سواء الوقائية منها من خلال التوعية الرقمية ودور المؤسسات والتدابير التقنية، أو القانونية والقضائية عبر بيان التجريم والعقوبات، وإجراءات المتابعة والتحقيق، وكذا التعويض عن الأضرار الناجمة عن الانتحال الرقمي، وذلك بهدف الوصول إلى تصور متكامل يضمن حماية فعالة للهوية الرقمية في ظل التحديات التي تفرضها البيئة الرقمية الحديثة.

الكلمات المفتاحية: الانتحال الرقمي، الهوية الرقمية، الحماية القانونية، الجرائم المعلوماتية، التوقيع الإلكتروني، الإثبات الإلكتروني، المسؤولية القانونية.

Summary:

This memorandum addresses the issue of digital identity theft through a comprehensive treatment that combines the conceptual, legal and practical aspects. In the first chapter, the conceptual and legal framework of digital theft was addressed, where its nature was clarified through its definition and clarification of its various characteristics and forms, distinguishing it from similar concepts. The legal basis for protecting people from it was also highlighted through a review of constitutional and legislative protection, and criminal protection of digital identity. In addition to analyzing the position of the Algerian legislator in regulating this phenomenon, the second chapter focuses on protection mechanisms, whether preventive through digital awareness and the role of technical institutions and measures, or legal and judicial through a statement of criminalization and penalties, follow-up and investigation procedures, as well as compensation for damages resulting from digital plagiarism, with the aim of arriving at an integrated vision that ensures effective protection of digital identity in light of the challenges posed by the modern digital environment.

Keywords: digital plagiarism, digital identity, legal protection, cybercrime, electronic signature, electronic proof, legal liability.

