وزارة التعليم العالي و البحث العلمي

جـــــــــامـــــعة أكلي محند اولحاج- البويرة

كلية الحقوق و العلوم السياسية

قسم القانون العام

جريمة الاحتيال باستخدام وسائل تقنية المعلومات

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر

تخصص قانون جنائي و علوم جنائية

إعداد الطالبيتين :

_العمري ريمة أنفال

_بكيري مروى

إشراف الأستاذ:

_يحياوي فاتح

لجنة المناقشة

الأستاذ يحياوي فاتح.....مشرفا

الأستاذ خيليفي سمير .....رئيسا

الأستاذ بوديسة كريم.....ممتحنا

السنة الجامعية : 2025/2024

الإهداء

الحمد لله الذي بنعمته تتمّ الصالحات،

له الحمد أولًا وآخرًا، ظاهرًا وباطنًا، فما كان لهذا العمل أن يكتمل لولا توفيقه وعونه سبحانه.

إلى نفسي،

التي صبرت وثابرت، وسهرت الليالي لتبلغ هذا المنجز، شكرًا لي على الإصرار، وعلى الاستمرار رغم كل ما كان.

إلى من كانوا بعد الله عوني وسندي،

إلى عائلتي الكريمة، أمي و أبي، أسأل الله أن يطيل في أعمارهم بالصحة والعافية، ويرزقهم السعادة والرضا في الدنيا والآخرة، فبرّهم دعامة نجاحي.

إلى إخوتي الأحبّاء: سارة، رضا، دينا، علاء ،سيلينا، ليليا،... أنتم النبع الذي لا ينضب من الحب والدعم.

وفلّتاي الصغيرتين: ميلا ورنيم، أنتن البهجة التي تزيّن عالمي.

إلى أصدقائي الأعزاء الذين شاركوني لحظات التحدي والنجاح،

إلى إشراق و ياسمين

شكرًا لقلوبكم النقية، ولكلماتكم التي منحتني القوة في كل حين.

وإلى صديقتي وزميلتي في البحث، مروى،

رفيقة الدرب العلمي، أسأل الله أن يوفقك ويسدد خطاك، وأن يكلل جهودك بالنجاح والتوفيق في كل مسيرتك.

لكم جميعًا أُهدي هذا العمل، عربون شكر وامتنان لا ينتهي.

أنفال

الإهداء

اللهم لك الحمد والشكر كما ينبغي لجلال وجهك وعظيم سلطانك

الحمد لله، والصلاة والسلام على رسول الله ﷺ.

إلى من كانوا النبع الأول لكل حبٍّ وعطاء...

إلى نبض القلب ودفء الروح يا من كنتِ الحضن الذي لا ينكسر في وجه العواصف، والصدر الذي أظل عليه مهما كانت الحياة قاسية.

شكراً لكِ على كل لحظة حب لم تقاس، على كل تضحية لم ترى، وعلى صبرك الذي لا يقال وعلى كل دعاء صادق رافقني في دربي، ولحنانك الذي لا مثيل له.

"امي الغالية حفظك الله و اطال في عمرك"

الى سندي الأول، وضلعي الثابت... القدوة التي مضيت على أثرها، إليك يا من كان وجودك أمانًا، وصمتك دعمًا، ونظراتك تشجيعًا دون كلمات...

شكراً لثقتك التي منحتني القوة ولحضورك الثابت في كل خطواتي ، كل لحظة إنجاز تحمل من ظلك الكثير.

"ابي الغالي حفظك الله و اطال في عمرك"

إلى إخوتي وكافة عائلتي الصغيرة منها والكبيرة.

إلى صديقاتي العزيزات، إشراق وياسمين، كنتما الحضور الأجمل في الرحلة، بضحكتكما، بدعمكما، وبأثرٍ لا يُنسى في أيام التعب، نهاد وسيلين رفيقتَي الزمن الجميل رغم أن الجامعة لم تجمعنا، الا ان ذكراكما في قلبي دائمًا حاضرة، و إلى صديقتي وزميلتي في هذه المذكرة أنفال، لك شكر خاص لا يكفيه الكلام... كنتِ العون في التفاصيل، والسند في لحظات التوتر، والرفيقة في كل مرحلة من هذا الطريق، هذا العمل يحمل جزءًا من جهدك و روحك الجميلة.

إليكم جميعًا... أهديكم ثمرة هذا الجهد، فبكم كان الانجاز.

مروى

شكر و تقدير

قال رسول الله صلى الله عليه وسلم: "من لا يشكر الناس، لا يشكر الله عز وجل."

الحمد لله الذي تتم بنعمته الصالحات، وبتوفيقه تُنجز الأعمال وتُدرك الغايات. نحمده سبحانه على ما منّ به علينا من عون وتيسير، حتى تمكنا من إنجاز هذا العمل.

نتوجّه بخالص عبارات الشكر والتقدير إلى الأستاذ المشرف الدكتور يحياوي فاتح، لما قدّمه لنا من توجيهات وملاحظات ساهمت في إنجاز هذه الدراسة.

كما نعبّر عن امتناننا للأستاذ الدكتور سمير خيليفي على دعمه وتعاونه الذي كان محل تقدير منا.

ولا يفوتنا أن نشكر أساتذة قسم الحقوق، وأعضاء لجنة المناقشة الكرام، وعائلاتنا الكريمة، وكل من قدّم لنا يد العون والمساندة، من قريب أو بعيد، خلال مختلف مراحل هذا البحث.

مـــقدمة

مقدمة :

مرت جريمة الاحتيال بتحولات جوهرية عبر مختلف العصور، إذ لم تكن لها في بداياتها معالجة قانونية مستقلة، بل كانت تندرج ضمن صور الاستيلاء على أموال الغير كالسرقة وخيانة الأمانة والتزوير، ومع التحولات الاقتصادية والاجتماعية التي عرفتها أوروبا، ولا سيما عقب الثورة الفرنسية، برزت الحاجة إلى الإعتراف بهذه الجريمة ككيان مستقل، ما أدى إلى إدراجها في التشريعات الوضعية، وتحديد أركانها وعقوباتها بوضوح، ويُعد ظهور مصطلح "الطرق الاحتيالية" في المادة 224 من قانون العقوبات الفرنسي نقطة تحول أساسية، إذ جاء بديلاً لمفهوم "التدليس"، ليكرس التوجه نحو ضبط قانوني خاص بهذه الجريمة.

ومع مطلع الألفية، شهدت جريمة الِاحتيال قفزة نوعية نتيجة الطفرة التكنولوجية وظهور الإنترنت والإعلام الآلي، مما مكّن الجناة من تنفيذ عملياتهم بوسائل متطورة يصعب تتبعها، فقد وفّرت بيئة الفضاء الرقمي إمكانات واسعة لنقل البيانات وتداول المعلومات بسرعة، لكن في الوقت ذاته، أتاحت فرصًا جديدة لِارتكاب أفعال إجرامية أكثر تعقيدًا، في مقدمتها الِاحتيال بِاستخدام وسائل تقنية المعلومات، الذي أضحى من أكثر الجرائم شيوعًا وخطورة في العصر الرقمي.

حيث شهد مؤشر هذا النوع من الجرائم في الجزائر ارتفاعًا ملحوظًا خلال السنوات الأخيرة، وهو ما تؤكده الإحصائيات الرسمية الصادرة عن المديرية العامة للأمن الوطني وقيادة الدرك الوطني، حيث تجاوز عدد هذه الجرائم في سنة 2024 ما يفوق 1300 قضية، مقارنة بـ1100 قضية سنة 2023، مما يمثل ارتفاعًا بنسبة تقارب 113% منذ سنة 2022، وتعكس هذه الأرقام تنامي ظاهرة الِاحتيال المعلوماتي، التي تنفذها شبكات إجرامية متخصصة تستغل وسائل تقنية المعلومات الحديثة لِاختراق الحسابات البريدية والبنكية وسرقة مبالغ مالية معتبرة بطرق احتيالية

لا تتطلب سوى "نقرة زر واحدة[1]" ، يعتمد مرتكبوه غالبًا على مهارات عالية في البرمجة أو الاختراق، ما يجعلهم قادرين على التلاعب بالبيانات الرقمية وتحقيق مكاسب مالية دون ترك أثر واضح، وتتنوع أساليبه بين استغلال البريد الإلكتروني، وتطوير البرمجيات الخبيثة، واختراق الحسابات البنكية، وصولًا إلى انتحال الصفات وتزوير المعطيات الشخصية على منصات الدفع الإلكتروني ووسائل التواصل ، لتنفيذ عمليات الاحتيال عن بعد ، وفي ظل فوضى التجارة الإلكترونية وغياب الرقابة على الإعلانات المشبوهة المنتشرة عبر المواقع، أصبح العديد من المواطنين عرضة لهذه الأساليب الإجرامية، ما يعكس محدودية الوعي الرقمي لدى فئة واسعة من المتعاملين مع الفضاء الافتراضي.

أمام هذا الواقع، أضحت الجرائم المعلوماتية، وعلى رأسها الاحتيال باستخدام وسائل تقنية المعلومات، تمثل تهديدًا حقيقيًا لأمن الأفراد والمؤسسات، سواء من حيث المساس بالمعاملات المالية، أو انتهاك خصوصية البيانات، أو زعزعة الثقة في البيئة الرقمية، من هنا تبرز الحاجة إلى معالجة هذه الظاهرة في ظل ما تطرحه من إشكالات قانونية وإجرائية، سواء على مستوى تحديد مفاهيمها وأركانها، أو من حيث فعالية الوسائل المعتمدة لمكافحتها، في سياق سعي المشرّع إلى تحقيق التوازن بين حماية المجتمع والحفاظ على الحقوق الرقمية.

وبناءً على ما سبق، أصبحت هذه الجريمة جديرة بالبحث والدراسة، بما يسمح بإحاطة شاملة بأبعادها، وتحليل سبل مواجهتها القانونية والإجرائية، انطلاقًا من منظور تشريعي يعكس التحديات التي تفرضها البيئة المعلوماتية الحديثة.

[1] قناة النهار تي في، "نصب واحتيال على مواقع التواصل.. مواطنون يقعون في فخ المحتالين إلكترونيًا"، YouTube [فيديو]، نُشر في 17 ماي 2025، متاح عبر: https://youtu.be/uzczBOU9idM

1. أهمية الدراسة :

من خلال الأبحاث الأكاديمية التي نقوم بها، نهدف إلى تسليط الضوء على القضايا القانونية المعقدة التي تحتاج إلى استقصاء دقيق وتحليل عميق وتفسير شامل، وذلك بهدف توعية الجمهور ولفت انتباهه إلى القضايا المهمة ، ومن أبرز هذه القضايا جريمة الاحتيال باستخدام وسائل تقنية المعلومات بشكل أساسي وتتمثل أهمية هذه الدراسة في:

- تسليط الضوء على الجريمة المستحدثة المتمثلة في الاحتيال باستخدام وسائل تقنية المعلومات في ضوء التشريع الجزائري، ودراسة مدى تغطية النصوص القانونية لهذا النوع من الجرائم.
- مناقشة المفاهيم القانونية المتعلقة بالجرائم المعلوماتية وربطها بالأحكام القانونية الخاصة بالإجراءات، مع التركيز على عملية التحصيل والاستقصاء في مجال الإثبات.
- دراسة العوائق والتحديات التي تواجه السلطات المعنية في مكافحة هذه الجرائم، والعمل على فهم طبيعتها وتعقيداتها لإيجاد الحلول المناسبة لمكافحتها.

2. أسباب اختيار الموضوع :

أ.الأسباب الذاتية :

- الرغبة في المساهمة في رفع الوعي المجتمعي بمخاطر الاحتيال المعلوماتي، والتنبيه إلى آثاره السلبية المتزايدة في ظل تنامي استخدام وسائل تقنية المعلومات.
- الاهتمام الشخصي بالقضايا الجنائية، باعتبارها مجال تخصصنا.

ب.الأسباب الموضوعية:

- انتشار الجرائم المعلوماتية بشكل كبير، مما يجعلها تهدد الأمن على المستويين الوطني والدولي، خاصة من الناحية الاقتصادية.
- استكشاف الثغرات والجوانب الخفية التي تميز هذه الجريمة وفهم خصائصها بشكل دقيق.
- حداثة الموضوع وأبعاده الخطيرة جعلاه موضوعًا مهمًا يستحق الدراسة.
- تنوع أساليب الاحتيال وتعددها، وعدم احتوائها في إطار قانوني واحد، مما استدعى دراسة هذا الموضوع بشكل مفصل وعميق.

3. أهداف الدراسة :

تسعى هذه الدراسة إلى تحقيق جملة من الأهداف المرتبطة بجريمة الاحتيال باستخدام وسائل تقنية المعلومات، ويمكن بيانها كما يلي:

- التعرف على طبيعة وأساليب جريمة الاحتيال باستخدام التكنولوجيا الحديثة والوسائل الإلكترونية، مع تسليط الضوء على التقنيات المستخدمة في تنفيذها.
- رفع الوعي لدى الأفراد والمؤسسات حول أنواع الاحتيال والتقنيات المستخدمة، بهدف الوقاية من الوقوع كضحايا لهذه الجرائم.
- دراسة الوسائل المستحدثة التي يعتمدها الجناة في ارتكاب هذه الجريمة .
- بيان صور الاحتيال باستخدام وسائل تقنية المعلومات في وسائل الدفع الإلكترونية والخدمات الرقمية.

4. المنهج المتتبع :

ركزنا في دراسة هذا الموضوع على المنهج الوصفي التحليلي و هما الأنسب لمعالجة موضوع البحث اعتمدنا فيه على المنهج الوصفي لوصف الجريمة، والتطرق لخصائصها و مميزاتها عن الجرائم الاخرى.

اتبعنا في هذه الدراسة المنهج التحليلي خاصة في الجوانب المتعلقة بالنصوص القانونية التي أقرها المشرع الجزائري، سواء في قانون العقوبات او القوانين الاخرى.

5. إشكالية الدراسة :

إشكالية الدراسة تدور حول كيفية تعامل المشرع الجزائري مع جريمة الاحتيال باستخدام وسائل تقنية المعلومات، حيث يختلف موقف التشريعات في مواجهتها، بعض التشريعات استحدثت نصوصًا قانونية خاصة بهذا النوع من الجرائم، بينما عمدت أخرى إلى تعديل هذه النصوص ، و تتمثل إشكالية هذه الدراسة في :

إلى أي مدى واصل المشرع الجزائري تحقيق فعالية مواجهة جريمة الاحتيال باستخدام وسائل تقنية المعلومات .

6. **تقسيم الدراسة** :

تم إعداد خطة البحث وفق ترتيب موضوعي ومنهجي يتيح تقديم صورة شاملة حول الموضوع، من خلال تقسيم الدراسة إلى فصلين رئيسيين تسعى هذه الخطة الثنائية إلى تناول مختلف جوانب البحث بشكل متكامل كما يلي:

في الفصل الأول المعنون بـ "الطبيعة الخاصة لجريمة الاحتيال باستخدام وسائل تقنية المعلومات".

أما الفصل الثاني المعنون ب "المواجهة الاجرائية لجريمة الاحتيال باستخدام وسائل تقنية المعلومات " .

الفصل الأول :

الطبيعة الخاصة لجريمة الاحتيال باستخدام وسائل تقنية المعلومات

تمهيد:

إن التطور التكنولوجي المتسارع فرض على المجتمعات ضرورة التكيّف مع هذه الطفرة التقنية، من خلال إدماج الوسائل الرقمية في مختلف المعاملات اليومية ، نظراً لما توفره من مزايا تظهر في تسريع الإجراءات و توفير الوقت والجهد ، غير أن هذا التقدم ورغم إيجابياته العديدة لم يخلُ من آثار سلبية ، لعل أبرزها ظهور نمط جديد من الجرائم المستحدثة التي تستند على وسائل تقنية المعلومات في تنفيذها .

وتعد جريمة الاحتيال باستخدام وسائل تقنية المعلومات أكثر صور هذه الجرائم شيوعا ، إذ تكتسي طابعاً حديثاً سواء من حيث الأسلوب الذي تُرتكب به ، أو من حيث الأهداف والنتائج المترتبة عنها ، فقد أتاح الاستخدام السلبي للتقنية الحديثة للمحتالين فرصاً واسعة لاستغلال الثغرات الرقمية وتنفيذ عمليات احتيالية بمختلف الطرق تستهدف الأفراد والمؤسسات على حد سواء .

في هذا الفصل يتم التطرق إلى تحديد الطبيعة الخاصة لجريمة الاحتيال باستخدام وسائل تقنية المعلومات من خلال التقسيم التالي :

المبحث الأول : ماهية جريمة الاحتيال باستخدام وسائل تقنية المعلومات

المبحث الثاني : صور جريمة الاحتيال باستخدام وسائل تقنية المعلومات

المبحث الأول

ماهية جريمة الاحتيال باستخدام وسائل تقنية المعلومات

لا شك في أن جرائم الاحتيال باستخدام وسائل تقنية المعلومات تُعَدّ امتدادًا لجرائم الاحتيال التقليدية المعروفة، غير أنها تختلف عنها من حيث الوسيلة المستخدمة، إذ تُرتكب عبر الشبكة المعلوماتية وتستغل البيئة الرقمية لتحقيق أهدافها ، وقد ازدادت خطورة هذا النوع من الجرائم مع تزايد اعتماد الأفراد والمؤسسات على تخزين البيانات والمعاملات في أنظمة إلكترونية، مما جعل هذه المعطيات أكثر عرضة للوصول غير المشروع ، خاصة في ظل التطور المتسارع لوسائل الاتصال الحديثة.

ورغم الجهود المبذولة لتعزيز الحماية السيبرانية لا تزال الثغرات التقنية قائمة، وهو ما يجعل هذه الجريمة من بين أبرز التحديات المطروحة على الساحة القانونية، لكونها تتطلب معالجة دقيقة تأخذ بعين الاعتبار طبيعتها التقنية المعقدة وسرعة تطورها ، و سنحاول في هذا المبحث التطرق لمفهوم جريمة الاحتيال باستخدام تقنية المعلومات (المطلب الاول) ، و نتطرق الى أركان جريمة الاحتيال باستخدام وسائل تقنية المعلومات (المطلب الثاني) .

المطلب الأول

مفهوم جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تطورت أنماط الاحتيال بتطور الوسائل التكنولوجية، فانتقلت من الأساليب التقليدية المعهودة إلى أساليب رقمية معقدة تستغل البيئة المعلوماتية بشكل ممنهج، وقد أدى هذا التحول إلى بروز أنماط جديدة من الجرائم الاحتيالية التي يصعب ضبطها بالمعايير الكلاسيكية، نظراً لما تنطوي عليه

من طابع غير مادي، وارتباطها الوثيق بالتقنيات الحديثة، ويُعدّ الاحتيال عبر وسائل تقنية المعلومات من أكثر هذه الأنماط انتشارًا وخطورة ، لِما له من آثار مباشرة على الثقة في التعاملات الإلكترونية ، وعلى الأفراد والمؤسسات على حدّ سواء.

في هذا الاطار سنتطرق في هذا المطلب إلى تعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات (الفرع الأول) ، ثم التطرق لأهم خصائص هذه الجريمة (الفرع الثاني) ، وصولا إلى تحديد اطرافها (الفرع الثالث) .

الفرع الأول : تعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات

للتطرق لتعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات لا بد من اعطاء صورة واضحة لجريمة الاحتيال في مفهومها التقليدي و معرفة وسائل تقنية المعلومات .

أولا: تعريف الاحتيال

1. تعريف الاحتيال لغة:

الاحتيال لغة من كلمة حيل و الحيلة اسم من المصدر احتيال الحيل و الحو....، يقال : لا حيل ولا قوة لغة في حول وهو (أحيل) منه أي أكثر حيلة.[1]

كما يعني الاحتيال الحذق في تقليب الأمور من خلال توظيف الفكر للوصول إلى المقصود.[2]

ويراد ايضا أن مصطلح "الاحتيال" عدة معانٍ، منها الذكاء في تدبير الأمور وتغييرها، والسعي لتحقيق الهدف بدهاء، أو الوصول إلى غاية تنطوي على حكمة بأسلوب غير ظاهر، كما يشير إلى الخداع للاستيلاء على أموال الآخرين، والمراوغة، وتحريف الحقائق لقلب الحق باطلاً والباطل

[1] محمد بن ابي بكر بن عبد القادر الرزاي ، مختار الصحاح ، بدون طبعة، دار الكتاب العربي ، لبنان ،1981، ص 166.
[2] احمد بن محمد بن علي الفيومي المقرئ ، المصباح المنير في غريب الشرح الكبير ،مكتبة لبنان ، 2009، ص 84.

حقًا، بهدف تحقيق غاية المحتال بوسائل ملتوية و غير مشروعة،اي عن طريق المكر و الخديعة و الكيد .[1]

2.تعريف الاحتيال اصطلاحا :

يختلف الفقهاء في تقديم تعريف محدد لجريمة الاحتيال، ويعود ذلك إلى تباين وجهات نظرهم بشأن العناصر التي تُشكِّل هذه الجريمة، بحيث هناك من يعرفه بأنه الاستيلاء على أموال مملوكة للغير من خلال الخداع والتضليل، مما يؤدي إلى حمل المجني عليه على تسليم تلك الأموال للجاني دون وجه حق[2]، بينما عرَّفها آخرون بأنها الاستحواذ غير المشروع على مال مملوك للغير من خلال وسائل احتيالية تهدف إلى الإيقاع بالمجني عليه في الغلط، مما يؤدي إلى تسليمه المال دون وعي بحقيقة الأمر.[3]

كما يُعرَّف الاحتيال بأنه أي تصرف أو إيهام يهدف إلى خداع المجني عليه وإيقاعه في الغلط، مما يؤدي إلى اقتناعه بناءً على المظهر الخارجي المضلل الذي يقدمه الجاني ، وبذلك فإن المجني عليه في جريمة الاحتيال هو الشخص الذي وقع ضحية للخداع ، فانخدع بالحيلة التي استخدمها الجاني، مما دفعه إلى تسليمه المال دون إدراك لحقيقة الأمر.[4]

لم تتضمن معظم التشريعات العربية تعريفًا صريحًا لهذه الجريمة في نصوص قوانينها، وهو توجه نرى أنه مناسب نظرًا للطبيعة المتغيرة والمتعددة الأوجه لهذه الجريمة، حيث تخضع لمتغيرات

---

[1] ابن منظور ، لسان العرب ، ج 12، دون طبعة، دار صادر للطباعة ، بيروت 1998،ص 187.

[2] محمد هشام الصالح ،جريمة الاحتيال" دراسة مقارنة" ،رسالة ماجيستر في القانون العام ،جامعة النجاح، نابلس، فلسطين،2008، ص 7.

[3] عادل ابراهيم العاني، جرائم الاعتداء على الاموال في قانون العقوبات ؛ السرقة - الاحتيال - اساءة الإئتمان، دون طبعة، دار الثقافة للنشر، عمان1997، ص141.

[4] محمد الشوابكة ، جرائم الحاسوب و الانترنيت الجريمة المعلوماتية ، الطبعة الأولى، دار النهضة العربية ، القاهرة ، 2007، ص 379.

الزمن وتتطور بتطوره ، ومن المعلوم أن وضع التعريفات القانونية ليس من اختصاص المشرّع، بل هو دور الفقهاء القانونيين، كما تباينت القوانين في تسمية هذه الجريمة، حيث اعتمدت بعض التشريعات مصطلح "جريمة النصب "مثل القانون المصري و القانون المغربي بالمقابل اعتمدت بعض التشريعات الأخرى مصطلح "جريمة الاحتيال" مثل القانون الإمراتي و القانون السعودي ، وعلى الرغم من هذا التباين إلا ان غالبية الفقه اتفق على انسبية مصطلح الاحتيال .

بالنسبة إلى المشرّع الجزائري فانه تطرق لجريمة الاحتيال في قانون العقوبات في المادة 372 وذكر جريمة النصب من خلال صورها المتعددة بأنها كل سلوك يهدف إلى الإضرار بالمجني عليه من خلال التلاعب بالوقائع أو المستندات أو البيانات، أو إيهامه بمشروعات كاذبة أو وقائع غير صحيحة، مما يؤدي إلى خداعه ودفعه إلى تسليم أمواله أو ممتلكاته للجاني دون وجه حق.

وقد اعتبر المشرّع أن هذه الجريمة لا تقتصر على الأفعال التقليدية، بل تشمل استغلال الوظائف أو الألقاب أو الأسماء بطرق احتيالية، مما يؤدي إلى خداع الضحايا وإقناعهم بمشروعات وهمية أو وقائع مزيفة .كما اشار في المواد من 243 الى 246 من قانون العقوبات أن جريمة الاحتيال يمكن أن تتخذ أشكالًا متعددة، مثل انتحال الصفة، التزوير، التلاعب بالمستندات، واستغلال الثقة لتحقيق مكاسب غير مشروعة.[1]

أما بالنسبة الى المشرّع الفرنسي فقد تناول جريمة النصب بشكل واضح في المادة 313، الفقرة الأولى من قانون العقوبات، والتي تنص على أن "تُرتكب جريمة النصب عندما يعمد شخص، سواء كان طبيعيًا أو معنويًا، إلى خداع الغير باستخدام اسم أو صفة مزيفة ، أو إساءة استغلال

[1] ولحيت شهيرة ، صويح دنيا زاد، الاحتيال الالكتروني، مجلة الدراسات القانونية و الاقتصادية ، العدد 4، ديسمبر 2019 ص 39.

صفة صحيحة ، أو اللجوء إلى أساليب تدليسية ، مما يدفع الضحية إلى تسليم أموال أو ممتلكات أو عقارات، أو تقديم خدمة، أو الالتزام بتصرف قانوني أو الإعفاء منه".[1]

ثانيا : تعريف تقنية المعلومات

1.تعريف تقنية المعلومات لغة :

كلمة "تقنية" هي تعريب لمصطلح "تكنولوجيا"، الذي يُعد ترجمة حرفية لكلمة technology في الإنجليزية، والمقابلة لكلمة technologia في الفرنسية ، ويرجع أصلها إلى الكلمة الإغريقية القديمةtechnologas ، التي تتألف من شقين: الأول techno ، ويشير إلى الصنعة أو الفن أو المهارة، أما الشق الآخر logas ، فيعني العلم أو الدراسة وعند جمع المقطعين، يصبح معنى الكلمة "علم الصنعة أو المهارة" ، وقد تُرجمت كلمة "تكنولوجيا" إلى العربية بصيغتين هما:

تقنية او تقانة [2] ، كما جاء في لسان العرب "أتقن الشيء" تعني إحكامه، و"التقانة" تدل على الإتقان، أي الإحكام والدقة في صنع الأشياء، كما يُقال: "رجلٌ متقنٌ "أي حاذقٌ ومُلمٌّ بصنعته، و"تقنَ الشيءَ" أي أجاد صناعته بإحكام ومهارة[3].

---

[1] -Art 313 /1: l'escroquerie est le fait: si par l'usage d'un faux nom ou d'une fausse qualité ،soit par l'abus d'une qualité vraie ،soit par l'emploi de manœuvres frauduleuses ،de tromper une personne physique ou morale ou de la déterminer ainsi ،à son préjudice d'un tiers ،a remettre de fonds ،des valeurs ou un bien quelconque à fournir un service ou consentir un acte opérant obligation ou décharger.

[2]عبد الغفور عبد الفتاح قاري، معجم مصطلحات المكتبة والمعلومات: انجليزي- عربي، مكتبة الملك الوطنية، الرياض، 2000، ص 279 .

[3] ابن منظور ، لسان العرب ، المرجع سابق ، ص 437.

أما كلمة "المعلومات" هي جمع "معلومة"، والمفرد مشتق من الجذر (ع ل م) ، والذي تدور دلالته بشكل عام حول المعرفة التي يمكن اكتسابها ونقلها، يُقال: "علِمَ الشخصُ بالخبر" أي أدركه وعرفه وشعر به[1] ، كما أن لفظ "علِمَ" مأخوذ أيضًا من معنى الإعلام بالشيء، فيُقال: "أعلم فلانًا بالخبر" أي أخبره به، و"أعلم فلانًا بالأمر" أي جعله على دراية ومعرفة به[2].

وبذلك، تُعرَّف تقنية المعلومات لغةً بأنها: "العلم أو المهارة المتعلقة بمعالجة المعلومات ونقلها وتوظيفها بطرق دقيقة ومنهجية لتحقيق غايات محددة .

2.تعريف تقنية المعلومات اصطلاحا :

يقصد بتقنية المعلومات أنها العمليات التي تشمل جمع البيانات بمختلف أشكالها ، سواء أكانت صوتية، أو مرئية، أو رقمية، أو نصية، ثم معالجتها، وتخزينها، وبثها من خلال أنظمة إلكترونية متقدمة وتقنيات اتصال حديثة ، ويُنظر إليها أيضًا على أنها المجال الذي يسعى إلى تطوير وسائل فعالة تُمكّن من الوصول إلى المعلومات بسرعة وتبادلها بسهولة[3].

كما عرّفها بعض الفقهاء بأنها تكامل بين الحواسيب ووسائل الاتصال، بما في ذلك الألياف البصرية والأقمار الصناعية، وتمثل هذه الابتكارات منظومة متكاملة لمعالجة البيانات وتخزينها وتداولها خارج الإطار البشري، مما يعزز فعالية الوصول إلى المعلومات واستثمارها في مختلف القطاعات[4].

---

[1] هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالت الكاتبة، القاهرة، 1995، ص41 .

[2] معجم الوسيط ، مجمع اللغة العربية، القاهرة ج2 ، الطبعة 3 ،1985 ، ص647.

[3] محمود علم الدين، تكنولوجيا المعلومات وصناعة االتصال الجماهيري، دون طبعة، العربي للنشر والتوزيع ،1990، ص38.

[4] محمد محمد الهادي، تكنلوجيا المعلومات و تطبيقاتها، دون طبعة، دار الشروق، القاهرة ،1989 ص، 32 .

وتضمنت المادة "2" من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المصادق عليها من قبل الجزائر 2014، تعريف تقنية المعلومات بانها أي وسيلة مادية أو معنوية، أو مجموعة من الوسائل المترابطة أو المستقلة، تُستخدم في تخزين المعلومات وتنظيمها واسترجاعها ومعالجتها وفقًا للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها، سواء عبر أنظمة مستقلة أو ضمن شبكة، بوسائل اتصال سلكية أو لاسلكية، بهدف تطويرها وتبادلها بكفاءة.[1]

ثالثا : الاحتيال باستخدام وسائل تقنية المعلومات

تُعد جريمة الاحتيال المرتبطة بتقنية المعلومات من أكثر الجرائم انتشارًا نظرًا لبساطتها وسهولة تنفيذها، يتم ارتكاب هذا النوع من الجرائم من خلال تعديل البيانات قبل إدخالها أو أثناء عملية الإدخال في إحدى وسائل تقنية المعلومات ، وقد يُجرى هذا التعديل من قِبل أي شخص يمتلك صلاحية الوصول إلى إجراءات إعداد البيانات أو تسجيلها أو نقلها أو فحصها أو مراجعتها أو تحويلها، مما يسهل التلاعب بها لتحقيق أغراض احتيالية.[2]

وفي هذا السياق، يُعرَّف الاحتيال المتصل بتقنية المعلومات بأنه جريمة تُرتكب باستخدام أساليب احتيالية تهدف إلى خداع الضحية، سواء من خلال إيهامه بوجود مشروع وهمي أو إحداث الأمل لديه في تحقيق أرباح عبر وسائل تقنية المعلومات ، وقد يتم ذلك من خلال تواصل الجاني مع

[1] المادة 2 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.المبرمة يوم2010.12.21 والماصدق عليها موجب المرسوم الرئاسي رقم 252-14المؤرخ في 2014/09/08 ج, ر 57 لسنة 2014.

[2] محمد الامين البشرى، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004 ، ص92 .

الضحية عبر الشبكة، أو من خلال التلاعب المباشر ببيانات الحاسوب باستخدام معلومات غير صحيحة، مما يسمح له بإيهام النظام الإلكتروني والتحايل عليه ليقوم الأخير بتسليمه الأموال.[1]

وفي إطار مكافحة هذه الجريمة، نصت المادة (11) من الاتفاقية العربية تحت عنوان "جريمة الاحتيال" على أن الاحتيال المتصل بتقنية المعلومات يُعرَّف بأنه التسبب عمدًا ودون وجه حق في إلحاق الضرر بالمستفيدين والمستخدمين، وذلك بنية الاحتيال لتحقيق منافع أو مصالح غير مشروعة، سواء للجاني نفسه أو لغيره، وذلك من خلال:

_إدخال أو تعديل أو محو أو حجب المعلومات والبيانات.

_التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

_تعطيل الأجهزة أو البرامج أو المواقع الإلكترونية.[2]

يتضح أن معظم التشريعات العربية لم تقدم تعريفًا محددًا لجريمة الاحتيال المرتبط بتقنية المعلومات في قوانينها، وهو نهج يُنظر إليه على أنه إيجابي نظرًا للطبيعة المتغيرة لهذه الجريمة وتطور أساليبها مع مرور الزمن و عدم إمكانية حصرها، وبالرجوع إلى الفقه القانوني، نجد أن هناك تباينًا في التسميات والتعريفات لهذه الجريمة، حيث يُطلق عليها البعض مصطلح "الاحتيال الإلكتروني"، والذي يُعرَّف بأنه سلوك احتيالي يعتمد على منهجية الحوسبة بهدف الحصول على امتياز مالي بطرق غير مشروعة[3].

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة الماجستير في القانون تخصص القانون الدولي الاعمال، كلية الحقوق، جامعة مولود معمري، تيزي وزو ،2013 ، ص54.

[2] المادة 11 من الاتفاقية العربية لمكافحة الجرائم المتصلة بتقنية المعلومات .

[3] عبير علي محمد النجار جرائم الحاسب في الفقه الاسلامي ، رسالة الماجستير في الفقه المقارن ، كلية الشريعة و القانون ، الجامعة الاسلامية غزة، 2009، ص 7.

