جـــامعـــة غـــردايـة

كلية الحقوق و العلوم السياسية

قـــسم حـــــقوق

الجرائم الواقعة على النقود الالكترونية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي

في مسار الحقوق تخصص: القانون الجنائي و العلوم الجنائية

اعداد الطالب:

– روابـــح رابـــح

اشراف الاستاذ:

– أ.د.شول بن شهرة

المشرف المساعد

– د.آيت عودية محمد بلخير

السنة الجامعية

1439هـ–1440/2018م–2019م

جـــامعـــة غـــردايـة

كلية الحقوق و العلوم السياسية

قـــسم حـــــقوق

الجرائم الواقعة على النقود الالكترونية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي

في مسار الحقوق تخصص: القانون الجنائي و العلوم الجنائية

اعداد الطالب:

– روابـــح رابـــح

اشراف الاستاذ:

– أ.د.شول بن شهرة

المشرف المساعد

– د.آيت عودية محمد بلخير

السنة الجامعية

1439هـ–1440/2018م–2019م


بسم الله الرحمن الرحيم

الآية الكريمة

بسم الله الرحمن الرحيم

قال الله تعالى:

(قالوا سبحانك لا علـم لنا إلا ما علمتنا أنك أنت العليم الحكيم)

الآية 32من سورة البقرة

الشكر

كلمة شكر عرفان

أولا و قبل كل شيء أشكر الله عز و جل الذي وفقني
في إتمام هذا العمل المتواضع وما كنت لأنهيه لو لا فضله علي.

كما أتقدم بالشكر الجزيل إلى **البروفيسور شول بن شهرة** على قبوله
الإشراف على مذكرتي.

كما أتقدم بالشكر و العرفان إلى **الدكتور آيت عودية محمد بلخير**
محمد على النصائح والتوجيهات القيمة.

كما اشكر **اللجنة المحترمة** على تكرمها بمناقشة هذا البحث المتواضع.

و لكل من ساهم من قريب أو من بعيد في إتمام هدا العمل.

الإهداء

اهداء

إلى التي زرعت في قلبي حب العلم

و وضعت بين جنباني القوة و العزيمة

و وضعت الجنة تحت قدميها

إلى **أمي الغالية**.

إلى الذي وهبني كل رعايته و اهتمامه

إلى الذي لا يمكن للكلمات أن توفي حقه و لا يمكن

للأرقام أن تحصي فضائله

إلى سندي و قوتي **والدي العزيز**

أدامه الله لي.

إلى **زوجتي الكريمة** وابنتي **خيرة** و ابني **أحمد**

وكل العائلة بدون استثناء.

كما اهديه **لجميع زملائي** في كلية الحقوق و العلوم السياسية.

رابح

المختصرات

قائمة المختصرات

أولا: باللغة العربية

الرقم	الاختصار	الدلالة
01	**ص**	الصفحة
02	**ص ص**	من الصفحة... إلى الصفحة....
03	**د ط**	دون طبعة
04	**ج**	الجزء
05	**ج ر ج ج**	جريدة رسمية للجمهورية الجزائرية
06	**ع**	عدد

ثانيا: باللغة الأجنبية

الرقم	الاختصار	الدلالة
01	**P.O.S**	Point of sale -نقاط البيع
02	**P**	Page – صفحة
03	**FATF**	Financial Action Task Force مجموعة العمل المالي

ملخص الدراسة

ملخص الدراسة:

لقد نتج عن ظهور التكنولوجيا و الانترنت في المجال المالي و الاقتصادي و حتى الاجتماعي ما يسمى بالنقود الالكترونية سواء على مستوى الأفراد أو الشركات أو الدول ،و مع انتشار ما يسمى بالتجارة الالكترونية و تمدد ثقافة التعاملات الالكترونية ،اصبح للنقود الالكترونية مكانة عالية لامتيازها بعدة خصائص، أهمها سهولة انجاز العمليات المالية على نطاق واسع و متنوع سواءا في التعاملات التجارية او المدنية .

وترتب عن الأهمية المتزايدة للنقود الالكترونية عدة مشاكل قانونية أخطرها الجرائم التي تهدف الى الاستيلاء عليها مثل جريمة غسيل الاموال ، وجريمة التزوير و سرقة البطاقة الائتمانية كونها اداة حاملة للنقود الالكترونية و ظهور جرائم جديدة و تقنية مثل القرصنة الالكترونية و جريمة الاحتيال الالكتروني ،مما أدى إلى ضرورة توفير حماية جنائية لها.

وعليه اتجهت الجهود المبذولة في ذلك من اجل توفير حماية للنقود الالكترونية سواء في إطار نصوص عامة أو في نصوص خاصة بتجريم هذه الجرائم او خلق اليات تساعد في الحد منها و الكشف عنها.

الكلمات المفتاحية: نقود الكترونية، نقود افتراضية، تعدين، قرصنة الكترونية، احتيال الكتروني، بطاقة ائتمانية.

Study Summary:

As a result of the emergence of technology and the Internet in the financial, economic and even social so-called electronic money both at the level of individuals or companies or countries, and with the spread of electronic commerce and expand the culture of electronic transactions, electronic money has a high position of excellence with several characteristics, Finance is widespread and diversified in both commercial and civil transactions.

The growing importance of e-money has led to several legal problems, the most serious of which are the crimes aimed at seizing them, such as the crime of money laundering, the crime of forgery and theft of the credit card as a tool that includes electronic money and the emergence of new and technical crimes such as electronic piracy and the crime of electronic fraud, To provide criminal protection.

Accordingly, the efforts exerted in this regard in order to provide protection for electronic money whether in the framework of general texts or in special texts to criminalize these crimes or to create mechanisms to help reduce and detect them.

Keywords: electronic money, virtual money, mining, electronic piracy, electronic scam, credit card.

*

مقدمـــة

المقدمة

بعد ما شهد العالم تطوراً تكنولوجياً غير مسار حياة البشر بطريقة سريعة و رائعة وبشكل عكسيٍ تماما، شمل هذا التطور كافة مناحي الحياة الاقتصادية والقانونية والاجتماعية والثقافية. و انبثق عن هذا التطور في أواخر القرن العشرين مجموعة من الظواهر المختلفة مثل الانترنت و التجارة الإلكترونية، و وسائل التعامل المالي الإلكترونية التي من أبرزها النقود الإلكترونية؛ حيث خرجت هذه الاخير عن التقليد كون من يصدرها كان الا البنوك و تولى إصدارها جهات غيره ؛ و تنوع النقود الالكترونية شكلا و نوعا و قيمة ، مما ولد طردا مجموعة من المشاكل الكثيرة رغم اهميتها في سيرورة الاقتصاد الحديث ، و من المشاكل التي جلبتها النقود الالكترونية الى الحياة الاقتصادية السلوكات الاجرامية بكل انواعها ، و التي اثرت عليها و على الاقتصاد بشكل ملحوظ ، مما اضطر المتعاملين بها دولا كانت او مؤسسات و افراد الى التعامل الجدي مع هذه الظواهر او الجرائم.

و النقود التقليدية عموما قبل اختراع النقود الالكترونية ، قد شملت عدة جرائم من اشهرها غسيل الاموال التي تعتبر من ابرز السلوكات الاجرامية التي مستها و كذلك التزوير الذي يقوم على خلق نقود مشابه للحقيقية ، كما لا ننسى السرقات التي كانت سابقا تستهدف البنوك و الافراد ، كل هذه الجرائم تعتبر من الجرائم التقليدية ، بظهور النقود الالكترونية امتدت هذه الجرائم بشكل اخر يبقى مقصدها دائما و ابدا الاستيلاء على الاموال و لكن بطرق مختلفة ، اضافة الى ظهور جرائم جديدة ظهرت مع التطور التقني الذي لحق الحياة البشرية.

ومع اختراع الكمبيوتر و تقنيات الاتصالات و ظهور النقود الالكترونية تزامن كل هذا بظهور جرائم حديثة مست كل مجالات الحياة و لم تسلم كذلك النقود الالكترونية منها ، ومن الجرائم الحديثة القرصنة و هي جريمة تقنية تعتمد على الدخول و الولوج الى الانظمة و الكمبيوترات لغرض السرقة او التجسس و غيرها ، كما ظهر ايضا ما يسمى بالاحتيال الالكتروني و الذي يعتمد على الخداع و التدليس للحصول على اموال الغير و لكن بأساليب حديثة تعتمد على التكنولوجيا كذلك ، كل هذا و ما قبله من جرائم جعل العالم بكل اطرافه يتحرك لإيجاد حلول و آليات لمكافحة هذه الظواهر الاجرامية التي مست الحياة الاقتصادية و الاجتماعية و قصد حماية الحقوق الفردية و الجماعية.

اولا–اهمية الموضوع

تكمن اهمية الموضوع في حداثة النقود الالكترونية و اهميتها في الحياة البشرية و كذا حداثة الجرائم الواقعة عليها مما قد تستهوى الباحثين لأنها لم تكن معروفة من قبل، و لأنها خطيرة فعلا لجسامة اضرارها على الاقتصاد القومي

و الذمم الفردية ،كما ان دراستها تساعد ايضا في نشر الوعي و اعتبارها الية مكافحة من اليات التي انتجت كمحاولة لصد مثل هذه الجرائم المستحدثة.

ثانيا– اسباب الدراسة:

1–الاسباب الذاتية:

ومن الاسباب الشخصية كوننا تعاملنا سابقا في النقود الالكترونية عبر مواقع الانترنت بالشراء و التجارة الالكترونية و استعمال بطاقة ماستر كارد ا لخاصة بنا و البيع فيما يخص بعض العملات الالكترونية الافتراضية لأكثر من 09 سنوات مع الدخول فيما يسمى بالتعدين في العملات الافتراضية و هذا ما دفعنا الى اقتراح الموضوع والتعمق فيه .

2–الاسباب الموضوعية :

ومن الاسباب التي دفعتنا الى دراسة حداثته قانونا و تشريعا من جهة و اهميته في الحياة من جهة اخرى ، مما دفعنا في البحث على تبيان الجرائم الماسة لهذا العنصر الهام و ماهية الاليات المتخذة ضد هذه الجرائم و مدى ملائمتها للواقع التقني الحالي .

ثالثا–اهداف البحث:

يهدف هذا البحث الى :

- التعريف بالنقود الالكترونية و تحديد انواعها و اشكالها و ما تمتاز به عن النقود التقليدية(الورقية).
- تبيان الجرائم التي تمس النقود الالكترونية واظهار اساليبها المعتمدة والتي قد تصادف المتعاملين.
- عرض الجهود الدولية و الوطنية التي نتجت كرد فعل لصد هذه الجرائم و كذلك الاليات و التقنيات المتبعة للحيلولة دون الوقوع تحت السلوكات الاجرامية التي ربما تصادف أي متعامل مما قد تساعد في تجنبه ذلك.

رابعا–الدراسات السابقة:

الدراسات السابقة فقد تناولت مواضيع الجرائم الالكترونية عموما مع بعض جوانب دراستنا و نذكر:

- دراسة معنونة بـ" الحماية الجنائية لبطاقة الائتمان " وهي اطروحة مقدمة لنيل شهادة ماجستير في العدالة الجنائية، فيصل بن عادل ابو خلف، نوقشت بجامعة نايف، كلية الدراسات العليا ، السعودية،سنة2008.
- دراسة معنونة بـ" الحماية الجنائية للبطاقة الائتمانية الممغنطة "و هي اطروحة مقدمة لنيل شهادة دكتوراه في قانون العقوبات و العلوم الجنائية، بن تركي ليلى، نوقشت بجامعة قسنطينة، كلية الحقوق ،سنة2017.

- دراسة معنونة بـ"الحماية الجنائية للتجارة الالكترونية –دراسة مقارنة–"وهي اطروحة مقدمة لنيل شهادة دكتوراه تخصص قانون خاص ،صالح شنين ، نوقشت بجامعة تلمسان، كلية الحقوق، سنة 2013.
- دراسة معنونة بـ" آليات مكافحة جرائم تكنولوجيات الاعلام و الاتصال في ضوء القانون رقم 04/09 "، و هي اطروحة مقدمة لنيل شهادة ماجستير تخصص قانون جنائي، نوقشت بجامعة ورقلة ، كلية الحقوق و العلوم السياسية، سنة2013.
- دراسة معنونة بـ " الاحتيال الالكتروني" وهي اطروحة مقدمة لنيل شهادة ماجستير تخصص قانون عام ،سامر سلمان عبد الجبوري، ، نوقشت بجامعة النهرين، كلية الحقوق، العراق،سنة2014.
- دراسة معنونة بـ" تجريم الاحتيال الالكتروني في القانون القطري والمقارن"، وهي اطروحة مقدمة رسالة ماجستير تخصص قانون عام، حمد عبدالله حيي بو غانم السليطي، كلية القانون ،جامعة قطر، قطر، سنة 2018.

تطرقت هذه الاطروحات الى الجرائم الالكترونية عموما و ايضا تناولت اليات الحماية الجنائية للبطاقات الائتمانية و هي جانب من دراستنا للموضوع كما تناولت الاحتيال الالكتروني كذلك كجريمة مست النقود الالكترونية ، غير ان هناك العديد من الدراسات و الاعمال تندرج ضمن المقالات و المناشير الالكترونية التي تناولت فعلا النقود الالكترونية من ناحية المفهوم و الانواع لكن لم تتناول فعلا مجموع الجرائم التي قد تمس هذه الاخيرة، و التي سنحاول ان نغطي النقص من خلال دراستنا لها.

خامسا–صعوبات البحث:

من الصعوبات التي واجهتنا في دراسة هذا الموضوع ، هي قلة المراجع التقنية والتي تربط بعض الجرائم بالنقود الالكترونية ، كما وجدنا صعوبة في الالمام بالمعاني الحقيقية للمصطلحات التقنية في المراجع الاجنبية التي فعلا المت بالموضوع من قرارات و قوانين و مقالات، كما ان اتسام القانون و المشرع بالجمود على خلاف ما تتصف به هذه الجرائم باللحظية فان اكبر مشكل هو ايجاد تشريعات خاصة بهذه الجرائم تبين على الاقل الوجه الاجرامي لها كون الروتين الذي تسير به القوانين و جمودها وبطء تطورها جعل وجود الية مراجع قانونية تسند البحث بشكل اكثر الا في القوانين المقارنة.

سادسا–نطاق الدراسة :

1–النطاق المكاني : تناولنا الموضوع في مجموع القوانين التي حاربت الجرائم الواقعة على النقود الإلكترونية بين بعض المشرعين و الاتفاقيات ، والتي تراوحت بين الجامعة لكل الجرائم بصيغة العموم و المخصصة لبعض الجرائم مثل ما صرح به المشرع البحريني و القطري حول الاحتيال و القرصنة و غيرها كما لا ننسى المشرع الجزائري الذي اعطى العمومية لمثل هذه الجرائم من باب استعمال الحواسيب و الانظمة و ما ينجر عنها.

2–النطاق الزماني: لا يوجد اي زمان لموضوعنا فهو ممتد منذ نشأت النقود الالكترونية و ما يقع عليها من جرائم.

3–النطاق الموضوعي: يدور موضوع بحثنا حول النقود الالكترونية و ما يمسها من جريمة بنوعيها الجرائم ذات الطبيعة المادية و المتمثلة في غسيل الاموال و سرقة و تزوير البطاقة الائتمانية ، و الجرائم ذات الطبيعة الالكترونية و التي تتمثل في القرصنة و الاحتيال الالكتروني مع محاولات المتعاملين و الاطراف الوطنية و الدولية لصد هذه الجرائم.

سابعا–اشكالية البحث:

وكون موضوع دراستنا يتناول الجرائم الواقعة على النقود الالكترونية و محاولة منا بعرض المفاهيم الموجودة حول هذه الجرائم و علاقتها بالنقود الالكترونية و كذا الحلول التي تولتها القوانين و التشريعات الوطنية و الدولية لصد هذه الجرائم و محاولة منا للإلمام بكل جوانب الموضوع طرحنا الاشكالية التالية:

الى أي مدى أوجدت القواعد القانونية القائمة حماية كافية ضد الجرائم الواقعة على النقود الالكترونية؟

بحيث يمكن استقراء بعض الإشكاليات الفرعية كالتالي:

1. ماهية النقود الالكترونية؟ و ما يميزها عن النقود التقليدية؟ وما طبيعتها القانونية؟
2. الى اي مدى يمكن اعتبار النقود الالكترونية محلا للجرائم؟
3. هل تتمتع النقود الالكترونية بذات الحماية للنقود الالكترونية؟

ثامنا–منهج الدراسة:

لما كان موضوع الدراسة حديثا ويفتقد لقواعد تشريعية التي تختص به فعليا دون احتساب تطبيق القواعد العامة، فقد انتهجنا في هذه الدراسة المنهج الوصفي من خلال وصف اولا الجرائم الواقعة على النقود الالكترونية بعرضها عرضا ممنهجا بغية الوصول إلى مواطن القصور التي تتطلب تدخل المشرع او امكانية التعاون الدولي لإيجاد

حلول جدية ، كما انتهجنا ايضا المنهج التحليلي بتحليل مجموع القوانين و الاليات المطروحة و ما يتطلبه الموضوع من آليات فنية كما استعملنا ايضا المنهج المقارن بذكر بعض القوانين المقارنة فيما يخص الموضوع.

تاسعا–خطة الدراسة:

في ضوء الاجابة على التساؤلات المطروحة سابقا التي نتجت عن اشكالية البحث و سعيا منا على تحقيق الهدف من وراء الدراسة اعتمدنا تقسيم الدراسة الى:

فكانت البداية بـ**مبحث تمهيدي** تناولنا فيه الإطار المفاهيمي لمصطلح النقود الالكترونية مجزئا الى **مطلبين الاول** تعريف هذه الأخيرة و خصائها و **الثاني** تضمن اشكالها و طبيعتها القانونية، ثم يأتي بعدها فصلين ، **الفصل الاول** تحدثنا فيها على الجرائم الوقعة على النقود الالكترونية ذات الطبيعة الالكترونية مقسم الى **مبحثين** منه غسيل الاموال كـ**مبحث اول** و سرقة و تزوير البطاقات الائتمانية كـ**مبحث ثاني** ، ليأتي **الفصل الثاني** كسابقه بـ**مبحثين** عرضنا فيه الجرائم الواقعة على النقود الالكترونية ذات الطبيعة الالكترونية ، في **المبحث الاول** كانت القرصنة من الجرائم الالكترونية الماسة للنقود الالكترونية و الاحتيال الالكتروني موضوع **المبحث الثاني**.

المبحث التمهيدي

ماهية النقود الالكترونية

المبحث التمهيدي

ماهية النقود الالكترونية

ان انتشار مصطلح النقود الإلكترونية و توسع مجال استعمالها في الكثير من الميادين خلافا عن ما شاع عن تمركز نشاطها في التجارة الالكترونية فقط و امتداده الى الحياة العادية كأداة وفاء بين المتعاملين بها ،-ادى الى قيام حاجة لوضع تعريف دقيق لها ، وتحديد أهم خصائصها التي تفردها عن غيرها (المطلب الاول) و كذلك تبيان الاشكال التي قد تتخذها ، فهل هي كالنقود العادية تكون بشكل فئات ام شيء اخر؟ مع مدى قانونيتها و قبول التشريعات لها (المطلب الثاني) .

المطلب الاول

تعريف و خصائص النقود الالكترونية

ولكي نحدد المعنى الحقيقي للنقود الإلكترونية وجب علينا تعريف النقود الالكترونية لغة و اصطلاحا حتى نعطي الاطار المعرفي حدود واضحة اضافة الى تمييزه عن النقود التقليدية بذكر خصائصه

الفرع الاول

تعريف النقود الالكترونية

فالنقود الالكترونية تنقسم الى مصطلحين نعرفهما ثم بعد ذلك نبين بعض التعاريف التي وردت بخصوص هذا المصطلح

اولا: التعريف اللغوي

1. **النقود** : من نقد ، و جمعها نقود ، و الفاعل منها ناقد و جمعه نقاد ،و جاء في لسان العرب "النقد هو خلاف النسيئة"، أي ما يدفع في حينه ولا يؤجل، والنسيئة هي تأخير الثمن [1].

يختلف تعريف النقود عند طوائف الفقهاء، فعند فقهاء اللغة للنقود عدة تعاريف، فمنها : " الإعطاء حالا وعاجلا "، ومنها " التمييز المطلق للدراهم وغيرها "، ومنها " الوازن الجيد من النقد "، والرابط بين تلك المعاني هو : الظهور والبروز كما بين ذلك أحمد بن فارس في مقاييس اللغة[2]، وأما فقهاء الشريعة فقد اهتموا بتعريف النقدين : الذهب والفضة لكونها ثمن للأشياء، فمنهم من جعل " النقود مخزن للثروة وليست غرضاً في ذاتها، بل وسيلة إلى كل غرض، تمكن الفرد من استخدام ثروته متى أراد وكيفما أراد "، ومنهم من أبرز خاصية هامة فيأن "

1 – ابن منظور، جمال الدين بن مكرم الأنصاري ، لسان العرب ،دار صادر،بيروت،2003،المجلد الثالث،ص425.

2 – ابن فارس، معجم مقاييس اللغة، تحقيق عبد السلام هارون القاهرة، مطبعة عيسى البابي الحلبي وشركاه، 1972، ج5، ص467.

الذهب والفضة مخزن للقوة الشرائية "، ومنهم من استوعب وظائف الذهب والفضة وعرفها بأنها : " قيمة لكل متمول، وهما أصل المكاسب والذخيرة والقنية "، وأخيراً : منهم من اعتبر " النقود شيئاً اعتبارياً مرده إلى العادة والاصطلاح "، وهذا ما اثبته الواقع الحالي بسيادة النقود الورقية في أيامنا هذه، وأما فقهاء الاقتصاد فقد اختلفوا كما اختلف غيرهم من الفقهاء، فمنهم من عرف النقود تعريفاً وظيفياً بأنها " تشمل جميع تلك الأشياء التي تقبل بصورة عامة على أنها وسائل للدفع، وتلاقي قبولا عاما في دفع الديون وتسديد قيم البضائع والخدمات "، ومنهم من عرفها بأنها : " أي شيء يلقى قبولاً عاماً كوسيلة للتبادل، أي وسيلة للوفاء بالديون ويعمل في نفس الوقت كمقياس للقيم وكخزانة للثروة "، ومنهم من عرفها بأنها : "كل ما هو مقبول عموماً في الدفع مقابل السلع، أو في الإبراء في جميع التزامات الأعمال "[1].

2. الإلكترونية:

"الإلكترونية من (الإلكترون): وهو دقيقة ذات شحنة كهربائية سالبة، شحنتها هي الجزء الذي لا يتجزأ من الكهربائية"[2].

ثانيا: التعريف الاصطلاحي

نظرا لأهمية **النقود الإلكترونية**[3] وكثرة استعمالها بالوقت الحاضر فقد ظهرت عدة تعريفات لها من مختلف الباحثين والفقهاء فتعددت تعريفات النقود الإلكترونية نظرا لحداثتها وتطورها السريع بحيث أصبح كل تعريف ينظر إليه من زاوية معينة وسبب هذا هو التقدم التكنولوجي في مجال الاتصالات وتطور الصناعة البنكية وظهور التجارة الإلكترونية وكل هذا أدى إلى ظهور النقود الإلكترونية بسبب صعوبة استخدام النقود العادية لإتمام المعاملات الإلكترونية إلا أن مفهوم النقود الإلكترونية أثار خلاف بين الكثير، فقسم أعطاه مفهوم واسع باعتبارها تلك النقود التي يتم تداولها عبر وسائل الكترونية دون تمييز الوسائل (شيك، بطاقة ذكية) وأعطاها القسم الآخر، مفهوم ضيق واعتبرها قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدمة و غير مرتبطة بحساب بنكي وتحظى بقبول واسع من غير من قام بإصدارها وتستعمل كأداة للدفع لتحقيق أغراض مختلفة[4]،نذكر "بعض التعريفات التي وردت في الدراسات التي تناولت موضوع النقود الإلكترونية وبعدها نشير إلى التعريف الأشمل والأقرب الذي يخدم مجال

1 – هلال درويش، اقتصاديات نقدية، تاريخ – حركة – تشريع، دار المعرفة، الطبعة الأولى، 1427-2007، ص23 وما بعدها.

2 – مجمع اللغة العربية، المعجم الوسيط، الطبعة الرابعة، مكتبة الشروق الدولية،مصر،2004، ص24.

3 -تجدر الاشارة ان ظهور النقود الالكترونية كان من قبل شركة(Digi Cash) الهولندية1994 و في نهاية 1995 بدا بنك (Mark Twain) الامريكي بإصدارها بالدولار.

4- نورا صباح عزيز الجزراوي ، أثر استعمال النقود الإلكترونية على العمليات المصرفية ، رسالة ماجستير قانون الخاص ،كلية الحقوق جامعة الشرق الأوسط للدراسات العليا، الاردن ، السنة الجامعية2010-2011، ص ص:21-22.

الدراسة ومن هذه التعريفات ما يلي:

– النقود الإلكترونية: (**أنها قيمة نقدية لعمله تصدر بشكل إلكتروني من قبل القطاع العام أو القطاع الخاص، ويتم تخزينها في جهاز إلكتروني**)[1].

– النقود الإلكترونية: (**أنها قيمة مخزنة على أداة إلكترونية بشكل مسبق بحيث تكون متاحة للمستهلك بعد ذلك**)[2].

– النقود الإلكترونية : (**أنها قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدمة وغير مرتبطة بحساب بنكي وتحظى بقبول واسع من غير من أصدرها وتستعمل كأداة للدفع ولتحقيق أغراض مختلفة**)[3].

– النقود الإلكترونية : (**أنها مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإلكترونية أن تحل فعلية محل تبادل العملات التقليدية**)[4]

وتعرف النقود الإلكترونية من الناحية القانونية (**أنها عبارة عن أرقام تتداول إلكترونية، ويمثل كل رقم قيمة مالية في حد ذاته وتستخدم هذه القيم للوفاء بأثمان السلع والمنتجات التي يبتاعها المستهلك بدلا من النقود الحقيقية وأن قوة الإبراء الموجودة في هذه النقود هي قوة إبراء اتفاقية وليست قانونية بحيث يستطيع المدين سداد ديونه بها فهي مستمدة من رضاء المستهلك لاستخدامها، وقبول التاجر لها كوسيلة وفاء**)"[5].

وقد عرفها **البنك المركزي الأوروبي**[6] بأنها مخزون الكتروني لقيمة نقدية على وسيلة نقلية يستخدم بصورة شائعة القيام بمدفوعات المتعهدين غير من أصدرها دون الحاجة إلى وجود حساب بنكي ، عند إجراء الصفقة و تستخدم كأداة محمولة مدفوعة مقدما ويعد هذا التعريف هو الأقرب للصحة نظرا لدقته وشموليته لصور النقود الإلكترونية، واستبعاده الظواهر الأخرى التي يمكن أن تتشابه معها.

و ايضا : "ان فكرة العملة الرقمية هي الفكرة البسيطة التي تقول إن تبادل القيمة لم يعد بحاجة إلى نشأته مع

---

[1]– نهى خالد عيسى الموسري وإسراء خضير مظلوم الشميري ، النظام القانوني للنقود الالكترونية، مجلة جامعة بابل للعلوم الإنسانية، المجلد22، العدد الثاني، .2014ص265.

[2] – Bank for International Settlements (BIS), (1996), Implication for central banks of the development of electronic money, Basle, P. 13.

[3]– نهى خالد عيسى الموسري وإسراء خضير مظلوم الشميري، المرجع السابق.ص267

[4]– سمية عبابسة ، وسائل الدفع الالكتروني في النظام البنكي الجزائري، مجلة العلوم الانسانية العدد6، الجزائر2016، ص348.

[5] – شريف محمد غنام، محفظة النقود الإلكترونية (رؤية مستقبلية)، دار النهضة العربية، مصر، بدون سنة نشر، ص ص:32-34

[6] –البنك المركزي الأوروبي (بالإنجليزية) (European Central Bank :المصرف المركزي الأوروبي) هو المصرف المركزي للاتحاد .وهو المسؤول عن تحديد الخطوط العريضة للسياسة النقدية في منطقة اليورو، واتخاذ القرارات اللازمة لتنفيذها. أنشأ في عام 1998 ومقره الرئيسي في فرانكفورت،ألمانيا .

تبادل السلع المادية. منذ إنشاء الإنترنت التجاري، تمكنت برامج الأرقام الرقمية التسلسلية الفريدة من التداول بأمان عبر الإنترنت لتحل محل السلع الفعلية.

تم تعريفها ايضا **بالعملة الرقمية** هي مصطلح عام للقيمة الإلكترونية الصادرة من القطاع الخاص و التي يتم تداولها عبر الإنترنت خارج البنوك التقليدية. يشار إليها أحيانًا بشكل فضفاض على أنها "أموال يتم تداولها عبر الإنترنت و لكن ليس من خلال بنك".

مع الإنترنت جاء الطلب العام للتشفير المتقدمة. أتاح توفر التشفير غير المكلف وسهل الاستخدام إجراء المعاملات المالية عبر الإنترنت من خلال شبكات صغيرة غير مملوكة ملكية خاصة. فقد مثلت المعاملات عبر الإنترنت الخاصة وغير المكلفة والآمنة تباينًا تامًا مع المشهد المالي قبل بضعة عقود فقط عندما كان هذا النوع من التشفير المتقدم والأمان متاحًا فقط للمؤسسات المالية الكبيرة و الحكومات. اليوم، وبسبب الإنترنت، تتوفر المعاملات الآمنة الخاصة بسهولة لجميع المستخدمين عبر الإنترنت. في العقد الماضي، ظهرت أنواع جديدة من العملات الرقمية الخاصة عبر الإنترنت.

توفر القدرة على توفير طريقة سهلة التنظيف على الفور لتحويل الأموال و ممارسة الأعمال التجارية على نطاق عالمي، ميزة الاعتماد الرقمي ميزة غير عادية على المنتجات المصرفية التقليدية.

بدون الرسوم واللوائح المصرفية المعتادة، يمكن لمستخدم العملة الرقمية نقل الأموال على الفور في جميع أنحاء العالم بكفاءة أكثر من الأسلاك المصرفية التقليدية.

باستخدام العملة الرقمية، أصبح من الممكن الآن لأي شخص أن يرسل الأموال على الفور خارج نطاق جميع الأنظمة المصرفية الحالية و الرقابة الحكومية"[1].

وقد عرفت ايضا: "العملات الرقمية هي وحدات إلكترونية تصدر من القطاع الخاص وتنتشر على الإنترنت. لا تقبل البنوك العملة الرقمية الخاصة كوديعة، و ليس الإنترنت مناقصة قانونية. للوحدات أسماء تجارية مثل "DigitalGrams" و "Evos" و "GoldGrams" و "e-currency" وغيرها الكثير ،قبول هذه الوسيلة الرقمية للتبادل هو 100 % ثابت وفي تزايد.

[1]-P. Carl Mullan,**The Digital Currency Challenge**, Palgrave Advances in the Economics of Innovation and Technology,2014 ,p 5.

من المرجح أن يتم تسويقها بقيمة الأصول، ومن الأمثلة على ذلك العملات الرقمية المدعومة من الذهب و الفضة و الدولار"[1].

و يمكن تعريفها ايضا " (**قيمة نقدية مخزنة على وسيلة الكترونية مدفوعة مقدما و غير مرتبطة بحساب بنكي وتحظى بقبول واسع من غير من قام بإصدارها وتستعمل كأداة للوفاء**) "[2].

و يعتبر هذا التعريف الاخير شاملا لكل خصائص المصطلح مما يغطي كل الانواع و الاشكال التي لم تتناولها بعد التعاريف التي انحصرت على نوع واحد او خاصية واحدة ، غير ان التطور في العقد الاخير اظهر شكل جديدا من النقود الالكترونية اطلق عليه مصطلح **العملات الافتراضية**[3] ادرجت على اتفاق عموم الباحثين و الهيئات و المؤسسات الاقتصادية تحت صنف النقود الالكترونية كونها تشمل غالبية خصائص النقود الالكترونية وكونها غيرت الكثير من المفاهيم و حتى بعض السياسات النقدية و القانونية لبعض الدول فوجب علينا ذكر بعض التعاريف التي تناولتها و منها :

– قيل هي:" تمثيل رقمي للقيمة، يصدر بواسطة مطورين خاصين باعتباره وحدة حساب، ويمكن الحصول عليه

---

[1]–P. Carl Mullan,**A History of Digital Currency in the United States**,New Technology in an Unregulated Market, Palgrave Advances in the Economics of Innovation and Technology,2016 ,p 6.

[2] –نهى خالد عيسى الموسري وإسراء خضير مظلوم الشميري ،المرجع السابق، ص 267..

[3]– تم طرح فكرة هذه النقود من طرف مبرمج استعمل اسم مستعار وهو **ساتوتشي ناكاموتو SatoshiNakamoto**، وقدمها في بحث نشره في عام 2008م، وعرفها بأنها نظام نقدي جديد للدفع الإلكتروني، وبأن التعامل بها وتحويلها يكون مباشرة بين مستخدمين بطريق الند للند، دون الاعتماد على طرف وسيط. وهذه العملة ترتكز على التشفير بين طرفين حيث يقدم احدهم خدمة متمثلة في فك شيفرة معينة بقوة حاسوبية ياخذ مقابلها هذا الشخص نوع معين من النقود تابعة لتلك التشفيرة لها قيمة معينة تكون بالدولار ، وتبني على نظام مجهولية المعاملات الإلكترونية حيث تقوم التحويلات على رقم محفظة لايدل على أي شيء مجرد ارقام تسلسلية لاتعرف على صاحبها، وذلك بهدف الابتعاد عن مركزية البنوك الكبرى، فهي لا تراقب من قبل البنوك بأنواعها المختلفة والهيئات ولا تخضع لقوانين البنوك حيث فتحت لها الكثير من المحافظ بدل البنوك و كثير من منصات التبادل بدل من الاسواق فيقوم المستخدمين و المالكين لها بتداولها بالدولار و غيره من الاصول النقدية الالكترونية المقبولة،غير انه في الاخير كشف رجل الأعمال الاسترالي (كريغ ستيفين رايت) عن كونه مخترع عملة بتكوين وأن قد تخفى بمسمى مستعار وهو (ساتوشي ناكاموتو)، وجاء اعتراف (رايت) لينهي سنوات من التكهنات بشأن صاحب الفكرة الأصلية للعملة الافتراضية القائمة على نظام الدفع النقدي الرقمي. وقدم عددا من الأدلة التي تثبت مزاعمه، ومنها كمية من العملات المعروفة بأنها كانت مملوكة لمخترع البتكوين، ومنها: مفاتيح التشفير التي استخدمت الإرسال 10 بتكوين إلى خبير التشفير (هال فيني) في يناير 2009م كأول معاملة بعملة بتكوين، ووقع رسائل إلكترونية خلال لقاء مع بي بي سي، مستخدما مفاتيح تشفير ابتكرت خلال الأيام الأولى من عملية تطوير عملة البتكوين، وأضاف" :كنت الجزء الرئيسي في العملية، لكن أناسا آخرين ساعدوني"، وأضاف أنه يعتزم الكشف عن معلومات تسمح لآخرين بالتأكيد من خلال استخدام أنظمة التشفير أنه هو نفسه (ناكاموتو). كما أكد أعضاء بارزون في مجموعة بتكوين وفريق التطوير الرئيس مزاعم (رايت) ، وكشف (رايت) عن هويته لثلاث مؤسسات إعلامية هي: مؤسسة بي بي سي، ومجلة الإيكونوميست البريطانية، ومجلة جي كيو.

انظر:http://www.bbc.com/arabic/scienceandtech/2016/05/160501_craig_wright_revealed_bitcoin اخر زيارة للموقع بتاريخ 01-04-2019 بتوقيت:18:03.

وتخزينه والوصول إليه والتعامل به إلكترونية، ويستخدم لمجموعة متنوعة من الأغراض عند اتفاق طرفين على استعماله"[1].

وعرفت بأنها:" تمثيل رقمي لقيمة نقدية ليست صادرة عن بنك مركزي أو عن سلطة عامة، وليست مرتبطة بالضرورة بالعملة الورقية، ولكنها مقبولة لدى أشخاص طبيعيين أو اعتباريين كوسيلة للدفع، ويمكن نقلها وتخزينها أو تداولها إلكترونية"[2].

– وعرفت بأنها: "وسيط تبادل تعمل مثل العملة في بعض البيئات، ولكنها لا تملك كل صفات العملة الحقيقية"[3].

– كما تم تعريفها بأنها: "أحد أنواع النقد الرقمي غير المنظم اللامركزي)، يصدر عن مطورين يسيطرون عليه في العادة، ويستخدم ويكون مقبولا بين أعضاء مجتمع افتراضي محدد"[4].

– قيل هي: عملة افتراضية تعمل خارج نظام النقد الرسمي، فهي تمثيل رقمي القيمة النقدية صادر عن غير البنك المركزي والمؤسسات الائتمانية، تستمد قيمتها من الثقة الكائنة في القبول الطوعي لها[5].

– عرفت بأنها: مجموعة من البروتوكولات والتوقيعات الرقمية تحل فيها الرسالة الإلكترونية بالفعل محل تبادل العملات النقدية التقليدية.

– قيل هي:" تسجيل لقيمة العملة الموثقة والمقيدة في شكل إلكتروني، وتحتوي وحدة النقود الافتراضية على رقم مرجعي، وهو رقم لا يتكرر ويميز العملة الرقمية الافتراضية، كما هو شأن الرقم المتسلسل بالنسبة لورقة النقد، وسميت نقوداً رقمية لأنها تقوم بوظائف النقود وتظهر في صورة رقمية وتتداول بشكل إلكتروني، وهي آليات للدفع مختزنة القيمة أو سابقة الدفع التي تمكن ممن إجراء مدفوعات من خلال استخدام الإنترنت، والمتعارف عليها باسم نقود الشبكة أو النقود السائلة الرقمية، وعليه يمكن القول بأن النقود الافتراضية تعبير يستخدم في الأساس لوصف

[1]– IMF Staff Team,Virtual Currencies and Beyond: Initial Considerations, International Monetary Fund, January 2016, p7.
[2]- EBA Opinion on "virtual currencies", European Banking Authority, 4 July 2014, p 11.
[3]- Fin CEN Continues to Face Challenges with Money Services Businesses, Department of the Treasury, November 10, 2015, p 3.
[4]- Virtual Currency Schemes, European Central Bank, October 2012, p:13, Virtual Currency Schemes-a further analysis, European Central Bank, February 2015, p 4.
[5]- Annual Report 2014, Deutsche Bundesbank, p 53.

مجموعة متنوعة من آليات الدفع محدودة القيمة، وأهم ما يميزها هو أن قيمتها مسددة مسبقا أو أن قيمتها مختزنة في داخلها"[1].

و بناءا على التعريفات السابقة يمكن القول بان العملة الافتراضية هي :

عملة افتراضية رقمية(ليس لها كيان مادي ملموس او وجود فيزيائي) منتجة بواسطة برامج حاسوبية ولا تخضع للسيطرة او التحكم فيها من جانب بنك مركزي أو أي إدارة رسمية دولية، يتم استخدامها عن طريق الإنترنت في عمليات الشراء والبيع أو تحويلها إلى عملات أخرى، وتلقى قبولا اختياريا لدى المتعاملين فيه[2].

ومن هنا يمكن القول ان النقود الالكترونية مهما تنوعت تبقى مقبولة بشكل واسع و هذا في تسهيلاتها التي قدمتها عوض التعاملات البنكية التقليدية مما تقتضيه التجارة الالكترونية من سرعة و امان و غيرها من السمات التي جذبتهم اليها .

الفرع الثاني

خصائص النقود الالكترونية

لقد سبق الإشارة إلى أن النقود الإلكترونية عبارة عن **قيمة نقدية مخزنة على وسيلة الكترونية مدفوعة مقدما وغير مرتبطة بحساب بنكي وتحظى بقبول واسع من غير من قام بإصدارها و تستعمل كأداة للوفاء** ومن هنا يمكن استخلاص الكثير من الخصائص. نذكر منها:

اولا:قيمة نقدية:

بالرغم من الطابع الإلكتروني لهذه الوحدات المستخدمة في الدفع إلاّ أنّها تمثل قيمة مالية وتشبه فعلا النقود العادية، مع فارق وحيد هو أنه بدل أن تكون في صورة ورقية أو معدنية، فهي في صورة لا مادية غير ملموسة يتم تداولها بشكل إلكتروني، وتبقى صالحة كأداة وفاء في المشتريات العادية البسيطة و اليومية التي يقوم بها المستهلكون عبر الإنترنت ،غير انه يجب التنويه ان قيمة كل من العملات تختلف مما هي عليه بالنسبة للعملة الافتراضية التي تتغير قيمتها حسب السوق الموازية للعملات العادية و هي سوق لتبادل العملات مع العملات الرقمية القانونية كالدولار و اليورو .

---

[1] –شايب محمد، تأثير النقود الإلكترونية على دور البنك المركزي في إدارة السياسة النقدية، الملتقى الدولي الخامس حول الاقتصاد الافتراضي وانعكاساته على الاقتصاديات الدولية، المركز الجامعي بخميس مليانة، الجزائر، (13- 14 مارس 2012م)، ص9.

[2]– عبدالله بن سليمان بن عبدالعزيز الباحوث، النقود الافتراضية مفهومها وأنواعها وآثارها الاقتصادية ، المجلة العلمية للاقتصاد والتجارة ،العدد 01 ،مصر، يناير2017م ،ص ص:21-22

ثانيا : وحدات مخزونة على وسيلة الكترونية:

النقود الالكترونية عبارة عن وحدات أو أرقام مخزنة على وسيلة الكترونية، بيد أن طريقة التخزين تختلف باختلاف التطبيق التقني، فمنها من تؤسس على بطاقة ، ومنها من تؤسس على برامج في الشبكة كالمحافظ والحسابات التي يمكن الولوج اليها عبر الشبكة . وتتسم هذه الوحدات بكونها تتألف من أرقام او رموز يمثل كل رقم او رمز قيمة نقدية معينة سلفا من قبل المصدر ..والملاحظ بهذا الخصوص ان التطورات التقنية الالكترونية سوف تتواصل وتنمو يوما بعد يوم، وهذا ما يؤثر وبفاعلية على تصميم أنظمة النقد الالكتروني في المستقبل. وهذا الأمر يحتاج بطبيعة الحال الى تطورات في الفكر القانوني تتواءم مع التقدم الهائل في وسائل التقنية الحديثة باستمرار[1].

