جامعة محمد خيضر بسكرة
كلية الحقوق والعلوم السياسية
قسم القانون عام

مذكرة ماستر

ميدان: الحقوق والعلوم السياسية
فرع: الحقوق
تخصص: قانون جنائي.

رقم: .....

إعداد الطالب:
قيري ندى
شخاب شيماء.

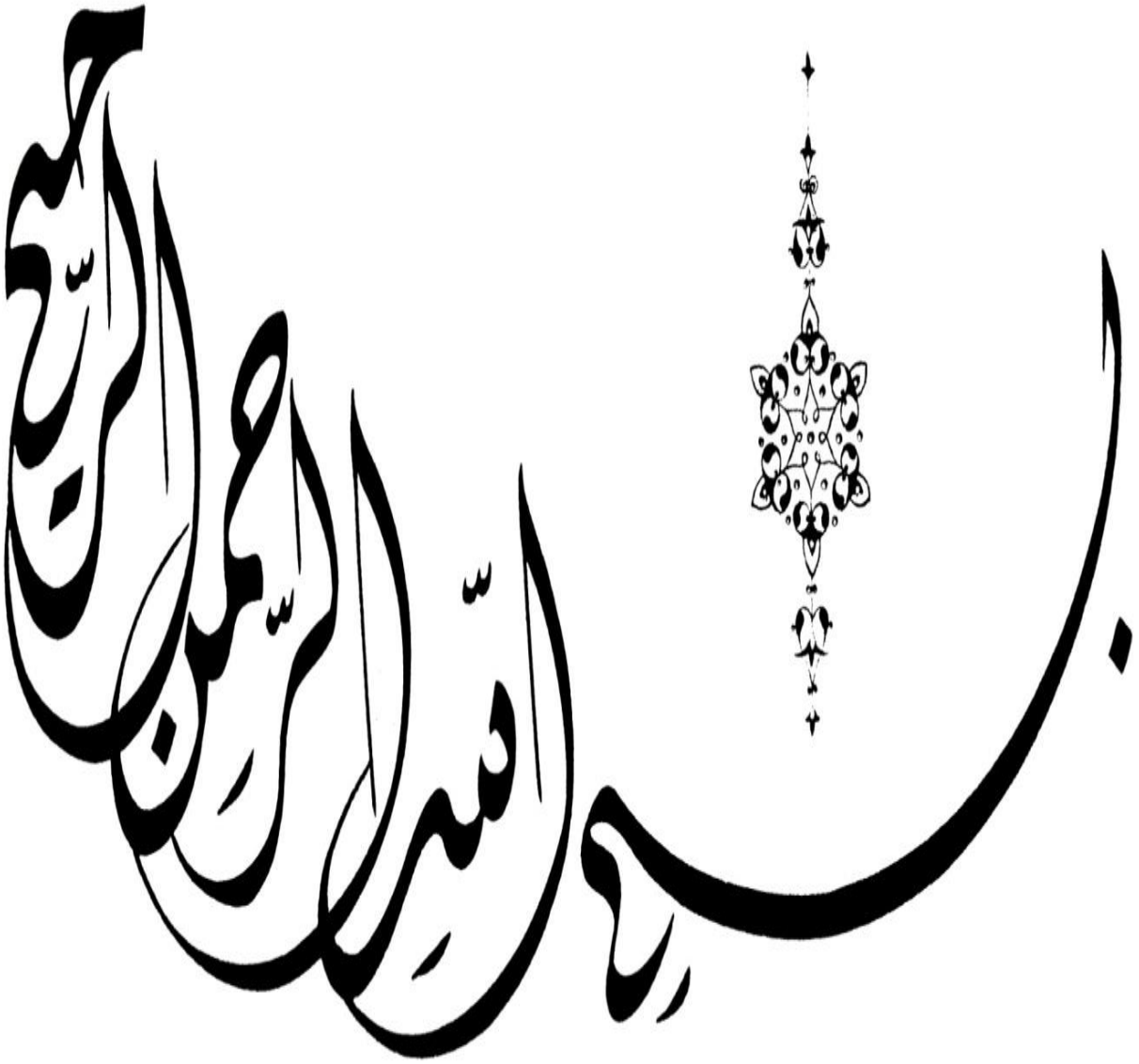
يوم: .....

جريمة الاحتيال الإلكتروني في التشريع الجزائري

لجنة المناقشة:

العضو 1	الرتبة	الجامعة	رئيسا
دعدوعة عبد المنعم	أ.مح .أ	جامعة محمد خيضر بسكرة	مشرفا
العضو 3	الرتبة	الجامعة	مناقشا

السنة الجامعية: 2025 -2026



شكر وعرفان

الحمد والشكر لله الحي القيوم أولاً وآخراً وامتثالاً لقوله صلى الله عليه وسلم
من لا يشكر الناس لا يشكر الله"
نتوجه بجزيل الشكر وجميل العرفان للأستاذ "دعدوعة عبد المنعم"
الذي تكرم بقبول الإشراف على هذه المذكرة وعلى جميع التوجيهات والملاحظات والنصائح
فلقد كان نعم المرشد ونعم المعين والذي منحنا الكثير من وقته وصبره
فلولا تفضله علينا لما استطعنا إتمام هذه المذكرة
كما لا يفوتنا أن نتقدم بوافر التقدير والاحترام لأعضاء اللجنة المحترمين على إثراء قراءة
المذكرة وقبولها وتصويبها. وكذلك نتقدم بخالص الشكر إلى كل من درسنا من أساتذة كلية
الحقوق والعلوم السياسية بجامعة بسكرة
وإلى كل موظفي المكتبة وجزاهم الله كل خير وفي الأخير نشكر كل من قدم لنا يد العون
والمساعدة من قريب أو من بعيد ونسأل الله
عز وجل أن يجعل ذلك في ميزان حسناتهم إنه قريب مجيب

اهداء

(وَمَا تَوْفِيقِي إِلَّا بِاللهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنيب)

لكَ يا ربّ الحمدُ كما ينبغي لجلال وجهك وعظيم سلطانك، فما كان لهذا الإنجازِ أن يُزهرَ لولا عظيمُ فضلك وما بلغتُ هذه اللحظةَ إلا بكَ، واليكَ، ومنكَ أحمدُك يا الله حمدًا لا يحدُّه مدى ولا يُحيطُ به مقال.

إلى النور الذي أضاء دربي، اهدي هذا النجاح لنفسي أولا ثم إلى كُل من سعى معي لإتمام هذه المسيرة دمتم لي سندا لا عمرًا

إلى العزيز الذي حملت اسمه فخرًا، إلى معلمي الأول الرجل الذي سعى طوال حياته لنكون الأفضل.

أبي الغالي

إلى من كانت الداعم الأول لتحقيق طموحي إلى من كانت ملجأي ويدي اليمنى في هذه المرحلة إلى القلب الحنون إلى من كانت دعواتها تحيطني

أمي الغالية_

وإلى من شد الله بهم عضدي فكانوا خير مُعين كنتم دائمًا دعمي وسندي وجودكم في حياتي كان الأمان والفرحة التي أحتاجها لأكمل هذا المشوار

أختي رميساء سندي توأم روحي رفيقة الطريق إلى من كانت السند أوقات الضعف ومن شاركتني التعب طيلة المشوار

_إخوتي

وإلى أغلى إنسان على قلبي صديقتي ورفيقتي وزوجة خالي هاجر التي دعمتني في كل الأوقات، خالي وسجود ومعين ورسيم لكم بصمة خاصة في حياتي

_خالي وزوجته__

لطالما تمنيت ان تقر عينها برؤيتي في يوم

كهذا الى التي توسدها التراب قبل ان تحقق أمنيتها إلى سر مناضلتي واجتهادي الى جدتي رحمة الله عليها فرحتي تنقصها وجودك ونجاحي ينقصه فخرك بي

جدتي رحمة الله عليها

الى صديقتي التي كانت بجانبي منذ البداية الى النهاية رغم كل الصعوبات التي مرت علينا وشريكتي في هذه المذكرة

وإلى إلى أستاذي المشرف دعدوعة عبد المنعم الذي تكرم بقبول الإشراف على هذه المذكرة شكرًا لتوجيهاتك السديدة، وإرشاداتك القيمة التي أضاءت لي دربي في هذه الرحلة أقدر علمك وصبرك وجهدك المبذول

وأخر دعوانا أن الحمد لله رب العالمين

قيري ندى

اهداء

ما سلكنا البدايات إلا بتسييره وما بلغنا النهايات إلا بتوفيقه وما حققنا الغايات إلا بفضله فالحمد الله الذي وفقني لتثمين هذه الخطوة في مسيرتي
الدراسية
أُهدي ثمرة جهدي
إلى نفسي الطموحة جدا التي لم تخذلني
أبي، من بذل الغالي والنفيس وكان نوري
وسراجي الذي لا ينطفئ
أمي، التي جعل الله الجنة تحت أقدامها،
وسهلت لي الشدائد بدعائها
جدتي الغالية، مصدر قوتي وحنانها بلسم
جراحي
إخوتي، أضلعي الثابتة وأمان أيامي وينابيع عطائي
صديقاتي، من شاركنني التفاصيل وساندنني في الرحلة
أستاذي المشرف دعدوعة عبد المنعم
شخاب شيماء

مقدمة

مقدمة

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة تسمى بالثورة المعلوماتية، حيث اظهرت هذه الثورة التكنولوجية اثار ايجابية احدثتها عل شكل تنقل نوعي وحضاري في حياة الافراد والمجتمع، مما لا شك فيه ان هذا التنقل الحضاري بما فيه التقنيات الجديدة التي غزت عالم في العصر الحديث اثرت في كافة نواحي الحياة الانسانية من سلوكيات وغيرهم.

فمع التطورات التكنولوجية التي يشهدها العالم في العقود الأخيرة ظهرت طائفة من الجرائم التي كانت تعرف بأنها تقليدية، ليصبح ارتكابها متناسبا مع هذه التطورات ومن هذه الجرائم جريمة الاحتيال الالكتروني.

فجريمة الاحتيال من الجرائم التقليدية الحديثة بمعنى أنها معروفة من القدم ففي السابق كانت تقوم على التعامل ما بين طرفين يعرف كل منهما الآخر، أما الآن مع استخدام التقنيات الحديثة والأجهزة الالكترونية الحديثة والتحول الرقمي أصبح المجني عليه في أغلب الأحيان لا يعرف الطرف الآخر وقد يكون عن طريقة وهمية لا يستطيع الوصول إليه مباشرة.

فهذه الجريمة تتجدد بتجدد مظاهر الحياة والاقتصاد والعلوم، وتعتمد على فاعل يستخدم فن الخداع بحيث يقنع ضحاياه بتسليمه أموالهم ثقة به، فالاحتيال مهارة سلوكية يتقنها بعض المجرمين، أما المجني عليه يكون فردا يسعى لجمع ثروة بطريقة سريعة وسهلة.

فتعتبر جريمة الاحتيال الالكتروني من أهم جرائم الاعتداء على الأموال التي يتضمنها عنصر الخداع في التعامل المالي بين الأفراد، فأمام تطور هذا النوع من الأساليب الاجرامية وتزايد استعمال شبكات الاتصال الحديثة والأنظمة المعلوماتية والمستجدة ظهرت إشكالات قانونية هامة، خاصة بما يتعلق منها بمسألة حماية الحقوق والبيانات المختلفة المتداولة عبر الوسائط الالكترونية.

وقد أخذت جرائم الاحتيال بالازدياد والتنوع والتطور، وبالنظر لآثارها السلبية الخطيرة بشكل مباشر وغير مباشر على خطط وبرامج التنمية الشاملة المستدامة، مما يتطلب مواجهتها بشكل حاسم.

اهمية الدراسة

حيث تبرز اهمية هذه الدراسة في تناولها ظاهرة إجرامية مستحدثة ونظرا لما تشكله من تهديد على كافة الأصعدة الاجتماعية والاقتصادية وخطرها على المجتمع والفرد ولما تعالجه من موضوعات نعيشها في حياتنا اليومية، فاستحدثت أساليب جنائية جديدة فتحت المجال لارتكاب هذه الجرائم مثل استخدام الحواسيب والهواتف الذكية والبرمجيات والشبكة الإلكترونية في خداع الضحية وإيهامها بمعلومات أو خدمات مزيفة لتحقيق منفعة غير قانونية حيث تعددت وتجددت صور هذه الجريمة وغيرها من الأساليب التي تهدد الأمن المعلوماتي والاقتصادي للأفراد والدول.

وتتجلى أهميتها أيضا من خلال ارتباطها الوثيق والمباشر بمكافحة الجريمة الإلكترونية ولما لهذه الجريمة من خصائص.

أهداف الدراسة

بحيث تهدف هذه الدراسة إلى تحديد مفهوم جريمة الاحتيال الالكتروني وخصائصها ولما يتميز به مرتكبيها عن باقي الجناة التقليديين والى تبيان صور وأساليب الاحتيال الالكتروني

ودراسة موقف المشرع من هذه الدراسة، وتبيان اساليب الوقاية في هذه الجريمة.

أسباب اختيار الموضوع

وقد جاء اختيار هذا الموضوع نتيجة أسباب موضوعية وذاتية في دراسة ظاهرة الاحتيال الإلكتروني؛ فموضوعياً يبرز التزايد المتسارع لهذه الجرائم وما تخلّفه من خسائر اقتصادية

ونفسية واجتماعية، وتطور أساليبها مع التقدم التقني، وقصور التشريعات في مواجهتها، ونقص الدراسات المتخصصة بها. أما ذاتياً فيأتي الاهتمام الشخصي بهذا المجال والرغبة في الإسهام في حماية المجتمع، إلى جانب التخصص الأكاديمي وتوافر المراجع اللازمة للبحث.

نظرا لما سبق ذكره ارتأينا طرح الإشكالية التالية: **ما مدى فعالية النصوص القانونية المتعلقة بمكافحة جريمة الاحتيال الالكتروني؟**

تتفرع عن هذه الإشكالية الأسئلة الفرعية التالية:

-هل واكبت النصوص القانونية الجزائرية (خاصة قانون العقوبات وقانون الإجراءات الجزائية وقانون المعاملات الإلكترونية) التطورات المستمرة في أساليب الاحتيال الإلكتروني؟

-هل جرم المشرع الجزائري جميع صور الاحتيال الإلكتروني كالانتحال الرقمي، والاحتيال عبر منصات التواصل الاجتماعي، أم توجد ثغرات تشريعية؟

-كيف يتعامل قانون الإجراءات الجزائية مع تحديات جمع الأدلة الإلكترونية؟

-كيف تساهم النصوص القانونية في حماية الضحايا وتعويضهم، وتوعية الجمهور للوقاية من هذه الجرائم؟

الدراسات السابقة

قراوي كلثوم أطروحة لنيل شهادة الدكتوراه علوم في القانون العام بعنوان جريمة الاحتيال الالكتروني تناولت في دراستها الأحكام الموضوعية والقواعد الإجرائية لجريمة الاحتيال الالكتروني. فقد ناقشت الدراسة الصعوبات التقنية التي تواجه القضاء في التحقق من صحة الأدلة الرقمية.

- بولحية شهيرة وسويح دنيا مقال منشور في مجلة الدراسات القانونية والاقتصادية، المركز الجامعي -بريكة، الجزائر، بينت الدراسة مختلف تعاريف الاحتيال والاحتيال الالكتروني،

اضافة الى بيان اساليب الاحتيال الالكتروني، كما وضحت خصائص جريمة الاحتيال الكتروني ووسائل الحماية.

المنهج المتبع

وانتهجنا في دراستنا المنهج الوصفي التحليلي من خلال وصف المفاهيم وكذلك تحليلها لاحتوائها على مصطلحات قانونية.

صعوبات الدراسة

إن هذا البحث كغيره من المواضيع لا يخلو من الصعوبات، من أبرزها قلة الدراسات والابحاث التي تعالج الموضوع من ناحية التشريع الجزائري، لكن حاولنا الاعتماد على مصادر ومراجع علمية متنوعة وحديثة لضمان المصداقية.

تقسيم الخطة

ولمعالجة موضوع جريمة الاحتيال الالكتروني ارتأينا إلى تقسيم الخطة إلى فصلين، الفصل الأول بعنوان الإطار المفاهيمي لجريمة الاحتيال الإلكتروني متكون من مبحثين المبحث الأول يتحدث عن مفهوم جريمة الاحتيال الالكتروني والمبحث الثاني يتحدث عن أركان جريمة الاحتيال الالكتروني.

أما الفصل الثاني بعنوان إجراءات التحقيق في جريمة الاحتيال الالكتروني ووسائل الوقاية منها كان مقسم إلى مبحثين فالمبحث الأول نتحدث عن كيفية إجراءات التحقيق في هذه الجريمة والعقوبات المقررة لها، والمبحث الثاني وسائل الوقاية من جريمة الاحتيال الالكتروني مركزا على جهود مؤسسات الدولة في مكافحة جريمة الاحتيال الالكتروني.

الفصل الأول

الإطار المفاهيمي لجريمة الاحتيال الالكتروني

الفصل الأول

الإطار المفاهيمي لجريمة الاحتيال الالكتروني

جريمة الاحتيال هي من الجرائم الواقعة على الاموال، وتتسبب في تدهور الوضع الاقتصادي للمجتمع. فانتشار هذه الجريمة يؤدي إلى فقدان الثقة بين الأفراد، ويثير التشكيك في مصداقية التعاملات المالية. هذا خاصة في مجتمعنا الذي يتسم بالمقومات الاجتماعية الحسنة مثل الطيبة والتسامح والثقة بالآخرين، والتي يمكن استغلالها من قبل المحتالين الذين يستخدمون أساليب لخداع والكذب والتمثيل، مما يجعل الشخص ضحية سهلة لهذه الحيل والتلاعب.

يُعد الاحتيال الإلكتروني أداة رئيسية في ارتكاب جرائم الاحتيال الحديثة. فيستخدم الجناة أجهزة الكمبيوتر، والإنترنت، وآلات الدفع الآلية، بما في ذلك الهواتف المحمولة، سواء كوسيلة لارتكاب الجريمة مثل تزوير بطاقات الائتمان، أو عبر إرسال رسائل نصية مضللة، أو باختراق شبكات الإنترنت ونشر معلومات مضللة، أو باستخدام برامج خبيثة لسرقة بيانات مصرفية واستغلالها.

فسنتطرق في هذا الفصل إلى مفهوم الاحتيال الالكتروني وخصائصه وصوره (المبحث الاول) ثم إلى أركان هذه الجريمة (المبحث الثاني).

المبحث الأول: مفهوم جريمة الاحتيال الإلكتروني

اتسعت رقعة جريمة الاحتيال الالكتروني مع الانتشار الكبير لاستخدام وسائل تقنية المعلومات وشبكات التواصل الاجتماعي، فلذلك يعد الاحتيال من الظواهر الإجرامية المتفشية في معظم المجتمعات، ذلك بسبب الخصائص التي تمتاز بها هذه الجريمة.

فلا يمكن تناول جريمة الاحتيال باستخدام وسائل تقنية المعلومات قبل التعريف بهذه الجريمة إلا من خلال دراسة خصائصها والتطرق الى صور هذه الجريمة، فتطرقنا الى تعريف جريمة الاحتيال الالكتروني (مطلب اول) ثم الى خصائص هذه الجريمة وتمييزها عما يشابهها من جرائم (مطلب ثاني) واساليب وصور جريمة الاحتيال الإلكتروني (مطلب ثالث).

المطلب الأول: تعريف جريمة الاحتيال الالكتروني

مع التطور التكنولوجي الهائل لم يعد الاحتيال يقتصر على الأساليب التقليدية فقط، بل تطور ليأخذ شكلاً جديداً يُعرف بالاحتيال الالكتروني، الذي يُمارس عبر الفضاء الرقمي باستخدام تقنيات حديثة وأساليب متطورة عبر شبكة الانترنت.

ويعد خطوة مهمة فهم مفهوم جريمة الاحتيال الإلكتروني، ولهذا سنتطرق في هذا المطلب إلى التعريف اللغوي والاصطلاحي (الفرع الأول) ثم إلى تعريف الجريمة الإلكترونية (الفرع الثاني).

الفرع الاول: التعريف اللغوي/الاصطلاحي

أولا: التعريف اللغوي

الاحتيال هو الحذق، وجودة النظر، والقدرة على دقة التصرف، ويقال رجل حول: ذو حيل، ويقال هو أحول من أي أكثر حيله، وما أحوله، ورجل حول، بتشديد الواو أي بصير بتحويل الامور، ويقال تحول الرجل وأحتال أذا طلب الحيلة، والاحيال والمحاولة: مطالبتك الشيء بالحيل.[1]

والحيلة لغة وعرفاً المكر والخديعة والكيد لكل فعل يقصد فاعله به خلاف ما تقضيه ظاهره.[2]

وايضا الاحتيال لغة: من حيل، والحيلة اسم من المصدر: احتيال، وكذا الحَيْل والحول، يقال لا حيل ولا قوة، لغة في حول. يقال ما له حيلة، وهو أحيل منه: أي أكثر حيلة. [3]

[1] ابن منظور، لسان العرب المحيط، الجزء الأول، دار اللسان العربي، بيروت، ص 759

[2] خالدي علي سليمان عبد الله، جريمة الاحتيال باستخدام وسائل تقنية المعلومات في التشريع المقارن، دار الجامعة الجديدة، الإسكندرية،2021، ص63

[3] محمد بن ابي بكر الرازي، دار الكتاب العربي، بيروت، 2001، ص 166

ومصطلح الاحتيال استعمل في العديد من الآيات القرآنية، لقوله تعالى في سورة النساء الآية 29: "يَا أَيُّهَا الَّذِينَ أمْنُوا لَا تَأْكُلُوا أَمْوَالَكُم بَيْنَكُم بِالْبَاطِلِ إِلَّا أَن تَكُونَ تِجَارةً عَن تَرَاضٍ مِنكُمْ وَلَا تَقْتُلُوا أَنْفُسَكُمْ إِنّ اللَّهَ كَانَ بِكُمْ رَحِيمًا".[1]

وعلى هذا فالاحتيال بناءً على ما تقدَّم، يُعَدُّ لجوءاً إلى الحيلة. والحيلة في اصطلاح الفقهاء تحمل معنى أضيق من مدلولها اللغوي، إذ تمثّل نوعاً من التصرّف ينتقل به الفاعل من حالة إلى أخرى، ثم شاع استعمالها عرفاً في سلوك المسالك الخفية التي تُوصِل إلى تحقيق الغرض، بحيث لا ينتبه إليها المرء إلا بقدر من الذكاء والفطنة.[2]

ثانيا: التعريف الاصطلاحي

تتنوع التعريفات الاصطلاحية للاحتيال تبعا لاختلاف زاوية نظر كل فقيه، فيعرف الاحتيال بأنه" إسقاط الواجب أو استحلال المحرم بفعل لم يقصد به ما جعل ذلك الفعل من أجله". [3]

كما عُرف أيضاً بأنه نوع خاص من التصرف والعمل ينتقل به الفاعل من حالة إلى أخرى، ثم غلبه الاستعمال العرفي للدلالة على سلوك المسالك الخفية التي يتوصل بها الفرد إلى هدفه دون أن ينتبه إليها إلا من يتسم بنوع من الذكاء والفطنة. وهذا المعنى أخص من سابقه، إذ إن الاستعمال العرفي الغالب يشير إلى التوصل إلى غرض محظور شرعاً أو عقلاً أو عادة.[4]

ويمكن تعريف الاحتيال كذلك بأنه كل تظاهر أو إيحاء من شأنه أن يوقع المجني عليه في الخطأ، بطريقة تؤدي إلى اقتناعه المباشر بالمظهر المادي الخارجي؛ بمعنى أن المجني عليه في جريمة الاحتيال هو من استولت عليه حيلة الجاني، فانخدع بها وسلمه ماله.[5]

[1] القران الكريم، سورة النساء، ج 5، الآية 29
[2] الفيل علي عدنان، الإجرام الإلكتروني دراسة مقارنة، مكتبة زين الحقوقية، ط1، العراق، 2011، ص 16
[3] سامر سلمان الجبوري، جريمة الاحتيال الالكتروني دراسة مقارنة، مكتبة زين الحقوقية، ط1، بغداد، 2018، ص 35
[4] محمد محرم علي، جريمة النصب والاحتيال والتجارة الإلكترونية، دار النهضة العربية، القاهرة، 1998، ص27
[5] على حسن الطوالبة، الجرائم الالكترونية ، مؤسسة فخراوي للدراسات والنشر البحرين، ط 2،البحرين، 2009،ص 180

أما الدكتور رؤوف عبيد فقد عرف الاحتيال بأنه كل كذب مصحوب بوقائع خارجية أو أفعال مادية، من شأنه أن يولّد اعتقاداً لدى المجني عليه بصدق هذا الكذب، مما يدفعه إلى تسليم ما يُراد منه تسليمه طواعية واختياراً. [1]

وفي الفقه القانون الجنائي، تعاريف متعددة للاحتيال فمنهم من عرفه بانه" الاستيلاء على شيء مملوك بطريقة احتيالية بقصد تملك ذلك الشيء.

وعرف أيضاً بأنه: سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي.[2]

تختلف التشريعات في تحديد التسمية الملائمة لهذه الجريمة، ومن ذلك القانون الفرنسي الذي استخدم لأول مرة عبارة طرق احتيالية، إذ اعتبر الاحتيال جريمة مستقلة بذاتها بموجب نص المادة (405). وقد نصّ هذا النص على أن "كل من يتوصل الى أن يسلب، أو يشرع في سلب مال أو بعض ثروة الغير"، وأضاف ظرفا مشددا لجريمة الاحتيال أو الشروع فيها، يتحقق عندما ترتكب إما بانتحال صفة ضابط في الشرطة القضائية، أو مأمور الضبط في دائرة الدولة المدنية، أو في الجيش الفرنسي الأجنبي". [3]

عرف بعض الفقه المصري جريمة الاحتيال بأنها: «الاستيلاء على مال منقول مملوك للغير عن طريق خداع المجني عليه وحمله على تسليمه». في حين عرفها آخرون بأنها: الاستيلاء على الحيازة الكاملة لمال الغير باستخدام وسيلة تنطوي على خداع، تؤدي إلى تسليم ذلك المال، كما ورد في ذات الاتجاه الفقهي تعريف يقضي بأنها: الاستيلاء على شيء مملوك للغير بنية تملكه، وذلك عبر وسائل الاحتيال المنصوص عليها قانوناً.[4]

[1] رؤوف عبيد، مبادئ علم الاجرام و العقاب، دار الفكر العربي ،القاهرة ،مصر ،2004،ص 59.

[2] محمد علي السالم عياد الحلبي ، "الجرائم الواقعة على الأموال في القانون المقارن "، دار الوراق، ط1،عمان، 2010،ص133

[3] سويح دنيا زاد، بولحية شهيرة، الاحتيال الالكتروني ،مجلة الدراسات القانونية والاقتصادية، المركز الجامعي بريكة ،العدد 04، 2019 ،ص38

[4] عبد القادر الشيخلي، جريمة الاحتيال في قوانين عقوبات الدول العربية، منشورات الحلبي الحقوقية،ط1،لبنان، 2009 ، ص 34

وعليه، لا يختلف التعريف الاصطلاحي (الفقهي) للاحتيال اختلافاً جوهرياً عن التعريف اللغوي، إذ يبدو التقارب بينهما واضحاً من خلال المعنى العام للاحتيال بوصفه كل فعل كيديّ، غير أن الفقهاء قد صاغوا تعريف الاحتيال اصطلاحاً من منظور شرعي تحديداً.