وفي المقابل يُطلق عليها فقهاء آخرون مصطلح "الاحتيال المعلوماتي"، وهو سلوك غير مشروع يستهدف التلاعب بالمعلومات والبيانات المخزنة في أنظمة الحاسوب، سواء من خلال إدخال بيانات غير مصرح بها، أو التعديل على الأوامر والتعليمات البرمجية، أو تنفيذ أي إجراء من شأنه التأثير على وظائف النظام ، ويشمل ذلك أي تعديل غير قانوني على البيانات، سواء كانت ذات طبيعة مالية أو غيرها، مما يؤدي إلى تحقيق مكاسب غير مشروعة أو إلحاق الضرر بالآخرين.[1]

وبناءً على ما سبق، يمكن استخلاص تعريف شامل لجريمة الاحتيال باستخدام وسائل تقنية المعلومات، على أنها سلوك احتيالي يتم من خلال استخدام الوسائل التقنية الحديثة، سواء عبر الإنترنت أو من خلال التلاعب المباشر بالبيانات الرقمية، بقصد خداع الضحية أو النظام المعلوماتي ذاته، وذلك لتحقيق منافع أو مكاسب غير مشروعة للجاني أو لغيره، أو لإلحاق الضرر بالغير، وغالبًا ما يُنفّذ هذا السلوك عبر إدخال أو تعديل أو حذف بيانات رقمية، أو التدخل في وظيفة الأنظمة المعلوماتية بما يخدم الهدف الاحتيالي.

الفرع الثاني : خصائص جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تعتبر جريمة الاحتيال باستخدام وسائل تقنية المعلومات امتدادًا حديثًا لجريمة الاحتيال التقليدي، حيث يتشابه كلاهما في العديد من الخصائص، ومع ذلك فإن الاحتيال باستخدام وسائل تقنية المعلومات يتميز عن نظيره التقليدي بعدد من السمات التي تجعله أكثر تعقيدًا وخطورة، ومن بين هذه الخصائص ما يلي:

[1] ولحيت شهيرة ، المرجع السابق ،ص 39.

أولا: جريمة الاحتيال المعلوماتي جريمة عابرة للحدود

تُعد جريمة الاحتيال باستخدام وسائل تقنية المعلومات من الجرائم العابرة للحدود، حيث لم يعد نطاقها مقتصرًا على نطاق محلي، بل أصبحت ذات طابع عالمي ، فلم يعد الفاعل بحاجة إلى الحضور في مسرح الجريمة بل يمكنه تنفيذ أفعاله الاحتيالية عن بُعد باستخدام تقنيات الحاسوب والاتصال ، وينشأ هذا البعد الجغرافي بين الجاني والفعل المرتكب ، وكذلك بين المعلومات التي كانت محل الاعتداء مما يجعل عملية تعقب الجناة أكثر تعقيدًا ، فقد يتمكن الجاني من ارتكاب جريمته عبر اختراق ذاكرة حاسوب موجود في دولة أخرى ، الأمر الذي قد يلحق الضرر بشخص ثالث في بلد مختلف ، مما يُضفي على هذه الجريمة طابعًا دوليًا يستدعي تعزيز التعاون القانوني والأمني بين الدول لمواجهتها بفعالية.[1]

ثانيا : صعوبة اكتشاف واثبات جرائم الاحتيال المعلوماتي

تُعد جرائم الاحتيال باستخدام وسائل تقنية المعلومات من أكثر الجرائم تعقيدًا وصعوبة في الإثبات والكشف، حيث تتميز بطابعها الخفي مما يجعل ضبط مرتكبيها أمرًا بالغ الصعوبة ، فهذه الجرائم تُرتكب في فضاء رقمي غير ملموس، الأمر الذي يؤدي إلى غياب الأدلة المادية التقليدية التي تعتمد عليها التحقيقات الجنائية في الجرائم الأخرى ، كما أن الأدلة الرقمية حتى عند توافرها تكون عرضة للزوال السريع إذ يتم تخزينها في ذاكرة الأنظمة الحاسوبية لفترات قصيرة ، هذا ما يجعل صعوبة عملية استرجاعها عند الحاجة.

ومن التحديات الأخرى التي تواجه كشف هذه الجرائم، ضخامة البيانات التي يتعين فحصها عند التحقيق، حيث تتطلب عملية الوصول إلى الأدلة تحليل كميات هائلة من المعلومات وهو ما

[1] سعيداني نعيم ، اليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ،رسالة الماجستير في العلوم القانونية ،كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر ، باتنة ، 2013، ص 32.

يشكل عبئًا إضافيًا على الأجهزة الأمنية والجهات المختصة ، كما أن بعض المؤسسات مثل البنوك والشركات الكبرى ، قد تتردد في الإبلاغ عن تعرضها لمثل هذه الجرائم خشية فقدان ثقة عملائها أو التأثير سلبًا على سمعتها التجارية مما يساهم في تفاقم الظاهرة وصعوبة مكافحتها[1].

ثالثا : الطابع التقني لجريمة الاحتيال المعلوماتي

إن ارتكاب جريمة الاحتيال باستخدام وسائل تقنية المعلومات يستلزم وجود وسيلة إلكترونية أو تقنية، مثل الحواسيب أو الهواتف النقالة المتصلة بشبكة الإنترنت، حيث لا يمكن تصور وقوع هذه الجريمة دون الاعتماد على أدوات تكنولوجية متطورة ، فهذه الوسائل تشكل العنصر الأساسي في تنفيذ الاحتيال، إذ تتيح للجناة إمكانية الوصول إلى البيانات الرقمية والتلاعب بها بطرق يصعب اكتشافها وتتبعها.

وتتنوع الأساليب المستخدمة في هذه الجريمة، مثل استغلال بطاقات الائتمان من خلال تشفير بياناتها والتلاعب بها بوسائل تكنولوجية متقدمة لتحقيق مكاسب غير مشروعة، ويكمن جوهر الاحتيال باستخدام تقنية المعلومات في استغلال التطور الرقمي لتنفيذ عمليات احتيالية معقدة، مستفيدين من خصائص الوسائل الإلكترونية التي تتيح لهم إخفاء هويتهم والتحايل على الأنظمة الأمنية، مما يزيد من صعوبة كشف الجريمة وملاحقة مرتكبيها.

ونظرًا للطابع التقني الذي تتطلبه جريمة الاحتيال باستخدام تقنية المعلومات، فإن عمليات كشفها والتحقيق فيها تستلزم أيضًا مستوى عالٍ من المعرفة التقنية، غير أن الجهات الأمنية والقضائية

[1] اسمهان بن مالك ، خصائص الجريمة المعلوماتية و اسباب ارتكابها، مجلة البيبان للدراسات القانونية والسياسية، جامعة البشري الابراهيمي ، برج بوعريريج ، العدد 1، جوان 2019، ص 114.

لا تزال تعاني من نقص في هذه المعارف ، مما يفرض الحاجة إلى تعزيز التخصص في مجال التقنية بهدف تمكين الأجهزة الأمنية والقضائية من مواجهة هذه الجرائم بفعالية.

كما أن القوانين التقليدية لم تعد قادرة على مواكبة التطور السريع في التكنولوجيا ، الأمر الذي أدى إلى ظهور أنماط جديدة من الجرائم لم تكن معروفة سابقًا، مما جعل التشريعات القائمة عاجزة عن التصدي لها ، وفي ظل هذا الواقع أصبح من الضروري تدخل المشرّعين لوضع قوانين حديثة تتناسب مع التطورات المتسارعة مع ضمان احترام مبدأ الشرعية الجنائية ، وإلى جانب ذلك يظل التعاون بين الجهات القانونية والخبراء المتخصصين في تقنية المعلومات ، بالإضافة إلى التنسيق الدولي ، عاملًا حاسمًا في مكافحة هذه الجرائم والحد من انتشارها[1].

الفرع الثالث : أطراف جريمة الاحتيال باستخدام وسائل تقنية المعلومات

في جريمة الاحتيال باستخدام وسائل تقنية المعلومات يكون لدينا طرفان رئيسيان: الجاني والمجني عليه ، الجاني هو الشخص الذي يستخدم التكنولوجيا لتنفيذ جريمة الاحتيال، بينما المجني عليه هو الشخص الذي يتعرض لهذه الأفعال الاحتيالية ويُستغل من خلالها، وهو ما نتطرق له في هذا الفرع :

أولا : الجاني في جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تختلف جريمة الاحتيال المعلوماتي عن الجرائم التقليدية من حيث طبيعة الجاني والمهارات التي يمتلكها، حيث تعتمد بشكل أساسي على الخبرة التقنية والمعرفة بأنظمة الحاسوب وشبكات الإنترنت، دون الحاجة إلى استخدام العنف أو القوة الجسدية ، فبينما لا يتطلب المجرم في الجرائم التقليدية مستوى علميًا معينًا، فإن مرتكب جرائم الاحتيال المعلوماتي يحتاج إلى كفاءة تقنية تمكنه

[1] صغير يوسف، المرجع سابق ، ص 20.

من تنفيذ الجريمة بطرق معقدة وإخفاء آثاره لتجنب كشفه وبسبب هذا الطابع التقني، غالبًا ما يكون الجناة من ذوي الخبرة في مجال تقنية المعلومات.[1]

يتم تصنيف مرتكبي جرائم الاحتيال المعلوماتي إلى الفئات التالية:

المخترقون :(Hackers) وهم أفراد يمتلكون مهارات متقدمة في تقنية المعلومات ويدفعهم فضولهم لاختراق الحسابات الشخصية بوسائل غير قانونية، يتميز هؤلاء الجناة بميولهم التطفلي، حيث يسعون إلى استعراض قدراتهم الذهنية والتقنية في مجال التكنولوجيا الحديثة ، وغالبًا ما يكونون من فئة الشباب، وتتركز أنشطتهم على اختراق المواقع الرسمية ، وفي بعض الحالات ، يستهدفون الحسابات الخاصة بدافع إثبات الذات[2].

المحترفون :(Professionals) تُعد هذه الفئة الأخطر بين مرتكبي جرائم الاحتيال المعلوماتي، حيث يسعون إلى تحقيق مكاسب غير مشروعة من خلال التعدي على الحسابات المصرفية واختراقها ، كما قد يكون لبعضهم دوافع سياسية تدفعهم إلى استهداف المواقع الرسمية والتلاعب بها لتحقيق أهداف معينة.

الحاقدون :(Malicious Attackers) لا تهدف هذه الفئة إلى تحقيق مكاسب مادية أو أهداف سياسية، وإنما يرتكبون جرائمهم بدافع الانتقام أو بدوافع عقائدية أو طائفية ، إذ يكون الدافع الرئيسي لأفعالهم مرتبطًا بمشاعر الحقد أو الرغبة في الانتقام[3].

---

[1] حكيم سياب ، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية ، دراسات وأبحاث زيان عاشور، الجلفة ،العدد 01 ، ص 223.

[2] دحمان صبايحية خديجة ،جرائم السرقة و الاحتيال عبر الانترنيت ، دراسة بين الفقه الاسلامي و القانون الجزائري ، رسالة الماجستير في العلوم الاسلامية ، كلية العلوم الاسلامية، جامعة الجزائر ، 2013 ، ص33 .

[3] محمود محمد طه ، المواجهة التشريعية الجرائم الكمبيوتر والانترنت ، الطبعة الأولى، دار الفكر والقانون، المنصورة، 2013، ص 15.

ثانيا: المجني عليه في جريمة الاحتيال باستخدام وسائل تقنية المعلومات

يتعرض الضحايا في جرائم الاحتيال المعلوماتي لفقدان أموالهم نتيجة استغلال بياناتهم الشخصية والمالية بطرق غير مشروعة، حيث يستهدف المحتالون المعلومات الحساسة المتعلقة بالمستحقات المالية، الإيداعات المصرفية، بطاقات الائتمان، الحسابات المالية و تقارير الميزانية، مما يجعل أصحابها عرضة لخسائر مالية جسيمة.

غالبًا ما يقع الأفراد ضحية لأساليب احتيالية متطورة، حيث يستغل محترفو التقنية شبكة الإنترنت في خداعهم من خلال الترويج لمشاريع زائفة أو منتجات وخدمات غير حقيقية ، مما يدفع الضحايا إلى مشاركة بياناتهم الائتمانية دون دراية بالمخاطر، وفي كثير من الحالات تُستخدم هذه المعلومات لإجراء عمليات شراء غير قانونية أو لسداد مبالغ مالية دون علم الضحية ، مما يؤدي إلى استنزاف أموالهم وإيقاعهم في مشكلات مالية معقدة[1].

لا يقتصر الاحتيال على الأفراد الطبيعيين فحسب ، بل يستهدف أيضًا الأشخاص المعنويين، كالقطاعات المالية والشركات الكبرى، التي تعتمد بشكل كامل على الأنظمة الرقمية في إدارة بياناتها وأصولها ، ويجعل هذا الاعتماد المتزايد هذه المؤسسات عرضة للهجمات الإلكترونية التي تستهدف أموالها وبياناتها الحساسة.

تتردد الشركات في أغلب الأحيان عن الإبلاغ عن هذه الجرائم حفاظًا على سمعتها، مما يشجع الجناة على مواصلة أنشطتهم ، وتعد البنوك والمؤسسات المالية الأكثر استهدافًا ، تليها الشركات

[1] بورابة صورية ، عبد الكافي مريم ، جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الالكترونية ، مجلة القانون والعلوم السياسية ، المجلد 8 ، العدد 01، جامعة طاهري محمد بشار، الجزائر ، 2022، ص415.

الخاصة مثل شركات التأمين ، نظرًا لما تمتلكه من موارد مالية ضخمة ومعلومات ذات أهمية اقتصادية ، هذا ما يجعلها عرضة لأساليب الاحتيال مختلفة[1].

المطلب الثاني

أركان جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تقوم جريمة الاحتيال باستخدام وسائل تقنية المعلومات على عدة أركان ، أولها الركن الشرعي الذي يستند على مبدأ شرعية التجريم حيث يتم تحديد القوانين الخاصة التي تنظم جريمة الاحتيال و العقوبات الخاصة بهذه الجريمة، اما الركن المعنوي لجريمة الاحتيال باستخدام وسائل تقنية المعلومات يتضمن القصد بنوعيه العام و الخاص و بالنسبة للركن المادي فيتكون من فعل الاحتيال ووسائل الخداع المستخدمة، و يترتب عليه نتيجة تتمثل في الاستيلاء على مال الغير مع وجود علاقة سببية تربط بين الاحتيال و الاستيلاء .

وبناءً على ما تقدم، سيتم تقسيم هذا المطلب إلى ثلاثة فروع رئيسية تُعنى بتحليل الأركان المكونة لجريمة الاحتيال المرتكبة باستخدام وسائل تقنية المعلومات تهدف إلى تحليل الجوانب القانونية والمادية للجريمة محل البحث، حيث سيتناول (الفرع الأول) الركن الشرعي الذي يُنظّم هذا النوع من الأفعال، في حين سيتعرض (الفرع الثاني) الركن المعنوي ، ثم في (الفرع الثالث) الركن المادي للوقائع والسلوكيات التي تُشكّل الفعل الإجرامي.

الفرع الأول : الركن الشرعي

يعتبر الركن الشرعي أحد الأركان الأساسية لقيام الجريمة، حيث لا يمكن تجريم أي فعل أو توقيع عقوبة دون وجود نص قانوني واضح وصريح يحدد الأفعال المجرّمة والعقوبات المقررة لها، وذلك

[1] دحمان صبايحية خديجة ، المرجع سابق ، ص35.

استنادًا إلى مبدأ "لا جريمة ولا عقوبة إلا بنص" المنصوص عليه في المادة 1 من قانون العقوبات الجزائري، ونظرًا للتطور التكنولوجي السريع وظهور أنماط جديدة من الجرائم، كان لزامًا على المشرّع الجزائري أن يتدخل لتأطير الجرائم السيبرانية، ومن بينها جريمة الاحتيال باستخدام وسائل تقنية المعلومات، إلا أن المشرع الجزائري لم ينص على مواد خاصة تجرم الاحتيال باستخدام وسائل تقنية المعلومات، مما استلزم تطبيق القواعد العامة لجريمة الاحتيال وفقًا للمادتين 372 و 373 من قانون العقوبات الجزائري، ويعكس هذا الإطار القانوني حرص المشرع على حماية المصالح الأساسية للمجتمع، حيث قام بوضع قواعد إلزامية يترتب على مخالفتها توقيع العقاب[1].

ولقد نصت المادة 372 من قانون العقوبات الجزائري[2] على كافة الافعال المادية التي تشكل جريمة الاحتيال، بحيث يعتبر كل من تمكن الحصول على اموال أو ممتلكات أو سندات او تعهدات مالية ، سواء كانت بطريقة مباشرة او من خلال تقديم وعود او تبرئات من الالتزامات او التصرفات المشابهة ، هو مرتكب لهذه الجريمة ، ويشمل ذلك جميع الافعال الاحتيالية التي تهدف الى الاستيلاء على ثروات الغير سواء كليا او جزئيا، او حتى الشروع في ذلك باستخدام اساليب خداع مثل استخدام اسماء أو صفات مزورة، أو التظاهر بسلطة غير حقيقية ، أو تقديم وعود كاذبة بالفوز أو حدوث حوادث وهمية ، بينما في جريمة الاحتيال باستخدام وسائل تقنية المعلومات لم يخصص المشرع الجزائري نصا منفصلا لهذه الجريمة ، إلا ان نص المادة 372 يعكس مرونة في التعاطي مع التطورات الحديثة في وسائل الاحتيال بما في ذلك استخدام الحاسب الالي ، الانترنت ، و غيرها من الوسائل المستقبلية التي قد تطرأ .

[1] سامية العايب ، منار عراية ، "الحماية الجزائية للمستهلك من جريمة النصب الالكتروني "، مجلة هيرودوت للعلوم الانسانية و الاجتماعية ، جامعة 8 ماي 1945 قالمة ، الجزائر ، العدد3 ، 2021، ص ص229-243.

[2] انظر المادة 372 من الأمر رقم 66-156 المؤرخ في 18 صفر الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات المعدل و المتمم ج.ر.ج.ج ، العدد 49 لسنة 1966.

وفي غياب نصوص قانونية خاصة بجريمة الاحتيال باستخدام وسائل تقنية المعلومات، يتم تطبيق قانون مكافحة الجريمة المعلوماتية رقم 09-04 المؤرخ في 5 غشت 2009[1] على بعض الأفعال المرتبطة باستخدام التكنولوجيا، هذا القانون يعالج بعض أنواع الجرائم الإلكترونية مثل التسلل و الدخول إلى الأنظمة المعلوماتية أو الوصول غير المشروع إلى البيانات المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر7 من قانون العقوبات ، إلا انه لم يتطرق بشكل صريح إلى جريمة الاحتيال باستخدام وسائل تقنية المعلومات على الرغم من ذلك، يمكن اعتبار بعض المواد المتعلقة بالدخول غير المشروع إلى الأنظمة المعلوماتية ذات صلة بالاحتيال باستخدام وسائل تقنية المعلومات، خاصة في حالات استخدام التقنيات للدخول الى الانظمة المعلوماتية او البقاء فيها لاستخراج معلومات بطريقة غير قانونية او تعديلها او محوها بهدف الاحتيال.

و كما رأينا من قبل رغم وجود نصوص متعلقة بالجرائم المعلوماتية في قانون 09-04 ،إلا أن هذه النصوص تتعامل مع الجرائم الإلكترونية بشكل عام ولا تحدد بشكل دقيق سبل معالجة الاحتيال باستخدام وسائل تقنية المعلومات ومن هنا يمكن القول إن التشريع الجزائري لا يزال بحاجة إلى إدخال تعديلات لتخصيص نصوص قانونية واضحة وشاملة تتعلق بجريمة الاحتيال باستخدام وسائل تقنية المعلومات بشكل مستقل و منفصل ، لمواكبة التقدم التكنولوجي والتحديات الجديدة التي تطرأ في مجال الجرائم المعلوماتية.

الفرع الثاني : الركن المعنوي

تعتبر جريمة الاحتيال المعلوماتي من الجرائم العمدية، رغم أن المشرع الجزائري في المادة 372 من قانون العقوبات الجزائري لم ينص صراحة على ضرورة توافر العمد ، وذلك لأن الجرائم

[1] قانون رقم 09-04 مؤرخ في 14شعبان عام 1430 الموافق 5 غشت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها ، ج.ر.ج.ج ، عدد47، 2009.

العمدية هي الأصل في هذا النوع من الجرائم، فالخطأ غير العمدي لا يتناسب مع جريمة الاحتيال التي تعتمد على استخدام أساليب وطرق خداعية تهدف إلى إقناع الضحية وتسليمه المال عن طريق التمويه والتلاعب ، و ذلك يتطلب درجة من الذكاء والقدرة على التخطيط والتنفيذ ، فلا تقع جريمة الاحتيال المعلوماتي بشكل عفوي ، لانها تقوم على ترتيب الامور بشكل منظم حتى يمكن الايقاع بالمجني عليه ، و في هذه الجريمة يفترض توفر القصد الجنائي بنوعيه العام و الخاص.

يتوافر القصد الجنائي العام بتوافر عنصري العلم والإرادة ، إذ يشترط أن تكون إرادة الجاني موجهة نحو ارتكاب الفعل المحظور، وأن يكون قاصدا النتيجة التي تترتب على ذلك الفعل ، وهذا يتطلب أن تكون إرادة المتهم نافذة من الناحية القانونية، أي أنه يجب أن يكون الجاني واعيًا بأفعاله، مدركًا أنها تندرج ضمن أفعال الاحتيال و المناورات التي تهدف إلى خداع المجني عليه لدفعه لتسليم ماله ، كما يجب أن يعلم الجاني أن المال الذي يستولي عليه مملوك لشخص آخر[1].

أما القصد الجنائي الخاص، فيتمثل في نية الجاني تملك المال الذي استلمه من المجني عليه مع عزمه على حرمان المالك الحقيقي منه ، فإذا كان الهدف من ذلك هو الاستفادة من المال ثم إعادة تسليمه إلى صاحبه، فإن الجريمة لا تتحقق.

كما لا تعتبر جريمة إذا كان القصد مجرد المزاح مع صاحب المال، دون نية الاستيلاء عليه أو حيازته بشكل دائم[2].

[1] محمود احمد طه ، المرجع السابق، ص157.

[2] منصور رحماني ، المرجع سابق ، ص23.

الفرع الثالث : الركن المادي

تتطلب جريمة الاحتيال باستخدام وسائل تقنية المعلومات نفسها نفس باقي الجرائم الاخرى توافر الركن المادي الذي يعد أساسا لقيام الجريمة ، ولا يختلف هذا الركن في هذا النوع من الجرائم كثيرا عن الجرائم التقليدية إذ لا يمكن اعتبار الجريمة مكتملة من دون توافر هذا الركن الذي يتمثل في ذلك الفعل او السلوك الذي يقوم به الجاني بهدف الوصول الى مبتغاه وهو إيهام المجني عليه و اجباره على تسليم ماله باستخدام وسائل الخداع و الحيلة[1] .

إلا أن الركن المادي في جريمة الاحتيال يحظى بالنصيب الاوفر من الشرح و التمثيل ، و ذلك لأهميته و كثرة التفاصيل فيه[2] ، فيتكون الركن المادي لجريمة الاحتيال من عدة عناصر نذكرها كالتالي:

أولا: السلوك الاجرامي

وهو ذلك الفعل أو ذلك النشاط الغير مشروع الذي يخالف القوانين المعمول بها و يترتب عليه ضرر أو تلاعب بحقوق و مصالح الاخرين، ويتمثل السلوك الاجرامي في التدليس و خداع المجني عليه بما يجعله يصدق ذلك الادعاء الكاذب، وبالتالي يدفعه لتسليم المال للجاني ، فالتدليس يتضمن تقديم معلومات مضللة حول حقيقة واقعة معينة بهدف إيقاع الشخص في الغلط[3]، وبالعودة الى نص المادة 372 من قانون العقوبات الجزائري نجد أن الاحتيال يتم إما

[1] هدى قشقوش ، "جرائم الحاسب في التشريع المقارن " ، الطبعة الأولى، دار النهضة العربية ،القاهرة ،1992 ، ص762.

[2] كريم منشد خنياب الاسدي ، جرائم النصب و الاحتيال و علاقتها بالجرائم المشابهة لهما في القانون الجنائي ، الطبعة الأولى، دار النشر الان ناشرون و موزعون، عمان ، الاردن ، سنة 2015، ص 88.

[3] محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ، الطبعة الثالثة، دار النهضة العربية، القاهرة ، 1992، ص 991.

باستعمال أسماء أو صفات كاذبة او سلطة خيالية او اعتماد مالي خيالي او بإحداث الأمل في الفوز بأي شيء او في وقوع حادث أو أية واقعة اخرى وهمية او الخشية من وقوع شيء منها[1].

فكما نلاحظ ان الرابط المشترك بين هذه الأشكال هو استخدام الجاني لأساليب متعددة من الكذب والتضليل، حيث يتعمد استخدام أكثر من وسيلة لإقناع المجني عليه بصحة ادعاءاته وهذا ما يميز هذه الجريمة عن الكذب البسيط ويحولها إلى جريمة نصب واحتيال، وهو ما يعكس نية الجاني في استغلال الضحية بطرق معقدة.

كما أن الوسائل التي يستعملها الجاني لإيهام المجني عليه بصحة ادعاءاته لا حصر لها ، لكنها تشترك في تحقيق نتيجة واحدة و هي تصديق المجني عليه للجاني و تسليمه ما كان مطلوبا منه.

و من المتعارف عليه فقهيا انه يشترط لقيام جريمة الاحتيال المعلوماتي توفر بيئة رقمية متصلة بالإنترنت، مع تحديد واضح لبداية النشاط الإجرامي ونتيجته ، فيجب على الجاني في هذه الجرائم أن يهيئ الوسائل التقنية اللازمة لتنفيذ الجريمة، مثل إعداد برامج وصفحات مزورة، وقد يتطلب الأمر أيضاً استخدام أدوات مثل الفيروسات لتسهيل تنفيذ الجريمة، كما يمكن أن يشمل هذا النشاط الإجرامي الاعتداء على أنظمة المعالجة الألية او الدخول غير المصرح به إلى الأنظمة الرقمية، كما جاء في نص المادة 394 مكرر من قانون العقوبات الجزائري أو التلاعب بالبيانات لتغييرها أو تعديلها بهدف انتهاك خصوصية الأفراد والاحتيال عليهم ، أو لسرقة أموالهم أو تحويلها بطرق غير قانونية[2].

[1] باسم شهاب ، جرائم المال و الثقة العامة (السرقة ، خيانة الامانة ، الاحتيال ، اصدار شيك دون رصيد) مع الجرائم الملحقة بها او القريبة منها في ظل التشريعات الجزائرية و المقارنة ، دون طبعة، دار بيرتي للنشر، الجزائر ، 2013، ص ص 186 . 187

[2] انظر نص المادة 394 مكرر من قانون العقوبات الجزائري .

تتنوع أساليب ارتكاب جريمة الاحتيال المعلوماتي تبعا لتطور وسائل تقنية المعلومات ، لذلك سنقوم بعرض أهم الأساليب التقنية المستخدمة في ارتكاب جريمة الاحتيال المعلوماتي :

يعد التلاعب في إدخال وإخراج البيانات من أبرز أشكال الاحتيال المعلوماتي إذ يتميز هذا النوع من التلاعب بسهولة التنفيذ، مما يجعله من أكثر الأنماط شيوعًا في هذا المجال، على سبيل المثال في الولايات المتحدة، بلغ عدد حالات الاحتيال المتعلقة بتلاعب البيانات المدخلة إلى الحاسوب حوالي 62% من إجمالي الحالات المكتشفة حتى عام 1984. [1]

تنقسم وسائل التلاعب في مرحلة إدخال البيانات إلى ثلاث طرق رئيسية:

التعديل على البيانات: يتم تعديل البيانات قبل أو أثناء إدخالها إلى النظام، سواء بإضافة أجزاء جديدة أو استبدال جزء منها هذا التغيير قد يكون كليًا أو جزئيًا، مما يؤدي إلى تغيير معنى البيانات.

الحذف: يمكن أن يتضمن التلاعب حذف جزء من المعلومة أو حتى حذفها بالكامل، مما يؤدي إلى فقدان المعنى أو تغييره بشكل كامل.[2]

الإعاقة: يتم إدخال المعلومة في مكان غير مخصص لها، مما يعيق استخدامها بشكل صحيح ، هو ما نصت عليه المادتين 5 و 8 من اتفاقية بودابست بشأن الجريمة المعلوماتية[3]، و كذا

[1] نهلا عبد القادر المومني ،الجرائم المعلوماتية، دون طبعة، دار الثقافة، عمان، الاردن، 2010، ص 190 .

[2] المرجع نفسه ، ص 191.

[3] انظر المادتين 5 و 6 من اتفاقية مجلس أوروبا المتعلقة بالجريمة المعلوماتية (اتفاقية بودابست)، الموقعة بتاريخ 23 نوفمبر 2001.

قانون العقوبات الفرنسي في نص مادته 1/323، [1]بينما لم يتطرق المشرع الجزائري لهذا النوع من الافعال المجرمة.

من الأمثلة على هذا النوع من التلاعب ما وقع في الأردن عام 1994 عندما قام أحد مدخلي البيانات بتسجيل أسهم بأسماء وهمية، وبيعها في السوق المالية بمبالغ طائلة ، كذلك في أحد البنوك السويسرية، قام موظف بالتلاعب في المعاملات المالية عن طريق ضرب القيم الفعلية للمعاملات في ألف، مما مكنه من الاستيلاء على مبلغ 700,000 فرنك سويسري.

أما التلاعب في مرحلة إخراج البيانات فهو أقل شيوعًا، حيث يتم التلاعب في البيانات عند إخراجها من النظام، بشرط أن تكون قد ادخلت بشكل صحيح من البداية ، ورغم قلة الحالات التي تم الإبلاغ عنها، فإن التلاعب في هذه المرحلة يظل وسيلة خطر عند حدوثها[2].

من جهة أخرى، فإن التلاعب في البرامج يعد من الوسائل المعقدة والأكثر خطرًا ، يتطلب هذا النوع من التلاعب مهارات متقدمة في البرمجة ويشمل تغيير البرامج المستخدمة أو إضافة برامج جديدة، مما يمكن الجناة من تعديل البيانات أو اختراق الأنظمة ، بعض الأمثلة على ذلك تشمل تعديل برامج إدارة الحسابات في البنوك للحصول على أرباح غير مشروعة، أو برمجة النظام لاستخلاص مبالغ صغيرة وتحويلها إلى حسابات الجناة.

كما قد يتم التلاعب عبر خلق برامج وهمية مخصصة لارتكاب الجريمة ، كما حدث عندما قامت إحدى الشركات الأمريكية بإنشاء وثائق تأمين وهمية وتزويرها لبيعها وتحقيق أرباح غير مشروعة.

[1] Code pénal, art. 323-1, al. 1 (France). (n.d.). Accès ou maintien frauduleux dans un système de traitement automatisé de données.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 192.

أما في حالة التلاعب بالبيانات عبر الشبكات عن بُعد، فإن هذه الوسيلة تسمح للجناة بالقيام بالأعمال الإجرامية من أي مكان طالما كانت الأجهزة متصلة بشبكة الإنترنت، هذه الوسيلة جعلت الاحتيال أسهل وأصعب في الاكتشاف في نفس الوقت ، وقد تم استخدام هذه الطريقة من قبل مجرم برمجة في أحد البنوك الأمريكية لزرع فيروس في الشبكة وتحويل الأموال إلى حسابه الخاص في نيويورك[1].

ثانيا : النتيجة الاجرامية

تُعد النتيجة الإجرامية العنصر الثاني للركن المادي في جريمة الاحتيال، وتتجسد هذه النتيجة في تسليم المال من الضحية إلى الجاني ، و من أجل تحقق جريمة الاحتيال، يجب أن تؤدي الوسائل الاحتيالية التي حددها المشرع، إلى إقناع المجني عليه بتسليم ماله طواعية .

أما إذا لم يتحقق هذا الأثر، كأن يفطن المجني عليه للخدعة ويمتنع عن التسليم، فإن ذلك يُشكل شروعاً لا جريمة تامة، وقد كرس المشرع الجزائري هذا المفهوم في المادة 372 من قانون العقوبات، حيث ربط تمام الجريمة بحصول الجاني فعلاً على المال أو شروعه في ذلك، مما يعكس تبنّيه لفكرة النتيجة المادية الملموسة كشرط لقيام الجريمة، وبالتالي فإن وجود الضرر ولو كان بسيطاً، يُعد مظهراً ضرورياً لتحقيق النتيجة الإجرامية، التي تمثل الغاية التي يسعى إليها الجاني من خلال فعله الاحتيالي.[2]

[1] نهلا عبد القادر المومني، المرجع السابق، ص ص 193-195.

[2] باسم شهاب ، المرجع السابق ، ص ص 189 190.

ثالثا : العلاقة السببية

تربط العلاقة السببية في الاحتيال بين المناورات الاحتيالية وتسليم المال ويتوسط بين ذلك الفعل وهذه النتيجة حلقة اتصال تجمع بينهما ، الا وهي ذلك الغلط الذي يترتب على المناورات الاحتيالية ، كما ينبغي أن يتم التسليم تحت تأثيره ، ويعني ذلك وجود صلة سببية بين المناورات الاحتيالية والغلط وصلة السببية بين الغلط والتسليم فيه[1] ولتوفر العلاقة السببية لا بد من توفر مجموعة من الشروط[2] :

1 - يجب أن يكون هناك سلوك إيجابي - طريقة احتيالية - قد أقدم عليها الجاني.

2 - يجب أن يتم استخدام الأسلوب الاحتيالي قبل تسليم المال.

3 - ينبغي أن يكون السلوك الإيجابي (الذي يتسم بالخداع) له تأثير على الضحية، مما يدفعها لتسليم المال المطلوب.

4 - يجب أن يكون الضحية هو الذي وقع في الخطأ نتيجة الخداع الذي أقدم عليه الجاني .

[1] محمود نجيب حسني ، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، المجلد الأول، منشورات الحلبي الحقوقية ، 1998 ، ص371.

[2] منصور رحماني ، المرجع السابق، ص22.