ثالثا: الدفع بالنقود الالكترونية يتم عبر شبكة الكترونية :

إن هذه الخاصية تجعل من النقود الالكترونية ذات طابع دولي، حيث أن شبكة الأنترنت غير مقيدة أو محدودة بمكان معين ،وهي صفة لصيقة بطبيعة العملية التي وجدت خصيصا لها وهي التجارة الإلكترونية وعقودها المتسمة بالطابع الدولي عموما، وهي غير مادية، كونها مشكلة من متتاليات رقمية مشكلة من رقمي |0| و |1| ،لكن طبيعتها الدولية لا تعني أنّها أصبحت من العملات الصعبة.

ويرى الاقتصاديون أنه لكي نكيف العملة بأنها دولية، حينما يتم اعتمادها من طرف عدد كبير من الدول، وتستعمل كوسيلة وفاء في منطقة تتعدى حدود الدولة التي أصدرتها.

نستنتج إذن أن هذا التكييف يتماشى مع طبيعة النقود الالكترونية، التي تتعدى حدود استعمالها حدود الدولة المصدرة بإمكانية استعمالها عبر الشبكة العنكبوتية[2].

رابعا: قبول التعامل فيها بشكل واسع:

تحظى النقود الالكترونية بقبولها في التعامل واسع من الاشخاص والمؤسسات غير تلك التي قامت بإصدارها، فيتعين إذن الا يقتصر استعمالها على مجموعة معينة من الافراد، او لمدة محدده من الزمن، او في نطاق اقليمي محدد، فالنقود، ولكي تعد نقودا يتعين ان تحوز ثقة الافراد وتنال قبولهم باعتبارها اداة صالحة للدفع ووسيطا للتبادل، هذا من ناحية ، ومن ناحية اخرى لا يجوز اعتبار هذه الوسائل نقودا الكترونية في حالة ما اذا كان

[1]-باسم علوان العقابي و علاء عزيز الجبوري و نعيم كاظم جبر، النقود الالكترونية ودورها في الوفاء بالالتزامات التعاقدية، مجلة اهل البيت ،العدد 06، العراق 17-05-2008، ص 83.

[2]- واقد يوسف، النظام القانوني للدفع الالكتروني ، رسالة ماجستير ،كلية الحقوق جامعة مولود معمري تيزي وزو، الجزائر ،السنة الجامعية2010-2011،ص43.

مصدرها ومتلقيها هو شخص واحد. فعلى سبيل المثال، لا تعد بطاقات الاتصال التليفوني نقودا الكترونية نظرا لكون من اصدرها ومن يقبلها هو هيئة واحدة _ اي هيئة او شركة الاتصالات التليفونية- حيث لا يصلح العمل بهذه البطاقة الافي اجهزة التليفون التي خصصتها تلك الهيئة او الشركة لهذا الغرض[1].

خامسا: "يمكن أن تصدرها المؤسسات الخاصة:

على عكس النقود القانونية التقليدية التي يتم إصدارها والتحكم في كمها وشكلها من طرف البنك المركزي في كل دولة فإن النقود الإلكترونية يتم إصدارها في غالبية الدول عن طريق شركات خاصة أو مؤسسات ائتمانية خاصة ومختصة في هذا المجال، ولهذا يطلق على هذه النقود اسم النقود الخاصة"[2].

كما يمكن ان نذكر بعض الاختلافات بين من يصدر هذه العملات و بين من يمكنه ان يقدم وسائل لاستعمالها فمثلا يعتبر بريد الجزائر وما يقدمه من خدمة كخدمة البطاقة الذهبية و التي تساعد في خدمات السحب عبر السحابات الالية و عمليات الدفع من خلال الموقع لفواتير معينة عن الحساب الشخصي للعميل، كما نذكر ايضا موقع بايبال Paypal[3]المعروف الذي يقدم خدمة التوفير و عمليات التحويلات البنكية الالكترونية وامكانية ربط بطاقات الماستر كاردMastercardو الفيزا كارد Visacard و غيرها من البنوك المشهورة كل هذه تعتبر خدمات للتعامل بالنقود الالكترونية سواءا من اجل التبادل او الدفع وليست لها امكانية اصدار اي نقود الكترونية اما بخصوص النقود الالكترونية الافتراضية كعملة البيتكوين Bitcoin[4] فتعتبر المواقع

---

[1]- -نهى خالد عيسى الموسري وإسراء خضير مظلوم الشميري ، المرجع السابق ، ص ص :267-268.

[2]- محمد إبراهيم محمود الشافعي، الآثار النقدية والاقتصادية والمالية للنقود الإلكترونية، بحث مقدم في مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الامارات، 10و 12ماي 2003، ص140.

[3]- **باي بال**بالإنجليزية (PayPal) :هو موقع ويب تجاري يسمح للمستخدم بتحويل المال عبر الإنترنت والبريد الإلكتروني لعناوين مختلفة. كما يمكن للمستخدم إرسال المال المرسل إليه إلى الآخرين أو تحويله لحساب في المصرف .تعد خدمة العملة الإلكترونية بديلة عن الطرق الورقية لتقليدية كالشيكات أو الحوالات المالية .ولقد تم تأسيس الشركة من قبل ماكس ايفيتشن وبيتر ثيل وإيلون ماسك ولوك نوزيك.

للاطلاع اكثر انظر الرابط :https://ar.wikipedia.org/wiki/%D8%A8%D8%A7%D9%8A_%D8%A8%D8%A7%D9%84

اخر زيارة للموقع بتاريخ 03-04-2019 بتوقيت:17:44.

[4]- **بيتكوين** بالإنجليزية (Bitcoin) :هي عملة معماة ونظام دفع عالمي يمكن مقارنتها بالعملات الأخرى مثل الدولار أو اليورو، لكن مع عدة فوارق أساسية، من أبرزها أن هذه العملة هي عملة إلكترونية بشكل كامل تتداول عبر الإنترنت فقط من دون وجود فيزيائي لها .وهي أول عملة رقمية لامركزية – فهي نظام يعمل دون مستودع مركزي أو مدير واحد، أي أنها تختلف عن العملات التقليدية بعدم وجود هيئة تنظيمية مركزية تقف خلفها. وتتم المعاملات بشبكة الند للند بين المستخدمين مباشرة دون وسيط من خلال استخدام التشفير .يتم التحقق من هذه المعاملات عن طريق عُقد الشبكة وتسجيلها في دفتر حسابات موزع وعام يسمى سلسلة الكتل .اخترع البيتكوين شخص غير معروف أو مجموعة من الناس عرف باسم ساتوشي ناكاموتو وأُصدر كبرنامج مفتوح المصدر في عام 2009.

يمكن الاطلاع اكثر عبر الرابط:

https://ar.wikipedia.org/wiki/%D8%A8%D9%8A%D8%AA%D9%83%D9%88%D9%8A%D9%86 اخر زيارة للموقع بتاريخ 03-04-2019 بتوقيت:17:56.

التي تقوم على اصدار هذه العملات هي التي تقوم بإعطاء بدل لها بقيمة معينة وتنشا لها محافظ و اسواق تبادلات ليقوم مالكوها بالتعامل بها مع انشاء محافظ الكترونية تخص عملة البيتكوين التي تعمل عمل البنوك او صناديق ائتمان الكترونية بإمكان المتعاملين فيها بتحويل العملة منها الى الاسواق بشكل آمن و سري و تحويلها الى عملات اخرى في اسواق او مواقع تبادل موثوقة و التي تسمى **منصات التبادل**[1].

سادسا: الأمان والسرية:

من أهم ما تمتاز به النقود الالكترونية ميزة الأمان والسرية. والمقصود بالأمان أن عملية تحويل النقود الالكترونية تتم بطريق بحيث لا يمكن لأحد أن يعدل او يلغي شيئا منها. أما السرية فتعني أن الصفقة الالكترونية تتم بصورة مجهولة ولا يمكن لأي شخص الولوج الى أنظمة الدفع الالكترونية. ويرجع السبب في ذلك الى التقنية المتطورة للكروت والبرامج الحديثة التي تهيئ حوارة الكترونية سرية وأمنا بين مستعملي النقود الالكترونية . بيد أن المسألة ليست بهذه السهولة، فالتعامل الالكتروني عمومايكون محفوفا بمخاطر الأمن والاختراق الذي يمكن ان يحدث في صفقات المستهلك او التاجر من خلال تتبع مالك النقود الالكترونية أثناء إجراء الصفقة . والأمثلة على ذلك كثيرة لعل من أهمها سرقة المعلومات المالية أو النقود او تعطيل المواقع الشبكية من قبل قراصنة الانترنيت. والواقع أن مشكلة الخرق الأمني للصفقات الالكترونية تكون أوضح واشد في النقود التي تستند على برامج الحاسوب والمتصلة بشبكة الاتصالات الدولية. لان الصفقة لا تتم الا من خلال شبكة الانترنيت ووجوب تدخل طرف ثالث فيها كما سوف يجيء. ونتيجة لهذه المشكلة فقد تعددت التقنيات لمنع مثل هذه الخروقات، منها استخدام الكتابة المشفرة والمستندة على برامج. ففي البطاقة الالكترونية الفرنسية نرى مثلا أنها تحتوي على مفتاح خاص يسمح للمستهلك الذي يملكه فقط للدخول الى النظام الالكتروني لها ومن ثم إجراء الصفقة. فالمستهلك يستطيع إدخال بطاقته في قارئ البطاقات الالكترونية ويدخل الرمز الخاص به (pin)، وبدون إدخال هذا الرمز يصبح من المستحيل الولوج إلى نظام البطاقة، ومن ثم إجراء الصفقة. وعلى أية حال أن الحاجة الضرورية للحد او لمنع الأنفاق المتكرر للوحدات النقدية الالكترونية تدفع بحسب ما يرى البعض لابتكار وسائل تقنية للكشف المبكر عن الخرق او التزييف، وذلك من خلال أنشاء بيانات تتكون من أرقام متسلسلة للوحدات الالكترونية عن طريق نظام بسيط يعرف من خلاله مصدر الوحدات الالكترونية أرقام الوحدات التي قام بإصدارها ومن ثم يتحقق

[1]-**منصات تداول العملات الالكترونية** هي بيوت لتبادل العملات على الإنترنت وبعضها يستخدم حصريًا لتنفيذ معاملات النقود الالكترونية بشكل أساسي ، يمكنك استخدام الأنظمة الأساسية بالعملة الرقمية التي ترغب في استبدالها بالمبلغ المكافئ للعملة الرقمية الأخرى
للاطلاع اكثر انظر الرابط:https://tradebytrade.com/cryptocurrency-trading-platforms/ اخر زيارة للموقع بتاريخ 2019-04-03 بتوقيت:18:17.

بسهولة من أنها مستهلكة سابقا أم لا . ومع كل ما تقدم فانه ليس هناك أمن مطلق لا في العالم الالكتروني ولا في العالم الطبيعي للأعمال المصرفية، لذا يجب أن تحتوي التقنية الأمنية للوحدات الالكترونية على ما يأتي:

1. أن الدخول إلى النظام لا يتم إلا للمستهلك المخول.

2. ضرورة أن تحتوي البرامج المتضمنة في النقود الالكترونية على إمكانية التحقق من هوية وصلاحيات الأطراف بإجراء الصفقات.

3. توفير الضمان التقني بان البيانات لم تعدل لا عرضا ولا بسوء نية أثناء المرور على شبكة

4. الانترنيت. . منع الدخول الى نظام الحاسوب المركزي وقاعدة البيانات الخاصة بالمصدر.

5. الإبقاء على سرية المعلومات أثناء مرورها على شبكة الانترنيت.

6. ويجب الإشارة في هذا الخصوص الى ان السرية وان كانت مفيدة لحماية مستهلكي النقود الالكترونية بيد ان السرية الكاملة ليست مرغوبة مطلقا لأنها تساعد على تنشيط السلوك الإجرامي وإجراء الصفقات المشبوهة. فمستعملو الطرق الاحتيالية لا يستخدمون نظاما يعتقدون انه مراقب وهناك من يرصد كل حركة أو نقل للأموال بصورة مخالفة للقانون . ويتم ذلك عن طريق قاعدة البيانات المركزية للمصدر، اذ تحقق بعض أنظمة النقود الالكترونية تسجيل الصفقات المنفذة فعلا عبر الوحدات التي أصدرها، وهذا يهيئ وسائل المراقبة النشيطة للصفقات وعلى درجة عالية جدا بحيث أن أية صفقة فيها من وسائل الاحتيال او تعديل الأرصدة على البطاقة الالكترونية ستكتشف بسهولة[1].

سابعا: سهلة وسريعة التحويل:

- تحتفظ النقود الإلكترونية بقيمتها باعتبارها معلومات رقمية مستقلة عن أي حساب أخر.
- تحويل قيمة النقود الإلكترونية إلى أي شخص وذلك عن طريق تحويل المعلومات الرقمية إمكانية تحويل هذه النقود عن طريق الشبكات مثل الإنترنت أو الشبكات الاتصال اللاسلكية أخرى.
- سهولة استخدامها مقارنة مع وسائل الدفع الأخرى، لذا تشجع المستهلك على استخدامها، و يكون قبول نظامها ضمان لاستمرار حياة هذه النقود باستعمالها الدائم.
- تستخدم في أي وقت تماشيا مع طبيعة الإنترنت وما تقتضيه طبيعة التجارة الدولية لاختلاف الأوقات بين الدول[2].

[1]- باسم علوان العقابي و علاء عزيز الجبوري و نعيم كاظم جبر، المرجع السابق، ص ص: 82-83

[2]- واقد يوسف، المرجع السابق، ص41.

– العملة الرقمية قابلة للاستبدال بحرية للعملات الرقمية الأخرى[1].

ثامنا: النقود الالكترونية ليست متجانسة:

حيث أن كل مصدر يقوم بإصدار نقود إلكترونية مختلفة، فقد تختلف من ناحية القيمة فمثلا عملة البيتكوين وصلت الى حد خيالي مقابل الدولار وصلت الى 20 الف دولار لتنخفض و تبقى في تذبذب أو من حيث عدد السلع والخدمات التي يمكن يشتريها بهذه النقود، حيث تختلف من فئة إلى أخرى ومن مستهلك إلى آخر .

تاسعا: وجود مخاطر لوقوع أخطاء بشرية وتكنولوجية :

تظل هذه الوسيلة عرضة لوقوع مشاكل كثيرة خصوصا في ظل عدم وجود إطارات مدربة ولديها الخبرة الكافية تكون قادرة على إدارة المخاطر المترتبة على مثل هذه التقنيات الحديثة.

حيث أن التعامل بالنقود الالكترونية دون ظهور هوية الأطراف الحقيقية يخلق فرصة لدى مرتكبي جرائم غسيل الأموال لاستخدامها في الجريمة، حيث لن يكون مضطرا للإفصاح عن هويته وشخصيته وبما أن النقود الالكترونية لها طابع سري يجعل من الصعب جدا أن تقوم السلطات المختصة بفحص ومراقبة السجلات والعمليات المالية المصرفية وبالتالي من الصعب مراقبة جريمة غسيل الأموال.فضلا عن أن استخدام هذه النقود يتم من خلال استخدام أجهزة الكمبيوتر والأنظمة الالكترونية وقد يتم تعطيل هذه الأجهزة والانظمة بطريقة مقصودة حتى لا تترك اثرا لذلك وقد يكون العطل تلقائيا، وفي هذه الحالة يكون من الصعب جدا اكتشافها، إضافة إلى ذلك فإن النقود الالكترونية توسع من موضوع أو محل جريمة غسيل الأموال، حيث تعمل النقود الالكترونية على تأمين الأموال غير المشروعة وفي هذه الحالة لا تستطيع البنوك ممارسة رقابتها على الأسواق المالية[2].

عاشرا: غير قابلة للتلف ولا للتجديد:

فالنقود الالكترونية ليست كالنقود المعدنية او الورقية فلا يمسها التجديد في حالة تغيير شكلها او التجديد في حالة تلفها تبقى تحمل نفس قيمتها المالية التي يعطيها مصدرها .

حادي عشر: أداة وفاء

تصدر النقود الإلكترونية لغرض واحد وهو دفع وسداد قيمة المشتريات وتصدر خصيصا لهذا الغرض، بحيث لم

[1]- P. Carl Mullan, **A History of Digital Currency in the United States**,p 6.

[2]–بسام أحمد الزلمي و عبود سراج، دور النقود الالكترونية في عمليات غسيل الأموال، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، كلية الحقوق جامعة دمشق، 2010، ص 557 و558.

تكن موجودة قبل ذلك على عكس النقود العادية، وبالتالي هي مؤقتة بعملية الدفع، بحيث إذا ما تمت عملية الدفع تحولت إلى مصدرها وتصبح نقودا عادية، ولا تبقى في صورتها الرقمية وإنما يتم استردادها لحالتها العادية كنقود عادية.

بمعنى هي عملية تحويل للنقود العادية مؤقتا إلى صورة رقمية للقيام بعمليات معينة وبمجرد انتهائها تعاد العملية العكسية وترجع إلى طبيعتها، اما بخصوص العملات الافتراضية فهي كذلك تاخذ نفس المنصات بعد ان يتم تداولاها الى عملات تقبل الرجوع الى اصول مادية كالدولار و اليورو.

و هناك الكثير من الخصائص التي تتميز بها كل عملة على حدا غير ان ماتم ذكره يتسم بالاشتراك بينها سواءا افتراضية او رقمية قانونية.

المطلب الثاني

اشكال النقود الالكترونية و طبيعتها القانونية

ان صدور النقود الالكترونية لابد له ان يتخذ شكلا معينا حتى يستعملها متداولوها بشكل مقبول و قابلة للتعامل المطلوب و بهذا وجدت العديد من الاشكال التي قد تاتي بها النقود الالكترونية (الفرع الاول) ،كما ان التعامل بها اتخذ منحى قانوني في بعض الدول و منحن اخر لدى البعض الاخر(الفرع الثاني) وكل هذا ولده الخوف من هذا العنصر الجديد و من مستقبله الغامض كل هذا سنتناوله في الفروع القادمة

الفرع الاول

أشكال النقود الالكترونية

تحدثنا في السطور الماضية على أن كل النقود الالكترونية في نهاية المطاف لها بدل مادي واقعي يتمثل في عملة عادية لها قيمة مالية معينة على حسب قيمة التعامل بها ، و كما ذكرنا سابقا ان النقود نوعان من لديها بدل مباشر مدعوم ماليا مثل العملات الورقية و المعدنية وهي النقود الالكترونية القانونية كالدولار و اليورو والدينار الجزائري و غيرها ... و بين العملات الافتراضية و التي تفصل بينها وبين القيمة القانونية البدل الالكتروني أو الأصول الالكترونية المعترف به ماليا(الدولار و اليورو....) غير ان الاختلاف يكمن في القبول لدى بعض الدول و الرفض لدى بعضها الآخر الذي ولده الخوف من التغير الدائم في قيمتها، و لنصل إلى الفهم الصحيح حول مصطلح النقود الالكترونية و لنأخذ صورة أوضح له وجب علينا ان نوضح الهيئة التي يمكن ان تتشكل فيها أو بها

هذه النقود اي أين يمكن أن توجد او بماذا يمكن ان تستعمل هل كالعملات التقليدية(الورقية و المعدنية) او بشكل آخر بها نأتي بشرحها في هذا الفرع حسب العناصر الآتية:

1. المحفظة الالكترونية المادية:

"قد تكون المحفظة الإلكترونية عبارة عن **بطاقة بلاستيكية ممغنطة** (مزودة بشريحة – رقاقة – حوسبية (Chip)، يمكن تثبيتها على الكمبيوتر الشخصي أو تكون **قرصا مرنا** يمكن إدخاله في فتحة القرص المرن في الكمبيوتر الشخصي ليتم نقل القيمة المالية (منه أو إليه) عبر الإنترنت ؛ ويمكن استخدام المحفظة الإلكترونية للدفع عبر الإنترنت وفي الأسواق التقليدية التي تستعمل أنظمة الدفع الإلكتروني"[1].

كما سبق فان المحافظ الالكترونية تختلف بين البطاقات و الأقراص و قد تتعدى ذلك إلى برمجيات ولكن حديثنا هنا يكون على المادية منها و الأكثر استعمالا ألا و هي البطاقات البلاستيكية، و قد أوضحت بعض البحوث ماهيتها بـ:

"البطاقات البلاستيكية الممغنطة: وهي البطاقات البلاستيكية والمغناطيسية التي تصدرها البنوك لعملائها للتعامل بها بدلا من حمل النقود، واشهرها الفيزا(**Visa**) ،والماستر كارت (**Master Card**)،وامريكان اكسبرس (**American Express**)وتكون هذه البطاقات مدفوعة القيمة المالية سلفا ومخزنة فيها ، ويمكن استخدام هذه البطاقات للدفع عبر الانترنت وغيرها من الشبكات ، كما يمكن استخدامها للدفع في نقاط البيع التقليدية Point of sale -P.O.S ، حيث يقوم المستخدم سلفا بدفع مقدار من النقود التي يتم تمثيلها بصيغة الكترونية رقمية على البطاقة الذكية وعندما يقوم المستخدم بعملية شراء سواء أكان ذلك عبر الانترنت ام في متجر تقليدي يتم خصم قيمة المشتريات وهنالك العديد من منتجات النقود الالكترونية التي يمكن اعادة تحميلها بقيمة مالية عن طريق ايداع نقود في البنك او عن طريق اي حركة مالية اخرى ملائمة"[2] .

كما يجدر بالذكر ان البطاقات تتنوع من حيث الغرض من حيث حجم الذاكرة و من حيث القيمة و الامتيازات التي تقدمها المؤسسات المصدرة لها فمنها الماسية و الذهبية و الفضية و الذكية (من حيث الحجم) و الائتمانية و غير الائتمانية و الكثير الكثير من البطاقات الممغنطة البلاستيكية و للتنويه ان اغلب البطاقات تترافق

[1]– بختي ابراهيم ، دور الانترنت و تطبيقاته في مجال التسويق –دراسة حالة الجزائر–، دكتوراه دولة ، قسم العلوم الاقتصادية كلية العلوم الاقتصادية و علوم التسيير جامعة الجزائر، الجزائر،2002، ص116.

[2]– نهى خالد عيسى الموسري وإسراء خضير مظلوم الشميري، المرجع السابق، ص270.

مع مفتاح سري Pin أثناء الاستعمال أمام الصرافات الالية للسحب او للتخليص في بعض المحلات او المعاملات التجارية عبر الانترنت وكذلك بطاقة الصادر عن بريد الجزائر المسماة ب"**الذهبية**"[1] اثناء تخليص فاتورة معينة عبر موقع البريد فانها تطلب إدخال مجموعة الأرقام التعريفية الموجودة على ظهرها اضافة الى الرقم السري للتاكيد.

2. البرمجيات و الحسابات الالكترونية:

ان اغلب النقود الالكترونية تكون مخزنة كما ذكرنا سابقا بصيغة الكترونية رقمية غير ان الاساس الاكيد في هذا التخزين يكون من خلال محفظة الكترونية رقمية أي حساب الكتروني يعتبر كخزنة رقمية ان صح التعبير اما تكون مرتبطة ببطاقة و مفتاح سري كما شرحناه في البطاقات البلاستيكية من خلاله يمكنك التحويل عن طريق ادخال عنوان المرسل اما "انظمة برمجية تتيح مكافئا الكترونيا لا يحتاج الى بطاقة بلاستيكية فهي انظمة تعتمد بالكامل على برمجيات مخصصة لدفع النقود عبر الانترنت.

ولكي يكون نظام النقود الالكترونية المعتمد بالكامل على البرمجيات فعالا وناجعا لابد من وجود ثلاثة أطراف فيه هي الزبون او العميل و المتجر البائع والبنك الذي يعمل الكترونيا عبر الانترنت ، (Online Bank)والى جانب ذلك، لا بد من ان يتوافر لدى كل طرف من هذه الاطراف برنامج النقود الالكترونية نفسه، ومنفذ الى الانترنت، كما يجب ان يكون لدى كل من المتجر والعميل حساب بنكي لدى البنك الالكتروني الذي يعمل عبر الانترنت، وبالفعل فقد اصبح من الممكن عن طريق استخدام برمجيات معينة من اشهرها برنامج (E.Cash) استخدام النقود الالكترونية لإتمام عمليات الشراء والدفع عبر الانترنت، كما ان هذه البرمجيات تتيح ارسال النقود الالكترونية على شكل مرفق (attachment) في رسالة بريد الكتروني"[2]و رقما سريا يكفي كبعض المحافظ مثل بايبال و الذي يقوم على إرسال الأموال بادخال ايميل المرسل اليه كون الايميل هو عنوان

1- **البطاقة الذهبية** بالفرنسية (Carte Edahabia) : أطلقت مؤسسة بريد الجزائر قبل ايام بطاقة ذكية مغناطيسية جديدة و هي بطاقة ائتمان تسمح بالعديد من الخدمات الإضافية هن البطاقة التقليدية القديمة، و هذه البطاقة ستكون هي الأكثر شعبية بين الجزائريين و ستعطي خدمة الدفع الإلكتروني.

تتيح هذه البطاقة التي تعمل بنظام (EMV) لحامليها، زيادة على إجراء مختلف عمليات سحب ودفع الأموال على حساباتهم البريدية عبر الأنترنت، تسديد الفواتير الاستهلاكية الخاصة بالكهرباء والغاز والماء، الهاتف الثابت، الانترنت و انطلاق ايضا دفع البنزين في محطات شركة نفطال .

للاطلاع اكثر يمكن زيارة : https://ar.wikipedia.org/wiki/البطاقة_الذهبية_للدفع_الالكتروني_لبريد_الجزائر. اخر زيارة للموقع بتاريخ 04-04-2019 بتوقيت:18:28.

2- نهى خالد عيسى الموسري وإسراء خضير مظلوم الشميري، المرجع السابق،ص271.

الحساب ثم ادخال القيمة التي تريد ارسالها ثم يطلب منك رقم السري لتاكد التحويل كما يمكنك ربط حساب البايبال بالبطاقات لغرض استعمال بشكل متزامن ، ايضا في خاصية التخليص لدى بريد الجزائر لولا تلك البرمجيات لا يمكن للعميل ان يقوم بتخليص الفواتير دون الاعتماد على المؤسسات التي أوكلت لها صلاحية استقبال الفواتير مثل مراكز بريد الجزائر و بهذا ان اغلب عمليات التجارة الالكترونية في الآونة الأخيرة أعطت مجال واسع للعمل دون الاعتماد على المؤسسات المالية المعتمدة و تنتهي مهامها بإصدار البطاقات أو إنشاء الحسابات الالكترونية الحافظة للعملات الالكترونية.

ايضا تجدر الاشارة الى ان هناك ايضا أشكال اخرى اقل استعمالا و ظهور مثل :

3. "**الشيكات الإلكترونية** : تحرر الشيكات الالكترونية باستخدام التقنية الرقمية وتأخذ نفس المسارات التي يأخذها الشيك التقليدي الورقي منذ لحظة إصداره مرورا بعملية التسليم ثم التحصيل و القيد في الحساب يتم إرسال الشيك الإلكتروني بالانترنيت من المشتري بعد توقيعه الكترونيا إلى البنك ، هذا الأخير يقبله ويظهره ثم يرده إلكترونيا إلى بنك البائع للتحصيل الإلكتروني من بنك المشتري، وهذه الوسيلة تستخدم على نطاق واسع في الاقتصاديات المتقدمة ، كما يشهد استخدامها نموا في الاقتصاديات النامية، خاصة في مجال تسوية المعاملات كبيرة القيمة نسبيا "[1].

و الملاحظ على العمومي ان تنقل العملات الالكترونية اما يكون مادية متمثل في البطاقة و الاقراص و اما رقميا الحسابات و المحافظة الرقمية و الشيكات الالكترونية اثناء التعامل او السحب

و يكون السحب كمعلومة اضافية اما عن طريق البنوك المعتمدة و المصدرة لهذه النقود او البطاقات الحاملة للنقود او عن طريق الصرافات الآلية للنقود (ATM)[2] المتواجدة عبر نقاط معينة كما هي متواجد بالنسبة لبريد الجزائر او البنوك الوطنية كالبنك الوطني الجزائري BNA او بنك التنمية المحليةBDL ، نجدها خارج المراكز او في المطارات لبعض المؤسسات المالية العالمية.

[1] –شول بن شهرة، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه تخصص، كلية الحقوق و العلوم السياسية، جامعة بسكرة، الجزائر، السنة الجامعية2009-2010،ص ص:40-41.

[2] – **الصراف الآلي بالانجليزية** (automated teller machine) (ATM) هو جهاز الكتروني يوفر لعملاء المؤسسات المالية إجراء المعاملات المالية في الأماكن العامة كبديل عن الحاجة إلى موظف. للقيام بآي عملية، يجب على العميل إدخال بطاقة بلاستيكية مرمزة تحتوي على رقم خاص بالعميل وبعض المعلومات الأمنية. ومن العمليات المالية التي يسمح بالقيام بها من خلال الصراف الآلي الوصول إلى الحسابات المصرفية وسحب النقود ومعرفة أرصدة الحسابات، وإيداع النقود أيضا.للاطلاع اكثر يمكن زيارة :https://ar.wikipedia.org/wiki/صراف_آلي اخر زيارة للموقع بتاريخ 04-04-2019 بتوقيت:18:39.

الفرع الثاني

الطبيعة القانونية للنقود الالكترونية بين الفقه و القانون

فقد كثر الحديث عن النقود الالكترونية بشكل مختلف في الآراء بين الباحثين و المتعاملين منجهة و من جهة اخرى بين القوانين محاولين وضع هذه الظاهرة الجديدة في اطار قانوني يليق بها نفصلها في الاتي:

اولا: في الفقه

تضاربت الكثير من الآراء حول تحديد الطبيعة القانونية للنقود الالكترونية بين من يؤيدها كأداة وفاء و لها بديل مادي يقبلها المتعاملون و يعطيها صفة النقود الحقيقية مادامت تقوم بكل وظائف النقود التقليدية، و هناك من لا يقبلها ولا يعتبرها من قبيل النقود إطلاقا ولا تعد أداة نقدية بالمعنى الحقيقي كونها لا تخضع لرقابة البنك المركزي.

وهناك من يأخذ الراي الوسط بين الرأيين السابقين . لذا سنتطرق إلى هذه الآراء في النقاط الاتية:

1. النقود الالكترونية صيغة غير مادية للنقود الورقية

يركز أصحاب هذا الرأي على الفرق بين النقود الورقية والنقود الالكترونية، حيث أن هذه الأخيرة تأخذ شكل غير مادي أي من طبيعة معلوماتية وبالتالي فهي صيغة غير مادية للنقد الورقي حيث يتم تحويل شكل النقود الورقية إلى نقود الكترونية، أي أصبحت عبارة عن معلومات تخص النقود تنتقل من شخص لآخر لذا تعتبر هذه المعلومات أهم من النقد نفسه وهذا يعد فرقا جوهريا[1].

من الضروري الإصرار على الظاهرة التالية: إن العملة غير المادية في شكل "مؤسسة" مكلفة بخدمة عامة ، خاضعة لسيطرة سياسية مناسبة ، لن تشكل أي مشكلة. بعبارة أخرى ، ليس شكل العملة ، ماديًا أو غير مادي ، هو الذي يطرح المشكلات ، بل هو جوهر تعريفها ، الذي يصرح أو لا يسيطر عليها من قبل المصالح الخاصة[2].

[1]– باطلي غنية،خصائص وأشكال النقود الإلكترونية: دراسة تحليلية نظرية ،مجلة العلوم السياسية والقانون ،العدد07، ، ألمانيا2018 ،ص360 .

[2]-valérie bugault , nature juridique et fonction politique des monnaies et cryptomonnaies, étude et analyse juridique du concept monétaire et de son évolution. monnaie et cryptomonnaie : une même nature juridique contradictoire : à la fois « unité de mesure » et « réserve de valeur », Octobre 2018,
اخر زيارة للموقع بتاريخ 05-04-2019 بتوقيت 19:09: https://lesakerfrancophone.fr/nature-juridique-et-fonction-politique-des-monnaies-et-cryptomonnaies

ورأي أخر يقول أيضا :ينبغي تناول مسألة ما إذا كانت النقود الإلكترونية مالًا مناسبًا من منظور تطوري ، حيث يحدد الأشخاص بمرور الوقت "نقود" أي سلعة او أدوات مالية معينة .قد تصبح النقود الإلكترونية في وقت ما نقودًا في نظر الناس، ويجب تصميم اللوائح مع وضع هذا الاحتمال في الاعتبار.

من شأن الإطار التنظيمي الموضح أعلاه أن يوفر للعملاء خيارًا أوسع نطاقًا لأدوات النقود الإلكترونية مما هو متاح حاليًا (من أولئك الذين يمنحون حماية كاملة من مخاطر السيولة والمخاطر الائتمانية لمن يمنحون إمكانية الوصول إلى تسهيلات الإقراض) ، وسيسمح للنقود الإلكترونية بأن تصبح ليس فقط اداة تبادلات ولكن يحتمل أن يكون أداة ادخار كذلك) مع ما ينطوي عليه ذلك من آثار ضمنية محتملة[1].

أخيرًا، مثل هذا الإطار من شأنه أن يحفز البنوك وغير البنوك على استغلال ميزتها النسبية، مع احتمال منافسة غير البنوك على شريحة من النقود الإلكترونية المحمية بالكامل والبنوك قادرة على تكرار قدرتها على إنشاء الأموال الإلكترونية. المال عن طريق الإقراض والعملية التي يتم بها الإصدار تكون بإجراء تحويل في شكل النقود من النقود الورقية إلى النقود الالكترونية، لذا فإن النقود الالكترونية تحل محل النقود العادية ويكون لدى المصدر سواء كان بنك أو مؤسسة مالية مساواة في النقود التي تدخل وهي النقود التقليدية والتي سوف تستعمل في شحن البطاقة بالنقود الالكترونية، وتمك التي تخرج هي النقود الالكترونية.

ولقد تعرض أصحاب هذا الرأي إلى النقد على أساس أن هذه النظرية تثير الكثير من المشاكل الواقعية، حيث أن النقود التقليدية التي تستعمل لشحن البطاقات بالنقود الالكترونية تبقى دائما داخل النظام النقدي. وتضاف إليها أصول مصدر تلك النقود الالكترونية وبالتالي سيكون هناك ازدواج في الكتلة النقدية لان النقود الموجودة في البطاقة هي نفسها الموجودة في حساب المصدر، ومن ثم يمكن لكل من صاحب النقود ومصدرها استعمال كل من النقود الالكترونية والنقود التقليدية بشكل متزامن ومستقل.

2. النقود الالكترونية أداة تبادل وليست أداة دفع

يعتبر هذا الرأي إصدار النقود الالكترونية نوعا من بيع أصول المصدر .فهذه النقود تشترى من المصدر مقابل مبلغ معادل من النقود التقليدية، أو بتعبير آخر يتم شراء إصدارات النقود الالكترونية بما يعادلها من نقود المصارف المركزية .فنحن هنا بصدد نقود تشتريها نقود أخرى .وكذلك فإنه في نهاية دورة حياة النقود الالكترونية يقوم

[1]-**BiagioBossone ,**Electronic money versus money: An assessment of regulation**,** Conclusion**,** 25 January 2017 https://voxeu.org/article/electronic-money-enhancement-or-replacementاخر زيارة للموقع بتاريخ 05-04-2019 بتوقيت 19:42:.

المصدر الذي يستردها بالتصرف كمشتر لها من البائعين الذين تلقوها نظير مبيعاتهم .وطبقا للمنطق السالف فإن مؤسسات الإصدار ملزمة بالاحتفاظ "بالنقود التقليدية "التي تلقتها في مقابل "بيع "النقود الالكترونية مما يشكل تقييدا لقدرة تلك المؤسسات على إصدار النقود الالكترونية[1].

3. :النقود الالكترونية أداة ائتمان:

يرى بيتر إيلي B.ley[2] أن النقود الالكترونية التي هي الرصيد النقدي المسجل الكترونيا على بطاقة مخزنة القيمة –تعتبر ائتمانا، لأن هذا الرصيد يعد نوعا من الديون بالنسبة لمصدرها .و يتمثل الالتزام القانوني لمصدر البطاقة اتجاه حاملها في الوحدات النقدية و الرقمية الالكترونية (electronic bits) المسجلة على البطاقة، و هو ما يتشابه به مع حقيقة أن الالتزام القانوني للحكومة في مواجهة حامل العملة يتمثل في قطعة العملة ذاتها[3].

4. النقود الالكترونية صورة افتراضية لتدفق ثلاثي الاقطاب:

يتطلب وجود هذه النقود والتعامل بها ثلاث أطراف وهم المصدر، المستهلك، والتاجر (المستفيد)، ويعتبر اصحاب هذا الرأي أن الأموال أو النقود التي يتلقاها مصدر النقود الالكترونية ماهي إلا وديعة بنكية لدي شخص ثالث، إذ أن إصدار و إيداع النقود الالكترونية لدى مصدرها لا يشكلان عملية واحدة بل عمليتين مستقلتين، فصاحب الحساب يقرض النقود لمصدر النقود الالكترونية وبالتالي يعتبر المصدر لدينا لصاحب الحساب، وعندما يتم إصدار النقود الالكترونية لا تعطى على سبيل الحيازة وانما على سبيل القرض. وعلى هذا الأساس لا تعتبر النقود الالكترونية من أصل مالي وانما صورة افتراضية للدورة الكاملة التي تشكل إيداع النقود التقليدية عن إصدار نقود الكترونية ثم تدميرها أو تحطيميا أو بمصطلح أسلم محوها عند إجراء كل عملية من عمليات الدفع النقدي[4].

ثانيا: في القانون

ان النقود الالكترونية حسب التعاريف التي ذكرناها في المواضيع السابقة تختلف دعامتها بين القبول و من يصدرها و يدعمها لهذا فان مبدا التخوف من الخسارة و التأثير السلبي على الاقتصاد عموما بداية من التجارة والتي تتمحور على المبادلات باستعمال اغلبيتها على التبادل الالكتروني للأموال بهذا فقد عملت القوانين على

[1]–لوصيف عمار، استراتيجيات نظام المدفوعات للقرن الحادي والعشرين ،رسالة ماجستير في العلوم الاقتصادية،كلية العلوم الاقتصادية وعلوم التسيير جامعة منتوري قسنطينة،الجزائر،2009،ص:52

[2]–بيتر إيلي B.ely : رئيس شركة الاستشمارات المصرفية و شركة Ely في الإسكندرية.

[3]– لوصيف عمار ،المرجع السابق، ص ص 52-53.

[4]– باطلي غنية، المرجع السابق ،ص 361.

حماية كل المبادلات او عمليات التي تدور سواءا بتدخل الدولة او بدونها ، فمنها من فتح المجال لمثل هذه التعاملات بشكل العادي كونه هو مصدر لتلك النقود الالكترونية او قام بتنظيمها عن طريق قوانين و لوائح تحدد كيفية التعامل بها ومنها من منع ذلك خوفا من مستقبلها الغامض ، و كما سبق الذكر فان النقود الالكترونية تنقسم من حيث البدل المادي الى ماهو موجود مباشرة كالدولار كقيمة الكترونية و قيمة مادية و بين النوع الاخر من له بدل الكتروني مدعوم ماديا مثل العملات الافتراضية كالبيتكوين و غيرها من العملات التي ظهرت في العقد الاخير والتي زعزعت الكثير من الاراء و القوانين حول النقود الالكترونية و مصداقيتها القانونية و الاقتصادية، ويرجع ذلك إلى تأثير شعبية البيتكوين وارتفاع قيمتها السوقية على قيمة العملات القانونية في الدول، فقد شعرت بعض الحكومات بالتهديد بسبب عدم فهم طبيعتها.

ويختلف الوضع القانوني للبيتكوين من دولة لأخرى، وقد نشر موقع " هاو ماتش" خريطة توضح مدى قبول مختلف الدول حول العالم للبيتكوين

المصدر : موقع https://howmuch.net/articles/bitcoin-legality-around-the-world

ويعكس اللون الأخضر في الخريطة الدول التي تقنن عملة البيتكوين رسميًا، في حين يمثل اللون البرتقالي الدول المحايدة التي لا تقنن البيتكوين صراحة، وفي الوقت نفسه لا تفرض قيودًا على تداول العملات الرقمية،

وتمثل المناطق المظللة باللون الوردي الفاتح الدول التي تفرض قيودًا وقوانين في محاولة لإبطاء التعامل بالعملات الرقمية، في حين تمثل الدول المظللة باللون الوردي الداكن التي تحظر البيتكوين تمامًا وتعتبر التعامل بها غير قانوني ، في حين تمثل الدول المظللة بالرمادي تلك التي لم تقل كلمتها بعد بشأن شرعية البيتكوين والعملات الرقمية.

فيما يلي تفاصيل للخريطة ، استنادًا إلى الشرعية العالمية لعملة البيتكوين من بين 246 دولة:

- قانوني ومحايد (الأخضر والبرتقالي): 99 دولة أو 40 ٪ من العالم(قانوني مثل اليابان[1])
- محظور (وردي فاتح): 7 دول أو 3 ٪ من العالم
- غير قانوني (الوردي الداكن): 10 دول أو 4 ٪ من العالم(مثل الجزائر[2])
- لا توجد معلومات (رمادي): 130 دولة أو 53 ٪ من العالم

بشكل عام ، ما زالت غالبية العالم لم تعلق بعد على مشروعية بيتكوين، لا تزال الصناعة الناشئة غير مفهومة تمامًا من قبل المنظمين العالميين ، مما قد يفسر سبب تعليق بعض البلدان على الحركة. مع مرور الوقت، ستخرج البلدان التي بقيت على الهامش في نهاية المطاف بمجموعة من اللوائح التي إما أن توافق على استخدام Bitcoin أو تشويه النشاط. يستمر ارتفاع شعبية البيتكوين في تجاوز التوقعات ، ولكن لن ترى جميع البلدان العملة المشفرة في صورة إيجابية[3].

كما ان القبول و الرفض يتفاوت بين الدول الغربية و الدول العربية بين من يقبلها مع تقنينها وبين المحايدة و الرافض نهائيا لها[4].