فلقد خصص المشرع الجزائري جريمة الاحتيال في القسم الثاني من قانون العقوبات، تحت عنوان "النصب وإصدار شيك دون رصيد"، إذ نصت المادة 372 من القانون ذاته على أن: كل من يتمكن من استلام أو تلقي أموال، أو منقولات، أو سندات، أو تصرفات، أو أوراق مالية، أو وعود، أو مخالصات، أو إبراء من النزاعات، أو يحصل على أي منها، أو يشرع في ذلك، وكان هذا الفعل قد تم عن طريق الاحتيال بقصد سلب كامل ثروة الغير أو جزء منها، أو الشروع في سلبها، سواء كان ذلك باستعمال أسماء أو صفات كاذبة، أو سلطة وهمية، أو اعتماد مالي مزيف، أو بإثارة الأمل في الفوز بشيء، أو في وقوع حادث أو أي واقعة أخرى غير حقيقية، أو بإثارة الخوف من وقوع شيء منها.[1]

الفرع الثاني: تعريف الجريمة الالكترونية

تتعدد المسميات المُناطة بالجريمة الإلكترونية، فيُشار إليها أحيانًا بجريمة الكمبيوتر والإنترنت، وأحيانًا أخرى بالجريمة الإلكترونية، كما يصفها البعض بجريمة إساءة استخدام تقنية المعلومات، في حين يُطلِق عليها آخرون مصطلح الجرائم المستحدثة. [2]

ورد التعريف اللغوي للفظ "الجَرِيمَة" في معجم لسان العرب على النحو الآتي: "الجَرِيمَة لَفْظٌ مُشْتَقٌ مِنَ الفِعْل جَرَمَ يَجْرِمُ وَاجْتَرَمَ وَأَجْرَمَ إِجْرَامًا وَجُرُومٌ، والجرْمٌ مَعْنَاهُ التَّعَدِّي وَاقْتِرَافْ الذُّنُوبْ بِحَقِّ الغَيْرُ، وَلِهِذَا يُعَاقِبُ المولى عَزَّ وَجَلْ كُلَّ مَنْ اِقْتَرَفَ/يَقْتَرِفُ جُرْمًا وَذَلِكَ اِسْتِنَادًا لِمَا وَرَدَ فِي آيَاتِ التَّرْتيلِ الحَكِيمِ كَالآيَة 40 مِنْ سُورَةِ الأَعْرَافْ وَالَّتِي يَقُولُ فِيهَا سُبْحَانَهُ وَتَعَالَى: {إِنَّ الَّذِينَ كَذَّبُوا بِآيَاتِنَا وَاسْتَكْبَرُوا عَنْهَا لَا تُفَتَّحُ لَهُمْ أَبْوَابُ السَّمَاءِ وَلَا يَدْخُلُونَ الجَنَّةَ حتى يَلِجَ الْجَمَلُ فِي سَمِّ الْخِيَاطِ وَكَذَلِكَ نَجْزِي الْمُجْرِمِينَ)"، بَيْدَ أن إبراهيم أنس وبعضٍ من أعلام اللغة ورد عنهم بخصوص تعريف لفظ "الجَرِيمَة" ما يأتي: "الجَرِيمَة مِنْ قَوْلِنَا أَجْرَمَ بِمَعْنَى اِرْتَكَبَ الجُرْمَ، وَيُقَالُ

[1] سعدي حيدرة، الجرائم ضد الأشخاص والأموال، القسم الخاص بين النص والواقع، ألفا للوثائق ، طبعة1 ،2021،ص315
[2] محمد عبد الرحمن عنانزه ،القصد الجرمي في الجرائم الالكترونية ،دار الأيام للنشر والتوزيع ،ط1 ، الأردن، 2017 ،ص60

كَذَلِكَ أَجْرَمَ عَلَيْهِمْ وَإِلَيْهِمْ أَيْ جَنَى جِنَايَةً، وَالجَرِيمَة بِوَجْهِ عَامْ كُلُ أَمْرٍ إِيجَابِي أَوْ سَلْبِي يُعَاقِبْ عَلَيْهِ القَانُونْ سَوَاءٌ أَكَانَتْ مُخَالَفَةً أَمْ جُنْحَةً أَوْ جِنَايَةً. "[1]

فمصطلح الجريمة الالكترونية يتكون من شقين وهما "الجريمة "و "الالكترونية:

تُعرف الجريمة بشكل عام بأنها سلوك غير مشروع يصدر عن إرادة جنائية، ويرتب عليه القانون عقوبة أو تدبيراً احترازياً. ويُحدد هذا التعريف أركان الجريمة المتمثلة في: السلوك غير المشروع، والإرادة الجنائية، والعقوبة أو التدبير الاحترازي الذي يقرره القانون، وكل ذلك يؤمن وصفاً دقيقاً للجريمة. ومن جهة أخرى، عرّف بعض فقهاء القانون الجنائي الجريمة بأنها سلوك إنساني يُعاقب عليه بوصفه خرقاً لقيم المجتمع أو تهديداً لمصالح أفراده الأساسية، أو هي كل نشاط خارجي صادر عن إنسان، سواء تمثل في فعل أو امتناع، يقرر القانون بسببه عقاباً. "[2]

أما الالكترونية فهي مصطلح يستخدم لوصف فكرة جزء من الحاسب او عصر المعلومات

هناك تعريفات حاولت التوسع في مفهوم الجريمة الالكترونية فعرفوها كالاتي:

يُقصد بالجريمة المعلوماتية كل فعل أو امتناع متعمد ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال والأشياء المعنوية. وقد وضع الخبير الأمريكي باركر مفهوماً واسعاً لها إذ عرّفها بأنها: كل فعل إجرامي متعمد، أياً كانت صلته بتقنية المعلومات، يترتب عليه إلحاق خسارة بالمجني عليه أو تحقيق كسب للفاعل.[3]

أما وفقاً للتعريف الضيق للجريمة الإلكترونية، فقد عُرفت بأنها الجرائم التي تقع على النظام الإلكتروني أو الشبكة المعلوماتية، أو هي نشاط غير مشروع موجه لنسخ المعلومات المخزنة داخل النظام الإلكتروني أو التي يتم نقلها عبره، أو تغييرها، أو حذفها، أو الوصول إليها. وبناءً على هذا التعريف، يضيق مفهوم الجرائم الإلكترونية بحيث يُحصر فيما يقع على

[1] حسن كليبي ، نجمة الطيب ، جريمة النصب الالكتروني من منظور المشرع الجزائري،مجلة المفكر،المجلد20،العدد، السنة 2025ص 67

[2] محمد عبد الرحمن عنانزه ،المرجع السابق،ص61

[3] نهلا عبدالقادر المؤمني، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع, الطبعة الأولى، عمان، 2008،ص46

النظام الإلكتروني أو داخله فقط، ويُحدد الأنشطة غير المشروعة على سبيل الحصر. ومن هنا يرى البعض أن الجريمة الإلكترونية في ظل هذا الاتجاه تصبح أشبه بالخرافة[1].

وقد عرّف الفقه الجزائري الجريمة الإلكترونية بتعاريف متعددة، منها: تعريفها بأنها الجريمة التي تُرتكب باستخدام جهاز الكمبيوتر عبر الاتصال. كما عرّفها البعض على أنها كل فعل أو امتناع عن فعل يقوم به شخص بقصد الإضرار بالمكونات المادية والمعنوية للحاسب وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها. ومن التعاريف أيضاً أنها استخدام الأجهزة التقنية الحديثة كالحاسب الآلي والهاتف النقال أو أحد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع.[2]

المطلب الثاني: خصائص جريمة الاحتيال الالكتروني وتمييزها عما يشابهها من الجرائم

تعد جريمة الاحتيال الإلكتروني من الجرائم المستحدثة المنتشرة بشكل واسع، تتميز بخصائص تميزها عن جريمة الاحتيال التقليدي التي تعتمد على الذكاء المعلوماتي،

وسنتطرق في هذا المطلب الى تبيان خصائص جريمة الاحتيال الالكتروني (الفرع الأول) ثم تمييزها عما يشابهها (الفرع الثاني)

الفرع الأول: خصائص جريمة الاحتيال الالكتروني

1جريمة مستحدثة

إن التقدم العلمي والتكنولوجي، وما صاحبه من تحول نوعي في ظل العولمة، قد تجاوز القدرات الرقابية للدولة وإمكاناتها، بل وأضعف من قدرتها على تطبيق قوانينها، بما بات يهدد أمنها وسلامتها. ولهذا تُعتبر الجريمة الإلكترونية جريمة مستحدثة تفرز إشكاليات عديدة وتحديات كبرى أمام الدول بغية التصدي لها. وقد تزامن تطور هذا النوع من الجرائم مع التطورات التي طرأت على التقنيات والتكنولوجيا التي يسرت سبل التواصل وانتقال المعلومات

[1] محمد عبد الرحمن عنانزه، المرجع السابق ،ص63

[2] راضية عيمور، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد الأول، المجلد السادس ، السنة 2022، ، ص 90

بين مختلف الشعوب والحضارات، وسهلت حركة المعاملات، بحيث أصبحت لغة العصر تقوم على تداول الصوت والصورة والمعلومة عبر مسالك الاتصالات المتنوعة. وانتقل الأفراد اليوم من العالم الواقعي إلى العالم الافتراضي، وانتقلت الجريمة تبعاً لذلك. فتُستخدم شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها، إذ تعد حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم، كالمؤسسات العامة والخاصة والبنوك والشركات بكافة أنواعها والأشخاص وغيرهم، والذين غالباً ما يكونون الضحية.[1]

2. جريمة عابرة للحدود

إن جرائم الاحتيال الإلكتروني تمثّل شكلاً من أشكال الجرائم العابرة للحدود، إذ لم يعد مسرح الجريمة محلياً بل أصبح عالمياً. فالفاعل لا يتواجد مادياً على مسرح الجريمة، وذلك بفعل التباعد المكاني بين الفعل المرتكب عبر الحاسوب والفاعل من جهة، وبين المعلومات محل الاعتداء من جهة أخرى. فالجاني يستطيع ارتكاب جريمته بالدخول إلى ذاكرة حاسوب آلي موجود في بلد آخر، وقد يُلحق هذا الفعل ضرراً بشخص ثالث في بلد آخر. وعليه، تُعتبر الجريمة داخلية عندما تقع داخل حدود الدولة، أي تُرتكب في النطاق الجغرافي للدولة، في حين تُعد جريمة دولية عندما تتجاوز حدود الدولة وتتعلق بالقانون الدولي.[2]

وأيضا هذه الجريمة لا تعرف الحدود بين الدول والقارات حيث ادت تكنولوجيا المعلومات الى نتيجة مفادها ان اماكن متعددة في دول مختلفة قد تتأثر بجريمة من جرائم الاعتداء على نظم المعلومات الواحدة في ان واحد، حيث يمكن ان تقع جريمة من جاني في دولة ويكون المجني عليه في دولة أخرى.[3]

فبعد ظهور شبكات المعلومات، لم يعد ثمة حدود مرئية أو ملموسة تعيق نقل المعلومات عبر الدول المختلفة. إذ إن القدرة التي تتمتع بها الحواسيب وشبكاتها على نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة تفصل بينها آلاف الأميال، أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

[1] الطاهر ياكر الجرائم الإلكترونية، الأحكام الموضوعية والإجرائية، دراسة مقارنة، دار بلقيس ،الجزائر،2024،ص29
[2] خالدي علي سلمان عبد الله، المرجع السابق، ص702
[3] محمد عبد الرحمن عنانزه،المرجع السابق، ص 66

فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعلت من الممكن ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة، بينما يتحقق الفعل الإجرامي في دولة أخرى.[1]

وتتميز هذه الجريمة بصعوبة اكتشافها وإثباتها، إذ لا تترك أثراً مادياً ظاهراً يمكن ملاحظته أو ضبطه، وهذا أدى بدوره إلى صعوبة إثبات فاعلها، فالدليل المادي يُدمّر بعد الاستخدام مباشرة، وذلك على خلاف الجرائم الأخرى. فهي تقع في بيئة افتراضية تقنية لا تترك أي آثار حسية. وتعود صعوبة إثباتها إلى عدة أسباب، من أبرزها طابعها التقني الذي يضفي عليها بعض التعقيد، ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، وكذلك أحجام المجني عليهم أنفسهم عن الإبلاغ عنها في حالة اكتشافها وخاصة الجهات والمؤسسات المالية تجنبا للإضرار بسمعتها ومكانتها وهزا للثقة في كفاءتها.

يعد أمر اثباتها من أهم التحديات التي تواجه الأجهزة الأمنية، ويزداد الإثبات صعوبة في الجريمة الإلكترونية، حيث إن اكتشاف الجريمة الإلكترونية أمر ليس بالسهل.[2]

تقع هذه الجريمة أيضًا في بيئة إلكترونية، وتكون الأدلة الناتجة عنها أدلة إلكترونية. إذ يُمكن للمجرم الإلكتروني أن يتخلص من الآثار المادية لجريمته بفضل التقنيات المعلوماتية، وأن يُخفي الدليل الرقمي الإلكتروني، وذلك من خلال استخدامه تقنية لارتكاب الجريمة وتقنية أخرى لإخفاء العمليات التقنية التي تم توظيفها لارتكابها. وهذا الأمر يجعل بدوره عملية التحري عن الدليل الرقمي الإلكتروني للجريمة من قِبَل المختبر الجنائي الإلكتروني والخبراء المتخصصين بالغة الصعوبة[3].

4. جريمة يسهل ارتكابها

تتسم الجريمة المعلوماتية في غالب صورها بطابع الخفاء والاستتار، حيث لا يدرك الضحية وقوعها عليه حتى وإن كان متصلاً بشبكة الاتصالات في اللحظة ذاتها التي ترتكب فيها.

[1] نهلا عبد الله مومني ، المرجع السابق، ص 51
[2] سيد علي السيد محمد ،الجرائم الإلكترونية ماهيتها صورها، دار التعليم الجامعي، الإسكندرية ،2024،ص26
[3] ميرفت محمد حبايبه، مكافحة الجريمة الإلكترونية دراسة مقارنة في التشريع الجزائري، دار اليازوري العلمية، عمان،2023، ص45

ويعود ذلك إلى ما يتمتع به مرتكبو هذه الجرائم من كفاءات تقنية متقدمة تُمكّنهم من تنفيذ أفعالهم الإجرامية بمهارة ودقة بالغتين، ومن أبرز صور ذلك: إطلاق الفيروسات الإلكترونية المدمرة، والاستيلاء على الأموال وانتهاك البيانات الخاصة أو إتلافها، فضلاً عن التجسس واعتراض الاتصالات وما شابه ذلك من صور الاعتداء الرقمي.

ويُضاف إلى ذلك أن كثيراً من هذه الجرائم تتحقق في زمن بالغ القصر، قد لا يتجاوز الثانية أو جزءاً منها، مما يُعسّر اكتشافها في حينه، إذ لا يُدرك وقوعها في الغالب إلا بعد مضي فترة زمنية قد تطول، كما هو الحال في برامج التخريب والتجسس، وعمليات سرقة البيانات والأموال. ولا شك أن التطور التقني المتسارع قد أسهم إسهاماً مباشراً في تعزيز هذه الظاهرة، من خلال ما أفرزه من أدوات وبرمجيات متطورة تُيسّر تنفيذ الجريمة المعلوماتية وتُكيّفها وفق أهداف الجاني ومقاصده.[1]

على النقيض من الجرائم التقليدية التي تستلزم بذل جهد جسدي ملموس، سواء في صورة عنف مباشر كجرائم القتل والاختطاف، أو في صورة اختراق مادي للممتلكات كالخلع والكسر في جرائم السرقة، فإن الجرائم المعلوماتية تنتمي إلى ما يُعرف بالجرائم الصامتة" التي لا تقوم على الإكراه الجسدي أو استخدام القوة المادية. وإنما يرتكز تنفيذها في جوهره على امتلاك الجاني قدراً من الكفاءة التقنية التي تُمكّنه من التعامل مع أنظمة الحاسوب واستغلالها في ارتكاب الأفعال المحظورة قانوناً.[2]

تتميز الجريمة المعلوماتية كذلك بسهولة إخفائها نسبياً، فعلى الرغم من أن الجرائم المرتكبة عبر شبكة الإنترنت تبقى آثارها قائمة وقابلة للملاحظة، إلا أن الطابع الإلكتروني الذي يغلب على أدلتها يجعل التعامل معها أمراً بالغ التعقيد، إذ تستعصي على المحقق العادي الذي يفتقر إلى الخبرة الفنية المتخصصة. وتتجلى هذه الإشكالية بصورة واضحة في جرائم البريد الإلكتروني، حيث يتعذر على جهات التحري تحديد مصدر المرسل والكشف عن هويته.

تستلزم الجرائم المعلوماتية ذات الطابع الاقتصادي، كعمليات التحويل الإلكتروني غير المشروع للأموال، توافر كفاءة تقنية ومهارة فنية رفيعة المستوى لدى مرتكبها، مما يميزها عن

[1] الطاهرياكر، المرجع السابق، ص30
[2] نهلا عبد القادر المومني، المرجع السابق، ص58

سائر صور الإجرام التقليدي. فضلاً عن ذلك، فإن الدوافع التي تحمل المجرم المعلوماتي على ارتكاب جرائمه كثيراً ما تختلف في طبيعتها عن تلك التي تدفع المجرم التقليدي، مما يجعل الشخصية الإجرامية في البيئة الرقمية ذات خصائص مغايرة تستوجب دراسة متخصصة ومقاربة مختلفة في التعامل معها .[1]

5. خصوصية مجرمي المعلومات

يختلف مرتكب هذه الجريمة عن المجرم العادي (مرتكب الجريمة التقليدية)

تختلف طبيعة الجرائم المعلوماتية اختلافاً جوهرياً عن غيرها، إذ تعد في الغالب الأعم جرائم تقنية فنية بطبيعتها. وغالباً ما يرتكبها أشخاص من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل أولئك الذين يمتلكون حداً أدنى من المعرفة والقدرة على استخدام الحاسوب والتعامل مع شبكة الإنترنت.

فعلى سبيل المثال، تستلزم الجرائم المعلوماتية ذات الطابع الاقتصادي، كالتحويل الإلكتروني غير المشروع للأموال، مهارة وقدرة تقنية فنية عالية جداً من جانب مرتكبها. كما أن الدوافع التي تدفع المجرم المعلوماتي إلى ارتكاب هذا النوع من الإجرام قد تختلف عن الدوافع الكامنة وراء ارتكاب الجرائم من قبل المجرم التقليدي.[2]

ويتميز أغلب مرتكبي هذه الجريمة بخبرة فائقة ومعرفة متقدمة في مجال تقنية المعلومات؛ إذ لا بد أن يكون مرتكب جريمة الاحتيال الإلكتروني واسع الخبرة وعالي المعرفة في هذا المجال ليتمكن من ارتكاب جريمته عبر شبكة الإنترنت، بما يمكنه من تنفيذها والعمل على إخفائها وعدم اكتشافها. ولهذا نجد أن معظم مرتكبي جرائم الاحتيال الإلكتروني هم من خبراء تقنية المعلومات، وهو ما يجعل الشرطة توجه اهتمامها أولاً إلى خبراء الحاسوب عند وقوع مثل هذه الجرائم.[3]

[1] الطاهر ياكر، المرجع السابق ،ص31
[2] نهلا عبد القادرمومني، المرجع السابق ،ص59
[3] خالد علي سلمان عبد الله، المرجع السابق، ص 74

وكما ان من خصائص المجرم الالكتروني انه يمتلك السلطة بشكل مباشر او غير مباشر، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول الى النظام المعلوماتي

المقدرة على تطوير سلوكه الاجرامي، قدرته العقلية وسرعة اكسابه المهارة التقنية تؤدي به الى تطوير وسائل وأساليب ارتكاب الجريمة ومحاولة الوصول الى اعلى المهارة التقنية المتمثلة في اثبات قدرته في تنفيذ الجريمة بمهارة.

كذلك من خصائص المجرم الالكتروني القدرة على ابتكار الاساليب والوسائل اللازمة لتنفيذ وإتمام نشاطه الجرمي.

يغلب على معظم مرتكبي الجريمة الإلكترونية أنهم من جيل الشباب، إضافة إلى كونهم من ذوي المناصب المرموقة والتخصصات الرفيعة في مجالات أعمالهم. كما أنهم لا يولون أي اهتمام يُذكر إزاء القيم غير المرتبطة بآثار مادية، ولا يدركون في كثير من الأحيان أن سلوكهم الإجرامي جدير بالعقاب.[1]

الفرع الثاني: تمييز جريمة النصب والاحتيال عن غيرها من الجرائم

1جريمة الاحتيال والسرقة

يمكن أن نفرق بين جريمتي السرقة والاحتيال حسب الفوارق التالي:

من حيث محل الجريمة، فإن جريمة السرقة لا تقع إلا على المنقولات فقط، بينما جريمة الاحتيال لا تقع على المنقولات فحسب، بل قد تمتد لتشمل العقار، وبالتالي فهي تقع على أي مال بغض النظر عن نوعه أو صفته.

وتقوم جريمة الاحتيال على إيقاع المجني عليه في فخ أو خدعة تدفعه إلى تسليم ماله طواعية، في حين أن حصول التسليم في جريمة السرقة قد ينفي قيام هذه الجريمة. بل إن التسليم في جريمة النصب والاحتيال يُعد شرطاً أساسياً لتحقق أركانها.

[1] محمد عبد الرحمن عنانزه، المرجع السابق، ص73

كما يشترط في جريمة الاحتيال أن يكون رضا المجني عليه صادراً عن إرادة سليمة غير مشوبة بأي عيب من عيوب الإرادة. في المقابل، فإن عدم رضا المجني عليه يُعد شرطاً لقيام جريمة السرقة.

تتحقق جريمة الاحتيال بالمناورات الاحتيالية التي حددها المشرع على سبيل الحصر، فإذا لم توجد هذه المناورات لا تقوم جريمة الاحتيال. في حين أن جريمة السرقة لا تتطلب المناورات، وإنما قوامها الاستيلاء على مال الغير بطريقة خلسة.

تبنى جريمة السرقة على أساس الحيازة الكاملة، كما رأينا، بينما جريمة الاحتيال،

تقع على الملكية، وتتفق الجريمتان، في أن الاستيلاء هو على مال الغير بنية التملك.[1]

فالمشرع الجزائري، نجد أنه لم يُعرف السرقة تعريفاً صريحاً، وإنما جاء في المادة 350 من قانون العقوبات الجزائري قوله: "كل من اختلس شيئاً غير مملوك له يعد سارقاً". وبهذا يكون المشرع قد منح مفهوماً قائماً على الفعل الذي يقوم به من لا يملك الشيء ويقدم على اختلاسه، مع العلم بأن المشرع قد حدد الشيء الذي يكون محلاً للاختلاس.[2]

2جريمة الاحتيال وخيانة الأمانة:

تختلف جريمة الاحتيال عن خيانة الأمانة:

في جريمة النصب، ينتقل محل الجريمة عن طريق التسليم، وذلك بعد إيقاع إرادة المجني عليها في خلط أو سوء اعتقاد أو تقدير خاطئ ناتج عن المناورات الاحتيالية.

في حين أن تسليم محل جريمة خيانة الأمانة يتم عن طريق عقد من العقود الواردة على سبيل الحصر في المادة 376 من قانون العقوبات الجزائري.

[1] سعدي حيدرة، المرجع السابق، ص320

[2] عمري عبد القادر، جريمة السرقة بين الشريعة والتشريع الجزائري، مجلة الدراسات القانونية، مجلد3، عدد 01، جامعة المدية، الجزائر، 2017ص ص04,05

أما جريمة الاحتيال، فإن الفعل المعاقب عليه هو الاستلام، ويكون الاعتداء فيها موجهاً على حق الملكية، وعلى إرادة المجني عليه بحيث تصبح معيبة، وذلك بتأثرها بالوسائل الاحتيالية.

بينما في جريمة خيانة الأمانة الفعل المعاقب عليه هو إما الاختلاس أو التبديد بسوء نية، الاعتداء يقع أولا على الحيازة الناقصة، وتحويلها إلى حيازة كاملة.[1]

جريمة خيانة الأمانة من الجرائم الواقعة على الأموال مفادها أن يسلم المجني عليه أمواله بإرادته، لأن الفاعل الرقمي كان قد أعطى لمسته في أساليب الإيهام التي كان يمارسها عليه، وإنما استنادا إلى قيام عقد من عقود الائتمان المنصوص عليها في النص القانوني المدني الجزائري مثل الوديعة أو العارية، فلو لم يكن مثل هذا العقد لما سلم الضحية أمواله للمتهم ولم تكن فعل خيانة الأمانة، وأخذ الأموال بالباطل.[2]

3تمييز جريمة الاحتيال عن جريمة التدليس المدني

لم يكن فعل الاحتيال، بوصفه فعلاً جنائياً له عقوبته الجنائية المقررة، ظاهراً بصورة واضحة، إذ كان يلفه شيء من الغموض يتداخل فيه معنى الاحتيال الجنائي مع التدليس والغش المدني، وكانت التشريعات الجنائية القديمة تستعمل اللفظ نفسه. والتدليس في النص الجنائي هو اللفظ المستعمل في القانون المدني ليعبر عن الغش في المسائل المدنية، واستمر هذا الخلط حتى عندما عدل النص الجنائي الفرنسي مستبدلاً لفظ "الطرق الاحتيالية" بلفظ "التدليس"، مما ميز بين جريمة الاحتيال وأفعال التدليس في المجال المدني.[3]

تتفق جريمة الاحتيال الإلكتروني مع الصورة التقليدية للاحتيال في جوهرها؛ فكلاهما يقوم على "فن الخداع" واستخدام الحيلة للإيقاع بالضحية. ففي الحالتين، يسعى الجاني بذكاء ودهاء إلى إقناع الشخص بالتخلي عن أمواله طواعية وبكامل إرادته، ليكون الهدف النهائي هو الاستيلاء على ممتلكات الغير وحرمانهم منها للأبد.

[1]سعدي حيدرة، المرجع السابق، ص321
[2]عبد العزيز سعد، جرائم الاعتداء على الأموال العامة والخاصة، دار هومة، ط4، الجزائر،2007، ص118
[3] عبد القادر الشيخلي، المرجع السابق، ص52.53

لكن، وبالرغم من اتحاد الهدف، فإن الوسيلة تخلق فرقاً شاسعاً؛ فبينما يعتمد الاحتيال التقليدي عادةً على المواجهة المباشرة أو الأساليب اليدوية البسيطة، يأتي الاحتيال عبر الإنترنت بصورة أكثر تعقيداً وخطورة. هنا، يستبدل المجرم لغته المباشرة بالبرمجيات، مستغلاً الثغرات التقنية لتنفيذ عمليات تلاعب واسعة ومتكررة آلياً، وبأقل قدر من الظهور المباشر، مما يجعل أثرها أسرع وانتشارها أوسع.[1]

4تمييز جريمة الاحتيال الالكتروني عن جريمة الابتزاز

يعرف الابتزاز اصطلاحاً بأنه: استخدام التهديد بالأذى الجسدي أو النفسي، أو الإضرار بالسمعة والمكانة الاجتماعية عبر تلفيق الفضائح وإلصاق التهم، ونشر الأسرار، مما يجبر الشخص المهدد على الدفع مكرهاً لمن يمارس الابتزاز عليه.[2]

حيث يتفق الاحتيال مع الابتزاز في أن كلاً منهما يترتب عليه الحصول على المال بناءً على رضا معيب، كما يترتب عليه كسب أو خسارة غير مشروعة. ويفترقان في أن المبتز يحصل على المال بناءً على التخويف والتهديد، أما المحتال فيحصل عليه بناءً على الخداع والغش والتدليس.[3]

وختاما يمكن القول ان جريمة الاحتيال الإلكتروني تتميز عن الاحتيال التقليدي من حيث استخدامها للتقنيات الحديثة التي تجعل منها سهلة التطبيق.

المطلب الثالث: صور واساليب جريمة الاحتيال الإلكتروني

يعد الاحتيال الإلكتروني من أبرز الجرائم المستحدثة التي أفرزها التطور التكنولوجي المتسارع، حيث اتخذ صورًا وأساليب متعددة تتسم بالتجدد والتعقيد. ولم يعد هذا النوع من الاحتيال مقتصرًا على وسائل تقليدية، بل أصبح يعتمد بشكل أساسي على البيانات الرقمية والتقنيات الحديثة، حيث يعكس تنوع هذه الأساليب والصور مدى خطورة هذه الجريمة.

[1]أسامة حمدان، الرقب، جرائم النصب والاحتيال، (الأساليب، المظاهر، العلاج)، دار يافا العلمية للنشر والتوزيع، ط1، عمان، ص31

[2]غليلة الحسين، معاوي عبد الناصر، الابتزاز الإلكتروني، مذكرة لنيل شهادة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسة، جامعة20أوت1965، سكيكدة ،2024، ص28

[3]عبد القادر الشيخلي، المرجع السابق، ص52

فسنتطرق إلى صور هذه الجريمة في (الفرع الأول) وإلى أساليب الاحتيال في هذه الجريمة في (الفرع الثاني).

الفرع الأول: صور الاحتيال الإلكتروني

1.الإحتيال عبر بطاقات الائتمان

يقوم هذا النوع من الاحتيال على إنشاء مواقع وهمية على شبكة الإنترنت تحاكي المواقع الأصلية للشركات والمؤسسات الموجودة على الشبكة، بحيث يظهر الموقع الوهمي وكأنه الموقع الأصلي الذي يقدم الخدمة. فيستقبل هذا الموقع جميع التعاملات المالية والبنكية والتجارية، وغالب هذه التعاملات تعتمد على البطاقات الائتمانية، مما يعني الحصول على تلك البطاقات الائتمانية، بالإضافة إلى خلق نوع من عدم الثقة تجاه المواقع الأصلية.[1]

ويقوم أيضا عن طريق الشبكات غير المحمية التي تشكّل باباً مفتوحة للقراصنة، خاصةً حين تكون كلمات المرور ضعيفة، كما أن يكون المستخدم قليل الخبرة فيصبح هدفاً سهلاً للمحتالين الذين يستغلون عدم معرفته للأنترنت للنفاذ إلى أجهزته وبريده الإلكتروني. أيضا سرقة البطاقات الإلكترونية تتم بأساليب متعددة منها تركيب أجهزة خفية على آلة الصراف الآلي لالتقاط البيانات والأرقام السرية، أو اختراق مواقع بعض الشركات التي تتعامل في مجال التسوق الإلكتروني للاستيلاء على معلومات العملاء، وصولاً إلى اعتراض البيانات أثناء نقلها بين المستخدم ومزود الخدمة للنفاذ إلى قواعد البيانات الحساسة. [2]

تجري المعاملات المالية عبر بطاقات الائتمان في الفضاء الرقمي المفتوح، مما يُعرّض حاملي هذه البطاقات لمخاطر جسيمة، إذ يواجهون تهديدات مستمرة من قِبَل فئات إجرامية منظمة تسعى إلى اختراق بياناتهم الشخصية والمالية والاستيلاء عليها، بهدف توظيفها في عمليات شراء غير مشروعة. وقد أفرز هذا الواقع ظاهرة الاحتيال على بطاقات الائتمان،

[1] Mamene Besma، "Images and Manifestations of Electronic Fraud on Persons and Funds through Digital Data،" *Law، Society and Authority Journal*، Vol. 14، No. 1, 2025، p. 92.