المبحث الثاني

صور جريمة الاحتيال باستخدام وسائل تقنية المعلومات

أصبحت الوسائل الرقمية تحتل مكانة مركزية في الحياة اليومية مع تسارع التطور التكنولوجي ، سواء في المعاملات المالية عبر وسائل الدفع الإلكترونية، أو في التواصل وتبادل البيانات من خلال الخدمات الإلكترونية المختلفة كالبرامج الرقمية و وسائل التواصل الاجتماعي ، غير أن هذا التوسع أتاح للمحتالين فرصاً جديدة لاستغلال هذه المنصات بطرق خادعة ومتطورة ، مستهدفين الأفراد والمؤسسات على حد سواء، ويُعد الاحتيال الذي يستهدف وسائل الدفع الإلكترونية، وكذا الاحتيال عبر الخدمات الإلكترونية من أبرز صور الجريمة المعلوماتية المعاصرة ، حيث تتخذ هذه الأفعال أشكالاً متعددة تجمع بين الخداع التقني والاحتيال باستخدام تقنية المعلومات ، في ظل بيئة رقمية مفتوحة ومعقدة.

وفي هذا السياق، سنتناول في (المطلب الأول) صور الاحتيال على وسائل الدفع الإلكتروني ، ثم ننتقل في (المطلب الثاني) إلى صور الاحتيال التي تطال الخدمات الإلكترونية .

المطلب الأول

الاحتيال على وسائل الدفع الإلكتروني

يعد مصطلح الدفع الإلكتروني مصطلحا جامعا لمختلف الوسائل التي تعتمد على التقنيات و التكنولوجيا الحديثة لتسهيل العمليات المالية ومن أبرز هذه الوسائل نذكر التحويل الإلكتروني للأموال و الدفع بإستخدام البطاقات الإلكترونية كبطاقة الإئتمان.

كما يعتبر الدفع الإلكتروني نظاما متكاملا يعتمد على تقنيات متقدمة و برامج متطورة تهدف الى تسهيل اجراء العمليات المالية مع الحرص على قيامها بشكل آمن، بما يتوافق مع الأطر التنظيمية المعمول بها لضمان سرية و امان و حماية اجراءات الشراء و ضمان وصول الخدمة للمستفيدين.

إلا أنه مع زيادة استخدام هذه الوسائط نتج تزايد في المخاطر المرتبطة بالاحتيال، مما يستدعي التطرق في مطلبنا هذا الى صور الاحتيال على وسائل الدفع الإلكتروني بمختلف اشكاله.

الفرع الأول: الاحتيال على بطاقات الائتمان

لطالما كانت النقود هي الوسيلة الأساسية التي اعتمد عليها الإنسان لتسديد تكاليف شراء السلع والخدمات المقدمة له، إلا أن التطور السريع للتكنولوجيا اضافة الى ظهور الإنترنت أدى إلى ضرورة تطوير وسائل دفع حديثة تواكب هذا التقدم، وهو ما تجسد في ظهور بطاقات الائتمان البنكية.

أولا : تعريف بطاقات الائتمان

تعرف بطاقات الائتمان بمصطلحات كثيرة منها بطاقات الدفع الالكتروني، النقود الائتمانية، النقود البلاستيكية، بطاقات الوفاء الحديثة، بطاقات الائتمان الممغنطة، بطاقات الضمان النقود الإلكترونية ، الحافظة الإلكترونية، الكروت ذات القيمة المحفوظة والنقود البولمرية ، ولكن

أكثرها شيوعا هو مصطلح بطاقات الائتمان[1]، ولقد تباينت الآراء حول تعريف بطاقة الائتمان نظرا لحداثة هذا النوع من المعاملات و كذا عدم تطرق التشريعات لتعريفها تعريفا جامعا مانعا.

[1]عماروش خديجة ايمان ، بطاقة الائتمان في الجزائر : دراسة حالة بطاقة فيزا الدفع المسبق لبنك التنمية المحلية (BDL)"، مجلة الاصلاحات الاقتصادية و الاندماج في الاقتصاد العالمي، المجلد12 ، العدد24، جامعة احمد بوقرة، بومرداس، الجزائر 2017 ، ص ص220-204.

عرفت بطاقة الائتمان بأنها وسيلة حديثة تم اختراعها و تطويرها استجابة للإحتياجات التي فرضتها البيئة و مواكبة للتقدم التكنولوجي ، و هي بطاقة تتيح لحاملها سحب الأموال أو نقلها بكل أريحية، إلا انه من غير الممكن إصدارها إلا من قبل هيئة مالية معترف بها كالمؤسسات المصرفية أو الخزينة العامة ، مصالح البريد أو أي جهة اخرى مرخص لها بإصدار هذه البطاقات[1].

عرفها البعض الآخر تحت مسمى "بطاقات الوفاء" بأنّها عقد يتعهد بمقتضاه مصدر البطاقة بفتح اعتماد بمبلغ معين لمصلحة شخص آخر، هو حامل البطاقة الذي يستطيع بواسطتها الوفاء بمشترياته لدى المحلات التجارية التي ترتبط مع مصدر البطاقة بعقد تتعهد فيه بقبولها الوفاء بمشتريات حاملي البطاقات على أن تتم التسوية النهائية بعد كل مدة محددة.[2]

كما تعرف أيضاً بأنها : "البطاقات التي تتم معالجتها إلكترونياً لاستخدامها في أغراض متعددة من خلال المعلومات المخزنة عليها والدخول بها على الآلات المعدة لذلك بغية تحقيق أغراض معينة"[3].

[1] بورايو هاجر اميرة، واقع استخدام البطاقات البنكية في الجزائر -دراسة مقارنة لعينة من البنوك العمومية الجزائرية- ، مجلة الابحاث الاقتصادية لجامعة البليدة2، المجلد13، العدد18، جامعة "لونيسي علي"، البليدة ، الجزائر، ص368.

[2] فايز نعيم رضوان، "بطاقة الوفاء المطبعة العربية"، دون طبعة، دار النهضة العربية ، القاهرة ، مصر، 1990، ص8.

[3] كميت طالب البغدادي ، "الاستخدام غير المشروع لبطاقات الائتمان" ، دون طبعة، دار الثقافة للنشر و التوزيع ، عمان ، 2008 ، ص52.

ثانيا : طرق الاحتيال على بطاقات الائتمان

رغم التطور الكبير في استخدام بطاقات الائتمان والخدمات الرقمية التي توفرها، شجع ذلك بعض محترفي النصب والتزوير و المخترقين على الدخول لمجال بطاقات الائتمان و استخدامها غير المشروع[1] كما سنوضحه كالتالي:

1. استنساخ البطاقات :

يُعد استنساخ بطاقات الائتمان أحد أقدم وأكثر أساليب الاحتيال شيوعًا ، ففي هذا النوع من الاحتيال يقوم المحتالون باستخدام أجهزة تسمى "سكيمرز" لنسخ بيانات البطاقة من الشريط المغناطيسي أو من الشريحة الإلكترونية ، فيمكن تركيب هذه الأجهزة في أجهزة الصراف الآلي أو على نقاط البيع، وعند قيام المستخدم بإدخال بطاقته ، يتم سرقة البيانات[2] .

يستخدم جهاز "السكيمر" لسرقة بيانات بطاقات الائتمان للقيام بالمعاملات المالية ، مهمة هذا الجهاز تنطوي حول قراءة البيانات المخزنة على الشريط المغناطيسي أو الشريحة الإلكترونية للبطاقة دون علم صاحبها، حيث عادةً ما يُثبت على أجهزة نقاط البيع أو أجهزة الصراف الآلي، فعندما يتم إدخال البطاقة في الجهاز المزود بالسكيمر يقوم هذا الاخير بنسخ البيانات مثل رقم البطاقة، تاريخ انتهاء الصلاحية و رمز الأمان.

---

[1] مخلوفي عبد الوهاب ، هوام علاوة، "اثر الاستخدام غير المشروع لبطاقات الائتمان و علاقته بجريمة تبييض الاموال"، مجلة العلوم الانسانية ، جامعة باتنة 1 الحاج لخضر ، باتنة ، الجزائر ، العدد 46، 2017، ص 354.

[2] ستان كامينيسكي ، "كيف يسرق مجرمو الإنترنت الأموال من البطاقات المصرفية — وكيفية حماية نفسك من هذه السرقة" ، منشور على الموقع https://me.kaspersky.com/blog/how-to-protect-emv-and-nfc-bank-cards/10461/ تاريخ الاطلاع 09/04/2025 على الساعة 14:00.

في بعض الحالات يمكن أن يتضمن "السكيمر" كاميرات صغيرة أو أجهزة تتبع لسرقة الرقم السري، ونتيجة لذلك يقوم المحتالون باستخدام هذه البيانات لإجراء معاملات احتيالية أو لاستنساخ البطاقة (عملية تعرف بالكشط). [1]

و يقصد بالكشط تلك العملية الاحتيالية التي يتم فيها نسخ البيانات المخزنة على البطاقة الأصلية المتحصل عليها باستخدام تقنية "السكيمر"، حيث يقوم المحتالون باستخدام هذه البيانات لنسخها على بطاقة جديدة ، كما يمكن أن تشمل هذه البيانات رقم البطاقة ، تاريخ انتهاء الصلاحية، ورمز الأمان ، بالإضافة إلى الرقم السري فبعد استنساخ البطاقة يصبح من الممكن للمحتال استخدامها لإجراء معاملات غير قانونية، سواء في المتاجر أو عبر الإنترنت.[2]

ولكن بالرغم من أن استخدام البطاقات الذكية المزودة بشريحة (EMV) قد قلل من فعالية هذه الأنواع من الاحتيال، إلا أن المحتالين لا يزالون قادرين على استخدام تقنيات متطورة لنسخ البيانات من الشريحة نفسها، مما يجعل عملية الكشط ممكنة حتى مع وجود تقنيات الأمان المتقدمة، و تعتبر تقنية (EMV) نظامًا عالميًا حديثًا يُستخدم في بطاقات الدفع المعتمدة على الشرائح الذكية، حيث توفر هذه التقنية مستوى أعلى من الأمان والسهولة لكل من العملاء والتجار، و تعود تسميتها الى أوائل حروف أسماء الشركات الثلاث التي قامت بتطويرها في التسعينيات: "Europay" و"Mastercard" و"Visa"، ومع مرور الوقت تم اعتماد هذه التقنية بشكل واسع

[1] Louis DeNicola, What Is Card Skimming and How Can You Avoid It?, What Is Card Skimming and How Can You Avoid It? - Experian منشور على الموقع ,تاريخ الاطلاع 2025/04/09 ,على الساعة 14:15

[2] الاحتيال على بطاقة الائتمان: كيفية منع الاحتيال على بطاقة الائتمان واكتشافه وماذا تفعل إذا كنت ضحية، منشور على موقع الاحتيال على بطاقة الائتمان: كيفية منع الاحتيال على بطاقة الائتمان واكتشافه وماذا تفعل إذا كنت ضحية - FasterCapital ، تم الاطلاع في تاريخ 2025/04/09، على الساعة14:18.

في مختلف دول العالم، بما في ذلك أوروبا وكندا وآسيا، ولاحقًا أصبحت معتمدة بشكل متزايد في الولايات المتحدة.

تعمل بطاقات (EMV) من خلال شريحة إلكترونية صغيرة مدمجة داخل البطاقة تختلف عن البطاقات التقليدية التي تستخدم الشريط المغناطيسي، إذ تقوم الشريحة بإنتاج رمز مختلف وفريد لكل معاملة مالية، مما يجعل من الصعب على المحتالين نسخ البيانات أو استخدامها مرة أخرى.[1]

فلتجنب الوقوع ضحية لهذه الأنواع من الاحتيال ينصح بمراقبة الحسابات البنكية بانتظام للكشف عن أي معاملات غير قانونية مع استخدام بطاقات ذكية مزودة بالشرائح الإلكترونية ، والتأكد من عدم وجود أجهزة غريبة أو ملحقات على أجهزة الدفع مثل أجهزة الصراف الآلي أو نقاط البيع، ومن المستحسن و الآمن عدم إدخال الرقم السري في أماكن غير آمنة، والتأكد من سلامة الأجهزة قبل استخدامها وذلك تفاديا للوقوع في فخ هذه الاساليب الاحتيالية.

2. سرقة بيانات البطاقة عبر الانترنت :

يسعى المحتالون إلى الحصول على تفاصيل بطاقة الائتمان بهدف استخدامها في إجراء المعاملات المالية عبر الانترنت، فعادةً ما تشمل هذه التفاصيل رقم البطاقة، تاريخ انتهاء الصلاحية، و رمز التحقق (CVV/CVC)، وفي بعض البلدان قد تشمل أيضًا اسم حامل البطاقة،

[1] الاحتيال أثناء تقديم البطاقة: مكافحة الأنشطة الاحتيالية باستخدام تقنية EMV، منشور على الموقع الاحتيال أثناء تقديم البطاقة: مكافحة الأنشطة الاحتيالية باستخدام تقنيةEMV - FasterCapital ، تم الاطلاع عليه في تاريخ 2025/04/09، على الساعة 14:22.

الرمز البريدي، أو حتى رقم جواز السفر[1]، ولجمع هذه البيانات بشكل غير قانوني يستخدم المحتالون طرق خاصة المبينة كالتالي :

أ. انشاء مواقع و تطبيقات وهمية على الإنترنت :

تعد المواقع و التطبيقات الوهمية من أكثر الأساليب الحديثة استعمالا لسرقة بيانات بطاقات الائتمان و يظهر هذا كالتالي :

❖ **تصميم مواقع وهمية تحاكي المواقع الحقيقية :**

يتم تصميم هذه المواقع لتبدو وكأنها رسمية لشركات تجارية، فتصبح مواقع تلك الشركات في خطر عندما يقوم بعض المحتالين بمحاكتها من ناحية التصميم والخصائص الى درجة اقناع الضحية بإدخال معلوماته الشخصية فيها كالاسم ورقم بطاقة الائتمان ، وعادة ما يتخذ هؤلاء اللصوص من مواقعهم تلك صفة التبعية للمواقع الأم وعلى أساس أنها تقدم تخفيضات أسعار ثم يزودونها ببيانات شحن للضحية الذي لا يشك أبداً في قانونية ذلك الموقع[2] ، بالاضافة الى انشاء مواقع تحاكي مواقع البنوك أو خدمات الدفع الإلكتروني إلا ان الهدف منها هو إيقاع الضحايا في فخ الاحتيال وسرقة معلوماتهم الحساسة مثل أرقام بطاقاتهم الائتمانية ، رموز الأمان (CVV)، وأحيانًا حتى الارقام السرية الخاصة بهم.

و عادةً ما يتم استخدام المواقع الوهمية في هذه الحالات:

---

[1] ستان كامينسكي، كيف يسرق مجرمو الإنترنت الأموال من البطاقات المصرفية — وكيفية حماية نفسك من هذه السرقة، منشور على موقع https://me.kaspersky.com/blog/how-to-protect-emv-and-nfc-bank-cards/10461/، تم الاطلاع في تاريخ 09/04/2025،على الساعة 14:37.

[2] خالد سيف الدين ، "الاحتيال المتغير في عالم بطاقات الائتمان" ، منشور على موقع الاحتيال المتغير في عالم بطاقات الائتمان تاريخ الاطلاع : 09/04/2025 على الساعة 14:56.

- **العروض والصفقات المضللة:**

يقدم المحتالون عروضًا مغرية مثل خصومات ضخمة أو هدايا مجانية عبر مواقع وهمية تبدو حقيقية، و لحظة ادخال المستخدم بياناته الشخصية والمالية، يتم سرقتها.

وفي حادثة مماثلة، قامت شبكة إجرامية بالاحتيال على عدد من المواطنين من خلال عروض وهمية لبيع هواتف وسيارات بالتقسيط حيث طلبوا من الضحايا إرسال معلومات بطاقاتهم الذهبية، مما مكنهم من الوصول إلى حساباتهم عبر تطبيق "بريدي موب" وسرقة مالية كبيرة[1]

- **مواقع التسوق المزيفة:**

يقوم المحتالون بإنشاء مواقع تسوق إلكترونية وهمية لبيع منتجات غير موجودة أو لسرقة تفاصيل بطاقات الائتمان الخاصة بالمستخدمين فيطمع الضحايا في العروض الزائفة ظنا منهم أنهم بصدد القيام بعملية شراء مشروعة الا انهم في الواقع يقعون في فخ الاحتيال، حيث يتم سرقة بياناتهم المالية بمجرد إدخالها في تلك المواقع المزيفة .[2]

❖ **انشاء تطبيقات وهمية مشابهة للتطبيقات الاصلية :**

تعد التطبيقات الوهمية من أبرز الأساليب التي يعتمد عليها المحتالون لسرقة بيانات بطاقات الائتمان، بحيث يقوم المحتالون بتصميم تطبيقات مزيفة تحاكي التطبيقات الأصلية الشهيرة مثل تطبيقات البنوك أو التطبيقات المصرفية أو تطبيقات الدفع الإلكتروني و عادةً ما تكون هذه التطبيقات مشابهة جدًا للتطبيقات الحقيقية من حيث الشكل والوظائف، مما يصعب على

[1] سمير منصوري ، "محتالون يستولون على اربعة ملايير باستعمال "بريدي موب" منشور على الموقع : محتالون يستولون على أربعة ملايير باستعمال "بريدي موب – "الشروق أونلاين تاريخ الاطلاع : 09/04/2025 على الساعة 15:14.

[2] احمد الشريف، احترس من عصابات المتاجر الوهمية لسرقة بيانات بطاقات الائتمان، منشور على الموقع احترس من عصابات المتاجر الوهمية لسرقة بيانات بطاقات الائتمان .. ما القصة؟، تاريخ الاطلاع 2025/04/09، على الساعة 14:52.

المستخدمين اكتشاف الاحتيال، فبمجرد تحميل المستخدم للتطبيق الوهمي وفور تسجيل الدخول باستخدام بياناته الشخصية يقوم المحتالون بسرقة هذه البيانات و استغلالها في معاملات مالية غير قانونية.

إضافة إلى ذلك، قد تحتوي بعض التطبيقات على وظائف خادعة تطلب من المستخدم إدخال بيانات أخرى مثل رمز التحقق أو تفاصيل الحساب المصرفي و تتضاعف خطورة هذه التطبيقات عند نشرها عبر متاجر التطبيقات غير الرسمية أو من خلال روابط مشبوهة يتم إرسالها عبر الرسائل النصية أو البريد الإلكتروني ، لذلك من الضروري تحميل التطبيقات من المتاجر الرسمية فقط والتحقق من صحة المصدر قبل إدخال أي معلومات شخصية و حساسة[1].

و في هذا السياق ، يُعد تطبيق "بريدي موب" مثالًا واضحًا على كيفية استغلال المحتالين للثقة في التطبيقات المشهورة ، هذا التطبيق الذي يتيح للمستخدمين إجراء المعاملات الإلكترونية وسحب الأموال باستخدام بطاقة الدفع الخاصة بهم، إلا انه في بعض الحالات قد يقوم المحتالون بتصميم تطبيقات وهمية تحمل نفس الاسم والشعار لتشجيع المستخدمين على تحميل التطبيق الزائف من مصادر غير رسمية ، فبعد تحميل ذلك التطبيق الوهمي وتسجيل الدخول باستخدام بيانات البطاقة ، تتم سرقة تفاصيل البطاقة مثل رقم الحساب و رمز التحقق و الرقم السري لذلك وجب على المستخدمين توخي الحذر وعدم تحميل التطبيقات من متاجر غير رسمية أو روابط مشبوهة لضمان أمان بياناتهم المالية.

[1] Lukas Stefanko, Fake banking apps on Google Play leak stolen credit card data, منشور على الموقع الالكتروني Bogus apps found on Google Play leak stolen credit card credentials, تاريخ الاطلاع 2025/04/08, ساعة الاطلاع 15:30

وفي إطار حماية المستخدمين من هذه الهجمات، أطلقت المنظمة الجزائرية لحماية وإرشاد المستهلك نداءً عاجلًا لمستخدمي تطبيق "بريدي موب" يوم الأحد 06 أفريل 2025 وذلك ببيان رسمي، حذرت فيه المنظمة من تزايد محاولات الاحتيال الإلكتروني الذي يستخدم فيها المحتالون تقنيات خادعة وانتحال صفة موظفين رسميين من بريد الجزائر للإيقاع بالضحايا، كما قدمت المنظمة نصائح للمستخدمين لضمان أمان بياناتهم وحمايتها من هذه الممارسات الاحتيالية، وذلك بحرصها على التشديد بعدم مشاركة المعلومات الشخصية مع أي جهة تدعي تمثيل بريد الجزائر، خاصة إذا كانت تطلب معلومات حساسة ، كما شددت على ضرورة تجنب مشاركة الرقم السري أو أي بيانات مالية عبر الهاتف أو الرسائل النصية .[1]

3. البرمجيات الخبيثة المحمولة :

يمثل هذا النوع من البرمجيات تهديدًا متزايدًا لأمن الهواتف الذكية وخصوصية المستخدمين، حيث يهدف المحتالون من خلالها إلى سرقة بيانات حساسة مثل تفاصيل بطاقات الائتمان والمعلومات البنكية المخزنة في الهواتف المحمولة ، فتعمل هذه البرمجيات على التسلل إلى الأجهزة من خلال تطبيقات ضارة قد يتم تنزيلها من متاجر غير موثوقة أو عبر روابط مشبوهة بعد التثبيت ، كما تقوم بمراقبة المدفوعات عبر الهاتف المحمول، حيث يمكنها تسجيل البيانات المدخلة من قبل المستخدمين، بما في ذلك الأرقام السرية وكلمات المرور.

إضافة الى إمكانية تسلل هذه الاخيرة إلى التطبيقات المصرفية و القيام بسرقة الأموال عن طريق إنشاء صفحات مزيفة تطلب من المستخدمين إدخال بياناتهم المصرفية.

[1] الهام هواري ، "تحذير عاجل لمستخدمي "بريدي موب" من الاحتيال الالكتروني" ، منشور على موقع تحذير عاجل لمستخدمي "بريدي موب"من الاحتيال الإلكتروني ، تاريخ الاطلاع 08/04/2025 على الساعة 15:49.

و مثالا على ذلك، اكتشاف تطبيقات خبيثة مثل SharkBot[1] و MaliBot[2]، التي تهدف إلى سرقة معلومات حسابات المستخدمين المصرفية من خلال تقنيات التصيد الاحتيالي، حيث يتم إنشاء صفحات مزيفة لطلب بيانات تسجيل الدخول والمعلومات الشخصية وبمجرد أن يتمكن المحتالون من جمع هذه البيانات، يمكنهم استخدامها لتنفيذ معاملات مالية غير مصرح بها.

الفرع الثاني : الاحتيال على نظم التحويل الالكتروني للأموال

يُعد التحويل الإلكتروني للأموال من الخدمات المصرفية التي يلتزم البنك بتقديمها لعملائه، حيث يقوم البنك بتنفيذ تعليمات الزبون المتعلقة بتحويل الأموال، وذلك من خلال تحويل المبالغ المطلوبة إلى الجهة المستفيدة، أو استقبال التحويلات الواردة لحساب العميل[3].

و يعرف نظام التحويل الإلكتروني للأموال على أنه أحد الأنظمة الذكية التي تتيح تحويل الأموال بين المصارف بطريقة إلكترونية آمنة و سريعة، وهو تلك العملية التي يتم فيها قيد مبلغ معين من المال في الجانب الدائن(أي الحساب الذي يستلم المال) لحساب آخر سواء كان هذا الحساب خاصًا بالشخص نفسه أو يعود لشخص آخر.

[1] عبد الرحمان الحاج، "تحذير عاجل من أندرويد بسبب برامج خبيثة تتسلل إلى الحسابات المصرفية"، منشور على موقع الأمان المصرفي في خطر: تسلل البرامج الخبيثة إلى الهواتف - مجلة هي تاريخ الاطلاع 09/04/2025 على الساعة 16:20.

[2] كتبت هبة السيد ، "برمجيات خبيثة متطورة تضرب نظام أندرويد وتستهدف الخدمات المصرفية"، برمجيات خبيثة متطورة تضرب نظام أندرويد وتستهدف الخدمات المصرفية تاريخ الاطلاع 09/04/2025 على الساعة 16:28.

[3] الكيلاني محمود ، "الموسوعة التجارية و المصرفية" ، المجلد الرابع ، عمليات البنوك ، دراسة مقارن ، دون طبعة، دار الثقافة للنشر و التوزيع 2008 ، ص413.

ومن أشهر نظم التحويل الالكتروني للأموال نذكر باختصار نظام "FedWire[1]" الذي يُستخدم في التحويلات الفورية بين البنوك الأمريكية للمعاملات الكبرى [2]، ونظام "CHIPS[3]" المتخصص في تسوية التحويلات الكبيرة بالدولار الأمريكي داخليًا ودوليًا في نفس اليوم[4] ، أما نظام " SWIFT" يعد أكبر شبكة لنقل رسائل التحويلات المالية بين البنوك والمؤسسات المالية في مختلف أنحاء العالم، فهو يقوم بنقل الرسائل المتعلقة بالتحويلات المالية عبر الحدود بين البنوك الدولية دون اجراء المقاصة بينها مما يتيح للبنوك إجراء المدفوعات الدولية بأمان و سرعة.

تعتمد معظم المؤسسات المالية حول العالم على SWIFT لتبادل معلومات التحويل حيث يعالج النظام مليارات الدولارات يوميًا وهو عنصر اساسي في النظام المالي العالمي الذي بدوره يسهل المعاملات المالية الدولية.[5]

ورغم توفير هذا النظام سهولة كبيرة و اختصار للوقت، لا تخلو هذه العمليات من التحديات؛ حيث تبقى المخاوف الأمنية في صدارة النقاشات المتعلقة بالتحويلات الإلكترونية للأموال ، إذ

[1] شبكة "فيد واير" (Fedwire) – وهي اختصار لـ Federal Reserve Wire Network و يعد من اقدم و اهم انظمة التحويل الالكتروني للأموال في الولايات المتحدة الامريكية و هو شبكة التحويلات المالية التابعة للاحتياطي الفيدرالي الأمريكي، تتكوّن من 12 بنكًا إقليميًا، وتُستخدم للتحويلات الإلكترونية بين المؤسسات المالية بدأت باستخدام التلغراف حتى 1973، وأُتيحت عضويتها لمؤسسات الإيداع منذ عام 1980.

[2] عايض راشد المري، التحويل الالكتروني للأموال دراسة مقارنة، مارس 2024، مقال منشور على الموقع الالكتروني التحويل الإلكتروني للأموال – دراسة مقارنةKilaw Journal – ، تاريخ الاطلاع 2025/04/10، على الساعة 11:36

[3] يُعد نظام CHIPSمن أكبر نظم الدفع بين البنوك في الولايات المتحدة، ويتميز بطابع وطني ودولي حيث يختص بالتحويلات بالدولار الأمريكي عبر نظام مركزي يربط حواسيب البنوك الأمريكية والأجنبية لتحويل الأموال داخل وخارج الولايات المتحدة.

[4] ليندة عبد الله ، تبييض الاموال عن طريق الاعتماد المستندي للأموال" ، مجلة جيل البحث العلمي ، عدد خاص عن اعمال المؤتمر الدولي الرابع عشر ، طرابلس 25-24 مارس 2017 متوفر على موقع تبييض الأموال عن طريق الاعتماد المستندي الالكتروني | ليندة عبد الله JiL.Center - ، تاريخ الاطلاع 11/04/2025 ، على الساعة 15:12.

[5] ليندة عبد الله ،المرجع نفسه، تاريخ الاطلاع 11/04/2025 ، على الساعة 15:47.

أسهم الارتفاع الكبير في المعاملات الرقمية في زيادة الأنشطة الإجرامية الإلكترونية[1] ، و من طرق الاحتيال على التحويل الالكتروني للأموال نذكر البعض كالتالي:

أولا : الدخول غير المشروع للنظام لأغراض شخصية

أحيانًا لا يتم اختراق النظام من الخارج، بل يُرتكب الجرم من داخل المؤسسة من قبل موظفين أو أشخاص لديهم صلاحيات وصول للنظام، حيث يستخدمون هذه الصلاحيات لتحقيق أغراض شخصية لا تمت بصلة لمهامهم الوظيفية، مثل التلاعب بالبيانات أو تنفيذ تحويلات مالية دون تصريح.[2]

ثانيا : التلاعب بالبيانات او تدميرها عبر الفيروسات أو البرامج الخبيثة

يستغل بعض الجناة معرفتهم بالنظام الداخلي للمؤسسة المالية، فيقومون بإدخال أوامر للحاسوب تؤدي إلى تدمير أو تعطيل البيانات وتتم هذه العمليات عادة باستخدام برامج ضارة أو فيروسات، إما لمسح البيانات الحساسة أو لإحداث خلل يُعطل النظام بشكل كامل، وغالبًا ما ينفذها موظفون مطّلعون على البنية التقنية للنظام .[3]

ثالثا : استغلال البيانات المخزنة في أنظمة الحاسوب

يُعد هذا النوع من أخطر التهديدات لنظم التحويل الإلكتروني للأموال، حيث يقوم المجرم باختراق شبكة الحاسب التي تحتوي على معلومات حساسة ، مثل أرقام البطاقات البنكية الائتمانية ومن خلال استخدام جهازه الشخص ، يقوم باختيار رقم بطاقة معين ، ومن ثم يطلب تحويل الأموال

[1] "التحويل الإلكتروني: تحويل الأموال الإلكتروني: التحويل الإلكتروني وRTGS: فهم أنظمة الدفع الإلكترونية" ، منشور على موقع التحويل الإلكتروني: تحويل الأموال الإلكتروني: التحويل الإلكتروني و RTGS: فهم أنظمة الدفع الإلكترونية - FasterCapital ، تم الاطلاع في تاريخ 11/04/2025 على الساعة 08:26.

[2] سامر سليمان الجبوري، "جريمة الاحتيال الالكتروني دراسة مقارنة"، الطبعة الأولى، مكتبة زين الحقوقية، 2018، ص118.

[3] المرجع نفسه ، ص 119.

المرتبطة به وتُصبح عملية الكشف عن هذا النوع من الجرائم شديدة الصعوبة ما لم يُلاحظ تطابق غير اعتيادي في الأسماء أو الأرقام.[1]

رابعا: تصميم برامج مخصصة لتحويل الأموال بصورة آلية

يقوم الجناة بتصميم برامج تقوم بتحويل الأموال تلقائيًا من حسابات محددة إلى حساباتهم الخاصة ومثال شهير على ذلك، ما حدث في مصرف الكويت التجاري ، حيث قام أحد موظفي البنك بتطوير برنامج ينقل مبالغ مالية من خمسة حسابات راكدة إلى حساب جديد باسمه ، موزعة على خمسة فروع مختلفة ، وتم توقيت العملية لتُنفذ أثناء وجوده خارج البلاد بعد انتهاء عقد عمله[2].

الفرع الثالث : الاحتيال على منصات الدفع الرقمي

تُعد منصات الدفع الرقمي أحد الابتكارات المحورية في مجال المعاملات المالية الإلكترونية ، إذ تُتيح للأفراد والمؤسسات تنفيذ عمليات تحويل الأموال، الشراء والدفع مقابل الخدمات، عبر شبكة الإنترنت دون الحاجة إلى التعامل المباشر بالنقد أو الوسائل الورقية التقليدية .[3]

ويُقصد بمنصة الدفع الرقمي أنه نظام تقني يوفر بيئة إلكترونية آمنة ومتصلة بالإنترنت، تمكّن المستخدمين من تنفيذ العمليات المالية عن بُعد، باستخدام وسائل دفع متعددة مثل البطاقات البنكية، المحافظ الإلكترونية، أو حسابات الدفع المربوطة بالبنوك أو بمؤسسات مالية مرخصة.[4]

---

[1] سامر سليمان الجبوري ، المرجع السابق ، ص 200.

[2] درار نسيمة ، "الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني" دراسة مقارنة، جامعة أبو بكر بلقايد، الجزائر، أطروحة دكتوراه، 2015 -2016، ص 146.

[3] نهال نعواش ، وسائل الدفع الإلكترونية ، منشور على الموقع الاكتروني https://mawdoo3.com ، تاريخ الاطلاع 04/09/2025 ، على الساعة 8:21

[4] دويني مختار، وسائل الدفع الإلكتروني ومدى مساهمتها في تطور التجارة الإلكترونية في الجزائر، مجلة القانون العام الجزائري والمقارن ، المجلد 7، العدد1 ، جامعة جيالي ليابس ، سيدي بلعباس ، 2021 ، ص 194.

تعتمد هذه المنصات على بنية معلوماتية متقدمة تتيح التكامل مع البنوك ،وأنظمة التحقق الإلكتروني ومزودي الخدمات التجارية، ما يجعلها وسيطًا فعالًا في تسهيل التجارة الإلكترونية ودفع الفواتير وتحويل الأموال داخليًا ودوليًا .

من أشهر الأمثلة على منصات الدفع الرقمي عالميًا: PayPal ، Stripe، Apple Pay، Google Pay، Amazon Pay، في حين توجد منصات محلية أو إقليمية التي اعتمدها العالم العربي مثل: فوري (مصر)، ماد باي (السعودية)، بريدي موب (الجزائر)، والتي تلعب دورًا حيويًا في تعزيز الشمول المالي والرقمنة.

يتم الاحتيال على منصات الدفع الإلكتروني عبر استخدام بطاقات الائتمان بأنواعها المختلفة، نظرًا لاحتياج هذه المنصات إلى وسائل الدفع الإلكتروني أثناء المعاملات المالية عبر الإنترنت، سواء كانت البطاقات صادرة عن بنوك محلية أو مؤسسات مالية دولية ، و عملية الاحتيال على هذه المنصات تكون بإحدى الطرق التالية :

أولا : احتيال الأفراد على منصات الدفع الرقمي

يتم هذا النوع من الاحتيال عبر الدخول غير المصرح به إلى النظام المعلوماتي لهذه المنصات، والذي يعاقب عليه حسب المادة 394 مكرر من قانون العقوبات الجزائري ، يشمل هذا محاولة الوصول إلى الأنظمة الرقمية أو البيانات المخزنة فيها بشكل غير قانوني، سواء كان ذلك عبر تجاوز القيود الأمنية أو استغلال ثغرات في نظام المنصة ، يتمثل الفعل المادي في الدخول إلى

النظام دون إذن من صاحبه ، أو في تجاوز الصلاحيات الممنوحة للمستخدمين، وهو ما يمكن أن يشمل الوصول إلى معلومات حسابات المستخدمين أو البيانات المالية[1].