[1]- القانون المعدل لتسوية الأموال (المعروف باسم "قانون العملة المشفرة") الذي تم تفعيله في 25 ماي 2016 ، وأصبح ساري المفعول في 1 أفريل 2017 ، قبل الموعد المتوقع أصلاً، للاطلاع اكثر انظر لموقع وكالة الخدمات المالية FSA: https://www.fsa.go.jp/

[2]- انظر الملحق رقم 01.

[3]- راوول، تصور حول مشروعية بيتكوين حول العالم، نشر بتاريخ15-01-2018 ،https://howmuch.net/articles/bitcoin-legality-around-the-world ،اخر زيارة للموقع 06-04-2019 بتوقيت20:03.

[4]-انظر الملحق رقم 02 و 03.

الفصل الاول

صور الجرائم الواقعة على النقود الالكترونية ذات الطبيعة المادية

تمهيد

ان طبيعة النقود الالكترونية و التي تتمثل في الطبيعة الالكترونية الرقمية لم تمنعها من استعمال الوسائل المادية التي ساعدت و سهلت كثيرا في انتشار قابلية التعامل السلسة بها في التعاملات التجارية التي تتسم هي الاخرى بالسرعة ، فباستعمالها لهذه الوسائل و النشاطات المادية جر عنه الكثير من السلوكيات الاجرامية و اوقع عليها بعض الجرائم التي لم تكن لتصل الى النقود الالكترونية كونها غير ملموسة ولا يمكن الحصول عليها بأساليب اجرامية تقليدية مما جعل الاساليب الاجرامية تتطور وصولا لها من اجل الاستيلاء عليها و الربح منها ، و من بين الجرائم التي تمكن المجرمين عن طريقها في النفاذ الى النقود الالكترونية جريمة غسيل الاموال و التي استعمل مفتعلوها مجموع العمليات التي ساهمت فيها النقود الالكترونية بكسر حواجز الحدود و حجب اعين القانون (المبحث الاول) ،كما ظهرت جريمة اخرى تستهدف احد ادوات النقود الالكترونية و اكثرها استعمال و هي البطاقة الائتمانية و التي لم تسلم من الاجرام بوقوعها هي الاخرى في جريمتي السرقة و التزوير(المبحث الثاني) لغرض السطو و الحصول على ما تحمله من نقود الكترونية ،بهذا سنحاول القاء الضوء على هاتين الجريمتين و اظهار علاقتهما بالنقود الالكترونية في الفصل.

المبحث الاول

جريمة غسيل الاموال

كان لزاما على المجرمين المحترفين اثناء حصولهم على الاموال المتحصل عليها من فعل اجرامي ان يخفوا ما تحصلوا عليه من باب ابعاد التهمة عنهم مما ينتج عنها ما يسمى بغسيل الاموال تلك العملية التي يقوم بها المجرمين لكي يبعدوا مجموع الاموال عن مصدرها الاجرامي بعدة اساليب و مع التطور الحاصل في مجال المال و ظهور النقود الالكترونية اعطى اسلوبا جديدا بعيدا عن الرقابة القانونية لهذه العملية(غسيل الاموال) و بهذا وجب علينا ان نأخذه ضمن دراستنا ،بان نذكر هذه الجريمة كإحدى الجرائم الواقعة على النقود الالكترونية بتحديد مفهومها (المطلب الاول)و اركانها التي تنتج المسؤولية الجزائية و كذلك مدى انتشارها في مجال التعامل بالنقود الالكترونية و علاقتها بها(المطلب الثاني) و مجموع الجهود الدولية و الوطنية التي استحدثت لهذه الجريمة في ها المجال الجديد(المطلب الثالث).

المطلب الاول

مفهوم جريمة غسيل الاموال

سنتطرق في العناصر القادمة الى التعريف بجريمة غسيل الاموال في المواثيق الدولية و الاراء الفقهية و التشريعات الوطنية و لنقارن الرؤى في فهم هذا المصطلح مع ذكر اركانها التي تحمل المسؤولية و الاساليب المعتمدة لارتكابها في الفروع الاتية:

الفرع الاول

تعريف جريمة غسيل الاموال

سنعرف غسيل الاموال لغة و اصطلاحاً لدى الكثير من الجهات و الاراء مع ما تناولت القوانين بالصراحة او الضمنية في النقاط الاتية:

اولا: التعريف اللغوي

أ. **غسيل** : غَسَلَ الشيء يَغسِلُهُ غَسْلاً و غُسْلاً، وقيل الغَسْلُ المصدر من غسَلْت، والغُسْلُ بالضم، الاسم من الإغْتِسَال، يقال غُسْل وغُسُل.

والغَسُول: الماء الذي يُغْتَسل به، وكذلك المِغْتَسَل. والمِغْسِل: ما غُسِلَ فيه الشيء. وغُسَالَة الثوب: ما خرج منه بالغُسْل.[1]

[1]- ابن منظور، المرجع السابق، المجلد الحادي عشر، ص:494 وانظر ايضا :المعجم الوسيط ، ص653.

وفي التنزيل العزيز: "هذا مغتسل بارد وشراب"[1] .

ب. **الأموال:** لغة مال مُولاً و مَؤُولاً: كَثُرَ مَالُهُ، إذا صَار ذَا مَالٍ، وهي مَالُهُ، وفلاناً أَعطَاهُ المال[2]،اصطلاحا: اسم لجميع ما يملكه الإنسان، وأصله ما يميل إليه الطبع ويمكن ادخاره كالنقد، وما يمكن أن يقوم مقامه.

ويطلق على هذه الظاهرة مصطلح غسيل الأموال، أو مصطلح تبييض الأموال[3].

ثانيا: التعريف الاصطلاحي

كثرت المفاهيم و الآراء حول مصطلح هذه الجريمة بين الفقهاء حسب رؤيتهم الخاصة او انتمائهم لكل مجال سواء كان تقني أو قانوني و أيضا بالنسبة لبعض الهيئات و المؤسسات التي لها علاقة بميدان هذه الجريمة غير ان الاتفاق على مفهوم واحد ان العملية تقوم على اخفاء او تنظيف الأموال القذرة لإعطائها وجه الشرعية ونذكر من التعاريف الآتي:

-"يعني أي فعل أو شروع فيه يهدف إلى إخفاء أو تمويه طبيعة أو كنه المتحصلات المستمدة من أنشطة غير مشروعة بحيث تبدو كما لو كانت مستقاة من مصادر مشروعة ليتسنى بعد ذلك استخدامها في أنشطة مشروعة داخل الدولة أو خارجها"[4].

-وقد تم تعريفها بانها"مجموعة الأنشطة التي تتم بعيدا عن أجهزة الدولة القانونية، ولا تسجل في حسابات الدخل الوطني وهذه الأنشطة تمثل مصدرا للأموال القذرة التي يحاول أصحابها تبييضها في مرحلة تالية وذلك بإجراء مجموعة من العمليات والتحويلات المالية والعينية على هذه الأموال لتغيير صفتها غير المشروعة ، وإدخالها ضمن النظام الشرعي لإكسابها صفة مشروعة ، وبذلك تهدف عمليات تبييض الأموال إلى إخفاء مصادر أموال

---

[1]- سورة –ص-الآية 42.

[2]- ابن منظور، المرجع السابق، ص636.

[3]-**من التشريعات التي تستخدم مصطلح غسل أو غسيل الأموال نذكر:**

- مصر: القانون رقم 80 لسنة 2002، المعدل بالقانون رقم 78 لسنة 2003.
- المغرب: القانون رقم 05-43.
- سوريا: القانون رقم 33 لسنة 2005.

من التشريعات التي تستخدم مصطلح تبييض الأموال نذكر:

-الجزائر :القانون رقم 05-01 المتعلق بمحاربة تبييض الأموال وتمويل الإرهاب ومكافحتهما،

- فرنسا: القانون رقم 96-392 المتعلق بمكافحة تبييض الأموال والاتجار في المخدرات والتعاون الدولي في مجال حجز ومصادرة متحصلات الجريمة،

-لبنان: القانون رقم 318لسنة 2001 بشأن مكافحة تبييض الأموال.

[4]-محي الدين عوض،جرائم غسل الاموال ، مركز البحوث و الدراسات- جامعة نايف- السعودية ،الطبعة الاولى، 2004،ص 15.

المجرمين وتحويلها بعد ذلك لتبدو كاستثمارات قانونية."[1]

-وكذلك عرفت بانها "أموالًا قذرة ، ملوثة قانونيًا بحقيقة أنه تم ربحها من خلال أنشطة غير قانونية، إذا استثمرت المنظمة الأموال القذرة في عمل تجاري لشراء حصة ملكية في النشاط التجاري المشروع ، فسيحقق للمؤسسة الحصول على حصة من أرباح هذا العمل المشروع، إن حصة الملكية في العمل المشروع تولد أموالًا نظيفة و غير ملوثة قانونيًا"[2].

-كما تعرف عملية غسيل الأموال: " أنها كل عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسبت منه الأموال" [3] .

- وهناك تعريف آخر "غسل الأموال هو إعادة تدوير أو نقل الممتلكات، التي هي عائدات إجرامية، لغرض إخفاء الطبيعة غير القانونية للأصول الحكومية و أصلها.

أي نشاط إجرامي يحقق ربحًا كبيرًا– الابتزاز والاتجار بالمخدرات و الاتجار بالأسلحة وأنواع معينة من جرائم ذوي الياقات البيضاء – يمكن-أن يؤدي إلى غسل الأموال"[4].

وقد تم تعريفها أيضا من قبل الكثير من المنظمات و الهيئات الدولية و الاتفاقيات والتي تنوعت مفاهيمها بين الضيق و الواسع في تحديد المعنى الحقيقي لهذه الجريمة نذكر منها:

-**إعلان بازل**[5]لسنة1988لغسيل الأموال بأنه **"**جميع الأعمال المصرفية التي يقوم بها الفاعلون وشركاؤهم بقصد إخفاء مصدر الأموال وأصحابها**"**وهو ما ادخلته في مجموع الافعال المجرمة التي تعمل على اخفاء عائدات الاتجار بالمخدرات و الموثرات العقلية .

-**تعريف فاتف(FATF)**[6]، يعرف مصطلح غسيل الأموال بأنه تجهيز عائدات الجريمة لإخفاء منشئها غير القانوني بهدف إسباغ الشرعية على المكاسب غير المشروعة من الجريمة .ويشير الفريق في توصياته الأربعين إلى

---

[1]– عبد الودود خربوش، التجربة المغربية في مواجهة جرائم غسل الأموال و علاقتها بالاتجار الغير الشرعي بالمخدرات ،ندوة بعنوان :غسيل الأموال و اثره في انتشار المخدرات، السعودية، 2012 ،ص03.

[2]–Jeffrey H . Mastuura, digital currency : An International Legal and Regulatory Compliance Guide, Bentham Science Publishers, U.A.E,2016 ,p 38.

[3]– محمد فتحي عيد، الإجرام المعاصر، الرياض: منشورات أكاديمية نايف للعلوم الأمنية، 1999 ،ص280.

[4]–Solliciteur Général et de la Justice du Canada, Le Blanchiment de la Monnaie Electronique,Canada,1998,p 1 .

[5]–هي لجنة للرقابة على البنوك عرفت بلجنة بازل ، شكلت من محافظي البنوك المركزية لمجموعة البلدان العشر بالإضافة إلى ثلاث دول أخرى .وقد أصدرت عدة إرشادات ومعايير الرقابة البنكية.

[6]– مجموعة العمل المالي بالإنجليزية (Financial Action Task Force)ويختصر: فاتف (FATF)، هي منظمة حكومية دولية مقرها في العاصمة الفرنسية باريس، أسست سنة 1989م، وتهدف مجموعة العمل المالي لمحاربة تزوير العملات وتمويل الإرهاب، ولديها 37 عضواً في المنظمة،

تعريف غسيل الأموال الواردة في اتفاقية (فيينا)لمكافحة الإتجار غير المشروع بالمخدرات والمؤثرات العقلية، ويوصي بتوسيع نطاق الجرائم الأصلية لذلك التعريف لتشمل الجرائم الخطيرة.

-**برنامج الأمم المتحدة الدولي لمكافحة المخدرات**: "عملية يلجأ إليها تجار ومهربو المخدرات المؤثرات العقلية لإخفاء وجود دخل أو لإخفاء مصدره غير المشروع أو استخدام الدخل في وجه غير مشروع، ثم يقومون بتمويه ذلك في الدخل لجعله يبدو وكأنه تحقق من مصدر مشروع، وهو عبارة مختصرة يعني: التصرف في النقود بطريقة تخفي مصدرها وأصلها الحقيقي".

-**الهيئة الدولية لمراقبة المخدرات**: "التسريب الخفي للأموال ذات المنشأ الإجرامي إلى القنوات القانونية للأعمال التجارية المشروعة، مما يجعلها تبدو عادية وقانونية ومشروعة."

-**المنظمة الدولية للشرطة الجنائية(الانتربول)** فتعرف غسيل الأموال بأنه: عمل أو الشروع في عمل يهدف إلى التكتم أو التستر على طبيعة الأرصدة المكتسبة بصورة غير مشروعة، بحيث يبدو أنها قد جاءت من مصدر مشروع".

-**المذكرة الإيضاحية للقانون العربي الاسترشادي لمكافحة غسيل الأموال وتمويل الإرهاب**[1] في المادة 02 البند-و- :

1- كل سلوك ينطوي على تحويل المتحصلات أو نقلها مع العلم بأنها عائدات جرائم بفرض إخفاء أو تمويه المصدر غير المشروع أو مساعدة أي من الجناة في الجريمة الأصلية على الإفلات من العقوبة .

2- إخفاء أو تمويه الطبيعة الحقيقية للمتحصلات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها مع العلم أن هذه المتحصلات عائدات جرائم أصلية .

3- اكتساب المتحصلات أو حيازتها أو استخدامها مع العلم وقت تلقيها بأنها عائدات جرائم أصلية متى كان الجاني غير مرتكب الجريمة الأصلية وهي الجريمة مصدر الأموال محل الغسيل.

اما بالنسبة للتشريعات فقد تعددت اخراجاتها بين الموافق موافقة تامة و بين المتحفظ في مجموعة الاتفاقيات و المعاهدات الدولية و الاقليمية التي انشات كنتيجة مباشرة او غير مباشرة لمحاولة مكافحة هذه الجريمة و نذكر منها الاهم وهو القانون الجزائري و الذي كنتيجة لذلك، صادق المشرع الجزائري على اتفاقية فيينا لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية عام 1988 ، وبها تم تحريم عمليات غسيل الأموال بمقتضى

[1]- أعتمدت بقرار مجلس وزراء العدل العرب رقم 1000/د29 بتاريخ 2013/11/26 صنعاء – اليمن.

التعديلات التي أدخلت على قانون العقوبات، فتمت –بمقتضى هذه التعديلات إضافة المواد من 389 مكرر إلى 389 مكرر 09، إضافة الأحكام المتعلقة بجريمة غسل الأموال

حرصا من المشرع الجزائري على مواكبة الالتزامات المنصوص عليها في الاتفاقيات الدولية والإقليمية، وتأكيدا منه على سياسة تحريم هذه العمليات، أصدر القانون رقم 05-01، المعدل والمتمم بمقتضى الأمر رقم 12-02 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما[1]، والذي يتبين الآليات الوقائية والردعية الكفيلة بمحاربة ظاهرة غسل الأموال، وما يتبعه من نصوص تنظيمية وتكميلية.

الفرع الثاني

أركان جريمة غسيل الأموال

إن جريمة غسل الأموال على النحو السالف تفترض توافر جريمة سابقة تسفر عن أموال يقوم الجاني بارتكاب أفعال يتحقق بها غسيل تلك الأموال، مع توفر القصد الجنائي لديه .

هكذا يتبين أن البنيان القانوني لجريمة غسيل الأموال يضم مختلف المكونات التي يتطلبها النص المجرم، فلا يقتصر الأمر على الركنين التقليديين (المادي والمعنوي) بل يشمل ما قد يستلزمه النص من شروط أولية أو أركان مفترضة أو عناصر خاصة يؤثر توافرها أو تخلفها على الجريمة وجودا وعدما، كما يتصل بالبنيان القانوني لجريمة غسيل الأموال بعض الظروف التي يترتب عليها تغيير في قدر العقوبة المستحقة ومن تكامل هذه الجوانب يصير السلوك المؤثم جريمة يستحق فاعلها الجزاء المقرر في النص.

فباستجلاء عناصر جريمة غسل الأموال، نجدها تقوم على ركن مفترض تجسده الجريمة الأصلية (أولا) والركن المادي (ثانيا) والركن المعنوي (ثالثا)

اولا: الركن المفترض

"إن التشريعات المقارنة اختلفت نسبيا في تحديد طبيعة الركن المفترض لجريمة تبييض الأموال وذلك حسب أنظمتها القانونية ونظرتها للأموال المبيضة.

حيث أن كل التشريعات التي تجري بها عمليات تبييض الأموال تتفق على أن جريمة تبييض الأموال هي جريمة

[1]- القانون رقم 05-01 المتعلق بمحاربة تبييض الأموال وتمويل الإرهاب ومكافحتهما، المؤرخ في 10-02-2015، ج ر ج ج، ع 11، لسنة 2005، المعدل والمتمم مقتضى الأمر رقم 12-02 المؤرخ في 13-02-2012، الصادر في ج ر ج ج، ع 08، المؤرخة في 15-02-2015.

تابعة لجريمة سبق ارتكابها، تسمى الجريمة الأولية والتي نتجت عنها هذه الأموال غير المشروعة، لتأتي بعدها مرحلة تتمثل في عملية تبييض هذه الأموال لتطهيرها وتنظيفها بإحدى الصور الممكنة.

وعند ارتكاب إحدى صور السلوك الإجرامي للجريمة يفترض بداية وجود جريمة سابقة نتجت عنها أموال غير مشروعة، وهو ما يعرف بالركن المفترض، ومنه فإذا لم يتحصل عن الجريمة أية أموال فلا مجال للحديث عن جريمة تبييض الأموال، لأنه يشترط في جريمة تبييض الأموال وجود أموال متحصل عليها من جريمة سابقة. وعليه فإن هناك شرطين يجب توفرهما للحديث عن الركن المفترض

أولا- وجود جريمة سابقة: لتحديد الجريمة الأولية أو الأصلية أو ما يسمى الجريمة السابقة انتهجت التشريعات المقارنة ثلاث أساليب هي:

الأسلوب المطلق: أي ترك المجال مفتوح في تحديد الجريمة السابقة ليشمل كل الجرائم المعاقب عليها في التشريع المعمول بها.

أسلوب التقييد :أي أن المشرع قيد مجال التجريم حسب نوع معين من الجرائم التي تسبق عمليات تبييض الأموال

الأسلوب المختلط: إن المشرع أخذ بنوع معين من الجرائم دون تحديد المجال الذي يشمله هذا النوع من الجرائم، في حين حصر بعض الأنواع من الجرائم التي تجرم عمليات التبييض التي تقع على الأموال المتحصلة منها.

بالنسبة للمشرع الجزائري: حدد المشرع الجزائري الجريمة الأصلية في المادة 389 مكرر من القانون العقوبات التي تنص على «... عائدات الإجرامية...» كما عرفها حسب المادة الثانية من القانون 01 / 06 المتعلق بمكافحة الفساد « العائدات الإجرامية كل الممتلكات المتأتية أو المتحصل عليها بشكل مباشر أو غير مباشر من ارتكاب الجريمة»[1] مما يفيد أنه أخذ بالأسلوب المطلق، أي تعد جريمة تبييض الأموال كل الأموال الناتجة عن جريمة دون تحديد نوع هذه الجريمة هذا المشرع الجزائري وسع مجال ونطاق التجريم في هذا الخصوص وهو أحسن ما فعل، حيث أن هذا النص التشريعي يواكب هذه الظاهرة الإجرامية مهما تغيرت أساليب وكيفية ارتكابها ولا تترك المجال لتنصل المجرمين من المتابعة الجنائية"[2].

[1] - الجريدة الرسمية الجزائرية رقم14، مؤرخة في08مارس2006، ص5.

[2] -بن الاخضر محمد، الاليات الدولية لمكافحة جريمتي تبييض الاموال و تمويل الارهاب الدولي، اطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة تلمسان، الجزائر، السنة الجامعية2014-2015، ص ص:41-42

ثانيا: الركن المادي

هو مجموعة العناصر المادية المكونة للسلوك الإجرامي، بحيث تتخذ مظهرا خارجيا تلمسه الحواس على وجه من الأوجه، يصدر من الفاعل ويحقق نتيجة معاقب عليها تؤدي إلى الاعتداء على المصالح المجتمع التي يحميها القانون، شريطة وجود علاقة السببية بين السلوك والنتيجة.

عناصر الركن المادي: وتتمثل عناصر الركن المادي فيما يلي

1. **السلوك الإجرامي**: نص عليه المشرع في المادة 02 من القانون 05-01، حيث حاول النص على عدة صور سعيا منه لتغطية كافة أنماط السلوك الإجرامي[1]، وهذه الصور:

- كل تحويل للممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لها.

- كل مساعدة لأي شخص متورط في ارتكاب الجريمة الأصلية التي تحصلت منها هذه العائدات الإجرامية، للإفلات من الآثار القانونية لأفعاله.

- كل سلوك يؤدي إلى إخفاء أو تمويه الطبيعة الحقيقية للممتلكات، أو مصدرها أو حركتها أو مكانها أو كيفية التصرف فيها أو الحقوق المتعلقة بها، مع علم الفاعل بأنها عائدات إجرامية

- كل سلوك يؤدي إلى اكتساب ممتلكات أو حيازتها أو استخدامها، مع علم متلقيها بأنها تشكل عائدات إجرامية

- كل مشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة أو التواطؤ أو التآمر على ارتكابها أو محاولة ارتكابها والمساعدة، أو التحريض على ذلك أو تسهيله، وإسداء المشورة بشأنه شرح عناصر السلوك الإجرامي وشرحا للعناصر الماضية

- اكتساب الأموال: يعني تلقيها على سبيل التكسب أو التربح من مصدر الجريمة، بطريق مباشر أو غير مباشر
- حيازة الأموال؛ تعني الاستئثار بها على سبيل التملك والاختصاص دون الحاجة إلى الاستيلاء عليها، بحيث يكون له حق التصرف فيها.
- التصرف في الأموال: يكون بنقل ملكيتها أو حيازتها للغير أو رهنها. :حفظ الأموال: يكون بحجبها عن الغير ومتابعتها

[1] -راجع المادة 02 من قانون الوقاية من تبييض الاموال و تمويل الارهاب و مكافحتهما رقم 05-01.

• نقل الأموال، يكون عن طريق نقلها من مكان لآخر سواء كان النقل ماديا باستخدام وسائل النقل، أو مصرفيا عن طريق البنوك، أو تقنيا باستخدام وسائل التقنية الحديثة كالنقل الالكتروني

• تحويل الأموال: هو تغيير شكل الأموال أو العملة، بإجراء عمليات مصرفية أو غير مصرفية أو إلى سبائك ذهبية، أو عن طريق بطاقات ائتمان مزورة....الخ[1]

2. **النتيجة الإجرامية:** حدد القانون عنصر النتيجة في جريمة غسيل الأموال بانها ".... إخفاء لو تمويه الطبيعة القانونية للممتلكات أو مصدرها، أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها....، وإخفاء المال يعني: حيازة المال المتحصل من الجريمة المصدر لكي لا يترك الغير حقته أو مصدره أو مكانه لو صاحبه أو الحيلولة دون اكتشاف ذلك، سواء كانت الحيازة مستترة أو علانية، وبالتالي يصدر من الجائي نشاط أو فعل إيجابي يتمثل في عملية إخفاء المال القذر وعادة ما يتم ذلك في البنك مرك، ولا يقتصر الإخفاء على الفعل المادي فحسب بل يمتد أيضا إلى بعض التصرفات القانونية، مثل عملية إستخدام غير حقيقي في شركة وهمية، كما قد يكون بفعل سلبي كالامتناع عن الإعلان عن أمر معين إذا كان هناك إلتزام بالإعلام،

أما التمويه فهو عبارة عن مجموعة الأفعال الرامية إلى إضفاء مظهر مشروع على الأموال، من خلال مجموعة من العمليات المتابعة والمعقدة، التي تؤدي إلى طمس صفتها غير المشروعة

3. **العلاقة السببية:** بان تكون هذه الأفعال فقط هي التي أدت إلى إخفاء حقيقة المصدر غير المشروع لها، وهي الرابطة التي تصل بين النشاط والنتيجة الجرمية، فيتم بواسطتها كيان الركن المعنوي، فتكون النتيجة الجرمية هي ثمرة للنشاط المادي..

ثالثا: الركن المعنوي: "هو العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وتتمثل في سيطرة الجاني على الفعل وآثاره، من خلال العلم الحقيقي به، إذن فجوهر هذا الركن هو الإرادة والعلم، بأن يكون الفعل قد ارتكب عمدا وعن قصد، إلا أن هناك دولا قليلة تجرم فعل غسيل الأموال ولو تم عن إهمال وعدم اكتراث كسويسرا مثلا، وقد نص عليه المشرع الجزائري من خلال المادة 02 من القانون 05-01 بقوله ".....مع علم عائدات إجرامية...."، بالنسبة لكل سلوك من السلوكات المكونة للركن المادي.

-عناصر الركن المعنوي:

1. **القصد العام:** بأن يكون الجاني على علم بأن الأموال محل الغسل، متحصل عليها من أحدى الجرائم أو من مصدر غير مشروع.

2. **القصد الخاص:** هو تعمد الوصول إلى نتيجة معينة أو ضرر معين نابع من إرادة.

[1]- صالحة العمري، جريمة غسيل الاموال وطرق مكافحتها، مجلة الاجتهاد القضائي ،العدد الخامس ، الجزائر، سبتمبر2009، ص188.

و عليه فاذا كان الجاني يجهل ان المال المتحصل عليه من مصدر غير مشروع ،انتفى القصد الجنائي لتخلف اجد عناصره ، كان يكره الغاسل على هذا الفعل مثلا.

رابعا :الركن الشرعي

يقصد بهذا الركن مبدأ شرعية الجرائم بحيث "لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون "، ويترتب على هذا أن القاضي لا يمكنه أن يعاقب شخصا على فعل لم يجرمه المشرع، والحقيقة أنه عن طريق الركن الشرعي يتم تحديد الوصف الجنائي للفعل موضوع الواقعة، ففي الجزائر كانت ظاهرة غسيل الأموال لا تعد جريمة قبل صدور القانون 05-01، وبالتالي لم يكن للقاضي القدرة على العقاب عليها، ولكن بعد صدور قانون 05-01 أصبحت هذه الظاهرة من الأفعال المجرمة التي يترتب على ارتكابها توقيع عقوبات معينة، حيث حدد الأفعال المكونة لها والعقوبات المطبقة عليها، وذلك في الفصل الخامس المعنون بأحكام جزائية في المواد من 31 إلى 34"[1].

الفرع الثالث

اساليب و مراحل جريمة غسيل الاموال

وقد يتخذ المجرمين اساليب و حيل مختلف للقيام بالجريمة بأكمل وجه حتى يتحصلون على النتيجة المطلوبة منها و لجريمة غسيل الاموال مراحل و اساليب هي كذلك تسير من خلالها عملية الغسيل وصولا الى شرعنة اموالهم نذكر منها:

اولا : اساليب غسيل الاموال

يقصد بأساليب غسيل الاموال الطرق التي يستخدمها المبيضون في تحويل تلك العائدات الملوثة إلى اصول وممتلكات تبدو في صورة شرعية ، وعادة يلجأ هؤلاء الى سوء استخدام المؤسسات المالية وغير المالية وحتى بدون مؤسسات في عمليات غسيل الاموال ، وقد تعددت أدوات غسيل الأموال في الوقت الحالي باستخدام أساليب أحدث مثل التكنولوجيا وأكثر قدرة على إخفاء مصادر هذه الأموال وغسلها، منها الأساليب المصرفية المتنوعة مثل استخدام المصرف كواجهة وفتح الحسابات السرية وحسابات مجهولي الهوية، والغسل بالقرض المضمون، والغسيل بالديون الوهمية، والغسيل من خلال خصم الأوراق التجارية، والغسيل من خلال عمليات الأسواق المالية، وصناديق الاستثمار، وشركات التأمين، وإنشاء الشركات الوهمية واستغلال حسابات الشركات، وشركات الواجهة ، والمقاولات، وتجارة المعادن الثمينة، والموجودات النفيسة، والمزادات، ومعارض البيع بالتقسيط،

[1]- صالحة العمري، المرجع السابق، ص ص189-190

والنظم غير الرسمية لتحويل القيمة، وشركات السفر والسياحة، و الهدايا، واليانصيب، وغير ذلك من أدوات ونذكر من الادوات الحديثة التعاملات النقدية الالكترونية غير الرسمية و المتمثلة في التحويلات وتبادل العملات بطريقة عادية بدون مراقبة، وقد صنفت مجموعة العمل المالي للشرق الاوسط وشمال افريقيا بعض الطرق و التي سمتها "الحالات العملية"[1].

ثانيا : مراحل غسيل الاموال

1. **مرحلة التوظيف**: الإيداع، الإحلال، التوضيب، الأمطار كما يطلق عليها أيضا مرحلة التمهيد Placement أو الإعداد للغسيل Prélavage

وهي العملية الأولى التي يبدأ فيها غاسل الأموال بالتخلص من الكميات الضخمة من النقود السائلة المتحصل عليها من النشاط الإجرامي الأصلي، حيث أن السيولة النقدية هي أكثر وسائل التبادل شيوعا في عالم الإجرام وتعد أكثر الوسائل قبولا بالنسبة للعديد من الناشطين في هذا العالم على أساس أن بقاء كميات كبيرة من النقود في هذه المرحلة يقوم صاحب المال القذر بتوظيف أمواله عن طريق بعض الأساليب التالية: التحويل والإيداع عن طريق البنوك، الصفقات النقدية ،إعادة الإقراض، الفواتير المزورة، النقود البلاستيكية، الإنترنت، وكذا أعمال أخرى مختلفة ،المزادات للقطع الفنية النادرة أو السيارات القديمة الطراز، شراء المحلات التجارية أو المشروعات الصغيرة الفاشلة التي تصبح بعد فترة من أعظم الشركات الناجحة.

كما تلعب صالات القمار والكازينوهات، وشركات الصرافة دورا رئيسا في عمليات غسل الأموال.

كما تعد مرحلة التوظيف المرحلة التي يتعرض فيها الغاسل لأكبر خطر فبالرغم من أن الأموال غير المشروعة تكون قد قطعت – خلال هذه المرحلة – شوطا كبيرا في طريق إضفاء صفة المشروعية عليها، غير أن هذه الأموال غير المشروعة تكون لا تزال عرضة لاكتشاف أمرها لأنه ليس من العسير التعرف على من قام بعملية الإيداع للأموال ومن ثم علاقته بمصدر هذه الأموال سواء كان نفس الشخص الذي حقق الأموال أو من ينوب عنه في هذا المجال أو من خلال إحدى الشركات التي يمتلكها كشخصية اعتبارية ...هذه المرحلة إذن هي أضعف حلقات غسيل الأموال مقارنة مع المراحل التالية"[2].

[1]- انظر الملحق رقم 04

[2]- فريد علواش، جريمة غسل الأموال – المراحل والأساليب، مجلة العلوم الانسانية، العدد الثاني عشر، الجزائر، نوفمبر2007، ص 251.

2. مرحلة التغطية أو التمويه أو الخلط أو الترقيد:

وفي هذه المرحلة يلجأ غاسلو الأموال إلى عدة عمليات مصرفية على ودائعهم ويكون فيها نوع من التعقيد والتمويه والتشابك مع التشابه من حيث التكرار والحجم وتعقيداتها وهي جوهر عملية الغسل حيث يتم فيها إخفاء عدم مشروعية الأموال غير المشروعة، ويمكن استخدام هذه الأموال في شراء أوراق مالية أو عقود تأمين أو أدوات استثمار قابلة للتحويل على شكل شيكات أو حوالات بريدية أو سندات لأمر حاملها أو يتم تحويلها الكترونياً من خلال شبكات الانترنت إلى حسابات أخرى في مناطق ودول مختلفة، كما وتلعب الشركات الوهمية دوراً بارزاً في هذه المرحلة[1].

3. مرحلة الدمج:

"و تلك هي المرحلة النهائية من مراحل غسل الأموال والتي يتم فيها إضفاء الشرعية على العائدات غير المشروعة بعد أن انقطعت صلتها تماما منشأها الإجرامي عقب مرحلتي الإيداع والتمويه. حيث يعاد ضخ الأموال التي تم غسلها في الاقتصاد مرة أخر كأموال مشروعة وتكتسب مظهرة قانونية. وذلك بأن تشترك الأموال الناشئة عن الفعل غير المشروع في مشروع تجاري أخري يعرف عنه مشروعيته ومشروعية مصدر رأسماله بحيث يصعب الفصل بين المال المتحصل من مصدر غير مشروع والمال المتحصل من مصدر شرعي وبالتالي يعاد ظهور الأموال غير المشروعة التي تم غسلها مختلطة ومندمجة في النظام الشرعي، وتبدو وكأنها متولدة عن أعمال مشروعة. ويغلب أن تكون البنوك أو المؤسسات المالية طرفة أصلية مشاركة في عملية غسل الأموال وأن كان يتعذر إثبات سوء النية أو التواطؤ مع أصحاب الأموال غير المشروعة"[2].

المطلب الثاني

علاقة النقود الإلكترونية بجريمة غسيل الأموال:

تعد النقود الإلكترونية أداة وفاء جديد و مقبولة لدى الغالبية وسهلة الاستخدام وسريعة الحركة، ومن المفترض أن تشكل حدثا ايجابيا في عمليات التعامل الاقتصادي .غير ان هاته الاخيرة لم تسلم من ايدي غاسلو الأموال ولم يتركوها تؤدي هدفها الإيجابي الذي وجدت من أجله، فعمدوا فور ظهورها لاستخدامها لارتكاب جريمتهم فجعلوها ذات وجهين إيجابي وسلبي بدلا من أن تكون ذات وجه إيجابي فقط. ولتتضح الصورة ويمكن ربط العلاقة

---

[1]– طايل كايد المجالي، النماذج العربية و الدولية في مكافحة غسل الاموال، حلقة علمية بعنوان: غسل الأموال وأثره في انتشار المخدرات، السعودية، 11-2012/6/13،ص8.

[2]– عزت الشيشيني، أساليب مكافحة غسل الأموال ومكافحة المخدرات جمهورية مصر العربية نموذجا، غسل الاموال و اثره في انتشار المخدرات،السعودية،11-13 /2012/06، ص8.

جيدا بين جريمة غسيل الأموال والنقود الإلكترونية فقد وضعنا التوضيحات القادمة في الفروع التالية :

الفرع الأول

"النقود الإلكترونية تسهل ارتكاب جريمة غسيل الأموال

يتم التعامل بالنقود الإلكترونية دون الحاجة إلى ظهور الهوية الحقيقية للمتعاملين وأحيانا دون ظهور هويتهم إطلاقا ، وهذا يخلق فرصة لدى غاسل الأموال لاستخدامها في ارتكاب جريمته، إذ لن يكون مضطرة للإفصاح عن شخصيته حتى لو كان له تاريخ حافل في ارتكاب جريمة غسل الأموال. كما أن للنقود الإلكترونية طابع من السرية يجعل مهمة السلطات المختصة بمراقبة جريمة غسل الأموال مهمة صعبة جدا حيث يصعب مراقبة السجلات والعمليات المالية والمصرفية التي تتم باستخدام هذه النقود.

فضلا عن أن استخدام هذا النوع من النقود يعتمد بالدرجة الأولى على استخدام أجهزة الكمبيوتر والأنظمة الإلكترونية وقد تتعطل هذه الأجهزة والأنظمة التي تحفظ هذه النقود سواء كان هذا العطل مقصودة نتيجة أعمال جرمية أو محطة تلقائية، وفي هذه الحالة يصبح من المستحيل مراقبة العمليات التي تتم باستخدام النقود الإلكترونية ومن ثم يخلق المجال واسعة لارتكاب جريمة غسل الأموال. ومن جهة أخرى فمن المعروف أن المصارف المركزية تؤدي دورا لا يستهان به في منع ارتكاب جريمة غسل الأموال ، وذلك من خلال مراقبتها للأسواق المالية، وهنا يبرز خطر نمو النقود الإلكترونية التي تؤدي دون شك إلى التأثير في ميزانية المصارف المركزية، ومن ثم تقلص هذه الميزانية بسبب انخفاض القاعدة النقدية، وهذا يفقد المصارف المركزية قدرتها على مراقبة الأسواق النقدية"[1].

اضافة إلى هذه الملاحظات نجد أن طبيعة النقود الالكترونية و قلة المراقبة عليها وعدم وضع الدولة يدها أو نظرها عليها فإنها تفتح مجال خصبا أمام توسع جريمة غسيل الأموال و هذا ما سنوضحه في الآتي.

الفرع الثاني

"النقود الإلكترونية توسع محل جريمة غسل الأموال

يتمثل محل جريمة غسل الأموال بالأموال غير المشروعة الناتجة عن ارتكاب الجرائم، وقد تساعد النقود الإلكترونية في تأمين هذه الأموال غير المشروعة التي تحتاج إلى الغسيل. فمثلا يؤدي استخدام هذه النقود إلى زيادة حالات التهرب الضريبي حيث يصعب على الجهات المكلفة بتحصيل الضرائب مراقبة الصفقات التي تتم عبر

[1]- بسام احمد الزلمي، المرجع السابق، ص ص:557-558.

شبكة الإنترنت باستخدام هذه النقود، ويصعب ومن ثم فرض الضرائب عليها، ولا شك أن الأموال التي تنتج عن التهرب الضريبي تعد أموالا غير مشروعة تحتاج إلى الصعب التحقق من صحتها عند إبرام الصفقات، فقد يكتشف بعد إتمام الصفقة أن النقود الإلكترونية التي سويت بها هذه الصفقة مزيفة، ومن ثم فإن الأموال الناتجة عنها هي أموال غير مشروعة تحتاج إلى الغسيل.

ويضاف إلى ذلك أيضا أنه توجد إمكانية حقيقية لاستخراج نسخ مزيفة من النقود الإلكترونية من خلال معرفة تفاصيل النقود الإلكترونية الأصلية وإذا تحقق ذلك فإن هذه النقود المزيفة تعد أموالا غير مشروعة. كما أن هذه النقود معرضة للسرقة من خلال الدخول غير المشروع إلى أجهزة وأنظمة الحساب الشخصي المحفوظة على أجهزة الكمبيوتر عن طريق ما يعرف بفك التشفير غير المشروع ، وهذه السرقة لا تختلف عن سرقة النقود التقليدية فحصيلة كل من السرقتين تعد أموالا غير مشروعة .

إذا تخلف عمليات غسل الأموال آثار خطيرة على نواحي الحياة جميعها دون استثناء. وقد أتت النقود الإلكترونية لتزيد من حدة هذه الآثار عبر زيادة معدلات جرائم غسل الأموال سواء من خلال تأمين المزيد من الأموال غير المشروعة التي يتم غسلها، أو من خلال تأمين المزيد من الأموال غير المشروعة التي يتم غسلها، أو من خلال تسهيل ارتكاب جريمة غسل الأموال"[1].

الفرع الثالث

مراحل و أساليب غسيل الاموال عن طريق النقود الالكترونية

وكما شرحنا سابقا حول مجموعة الأساليب التقليدية التي يستعملها غاسلو الأموال بشكل عام وكذا مراحل جريمة غسيل الأموال التي تمر عبر ثلاث مراحل وهي الايداع او التوظيف اولا ثم التمويه او الاخفاء ثانيا و أخيرا الدمج و قصد ربط العلاقة بين النقود الالكترونية و جريمة تبييض الأموال سنعرج عنها بشكل توضيحي مدعما بأمثلة بأساليب حديثة في هذا المجال نسردها في النقاط الآتية:

بما أن التعامل التي تقتضيه النقود الالكترونية ذا طبيعة الكترونية خالصة بعد تحويل الأموال المادية إلى أموال ذات هيئة أو طبيعة رقمية الكترونية فان اغلب الأساليب التي تعتمد هنا لها صلة بالتكنولوجيا الحديثة و الرقمنة و ما إلى ذلك من بين الأساليب التي تعتمد نذكر مايلي:

[1]- بسام احمد الزلمي، المرجع السابق ، ص ص:558-559

اولا: تبادل العملات الالكتروني:

ان اكبر مجال قد تنشط فيه جريمة تبييض او غسيل الاموال هو مجال التبادل الالكتروني للاموال حيث يعتمد على كل مراحل الجريمة دون أي مجال للشك او المراقبة حيث يقوم على عدة عمليات التي لا تتطلب تلك الاجراءات المعمول بها في التبادلات التقليدية مع تواجد رقابة الدولة او احد هياكلها الرسمية.

وكمثال لذلك، فإننا نذكر اقسام تبادل العملات الموجودة على مستوى المنتديات الالكترونية في بعض المواقع مثل موقع (الجلفة) او (ستار7العرب) [1] فان مثل هذين الموقعين لديهما قسم تحت عنوان تبادل العملات بكل انواعها حيث تقوم العملية اما مباشرة او عن طريق وسيط يسمى تاجر عملات معتمد يقود باخذ عمولة التبادل دون طلب أي هوية لأي طرف فقط العملية تقوم على ان البائع يقوم بعرض مبلغ معين للبيع لنقول 300 دولار على احد البنوك الالكترونية مثل بايبال (Paypal) بطلب منه اما تحويلها الى عملة اخرى لبنك اخر او تحويلها الى دينار جزائري عن طريق بريد الجزائر فتاتي هنا الحجوزات التي لا نعلم مصدر اموالها اذا كانت قانونيا ام لا، ليتم ارسالها الى الحساب البريدي الخاص بالبائع ليتأكد بعد ذلك تتم العملية بشكل عادي فلنوضح اكثر سنتبع مراحل جريمة غسيل الاموال حسب المثال السابق المرحلة الاولى عملية الايداع او التوظيف يقوم بها الغاسل عن طريق عملية الشراء او ارسال المال الى بائع العملة الالكترونية نأتي الان الى المرحلة التي بعدها و هي الاخفاء او التمويه فكون النقود الالكترونية غير ملموسة او محسوسة و سهلة التنقل و قد تدخل ضمن عمليات تبادل اخرى او شراء عبر الانترنت او تحويلها الى بنوك الكترونية اخرى فأننا قد جسدنا مرحلة التمويه او الاخفاء لنستخلص منها نقود نظيفة نستعملها في المرحلة التي تليها و هي الادماج او الدمج و اعادة ادخالها الى دورة الاقتصاد بشكل اخر اما بتحويلها الى النقود التقليدية او استعمالها في مجال اخر او دولة اخرى او تحويلها الى عملة او سلعة عبر الانترنت.