[2] Meriem Abdelkafi ،Souraya Bourbaba، "Information Fraud Crime on Electronic Financial Cards" ،Journal of Law and Political Sciences، vol. 8، no. 1، Algeria،2022، p. 406.

القائمة على انتزاع المعلومات السرية المرتبطة بها واستخدامها من قِبَل أطراف غير مخولة بصورة مخالفة للقانون[1]

2الإحتيال عبر البريد الالكتروني

يُصنَّف هذا الأسلوب من بين أكثر الأساليب الإجرامية انتشارًا وخطورةً في آنٍ واحد، كونه يستند إلى منهجية مزدوجة تجمع بين التضليل النفسي والتقني معًا. إذ يلجأ الجاني إلى إرسال رسائل إلكترونية مُصمَّمة بعناية فائقة لمحاكاة المراسلات الرسمية الصادرة عن جهات موثوقة، وذلك من خلال انتحال الشعارات والهويات البصرية وعناوين البريد الإلكتروني بصورة تكاد تكون مطابقة للأصل. وتعتمد هذه الرسائل الاحتيالية في الغالب على تضمين محتوى مُثير للقلق أو الاستعجال، بما يدفع الضحية إلى اتخاذ قرارات متسرعة دون إعمال التفكير أو التحقق المسبق.

وتتجلى أبرز الأساليب التي تعتمد عليها هذه الرسائل الاحتيالية في توظيف جملة من الذرائع المُضلِّلة، أبرزها: التهديد بتعليق الحساب المصرفي أو إغلاقه نهائيًا خلال إطار زمني ضيّق لا يتجاوز أربعًا وعشرين ساعة ما لم تُستكمل إجراءات تحديث البيانات الشخصية، فضلًا عن إيهام الضحية بوجود تحويل مالي معلَّق يستوجب التحقق والتأكيد الفوري. ويمتد نطاق هذه الأساليب ليشمل كذلك إخطار الضحية زورًا بفوزها بجوائز مالية أو عينية ذات قيمة مرتفعة، مشروطةً بالتفعيل" عبر روابط إلكترونية مُعدَّة لاستدراج بياناتها الحساسة والإيقاع بها.[2]

3. الاحتيال عبر انتحال الشخصية

تستلزم هذه العمليات الإجرامية قدرًا عاليًا من الذكاء والدهاء، وتندرج ضمن طائفة الجرائم التي يُتوصَّل فيها إلى الهوية الرقمية للأفراد بأساليب غير مشروعة، يعمد من خلالها

[1] أسامة حمدان الرقب، المرجع السابق، ص 163

[2] أبو بكر تيتاوي، إلياس مالك قرادي، جرائم النصب والاحتيال الإلكتروني في التشريع الجزائري، مذكرة التخرج لنيل شهادة ماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، جامعة إليزي، سنة 2024-2025ص18،17

الجاني إلى نشر معلومات ذات طابع سري أو مضلل أو مغلوط تمسّ الضحية، سواء أكانت فردًا طبيعيًا أم مؤسسة تجارية.[1]

أما انتحال الشخصية فيُعدّ من أكثر الأساليب الاحتيالية شيوعًا في هذا السياق، إذ يلجأ فيه المجرم المعلوماتي إلى التظاهر بهوية شخصيات بارزة وذات مصداقية، بهدف استدراج البيانات والمعلومات اللازمة لتنفيذ مخططاته الاحتيالية. ويتوخى هذا النوع من الاحتيال الشخصي تحقيق غايتين رئيسيتين: الإضرار بسمعة الضحية والنيل من مكانتها، أو تحقيق مكاسب مالية غير مشروعة على حسابها.[2]

4الإحتيال عبر مواقع تعريف الإنترنت

من الممكن إخفاء أو إنشاء أحد مواقع التعريف بالأنترنت بشكل احتيالي من خلال تكنولوجيا الانترنت حيث يبدأ التلاعب بتفاصيل مواقع الانترنت أو بتغيير مصدر الرسالة التي تبدو أنها آتية من مستخدم آخر، وبالرغم من محاولة اكتشاف أولئك الأشخاص المتسللون والمحتالون على الانترنت ولكن لا وسيلة لمعرفتهم[3].

يجري الترويج لهذه المواقع والتطبيقات المزيفة عبر منظومة متنوعة من القنوات الرقمية، تشمل منصات التواصل الاجتماعي والرسائل النصية القصيرة والإعلانات الممولة. وما إن تزور الضحية هذه المواقع حتى يُطلب منها إدخال بياناتها المصرفية أو إتمام عملية شراء مزعومة، ليتبيّن لها في مرحلة لاحقة أن مبالغ مالية قد أُستُقطعت من حسابها دون أن تحصل في المقابل على أي سلعة أو خدمة، مما يكشف عن الطابع الاحتيالي الصريح لهذه المنصات الإلكترونية المزورة.[4]

نص المادة 394 مكرر من قانون العقوبات الجزائري يعتبر هذا الفعل من صور النصب المعلوماتي، حيث يعاقب كل من استخدم وسيلة إلكترونية لخداع الغير بهدف تحقيق

[1] Mamene Besma، *Op. cit.*، p. 98.

[2] سويح دنيا زاد، بولحية شهيرة، المرجع السابق، ص40

[3] عبدالله سيف الكيتوب، الأحكام الإجرائية جريمة الاحتيال المعلوماتي، ط 2013، دار النهضة العربية، القاهرة، ص 34

[4] ابوبكر تيتاوي الياس مالك قرادي، المرجع السابق، ص21

ربح غير مشروع. كما يندرج هذا السلوك ضمن جرائم انتحال المواقع أو استعمال علامات مضللة، وهي جرائم تتطلب رقابة رقمية صارمة وتعاوناً دولياً لتفكيكها[1].

وتُعرف هذه البرمجيات بأنها برمجيات خبيثة تصيب الأجهزة والحواسيب والشبكات، ولديها القدرة على التكاثر والانتشار السريع. ويمكن الإصابة بهذه الفيروسات والبرمجيات الخبيثة عن طريق الروابط والصفحات والإعلانات الترويجية الإلكترونية المشبوهة على الإنترنت أو المستلمة عبر البريد الإلكتروني أو حتى الرسائل النصية، كما يمكن الإصابة بها عن طريق تصفح وتنزيل الملفات الرقمية المقرصنة من على الإنترنت أو نقلها من جهاز إلى آخر.

فالفيروسات الخبيثة تعد من الأضرار الجسيمة التي يمكن أن تلحق بالأجهزة والحواسيب المستهدفة، حيث يمكن أن تتسبب في تعطيل جزئي أو تشفير كامل لكافة الملفات المخزنة على الجهاز. في بعض الحالات الخطيرة، يشترط وجود تنظيم محكم خلف الإصابة بالبرمجيات الخبيثة، حيث يتطلب القراصنة من الضحايا دفع فدية مالية مقابل فك تشفير الملفات واستعادتها، ما يعرف في ميدان الجرائم الإلكترونية بجرائم الفدية.[2]

الفرع الثاني: أساليب الاحتيال الإلكتروني

لقد أسهمت التقنية الرقمية في فتح آفاق غير مسبوقة في مجال التجسس والاستخبارات، إذ لم تعد العمليات الاستخباراتية مشروطةً بالتسلل البشري المادي إلى داخل الدول والمؤسسات، بل باتت الجهات المعنية قادرةً على الحصول عن بُعد على ما تبتغيه من معلومات حساسة وبالغة الخطورة.

وتتسم الوسائل التقنية في مجال تكنولوجيا المعلومات بالتنوع الواسع الذي يُعسّر حصرها واستيعابها، لا سيما أنها في تطور مستمر ومتسارع، وتبذل كثير من الجهات والدول جهودًا بحثية دؤوبة للارتقاء بمستوى صناعتها والوصول إلى مراحل متقدمة في هذا المجال، وتتمثل أبرز هذه الوسائل فيما يلي:

[1] الأمر رقم 66-155 قانون العقوبات
[2] لطاهر ياكر، المرجع السابق، ص26

1. استعمال هوائيات مع ربطها بحاسوب خاص

إذ تتيح هذه الهوائيات إمكانية استقبال الموجات الكهرومغناطيسية المنبعثة من الحاسوب أثناء فترة تشغيله، مع القدرة على تسجيلها ومعالجتها وتحليلها وترجمتها إلى معلومات واضحة وقابلة للاستخدام، ويمتد نطاق هذه العملية الاستخباراتية ليشمل مسافات تتجاوز ثلاثمائة قدم من الحاسوب المستهدف، مما يمنح هذه التقنية قدرًا عاليًا من الفاعلية والخطورة في آنٍ معًا.

2. استعمال تقنية أبواب المصيدة

تُعرف هذه التقنية كذلك بتقنية الأبواب الخلفية، وتقوم في جوهرها على إبقاء ثغرات مقصودة داخل البرنامج أثناء مرحلة إعداده وتطويره، وذلك بذريعة تيسير الوصول إليه لاحقًا لمعالجة ما قد يطرأ من أخطاء برمجية. والأصل في هذه الثغرات أن تُحذف وتُغلق كليًا في النسخة النهائية المُصدَرة من البرنامج، غير أنها قد تُترك عمدًا ومتعمدةً، مما يُفضي إلى إمكانية استغلالها من قِبَل أي طرف يتمكن من اكتشافها، والتوصل من خلالها إلى المعلومات والبيانات المخزنة في الحاسوب المستهدف.[1]

3الاعتراض للمعلومات المنقولة عبر النظام المعلوماتي

تقوم هذه التقنية على معرفة محتوى اتصال قد يتم داخل نظام حاسوب واحد، أو بين نظامين مختلفين أو بين عدة أنظمة ترتبط فيما بينها من خلال شبكا اتصالات وذلك بالتقاط المعلومات التي يتضمنها هذا الاتصال والتقاط الموجات الكهربائية الصادرة عن النظام المعلوماتي تعد الوسيلة الاساسية لاعتراض المعلومات المتنقلة عبر النظام.[2]

[1]نهلا عبد القادر مومني، المرجع السابق، ص128
[2]نهلا عبد القادر مومني، المرجع نفسه، ص130

المبحث الثاني: أركان جريمة الاحتيال الإلكتروني

أصبحت الجريمة الإلكترونية من أخطر الجرائم المستحدثة التي تؤرق العالم بأسره، وتهدد أمن وسلامة الدول، الأمر الذي دفع بالدول إلى البحث عن آليات جديدة تتلاءم مع خطورة هذه الجريمة ولما كان القانون هو الوسيلة المثلى لتنظيم المجتمع وحمايته وضمان أمن الأفراد واستقرارهم، ولهذا كان على التشريعات مواكبة التطورات وخاصة في مجال الجريمة الإلكترونية والتي تقوم على ثلاثة أركان رئيسية تتمثل في الركن الشرعي (مطلب أول) والركن المادي (مطلب ثاني)، والركن المعنوي (مطلب الثالث)

المطلب الأول: الركن الشرعي لجريمة الاحتيال الإلكتروني

يعد الركن الشرعي من الأركان الأساسية في أية جريمة، ويتمثل في الصفة غير المشروعة للفعل أو النص الشرعي المجرم، أي القاعدة الجنائية، لأن الجريمة لا توجد أصلا دون توافر القاعدة الجنائية ،التي تحدد الجريمة و ترسم حدودها، في جميع التشريعات الدول، نجد ان الركن الشرعي فيها لا جريمة ولا عقوبة إلا بنص قانوني، ويترتب على ذلك أن القاضي لا يمكن معاقبة شخص على فعل لم يجرمه المشرع، أي أن التشريع هو المصدر الرئيسي للقاعدة القانونية، وهذا ما نجده أيضا في الجريمة الإلكترونية فلا بد من النص القانوني حتى يطبق الجزاء على المجرم.

الفرع الأول: القاعدة العامة للركن الشرعي

يعتبر التشريع هو المصدر الأساسي للفصل في أية قضية، كما أن سلطة القاضي الجنائي محدودة بالنص التشريعي، إذ لا يجوز للقاضي تغيير قاعدة قانونية، ولا تفسيرها، ولا استبدالها، ولا انشاء نص تشريعي، وذلك ضمانا لتحقيق العدالة والشفافية[1].

يقصد هنا "بالركن الشرعي" في اصطلاح فقهاء القانون هو البنيان القانوني للجريمة، وهو ما يعرف عليه أيضاً الركن القانوني للجريمة، ففي الصياغات الفقهية القديمة كان يعرف الركن الشرعي بنص التجريم الذي يخلق الجريمة، بمعنى أنه لا جريمة بدون نص، وهذا قول

[1] حنان ريحان المبارك المضحكي، الجرائم المعلوماتية (دراسة مقارنة)، منشورات الحلبي الحقوقية، ط1، لبنان،2014، ص58

مردود عليه، إذ لا يتصور أن يكون نص التجريم ركنا من أركان الجريمة، لأنه لو كان كذلك، لوجب العلم بنص التجريم لقيام القصد الجنائي، وكان الجهل به ينفي وجود القصد الجنائي، وهو ما يتنافى مع القاعدة العامة المقررة بأن الجهل بالقانون ليس عذرا[1].

أولا: مبدأ الشرعية الجزائية

لقد تطور مفهوم الركن الشرعي تدريجياً ليستقر في صورته الحالية التي مفادها أن المقصود من النص هو الصفة غير المشروعة للفعل المُشكِّل للجريمة، ولا يكتسب الفعل صفة التجرِيم إلا إذا ورد نص قانوني يُجرِّمه، وذلك وفقاً لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على أن «لا جريمة ولا عقوبة أو تدابير أمن بغير قانون». وقد تجلّى هذا الاتجاه أيضاً في نص المادة 372 من قانون العقوبات الجزائري، التي حدّدت أركان جريمة النصب والعقوبات المقررة لمرتكبيها، إذ جاء فيها: «كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات، أو إلى الحصول على أي منها أو شرع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه، إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي، أو بإحداث الأمل في الفوز بأي شيء، أو في وقوع حادث أو أية واقعة أخرى وهمية، أو الخشية من وقوع أي شيء منها، يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 100.000 دج إلى 500.000 دج. وإذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعية، فيجوز أن تصل مدة الحبس إلى عشر سنوات والغرامة إلى 200.000 دينار».

يتضح من هذا النص أن جريمة الاحتيال تُعد إحدى جرائم الأموال المنقولة، كونها تقع على النقود أو العروض أو السندات المخالفة أو أي متاع منقول، وقد تقع استثناءً على التصرف في مال ثابت لا يمتلكه الجاني، كما أنها تمثل اعتداءً على حق الملكية.[2]

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، جرائم ضد الأشخاص وجرائم ضد الأموال وبعض الجرائم الخاصة الجزء الأول، دار هومة لطباعة والنشر والتوزيع، الجزائر، الطبعة 2024 ،21، ص324.

[2] أحسن بوسقيعة، المرجع نفسه، ص325

وتتوفر لدى الجاني نية الاستيلاء على مال الغير، وتتمثل وسيلته في تحقيق الكسب غير المشروع الاحتيال، أي خداع المجني عليه وتضليله بحيث يقع في الغلط فيقدم تحت تأثيره إلى تسليم ماله إلى الجاني.[1]

يُقصد بمبدأ الشرعية الجزائية أن المشرع وحده هو المخول بتحديد الأفعال المُعاقَب عليها (الجرائم) وتحديد الجزاءات المطبقة على مرتكبيها (العقوبات).

وتجدر الإشارة إلى أن هذا المبدأ يستلزم الأخذ بمبدأ الفصل بين السلطات، إذ إن السلطة التشريعية وحدها تمتلك صلاحية بيان الأفعال التي تشكّل جرائم وتقرير الجزاء الواجب تطبيقه على تلك الأفعال، باعتبارها صاحبة الاختصاص الأصيل في سن القوانين. وبالتالي، تنحصر سلطة القاضي في تطبيق النصوص التشريعية الصادرة عن السلطة التشريعية، فلا يجوز للقاضي أن يعتبر فعلاً ما جريمة إلا إذا ورد نص قانوني يقضي بذلك، وإذا وُجد الفعل مجرَّماً، فلا يجوز توقيع غير العقوبة المنصوص عليها في القانون. كما لا يجوز للسلطة التنفيذية توقيع جزاءات جنائية غير تلك التي قضت بها الأحكام القضائية، ولا تصحيح تلك الأحكام بأسلوب يخالف ما نصت عليه القانون[2].

لا أن مبدأ الشرعية قد تعرض لانتقادات، من أبرزها أنه يُقيّد سلطة القاضي الجزائي ويحول دون تحقيق العدالة المجتمعية، لا سيما عند ارتباط الأمر بالتطور التقني وتأخر المشرع في إصدار قوانين تواكب هذا التطور، مما يتيح الفرصة أمام مرتكبي الأفعال التي تضر بمصالح الأفراد والمجتمع وتنال من أمنه، حيث إن التدخل التشريعي العقابي غالباً ما يكون متأخر[3].

وقد طرأ تطور ملحوظ على مبدأ الشرعية، تمثل في منح القاضي قدراً من المرونة والسلطة التقديرية فيما يتعلق بتقدير العقوبة بما يتناسب مع ظروف الجريمة، إذ تطور التشريع وجعل للعقوبة حدّاً أقصى وأدنى يتخير القاضي من بينهما ما يراه أكثر ملاءمة لوضع الجاني، بل تعدى الأمر إلى منح القاضي سلطة الأمر بوقف تنفيذ العقوبة متى تبين له من ماضي

[1] نبيل صقر، الوسيط في شرح جرائم الأموال، دار الهدى، الجزائر،2012، ص90

[2] الفيل علي عدنان، مرجع سابق، ص35

[3] خالد علي سلمان عبد الله، المرجع السابق، ص118

المتهم وأخلاقه وظروفه ما يبرر ذلك. كما مُنحت السلطة التنفيذية حق التدخل في تنفيذ العقوبة بما تراه محققاً للغاية منها، كإصدار قرار العفو، وتخفيف العقوبة، والإفراج الشرطي عن المسجون قبل انتهاء مدة عقوبته إذا ثبت صلاحه.[1]

خلاصة القول، إنه بالرغم من المرونة التي طرأت على مبدأ الشرعية الجزائية، إلا أنها اقتصرت على شقه الثاني المتعلق بتقدير العقوبة، دون أن تمتد إلى الشق الأول المتعلق بالتجريم، إذ يظل القاضي ممنوعاً من أي سلطة تقديرية في شأن تحديد الأفعال المجرّمة.

الفرع الثاني: قاعدة التجريم والعقاب لجريمة الاحتيال الالكتروني في التشريع الجزائري

إن تطور جريمة الاحتيال باستخدام وسائل تقنية المعلومات، وتعدد صورها، وضخامة ما تحدثه هذه الجرائم سواءً من المخاطر الاقتصادية والأمنية والاجتماعية أدى لتصدي بعض الدول لهذه الجريمة عبر نصوص قانونية خاصة للحد من سرعة انتشارها، ولكن تجدر الإشارة هنا إلى حداثة هذه الجريمة فلا إشكالية تثار عند الحديث عن الأجهزة الإلكترونية المادية حيث تنطبق عليها نصوص التجريم التقليدية.

ما أن أغلب النصوص في التشريعات المقارنة لم تنص بشكل صريح على جريمة الاحتيال الإلكتروني، وإنما نجد أن تجريم فعل الاحتيال يُستفاد من مضمون ودلالات النصوص التشريعية المختلفة.

وتتمثل شرعية جريمة الاحتيال في النص القانوني الذي ينص صراحة على ذلك، حسب ما ورد في المادة 372 من قانون العقوبات. كما نص المشرع على القيود الخاصة الموقفة لمباشرة الدعوى العمومية بموجب المادة 373، حيث تسري الإعفاءات وقيود مباشرة الدعوى العمومية المنصوص عليها في المادتين 368 و369 على جنحة الاحتيال المقررة في المادة 372.

[1]الفيل علي عدنان، مرجع سابق، ص35

كما ربط المشرع الجزائري مفهوم هذه الجريمة بانتحال الوظائف والالقاب او الاسماء واساءة استعمالها، واعتبرت من قبيل جريمة التحايل والاحتيال[1]، إن التحايل والنصب لا يقتصر غرضهما على تحقيق العائد المادي فحسب، بل قد يعود إلى اعتبارات أخرى متنوعة كالانتقام، ويأخذ اشكالا متعددة مثل ما اشارت اليه المواد (243-246) من قانون العقوبات الجزائري:

-التدخل في غير الصفة المقررة قانوناً في الوظائف العمومية والمدنية والعسكرية، أو القيام بعمل من أعمال هذه الوظائف.

-استعمال شخص لقباً متعلقاً بمهنة منظمة قانوناً، أو شهادة رسمية، أو صفة حددت السلطة العمومية شروط منحها، أو ادعاء الشخص لنفسه شيئاً من ذلك دون استيفاء الشروط المفروضة لحملها.

-انتحال شخص لنفسه -بصورة عادية أو في عمل رسمي -لقباً أو رتبة شرفية.

ونظراً لأن التحايل والاحتيال الإلكتروني الرقمي المعلوماتي يُعد من الجرائم المستحدثة التي تكتسي بحكم طبيعتها طابعاً دولياً، كونها ترتكب عبر الشبكة الدولية للمعلومات أو في الوسط المعلوماتي، وذلك بفعل سرعة انتشارها وتجاوزها للحدود الجغرافية، قد سارعت العديد من الدول والمنظمات الدولية إلى تطوير منظومتها القانونية، ومسايرة التطور الحاصل في مجال الجرائم الرقمية، او التي أبرزها جريمة الاحتيال الالكتروني. [2]

[1]لأنه في المقابل نجد أن التشريعات اختلفت في تسمية هذه الجريمة، فالمشرع الفرنسي تناولها لأول مرة بعبارة طرق احتيالية واعتبر الاحتيال والنصب جريمة قائمة بذاتها في نص المادة (405)، التي نصت على انه كل من يتوصل الى ان بسلب او يشرع في سلب مال او بعض ثروة الغير. كما ان المشرع المصري تناول هذه الجريمة في نص المادة (336) من قانون العقوبات، حيث اعتبرت الاحتيال ينال بالاعتداء على حق ملكية المال العام المنقول والاستيلاء على مال منقول مملوك للغير

[2]وكانت الدول المتقدمة هي السباقة في مواجهة الجرائم الالكترونية، سواء عن طريق وضع التشريعات الجزائية، أو من خلال تعديل النصوص القائمة لتشمل هذه الجرائم المستحدثة. وبعد التشريع الفرنسي من أوائل التشريعات التي تناولت لجرائم الالكترونية بما فيها جرائم النصب والاحتيال على بطاقات الائتمان وذلك منذ عام 1988 بقانون Godfrain. اما على صعيد الاتفاقيات الدولية فتم انعقاد مؤتمرات وابرام العديد من الاتفاقيات الدولية لمكافحة الجرائم الالكترونية، منها اتفاقية بود الست لمكافحة جرائم المعلوماتية والانترنيت 2001، القانون العربي النموذجي الاسترشادي لمكافحة الجريمة لمعلوماتية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 عبد الكافي مريم بورابة صورية جريمة الاحتيال لمعلوماتي الواقعة على البطاقات المالية الالكترونية مجلة القانون العلوم السياسية مجلد 08 عدد 2022 01)، ص406-427

من جانبه، اتجه المشرع الجزائري إلى استحداث نصوص إجرائية وعقابية تتعلق بالأفعال المكونة للجرائم الإلكترونية، بما في ذلك جرائم التحايل والاحتيال الإلكتروني، كما تمت المصادقة على بعض الاتفاقيات الدولية التي تتناول هذا السلوك الإجرامي. ومن بين أهم التشريعات التي أصدرها المشرع الجزائري في هذا المجال، يمكن ذكر ما يلي:

. القانون رقم 15-04 المؤرخ في 2004/11/10 والمعدل والمتمم للأمر 156-66

المتضمن قانون العقوبات، حيث اضاف القسم السابع تحت عنوان" المساس بأنظمة

المعالجة الآلية للمعطيات في المواد من 394 مكرر الى 394 مكرر 7

. القانون رقم 22-06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية.

. القانون رقم 04-09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من لجرائم المتصلة بتكنولوجيا الاعلام والاتصال، ويهدف هذا القانون الى وضع نصوص اجرائية تتناسب مع الجرائم الالكترونية.

ومما يلاحظ أن المشرع الجزائري لم يبادر إلى وضع نص خاص محدد ودقيق لمفاهيم وصور جرائم التحايل والاحتيال الإلكتروني، إذ اكتفى فقط بالإشارة إليها في المادة 394 مكرر 2 من النص القانوني 04-05 من قانون العقوبات، وذلك من خلال مفهوم "الاتجار بالمعطيات المعلوماتية عبر النظم المعلوماتية بهدف الربح".

ما على المستوى العربي، فقد نصت المادة (4) من المشروع النموذجي العربي الموحد على تجريم الاحتيال الإلكتروني، حيث جاء فيها: "كل من استحوذ بالالتقاط بطريق التحايل على البرامج والبيانات المخزنة بالحاسب والمسجلة على شريط أو أسطوانات ممغنطة أو التي تظهر على الشاشة يعاقب".[1]

كما أقرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010م تجريم الاحتيال الإلكتروني في المادة (11) منه، حيث عرفته بأنه: "التسبب بإلحاق الضرر بالمستفيدين

[1] خالد علي سلمان عبد الله، مرجع سابق، ص120

والمستخدمين عن قصد وبدون وجه حق، بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل أو للغير، وذلك عن طريق:

. إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات

. التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييره

. تعطيل الأجهزة والبرامج والمواقع الالكتروني

على الرغم من أن المشرع في التشريعات المقارنة والدول الأجنبية قد عمل على تحديد صور الاحتيال المعلوماتي وتقرير عقوبة لها، إلا أن الباحث يرى أن العقوبة ينبغي أن تتناسب مع حجم تأثير الجريمة ونتائجها. فإذا وقع الفعل الإجرامي بدافع التسلية وحب الاستطلاق، فإن العقوبة المفروضة ينبغي أن تكون أخف وطأة مقارنة بتلك المطبقة على الجرائم التي تخلف آثاراً بالغة الجسامة، كالتي تمس الحقوق الأساسية أو المعلومات ذات القيمة العالية. وبناءً على ذلك، يمكن اقتران شدة العقوبة بالعنصر القصدي والنتائج المترتبة على الفعل.

المطلب الثاني: الركن المادي لجريمة الاحتيال الإلكتروني

لا يختلف الركن المادي في جرائم الاحتيال الإلكتروني على الجرائم التقليدية، فلا جريمة دون أن يتوفر فيها الركن المادي(الفرع الأول) والمتمثل في السلوك الذي يقوم به الجاني من أجل تحقيق غايته وهي دفع المجني عليه تسليم ماله إلى الجاني بفعل الخداع، إلا أن تحديد الركن المادي في جريمة الاحتيال الإلكتروني تكتنفه بعض الصعوبات فيما يتعلق بتحديد النتيجة الإجرامية والرابطة السببية(الفرع الثاني)، وبناءً عليه فإن للركن المادي في الجرائم قواعد عامة سنبين مدى تطابقها مع جريمة الاحتيال الإلكتروني ، وسيتم تقسيم المطلب إلى فرعين

الفرع الأول: ماهية الركن المادي

يُقصد بالركن المادي للجريمة وجود فعل خارجي ملموس يمكن إدراكه بالحواس، وهو يعبّر بصورة خاصة عن الواقعة الإجرامية التي يشكّلها السلوك المادي الخارجي الذي ينص القانون على تجريمه. ويشمل الركن المادي كل ما يدخل في كيان الجريمة ويتسم بطبيعة مادية

محسوسة، وهو ضروري لقيام الجريمة إذ لا تُعرف في القانون جرائم بغير ركن مادي، ولذا عُرف لدى بعض الفقه ب "ماديات الجريمة".

تختلف الجرائم الإلكترونية عن غيرها من الجرائم التي تستلزم أعمالاً تحضيرية، إذ يصعب فيها الفصل بين العمل التحضيري والبدء في التنفيذ. فرغم أن القانون لا يعاقب على الأعمال[1] التحضيرية في الجرائم التقليدية، فإن الوضع يختلف في مجال تكنولوجيا المعلومات، حيث تُعتبر أفعال كشراء برامج الفيروسات التي لم تُطلق بعد على الشبكة الإلكترونية جريمة قائمة ذاتها.[2]

يتكوّن الركن المادي للجريمة الإلكترونية من ثلاثة عناصر: السلوك الإجرامي، والنتيجة، والعلاقة السببية. علماً أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كما في حال التبليغ عن الجريمة قبل حدوث نتيجتها. وبناءً على ذلك، اشترط الفقه القانوني لقيام الركن المادي ثلاثة عناصر أساسية هي:

أولاً: الفعل أو السلوك غير المشروع (النشاط الإجرامي):

يقصد به فعل الجاني الذي يحدثه في العالم الخارجي، فلا يمكن محاسبة الشخص على نواياه أو هواجسه الداخلية، وما يترتب على هذا السلوك من تغيير للحقيقة في واقعة معينة. وينقسم السلوك الإجرامي إلى نوعين:

1. السلوك الإيجابي: وهو كل قول أو فعل يجرمه القانون ويصدر عن الجاني مؤدياً إلى نتيجة في الجرائم الضارة، ويُعتبر في الجرائم الشكلية سلوكاً إجرامياً بذاته. تدخل جريمة الاحتيال الإلكتروني ضمن السلوك الإيجابي لما تحدثه من نتيجة. فجوهر النشاط الإجرامي في السلوك الإيجابي يتمثل في فعل الخداع الذي يهدف إلى تغيير الحقيقة في واقعة ما بما يؤدي إلى وقوع المجني عليه في لبس يدفعه إلى تسليم ماله للجاني. ولا يكفي الكذب لتحقيق النشاط الإجرامي، بل يلزم أن يقترن بإحدى الوسائل الاحتيالية[3].