الاحتيال في هذه الحالة يعتمد بشكل كبير على الغش والتلاعب باستخدام وسائل تقنية المعلومات، بحيث يتم استخدام أساليب مثل القرصنة الإلكترونية، أو الهجمات السيبرانية التي تهدف إلى تغيير أو حذف بيانات الدفع، أو تحويل الأموال إلى حسابات المحتالين ، كما قد تشمل الأفعال الأخرى التي تهدف إلى إعاقة قدرة النظام على إجراء العمليات بشكل طبيعي، مثل تعطيل الخدمات أو إتلاف النظام ، الأمر الذي يعطل عملية الدفع أو يؤدي إلى تسريب البيانات الشخصية والمالية[2].

ثانيا : احتيال الأفراد على المستخدمين داخل المنصات

يتمثل احتيال الأفراد على المستخدمين داخل منصات الدفع الرقمية في تصميم مواقع إلكترونية أو منصات تجارية تدعي أنها تقدم خدمات مالية أو تجارية موثوقة، على غرار منصات التحويلات المالية أو التداول عبر الإنترنت ، تلك المواقع التي تتسم بواجهة احترافية وتصميم متقن، قد تتخذ أسماء مشابهة لمنصات معروفة أو ذات سمعة جيدة ، مما يعزز من مصداقيتها الوهمية في نظر المستخدمين[3].

العملية تبدأ بترويج المحتالين لهذه المنصات الوهمية من خلال وسائل متعددة مثل رسائل البريد الإلكتروني المزيفة ، الإعلانات على وسائل التواصل الاجتماعي ، أو العروض المغرية التي

[1] حمودي ناصر ، الحماية الجنائية لنظم المعالجة الالية للمعطيات في التشريع الجزائري ، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 2، جامعة عبد الرحمان ميرة، بجاية ، 2016، ص74.

[2] حمودي ناصر ، المرجع نفسه ، ص 80.

[3] أسماء مبارك الريامي ، المرجع سابق ، ص 58.

تقدم فرصًا مربحة للاستثمار أو تسهيلات في تحويل الأموال ، كما يتم إقناع الضحايا بالاستثمار أو إجراء معاملات مالية عبر هذه المنصات على اعتبار أنها ستؤدي إلى تحقيق أرباح أو تسهيلات مالية.

عند إتمام الضحايا لتحويلاتهم المالية أو تزويدهم بالمعلومات الحساسة حول حساباتهم المصرفية، يتوارى المحتالون عن الأنظار، حيث تختفي المنصة الوهمية فجأة دون أي أثر، مما يترك الضحايا في حالة من الصدمة بعد اكتشافهم أنهم وقعوا ضحية لعملية احتيال ، هذه الأفعال تعتمد بشكل أساسي على الخداع واستخدام تقنيات متقدمة لاستغلال ثقة المستخدمين وإيهامهم بمصداقية الخدمات المقدمة ، هذا يجعل اكتشاف الاحتيال أمرًا صعبًا قبل وقوع الضحايا في الفخ .

المطلب الثاني

الاحتيال على الخدمات الإلكترونية

شهدت الخدمات الإلكترونية انتشارًا واسعًا وأصبحت جزءًا لا غنى عنه في مختلف المجالات، مثل التعليم، الإدارة، التجارة ، الصحة وغيرها ، فقد أسهم التطور التكنولوجي في تحسين كفاءة العمليات و تيسير الإجراءات، و كذا توفير الوقت والجهد، مما جعل الأفراد والمؤسسات يعتمدون بشكل متزايد على الحلول الرقمية في انجاز أعمالهم ومهامهم اليومية ومع توسع نطاق استخدامها، أصبحت هذه الخدمات أكثر تطورًا من خلال الاعتماد على تقنيات حديثة مثل الذكاء الاصطناعي مما عزز من فاعليتها وانتشارها.

غير أن هذا الانتشار الواسع جعلها أيضًا عرضة للاستغلال من قبل المحتالين، حيث لم تسلم من محاولات الاحتيال التي تستهدف استغلال ثغراتها لتحقيق مكاسب غير مشروعة ، فقد تنوعت

أساليب الاحتيال على الخدمات الإلكترونية ، سواء من خلال التلاعب بالبرامج الالكترونية اليه (الفرع الأول) ، أو استغلال البريد الإلكتروني (الفرع الثاني) ، أو استهداف مستخدمي وسائل التواصل الاجتماعي بطرق احتيالية مختلفة (الفرع الثالث) .

الفرع الأول : الاحتيال على البرامج الإلكترونية

يُعد الاحتيال على البرامج الإلكترونية من الجرائم المستحدثة التي رافقت تطور التكنولوجيا، ويستهدف هذا النوع من الاحتيال البرمجيات بوسائل غير مشروعة تمسّ سلامتها أو شرعيتها، ويندرج تحته عدد من الصور التي تعكس تنوّع الأساليب الاحتيالية المستخدمة في هذا المجال.

أولا: تعريف البرامج الإلكترونية

يشير مصطلح "البرمجيات" إلى جميع العناصر غير المادية التي يتكوّن منها نظام الحاسب الالي، والتي تشمل البرامج الأساسية اللازمة لتشغيل الجهاز، بالإضافة إلى برامج التطبيقات التي تُستخدم لأداء وظائف محددة، وتُعرَّف البرامج على أنها مجموعة من التعليمات المكتوبة بلغة برمجية، تُوجَّه إلى الحاسوب الإلكتروني بهدف تنفيذ عمليات معينة وتحقيق نتائج محددة ، أما من الناحية التقنية، فإن البرمجيات (Software) تُعدّ المكوّن المنطقي لنظام الحاسوب، حيث تتضمن البرامج التشغيلية، والوثائق المصاحبة لها، فضلًا عن الأدوات المساعدة التي تساهم في تشغيل الحاسوب وضمان أدائه لوظائفه بكفاءة.[1]

و تتعدد تصنيفات هذه البرامج الى انواع مختلفة تتمثل في :

[1] ايمن عبد الله فكري ، الجرائم المعلوماتية دراسة مقارنة في التشرعات العربية و الاجنبية ، الطبعة الأولى ، مكتبة القانون و الاقتصاد ، الرياض ، 2015 ،ص 49.

1. برامج النظام : (System Software)

تُعتبر هذه البرامج أساسية لعمل الحاسوب، حيث لا يمكن للمستخدمين التفاعل مباشرة مع الجهاز دون وجود نظام تشغيل يدير موارده وينسق عملياته، تساعد هذه البرامج في التحكم بالمكونات المادية للحاسوب مثل إدارة الملفات وتنظيم البيانات وحفظها، كما تسهم في تسهيل التفاعل بين المستخدم والجهاز من خلال بيئات تشغيل متعددة، ومن أبرز الأمثلة على هذه البرامج أنظمة التشغيل مثل Windows وLinux، وبرامج إدارة الملفات، بالإضافة إلى برامج التحكم في الأجهزة الطرفية كبرامج تعريف الطابعات ولوحات المفاتيح[1].

2. برامج تطبيقية : (Application software)

تعتبر نوع من البرمجيات المصممة لمساعدة المستخدمين على تنفيذ مهام محددة، حيث تعمل كوسيط بين المستخدم ونظام التشغيل لتقديم وظائف عملية، كمعالجات النصوص مثل Microsoft Word، وبرامج جداول البيانات مثلExcel ، ومتصفحات الإنترنت مثل Google Chrome، وبرامج تحرير الصور مثلAdobe Photoshop .

3. البرامج الثابتة : (Firmware)

هي نوع من البرمجيات المدمجة داخل مكونات الأجهزة الإلكترونية، حيث تُخزن على شرائح خاصة ضمن اللوحة الأم أو وحدات التخزين الداخلية، وتعمل هذه البرامج على توفير التعليمات الأساسية التي تتحكم في تشغيل الأجهزة وضمان تفاعلها مع المكونات الأخرى، تتميز البرامج

[1] العلمي علي اسلام ، بومسلة عبد القادر ، برامج الحاسب الالي ومدى خضوعها لاحكام الامر رقم 03-05 ، مجلة الفكر القانوني والسياسي ، العدد الثالث ، جامعة عمارثليجي ،الاغواط ،2018 ، ص 293 .

الثابتة بكونها غير قابلة للإزالة أو التعديل بسهولة، وتُستخدم في العديد من الأجهزة مثل الحواسيب، وأجهزة التحكم عن بعد، والهواتف الذكية، والمعدات الصناعية.

4. البرامج الوسيطة : (Middleware)

تصنف هذه البرمجيات على انها تعمل كحلقة وصل بين أنظمة التشغيل والتطبيقات المختلفة، مما يسهل عملية الاتصال والتفاعل بين البرامج والأنظمة المتنوعة، كما تساعد في تبادل البيانات وإدارة العمليات بين التطبيقات الموزعة عبر الشبكات أو بين الأنظمة غير المتجانسة، مما يعزز من كفاءة التشغيل وتكامل الأنظمة.[1]

ثانيا : طرق الاحتيال على البرامج الالكترونية

تتطلب عملية الاحتيال من الفاعلين خبرة عميقة للتلاعب في البرامج نظرا لطبيعتها الخاصة التي تستوجب التدخل في الكيان المنطقي للحاسب الالي ، ويكون هذا بالطرق التالية:

1. تعديل البرامج:

يلجأ بعض الأفراد إلى العبث بالبرامج الإلكترونية عبر تعديل محتواها أو تغيير وظائفها دون تصريح من الجهة المالكة مما يعد انتهاكًا لحقوق الملكية الفكرية ، وتشمل هذه التعديلات إدخال ميزات جديدة، مثل دعم لغات إضافية أو تحسينات برمجية لم تكن موجودة في النسخة الأصلية، وقد يتم ذلك بهدف تحسين تجربة المستخدمين أو زيادة انتشار البرنامج في مناطق معينة.[2]

---

[1] شيرين عبد السلام، اهم برامج الحاسب الالي،2سبتمبر2023 ، مقال منشور على الموقع الالكتروني أهم برامج الحاسب الآلي ووظائفها - موسوعة ،تاريخ الاطلاع 12 مارس 2025 ،على الساعة 22:09.

[2] غادة نصار ، الارهاب و الجريمة الالكترونية ، الطبعة الأولى ، العربي للنشر والتوزيع ،القاهرة ،2017، ص 21 .

يتم التعديل على البرامج في بعض الحالات بحذف بعض الوظائف الأساسية أو تعطيل آليات الحماية التي تفرضها الشركات المنتجة، مما يسمح باستخدامها بطرق غير مشروعة، كما قد يعمد البعض إلى إزالة أو تغيير بيانات حقوق النشر الخاصة بالمطورين الأصليين، أو حتى إعادة نشر البرامج تحت أسماء مختلفة، مما يسهم في انتشار نسخ غير مرخصة.[1]

تُستخدم في هذه العمليات أدوات متخصصة تتيح فك تشفير البرمجيات وتعديل ملفاتها الداخلية، مما يسهل إعادة توزيع البرامج المعدلة، وعلى الرغم من أن بعض هذه التعديلات قد تبدو مفيدة للمستخدمين، إلا أنها تشكل تعديًا على الحقوق القانونية لأصحاب البرامج.

2. قرصنة البرامج :

عند شراء البرامج، لا يحصل المستخدم على ملكيتها الفعلية بل يُمنح ترخيصًا لاستخدامها وفق شروط محددة، مثل منع نسخها أو توزيعها على أجهزة أخرى ، وتُعرف قرصنة البرامج بأنها الاستخدام أو التوزيع غير القانوني للبرمجيات، سواء لأغراض تجارية أو شخصية أي الحصول على نسخة غير مرخصة من البرنامج الالكتروني، وبعبارة أخرى من غير دفع القيمة المالية، التي تمثل ثمن النسخة الاكترونية للبرنامج .[2]

يمثل هذا الاعتداء انتهاكًا للحقوق الفكرية والمادية للشركات المنتجة مثل مايكروسوفت ، الفابت وأوراكل حيث يؤدي ذلك إلى خسائر مالية تؤثر على استقرارها الاقتصادي وعلى حقوق العاملين فيها .

---

[1] أسامة بن يطو، حمزة عبدلي ، حماية برامج الحاسب الالي في ضوء التشريع الجزائري و المواثيق الدولية ،مجلة المعارف جامعة اكلي محند الحاج ، البويرة ، العدد 19 ، ديسمبر2015 ،ص137.

[2]عبد الرحمان نشادي، الجرائم المعلوماتية في وسائل الاتصال الحديثة ،رسالة دكتوراه ، كلية العلوم و الاتصال ،جامعة الجزائر 3 ،2017 ،ص 147 .

3. انشاء برامج وهمية :

تصمم البرامج الوهمية لاستهداف الأنظمة الرقمية و المستخدمين ، ويتم ذلك باستخدام الطرق الاحتيالية كالخداع او الاستغلال الرقمي ، تعتمد على تقديم واجهات مزيفة توهم المستخدمين بوظائف غير موجودة ، مثل التطبيقات التي تدّعي توفير الحماية من الفيروسات لكنها في الواقع تعرض تحذيرات كاذبة لدفع المستخدمين إلى شراء إصدارات مدفوعة دون جدوى ، كما تنتشر برامج أخرى تُسوَّق على أنها أدوات لتحسين الأداء أو الاستثمار المالي ، لكنها تعمل فقط على خداع الضحايا وجمع الأموال قبل أن تختفي دون تقديم أي خدمة حقيقية ، وغالبًا ما يتم الترويج لهذه البرامج عبر مواقع غير رسمية وإعلانات مضللة، مما يزيد من صعوبة اكتشاف حقيقتها قبل وقوع المستخدمين في الاحتيال ، وفي بعض الحالات لا تقتصر هذه الأساليب على الأفراد بل تتسع لتشمل مؤسسات بأكملها، حيث يتم إنشاء شركات وهمية تعتمد على برامج مُزيفة لإدخال بيانات غير حقيقية في الأنظمة المالية [1].

أما النوع الاخر القائم على استخدام برامج ناقصة فتأخذ طابعًا أكثر تعقيدًا، حيث يتم تطويرها بوظائف حقيقية لكنها تحتوي على ثغرات تتيح للمبرمج أو الجهة المطوِّرة استغلالها لاحقًا، في بعض الحالات، تُستخدم هذه البرامج داخل الأنظمة المالية، حيث يتم تضمين فجوات صغيرة تتيح التلاعب بالحسابات دون اكتشاف فوري[2]، كما قد يتم برمجتها بحيث تتضمن "أبوابًا خلفية"

[1] محمد احمد الشوابكة ، المرجع السابق ، ص ص236-237.

[2] بشار خليل ، ما هو هجوم الباب الخلفي؟ المعنى، التعريف، الأمثلة ، مقال منشور على الموقع الالكتروني https://www.scs.org.sy/?q=scs/infomag/showarticlenode&id=921 ،تاريخ الاطلاع 17مارس20225،على الساعة 18:20.

(Backdoors)[1] تُمكّن الجهة المطوِّرة من الوصول إلى النظام أو تعديله حتى بعد تسليمه، وفي بعض الأحيان ، يتم توزيع البرامج الناقصة عمدًا من قبل الشركات لإجبار المستخدمين على شراء تحديثات أو إصلاحات ، مما يجعلها أداة لتحقيق أرباح غير مشروعة.[2]

الفرع الثاني : الاحتيال عبر البريد الإلكتروني

يعد البريد الإلكتروني وسيلة فعالة لتبادل الرسائل الإلكترونية بين الأجهزة المتصلة بشبكة الإنترنت، حيث يسمح بإرسال واستقبال الرسائل النصية، الصور، والمرفقات مثل المستندات أو ملفات معالجة النصوص، يتم إرسال هذه الرسائل عبر نظام بريد إلكتروني يتم تعيينه بعنوان خاص بكل مستخدم والذي بدوره يتيح له التواصل مع الآخرين على نطاق واسع عبر الشبكة الأنترنيت ، كما أن العديد من الشركات تقدم هذه الخدمة بشكل مجاني مما يسهل الوصول إليها، [3]إلا انها تستخدم بطرق غير مشروعة وذلك باستغلال الثغرات في الأنظمة الإلكترونية مما يجعل البريد الإلكتروني البيئة الانسب لجرائم الاحتيال ،و يظهر ذلك من خلال مايلي :

أولا : احتيال اليانصيب

يشير احتيال اليانصيب الى نوع من الاحتيال الذي يبدأ برسوم مسبقة مصحوبة بإشعار غير متوقع عبر البريد الإلكتروني يزعم أن المستلم قد فاز بمبلغ كبير في الياناصيب ،غالبًا ما يُطلب

[1] الباب الخلفي هو وسيلة تُمكّن المهاجمين من الوصول إلى نظام أو برنامج معين دون الحاجة إلى المرور عبر إجراءات الأمان العادية مثل كلمات المرور أو التحقق من الهوية، يتم إنشاء هذه الأبواب الخلفية إما عمدًا من قبل المطورين لأغراض الصيانة، أو يتم زرعها بشكل خفي من قبل مجرمي الإنترنت لاستغلالها لاحقًا.

[2] بلال بن جامع ، الجرائم المعلوماتية على شبكة الأنترنيت دراسة حالة جامعة عبد الحميد مهري قسنطينة 2 ، أطروحة دكتوراة في علم المكتبات و التوثيق ، معهد علم المكتبات و التوثيق ، جامعة قسنطينة 2 عبد الحميد مهري ، 2017/2016، ص 227.

[3] أوشن حنان ، وادي عماد الدين ، الإثبات الجنائي و الوسائل العلمية الحديثة ، دون طبعة، دار الخلدونية للنشر والتوزيع، الجزائر ، 2015 ، ص 115.

من الضحية الحفاظ على سرية هذا الإشعار بسبب "أخطاء في بعض الأرقام"، ويُوصى بالاتصال بـ "وكيل المطالبات" عند الاتصال، يطلب الوكيل عادة من الضحية دفع "رسوم المعالجة" أو "رسوم التحويل" حتى يتمكن من توزيع الأرباح، مع التهديد بعدم تلقي أي دفعات إذا لم تُدفع هذه الرسوم.

في العديد من الحالات ، يواجه الضحايا الذين يوافقون على الدفع طلبات مستمرة لتغطية "نفقات غير متوقعة"، مما يؤدي إلى سلسلة من المطالبات المالية التي تستمر حتى يدرك الضحية ما يحدث أو يستنفد أمواله ، في بعض الحالات يقدم المحتالون للضحايا خيار فتح حساب بنكي معني كبديل لدفع الرسوم مقدمًا ، يتم فرض إيداع مبدئي قدره 3000 دولار كشرط لفتح الحساب، إلا أن البنك المعني يكون وهميًا، رغم أنه قد يبدو شرعيًا بوجود موقع إلكتروني رسمي، يستخدم العديد من رسائل البريد الإلكتروني الاحتيالية اسماء يانصيب شرعية أو مؤسسات معروفة لتعزيز مصداقية الاحتيال، رغم أن هذا لا يعني أن تلك المنظمات أو المؤسسات تشارك في أي نوع من الاحتيال.[1]

ثانيا : مخطط الاحتيال النيجري 419

يشير "احتيال 419 النيجيري" إلى نوع من الخداع القائم على خيانة ثقة الضحية، حيث يتم إقناعه بدفع مبالغ مالية صغيرة نسبيًا على أمل الحصول لاحقًا على مكاسب مالية أكبر بكثير ، **و** تعود تسمية "419" إلى رقم المادة في القانون الجنائي النيجيري التي تجرّم هذا النوع من الأنشطة الاحتيالية.

[1] عبد الرحمان النشادي المرجع السابق، ص 123 .

ارتبط هذا النوع من الاحتيال في بداياته بمواطنين نيجيريين، إلا أن انتشاره تجاوز الحدود الجغرافية، حتى أصبح يُعرف عالميًا باسم "الاحتيال النيجيري" أو "احتيال 419"، يتميز هذا الاحتيال بطابعه العابر للحدود وبقدرته على التكيّف مع مختلف السياقات الثقافية والاجتماعية ، مستغلاً الطمع أو الثقة الزائدة لدى الضحايا لتحقيق أهدافه الاحتيالية، ويكون هذا بطرق التالية:

1- إرسال رسائل إلى الأفراد تُفيد بوجود إرث ضخم ، تركت من طرف شخصً ثري أو احد النبلاء في وصيته ، وغالبًا ما تُرفق مع هذه الرسائل وثائق مزورة على شكل وصايا قانونية ، تُظهر أن التواصل تم عبر مكاتب محاماة مزعومة تمثل أقارب المتوفى، ويتم خداع الضحايا من خلال دعوتهم للمطالبة بالإرث ، بشرط تقديم بياناته الشخصية البنكية و المالية اضافة الى دفع رسوم أولية تُوصف بأنها "رسوم قانونية" أو "رسوم معالجة"، في حين أن هذه الأموال لا وجود لها ، اي ان الهدف الحقيقي من هذه المراسلات هو الاستيلاء على المبالغ المدفوعة.[1]

2- إرسال رسائل عبر البريد الإلكتروني تبدو في ظاهرها صادرة عن جهات رسمية ، مثل مؤسسات حكومية أو البنك المركزي أو شركات نفط كبرى أو حتى مكاتب محاماة، وتزعم هذه الرسائل أن هناك مبالغ مالية ضخمة مودعة في نيجيريا، ويجب نقلها إلى الخارج بشكل عاجل لتفادي مصادرتها، بحيث يتم إقناع الضحية بالمساعدة في تحويل هذه الأموال، من خلال تزويدهم بتفاصيل حساباتهم البنكية لتسهيل التحويل المالي، ومع مرور الوقت، يبدأ المحتالون بطلب مبالغ مالية تدريجية تحت مسميات مختلفة مثل الضرائب، أو رسوم حكومية، أو تكاليف التدقيق

[1] خالد حامد مصطفى ، المسؤولية الجنائية لناشري الخدمات التقنية و مقدميها عن سوء استخدام شبكات التواصل الاجتماعي ،مجلة رؤى استراتجية ،مركز الامرات للدراسات و البحوث الاستراتجية ، المجلد 1 ، العدد 2 ، 2013 ، ص 12.

والتأمين، بل وأحيانًا يُطلب دفع رشاوى للمسؤولين ، ويستمر الضحايا في دفع هذه المبالغ على أمل الحصول على نسبة من الأموال الموعودة ، والتي في الواقع لا وجود لها.[1]

3- إرسال رسائل عبر البريد الإلكتروني مستهدفة الأفراد الذين قاموا بنشر سيرهم الذاتية على مواقع التوظيف الإلكترونية، حيث تحمل الرسالة شعاراً مزيّفاً لشركة تبدو رسمية ، وتتضمن عرض عمل مغرياً يتحدث عن راتب مرتفع وامتيازات، وغالباً ما يُطلب من الضحية الحصول على "تصريح عمل" يتيح له العمل في الدولة المعنية، ويُدرج في الرسالة اسم مسؤول حكومي للتواصل ، وبعد تواصل الضحية يبدأ بابتزازها عبر فرض رسوم متعددة مرتبطة بالحصول على التصريح وإجراءات أخرى، إلى أن تكتشف الضحية أنها وقعت ضحية لعملية احتيال منظمة[2].

ثالثا : الاحتيال الهرمي

تُعتبر طريقة الاحتيال عبر الرسائل المتسلسلة أو طريقة الهرم إحدى الأساليب الشائعة الاحتيال، يقوم المحتالون بإرسال رسائل عبر البريد الإلكتروني تتضمن قائمة تحتوي على عدد من الأسماء، في هذه الرسائل يُطلب من المستقبل إرسال مبلغ من المال إلى الشخص الوارد اسمه في أعلى القائمة بعد دفع المبلغ ، يُطلب من المستقبل شطب الاسم الوارد في الأعلى وإضافة اسمه في أسفل القائمة ، ثم يرسل الرسالة إلى مجموعة من الأشخاص الآخرين ليقوموا باتباع نفس الخطوات[3].

[1] عبد الرحمن ، محمد قدري حسن، جرائم الاحتيال الالكتروني ، مجلة الفكر الشرطي ، المجلد 20، العدد79 ، مركز بحوث الشرطة ، القيادة العامة لشرطة الشارقة ، الامارات، اكتوبر 2011 ، ص 108.

[2] عبد الرحمان النشادي ، المرجع سابق ، ص 124.

[3] اسماء مبارك الريامي، المرجع السابق، ص 57 .

يهدف المحتالون من هذه الطريقة إلى تمكين الشخص الذي يتلقى الرسالة من دفع اسمه إلى الأعلى، ما يؤدي إلى تلقيه أموالًا من الأشخاص الذين سينضمون إلى السلسلة ويدفعون المبالغ المقررة، ولكن مع مرور الوقت يدرك الضحية أن الأسماء الموجودة في القائمة هي في الغالب لأشخاص من نفس المحتال، وبالتالي يتم استغلال الضحايا للحصول على الأموال دون أي تعويض مالي لهم، في النهاية يتضح أن هذا النوع من الاحتيال يعتمد على إيهام الضحايا بالحصول على مكاسب مالية بينما في الواقع يتم استنزاف أموالهم لصالح المحتال الذي يدير العملية.

الفرع الثالث : الاحتيال في وسائل التواصل الاجتماعي

وسائل التواصل الاجتماعي هي منصات رقمية تتيح للمستخدمين التواصل والتفاعل مع الآخرين من خلال تبادل المعلومات والأفكار والمحتوى، أصبحت هذه الوسائل جزءًا أساسيًا من حياتنا اليومية، حيث تمكن الأفراد من التواصل ومتابعة الأحداث العالمية وكذلك متابعة الأخبار والعروض التجارية ، تشمل هذه الوسائل منصات شهيرة مثل فيسبوك، تويتر، إنستغرام، سناب شات، واتساب ..... ، ومع تزايد استخدام هذه الوسائل في جميع أنحاء العالم، تزايدت أيضًا المخاطر الأمنية المرتبطة بها، خاصة فيما يتعلق بالخصوصية والاحتيال باستخدام تقنية المعلومات ، ويظهر ذلك في ما يلي :

أولا : التصيد الاحتيالي

التصيّد الاحتيالي هو نوع من الهجمات الإلكترونية التي تستهدف خداع الأفراد أو المؤسسات للحصول على معلومات حساسة مثل كلمات المرور، ارقام بطاقات الائتمان او بيانات شخصية اخرى ، يتم تنفيذ هذا النوع من الهجمات باستخدام أساليب هندسة اجتماعية وهو استغلال ثقة الضحايا بدلا من الثغرات التقنية ، حيث يتنكر المحتالون في صورة جهة موثوقة ، مثل البنوك

أو شركات الخدمات، بهدف دفع الضحية إلى اتخاذ إجراء غير مدروس كإدخال بيانات شخصية أو مالية عبر وسيلة إلكترونية لا أساس لها ، تعتبر هذه الهجمات من أكثر أنواع الهجمات انتشارًا في وسائل التواصل الاجتماعي نظرًا لفعالية الأساليب المستخدمة فيها وسهولة استهداف الضحايا.[1]

يتضمن التصيّد الاحتيالي استخدام رسائل إلكترونية أو مكالمات هاتفية ما يعرف بالتصيد الشفهي، تعتمد على استخدام الصوت عبر بروتوكولات الإنترنت مثل المكالمات الهاتفية العادية أو الخلوية للوصول إلى المعلومات الشخصية والمالية للأفراد لتحقيق مكاسب مالية غير مشروعة بعد سرقة أرقام بطاقات الائتمان عن طريق خداع الضحية وإقناعها بأنها ستفوز بجائزة أو تحصل على خدمة مجانية.[2]

كما يتضمن التصيد الاحتيالي استخدام رسائل نصية قصيرة (SMS) تحمل رابطًا إلى موقع إلكتروني مزيف ، قد يبدو للوهلة الأولى أنه تابع لمؤسسة مشهورة وموثوقة ، وعند قيام الضحية بالنقر على الرابط يُطلب منها إدخال بيانات شخصية ، و في بعض الحالات قد يتم استخدام برامج خبيثة لتحميلها على الأجهزة لاستغلال المعلومات المخزنة أو تسجيل نشاطات التحويلات المالية .

[1] خالد بن سليمان الغثنبر ، سليمان عبد العزيز الهيشة ، الاصطياد الالكتروني الاساليب و الاجراءات المضادة ، الطبعة الاولى ، الرياض ، السعودية، 2009 ،ص 45.

[2] عبد الرحمان النشادي ، المرجع سابق ، ص 132.

ثانيا : الاحتيال عبر انتحال الهوية

يُعد انتحال الهوية أحد الأساليب الاحتيالية الشائعة في البيئة الرقمية ، ويقصد به قيام شخص بالحصول على معلومات تعريفية تخص شخصًا آخر سواء أكان طبيعيًا أو معنويًا واستخدامها بهدف تقمص هويته لتحقيق مكاسب غير مشروعة.[1]

تُستخدم بيانات الهوية المنتحَلة مثل الاسم، الصورة، العنوان، أو غيرها من المعلومات الشخصية لإنشاء حسابات وهمية تُستخدم لاحقًا في تنفيذ عمليات احتيالية ، وتتمثل أبرز صور هذا النوع من الاحتيال في إرسال طلبات مالية مزيفة ، أو انتحال صفة موظف أو جهة رسمية لإقناع الضحية بتحويل مبالغ مالية ، أو الوصول إلى معلومات مصرفية تُستغل لاحقًا في سرقة الأموال.[2]

وتزداد خطورة هذا النوع من الاحتيال في مواقع التواصل الاجتماعي، التي تتيح بيئة غير محمية بشكل كافٍ، حيث تُستغل الثغرات في أنظمة التحقق من الهوية لتسريب البيانات الشخصية للمستخدمين، وبسبب ضعف الإجراءات الأمنية يتمكن المحتالون من الوصول إلى هذه البيانات واستخدامها في أنشطة احتيالية، كالقيام بإنشاءحسابات مزيفة استنادًا إلى معلومات حقيقية مسروقة .[3]

---

[1] عبد العزيز بن إبراهيم بن محمد الشبل ، الاعتداء الإلكتروني : دراسة فقهية ، دون طبعة، دار كنوز اشبيليا للنشر والتوزيع، السعودية ، 2022، ص 479.

[2] دنيا عبد العزيز فهمي ، المسؤولية الناشئة عن اساءة استخدام مواقع التواصل الاجتماعي ، مجلة الحقوق للبحوث القانونية و الاقتصادية ، المجلد 2 ، العدد2، جامعة الاسكندرية ، مصر، 2019 ، ص 318 .

[3] المرجع نفسه ، ص319 .

ثالثا : الاحتيال باستخدام الروابط الوهمية

الروابط الوهمية هي إحدى أساليب الاحتيال باستخدام وسائل تقنية المعلومات التي يستخدمها الجناة على نطاق واسع عبر وسائل التواصل الاجتماعي لخداع المستخدمين واستدراجهم إلى مواقع مزيفة، يتمثل هذا النوع من الاحتيال في تعديل الروابط الأصلية أو استبدالها بروابط تحمل شكلاً مشابهًا للرابط الحقيقي بحيث تبدو آمنة وموثوقة ، لإقناع المستخدمين بالنقر عليها مؤدية بهم إلى مواقع ضارة يمكن أن تحتوي على برامج خبيثة أو تستهدف سرقة بياناتهم الشخصية مثل كلمات المرور والمعلومات المالية.[1]

غالبًا ما تكون هذه الروابط جزءًا من رسائل احتيالية مرسلة عبر الحسابات المزيفة أو الرسائل المباشرة (DM) التي تحتوي على روابط تبدو مشروعة ، مثل دعوات لزيارة صفحات تبدو مشابهة للمواقع الرسمية لمنصات التواصل الاجتماعي، هذه الروابط قد تكون أيضًا جزءًا من إعلانات مزيفة أو منشورات ترويجية مغرية.

يمكن التمييز بين عدة أنواع من الروابط الوهمية المستخدمة في عمليات الاحتيال باستخدام وسائل تقنية المعلومات و التي تظهر في ما يلي :

[1] Nihad hassan , Social media phishing: Attack tactics and mitigation strategies , منشور على الموقع الاكتروني Social media phishing: Attack tactics and mitigation strategies | Barracuda Networks Blog, على الساعة 15:50 , تاريخ الاطلاع 04/ 08 / 2025

1-التلاعب بالروابط:(URL Manipulation)

يتم تعديل الرابط الأصلي ليتضمن تغييرات طفيفة تجعله يبدو مشابهًا للرابط الحقيقي، ولكن في الواقع يؤدي إلى موقع مزيف ، قد تتضمن هذه التعديلات استخدام حروف غير مرئية أو تبديل حروف بأخرى مشابهة مثلا :

http://www.facebook.com.ajax.mul.end.ph، والذي يشير إلى صفحة مزيفة حين أن الرابط الأصلي الآمن هو: http://www.facebook.com/ajax/emu/end.php ،الفرق بين الرابطين قد لا يُلاحظ بسهولة من قبل المستخدم العادي، مما يجعله عرضة للوقوع في الفخ الاحتيال.[1]

2-استخدام الروابط المختصرة:(URL Shorteners)

يتم استخدام خدمات اختصار الروابط لتقليص الروابط الحقيقية إلى روابط قصيرة يصعب تمييزها عن الروابط الأصلية، يمكن للجناة استخدامها لإخفاء الوجهة الفعلية للرابط وتوجيه المستخدمين إلى مواقع احتيالية.

3-خطأ الكتابة في النطاق:(Typosquatting)

هذا النوع من الاحتيال يعتمد على استغلال الأخطاء الإملائية الشائعة التي يرتكبها المستخدمون عند كتابة الروابط، يقوم المحتال بتسجيل اسم نطاق مشابه جدًا للموقع الشرعي، ويُستخدم بشكل متزايد في وسائل التواصل الاجتماعي حيث يستغل المحتالون طبيعة التفاعل السريع وضعف

[1] عبد الرحمان نشادي ، المرجع سابق ، ص 134.

الانتباه لدى المستخدمين، فيعمدون إلى إرسال روابط مزيفة عبر الرسائل المباشرة أو نشرها ضمن تعليقات أو منشورات تبدو موثوقة.