فمثل هذه المواقع و الاسواق [2] التي تنعدم فيها الرقابة فتحت مجال واسعا لجريمة غسيل الاموال بسبب خصائصها التي توائم هذه الجريمة كعدم اظهار الهويات الحقيقية او التعامل بمبالغ لا تجلب الشبهة عن اشخاص كثر او حسابات و ارصدة كثيرة و السرعة و التعدد في التعاملات و العديد العديد من الميزات التي تجسد صراحة هدف جريمة غسيل الاموال و هو قطع العلاقة بين الاموال و مصدرها ، فبالنظر لهذه المواقع و ملاحظتها يعتبر التعامل فيها رهيب و واسع على المستوى العربي و الدولي، يصعب صراحة ضبطه او تحديد ما يمكن تحديده بين القانوني و غير القانوني.

---

[1]- انظر الملحق رقم 5 و 6.

[2]- مواقع او منصات تبادل عملات الكترونية مدعومة او غير مدعوة كالنقود الافتراضية ظهرت بشكل منظم فيه مسؤولين و مبادلين موثوق يقوم بالاستلام و التسليم كوسيط بين الاطراف حيث تقوم المبادلات على عرض موضوع بمبلغ مالي رقمي بعرض ثمن لبيع على ان يقوم المشتري بالحجز و يتم البيع عن طريق الوسيط او يكون البائع هو نفسه موضوع بالبائع المعتمد لدى المنصة، و حسب التجربة فان الموقعين المذكورين في الملحق3و4 تم التعامل معهما بشكل موثوق، و بدون أي اجراءات ادارية او رقابة و التي قد تفتح باب واسع امام الكثير من الجرائم اكثرها غسيل الاموال.

والملاحظ ايضا ان التعامل في مثل هذه المواقع دخل باب التجارة المربحة لدى الكثير من المتعاملين مما ولد جريمة اخرى و هي التهرب الضريبي مما يعني ان عائداتها مجرمة مع التداول المستمرة او تحويلها الى مجال اخر يعتبر توظيفًا و اخفاءًا و دمجًا لمصدرها الموضح سابقا ورغم ذلك تبقى الرقابة منعدمة في هذا الميدان.

ثانيا : مزادات على الانترنت او مواقع البيع الالكترونية

تقوم بها بعض الشركات التي لديها مزاد الكتروني لتنشأ مواقع إلكترونية وظيفتها المزاد الإلكتروني ، ولديها حسابات بنكية. يقوم البائع بإدخال البضائع من خلال هذا الموقع الإلكتروني فيقوم المشتري باختيار المنتج فيدفع مقابله عن تحويل مالي بالبطاقة بحساب لدى الشركة مشحون مسبقا (مرحلة التوظيف او الايداع) ، تدفع الشركة المال إلى حساب البائع ليرسل البضاعة إلى المشتري فإذا كان المشتري قد استلم البضاعة وأكد أن الأمر ، فتقوم الشركة بإيداع الأموال في حساب البائع .

وفي هذه الحالة يمكن لغاسلي الأموال استخدام هذه الأداة لغسل الأموال. وبالتالي ، فإن مواصفات البضائع

باهظة الثمن للبيع على ما يبدو على ان يتم عرض الموقع وشراء شخص آخر كمشتري رسمي واستلام البضائع ليتم الإعلان عنها وهكذا ، من قبل أحد مرتكبي غسيل الأموال القذرة ليتم تحويلها إلى الجاني الآخر(مرحلة التمويه او الاخفاء) و هي ما يسميها الغالبية بالتجارة الالكترونية وكمثال على ذلك نذكر موقع اي باي (eBay) و موقع امازون (Amazon) و الي اكسبراس(Ali express) و غيرها من المواقع التي تفتح امكانية تطبيق اسلوب او اسلوبين من اساليب هذه الجريمة و ايضا توظيف مراحلها بالشراء و اعادة البيع و توظيفها في شيء اخر(مرحلة الدمج) لتقوم المراحل الثلاثة في عملية واحدة كما سبق شرحها.

ثالثا: العملات الافتراضية و علاقتها بغسيل الاموال

كما عرفنا سابقا العملات الافتراضية تعتبر هي ايضا نوع من انواع النقود الالكترونية غير انها لا تملك اصلا نقديا مباشرا بل بدلا الكترونيا له اصول مالية و قيمة معينة تدعمها مؤسسات مصدرة لهذه العملات رغم ذل فان العملات الافتراضية انتشرت انتشارا واسعا و شهدت قبولا كبيرا كأداة وفاء مما اعطاها قيمة اقتصادية جلبت لها اعين محترفين غسيل الاموال ، و فعلا تم ادراجها ضمن الطرق الحديثة لجريمة غسيل الاموال و قد تم التصريح بذلك في التقرير المقدم من اليوروبول EuroPol [1] بيتكوين وقد ذكرناها على انها احد العملات الافتراضية

[1]– **يوروبول** هي وكالة تطبيق القانون الأوربية ، وظيفتها حفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوربي في مجالات مكافحة الجرائم الدولية الكبيرة والإرهاب انظر اكثر الى : يوروبول/https://ar.wikipedia.org/wiki/ .

"يمثل أكثر من 40 في المائة من جميع المدفوعات الجنائية المحددة "[1] في تحقيقات الجرائم الإلكترونية. يبقى مدى النظر إلى هذا كدليل على وجود تدفق في استخدام البيتكوين كطريقة دفع جنائية بارزة ، "ويمكن اعتبار أسواق التبادل و التعامل بمثابة مُسهل لاستخدام العملات المشفرة في أنظمة غسيل الأموال الحالية والمستقبلية. مع امكانية الوصول إلى هذه الأسواق السرية بسهولة وتكتسب شعبية بين المجرمين (السيبرانيين) لنشر وتأسيس أنشطة إجرامي"[2].

المطلب الثالث

الجهود و الاليات الدولية و الوطنية لمكافحة جريمة غسيل الاموال

ونظراً لكون جريمة غسيل الأموال قد تجاوزت في وقتنا الحاضر الحدود –جريمة عابرة للحدود– بسبب التطور المتسارع في حقل التكنولوجيا الحديثة، ونمو وازدهار حركة التبادل الاقتصادي التجاري وضعف الرقابة المالية والمصرفية لدى بعض الدول والمؤسسات المالية والمصرفية وسهولة اختراق أنظمتها المصرفية، فقد أخذت هذه الجريمة بالتزايد مما أدى إلى اقليمية ووطنية على كافة الأصعدة و اهتمامات دولية وفي مختلف المجالات وتزايد القناعات لدى المجتمع الدولي بضرورة تنسيق الجهود لمواجهة هذه الجريمة، فصيغت واعتمدت العديد من الاتفاقيات والصكوك الدولية لمواجهتها والحد من تداعياتها، كما أن بعض الدول قد أصدرت قوانين وتشريعات لمواجهة هذه الجريمة أيضاً.

الفرع الاول

الاتفاقيات و المواثيق

قامت بعض الدول بإنشاء العديد من الاتفاقيات كمحاولة منها لصد جريمة غسيل الاموال على الصعيدين الاقليمي و الدولي تعزيزا لجهود الدول الاخرى كون تصنيف جريمة غسيل الاموال من الجرائم الدولية و او الجرائم المنظمة و نذكر منها :

اولا : على المستوى الدولي

أ. اتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع في المخدرات والمؤثرات العقلية لعام1988:

"تم إعتماد هذه الاتفاقية في ديسمبر 1988بفيينا ، وقدكان من ضمن أهداف هذه الاتفاقية شن حملة على

[1]–تقرير اليورو بول ،بعنوان الجريمة المنظمة على الإنترنت تقييم التهديد،2015،ص46.

[2]–Rolf van Wegberg and Others, Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin, Journal of Financial Crime, Netherlands 2018 ,p 421.

الحافز الاقتصادي، الّتي تختبئ وراءه الأنشطة الإجرامية وهذا بمصادرة وحجز الأموال الناتجة عن المخدرات" [1].

ونصت المادة **الثالثة** على ضرورة إتخاذ كل طرف في قانونه الداخلي ، ما يجب من التدابير لمعاقبة كل من شأنه إخفاء الأموال أو مصدرها أو مكانها أو طريقة التّصرف بها ، مع العلم أنها مستمدة من جرائم المخدرات[2]. مع الإشارة إلى أن الاتفاقية تشترط وجود القصد الجنائي ضمن أركان جريمة تبييض الأموال ،ّ إذ أن نقل أو تحويل الأموال هو بطبيعته شيء مشروع . لأجل هذا فعلىّ المخالف أن يكون على علم ودراية بأن هذا التحويل للأموال هي ناتجة من جريمة الإتجار غير المشروع في المخدرات ، زيادة على أن يكون هدف الجاني هو إخفاء مصدر تلك الأموال أو مساعدة أي شخص متورط في ارتكاب جريمة الإتجار غير المشروع بالمخدرات من الإفلات من العقوبات القانونية المترتبة عن أفعاله.

تناولت هذه الإتفاقية عدة موضوعات نورد أهمها فيما يلي :

-تنظيم الإجراءات الخاصة بالحجز والمصادرة للأموال الناتجة عن المخدرات بالتبرع بها ، للجهات القائمة على مكافحة المخدرات أو إقتسامها مع أطراف أخرى بحسب الاتفاقيات المبرمة لهذا الغرض .

- تنظيم الاختصاص القضائي واجراءات تبادل تسليم المجرمين.

-تبادل المعلومات .

-تنظيم عمليات تدريب العاملين والمختصين"[3].

ب. إعلان المبادئ للجنة بازل 1988:

"قامت لجنة بازل في كانون أول 1988 باصدار وثيقة عرفت باسم بيان بازل بشأن منع الاستخدام الإجرامي للنظام المصرفي الأغراض غسيل الأموال.

وتدعو هذه الوثيقة، الأوساط المصرفية الدولية للالتزام بالمبادئ الأساسية لمواجهة غسيل الأموال، التي تتم من خلال الأنشطة المصرفية. وتشمل هذه المبادئ تحديد العملاء ومعرفة هويتهم معرفة كاملة، والامتثال للقوانين واللوائح الخاصة بالمعاملات المالية ورفض المعاونة في المعاملات التي يتضح ارتباطها بتمويه مصدر الأموال، وكذلك

[1]-راجع المادة 5من الاتفاقية.

[2]- لوحظ أن هذه الاتفاقية تقتصر على تجريم تبييض الأموال الناتجة عن المخدرات دون الأعمال غير المشروعة الأخرى، كالرشوة و الفساد الإداري و السياسي، و التهرب الضريبي و المتاجرة غير المشروعة في الأسلحة..

[3]- خوجة جمال، جريمة تبييض الاموال -دراسة مقارنة، مذكرة ماجستير قانون خاص،كلية الحقوق جامعة تلمسان،الجزائر،2008،ص ص:147-148.

التعاون مع سلطات القضاء والشرطة وغيرها من سلطات تنفيذ القانون الى اقصى مدى تسمح به اللوائح المتعلقة بصون اسرار العملاء"[1].

ج. اتفاقية الجريمة المنظمة لمكافحة الجريمة المنظمة عبر الوطنية2000(باليرمو):

"وتضم هذه الاتفاقية نصوص تهدف الى تعزيز أوجه التعاون الدولي لمختلف الأنماط الخطيرة للجريمة المنظمة عبر الوطنية منها جريمة غسل الأموال ومكافحتها:

- المادة (07) تضمنت عدد من تدابير المنع والوقاية في عمليات غسل الأموال من(انشاء نظام داخلي شامل للرقابة على المصارف والمؤسسات المالية وغيرها من التدابير).

- وما يتعلق بالمصادرة والضبط والتجميد في المادة (2) و(12) و(6) و(13) و(14) منها تسليم المجرمين في المادة (16) والمساعدات القانونية المتبادلة في المادة (18) وغيرها من المواد والتدريب والمساعدات التقنية في المواد (29) و (30) وغيرها".[2]

ثانيا: على المستوى العربي

كذلك هي الدول العربية سعت عل الدوام بالبحث عن كل السبل لمكافحة هذه الجريمة والتعاون الأمني على النطاق الإقليمي، ومن بين الجهود نذكر ما يلي:

أ. **الاتفاقية العربية المكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية لعام 1994**: وقعت هذه الاتفاقية في تونس عام 1994 من جانب وزراء الداخلية العرب، وتضمنت هذه الاتفاقية موادا بشأن مكافحة غسيل الأموال. ويلاحظ أن هذه الاتفاقية سلكت فج اتفاقية فيينا في مجال معالجتهما لظاهرة غسل الأموال نظرا لعدم وجود اختلاف بينهما[3].

ب. **مؤتمر التعاون الأمني عام 1996م** : "عقد هذا المؤتمر في تونس وحضره وزراء الداخلية في الدُّول الأعضاء ، من اجل تحقيق التنسيق الدولي والإقليمي لمنع وتعقب الجريمة ومصادرة العوائد المتحصلة منها ومكافحة غسل الأموال وتحقيق التعاون بين الانتربول في تسليم المجرمين وعدم استخدام الحسابات المصرفية السرية في إخفاء دخول تجارة المخدرات.

[1]- عبد الله عزت بركات ،ظاهرة غسيل الاموال و اثارها على الاقتصادية و الاجتماعية على المستوى العالمي ،مجلة اقتصاديات شمال افريقيا ،العدد الرابع،الجزائر2010،ص227

[2]- طايل كايد المجالي ،المرجع السابق،ص12.

[3]- عبد الله عزت بركات، المرجع السابق،ص229.

ج. **إعداد القانون العربي النموذجي الاسترشادي لمكافحة جرائم غسل الأموال** : الذي جاءت نصوصه في إطار ما تضمنته الصكوك والمواثيق الإقليمية الدولية ، بغية تعميميه على الدول العربية، للاسترشاد به في صياغة قوانين وطنية لمكافحة غسل الأموال ، او تطوير وتحديث التشريعات الوطنية ذات الصلة بمكافحة غسل الأموال"[1].

الفرع الثاني

الهيئات و الاجهزة

اولا: هيئة الأوروبول :

في 07 /02/ 1992تم توقيع إتفاقية " ماستراخت[2] " ، الّتي نصت على إنشاء "الاوروبول" ، أين تم توقيع إتفاقية إنشائها في عام 1995، و ذلك بهدف تحديد فاعلية التعاون الدولي بين الجهات المعنية فيما يتعلق بمكافحة الأنشطة الخطيرة للإجرام الدولي و من بين ذلك تبييض الأموال ، و تتدخل هيئة الإوروبول ّ في الجرائم التي تتعدى إقليم الدولة الواحدة إلى غيرها من الدول وتقوم بعمل أبحاث عن تلك النوعية من الجرائم ، وقد أسست الهيئة بنكا للمعلومات وتبادلها وتقدم الحلول الملائمة في التحقيقات الّتي تجرى فيما بين الدول الأعضاء في الإتحاد الأوروبي

ثانيا :انشاء مجموعة اجمونت 1995:

" في عام 1995 شكلت وحدات الاستخبارات المالية في الدول الأعضاء في لجنة "، FATF"منظمة تدعى "إيجموند جروب" ، وهي اتحاد لوحدات و أجهزة مكافحة تبييض الأموال في العالم ، وتضم في عضويتها أكثر من 69 وحدة لمكافحة تبييض الأموال"[3] .

ثالثا:الانتربول

" حيث تم انشاء إدارة متخصصة داخل هذا الجهاز الدولي، هدفها مكافحة غسل الأموال الناشئة عن ترويج المخدرات ، وذلك من خلال إقامة نظام مركزي لجمع المعلومات من الدول المختلفة من أجل استخدام أفضل لها"[1].

---

[1]- طايل كايد المجالي ،المرجع السابق، ص 15.

[2]- أبرمت معاهدة ماسترخت في 7فيفري 1992، ورغم أن المعاهدة لا تستهدف صراحة مشكلة غسيل الأموال، إلا أنها مع ذلك نصت على التعاون بين الأجهزة الداخلية في المجال الجمركي والشرطي وفي مجال مكافحة الإتجار بالمخدرات وغيرها من الجرائم الدولية الخطيرة.

[3]- خوجة جمال، المرجع السابق، ص 150.

[1]- طايل كايد المجالي، المرجع السابق، ص9.

رابعا: فريق العمل المالي الدولي (''FATF " Financial Action Task Force):

"وهي منظمة نشأت عن اجتماع الدول الصناعية السبع الكبرى في العالم، وفتحت هذه المنظمة عضويتها للدول الراغبة في الانضمام إليها وتهدف إلى مكافحة جريمة غسل الأموال وأنشأت لجان رقابية وبدأت تكشف عن بعض السلوكيات التي تقوم بها بعض العصابات المنظمة ولذي حظيت باهتمام الحكومات والمجالس التشريعية في العديد من دول العالم، ففي تقريرها الصادر سنة 2000م، كشفت عن قائمة بالدول التي لم تتعاون في مجال مكافحة غسل الأموال وعددها 15 دولة، كما قامت بإصدار 40 توصية لمكافحة جرائم غسل الأموال، من أهمها:

أ. تعديل نصوص قوانين السرية المصرفية على وجه يسهل ملاحقة غسل الأموال الملوثة.

ب. اتخاذ تدابير لمصادرة الأموال محل جريمة غسل الأموال.

ج. التزام المصارف بعدم فتح حسابات مجهولة الهوية أو بأسماء وهمية.

د. التزام المصارف بتجميد الحسابات التي تبلغها بها السلطات الرسمية وتحوم حولها الشبهات.

هـ. التشديد على مراقبة عمليات التحويلات المالية بين الدول.

و. تفعيل دور السلطات المعنية بالرقابة والملاحظة لهذه الجريمة خاصة البنوك المركزية والإنتربول من خلال استخدام التقنيات الحديثة لمواجهة تطور جريمة غسل الأموال"[1].

الفرع الثالث

مكافحة غسيل الاموال في الجزائر

و بهذا الصدد وتنفيذا للالتزامات الدولية الّتي انضمت إليها الجزائر تم إنشاء خلية معالجة الاستعلام المالي بموجب المرسوم التنفيذي رقم 127/02المؤرخ في 2002/04/07 الذي حدد هيكلها التنظيمي ووظائفها واختصاصاتها داخل وخارج الوطن ، لكن تم تنصيب هذه الخلية سنة 2004، "حيث نجد أن المشرع الجزائري جاء بمبدأ قانوني جديد بموجب القانون01/05[1] يتمثل في واجب الإخطار بالشبهة ، ويقصد به ضرورة تبليغ خلية معالجة الاستعلام المالي بكل عملية مهما كانت طبيعتها أي مالية أو مصرفية أو بيع أو شراء عقارات أو

[1]– مسعد عبدالرحمن زيدان ،المعالجة القانونية لجريمة غسل الأموال في ضوء أحكام القانون الدولي ،مجلة العربية للدراسات الامنية ،العدد 69 السعودية2017،ص ص:63-64.

[1]– المادة 19من القانون 01/05المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب و مكافحتهما.

منقولات... إلخ ، تثير شكوك بخصوص كونها تمت بأموال متحصل عليها من جناية أو جنحة وبالأخص الجرائم المنظمة .

فعلى الهيئات والأشخاص المختصين الّذين يعنيهم القانون كما ورد في أحكام الفقرة الأولى من المادة 4من المرسوم ، 127/02رفع تقارير كافة الأنشطة المشبوهة والبيانات الأخرى المطلوبة ، كتقارير المعاملات النقدية إلى خلية معالجة الاستعلام المالي"[1] ، التي فرضها على المؤسسات المالية و التي تعتبر الامكنة الاكثر نشاطا لجريمة غسيل الاموال و ذلك بوسائل محدد في قانون 01/05 منها الاخطار بالشبهة و التعرف على العملاء.

اما عن العقوبات و التقنينات فإن المشرع الجزائري لم يشر صراحة إلى جريمة تبييض الأموال، ولا إلى العقوبة المقررة لها إلى غاية صدور القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات حيث نص صراحة على إدراج جريمة تبييض الأموال ومعاقبة مقترفيها وهذا ضمن القسم المستحدث 06 مكرر من المادة 389 مكرر إلى 389 مكرر 7 حيث حدد المشرع الجزائري الأفعال المكونة بجريمة تبييض الأموال، وكذا العقوبات التي تلحق مرتكبيها.

المبحث الثاني

جريمة سرقة و تزوير البطاقات الائتمانية

ادى ظهور النقود الالكترونية الى استحداث عدة اساليب للتعامل مع هذه الظاهرة الحديثة و المتطورة مما ولد اختراعات كثيرة مثل الحسابات البنكية الالكترونية و البرقيات المالية وصولا الى ما يسمى بالبطاقات الائتمانية و التي سهلت الكثير عن اصحابها من حيث خفة حملها مقارنة بما كان يعانيه نقل الاموال و ايضا من حيث الامان و احتمالية السطو و السرقة ، غير ان كل هذا لم يمنع المجرمين و المحتالين من خلق اساليب للوصول الى تلك الاموال و من بين الاساليب المستعمل في سرقة النقود الالكترونية التي تحملها البطاقات الائتمانية السرقة و التزوير و التي سنبين معنى هذين الجريمتين (المطلب الاول) و ماهي اركانها التي تقام عليها مسؤولية السارق و المزور في البطاقة الائتمانية كما نذكر الاساليب المعتمدة في كلتا الجريمتين مع توضيح العلاقة الرابطة بين هذين الجريمتين الواقعتين على البطاقة الائتمانية و مدى وقوعهما (و وصول اثرهما) على النقود الالكترونية (المطلب الثالث) و هل تم خلق حلول لحماية هذا الحق و تكفل به القانون (المطلب الثالث) بذكر الجهود التي بذلتها الاوساط المتعاملة بالبطاقة الائتمانية لمكافحة جريمة السرقة و التزوير الواقع على البطاقة الائتمانية.

[1]- خوجة جمال، المرجع السابق، ص 132.

المطلب الاول

مفهوم جريمة سرقة و تزوير البطاقات الائتمانية

و للوصول لتعريف جريمتي السرقة و التزوير الواقع على البطاقة الائتمانية لابد منا ان نعرف مصطلح البطاقة الائتمانية لكي نفهم حدود الجريمتين من ناحية اركانها كون البطاقة الائتمانية عنصر حديث و متطور قد تختلف فيه اساليب ارتكاب الجريمتين عن الجرائم التقليدية الاخرى كل هذا نبينه في الفروع القادمة.

الفرع الاول

التعريف جريمة سرقة و تزوير البطاقة الائتمانية

ان الاختلاف الحاصل في التعاريف المتداولة لدى الفقهاء و كذلك لدى المشرعين استلزم علينا ان نعرف العناصر الثلاث من سرقة و تزوير و بطاقة ائتمانية لغةً و اصطلاحاً و تشريعاً في العناصر التالية:

اولا: التعريف اللغوي و الاصطلاحي و التشريعي للبطاقة الائتمانية

لابد لنا ان نعرف هذا المصطلح حتى نحدد المفهوم الحقيقي له بحيث نقوم بذلك لغة و اصطلاحا و تشريعا

1. التعريف اللغوي:

- **البطاقة:**" تعني الورقة، أو هي الرقعة الصغيرة من الورق أو غيره يكتب عليها بيان ما تعلق عليه"[1].
- **الائتمان:** على وزن افتعال وهو من الأمان والثقة.

2. التعريف الاصطلاحي:

"بطاقة خاصة، تصدرها مؤسسة مالية، تخول حاملها الحصول على السلع والخدمات والسحب النقدي دون أن يدفع المقابل حالاً، ويلتزم المصدِر للبطاقة بالدفع عن حاملها، والتحصيل منه فورياً بالخصم من حسابه أو آجلاً خلال مدة معينة".

وقد "ظهرت أول شركة متخصصة في إصدار البطاقات في سنة 1949م وهي شركة داينرز كلوب(DinersClub) وقد اقتصرت في البداية على إصدار بطاقة خاصة برواد المطاعم، ثم ظهرت كارت بلانش (Carte Blanch) و أمريكان اكسبرس(American Express) وفي سنة 1951م انتقلت عملية إصدار البطاقات إلى البنوك حيث بدأ بنك فرانكلين في نيويورك

(Franklin National Bank) بإصدار البطاقة، وفي نحو سنتين زاد عدد البنوك المصدرة البطاقات في الولايات المتحدة عن 100بنك.

[1]- ابن منظور، المرجع السابق، المجلد العاشر، ص:21

وكانت القفزة الكبرى في عالم بطاقات الائتمان عندما سمح بنك أمريكان Bank American للمصارف الأخرى ورخّص لها بإصدار البطاقة الائتمانية، مما جعل هذه البطاقة تتحرر من إقليميتها لتنتشر عبر العالم ، وصار أكثرها انتشاراً بطاقة Visa وبطاقة Master Card وفي عام 1970م ظهرت فكرة بطاقة الائتمان بمفهومها الربوي إذْ تؤدي هذه البطاقة قرضاً بفائدة ثابتة على رصيد البطاقة ، وانتشرت هذه البطاقة حتى تسابق الناس للحصول عليها وتضخمت أرباح الشركات المصدرة لها ".[1]

ومنها انواع كثيرة نذكر مثلا : بطاقة الحسم الفوري أو البطاقة المدينة Debit Card .وبطاقة الائتمان العادية أو بطاقة الحسم الآجل CHARGE CARD و بطاقة الائتمان المتجدد أو بطاقة الائتمان القرضية Credit Card With Revolving Credit وأشهرها هي: فيزا(VISA) وماستر كارد (Master Card) و أمريكان إكسبريس (American Express).

3. التعريف التشريعي:

من خلال نص المادة 543 مكرر 23 ق ت والمادة 69 من الأمر 11/03 المتعلق بالنقد والقرض المذكورة سابقا، نجد بأن المشرع الجزائري قد عرف بطاقات ووسائل الدفع بصفة عامة دون أن تختص وسيلة بطاقة الائتمان الإلكترونية بتعريف خاص، إلا أنه يستشف من نص المادة 69 أن المشرع في استعماله لعبارة مهما يكن السند أو الأسلوب التقني المستعمل قد اعتمد منهج الحياد أو التعادل التقني فاتحا المجال أمام ما يستجد من وسائل تكنولوجية حديثة ومنها بطاقة الائتمان الإلكترونية

ثانيا : التعريف اللغوي و الاصطلاحي و التشريعي للسرقة

وهو كذلك نقوم بتعريفه في التعريفات الثلاث

1. التعريف اللغوي:

" يُقالَ سَرَقَ بفتح الراءَ سَرَق منه الشيء ، ومنه يَسْرُقُ سرقاً فهو سَارِقٌ بكسر الراء ، والتسريق : النسبة إلى السرقة[1]" "واسترق السمع أي استرق مستخفياً ، يقال : هو يسارق النظر إليه إذا اهتبل غفلته لينظر إليه ، والاستراق : الختل سراً ،كالذي يستمع . ويقال لسارق الشعر سراقة ، ولسارق النظر إلى الغلمان : الشافن "[2].

[1]– إبراهيم محمد شاشو، بطاقة الائتمان حقيقتها وتكييفها الشرعي، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية ، المجلد السابع و العشرون ،العدد الثالث،سوريا2011 ،ص ص:655-656.

[1]–مجد الدين محمد بن يعقوب الفيروزأبادي، القاموس المحيط، مؤسسة الرسالة للطباعة و النشر،لبنان،2005، الطبعة الثامنة، ص 893.

[2]–ابن منظور، المرجع السابق، ص ص:155-156.

2. التعريف الاصطلاحي:

هو اخذ شيءٍ ملك للغير خلسةً او غصبًا

3. التعريف التشريعي:

لقد نص المشرع الجزائري على جريمة السرقة بموجب المادة **350**من قانون العقوبات الجزائري، حيث جاء فيا بأن: "كل من اختلس شيئا غير مملوك له يعد سارق."[1]

ثالثا : التعريف اللغوي و الاصطلاحي و التشريعي للبطاقة الائتمانية

مقسم كذلك تعريف هذا المصطلح الى تعريف لغوي و اصطلاحي و تشريعي

1. التعريف اللغوي:

"تزوير [مفرد]: مصدر زوَّرَ/ زوَّر على.

- زوَّرَ/ زوَّر على يزوّر، تزويرا، فهو مزوِّر، والمفعول مزوَّر.
- زوّر الكلام: كذب فيه، زخرفه وموهه "زوّر الشاهد ما وقع في الحادث".
- زوّر توقيع المدير: قلده و زَيَّفه بقصد الانتفاع به بغير حق "اكتشف تزويرا في المستندات- زوّر النقود."
- تزوير انتخابي: (قن) مجمل المخالفات المتعلقة بالترشيح ولوائح الانتخابات وعملية التصويت وعد الأصوات"[2].

2. التعريف الاصطلاحي:

يعرف التزوير على أنه تغيير الحقيقة في الاموال و الوثائق والسندات و المحررات الرسمية و غير الرسمية، بقصد الغش بالأساليب المحددة قانونا، والتي تلحق ضررا بالضحية.

3. التعريف التشريعي:

نص المشرع الجزائري على جريمة العقوبات في المواد من214 إلى229 غير انه لم يعطي تعريفا صريحا حيث حدد فقط الافعال التي تنشق عنها تغيير حقيقة الاشياء و مواضيع مثل بتقليد أو بتزييف ، باصطناع ، بإدراج ،بإضافة ، بإسقاط ، بتزييف و غيرها من المصطلحات في المواد السابقة الذكر.

[1]- أنظر المادة 350من القانون 01- 14المتضمن قانون العقوبات.

[2]-احمد مختار عمر و فريقه ،معجم اللغة العربية المعاصرة، عالم الكتاب للنشر و التوزيع و النشر،مصر،2008،الطبعة الاولى، ص 1009.

الفرع الثاني

اركان جريمة سرقة و تزوير بطاقات الائتمان

ولقيام المسؤولية الجزائية لأي جريمة لابد ان تقوم على اركانها الثلاث الركن المادي و المعنوي و الشرعي الذي يجرم الفعل و هذا ما نتناوله في العناصر الاتية:

أولا: جريمة سرقة بطاقة الائتمان أو رقمها السري

فالسرقة هناك تقع ايضا على سرقة رقمها السري ايضا دون اللجوء الاتصال المادي بالضحية عن طريق اختراقه بالقرصنة رغم انها تعتبر جريمة ذات طابع الكتروني على عكس سرقة البطاقة في حد ذاتها و لاتهمنا هنا غير انها تعتبر سرقة و سنتحدث عنها في العناصر القادمة وسنتكلم عنها بصفتها المادية ، وفيما يلي نستعرض مختلف أركان هذه الجريمة:

1. **الركن المادي** :"يتمثل الركن المادي لجريمة السرقة في فعل الاختلاس الذي يعرف على انه أخذ مال الغير دون رضا مالكه أو حائزه ، ومن هذا التعريف يتبين أن فعل الاختلاس يتكون من عناصر أساسية ، فالعنصر المادي يتمثل في الاستيلاء على الشيء المملوك للغير، وأما العنصر المعنوي فهو عدم رضا صاحب هذا الشيء على هذا الفعل المجرم، كذلك فيما يتعلق بمحل الجريمة فان فعل السرقة يقع على شيء مملوك للغير وتقع على المنقولات دون العقارات، و بطاقة الدفع تعتبر مال منقول ملك لحاملها لا يحق لغيره التصرف فيه.

2. **الركن المعنوي** :تقوم جريمة السرقة على القصد الجنائي العام و الخاص، فأما القصد الجنائي العام فهو العلم والإرادة، أي أن الجاني يعلم أن الشيء ملك للغير، والاستيلاء عليه فعل مجرم قانونا، ومع ذلك تتجه إرادته للقيام بهذا الفعل المجرم. و فيما يخص بطاقة الائتمان فالجاني يعلم أنها ملك لصاحبها ولا يجوز له التصرف فيها، وهذا الفعل يعد سرقة ومع ذلك تتجه إرادته لسرقتها .

وأما القصد الجنائي الخاص يقصد به نية التملك، ولكن مع تطور القضاء أصبح لا يؤخذ به كشرط لقيام جريمة السرقة، وإنما تقوم بمجرد الاستيلاء على الشيء واستخدامه. وبالتطبيق على بطاقة الدفع الالكتروني فإن جريمة السرقة تقوم بمجرد استيلاء الغير عليها، مع علم هذا الأخير بأن هذا الفعل يعد جريمة يعاقب عليها القانون، حتى ولو لم تكن نيته تملكها، والدفع بذلك يعد باطلا."[1]

[1]-خولة بوقديرة، الجرائم الواقعة على بطاقات الدفع الالكتروني، مذكرة ماستر، جامعة ام البواقي، الجزائر، السنة الجامعية2017-2018،ص38.

3. **الركن الشرعي:** نصت عليه المادة 350من قانون العقوبات وما يليها[1]، تتضمن العقوبات المقررة لجريمة السرقة.

اما عن جريمة سرقة الرقم السري للبطاقة عندما يقوم الفاعل بسرقة الرقم السري للبطاقة الائتمانية، حيث يستطيع الحصول عليه واستخدامه في السحب او التحويل ،ومن بين أهم عوامل الحصول عليه نذكر **إهمال صاحبها** نتيجة تدوين الرقم السري على وجه البطاقة ، وتركها عرضة لنظر الغير الذي يتمكن من معرفته بكل سهولة، كذلك قد يقوم حاملها بتكرار الرقم السري على مسمع أو أنظار الغير أثناء قيامه بعملية سحب النقود امام السحابات الآلية و هذا يسمى **التجسس** ، و كل هذا نتيجة لعدم اخذ الحذر اللازم ، و للذكر اساليب السرقة الاخرى تعتمد على التكنولوجيات و القرصنة و الاختراقات سواءًا على الاجهزة الخاصة الكمبيوترات المنزلية او الاجهزة العامة مثل المصارف و الشركات المالية المصدرة للبطاقات.

ثانيا: جريمة تزوير البطاقة الائتمانية

1. **الركن المادي:** هي كل الافعال التي ذكرتها المواد من 214 و ما يليها من قانون العقوبات[2]، و التي تضفي الى تغيير الحقيقة الظاهرية او الباطنية او الفعلية مع وجوب أن يقع التزوير على المحررات التي تشكل سندات بما في ذلك المحررات العمومية و الرسمية و العرفية، وكذلك المحررات التجارية والمصرفية .أو في بعض الوثائق الإدارية، غير ان الملاحظ في بعض البحوث التي تتحدث عن كون البطاقة محرر ام لا فالغالب ان الصفات التي تجمع المحررات تتصف بها البطاقة الائتمانية كحملها لمعلومات خاصة بصاحبها و لها قيمة مالية و تصدر جهات رسمية او معترف بها و هذا ما اتجه اليه بالإجماع كل الباحثين في هذا الامر كون التزوير الذي يقع على البطاقة يدخل ضمن تزوير المحررات والسندات الرسمية، يضاف الى ذلك وجود ضرر مادي و معنوي ولا يشترط ان يمس المضرور مباشرة بل يكفي ان يكون محتمل الوقوع ويكون في البطاقات الائتمانية على الجهة مصدرة البطاقة دون احتساب المساس بحقوق المصدرة له او صاحب البطاقة .

2. **الركن المعنوي** :جريمة التزوير من الجرائم العمدية التي تستوجب القصد الجنائي العام والخاص معا كالآتي:

–القصد الجنائي العام :ويقصد به العلم و الإرادة، وذلك أن تتجه إرادة الجاني إلى تغيير الحقيقة مع علمه أن هذا التغيير فعل مجرم قانونا، يترتب عليه ضرر محتمل، أو وقع بالفعل اما عن **القصد الجنائي الخاص** يقوم

[1] – المواد من 350الى371مكرر من قانون العقوبات الجزائري.

[2] – المواد 214 الى 229 من قانون العقوبات الجزائري.

باتجاه نية الجاني لاستعمال المحرر فيما زور من أجله، أو دفع مضرة عن الغير أو عن نفسه و في البطاقة الائتمانية يكون من اجله أي لسحب المال او تحويله.

3. **الركن الشرعي**: نص المشرع الجزائري على عقوبة جريمة التزوير في المحررات التجارية أو المصرفية أو الشروع فيها، بموجب نص المادة 219من قانون العقوبات، هذا عن العقوبة الأصلية، اضافة الى العقوبات التكميلية[1] الواردة في نفس القانون.

الفرع الثالث

اساليب السرقة و انواع التزوير للبطاقات الائتمانية

قد تتشابه الجرائم مع بعضها البعض في كثير من النواحي غير انها قد تختلف في الاساليب و التي تفرضها عليها المواضيع المستهدفة و من ذلك فان اساليب السرقة و التزوير في الجرائم التقليدية تختلف عن الواقعة على البطاقة الائتمانية لهذا سنفرقها بالعناصر الاتية:

اولا السرقة:

قد تستعمل اساليب عدة و من عدة اطراف قد تشترك فيما بينها او من طرف واحد فقد يشترك السارق مع احد موظفي البنوك المصدرة للبطاقات و قد يعتمد السارق على نفسه سنذكرها في النقاط الاتية :

1. **الاشتراك في السرقة** : بالنسبة لموظف البنك او المؤسسات المالية المصدرة للبطاقات بان يقدم بيانات تساعد في سرقة ما تحمله البطاقة من نقود الكترونية او المساعدة في تقليد و اصطناع بطاقة تساعد على ذلك مما يجعلها اسلوب للسرقة و التزوير معا.

2. **التجسس**: وهو الاسلوب المعتمد لدى غالبية السارقين حيث يتمركزون بجانب السحابات الالية لغرض التقاط اي معلومة سواءا سمعا او بصرا لأي ارقام سريا او ارقام تعريفية للبطاقات الائتمانية لاستعمالها في المعاملات المالية كالتحويل الالكتروني او الشراء من الانترنت.

3. **السرقة المباشرة**: اما ان تكون خلسة عن طريق النشل او غصبا عن طريق الاعتراض بالأسلحة و قطع الطريق او نشلها بالقوة .

4. **السرقة غير المباشرة**: و التي تاتي بعد ان يتم سرقة البطاقة و فك تشفيرها و سرقة ما فيها من نقود الكترونية و رميها او سرقة المعلومات التي تحتويها قصد استعمالها في بطاقة اخرى مرة اخرى.

[1] – المنصوص عليها في المادة 09 من قانون العقوبات الجزائري.

ويوجد ايضا اساليب تقنية تكنولوجية للسرقة مثل مواقع الكترونية مفخخة للايهام الضحايا و سرقة مفاتيحهم السرية و ارقام التعاريف لبطاقات التي قد تكتب على تلك المواقع .

ثانيا التزوير: صنف خبراء الكشف عن التزوير أساليبه إلى أسلوبين: التزوير الكلي للبطاقة و الجزئي لها:

1. "**التزوير الكلي** : يتم التزوير الكلي عن طريق اصطناع البطاقة بالكامل وذلك بتقليد ما عليها من نقوش وعلامات وكتابة وحروف وشريط ممغنط وتوقيع حامل البطاقة.

وهذا النوع من التزوير يسميه البعض بالتقليد – تفريق بينه وبين التزوير – باعتبار أن التقليد هو تزوير كلي للبطاقة ، والتزوير هو تقليد جزئ للبطاقة ويقصد بالتقليد – بصفة عامة – صناعة شئ على غرار شئ آخر .

وفي مجال بطاقات الائتمان يقصد بالتقليد صناعة بطاقة سحب أو بطاقة وفاء على غرار بطاقة أخرى وهذا النوع من التزوير يقل في جانب النوع الذي قبله ، حيث إنه يتطلب نوعا خاصة من الآلات المصنعة له ، ورجال مهرة في تصنيع مثل هذا النوع من البطاقات ولذا فانه في الغالب تقوم بمثل هذه الأعمال منظمات وعصابات عالمية تتنوع في مسرح الجريمة مثال ذلك: تلك القضية التي جرت أحداثها بين هونج كونج وتايوان ، وتتخلص وقائعها في قيام عصابة إجرامية اتخذت لنفسها مصنعا لصناعة البلاستيك في منطقة المدينة Taipel، ومتابعة أفراد العصابة وجد أنهم بدأوا بشراء التجهيزات المادية اللازمة الإنتاج البطاقة وهي: الشريط الممغنط وآلة التصوير وآلة طباعة الشبكة الحريرية وما يتوافق معها من أحبار وآلة طباعة الحروف الفاخرة ، وآلة لتشفير البيانات على الشريط الممغنط ، وآلة تغليف البطاقة ، وقد كان أفراد العصابة يقومون بنقل هذه البيانات إلى البطاقات المصطنعة تقليدا لنظائرها الصحيحة ، ثم يبيعون هذه البطاقات المقلدة إلى منظمات إجرامية أخرى لترويجها واستخدامها في اليابان وتايوان وهونج كونج نظير مبالغ عالية".[1]

2. **التزوير الجزئي** :" يتحقق بالعبث في بعض البيانات التي تتضمنها البطاقة ، كما في حالة نزع الشريط الممغنط الخاص بالحامل الأصلي ووضع الشريط الممغنط الخاص بالجاني

و هذا النوع من التزوير هو الأكثر انتشارا في ساحة جريمة تزوير بطاقات الائتمان، ويتم ذلك بطريق التقليد باستخدام بيانات صحيحة لبطاقات سليمة لشخص حقيقي، ويحصل عليها المزورون بطرق عديدة منها:

[1]– فهد بن عبد الله بن علي العرفج، جريمة تزوير بطاقات الائتمان وعقوبتها دراسة مقارنة، رسالة ماجستير، المعهد العالي للقضاء جامعة الإمام محمد بن سعود الإسلامية، السعودية، السنة الجامعية2007-2008،ص ص:72-73.

أ- من خلال نسخ الكوبون المتخلفة عن الاستعمال الصحيح للبطاقات لدى التجار، بعد تخلص هؤلاء التجار منها بإلقائها في سلال المهملات.

ب- من خلال بيانات بطاقة صحيحة يتم الحصول عليها بتصويرها فوتوغرافيا بواسطة التاجر، مثل أصحاب المطاعم الذين يقومون باستعمال بطاقات العملاء بعيدا عن أعينهم – أو باستعمال جهاز الفيديو مثل ما حدث فعلا من قيام أحد الجناة بتصوير بطاقة وفاء صحيحة استدل بها مقدم برنامج تلفزيون حول نظام الوفاء بالبطاقات.