[1] الطاهر ياكر، مرجع سابق، ص39

[2] الطاهر ياكر، المرجع السابق، ص39

[3] علي القهوجي، شرح قانون العقوبات، دار النهضة العربية، القاهرة،1993م، ص762

.2السلوك السلبي: ويتمثل بسلوك أو موقف يتخذه المكلف بقاعدة قانونية تفرض عليه فعلاً لا يقوم به، فينشأ السلوك السلبي عن امتناع الشخص أو إحجامه عن القيام بعمل يوجبه القانون مع قدرته على تنفيذه ،

من المتعارف عليه فقهياً أن السلوك المادي لجرائم الاحتيال الإلكتروني يشترط وجود بيئة رقمية واتصال بالإنترنت، بالإضافة إلى الإلمام ببداية النشاط الإجرامي ونتيجته. فيتعيّن على مرتكب جريمة الاحتيال الإلكتروني تجهيز وسيلة تقنية المعلومات المراد استخدامها في الجريمة، وإعداد البرامج اللازمة، وقد يحتاج إلى تهيئة صفحات ومعلومات أخرى كالفيروسات تمهيداً لاستخدامها في الجريمة[1].

وعليه، تتطلب هذه الجريمة أعمالاً تحضيرية، كشراء البرامج المعدة لاختراق أنظمة الحاسوب أو لفك الشفرات وسرقة كلمات السر الخاصة بالمقتنيات الإلكترونية كبطاقات الائتمان والبريد الإلكتروني. ويتطلب هذا النشاط الإجرامي الدخول غير المشروع أو غير المصرح به للتلاعب بالبيانات وانتهاك الخصوصية الشخصية للأفراد، بقصد إلحاق الضرر بصاحبها أو تحويل الأموال والاستيلاء عليها. ويُعد هذا النشاط من أهم صور الركن المادي لجريمة الاحتيال الإلكتروني. وإن كانت بعض الجرائم قد تتحقق بوجود سلوك سلبي، إلا أن قيام السلوك السلبي في جريمة الاحتيال الإلكتروني يبدو صعباً، ذلك أن مرتكب هذه الجريمة لا بد أن يتدخل بسلوك إيجابي لارتكابها.[2]

ثانيا: النتيجة الإجرامية

تُعرَّف النتيجة الإجرامية بأنها الأثر الذي يُحدثه السلوك الإجرامي في الواقع الخارجي، وقد يتمثل هذا الأثر في تغيير حسي ملموس لذلك الواقع. غير أنه تجدر الإشارة إلى أن النتيجة، باعتبارها عنصراً من عناصر الركن المادي، تستند إلى ما يعتد به المشرع ويُرتِّب عليه جزاءً، بغض النظر عن كامل الآثار التي قد يُحدثها السلوك الإجرامي. فعلى سبيل المثال، قد لا يحدث السلوك الإجرامي أثراً مادياً ملموساً، كأن يقوم الجاني بمحاولة اختراق نظام معلومات

[1]برنامج الفيروس له تأثير كبير على برامج الحاسب الآلي لما له من قدرة على إحداث تغيير في البرامج والبيانات المتداولة على الحاسب تصل إلى الاتلاف الكلي للبرامج، وأول ظهور برامج الفيروس عام 1959م، أنظر أيمن عبد الحفيظ، "الاتجاهات الفقهية والأمنية لمواجهة الجرائم المعلوماتية"، دون دار نشر، 2005م، ص 67

[2]خالد علي سلمان عبد الله، مرجع سابق، ص124

لحاسوب آلي بهدف الاستيلاء على معلومات وبيانات أرصدة أو مستندات مالية لتحويلها إلى حسابه الخاص، إلا أن نظام الحماية لذلك الحاسب لا يسمح له بالدخول إلى تلك البيانات والمعلومات. ففي هذه الحالة، يكون السلوك الإجرامي لم يُحقق نتيجته المتمثلة في الاستيلاء على المال.

إن الهدف الذي يسعى الجاني إلى تحقيقه في جريمة الاحتيال الإلكتروني هو الاستيلاء على مال منقول مملوك للغير باستعمال وسائل تقنية المعلومات. فإذا لم تتحقق هذه النتيجة عن السلوك الإجرامي، فإننا نكون بصدد الشروع في ارتكاب هذه الجرائم[1].

إذ يُعَدُّ الشروع جريمة تبدأ فيها الأفعال التنفيذية، إلا أن النتيجة الإجرامية لا تتحقق لظروف خارجة عن إرادة الفاعل. والشروع بجميع أنواعه (التام والناقص) يمكن تصوُّره في جريمة الاحتيال الإلكتروني. فمَن يخترق نظاماً إلكترونياً لأحد المصارف عبر الإنترنت ويُدخل البيانات اللازمة لإجراء عملية احتيال عن طريق تحويل أموالٍ بصورة غير مشروعة، ثم لا تتم النتيجة الإجرامية ولا يتحقق التحويل بسبب خلل في إدخال البيانات، فإن نشاط الفاعل هذا يُشكِّل فعلاً احتيالياً.[2]

ثالثا: العلاقة السببية

تأتي العلاقة السببية، في النظرية العامة للجريمة، كجزء من الركن المادي، فهي حلقة الاتصال بين السلوك الإجرامي والنتيجة الإجرامية، ويتمثل دورها في بيان ما كان للفعل من نصيب في إحداث النتيجة، وإثبات أن الفعل كان سبباً في حدوثها. ويُشتَرَط في جريمة الاحتيال أن يكون تسليم المال من المجني عليه إلى الجاني مبنياً على الكذب والخداع والمناورات الاحتيالية التي استخدمها الجاني. فإذا سلَّم المجني عليه ماله للجاني دون أن تكون تلك الطرق

[1] احمد محمد مصطفى، جرائم الحاسبات الالية في التشريع المصري، دراسة مقارنة، دار النهضة العربية، القاهرة،2010م، ص107

[2] محمد طارق الخن، جريمة الاحتيال الالكتروني عبر الانترنت، الاحكام الموضوعية والاحكام الإجرائية، منشورات الحلبي الحقوقية، ط1، بيروت ،2011 ص 178.177

الاحتيالية سبباً في ذلك، فإن هذا الأمر ينفي صفة السببية بين الاحتيال والتسليم، وبالتالي لا تقوم جريمة الاحتيال[1]

وعنصر السببية ضروري في جميع الجرائم التي تربط بين السلوك الإجرامي والنتيجة المترتبة عنه. غير أن النتيجة الإجرامية في جريمة الاحتيال الإلكتروني قد لا تترتب حتماً عن السلوك الإجرامي، ولا بمقتضى طبيعة الأشياء. وفي هذه الحالة، يكون عنصر السببية ذا أهمية بالغة، بل عنصراً قائماً بذاته. فقد يقوم المجني عليه بتسليم ماله للجاني ليس بسبب ما انطلى عليه من الأساليب الاحتيالية، وإنما بدافع الشفقة على الجاني، أو بهدف القبض عليه متلبسا.[2]

الفرع الثاني: تحقق الركن المادي لجريمة الاحتيال الإلكتروني

تقوم الجريمة عموماً على ثلاثة عناصر أساسية تدخل في تكوين الركن المادي، وهي: السلوك الإجرامي، والنتيجة، والعلاقة السببية. ونظراً إلى أن جريمة الاحتيال المعلوماتي تمثل تداخلاً بين الاحتيال التقليدي والجريمة المعلوماتية، فإن دراستها تستلزم بيان مكونات الركن المادي لكل منهما على حدة.

أولا: السلوك الإجرامي (وسائل التدليس والاحتيال)

نصّت المادة 372 من قانون العقوبات الجزائري على الأفعال التي تشكّل السلوك الإجرامي في جريمة الاحتيال، ويمكن إجمالها في العناصر التالية:

– الكذب: يتمثل في تقديم معلومات زائفة على أنها حقيقية، سواء كان ذلك شفوياً أو كتابياً. وعلى سبيل المثال، ادعاء شخص امتلاكه قدرات خارقة كالشفاء من الأمراض أو التنبؤ بالمستقبل بقصد إقناع الضحايا، مما يدفعهم إلى تسليمه أموالاً أو ممتلكات.[3]

[1] جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة، عمان،2010، ص54

[2] بلال امين زين الدين، جرائم نظم المعالجة الالية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، ط1، الإسكندرية، 2008، ص158

[3] فاطمة الزهراء رمضاني، علي بدرائي، القصور التشريعي في مجال الجريمة المعلوماتية في التشريعين المغربي والجزائري، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، الجزائر، العدد 02، المجلد 07،2022، ص 866

– المظاهر الخارجية المصاحبة للكذب: لا يكفي الكذب وحده لقيام جريمة الاحتيال، بل يجب أن يكون مدعوماً بوسائل أو أساليب ظاهرية توهم المجني عليه بمصداقيته، ومن هذه الوسائل: الاستعانة بشخص آخر لتأكيد الرواية الاحتيالية، استخدام أوراق أو مستندات صحيحة أو مزورة، استغلال وسائل الإعلام والنشر لنشر معلومات مضللة، انتحال صفة صحيحة (كصفة موظف رسمي أو طبيب)، أداء تمثيليات توهم بالمكانة أو السلطة، القيام بأعمال مادية توهم بوجود مشروع فعلي، واستغلال وقائع ناقصة لإقناع الضحية [1]

يتجلى هذا الركن في جريمة الاحتيال الإلكتروني في قيام الجاني باستخدام وسائل إلكترونية أو رقمية بهدف خداع المجني عليه واستغلال جهله أو ثقته. ومن أبرز هذه الوسائل: رسائل الاحتيال عبر البريد الإلكتروني(Phishing) ، المواقع الإلكترونية الوهمية، الحسابات المزورة على شبكات التواصل الاجتماعي، أو التطبيقات المزيفة. وغالباً ما تتضمن هذه الوسائل ادعاءات كاذبة مثل الفوز بجائزة، أو ضرورة تحديث معلومات بنكية، أو طلب مساعدة مالية مستعجل.

. ثانيا: النتيجة

قصد بالنتيجة الإجرامية الأثر الطبيعي المترتب على السلوك، متى اعتُبر من الوجهة التشريعية عدواناً على حق أو مصلحة يحميها القانون. وتُمثل النتيجة الإجرامية ذلك التغيير الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي، والذي يعتد به القانون فيجعله عنصراً من العناصر المكونة لجريمة معينة، بحيث لا تقع الجريمة تامة إلا بتوافره مع بقية العناصر الأخرى. فالنتيجة الإجرامية تعد إحدى عناصر الركن المادي في الجريمة.

ويستخلص من تعريف النتيجة على النحو السابق أن لها مدلولين، أولها طبيعي مادي يمكن إدراكه حسيا[2]، يتجسد في الأثر أو الآثار المترتبة على السلوك، والنتيجة بهذا المعنى تمثل تغييراً يحدث في العالم الخارجي. وثانيها مدلول معنوي قانوني يتمثل في العدوان على الحق أو المصلحة التي ارتآها المشرع جديرة بالحماية الجنائية، ويترتب على النتيجة بهذا المعنى أحكام قانونية عديدة فيما يتعلق بتحقق صلة السببية، والشروع، والقصد الجنائي.

[1] فاطمة الزهراء، المرجع نفسه، ص867

[2] محمود نجيب حسني، شرح قانون العقوبات، دار النهضة العربية، القاهرة، مصر،1988، ص144

يرى أن النتيجة قد لا تكون عنصراً في بعض الجرائم الأخرى التي تقوم وتكتمل دون تحققها، وقد درج الفقه على تسمية الجرائم التي يلزم فيها تحقيق نتيجة بالجرائم المادية أو جرائم الضرر، في حين تُطلق تسمية الجرائم الشكلية أو جرائم الخطر على الجرائم التي لا يلزم فيها تحقيق نتيجة.

ما تُثير النتيجة الإجرامية في جرائم الحاسوب والإنترنت مشاكل متعددة، من أبرزها مسألة مكان وزمان تحقق النتيجة الإجرامية. فهل تُعد هذه الجريمة مرتكبة سلوكاً ونتيجة في العالم الافتراضي، أو أن هناك امتداداً للنتيجة لكي يتحقق منتهاها في العالم المادي؟ أو يتحقق أولها في العالم الافتراضي ثم يكون هناك امتداد في النتيجة من العالم الافتراضي إلى العالم المادي؟ وذلك قياساً على أثر النتيجة الإجرامية ذات البعد الدولي، سواء في شكل امتداد الضرر أو الخطر إلى ما يتجاوز الحدود الإقليمية التي وقع فيها السلوك المجرم، وتأخر حدوث النتيجة، حيث يأخذ هذا الامتداد شكل العدوان على حق أو مصلحة قائمة ومشروعة في دولة أخرى أو دول متعددة.[1]

ويُؤخذ في الاعتبار أيضاً أن هناك جرائم يكون لها وجود سواء عبر الإنترنت أو عبر الحاسوب، أي كل جرائم التقنية التي لا يمتد أثرها إلى العالم المادي، ويشمل ذلك بطبيعة الحال صعوبة اكتشافها وإقامة الدليل على ارتكابها. وهذا ما جعل القانون المقارن يتجه إلى محاولة إرساء رؤية قانونية لتقدير قيام المسؤولية الجنائية في كل محاولة إفساد أو إعاقة مصلحة معلوماتية. وبناءً على ذلك، ينطلق النهج وفقاً لهذه النظرية من الأخذ في الاعتبار بضرورة أن تكون كل علاقة مشبوهة تهدف إلى تعطيل أو المساس بالخدمات التي يقدمها الإنترنت أو الحاسوب لمستخدمه الشرعي. وكل ذلك يؤدي بالضرورة إلى الاهتمام بالنتيجة الإجرامية ذات النشاط المادي للجريمة، باعتبارها الخلاصة النهائية التي ما كان المشرع المقارن ليتحرك إلا بسببها. ومن ثم يلزم هنا التعرّض لتأثير منطق العالم الافتراضي في العالم المادي، وذلك بهدف التعرف على نوعية النتيجة وهذا التأثير الذي أقرّ به المشرع الجنائي.[2]

[1] خالد علي سلمان عبد الله، المرجع السابق، ص128-129

[2] ميرفت محمد حبايب، المرجع السابق، ص171

هكذا نجد أن النتيجة الإجرامية تُشكّل عنصراً هاماً من عناصر الركن المادي للجريمة المعلوماتية، وتتوقف عليها العديد من أحكام النظرية العامة لقانون العقوبات. فبدون المساس بالنظام المعلوماتي لا يمكن تصوّر قيامها، ولا حتى البحث فيها، إلا إذا تعلق الأمر بإحدى جرائم الخطر الماسة بهذا النظام، والتي يتطلب بناؤها القانوني حصول نتيجة في معنى العدوان الفعلي على حق أو مصلحة معلوماتية يحميها القانون. كما أن الشروع لا يكون متصوراً ولا معاقباً عليه إلا حين يمكن تصوّر حدوث نتيجة، حيث يقع كل السلوك أو بعضه وينتفي معه حدوث النتيجة وذلك في الجرائم العمدية. أما إذا لم يكن تصوّر حدوث نتيجة ممكناً، فلا عقاب على الشروع في الجرائم غير العمدية.[1]

ثالثا:العلاقة السببية بينهما

تُعتبر العلاقة السببية في الجرائم الإلكترونية عنصراً مهماً من عناصر الركن المادي، إذ تقوم على البحث عن الصلة بين الفاعل والفعل الذي ارتكبه من جهة، وبين الحاسوب من جهة أخرى، كما أنها تحدد نطاق المسؤولية الجزائية.[2]

تناول المشرع الجزائري الجريمة الإلكترونية في قانون العقوبات، حيث يتجلى الركن المادي لجريمة الدخول غير المشروع في فعل الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات أو إلى جزء منه، والدخول المقصود هو الاتصال بنظام الكمبيوتر بأي طريقة كانت، ويُقصد به الدخول المعنوي باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي. ويتحقق الضرر بحذف المعطيات أو تغييرها في المنظومة أو تخريب نظام اشتغالها، وذلك وفقاً للمادة 394 مكرر/2. كما يتخذ السلوك الإجرامي في جريمة البقاء صورة الوجود داخل نظام المعالجة الآلية للمعطيات، وتُعد هذه الجريمة من الجرائم الشكلية التي لا يُشترط فيها حدوث نتيجة إجرامية محددة، إذ يكفي البقاء غير المصرح به داخل النظام المعلوماتي لقيام الركن المادي لهذه الجريمة، وذلك حسب المادة 394 مكرر.

وجاء في المادة 349 مكرر/1 بشأن جريمة التلاعب بمعطيات الحاسوب الآلي أن السلوك الإجرامي يتمثل في فعل إدخال معطيات جديدة غير صحيحة أو محوها أو تعديلها،

[1] سليمان عبد المنعم، النظرية العامة لقانون العقوبات، دار المطبوعات الجامعية، الإسكندرية، مصر،2014، ص412

[2] حنان ريحان المبارك المضحكي، المرجع السابق، ص89،90

سواء باستخدام القنبلة المعلوماتية أو عن طريق برامج الفيروسات عموماً، ويكفي توافر إحدى هذه الأفعال لقيام الركن المادي. وتُعتبر هذه الجريمة من جرائم الضرر المادي، إذ لا يكفي أن يهدد السلوك سلامة المعطيات، بل يجب أن يقع ضرر فعلي على هذه المعطيات متمثل في تغيير حالتها، فهي بذلك تتطلب نتيجة معينة تترتب على السلوك الإجرامي، ألا وهي تغيير حالة المعطيات.[1]

ثانياً: تكييف الأموال الكتابية أو البنكية في جريمة الاحتيال الإلكتروني

ان المحل المادي لجريمة الاحتيال يتمثل في الأشياء المادية، وبالتالي إذا قام شخص بالاحتيال على جهاز حاسوب آلي وتوصل إلى الاستيلاء على منقول مادي أو مبالغ نقدية بأي طريقة، فإن ذلك يقع تحت طائلة العقاب بمقتضى جريمة الاحتيال دون غرابة. غير أن الصعوبة تكمن في حالة تم هذا الاستيلاء عن طريق القيد الكتابي، كأن يتلاعب شخص في البيانات المخزنة في الحاسوب الآلي بغرض تحويل أرصدة الغير إلى حسابه، أي أنه يقوم بالاستيلاء على نقود كتابية أو بنكية. وهنا تثار الإشكالية: هل حدث استيلاء على المال أم لا؟

النسبة للتشريع الفرنسي، فقد ابتدع القضاء نظرية "التسليم المعادل"، التي أقرتها محكمة النقض الفرنسية، حيث اعتبرت أن مجرد القيد الذي لا يقتضي تسليم شيء مادي أيّاً كان يُعد من قبيل التسليم المعادل. وفي الولايات المتحدة الأمريكية، أصدر المشرع الأمريكي قوانين عرّف من خلالها المال على أنه كل شيء يمثل قيمة، ويشمل هذا التعريف جميع الأموال الكتابية أو البنكية، وقد حذا حذو المشرع الأمريكي في هذا الخصوص كل من المشرع الكندي والهولندي والسويسري.[2]

لكي تتحقق هذه العلاقة، يجب توافر ثالثة شروط رئيسية:[3]

.1أن يكون التسليم قد تم بفعل الوسائل الاحتيالية: يجب أن تكون الوسائل المستعملة من قبل الجاني، سواء كانت أقوالاً خادعة أو وثائق مزيفة أو مظاهر احتيالية، هي التي أحدثت

[1] ميرفت محمد حبايبه، المرجع السابق، ص171،172

[2] خالد علي سلمان عبد الله، المرجع السابق،132.133

[3] اسامة حمدان الرقب، المرجع السابق، ص 53

أثرها المباشر في نفس المجني عليه وأقنعته بصحة المزاعم المقدمة، مما دفعه إلى تسليم المال أو المنقول.

.2أن يكون المجني عليه جاهلاً بالحقيقة: فلو كان الضحية على علم بالحقيقة، أو كان متحفظاً في قراره، فإن عنصر العلاقة السببية ينهار ولا تتحقق الجريمة في شكلها الكامل. إذ يجب أن يكون الجهل ناتجاً عن الاحتيال، لا عن إهمال من المجني عليه أو تقصير منه في التحقق.

.3أن تكون الأفعال الاحتيالية هي السبب المباشر في اتخاذ قرار التسليم: أي أن يكون هناك ترابط زمني ومنطقي بين الفعل الاحتيالي وقرار التسليم. فإذا تدخل سبب أجنبي أو خارجي آخر، فإن العلاقة السببية تنقطع، ولا يمكن مساءلة الجاني عن النتيجة التي لم تترتب مباشرة عن فعله.

في سياق الجرائم المعلوماتية، تتجلى هذه العلاقة عندما يقع مجني عليه ضحية للخداع الرقمي، كأن يستجيب لرسالة إلكترونية توهمه بربح جائزة ويقوم بتحويل مبلغ مالي أو تقديم بياناته البنكية. فإذا ثبت أن قرار المجني عليه بالتسليم لم يكن ليقع لولا الأفعال الاحتيالية التي مارسها الجاني باستخدام وسائل رقمية، فإن العلاقة السببية تُعد متحققة، وبالتالي تقوم أركان الجريمة بكاملها.

وعليه، نرى أنه لكي يتحقق الركن المادي في الجريمة الإلكترونية لا بد من وجود جهاز إلكتروني وتجدر الإشارة إلى أن إثبات الركن المادي في النصب الإلكتروني قد يكون أكثر تعقيداً من النصب التقليدي، نظراً لغياب التفاعل المادي المباشر بين الجاني والضحية، ولجوء الجناة إلى أدوات رقمية يصعب تتبعها. ولهذا فإن مهمة القاضي الجنائي تتطلب دقة كبيرة في تحليل الأدلة الإلكترونية وربط الوقائع بعضها ببعض، وذلك لإثبات أن الوسيلة الاحتيالية كانت السبب الحقيقي الذي دفع المجني عليه إلى التسليم.[1]

[1]علي ابراهيم بن دارج، محاضرات في الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية، المركز الجامعي أفلو، الاغواط،2021، ص 5

المطلب الثالث: الركن المعنوي لجريمة الاحتيال الإلكتروني

يدخل الركن المعنوي في جانب التحليل الشخصي والذاتي لبنيان الجريمة، إي إرادة الجاني ومسئوليته عن الفعل أو الامتناع المنسوب اليه (فرع أول)، بالإضافة إلى توفر القصد الجنائي بصوره المختلفة والذي يتحقق بتحقق النتيجة الجريمة الجرمية وإصرار الجاني على هذا القصد (فرع ثاني)، بالإضافة إلى علمه بأن فعله غير مشروع وأن القانون يعاقب على ارتكاب هكذا أفعال (فرع ثالث)، وسيتم تقسيم المطلب إلى ثلاثة فروع كالآتي:

الفرع الأول: ماهية الركن المعنوي للجريمة

يُقصد بالركن المعنوي العلاقة القائمة بين القصد الجنائي والإرادة المتوافرة لدى الجاني لارتكاب جريمته، أي اتجاه السلوك الإجرامي نحو تحقيق النتيجة الإجرامية. ووفقاً لذلك، يلزم لقيام الجريمة في هذا التحليل أن يأتي الجاني الفعل أو الامتناع وهو متمتع بإرادة حرة قادرة على الاختيار، وواعية قادرة على الفهم والإدراك، ومذنبة أو آثمة، أي جديرة باللوم.[1]

بناءً على ما سبق، يفترض الركن المعنوي التحقق من أن الفعل غير مشروع، لأنه إذا كان مشروعاً لم تكن العلاقة به محلاً للوم، ومن ثم فإن التأكد من تجريم القانون سابق على التحقق من توافر الركن المعنوي. فلكل جريمة طبيعة خاصة وعناصر ذاتية لتحقق الركن المعنوي فيها.[2]

وتأسيساً على ذلك، فإن الركن المعنوي على العموم يُعد انعكاساً لماديات الجريمة في نفسية المجرم، فالإرادة تتجه إلى تحقيق تلك الماديات، أما الركن المادي فهو النية الإجرامية التي يأتي بها الجاني والتي تتجسد في كيان مادي محسوس.

الركن المعنوي من حيث نظرية السياسة الجنائية يُعد منطقة دستورية خالصة، ويكفي هنا الإشارة إلى أن منطق الشروع في ارتكاب الجرائم لا يتقرر إلا بناءً على تحديد الركن المعنوي في هذه الجرائم، وبالتالي فإن استحقاق العقاب لا يكون سوى في الجرائم التي يبرز

[1] احمد عوض بلال، الاثم الجنائي، دار النهضة العربية، القاهرة،2003، ص21

[2] بدوي حنا، الاحتيال، زين الحقوقية والأدبية، ط2، بيروت،2003، ص169

فيها الركن المعنوي في صورة عمد مصحوب بجريمة من الجرائم المادية ذات نتيجة، وتتحدد معالمه على هذا الاساس.[1]

الفرع الثاني: القصد الجنائي

القصد الجنائي هو الهدف المباشر للسلوك الإجرامي والذي ينحصر في حدود ارتكاب فعل الجريمة، وهو ما يتطلب توافر النتيجة وتأكيد وقوعها، والأصل في ذلك ارتكاب هذا الفعل غير المشروع، فلا يمكن انتقاء العلم كعنصر أساسي للقصد الجنائي. وللقصد الجنائي عناصر يجب توافرها، وهي:

أولاً: عناصر القصد الجنائي.

لا يتحقق القصد الجنائي إلا بتوافر عنصري العلم والإرادة، وذلك على النحو التالي:

.1العلم: لا يتحقق القصد الجنائي إلا إذا كان الجاني يعلم بالعناصر الأساسية لقيام الجريمة، سواء تعلق ذلك بسلوكه الإجرامي أم بموضوع الاعتداء. ففي جريمة الاحتيال، لا يتحقق القصد الجنائي إلا إذا كان الجاني يعلم أن المال الذي استولى عليه هو ملك لغيره.

.2الإرادة: الإرادة هي نشاط نفسي يتجه إلى تحقيق غرض معين. فإذا كان غرض الجاني تحقيق نتيجة إجرامية، كانت الإرادة المتجهة إلى الفعل المنطوي على إحداث النتيجة هي "القصد الجنائي". والغرض هو الهدف القريب الذي تتجه إليه الإرادة، أما الباعث فهو عبارة عن الدافع إلى إشباع حاجة معينة، وهذا الدافع له طبيعة نفسية بخلاف الغاية التي لها طبيعة موضوعية. فإذا أراد الجاني أن يحتال على المجني عليه لضائقة مالية مر بها، كانت الغاية التي يسعى إليها هي الحصول على المال، أما الغرض فهو خداع المجني عليه للاستيلاء على أمواله. فهذا الغرض يتصور الجاني تحقيقه بخداع المجني عليه والكذب عليه وإيهامه بصدق مناورات الاحتيال، أما الباعث على ما فعله فهو الاستيلاء على الأموال لسد الضائقة المالية التي يمر بها.[2]

[1] حاتم عبد الرحمان منصور شحات، الاجرام المعلوماتي، دار النهضة العربية، ط1،القاهرة،2002، ص344

[2] أشرف توفيق شمس الدين، "شرح قانون العقويات "النظرية العامة للجريمة والعقوبة"، دار النهضة العربية، القاهرة، 2009م، ص 155

ثانياً: صور القصد الجنائي

إن القصد الجنائي عنصر هام من عناصر الركن المعنوي للجريمة، وينقسم إلى قسمين: قصد عام وقصد خاص. بمعنى أن هناك جرائم لا بد من توفر القصد العام ليتحقق وجود الركن المعنوي وتنعقد المسؤولية الجنائية لها، وهناك جرائم لا بد من توفر القصد الخاص إلى جانب القصد العام، وذلك على النحو الآتي:

1. القصد الجنائي العام: يهدف الجاني عند ارتكابه الواقعة الإجرامية مع العلم بعناصرها إلى تحقيق غرض معين، كي تتم الجريمة ويتوافر لها القصد الجنائي العام. ففي جريمة الاحتيال الإلكتروني، يكون الغرض من وراء هذه الجريمة الاستيلاء على مال مملوك للغير. وعليه، فالقصد الجنائي العام أمر ضروري ومطلوب في جريمة الاحتيال الإلكتروني بشكل خاص، وفي الجرائم التقليدية والمستحدثة بشكل عام. نخلص مما سبق إلى أن هناك ثلاثة شروط يجب توافرها لكي نكون بصدد وجود قصد عام في جريمة الاحتيال:

-علم الجاني بأن الأسلوب المستخدم هو أسلوب احتيالي من شأنه حمل الغير على تسليم ماله

-علم الجاني بأن المال الذي يسعى إلى الحصول عليه مملوك للغير.