غالبًا ما تختلف هذه الروابط عن الأصل بحرف واحد أو عبر تبديل بسيط (مثل استبدال حرف "o" برقم "0")، تؤدي بالمستخدم إلى مواقع مزيفة تُحاكي التصميم البصري للموقع الأصلي بهدف خداعه وسرقة بياناته الشخصية، كما تُستخدم هذه التقنية في الإعلانات الممولة الوهمية التي تروج لعروض مزيفة عبر روابط تحتوي على نطاقات مشابهة للمواقع المعروفة، مما يزيد من احتمالية استدراج الضحايا للهجمات الإلكترونية ، على سبيل المثال قد يظهر الرابط الوهمي على الشكل التالي :[1]

الرابط الأصلي : http://www.google.com

الرابط الوهمي : http://www.goglle.com

[1] Perbh dev singh , URL manipulation techniques: Punycode, typosquatting, and more , منشور على الموقع الالكتروني URL manipulation techniques: Punycode, typosquatting, and more | Barracuda Networks Blog, تاريخ الاطلاع04/ 08 / 2025 ,على الساعة 17:00

خلاصة الفصل الأول :

نخلص مما سبق التطرق إليه في هذا الفصل ، إلى أن هذه الجريمة قد فرضت نفسها كأحد أبرز مظاهر الانحراف في العصر الرقمي ، لما تتسم به من خصائص قانونية وتقنية تجعلها تختلف جذريًا عن صور الاحتيال التقليدي.

فقد أصبحت الوسائل المعلوماتية أداة مركزية في تنفيذ أفعال احتيالية معقدة ، تتسم بالسرعة والدقة والقدرة العالية على التمويه والخداع ، مما يصعّب من عملية اكتشافها في مراحلها الأولى وقد ساهم هذا الواقع الرقمي في خلق بيئة خصبة لظهور فئة جديدة من الجناة تعتمد في نشاطها الإجرامي على المعرفة التقنية والمهارات الإلكترونية المتقدمة ، بعيدة عن الأساليب التقليدية التي كانت تعتمد على الاتصال المباشر بالضحية.

كما تبيّن من خلال هذا الفصل أن جريمة الاحتيال المعلوماتي تتسم بمرونة كبيرة في الوسائل والأساليب ، وتتنوع صورها وهو ما يُضفي عليها طابعًا خاصًا سواء من حيث طريقة تنفيذ هذه الجريمة أو من حيث طبيعة البيانات والمعلومات المستهدفة.

وبذلك، يمكن القول إن الاحتيال باستخدام وسائل تقنية المعلومات يُمثل نموذجًا متطورًا للجريمة، لا يقتصر أثره على الجانب المالي فحسب ، بل يتعداه ليشمل الثقة في المنظومة الرقمية برمّتها، ويُبرز حجم التحوّل الذي طرأ على الجريمة نتيجة التقدّم التكنولوجي المستمر.

الفصل الثانى :

المواجهة الاجرائية لجريمة الاحتيال باستخدام وسائل تقنية المعلومات

تمهيد :

فرضت الجرائم المعلوماتية واقعًا جديدًا على المنظومات القانونية والإجرائية، نتيجة لما تتسم به من خصائص فريدة تتعلق ببيئتها الرقمية، ووسائل ارتكابها غير التقليدية، وصعوبة تعقّب الجناة داخل فضاء افتراضي تتلاشى فيه الحدود الجغرافية، بحيث لم يعد كافيًا التعامل مع هذه الجرائم من خلال أدوات الإثبات والتحري الكلاسيكية، بل أصبح من الضروري تبني آليات مستحدثة تراعي طبيعتها التقنية، وتسمح بتأمين الاستجابة الإجرائية المناسبة التي تضمن فعالية العدالة الجنائية في ظل هذا التحول الرقمي المتسارع.

وانطلاقًا من ذلك، تقتضي مواجهة جريمة الاحتيال باستخدام وسائل تقنية المعلومات الجمع بين بعدين متكاملين: بُعد إجرائي يتعلق بوسائل الاستدلال وإثبات الجريمة، وبُعد قانوني يرتبط بالسياسات التشريعية والجزاءات العقابية.

لذا نقسم هذا الفصل إلى مبحثين:

المبحث الأول : الاستدلال كوسيلة لإثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات

المبحث الثاني : مكافحة جريمة الاحتيال باستخدام وسائل تقنية المعلومات

المبحث الأول

الاستدلال كوسيلة لإثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات

أحدثت الثورة الرقمية تغييرا في مفهوم الجريمة بحيث انها لم تعد محصورة في الأوساط التقليدية، بل اِمتدت إلى الفضاء الإلكتروني حيث باتت جرائم الاحتيال المعلوماتي من أبرز التحديات التي تواجه العدالة الجنائية الحديثة، فالجاني اليوم قد يختبئ خلف شاشات الحواسيب أو الهواتف الذكية مستخدماً تقنيات معقدة لتنفيذ مخططاته الاحتيالية، مما يصعّب من مهمة كشفه بالطرق المعتادة.

أمام هذا التطور برزت أهمية الاستدلال الإلكتروني كوسيلة أساسية في تتبع الجريمة الرقمية، وذلك من خلال وسائل واجراءات متقدمة تشمل المعاينة الإلكترونية لمسرح الجريمة الافتراضي، التفتيش الإلكتروني للأجهزة والأنظمة و الضبط المعلوماتي للبيانات الرقمية ذات الصلة، إضافة إلى تحليل الأدلة الرقمية واِستخلاص ما يثبت وقوع الجريمة ونسبتها إلى مرتكبها.

ويثور التساؤل عن مدى حجية المخرجات الاِلكترونية في الاِثبات، نظرا لطبيعتها الخاصة بالمقارنة بوسائل الاِثبات التقليدية .

بناءا على ذلك ارتأينا تقسيم هذا المبحث لمطلبين، نستعرض اجراءات التحري في جريمة الاِحتيال المعلوماتي(المطلب الأول)، و الدليل الرقمي في جريمة الاحتيال المعلوماتي(المطلب الثاني)

المطلب الأول

اجراءات التحري في جريمة الاحتيال بِاستخدام وسائل تقنية المعلومات

برزت جريمة الاحتيال باستخدام وسائل تقنية المعلومات كإحدى أخطر صور الجرائم المعلوماتية، فقد فرضت خصوصيات هذا النوع من الجرائم تحديات كبيرة أمام أجهزة إنفاذ القانون لاسيما على مستوى مرحلة التحري، ما استوجب إعادة النظر في آليات التحري التقليدية، و سعى المشرّع الجزائري الى العمل على مواءمة المنظومة القانونية مع هذا النوع من الإجرام المستحدث من خلال الإبقاء على الإجراءات الكلاسيكية كالمعاينة، التفتيش و الضبط و الخبرة إلى جانب إدراج آليات تحرٍ متطورة تتلاءم مع البيئة الرقمية، وذلك بموجب القانون 06-22[1] المعدل لقانون الاجراءات الجزائية، حيث أتاح اعتماد اجراءات جديدة كالتسرب ، اعتراض المراسلات و تسجيل الاصوات والتقاط الصور اضافة الى المراقبة الإلكترونية، ويأتي هذا التكامل بين الاجراءات التقليدية والمستحدثة كآلية تشريعية تهدف إلى ضمان فعالية البحث والتحري دون الإخلال بمبادئ الشرعية والإجراءات العادلة.

وعليه يتم التطرق الى الاجراءات التقليدية (الفرع الأول) بعدها دراسة الاجراءات المستحدثة (الفرع الثاني) .

[1] قانون رقم 06-22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

الفرع الأول : الإجراءات التقليدية للتحري في جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تُعد الاجراءات التقليدية للتحري، أساسية في الكشف عن الجرائم، وقد تم تبنيها أيضاً في التعامل مع الجريمة المعلوماتية رغم خصوصيتها، ويكمن دور هذه الإجراءات في جمع الأدلة المادية والرقمية ذات الصلة، مع ضرورة مراعاة الدقة التقنية عند تنفيذها، تجنبًا لأي مساس بسلامة البيانات أو فقدانها؛ وعلى الرغم من استناد هذه الوسائل على القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية، فإن فعاليتها في هذا المجال تتوقف على مدى ملاءمتها للبيئة الرقمي.

أولا: المعاينة

تهدف المعاينة بِاعتبارها اِجراء من إجراءات التحقيق الابتدائي إلى مشاهدة واثبات الآثار المادية التي خلفها ارتكاب الجريمة بهدف الحفاظ عليها من التلف أو التعديل أو الإخفاء، وهي إجراء غالبا ما يكلف به ضباط الشرطة القضائية حسب المادة 49[1] من قانون الاجراءات الجزائية الجزائري "اذا اقتضى الامر اجراء معاينات لا يمكن تأخيرها فلضابط الشرطة القضائية ان يستعين بأشخاص مؤهلين لذلك..." ، قضاة التحقيق وذلك وفق المادة 79[2] من نفس القانون، وتكتسب المعاينة أهمية خاصة في الجرائم التقليدية التي تترك آثارًا مادية بمسرح الجريمة تُمكن من التحفظ عليها وتحليلها لاحقًا، أما في الجرائم المعلوماتية فتتراجع هذه الأهمية لعدة أسباب، أبرزها قلة

[1] انظر المادة 49 من الأمر رقم 15-02 المؤرخ في 23 جويلية 2015 المعدل و المتمم للأمر رقم 66-155 المؤرخ في 8 جوان 1966، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد40، الصادر بتاريخ 23 جويلية 2015.

[2] انظر المادة 79 من قانون الاجراءات الجزائية.

الآثار المادية الناجمة عنها وطول المدة التي قد تفصل بين ارتكاب الجريمة واكتشافها، ما قد يُعرض الأدلة الرقمية للضياع أو التلاعب[1].

وتختلف المعاينة في جريمة الاحتيال المعلوماتي بحسب طبيعة الجريمة، فإذا كانت الجريمة مرتكبة بواسطة الحاسوب فإن المعاينة تركز على الأدوات المادية المستخدمة مثل بطاقات الدفع الإلكتروني، أجهزة الصرف الآلي، وأجهزة البيع، حيث يعمل رجال الضبطية القضائية على فحص هذه الأدوات للتأكد من سلامتها أو التلاعب بها مع توثيق كل ما يُعثر عليه من خلال الصور وتسجيل تاريخ ومكان الضبط، ثم التحفظ على الأدلة في أحراز مختومة تُسلم للنيابة العامة؛ أما إذا كانت الجريمة واقعة على البيانات ذاتها فإن المعاينة تأخذ طابعاً رقمياً، حيث يطلع ضباط الشرطة القضائية على المواقع الإلكترونية والبرمجيات التي استخدمها الجاني وقد يتم نسخ البيانات الرقمية خوفاً من فقدانها، كما تتم معاينة البريد الإلكتروني، غرف الدردشة، والملفات المخزنة، وهي عمليات تقترب من التفتيش أكثر من المعاينة، كما يمكن أن تتم هذه المعاينة عن بعد عبر أجهزة أخرى متصلة بالجهاز الأصلي خصوصاً إذا كان بمكان عام مثل مقهى إنترنت، وتماشياً مع الطبيعة المتغيرة للجريمة المعلوماتية أتاحت بعض التشريعات كالقانون الأمريكي 18 U.S.code §2703[2] واتفاقية بودابست[3] إمكانية توجيه أمر تحفظ عاجل لمزودي خدمة الإنترنت لضمان الحفاظ على البيانات المعرضة للضياع أو التعديل، وهو ما تبنته أيضاً الاتفاقية

[1] علي عدنان الفيل، "إجراءات التحري و جمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية (دراسة مقارنة)"، دون طبعة، دار الكتب و الوثائق العلمية، مصر، 2012، ص32.

[2] 18 U.S. Code § 2703 - Required disclosure of customer communications or record .

[3] اتفاقية بودابست المتعلقة بالجريمة المعلوماتية، المعتمدة من طرف مجلس أوروبا في 23 نوفمبر 2001، ودخلت حيز التنفيذ في 1 يوليو 2004.

العربية التي شددت على ضرورة تمكين السلطات من اتخاذ إجراءات سريعة لحفظ المعلومات الرقمية[1].

و تبقى المعاينة ذات دور مهم في هذا النوع من الجرائم شريطة الالتزام بجملة من القواعد الفنية المتمثلة في:

- تصوير الحاسوب والأجهزة الطرفية المتصلة به، مع التركيز على الأجزاء الخلفية وتوثيق الأوضاع العامة للمكان.
- تسجيل تاريخ ووقت ومكان التقاط كل صورة بدقة لضمان توثيق سليم.
- ملاحظة طريقة إعداد النظام الإلكتروني وفحص التوصيلات والكابلات المرتبطة به.
- إجراء حصر دقيق لكافة الأجهزة الإلكترونية الموجودة في مكان المعاينة.
- في حال وجود شبكة اتصال، يجب البحث أولًا عن الخادم المركزي لتتبع الاتصالات والبيانات.
- التأكد من خلو المكان من أي مجال مغناطيسي خارجي قد يؤدي إلى تلف أو محو البيانات.
- التحفظ على محتويات سلة المهملات، بما في ذلك الأوراق الممزقة، الأقراص، والأشرطة الرقمية.
- ضبط مستندات الإدخال والإخراج الورقية المرتبطة بالجريمة.
- استخدام أجهزة مانعة للكتابة أثناء فحص الأقراص الرقمية لمنع تعديل البيانات.

[1] بن عمر ياسين، "جريمة النصب المعلوماتي(دراسة مقارنة)"، اطروحة مقدمة لنيل شهادة الدكتوراه العلوم في الحقوق، جامعة الحاج لخضر -1-باتنة، 2022/2021، ص195.

- حصر إجراء المعاينة على محققين مؤهلين يمتلكون خبرة تقنية ومعرفة في مجال الجرائم المعلوماتية.
- التحفظ على النسخ الأصلية للأدلة وعدم الاكتفاء بنسخها فقط.
- مراعاة ظروف تخزين الأدلة الرقمية، وتفادي وضعها قرب مصادر إرسال أو في أماكن غير آمنة.
- منع إدخال أي بيانات جديدة على الأجهزة، وضبط برامج النظام باستخدام أدوات تحميل متخصصة.[1]

ثانيا: التفتيش

يُعد التفتيش من أهم الإجراءات التحقيقية التي تهدف إلى كشف ملابسات الجريمة وجمع الأدلة الجنائية، إلا أنه يُعتبر من الإجراءات التي تمس بحقوق الإنسان لما له من ارتباط وثيق بحرمة الحياة الخاصة وسرية المراسلات وحرمة المسكن، وقد أحاطه المشرع بعدد من الضمانات الصارمة حمايةً لهذه الحقوق؛ ومع تطور تكنولوجيا الإعلام والاتصال وظهور الجرائم المعلوماتية كنوع مستحدث من الإجرام، برزت تحديات جديدة في تنفيذ التفتيش سواء من حيث طبيعة الأدلة المستهدفة أو من حيث الطابع اللامادي لمسرح الجريمة، فالجريمة المعلوماتية غالبًا ما ترتكب عبر بيانات إلكترونية وأنظمة رقمية يصعب الوصول إليها بالوسائل التقليدية، ولذا بات من الضروري تكييف إجراءات التفتيش مع هذه المعطيات الجديدة، من خلال وضع ضوابط قانونية دقيقة توازن بين حماية الحريات الفردية وضمان فعالية التحقيق؛ وقد تضمن القانون الجزائري رقم

[1] علي عدنان الفيل، المرجع السابق، ص33.

09-04[1] أحكاماً خاصة تتعلق بتفتيش الأنظمة المعلوماتية، تكمّلها النصوص العامة لقانون الإجراءات الجزائية بما يكفل الإطار القانوني اللازم لمواجهة هذا النوع من الجرائم.

ووفقًا للمادة 05 من القانون 09-04 ، يمكن للسلطات المختصة الدخول إلى المنظومة المعلوماتية، سواء بشكل مباشر أو عن بُعد، بهدف التفتيش في جهاز الكمبيوتر أو أحد مكوناته المادية والمعنوية[2]؛ فالحاسوب الألي ينقسم إلى مكونات مادية وأخرى معنوية كالتالي:

- **المكونات المادية:** تشمل الأجهزة الفعلية مثل وحدة الإدخال (مثل لوحة المفاتيح والفأرة)، وحدة الذاكرة (التي تخزن البيانات والبرامج)، وحدة المعالجة المركزية (CPU) التي تعالج البيانات، وحدة التحكم، ووحدات الإخراج (مثل الشاشة والطابعة).
- **المكونات المعنوية:** تشمل البرمجيات والبيانات المخزنة مثل البرامج وقواعد البيانات تعتبر هذه المكونات "كيانات منطقية"، أي أنها ليست مادية، بل بيانات إلكترونية معقدة تتطلب تقنيات خاصة للوصول إليها وفك تشفيرها[3].

كما يجدر الاشارة الى أحد صور اجراء تفتيش النظم المعلوماتية الذي أقرها المشرع الجزائري في المادة 5 من القانون 09-04 المتمثل في التفتيش عن بعد، الذي يتيح للسلطات المختصة الدخول إلى النظم المعلوماتية، بهدف الوصول إلى البيانات التي قد تكون مرتبطة بجريمة أو تخدم تحقيقًا معينًا وفي حال وجود دليل على أن المعطيات المراد الوصول إليها مخزنة في منظومة معلوماتية مرتبطة وظيفيًا بالمنظومة الأولى، يجوز تمديد التفتيش إليها بعد إخطار الجهة القضائية المختصة، أما إذا تبين أن المعطيات محل البحث مخزنة في منظومة معلوماتية تقع

[1] القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] انظر المادة 05 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] زبيحة زيدان، "الجريمة المعلوماتية في التشريع الجزائري و الدولي"، دون طبعة، دار الهدى، الجزائر، 2011، ص131.

خارج التراب الوطني فلا يُسمح بالولوج إليها إلا في إطار التعاون القضائي الدولي ووفقًا للاتفاقيات الثنائية أو متعددة الأطراف ومبدأ المعاملة بالمثل.

وغالبًا ما تكون هذه البيانات والبرمجيات المخزنة وسيلة لارتكاب الجريمة أو تحتوي على أدلة مهمة، وقد سمح القانون 09-04 في مادته السادسة[1] بنسخ هذه المعطيات أو نقلها إلى دعامات إلكترونية لتخزينها واستغلالها في التحقيق شرط أن يتم ذلك في إطار قانوني يضمن احترام حقوق الملكية الفكرية، ويُنفَّذ تحت إشراف تقنيين وخبراء مختصين لضمان الدقة والسلامة التقنية.

وعند الحديث عن تفتيش المكونات المادية للحاسوب فإن الإجراء يُعتبر أبسط نسبيًا، إذ يمكن ضبط الأجهزة وحجزها أو حتى إتلافها عند الضرورة باعتبارها أشياء مادية ملموسة، غير أن الإشكال الحقيقي يثور عند تفتيش المكونات المعنوية، كالبرامج وقواعد البيانات المحمية بكلمات مرور أو الشيفرات والتي تتطلب أدوات وتقنيات متخصصة لفك تشفيرها، لذلك يكتسي هذا النوع من التفتيش طابعًا تقنيًا معقدًا مما يستوجب إشراك مختصين في الميدان لضمان فعاليته وشرعيته[2].

ولا يمكن تنفيذ تفتيش المنظومة المعلوماتية إلا بتوفر شروط شكلية وموضوعية محددة نذكرها كالآتي:

1. الشروط الموضوعية للتفتيش الالكتروني:

يستلزم إجراء التفتيش توافر شروط موضوعية محددة، يجب على الجهة القائمة به الالتزام بها وإلا فقد الإجراء أثره القانوني، وتتمثل هذه الشروط في وجود سبب مشروع للتفتيش وتحديد المحل المراد تفتيشه، و السلطة المختصة بالتفتيش، نتفصل ذلك فيما يلي:

[1] انظر المادة 06 من القانون 04/09.

[2] زبيحة زيدان، المرجع السابق، ص135.

أ. سبب التفتيش :

يعد التفتيش من إجراءات التحقيق التي تُباشر عادة بعد وقوع جريمة معينة وإسنادها إلى شخص ما، سواء كان مرتكبًا مباشرًا لها أو مساهمًا فيها، أو عند وجود دلائل أو قرائن تشير إلى أشياء أو بيانات يمكن أن تُسهم في إثبات الجريمة أو كشف حقيقتها، ويُقصد بسبب التفتيش وجود مبرر قانوني يهدف إلى الحصول على دليل ضمن تحقيق قائم، بغرض الوصول إلى الحقيقة؛ ويشترط أن يستند هذا الإجراء إلى مبررات موضوعية توضح السبب والهدف منه وفي مقدمتها وقوع جريمة فعلية لا محتملة، فالتفتيش لا يجوز إلا إذا كانت الجريمة المعلوماتية قد حدثت بالفعل حتى وإن وُجدت مؤشرات على احتمال وقوعها، لأن ذلك يتنافى مع طبيعة التفتيش باعتباره إجراءً من أعمال التحقيق الابتدائي؛ وفي القانون الجزائري تشمل الجريمة المعلوماتية جرائم المساس بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى أي جريمة تُرتكب أو يُسهل ارتكابها بواسطة منظومة معلوماتية أو نظام اتصالات إلكتروني، مثل الهاتف المحمول أو أجهزة التسجيل أو وسائل الإعلام الإلكترونية، وهو ما يبرر قانونًا اللجوء إلى تفتيش هذه الوسائط عند قيام الدليل على استخدامها في النشاط الإجرامي، ويُشترط إلى جانب وقوع الجريمة، أن يكون هناك اتهام موجه إلى شخص معين، يتضمن دلائل قوية ترجح علاقته بالجريمة، سواء بوصفه فاعلًا أو شريكًا أو حائزًا لأدلة رقمية ذات صلة، ولا يهدف التفتيش إلى جمع الأدلة بشكل عشوائي، بل يجب أن يكون مبنيًا على معطيات جدية تُظهر احتمالية العثور على دليل ضمن النظام المعلوماتي الخاص بالشخص المعني؛ وعليه يجب أن يُبنى الإذن بالتفتيش على قرائن قانونية معقولة وأن يكون الاتهام جديًا

ومراقبًا من قبل الجهة المختصة، إذ لا يكفي مجرد الاشتباه أو الظن، بل لا بد من توفر عناصر موضوعية تعزز وجود علاقة بين الشخص محل التفتيش والجريمة المعلوماتية المرتكبة.[1]

ب. محل التفتيش:

لا يقتصر محل التفتيش في البيئة الإلكترونية على الأماكن المادية كالمنازل أو المكاتب، بل يشمل الحاسب الآلي بكل مكوناته سواء كانت مادية أو معنوية[2]، ففي جريمة الاحتيال المعلوماتي، يتمثل محل التفتيش في الأجهزة الإلكترونية التي استخدمها الجاني أو التي يُحتمل أن تحتوي على بيانات تُثبت الواقعة، مثل برامج الاحتيال، سجلات المعاملات، أو البريد الإلكتروني المستخدم في النصب؛ ويمتد التفتيش أيضًا إلى قواعد البيانات أو الحسابات الإلكترونية المحفوظة على خوادم الإنترنت، التي يمكن أن تكشف شبكات احتيالية أوسع.

ج. السلطة المختصة بالتفتيش:

يعتبر التفتيش اجراء خطير لمساسه بالحريات والحقوق الأساسية للأفراد سواء في إطار الجرائم التقليدية أو الجرائم الإلكترونية، مما يقتضي ضرورة إخضاعه لضوابط قانونية صارمة، وقد اسند المشرع الجزائري سلطة إجراء التفتيش إلى جهات التحقيق المختصة ضمانًا لاحترام مبدأ الشرعية وحماية للخصوصية، ومع ذلك وحرصًا على سرعة تنفيذ إجراءات التحقيق وفعاليتها، أجاز القانون للسلطة القضائية أن تُكلّف أعوان الضبطية القضائية بتنفيذ عمليات التفتيش كما سمح بالاستعانة بأشخاص مؤهلين في المجال المعلوماتي خاصة في القضايا ذات الطابع الرقمي، وفقًا لما نصّت

[1] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية و السياسية، المجلد 03، العدد 05، جامعة قاصدي مرباح، ورقلة، الجزائر، 2012، ص165.

[2] مجدوب نوال، "الآليات الإجرائية للكشف عن الجريمة المعلوماتية"، مجلة البحوث القانونية والاقتصادية، المجلد 06، العدد03، المركز الجامعي مغنية، الجزائر، 2022، ص196.

عليه المادة 49[1] من قانون الإجراءات الجزائية، وتُجسّد هذه الآلية التوازن بين متطلبات التحقيق وضرورة احترام الحقوق الفردية في البيئة الرقمية.[2]

2. الشروط الاجرائية و الشكلية للتفتيش الالكتروني:

تُعد الشروط الشكلية للتفتيش من الضوابط الأساسية التي فرضها المشرع بهدف تنظيم هذا الإجراء وضمان مشروعيته، فهي تمثل مجموعة من القواعد الإجرائية التي ينبغي الالتزام بها عند مباشرة التفتيش بغرض التأكد من صحته القانونية وصيانة نتائجه من البطلان، كما تهدف هذه الشروط إلى توفير الحد الأدنى من الحماية القانونية للمتهم من خلال ضمان احترام حريته الفردية ومنع التعسف أو الاستغلال من طرف الجهات المخولة بالتفتيش، وتُعتبر الشكلية، في هذا السياق أداة لضبط السلطة وتقييدها ضمن الإطار القانوني المرسوم و بذلك سنُعالج في ما يلي أهم القواعد الشكلية التي يجب توفرها عند تنفيذ إجراء التفتيش:

أ. وقت اجراء التفتيش:

لقد أولى المشرع الجزائري أهمية خاصة لمسألة وقت إجراء التفتيش إدراكًا منه لما قد ينطوي عليه هذا الإجراء من مساس بحرمة المساكن وخصوصية الأفراد، لذلك نصّ في قانون الإجراءات الجزائية على ضرورة احترام توقيت زمني محدد يتمثل في الفترة الممتدة من الساعة الخامسة صباحًا إلى الساعة الثامنة مساءً طبقا للمادة 47[3] قانون اجراءات جزائية، وهو ما يُعد قاعدة عامة تهدف إلى حماية الحقوق والحريات، غير أن المشرع وبالنظر إلى طبيعة بعض الجرائم

[1] انظر المادة 49 من الأمر رقم 15-02 الذي يتضمن قانون الاجراءات الجزائية، المعدل و المتمم.

[2] مجدوب نوال، المرجع السابق، ص197.

[3] انظر المادة 47 من الأمر 15-02 المتضمن قانون الاجراءات الجزائية.

وخطورتها، أقرّ استثناءات تسمح بتجاوز هذا التوقيت طبقا لنص المادة 3/47[1] من ق.إ.ج، شريطة الحصول على إذن مسبق من وكيل الجمهورية المختص؛ وتشمل هذه الحالات الجرائم المتعلقة بالمخدرات والجريمة المنظمة عبر الحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم غسل الأموال، والإرهاب والجرائم المرتبطة بالتشريع الخاص بالصرف؛ ويُجسّد هذا الاستثناء توازنًا دقيقًا بين ضرورة إنفاذ القانون وفعالية التحقيق من جهة، وضمان احترام الحريات الفردية من جهة أخرى.[2]

ب. وجود اذن بالتفتيش:

يشكل إذن التفتيش أحد الشروط الجوهرية التي أقرها المشرع الجزائري عند مباشرة إجراءات التفتيش في مجال الجرائم الإلكترونية وذلك بالنظر إلى ما ينطوي عليه هذا الإجراء من مساس بمبدأ السرية الرقمية وحرمة الحياة الخاصة، إذ تتطلب طبيعة هذا النوع من الجرائم تدخلاً دقيقًا وسريعًا في كثير من الأحيان بسبب سرعة زوال أو طمس الأدلة الرقمية، ومع ذلك لم يغفل المشرع الجزائري ضرورة ضبط هذا التدخل بوسائل قانونية تكفل عدم التعسف.

فاشترط صدور إذن مسبق من وكيل الجمهورية او قاضي التحقيق و ذلك تطبيقا لنص المادة 44[3]من قانون الاجراءات الجزائية، ضمانًا لاحترام الضوابط الإجرائية ومراعاة للحقوق الدستورية،

[1] انظر المادة 3/47 من نفس القانون.

[2] عز الدين عثماني، "إجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الاتصال و المعلوماتية"، مجلة دائرة البحوث و الدراسات القانونية و السياسية-محبر المؤسسات الدستورية و النظم السياسية، المجلد02، العدد04، جامعة العربي تبسي، تبسة، الجزائر، 2018، ص57 .

[3] انظر المادة 44 ق 15-02 المتضمن قانون الاجراءات الجزائية.

ويُعد هذا الإذن أداة رقابة قضائية مسبقة تهدف إلى تحقيق توازن بين متطلبات كشف الحقيقة في قضايا تقنية معقدة وبين صون الحريات الفردية من الانتهاك.[1]

ج. حضور المتهم أثناء التفتيش:

يقتضي القانون كقاعدة عامة أن يتم التفتيش بحضور المتهم أو من ينوب عنه وذلك كضمانة أساسية تصون حرمة الحياة الخاصة للأفراد ومساكنهم وتحُدّ من احتمال تعسف السلطة القائمة بالتفتيش تحت طائلة بطلان هذا الإجراء وفق المادة 45 من قانون الاجراءات الجزائية، غير أن المشرع الجزائري خرج عن هذا المبدأ في سياق الجرائم الماسة بأنظمة المعالجة الالية للمعطيات كما نصت الفقرة الثالثة من المادة 45[2] قانون اجراءات جزائية، حيث أجاز لأعوان الضبط القضائي مباشرة عملية التفتيش دون التقيد بشرط حضور المتهم أو ممثله القانوني بل حتى في غياب الشهود، مراعاة لخصوصية هذا النوع من الجرائم التي تتسم بالسرعة وسهولة إتلاف الأدلة الرقمية، ويُعد هذا الاستثناء استجابةً لطبيعة البيئة الرقمية التي تفرض مرونة أكبر في الإجراءات، شريطة أن يتم توثيق نتائج التفتيش في محضر رسمي؛ وإذ لم يضع المشرع أحكامًا خاصة بمحاضر التفتيش في الفضاء المعلوماتي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر بشكل عام وفي حال تم التفتيش من طرف قاضي التحقيق يتوجب أن يتم بحضور كاتب ضبط وأن يُوقع المحضر من طرفه، وإلا اعتُبر باطلًا؛ وتكمن أهمية المحضر في تمكين الجهات القضائية من بسط رقابتها على مدى احترام الإجراءات القانونية أثناء التفتيش، مما يضمن احترام حقوق الأفراد ويحول دون المساس بحريتهم دون سند قانوني، ويترتب على الإخلال بالمتطلبات الشكلية وفقًا للمادة 48 من قانون الإجراءات الجزائية بطلان إجراء التفتيش، وبالتالي

[1] مجدوب نوال، المرجع السابق، ص197.

[2] انظر المادة 45 من الأمر رقم15-02 المتضمن قانون الاجراءات الجزائية.

استبعاد الأدلة المستخرجة منه حفاظًا على ضمانات المحاكمة العادلة، ويُلاحظ كذلك أن هذا النوع من التفتيش يتطلب كفاءة تقنية عالية ما يستوجب أحيانًا الاستعانة بأهل الخبرة المتخصصين لضمان سلامة الإجراءات ودقة التوثيق.[1]

ثالثا: الضبط المعلوماتي

يُعد الضبط من أهم الإجراءات التي تلي عملية التفتيش، ويهدف إلى وضع اليد على كل ما له صلة بالجريمة ويسهم في كشف الحقيقة بشأنها[2]، وقد عرفه قانون الإجراءات الجزائية على أنه الاستيلاء القانوني على شيء يرتبط بجريمة وقعت، سواء كان هذا الشيء أداة استُعملت في ارتكاب الجريمة أو نتيجة عنها أو أي عنصر يفيد في إثبات التهمة أو نفيها؛ وتتحدد الطبيعة القانونية للضبط بحسب ظروفه، فإن تم تجريد شخص من حيازته لشيء معين عُدّ ذلك من إجراءات التحقيق، أما إذا تم الاستيلاء عليه دون وجود حيازة قائمة فيُعد من أعمال الاستدلال؛ وتجدر الإشارة إلى أن الضبط لا يرد إلا على الأشياء المادية، سواء كانت منقولة أو عقارات ولا يشمل الأشخاص الذين يخضعون لإجراءات قانونية مستقلة كالتوقيف أو القبض، وفي سياق الجريمة المعلوماتية تتخذ المحجوزات طابعًا مميزًا إذ قد تكون مادية مثل الحواسيب والأجهزة الرقمية، أو إلكترونية كالمعطيات والبيانات المعالجة رقمياً وهو ما يفرض تكييفًا خاصًا للإجراء وضوابط تقنية تضمن قانونيته وحجّيته أمام الجهات القضائية.[3]

ولقد نصّ المشرع الجزائري صراحة على إجراءات ضبط المعطيات المعلوماتية في المواد من 6 إلى 9 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

[1] مجدوب نوال، المرجع السابق، ص198.

[2] رشيدة بوكر، الحماية الجزائية للتعاملات الالكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020، ص 540.

[3] علي عدنان الفيل، المرجع السابق، ص54.

والاتصال ومكافحتها[1]، حيث بيّن أن السلطة التي تباشر التفتيش إذا عثرت على بيانات رقمية تفيد في كشف الجريمة أو مرتكبيها و انه ليس من الضروري حجز كل المنظومة، يتم نسخ هذه البيانات و المعطيات على وسيط إلكتروني قابل للحجز و الوضع في احراز وفقًا للقواعد المقررة في قانون الإجراءات الجزائية[2]؛ كما أوجب القانون على السلطة القضائية المختصة ضمان سلامة هذه البيانات داخل النظام المعلوماتي واتخاذ ما يلزم من إجراءات تقنية لمنع الاطلاع أو التلاعب بها وفقا للمادة 7 من القانون 09-04، خاصة إذا تعذر نسخها لأسباب تقنية، وقد أجاز المشرع الاستعانة بأشخاص مؤهلين تقنيًا للقيام بهذه المهمة مع التأكيد على أن استعمال البيانات المستخرجة يكون محصورًا في نطاق التحقيق فقط وتحت طائلة العقوبات في حال استخدامها خارج هذا الإطار.