ج- النصب باستخدام بطاقات الدفع ، حيث يقوم الجان بتقديم أوراق أو مستندات منسوبة إلى الغير مع البطاقة المزورة، وذلك لإيهام التاجر بأنه الحامل الشرعي لها وبذلك يتسنى للجاني الحصول منه على ما يريد من السلع الخدمات".[1]

و للاضافة فان التزوير يعتمد على وسائل وادوات لا باس ان نذكر منها :

-جهاز المسح(scanner) -قارئ بطاقات lecteur carte خاص بالبطاقة الائتمانية -جهاز الطبع بحروف نافرة او البارزة- طابعة بطاقات.

المطلب الثاني

علاقة البطاقة الائتمانية بالنقود الالكترونية

ان البطاقة الائتمانية كاداة حديثة النشأة استحدثت للقيام ببعض العمليات التي ترتبط ارتباطا وطيدا بالتطور السريع الحاصل في الحياة الاقتصادية التي حركت ماكينة التكنولوجي لتغطية هذه السرعة سهل طردا حركة النقود الالكترونية بين المتعاملين الاقتصاديين ، فان اي تغير او مساس بهذه الاداة يمس النقود الالكترونية حتما و بهذا وجب علينا اظهار هذه العلاقة العكسية بين النقود الالكترونية و البطاقة الائتمانية في الفروع التالية :

الفرع الاول

البطاقة الائتمانية وسيلة دفع

يتبين بالإجماع في الكثير من التعاريف التي ظهرت عن العديد من الفقهاء و الباحثين في عنصر البطاقة الائتمانية على انها اداة وفاء حاملة للنقود الكترونية ذان قيمة مالية مدعومة من مصدريها ، و من بين هذه التعاريف نذكر "أداة مصرفية للوفاء بالالتزامات مقبولة على نطاق واسع محلية ودولية لدى الأفراد والتجار كبديل

[1]- فهد بن عبد الله بن علي العرفج ،المرجع السابق، ص ص:70-71.

للنقود لدفع قيم السلع والخدمات المقدمة لحامل البطاقة مقابل توقيعه على إيصال بقيمة التزامه الناشئ عن شرائه للسلعة أو حصوله على الخدمة على أن يقوم القابل بتحصيل القيمة من البنك المصدر للبطاقة عن طريق البنك الذي صرح له بقبول البطاقة كوسيلة دفع، ويطلق على عملية التسوية بين البنوك الأطراف فيها اسم نظام الدفع الالكتروني والذي تقوم بتنفيذه المنظمات العالمية الراعية للبطاقة".[1]

" فعندما يريد حامل البطاقة الحصول على نقود أو سلعة أو خدمة فإنه يبرز بطاقته أمام التاجر أو المصرف ، ثم يأخذها التاجر أو المصرف ليتأكد من صحة المعلومات المتعلقة بالبطاقة وتاريخ انتهاء صلاحيتها، ثم يتم تسجيل رقم البطاقة على قسيمة تبين الخدمة أو السلعة التي قدمت لصاحب البطاقة وتاريخ تقديمها ليوقع عليها.

ثم يقوم البائع بتقديم هذه القسيمة إلى الجهة المصدرة للبطاقة أو أحد فروعها، ليحصل على المبلغ المذكور في القسيمة، وبعد التأكد من صحة البيانات المقدمة من طرف البائع يصبح المصرف ملزم بدفع المبلغ المذكور للتاجر، وذلك بغض النظر عما إذا كان لحامل البطاقة رصيد في المصرف يماثل المبلغ المدفوع أم لا.

وبعد ذلك يرسل مصدر البطاقة أو المصرف إلى حامل البطاقة فاتورة بقيمة الخدمات أو المشتريات التي تحصل عليها والتي قام المصرف بتسديد قيمتها نيابة عنه أو من حسابه في المصرف"[2]، اما عن طريق المصرف او ماكينات الصرف تكون العملية مباشرة .

الفرع الثاني

البطاقات الائتمانية وعاء للنقود الالكترونية

و لتحديد معنى ان تكون البطاقات الائتمانية وعاء للنقود الالكترونية فان التعريفات الاصطلاحية و التقنية و حتى القانونية قد وضحت بإطناب هذا المعنى و نذكر منها :

" وهي البطاقات البلاستيكية والمغناطيسية التي تصدرها البنوك لعملائها للتعامل بها بدلا من حمل النقود، واشهرها الفيزا (Visa) والماستر كارت (Master Card)وامريكان اكسبرس (Express American) وتكون هذه البطاقات مدفوعة القيمة المالية سلفا ومخزنة فيها .....حيث يقوم المستخدم سلفا بدفع مقدار من النقود التي يتم تمثيلها بصيغة الكترونية رقمية على البطاقة الذكية وعندما يقوم المستخدم بعملية شراء سواء أكان ذلك عبر الانترنت ام في متجر تقليدي يتم خصم قيمة المشتريات وهنالك العديد من منتجات النقود الالكترونية التي يمكن اعادة تحميلها بقيمة مالية عن طريق ايداع نقود في البنك او عن طريق اي حركة مالية اخرى ملائمة"[1].

---

[1]- فهد بن عبد الله بن علي العرفج، المرجع السابق ، ص18.

[2]-ابراهيم محمد شاشو، المرجع السابق، ص 660.

[1]- نهى خالد عيسى الموسري وإسراء خضير مظلوم الشميري، المرجع السابق، ص 270.

وفي تقرير له عرف البنك المركزي الأوروبي سنة 1998بما يمكن تسميته بالنقود الإلكترونية على " أنها مخزن إلكتروني للقيمة النقدية على جهاز تقني يمكن استخدامه على نطاق واسع لإجراء مدفوعات إلى تعهدات غير الجهة المصدرة دون ان تنطوي بالضرورة على حسابات مصرفية في المعاملة ، ولكنها تعمل كأداة لحامل الدفع المسبق.

ركز تقرير عام 1994 تحليله على البطاقة المدفوعة مسبقًا متعددة الأغراض أو "المحفظة الإلكترونية" التي تم تعريفها على أنها بطاقة بلاستيكية تحتوي على قوة شرائية حقيقية ، والتي دفعها العميل مقدمًا (منتجات قائمة على البطاقات)".[1]

كل هذا يدل تقنيا او عمليا ان البطاقة الائتمانية بكل اشكالها و ميزاتها تحمل قيمة مالية ذات صيغة الكترونية اما عن التعاريف القانونية للبطاقة الائتمانية نذكر ما عرفه المشرع الجزائري في :

تنص المادة 543مكرر 23من القانون التجاري: " تعتبر بطاقة الدفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أمواله " [2].

كما نصت م 69في الأمر 03-11المتعلق بالنقد والقرض على أنه " تعتبر وسائل الدفع كل الأدوات التي تمكن من تحويل أموال مهما يكن السند أو الأسلوب التقني المستعمل " [1].

كما ان خصائصها المذكورة في المادتين أعلاه المالية من معاملات و تحويلات و خصومات و سحوبات اكبر دليل على انها متعلقة بعنصر المال و النقود الالكترونية ، و الفنية و الشكلية و التقنية في كونها وحدة تخزين و شكلها ميزاتها التقنية اللذان يستعملان في السحابات الالية و قارئات الكروت التي تستعمل في المحلات من اجل ايفاء المبالغ و خصمها تبين بصورة واضحة ان البطاقة اداة ايصال و نقل للنقود بصيغتها الالكترونية .

الفرع الثالث

النقود الالكترونية محل جرائم البطاقات الائتمانية

ان ارتباط جرائم البطاقة الائتمانية بالنقود الالكترونية ظاهر جليا في نية مرتكبي هاته الجرائم وغايتهم من ارتكابها غير انه وجب علينا ربط العلاقة بين البطاقة و النقود الالكترونية بتوضيح ما يميز هذه الجرائم عن غيرها

[1]– البنك المركزي الاوروبي ، تقرير حول النقود الالكترونية ،المانيا 1998،ص 7 .

[2]– الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 75- 59 في 20رمضان 1395الموافق لـ 27سبتمبر 1975بالمرسوم التشريعي رقم 93-08المؤرخ في 25-04-1993، المتضمن القانون التجاري المعدل والمتمم، الجريدة الرسمية عدد27 ،الصادر في 27 أفريل 1993.

[1]– الجمهورية الجزائرية الديمقراطية الشعبية، أمر رقم 03 / 11 المؤرخ في 27 جمادى الثانية عام1424، الموافق لـ 26-06-2003، المتعلق بالنقد والقرض، الجريدة الرسمية عدد 52.

وصولا الى النقود الالكترونية كنتيجة اخيرة عنها و هذا تبعا لما يميز البطاقة الائتمانية تتطابق مع خصائص النقود الالكترونية تطابق تاما يجعل كل اسقاطات اركان تلك الجرائم تمس كل خاصية من خصائص النقود الالكترونية و سنوضحها في النقاط الاتية :

1. جريمة السرقة : فحسب نص المادة 350من قانون العقوبات الجزائري، حيث جاء فيها بأن: "كل من اختلس شيئا غير مملوك له يعد سارق"[1].

و اسقاط كل ما ذكر فيها على البطاقة الائتمانية فأنها ملك لحاملها دون غيره ، فإن أحكام هذه الجريمة تطبق على من قام بهذا الفعل ، "فالركن المادي لجريمة السرقة يقوم على فعل الاختلاس كنشاط إجرامي يؤدي إلى حيازة السارق للشيء محل السرقة من حيازة صاحبه الشرعي إلى حيازته بدون علم و رضا صاحب البطاقة و لان البطاقة تحمل تلك المعلومات الخاصة من اسم و رقم حساب حاملها و ما الى ذلك من تلك الامور الشخصية فإنها ملك له فقط دون غيره فالغير الذي يختلسها هنا يعد سارقا ، بالرجوع إلى نص المادة يجب أن تقع السرقة على مال منقول مملوك للغير و منه لكي تقوم جريمة السرقة يجب أن تتوفر شروط الاتية و هي :

- أن يكون محل السرقة مالا: و البطاقة الائتمانية تعتبر مالا مخزنة داخلها و قد صنفت حسب القوانين و التعاريف الفقهية انها مال مخزن و منقول
- أن يكون محل السرقة مالا منقول: و هذه خاصية البطاقة انها اداة نقل للاموال و ذات قيمة مالية .
- أن يكون محل السرقة مالا مملوك للغير: و هذا ما تحمله البطاقة في داخلها من مال يخص صاحبها او من اصدرت لأجله كونها شخصية."[1]

2. جريمة التزوير: كما ورد سابقا فان تصنيف البطاقة الائتمانية مستندا او محررا قابلا للتزوير فانها تدخل ضمن الافعال المجرمة قانونا حسب المادتين 219و220 من قانون العقوبات ، وعليه فإن أي مساس بتلك البيانات يشكل الركن المادي لجريمة التزوير سواءا ظاهريا او جوهريا للبطاقة ،كأن يعمد الجاني إلى تغيير النقوش التي تحملها أو التلاعب في الأرقام المكتوبة عليها أو عن تقليدها، حيث يكفي أن يكون التقليد يشبه البطاقة الاصلية ويجعلها مقبولة للتعامل نتيجة توصل المقلد إلى سحب أموال و القيام بالعلميات التي تقوم بها البطاقة الاصلية وصولا الى المال المنشود لارتكاب هذا الجرم بطرق تكنولوجية تخول المقلدين بإيجاد الارقام السرية للبطاقة و جعل البطاقة المقلدة تعمل عمل الاصلية .

---

[1] – الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم66-156مؤرخ في 18صفر،1386الموافق ل 8يونيو 1966، المتضمن قانون العقوبات ،الجريدة الرسمية عدد49،مؤرخة في 11جوان1966معدل ومتتم.

[1] – كميت طالب بغدادي ، الاستخدام غير المشروع لبطاقة الائتمان (المسؤولية الجزائية والمدنية)، دار الثقافة للنشر و التوزيع، الاردن، ط1، 2008، ص ص:190-191.

و بهذا فان القول بان محل الجرائم الواقعة على البطاقة الائتمانية هو النقود الالكترونية او القيمة المالية ذات الطبيعة الالكترونية التي تحملها البطاقات مهما وقعت عليها أي جريمة باي شكل او اسلوب كونها تتطابق مع بخصائصها مع النقود الالكترونية و أي مساس بها يهدف الى المساس بالنقود التي تحملها.

المطلب الثالث

الجهود و الاليات الدولية لمكافحة جريمة سرقة و تزوير البطاقة الائتمانية

و كأي جريمة من الجرائم التي تقع على الاشخاص او الاموال وجب ان تتحرك لها كل الاطراف و الجهات من هيئات و مؤسسات و دول بمكافحة هذه الجرائم فان جريمتي السرقة و التزوير كذلك تم قيام مجموعة من الجهود لمكافحتهما بكل الطرق الفنية العملية التي تقوم بها الهيئات التي لها احتكاك مباشر بالبطاقة الائتمانية و الطرق القانونية التي تحمي و تنظم البطاقة من صدورها وصولا الى استعمالها و مجموعة التعاملات التي تنتج عن استعمالها و كل ذلك في سبيل الحد منهما و محاولة مكافحتهما و نذكر منها :

الفرع الاول

الجهود الدولية و الوطنية في الاتفاقيات و القوانين

و بتأثير هذه السلوكيات الاجرامية تحركت الدول جماعيا و فرديا ،فظهرت العديد من الجهود نذكر منها :

اولا : الجهود الدولية:

مما لا شك فيه ان جميع الدول تعاني ايضا من هذه الجرائم مما اطرها الى التحرك السريعة لمكافحتها و الحد منها كونها تمس المصالح الخاصة و المشتركة للدول و من بين الجهود الدولية نذكر:

1. الاوروبول

في 07 /02 /1992تم توقيع إتفاقية " ماستراخت[1] " ، الّتي نصت على إنشاء "الاوروبول" ، أين تم توقيع إتفاقية إنشائها في عام 1995، و ذلك بهدف تحديد فاعلية التعاون الدولي بين الجهات المعنية.

"ومن التطبيقات العملية للتعاون الدولي في هذا المجال، عملية أوديسيوس : التي تمت في 26 فبراير 2004 بمبادرة من يوروبول ، وقامت قوات الشرطة خلالها بعمليات شملت 10 دول وهي (أستراليا ، بلجيكا، كندا ، ألمانيا، هولندا، النرويج ، بيرو، إسبانيا، السويد، بريطانيا).

[1]– أبرمت معاهدة ماسترخت في 7فيفري 1992، نصت على التعاون بين الأجهزة الداخلية في المجال الجمركي والشرطي وفي مجال مكافحة الإتجار بالمخدرات وغيرها من الجرائم الدولية الخطيرة .

وتعتبر ملفات التحليل المبلغة من قبل سلطات التحقيق التابعة للدول الأطراف في الإتحاد الأوروبي في جرائم الإعتداء على بطاقات الائتمان ، أحد أهم الوسائل التي يعتمد عليها المحققين في مكافحتهم للشبكات الإجرامية، كما أن من التطبيقات العملية للتعاون الدولي من ذلك النوع من الجرائم أطلق عليه (عملية محطم الجليد Icebreaker) التي قامت بها يوروبول(Europol) في 14 يونيو 2005 حيث تم من خلالها مداهمة وتفتيش شبكات الحاسب الآلي في ثلاث عشرة دولة أوروبية وهي النمسا، بلجيكا، فرنسا، ألمانيا، المجر، أيسلندا، إيطاليا، هولندا ،بولونيا، البرتغال، سلوفاكيا، السويد، بريطانيا العظمى، كما تم توقيف أفراد من كل من فرنسا، المجر، أيسلندا و السويد"[1].

2. الانتربول:

ساعد هذا الجهاز كذلك على الحد من مجموع الجرائم الواقعة على البطاقات الائتمانية من حيث انها اصبحت ذات طبيعة دولية حيث اختصت بعض منظمات بتزوير و تقليد البطاقات الائتمانية مما حرك هذا الجهاز على نحو تلقائي لمحاولة الكشف و مكافحة هذه الجريمة و التي اتسمت بالتنظيم و الدولية مما تحرك اختصاص هذا الجهاز .

كما ان هناك مجموع اتفاقيات ساهمت بشكل ولو غير مباشر في مكافحة جريمتي التزوير و السرقة للبطاقة الالكترونية و التي تمس جانبها الالكتروني حيث شملت منها اتفاقية بودابيست التي ساهمت في مكافحة السرقات الالكترونية التي تساعد في تقليد ماهو مسروق من ارقام و مفاتيح لخلق بطاقات مزورة بالتكاثف الدولي بين الدول الاعضاء او بدخول دولة ليست عضوا و نذكر ايضا اتفاقية باليرمو التي ساهمت في التعاون الدولي في كثير من المجال التي مست ايضا هذا المجال الاجرامي و كذا "الاوروجست و هو جهاز يوجد على المستوى الأوروبي يساعد على التعاون القضائي والشرطي في مواجهة مكافحة جميع أنواع الجرائم الخطيرة للانترنت.

وتنعقد اختصاصاته عندما يمس ذلك الإجرام دولتين على الأقل من أعضاء الإتحاد الأوروبي أو دولة عضو مع دولة من دول العالم الثالث أو دولة عضو مع الرابطة الأوروبية وهي في ذلك غير مقتصرة على الأشخاص فقط إنما تشمل كذلك المؤسسات ، وتؤدي مؤسسة الأوروجست عملها بالتنسيق مع الأوربول ،حيث يزودها

[1]– بن تركي ليلى، الحماية الجنائية لبطاقة الائتمان الممغنطة، رسالة دكتوراه تخصص قانون العقوبات و العلوم الجنائية، كلية الحقوق جامعة منتوري قسنطينة، الجزائر، 2017، ص:329

بالتحليلات اللازمة للقيام بالتحقيقات في الجرائم المنظمة "[1].

ثانيا : الجهود الوطنية

نذكر بعض التشريعات التي ساعدت على حماية البطاقة الائتمانية اما بقوانين خاصة لحماية هذه الاداة من الضرر او قوانين عامة ، في مضامينها ذكرت صراحة مصطلح البطاقة الائتمانية وبين من صنفها ضمن المستندات و المحررات و الاساليب التقنية :

1. موقف المشرع الفرنسي:

يمكن القول أن فرنسي هي السباق فيما يخص انشاء قانون جزائي خاص بالبطاقة الائتمانية هو " قانون أمن الشيكات وبطاقات الوفاء " والذي يعتبر أول قانون جزائي خاص يتناول الأفعال غير المشروعة المرتكبة بواسطة البطاقة ، ويتضمن مكافحتها بالعقوبة الرادعة، بحيث ذكر المشرع الفرنسي صراحة فعل التزوير أو التقليد للبطاقة وكذا في حال استعمال هذه البطاقة المزورة وذلك بتوافر علم الجاني بتزويرها أو تقليدها، حيث "نص المشرع الفرنسي على حماية جنائية خاصة لبطاقات الائتمان بموجب القانون رقم 91 لسنة 1991 بنص المادة 67 /2 وذلك بالنص (على معاقبة كل من زيف أو عدل أحد بطاقات السداد و كل من استخدم أو حاول استخدام بطاقة سداد أو بطاقة مدنية ثم تزييفها أو تعديلها وهو على علم بذلك. كذلك كل ما من اتفق على استلام مستحقاته عن طريق بطاقة سداد تم تزييفها أو تعديلها مع علمه بذلك) "[1].

2. موقف المشرع المصري

بخصوص المشرع المصري جاء خالية من أية نصوص تعاقب على هذه السلوكات غير المشروعة، و اعتمد العقوبات الموجودة في القانون العام في المواد التي تنص على جرائم السرقة والتزوير دون تخصيص أي قانون ينفرد بالجرائم التي قد تمس البطاقة الائتمانية.

ثالثا: موقف المشرع الجزائري

مما تتسم به الجزائر انها السباقة عربيا في سد الفراغ القانوني في بعض المجالات الذي يقع فيه القضاء أثناء طرح هذه الجرائم للفصل فيها، وهذا من خلال التعديلات الاخيرة في قانون العقوبات إلا أن هذا التعديل الذي طرحه

[1] – بن تركي ليلى، المرجع السابق،ص330.

[1] – فيصل بن عادل ابو خلف، الحماية الجنائية لبطاقات الائتمان، رسالة ماجستير في العدالة الجنائية، كلية الدراسات العليا جامعة نايف، السعودية،2008،ص 144.

المشرع الجزائري ليس ملما بكافة الأجزاء، وجاء بصفة التعميم أي لم يخصص لكل نوع من الجريمة ما يقابلها من جزاء هذا ما يستوجب الإسراع في إعداد قانون خاص بالجرائم الماسة ببطاقات الائتمانية والتي أغفلها المشرع الجزائري في هذا التعديل.

كما تضمن الأمر 03-11 المتعلق بالنقد والقرض أول قانون جزائري تضمن التعامل الالكتروني الحديث في القطاع المصرفي ويتضح ذلك في المادة 69 منه " تعتبر وسائل الدفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكن السند أو الأسلوب التقني المستعمل"[1]، أي ان جريمة التزوير الواقعة على البطاقات الائتمانية تدخل ضمن القانون العام و التي تعاقب عليها مواد التزوير بشكل عام (في المواد 219 الى 221 من ق ع) كونها كما صرحت المادة السابقة محرر او سند ولكن بأسلوب تقني تكنولوجي ، كما ننوه على عملية السرقة ايضا بطبيعتها المادية كذلك تطبق عليها مبادئ القانون العام اما بخصوص السرقة الالكترونية للبطاقة عن طريق الولوج الى الكمبيوترات الشخصية و البنوك و سرقت الارقام السرية و معلومات التي تسمح بسرقة محتوى بالطاقة من نقود الكترونية فقد ادرجت ضمن قسم خاص(394 من ق ع) و الذي سنأتي بشرحه في العناصر القادمة .

الفرع الثاني

الجهود الفنية و الادارية لمكافحة الجرائم الواقعة على البطاقة الائتمانية

و بسبب كثرة الاطراف بين المعاملات التي تستوجب البطاقة المرور بها لكي تقوم بعملها فان الجهود يجب ان تتكاثف بين هاته الاطراف بطريقة او بأخرى اما عن طريق الاتصال ببعضها او تطوير مستوى الوعي الكامل بمجريات خلق تلك البطاقات وطرق التعامل معها و بها وبهذا فان كل من المؤسسات المصدرة للبطاقات و المتعاملين بها و اصحابها يجب ان يقوموا بعدة اجراءات و حلول قد تساعد في مكافحة مثل هذه الجرائم و نذكر منها بالنسبة لـ:

اولا: بالنسبة للمؤسسات المصدرة للبطاقات : و اغبلها البنوك ثم تليها المؤسسات المالية المعتمدة من قبل الدول المنشاة بها تلك المؤسسات و كمثال نذكر مؤسسة فيزا visa و ماستر كارد Master card الى خلق مجموعة من الحلول الفنية التي تصعب عمليات التزوير و بالتالي عمليات السرقة ايضا تكون صعبة و ايضا بما قامت به البنوك من اجراءات صارمة حول عمليات انشاء الحسابات و الاجراءات العملية لأي عملية مثل

[1] –للاطلاع اكثر انظر للمادة 69 من قانون الصرف وال نقد رقم 11/03المؤرخ في 26-06-2003.

استعمال **اسلوب الحماية الثنائي** او المصادقة[1] عن طريق الرسائل االقصيرة SMS لتاكيد الدخول او التحويل بين الارصدة ، و من بين احدث الانظمة المضافة لخدمة الحساب الالكتروني البريدي اضاف بريد الجزائر خدمة التحويل بين الارصدة في شهر ماي 2019 [2]و هي ما قد يزيد من خطورة جريمة سرقة و تزوير البطاقات كون امكانية السارق او المزور من تحويل الاموال الى ارصدة و حسابات اخرى فقد اقتصرت الخدمة التي اطلقها بريد الجزائر على تطبيق هاتفي و بطاقة الذهبية ، مما يجعل من تقنية او آلية المصادقة هي الأضمن حمايةً و احسنها التي يستقبل فيها العميل رسالة قصيرة SMS على هاتفه لتأكيد التحويل او الدخول مما يصعب فعلا اي تحويل كان دون ان يقوم به صاحب الرصيد حماية له من الاستيلاء و السطو على موالة ، و كذا السرعة في تجميد الحسابات في حالات التبليغ التي تصدر عن اصحاب البطاقات او أي خطأ فني في السحابات الالية لاحتمال تلاعب شخص اخر غير صاحبها و الكثير من الاجراءات التي ساهمت كثيرا في الحد من انتشار جرائم التزوير و السرقة و من بين اشهر الحلول التوجه الى البطاقة الذكية و التي تقوم بتخليق ارقام سرية جديدة في عملية شراء مما قد يصعب الامور امام عمليات السرقة و التزوير التلقائي لأي بطاقة ، كما ان تركيب الكاميرات امام السحابات الالية تساعد ايضا عمليات السحب بالبطاقة المزورة اثناء التبليغ بفقدان المبالغ المالية او من خلال عمليات السحب البطاقات المسروقة و العمل على التعاون بين المؤسسات يساعد ايضا في حالات التحويلات التي قد تمس المتضررين من هاته الجرائم عن طريق تحويلات اموالهم .

ثانيا: بالنسبة المتعاملين الاقتصاديين: كما هو متعارف ان التعامل بالبطاقة الائتمانية يكون عبر تقديمها في حالة القيام بعملية شراء او تسوق لأي حامل لها امام تاجر او من يقدم الخدمة ، فان اهمية وعي المتعاملين او مقدمي الخدمات كذلك يساعد في مكافحة الجرائم الواقعة على البطاقات الائتمانية مثل التفطن الى الشكل الخارجي للبطاقة او التفطن الى برمجيات التي قد تظهر اثناء عملية تحريك البطاقة في قارئ البطاقة او عدم تطابق البيانات الخارجية للبيانات الداخلية للبطاقة فان دور التجار او مقدمي الخدمة تكون بالتبليغ او التحفظ على البطاقة مع استعمال أي اسلوب يكشف الفاعلين، و كذلك عدم قبول أي تعامل ببطاقات لم تكن في حوزة

[1]–**المصادقة** Authentification : **او الترخيص** هي عبارة عن كلمات مفتاحية خاصة او رسائل بريدية او رسائل قصيرة SMS عبر الهواتف المحمول لتأكيد هوية القائم بعمليات الدخول او الولوج الى الانظمة او الشبكات بارسالها الى صاحب الحساب في بريده الالكتروني او هاتفه الشخصي او الظهور امامه مباشرة في حالات الكلمات المفتاحية و تسمى ايضا بالحماية "ثنائية الخطوة security second step" و تكون اما بارسال كود متكون من حروف او مجموع ارقام و هي تمنع بطريقة احسن فكرة الاختراق او التلاعب بالحسابات و الانظمة

[2]– اطلق بريد الجزائر خدمة التحويل بين الارصدة في شهر ماي 2019 عبر ارسال رسائل تؤكد الخدمة الى ارقام هواتف زبائن شركة موبيليس تحت عنوان "حوالتك" و ذلك يوم 24-05-2019.

اصحابها ، التنبه لحجم التعاملات التي تثير شبهات و غيرها من الامور التي يجب ان يكونوا على ادراك بها و واعين بانها تساعدهم ايضا في ضمان التعاملات الجيدة و المضمونة .

ثالثا: بالنسبة لحاملي او اصحاب البطاقات:

ان اصحاب البطاقات لهم كذلك دور في عملية مكافحة جرائم السرقة و التزوير فالوعي الكامل بان اعين المترصدين و المتربصين امام السحابات الالية و كذلك عدم الكشف عن الارقام السرية او التلفظ بها بصوت عالي اثناء عملية السحب او كتابتها في البطاقة يحد لو بشكل لا باس به من هذه الجرائم او اظهار البطاقة بشكل واضح امام العلن مما يساعد على نقل مجموع الارقام التعريفية المنقوشة فيها و الكثير الكثير من السلوكات الطائشة التي تساهم في عملية اما تزور البطاقة او سرقة معلوماتها او بالتشجيع على سرقتها .

و نضيف ايضا ان سرعة التبليغ و عدم الاهمال اثناء وقوع صاحب البطاقة لأي جريمة خصوصا السرقة او فقدان مبالغ من الحسابات يساعد بشكل كبير في سرعة التعامل مع الجريمة بشكل يفتح مجال الردع ضد أي جريمة قد تمس صاحبها و حساباته المالية ، فالتنبه و الحذر و التبليغ يعتبران هما ايضا اسلوبين ممزين للحد من جريمتي التزوير و السرقة كما ان هناك اساليب اخرى اقل تأثيرا عن الاسلوبين السابقين و هما استعمال الارقام السرية المعقدة التي تحول دون استعمال البطاقات المسروقة دون حسبان عمليات تشفيرها و ادخال الرقم برمجيا غير انها تساعد ولو بشكل ضئيل بالتشويش امام عمليات السرقة العادية و تدحض أي عملية سحب محتملة.

و رغم ذلك فان الجهود الوطنية و الدولية لا تمنع من انتشار الجرائم التي تمس البطاقات الائتمانية كون هذه الاخيرة تعتمد اعتمادا واضحا على التكنولوجيا و التي خلقت معوقات امام الكثير من الدول و الهيئات و المؤسسات المالية كون الجريمة ايضا تتطور تبعا لمقتضيات ظروفها و مدى تعطش المجرمين الى ارتكاب الافعال التي تجلب الربح فانه و من هنا وجب التطوير المستمر لكل الجوانب المحيطة بسيرورة التعامل بالبطاقات من بداية بنائها الى غاية انتهاء صلاحيتها او الغاء التعامل بها و ذلك ضمانا للتعاملات الجيدة بين اطراف التي خلق لأجلها هذه البطاقة لتسهل التعامل فيما بينها و ضمان سيرورة الحياة الاجتماعية والاقتصادية على السواء.

خاتمة الفصل:

لقد تطرقنا في هذا الفصل إلى الجرائم التي تقع على النقود الإلكترونية ، من غسيل للأموال وما ساعد هذه الجريمة من خصائص تتميز بها هذا النوع من النقود كما اسهمت ظهور النقود الالكترونية الافتراضية بتوسيع محل جريمة غسيل الاموال ، كون هذه النقود الافتراضية لا ترتكز على الدعائم القانونية غير ان قابلية التعامل بها و قيمتها المالية فتح مجال لا رقابة لهذه الجريمة، وكما تطرقنا لسرقة و تزوير البطاقة الائتمانية باعتبارها اداة ووسيلة من وسائل التعامل بالنقود الالكترونية كمحالة منا بإيضاح الافعال الاجرامية التي تقع على هذه الاداة موضحين الاساليب المعتمدة على سبيل المثال لا الحصر ، كل هذا ايضاحا الى ان الطبيعة الرقمية للنقود الالكترونية بكل انواعها لا تمنع وصول الجريمة اليها كما لا تمنع وجود حلول قانونية و فنية لمكافحة هذه الجرائم التي استحدثت اساليب تواكب تطور تكنولوجيا الرقمنة المالية قصد السلب و الاستيلاء و هذا ما تطرقنا اليه في الجهود التي وجدت دوليا واقليميا و وطنيا من اتفاقيات و مواثيق و تشريعات ظهرت كنتيجة لذلك ، و استخلاصا لما ذكرناه في الفصل السابق ان طبيعة النقود الالكترونية سهلت ظهور عدة انواع من الجرائم صنفت على طبيعتين ماديا و تم ذكر امثلة عنها في الفصل السابق و جرائم الكترونية من نفس طبيعة النقود الالكترونية و هذا ما سنتناوله في (الفصل الثاني).

الفصل الثاني

صور الجرائم الواقعة على النقود الالكترونية ذات الطبيعة الإلكترونية

تمهيد:

ان سير التطور التكنولوجي الذي نتجت عنه تحويل النقود الورقية الى نقود الكترونية و ظهورها مس بطريقة سلبية الاساليب الاجرامية التي كانت تقع على التقليدية منها قبل ولادة الشكل الجديد للنقود ، و من الجرائم الحديثة التي انتشرت هي **القرصنة** (المبحث الاول)و التي وجدت النقود الالكترونية احد ابرز اهدافها و اسهلها ، حيث اصبحت هذه الجريمة جريمة قائمة بذاتها تعتمد على اساليب معينة و تقوم كغيرها من الجرائم على الاركان الثلاث المميزة لها ، فالقرصنة لا تختلف اختلافا كبيرا عن التقليدية منها(قرصنة السفن) الا بالأسلوب و الطبيعة ، هناك جريمة هي اخرى تعتبر تطورا حقيقيا و هي **الاحتيال الالكتروني** (المبحث الثاني)كونه يعتمد اعتمادا اساسيا على تغيير الحقيقة كجريمة متطورة عن نظيره التقليدي و هي الاحتيال التقليدي غير انه يعتبر ذا طبيعة الكترونية رغم كونه يعتمد على الخداع و الكذب ، هتين الجريمتين يعتبران من نفس طبيعة النقود الالكترونية مما وجب علينا دراستهما على سبيل المثال لا الحصر و قد تكون هناك جرائم اخرى و لكن هذه اشهرها و اكثرها انتشارا.

المبحث الاول

جريمة القرصنة الالكترونية

و كون جريمة القرصنة من السلوكيات الاجرامية التي لاح بها التطور التكنولوجي و التي ظهرت في بظهور الكمبيوتر و انتشار الانترنت وتكنولوجيا السمعي بصري مما فتح المجال امام الاطماع الاجرامية بالتوجه الى هذا المجال للحصول على الارباح السهلة والسريعة وكون ظهور النقود الالكترونية في فترات هذا التطور و انها لم تسلم ايضا من هذه الجريمة ، فقد اختلفت الاراء حول المعنى الحقيقي للقرصنة بعد هذه التطورات بعدما كانت مقتصرة على السفن البحرية و بهذا وجب علينا في دراستنا هذه ان نحدد المعنى الحقيقي للقرصنة (المطلب الاول) و ان نميزها و نذكر اركانها ،كما نرى مدى تأثيرها و علاقتها بالنقود الالكترونية (المطلب الثاني) ، و ردود فعل الافراد و الدول مما سببته هذه الظاهرة و الحلول التي انتجتها لمكافحتها و الحد من انتشارها (المطلب الثالث) كل هذا سنسرد في العناصر القادمة.

المطلب الاول

مفهوم جريمة القرصنة الالكترونية

ان انحصار مصطلح القرصنة في بداية ظهورها كان في السطو على السفن و مع التطور الحاصل على العديد من الاصعدة ظهرت سلوكيات صنفت قرصنة كالسطو على الطائرات و غيرها مما غير منظور الكثير حول معنى القرصنة مما اضطرنا الى البحث عن التعاريف و تحديد مميزات هذه الجريمة بالتغير الحاصل عليها و اساليب التي تستعمل في ارتكابها لكي نفرق بينها و بين اي جريمة من هذا النوع

الفرع الاول

التعريف بجريمة القرصنة الالكترونية

و من مقتضيات البحث ان نعرف المصطلحات لغة و اصطلاحا حتى نستطيع الاحاطة بجوانب الموضوع و من هنا نقسم التعريف الى:

اولا: التعريف اللغوي

قَرْصَنَ يُقَرْصِنُ قُرْصَنًا فهو مُقَرصِنْ ، قَرْصَنَ فلان: 1- قام بأعمال سلب بحري، 2- حول اتجاه سفينة او طائرة لغرض اقتصادي او سياسي " زادت قرصنة الطائرات في العصر الحديث".

قُرصَان [مفرد]: ج قَرَاصِنَة و قَرَاصِنٌ و قَرَاصِينٌ.

قَرْصَنَة[مفرد] :1-مصدر قَرصَنَ،2- سَطو على حقوق الملكية الفكرية او الادبية او الفنية "قَرصنَة حقوق المؤلفين- القرصنة في مجال التسجيلات الموسيقية".[1]

ثانيا: التعريف الاصطلاحي

ان الحديث عن القرصنة تعدى ان يكون في المجال البحري و الجوي بالسطو على ما تحمله السفن و الطائرات بالتدريج تزامنا مع التطور الحاصل على مستوى حياة الانسان فقد اتجه الى الاعتداء على الملكيات الفكرية و الادبية بعد انتشار التكنولوجيا التي تسمح بالتوسع دون الاحتكاك المباشر ، وعموما بعد هذا التطور انتشرت القرصنة التي تحولت الى قرصنة الكترونية فلم تعد محصورة على السرقة التي طالت التسجيلات الموسيقية بالنسخ و التوزيع دون اخذ التصريحات من اصحابها او دون اخذ اذنهم بل تعدت ذلك ايضا بظهور الانترنت حيث اصبح الولوج الى الشبكات الكبرى لعدة اهداف منها التخريبية و الربحية و التجسيسية و غيرها .

و هذا ما يهمنا هنا هو القرصنة الالكترونية او ما تسمى بـ "(الهاكينج Hacking) ليست مقصورة على اقتحام الشبكة بل حتى الحاسوب الشخصي وما يحمله قرصه الصلب الخاص من معلومات قد يكون عرضة للقرصنة فمن خلال الشبكة يمكن للقراصنة الدخول إلى أي حاسوب لا تتوفر فيه الحماية المطلوبة ومن ثم سرقة المعلومات منه بنسخها ومن ثم لصقها أو تخزينها على أقراص مضغوطة وأكثر الحواسيب عرضة لهذا النوع من القرصنة تلك التي تستخدم لأغراض عسكرية أو لغايات مصرفية في البنوك والمصارف العامة والخاصة إذ يستطيع قرصان الحاسوب أن يدخل إلى مجلدات القرص الصلب وان يفتح الملفات وبالتالي يتمكن من تحويل مبالغ مالية من حساب مصرفي إلى أخر دون الحاجة إلى قناع ومسدس وتهديد وقتل"[2].

[1]-احمد مختار عمر و فريقه، نفس المرجع، ص 1798.

[2]- زياد خلف عبد الله الجبوري، محمد شطب عيدان المجمعي، القرصنة التكنولوجية و اثرها على العلاقات الامريكية-الصينية، مجلة جماعة تكريت للعلوم الانسانية،المجلد15، العدد التاسع،العراق2008،ص 431.

ثالثا: التعريف الفقهي

"يشير مفهوم القرصنة الإلكترونية إلى ممارسات غير مشروعة على شبكات الحاسب الآلي، تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيّا.

ويقوم بهذه الممارسات قراصنة معلومات محترفون، أو شركات متنافسة ضد بعضها البعض، أو فيما بين موظفي المنشأة الواحدة؛ حيث قدرت بعض الدراسات الحديثة أن 85% من عمليات اختراق برامج الحاسب الآلي تتم من خلال موظفي الشركات"[1].

"وقد عرفها الفقه الأمريكي بأنها "الجريمة المرتبطة بالتكنولوجيا والكمبيوتر والإنترنت ، ومن أشهر تلك الجرائم الواقعة على الحكومات ومسئولي الصناعة والمواطن حول العالم وتتضمن الآتي:

– الإختراق (cracking):هو عبارة عن الدخول الغير مصرح به لأنظمة الكمبيوتر لإرتكاب جريمة، مثل إختراق أكواد لتشغيل البرامج المؤمنة بدون الكود السرى أو الرخصة السارية، أو إختراق المواقع الإلكترونية وبذلك يتم حرمان المستخدمين الشرعيين من الخدمات الخاصة بتلك المواقع ، محو أو إفساد المعلومات إلى جانب تشويه مواقع إلكترونية.

– الإختراق التليفونى (phreaking):ويتم ذلك من خلال إستخدام الكمبيوتر أو أي جهاز آخر للتحايل على نظام اتصالات للحصول على مكالمات مجانية دون وجه حق أو إلصاقها بحساب شخص أخر.

– الملاحق (cyberstalking):ويحدث ذلك من خلال ملاحقة وإرهاب أشخاص بعينهم أو مؤسسات بعينها من خلال الكمبيوتر مسبباً لهم الخوف من إلحاق الضرر لهم "[2].

ومن الظاهر ان القرصنة الالكترونية دائما ما تقترن بمصطلح الاختراق أي الدخول او الولوج الى كمبيوترات او المواقع او الشبكات بقيام الفاعلين(القراصنة او الهاكرز) بذلك دون اذن اصحابها مما يجعل فعلهم غير قانوني و مجرم.

[1]– تعريف الاكاديمية العربية البريطانية للتعليم العالي للاستطلاع اكثر انظر الى :
www.abahe.uk/information-technology-enc/71102-piracy.html. اخر زيارة للموقع :13-05-2019 بتوقيت 2:01.

[2]–محمد فرج عبد العزيز ابو ريشة ، جرائم الانترنت ،www.aboudreisha-law.com/**جرائم–الانترنت** ،اخر زيارة للموقع :13-05-2019 بتوقيت 2:20.

الفرع الثاني

اركان جريمة القرصنة الالكترونية

و ككل الجرائم فان جريمة القرصنة هي ايضا لها ركن مادي و معنوي و شرعي نفصلها في النقاط الاتية:

أولا: الركن المادي

و القاعدة العامة في الأفعال المجرمة هي إما القيام بفعل أو الامتناع عن فعل بحيث جاءت التعريفات السابقة كون القرصنة هي القيام بفعل او الامتناع عن فعل يقع على الحواسيب أو الأنظمة عموما و بعموم المفاهيم لأي نظام أو شبكة لا تسمح بالدخول دون إذن ، و بما ان القرصنة دائما ما تقترن بالولوج و الدخول الى شبكات و كمبيوترات دون إذن صاحبها دون احتساب الأفعال الأخرى كالتخريب و السطو و سرقة المعلومات و التعديل عليها و اعتبار هذا الفعل مجرم و غير قانوني فان القيام بالولوج أو الدخول إلى الأنظمة و الشبكات دون تصريح من صاحبها حتى و لم يمس أي شيء من النظام فان هذا الفعل في حد ذاته مجرم .

و هذا ما وقع فيه الاختلاف لدى بعض التشريعات حيث أن بعضها يجرم البقاء فقط بعد الولوج داخل النظام أو الشبكة و البعض الآخر يجرم مجرد الدخول كون انتشار برامج الحماية اكبر دليل على نية الفاعل الإجرامية و كون خصوصية هذه الأنظمة و الشبكات لا تسمح بالدخول و لأي كان إلا بالتصريح و هذا ذهب إليه المشرع الجزائري في المادة 394 مكرر بقول "يدخل **أو** يبقى"[1] فالدخول يكفي لتجريم الفاعل بل ذهب إلى تجريم المحاولة فقط و الشروع في ذلك ، و كذلك المساعدة على تسهيل عمليات القرصنة مجرمة أيضا و يكون ذلك بإفشاء الثغرات أو إعطاء البرامج التي تساهم في الهجمات وهذا ما صرح به المشرع في المادة 394 مكرر05 ، إما بخصوص الامتناع عن فعل فان عدم التبليغ عن فعل القرصنة أو الامتناع عن المساعدة لردع هذه الجريمة مجرم كذلك في القواعد العامة كونه يمس الأشخاص في أموالهم أو ممتلكاتهم ولكن ليس مصرح به صراحة .