-انصراف إرادة الجاني إلى إتيان فعل إيجابي قائم على أحد الأساليب الاحتيالية[1]

2.القصد الجنائي الخاص: لا يختلف القصد الجنائي الخاص عن العام من حيث العناصر التي يجب توافرها، ألا وهي الإرادة والعلم بالواقعة والعقوبة المقررة لها، وإنما يزيد عنه في تحديد الإرادة الإجرامية لدى الجاني إما بباعث معين قد يدفعه إلى ارتكاب الجريمة، أو بنتيجة محددة يريدها الجاني[2].

وبناءً على ما سبق، فإن القصد الجنائي العام متوفر في جريمة الاحتيال الإلكتروني، وقد يكون القصد الجنائي الخاص متوفراً في جريمة الاحتيال الإلكتروني على وجه الخصوص

[1]محمد علي السالم عياد الحلبي، الجرائم الواقعة على الأموال في القانون المقارن، مؤسسة الوراق للنشر والتوزيع، ط1، عمان، 2009، ص167.168

[2]خالد علي سلمان عبد الله، المرجع السابق، ص138

إذا ارتبط سلوك الجاني باستهداف شخص بعينه أو أي طرف آخر وأصر على إلحاق الضرر بهذا الشخص على وجه الخصوص. فالركن المعنوي للجريمة هو الوجه الخفي للسلوك الذي قام به الجاني والمتضمن توفر الإرادة والإصرار على هذا الفعل مع العلم بعدم شرعيته.

الفرع الثالث: تحقق الركن المعنوي في جريمة الاحتيال الإلكتروني

توصف جريمة الاحتيال الإلكتروني بأنها جريمة عمدية، لا قيام لها دون توافر القصد الجنائي. ويقتضي هذا القصد أن يكون المتهم عالماً بأن التلاعب بمعطيات الحاسوب والبيانات المدخلة إلى النظام المعلوماتي من شأنه أن يجعل الحاسوب يستجيب وفقاً لتلك بالمعلومات.[1]

وعليه، يجب أن يدرك الفاعل أن إدخاله للمعلومات يُعد تلاعباً بها، دون اشتراط أن يتم هذا التلاعب بوسيلة محددة، بل يكفي أن تنطوي الوسيلة المستخدمة على تلاعب بالمعلومات. كما يجب أن يعلم الجاني أن المال الذي استولى عليه مملوك للغير، سواء كان مملوكاً للمجني عليه أو لشخص آخر، إذ أن الغالب في جرائم الاحتيال الإلكتروني –ولا سيما في حالات التحويل الإلكتروني غير المشروع للأموال –هو عدم علم الجاني بشخصية المجني عليه.

وتجدر الإشارة هنا إلى وجود خلاف فقهي بشأن وجوب توفر القصد الخاص في هذه الجريمة. فقد ذهب بعض الفقهاء إلى أن الاحتيال الإلكتروني جريمة يكفي لقيامها القصد العام دون الحاجة إلى القصد الخاص، مستندين إلى أن الاستيلاء على المال إنما هو نتيجة للاحتيال، وأن إرادة هذه النتيجة ليست سوى نية تملك الشيء، وهذه النية لا تشكل غاية خاصة تخرج عن العناصر المكونة للجريمة.[2]

وخلاصة القول، فإن جريمة الاحتيال الإلكتروني، باعتبارها جريمة عمدية، تستلزم توفر الركن المعنوي المتمثل في القصد الجنائي، حيث لا يكفي القصد الجنائي العام بعنصريه العلم والإرادة، بل لا بد من توفر القصد الجنائي الخاص، وهو اتجاه نية الجاني إلى تملك المال الذي تسلمه من المجني عليه. ولا عبرة بالبواعث الدافعة إلى ارتكاب الجريمة، إذ أن الباعث لا يُعد عنصراً من عناصر القصد الجنائي. فإذا قام الجاني بالتلاعب في المعلومات التي يحتويها

[1] محمد علي السالم عياد الحلبي، المرجع نفسه، ص170

[2] حسن كليبي، نجمة الطيب، المرجع السابق، ص79

النظام المعلوماتي بقصد إجراء تحويل إلكتروني للأموال لاستيفاء دين، أو لإظهار قدرته ومهارته في مجال تكنولوجيا المعلومات، فإن توفر هذا الباعث لا ينفي قصد الاحتيال.

خلاصة الفصل الأول

في الفصل الأول، عالجنا الإطار المفاهيمي لجرائم الاحتيال الإلكتروني بوصفها جرائم مستحدثة ناتجة عن التقدم التكنولوجي، تقوم على الخداع الإلكتروني والاستيلاء على أموال الغير دون مواجهة مباشرة، عبر استخدام وسائل رقمية حديثة، كما تبرز خصائصها الفريدة من حيث تنوع الصور والأساليب، والطابع غير المادي، وسرعة التنفيذ، وصعوبة التتبع، فضلاً عن كون الأدلة فيها رقمية ومعقدة تقنياً، مما يميزها عن الجرائم التقليدية.

وقد جرى تحليل الأركان الأساسية لهذه الجريمة، المتمثلة في الركن الشرعي (التجريم)، والركن المادي (استخدام وسائل احتيالية عبر الشبكة المعلوماتية)، والركن المعنوي (نية التملك غير المشروع).

الفصل الثاني

إجراءات التحقيق في جريمة الاحتيال الالكتروني ووسائل الوقاية منها

الفصل الثاني

إجراءات التحقيق في جريمة الاحتيال الالكتروني ووسائل الوقاية منها

مع تزايد انتشار الجرائم الإلكترونية، وازدياد اعتماد الأفراد والمؤسسات على الوسائط الرقمية في معاملاتهم اليومية، باتت جرائم النصب والاحتيال الإلكتروني تمثّل واحدة من أخطر التهديدات التي تستهدف أمن المعلومات، وتُضعف ثقة المتعاملين في البيئة الرقمية. وتكمن خطورة هذه الجرائم في طبيعتها المتطورة، القائمة على وسائل تقنية معقدة وأساليب احتيالية يصعب أحيانًا اكتشافها أو توقعها، الأمر الذي يستلزم وجود استجابة قانونية فعّالة وآليات ردع ملائمة لحماية الأفراد والمجتمع.

وفي هذا السياق، تبرز الحاجة إلى إقرار منظومة عقابية متكاملة تجمع بين عقوبات أصلية تتناسب مع جسامة هذه الأفعال، وعقوبات تكميلية تُعزز الردع العام والخاص، وتسهم في تحقيق العدالة. غير أن الاعتماد على العقوبات وحدها لا يكفي لمواجهة الظاهرة، مما يقتضي تبني وسائل وقائية تقوم على توظيف التكنولوجيا الحديثة، ونشر التوعية الإعلامية والاجتماعية، بهدف بناء وعي رقمي قادر على الحد من فرص وقوع هذه الجرائم، وتمكين الأفراد من التصدي لها بفعالية.

يتفرع هذا الفصل إلى مبحثين رئيسيين: يُعرض في الأول منهما إجراءات التحقيق في جريمة الاحتيال الالكتروني والعقوبات المقررة لها، بينما يُخصص الثاني لدراسة الوسائل الوقائية المعتمدة للحد من انتشار هذه الجرائم.

المبحث الأول: إجراءات التحقيق في جريمة الاحتيال الالكتروني والعقوبات المقررة لها

أصبحت الجرائم الإلكترونية، وعلى رأسها جرائم النصب والاحتيال، من أبرز التحديات التي تواجه النظم القانونية في العصر الرقمي، لما تسببه من أضرار مادية ومعنوية جسيمة. وقد استدعى ذلك من المشرّع التدخل لتقنين عقوبات رادعة تتناسب مع خطورة هذه الأفعال. ويهدف هذا المبحث إلى تسليط الضوء على الإجراءات التحقيق في الجريمة الالكترونية (المطلب الأول) والعقوبات التي يقرّرها القانون لمواجهة هذه الجرائم، سواء كانت عقوبات أصلية تشكل الأساس في الردع، أو عقوبات تكميلية تُفرض لتحقيق غايات وقائية أو إصلاحية إضافية (المطلب الثاني)

المطلب الأول: إجراءات التحقيق في جريمة الاحتيال الالكتروني

الهدف الأول لهذه الإجراءات هو جمع وفحص الأدلة الالكترونية التي تفيد وقوع الجريمة ونسبتها إلى فاعلها، كما أن هذه الإجراءات يمكن مباشرة أي منها طالما أنها تفيد في كشف الحقيقة وتفيد المحقق في مباشرته وفق الحدود المشروعة. فالقاعدة أن إجراءات الدعوى الجنائية لا تبدأ إلا بما تتخذه النيابة العامة من أعمال التحقيق، وكذلك الخصومة الجنائية لا تنعقد إلا بذلك، فسنتطرق في هذا المطلب الى إجراءات التي تتمثل في المعاينة والتفتيش (الفرع الأول) ثم الى إجراءات الضبط والتنصت والمراقبة (الفرع الثاني).

الفرع الأول: إجراءات المعاينة والتفتيش

أولا: المعاينة

اجراءات عملية المعاينة تأتي كإجراء تالي لتلقي بلاغ عن وقوع إحدى الجرائم المعلوماتية، وبعد تُعتبر إجراءات المعاينة في مجال الجرائم المعلوماتية مرحلة لاحقة لتلقي البلاغ بوقوع إحدى هذه الجرائم. فبعد التحقق من البيانات الأساسية الواردة في البلاغ، واستكمال الإجراءات القانونية اللازمة من قبل الجهات المختصة، يُشرَع في الانتقال إلى مسرح

الجريمة من أجل معاينته[1]. غير أن مسرح الجريمة المعلوماتية يختلف بطبيعته عن مسرح الجريمة التقليدية، كالقتل أو السرقة؛ فقد تتخذ الجريمة المعلوماتية صفة الجريمة المستمرة، كما هو الحال في بعض الجرائم الاقتصادية كالسرقة والاحتيال، وقد يكون مسرحها مماثلاً لمسرح الجرائم الأخرى كما في جرائم التزوير وإتلاف البرامج وتفجير المباني.

هذا وتقتضي عملية المعاينة في البيئة الإلكترونية الالتزام بجملة من الضوابط، في مقدمتها: توثيق حالة الحاسب الآلي والأجهزة الطرفية المرتبطة به عبر التصوير الفوتوغرافي، مع تدوين وقت وتاريخ ومكان التقاط كل صورة بدقة.

إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.

إعداد خطة المعاينة، موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الكامل.

ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين يتم عرض الأمر فيما بعد على المحكمة.

عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير لسليمة، وفحصها، وترفع من عليها البصمات ذات الصلة بالجريمة.

التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة.

قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات.[2]

يجب أن تُجرى إجراءات المعاينة وفق مبدأ المشروعية وفي الحدود التي ترسمها القوانين الجنائية. ورغم أن المعاينة تعد إجراءً وارداً في جميع أنواع الجرائم، فإن أهميتها تتفاوت من

[1] بن نعوم خالد، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، ب، كلية الحقوق، القسم الخاص، جامعة عبد الحميد بن باديس، مستغانم،2018-2019، ص74

[2] محمد علي السالم عياد الحلبي، المرجع السابق، ص174

جريمة إلى أخرى؛ إذ تتضاءل فائدتها في بعضها كجريمة التزوير المعنوي وجريمة السب، حيث تكون المعاينة فيهما غير مجدية. في المقابل، تبرز أهمية معاينة الجرائم التقليدية والاطلاع على مسرحها في تمكين الجهات المعنية من تصوّر كيفية وقوع الجريمة، واستجلاء ظروفها وملابساتها، فضلاً عن توفير الأدلة المادية التي يمكن جمعها عبر هذه المعاينة.

إلا أن المعاينة لا تؤدي الدور نفسه في الكشف عن غموض الجريمة المعلوماتية، ولا في ضبط العناصر التي قد تُسهم في إثبات وقوعها أو إسنادها إلى مرتكبها.[1]

ثانيا: التفتيش

والتفتيش هو اجراء من اجراءات التحقيق الابتدائي وهو في الاصل من اختصاص سلطة التحقيق والممثلة في قاضي التحقيق والنيابة العامة باختلاف التشريعات، إلا انه واستثناء يخول لرجال الضبط القضائي في الحالات التي يحددها القانون[2].

التفتيش هو البحث في مستودع سر المتهم، ويُعد إجراءً من إجراءات التحقيق يتطلب أوامر قضائية لمباشرته. وينبغي على المحقق الجنائي المبادرة إلى إجراء التفتيش قبل أن يتمكن الجاني من طمس معالم الجريمة وإخفاء كل ما يتصل بها، وهو قادر على فعل ذلك إذا اتسع له الوقت وسنحت له الفرصة.

والتفتيش، في مدلوله القانوني بالنسبة للجرائم الإلكترونية، لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية. إذ يُقصد به أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة بهدف الدخول إلى نظم المعالجة الآلية للبيانات، بما تشمله من مدخلات وتخزين ومخرجات، وذلك للبحث فيها عن أفعال غير مشروعة تُشكل جناية أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها.[3]

و كذلك التفتيش هو البحث عن أدلة مادية بصدد الواقعة الجرمية الجاري التحقيق بشأنها من اجل كشف الحقيقة والاستدلال على نية وغاية الجاني من ارتكاب الجريمة ، ففي

[1] أمير فرج يوسف، الاثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، مكتبة الوفاء القانونية، ط1، الإسكندرية،2016م، ص ص300 ،301

[2] عبد الرحمن عنانزه، المرجع السابق، ص193

[3] قراوي كلتوم جريمة الاحتيال الإلكتروني، أطروحة لنيل شهادة دكتوراه علوم في القانون العام، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق، جامعة الجزائر 2025/2024ص188

الجرائم الالكترونية فأنه يختلف عن الجرائم الاخرى ، فيما يتعلق بمحل الجريمة والوسائل والأساليب المستخدمة فيها ، وكون هذه الجرائم مستحدثة لا تترك اثار مادية ويمكن محو وإخفاء الأدلة بسهولة مما يوجب على سلطة التحقيق المختصة الالمام بمفردات ومكونات وطبيعة النظام الالكتروني ، وكيفية تفتيش وضبط الأدلة والتحفظ عليها سواء ما تعلق منها بالشق المادي او المعنوي والمتمثل بالبيانات والمعلومات والبرامج، كما تجدر الاشارة الى ان اجراءات التفتيش يجب ان تكون وفقا لأحكام القانون وان لا تنتهك حريات الافراد وحقوقهم او ان تنتهك حرمة مساكنهم.[1]

يُقصد بالتفتيش في سياق جرائم الإنترنت كونه إجراءً قانونياً يُتيح جمع الأدلة ذات الطابع الإلكتروني، سواء تلك المخزنة أو المسجلة رقمياً. كما أن عملية البحث في الشبكات الإلكترونية تخول السلطات المختصة توظيف الوسائل الرقمية للكشف عن البيانات أو الأدلة المطلوبة أينما وجدت. غير أن ثمّة من يصف مهمة الولوج إلى البيئة المعلوماتية بالعديمة الجدوى، وذلك نظراً لما تعترضها من صعوبات أثناء التنفيذ، خصوصاً في الفضاءات الافتراضية، على النقيض من الجرائم التقليدية التي لا تثير مثل هذه الإشكاليات.

إن تفتيش نظم الحواسيب تفتيش للفضاء الإلكتروني وأوعية التخزين وتفتيش للبيانات التي يحفظها جهاز الكمبيوتر إن كان مزوداً بحافظات إلكترونية للعمليات المنجزة من خلاله وهو أمر يتعلق بالقدرة على تحديد المطلوب مسبقاً وليس مجرد سبرغور نظام معلومات إلكتروني لأن التعامل وفق المسلك الأخير قد يكون له عواقب قانونية أهمها بطلان الإجراءات لأنها خارج نطاق أمر التفتيش أو قد تنطوي الإجراءات على كشف خصوصية البيانات المخزنة في النظام.[2]

يمكن لقاضي التحقيق المختص القيام بكل إجراءات التحقيق الضرورية للكشف عن الحقيقة، ويدخل في ذلك كل ما يتعلق بجمع الأدلة كما منحت له المادة 69 من ق. إ. ج. ج اتخاذ إجراءات البحث والتحري والاستعانة بالقوة العمومية عند الاقتضاء، والتفتيش بشكل عام هو أحد اجراءات التحقيق التي تقوم به سلطة مختصة قانونا بهدف البحث عن الادلة المادية للجريمة في محل خاص يتمتع بالحرمة أو لدى شخص على علم بذلك وفق أحكام القانون.

[1] محمد عبد الرحمن عنانزه، المرجع السابق،192
[2] امير فرج يوسف، المرجع السابق، ص303

وقد حدد المشرع الجزائري بموجب المادة 78 من قانون الإجراءات الجزائية أوقات التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا وقد نص على ذلك في قانون الإجراءات الجزائية "لا يجوز البدء في التفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا و لا بعد الساعة الثامنة مساء".[1]

إلا أنه و في حالات استثنائية يجوز الخروج عن تلك القاعدة فعند ما يتعلق الأمر بجرائم المخدرات والمؤثرات العقلية أو الجريمة المنظمة عبر الحدود الوطنية أو الجَرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم الأموال و الإرهاب و كذلك الجَرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص، ويتبين من هذا أن المشرع الجزائري أجاز إجراء التفتيش في أي وقت من أوقات النهار والليل في جرائم معينة حددها المشرع ومن بينها الجَرائم المتعلقة بالمعالجة الآلية للمعطيات.[2]

باعتبار التفتيش من أكثر إجراءات التحقيق، حرص المشرع الجزائري على وضع شروط له وهي تتمثل في شروط موضوعية وشكلية:

أ-الشروط الموضوعية

1سبب التفتيش يهدف للوصول إلى الدليل باعتباره وسيلة من وسائل التحقيق الجنائي وذلك من أجل الوصول للحقيقة، ويتحقق سبب التفتيش عند وقوع جريمة ويتم اتهام أشخاص بأمارات وقرائن قوية تفيد في إثبات الجريمة أو كشفها ولتحقيق السبب لا بد من وقوع جريمة الكترونية بالفعل.

2محل التفتيش: وهو نوعين

أ. تفتيش الأجهزة والوسائل الإلكترونية داخل مسكن له حرمة: يكون محلا لتفتيش الأجهزة والوسائل الإلكترونية التي تكون موضوعة في مسكن له حرمة وتتكون من حواسيب وأجهزة.
ب . تفتيش الشخص بعينه ويقصد بالشخص محل التفتيش كل ما يتعلق بكيانه المادي فقد يكون الحاسوب أخذ هذه الكيانات وما يحتويه من بيانات، ويتم تفتيشه كما يفتش أي شخص.

[1]القانون رقم 25-14مؤرخ في 9 صفر عام 1447المافق ل 8 غشت سنة 2025
[2]الطاهر ياكر، المرجع السابق، ص118،117

3غاية التفتيش

تتمثل الغاية الجوهرية من التفتيش في البحث عن الدليل الذي يُسهم في كشف الحقيقة، وكذلك كل ما يُعين المحققين من عناصر تتصل بمحل الجريمة. والهدف من ذلك، في سياق الجرائم الإلكترونية، هو الحصول على الدليل الرقمي الذي يُساعد في كشف ملابسات الجريمة المعلوماتية الخاضعة للتحقيق من قبل الجهات المختصة.[1]

الفرع الثاني: إجراءات الضبط والتنصت والمراقبة الالكترونية

أولا: إجراءات الضبط

يُعرّف الضبط بأنه وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبها. فالضبط هو الوسيلة القانونية التي تضع بواسطتها السلطة المختصة يدها على جميع الأشياء التي وقعت على الجريمة، أو نتجت عنها، أو استُعملت لاقترافها. وعليه، يكون الضبط أثراً مباشراً للتفتيش، باعتبار أن التفتيش هو ضبط الأدلة أو الأشياء التي تفيد في إظهار الحقيقة في الجريمة، فالضبط هو نتيجة للتفتيش. وقد يقع الضبط استناداً لأسباب أخرى كالمعاينة. ويترتب على ذلك أن بطلان التفتيش يؤدي إلى بطلان الضبط.[2]

يُعرف الضبط أيضاً بأنه ضبط الأدلة المادية للكشف عن الجريمة، ويكون ذلك بوضع اليد على الدعائم المادية التي تُخزّن فيها البيانات الإلكترونية والمعلومات المتصلة بالجريمة. كما يُستخدم في ضبط الجريمة المعلوماتية برامج خاصة بهدف الولوج إلى البيانات المراد ضبطها، إلى جانب وضع اليد على الدعائم المادية.[3]

عليه، فإن الضبط في جريمة الاحتيال المعلوماتي يعني الاستيلاء على الدعائم المادية الحاوية للبيانات الإلكترونية والمعلومات المرتبطة بالجريمة، والتي من شأنها الإسهام في الكشف عن الحقيقة وتحديد هوية مرتكبيها، مع الاستعانة في ذلك بوسائل غير تقليدية، تتمثل في برامج متخصصة تُيسّر الولوج إلى البيانات المراد ضبطها والإمساك بها.[4]

---

[1] صلجة خلود، شبل مروى، جريمة الاحتيال الإلكتروني بتشريع جزائري، مذكرة مكملة لنيل شهادة الماستر تخصص قانون جنائي وعلوم جنائية، جامعة سكيكدة 2024-2025، ص51

[2] عبد الله سيف الكيتوب، المرجع السابق، ص141

[3] محمود إبراهيم غازى، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، ط 1 ،2014، ص712

[4] خالد علي سلمان عبد الله، المرجع السابق، ص 245،246

1. ضبط المكونات المادية في جريمة الاحتيال الالكتروني

يدور هنا الحديث على الأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتي والتي لها قيمة في اثبات جريمة الاحتيال المعلوماتي ونسبتها للمتهم وهي:

1-المخرجات والمستندات الورقية: كثير من جرائم الاحتيال المعلوماتي ما تترك ورائها قدر كبير من الأوراق والمستندات الرسمية منها والخاصة، ولكن وجود الحاسب الآلي يتيح إمكانية حفظ هذه المعلومات على الحاسب نفسه .

2-جهاز الحاسب الآلي: يجب أن يتم تحديد الحاسب التي تمت من خلاله الجريمة أو التي وقعت عليها الجريمة، والخبير في مجال الحواسيب الإلكترونية يستطيع التعرف على الحاسب ومكوناته وكيفية التعامل معه، وتتمثل مكونات الحاسب في وحدة المعالجة المركزية ولوحة المفاتيح والشاشة، ومع ظهور وسائل تقنية جديدة صغيرة الحجم كالهاتف النقال و اللابتوب فإن هذه الأجهزة يجب ضبطها وتحريزها ككتلة واحدة.

3-الأقراص المغناطيسية: وهي الأقراص التي تحتوي على بيانات ومعلومات هائلة الحجم وقد تكون في مكان لا يوجد فيه الحاسب الآلي الخاص بالجريمة إلا أن المعلومات المخزنة عليها قد تفيد في مراحل التحقيق في الجريمة وقد توجد بأعداد كبير في الشركات والبنوك وتكون مغلفة بأغلفة توضح محتويات كل منها.

4-الأشرطة الممغنطة: وهي عبارة عن شرائط ممغنطة تستخدم عادة للحفظ والتخزين وقد تكون في مكان آمن بعيد عن الحاسب الآلي.

5-المودم: وهي أجهزة يمكن من خلالها اتصال أجهزة الحاسب الآلي ببعضها البعض.

6-الطابعات: وتنقسم إلى نوعين منها العادية وأخرى التي تعمل بتقنية الليزر، والأجهزة الحديثة التي يمكن تخزين المستندات والمعلومات التي تمت طباعتها.

ب . ضبط المكونات المعنوية في جريمة الاحتيال الالكتروني

وإجراء الضبط في مجال الفضاء الإلكتروني متعلق بضبط الأدلة المتحصل عليها من التفتيش، وهي البيانات المعلوماتية وتعد مراقبة المكالمات السلكية واللاسلكية تحت رقابة القضاء وذلك لضبط ما يفيد في كشف الحقيقة أحيانا. [1]

[1]محمود إبراهيم غازى، المرجع السابق،210

ثانيا: التنصت والمراقبة في جريمة الاحتيال الالكتروني

يُعد التنصت والأشكال الأخرى للمراقبة الإلكترونية من الإجراءات المثيرة للجدل، إلا أنها تظل مسموحاً بها في ظل ظروف معينة وفي جميع الدول تقريباً. فقد كفل الدستور حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والإلكترونية، كما حظر مراقبتها أو التنصت عليها أو الكشف عنها، إلا لضرورة قانونية وأمنية وبقرار قضائي. وعليه، يكون الدستور قد أجاز التنصت والمراقبة الإلكترونية، ولكن في حدود معينة تتمثل في ضرورة قانونية وصدور قرار قضائي بذلك.[1]

يرتكز التنصت على اتخاذ موقع محدد داخل شبكة الاتصالات منصةً للعمل، بهدف تسجيل البيانات المتبادلة بين الأنظمة المعلوماتية وحفظها. والمقصود بالشبكات في هذا السياق: ربط جهازين أو أكثر من أجهزة النظام المعلوماتي بعضها ببعض عبر وسائل الاتصال السلكية أو اللاسلكية، أو هي مجموعة من الحواسيب المترابطة في منظومة واحدة.

أما المراقبة الإلكترونية فتُعرَّف بأنها الرصد المنهجي لشبكات الاتصال، وتتمثل في النشاط الذي يمارسه المراقب بتوظيف التقنيات الإلكترونية الحديثة، بغية جمع البيانات والمعلومات المتعلقة بالمشتبه فيه، سواء أكان هذا المشتبه فيه شخصًا طبيعيًا أم مكانًا بعينه. [2].

المراقبة الالكترونية تعد وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، يقوم بها مراقب إلكتروني يتمثل في مأمور ضبط قضائي ذو كفاءة تقنية عالية تتماشى مع نوع جريمة الاحتيال المعلوماتي، مستخدما في ذلك التقنية الالكترونية وعبر شبكة الإنترنت، وذلك من خلال مراقبة أحد الهكرة ممن قام باختراق الحاسب الآلي الخاص بالمجني عليه، أو يقوم بإعداد صندوق بريد إلكتروني مستنسخ لمراقبة المشتبه فيه.[3]

[1] أمير فرج يوسف، المرجع السابق، ص319
[2] قراوي كلتوم، المرجع السابق، ص 190
[3] محمود إبراهيم غازي، المرجع السابق، ص716

والتنصت والمراقبة الالكترونية لشبكات الحاسب الآلي، هو أحد إجراءات التحقيق في جريمة الاحتيال المعلوماتي، وبرغم ما يثيره هذا الإجراء من جدل، فإنه مسموح به تحت ظروف معينة في جميع الدول تقريبا[1].

حسب رأينا أنه وما دام التنصت والمراقبة الالكترونية هي إحدى إجراءات التحقيق في الجريمة المعلوماتية ومنها جريمة الاحتيال المعلوماتي، فإنه لا مانع من القيام بها طالما أن ذلك يفيد في كشف حقيقة تلك الجريمة، وطالما أن ذلك يتم من خلال السلطات المختصة وفي ضوء ما تفوضه التشريعات من صلاحيات.

المطلب الثاني: العقوبات المقررة لجريمة الاحتيال الالكتروني

العقوبة هي عبارة عن جزاء جنائي يقرره القانون ويوقعه القضاء على المجرم ومن سمات العقوبة أنها توصف بأنها مؤلمة ومحقرة ، فهي توصف بأنها مؤلمة إذ يعاني منها المجرم عند توقيعها عليه، لأن كل عقوبة تصيب الجاني في حياته أو حريته أو ذمته المالية مثل الإعدام، السجن، الحبس، الغرامة...الخ، وأيضا توصف بأنها محقرة فهي تنزل من القيمة الاجتماعية للشخص أي أنها تنزل من القيمة للجاني ويوصم بالعار.

العقوبات في الشريعة الإسلامية نوعان: عقوبات مقدرة شرعًا، وعقوبات غير مقدرة شرعًا أما في القانون الوضعي العقوبات محددة من حيث النوع والمقدار من قبل السلطة المختصة بالتشريع ومنصوص عليها في نص قانوني مكتوب.