و تعكس هذه الأحكام وعي المشرع الجزائري بخصوصية الأدلة الرقمية وضرورة تكييف الإجراءات التقليدية مع الطابع التقني للجرائم المعلوماتية.[3]

رابعا: الخبرة

تُعد الخبرة إجراءً من إجراءات التحري الأساسية في الجرائم المعلوماتية وذلك نظرًا للطبيعة التقنية المتطورة لهذه الجرائم والتي تتطلب معرفة متخصصة لفهم كيفية ارتكابها وتعقّب آثارها الرقمية، وقد أدرك المشرع الجزائري هذه الخصوصية فنصّ في الفقرة الأخيرة من المادة الخامسة من القانون رقم 09-04 على إمكانية تسخير أي شخص مؤهل تقنيًا من قبل السلطات المكلفة بالتفتيش، وذلك لمساعدتها في التعامل مع الأنظمة المعلوماتية محل البحث أو لفهم التدابير

[1] انظر المواد من 06 الى 09 من القانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيات الاتصال و الاعلام و مكافحته.

[2] انظر المادة 06 من القانون 09-04.

[3] صالح شنين، "إجراءات التحري و التحقيق في جرائم تكنولوجيات الاعلام و الاتصال في التشريع الجزائري – القانون09_04"، مجلة الدراسات الحقوقية، المجلد 01، العدد 01، جامعة عبد الرحمان ميرة، بجاية، الجزائر، 2014، ص ص283-284.

الأمنية المطبقة على البيانات محل التفتيش، وتُشكّل هذه الاستعانة بالخبراء خطوة وقائية ضرورية في مرحلة التحري تُمكّن الجهات المختصة من اتخاذ الإجراءات المناسبة لضمان سلامة البيانات ومنع التلاعب بها، كما تتيح التعامل مع البنية التقنية للجريمة بكفاءة ودقة، ويُعتبر هذا التوجه من مظاهر تكييف الإجراءات الجزائية التقليدية مع متطلبات البيئة الرقمية الحديثة.[1]

الفرع الثاني: الإجراءات المستحدثة للتحري في جريمة الاحتيال باستخدام وسائل تقنية المعلومات

أدى التطور السريع لأساليب ارتكاب الجرائم المعلوماتية وتعقيد بنيتها التقنية للجوء المشرع الجزائري إلى استحداث جملة من إجراءات التحري الخاصة التي تراعي الخصوصية التقنية لهذا النمط من الإجرام، لا سيما في جرائم الاحتيال الإلكتروني والاعتداء على نظم المعالجة الآلية للمعطيات، وقد تمّ تبنّي مقاربة تقنية تكمّل الاجراءات القانونية التقليدية، وذلك من خلال السماح باستخدام أدوات وأساليب حديثة تعتمد على تحليل البيانات الرقمية، وتتبع أثر الجريمة عبر الشبكة المعلوماتية وفحص محتويات الأجهزة الإلكترونية، وتُصنف هذه الإجراءات المستحدثة ضمن نطاق التحريات الفنية التي تهدف إلى تمكين جهات الضبط والتحقيق من كشف الأدلة الرقمية وتحديد مرتكبي الجريمة.

ومن بين هذه الإجراءات المستحدثة التي أقرّها المشرع الجزائري، نجد المراقبة الإلكترونية، اعتراض المراسلات السلكية واللاسلكية واخيرا التسرب، باعتبارها من أبرز آليات التحري في محيط الجريمة الرقمية.

[1] حليم رامي، "اجراءات استخلاص الدليل في الجرائم المعلوماتية"، دفاتر البحوث العلمية، المجلد 09، العدد 01، جامعة البليدة2 لونيسي علي ، الجزائر، 2021، ص232.

أولا: المراقبة الالكترونية

نصّ المشرع الجزائري على المراقبة الإلكترونية كأحد الإجراءات التقنية الخاصة بالتحري التي تهدف إلى تعقّب النشاطات الرقمية للمشتبه فيهم وجمع الأدلة ذات الطبيعة الإلكترونية، وتُعرف المراقبة الإلكترونية بأنها وسيلة فنية تهدف إلى رصد وتسجيل الاتصالات الرقمية والمعلومات المتبادلة عبر الشبكات المعلوماتية، ويتم ذلك باستخدام وسائل تكنولوجية متقدمة تحت إشراف جهات مختصة ووفق ضوابط قانونية محددة؛ وقد تم إدراج هذا الإجراء بموجب القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، لاسيما في مادته الرابعة التي حددت الحالات التي يجوز فيها اللجوء إلى المراقبة الإلكترونية، ومنها الوقاية من الجرائم ذات الطابع الإرهابي، أو عند توفر معلومات جدية حول وجود تهديد موجه إلى منظومة معلوماتية تمس النظام العام أو مؤسسات الدولة أو الاقتصاد الوطني، أو في سياق التحقيقات والتحريات القضائية، وكذلك عند تنفيذ طلبات التعاون القضائي الدولي.

وتُعد المراقبة الإلكترونية من الوسائل ذات الأثر البالغ على الحقوق والحريات، خصوصًا فيما يتعلق بالحياة الخاصة وحرمة الاتصالات ولهذا قيدها المشرع بشرط جوهري يتمثل في الحصول المسبق على إذن قضائي يصدر عن السلطة القضائية المختصة، ويُشترط أن يكون مسببا ومحددًا في الزمان والمكان والهدف، كما يتم تنفيذ عملية المراقبة من قبل أعوان الشرطة القضائية المتخصصين في المجال المعلوماتي وبمساهمة مقدمي خدمات الإنترنت والاتصالات، الذين يُلزمهم القانون بتقديم البيانات التقنية المتعلقة بالاتصالات الجارية وهو ما ورد في الفصل الرابع من نفس القانون، حيث حددت المادة 11 منه طبيعة المعطيات الواجب تسليمها، وتشمل هوية

[1] القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المستخدم، نوع الأجهزة الطرفية المستعملة، توقيت ومدة الاتصالات، وأسماء المواقع التي تم زيارتها.

وفي هذا الإطار، ألزم المشرع الجزائري حسب المادة 11 من القانون 09-04 مقدمي الخدمات بحفظ هذه البيانات لمدة سنة كاملة من تاريخ تسجيلها، وهي مدة مشابهة لما هو معمول به في التشريع الفرنسي، في محاولة لضمان إمكانية الرجوع إلى البيانات في حالة فتح تحقيق لاحق.

وعليه، فإن المراقبة الإلكترونية تُعد من الوسائل الحديثة المهمة في مجال التحري الجنائي المعلوماتي، إلا أن فعاليتها تظل مرتبطة بمدى توازن استخدامها مع احترام الحقوق الأساسية للأفراد وعلى رأسها الحق في الخصوصية.[1]

ثانيا: اعتراض المراسلات السلكية و اللاسلكية

يُعتبر اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور من الوسائل التقنية المستحدثة في قانون الإجراءات الجزائية الجزائري، التي تهدف إلى تعزيز فعالية التحريات في مواجهة الجرائم المعقدة، لاسيما جرائم الاحتيال المعلوماتي التي تتسم بالغموض والسرية العالية وتُرتكب عن بعد باستعمال وسائط الاتصال الرقمية؛ وقد جاء إدراج هذه الإجراءات في المواد من 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية[2]، لمواكبة تطور الجريمة خاصة في مجالات مثل تبييض الأموال، الإرهاب، الفساد، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وهي البيئة نفسها التي ينشط فيها مرتكبوا جريمة الاحتيال المعلوماتي.

[1] بن عمر ياسين، المرجع السابق، ص ص194-196.

[2] المادة65 مكرر5 الى 65 مكرر10 من الأمر رقم 15-02 المتضمن قانون الاجراءات الجزائية.

ويتمثل اعتراض المراسلات في مراقبة سرية للمراسلات السلكية واللاسلكية، بما فيها الاتصالات الهاتفية والبيانات المتبادلة عبر الشبكة المعلوماتية، بغرض جمع أدلة ضد الأشخاص المشتبه في تورطهم في جرائم إلكترونية مثل الاحتيال عبر البريد الإلكتروني، التصيّد الاحتيالي أو إنشاء مواقع إلكترونية وهمية بهدف سرقة البيانات، ويعكس هذا المفهوم توجّه المشرّع نحو الأخذ بتفسير موسع يتماشى مع ما ذهبت إليه اتفاقية بودابست المتعلقة بمكافحة الجريمة المعلوماتية[1]، التي اعتبرت أن وسائل النقل المعلوماتي تشمل مختلف أنماط الاتصال الرقمي وليس الهاتف فحسب.

أما تسجيل الأصوات، فيقصد به تسجيل المحادثات أو المكالمات الهاتفية ذات العلاقة بالجريمة و بالنظر إلى الطبيعة التقنية المعقدة لهذا النوع من الجرائم، اعتمد المشرع الجزائري في تنظيم إجراءات تسجيل الأصوات على المعيار الموضوعي بدلًا من المعيار المكاني، أي أن العبرة ليست بمكان الحديث بل بمحتواه، وبالتالي فإن تسجيل المحادثات أو المكالمات الهاتفية يكون جائزًا قانونًا متى ما كان محتواها يحمل دلالة على ارتكاب فعل إجرامي أو الأمر بتنفيذه حتى وإن تم إجراؤها في مكان خاص، وهذا التوجه ينسجم مع ما أخذ به كل من المشرع الفرنسي والمصري، إذ يتيح للسلطات المختصة إمكانية أوسع في تتبع الجريمة، وهو ما يبدو ضروريًا في حالات الاحتيال المعلوماتي التي تعتمد في الغالب على التواصل غير الرسمي والمتنقل، مما يجعل حصر الإثبات في الأماكن الخاصة قيدًا غير واقعي ولا عملي؛ وفي السياق ذاته يُعد التقاط الصور وسيلة ضرورية في توثيق الأدلة البصرية المتعلقة بنشاط المشتبه فيه، كتوثيق لحظة استخدام جهاز إلكتروني للقيام بعملية احتيال، أو تسجيل تواجده في مكان الجريمة، ومع أن هذه الإجراءات تمثل اختراقًا لحرمة الحياة الخاصة فقد حرص المشرّع على إحاطتها بجملة من الضمانات الصارمة، كاشتراط تنفيذ ما سبق بإذن من وكيل الجمهورية المختص و تحت المراقبة

[1] اتفاقية بودابست المتعلقة بالجريمة المعلوماتية.

المباشرة منه و في حالة فتح تحقيق قضائي تتم الاجراءات السابقة الذكر بناءا على إذن من قاضي التحقيق و تحت مراقبته المباشرة و هذا وفق ما نصت عليه المادة 65 مكرر 5 من قانون الاجراءات الجزائية.

وإدراج هذه الإجراءات ضمن وسائل التحري في الجرائم الالكترونية يتماشى تمامًا مع خصوصية جريمة الاحتيال المعلوماتي، حيث أن المحتال الإلكتروني لا يعتمد أساليب مادية مباشرة بل يُخفي نشاطه خلف وسائط إلكترونية تتطلب أدوات رصد تقنية متطورة لكشفها، ومع ذلك يظل التحدي الأكبر في التوفيق بين مقتضيات مكافحة الجريمة الحديثة وضمانات حماية الحقوق والحريات الفردية.[1]

ثالثا: التسرب

نظرا لتعقيد الجرائم المعلوماتية و خاصة جريمة الاحتيال المعلوماتي والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جاء المشرع بإجراء التسرب كإحدى الوسائل الخاصة التي أقرها المشرع الجزائري بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية،[2] وذلك بغرض تعزيز فعالية التحري والكشف عن هذا النوع من الجرائم التي غالبًا ما تُرتكب في بيئات مغلقة أو من خلال شبكات معقدة يصعب اختراقها بأساليب تقليدية.

وقد تم تعريف التسرب في المادة 65 مكرر 12 من نفس القانون، على أنه: "قيام ضابط أو عون من الشرطة القضائية، تحت مسؤولية ضابط مكلف بتنسيق العملية، بمراقبة أشخاص يُشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"[3]؛ ويستمد هذا الإجراء

[1] حليم رامي، المرجع السابق، ص ص235-237.

[2] المادة 65 مكرر05 من الأمر رقم 15-02 المعدل و المتمم للأمر رقم 66-155 ، المتضمن قانون الاجراءات الجزائية.

[3] المادة 65 مكرر12 من الأمر رقم 15-02 المعدل و المتمم للأمر رقم 66-155 ، المتضمن قانون الاجراءات الجزائية.

خطورته من طبيعته السرية واعتماده على التمويه والخداع للوصول إلى المعلومة، مما يجعله أحد أخطر أدوات التحري لما ينطوي عليه من مخاطر على المتسرب نفسه، سواء من الناحية القانونية أو الشخصية.

وإن كان المشرع الجزائري أطر اجراء التسرب الكلاسيكي إلا أن هذا لا يمنع من تكييف هذه الحيلة الاجرائية مع الرقمية و بالتالي يمكن إنابة بعض رجال الضبطية القضائية لعملية التسرب الرقمي[1] على سبيل المثال، إذا كانت هناك شبكة تقوم بسرقة بيانات بطاقات الائتمان وبيعها عبر الإنترنت، قد يقوم رجال الضبطية القضائية بمحاكاة دور مشتري محتمل و الدخول إلى موقع بيع البيانات المسروقة وشراء بطاقة ائتمان مسروقة باستخدام هوية مزيفة خلال هذه العملية، يتم جمع الأدلة مثل تفاصيل الاتصال مع المحتالين، وعناوين الويب التي تُستخدم لبيع البيانات المسروقة، وبذلك نرى اهمية هذا الاجراء في مجال الاحتيال المعلوماتي حيث يعد مناسبًا من حيث الطابع الهيكلي والتنظيمي للجماعات الإجرامية التي غالبًا ما تعتمد على الاتصال الإلكتروني والتنسيق عبر وسائل رقمية يصعب كشفها دون التغلغل المباشر فيها، وهو ما يُوفره التسرب الرقمي ، فالجاني في هذه الحالة يمكن أن يُخفي هويته الرقمية الحقيقية أو يستخدم شبكات مشفرة، الأمر الذي يصعّب على السلطات تتبعه دون "اختراق" فعلي للبيئة الافتراضية أو الواقعية التي يتحرك ضمنها.[2]

حرص المشرع على وضع ضمانات موضوعية وإجرائية لهذا الإجراء لضمان تقييده بعدم التعسف، ومن أبرزها:

[1] رشيدة بوكر ، المرجع السابق ، ص554.

- اشتراط الإذن القضائي المسبق من وكيل الجمهورية او قاضي التحقيق بعد اخطار وكيل الجمهورية طبقا لنص المادة 65 مكرر11.
- تسبيب الإذن وتحديد الجريمة المعنية بالتسرب بدقة، كما تنص عليه المادة 65 مكرر 05[1].
- تحديد مدة زمنية لا تتجاوز أربعة أشهر (قابلة للتمديد بشروط) وذلك تفاديا للاستغلال المفرط لهذا الإجراء.
- سرية هوية الضابط أو العون المتسرب كما جاء في المادة 65 مكرر 13[2].

ومن الجدير بالذكر أن المشرع الجزائري، بموجب المادة 26 من القانون 05/20 المتعلق بالوقاية من التمييز وخطاب الكراهية[3]، وسّع نطاق تطبيق التسرب ليشمل أيضًا الجرائم المرتبطة بخطاب الكراهية، مما يعكس مرونة الإجراء في التكيف مع مختلف الجرائم المستحدثة.

يعد التسرب الإلكتروني رغم خطورته إجراءً فعالًا وضروريًا للكشف عن الجرائم المعلوماتية المعقدة وعلى رأسها الجريمة محل دراستنا جريمة "الاحتيال باستخدام وسائل تقنية المعلومات"، بشرط احترام الضوابط القانونية الصارمة التي توازن بين متطلبات التحقيق وضمانات حقوق الإنسان، خصوصًا ما يتعلق بسرية الحياة الخاصة وسلامة الأشخاص المتورطين في العملية.

[1] انظر المادة 65 مكرر05 من قانون الاجراءات الجزائية المعدل و المتمم.

[2] انظر المادة 65 مكرر13، من قانون الاجراءات الجزائية المعدل و المتمم.

[3] القانون رقم 20/05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما المؤرخ في 28 أفريل 2020، جريدة رسمية، عدد 25، الصادرة في 29 أفريل 2020.

المطلب الثاني

الدليل الرقمي في جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تُعد الجرائم المعلوماتية من أبرز صور الجريمة المعاصرة التي تطرح إشكالات قانونية معقدة، خاصة على مستوى الإثبات، إذ ان الوسائل التقليدية المعتمدة في قانون الإجراءات الجزائية لم تعد كافية للتعامل معه فقد نتج عن الطبيعة التقنية و الفنية للجرائم المعلوماتية في مجال الاثبات الجنائي شكل جديد من الأدلة، يطلق عليه الدليل الرقمي أو الدليل الالكتروني و قد اِعتدت به المحاكم الجنائية في بعض النظم القانونية المقارنة سواء من حيث قيمته القانونية أو من حيث حجيته في الاثبات .

وبذلك حري بنا معرفة الدليل الرقمي (الفرع أول) و أنواع الدليل الرقمي (الفرع الثاني) وحجية الدليل الرقمي (الفرع الثالث) .

الفرع الأول: تعريف الدليل الرقمي

لقد تعددت التعاريف المتعلقة بالدليل الرقمي إذ اختلفت بحسب الزاوية التي نظر منها الباحثون، فبينما اعتمد بعضهم على الجانب التقني في تحديد معناه، ركز آخرون على البعد القانوني.

يمكن تعريف الدليل الرقمي بأنه مجموعة من البيانات التي تُعد وتُنقل وتُخزَّن رقمياً، بحيث تُستخدم لتمكين الحاسوب من تنفيذ مهام محددة وهو كذلك الدليل الذي يستند إلى العالم الافتراضي ويقود إلى كشف واقعة غير مشروعة وربطها بمرتكبها، كما يُعرف أيضًا بأنه الدليل الناتج عن أجهزة الحاسب الآلي، ويأخذ شكل موجات أو نبضات مغناطيسية أو كهربائية تُجمع وتُحلل باستخدام تقنيات وبرامج متخصصة ليُقدَّم لاحقًا في صورة معلومات قابلة للاِعتماد أمام القضاء سواء كانت

على شكل نصوص مكتوبة، صور، أصوات، أشكال أو رسوم، بهدف إثبات العلاقة القانونية بين الجريمة وفاعلها والمجني عليه.[1]

بناءًا على ذلك، فإن الدليل الرقمي المعتمد لإثبات الجرائم المعلوماتية هو معلومات تستند إلى منطق العقل ومعايير العلم، يتم الحصول عليها بطرق قانونية وعلمية من خلال ترجمة البيانات الحسابية المخزنة في أجهزة الحاسب وملحقاته ليُعاد تفسيرها في صيغ مفهومة قابلة للتوظيف الجنائي، ولا يقتصر اِستعمال هذا النوع من الأدلة على الجرائم المعلوماتية فقط، بل يمتد ليشمل الجرائم التقليدية كالمخدرات، والقتل، والاختطاف.

ومع أن بعض التعريفات تحصر الدليل الرقمي في ما يُستخرج من الحاسب الآلي، إلا أن هذا الطرح يُعد تضييقًا لمجاله إذ يمكن أن يكون مصدر الدليل أي جهاز رقمي آخر كالهاتف المحمول، أو آلات التصوير، أو أي تقنية تعتمد النظم الرقمية في تشغيلها[2].

ترجع تسمية الدليل الرقمي، "بالرقمي" إلى البيانات الموجودة داخل الوسط الإفتراضي سواء كانت صوراً أو تسجيلات أو نصوص، والتي تأخذ شكل الرقمين (1 أو 0)، و يتم تحويلها عند عرضها لتأخذ شكل صور أو مستندات أو تسجيلات.[3]

وعليه، يمكن القول أن الدليل الرقمي هو كل ما يُستخلص من أو من خلال النظم المعلوماتية والبرمجية أو أجهزة الحاسب الآلي أو شبكات الاتصال، عبر إجراءات قانونية وفنية، ليُعرض

---

[1] بلجراف سامية، "سلطة القاضي في قبول و تقدير الدليل الرقمي"، مجلة الدراسات القانونية المقارنة ، المجلد07، العدد01، جامعة محمد خيضر ، بسكرة ، 2021، ص 679.

[2] المرجع نفسه ،ص680 .

[3] قراوي كلثوم، "مشروعية الجليل الالكتروني في الاثبات الجزائي"، مجلة طبنة للدراسات العلمية الاكاديمية ، المجلد5 ،العدد 01، جامعة الجزائر 1، 2021،ص 979 .

على القضاء بعد تحليله علميًا باستخدام أدوات متخصصة وتفسيره في صورة مكتوبة أو مرئية أو صوتية، بهدف إثبات وقوع الجريمة وتحديد المسؤولية الجنائية.

كما يجدر بالذكر أن المشرع الجزائري لم يعرف الدليل الرقمي سواء في القانون 09-04 السالف الذكر أو حتى في المرسوم 261-15[1].

وبحكم طبيعته الرقمية يتّسم الدليل الرقمي بجملة من الخصائص تميّزه عن الأدلة التقليدية وتعكس أهميته في مجال الإثبات الجنائي، فهو يعد نوعًا متطورًا من الأدلة العلمية يتميز بطبيعته غير الملموسة، حيث يتكون من بيانات ومعلومات رقمية لا يمكن إدراكها أو التعامل معها إلا من خلال أجهزة إلكترونية وبرامج تقنية متخصصة، ما يجعله بحاجة إلى بيئة تقنية متكاملة لمعالجته وفهمه كما يتمتع بطابع ديناميكي فائق السرعة، إذ يمكن نقله واسترجاعه بسهولة عبر شبكات الاتصال دون أن يحده الزمان أو المكان مما يميّزه عن الأدلة التقليدية التي تتطلب الارتباط المباشر بمسرح الجريمة.

كما يعد الدليل الرقمي دليلا قابل للِاسترجاع حتى بعد حذفه، إذ تظل آثاره الرقمية قابلة للِاستخلاص بواسطة أدوات تقنية مع احتفاظه بقيمته القانونية مما يشكل ضمانة قوية لحمايته من التلف أو الضياع، ويعزز مكانته كوسيلة إثبات موثوقة في مجال الجريمة المعلومات.[2]

[1] المرسوم الرئاسي رقم 15-261 مؤرخ في 08/10/2015 يحدد كيفية تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر العدد 35 مؤرخة في 08/10/2015.

[2] عبد القادر عميمر، "اليات اثبات الجريمة المعلوماتية في التشريع الجزائري" (دراسة مقارنة) ،أطروحة لنيل شهادة دكتوراه علوم في القانون العام تخصص القانون الجنائي والعلوم الجنائية ، كلية الحقوق ، جامعة الجزائر 1(بن يوسف بن خدة) ، 2020/2019 ، ص ص131-133.

الفرع الثاني : أنواع الدليل الرقمي

يتبين مما سبق أن من أبرز خصائص الأدلة الجنائية الرقمية هو اتسامها بطابع ديناميكي فائق السرعة، إذ يمكنها الانتقال من مكان إلى آخر عبر شبكات الاتصال متجاوزة بذلك حدود الزمان والمكان التقليديين، اِضافة اِلى اِتسامها بِارتباط وثيق بالتطور التكنولوجي المتسارع نظرا إلى البيئة الرقمية المتقدمة التي تنشأ فيها، والتي تتيح إمكانية تتبّع وتحليل المعلومات المرتبطة بسلوك الجناة في الوقت الفعلي.

انطلاقاً من الخصائص السابقة الذكر، يتخذ الدليل الرقمي أنواعا و أشكالا متعددة ومتنوعة، سيتم التطرق إليها على النحو الآتي:

أولا: أدلة اعدت لتكون وسيلة اثبات

يقصد بهذا النوع من الأدلة الرقمية تلك التي تم إنشاؤها أو حفظها من البداية في سياق وظيفي أو تقني يهدف إلى اِستخدامها لاحقًا كوسيلة إثبات قانونية ، بمعنى أن وجود هذه الأدلة لم يكن عشوائيًا أو عرضيًا بل إنها وُجدت لتسجل بيانات ومعطيات قد يُستند إليها قانونيًا لإثبات واقعة أو نفيها وهذا النوع من الأدلة يُنظر إليه عادة بدرجة عالية من الموثوقية، نظرًا لما يتمتع به من طابع موضوعي واِعتماد على الأنظمة الإلكترونية في إنشائه أو حفظه[1].

تنقسم هذه الأدلة إلى نوعين كالتالي:

[1] سالمي نضال ، "الاطار التنظيمي للدليل الرقمي في الاثبات" ، مجلة القانون و المجتمع، المجلد10، العدد01، جامعة وهران 2- محمد بن احمد-، الجزائر، 2022، ص ص335 -334.

1. التسجيلات التي تُنتج تلقائيًا بواسطة الآلة :

هي بيانات يتم توليدها بشكل أوتوماتيكي دون تدخل مباشر من الشخص المستخدم للنظام وتُعد هذه البيانات ناتجًا مباشرًا لعمل النظام أو الجهاز الإلكتروني الذي يسجّل وقائع معينة بشكل لحظي أو دوري، وتُخزَّن هذه البيانات بشكل منتظم تلقائي.

مثل:

- سجلات المكالمات الهاتفية الصادرة والواردة والتي تحفظها شركات الإتصال.
- فواتير استخدام الإنترنت، أو أنظمة تسجيل الدخول والخروج في المؤسسات، أو بيانات أجهزة التتبع.
- و يعتبر هذا النوع من أكثر أنواع الأدلة حيادية وموضوعية، نظرًا لأنه لا يخضع لإرادة الشخص أو تدخله المباشر، مما يمنح هذه السجلات حجية قوية أمام القضاء باعتبارها ناتجًا آليًا يصعب التلاعب به دون ترك أثر تقني[1].

2. السجلات التي تُنشأ جزئيًا بواسطة تدخل الإنسان وجزئيًا بواسطة الآلة :

يقوم المستخدم في هذا النوع من الأدلة بإدخال بيانات معينة إلى النظام ثم تتولى البرمجيات معالجة هذه البيانات تلقائيًا وإخراج نتائج معينة، ويمثل هذا النوع تفاعلًا بين المدخلات البشرية والعمليات الآلية، حيث يكون للإنسان دور في تزويد النظام بالبيانات الأولية في حين تقوم الآلة بمعالجة هذه المدخلات وفقًا لقواعد مبرمجة مسبقًا[2].

مثال على ذلك:

[1] بلجراف سامية، المرجع السابق، ص682.

[2] بلجراف سامية، المرجع نفسه ، ص683.

قيام موظف بإدخال معلومات مالية إلى برنامج محاسبة، ثم يقوم البرنامج بحساب الضرائب والمبالغ المستحقة وإصدار تقرير مالي نهائي.

في هذه الحالة، لا يُعتد فقط بالمدخلات، بل أيضًا بنتائج المعالجة التي أنتجها النظام وفقًا لمنطق حسابي دقيق ومحدد سابقا، مما يجعلها مقبولة كدليل تقني له قيمة إثباتية.

يعني بِاختصار يمكن القول أن الأدلة التي أُعدت لتكون وسيلة إثبات تتميز بكونها ناتجة عن أنظمة إلكترونية تحفظ وتسجّل البيانات بشكل منتظم ودقيق، إما بشكل تلقائي بالكامل أو بمزيج من التدخل البشري والمعالجة الآلية.

وتُعد هذه الأدلة ذات قيمة عالية في الإثبات القانوني نظرًا لما تتمتع به من خصائص تتعلق بالدقة والحياد وصعوبة التلاعب بها دون ترك آثار رقمية يمكن تتبعها.

ثانيا : أدلة لم تعد لتكون وسيلة اثبات

يطلق على هذا النوع في الفقه القانوني اسم "البصمات الرقمية" أو "الآثار المعلوماتية"، وهي الأدلة التي لا يقصد الفاعل أو المستخدم إنتاجها أو الاحتفاظ بها بغرض التوثيق أو الإثبات، وإنما تنشأ بشكل تلقائي وعفوي نتيجة لِاستخدامه للتقنيات أو للشبكة المعلوماتية، دون أن يكون على وعي أو رغبة بوجودها أو بتخزينها[1].

بمعنى آخر، هذه الأدلة تظهر كنتيجة عرضية أو جانبية لسلوك المستخدم، وغالبًا ما تكون من مخلفات الجريمة الإلكترونية، وتُشكّل جزءًا مهمًا من آليات تعقّب مرتكبي الجرائم المعلوماتية.

[1] بلجراف سامية، المرجع السابق، ص 684.

فتكمن خصوصية هذا النوع من الأدلة في كونه ناتجًا عن سلوك الجاني ذاته، ولكن دون قصد مباشر أو إرادة منه في حفظ ذلك الأثر الرقمي ، فالجاني أثناء ارتكابه للفعل الإجرامي عبر الوسائط الإلكترونية يترك خلفه مجموعة من البيانات التي تسجَّل تلقائيًا في أنظمة التشغيل أو على الشبكة، مثل:

- سجل الرسائل التي أرسلها أو استقبلها عبر البريد الإلكتروني أو تطبيقات التواصل الاجتماعي.
- بيانات الاتصالات عبر الإنترنت (IP address، توقيت الاتصال، مدته...)
- آثار التصفح أو تحميل الملفات.
- بصمات رقمية داخل الأجهزة المستخدمة (مثل الكوكيز، ملفات الدخول، السجلات الخلفية).

وغالبًا ما يكون الفاعل غير مدرك لحقيقة أن هذه البيانات تُحفظ أو تُسجل تلقائيًا، ما يجعلها ذات أهمية كبيرة في الإثبات، لأنها دليل على سلوك قام به حتى وإن لم تكن نيته حفظه[1].

رغم أن هذه الأدلة لم تُنشأ بقصد أن تكون وسيلة إثبات، إلا أن التطور التقني جعل من الممكن ضبطها واستخراجها باستخدام أدوات وتقنيات متقدمة حتى بعد فترة من وقوع الجريمة وهو ما يضفي عليها قيمة كبيرة في مجال التحري و التحقيق الجنائي الالكتروني، إذ تمثل شاهدًا صامتًا على ما جرى، يمكن تحليله واستنتاج معلومات بالغة الدقة عنه[2].

[1] سالمي نضال، المرجع السابق ، ص336.

[2] سالمي نضال ، المرجع نفسه ، ص337.

ومنه فإن الأدلة التي لم تُعد لتكون وسيلة إثبات هي من أهم مصادر الإثبات في مجال الجرائم الإلكترونية فهي تتميز بطابع موضوعي ودرجة عالية من المصداقية، طالما تم الحصول عليها وفقًا للقواعد القانونية وباستخدام وسائل فنية دقيقة.

تؤكد هذه الأدلة أن العالم الرقمي لا يتيح لمرتكب الجريمة الإفلات بسهولة، لأن كل تفاعل أو اتصال يترك أثرًا يمكن تتبعه لاحقًا.

إضافة الى أنواع الأدلة الرقمية التي ذكرناها سابقا ، هذا الأخير يأخذ عدة اشكال متنوعة يمكن استخلاص الدليل الرقمي منها ، نذكر اهمها كالتالي :

1. **المخرجات الورقية** :

يقصد بها النصوص أو البيانات التي يتم إدخالها عبر الحواسيب أو الآلات الرقمية، ثم تُطبع باستخدام أجهزة الطباعة الإلكترونية وتشمل هذه الفئة:

- الرسائل الإلكترونية المطبوعة.
- التقارير أو المستندات التي أُعدت عبر برامج رقمية (مثل Word أو Excel).
- بيانات المستخدم أو سجلات الدخول والخروج من الأنظمة.

ورغم أن هذه المخرجات تنتقل من الشكل الرقمي إلى الشكل الورقي، إلا أنها لا تفقد صفتها الرقمية بل يُنظر إليها على أنها تمثّل محتوى رقميًا تمت طباعته ويظل من الممكن التحقق من مصدره وصحته عبر الرجوع إلى النسخة الإلكترونية الأصلية[1].

[1] عبد القادر عميمر، المرجع السابق، ص 143.

2. أدلة إلكترونية سمعية :

المقصود بـ "أدلة إلكترونية سمعية" أو كما يسميها البعض "المخرجات الإلكترونية اللاورقية" أو "الأدلة اللاورقية"، هي تسجيلات صوتية يتم استخدامها كدليل في القضايا أو التحقيقات، ولكنها ليست موجودة على ورق[1]، بل على أجهزة إلكترونية نذكر منها مثلا :

- الأقراص المدمجة (CD / DVD).
- الأشرطة الممغنطة.
- وحدات التخزين المحمولة (USB، HDD).
- المصغرات الفيلمية (Microfilms).

3. أدلة العرض المرئي :

تمثل هذه الفئة البيانات التي تُعرض على شاشات الكمبيوتر أو عبر أجهزة العرض المرئي، وهي من أكثر الأشكال استخدامًا لعرض المعلومات لحظة إدخالها أو بعد معالجتها.

وتشمل:

- المعلومات الظاهرة على شاشة الحاسوب أثناء تنفيذ البرامج.
- نتائج المعالجة الرقمية التي تُعرض أمام المستخدم (مثل الرسائل التحذيرية، الإشعارات، نتائج البحث، إلخ).
- التفاعل البصري بين المستخدم والنظام(مثل النقر على زر، اختيار قائمة، ملء نموذج على الإنترنت...) كل هذا يتم بشكل مرئي على الشاشة.

[1] ديلمي حنان، "الدليل العلمي الالكتروني في القانون الجنائي الجزائري"، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر اكاديمي في الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريريج ، 2022/2021، ص13.

رغم أن هذه البيانات ليست مطبوعة أو محفوظة دائمًا، إلا أنها تُشكل دليلًا مهمًا إذا تم تصويرها أو تسجيلها (مثلًا عبر لقطات الشاشة أو تسجيل الشاشة بالفيديو)[1].

الفرع الثالث : حجية الدليل الرقمي في الاثبات الجزائي

لقد اصبح من الضروري البحث عن مدى حجية الأدلة الرقمية نظرا لطبيعتها التقنية و تعقيدها، أمام القضاء والضوابط القانونية والفنية التي تحكم قبولها كأساس للإدانة أو البراءة، في إطار يضمن تحقيق العدالة واحترام ضمانات المحاكمة العادلة.

أولا : شروط قبول الدليل الرقمي كوسيلة إثبات في الجريمة المعلوماتية

يُثار بشأن الأدلة الرقمية إشكال قانوني يتعلق بمدى قبولها كوسيلة إثبات أمام القضاء، وهذا بسبب طبيعتها التقنية المعقدة، وما قد تتعرض له من أخطاء أو تزييف أو تحريف أو تلف سريع، مما قد يؤثر على مصداقيتها ، و المشرع الجزائري لم يقيد هذه الأدلة بشروط قانونية محددة ، بل ترك تقديرها للسلطة التقديرية للقاضي، الذي يقع على عاتقه التأكد من توافر مجموعة من الشروط لقبولها كأساس يُبنى عليه الحكم، سواء بالإدانة أو البراءة[2].