ثانيا: الركن المعنوي

إن أي جريمة تقع أو متوقعة الحدوث ليست كيانا ماديا فحسب بل وجب ان تقوم على كيان نفسي ايضا يدفع أي فعل للحدوث و كذلك هي جريمة القرصنة فان الأفعال التي تتأتى عنها و التي تتصف بالإجرامية لابد ان تقوم على النية الإجرامية و القصد الجنائي الذي يبعثها الى الوجود مع علمه بإجرامية فعله و توجه ارادته لارتكابه و القصد الجنائي ينقسم الى القصد الجنائي العام و القصد الجنائي الخاص ، فعن القصد الجنائي العام

[1]- انظر قانون العقوبات الجزائري من المادة 394مكرر الى 394 مكرر07.

يقوم على علم ان هذا الفعل مجرم و مع ذلك تتجه نيته الاجرامية الى فعله و اما عن القصد الجنائي الخاص فانه الهدف من قيامه بالفعل و الغرض منه كونه يعلم بان السلوك مجرم و معاقبا عليه و قد اختلفت هنا التشريعات ايضا في هذه النقطة بحيث صرحت مجموعة منها ان تجريم الا بتوافر القصد الجنائي الخاص لكي تحمل مسؤولية و هذا ما تجه اليه المشرع الفرنسي حيث اعتمد على تواجد القصدين معا.

ومثال ذلك جريمة السرقة من البريد الالكتروني او الكمبيوتر كون السرقة في حد ذاتها تعتبر فعل مجرم بمجرد علم الجاني بذلك و اتجاه إرادته اليها قد وفر القصد الجنائي الخاص و هنا لا يكفي بل يجب ان يتوفر ايضا عنصر القصد الجنائي الخاص و المتمثل هنا في عنصر التملك للمعلومة المسروقة من البريد او الكمبيوتر، اما عن المشرع الجزائري و الذي اعتبر ان القصد الجنائي العام كاف لتحميل المسؤولية الجزائية للفاعل كون العلم بان الفعل مجرم مع ذلك اتجاهه له يعتبر دليلا كافيا لترتيبه المسؤولية ، و بالنظر الى التطور الحاصل على مستوى انظمة و برامج الحماية و خصوصية الشبكات التي قد تصبح احيانا مغلقة دون اتصال بالأنترنت يعتبر اي فعل من افعال القرصنة يعتبر هنا مجرما صراحة كون عنصر الخصوصية هو الغالب .

وبالنظر الى اغلب التشريعات و اسقاطا على التطورات التكنولوجية و الأضرار التي وقعت فمجرد الولوج فقط او محاولة ذلك كما صرح المشرع الجزائري (394مكرر" أو يحاول ذلك")ترتب مسؤولية جزائية يعاقب عليها القانون دون النظر الى نية فاعليها.

ثالثا: الركن الشرعي

فلابد لكي يكون الفعل فعلا مجرما ان تصفه مادة او يدرج في قانون خاص او تعقد من اجله اتفاقية و في اغلب التشريعات و الاتفاقيات فيمكن القول ان هذه الجريمة كغيرها من الجرائم جرمت كونها تمس الأمن و الحياة الخاصة و العامة للأفراد و المجتمعات بسوء استعمال الاجهزة او الولوج و الدخول او الاعتراض غر القانوني كما جاءت به –على سبيل المثال لا الحصر– دوليا على ذلك التوصية رقم 89(9) المتعلقة بالجرائم المرتبطة بالحاسب الآلي[1] التي أصدرها المجلس الأوربي والاتفاقية التي تخص الإجرام المعلوماتية أو السيبيري الموقعة في نوفمبر سنة 2001 ببودابست ، ودخلت حيز التنفيذ في جويلية سنة 2004 ، وصادقت عليها بعض أعضاء المجلس الأوربي بالإضافة إلى كندا واليابان والولايات المتحدة الأمريكية وجنوب إفريقيا حيث جعل منها وثيقة دولية ملزمة بالنسبة للدول الأطراف فيها، كما ذكرنا سابقا فان القرصنة دائما ما تنطبق على فعل الدخول او الاختراق او

[1]– المجلس الاوروبي ، التقرير التفصيلي لاتفاقية بودابيست، فرنسا، 23نوفمبر2001، ص4.

الولوج الى الشبكة او الكمبيوترات بدون تصريح وان هذا الفعل في حد ذاته مجرم و هذا فعلا ما صرح به المشرع الجزائري في جرائم المساس بأنظمة المعالجة الآلية (م 394 مكرر إلى المادة 394 مكرر 7 من قانون العقوبات) ، و بإسقاط القاعدة العامة للركن المادي لأي جريمة على المصرح به المشرع الجزائري يمكن القول بالقرصنة هي كل فعل أو الامتناع عن فعل يمس نظام المعالجة الآلية، ولهذا صنفت القرصنة كجزء من الجرائم الالكترونية.

الفرع الثالث

خصائص و أساليب جريمة القرصنة الالكترونية

إن جريمة القرصنة كغيرها من الجرائم تتصف بخصائص قد تميزها عن الجرائم الأخرى و كذا باعتمادها أساليب معينة تجعلها تختلف اختلافا كبيرا عن بقية الأفعال المجرمة المعروفة لهذا وجب علينا أن نشرحها في العناصر الآتية:

أولا :خصائص جريمة القرصنة الالكترونية

لعل ابزر الخصائص التي تتسم بها جريمة القرصنة نذكر الآتي:

1. **دولية عابرة للحدود** : "من أهم الخصائص التي تميّز الجريمة الإلكترونية، أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الانترنت و تقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، بسبب السرعة الهائلة في تنفيذها، يمكن أن تقع الجريمة من طرف الجاني في دولة والمجني عليه في دولة أخرى في وقت يسير جّدا.

هذه الطبيعة التي تتمّيز بها الجريمة الإلكترونية أدت إلى خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول القانون الواجب تطبيقه، بالإضافة إلى إشكاليات تتعلّق بإجراءات الملاحقة القضائية، وغيرها من المشاكل التي تثيرها الجرائم العابرة للحدود بشكل عام"[1].

2. **جريمة ناعمة**: و التي تتسم بعدم الاحتكاك الجسدي او المادي بين الجاني و الضحية فهي تستعمل التكنولوجية و الأجهزة التقنية و أسلحة ازرار لوحة المفاتيح مما لا يولد أي اتصال مباشر بين الطرفين، وهذا يصعب عملية إثبات او معرفة مرتكبيها.

3. **صعبة الإثبات** : و كما سبق الذكر تعتبر من الجرائم التي لا يحتك الجاني فيها بالضحية وبالتالي فهي من الجرائم النظيفة التي لا أثر فيها للعنف فهي مجرد عمليات تغيير أو تخريب للأرقام والبيانات الإلكترونية المخزنة في

[1]- باطلي غنية، الجريمة الإلكترونية "دارسة مقارنة"، الدار الجزائرية للنشر و التوزيع، الجزائر، 2015، ص ص:49- 50.

الكمبيوترات او السرقات والتحويلات المالية وليس لها أية آثار مادية خارجية ، مما يصعب عملية تقفي الجاني، وما تحتاجه هذه العملية من فحص لكمٍّ هائل من الوثائق والبيانات والمعلومات المخزّنة. هذا بالإضافة إلى سهولة محو دليل الجريمة بسرعة قبل اكتشاف أمر الفاعل مما يجعل من عملية كشف القرصنة أمراً في غاية الصعوبة، وكذا قدرة القراصنة على حماية أنفسهم باتخاذ التدابير الأمنية الواقية التي تزيد صعوبة عمليات البحث عن الأدلة المؤدية إلى إدانتهم وذلك باستخدامهم لكلمات المرور صعبة جدا و معقدة ،تشفيرات لا يمكن لأي حواسيب عادية القيام بفكها او التمويه بتغيير اماكن اتصالهم عن طريق برامج التمويه الشبكي التي تجعل تقفي اثر او مكان اتصال الجاني المحترف صعبا جدا، كل هذا كون مسرح الجريمة غير مادي و ملموسة بدون أي اثر لفعل يربطه بصاحبه.

4. مرتكبوها ذوو صفات خاصة[1] : ان القيام بعمليات الولوج مع تطورات برامج الحماية و أنظمتها العالية و انتشار ثقافة الامن السيبراني لدى الكثير من المؤسسات و الاشخاص ليس من السهل القيام باي عملية قرصنة او هجمة الكترونية ان يقوم بها شخص عادي فلابد ان يكون له خلفية تقنية و علمية كافية للقيام بذلك فالقرصنة تعتمد على العديد من العلوم نذكر منها علم التشفير و الرياضيات و اللغات الاجنبية و لغات البرمجة و معرفة عالية بأدوات الاتصال و اجهزتها لهذا يتسم اغلب القراصنة بالذكاء و الكفاءة العالية في هذا المجال.

ثانيا : اساليب جريمة القرصنة الالكترونية:

لقيام أي جريمة لابد لها ان تعتمد على اساليب و ادوات لكي تسير كما سطر لها و من بين اشهر اساليب البرمجيات الخبيثة او عن طريق برامج الفحص الشبكي و التي نفصلها في النقاط الاتية :

أ. "**الفيروسات هي** إحدى أنواع البرامج الآلية، إلا أن الأوامر المكتوبة في هذه البرامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته. في برامج قد تم تصميمها لإلحاق الضرر بنظام الحاسب، عن طريق ربط نفسه بالبرامج الأخرى، وكذلك القدرة على إعادة تكرار نفسه؛ بحيث يتوالد ويتكاثر؛ مما يتيح له فرصة الانتشار داخل جهاز الحاسب في أكثر من مكان في الذاكرة؛ ليدمر البرامج والبيانات الموجودة في ذاكرة الجهاز. وتكمن خطورة الإصابة بالفيروس في أنه يؤدي إلى تعطيل عمل البرامج أو تقليل سرعتها، أو إصابة الجزء الخاص بتشغيل جهاز الكمبيوتر، مما يؤدي إلى إيقاف عمل الجهاز. أو قد يؤدي الفيروس إلى مسح منطقة جدول التقسيم، وهو ذلك

[1]– نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، ليبيا، - 25 24مارس 2017 ،ص7.

الفهرس الذي يحتوي على أسماء الملفات وأماكن وجودها على القرص الصلب"[1]، وليس بالضرورة ان تقوم بالتدمير فالفيروسات عموما تعمل على ما برمجت لأجله قد يكون للكشف عن الثغرات تحضيرا لهجومات او السطو و نقل المعلومات او التجسس فقط و تتعدد فيروسات حسب مبرمجيها كذلك و اهدافهم و تتنوع وهي كثيرا نذكر مثلا الدودة الحاسوبية و حصان طروادة و غيرها من البرامج الخبيثة.

- **"دودة الحاسوب (Computer Worm)** :وهي برامج حاسوب خبيثة صغيرة قائمة بذاتها قادرة على استنساخ برمجيتها من أجل الانتشار إلى حواسيب أخرى، وعادة تستخدم شبكة حاسوب لنشر نفسها معتمدة على أخطاء أمنية في الحاسوب المستهدف للوصول إليه.

وعلى عكس فيروس الحاسوب، لا تحتاج الدودة لأن ترفق نفسها ببرنامج موجود كي تنتشر. وهي تسبب عادة بعض الضرر للشبكة حتى لو كان ذلك باستهلاك عرض النطاق الترددي، في حين أن الفيروسات تعمل دائما تقريبا على إفساد أو تعديل الملفات المستهدفة.

- **حصان طروادة (Trojan Horse)** :وهي شفرة برمجية صغيرة، وهي ليست فيروسا أو دودة حاسوب، لأنها لا تكرر ذاتها على النظام المحلي أو عبر شبكة الحاسوب، وإنما يتم إرفاقها مثلا برسالة بريد إلكتروني أو مع برنامج ذي شعبية عالية، وتقوم ببعض المهام الخفية لمنح المخترق حقوقا مميزة على النظام، في حين تتنكر كأنها برنامج سليم.

بمعنى آخر، تفتح شفرة حصان طروادة "بابا خلفيا" في الحواسيب المستهدفة لتحولها إلى مسرح للمتسللين الذين يسعون للحصول على وصول غير مصرح به إلى الجهاز المستهدف، أي اختراقه، بهدف سرقة البيانات أو حذفها أو إرسال رسائل بريد إلكتروني باسم المستخدم أو حتى السيطرة على الشبكة بأكملها.

- **بوتنت (Botnet)** :وهي كلمة مركبة من "روبوت" و"نتوورك"، وتعني بالتالي "روبوت الشبكة"، وهي إحدى أبرز الوسائل المستخدمة في هجمات الحرمان من الخدمة الموزعة.

و"بوتنت" عبارة عن مجموعة البرمجيات الخبيثة المتصلة بالإنترنت التي تتواصل مع برامج أخرى شبيهة، بهدف أداء مهام معينة، وقد تكون المهمة عادية مثل التحكم بقناة الدردشة على الإنترنت (IRC)، أو خبيثة مثل

[1]-لتيم فتيحة- لتيم نادية، الامن المعلوماتي للحكومة الالكترونية و ارهاب القرصنة، مجلة المفكر، الجزائر2015، العدد12، ص245.

استخدامها لإرسال بريد إلكتروني غير مرغوب فيه (سبام)، أو المشاركة في هجمات الحرمان من الخدمة الموزعة، لكنها عادة ما ترمز إلى الجانب الخبيث"[1].

ب. كل هذه تعتبر برامج خبيثة الاشهر في القرصنة اضافة الى برامج الفحص Scanner و مكسرات كلمات السر للشبكات (Password Crackers)[2] و هي عدة برامج قد تاتي مع اجهزة قوي في معالجاتها من اجل اختراق شبكة مستهدفة.

اضافة الى كل ما سبق نشير الى ان القراصنة يعتمدون اعتمادا كبيرا على الماديات مثل الاجهزة المتطورة المتمثلة في الحواسيب الخارقة لعمليات التشفير السريعة و اجهزة الفحص التلقائي المدمج معها مكسرات مفاتيح الشبكات التي تعمل تلقائيا على فك شفرة شبكات الاتصالات الداخلية او المغلقة سواءا سلكيا او لا سلكيا مع وجود طبعا للأجهزة بث و استقبال قوي و بعيدة المدى و الكثير الكثير من الطرق و التي يستعملها و يعرفها الخبراء المحترفون في هذا المجال .

المطلب الثاني

علاقة جريمة القرصنة الالكترونية بالنقود الالكترونية

كون أي جريمة وقعت او مفترضة الوقوع كان لزاما ان تمس او تستهدف شيئا معينا تقع عليه وما ندرسه في بحثنا هذا المتعلقة بالنقود الالكترونية مجموعة الجرائم الواقعة عليها وجب علينا ربط العلاقة الموجودة بين القرصنة و النقود الالكترونية و التي قد تستهدفها هذه الجريمة وبذلك سنفصلها في الفروع التالية:

الفرع الاول

القرصنة الالكترونية و النقود الالكترونية من بيئة واحدة

ان الكثير ممن يستعلمون الفضاء السيبراني من انترنت و برامج شبكية او وسائل التكنولوجيا عموما يعلمون جيدا ان هذا المجال ذو طبيعة غير ملموسة بمعنى اخر طبيعته تقنية غير مادية الا في اجهزتها و ان وجوده افتراضي فهذا الميدان او البيئة الافتراضية هي المكان الذي تلتقي فيه كل من جريمة القرصنة و النقود الالكترونية و اللتان

[1] – شبكة قدس الاخبارية، البرمجيات الخبيثة و اساليب،www.qudsn.co/post/58085 /البرمجيات-الخبيثة-وأساليب-القرصنة ،اخر زيارة للموقع :15-05-2019 بتوقيت 21:51.

[2] – ادوات القرصنة Hacking tools انظر للموقع :http://www.insecure.in/hacktools_02.asp اخر زيارة للموقع بتاريخ :15-05-2019 بتوقيت 23:14.

ينتميان الى الطبيعة التقنية الالكترونية هذه ثاني ميزة يلتقيان فيها بعد وجودهما وقيام نشاطهما داخل نفس البيئة ، وكذلك اساليب اعتمادهما للسيرورة العادية فكل من القرصنة الالكترونية والنقود الالكترونية تعتمدان على تكنولوجيا الاتصال و الانترنت لتقوم كل منهما بعملها الاولى للقيام بالهجمات و السطو و السرقة و ما الى ذلك و الثانية للتحويلات و المعاملات المالية فلابد ان تكون هناك طريقة ربطهما بين الضحية و الجاني في القرصنة الالكترونية و بين الدائن و المدين في النقود الالكترونية ، و جدير بالذكر ان تواجد الطرفين في كلا العنصرين في هذا العالم كذلك ليس ضروري ان يكون مباشرا بل عن بعد يكفي كما سبق الذكر وجود سبيل للاتصال بينهما فقط، ولا ننسى اعتمادهما على الاجهزة التقنية كوسائل الاتصال و الكمبيوترات للقرصنة و السحابات الالية و قارئات التلخيص بالنسبة الى النقود الالكترونية التي تخزن في البطاقات الائتمانية، فكلاهما من بيئة واحدة و هي البيئة الالكترونية الرقمية.

الفرع الثاني

النقود الالكترونية ابرز اهداف القرصنة الالكترونية

وعموما لا تحتاج القرصنة إلى الكثير من التحليل ، فالدافع يمكن فهمه بسهولة: فالمنظمات الإجرامية او المجرمين في اغلبهم ينجذبون ببساطة إلى الربح العالي و السهل الذي يولده أي فعل يجلب ذلك ولو كان مجرما . و لقد ادت فعلا القرصنة هذا الغرض بحيث اصبحت اغلب الهجمات الالكترونية تستهدف الاموال الالكترونية سواءا على الصعيد الخاص ضد الافراد و المؤسسات المالية الخاصة او على الصعيد العام ضد البنوك بالقيام بالسطو و التحويل ، فحسب الاحصائيات المصرح بها في كثير من الاحيان حول الخسائر التي تنجر عن القرصنة تكون في جانبها المالي هي الغالبة ، وذلك "عندما تتحول الجريمة الإلكترونية أو القرصنة إلى صناعة تحقق المليارات، تصبح البنوك وأسواق المال والمرافق في خطر، خاصة في ظل انخفاض التأمين ضد المخاطر الإلكترونية والذي لامس 3 مليارات دولار عام 2017. فيما ستكلف الجريمة السيبرانية الشركات أكثر من تريليوني دولار بحلول عام 2019"[1]، ومع التطور التكنولوجي الحاصل في الانترنت و وسائل الاتصال فتح شهية الكثيرين و سهل الاعمال الاجرامية بشكل لا يوصف كون القرصنة لا تحتاج الى جهد كبير و قلة المخاطر المحتملة كغيرها من الجرائم التقليدية مع عائد مالي معتبر و الذي قد يصل بالمليارات الدولارات في هجمة واحدة و هذا ما نوضح في

[1]- المجلة، البنوك وأسواق المال في مرمى القرصنة، انظر للموقع :www.arb.majalla.com/2018/07/article55267586 /البنوك-وأسواق-المال-في-مرمى-القرصنة ، اخر زيارة للموقع : 16-05-2019 بتوقيت00:35.

الفرع القادم، و مما يؤكد ايضا تحول اهتمام القرصنة الى النقود الالكترونية مجموع الخسائر الواقعة في انظمة الحماية و النشاط القائم على تطوير الحماية الخاصة بالبنوك و المؤسسات الخاصة.

الفرع الثالث

اثار جريمة القرصنة الالكترونية على النقود الالكترونية

ان وقوع اي جريمة على شخص او شيء لابد ان يترك اثرا واضحا او ضررا معين فجريمة القرصنة و استهدافها للنقود الالكترونية و تحققها الفعلي عليها ترك خسائر عظيم على المستويين الخاص و العام وطنيا و دوليا و من بين الخسائر التي ذكرت و صرح بها نشير الى الاتي:

أ. " ألبرت غونزاليس الذي اتهم بأنه العقل المدبر في أكبر سرقة لأجهزة الصراف الآلي وبطاقات الائتمان بالتاريخ، حيث يعتقد أنه وجماعته من القراصنة باعوا خلال الفترة من 2005 إلى 2007 أكثر من 170 مليونا من أرقام بطاقات الصراف الآلي وبطاقات الائتمان.

الروسي فلاديمير ليفين الذي تمكن عام 1994 مستخدما حاسوبه المحمول في شقته بمدينة سانت بطرسبرغ من تحويل عشرة ملايين دولار من حسابات عملاء في بنك "سيتي بانك" إلى حساباته الشخصية حول العالم، وبعد اعتقاله تمت استعادة المال المسروق باستثناء أربعمائة ألف دولار. "[1]

"خسارة بنك الخليج الكويتي تصل إلى أكثر من 10 ملايين دولار، جراء قرصنة إلكترونية على حسابات بعض العملاء"[2].

"البلاد.نت : تعرض الموقع الرسمي لبنك الفلاحة وال تنمية الريفية للقرصنة من قبل هاكرز"[1] مما يؤكد ان اغلب الهجمات هدفها متمثل في تحويل النقود بطبيعتها الالكترونية .

---

[1]- موقع الجزيرة :www.aljazeera.net/knowledgegate/newscoverage/2015/1/5 /القرصنة-الإلكترونية-سلاح-العصر-الرقمي ، اخر زيارة للموقع 16-05-2019 بتوقيت 00:48.

[2]- مروان رجب، 10 ملايين دولار خسائر بنك كويتي جراء قرصنة إلكترونية، موقع الخليج الجديد ، http://www.thenewkhalij.news/اقتصاد/10-ملايين-دولار-خسائر-بنك-كويتي-جراء-قرصنة-إلكترونية اخر زيارة للموقع:16-05-2019 بتوقيت :01:13 .

[1]-جريدة البلاد، قرصنة موقع بنك "بدر"، www.elbilad.net/article/detail?titre=قرصنة-موقع-بنك-بدر&id=94743K ، اخر زيارة للموقع:16-05-2019 بتوقيت01:36.

لم تسلم ايضا النقود الالكترونية بصيغتها الافتراضية من جريمة القرصنة ومن بين الخسائر المذكور التي اعلنتها " شركة ''كوينتشيك''- إحدى أكبر شركات تبادل العملات الرقمية في اليابان- إنها فقدت ما قيمته نحو 534 مليون دولار أمريكي من العملة الافتراضية، في هجوم قرصنة إلكرونية على شبكتها.

وقال تقرير نشرته ''بي بي سي'' اليوم: إن الشركة أوقفت التداول بجميع العملات الرقمية باستثناء عملة ''بيتكوين'' إلى أن قيمت حجم خسائرها الناجم عن فقدان عملة ''نيم''، وهي عملة رقمية أقل شهرة من ''بيتكوين''"[1].

"ولم تعد الحسابات البنكية الشخصية هدفاً لعمليات القرصنة؛ وإنما امتدّت إلى البورصات العالمية، ومنها هيئة الأوراق المالية والبورصات الأمريكية(SEC) ، التي تعرّضت لهجوم قراصنة في العام 2016، استطاعوا الوصول إلى البيانات الشخصية لآلاف العملاء وإجراء بعض الصفقات المربحة وتحويل أرباحها إلى حساباتهم.

وبحسب تقرير صادر عن مركز الدراسات الاستراتيجية في واشنطن بالتعاون مع شركة "مكافي" لبرامج الأمن المعلوماتي، فإن الاقتصاد العالمي يتكلف سنوياً نحو 600 مليار دولار من جراء تلك العمليات، وهذا الرقم مرشّح للزيادة في السنوات المقبلة، لا سيما في ظل انتشار العملات الرقمية التي أصبحت سوقاً سوداء وملاذاً لتحويل ما يتم الاستيلاء عليه .

ب. وفي تفصيل لبعض الخسائر الناتجة عن هجمات قراصنة الشبكة العنكبوتية، كشفت دراسة أجرتها شركتا "كاسبرسكي لاب" (المختصة بأمن الحواسيب) و"B2B International" (مختصة بأبحاث السوق)، ونشرتها في أبريل الماضي، أن كل هجوم إلكتروني تتعرّض له الشركات المالية يكبّدها خسائر تُقدر بنحو مليون دولار أمريكي في المتوسط.

وأشارت الدراسة إلى أن أكثر الشركات المستهدفة بالهجمات الإلكترونية هي شركات الخدمات المالية العالمية وشركات قطاع الطاقة، وأن هذه الهجمات تكلّف الشركات ما يعادل 40 ألف دولار أمريكي في الساعة"[1].

[1]- موقع روتانا، أكبر حادث سرقة رقمية في العالم لشركة يابانية،/www.rotana.netأكبر-حادث-سرقة-رقمية-في-العالم-لشركة-يا/، اخر زيارة للموقع بتاريخ:16-05-2016 بتوقيت 01:44.

[1]- حنين ياسين، كيف تستنزف "حرب السايبر" 600 مليار دولار سنوياً من اقتصاد العالم؟، الخليج اونلاين، /www.alkhaleejonline.netاقتصاد/كيف-تستنزف-حرب-السايبر-600-مليار-دولار-سنوياً-من-اقتصاد-العالم؟، اخر زيارة للموقع:16-05-2019 بتوقيت 02:09.

المطلب الثالث

الجهود و الاليات المبذولة لمكافحة جريمة القرصنة الالكترونية

و نظرا للتغيرات التي أحدثتها الانترنت و تكنولوجيا الاتصال خصوصا بظهور سلوكات اجرامية مست نواحي الحياة ، مما حركت الكثير من الجهود الدولية و الوطنية للتصدي لمثل هذه الجرائم ، اضافة الى تطوير الكثير من الاليات الفنية و الادارية للمساعدة في مكافحتها خصوصا جريمة القرصنة التي استفحلت في الآونة الاخيرة على كل الاصعدة الدولي و الوطني و في جميع مجالات الحياة وبهذا سنتطرق الى بعض هذه الجهود في الفروع القادمة :

الفرع الاول

الجهود الدولية و الوطنية لمكافحة جريمة القرصنة الالكترونية

ان أي فعل لابد ان يكون له ردة فعل و هذا ما كان نتيجة الاضرار التي ولدتها جريمة القرصنة من جهود دولية و وطنية نذكر منها:

اولا: الجهود الدولية

أ. **الاتفاقية الأوربية لمكافحة جرائم الأنترنت (2001 اتفاقية بودابست)** :

"وتعد الاتفاقية الوحيدة، والمعروفة بالاتفاقية الدولية لمكافحة الجرائم التي ترتكب عبر الأنترنت)، حيث شهدت العاصمة المجرية بودابست في 2001/11/23 ولادة أول معاهدة دولية هدفها مكافحة جرائم الأنترنت، وتقوية الجهود الدولية من أجل التعاون والتضامن في محاربة هذه الجرائم والحد منها، وخاصة بعد أن أصبحت تلك الجرائم تشكل خطرا يهدد الأشخاص والممتلكات "[1]، واستنادا إلى المواد في المعاهدة من 2-13 فان الاتفاقية تلزم الدول الأعضاء فيها (وهي هنا الدول الأوروبية وأي دولة توقع عليها أو تنضم إليها من خارج المجموعة الأوروبية) باتخاذ التدابير التشريعية والإجراءات الملائمة لتجريم تسع جرائم في ميدان جرائم التقنية "[1] نذكر منها فقط :

[1]- محمد خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستوين الدولي و الوطني(دراسة مقارنة)، مجلة كلية القانون للعلوم القانونية و السياسية ،العدد36،العراق2018،ص98.

[1]- مركز هاردو، التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات، مركز هاردو لدعم التعبير الالكتروني، مصر،2018 ، ص23.

الدخول غير القانوني المتعمد- الاعتراض غير المشروع- كل هذه الاعمال شددت في حالات التدمير او التزوير او تعديل و غير ها الافعال الماسة لتلك المعطيات

ب. **القانون الاماراتي العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها قرار رقم 2004/417** :

بخصوص مكافحة جرائم تقنية المعلومات الحديثة في نطاق الأمانة العامة لجامعة الدول العربية والذي اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم 495- د 19 - 2003/10/8 و مجلس وزراء الداخلية العرب في دورته الحادية و العشرين .تحت رقم 417-د 2004/21 و يتضمن القانون العربي الإسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها من المادة 03 منه بالدخول و الولوج العمدي دون وجه حق و التي تؤكد في الفقرة الثانية على الافعال الماسة بالمادة المعلوماتية لتلك المواقع و الانظمة بقولها " فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصية يكون الحد الأدنى لعقوبة الحبس ..... ولعقوبة الغرامة ....."[1] ، و ايضا ما صرحت به من تزوير في مستندات المعالجة في النظام المعلوماتي يعتبر معاقبا عليه ايضا وكذا المادة 06 من هذ القانون التي نصت صراحا على احد اساليب القرصنة وهو الحقن او دس احد البرامج الخبيث في الانظمة او الشبكات بقولها "كل من أدخل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها ، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات بغرض ذلك ولم يتحقق غرضه يعاقب بالحبس..... والغرامة ..... أو بإحدى هاتين العقوبتين"

ج. **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:**

حيث حررت هذه الوثيقة بمصر بتاريخ 2010/10/21 و وافقت عليها الجزائر بنفس اليوم ، وتتكون الاتفاقية من 43مادة، و نظمت في الفصل الثاني مواد تجريم افعال القرصنة و الجرائم المتعلقة بتقنية المعلومات ، خصوصا ما صرحت به المادة 05 تحت عنوان "الدخول غير المشروع" بذكر مصطلحات "الدخول أو البقاء وكل اتصال غير مشروع" و تشدد العقوبة في حالات التالية "محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة والاجهزة والانظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين" [1]، كما يجدر الذكر هنا ان الاتفاقية نصت صراحة على احد وسائل استعمال النقود الالكترونية تحت مصطلح

[1]- انظر الملحق رقم 07.

[1]- راجع المادة 05 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وسائل الدفع الالكترونية في نص المادة 18 تحت عنوان "الاستخدام غير المشروع لأدوات الدفع الالكترونية " و جرمت الافعال تالية :"

1- كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة مةن أدوات الدفع الالكترونية بأي وسيلة كانت.

2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها لل ير أو سّ هل لل ير الحصول عليها.

3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع

4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك."[1]

وكان الهدف من الاتفاقية تعزيز التعاون و تدعيمه بين الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها

ثانيا : الجهود الوطنية

1. المشرع الفرنسي:

ونجد أن المشرع الفرنسي قام بإدارج الفصل الثالث من القانون العقوبات الفرنسي تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات و هذا في محاولة منه لمكافحة القرصنة و الجريمة الالكترونية عموما ، و يظهر ذلك في تجريمه لبعض الأفعال المساهمة في حدوث ذلك ، كتجريمه لفعل البقاء والدخول بطريق الغش إلى نظام المعالجة الآلية للمعطيات حيث عاقب على ذلك بعقوبة الحبس لمدة سنتين وغرامة قدرها 30000 أورو و أي مساس او ضرر سببه هذا الدخول تشدد العقوبة[2]، غير ان ما لوحظ على المشرع الفرنسي لم يعرف القرصنة او الجريمة الالكترونية بل اكتفى بتحريم الافعال الناتجة عنها و المساعدة لها في المواد 323-1 الى 323-7 من قانون العقوبات الفرنسي.

2. المشرع المصري

اقر المشرع المصري اخيرا قانون خاصة بمتابعة و مكافحة الجرائم الالكترونية تحت عنوان "قانون مكافحة جرائم تقنية المعلومات" رقم 175 الصادر بتاريخ 14 اوت 2018 في الجريدة الرسمية رقم 32 مكرر(ج) ، حيث تم التعريف ببعض المصطلحات التي تنتمي لجريمة القرصنة في مصطلحي الاعتراض و الاختراق في الباب الاول –

[1]- راجع المادة 18 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2]- راجع المادة 323-1 من قانون العقوبات الفرنسي.

الاحكام العامة في نص المادة 01 ،كما جرم الافعال المؤدية لذلك في الباب الثاني تحت عنوان الجرائم و العقوبات من المادة 12 و ما يليها.

3. المشرع الجزائري:

و عملا على ضمان السير السليمة للتكنولوجيا عهد كذلك المشرع الجزائري على حماية هذه الميزات التي اتى بها التطور التكنولوجي عبر تنشيط بعض الاليات نذكر منها :

أ. القوانين :

حيث اخص هذه الجريمة و نفس النوع من الجرائم الالكترونية بقانون خاص يقوم محاولة الوقاية منها تحت04/09 المؤرخ في 05أوت 2009المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ،كما ادرجها في قانون العقوبات في قسم خاص وهو القسم السابع مكرر03 تحت عنوان المساس بانظمة المعالجة الالية للمعطيات من المواد 394 مكرر الى 394 مكرر 7.

ب. الهيئات

- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته:** حيث انشات بمقتضى القانون 04/09المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] في مادته 13 بقولها :" تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة و تنظيمها و كيفيات سيرها عن طريق التنظيم" [2]، "وتتولى هذه الهيئة وفقا للمادة 14تنشيط وتنسيق عمليات بالوقاية من جرائم الاتصال والمعلومات ومكافحتها ،ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية ،وأيضا وتبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

[1] – الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 المؤرخ في 14شعبان عام 1430 الموافق 05غشت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، الجريدة الرسمية عدد47،مؤرخة في 16 غشت2009.

[2]– انظر الملحق رقم 08

- كما أنشأت الجزائر **مركز لمكافحة جرائم الانترنت على مستوى الدرك الوطني** في إطار مسايرتها للتطور التكنولوجي وما يصاحبه من أنواع جرائم الانترنت "[1]، وكذا انشاء **خلايا ولائية لمكافحة الجريمة الالكترونية** على مستوى مديريات الامن الوطني في كل ولايات الوطن.

الفرع الثاني

الجهود الفنية و التقنية لمكافحة جريمة القرصنة الالكترونية

ان محاولة ايجاد حلول فنية و تقنية لمكافحة جريمة القرصنة و الجرائم الالكترونية و جرائم الاتصال و التكنولوجيا دائما ما تتسم بالجدية كونها الحل الوحيد عمليا كون هذه الجرائم صعبة الاثبات مما يغيب عمل القوانين و العقوبات الردعية و تتمثل الحماية الفنية في خلق أنظمة حماية معلوماتية كالتشفير و انظمة الحماية المشددة، و برامج كالبرامج المضاد للفيروسات، و نذكر منها مايلي :

اولا التشفير Cryptologie :"ينقسم علم التشفير إلى Cryptographie الذي يشمل دراسة الآليات المخصصة لضمان السرية، وتحليل التشفير cryptanalyse الذي يهدف إلى إبطال الحماية أو وضعها"[2]، "التشفير و هو تحويل المعلومة من نص واضح إلى آخر غير مفهوم و قد أستحسن هذا النوع من النظام لنجاعته في عدم كشف المعلومات على شبكة الانترنت.

ثانيا جدار الحماية fire well: هو حاجز يوضع بين الشبكة الداخلية وخادم شبكة الانترنت ومن أهم مهامه فحص المعلومات الداخلة والخارجة والسماح لها بالمرور في حالة مطابقتها للمواصفات وتقديم تقارير عن التحركات المشبوهة ولكنه يمكن أن يعطل بعض المعلومات ويحدث عطب.

ثالثا التوقيع الرقمي: و هي تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية"[3].

رابعا مضادات الفيروسات : هي برامج مهمتها حماية الانظمة و البرامج الاخرى من الفيروسات او البرمجيات الخبيثة التي قد تدمر المعطيات المكونة للبرامج او الانظمة و هناك شركات مخصصة و معتمدة دوليا مهمتها انشاء

---

[1]- صالح شنين، الحماية الجنائية للتجارة الالكترونية (دراسة مقارنة) ، رسالة دكتوراه تخصص قانون خاص، كلية الحقوق جامعة ابو بكر بلقايد تلمسان، الجزائر2013،ص ص:220-221.

[2]- احمد مسعود مريم ، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم04/09، رسالة ماجستير تخصص قانون جنائي، كلية الحقوق جامعة قاصدي مرباح ورقلة،الجزائر،2013،ص:21.

[3]- مركز هاردو، المرجع السابق،ص:30.

و تطوير مثل هذه البرامج مثل ماكافي[1] و كاسبرسكي لاب[2] و غيرها.

يجدر بالذكر ان هناك حلول تقنية اخرى مثل البصمة الالكترونية و الشهادات الالكترونية من بين ادوات حماية المراسلات و الحسابات الرقمية.

اما بخصوص الاساليب التقنية الفنية لحماية الانظمة و الحسابات الرقمية نذكر:

المصادقة Authentification : **او الترخيص** هي عبارة عن كلمات مفتاحية خاصة او رسائل بريدية او رسائل قصيرة SMS عبر الهواتف المحمول لتأكيد هوية القائم بعمليات الدخول او الولوج الى الانظمة او الشبكات بإرسالها الى صاحب الحساب في بريده الالكتروني او هاتفه الشخصي او الظهور امامه مباشرة في حالات الكلمات المفتاحية و تسمى ايضا بالحماية "ثنائية الخطوة Security Second Step" و تكون اما بإرسال كود متكون من حروف او مجموع ارقام و هي تمنع بطريقة احسن فكرة الاختراق او التلاعب بالحسابات و الانظمة، خصوصا ان اغلب الانظمة المالية اصبحت تعتمد اعتمادا كبيرا على الحواسيب و الانظمة المعلوماتية ، من بين احدث الانظمة المضافة لخدمة الحساب الالكتروني البريدي اضاف بريد الجزائر خدمة التحويل بين الارصدة في شهر ماي 2019 [3]و هي ما قد يزيد من خطورة القرصنة على الحسابات كون امكانية القرصان في الاطلاع على الارقام السرية للضحية بعد ولوجه الى الكمبيوتر ،ومع ان هذه الخدمة لم تصل الى الاجهزة الحاسوبية بل بقيت محصورة في تطبق هاتفي و السحاب الالي باستعمال بطاقة الذهبية الا امكانية الدخول عن طريق التطبيق و تحويل الاموال من أي هاتف بعد معرفة الارقام السرية التي سرقت من الكمبيوتر المُقَرْصَنْ تجعل من تقنية او آلية المصادقة هي الأضمن حمايةً و احسنها التي يستقبل فيها العميل رسالة قصيرة SMS على هاتفه لتأكيد التحويل او الدخول مما يصعب فعلا اي قرصنة كانت و يحمي الحسابات من الاستيلاء و السطو.

رغم ذلك فان ما نتج عن جريمة القرصنة من اضرار مالية وجب على كل الاطراف اعادة النظر و التعاون لإيجاد بدائل جدية و فعالة لمكافحة هذه الجريمة .

---

[1]- ماكافي (McAfee): شركة أمن وبرامج مضادة للفيروسات تأسست عام 1987 و مقرها في سانتا كلارا، كاليفورنيا وهي تنتج برنامج مكافي فايرس كان وغيره من البرامج.

[2]- كاسبرسكي لاب(Kaspersky Lab) هي شركة متخصصة في أمن الحواسيب.تأسست سنة 1997 تقدم حلول وتطبيقات لبرامج مضادة للفيروسات .مقرها الرئيسي في العاصمة الروسية موسكو

[3]- اطلق بريد الجزائر خدمة التحويل بين الارصدة في شهر ماي 2019 عبر ارسال رسائل تؤكد الخدمة الى ارقام هواتف زبائن شركة موبيليس تحت عنوان "حوالتك" و ذلك يوم 24-05-2019.

المبحث الثاني

جريمة الاحتيال الالكتروني

ان جريمة الاحتيال الالكتروني احد الجرائم التي تستهدف النقود الالكترونية كمحل لها و هي تلك الامتداد المتطور عن الاحتيال التقليدي الذي عرف على انه السطو و الاستيلاء على المال باي شكل كان عن طريق الاساليب الاحتيالية بالغش و الخداع و الكذب، وبهذا التطور الذي مست هذه الجريمة في اساليبها و طبيعتها وصلا الى الهيئة الجديدة و المتمثلة في جريمة الاحتيال الالكتروني لابد لنا ان نعرف هذا المصطلح (المطلب الاول) و ان نحدد المفاهيم التي قدمها الفقهاء بسرد اركانها و تمييزها عن الجريمة التقليدية ، كما سنذكر الاختلاف الحاصل في محل الجريمة و الذي هو محل اهتمام دراستنا و المتمثل في النقود الالكترونية و تاثرها بجريمة الاحتيال(المطلب الثاني) ، مع ما اوجدته الدول و المؤسسات المالية من حلول(المطلب الثالث) لصد هذه الجريمة التي تمس مصالح الجميع.

المطلب الاول

مفهوم جريمة الاحتيال الالكتروني

و للفهم الحقيقي لجريمة الاحتيال الالكتروني وجب علينا التطرق الى تعريف هذا المصطلح تعريف شاملا لغة واصطلاحا و كذلك الاحاطة باركان هذه الجريمة و تمييزها عن غيرها من الجرائم بتبيان خصائصها كما سنتطرق الى الاساليب التي يعتمدها المحتالين في هذا المجال كل هذا سنتطرق اليه في الفروع القادمة

الفرع الاول

تعريف جريمة الاحتيال الالكتروني

كل تعريف يجب ان يحمل معنيين المعنى اللغوي و هو ما يشتق منه المعرف و المعنى الاصطلاحي و الذي ينتج عن نظرة الاخرين لهذا المعرف و من هنا نعرف الاحتيال الالكتروني لغة و اصطلاحا في العناصر التالية

اولا : تعريف الاحتيال الالكتروني لغةً

1. "**احتيال** [مفرد]: ج احتيالات (لغير المصدر):1.مصدر احتال/ احتال على/ احتال في/ احتال) 2. (قن) جنحة يجترمها من يبتز مال الغير بالخديعة "وجهت إليه تهمة الاحتيال".