فسنتطرق في هذا المطلب الى العقوبات الأصلية لجريمة الاحتيال الالكتروني (الفرع الأول)ثم الى العقوبات التكميلية (الفرع الثاني)

الفرع الأول: العقوبات الأصلية

تنص المادة 372 من قانون العقوبات الجزائري على أن العقوبة الأصلية لهذه الجريمة يعاقب بالحبس من سنة على الأقل الى خمس سنوات على الأكثر وبغرامة من 20000 إلى 100000 دج، الجاني الذي ارتكب جريمة النصب بالعقوبات كالاتي: الحبس من سنة إلى خمس سنوات على الأقل والغرامة المالية المقدرة ب 20000 إلى 100000 د ج، وفي نص

[1]عبد الله سيف الكيتوب، المرجع نفسه، ص149

المادة 53 مكررة 4 من ق. ع. ج (رقم 06-23 المؤرخ في 20 ديسمبر (2006) إذ كانت العقوبة المقررة قانونا في مادة الجنح والحبس أو الغرامة.[1]

وتقرر إفادة الشخص الطبيعي غير المسبوق قضائيا بالظروف المخففة، يجوز تخفيض عقوبة الحبس إلى شهرين والغرامة إلى 20.000 د.ج ,كما يمكن الحكم بإحدى هاتين العقوبتين فقط، على أن تقل عن حد الأدنى المقرر قانونا للجريمة المرتكبة، وإذا كانت العقوبة الحبس هي وحدها المقررة يجوز استبدالها بغرامة، على ألا تقل عن 20.000 دج وألا تتجاوز.500.000 دج .[2]

إذا كان المتهم مسبوقا قضائيا، بمفهوم المادة 53 مكررة 5 أدناه ، فإنه لا يجوز تخفيض العقوبة الحبس والغرامة عن الحد الأدنى المقرر قانونا في جنحة المرتكبة عمدا، ويتعين الحكم بهما في حالة النص عليهما معا، ولا يجوز في أي استبدال الحبس بالغرامة

كما يجوز لقاضي الموضوع أن يحكم على الجاني علاوة على ذلك بالحرمان من الحقوق الواردة في المادة 14 من قانون العقوبات أو بعضها وبالمنع من إقامة تتراوح بين سنة (1) على الأقل وخمس سنوات (5) على الأكثر ، وهو موقف يساير الاتجاه العام في قانون العقوبات الذي يساوي بين عقوبة الجريمة التامة والشروع فيها ومع ذلك إذا استخدم الجاني جرائم أخرى لارتكاب الاحتيال، فقد يتعرض لعقوبات إضافية وفقا لما يقرره القانون فالعقوبات الأصلية المطبقة على الشخص الطبيعي في هذا النوع من الجرائم يختلف حسب الخطورة الإجرامية التي قدرها المشرع في مثل هذه التصرفات، إذ تجد سلم الخطورة يتضمن ثلاث درجات: الجريمة البسيطة تكون العقوبة المقررة من 3 أشهر إلى سنة حبس و 50000 دج إلى 100000 دج غرامة حسب المادة 394 مكررة.

الجريمة المشددة تضاعف العقوبة إذا تترتب عن أفعال تغيير المعطيات أو حذف معلومات مهمة بالدولة وتكون العقوبة الحبس من ستة أشهر إلى سنتين، وغرامة 50000 دج إلى150000 دج إذا ترتب عن تخريب النظام حسب المادة 394 مكرر 23، ولقد حدد المشرع الجزائري الجريمة النصب غرامة مالية محددة بين الحد الأدنى والحد الأقصى فلا يمكن تجاوزها، وتتمثل في إلزامه بدفع لا أقل ولا أكثر عن حد معين .[3]

[1] بولحية شهيرة، سويح دنيا زاد، المرجع السابق ص39

[2] الحسن بن شيخ، مذكرات في القانون الجزائي الخاص، الجرائم ضد الأشخاص والجرائم ضد الأموال، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012 ص202.

[3] قراوي كلثوم، مرجع سابق، ص117

كما أن العقوبة لا يقتصر تطبيقها على الجريمة التكميلية فقط بل تطبق أيضا على الشروع فيها أي محاولة نصب الثروة الغير، ولقد عبر عنها المشرع في نص المادة 372 .

فلا تكتمل جريمة النصب والاحتيال لانعدام أحد أركانها فتكون حينئذ أما حالة شروع في جريمة النصب والاحتيال، ويتحقق ذلك في حالة بدأ الجاني في تنفيذ جريمته لكن لا يتمكن من إتمامها لأسباب خارجة عن نطاقه أي لا دخل لإرادته فيها، ولقد أخض المشرع الجزائري معيار البدء في التنفيذ فيشمل إلى جانب الأفعال التي تكون الركن المادي لها والتي تؤدي إلى وقوعه مباشرة. ولا يتحقق الشروع إلا إذا كان القصد الجنائي للجاني معلومة وثابتا أي يجب أن يظهر الجاني نيته في الاستيلاء على مال المجني عليه بعد استعماله لوسيلة من الوسائل التدلسية سواء أن المجني عليه معنيا أو غير معين. [1]

الفرع الثاني :العقوبات التكميلية

نص المشرع الجزائري في نص المادة 372 ضمن فقرتها الثالثة على عقوبة أخرى وهي العقوبة التكميلية كما جاء فيها، وفي جميع الحالات يجوز أن يحكم القاضي على الجاني بالحرمان من جميع الحقوق الواردة في المادة 14 ق ع، ويجوز عند الاقتضاء في الجنحة وفي الحالات التي حددها القانون، أن تحظر على المحكوم عليه ممارسة حق أو أكثر من الحقوق المذكورة في المادة 8 لمدة لا تتجاوز 5 سنوات، وتنحصر هذه الحقوق في:

-عزل المحكوم عليه وطرده من جميع الوظائف والمناصب السامية في الحزب أو الدولة وكذا جميع الخدمات التي لها علاقة في الجريمة.

-الحرمان من حق الانتخاب والترشح وعلى العموم كل الحقوق الوطني السياسية ومن حمل أي وسام .

-عدم الأهلية لأن يكون مساعدا مخلفا أو خبيرا أو شاهدا على أي عقد أو أمام القضاء إلا على سبيل الاستدلال.

-عدم الأهلية لأن يكون وصيا أو ناظرا ما لم تكن الوصاية على أولاده.

-الحرمان من الحق التدريس وفي إدارة مدرسة أو الاستخدام في مؤسسة للتعليم وصفه أستاذا أو مدرسا أو مراقبا.

[1] ابوبكر التيتاوي، المرجع سابق، ص29

نشر الحكم ويستفاد من هذه الفقرة أن العقوبة هي عقوبة ذات طابع شكلي أي يجوز للقاضي أن يستغني عنها كلية وتتمثل هذه العقوبة بالحكم بالحرمان من جميع الحقوق أو بعض الحقوق الوطنية.

وتجدر الإشارة إلى أن تطبيق هاتين العقوبتين هو أمر جوازي، وتطبيقهما يكون بصدد تطبيق العقوبة الأصلية أو في حالة الظروف المشددة.[1]

حيث نص قانون العقوبات الجزائري على ظرفين مشددين لجنحة النصب والاحتيال وهي حسب المادة 382 الفقرة الثانية مكررة والتي جاء فيها "أنه تطبق عقوبات التفليس بالتدليس على الأشخاص الذين ثبتوا أنهم قدموا في . أو التسوية القضائية بطريقة التدليس ديونا وهمية سواء باسمهم أو بواسطة آخرون.[2]

1 إسماعيل الصادق، محمد بن سعيدان، جريمة النصب والاحتيال الإلكتروني، مذكرة مقدمة لنيل شهادة الماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية جامعة عمار ثليجي، الأغواط2025/2024 ص 29

[2]صلجة خلود، المرجع السابق، ص36

المبحث الثاني: وسائل الوقاية من جريمة الاحتيال الالكتروني

إنّ ارتكاب الجريمة الإلكترونية يعتمد على التقنيات الحديثة لارتكابها وحيث أنّ هذه التقنيات تعُتبر المحل والوسيلة للجريمة الإلكترونية المتبعة، وعليه فإنّ الوقاية من الجريمة الإلكترونية، وكون أن الوقاية خير من العلاج فإنه لا بدّ من أن تكون الأساليب المتَّبعة للوقاية من الجريمة الإلكترونية معتمدة على أساليب تقنية، وعليه سوف يتم الحديث في هذا المبحث عن الطرق التقنية المُتّبعة للوقاية من جريمة الاحتيال الإلكترونية (المطلب الأول)، بالإضافة إلى الطرق التوعية الوقائية من جريمة احتيال الالكتروني (المطلب الثاني) .

المطلب الأول: الطرق التقنية المتبعة للوقاية من الجريمة الالكترونية

يشهد العصر الرقمي تطورا متسارعا في أساليب حماية المستهلك، مما استدعى وسائل تقنية (الفرع الأول)، ووسائل إدارية (الفرع الثاني)، متكاملة لضمان أمن المعاملات الإلكترونية، بحيث يتناول هذا المطلب أبرز تلك الوسائل ودورها في تعزيز الثقة في البيئة الرقمية.

الفرع الأول: الوسائل التقنية لحماية المستهلك في البيئة الرقمية

أولا: تقنية تشفير المعلومات

يُعتبر تشفير المعلومات من أبرز الوسائل والأدوات المبتكرة في مجال الوقاية من الجريمة الإلكترونية، حيث يُسهم في توفير الأمن وسلامة المعلومات وسريتها، وكذلك في حماية الصفقات التي تتم عبر شبكة الإنترنت. ولا يقتصر دور تشفير المعلومات على الوقاية من الجريمة الإلكترونية وتأمين سرية الرسائل الرقمية المتبادلة، بل يمتد ليشمل وظائف أخرى تتعلق بدعم وتسهيل إجراءات الإثبات مفهوم التشفير وطرق التشفير وأهمية التشفير في الوقاية من الجريمة الإلكترونية.[1]

[1] طوني عيسى، التنظيم القانوني لشبكة الانترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، ط1، 2001، ص11

-مفهوم التشفير:

"التشفير هو تحويل بيانات إلكترونية إلى شكل يستحيل به قراءتها وفهمها دون إعادتها إلى هيئتها الأصلية".[1]

بناءً على ذلك، فإن التشفير عبر الإنترنت يعني إخفاء المعلومة داخل بياناتها الأساسية، بحيث لا تعبر هذه البيانات -حال ظهورها -عن معناها الحقيقي. فالتشفير هو برمجة تفرض شيفرة تحمي ظاهر المعلومات، وتمنع غير المخول لهم بالتعامل مع الموقع من الدخول إليه إلا بإذن صريح من المالك.

ويُعرف التشفير بموجب القانون العربي النموذجي بأنّه "تحويل البيانات المعالجة إلكترونيا الي رموز لعدم تمكين الغير من انتهاك سريتها،

كما يُعرَّف بأنه عملية تحويل المعلومات المقروءة إلى إشارات غير مفهومة، أو الطريقة التي تسمح بترقيم الرسائل بحيث لا يمكن فهمها من قبل الغير، وهي تقنية تساهم بفاعلية في ضمان سرية المراسلات بين المرسل والمتلقي[2].

وبناءً على ما تقدم، يمكن تعريف التشفير بأنه تحويل جميع البيانات المرسلة إلكترونياً إلى شكل يستحيل معه قراءتها وفهمها دون استخدام مفتاح فك التشفير الخاص بهذه البيانات.

- طرق التشفير في الميدان المعلوماتية يمكن تصنيف التشفير المعلوماتي إلى الأنواع الآتية :

-تقنية التشفير المتماثل:(Symétrique Encryptions)

تعتمد هذه التقنية على استخدام المفتاح الخصوصي نفسه لكل من عملية التشفير وفك التشفير. ومعنى ذلك أن نظام الكتابة المشفرة بالمفتاح الخصوصي يعمل بواسطة مفتاح واحد

[1]عبان عميروش، التنظيم القانوني للتشفير كآلية للتصديق الالكتروني في التشريع الجزائري والتشريعات المقارنة، المجلد07، العدد01، جوان2022، ص1238 1239

[2]اندي اوبل، كشف اسرار قواعد البيانات، ط1الدار العربية للعلوم، لبنان،2014، ص263

يمتلكه كل من مرسل الرسالة ومتلقيها، على ألا يُرسل هذا المفتاح مع الرسالة، بل يُرسل بطرق أخرى حرصاً على حماية سريته ومنع اطلاع غير عليه[1].

-تقنية التشفير غير المتماثل:(Asymétrique Encryptions)

تستخدم هذه التقنية مفتاحين لكل مستخدم، بحيث يتم تشفير المعلومات باستخدام المفتاح العام، ولا يمكن فك التشفير والوصول إلى تلك المعلومات إلا بواسطة المفتاح الخاص لصاحب المفتاح العام الذي تمت عملية التشفير على أساسه. ورغم الارتباط بين المفتاح العام والخاص، فإن أياً منهما لا يدل على الآخر[2].

وقد برزت إشكالية المصادقة على المفتاح العمومي، أي ضمان أن هذا المفتاح صادر فعلاً عن المستخدم ولم يُستخدم بطريقة غير مشروعة من قبل الغير، وعُولجت هذه المسألة بتدخل طرف ثالث محايد (يُعرف بنظام مصادقة الشخص الثالث)[3]،

مثال على ذلك، استحداث شركة"Apple" لنظام التشغيل الخاص بها (iOS 11)، واستخدامها نظام التشفير لجميع بيانات مستخدمي منتجاتها، توفيراً لأعلى قدر ممكن من الأمان لعملائها.

-دور التشفير في الوقاية من الجريمة الإلكترونية

في مجتمعنا التكنولوجي المعاصر، أصبحت الكتابة المشفرة إحدى الأدوات الرئيسية لضمان السرية والثقة، والتحكم في دخول المستخدمين، والتسديد الإلكتروني، وأمن الشركات، وغير ذلك. وقد جعل هذا من تقنية التشفير في مقدمة الوسائل التقنية الوقائية من الجريمة الإلكترونية، وذلك لتحقيق الأمن المعلوماتي وحماية المعاملات والصفقات المتبادلة عبر الإنترنت. كما يُسهم التشفير في تدعيم الإثبات الإلكتروني.

[1] بوعقل مصطفى، اونان بومدين، مباركي سمراء، اليات وقاية المعاملات الالكترونية في ظل حكومة تكنولوجيا المعلومات، les cahiers du mecas، جامعة الجيلالي ليابس، سيدي بلعباس، العدد12، جوان2016، ص383

[2] ميرفت محمد حبايب، المرجع السابق، ص128.129

[3] ميرفت محمد حبايب، المرجع نفسه، ص129

ونظراً لأن لكل شخص أسراراً تتفاوت من فرد لآخر، فعندما يصبح من الضروري إرسال هذه المعلومات السرية عبر شبكة الإنترنت، يتم نقلها بشكل مشفر. وتؤدي هذه الكتابة المشفرة دوراً كبيراً في ضمان الخصوصية، من خلال الاحتفاظ بالمعلومات بصيغة مخفية عن أي شخص لا يمتلك صلاحية الوصول إليها.[1]

على الرغم من الأهمية البالغة لتقنية التشفير في الوقاية من الجريمة الإلكترونية، إلا أن لها مخاطر أيضاً. وتتمثل هذه المخاطر في أن التشفير قد يجعل مهمة الشرطة مستحيلة، لأنه يمنعها من اكتشاف الجرائم التي تحتوي عليها الحاسبات الآلية، وخاصة فيما يتعلق بالإرهاب، ومرة في صور الإباحية، يشكل التشفير عقبة أمام التحقيق الابتدائي، حيث يجعل نظام التشفير من المستحيل إقامة الدليل على ارتكاب الجريمة.

ونظراً للخطورة التي ينطوي عليها التشفير، أصدرت بعض الدول، مثل هولندا، مشروع قانون يُخضع عملية التشفير لشرط الحصول على ترخيص، مع إلزام المستخدمين بإيداع مفاتيح التشفير لدى مكتب متخصص ملزم بالسرية. ويتعين على هذا المكتب تقديم تلك المفاتيح إلى رجال البحث الجنائي الذين حصلوا على أمر بالضبط والتفتيش من سلطات التحقيق. غير أن احتمال إفشاء هذه المفاتيح قد يُضعف من وسائل الحماية من الجريمة الإلكترونية. وبسبب هذا الاعتبار، قدر المشرع الفرنسي أن استخدام التشفير في نقل المعلومات قد يُسهّل الأنشطة الإجرامية، مما دفعه إلى التدخل وتنظيم هذه العملية بنصوص قانونية.

ثانيا : بروتوكول المعاملات المالية الآمنة Secure Electronique– SET) (Transaction)

هو بروتوكول أُنشئ عام 1997 في الولايات المتحدة الأمريكية بهدف تأمين المعاملات المالية عبر الإنترنت. يشبه هذا البروتوكول بروتوكول (SSL) من حيث آلية التشفير، إلا أنه يتخصص أكثر في التعاملات المصرفية. يعتمد بروتوكول SET على إصدار شهادات رقمية

[1] ميرفت محمد حبايب، المرجع السابق، ص130

من البنوك، كما يتكامل مع برامج "المحفظة الإلكترونية" لتوثيق هوية حامل البطاقة وتأكيد العمليات المالية دون كشف بيانات البطاقة للجهات الوسيطة.[1]

ثالثا: البصمة الرقمية (HASHING)

تُستخدم خوارزميات التمويه أو(الهاشينغ) لتوليد بصمة رقمية فريدة تمثل رسالة أو ملفاً معيناً. ولا يمكن عكس هذه البصمة لاسترجاع النص الأصلي، وإنما تستخدم للتحقق من سلامة الرسائل وعدم تعديلها أثناء الإرسال .[2]

رابعا: التوقيع الالكتروني

عد التوقيع الإلكتروني بمثابة هوية المرسل، ويضمن عدم تغيير الوثيقة بعد توقيعها. يستخدم المرسل مفتاحه الخاص لتوقيع الوثيقة، بينما يتحقق المستقبل من صحتها باستخدام المفتاح العام. ولهذا التوقيع أهمية كبرى في المعاملات التجارية والقانونية عبر الانترنت.

خامسا: الجدار الناري

يرتبط مفهوم الجدار الناري بتعريف هذه التقنية المستخدمة في الوقاية من الجريمة الإلكترونية، ثم تحديد أهم الخصائص المميزة لها، وأخيراً بيان أهميتها في هذا المجال.

يرى أغلب خبراء النظم المعلوماتية أن الجدار الناري[3] هو عبارة عن نظام أو مجموعة أنظمة تعمل على تعزيز صد الوصول إلى المعلومات بين شبكتين. وتختلف الوسائل المعتمدة في ذلك، لكنه من حيث المبدأ يمكن تعريفه بأنه برنامج يمكن أن يكون على هيئة جهاز متكامل أو برنامج يُحمَّل على حاسوب بمواصفات جيدة، وتتمثل وظيفته في حماية شبكة الحاسب الآلي الداخلية وشبكة الإنترنت' وتتمثل مهمته الرئيسية في مراقبة جميع البيانات الداخلة والخارجة من الشبكة والتأكد من مطابقتها للشروط التي يحددها المستخدم للبرنامج مسبقاً.

[1] عز الدين غبش، حماية المستهلك الالكتروني في ظل الجرائم السيبرانية، المجلة الدولية للتحولات القانونية والسياسية، المجلد1، العدد1،2022، ص105

[2] عبد الله سيف الكيتوب، المرجع السابق، ص85

[3] ميرفت محمد حبايب، مرجع السابق، ص133

كماعرف الجدار الناري بأنه جهاز أو نظام يقوم بالتحكم في مسار ومرور البيانات داخل الشبكة أو بين الشبكات، سواء بالمنع أو بالسماح، وتُستخدم هذه التقنية غالباً عند الاتصال بالإنترنت. ويمكن تعريفه أيضاً بأنه برنامج أو جهاز لتنقية البيانات قبل دخولها إلى الشبكة المحلية، حيث تمر حزمة البيانات الواردة إلى الشبكة عبر الجدار الناري لفحصها، فإن كان الموقع المصدر لهذه الحزمة ضمن قائمة المواقع المحجوبة، فلن يسمح الجدار الناري بدخولها إلى الشبكة.[1]

ومن اهم خصائصه نجد:

·منع دخول المستخدمين غير المُصرَّح لهم إلى الشبكة.

• حماية استخدام الخدمات الهامة عند الدخول إلى الشبكة ومغادرتها، وتوفير حماية عامة من جميع الهجمات المحتملة.

• تحديد اتجاه البيانات الصادرة والواردة من وإلى الشبكة.

• تحديد الجهاز أو النظام أو الشبكة الموثوقة التي يُسمح لها بالتعامل مع الشبكة الداخلية المحمية.

• مراقبة البيانات العابرة من وإلى الشبكة، وتسجيل وتتبُّع الأحداث، والتنبيه من أي أخطار.

• حماية منافذ الشبكة، والعمل كذاكرة للمواقع التي تمت زيارتها لتسريع الوصول إليها فيما بعد.

على الرغم من الخصائص التي يتمتع بها الجدار الناري، إلا أنه لا يستطيع الحماية ضد الهجمات التي تحدث داخل الشبكة، أي من الأشخاص الموجودين داخل الشبكة المحمية ممن حصلوا على الثقة، أو ضد الهجمات التي تعبر الجدار الناري نفسه وتعتمد على ثغرات في بروتوكولات لا تستطيع الشبكة الاستغناء عنها.[2]

[1] عز الدين غبش، المرجع السابق، ص 105

[2] ميرفت محمد حبايب، مرجع السابق، ص136

كما لا يستطيع الجدار الناري حماية البيانات من القرصنة التي تجري من داخل الشبكة المحلية، ولا يستطيع تحديد هوية المخترق في هذه الحالة.

ما فيما يتعلق بوظيفة الجدار الناري في الوقاية من الجريمة الإلكترونية، فتتمثل في تنظيم تدفق حزمة الشبكة بين شبكات الحاسوب المكونة من مناطق متعددة متفاوتة الثقة، مما يسهم في توفير الحماية اللازمة للشبكة والمعلومات. ويعمل الجدار الناري على تخزين المعلومات والعمليات التي تمر من خلاله. وعليه، فإن دور الجدار الناري يتمثل في مراقبة جميع البيانات الداخلة والخارجة من الشبكة، والتأكد من مدى مطابقتها للشروط التي يحددها المستخدم مسبقاً. وتظهر أهمية هذه التقنية باعتبارها تشبهاً بنظام الفلتر الذي يمنع مستخدمي الإنترنت من الدخول إلى بعض المواقع المعينة على الشبكة، وذلك بإعطاء صاحب الشبكة الحق في التحكم فيما إذا كان مستخدمو الشبكة سيتمكنون من الدخول إلى مواقع معينة غير مرغوب فيها. وتُعد هذه ميزة ذات أهمية خاصة فيما يتعلق بتمكين الطفل أو القاصر من تصفح الإنترنت بطريقة آمنة، بحيث لا يتسنى له الوصول إلى المواقع الإباحية أو المواقع التي تُكسبه خبرات ضارة.[1]

سادسا: استخدام الوسائل الوسيطة :(PAY Pal)

تُستخدم المنصات الوسيطة لتوفير طبقة أمان إضافية بين المستهلك والبائع، بحيث لا تُكشف بيانات البطاقة مباشرة. يُعد موقع "باي بال" (PayPal)من أشهر هذه المواقع، ويُستخدم على نطاق واسع في التجارة الإلكترونية لما يوفره من حماية وضمان للمستخدمين.[2]

سابعا: الشهادة الرقمية (Digital certificat)

هي وثيقة إلكترونية تصدر عن جهة موثوقة (سلطة التصديق) وتُستخدم للتحقق من هوية الأطراف المتعاملة إلكترونياً. تحتوي الشهادة على معلومات عن مالكها، مثل الاسم والمفتاح العام، وتُستخدم غالباً في التوقيع الرقمي والتشفير. [3]

[1] ابوبكر تيتاوي، الياس مالك قرادي، المرجع السابق ص 106

[2] عز الدين غبش، مرجع السابق، ص 106

[3] ابوبكر تيتاوي، الياس مالك قرادي، المرجع نفسه، ص106

الفرع الثاني: الوسائل الادارية لحماية أمن المعلومات والوقاية من الاحتيال الالكتروني

تلعب الإدارة العليا دورًا محوريًا في ضمان أمن المعلومات داخل المؤسسات، من خلال اعتماد سياسات رقابية وإجراءات تنظيمية تضمن بيئة عمل محمية من التهديدات الرقمية. وتتمثل أبرز المهام الإدارية الوقائية في النقاط الآتية:[1]

أولا: وضع سياسة أمن معلومات واضحة ومثقفة

يُعد إعداد سياسة أمنية واضحة من أولى خطوات الوقاية، وتشمل تقديم مبادئ ومعايير الحماية الأساسية عبر وسائل مرئية أو منصات إلكترونية داخلية. وينصب الهدف الأساسي من ذلك على توعية الموظفين وتعريفهم بالضوابط الواجب اتباعها، مما يُرسخ ثقافة أمنية مؤسسية.[2]

ثانيا: تأمين الأجهزة ومراكز البيانات

يجب حماية الأجهزة ومخازن وسائط التخزين من الوصول غير المصرح به، وذلك من خلال منع الدخول العشوائي إلى غرف الحواسيب واعتماد وسائل متقدمة مثل بصمة الإصبع، أو بصمة العين، أو البطاقة الممغنطة. ويضاف إلى ذلك تنظيم عمليات التشغيل وتحديد المسؤوليات والصلاحيات بدقة.

ثالثا: تنظيم حماية قواعد البيانات

تتطلب حماية قواعد البيانات وجود هيكل تنظيمي واضح يُوزع من خلاله المهام والصلاحيات، وتُحدد فيه مسؤوليات كل موظف تجاه البيانات. كما يجب وضع ضوابط صارمة

---

[1] بوزكري جيلالي، الإدارة الالكترونية في المؤسسات الجزائرية واقع وافاق، أطروحة دكتوراه علوم في التسيير، تخصص إدارة أعمال والتسويق، قسم علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 3، الجزائر،2015 – 2016، ص155-154

[2] جمل عبد اللطيف وطرايش عبد الغني، الحماية الجنائية للمستهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري دراسة لتحليلية ومقارنة في ضوء القانون الفرنسي، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة الأغواط، المجلد 9، العدد1، 2025، ص1381-1404

على تشغيل البرامج ومعالجة البيانات داخلياً وخارجياً، وضمان أمن الشبكات وخطوط الاتصال المرتبطة بها.[1]

رابعا: إدارة آمنة لوسائط الحفظ والنسخ الاحتياطي

تشمل هذه الخطوة ضمان حفظ وسائط التخزين الخارجية في أماكن آمنة، مع جدولة عمليات النسخ الاحتياطي الدوري لحماية البيانات من الضياع أو التلاعب، بالإضافة إلى تحديث أنظمة الحفظ بانتظام لتفادي الثغرات.

خامسا: إدارة مغادرة الموظفين والمتابعة الداخلية

من الضروري منع التوظيف المؤقت العشوائي، وإلزام الموظف بتسليم كل ما بحوزته عند انتهاء عمله، مثل المفاتيح والبطاقات وكلمات المرور. كما ينبغي تغيير صلاحياته فور مغادرته. ويوصى كذلك بإجبار الموظفين على أخذ إجازات دورية لمراقبة النظام واكتشاف أي تلاعب قد يكون مستترا.[2]

سادسا : بناء قسم مختص بأمن المعلومات

فضل أن تحتوي المؤسسات الكبرى على قسم مستقل لأمن المعلومات يُشرف عليه مدير أمني مرتبط مباشرة بالإدارة العليا. ويضم هذا القسم كفاءات تقنية وأمنية متخصصة في تحليل البيانات، والتنسيق الأمني، والتعامل مع التهديدات الإلكترونية بكفاءة عالية.

سابعا: تعزيز التكوين المستمر:

من المهم عقد ندوات ومؤتمرات ومحاضرات متخصصة بشكل منتظم في مجال أمن المعلومات، مع تشجيع الموظفين على حضور المعارض والدورات التدريبية المتخصصة في هذا المجال، لضمان مواكبة أحدث التقنيات الأمنية.[3]

ثامنا : التحفيز وربط الترقية بالالتزام الأمني

[1] بوزكري جيلالي، المرجع السابق، ص154

[2] عز الدين غبش، المرجع السابق، ص101

[3] بوزكري جيلالي، المرجع السابق، ص154

عد ربط الترقية المهنية والحوافز بالالتزام بالضوابط الأمنية وسيلة فعالة لتعزيز المسؤولية الفردية داخل المؤسسة، ولتشجيع الموظفين على تطبيق السياسات الأمنية بدقة.

المطلب الثاني: طرق التوعية الوقائية لجريمة الاحتيال الالكتروني

نظراً للتقدم التكنولوجي، أصبحت شبكة الإنترنت تُشكّل تهديداً كبيراً لأفراد المجتمع عامة وللدولة، نظراً لظهور الجريمة الإلكترونية في الفضاء الإلكتروني بشكل كبير، ولما كانت المحكمة تقضي بأنّ "الوقاية خير من العلاج"، بالتالي فإنّه لا بدّ من اتباع أساليب وقائية للوقاية من وقوع الجريمة الإلكترونية، سواء بالطرق التقنية التي سبق الحديث عنها في المطلب الأول.

الفرع الأول: دور مؤسسات الدولة في العمل على التوعية للوقاية من الجريمة

لقد كشفت العديد من الدراسات التي أجريت حول الجريمة الإلكترونية والإجراءات والتدابير الوقائية منها، والتي يجب على الدولة التصدي لها، بأن أفضل الطرق التي يجب اتباعها للوقاية من الجريمة الإلكترونية هي طرق التوعية. وتتم هذه التوعية من خلال حملات لزيادة الوعي العام لكافة شرائح المجتمع، بالإضافة إلى ضرورة تدريب وتأهيل موظفي المؤسسات والإدارات العمومية على آليات الوقاية من الجريمة الإلكترونية والمخاطر الناشئة عن هذا النمط الإجرامي.