ومن أهم هذه الشروط أن يكون الدليل الرقمي يقينياً، أي أن يقترب من الحقيقة الواقعية قدر الإمكان ويبتعد عن الظنون والتخمينات، كما يجب مناقشة هذا الدليل علنًا أمام الخصوم تطبيقًا لمبدأ شفوية المرافعة إذ تنص المادة 212 من قانون الإجراءات الجزائية الجزائري في فقرتها الثانية على أنه: "لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضورياً أمامه"[3].

---

[1] سالمي نضال ، المرجع السابق ، ص339.

[2] نور الهدى محمودي، "حجية الدليل الرقمي في اثبات الجريمة المعلوماتية" ، مجلة الباحث للدراسات الاكاديمية ، المجلد02 ، العدد11 ، جامعة باتنة 1 الحاج لخضر، الجزائر ، 2017 ، ص 919.

[3] انظر المادة 212 من الأمر رقم 15-02، المتضمن قانون الإجراءات الجزائية المعدل و المتمم.

فيفهم من ذلك أن القاضي لا يجوز له الاعتماد على رأي الغير في تكوين قناعته ما لم يكن هذا الغير خبيرًا مختصًا وقد ارتاح ضميره إلى تقريره الفني وضمنه في أسباب حكمه وبالإضافة إلى ذلك، فإن الأدلة الرقمية التي يتم الحصول عليها بطرق مخالفة للقواعد الإجرائية تعتبر باطلة ولا يجوز الاستناد إليها في إصدار حكم بالإدانة ، كما يُشترط أن يكون الدليل الرقمي مشروعًا، أي أن تُجمع الأدلة وفقًا للإجراءات التي حددها القانون و التي قمنا بدراستها سابقا وذلك احترامًا لشرعية الإجراءات الجزائية.

ثانيا: سلطة القاضي الجنائي في قبول الأدلة الرقمية

تتحدد سلطة القاضي الجنائي في قبول الأدلة الرقمية تبعاً لطبيعة نظام الإثبات المعتمد في الدولة، حيث تتمايز الأنظمة القانونية بين "النظام اللاتيني" المعروف بنظام الاقتناع الشخصي أو الإثبات الحر، و"النظام الأنجلوسكسوني" الذي يُعرف بنظام الأدلة القانونية المحددة ، ففي النظام اللاتيني كما هو معمول به في التشريعات الفرنسية، الجزائرية والمصرية، يتمتع القاضي بحرية واسعة في تقدير الأدلة دون أن يُفرض عليه نوع معين منها ويحق له أن يباشر بنفسه إجراءات التحري والبحث عن الأدلة بما في ذلك الأدلة الرقمية، من خلال إصدار أوامر لمزودي خدمات الإنترنت بالحصول على بيانات مثل سجل المواقع، المحادثات، أو الشيفرات السرية، كما يخضع الدليل الرقمي في هذا السياق لرقابة القاضي من حيث مدى قبوله وصحته ومصداقيته.

أما في "النظام الأنجلوسكسوني" المطبق في دول كأمريكا وإنجلترا وجنوب أفريقيا، فإن القاضي يكون ملزماً بأنواع محددة من الأدلة يقرها القانون مسبقاً، ولا يجوز له الخروج عنها حتى وإن لم يقتنع بها شخصيا[1]، ويُحكم هذا النظام بقاعدتين رئيسيتين:

قاعدة استبعاد شهادة السماع، التي تستبعد الأدلة القائمة على ما لم يُدرك بالحواس مباشرة داخل المحكمة وقاعدة الدليل الأفضل، التي تشترط تقديم الأصل لإثبات محتوى مستند أو صورة ، ومع

[1] نور الهدى محمودي ، المرجع السابق ،919 .

تطور القوانين تم تكييف هذه القواعد لتشمل المستندات الرقمية حيث أُقر في القانون الأمريكي أن البيانات المخزنة إلكترونياً والمخرجات المطبوعة منها تُعد دليلاً أصلياً شريطة أن تعكس محتواها بدقة[1].

ومنه يمكن القول أن حجية الدليل الرقمي في الإثبات الجزائي تعد مسألة شائكة يتقاطع فيها التطور التقني ومتطلبات العدالة الجنائية، فمعظم التشريعات الحديثة سواء العربية أو الغربية اتجهت نحو منح القاضي الجزائي سلطة تقديرية واسعة في تقييم الأدلة كما ذكرنا سابقا، خصوصاً في الجرائم المعلوماتية التي تتطلب فهماً خاصاً لطبيعة الدليل الرقمي، وفي ظل نظام الإثبات الحر لا يُقيد القاضي بنوع معين من الأدلة وإنما يُلزم فقط بتسبيب حكمه وإبراز الأدلة التي كوّنت قناعته، إلا أن الطبيعة التقنية للدليل الرقمي تثير إشكالات عملية أهمها مدى مصداقية هذا الدليل وإمكانية التلاعب به من حيث الإضافة أو الحذف أو التحريف ما يجعل الاعتماد عليه يتطلب فحصاً دقيقاً، وقد اتفقت معظم التشريعات على أن قبول هذا النوع من الأدلة مرهون بمدى اقتناع القاضي بها، فإذا وجدها مقنعة ومنسجمة مع وقائع الدعوى جاز له الاستناد إليها أما إذا شك في صحتها أو رأى أنها تعارض أدلة أقوى فله استبعادها بشرط تسبيب قراره، وتختلف درجة حجية الدليل الرقمي باختلاف نظام الإثبات فهي مطلقة في النظام الحر، ومقيدة في النظام المختلط، وقد تكون منعدمة في النظام المقيد الذي لا يزال يعتمد على الوسائل التقليدية دون الاعتراف الكامل بالأدلة الرقمية[2].

[1] نور الهدى محمودي ، المرجع السابق ، ص920.

[2] سالمي نضال ، المرجع السابق، ص347.

المبحث الثاني

مكافحة جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تتطلب مواجهة الجرائم المعلوماتية بشكل عام والاحتيال المعلوماتي بشكل خاص، تنسيقًا فعالًا بين التدابير الوطنية والدولية ، فهذه الجرائم بما تحمله من طابع عابر للحدود لا تقتصر آثارها على دولة واحدة بل تمتد لتشمل دولًا متعددة مما يستدعي ضرورة تعاون الدول وتنظيم التشريعات لمواجهة هذه التحديات ، إذ لا يمكن لأي دولة أن تحقق نجاحًا ملموسًا في مكافحة هذه الجرائم بمفردها خاصة في ظل التطور السريع للتكنولوجيا و وسائل تقنية المعلومات، الأمر الذي حفز الدول والمنظمات إلى تفعيل التعاون الدولي و تكثيف الجهود الوطنية، إلى جانب تأسيس منظومة إجرائية قادرة على التصدي لهذا النوع المستحدث من الجرائم، ونظرًا لخصوصيات هذه الأخيرة أصبح من اللازم وضع الأطر القانونية الملائمة ، و إقرار جزاءات فعالة تتناسب مع خطورة هذه الأفعال وتضمن ردع مرتكبيها .

وهو ما سنتطرق له في هذا المبحث من خلال استعراض السبل التشريعية المعتمدة لمكافحة الجرائم المعلوماتية (المطلب الأول)، والجزاءات المقررة لجريمة الاحتيال باستخدام تقنية المعلومات (المطلب الثاني).

المطلب الأول

السبل التشريعية للحد من الجرائم المعلوماتية

أمام التوسع المستمر في نطاق الجريمة المعلوماتية، وما تفرضه من تهديدات تمس الأمن العام والاقتصاد الوطني والدولي، برزت الحاجة الملحّة إلى وضع إطار تشريعي قادر على مواكبة هذا

النوع من الإجرام المعقّد، وقد تنوعت المقاربات القانونية بين دول العالم والمنظمات الإقليمية والدولية التي سعت إلى سن قواعد قانونية تسهم في الحد من هذه الجرائم، سواء عبر تبني اتفاقيات دولية أو صياغة نصوص قانونية تُلائم الطابع العابر للحدود لهذه الظاهرة ، وعليه يتم في هذا المطلب التطرق إلى الجهود التشريعية على المستويين الدولي والإقليمي و كذلك جهود المشرع الجزائري، كمرحلة أساسية لفهم السياق القانوني العام الذي تندرج ضمنه مواجهة الجريمة المعلوماتية .

الفرع الأول : السبل التشريعية للحد من الجريمة المعلوماتية على المستوى الدولي

يقتضي التصدي للجريمة المعلوماتية تفعيل آليات التعاون الدولي، باعتبار أن هذه الجرائم كثيراً ما تصطدم بمبدأ إقليمية القوانين الجزائية وسيادة الدول على إقليمها، وفي هذا السياق برزت جملة من الجهود على المستوى الدولي يظهر هذا كالتالي :

أولا : دور هيئة الأمم المتحدة في مكافحة الجريمة المعلوماتية

تبذل منظمة الأمم المتحدة جهودًا معتبرة في مجال مكافحة الجريمة المعلوماتية ، لمواجهة مخاطر هذه الظاهرة على النطاقين الوطني والدولي ، وقد أكدت المنظمة في أكثر من مناسبة على ضرورة تعزيز التعاون بين الدول الأعضاء لمواجهة التحديات المتزايدة المرتبطة بهذه الجرائم، والحد من انتشارها وتفاقم آثارها ، ويتجلى هذا الدور من خلال إشرافها المباشر على عدد من المؤتمرات الدولية المعنية بمنع الجريمة ومعاملة المجرمين ، والتي خُصص جزء كبير منها لدراسة مختلف أوجه الجريمة المعلوماتية ، بما في ذلك جريمة الاحتيال باستخدام وسائل تقنية المعلومات.[1]

[1] محمود أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر و التوزيع ، الأردن ، 2005 ، ص 155.

منذ تأسيس منظمة الأمم المتحدة سنة 1945، أُوكل إلى المجلس الاقتصادي والاجتماعي مهمة الإشراف على رسم السياسات الدولية في مجال منع الجريمة وتحقيق العدالة الجنائية ، وقد تُوِّج هذا التوجه بتوصية سنة 1950 التي أفضت إلى إنشاء لجنة استشارية متخصصة في منع الجريمة ومعاملة المجرمين، تولت وضع الخطط والبرامج ذات الصلة ، وفي عام 1981 تم استبدال هذه اللجنة بلجنة منع الجريمة ومكافحتها ، عقب مؤتمر كيوتو سنة 1980 وذلك بهدف تعزيز التعاون وتبادل الخبرات بين الدول ، و كانّ المؤتمر السابع المنعقد في ميلانو سنة 1985 أول من شهد بداية الاهتمام الدولي بمكافحة الجريمة المعلوماتية لاسيما من خلال التوصيات المتعلقة بحماية البيانات والمعطيات الشخصية المعالجة إلكترونيًا .[1]

ويعد مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين المنعقد في هافانا عام 1990 محطة محورية في جهود المنظمة الأممية لمكافحة الجرائم المعلوماتية ، حيث قدّم توصيات مهمة ركّزت على دعم الإجراءات التشريعية والتحقيقية في هذا المجال ، لا سيما في ما يتعلق بالجرائم المرتبطة باستخدام الحاسب الالي ، ومن أبرز ما نص عليه القرار الصادر عن هذا المؤتمر[2]:

- حثّ الدول الأعضاء على تجريم إساءة استخدام الحواسيب وتكثيف الجهود لمكافحة الجرائم المتصلة بها.
- التأكيد على ضرورة مواءمة القوانين الوطنية المتعلقة بالتحقيقات والإثبات مع خصوصية الجرائم المعلوماتية .

[1] مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين، ميلانو، إيطاليا، 26 آب/أغسطس – 6 أيلول/سبتمبر 1985، الوثيقة A/CONF.121/22، منشورات الأمم المتحدة، نيويورك، 1980 ، الرابط : Previous Congresses

[2] مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، كوبا، 27 آب/أغسطس – 7 أيلول/سبتمبر 1990، الوثيقة A/CONF.144/28/Rev.1، منشورات الأمم المتحدة، نيويورك، 1991، الرابط : Report of the 8th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August-7 September 1990.

- دعوة الدول إلى اعتماد تشريعات جديدة تضع أُطرًا واضحة للجرائم المعلوماتية.
- التشجيع على الانخراط في الاتفاقيات الدولية ذات الصلة بتسليم المجرمين وتبادل المساعدة القانونية في المسائل الجنائية المرتبطة بالجريمة المعلوماتية.
- المطالبة بوضع معايير دولية لأمن معالجة البيانات والمعلومات.
- معالجة إشكالات الاختصاص القضائي في الجرائم المعلوماتية ذات الطابع العابر للحدود.
- العمل على إبرام اتفاقيات دولية تنظم إجراءات التفتيش والضبط المباشر عبر الحدود في الأنظمة المعلوماتية ، مع احترام حقوق الأفراد وسيادة الدول .[1]

كما تطرق المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد بالبرازيل سنة 1994[2]، إلى تصنيف الأفعال الإجرامية المرتبطة بالاحتيال عبر الكمبيوتر حيث أكد على ضرورة تجريم أفعال التزوير الإلكتروني ، إتلاف البيانات ، تعطيل الشبكات، و الدخول غير المشروع إلى الأنظمة ، كما تبنّى المؤتمر جملة من القواعد الإجرائية أبرزها السماح بالتفتيش والضبط في بيئة تكنولوجيا المعلومات ، والتعاون مع الضحايا ومستخدمي البيانات لأغراض قضائية، واعتراض الاتصالات داخل نظم الحاسوب ومراقبتها عند الضرورة القانونية.[3]

ثانيا : التعاون الدولي في مجال مكافحة الجريمة المعلوماتية

يُمكن إجمال صور التعاون الدولي في مجال مكافحة الجريمة المعلوماتية في الصور التالية:

---

[1] ليندة شرا بشة ، السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية ، الاتجاهات الدولية في مكافحة الجريمة الالكترونية ، دراسات وأبحاث ، المجلد01، العدد 01 ، جامعة زيان العاشور ، الجلفة ، الجزائر ، 2009 ، ص 245.

[2] الجمعية الدولية لقانون العقوبات، أعمال المؤتمر الخامس عشر – ريو دي جانيرو، 4–10 أيلول/سبتمبر 1994: الجريمة الاقتصادية وجرائم الكمبيوتر، منشورات AIDP، باريس، 1995.

الرابط: Congrès international de droit pénal (15 ; 1994 ; Rio de Janeiro)

[3] ليندة شرا بشة ،المرجع السابق، ص 246 .

1. تبادل المعلومات :

هو إجراء يتم فيه تزويد السلطات القضائية الأجنبية بالمعلومات والبيانات والقرائن ذات الصلة بجريمة قيد النظر، بما يشمل تفاصيل الاتهامات الموجهة إلى رعاياها في الخارج والإجراءات المتخذة ضدهم، وقد يتضمن هذا التبادل كذلك السوابق القضائية للجناة ، ويستند هذا الإجراء إلى أساس قانوني نصت عليه الفقرة الثانية البنود "و" و"ز" من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية.[1]

ونذكر كمثال على هذا التعاون ما نصّت عليه المادة 17 من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، على التزام الدولة الجزائرية بالاستجابة لطلبات المساعدة القضائية الدولية المتعلقة بتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة، وعلى أساس مبدأ المعاملة بالمثل[2].

2. نقل الاجراءات :

يُقصد بنقل الإجراءات أن تتولى دولة استنادًا إلى اتفاقية أو معاهدة، اتخاذ إجراءات جنائية تتعلق بجريمة معلوماتية ارتُكبت في إقليم دولة أخرى وذلك لمصلحة هذه الأخيرة ، متى توافرت مجموعة من الشروط في مقدمتها مبدأ التجريم المزدوج ، أي أن يكون الفعل محل الاتهام مجرما في كل من الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات ويُشترط أيضًا شرعية هذه الإجراءات ، بمعنى أن تكون هذه الإجراءات منصوصًا عليها في قانون الدولة المطلوب إليها، وأن تكون ذات طابع جوهري يُمكن أن يسهم بفعالية في كشف الحقيقة ، وقد أقرّت عدد من الاتفاقيات الدولية

[1] معاهدة نموذجية بشأن نقل الاجراءات في المسائل الجنائية ، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/118 المؤرخ في 14 كانون الأول / ديسمبر 1990 .

[2] المادة 17من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

والإقليمية هذا النمط من التعاون، من أبرزها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.[1]

3. الإنابة القضائية :

تُعد الإنابة القضائية الدولية من أبرز مظاهر التعاون القانوني بين الدول ، وتهدف إلى تمكين السلطة القضائية في دولة معينة من استكمال إجراء ضروري في مسار الدعوى يتعذر عليها تنفيذه داخل إقليمها، فيُطلب من سلطة قضائية مختصة في دولة أخرى القيام به ، وتُمارس الإنابة أساسًا في إطار القوانين الوطنية أو وفقًا للاتفاقيات الدولية، أو بناءً على مبدأ المعاملة بالمثل والمجاملة الدولية.[2]

تتضمن الإنابة مختلف إجراءات التحقيق ، كاستماع الشهود ،والتفتيش، وتقديم الخبرة دون حصر ما لم يُنص على خلاف ذلك ، ويُعدّ هذا النظام أداة إجرائية تسهم في مواجهة الحدود الإقليمية التي قد تعرقل تنفيذ بعض الإجراءات ، خصوصًا في القضايا ذات البعد الدولية كالجريمة المعلوماتية .[3]

---

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني / نوفمبر 2000، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 02-55، المؤرخ في 22 ذي القعدة عام 1422، الموافق 5 فبراير سنة 2002.

[2] العيساوي حسين ، الإنابة القضائية في القانون الخاص الجزائري ، مجلة الاستاذ الباحث للدراسات القانونية و السياسية ، المجلد 06، العدد 02 ، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف ، المسيلة، جانفي 2022 ،ص 2346.

[3] بن عودة نبيل ، درعي العربي ، الإنابات القضائية الدولية في المجال الجزائي، مجلة القانون الدولي و التنمية، المجلد 7 ، العدد 2 ، جامعة عبد الحميد بن باديس ، مستغانم ، 2020، ص 150.

الفرع الثاني : السبل التشريعية للحد من الجريمة المعلوماتية على المستوى الإقليمي

نتطرق في هذا الفرع إلى السبل التشريعية المتبعة على المستوى الإقليمي للحد من الجريمة المعلوماتية ، والتي تظهر في الجهود المبذولة من طرف المجلس الأوروبي وجامعة الدول العربية و الإتحاد الإفريقي .

أولا : دور المجلس الأوروبي في مكافحة الجريمة المعلوماتية

ساهم المجلس الأوروبي بشكل كبير في الحد من الجرائم المعلوماتية من خلال إقرار العديد من التوصيات التي تركز على حماية البيانات ذات الطابع الشخصي من الاستغلال وحماية تدفق المعلومات، في 28 يناير 1981 تم توقيع اتفاقية تحت إشراف المجلس الأوروبي تتعلق بحماية الأفراد من المخاطر الناجمة عن المعالجة الإلكترونية للبيانات الشخصية.[1]

وفي عام 1989 نشر المجلس الأوروبي دراسة تضمنت توصيات لتعزيز دور القانون في مواجهة الأفعال غير المشروعة المرتبطة بالحواسيب، بعدها في عام 1995 اصدرت التوصية رقم 13195 تناولت الإجراءات الجنائية في مجال الجرائم المعلوماتية ، استنادًا إلى المبادئ الواردة في هذه التوصيات ، قام المجلس الأوروبي في عام 1997 بتشكيل لجنة من الخبراء في مجال الجريمة عبر الفضاء الإلكتروني بهدف إعداد اتفاقية في هذا الإطار.[2]

ويُعد الإشراف على إعداد اتفاقية بودابست لمكافحة الجرائم المعلوماتية بتاريخ 21 نوفمبر 2001 أحد أبرز إنجازات المجلس الأوروبي في هذا المجال، إذ تهدف هذه الاتفاقية إلى مواءمة التشريعات الوطنية مع تحديات البيئة الرقمية المتغيرة، وقد تناولت الاتفاقية مختلف الجوانب

[1] اتفاقية مجلس أوروبا رقم 108 لسنة 1981 بشأن حماية الأشخاص تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، الموقعة في ستراسبورغ بتاريخ 28 يناير 1981.

[2] سعيداني نعيم ، المرجع السابق، ص 85 .

المتعلقة بالجريمة المعلوماتية ، ودخلت حيز النفاذ في الأول من يوليو 2004 لتُشكل بذلك أداة قانونية دائمة في دعم الجهود الدولية للحد من هذا النوع من الجرائم .[1]

رغم أن الاتفاقية وُضعت في إطار أوروبي ، إلا أنها اكتسبت طابعًا دوليًا يتجاوز حدود الإقليم الأوروبي بفضل انفتاحها على انضمام الدول من خارج المجلس ، حيث شهدت الاتفاقية توسعًا ملحوظًا في عدد أعضائها، إذ بلغ عدد الدول المصادقة عليها حتى تاريخ 22 أبريل 2024 ما مجموعة 72 دولة، كانت آخرها غرينادا التي أودعت وثيقة الانضمام في هذا التاريخ.[2]

وقد تضمنت هذه الاتفاقية 48 مادة موزعة في ثلاث أقسام أساسية :

_القسم الأول: يشمل المواد من المادة 2 إلى المادة 11، هذه المواد تحدد أنواع الجرائم التي تصنفها الاتفاقية، بما في ذلك الجرائم المرتبطة بأنظمة المعلومات و جرائم التلاعب بالبيانات مثل الاحتيال باستخدام وسائل تقنية المعلومات ، وتنظيم الجرائم المتعلقة بالاتصالات غير القانونية ، والاعتداء على البيانات.

_القسم الثاني: يختص بالإجراءات الجنائية المتعلقة بالبحث والتحقيق في الجرائم المعلوماتية، ويشمل المواد من المادة 12 إلى المادة 20، هذه المواد توضح كيفية تفتيش وضبط البيانات الرقمية أثناء مرحلة البحث و التحري ، وتحديد الإجراءات المناسبة لتحليل الأدلة الرقمية.

[1] اتفاقية بودابست المتعلقة بالجريمة المعلوماتية، المعتمدة من طرف مجلس أوروبا في 23 نوفمبر 2001، ودخلت حيز التنفيذ في 1 يوليو 2004.

[2] Parliamentarians for Global Action. PGA Congratulates Grenada on becoming the 72nd State Party to the Budapest Convention on Cybercrime. منشور على الموقع الاكتروني ، تاريخ الاطلاع 04/20/2025، على الساعة 18:40 https://www.pgaction.org/news/grenada-budapest-convention.html

_القسم الثالث: يتعلق بالتعاون الدولي بين الدول الأطراف في الاتفاقية ، ويشمل المواد من المادة 21 إلى المادة 37 تحدد سبل التعاون القضائي و التنسيق بين الدول في التحقيقات الدولية، وكذلك تبادل المعلومات و الخبرة حول الجرائم المعلوماتية.[1]

تتمثل أهداف اتفاقية بوداباست في ما يلي :

_تحقيق التوافق التشريعي بين الدول الأوروبية والدول غير الأوروبية المنضمة إليها لتنسيق القانون المشترك في مجال مكافحة الجرائم المعلوماتية.

_التأكيد على أهمية التعاون الإقليمي والدولي في مجال مكافحة جرائم الكمبيوتر والإنترنت، وتوفير دليل مرجعي لمساعدة الدول في تطوير تدابير تشريعية فعّالة لمواجهة هذه الجرائم.

_مكافحة الأنشطة التي تهدد سلامة المعلومات وأمن الأنظمة المعلوماتية و التي تشمل إساءة استخدام الحواسيب والشبكات ، مع تحديد الإطار الموضوعي والإجرائي المرتبط بالتحقيقات والمحاكمات على الصعيدين الوطني والدولي.

_تحقيق التوازن بين حماية حقوق الإنسان الأساسية ، كما ورد في اتفاقية مجلس أوروبا لحماية حقوق الإنسان لعام 1950 والعهد الدولي للحقوق المدنية والسياسية لعام 1966، وبين الحق في حماية الخصوصية وحيازة المعلومات ، وحقوق الملكية الفكرية ، مع ضمان ألا يؤثر ذلك على حقوق الأفراد في الوصول إلى المعلومات وحرية التعبير.[2]

---

[1] قطاف سليمان ، بوقرين عبد الحليم ، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري ، المجلة الأكاديمية للبحوث القانونية والسياسية ، المجلد 6 ، العدد 1 ، جامعة عمار ثليجي ، الاغواط ، الجزائر ، ص 339 .

[2] عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية و الانترنيت ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، لبنان ، 2007 ، ص126.

ثانيا : دور جامعة الدول العربية في مكافحة الجريمة المعلوماتية

تعتبر جامعة الدول العربية منظمة إقليمية تأسست في 22 مارس 1945، بموجب ميثاق وقّعت عليه سبع دول عربية (مصر، السعودية ،العراق ، سوريا، الأردن، لبنان ،اليمن) وتتخذ من القاهرة مقرًا دائمًا لها ، تضم في عضويتها كافة الدول العربية في قارتي آسيا وأفريقيا ، أنشئت بهدف توثيق الصلات بين هذه الدول وتنسيق السياسات في مختلف الميادين الاقتصادية والاجتماعية والثقافية ، فضلًا عن دعم القضايا ذات الاهتمام المشترك وتعزيز التعاون الأمني والتشريعي فيما بينها، تتولى الجامعة العربية من خلال أجهزتها المختلفة وعلى وجه الخصوص مجلس وزراء العدل العرب بدور محوري في توحيد المساعي القانونية والتشريعية للدول الأعضاء، من خلال إعداد قوانين استرشادية واتفاقيات إقليمية تهدف إلى مواجهة التحديات الحديثة كالجريمة المعلوماتية ، التي فرضت على الدول العربية ضرورة تبني أدوات تشريعية مشتركة ، كان من أبرزها إصدار القانون العربي الاسترشادي لمكافحة الجرائم المعلوماتية سنة 2004، والاتفاقية العربية لمكافحة الجرائم المرتبطة بتقنية المعلومات سنة 2010 .[1]

1. القانون العربي الاسترشادي لمكافحة الجرائم المعلوماتية :

في إطار الجهود التي تبذلها جامعة الدول العربية لمواجهة التحديات القانونية المرتبطة بتطور تقنية المعلومات ، صادق مجلس وزراء العدل العرب في دورته التاسعة عشرة سنة 2003 على

[1] محمود محمد صفاء الدين على شرشر ، الجهود الدولية والتشريعية لمكافحة جرائم الأنترنيت ، مجلة البحوث القانونية و الاقتصادية -المنوفية ، كلية الحقوق ، جامعة المنوفية ، مصر، 2021 ، ص 551.

القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات، وذلك بناءً على مشروع أُعدّ من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمري وزراء العدل والداخلية العرب. [1]

يهدف هذا القانون إلى تزويد الدول الأعضاء بنموذج تشريعي موحّد يمكن الاسترشاد به في وضع قوانين وطنية فعّالة للتصدي للجرائم المعلوماتية، وتوفير أساس قانوني لتعزيز التعاون القضائي العربي في هذا المجال[2].

وقد تضمّن هذا النص أحكامًا موضوعية موزعة على أربعة أبواب ، تناول أولها أهم صور الجرائم التي تُرتكب عبر النظم المعلوماتية ، شملت الجرائم الماسة بأمن المعلومات مثل الدخول غير المشروع والتشويش على البيانات ، وجرائم التزوير والاحتيال المرتبطة بالحاسوب، والجرائم ذات المحتوى غير المشروع كدعارة الأطفال، فضلًا عن الجرائم التي تمسّ بحقوق الملكية الفكرية، ورغم شمول القانون من حيث مضمونه الموضوعي، إلا أنه تعرّض لانتقادات تتعلق بغياب الإطار الإجرائي اللازم لا سيما ما يخص الاختصاص القضائي ، وضوابط التفتيش، وحجية الدليل الرقمي.

2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات :

تُعد الاتفاقية العربية لمكافحة الجرائم المرتبطة بتقنية المعلومات من أبرز الجهود التشريعية التي تبنتها جامعة الدول العربية لمواجهة التحديات الأمنية والقانونية التي تفرضها الجريمة المعلوماتية، وقد تم اعتماد هذه الاتفاقية خلال الاجتماع المشترك لمجلسي وزراء الداخلية والعدل العرب المنعقد

[1] بدري فيصل ، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي ، أطروحة دكتوراة تخصص قانون عام ، كلية الحقوق ، جامعة الجزائر 01 -بن يوسف بن حدة- ، 2018/2017 ، ص 33-34 .

[2] مشروع قانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات، المعتمد من طرف مجلس وزراء العدل العرب، الدورة التاسعة عشرة، القرار رقم 495 بتاريخ 8 أكتوبر 2003.

بمقر الأمانة العامة للجامعة بالقاهرة بتاريخ 21 ديسمبر 2010، حيث قامت 23 دولة عربية بالتوقيع عليها في اليوم نفسه ، بما في ذلك الجزائر.[1]

تضم الاتفاقية خمسة فصول رئيسية ، حيث تناول الفصل الأول الأحكام العامة والمصطلحات، أما الفصل الثاني فقد خصص لتجريم الأفعال الماسة بأنظمة وتقنيات المعلومات ، بينما نظم الفصل الثالث الإجراءات المتعلقة بالبحث والتفتيش في هذا النوع من الجرائم ، واهتم الفصل الرابع بمبادئ الاختصاص وأسس التعاون القضائي ، ليختتم الفصل الخامس بالأحكام الختامية، وتتميز هذه الاتفاقية بتفصيلها الدقيق للمسائل الإجرائية ، ما يجعلها نموذجاً عربياً مستلهماً من اتفاقية بودابست التي تم التطرق إليها سابقا.[2]

تهدف الاتفاقية إلى تعزيز التعاون العربي في المجال الجنائي المعلوماتي ، من خلال وضع إطار قانوني مشترك يسهّل ملاحقة مرتكبي الجرائم المعلوماتية عبر الحدود الوطنية ، ويعزز من فعالية الإجراءات القانونية الخاصة بالتحقيق والتفتيش، بما يراعي الخصوصية التقنية لهذه الجرائم ، كما تسعى الاتفاقية إلى توحيد المفاهيم والمساطر الإجرائية بين التشريعات الوطنية للدول العربية في مجال مكافحة الجريمة المعلوماتية ، إضافة إلى إرساء معايير قانونية مشتركة تتعلق بتجريم الأفعال الماسة بسرية وسلامة وتوفر نظم المعلومات، بما في ذلك جرائم الاحتيال والتزوير المرتبطة باستخدام تقنية المعلومات التي أصبحت تمثل خطراً متزايداً على أمن المعاملات الإلكترونية والبيانات الرقمية .[3]

---

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، المبرمة يوم2010.12.21 و المصادق عليها بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 2014/09/08 ، ج ر57 ، سنة 2014.

[2] حمي أحمد ، جرائم تقنية المعلومات وآليات مكافحتها وفقا لاتفاقية العربية لمكافحة جرائم المعلومات- دراسة مقارنة- ، أطروحة دكتوراه في الحقوق ، تخصص القانون الجنائي ، المركز الجامعي أمين العقال الحاج موسى أق أخموك تامنغست ، معهد الحقوق والعلوم السياسية ، 2019/2020 ، ص 52 .

[3] انظر :الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .

على الرغم من الأهمية البالغة التي تنطوي عليها الاتفاقية العربية لمكافحة الجرائم المرتبطة بتقنية المعلومات، إلا أن عدداً من الدول العربية الموقعة عليها لم تُصادق بعد على مضمونها، باستثناء بعض الدول كالمملكة العربية السعودية ومملكة البحرين، اللتين سعتا إلى مواءمة تشريعاتهما الوطنية مع أحكام هذه الاتفاقية ، من خلال سن قوانين داخلية تُعنى بمكافحة الجرائم المعلوماتية وفقاً لما ورد في نصوصها ، أما الجزائر فقد سعى المشرّع إلى إدراك هذا التوجه ، غير أن القانون 09-04 المتعلق بمكافحة الجرائم المعلوماتية ، والصادر بتاريخ 5 أوت 2009 جاء سابقاً لمصادقة الجزائر الرسمية على الاتفاقية ، التي لم تتم إلا بتاريخ 8 سبتمبر 2014 بموجب المرسوم الرئاسي رقم 14-252 المنشور في الجريدة الرسمية عدد 57 لسنة 2014 ، ويرتبط هذا التفاوت الزمني ببعض أوجه القصور في القانون الجزائري ، خصوصًا في الجوانب المتعلقة بجرائم الاحتيال المعلوماتي .[1]

ثالثا : اتفاقية مالابو لمكافحة الجريمة المعلوماتية

تُعد "اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات ذات الطابع الشخصي"، المعروفة باتفاقية مالابو الإطار القانوني الإقليمي الأول الذي يسعى لتنظيم المعاملات الإلكترونية وتعزيز الأمن السيبراني وحماية البيانات الشخصية في القارة الإفريقية ، تم اعتماد الاتفاقية في قمة مالابو المنعقدة بتاريخ 27 يونيو 2014، ودخلت حيز التنفيذ بعد التصديق عليها من قبل 15 دولة في 8 يونيو 2023 ، كانت موريتانيا آخر دولة صادقت على اتفاقية مالابو في 9 مايو

[1] ربيعي حسين ، آليات البحث و التحقيق في الجرائم المعلوماتية ، أطروحة مقّدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص قانون العقوبات و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة الحاج لخضر ، باتنة ، 2016 ، ص 141.