احتال/ احتال على/ احتال في /احتال لـ/ يَحتَال، احْتَلْ، احتِيالاً، فهو محتَال، والمفعول محتال عليه

• احتال الشخص: طلب الشيء بالجيل؛ أي بوسائل بارعة ابتغاء الوصول إلى المقصود "احتال على قتله: دبر حيلة لقتله- وجهت إليه تهمة النصب والاحتيال.

•احتال في الأمر: وجد حيلة أو وسيلة له"[1].

2. "**ألكتروني** [مفرد]: ج ألكترونيات اسم منسوب إلى الكترون

ألكترون [مفرد]: ج ألكترونات (فز) جزء من الذرة دقيق جدا ذو شحنة كهربائية سالبة"[2].

ثانيا: تعريف الاحتيال الالكتروني اصطلاحًا

"يمكن القول بصفة عامة أنه لا يوجد تعريف جامع ومانع لجريمة الاحتيال الالكتروني يمكن الرجوع إليه ، فقد تعددت التعريفات التي تناولت الإحتيال الالكتروني أو كما يسمى بالإحتيال المعلوماتي واختلفت فيما بينها من حيث العناصر التي ينبغي توافرها لتحقيقه ، ولقد توسعت غالبية التعريفات في مفهوم الإحتيال المعلوماتي حيث تربط بين الاستخدام غير المشروع للحاسبات الآلية لتحقيق ربح مادي غير مشروع "[3] ، و بعض الفقهاء ألصقه بالاحتيال التقليدي و فرقه بشكل بسيط عن التقليدي كونه يستعمل وسائل احتيالية حديثة و نذكر من التعاريف الاتي :

- "**الاحتيال المعلوماتي** هو البديل الاحتيالي للحاسوب بالمعنى التقليدي للكلمة . تتمثل عملية الاحتيال في استخراج البضائع أو الأموال من أشخاص غير متشككين من خلال الكلمات والمقترحات الدقيقة. عندما يستخدم شخص ما وسائل الاتصال الحديثة لهذا الغرض، فإن المشرع يعتبر أنه عملية احتيال. يتيح الإنترنت الوصول إلى عدد كبير من الضحايا بسرعة وبتكلفة منخفضة."[4]

عرف ايضا بـ: "(**الاحتيال الإلكتروني**) الخداع والخداع عبر الإنترنت"[5].

[1]- احمد مختار عمر و فريقه، المرجع السابق، ص ص:586-587

[2]- المرجع نفسه، ص ص:111-112

[3]- سامر سلمان عبد الجبوري، الاحتيال الالكتروني، رسالة ماجستير تخصص قانون عام، كلية الحقوق جامعة النهرين،العراق،2014،ص11.

[4]- Céllule de Traitement du Renseignement Financier , **Fraude informatique, lettre information N°30,** Sans date, p :01.

[5]- E-fraud (Electronic-FRAUD) Online trickery and deception.Look in :www.yourdictionary.com/e-fraud

- "تعريف **الاحتيال الالكتروني** (بأنه كل فعل أو سلوك متعمد من شخص أو مجموعة من الاشخاص بانتحال هوية لشخص طبيعي او معنوي و يستخدم فيه التقنيات الالكترونية بهدف تحقيق كسب مادي غير مشروع على الاموال او السندات وذلك عبر استخدام طرق احتياله او اتخاذ اسم كاذب او صفه غير صحيحة)"[1]

- و عرف ايضا "أي نوع من مخططات الاحتيال يستخدم مكونًا واحدًا أو أكثر من مكونات الإنترنت - مثل غرف الدردشة أو البريد الإلكتروني أو لوحات الرسائل أو مواقع الويب لتقديم معاملات احتيالية أو لنقل عائدات الاحتيال للمؤسسات المالية أو للآخرين متصل بالمخطط "[2].

- وحسب ما سبق من تعريفات و استنتاجا لها فان الاحتيال الالكتروني هو صورة حديثة عن الاحتيال التقليدي غير انه يتعمد على وسائل حديثة للقيام بالخداع مثل الانترنت و ما نتج عنها فالاحتيال التقليدي كما عرفه الفقهاء هو تغيير الحقيقة قصد الحصول على مال الغير بطرق احتيالية ،كذلك هو الاحتيال الالكتروني الاحتيال الالكتروني يهدف الى اخذ مال الغير بالطرق الاحتيالية الحديثة المعتمدة على الحاسوب و الانترنت و التكنولوجيا المتطورة.

الفرع الثاني

اركان جريمة الاحتيال الالكتروني

لابد في كل جريمة من توافر اركانها الثلاث ، وهم الركن المادي، والركن المعنوي ،و الركن الشرعي ،وجريمة الاحتيال الالكتروني لا بد فيها من وجود هذه الاركان، ليقع وصف الجريمة على هذه العملية، ولكي يتضح الأمر لا بد من تبيان لهذه الأركان على التفصيل:

اولا :الركن المادي:

"غالبا ما يكون الركن المادي في معظم الجرائم ايجابي -أي أن يحظر القانون من ارتكاب فعل-وجريمة الاحتيال الالكتروني من الجرائم الإيجابية، وعلى ذلك لقيام الركن المادي لجريمة الاحتيال الالكتروني، يجب ان يتوافر عدة عناصر رئيسية وتتمثل في السلوك الاجرامي(الطرق الاحتيالية) والمتمثلة بالخداع، الانترنت، النتيجة الجريمة وهي تسليم المجني عليه المال الى المحتال، واخيرا علاقة السببية بين السلوك الاجرامي والنتيجة الاجرامية والتي تتمثل

[1]- حمد عبدالله حيي بو غانم السليطي، تجريم الاحتيال الالكتروني في القانون القطري والمقارن، رسالة ماجستير ،كلية القانون جامعة قطر، قطر،السنة الجامعية:2017-2018،ص 11.

[2]- Micheal Kunzand Patrick Wilson :computer crime and computer fraud , the Professional Masters Degree, Univesity of Mayland , 2004,p 12.

حلقاتها في الغلط المترتب على الخداع"[1] ، و التي تقوم على تسليم المال الى الجاني كون الاحتيال عموما كان التقليدي منه او الالكتروني لم يعرف قانونا و لكن يستشف من موادها الافعال التي تبني فعل الاحتيال التي دائما ما صنفت الاحتيال من الافعال المجرمة الماسة للأموال و من ذلك ما اتت به المادة 372 من قانون العقوبات

الجزائري التي ذكرت عنصرين هامين للركن المادي لجريمة الاحتيال او النصب[2] وهي:

- تلقي او استلام المال باي صفة كان (منقول، مستند، اوراق مالية...)
- باستعمال الطرق الاحتيالية(و التي هنا تكون حديثة سنتطرق اليها في الاساليب)

و استنتاجا عن التعاريف السابقة فان:

- استخدام الانترنت و الحاسوب يعتبر من الافعال التي تكمل الركن المادي
- مع وجود نتيجة اجرامية و هي استلام او تلقي المال للجاني و التصرف فيه، و بالتالي فان القيام بالخداع و تغيير الحقيقة عن طريقة استعمال الحاسوب و الانترنت من اجل الحصول على المال يعتبر جريمة احتيال الكتروني.

ثانيا : الركن المعنوي

"جريمة الاحتيال الالكتروني من الجرائم العمدية التي تستلزم توافر القصد الجنائي العام بعنصري توافر العلم والإرادة، فضلا عن القصد الجنائي الخاص والمتمثل في انصراف نية الجاني المحتال الى الاستحواذ والاستيلاء على المال محل الجريمة وتملكه ملكية مطلقة.

القصد الجنائي العام ينقسم الى العلم و الارادة:

- **العلم**: ويقصد بالعلم علم الجاني بعناصر الجريمة أي ان المحتال يجب أن يكون على علم بأن الأفعال التي يقترفها ويأتيها يعدها القانون من قبيل الطرق الاحتيالية، وأن هذا النوع من السلوكيات من شأنها خداع المجني عليه وحمله على تسليم المال طوعية واختيارا تحت تأثير تلك الافعال الاحتيالية"[3].

- **الارادة**: و هي توجه ارادة الجاني للاستعمال الطرق الاحتيالية حسب ما صرحت به المادة 372 من قانون العقوبات بقولها" باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي

---

[1]- حمد عبدالله حيي بو غانم السليطي، المرجع السابق،ص28.

[2]- ارتأينا استعمال مصطلح الاحتيال كونه اوسع من مصطلح النصب لان معنى النصب يحمل الاعياء و التعب في مثل قوله تعالى" واذكر عبدنا ايوب اذ نادى ربه ان مسني الشيطان بنصب و عذاب" سورة(ص) الآية 41، و يحمل معاني كثير منها العداوة و الاحتيال اكثر دلالة و انتشارا لمعنى الخديعة و الغش و تغيير الحقيقة غير ان المشرع الجزائري استعمل مصطلح النصب و هذا من مخلفات الاستعمار الفرنسي و التي نتج عنها اختلاف في معنى المصطلحات القانونية عن المعاني اللغوية و قد لاح اثرها في النصب على مصطلح "Escroquerie" و هو اضيق .

[3]- حمد عبدالله حيي بو غانم السليطي، المرجع السابق ،ص41.

خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها"[1] غير انها تختلف اختلافا واضحا في كون الاحتيال الالكتروني قد يستعمل فعلا اسماءا او صفات كاذبة او سلطات خيالية قد تكون لشخصيات او بنوك او مؤسسات ولكن بشكل مغاير عن الاحتيال التقليدي دائما ما يكون في فضاء الانترنت و تصل الى المستهدف منها بأسلوب اخر .

- **القصد الجنائي الخاص:** والقصد الجنائي الخاص في جريمة الاحتيال الالكتروني يتمثل في اتجاه نية الجاني او المحتال إلى تملك المال محل الجريمة والتصرف فيه ، او الشروع في التصرف فيه حسب ما صرحت به المادة 372 من قانون العقوبات ، و الملاحظ هنا ان جريمة الاحتيال الالكتروني في حد ذاتها جريمة عمدية لأسباب عدة منها الاستعمال الواضح للتكنولوجيا و الاساليب الاحتيالية و كون محل الجريمة مال لا يترك مجالا لإيضاح القصد الجنائي الخاص المتمثل في الاستيلاء على تلك الاموال اكثر مما هو موضح بتمام تلك الافعال.

ثالثا : الركن الشرعي

ان الحديث عن تجريم الاحتيال الالكتروني صراحة كونه يختلف عن الاحتيال التقليدي لم يذكر صراحة ولكن يستشف من القواعد العامة التي تجرم الاحتيال التقليدي و كون النوعين يتطابقان في كثير من السمات التي تهدف دوما الى الاستيلاء على مال الغير و لكن يكمن الاختلاف في نوع الاساليب و من هنا فان النصوص الموجودة لتجريم هذا الفعل قائما على النصوص العامة و من ذلك ما اتى في قانون العقوبات الجزائري في المادة 372 ، و كون مجال نشاط الاحتيال الالكتروني هو الحواسيب الانترنت فانه يدخل في باب سوء استخدام الكمبيوتر و الانظمة الالية مما تطبق عليه كذلك مواد 394مكرر الى 394 مكرر07 [2]و كذلك مجموعة القوانين و النصوص و الاتفاقيات التي تجرم الافعال الناتجة عن استعمال الانترنت و تكنولوجيا الحواسيب

الفرع الثالث

خصائص و اساليب جريمة الاحتيال الالكتروني

ولنميز الاحتيال الالكتروني عن باقي الجرائم العادية مثل الاحتيال التقليدي و الالكترونية الاخرى وجب علينا تعداد خصاصه و اساليبه مما يجعله واضحة كجريمة قائمة بذاتها و ذلك في التفاصيل التالية :

[1] –راجع المادة 372 من قانون العقوبات الجزائري.

[2] راجع المواد 394 مكرر الى 394مكرر7 من قانون العقوبات الجزائري

اولا : خصائص جريمة الاحتيال الالكتروني

- **تستعمل الحواسيب** : "سمة الحاسب الآلي هي دائماً أداة الجريمة في جرائم الاحتيال وغيرها من الجرائم التي ترتكب على شبكة الانترنت ، هي سمة وخاصية منفردة عن أي جريمة أخرى ذلك ان الحاسب الآلي هو الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الانترنت وقيامه بتنفيذ جريمته أياً كان نوعها وعليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب اي جريمة من الجرائم التي ترتكب على شبكة الانترنت"[1]، و الاحتيال الالكتروني ليس كالقرصنة التي قد تستعمل اجهزة اتصال اخرى للقيام بالأعمال الاجرامية المراد القيام بها .

- **شبكة الانترنت** هي حلقة الوصل لارتكاب جريمة الاحتيال الالكتروني: ان جريمة الاحتيال الالكتروني من الجرائم التي ترتكب عبر شبكة الانترنت، وعليه فان شبكة الانترنت تعتبر هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الأهداف التي ما تكون غالبا ضحايا تلك الجريمة، الامر الذي يجعل معظم هذه الجهات (الضحايا) الى اللجوء الى وضع نظم امنية الكترونية لعدم اختراق مواقعهم والعمل على حمايتها والحد من الخسائر الفادحة التي يسببها الاختراق وحدوث جريمة الاحتيال.

- **محلها الربح او المال فقط**: ان جريمة الاحتيال الالكترونية ليس كغيرها من الجرائم الالكترونية فهي الجريمة الوحيد التي تهدف اساسا الى الاستيلاء على مال الغير دون هدف اخر كالقرصنة التي قد تهدف الى الجوسسة او التخريب .

- **تقوم على تغيير الحقيقة**: ان الاعتماد الاساسي لجريمة الاحتيال الالكتروني يقوم على تغيير حقيقة الصورة الواضحة امام الضحية مهما كانت المعلومات المقدمة له فهي دوما احتيالية غرضها الاستيلاء على المال و تسليمه طوعية الى المحتال، و ذلك باستعمال الكذب و الخداع في ذلك و هو ما يشترك فيه بالاحتيال التقليدي مع اختلافه في الاساليب.

- **خصائص مشتركة اخرى** : و تشترك ايضا مع الجرائم الاخرى كونها عالمية او عابرة للحدود و ايضا ان مرتكبيها ذوو سمات و كفاءة علمية متقدمة و انها صعبة الاثبات ....وغيرها من السمات التي تشترك بها مع الجرائم الالكترونية.

ثانيا : اساليب الاحتيال الالكتروني

ان لقيام اي جريمة لابد وجود اساليب و طرق تساعد على اتمام الفعل بشكل مبرمج له كذلك هو الاحتيال الالكتروني له اساليب تميزه عن غير من الجرائم و تساعد على الوصول الى الغاية المنشودة منهو هي الاستيلاء

[1]- سامر سلمان عبد الجبوري، المرجع السابق،ص:18.

على مال الغير و يقوم الاحتيال الالكترونية على:

أ. **الاصطياد بالرمح (Spear phishing)**: "**او التصيد** " وهو نوع من أنواع هجمات الاصطياد التي تركز على مستخدم واحد أو دائرة داخل منظمة، يتم شنها من خلال انتحال هوية جهة جديرة بالثقة لطلب معلومات سرية، مثل أسماء تسجيل الدخول وكلمات المرور.

وغالبا ما تظهر هذه الهجمات على شكل رسالة إلكترونية من الموارد البشرية للشركة أو أقسام الدعم الفني فيها، وقد تطلب من الموظفين تحديث اسم المستخدم وكلمات المرور الخاصة بهم، وبمجرد حصول المخترق على تلك البيانات فإنه يستطيع الولوج إلى مصادر الشبكة."[1]

"ويحرص المهاجمون المحترفون على استخدام البريد الإلكتروني لمجموعات مختارة بعناية من الأفراد بغية التصيد الاحتيالي، وذلك عبر وسائل التواصل الاجتماعي، ومعلومات المواقع أو الحقائق العامة عن مؤسستهم.

من ناحية أخرى، تستهدف عمليات التصيد الاحتيالي أكبر عدد من مستلمي الرسائل بحيث تنطلي الخدعة على نسبة ضئيلة منهم لتحقيق النجاح المحتمل. كما يمكن استخدام الفواتير الوهمية، وإشعارات التسليم والإيصالات والتحديثات المصرفية كوسيلة للخداع في هذه المحاولات"[2].

ب. **القرصنة** : وقد تستخدم كأداة مساعدة ايضا ضمن الرسائل الالكترونية الاحتيالية لغرض الولوج لكمبيوتر الضحية غير انها و مبدئيا اعتمدت اعتمادا كبيرا على اسلوب الحيلة التي ادرج في الرسالة التي تحمل معلومات حقيقية بصورة مغلطة لغرض الاستيلاء اما على المال او الحسابات المالية او الارقام السرية للحسابات و الارقام الخاصة بالبطاقات الائتمانية و ذلك بادراج برامج خبيثة بالنقر على مرفق في الرسالة يقوم احتياليا على التحميل التلقائي لهذه البرامج ، و البقاء داخل النظام المعلوماتي للضحية لتجميع ما يلزم من معلومات.

ج. **المواقع المزيفة**: وهو اسلوب يندرج في الرسائل المفخخة و الاحتيالية او ينتشر في مواقع التواصل الاجتماعي في بعض التعليقات يقوم على توجيه الضحايا الى صفحات مشابهة للمواقع الاصلية الخدماتية و التي قد يكون فيها الضحايا مشاركين فيها مما يساعد الجاني في حصوله على ة كلمات المرور او ارقام السرية للبطاقات الائتمانية و الحسابات البنكية بسبب ادخال الضحايا لمعلوماتهم و تكون هذه التعليقات و الرسائل ذات طابع

[1]– انظر اكثر الى موقع www.aljazeera.net/news/scienceandtechnology/2015/1/6/البرمجيات-الخبيثة-وأساليب-القرصنة، تاريخ الاطلاع :13-05-2019 بتوقيت 01:49.

[2]– بنك إتش إس بي سي الشرق الأوسط ، الجرائم الالكترونية ، www.business.algeria.hsbc.com/ar-dz/cybercrime، تاريخ اخر زيارة للموقع : 2019/05/18 بتوقيت 13:06.

تحفيزي اما بذكر خصومات او ميزات اضافية مقدمة تكون خادعة لجلبهم و دفعهم للقيام بعملية كتابة معلوماتهم التي تحول و تعرض في جهاز الجاني.

الرسائل القصيرة SMS:" قد تستعمل احيانا الرسائل القصيرة المنبثقة الى الهواتف الذكية و التي توجه الضحايا ايضا الى ارسال معلومات شخصية تساعد المحتالين في تجاوز عقبات الحماية الامنية التي تتطلبها عدم كتابة او حجز الارقام السرية و التي قد يستعملها اصحابها الاصليون و التي قد تحتوي على تواريخ ميلادهم او اسماء اقاربهم او اولادهم مما يسهل عملية الولوج الى الحسابات المالية او البنكية الخاصة بهم ليستولي عليها المحتال بتحويلها او استعمالها في الشراء كما قد تحمل هذه الرسائل في مضمونها موضوع المشاركة في مسابقة او اغراء مالي المضاعفة عبر تحويل مبلغ مالي الى حساب يذكر في الرسالة كل هذا غرض الاحتيال على جزء قليل او كبير من المال."[1]

تعتبر الاساليب الماضية هي الاشهر عالميا و المعروفة ظاهريا في عمليات الاحتيال الالكتروني الواقع على الاموال الالكترونية لأي ضحية تم الاستيلاء على اموالها و تم الكشف عنها او التبليغ بها.

المطلب الثاني

علاقة الاحتيال الالكتروني بالنقود الالكترونية

ان قيام اي جريمة الاحتيال الالكترونية لا يكون عبثا بل لابد من ان يهدف فاعلوها الى شيء معين من وراء القيام بها و كذلك هو الاحتيال حسب ما عرفه جموع الفقهاء انه فعل مجرم قائم على الاستيلاء على اموال الغير غير ان موضوعنا هنا هو الاحتيال الالكتروني مما يحصر محل الجريمة في محاولة الاستيلاء على الاموال ذات الطبيعة الالكترونية او ما سميناها النقود الالكترونية و لتبيان ذلك سنتطرق بالتفصيل الى تبيان العلاقة الرابطة بين النقود الالكترونية و هذه الجريمة في الفروع الاتية

الفرع الاول

الاحتيال الالكتروني و النقود الالكترونية طبيعة واحدة

و لتحديد مدى تطابق طبيعة النقود الالكترونية مع طبيعة جريمة الاحتيال الالكتروني وجب علينا تحديد مجال نشاطهما او ميدان استعمالها فالنقود الالكترونية كما عرفناها سابقا هي قيمة مالية مخزنة الكترونيا ، و تقوم الاطراف المرتبطة بها و المتمثلة في البنك او المؤسسة المصدرة لها و من يقوم بشرائها او تعبئتها في ادوات تخزينها و

[1] -موقع بوابة الشرق الالكترونية، هذه أسباب جرائم الاحتيال الإلكتروني والداخلية تحذر من التجاوب مع الرسائل المجهولة، الجمعة 11-01-2019 الساعة 2:00 ص، للاطلاع اكثر :www.al-sharq.com/article/11/01/2019 /هذه-أسباب-جرائم-الاحتيال-الإلكتروني-والداخلية-تحذر-من-التجاوب-مع-الرسائل-المجهولة، تاريخ اخر زيارة :18-05-2019 بتوقيت13:53.

الطرف الثالث الذي يستلمها لقاء خدمة او سلعة بالتعامل فيما بينها بأسلوب الاتصال الالكتروني اما عن طريق التحويلات و اما عن طريق السحب المباشر بالخصم بواسطة قارئات البطاقات الائتمانية فعموما كل عمليات النقود الالكترونية بين الاطراف الثلاث تعتمد على تكنولوجيا الاتصال الإلكتروني سواءا انترنت او شبكة خاصة، و كذلك الحال بالنسبة الى "عمليات الاحتيال الالكترونية بمحاولة عدد من الأشخاص سرقة البيانات الشخصية لحاملي البطاقات – و مستخدمي الإنترنت عبر الرسائل يريد إلكترونية أو روابط إلكترونية تقود المستخدمين إلى مواقع الكترونية شبيهة بالمواقع المعروفة، حيث تطلبه هذه المواقع الدين المستخدمين بيانات شخصية هامة ، يتم بواسطتها سحب مبالغ من أرصدة بعض العملاء أو تحويلها إلى حسابات أخرى أو الوقوع في مصيدة المشاركة أنشطة مالية ومصرفية غير مشروعة "[1]، مما يؤكد ان كل من النقود الالكترونية و جريمة الاحتيال الالكتروني تقعان في مجال واحد و كلاهما من طبيعة واحدة و هي الطبيعة الالكترونية ، ومما يربط العلاقة بينهما و يؤكد انهما من نفس الطبيعة استعمالهما تقريبا لنفس الادوات و المتمثلة في الحواسيب و الانظمة المعلوماتية فالنقود الالكترونية تعتمد على الحاسوب في انشاء الحسابات و التحويلات و كذلك المعاملات المالية الاخرى و الاحتيال هو الاخر يبدا من انشاء رسالة احتيالية على حاسوب الى ارسالها للضحية على حاسوب اخر او جهاز تقني اخر ، كما ان استعمالها لتكنولوجيا الانترنت و مدى اتساع هذه الاداة ادت كذلك الى اتساع استعمال او انتشار هذين العنصرين و اتصافهما بالعالمية و كسر حاجز الحدود الوطنية، فالنقود الالكترونية يمكن ان تحول من بنك الى اخر و من دولة الى اخرى عبر خطوط الانترنت بمجرد القيام بالأمر ، كما هو الحال بجريمة الاحتيال و التي قد يكون فاعلها في دولة و الضحايا المستهدفين في دول اخرى ، و بهذا تكون الانترنت و وسائل الاتصال اضافة الى الاجهزة الحاسوب و انظمة المعلومات ادوات مشتركة بين النقود الالكترونية و جريمة الاحتيال الالكتروني وهذا تأكيدا على طبيعتهما الواحدة.

الفرع الثاني

النقود الالكترونية محل جريمة الاحتيال الالكتروني

ان جريمة الاحتيال الالكتروني حسب ما تم تعريفها سابقا تقوم على تغيير الحقيقة بواسطة الحواسيب من اجل استيلاء على مال الغير و تسليمه طواعية و هذا ما يميز جريمة الاحتيال عن الجرائم الاخرى كالسرقة مثلا و التي تقوم على اخذ المال خفية او بالقوة اما الاحتيال يقوم على تسليمها طوعا للجاني ، و محل جريمة الاحتيال و

[1]– معهد الدراسات المصرفية ، الاحتيال الالكتروني– نشرة توعوية ، مجلة اضاءات ،العدد الاول، الكويت2008،ص 02.

نقصد هنا الاحتيال التقليدي حسب تعريفات الفقهاء مال مادي ملموس و هو ما يتعارض مع طبيعة الاحتيال الالكتروني و يفرقه عن نظيره التقليدي، "فمحل النشاط الإجرامي في هذه الحالة ليس مالا ماديا له كيان ملموس الا انه في إطار خصوصية الجريمة المعلوماتية فهو يصلح لان يكون محلا للاحتيال المعلوماتي ففكرة المال الملموس تتعارض مع الجريمة المعلوماتية فهذه الجريمة تقوم في أساسها على المعلومات والبيانات وبرمجتها بصورة الية، وفي بعض الأحيان في نقود وأعيان كأن يتمكن الجاني من سحب مبالغ نقدية من اجهزة الصرف الالي عن طريق بطاقة الائتمان بعد التوصل الى الرقم السري الخاص بها أو بتلاعب في بيانات أو برامج كي يستخرج الحاسب باسمه صكوك أو فواتير بمبالغ غير مستحقة يستولي الجاني عليها إلا انه في كثير من الحالات الأخرى يتمثل المحل في نقود كتابية كما لو تلاعب الجاني في البيانات أو البرامج كي يحول كل أو بعض أرصدة الغير أو فوائدها الى حسابه"[1]، حتى ان توافق الطبيعة بين جريمة الاحتيال الالكتروني و طبيعة النقود الالكترونية يجعل من النقود الالكترونية هي المحل الوحيد لهذه الجريمة حتى ولو تعددت اشكال نقود الالكترونية فانها في الاخيرة هي ذات قيمة مالية مخزنة او قيمة مالية الكترونية قد تكون خدمة فشكلها النهائي نقود الكترونية ، كون الاحتيال كجريمة واقع حتما على مال او ربح مما ينطبق على النقود الالكترونية كمحل لجريمة الاحتيال الالكترونية بدون ادنى شك.

الفرع الثالث

اثار الاحتيال الالكتروني على النقود الالكترونية

ان النتيجة الاجرامية في جريمة الاحتيال الالكترونية تتمثل في تسليم المال للجاني مما يعني ان هذه الجريمة تركت اثارا كغيرها من الجرائم في ممتلكاتهم و حقوقهم ومن هنا وجب علينا تبيان الاثار التي سببها الاحتيال الإلكتروني و نذكر على سبيل المثال لا الحصر الاثار التالية :

"مع بداية عصر الإنترنت في تسعينيات القرن الماضي وظهور خدمات البريد الإلكتروني ارتفعت عملية الاحتيال، وكانت الرسائل الإلكترونية التي تصل ممن يزعم أنه أمير نيجيري من أوائلها، وكانت تتمحور حول أمير نيجيري ثري (أو مستثمر، أو مسؤول حكومي) يعرض لك في رسالته فرصة لتحقيق مكاسب مالية مربحة.

ولكن الحيلة كانت في إغرائك في دفع جزء صغير من المبلغ مقدمًا، أو تسليم معلومات الحساب المصرفي، ومعلومات التعريف الأخرى؛ حتى يمكن إجراء التحويل. بالطبع، ستخسر "المال الأساسي"، ولن تتلقى أبدًا

[1]-سامر سلمان عبد الجبوري، المرجع السابق، ص ص:79-80.

سنتًا في المقابل. ومنذئذ لا تزال هذه الحيلة مستمرة، حتى أنها تطورت وتمكنت من جمع الملايين من أموال الاحتيال.

– "استخدم المخادع ويندي مردوخ، الذي زعم أنه رجل أعمال ومستثمر، عناوين البريد الإلكتروني وغيرها من التقنيات المقنعة، حيث تم خداع نجوم وسائل التواصل الاجتماعي لشراء رحلاتهم الخاصة إلى إندونيسيا، ودفع رسوم تصاريح مزيفة، كجزء من عملية الاحتيال. وكان من بين الضحايا أصحاب النفوذ، ومصورو السفر، الذين خسروا آلاف الدولارات في هذه العملية"[1].

– "الشرطة الدولية ''إنتربول INTERPOL ''ألقت القبض في عملية مشتركة مع لجنة الجرائم المالية والاقتصادية النيجيرية EFCC على رئيس شبكة إجرامية دولية تقف وراء الآلاف من عمليات الاحتيال عبر الإنترنت.

وأوضحت الإنتربول في بيان إنه يُعتقد أن المواطن النيجيري البالغ من العمر 40 عامًا، والمشهور باسم ''مايك''، يقف وراء عمليات احتيال تصل إلى أكثر من 60 مليون دولار أميركي وقع ضحيتها المئات في جميع أنحاء العالم، من بينها ضحية واحدة دفعت له مبلغ 15.4 مليون دولار"[2].

– "إذ تصاعدت عمليات الاحتيال من حالتين بألفي دولار في عام 2011 إلى 35 بلاغاً و80 طلب مساعدة في العام 2015، بينما وصلت تلك الحالات إلى 134 عملية في عام 2016 بقيمة خسائر صافية تبلغ 12 مليون ونصف المليون دولار فيما بلغ حجم خسائر النصف الأول من العام الجاري 4 ملايين دولار أميركي، وقع أكثرها على عاتق الأفراد أكثر من الشركات وفق إحصاء هيئة التحقيق الخاصّة بمكافحة تبييض الأموال وتمويل الإرهاب"[3].

[1]–البوابة العربية للاخبار التقنية ،أكثر عمليات الاحتيال الإلكتروني تعقيدا،موقع البوابة العربية للاخبار التقنية، انظر للموقع : www.aitnews.com/2019/04/01/أكثر-عمليات-الاحتيال-الإلكتروني-تعقى/ ، اخر زيارة للموقع بتاريخ:18-05-2019 بتوقيت23:36.

[2]–المرجع نفسه، انظر للموقع:www.aitnews.com/2016/08/02 /الإنتربول-تعتقل-زعيم-شبكة-عالمية-وراء/ ، اخر زيارة للموقع بتاريخ 1905-2019 بتوقيت 23:44.

[3]– عبد الرحمن عرابي، الاحتيال الإلكتروني... التخلف التقني للقطاع المصرفي اللبناني يمنع تفاقم القرصنة، ، نظر للموقع : www.alaraby.co.uk/investigations/2017/11/14/الاحتيال-الإلكتروني-التخلف-التقني-للقطاع-المصرفي-اللبناني-يمنع-تفاقم-القرصنة ، اخر زيارة للموقع بتاريخ:18-05-،2019 بتوقيت23:51.

– "أكد قائد وحدة مكافحة الجرائم الإلكترونية في مديرية الأمن العام ن واحدة من القضايا التي ضبطتها الوحدة قضية تتعلق بحوالات مالية بلغت الخسائر فيها 750 ألف دينار نتيجة الاحتيال الالكتروني، مشدداً على أهمية الحذر في التعامل الالكتروني بهذا المجال كي لا يقع المتعامل ضحية الاحتيال.

وتفاوتت نسب الجرائم خلال الأعوام الأربعة الأخيرة، فقد بلغت في العام 2013 (98) جريمة، بينما انخفضت قليلاً في العام الذي يليه الى (93) وفي العام 2015 انخفضت الى (91) جريمة، قبل أن ترتفع العام الفائت (2016) إلى 159 جريمة احتيال مالي الكتروني، فيما تُقدّر حتى منتصف العام الحالي إلى (56) جريمة"[1].

– "أكد النقيب محمد الخدري المكلف بتسيير أعمال مدير إدارة مكافحة الجرائم الإلكترونية بالإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني أن الإدارة تعمل على مكافحة الجرائم الإلكترونية بكافة أنواعها، وأوضح في مقابلة مع صفحة «الأمن» أن الإدارة تعاملت خلال عام 2016 مع 682 بلاغا، تركزت غالبيتها في إساءة استعمال أجهزة الاتصالات السلكية واللاسلكية، حيث بلغت البلاغات الواردة بهذا الشأن 339 بلاغا، يليها الاحتيال ب 82 بلاغا"[2]، مما يؤكد ان الاحتيال الالكتروني يعتبر في المرتبة الثانية في الجرائم الالكترونية في دولة البحرين في الجدول المبين في المقال المنشور في هذه الجريدة.

– و الملاحظ في الاثار السابقة لجريمة الاحتيال الالكتروني انها استهدفت الكثير من الاطراف منها الخاصة و العامة بشكل كبير و ضرر فادح وصل الى ملايين الدولارات في بعض الحالات مما قد يولد محاولات عديدة لصد هذه الظاهرة و ذلك حفاظا على الحقوق و حماية لها و هذا ما سنتناوله في المطلب القادم .

المطلب الثالث

الجهود و الاليات المبذولة لمكافحة جريمة الاحتيال الالكتروني

ان ظهور الاثار العميقة التي سببتها هذه الجريمة في الحياة الاقتصادية للأشخاص و المؤسسات و زعزعتها للذمم المالية كان لزاما منها باتخاذ تدابير و اليات لحماية حقوقها من هذه السلوكيات الخطيرة و قد كان ذلك في عديد من الجهود الدولية و الوطنية نسرد بعضها في الفروع الاتية:

[1]– اياد الفضولي، (56)جريمة احتيال مالي الكتروني إحداها "حوالة" بـ 750 ألف دينار، موقع هلا اخبار، الاردن، نشر بتاريخ: 16-05-2017، انظر للموقع:www.hala.jo/2017/05/16/56 -جريمة-احتيال-مالي-الكتروني-إحداها-حو/ ، اخر زيارة للموقع بتاريخ:19-05-2019 بتوقيت 00:09.

[2]– عبد الله الذيبان، مكافحة الجرائم الالكترونية، مجلة الامن، البحرين، بدون تاريخ، بدون صفحة

للاطلاع اكثر حمل من : www.policemc.gov.bh/mcms-store/pdf/b771c434-3124-4296-8a38-4f2931199362.pdf

الفرع الاول

الجهود الدولية و الوطنية لمكافحة جريمة الاحتيال الالكتروني

ان مجموع الجهود الدولية و الوطنية كانت متمثلة في تلك الاتفاقيات و القوانين الوطنية التي خصت الجرائم الالكترونية تحديدا –دون تخصيص جريمة الاحتيال الالكتروني بشيء محددا– و ذلك كسبيل لمكافحة هذه الجرائم و نذكر منها :

اولا: الجهود الدولية

من بين اهم ما جاءت به الجهود الدولية مايلي:

أ. **اتفاقية بودابيست:** "اما منظمة الأمم المتحدة، فقد أقرت تعريف الاحتيال المعلوماتي بناءا على توصية المجلس الأوربي رقم (R9/89) الذي جاء فيها " انه الادخال او المحو او التعديل او كبت البيانات أو برامج الحاسوب، او التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية أو فقد حيازة ملكية شخص آخر، بقصد الحصول على كسب اقتصادي غير مشروع له او الشخص آخر" وان جاز لنا انتقاد هذا التعريف فنلاحظ انه وان جاء شاملا واسع النطاق وتناول اساليب ارتكاب جريمة الاحتيال المعلوماتي ألا أن هذا النهج غالبا ما ينتقد لأنه بتعداده الأساليب ارتكاب الجريمة فانة يصبح قاصرا عن الاحاطة بالصور الجديدة التي قد تظهر بها هذه الجريمة مستقبلا لاسيما ونحن نعيش عصر تشهد فيه التقنية المعلوماتية تطورا متسارعا وبشكل يومي"[1].

ب. **قرار المجلس الاقتصادي والاجتماعي رقم39/2013** :المعنون "التعاون الدولي على منع الاحتيال الاقتصادي والجرائم المتصلة بالهوية والتحقيق فيها وملاحقة مرتكبيها قضائيا ومعاقبتهم" بإعداد دليلين إرشاديين عمليين بشأن الجرائم الحاسوبية والاحتيال الحاسوبي. وهما يشرحان أهم أركان وأنماط الجرائم الحاسوبية والاحتيال الحاسوبي، فضلاً عن أهم التدابير الفعالة للتحقيق في الجرائم والفصل في القضايا ذات الصلة لدى المحاكم . وقد وضع خبراء فنيون من العاملين في وحدة مكافحة غسل الأموال والجرائم الاقتصادية والبيئية

[1]– موفق علي عبيد، ساهر ماضي ناصر، ماهية جريمة الاحتيال المعلوماتي، مجلة جامعة تكريت للعلوم القانونية، العدد25،العراق2015، ص 198.

والجريمة المنظمة هذين الدليلين وهما متاحان لجميع العاملين في مجال الادعاء العام[1].

ج. **مؤتمر الامم المتحدة الثالث عشر لمنع الجريمة و العدالة الجنائية:** حيث ذكر مصطلح الاحتيال في تقرير لحلقة العمل 3 تحت عنوان "تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدِّي للأشكال المتطوِّرة للجريمة، مثل الجرائم الإلكترونية (السيبرانية) والاتجار بالممتلكات الثقافية، بما في ذلك الدروس المستفادة والتعاون الدولي" حيث جرمت الافعال التي تستعمل الحاسب و النظم المعلوماتية كوسائط لها للقيام بالجريمة و بينت مصطلح الاحتيال و ذلك في العنصر رقم 15 تحديدا الصفحة 08 من نفس الورقة و كذلك صرحت بنسب الاضرار الناجمة عن جريمة الاحتيال الالكترونية كجريمة الكترونية مقارنة بالاحتيال التقليدي في العنصر رقم23 في الصفحة 11 من هذه الورقة[2] ، فهذا التصريح و الاعتراف يعتبر اكبر دليل على وجود جهود دولية رامية لمكافحة هذه الجريمة و غيرها كما يساعد على دفع التعاون الدولي لمكافحتها.

ثانيا: الجهود الوطنية

تبقى الجهود الوطنية بخصوص جريمة الاحتيال الالكتروني متسمة بتطبيق القواعد العامة منها مع خلط في تطبيق جرائم المتعلقة بالاستخدام غير المشروع للأنترنت و اجهزة الاتصال مع ذلك لم تنعدم بعض التشريعات بتخصيص فعلي لبعض المواد بخصوص هذه الجريمة و نذكر بعض الجهود الوطنية في النقاط التالية:

أ. **المشرع القطري:** كان هو السباق في تقنين مصطلح الاحتيال الالكتروني حيث صرح به في قانون مكافحة الجرائم الالكترونية القطري رقم 14لسنة 2014، في الفصل الثالث تحت عنوان "التزوير و الاحتيال الالكتروني " في المادة رقم 11 و هذا نصها: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلاً من الأفعال التالية:

1-استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في انتحال هوية لشخص طبيعي أو معنوي.

2-تمكن عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، من الاستيلاء لنفسه أو لغيره على مال منقول، أو على سند أو التوقيع عليه، بطريق الاحتيال، أو باتخاذ اسم كاذب، أو بانتحال صفة غير صحيحة".

[1]- للاطلاع اكثر انظر الى تقرير معلومات عن الجهود التي تبذلها الدول الأعضاء لتنفيذ قرار المجلس الاقتصادي والاجتماعي رقم 39/2013 والسياسات والتدابير الوطنية في مجالات منع جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية والتحقيق فيها وملاحقة مرتكبيها قضائيا ومعاقبتهم، ماي 2014، ص 6.

[2]- انظر الملحق رقم 09

و من هنا يكون قد جمع المشرع القطري كل العناصر المكونة لتعريف جريمة الاحتيال الالكتروني محاولة منه مكافحة هذه الجريمة وتجريم الافعال القائمة عليها.

ب. المشرع البحريني : كذلك صنف انواع الجرائم بإصداره القانون رقم (60) لسنة (2014) بشأن جرائم تقنية المعلومات، و بهذا القانون اصبح المشرع البحريني من الدول السباقة في مكافحة الجرائم الحديثة ، حيث تم تجريم معظم السلوكيات الالكترونية الاجرامية الحديثة كالاختراق (المادة02)وإحداث التلف(المادة03) والتغيير وحجب البيانات(المادة03ف2) والتنصت (المادة04)والاستيلاء على الأموال بطرق احتيالية الكترونية(المادة08) ، وقد تطرقت المادة الاخيرة صراحة للاحتيال الالكترونية بالتنويه على الاستيلاء بطرق الخداع و الكذب على مال الغير في فقرتها الاولى[1].

ج. المشرع الفرنسي: لم ينص عليه صراحة بل اعتبره ضمن الاعمال الاجرامية الواقعة على انظمة المعالجة الالية للبيانات مثل الدخول و البقاء في المواد 232-1 الى 232-7 من قانون العقوبات الفرنسي[2].

د. **المشرع الجزائري**: حيث ان الاحتيال الالكتروني لم يحظى بالتخصيص التام من المشرع الجزائري بل طبقت عليه مبادئ القانون العام مثل استعمال خداع و الكذب في عمليات الاستيلاء في المادة 372 من قانون العقوبات اضافة الى الاستعمال العمدي عن طريق الغش للمساس انظمة المعالجة الالية للمعطيات والتي يستعملها الافراد و المؤسسات المالية في جوانب تمس النقود الالكترونية فانها تدخل ضمن الافعال المجرمة في المواد 394مكرر الى 394مكرر7 من نفس القانون و تجدر الاشارة الى ان استحداث خلايا مكافحة الجرائم على مستويات مديريات الامن الولائية و الدرك الوطني يعترف بها هي كذلك كونها جهود لمكافحة لمثل هذه الجرائم ،و كذلك ما نظمه قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام و الاتصال بإنشائه الهيئة المكلفة بمكافحة هذه الجرائم مصرحا في مادته الثانية نوع الجرائم التي يتكفل بها هذا القانون حيث يمكن ربك العلاقة بين الاحتيال الالكتروني و ادراجه ضمن هذه الجرائم كون يعتم اساسا على استعمال حاسوب في ذلك[3] ، كما نشير الى ان خلية معالجة الاستعلام المالي التابعة لوزارة المالية قد صرحت في

[1]- راجع الجريدة الرسمية البحرينية العدد:3178 الصادرة بتاريخ الخميس 09اكتوبر2014.

[2] -Nicole dausque : https://www.cppm.in2p3.fr/Jinfo/Dausque_legislation.pdf ,p16.

اخر زيارة للموقع بتاريخ 20-05-2019 بتوقيت:22:31.

[3] - انظر المادة 02 من قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام و الاتصال.