أولا: تدريب وتأهيل أفراد أجهزة الأمن وموظفي قطاع العدالة وتوعيتهم وآليات الوقاية من الجريمة الإلكترونية

تتطلب مكافحة الجريمة الإلكترونية تدريب الكوادر القادرة على مواجهة هذه الجريمة في حال وقوعها، بالإضافة إلى تدريبهم وتأهيلهم على طرق الوقاية منها. وحتى يكون لهذا التدريب نتائجه الإيجابية، لا بد أن تتوافر لدى المتدرب ذاته الصلاحية العلمية، والقدرات الذهنية والنفسية اللازمة لتلقي التدريب. ويقدّر بعض الخبراء أنه لا بد من توفر الخبرة الكافية في المجالات المرتبطة بعمليات الحاسوب والبرمجة. كما لا بد أن يتضمن البرنامج التدريبي طرق التوعية للوقاية من الجريمة الإلكترونية، بالإضافة إلى طرق وإجراءات التحقيق اللاحقة لوقوع الجريمة. وتشمل هذه البرامج أيضاً محاضرات وندوات دراسية، ونقل خبرات علمية في مختلف

جوانب عمليات الحاسوب الآلي وشبكات الإنترنت. فقد قام بعض رجال الشرطة والقضاء، نتيجة لعدم توفر التأهيل التقني للوقاية من الجريمة الإلكترونية، بتقديم يد المساعدة لمرتكبي الجريمة الإلكترونية دون قصد بسبب الجهل بالإجراءات الوقائية السابقة واللاحقة لارتكاب الجريمة. [1]

وبالنسبة للمنهج التدريبي، فيجب أن يشتمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات في شبكة المعلومات وأجهزة الحاسوب، وذكر مفاهيم معالجة البيانات، وتحديد نوعية وأنماط الجرائم الإلكترونية، وصفات المجرم الإلكتروني، والدوافع التي تدفعه إلى ارتكاب الجريمة الإلكترونية، وآليات التفتيش والتحقيق الإلكتروني.

كما أن التدريب والتأهيل للوقاية من الجريمة الإلكترونية يتم بإحدى الطرق التالية:

-التدريب أثناء العمل الوظيفي: حيث يتلقاه الموظف عن طريق تكليفه بالعمل مع شخص لديه الخبرة في مواجهة الجرائم الإلكترونية.

-التدريب من خلال حلقات دراسية وحلقات نقاش: تُعقد حول الجرائم الإلكترونية وأمن الحاسوب والشبكات، ويتضمن ذلك نقاشاً للمشاركين وخبراء الحاسوب المتخصصين في المعالجة الإلكترونية للبيانات، بالإضافة إلى رجال الشرطة المكلفين بمهمة القبض على مرتكبي الجرائم الإلكترونية.

وهذا التدريب المقصود به ليس التدريب التقليدي، إذ لا يكفي أن يتم توفير الخلفية والمعلومات القانونية حول موضوع الجريمة الإلكترونية وطرق الوقاية منها لرجال الأمن والقضاء، بل يجب إكسابهم خبرة فنية في مجال الجرائم الإلكترونية.[2]

ولتحقيق ذلك، لا بد من عقد المؤتمرات والندوات الدولية والإقليمية لتدريب وتأهيل رجال الأمن والقضاء، وإيجاد صيغة موحدة دولياً وإقليمياً تشمل الجوانب الفنية والتقنية، إضافة إلى الجوانب

[1] ياسر محمد الكومي أبو حطب، الحماية الجنائية والأمنية للتوقيع الالكتروني، الإسكندرية، منشأة معارف بلال حزي وشركاؤه،2014، ص387

[2] ياسر محمد الكومي محمود أبو حطب، مرجع نفسه، ص388

القانونية والتشريعية، وذلك من خلال الاستعانة بذوي الكفاءات المتميزة في تكنولوجيا المعلومات.

وكما أنه يتعين أن يتم تأهيل وتدريب رجال القضاء على كيفية التعامل مع الدليل تقني' بالإضافة إلى تدريب أجهزة الأمن المتخصصة بالجريمة الإلكترونية على أن يتم تدريبها على كافة الإجراءات التقنية اللازمة للوقاية من الجريمة الإلكترونية.

وتدريب الكوادر يختلف من دولة لأخرى بحسب تطور هذه الدولة وتقدمها، حيث إنه في بعض الاتفاقيات الدولية والإقليمية هناك نص صريح يشير إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينهم. [1]

إذ أثبت الواقع أن أية دولة لا تستطيع بمفردها القضاء على الجريمة في ظل هذا التطور. وقد يثور تنازع الاختصاص القضائي وفقاً لمبادئ الإقليمية والشخصي والعيني، مما قد يخل بمبدأ "عدم محاكمة الشخص عن الفعل الواحد أكثر من مرة".

تمر مواجهة هذه الظاهرة عبر سلسلة من العمليات، تبدأ بالتوعية والإعلام، على الرغم من أن الاتفاقيات الدولية المتعلقة بالمساعدة والتعاون القضائي غالباً ما تفتقر إلى التطبيق العملي. بحيث سنتطرق الى الجهود الدولية لمكافحة الاحتيال الالكتروني كالاتي:

أ: الاتفاقيات والمعاهدات الدولية لمكافحة الجريمة الإلكترونية

. اتفاقية برن (1886): أُبرمت لحماية المصنفات الأدبية والفنية[2]، وتقوم على مبادئ: المعاملة الوطنية، الحماية التلقائية، واستقلال الحماية. شملت الحماية حقوقاً استئثارية ومعنوية، وامتدت لتشمل البرمجيات كأعمال أدبية، إلا أنها لم تعالج النشر الإلكتروني عبر الإنترنت بسبب تعديلها قبل ثورة الاتصالات.

. اتفاقية الويبو (1967): ألزمت الدول الأطراف بحماية حقوق التأليف على الإنترنت، شاملة برامج الحاسوب وقواعد البيانات. أوجبت وضع جزاءات ضد التحايل على التدابير

[1] ميرفت محمد حبايب، المرجع السابق، ص 150

[2] ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة دراسات وأبحاث، الجلفة، العدد1، 2009، ص246.

التكنولوجية، وتجريم حذف المعلومات الإلكترونية الضرورية لإدارة الحقوق، مع تحديد مدة حماية لا تقل عن خمسين عاماً.

. اتفاقية تريبس (1994): وسعت نطاق الحماية القانونية للاختراعات وبراءات الاختراع، واعتمدت مبدأي قابلية جميع الاختراعات للحماية وعدم التمييز بينها. نصت على حماية البرمجيات بحقوق المؤلف لمدة 50 عاماً، وهدفت إلى تحرير التجارة العالمية مع توفير تدابير فعالة لإنفاذ حقوق الملكية الفكرية.[1]

. معاهدة بودابست (2001): وقعها مجلس أوروبا متأثراً بالتغيرات الرقمية والعولمة[2]، وعالجت ثلاثة محاور: جرائم الشبكات (كالإرهاب الإلكتروني، تزوير بطاقات الائتمان، واستغلال الأطفال)، الجوانب الإجرائية (الرقابة، اعتراض الاتصالات، وحماية البيانات)، والتعاون الدولي (تسليم المجرمين والمساعدة القضائية). سعت لتحقيق وحدة التشريعات، التوازن مع حقوق الإنسان، وتحديد اختصاص قضائي لجرائم تكنولوجيا المعلومات. الخلاف الوحيد تمثل في مجال محاربة التحريض على الكراهية العنصرية.[3]

. توصيات المجلس الأوروبي (1995)[4]: أصدر المجلس الأوروبي التوصية رقم 13195 لحث الدول على مراجعة قوانينها، وتضمنت: توضيح إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات، إلزام مقدمي خدمات الاتصال بالتعاون مع سلطات التحقيق، إصدار أوامر بتسليم البرامج والبيانات، وإيجاد إجراءات سريعة للاتصال بجهات أجنبية لجمع الأدلة.

---

[1] ليندة شراشبة، المرجع نفسه، ص247

[2] معاهدة بودابيست هي معاهدة تمت بالعاصمة المجرية بودابيست في2001 وهي أول معاهدة دولية تكافح جرائم الإنترنت وتبلور التعاون الدولي في محاربته، بعدما أصبحت عدة جرائم تهدد الأشخاص والممتلكات وبعد التوقيع عليها من طرف مسؤولين في الدول الأوروبية بالإضافة إلى أمريكا واليابان وكندا وجنوب إفريقيا، بعد مشاورات ومفاوضات دامت ما يزيد عن الأربع سنوات، حتى تم التوصل للصيغة النهائية والتوقيع عليها دون أي اعتراض، ودخلت حيز التنفيذ عام 2004

[3] مصطفى محمد موسى، "أساليب إجرامية بالتقنية الرقمية ومكافحتها"، مطابع الشرطة، ط2003 ،1م، ص 581

[4] مصطفى محمد موسى، المرجع نفسه، ص521

ب: القانون العربي النموذجي والاتفاقية العربية

على الرغم من أن الجريمة الإلكترونية لم تنتشر في الدول العربية مقارنة بغيرها، إلا أن ذلك لا يمنع من اتخاذ الإجراءات اللازمة. اعتمدت الدول العربية القانون العربي النموذجي، ثم وقعت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (القاهرة، 21 ديسمبر 2010)، والتي أصبحت سارية المفعول بعد تصديق الرئيس المصري عليها. وأكدت ديباجتها على تعزيز التعاون بين الدول العربية لدرء أخطار هذه الجرائم، حفاظاً على أمن الدول العربية ومصالحها.

الجرائم الإلكترونية التي عددتها الاتفاقية (13 جريمة): [1]

الدخول أو البقاء غير المشروع، الاعتراض غير المشروع لخط سير البيانات، الاعتداء على سلامة البيانات، إساءة استخدام وسائل تقنية المعلومات، التزوير، الاحتيال (عبر إدخال أو تعديل أو محو البيانات أو التدخل في وظائف الأنظمة)، الجرائم المتعلقة بالإباحية (مع تشديد العقوبة على إباحية الأطفال)، الجرائم المرتبطة بالإباحية، الاعتداء على حرمة الحياة الخاصة، الجرائم المتعلقة بالإرهاب، الجرائم المتعلقة بالجريمة المنظمة، انتهاك حقوق المؤلف والحقوق المجاورة، والاستخدام غير المشروع لأدوات الدفع الإلكترونية.

الإجراءات الجزائية وفق الاتفاقية:

. إنشاء جهاز متخصص ومتفرغ على مدار الساعة لتقديم المساعدة الفورية في التحقيق وجمع الأدلة الإلكترونية.

. ترك مجال تحديد جهة الضبط القضائي مفتوحاً للدول العربية

. تبني إجراءات متعلقة بـ البيانات الساكنة: حفظ عاجل للمعلومات المخزنة، إصدار أوامر تسليم المعلومات، إلزام مقدمي الخدمات بتقديم بيانات المشتركين.

. تبني إجراءات متعلقة بـ البيانات المتحركة: الجمع الفوري لبيانات المرور والمحتوى، واعتراض معلومات المحتوى.

[1] الفصل الثاني من الاتفاقية العربية، لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010

. إجراءات التفتيش والضبط: البحث عن الأدلة المادية والرقمية مع إمكانية تمديد نطاق التفتيش إلى أنظمة أخرى غير نظام المشتبه به، والاستعانة بالخبراء في المعلوماتية

ففي الأخير تقتضي مكافحة جرائم الإنترنت توحيد التشريعات ونظام الإثبات الإلكتروني، وتوثيق التعاون بين الأنظمة القانونية الداخلية دون المساس بسيادة الدول.[1]

ثانيا: التعاون الشرطي الدولي

تعود بدايات التعاون الشرطي الدولي إلى اتفاقية عام 1904 المتعلقة بمكافحة الرقيق الأبيض، والتي ألزمت الحكومات بإنشاء سلطات مختصة لتبادل المعلومات حول استغلال النساء في مجال الدعارة عبر الحدود. تلا ذلك عقد مؤتمر موناكو عام 1914، بمشاركة أربع عشرة دولة، بهدف وضع أسس للتعاون الشرطي الدولي، غير أن هذا المؤتمر لم يحقق نتائج عملية بسبب اندلاع الحرب العالمية الأولى[2].

يقوم التعاون الشرطي الدولي على أساس تجميع وتبادل بيانات المجرمين عبر المكاتب المركزية الوطنية لمنظمة الإنتربول، مع مراعاة مبدأ السيادة الوطنية، إذ لا تقوم المنظمة ذاتها بعمليات القبض، بل تترك هذه المهمة للشرطة الوطنية في الدولة المعنية.

بذل الدول المتقدمة، مثل الولايات المتحدة والسويد ودول الاتحاد الأوروبي، جهوداً حثيثة لتطوير أدائها في مجال مكافحة الجرائم المعلوماتية. تُعد الولايات المتحدة من أوائل الدول التي تصدت لهذه الجرائم على المستوى التشريعي، من خلال إنشاء إدارة متخصصة ضمن مكتب التحقيقات الفيدرالي (FBI) تضم فريقاً مدرباً على متابعة هذه الجرائم، والتحري عنها، وضبط الأدلة. وتتمثل آلية عمل هذه الإدارة في: الانتقال الفوري إلى موقع الجريمة، وضع خطة تحقيقية مكتوبة، البحث في السجلات، الاستعانة بوسائل المراقبة، تصوير الأجهزة وأرقامها المسلسلة ومخططات التوصيلات، تسجيل المعلومات المسلسلة للأجهزة والوسائط المتعددة، تصوير محتوى شاشات الكمبيوتر، والتمييز بين الأدلة لتجميع الكابلات. وفي أعقاب أحداث 11 سبتمبر 2001، طلب مكتب التحقيقات الفيدرالي من الشركات تعديل أنظمته وتوسيع

[1] ميرفت محمد حبايب، مرجع السابق، ص278

[2] كوثر مازوني، "الشبكة الرقمية وعلاقتها بالملكية الفكرية"، دار الجامعة الجديدة، طبعة 2008"م، ص 610،611

صلاحياته لمراقبة الاتصالات الإلكترونية، مع التأكيد على قصر التدخل على حالات الطوارئ فقط.[1]

ثالثا: التعاون القضائي الدولي

يؤدي القضاء دوراً هاماً في ردع المعتدين على المصالح المجتمعية. ويملك القاضي الجنائي سلطة أوسع من نظيره المدني، غير أنه يواجه صعوبتين رئيسيتين في مجال جرائم الحاسب: الأولى، تتعلق بتقييم الأدلة الرقمية في ضوء أنظمة الإثبات السائدة؛ والثانية، تتعلق بالتكييف القانوني للأفعال المستحدثة التي تختلف عن نظائرها التقليدية.

يحقق التعاون القضائي الدولي توفيقاً بين مبدأ سيادة كل دولة واستقلالها في ممارسة اختصاصها الجنائي على إقليمها، وبين ضرورة ممارسة حقها في العقاب. ويفرض هذا التعاون ضرورة ملحة لسببين رئيسيين: الأول، أن سلطات الدولة مقيدة بحدود إقليمها وفقاً لمبدأ السيادة، مما يمنعها من مباشرة الإجراءات القضائية خارج حدودها؛ والثاني، أن تطبيق قانون العقوبات يصبح مستحيلاً دون وجود قانون للإجراءات جنائية[2].

. وعلى الرغم من أهمية تدريب أعضاء الأجهزة القضائية والأمن في الدولة في مجال الوقاية من الجرائم الإلكترونية، وفي مجال البحث والتحري عنها حال اكتشافها وملاحقة مرتكبيها، إلا أنّ هناك صعوبات تظهر في تدريبهم، ومن هذه الصعوبات

أ–عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون.

ب–وجود فوارق فردية بين المتدربين وتأثيرها على عملية اكتساب للمهارات المستهدفة بقوة تامة ومتكافئة، لدى مختلف الأفراد المتدربين، لاسيما في المجال التقني[3]

ج–النظرة السلبية للمتدرب اتجاه العملية التدريبية على أنها عبء لا فائدة منها

[1] محمد عبيد الكعيبي، الجرائم الناشئة عن الاستخدام الغير مشروع بشبكة الانترنت، دار النهضة العربية، ط2،2009، ص591

[2] فتوح الشاذلي، "جرائم الكمبيوتر"، منشورات الحلبي، 2003م، ص 349

[3] خالد علي سلمان عبد الله، المرجع السابق، ص287

د-عدم قدرة البيئة التدريبية على تمثيل الواقع ولاسيما الواقع الافتراضي

هـ-ارتفاع تكلفة الدورات التدريبية، مما لا يتيح لكثير من الدول تمكين أفراد أجهزتها القضائية الأمنية من المشاركة فيها.

غير أنه، ورغم هذه الصعوبات، اهتمت العديد من الدول بتدريب أعضاء القضاء وأجهزة الأمن، إدراكاً منها لأهمية هذا التدريب. فمن الأمثلة على ذلك، قيام الجزائر بعقد الندوة الإقليمية الإفريقية الثانية والعشرين للمنظمة الدولية للشرطة الجنائية (الإنتربول)، بمشاركة ثلاث وخمسين دولة، وذلك لبحث الواقع الراهن والمستقبلي، وآليات مكافحة الأشكال الجديدة والمتجددة للجريمة المنظمة والعابرة للحدود، ومنها الجرائم الإلكترونية [1]

الفرع الثاني: دور أجهزة الدولة والمؤسسات المجتمع المدني في الدولة في التوعية الوقائية من الجريمة الالكترونية

نظراً للدور المحوري الذي يؤديه الإنترنت في العصر الراهن، وما له من تأثير بالغ على أفراد المجتمع، فقد أخذت مؤسسات الدولة تعزز دورها في مجال التوعية بمخاطر الجريمة الإلكترونية، بما يحقق الوقاية منها. وفي هذا السياق، أصدر المشرع الجزائري القانون رقم 09-04 لسنة 2009، المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي بموجبه أنشئت "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها". وقد حدد القانون مهام هذه الهيئة بموجب الفصل الرابع عشر (المادة 14)، والتي أبرزها تنشيط وتنسيق عمليات الوقاية من هذه الجرائم ومكافحتها.[2]

كما أُنشئ بموجب القانون نفسه "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، ونصت المواد من 335 إلى 342 على اختصاصاته وصلاحياته على النحو التالي:[3]

[1] ياسر محمد الكومي محمود أبو الحطب، مرجع سابق،388

[2] ميرفت محمد حبايب، مرجع السابق، ص152

[3] القانون (25-14)، المؤرخ في 9 صفر عام 1447، الموافق3 غشت سنة2025

·المادة 335: يُحدث بدائرة اختصاص مجلس قضاء الجزائر قطب جزائي وطني متخصص في متابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، كما يختص بالحكم في الجرائم المنصوص عليها في هذا الفصل إذا كانت تشكل جنحاً. ويُقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في مفهوم هذا القانون، أي جريمة ترتكب أو يُسهل ارتكابها باستخدام منظومة معلوماتية، أو نظام اتصالات إلكترونية، أو أي وسيلة أو آلية أخرى ذات صلة بهذه التكنولوجيات.

·المادة 336: يمارس وكيل الجمهورية لدى هذا القطب، وقاضي التحقيق، ورئيس القطب، صلاحياتهم في كامل الإقليم الوطني.

·المادة 337: يختص هؤلاء، حصرياً، بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التالية، وكذا الجرائم المرتبطة بها: الجرائم التي تمس بأمن الدولة أو الدفاع الوطني؛ جرائم نشر وترويج أخبار كاذبة من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع؛ جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية؛ جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية؛ جرائم الاتجار بالبشر أو الأعضاء البشرية أو تهريب المهاجرين؛ جرائم التمييز وخطاب الكراهية.

·المادة 338: يختص وكيل الجمهورية، وقاضي التحقيق، ورئيس القطب، حصرياً، بمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيداً والجرائم المرتبطة بها. ويُقصد بالجريمة الأكثر تعقيداً، في مفهوم هذا القانون، الجريمة التي تتطلب، نظراً لتعدد الفاعلين أو الشركاء أو المتضررين، أو لاتساع الرقعة الجغرافية لمكان ارتكابها، أو لجسامة آثارها أو أضرارها، أو لطابعها المنظم أو العابر للحدود الوطنية، أو لمساسها بالنظام والأمن العموميين، استعمال وسائل تحري خاصة، أو خبرة فنية متخصصة، أو اللجوء إلى تعاون قضائي دولي.

·المادة 339: تُطبق على الاختصاص الحصري للقطب الإجراءات المنصوص عليها في المواد من 346 إلى 348 من هذا القانون.

·المادة 340: يمارس وكيل الجمهورية، وقاضي التحقيق، ورئيس القطب، اختصاصاً مشتركاً مع الاختصاصات الناتجة عن تطبيق المواد 58 و70 و468 من هذا القانون، بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، وتُطبق في هذه الحالة الإجراءات المنصوص عليها في المواد من 317 إلى 329 من القانون نفسه[1].

·المادة 341: إذا تزامن اختصاص هذا القطب مع اختصاص القطب الجزائي الوطني الاقتصادي والمالي، يؤول الاختصاص وجوباً إلى الأخير.

·المادة 342: إذا تزامن اختصاص هذا القطب مع اختصاص القطب الجزائي الوطني لمكافحة الإرهاب والجريمة المنظمة عبر الوطنية، وفقاً لأحكام المواد 343 إلى 348 من

هذا القانون، يؤول الاختصاص وجوباً إلى الأخير[2]

أولا: دور الإعلام الأمني في الوقاية من الجريمة الإلكترونية:

مفهوم الإعلام الأمني: وهو من التعبير الذي يمارسه الجهاز الأمني بصوره الإيجابية المختلفة للتفهم والمشاركة مع المجتمع لتحقيق الأمن، ويتمثل الإعلام الأمني ما يصدر عن أجهزة الأمن من مجلات ونشرات وبرامج توعية تبث عبر شاشات التلفاز وتعمل على تحقيق التوعية للمجتمع، بما يكفي لتحقيق الاستقرار والأمان للمجتمع، ويلعب الإعلام الأمني دورا هاما في توعية المجتمع بكل أطيافه بالمخاطر التي قد يتعرض لها بشأن الجرائم الإلكترونية[3]. وبسبب تزايد الجريمة الالكترونية في العصر الحديث، وتزايد التعامل بالإنترنت، قام الإعلام الأمني بوضع خطة استراتيجية لتوعية الأفراد والشركات والمؤسسات بمخاطر الإنترنت وسُبل الأمان والحماية وطرق وأساليب الإبلاغ في حال وقوع جريمة إلكترونية[4]

[1] المادة 340، قانون إجراءات جزائية القانون (25-14)، المؤرخ في 9 صفر عام 1447، الموافق3 غشت سنة2025

[2] المادة342، المرجع نفسه

[3] المادة 14/أ من قانون رقم (04.09)، لسنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

[4] حفيظة رفاس، دور السياسة الجنائية للمشرع الجزائري في مكافحة الجرائم التكنولوجيا الحديثة، مذكرة تخرج لنيل شهادة الدكتوراه، قسم القانون العام، جامعة الدكتور الطاهر مولاي، سعيدة، الجزائر، 2019، ص204

ثانيا: دور المؤسسات التعليمية والثقافية في الوقاية من الجريمة الإلكترونية

تُسهم مؤسسات المجتمع المدني بدور هام في الوقاية من الجريمة الإلكترونية، وذلك من خلال الحد من انتشار السلوكيات غير المرغوب فيها في المجتمع، ومنع انحراف الأفراد، وتوجيه السلوك الاجتماعي الوجهة الصحيحة، وتعزيز القيم والأخلاق عبر الإخلاص في العمل، وحسن التربية والتوجيه، فضلاً عن فرض الرقابة والمتابعة على الأفراد بهدف رصد الظواهر الإجرامية ومعرفة أسبابها للوصول إلى طرق ووسائل علاجها. كما ينبغي التركيز في المناهج الدراسية على غرس القيم الأخلاقية، باعتبار أن الطالب يكون أكثر استجابة للتوجيه في هذه المرحلة العمرية[1].

إلى جانب ذلك، تُعتبر المدارس والجامعات ومراكز التكوين المهني من المؤسسات التي تتمتع بدور إيجابي في الوقاية من الجريمة الإلكترونية، وذلك من خلال قيام المدارس بتعليم الطلاب في المراحل التعليمية من الأساسية وحتى الثانوية على تقنيات التحكم في استخدام الإنترنت. وبناءً على هذه الأهمية، أدرجت العديد من دول العالم منهاج تكنولوجيا المعلومات كمادة تدريسية تُدرَّس في المدارس.

ثالثا: دور وزارة الاتصالات في الوقاية من الجريمة الإلكترونية

قامت وزارة الاتصالات الجزائرية، وحذت حذوها وزارة الاتصالات الفلسطينية، بتسويق نظام للمراقبة الأبوية على الإنترنت، يتيح هذا النظام لأولياء الأمور حجب جميع المواقع غير المرغوب فيها على الإنترنت بالنسبة للأطفال، وذلك باستخدام كلمة سر تكون بحوزة ولي الأمر. وبالمثل، تقوم وزارة الاتصالات الفلسطينية بتمكين أولياء الأمور من التقدم بطلب إلى الوزارة من أجل حظر جميع المواقع الإباحية على منصة يوتيوب، مما يمكن الأطفال من متابعة المحتوى على اليوتيوب دون التعرض لخطر مشاهدة مواقع إباحية[2].

[1] نبيل أبوالرب، الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين، رسالة ماجستير تخصص قانون عام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين،2018، ص82

[2] ابوبكر تيتاوي، إلياس مالك قرادي، المرجع السابق، ص91

رابعا: دور المؤسسات الدينية في الوقاية من الجريمة الإلكترونية

تُؤدي المؤسسات الدينية دوراً هاماً في الوقاية من الجريمة الإلكترونية، وذلك من خلال التربية الأخلاقية، وتقوية الوازع الديني بين أفراد المجتمع، والتنشئة السليمة للأفراد عبر وسائل التوعية الدينية المختلفة. ويتجلى هذا الدور في وضع المؤلفات والكتب ذات البعد الديني التي تتناول مخاطر هذه الجرائم، وتنظيم دورات ومحاضرات إرشادية حولها في أماكن العبادة والمدارس والجامعات وسائر المؤسسات، بالإضافة إلى تعزيز دور الخطباء في المساجد، بالتعاون مع وزارة الأوقاف، لتوعية الناس بهذه الظواهر، وبيان المخاطر الناشئة عن السلوكيات التي تتعارض مع الدين الإسلامي ومبادئ الشريعة الإسلامية، والإسهام في تنمية الوازع الديني والأخلاقي[1] لدى الأفراد.

خامسا: دور مؤسسات المجتمع المدني في الوقاية من الجريمة الإلكترونية

تُسهم مؤسسات المجتمع المدني بدور بارز في الوقاية من الجريمة الإلكترونية، وذلك من خلال إصدار نشرات توعوية، سواء المكتوبة منها أو الإلكترونية، بهدف توعية المواطنين، ولا سيما فئتي الشباب والأطفال، وتحذيرهم من خطورة الإنترنت على أمنهم المعلوماتي وخصوصياتهم، وكذلك على المجتمع ككل.

سادسا: دور الطرق الذاتية في الوقاية من الجريمة الإلكترونية

على الرغم من أن الجريمة الإلكترونية تشكل خطراً على مختلف طبقات المجتمع والدولة على السواء، إلا أن ثمّة طرقاً ذاتية للتوعية تمكّن الفرد من حماية نفسه وأسرته من هذه الجريمة، وتتمثل هذه الطرق فيما يلي:

أ: دور الأسرة في التوعية للوقاية من الجريمة الإلكترونية

تُعتبر الأسرة نواة المجتمع، سواء أكان بدائياً أم متحضراً. وفي عصر الإنترنت، يبرز دور الأسرة كدور محوري في التوعية للوقاية من الجريمة الإلكترونية، وتُعرف هذه التوعية بـ "الرقابة الأبوية"، التي تهدف إلى رفع مستوى الوعي الإلكتروني للآباء وتمكينهم من استخدام الإنترنت.

[1] نبيل أبو الرب، مرجع سابق، ص83

والعلاقة هنا طردية؛ فكلما زاد وعي الآباء بمعرفة استخدام الإنترنت، كلما قل ارتكاب الجرائم الإلكترونية، لأنهم يتمكنون من إرشاد أبنائهم إلى الاستخدام الآمن لشبكة الإنترنت.[1]

وبذلك يظل الأبناء تحت رقابة آبائهم، وتُعد هذه من أهم طرق التوعية الناجحة للوقاية من الجريمة الإلكترونية، وذلك من خلال توعية أفراد الأسرة وتوجيههم نحو السلوكيات الإيجابية وإبعادهم عن الجرائم. كما يبرز دور الأسرة في الوقاية من الجريمة الإلكترونية عندما تعمل على معاقبة أفرادها في حال ارتكاب أحدهم جريمة إلكترونية. وهذا الدور يفرض على مختلف الدول وضع برامج أسرية ضمن خططها التنموية والاجتماعية، بغية بناء جيل صالح.[2]

ب: الوقاية من الجريمة الإلكترونية على الصعيد الشخصي

لكل شخص القدرة على حماية نفسه من الجريمة الإلكترونية قبل وقوعها، وذلك باستخدام عدة طرق وقائية، منها ما يلي:

ـ استخدام التحديثات الدورية لبرامج مضادات الفيروسات ومضادات التجسس على جميع الأجهزة الإلكترونية، تفادياً للوقوع ضحية للجريمة الإلكترونية.

ـ لحرص على تحديث متصفح الإنترنت بشكل مستمر.

ـ عدم التواصل مع أي جهات أو مواقع إلكترونية لا تتوفر فيها معايير الأمان العالي، والاقتصار على التواصل مع جهات موثوقة تقوم بحماية معلومات وبيانات المرور الخاصة بالشخص.

ـ عدم الضغط على أي روابط أو إعلانات أو مرفقات، وعدم الرد على الرسائل الإلكترونية الواردة من مصادر غير معروفة أو غير موثوقة.

ـ عدم الرد على الرسائل التي تستفسر عن البيانات الشخصية أو المعلومات الأمنية الخاصة بالشخص، ولا سيما المعلومات البنكية، وعدم نشر البيانات على مواقع التواصل والإنترنت، حتى لا يقع الشخص ضحية للجرائم الإلكترونية في المستقبل.

[1] الحاج الطاهر زهير، مرجع سابق، ص93

[2] نبيل أبو الرب، مرجع سابق، ص83

ـ يمكن للشخص حماية نفسه من اللصوص الإلكترونيين من خلال عدم مشاركة إعدادات الخصوصية والأمان التي تحدد من يمكنهم مشاهدة نشاطه الإلكتروني[1].

بناءً على ما تقدم من طرق التوعية للوقاية من الجريمة الإلكترونية، أنه لا بد من إدراج طرق الوقاية من الجريمة الإلكترونية ضمن المنهاج المدرسي للمدارس، كما ينبغي أن تكون إحدى المتطلبات الجامعية الإجبارية في مرحلة التعليم العالي. وبالنسبة للمجتمع ككل، فلا بد من وجود برامج توعوية متخصصة تبث بشكل دوري على قنوات التلفاز الوطنية والمحلية، بالإضافة إلى نشر المنشورات الورقية والإلكترونية للتنبيه بمخاطر الجريمة الإلكترونية. ويُنسجم هذا الطرح مع الحكمة القائلة: "درهم وقاية خير من قنطار علاج"، وهو ما يتوافق مع توجه المشرع الجزائري الذي نص على الوقاية من الجريمة الإلكترونية قبل المكافحة في أحكام القانون رقم 09-04 لسنة 2009.

[1] ميرفت محمد حبايب، المرجع السابق، ص156

خلاصة الفصل الثاني

تناولنا في هذا الفصل جوانب الردع والحماية من جرائم النصب والاحتيال الإلكتروني، حيث اتضح أن المشرع قد أقر عقوبات أصلية تمثلت في الحبس والغرامات المالية بهدف زجر مرتكبي هذه الجرائم، بالإضافة إلى عقوبات تكميلية، مثل مصادرة الأدوات المستخدمة في ارتكاب الجريمة أو المنع من مزاولة بعض الأنشطة، وذلك لتعزيز فعالية الردع، كما تم اعتماد مجموعة من الوسائل الوقائية لمكافحة هذه الظاهرة، منها ما هو تقني وإداري، كتعزيز نظم الأمن السيبراني وتحسين إجراءات التحقق من الهوية، ومنها ما هو إعلامي وقانوني، كتنظيم حملات توعوية وتحديث الإطار التشريعي بما يواكب تطورات الجريمة الإلكترونية، وذلك في محاولة لبناء بيئة رقمية آمنة وتعزيز ثقة المستخدمين بها.

الخاتمة

خاتمة

ختاما، من خلال دراسة موضوع جريمة الاحتيال الإلكتروني ومدى خطورتها على المستوى العالمي، تكمن خطورتها في كونها عابرة للحدود والقارات، مما يمنحها خصوصية تميزها عن الجرائم التقليدية ويزيد من تعقيدها، لاسيما وأن الجاني يتمكن من التحكم بالفعل الإجرامي عن بُعد، مُلحقًا الضرر بالمجني عليه بخبرة عالية، مما يجعل مواجهته عملية معقدة تتطلب كفاءات تقنية متقدمة.

كما بيّنت الدراسة تعريف جريمة الاحتيال الإلكتروني، وطبيعتها، وأبرز سماتها، وتبين من خلال ذلك أنها تعتمد على أدوات ومكونات مغايرة لما هو سائد في الجريمة التقليدية، إذ تحتاج إلى وسائل خاصة لتحقق وجودها وتكتمل أركانها. كما أن مرتكبها يتسم بخصائص محددة تختلف نسبيًا عن المجرم التقليدي.

استعرضت الدراسة ايضا إجراءات التحقيق لفحص كافة الأدلة الالكترونية، مع تسليط الضوء على الصعوبات التي تواجه أعضاء النيابة العامة وضباط الشرطة القضائية والخبراء التقنيين وهذا بهدف الخروج بآليات الوقاية من جريمة الاحتيال الإلكتروني، كوسائل تقنية تتمثل في حماية برامج المعلومات وأنظمة الحوسبة من الاختراق والاحتيال المعلوماتي، وأساليب وقائية عبر نشر التوعية بمخاطر لهذه الجريمة قبل وقوعها، وذلك من خلال مؤسسات الدولة ومنظمات القطاع المدني، مما يُعد آلية وقائية فعالة لتجنب التعرض لمثل هذه الجرائم.

وبناء على ما تقدم، توصلنا من خلال هذه الدراسة الى مجموعة من النتائج نعرضها فيما يلي:

لا تزال النصوص القانونية الجزائرية بحاجة إلى مزيد من الدقة والشمولية، بما يمكنها من مواكبة الطابع المتجدد والمتطور للجرائم الإلكترونية.

.النصوص القانونية والأحكام الخاصة المتعلقة بالجريمة الإلكترونية غير كافية وتتطلب تعزيزًا.

.وسائل الوقاية الحالية، خاصة التقنية والإعلامية، غير مفعّلة بالقدر الكافي، مما يحد من أثرها الوقائي.

. تتميز جريمة الاحتيال الإلكتروني بطبيعة مزدوجة: فهي تقليدية من حيث المصلحة المعتدى عليها (المال)، ولكنها حديثة كليًا من حيث أسلوب ارتكابها الذي ارتبط بالتقنية العالية والتكنولوجيا الحديثة.

. الأساليب الإجرامية التي يستعملها الجناة تتمثل في الوسائل التي وفرتها لهم التقنية المتطورة، سواء لارتكاب الجريمة أو لمحاولة الإفلات من عواقبها، وهي أساليب عديدة ومتنوعة تتطور باستمرار وبسرعة فائقة.

. الوسائل الاحتيالية والخداع لم تعد تتم فقط في مواجهة المجني عليه الإنسان لإعدام إرادته، بل يمكن أن تتم في مواجهة الآلة (سواء الحاسوب أو الصراف الآلي)، على اعتبار أن هذه الآلة مجرد وسيط يعبّر عن إرادة المجني عليه الذي يقوم ببرمجتها؛ وبالتالي فإن خداع الحاسوب يعتبر خداعًا لذلك الشخص.

. بالمقارنة بين الأثر المترتب على الاحتيال التقليدي والاحتيال الإلكتروني، نجد الفرق واسعًا وشاسعًا، إذ يستولي الجاني في الجريمة الإلكترونية على أموال طائلة تفوق بكثير تلك التي يستولي عليها في الجريمة التقليدية وبأقل جهد، مما يدفع إلى القول إن العقوبة المقررة للجريمة التقليدية لا تتناسب مع الأثر الذي تخلّفه الجريمة الإلكترونية.

. الأضرار المادية الناتجة عن الاحتيال الإلكتروني تفوق بكثير الأضرار الناجمة عن الاحتيال التقليدي، إذ لا تتمثل فقط في سلب مال المجني عليه، بل تؤدي أيضًا إلى زحزحة الثقة في التعاملات المصرفية والمالية.

. اثبات الدليل الإلكتروني: توجد صعوبة تكتنف قبول القاضي الجزائي للدليل الإلكتروني كدليل إثبات، نظرًا لطبيعته الخاصة وطريقة الحصول عليه المعقدة، مما يثير الشك حوله. ورغم ذلك، يبقى الدليل الإلكتروني خاضعًا لسلطة القاضي التقديرية، فيمكنه قبوله والاقتناع به إذا كان مشروعًا، كما يمكن له استبعاده.

. التعاون الدولي: باعتبار جريمة الاحتيال الإلكتروني جريمة عابرة للحدود، فإنها تتطلب تعزيز التعاون الدولي. فإجراءات البحث والتحري تواجه إشكالات في مجال التفتيش والاختصاص القضائي بسبب ضعف التعاون الدولي، واختلاف النظم القانونية الإجرائية، وعدم وجود معاهدات ثنائية أو جماعية، وانعدام قنوات اتصال بين الدول.

. يُعد ضحايا جريمة الاحتيال الإلكتروني من الأسباب الأساسية التي تصعّب اكتشافها، إذ يحجم بعضهم عن التبليغ عنها بمجرد وقوعها، وذلك لخوفهم من عواقب التحريات التي قد تكشف خبايا قضايا مالية أخرى، أو خوفًا من فقدان ثقة الزبائن (خاصة في المؤسسات المالية والمصارف)، مما يساعد على ضياع معالم الجريمة.

. ساهمت إجراءات البحث والتحري المستحدثة بموجب القانون 04-09 (المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها)، إلى جانب إجراءات البحث والتحقيق المنصوص عليها في قانون الإجراءات الجزائية، في الإحاطة إجرائيًا بجوانب جريمة الاحتيال الإلكتروني.

وعلى ضوء هذه النتائج التي توصلنا اليها، قمنا بتحرير بعض التوصيات:

تدخّل المشرع الجزائري بالنص صراحةً على جريمة الاحتيال الإلكتروني باعتبارها جريمة قائمة بذاتها، مختلفة عن جريمة الاحتيال التقليدي، على أن يكون هذا النص شاملاً لكل الأركان القانونية لها، مع تحديد دقيق للأساليب التي تتم بها، بحيث لا يترك مجالاً للقاضي الجزائي للتفسير والقياس على نص المادة 372 من قانون العقوبات.

النص صراحةً وعلى سبيل الحصر على الوسائل التقنية والفنية التي تُستعمل لاستخلاص الدليل الإلكتروني أو للتأكد من سلامته من العبث، باعتبارها شرطًا لقبول هذا الدليل، وذلك وفق جدول أو لائحة يتولى إعدادها خبراء فنيون ومختصون.

ضرورة النص صراحة على الأدلة الإلكترونية كأدلة إثبات في المجال الجزائي، والاعتراف لها بحجية قاطعة من حيث مضمونها، كاستثناء على سلطة القاضي الجزائي في تقدير الدليل (كما فعل المشرع الجزائري بخصوص جريمة الزنا وجريمة السياقة في حالة السكر).

إفراد نص قانوني ينص صراحة على التقادم في جريمة الاحتيال الإلكتروني، ويقضي ببدء سريان آجال التقادم فيها من يوم اكتشافها (كما هو الحال في جريمة التزوير)، وليس من يوم ارتكابها كما تنص القواعد الجزائية العامة. ذلك لأن هذه الجرائم تكتشف بعد مدة طويلة من تاريخ ارتكابها، مما يلحقها التقادم ويفوّت على المجتمع حقه في متابعة الجاني، وعلى الضحية حقه في جبر الضرر.

العمل على الاقتداء بالدول المتقدمة والتعاون معها في مجال التكنولوجيا، والاستفادة من خبرتها في تشريع القوانين التي تعالج جريمة الاحتيال الإلكتروني، إذ لا يمكن لأي دولة النجاح في مواجهة هذا النمط من الجرائم بمفردها، وتبادل وحفظ المعلومات، وتدريب أجهزة العدالة، وفقًا لما نصت عليه العديد من الاتفاقيات الدولية.

الاهتمام بتدريب المحققين والقضاة على التعامل مع جريمة الاحتيال الإلكتروني باعتبارها جريمة مستحدثة ذات طبيعة فنية وعلمية معقدة وتكوين قضاة يتخصصون ويتفرغون للنظر والفصل فقط في هذا النوع من الجرائم، باعتبارها جريمة ذات نوع ونمط خاص

تشكيل جهاز يتكون من فريق من الخبراء الفنيين في مجال التكنولوجيا والتقنية العالية، مهمتهم مساعدة الضبطية القضائية وجهات التحقيق في قضايا جريمة الاحتيال الإلكتروني.

إنشاء محكمة خاصة بالجرائم المعلوماتية، يتولى تسييرها سلك قضائي خاضع لخبرة وتدريب فعال في مجال مكافحة الجرائم المعلوماتية، مع الاستعانة بخبراء أمن المعلومات.

قيام الدولة (ممثلة بمؤسساتها التعليمية والقانونية والإعلامية) بتحذير مواطنيها والمؤسسات المالية المختلفة من خطورة هذه الجريمة، وإرشادهم وتعليمهم ضرورة اتخاذ كافة الاحتياطات اللازمة لضمان عدم وقوعهم ضحايا.

توعية الضحايا بضرورة المسارعة إلى التبليغ عن الجريمة حال وقوعها، لتسنى للضبطية القضائية والمحققين التدخل السريع قبل طمس معالم الجريمة وهروب الجاني.

استحداث نصوص قانونية جديدة تكون أكثر صرامة وفاعلية مقارنة بالنصوص التقليدية، من خلال التشديد في العقوبات المقررة لمرتكبي جرائم الاحتيال الإلكتروني وغيرها من جرائم التكنولوجيا الحديثة، وذلك للتقليل من هذه الجرائم.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

I. المصادر

أولا: القران الكريم

-1القران الكريم،سورة النساء،ج 5،الاية 25.

ثانيا: القوانين والمراسيم

-1الأمر رقم 66-155 المؤرخ في 1966/06/08 المتعلق بقانون العقوبات المعدل والمتمم, الجريدة الرسمية, العدد 47 المؤرخ في 11 /1966/06

-2القانون رقم 14-25مؤرخ في 9 صفر عام 1447المافق ل 8 غشت سنة 2025.

-3المادة 14/أ من قانون رقم (04.09) ، لسنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

ثالثا: القواميس والمعاجم

1- ابن منظور، لسان العرب المحيط، الجزء الأول، دار اللسان العربي، بيروت،2000.

II. المراجع

أولا: الكتب

1-خالد علي سليمان عبد الله، جريمة الاحتيال باستخدام وسائل تقني المعلومات في التشريع المقارن، دار الجامعة الجديدة، الإسكندرية،2021

2-محمد بن ابي بكر الرازي،دار الكتاب العربي،بيروت،2001

3-الفيل علي عدنان، الإجرام الإلكتروني دراسة مقارنة، مكتبة زين الحقوقية، ط1، العراق، 2011،

4-سامر سلمان الجبوري ،جريمة الاحتيال الالكتروني دراسة مقارنة،مكتبة زين الحقوقية،ط1،بغداد 2018

5-محمد محرم علي، جريمة النصب والاحتيال والتجارة الإلكترونية، دار النهضة العربية، القاهرة،1998

6-علي حسن الطوالبة، الجرائم الالكترونية ، مؤسسة فخراوي للدراسات والنشر البحرين، ط 2، البحرين، 2009

7-رؤوف عبيد، مبادئ علم الاجرام العقاب، دار الفكر العربي،القاهرة،مصر ،2004

8-محمد علي السالم عياد الحلبي ، "الجرائم الواقعة على الأموال في القانون المقارن "، دار الوراق، ط1، عمان،2010

9-عبد القادر الشيخلي، جريمة الاحتيال في قوانين عقوبات الدول العربية، منشورات الحلبي الحقوقية، ط1، لبنان، 2009

10-سعدي حيدرة، الجرائم ضد الأشخاص والأموال، القسم الخاص بين النص والواقع، ألفا للوثائق ، ط1، 2021

11-محمد عبد الرحمن عنانزه ،القصد الجرمي في الجرائم الالكترونية ،دار الأيام للنشر والتوزيع ،ط1 ، الأردن،2017

12- نهلا عبدالقادر المؤمني، الجرائم المعلوماتية، ماجستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع, ط1،عمان ،2008

13-الطاهر ياكر الجرائم الإلكترونية، الأحكام الموضوعية والإجرائية، دراسة مقارنة، دار بلقيس ،الجزائر، 2024

14-سيد على السيد محمد، الجرائم الإلكترونية ماهيتها صورها، دار التعليم الجامعي، الإسكندرية ،2024

15-ميرفت محمد حبايبه، مكافحة الجريمة الإلكترونية دراسة مقارنة في التشريع الجزائري، دار اليازوري العلمية، عمان، 2023

16-عبد العزيز سعد، جرائم الاعتداء على الأموال العامة والخاصة، دار هومة، ط4، الجزائر،2007

17-أسامة حمدان، الرقب، جرائم النصب والاحتيال، (الأساليب، المظاهر، العلاج) ، دار يافا العلمية للنشر والتوزيع،ط1،عمان،2012

18-عبدالله سيف الكيتوب ،الأحكام الإجرائية جريمة الاحتيال المعلوماتي ،ط 1 ،دار النهضة العربية ،القاهرة،2013

19-حنان ريحان المبارك المضحكي، الجرائم المعلوماتية (دراسة مقارنة)، منشورات الحلبي الحقوقية، ط1، لبنان،2014

20-أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص الجرائم ضد الأشخاص و الأموال ، دار هومة،الجزائر ،ط 21،2024،

21-نبيل صقر، الوسيط في شرح جرائم الأموال، دار الهدى، الجزائر،2012

22-علي القهوجي، شرح قانون العقوبات، دار النهضة العربية، القاهرة، 1993م

23-احمد محمد مصطفى، جرائم الحاسبات الالية في التشريع المصري، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010

24-محمد طارق الخن، جريمة الاحتيال الالكتروني عبر الانترنت، الاحكام الموضوعية والاحكام الإجرائية، منشورات الحلبي الحقوقية، ط1، بيروت ،2011

25-جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة، عمان، 2010

26-بلال امين زين الدين، جرائم نظم المعالجة الالية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي،ط1، الإسكندرية، 2008

27-محمود نجيب حسني، شرح قانون العقوبات، دار النهضة العربية، القاهرة، مصر،1988

28-سليمان عبد المنعم، النظرية العامة لقانون العقوبات، دار المطبوعات الجامعية، الإسكندرية، مصر،2014

30-بدوي حنا، الاحتيال، زين الحقوقية والأدبية، ط2، بيروت، 2003

31-حاتم عبد الرحمان منصور شحات، الاجرام المعلوماتي،دار النهضة العربية، ط، 1 القاهرة، 2002

32-أشرف توفيق شمس الدين، "شرح قانون العقويات "النظرية العامة للجريمة والعقوبة"، دار النهضة العربية، القاهرة، 2009

33-أمير فرج يوسف، الاثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، مكتبة الوفاء القانونية، ط1،الإسكندرية، 2016

34-اطوني عيسى، التنظيم القانوني لشبكة الانترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، ط1،2001

35-اندي اوبل، كشف اسرار قواعد البيانات،الدار العربية للعلوم،ط1 ،لبنان،2014

36-ياسر محمد الكومي أبو حطب، الحماية الجنائية والأمنية للتوقيع الالكتروني، الإسكندرية، منشأة معارف بلال حزي وشركاؤه، 2014

37-محمد عبيد الكعيبي، الجرائم الناشئة عن الاستخدام الغير مشروع بشبكة الانترنت، دار النهضة العربية، ط2،2009

38-فتوح الشاذلي، "جرائم الكمبيوتر"، منشورات الحلبي، 2003م

ثانيا: المقالات العلمية

1-سويح دنيا زاد، بولحية شهيرة، الاحتيال الالكتروني ،مجلة الدراسات القانونية والاقتصادية، المركز الجامعي بريكة ، العدد،04, 2019.

2-حسن كليبي، نجمة الطيب، جريمة النصب الالكتروني من منظور المشرع الجزائري، مجلة المفكر، المجلد 20، العدد1، السنة 2025

3-راضية عيمور، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية العدد الأول، المجلد السادس ، السنة 2022.

4-عمري عبد القادر، جريمة السرقة بين الشريعة والتشريع الجزائري، مجلة الدراسات القانونية، مجلد3، عدد 01، جامعة 2، لمدية، الجزائر، 2017.

5-فاطمة الزهراء رمضاني، علي بدرائي، القصور التشريعي في مجال الجريمة المعلوماتية في التشريعين المغربي والجزائري، جلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة المسيلة، الجزائر، العدد 02 ،المجلد07، 2022.

6-عبان عميروش، التنظيم القانوني للتشفير كآلية للتصديق الالكتروني في التشريع الجزائري والتشريعات المقارنة، المجلد 07، لعدد 01، جوان2022

7-بوعقل مصطفى، اونان بومدين، مباركي سمراء، اليات وقاية المعاملات الالكترونية في ظل حكومة تكنولوجيا المعلومات les cahiers du mecas، جامعة الجيلالي ليابس، سيدي بلعباس، العدد12، جوان 2016.

8-ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة دراسات وأبحاث، الجلفة، العدد 1 ، 2009.

9-جمل عبد اللطيف وطرايش عبد الغني، الحماية الجنائية للمستهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري دراسة لتحليلية ومقارنة في ضوء القانون الفرنسي، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة الأغواط، المجلد 9، لعدد 1، 2025.

10-عزالدين غبش، حماية المستهلك الالكتروني في ظل الجرائم السيبرانية، المجلة الدولية للتحولات القانونية والسياسية، المجلد 1، العدد 1 , 2022

ثالثا :الأطروحات والرسائل الجامعية

1-قراوي كلثوم جريمة الاحتيال الإلكتروني، اطروحة لنيل شهادة دكتوراه علوم في القانون العام، تخصص قانون جنائي وعلوم بنائية، كلية الحقوق، جامعة الجزائر2024-2025.

2-حفيظة رفاس، دور السياسة الجنائية للمشرع الجزائري في مكافحة الجرائم التكنولوجيا الحديثة، مذكرة تخرج لنيل شهادة الدكتوراه، قسم القانون العام، جامعة الدكتور الطاهر مولاي، سعيدة، الجزائر، 2019.

3-بوزكري جيلالي، الإدارة الالكترونية في المؤسسات الجزائرية واقع وافاق، أطروحة دكتوراه علوم في التسيير، تخصص إدارة أعمال والتسويق، قسم علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 3، الجزائر،2015 -2016.

4-بن نعوم خالد، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، ب، كلية الحقوق، لقسم الخاص، جامعة عبد الحميد بن باديس، مستغانم،2019-2018.

5-صلجة خلود، شبل مروى، جريمة الاحتيال الإلكتروني بتشريع جزائري، مذكرة مكملة لنيل شهادة الماستر تخصص قانون جنائي و علوم جنائية، جامعة سكيكدة 2025-2024.

6-غليلة الحسين، معاوي عبد الناصر، الابتزاز الإلكتروني، مذكرة لنيل شهادة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسة، جامعة 20اوت1965، سكيكدة ،2024

7-أبو بكر تيتاوي، إلياس مالك قرادي، جرائم النصب والاحتيال الإلكتروني في التشريع الجزائري، مذكرة التخرج لنيل شهادة ماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، جامعة إليزي، سنة 2025-2024.

رابعا: الملتقيات والندوات العلمية

1-علي ابراهيم بن دارج، محاضرات في الجرائم المعلوماتية، كلية الحقوق والعلوم السياسية، المركز الجامعي أفلو، الاغواط، 2021.

خامسا: المراجع الأجنبية

1- Mamene Besma, "Images and Manifestations of Electronic Fraud on Persons and Funds through Digital Data," Law, Society and Authority Journal, Vol. 14, No. 1, 2025

2- Meriem Abdelkafi Souraya Bourbabas "Information Fraud Crime on Electronic Financial Cards" ‹Journal of Law and Political Sciences: vol. 8‹ no. 1‹ Algeria•2022• p. 406.

الفهرس

الفهرس

مقدمة .....أ–د

الفصل الأول الإطار المفاهيمي لجريمة الاحتيال الالكتروني.....6

المبحث الأول: مفهوم جريمة الاحتيال الإلكتروني.....6

المطلب الأول: تعريف جريمة الاحتيال الالكتروني.....7

الفرع الاول: التعريف اللغوي/الاصطلاحي.....7

الفرع الثاني: تعريف الجريمة الالكترونية.....10

المطلب الثاني: خصائص جريمة الاحتيال الالكتروني وتمييزها عما يشابهها من الجرائم..12

الفرع الأول: خصائص جريمة الاحتيال الالكتروني.....12

الفرع الثاني: تمييز جريمة الاحتيال عن غيرها من الجرائم.....17

المطلب الثالث: صور واساليب جريمة الاحتيال الإلكتروني.....20

الفرع الأول: صور الاحتيال الإلكتروني 21

الفرع الثاني: أساليب الاحتيال الإلكتروني.....24

المبحث الثاني: أركان جريمة الاحتيال..... 26

المطلب الأول: الركن الشرعي لجريمة الاحتيال الإلكتروني.....26

الفرع الأول: القاعدة العامة للركن الشرعي.....26

الفرع الثاني: قاعدة التجريم والعقاب لجريمة الاحتيال الالكتروني في التشريع الجزائري....29

المطلب الثاني: الركن المادي لجريمة الاحتيال الإلكتروني.....32

الفرع الأول: ماهية الركن المادي.....32

الفرع الثاني: تحقق الركن المادي لجريمة الاحتيال الإلكتروني.....36

المطلب الثالث: الركن المعنوي لجريمة الاحتيال الإلكتروني.....42
الفرع الأول: ماهية الركن المعنوي للجريمة.....42
الفرع الثاني: القصد الجنائي.....43
الفرع الثالث: تحقق الركن المعنوي في جريمة الاحتيال الإلكتروني.....45
خلاصة الفصل الأول.....47
الفصل الثاني إجراءات التحقيق في جريمة الاحتيال الالكتروني ووسائل الوقاية منها.....49
المبحث الأول: إجراءات التحقيق في جريمة الاحتيال الالكتروني والعقوبات المقررة لها...50
المطلب الأول: إجراءات التحقيق في جريمة الاحتيال الالكتروني.....50
الفرع الأول: إجراءات المعاينة والتفتيش 50
الفرع الثاني: إجراءات الضبط والتنصت والمراقبة الالكترونية.....55
المطلب الثاني: العقوبات المقررة لجريمة الاحتيال الالكتروني.....58
الفرع الأول: العقوبات الأصلية.....58
الفرع الثاني: العقوبات التكميلية..... 60
المبحث الثاني: وسائل الوقاية من جريمة الاحتيال الالكتروني.....62
المطلب الأول: الطرق التقنية المتبعة للوقاية من الجريمة الالكترونية.....62
الفرع الأول: الوسائل التقنية 62
الفرع الثاني: الوسائل الادارية 69
المطلب الثاني: طرق التوعية الوقائية لجريمة الاحتيال الالكتروني.....71
الفرع الأول: دور مؤسسات الدولة في العمل على التوعية للوقاية من الجريمة.....71

الفرع الثاني: دور أجهزة الدولة والمؤسسات للوقاية من الجريمة.....78
خلاصة الفصل الثاني.....85
خاتمة.....87
قائمة المصادر والمراجع.....92

الملخص: تناولت الدراسة تحليلاً قانونياً لجريمة الاحتيال بوصفها من أهم الجرائم الواقعة على الأموال وفق المادة 372 من قانون العقوبات الجزائري، التي حصرت وسائل التدليس في اتخاذ اسم أو صفة كاذبة أو استعمال مناورات احتيالية بقصد الاستيلاء على مال الغير، مرتكزة على علاقة سببية بين فعل الخداع والضرر اللاحق بالمجني عليه، وتُعد جنحة عقوبتها الحبس من سنة إلى خمس سنوات وغرامة من 20.000 إلى 100.000 دج مع إمكانية التشديد بظرفين. كما تم الربط بين انتشار الجرائم المستحدثة وتطور الإنترنت، مما أفرز جريمة الاحتيال الإلكتروني التي تعتمد على الخداع باستعمال تقنيات الشبكة المعلوماتية، وهدفت الدراسة إلى توضيح الإطارين المفاهيمي والقانوني للجريمة وآليات الوقاية منها بالأمن المعلوماتي والإعلام التوعوي، معتمدة المنهج الوصفي في ظل القانون الجزائري.

الكلمات المفتاحية: احتيال الكتروني، الرقمنة، قانون العقوبات، الحماية،

Abstract: The study presented a legal analysis of the crime of fraud as one of the most significant offenses against property under Article 372 of the Algerian Penal Code, which limits the means of deception to assuming a false name or status, or using fraudulent maneuvers with the intent to seize another's property. It is based on a causal relationship between the deceptive act and the harm suffered by the victim. This offense is classified as a misdemeanor, punishable by imprisonment of one to five years and a fine of 20,000 to 100,000 Algerian Dinars, with the possibility of aggravating circumstances under two conditions. The study also established a link between the rise of emerging crimes and the development of the internet, giving rise to the crime of cyber fraud, which relies on deception using information network technologies. The study aimed to clarify the conceptual and legal frameworks of the crime, as well as prevention mechanisms through information security and awareness campaigns, adopting a descriptive approach within the context of Algerian law.

Keywords : Cyber fraud, digitization, penal code, protection.