نشرتها التوعوية رقم 30 بمصطلح الاحتيال الإلكتروني "fraude informatique"[1] منوهة بالطرق التي يستعملها المحتالين للاستيلاء على اموال الضحايا و تحذيرا منها للوقوع تحت فخها .

و الملاحظ في الجهود الوطنية والدولية رغم محاولاتها الا انها تفتقر الى الحل العملي الحقيقي للحد من هذه الظاهرة وبقيت مجرد حبر على ورقة كون طبيعة هذه الجرائم ليست حسية او مادية ملموسة مما صعب تطبيق تلك الجهود غير انه يجب الالتفات تطوير الفرد و التوجه الى اليات تقنية و فنية تساعد على مكافحة هذه الجريمة و الجرائم المشابهة لها.

الفرع الثاني

الاليات الفنية و الادارية لمكافحة جريمة الاحتيال الالكتروني

ان العمل على مكافحة جريمة الاحتيال الالكتروني و غيرها من الجرائم الالكترونية لم يفلح بالوجه المطلوب من القوانين الصادرة لأجل ردعها كون هذه الجرائم غير ملموسة وصعبة الاثبات ولا تترك اثر على فاعلها مما يستوجب ايجاد حلول بديل سواءا تقنية كانت او ادارية تكون من مستوى هذه الجريمة و غيرها و من بين هذه الحلول نذكر:

كما ذكرنا سابقا في الحلول الفنية في جريمة القرصنة من تشفير و كلمات سر صعبة و مضادات فيروسات تعتبر حلول لهذه الجريمة(القرصنة) التي تعبر كأداة مساعدة للاحتيال الالكتروني نضيف الى ذلك ايضا :

1- "**استخدام جدار الحماية الناري** ويشبه هذا الجدار الحاجز بين طرفين اي بين الشبكة الداخلية المحلية لمؤسسة خاصة والشبكة العالمية العامة ليمنع تسريب البيانات الخاصة أو اختراق مجمع الشبكة الداخلية، بالإضافة الى استخدام رموز خاصة مثل كلمات مرور في التعاملات المالية.

المصادقة وهي تعد من أشهر طرق الحماية باستخدام كلمات مرور خاصة واسم مستخدم خاص للتحقق من شخصية المستخدم، باستخدام التوقيع الالكتروني بصمة اليد، بصمة العين ... وترددات موجة الصوت"[2] .

2- **التحكم بخصائص الدخول**، بان يتم تقسيم خصائص الدخول بحسب اسم المستخدم فان كان المستخدم عضوا يتم عرض المعلومات والخصائص الخاصة للأعضاء فقط وان كان من الإدارة يفتح له خصائص الإدارة وهكذا.

---

[1]-للاطلاع اكثر حمل النشرة:www.mf-ctrf.gov.dz/presse/Bulletin%2030%20Fraude%20informatique.pdf

[2]- معهد الدراسات المصرفية، المرجع السابق، ص ص:5-6.

3- "**التعرف على أسماء مواقع الاحتيال الالكترونية** المتورطة وادراجها في مختلف البرمجيات وخدمات التصفح و البريد الالكتروني بحيث يتم التعرف عليها تلقائيا لحماية المستخدمين من اي عملية احتيال عبر الإنترنت، أو إغلاق تلك المواقع التي تقوم بالاحتيال ومنع رسائل الاحتيال الإلكترونية من الوصول إلى المستهلكين وحاملي البطاقات حول العالم.

4- **التسوق عبر المواقع الالكترونية الآمنة والموثقة فقط**، مع التأكد من أن عنوان الموقع يبدأ بالأحرف <https> حيث أن حرف "S" يرمز إلى الكلمة "secure" أي أن الموقع المعني آمن تماما، أو التأكد من وجود صورة قفل عند أسفل يمين متصفح الانترنت الذي يستخدمه قبل القيام بعملية الشراء مع قراءة البنود الخاصة بها للحصول على معلومات دقيقة حول الإجراءات القانونية التي يمكن اتخاذها ضد التجار المشبوهين، ضرورة حفظ رقم التعريف الشخصي وعدم كتابته في أي مكان أو إرساله عبر الإنترنت، بالإضافة إلى وجوب التعامل بحرص مع البطاقات الإلكترونية كما تتعامل مع المبالغ النقدية"[1].

اما بخصوص التوعية الخاصة بالبنوك و المؤسسات المالية و حتى بالنسبة للأفراد فان احسن الاليات التي تساعد في مكافحة هذه الظهارة نذكر مايلي:

5- "إنشاء سياسة رسمية للبريد الإلكتروني :يرتفع عدد الموظفين الذين يقومون باستخدام هواتفهم الذكية الشخصية، أو اللوحات الشخصية وأجهزة الحواسيب الأخرى للعمل. فيمكنك استخدام سياسة للبريد الإلكتروني ليعلم الموظفين إذا كان مسموح لهم بتسجيل الدخول إلى البريد الالكتروني من أجهزتهم الشخصية.

وتستطيع سياسة البريد الالكتروني وضع بعض القواعد حول الدخول إلى البريد الالكتروني في حالة السفر من أجل العمل. على سبيل المثال:

يمكن أن تمنع السياسة دخول الموظفون إلى البريد الالكتروني باستخدام الحواسيب الآلية العامة (لأنه يمكن تثبيت برامج تسجيل الدخول) أو استخدام نقطة اتصال واي فاي عامة (لأنه يمكن أن تحدث الهجمات من خلالها)"[2].

[1]- معهد الدراسات المصرفية، المرجع السابق، ص6.

[2]- شركة دعائم التقنية،كيفية حماية البريد الالكتروني من الاختراق، للاطلاع اكثر انظر للموقع:www.it-pillars.com/ar/blog /كيفية-حماية-البريد-الالكتروني-؟/ ، اخر زيارة للموقع بتاريخ:19-05-2019 بتوقيت 13:17.

6- الاتصال المباشر بمصدر الرسالة: يجب ان تكون هذه الخطوة كخطوة اولى تبقى دائما في ذهن المواطن السبيط مبدا التأكد من أي رسالة و ان لا يقدم على أي شيء دون الاستفسار او الاتصال المباشر بمصدر الرسالة مما يجنبه الكثير من الاضرار التي قد تسببها جريمة الاحتيال الالكتروني.

7- **ثقافة التصفح الامن:** ان ثقافة التصفح الامن و عدم الانجرار وراء الروابط التي قد تحمل كوارث لا يحمد عقباها وجب ان تكون عند أي مستعمل للحاسوب او البريد الالكتروني او أي وسيلة اتصال بالانترنت مما قد تخبئه تلك الروابط او الرسائل من دسائس و اساليب ملتوية يقوم بها المحتالون ،وذلك عبر تفقد الرسائل بطرق فصح الروابط عن طريق نسخها و وضعها في مواقع الفحص و كذا الاحتيال عليها بوضعها في محركات بحث تكشف تلقائيا اذا كانت ملغمة ام لا بهذا تكون اول خطوة احترازية ضد الوقوع في مثل هذه الاساليب الاحتيالية.

8- **تطوير اساليب الحماية لدى المؤسسات المالية:** اما عن طريق تحديث البرامج المستعمل في عمليات الخدمة العادية(تحويلات سحوبات...) او بترقية مستوى الموظفين العاملين لديها و تكوينهم حسب مستجدات المجال التقني الذي لا يتوقف عن التطور مما قد يعكس ذلك على السلوكيات الاجرامية التي تضر المؤسسات و الافراد.

ان القيام بكل هذه الجهود و تطبيق كل هذه الاليات لا يكتمل الا بتواجد روح التعاون المشتركة بين كل الدول و الهيئات المحلية و الدولية و حتى الافراد و المؤسسات الخاصة و هذا من اجل حماية الحقوق المتمثلة في النقود الالكترونية و التي لابد ان تبقى في نشاطها و سيرورتها العادية في الحياة الاقتصادية بشكل لا يعيق المصالح المشتركة بين اطرافها .

خاتمة الفصل:

ان دراسة هاتين الجريمتين بكل تفاصيلهما قد اظهر الكثير من الصعوبات او العيوب القانونية التي تعاني منها الدول من بينها صعوبة الاثبات و معرفة مفتعلي الجرائم .

و رغم وجود بعض التشريعات التي صرحت مباشرة بتجريم ظاهرة القرصنة و الاحتيال الالكتروني ، اضافة الى وجود بعض المحاولات الاقليمية للحد من هذه الظواهر الا انها لا تصنف جميع الجرائم تصنيفا حقيقيا مما يجعل باب التطور الاجرامي في مجال قوانين و التهرب من العقوبات مفتوحا دائما بسبب هذا الغموض و العمومية التي تنقص من حجم الخطر الذي تحدث هذه الجرائم.

لذا يجب وضع دراسة مستقبلية قانونية او فنية تقنية كآلية حماية لما قد يحصل جراء تطور هذه الجرائم خصوصاً في هذه المرحلة التي يقبل فيها العالم على توسيع مجالات التكنولوجيا.

الخاتـــمة

الخاتمة

من خلال دراستنا للنقود الالكترونية بات جليا الدور الرئيسي الذي تلبعه هذه النقود ، من ميزات سهلت الكثير على البشرية في كل نواحي الحياة، سواًءا اقتصاديا أو اجتماعيا، ومما اعطاها قيمة ظهور ما يسمى بالأنترنت و التجارة الالكترونية هذان العنصران غيرا مجرى الحياة البشرية بشكل عكسيٍ تمامًا ، فكان من الضروري أن يتولاها(النقود الالكترونية) المشرع بالحماية، بنصوص قانونية تحدد المسؤولية الجنائية لكل معتدٍ كونها حق من الحقوق التي يجب حمايتها ، ولكن يظهر هنا فشل المشرع ولحد الساعة لا يوجد نص تشريعي في هذا المجال الا ما اتى به من اجل النقود الافتراضية في المادة 117 من قانون المالية لسنة2018 بالمنع التام لأي تعامل ، غير انه لا يخلو من كونه غطى مجموع الجرائم المتصلة بالأنترنت و استعمال وسائل المعالجة الالية المعطيات و التي لم تصرح صراحة بما يقع من جرائم على النقود الالكترونية.

ولعل بعض التشريعات الجزائية التي سبقتنا في إضافة لبعض انواع الجرائم الواقعة على النقود الالكترونية حمايةً جزائيةً خاصة، ومثل ما ذكرناه في موقف المشرعين القطري و بعض الدول الغربية التي نظمتها صراحة كاليابان و المانيا و الولايات المتحدة الامريكية.

وأخيرا ان قيامنا بهذه الدراسة يعتبر جهدا بسيطا و متواضعا ، هدفنا فيه توضيح هذا الموضوع في قالب علمي مطلوب لكن لا يجب أن يكون هذا حائلا دون التوسع في السلوكات الإجرامية التي تمس هذا الموضوع ، ولنصل في الختام إلى جملة من النتائج والتوصيات:

النتائج:

- النقود الالكترونية قيمة مالية مخزنة بطريقة الكترونية أي كانت الوسيلة المخزنة فيها قابل للتحويل و التبادل.
- ظهور العملة الافتراضية غير مفاهيم الدعم المادي و القانوني للنقود الالكترونية.
- رغم وجود قانون العقوبات 04-15 في قسمه السابع حول جرائم المعالجة الالية للمعطيات و قانون الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 09-04 ،فانه ينقص نص جزائي خاص يقرر عقوبات لبعض الجرائم مثل الاحتيال الإلكتروني في الجزائر.
- ضعف الرقابة المركزية على المؤسسات المالية المصرفية له دور كبير في انتشار هذا النوع من الجرائم المستحدثة.
- ضعف الرقابة على مواقع تبادل العملات الرقمية او الالكترونية يزيد من انتشار جريمة غسيل الاموال .

- مجرم الإلكتروني أخطر من المجرم التقليدي، لأنه صعب الاكتشاف ولا تبدو عليه ملامح الإجرام ويستغل ذكائه وخبرته التقنية لإرتكاب هذه الجرائم.
- صعوبة الكشف عن هذه الجرائم نظرا لطبيعتها غير المادية، وقابلية البيانات للحذف والإتلاف بسهولة لأنه يصل إليها من أي مكان بالعالم.

المقترحات:

1. على المشرع الجزائري ضرورة ايجاد نصوص صريحة خاصة بهذه الجرائم المستحدثة وعدم الاكتفاء بالنصوص التقليدية، كما يجب التحديث الدائم لهذه القوانين حتى تواكب كل التطورات الخاصة بهذه الجرائم.

2. ضرورة البحث المستمر والكشف عن هذه الجرائم، قصد اتخاذ إجراءات تتناسب مع مستوياتها التقنية العالية، تكون كفيلة بردعها والحد منه.

3. التكوين المستمر للجهات الأمنية المختصة في مكافحة هذه الجرائم بشكل دائم مع ما يتماشى ومستجدات تقنيات هذه الجرائم، وتوفير أحدث الوسائل والتجهيزات التقنية لضمان تحقيق أفضل النتائج.

4. إجراء دورات تحسيسية توعوية بالمخاطر المترتبة عن جرائم بطاقات الدفع الإلكتروني لفائدة جميع شرائح المجتمع، قصد تجنب وقوعهم كضحايا لهذه الجرائم من جهة، ومساهمتهم في الإبلاغ عنها من جهة أخرى.

5. عقد المؤتمرات والندوات العلمية بصفة دورية للوقوف على أحدث مستجدات هذه الجرائم.

6. تعزيز التعاون الدولي ودعوة إلى انضمام الجزائر للاتفاقيات والمعاهدات الأخرى التي تسعى لمكافحة هذا النوع من الجرائم.

مما سبق فقد حاولنا في هذه الدراسة أن نتناول موضوعا حديثا وهو الجرائم الواقعة على النقود الإلكترونية، والذي يعد من الموضوعات التي فرضت نفسها وبقوة خلال الفترة الحالية، لكونه يمثل إفرازا طبيعيا تولد عن التطور التكنولوجي والتقني الذي يشهده التعاملات الحاصلة في الحياة الاقتصادية و التجارة الالكترونية.

من خلال دراستنا وقفنا على بعض الجرائم التي قد تمس النقود الالكترونية، وخلصنا إلى أن ارتكابها اصبح صعب الاثبات مما يولد عبئا على التشريعات الجنائية كونها انشات محاولة منها لحماية الحقوق ، وبهذا و رغم الجهود التي وصلت اليها الدول و الافراد الا انها تعاب عليها النقص و اللافاعلية في بعض الجرائم وهذا ما ينطبق على المشرع الجزائري الذي يجب عليه النظر الى هذه النقطة الحساسة للسعي قدما بتعزيز ترسانته القانونية.

قائمة الملاحق

الملحق رقم :01

قانون رقم 17-11 مؤرخ في 8 ربيع الثاني عام 1439 الموافق 27 ديسمبر سنة 2017، يتضمن قانون المالية لسنة 2018.

المادة 117 : يمنع شراء العملة الافتراضية وبيعها واستعمالها وحيازتها.

العملة الافتراضية هي تلك التي يستعملها مستخدمو الإنترنت عبر شبكة الإنترنت، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو بالبطاقة البنكية.

يعاقب على كل مخالفة لهذا الحكم، طبقا للقوانين والتنظيمات المعمول بها.

صورة تبين المادة رقم 117 من قانون المالية لسنة 2018

المصدر : قانون المالية لسنة 2018

الملحق رقم :02

أبرز الدول الداعمة والرافضة للبتكوين			
دول داعمة	**دول محايدة**	**دول تفرض قيودًا**	**دول تحظر البيتكوين**
الولايات المتحدة	كازاخستان	الصين	وسيا
كندا	الهند	المكسيك	بوليفيا
أستراليا	باكستان	زامبيا	الإكوادور
البرازيل	كينيا	موريشيوس	أفغانستان
تشيلي	نيجيريا	جزر المالديف	
جنوب أفريقيا	الجابون	فانواتو	
كوبا	فنزويلا		
آيسلاندا	كولومبيا		
النرويج	بيرو		
اليابان	باراجواي		
نيوزيلندا	أوروجواي		
المملكة المتحدة	الأرجنتين		
إيرلندا	فيتنام		
فرنسا	ماليزيا		
إيران	إندونيسيا		
تركيا			
تايوان			
هونج كونج			

جدول: ابرز الدول الداعمة و الرافضة للبتكوين في الدول الغربية

المصدر: www.argaam.com/ar/article/articledetail/id/526420

الملحق رقم :03

الوضع القانوني للبتكوين في الدول العربية			
دول داعمة	**دول محايدة**	**دول تفرض قيودًا**	**دول تحظر البتكوين**
ليبيا	تونس	السعودية	الجزائر
العراق		مصر	المغرب
الإمارات			

جدول: الوضع القانوني للبتكوين في الدول العربية

المصدر: www.argaam.com/ar/article/articledetail/id/526420

الملحق رقم :04


١) عمليات ذات علاقة بالفساد (الفساد لتسهيل غسل الأموال وتمويل الإرهاب).
٢) غسل عائدات الفساد.
٣) استغلال الجمعيات الخيرية لتمويل الإرهاب.
٤) استخدام البنوك غير المقيمة (offshore banks) والشركات التجارية الدولية، والصناديق الاستئمانية في الخارج (offshore trusts).
٥) استخدام العملات الافتراضية (virtual currencies).
٦) استخدام الخدمات المهنية (المحامين وكتاب العدل والمحاسبين).
٧) غسل الأموال القائم على التجارة (Trade based money laundering) .
٨) الخدمات المصرفية الموازية (underground banking) / خدمات التحويلات البديلة / الحوالة).
٩) استخدام الإنترنت (التشفير ، الوصول إلى البيانات الشخصية، الأعمال المصرفية الدولية، إلخ).
١٠) استخدام وسائل ونظم الدفع الجديدة.
١١) غسل العائدات المتأتية من الجرائم الضريبية.
١٢) العقارات، بما في ذلك دور وكلاء العقارات.
١٣) تجارة الأحجار الكريمة والمعادن الثمينة.
١٤) الاتجار بالبشر وتهريب الأشخاص.
١٥) استخدام المخولين (nominees)، والصناديق الاستئمانية (Trust)، وأفراد الأسرة أو أطراف أخرى...
١٦) أنشطة القمار (الكازينوهات، سباق الخيل، المقامرة عبر الانترنت وغيرها).
١٧) مشتريات ثمينة (الأعمال الفنية والآثار وخيول السباق والسيارات، الخ).
١٨) الاستثمار في أسواق رأس المال واستخدام وسطاء.
١٩) الخلط (Mingling) : خلط العائدات غير المشروعة مع الأموال المشروعة واستثمارها في الأعمال التجارية.
٢٠) استخدام شركات وهمية.
٢١) تمويل انتشار أسلحة الدمار الشامل (WMD).
٢٢) قطع الأشجار غير المشروع.
٢٣) تحويل العملات (currency exchange).
٢٤) تهريب العملة.
٢٥) استخدام بطاقات الائتمان والشيكات والكمبيالات...الخ.
٢٦) التجزئة (structuring / smurfing).
٢٧) التحويلات المالية / استخدام الحسابات المصرفية في الخارج.
٢٨) تبادل السلع (المقايضة – على سبيل المثال إعادة الاستثمار في المخدرات غير المشروعة).
٢٩) استخدام هوية مزورة.
يرجى الإطلاع على الملحق رقم (٣) للحصول على أمثلة توضيحية.

الصورة تبين الحالات العملية لجريمة غسيل الاموال

المصدر : تقرير التطبيقات الدوري(كل سنتين) بمجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا MENAFATF 2014م، ص:62.

الملحق رقم:05

	2018/01/07 - 21:59 ayache	1228	1	2017/12/19 - 19:30 ayache	"" تنبيه مهم "" قد أعذر من أنذر - دخول اصحاب الوصف الازرق اجباري -
	2017/10/29 - 08:37	1795	1	2017/10/01 - 19:22	من يتعرض للنصب من اصحاب الوصف انا المسؤول عن أرجاع المال له$ 300 الله شاهد على كلامي
		2912	0	2015/10/14 - 16:20	اعـــــلان | كيفية وضع صورة من حسابك بشكل صحيح ليتم قبول موضوعك | تجاهل = رقابة
	اليوم - 03:25 hou1990ssam	47	4	17:38 - يوم أمس hou1990ssam	للبيع 85 اورو بايسيرا مقابل ccp
	اليوم - 02:04 bilal you	148	17	04:15 - أول أمس	متوفر PaySera €300 مقابل 218 دينار ccp أو بريدي
	اليوم - 00:06	285	47	05/24 - 12:28	متوفر Paysera € 300 مقابل CCP - BARIDIMOB - LTC * ETH * BTC
	يوم أمس - 23:42 InConNu Dz	261	17	05/17 - 22:38 InConNu Dz	مطلـــوب 300 $ |payoneer| بسعر جيـــد
	يوم أمس - 20:12 Cris 09	71	12	05/25 - 16:43 Djamel_jimmy	بـــيع 300 اورو Paysera / واحد اورو= 220 دج CCP - B
	يوم أمس - 19:43	53	8	05/25 - 19:05	(طلب) مطلوب 300 $ مقابل الدرهم Payoneer && &&
	يوم أمس - 19:11 houssem08	363	51	04/06 - 13:40 naouri_dz	بـــيع 300 أورو سكريل SKRILL مقابل للتحقق
	يوم أمس - 18:35 iMaD MaDaNi	165	12	05/01 - 13:12 InConNu Dz	مطلـــوب 300 $ |Skrill| بسعر جيـــد
	يوم أمس - 12:55 BIBIS	444	40	02/04 - 16:42 zouidzz	مطلوب 100 اورو بايسارة مقابل ccp
	يوم أمس - 12:14 Notomy	112	10	05/25 - 21:16 Notomy	متوفر 300 € اورو رصيد بايسيرا ~ Paysera مقابل CCP
	يوم أمس - 01:31 Amine med 94	364	16	04/03 - 23:49	متوفر PayPal €300 مقابل 210 دج
	يوم أمس - 00:12 iMaD MaDaNi	196	20	04/23 - 22:28 Notomy	مطلوب $300 سكريل ~ Skrill مقابل CCP
	أول أمس - 23:27 Master-str	134	8	05/18 - 21:01 avatar999	(طلب) مطلوب 300 دولار webmoney بسعر مناسب مقابل ccp.. للتحقق
	أول أمس - 23:08 africafm	142	10	05/24 - 17:06 africafm	متوفـــر 185 € [PAYSERA] بايسيرا مقابـــل CCP للتحقق
	أول أمس - 23:03 leva	98	21	05/18 - 20:08 leva	بـــيع 300 اورو Paysera / واحد اورو= 220 دج

الصورة تبين مواضيع البيع و الشراء للعملات الالكترونية و تحويلها

المصدر :منتدى ستار7العرب–قسم تبادل العملات

الملحق رقم:06

الصورة تبين مواضيع البيع و الشراء للعملات الالكترونية و تحويلها

المصدر :منتدى الجلفة-قسم بيع و شراء العملات الالكترونية-.

الملحق رقم :07

جامعة الدول العربية
الامانة الفنية لمجلس وزراء العدل العرب

قانون الإمارات العربي
الاسترشادي لمكافحة جرائم
تقنية المعلومات وما في حكمها

اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495 - د19 - 2003/10/8
ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 – د 21/ 2004

المادة (3) :

كل من دخل عمداً وبغير وجه حق موقعاً أو نظاماً معلوماتيا يعاقب بالحبس ... والغرامة ..... أو بإحدى هاتين العقوبتين .

فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصية يكون الحد الأدنى لعقوبة الحبس ..... ولعقوبة الغرامة.....

الصورة تبين القانون الاماراتي العربي الاسترشادي المادة 03

المصدر: القانون الاماراتي العربي الاسترشادي

الملحق رقم:08

25 شعبان عام 1430 هـ
16 غشت سنة 2009 م

الجريدة الرّسميّة للجمهوريّة الجزائريّة / العدد 47

5

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

المصدر : قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال

الملحق رقم:09

A/CONF.222/12

الأمم المتحدة

Distr.: General
2 February 2015
Arabic
Original: English

مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية

الدوحة، ١٢-١٩ نيسان/أبريل ٢٠١٥

البند ٥ من جدول الأعمال المؤقت*

النُهُج الشاملة الموازنة لمنع ظهور أشكال جديدة ومستجدّة للجريمة العابرة للحدود الوطنية والتصدّي لها على نحو ملائم

حلقة العمل ٣: تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدّي للأشكال المتطوّرة للجريمة، مثل الجرائم الإلكترونية (السيبرانية) والاتجار بالممتلكات الثقافية، بما في ذلك الدروس المستفادة والتعاون الدولي**

٢٣- وتوفّر استقصاءات الإيذاء الخاصة بالأفراد والمنشآت التجارية والتي تتناول فئات محدَّدة من عامة السكان مصدراً بديلاً مهمًّا للمعلومات. وتدلُّ تلك الإحصاءات على أنّ حالات تَأَذّي عامة السكان بالجريمة السيبرانية هي أكثر بكثير من تَأَذّيهم بأشكال الجرائم "التقليدية". إذ إنّ نسب التأذّي من الاحتيال المتعلق ببطاقات الائتمان عبر الإنترنت وسرقة الهوية والاستجابة لمحاولات التصيُّد الاحتيالي والتعرُّض لحالات نفاذ غير مأذون به إلى حساب البريد الإلكتروني تتراوح بين ١ و١٧ في المائة من إجمالي مستعملي الإنترنت في ٢١ بلداً من مختلف أنحاء العالم، في حين أنّ نسبة المتأذّين بالجرائم المعتادة، مثل السطو والسلب وسرقة السيارات تقلُّ عن ٥ في المائة في البلدان ذاتها.[٢١] وتفيد منشآت القطاع الخاص أيضاً عن نسب إيذاء مماثلة. ففي أوروبا، مثلاً، تفيد المنشآت عن نسب تعرُّض للإيذاء تتراوح بين ٢ و١٦ في المائة نتيجةً لأفعال مثل انتهاك البيانات الناشئ عن الاقتحام أو التصيُّد الاحتيالي.[٢٢] وتَبيَّن من دراسة أُجريت في عام ٢٠١٢ أنّ عدد ضحايا الاحتيال المتعلق بالهوية ازداد بما يزيد على ١ مليون ضحية، سرق فيها الجناة ما يزيد على ٢١ بليون

المصدر : مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية حلقة العمل3 : تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدّي للأشكال المتطوِّرة للجريمة، مثل الجرائم الإلكترونية(السيبرانية) والاتجار بالممتلكات الثقافية، بما في ذلك الدروس المستفادة والتعاون الدولي-العنصر رقم23-.

قائمة المراجع

اولا: المصادر:

- **القران الكريم.**

اولا: المصادر:

- **القران الكريم.**

ثانيا : المراجع

1. **النصوص القانونية:**

أ. **النصوص التشريعية:**

- **الاتفاقيات:**

• اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية(باليرمو) اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 نوفمبر 2000.

• الاتفاقية العربية لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية وافق عليها مجلس الوزراء الداخلية العرب بقرار رقم 215 الصادر بتاريخ 15-01-1994 في دورته 21.

• اتفاقية بودابست لمكافحة الجرائم المعلوماتية اعتمدت من لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة 8 نوفمبر 2001 وفتح باب التوقيع على الاتفاقية في بودابست، في 23 نوفمبر 2001.

• الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21ديسمبر 2010 صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252المؤرخ في 8سبتمبر 2014، الجريدة الرسمية للجمهورية الجزائرية، عدد 75، الصادرة بتاريخ 28سبتمبر 2014.

• قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها. اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495- د19 – 10/8/ 2003 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417- د 2004/21.

- **القوانين:**

• القانون 05-01 المؤرخ في 06 فيفري2005 المتعلق بمحاربة تبييض الأموال وتمويل الإرهاب ومكافحتهما.

- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156، المتضمن قانون العقوبات الجزائري.
- القانون 09-04 المؤرخ في 05أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم تكنولوجيا الإعلام والاتصال ومكافحتها.
- قانون المصري لمكافحة جرائم تقنية المعلومات رقم 175 الصادر بتاريخ 14 اوت 2018 في الجريدة الرسمية رقم 32 مكرر(ج).
- القانون البحريني رقم القانون رقم (60) لسنة (2014) بشأن جرائم تقنية المعلومات، الجريدة الرسمية البحرينية العدد:3178 الصادرة بتاريخ الخميس 09اكتوبر2014.
- القانون القطري لمكافحة الجرائم الإلكترونية رقم 14الصادر بتاريخ 15-09-2014، الجريدة الرسمية القطرية رقم 15 الصادرة بتاريخ 02-10-2014.
- القانون الفرنسي رقم 91-1382 المؤرخ 30 ديسمبر 1991 بشأن أمن الشيكات وبطاقات الائتمان.
- الأمر رقم 03-11المؤرخ في 27جمادى الثانية عام 1424الموافق لـ 26غشت سنة 2003، يتعلق بالنقد والقرض، الجريدة الرسمية للجمهورية الجزائرية، عدد52، الصادرة بتاريخ 27 غشت سنة 2003.

ب. النصوص التنظيمية:

- المرسوم التنفيذي 02-127 المؤرخ في 24 محرم 1423 الموافق 7 أفريل 2002 المتضمن انشاء وتنظيم وسير خلية معالجة الاستعلام المالي.

2. الكتب:

- ابن فارس، **معجم مقاييس اللغة**، تحقيق عبد السلام هارون، مطبعة عيسى البابي الحلبي وشركاه، القاهرة، 1972.
- ابن منظور جمال الدين بن مكرم الانصاري، **لسان العرب**، دار صادر،بيروت،2003.
- احمد مختار عمر وفريقه، **معجم اللغة العربية المعاصرة**، عالم الكتاب للنشر والتوزيع والنشر، مصر، 2008.
- باطلي غنية، **الجريمة الإلكترونية "دارسة مقارنة"**، الدار الجزائرية للنشر والتوزيع، الجزائر،2015.

- شريف محمد غنام، محفظة النقود الإلكترونية (رؤية مستقبلية)، دار النهضة العربية، مصر، بدون سنة نشر.
- مجد الدين محمد بن يعقوب الفيروزأبادي، **القاموس المحيط**، مؤسسة الرسالة للطباعة والنشر، لبنان، 2005 .
- مجمع اللغة العربية، **المعجم الوسيط**، مكتبة الشروق الدولية، مصر،2004.
- كميت طالب بغدادي ، **الاستخدام غير المشروع لبطاقة الائتمان (المسؤولية الجزائية والمدنية)**، دار التقافة للنشر و التوزيع، الاردن، 2008.
- هلال درويش، **اقتصاديات نقدية تاريخ – حركة – تشريع**، دار المعرفة، لبنان، 2007.

3. الابحاث الاكاديمية:

أ. اطروحات:

- بن الاخضر محمد، **الاليات الدولية لمكافحة جريمتي تبييض الاموال و تمويل الارهاب الدولي**، اطروحة دكتوراه، جامعة تلمسان، الجزائر، 2015.
- بن تركي ليلى، **الحماية الجنائية لبطاقة الائتمان الممغنطة**، رسالة دكتوراه، جامعة منتوري، الجزائر، 2017.
- شول بن شهرة، **الحماية الجنائية للتجارة الالكترونية**، رسالة دكتوراه، جامعة بسكرة، الجزائر، 2010.
- صالح شنين، **الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)**، رسالة دكتوراه، جامعة تلمسان، الجزائر، 2013.

ب. رسائل:

- احمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم04/09**، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر،2013.
- حمد عبدالله حيي بو غانم السليطي، **تجريم الاحتيال الإلكتروني في القانون القطري والمقارن**، رسالة ماجستير، جامعة قطر، قطر،2018.

- خوجة جمال، **جريمة تبييض الاموال –دراسة مقارنة**، رسالة ماجستير، جامعة تلمسان، الجزائر،2008 .
- سامر سلمان عبد الجبوري، **الاحتيال الإلكتروني**، رسالة ماجستير، جامعة النهرين، العراق،2014 .
- فيصل بن عادل ابو خلف، **الحماية الجنائية لبطاقات الائتمان**، رسالة ماجستير، جامعة نايف، السعودية، 2008.
- لوصيف عمار، **استراتيجيات نظام المدفوعات للقرن الحادي والعشرين**، رسالة ماجستير، جامعة منتوري، الجزائر،2009.
- نورا صباح عزيز الجزراوي، **أثر استعمال النقود الإلكترونية على العمليات المصرفية**، رسالة ماجستير، جامعة الشرق الأوسط للدراسات العليا، الاردن، 2011.
- واقد يوسف، **النظام القانوني للدفع الإلكتروني**، رسالة ماجستير، جامعة تيزي وزو،الجزائر،2011.

ج. مذكرات:

- خولة بوقديرة، **الجرائم الواقعة على بطاقات الدفع الالكتروني**، مذكرة ماستر، جامعة ام البواقي، الجزائر، 2018.

2. المقالات :

- إبراهيم محمد شاشو، **بطاقة الائتمان حقيقتها وتكييفها الشرعي**، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد السابع والعشرون، العدد الثالث، سوريا،2011 .
- باسم علوان العقابي وعلاء عزيز الجبوري ونعيم كاظم جبر، **النقود الإلكترونية ودورها في الوفاء بالالتزامات التعاقدية**، مجلة اهل البيت، العدد 06، العراق،2008.
- باطلي غنية، **خصائص وأشكال النقود الإلكترونية: دراسة تحليلية نظرية**، مجلة العلوم السياسية والقانون، العدد07، ألمانيا، 2018 .
- بسام أحمد الزلمي وعبود سراج، **دور النقود الإلكترونية في عمليات غسيل الأموال**، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، سوريا، 2010.

- زياد خلف عبد الله الجبوري، محمد شطب عيدان المجمعي، **القرصنة التكنولوجية واثرها على العلاقات الامريكية–الصينية**، مجلة جماعة تكريت للعلوم الانسانية،المجلد15، العدد التاسع، العراق، 2008.
- عبد الله الذيبان، **مكافحة الجرائم الإلكترونية**، مجلة الامن، البحرين، بدون سنة.
- عبد الله عزت بركات، **ظاهرة غسيل الاموال واثارها على الاقتصادية والاجتماعية على المستوى العالمي**، مجلة اقتصاديات شمال افريقيا، العدد الرابع، الجزائر، 2010.
- عبدالله بن سليمان بن عبدالعزيز الباحوث، **النقود الافتراضية مفهومها وأنواعها وآثارها الاقتصادية**، المجلة العلمية للاقتصاد والتجارة، العدد 01، مصر، 2017.
- فريد علواش، **جريمة غسل الأموال – المراحل والأساليب**، مجلة العلوم الانسانية، العدد الثانية عشر، الجزائر، 2007.
- لتيم فتيحة- لتيم نادية، **الامن المعلوماتي للحكومة الإلكترونية وارهاب القرصنة**، مجلة المفكر، الجزائر، 2015.
- محمد خليل يوسف جندي، **المواجهة التشريعية للجريمة المعلوماتية على المستوين الدولي والوطني (دراسة مقارنة)**، مجلة كلية القانون للعلوم القانونية والسياسية، العدد36، العراق، 2018.
- مسعد عبدالرحمن زيدان، **المعالجة القانونية لجريمة غسل الأموال في ضوء أحكام القانون الدولي**، مجلة العربية للدراسات الامنية، العدد 69، السعودية،2017.
- معهد الدراسات المصرفية، **الاحتيال الإلكتروني**، مجلة اضاءات، العدد الاول، الكويت، 2008.
- موفق علي عبيد، ساهر ماضي ناصر، **ماهية جريمة الاحتيال المعلوماتي**، مجلة جامعة تكريت للعلوم القانونية، العدد25، العراق، 2015.
- نهى خالد عيسى الموسري وإسراء خضير مظلوم الشميري، **النظام القانوني للنقود الإلكترونية**، مجلة جامعة بابل للعلوم الإنسانية، المجلد22، العدد 2، 2014.

3. المؤتمرات والملتقيات:

- شايب محمد، **تأثير النقود الإلكترونية على دور البنك المركزي في إدارة السياسة النقدية**، الملتقى الدولي الخامس حول الاقتصاد الافتراضي وانعكاساته على الاقتصاديات الدولية، المركز الجامعي بخميس مليانة، الجزائر، 13- 14 مارس 2012.
- طايل كايد المجالي، **النماذج العربية والدولية في مكافحة غسل الاموال**، حلقة علمية بعنوان "غسل الأموال وأثره في انتشار المخدرات، السعودية، 11-13 جوان 2012.
- محمد إبراهيم محمود الشافعي، **الآثار النقدية والاقتصادية و المالية للنقود الإلكترونية**، بحث مقدم في مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الامارات، 10- 12ماي 2003.
- نمديلي رحيمة، **خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة**، أعمال المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، ليبيا، 25 - 24مارس 2017 .

4. منشورات وتقارير:

- البنك المركزي الاوروبي، **تقرير حول النقود الإلكترونية**، المانيا، 1998.
- محمد فتحي عيد، **الإجرام المعاصر**، منشورات أكاديمية نايف للعلوم الأمنية، السعودية، 1999.
- مركز هاردو، **التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات**، مصر،2018.

5. المواقع:

- راوول، تصور حول مشروعية بيتكوين حول العالم https://howmuch.net/articles/bitcoin-legality-around-the-world.
- محمد فرج عبد العزيز ابو ريشة، جرائم الانترنت، www.aboudreisha-law.com/جرائم-الانترنت.
- شبكة قدس الاخبارية، البرمجيات الخبيثة واساليب، www.qudsn.co/post/58085/البرمجيات-الخبيثة-وأساليب-القرصنة.
- المجلة، البنوك وأسواق المال في مرمى القرصنة، www.arb.majalla.com/2018/07/article55267586/البنوك-وأسواق-المال-في-مرمى-القرصنة.

- موقع الجزيرة :
www.aljazeera.net/knowledgegate/newscoverage/2015/1/5/القرصنة-الإلكترونية-سلاح-العصر-الرقمي.
- مروان رجب، 10 ملايين دولار خسائر بنك كويتي جراء قرصنة إلكترونية،
http://www.thenewkhalij.news/اقتصاد/10-ملايين-دولار-خسائر-بنك-كويتي-جراء-قرصنة-إلكترونية.
- جريدة البلاد، قرصنة موقع بنك "بدر"، www.elbilad.net/article/detail?titre=قرصنة-موقع-بنك-بدر&id=94743K.
- موقع روتانا، أكبر حادث سرقة رقمية في العالم لشركة يابانية، www.rotana.net/أكبر-حادث-سرقة-رقمية-في-العالم-لشركة-يا/.
- حنين ياسين، كيف تستنزف "حرب السايبر" 600 مليار دولار سنوياً من اقتصاد العالم؟،
www.alkhaleejonline.net/اقتصاد/كيف-تستنزف-حرب-السايبر-600-مليار-دولار-سنوياً-من-اقتصاد-العالم؟.
- موقع الجزيرة، www.aljazeera.net/news/scienceandtechnology/2015/1/6/البرمجيات-الخبيثة-وأساليب-القرصنة.
- بنك إتش إس بي سي الشرق الأوسط، الجرائم الإلكترونية، www.business.algeria.hsbc.com/ar-dz/cybercrime.
- البوابة العربية للأخبار التقنية، اكثر عمليات الاحتيال الإلكتروني تعقيدا،
www.aitnews.com/2019/04/01/أكثر-عمليات-الاحتيال-الإلكتروني-تعقي/.
- عبد الرحمن عرابي، الاحتيال الإلكتروني... التخلف التقني للقطاع المصرفي اللبناني يمنع تفاقم القرصنة،
www.alaraby.co.uk/investigations/2017/11/14/الاحتيال-الإلكتروني-التخلف-التقني-للقطاع-المصرفي-اللبناني-يمنع-تفاقم-القرصنة.
- اياد الفضولي،(56) جريمة احتيال مالي الكتروني إحداها "حوالة" بـ 750 ألف دينار،
www.hala.jo/2017/05/16/56-جريمة-احتيال-مالي-الكتروني-إحداها-حو/.
- شركة دعائم التقنية، كيفية حماية البريد الإلكتروني من الاختراق، www.it-pillars.com/ar/blog/كيفية-حماية-البريد-الالكتروني-؟/.
- بوابة الشرق الالكترونية، www.al-sharq.com/article/11/01/2019/هذه-أسباب-جرائم-الاحتيال-الإلكتروني-والداخلية-تحذر-من-التجاوب-مع-الرسائل-المجهولة.

A. Les livres :

- Jeffrey H .Mastuura, **digital currency : An International Legal and Regulatory Compliance Guide**, Bentham Science Publishers, U.A.E, 2016.
- P,Carl Mullan,**The Digital Currency Challenge**, Palgrave Advances in the Economics of Innovation and Technology, United Kingdom,2014 .
- P. Carl Mullan,**A History of Digital Currency in the United States**,**New Technology in an Unregulated Market**, Palgrave Advances in the Economics of Innovation and Technology, United Kingdom,2016.

B. les Recherches académiques :

- Micheal Kunzand Patrick Wilson : **computer crime and computer fraud** , the Professional Masters Degree, Univesity of Mayland , 2004

C. Les articles :

- Rolf van Wegberg and Others, **Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin**, Journal of Financial Crime, Netherlands, 2018.

D. Publications et rapports :

- Bank for International Settlements (BIS, I**mplication for central banks of the development of electronic money**, 1996.
- Céllule de Traitement du Renseignement Financier , **Fraude informatique, lettre information N°30, Sans date.**
- Deutsche Bundesbank, **Annual Report** ,2014.
- European Banking Authority ,**Opinion on "virtual currencies"**, 4 July 2014.
- IMF Staff Team, **Virtual Currencies and Beyond: Initial Considerations**, International Monetary Fund, 2016.
- Office of Inspector General Department of the Treasury, **fin CEN Continues to Face Challenges with Money Services Businesses**, 2015.
- Solliciteur Général et de la Justice du Canada, **Le Blanchiment de la Monnaie Electronique**, Canada, 1998.
- valérie bugault , **nature juridique et fonction politique des monnaies et cryptomonnaies**, Octobre 2018.

E. Les sites :

- https://howmuch.net/articles/bitcoin-legality-around-the-world.
- www.fsa.go.jp/.
- http://www.insecure.in/hacktools_02.asp.
- www.yourdictionary.com/e-fraud.
- www.mf-ctrf.gov.dz/presse/Bulletin%2030%20Fraude%20informatique.pdf
- https://voxeu.org/article/electronic-money-enhancement-or-replacement.

الفهـــرس