2023 [1]، بعد مرور 30 يومًا من استلام الاتحاد الإفريقي لصك التصديق الخامس عشر مما أكمل الإجراءات اللازمة لدخول الاتفاقية حيز التنفيذ وفقًا لما تنص عليه المادة 36 من الاتفاقية.[2]

تتناول اتفاقية مالابو قضية الأمن السيبراني في إفريقيا، وتستهدف تنظيم الجرائم الإلكترونية وحماية البيانات الشخصية ،كما تركز على توحيد التشريعات بين الدول الأعضاء لضمان حماية الحقوق الرقمية ، وتعزيز التعاون بين الحكومات في مكافحة الجرائم السيبرانية، تهدف أيضا إلى دعم التجارة الإلكترونية وتقليص التكاليف المرتبطة بالاتصالات الرقمية ، وتحقيق بيئة رقمية آمنة ومستدامة بحيث تشمل العديد من البنود المتعلقة بحماية البيانات في مجالات متعددة ، بما في ذلك تأمين نظم المعلومات ، تحديد آليات التعاون القانوني بين الدول لتبادل البيانات وحماية الأمن الرقمي، كما تسعى إلى مكافحة الاحتيال المعلوماتي وغيره من التهديدات الإلكترونية ، من خلال وضع معايير للتعامل مع البيانات والمعلومات بشكل قانوني وآمن .[3]

رغم أهمية الاتفاقية باعتبارها الإطار القانوني الأول على مستوى القارة لمكافحة الجريمة المعلوماتية ، فإن أغلب الدول الإفريقية لم تُصادق عليها بعد من بينها الجزائر، ومع ذلك يُعتبر تصديق الدول التي أتمّت العملية خطوة هامة نحو تعزيز التشريعات الخاصة بالأمن السيبراني وحماية البيانات على مستوى القارة، مما يعكس حرص الاتحاد الإفريقي على إرساء قواعد قانونية مشتركة تتماشى مع التطورات التكنولوجية الحديثة.

---

[1] African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force ، منشور على الموقع الاكتروني https://citadellaw.africa/insight/african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force/ يوم الاطلاع 2025/22/04 ، ساعة الاطلاع 17:42 ،

[2] المادة 36 من اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، المعتمدة في الدورة العادية الثالثة والعشرون لمؤتمر الاتحاد الأفريقي، مالابو، 27 يونيو 2014.

[3] مريم لوكال ، قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني و حماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية و الاقتصادية ، المجلد 4 ، العدد 3 ، جامعة احمد بوقرة ، بومرداس ، 2021 ، ص 661.

الفرع الثالث : السبل التشريعية للحد من الجريمة المعلوماتية على المستوى الوطني

في ظل التوجهات الإقليمية والدولية الرامية إلى تطوير السياسات الخاصة بمكافحة الجرائم المعلوماتية و تعزيز آليات البحث والتحري في هذا المجال، سعى المشرع الجزائري إلى مواءمة المنظومة التشريعية الوطنية مع المستجدات التشريعية العالمية والتطور وسائل تقنية المعلومات، ويأتي هذا التوجه استجابة للتحولات التي شهدتها البلاد خصوصًا مع الانتشار الواسع لاستخدام شبكة الإنترنت خلال السنوات الأخيرة، وتزايد اعتماد الإدارات والمؤسسات العمومية على تكنولوجيا المعلومات، وهو ما انعكس على ارتفاع معدلات الجريمة المعلوماتية خصوصا الاحتيال باستخدام وسائل تقنية المعلومات ، وقد استدعى هذا الوضع تبنّي إجراءات قانونية تتسم بالفعالية ، من خلال وضع أطر تشريعية تهدف إلى الوقاية من هذا النوع من الجرائم والتصدي لها.

وفي هذا السياق ، جاء القانون رقم 04-15 الصادر بتاريخ 10 نوفمبر 2004 في مسار تطور التشريع الجزائري في هذا مجال التصدي للجرائم المعلوماتية ، حيث تضمن تعديلاً لقانون العقوبات بإضافة قسم مستقل تحت عنوان "جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، وقد شمل هذا القسم المواد من 394 مكرر إلى 394 مكرر 7، حيث تم من خلالها تجريم أفعال متعددة تتعلق بالدخول غير المشروع إلى الأنظمة المعلوماتية والاعتداء على سلامة وأمن البيانات ، سواء بالنسبة للأنظمة العمومية أو الخاصة ، مع تحديد العقوبات المناسبة لكل صورة من صور هذه الجرائم[1].

إلا أن تلك الجهود لم تكن كافية لتفعيل السياسة الجنائية بشكل كامل وذلك بسبب تعارض بعض أحكام قانون العقوبات مع قانون الإجراءات الجزائية حيث كانت المسائل المتعلقة بالاختصاص

[1] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966، والمتضمن قانون العقوبات الجزائري ، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

النوعي والإقليمي أحد العوامل التي حالت دون تنفيذ فعّال للنصوص العقابية ، هذا الواقع دفع المشرع إلى التدخل من جديد بموجب القانون رقم المؤرخ في 20 ديسمبر 2006 ، الذي عدل وأتمّ بعض مواد قانون الإجراءات الجزائية تحديدًا المواد من 45 إلى 47 ، والتي تناولت قواعد الاختصاص النوعي والمحلي في الجرائم المعلوماتية.[1]

وفي خطوة مكملة، صدر القانون رقم 09_04 المؤرخ في 5 أوت 2009، والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي يُعد أول قانون خاص يُنظم الجريمة المعلوماتية في الجزائر، بما في ذلك جرائم الاحتيال المعلوماتي، من خلال نصوص إجرائية وتنظيمية تُعنى بالتفتيش الإلكتروني، حجز الأدلة الرقمية، والتزامات مقدمي خدمات الإنترنت، بالإضافة إلى إنشاء هيئة وطنية مختصة بهذا المجال ، وقد تم تدعيم هذا القانون لاحقًا بـ المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، الذي أنشأ "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"، لتُشرف على عمليات البحث والتحقيق، وتدعمها تقنيًا من خلال "مديرية المراقبة الوقائية واليقظة الإلكترونية."[2]

في سياق تطور المنظومة التشريعية الوطنية، جاء القانون رقم 18-04 المؤرخ في 10 مايو 2018 والمتعلق بالبريد والاتصالات الإلكترونية ليشكل نقلة نوعية في تنظيم استخدام الشبكات الرقمية، حيث فرض هذا القانون التزامات واضحة على مزودي خدمات الاتصالات والإلكترونيات، من بينها ضرورة التحقق من هوية المشتركين وحماية سرية المراسلات والبيانات المتبادلة عبر الشبكات ، ورغم أن القانون لم يُجرّم بشكل مباشر جريمة الاحتيال المعلوماتي، إلا أن أحكامه

[1] القانون رقم 06-22، المؤرخ في 20 ديسمبر 2006، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84، المؤرخة في 24 ديسمبر 2006، المعدل والمتمم للأمر رقم 155/66، المؤرخ في 08 يوليو 1966.

[2] المرسوم الرئاسي رقم 15_261 المؤرخ في 08 أكتوبر 2015 المتضمن تحديد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيات الإعلام و الإتصال ، الصادر في الجريدة الرسمية عدد 53 بتاريخ 08 أكتوبر 2015.

أسهمت في تعزيز البيئة القانونية التي تحد من استغلال تقنيات الاتصالات لأغراض إجرامية، كما توفّر إطاراً تقنياً وقانونياً يدعم الجهود الزجرية المبذولة في هذا المجال، من خلال تمكين الجهات المختصة من اتخاذ الإجراءات اللازمة للرقابة والمراقبة في حالات التحقيق الجنائي. [1]

كما يشكل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي أحد المرتكزات الوقائية الأساسية التي اعتمدها المشرع الجزائري في سبيل التصدي للتهديدات التي تفرزها الجرائم المعلوماتية، فعلى الرغم من أن هذا النص لا يندرج ضمن التشريعات الردعية المخصصة لمكافحة الجرائم المعلوماتية بصفة مباشرة، إلا أن طبيعته التنظيمية والحمائية للمعطيات الشخصية تساهم بشكل غير مباشر في تضييق نطاق الأفعال الإجرامية التي تعتمد على استغلال البيانات لأغراض احتيالية، كسرقة الهوية أو التلاعب بالمعلومات الخاصة بالأفراد أو ابتزازهم ، ويهدف القانون بالأساس إلى فرض ضوابط صارمة على عمليات جمع ومعالجة وتخزين وتداول المعطيات، من خلال إلزام الجهات المعنية بالحصول على موافقة صريحة من الشخص المعني، وضمان سرية المعلومات، وتقييد استخدامها وفقًا لأغراض مشروعة ومعلنة. [2]

[1] القانون رقم 18-04 المؤرخ في 10 مايو 2018 المتعلق بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 27، الصادر بتاريخ 13 مايو 2018.

[2] القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 هـ الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 35، الصادرة بتاريخ 13 يونيو 2018.

المطلب الثاني

السبل الردعية للحد من جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تُعتبر جريمة الاحتيال من بين الجرائم التقليدية التي تناولها المشرع بالتجريم في إطار القواعد العامة المنصوص عليها في قانون العقوبات، حيث خصص لها جزاءات محددة تعكس خطورتها على المعاملات المدنية و التجارية ، ومع التطور التقني الهائل وظهور أشكال جديدة من الاحتيال عبر الوسائط الرقمية ، أصبح من الضروري إعادة النظر في هذه الجزاءات بما يتناسب مع تعقيدات الجريمة المعلوماتية وأثرها الواسع النطاق ، وقد تفاعل المشرع الجزائري مع هذه التغيرات من خلال تجريم صور جديدة من الاحتيال التقني وتقرير عقوبات خاصة بها ضمن التشريعات ذات الصلة ، وبناءً على ذلك نتناول في هذا المطلب الجزاءات المقررة لجريمة الاحتيال في (الفرع الأول) ، ثم الجزاءات الخاصة بجريمة الاحتيال المعلوماتي (الفرع الثاني).

الفرع الأول : الجزاءات المقررة لجريمة الاحتيال

نظّم المشرع الجزائري جريمة الاحتيال ضمن النصوص العامة لقانون العقوبات، مقرّرًا لها جزاءات تتنوع بحسب خطورة الفعل الإجرامي وطبيعته ، وتشمل العقوبات الأصلية و العقوبات التكميلية ، إضافة إلى الظروف المشددة للعقوبة وهو ما نتناوله في هذا الفرع .

أولا : العقوبات الأصلية لجريمة الاحتيال

تُعد العقوبة الأصلية الجزاء الأساسي الذي يُفرض على الجاني في حال ارتكابه جريمة ، وهي تشمل عادة العقوبات السالبة للحرية أو الغرامات المالية ، ويُطبق ذلك على أي فعل يُجرمه القانون وفق نصوصه الصريحة ، وفي العديد من الحالات يُعتبر هذا النوع من العقوبات كافيًا

لتحقيق الردع العام والخاص ، دون الحاجة إلى فرض عقوبات إضافية أخرى ما لم يُنص على خلاف ذلك في التشريعات أو إذا اقتضت ظروف الجريمة فرض جزاءات تكميلية أو مشددة .

وعليه فإنه في حال لم تُقترن جريمة الاحتيال بالظروف التي نص عليها القانون، يُعاقب الجاني بعقوبتين الأولى عقوبة الحبس التي تتراوح مدتها بين سنة واحدة على الأقل إلى خمس سنوات على الأكثر، والثانية عقوبة الغرامة المالية التي تتراوح قيمتها بين خمسمائة (500) دينار جزائري إلى عشرين ألف (20.000) دينار جزائري ، وذلك وفقًا لما جاء في المادة 372 من قانون العقوبات الجزائري، في فقرتها الأولى.[1]

أما بالنسبة لعقوبة الشخص المعنوي ، يعاقب حسب المادة 18 مكرر من قانون العقوبات الجزائري بفرض غرامة مالية مضاعفة من مرة إلى خمس مرات الحد الأقصى عن تلك المقررة للأشخاص الطبيعيين في جريمة الاحتيال .[2]

1. عقوبة الشروع في جريمة الاحتيال :

يُقصد بالشروع في الجريمة بوجه عام البدء في تنفيذ الفعل الإجرامي بقصد ارتكاب جناية أو جنحة ، غير أن النتيجة الجرمية لم تتحقق لسبب خارج عن إرادة الجاني ، وقد كرّس المشرع الجزائري هذا المفهوم في المادة 30 من قانون العقوبات و عاقب عليه كما في الجريمة التامة ، حيث نصّت على أن كل محاولة لارتكاب جناية أو جنحة تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها ، تعتبر كالجريمة نفسها إذا لم يخب أثرها إلا نتيجة ظروف مستقلة عن إرادة مرتكبها.[3]

---

[1] انظر المادة 372 من قانون العقوبات الجزائري .

[2] انظر المادة 18، من قانون العقوبات الجزائري .

[3] انظر المادة 30 قانون العقوبات الجزائري .

وعند تنزيل هذا الحكم على جريمة الاحتيال، باعتبارها من الجنح المعاقب عليها فإن الشروع فيها يتحقق كلما بدأ الفاعل في استعمال وسائل احتيالية من شأنها تضليل المجني عليه ودفعه لتسليم المال ، إلا أن النتيجة لم تتحقق كأن يتراجع المجني عليه في اللحظة الأخيرة أو يتدخل طرف ثالث يحول دون إتمام الجريمة ، ومثال ذلك أن يقدم الجاني وثائق مزورة لتدعيم أقواله، غير أن المجني عليه ينتبه للحيلة فيرفض تسليم المال.[1]

كما يُعد شروعا أيضًا إذا أدت الأفعال الاحتيالية إلى وقوع المجني عليه في الغلط ، غير أن هذا الغلط لم يكن السبب المباشر في تسليمه المال ، أما الأفعال التي تسبق البدء في التنفيذ كتلك التحضيرية التي تتمثل في إعداد الوسائل الاحتيالية أو الاتفاق مع شركاء لتدعيم الخدعة ، فإنها لا تشكل شروعًا في القانون الجزائري ، وإنما تبقى في نطاق الأعمال التحضيرية التي لا يعاقب عليها المشرع.[2]

2. الاشتراك في جريمة الاحتيال :

كثيرًا ما تتم جريمة الاحتيال بمساهمة أكثر من شخص، حيث يلعب الشريك دورًا أساسيًا إلى جانب الفاعل الأصلي ، فإن الشريك يعاقب بذات العقوبة المقررة للفاعل الأصلي متى ثبتت مساهمته في تنفيذ الجريمة سواء بالتحريض، أو التسهيل ، أو تقديم العون المادي أو المعنوي.[3]

فالمشاركة تتمثل في التعاون بين أكثر من شخص في تنفيذ الجريمة، مثل قيام أحد الأفراد بوضع خطة الاحتيال بينما يتولى آخر تنفيذها أو خداع الضحية، أما المساهمة فتتمثل في المشاركة

---

[1] باسم شهاب ، المرجع السابق ، ص189.

[2] عبد الله سليمان ، شرح قانون العقوبات الجزائري القسم العام، الجزء الأول ، ديوان المطبوعات الجامعية الجزائرية ، الجزائر،2005 ، ص 169.

[3] منصور رحماني ، المرجع السابق ، ص 26 .

غير المباشرة في الجريمة، كأن يساهم الشخص بتوفير الوسائل أو الأدوات اللازمة لارتكاب الاحتيال مثل تزويد شخص آخر بحسابات مصرفية مزيفة أو مساعدة في إنشاء موقع إلكتروني مزيف ،أما التحريض يشمل إقناع أو دفع شخص آخر إلى ارتكاب جريمة الاحتيال، و استخدام أساليب خداع معينة لاستغلال ضحاياها.

وبموجب المادة 42 من قانون العقوبات الجزائري ، يُعاقب الشريك أو المحرض بالعقوبة المقررة للجريمة نفسها إذا كانت هذه الجريمة معاقب عليها في القانون ، ويُعتبر الشخص الذي يساهم في تنفيذ الجريمة سواء كان عن طريق التحريض أو المساعدة ، شريكًا في الجريمة ويُحاكم وفقًا للمبادئ ذاتها التي تحكم الفاعل الرئيسي.[1]

ثانيا : الظروف المشددة لعقوبة جريمة الاحتيال

تُعرَف الظروف المشددة على أنها الوقائع التي تضاف إلى الواقعة الأصلية المنسوبة إلى المتهم وتُساهم في تعزيز الأثر الإجرامي الذي ارتكبه، حيث يُترتب على وجود هذه الظروف زيادة شدة العقوبة المقررة قانونًا ، سواء كان ذلك عبر زيادة مدة العقوبة أو تخطي الحد الأقصى المنصوص عليه، وفي هذا السياق قد يتغير الوصف القانوني للجريمة بإضافة هذه الظروف إما ببقاء الوصف ذاته أو بتبديله إلى وصف آخر يتناسب مع الطابع المتشدد للأفعال المرتكبة، وتهدف هذه الظروف إلى زيادة فعالية العقوبة بما يتناسب مع الخطورة البالغة للجريمة ، ويعتمد تفعيل هذه الظروف على توافر ملابسات خاصة أو عامة تتعلق بالجريمة محل الاتهام[2].

[1] انظر المادة 42 قانون العقوبات الجزائري.

[2] أسماء مبارك الريامي ، المرجع السابق ، ص 97 .

وبالرجوع إلى نص المادة 372 الفقرة 2 من قانون العقوبات الجزائري، حدد المشرع الظروف التي تُشدد فيها عقوبة جريمة الاحتيال، وهي كالتالي :

إذا وقعت الجنحة من شخص لجأ إلى الجمهور بقصد إصدار أسهم أو سندات أو حصص أو أية سندات مالية سواء لشركات أو مشروعات تجارية أو صناعي ، ضاعف المشرع الحد الأقصى لعقوبة الاحتيال لتوافر هذا الظرف ، بحيث يجب أن يكون مضمون المشروع الكاذب يتعلق بالمساهمة في شركة أو مشروع تجاري أو صناعي ، ويجب أن يتوافر في الأشخاص الذين يتولون إصدار الأسهم أو السندات أو الأذونات المالية عنصر الثقة التي تتخدع بها العامة ، مما يدفعهم للمساهمة أو تمويل عملية إصدار هذه الأوراق المالية لصالح شركات أو مشاريع معينة[1].

علة المشرع في تشديد العقوبة في هذه الحالة هي حماية صغار المدخرين، الذين غالبًا ما يكونون ضحايا هذه النوعية من الاحتيال ، كما أن هذا الظرف المشدد يعكس خطورة هذه الجريمة على الاقتصاد الوطني، حيث يُمكن أن يتسبب في ضرر واسع النطاق إذا تأثر عدد كبير من الأفراد بالاحتيال ، من خلال إعلانات أو نشرات تستهدف جمهورًا كبيرًا مما يؤدي إلى زيادة عدد الضحايا.[2]

كما تشدد العقوبة عندما تكون الدولة أو إحدى مؤسساتها هي الضحية ويتجلى ذلك في نص المادة 382 مكرر/2، حيث تُضاعف العقوبة لتصل إلى عشر سنوات حبسًا عندما تُرتكب الجنحة ضد الجهات العامة ، حمايةً للمال العام وصونًا لمكانة الدولة ومؤسساتها من المساس أو الخداع[3].

[1] أنظر المادة 372 فقرة 2 من قانون العقوبات الجزائري.

[2] محمد هشام صالح عبد الفتاح ، المرجع السابق، ص73.

[3] انظر المادة 382 مكرر 2 من قانون العقوبات الجزائري .

ثالثا: العقوبات التكميلية لجريمة الاحتيال

إضافة إلى العقوبات الأصلية لجريمة الاحتيال يُمكن أن يُحكم على الجاني بالعقوبات التكميلية أيضا والتي تُعد بمثابة عقوبات إضافية تهدف إلى ضمان ردع الجاني ومنع تكرار الجريمة ، [1]تشمل هذه العقوبات حسب المادة 9 مكرر 01 من قانون العقوبات مايلي :

- الحرمان من الحقوق الوطنية والمدنية مثل الحق في الانتخاب أو الترشح .
- العزل من الوظائف العمومية التي يشغلها الجاني إذا كانت لها علاقة بالجريمة المرتكبة.
- منع من مزاولة الأنشطة التجارية أو الاقتصادية التي قد تؤثر على المصلحة العامة أو تلحق ضررًا بالمجتمع.
- منع من شغل المناصب التي تتطلب الأمانة أو المصداقية ، مثل التدريس أو العمل كمساعد محلف أو خبير.
- سحب جواز السفر أو تعليق الحق في السفر لمدة معينة ، إذا كان مرتبطًا بالأمن العام أو بالتحقيق.

و بالنسبة للشخص المعنوي تتمثل العقوبات التكميلية حسب المادة 18 مكرر من قانون العقوبات في :

- حل الشخص المعنوي.
- غلق المؤسسة أو أحد فروعها لمدة لا تتجاوز خمس (5) سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات.

[1] منصور الرحماني ، المرجع السابق ، ص 24.

- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية، بشكل مباشر أو غير مباشر، نهائيًا أو لمدة لا تتجاوز خمس (5) سنوات.
- مصادرة الأشياء التي استُعملت في ارتكاب الجريمة أو نتجت عنها.
- نشر وتعليق حكم الإدانة في أماكن مناسبة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات ، وتنصب هذه الحراسة على النشاط الذي أدى إلى الجريمة أو ارتُكبت الجريمة بمناسبته.

الفرع الثاني : الجزاءت المقررة لجريمة الاحتيال باستخدام وسائل تقنية المعلومات

حرصًا على مواكبة التحولات التكنولوجية وما صاحبها من ظهور أنماط جديدة من الجرائم، عمد المشرع الجزائري إلى إدراج نصوص خاصة ضمن قانون العقوبات، تعنى بالأفعال غير المشروعة التي تستهدف الأنظمة والمعلومات الإلكترونية، وذلك من خلال المواد من 394 مكرر إلى 394 مكرر 7، ورغم أن هذه النصوص لم تخصص تنظيماً مستقلاً لجريمة الاحتيال المعلوماتي، إلا أن ما تضمنته من تجريم للدخول غير المشروع، أو البقاء غير المشروع، أو التلاعب بالبيانات والمعطيات الإلكترونية تنطوي ضمنًا على صور من الاحتيال المعلوماتي الذي يمس بحقوق الأفراد والمؤسسات، مما يسمح باستنباط الأحكام العقابية الخاصة بهذه الجريمة من خلالها وهو ما نتطرق إليه في هذا الفرع .

أولا : العقوبات الأصلية لجرائم المساس بأنظمة المعالجة الآلية للمعطيات

نظراً لتعدد صور الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات ، حدد المشرع الجزائري مجموعة من الأفعال التي تشكل مساساً الأنظمة والمعطيات المخزنة في المنظومة المعلوماتية ، وقد رتب على كل فعل من هذه الأفعال عقوبات أصلية تتناسب مع طبيعة الاعتداء وخطورته ، و هي كالتالي :

1. عقوبة جريمة الدخول و البقاء في نظام المعالجة الآلية للمعطيات :

أ. جريمة الدخول و البقاء في صورتها البسيطة :

يتحقق الدخول الغير المشروع لنظام معلوماتي عندما يقوم شخص بولوج هذا النظام أو الاتصال به دون إذن أو تفويض من صاحب الحق ، سواء باستخدام وسائل تقنية لاختراق وسائل الحماية أو بدونها، كما يتحقق البقاء غير المشروع حينما يستمر الفاعل داخل النظام رغم زوال الصفة أو الإذن الذي كان يبرر وجوده ، كمن ينتهي عقد عمله ولا يغادر النظام المعلوماتي أو يتجاوز حدود صلاحياته.[1]

وتقوم الجريمة في هذه الصورة بمجرد الدخول أو البقاء بدون وجه حق ، ومن الملاحظ أن الدخول أو البقاء غير المشروع قد يشكل في بعض الحالات المدخل الأساسي لارتكاب جرائم أخرى أشد خطورة مثل الاحتيال المعلوماتي ، حيث يستغل الفاعل هذا الولوج غير المشروع للتحصل على معطيات حساسة أو تنفيذ عمليات غير مشروعة داخل النظام.

وقد رتب المشرع الجزائري على هذه الأفعال، بموجب المادة 394 مكرر من قانون العقوبات، عقوبة الحبس من ثلاثة (3) أشهر إلى سنة ، وغرامة مالية تتراوح بين خمسين ألف دينار جزائري (50.000 دج) الى مئة ألف دينار جزائري (100.000 دج).[2]

ب. جريمة الدخول و البقاء في صورتها المشددة :

تتخذ الجريمة طابعًا مشددًا إذا كان الدخول أو البقاء في النظام المعلوماتي مصحوبًا بارتكاب أفعال تمس بسلامة المعطيات أو بحسن سير النظام، مثل حذف البيانات أو تغييرها أو إدخال

[1] زبيحة زيدان ، المرجع السابق ، ص 51.

[2] انظر المادة 394 مكرر من قانون العقوبات الجزائري .

معطيات جديدة، أو التسبب في اضطراب في تشغيل النظام، ويُعد هذا الشكل من الإجرام من أبرز صور الاحتيال المعلوماتي، لا سيما عندما يكون الهدف من هذه الأفعال تحقيق منفعة غير مشروعة أو الإضرار بالغير، إذ لا يقتصر السلوك الإجرامي على مجرد الولوج أو البقاء غير المصرح به، بل يمتد إلى الإضرار الفعلي بالمعطيات أو بالخدمات المقدمة عبر النظام، مما يبرر تشديد العقوبة.

شدد المشرع العقوبة في هذه الحالة حسب الفقرة الثانية من المادة 394 مكرر ، فرفعها إلى الحبس من ستة أشهر (6) إلى سنتين (2) ، وغرامة مالية من خمسين ألف دينار جزائري (50.000) إلى (150.000) دينار جزائري .

2. عقوبة جريمة التلاعب بمعطيات الحاسب الآلي :

يقصد بجريمة التلاعب بالمعطيات، قيام الجاني عن طريق الغش بإحدى صور الأفعال التالية: إدخال بيانات غير صحيحة إلى النظام، أو إزالة بيانات قائمة، أو تعديل بيانات موجودة، بما يؤدي إلى إفساد محتوى النظام أو تحريف نتائجه و تغيير حالة المعطيات فيه أو طمس المعلومات المسجلة داخله[1]، وتكمن خطورة هذا السلوك في أنه لا يستهدف فقط النظام في بنيته التقنية، بل يُسخَّر لتحقيق أغراض احتيالية تضر بمصالح الأفراد والمؤسسات على حدّ سواء.

يعاقب المشرع الجزائري على هذه الجريمة بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة مالية تتراوح بين خمسمائة ألف (500.000 دج) ومليوني (2.000.000 دج) دينار جزائري، طبقًا لما نصت عليه المادة 394 مكرر 1 من قانون العقوبات .[2]

---

[1] براهيمي جمال ، مكافحة الجرائم الالكترونية في التشريع الجزائري ، المجلة النقدية ، المجلد 11 ، العدد 2 ، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016 ، ص ص 131-132.

[2] انظر المادة 394 مكرر 1 من قانون العقوبات الجزائري .

3. عقوبة جريمة التعامل الغير مشروع في المعطيات :

تتعلق هذه الجريمة بالتصرفات الغير قانونية التي تشمل المعطيات التي تم معالجتها، تخزينها، أو إرسالها عبر الأنظمة المعلوماتية أو حتى تلك المتحصل عليها من إحدى الجرائم السابقة الذكر، ثم يتم التصرف بها خارج هذه الأنظمة ، تشمل هذه الأفعال تصميم المعطيات أو البحث فيها لإعداد برامج خبيثة أو لاختراق الأنظمة، بالإضافة إلى التجميع والتوفير المعطيات لاستخدامها في جرائم مثل الاحتيال ، قد تشمل هذه المعطيات معلومات حساسة تُستخدم للإضرار بالأفراد أو المؤسسات ، كما تشمل الجريمة الحيازة أو الإستعمال ،النشر والإفشاء للمعطيات الغير مشروعة عبر المنظومة المعلوماتية.[1]

يعاقب المشرع الجزائري على هذه الجريمة حسب المادة 394 مكرر 2 من قانون العقوبات بالحبس من شهرين (2) إلى ثلاث (3) سنوات و بغرامة مالية من (100,000) إلى (500,000) دينار جزائري .[2]

4. عقوبة الإتفاق الجنائي :

عاقب المشرع الجزائري على هذه الجريمة بموجب المادة 394 مكرر 5 من قانون العقوبات ، حيث نص على معاقبة كل من يشارك في اتفاق جنائي أو في مجموعة تهدف للإعداد لارتكاب جريمة معلوماتية أو أكثر ، وذلك بالعقوبات المقررة للجريمة نفسها التي تم الاتفاق عليها، حتى

[1] بعقيقي عبير ، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإمراتي -دراسة مقارنة- ، أطروحة دكتوراه في الحقوق تخصص النظام الجزائي و السياسة الجزائية المعاصرة ، كلية الحقوق و العلوم السياسية ، جامعة محمد خيضر ، بسكرة ، 2018/2017، ص 169.

[2] انظر المادة 394 مكرر 2 من قانون العقوبات الجزائري .

لو لم تتحقق الجريمة، أي أنه يكفي التحضير والتحفيز لهذه الجرائم، كما يتم فرض العقوبات على الأفعال المادية التي تسبق التنفيذ الفعلي للجرائم.[1]

5. عقوبة الشروع في جرائم المساس بأنظمة المعالجة الآلية للمعطيات :

عاقب المشرع الجزائري على الشروع في جرائم المساس بأنظمة المعالجة الآلية للمعطيات بموجب المادة 394 مكرر 7 من قانون العقوبات، حيث نص على معاقبة الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجريمة ذاتها، وقد جاء هذا التشريع في إطار احترام المبدأ الدولي لتجريم الشروع في الجرائم المعلوماتية، الذي يعكس أهمية حماية الأنظمة المعلوماتية من أي تهديدات ويرجع ذلك إلى خطورة هذه الجرائم ، وهو ما يتماشى مع التوجهات الدولية في هذا المجال، خصوصًا مع التشريعات المماثلة في دول أخرى مثل فرنسا[2].

ثانيا : الظروف المشددة لعقوبة جرائم المساس بأنظمة المعالجة الآلية للمعطيات

تشدد العقوبات المقررة للجرائم المعلوماتية وفقًا لما نصت عليه المادة 394 مكرر 3 من قانون العقوبات الجزائري إذا كان محل الاعتداء أنظمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، بحيث تضاعف العقوبات المنصوص عليها دون الإخلال بتطبيق عقوبات أشد عند الاقتضاء ، فقد نص المشرع على مضاعفة العقوبات الأصلية بحسب طبيعة الجريمة المرتكبة حسب طبيعة المعطيات محل الجريمة وخطورة الفعل المرتكب.[3]

وبما أن الشخص المعنوي قد يرتكب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات عن طريق ممثليه أو أجهزته، فقد نص المشرع الجزائري صراحة على معاقبته في المادة 394 مكرر 4 من

[1] بعقيقي عبير ، المرجع السابق، ص 115.

[2] بعقيقي عبير ، المرجع السابق ، ص 120.

[3] انظر المادة المادة 394 مكرر 3 من قانون العقوبات الجزائري .

قانون العقوبات أن الشخص المعنوي يعاقب بغرامة تساوي خمسة أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي، أما إذا استهدفت الجريمة المعلوماتية الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، فإن العقوبة الأصلية المضروبة في خمس مرات تتضاعف مرة أخرى، مما يجعل الغرامة تصل إلى عشرة أضعاف الحد الأقصى عن تلك المقررة للشخص الطبيعي.[1]

ثالثا : العقوبات التكميلية لجرائم المساس بأنظمة المعالجة الآلية للمعطيات

وفقًا للمادة 394 مكرر 6 من قانون العقوبات الجزائري، أخذ المشرع في اعتباره مراعاة حقوق الغير حسن النية في سياق تطبيق العقوبات التكميلية ، حيث تم النص على أن العقوبات التكميلية لا تشمل الأشخاص الذين لم يكن لهم علم بارتكاب الجريمة المعلوماتية، وهو ما يضمن حماية حقوق الأفراد الذين لم يتورطوا بشكل غير قانوني في الواقعة، و حدد هذه العقوبات في ثلاثة تدابير رئيسية:[2]

المصادرة: يتم مصادرة الأجهزة، البرمجيات، وكل الوسائل المستعملة في ارتكاب الجريمة المعلوماتية، وذلك بهدف تقليص الأدوات التي يمكن أن تستخدم مستقبلاً في ارتكاب جرائم مماثلة.

إغلاق المواقع الإلكترونية: يقصد بذلك غلق المواقع الإلكترونية التي كانت محلاً لارتكاب الجريمة المعلوماتية، بهدف الحد من استمرار استخدامها كفضاء لارتكاب مثل هذه الأفعال.

[1] بعقيقي عبير، المرجع السابق ، ص 128 .

[2] زبيحة زيدان ، المرجع السابق ، ص103 .

إغلاق المحل أو مكان الاستغلال: في حال تم ارتكاب الجريمة داخل محل معين، مثل مقهى إنترنت أو محل معلوماتي، يتم إغلاق هذا المكان بشرط أن يكون مالكه على علم بارتكاب الجريمة في موقعه.[1]

[1] عميري فيصل ، الحماية الجنائية للمعلوماتية في التشريع الجزائري ، مجلة افاق العلوم ، المجلد 7، العدد 1، جامعة الجزائر 01 ، 2022 ، ص 465.

خلاصة الفصل الثاني :

يتضح من خلال هذا الفصل أن جريمة الاحتيال باستخدام وسائل تقنية المعلومات لا يمكن معالجتها ضمن الأطر التقليدية التي وُضعت للجرائم العادية، إذ فرضت طبيعتها التقنية والحدودية استحداث منظومة قانونية خاصة، تستجيب لحجم التحديات التي تفرضها، وقد سعى المشرّع الجزائري إلى تعزيز فعالية التحري والمتابعة من خلال إدراج آليات إجرائية جديدة بموجب قانون الإجراءات الجزائية، كالتسرب الإلكتروني، اعتراض المراسلات، والمراقبة الالكترونية، بما يسمح بتتبع هذا النوع من الجرائم بكفاءة دون الإخلال بضمانات المحاكمة العادلة، كما برز الدليل الرقمي كأداة إثبات محورية، تكتسي طابعًا تقنيًا خاصًا وتستوجب إطارًا قانونيًا يكفل الاعتراف بها وحمايتها من العبث أو التلاعب.

في السياق ذاته، شكّل التعاون الدولي ركيزة أساسية في مكافحة هذا النوع من الجرائم، نظرا للطابع العابر للحدود الذي يميزها، ما جعل الاتفاقيات الدولية والإقليمية وكذا آليات المساعدة القضائية المتبادلة تمثل وسائل لا غنى عنها لتعزيز فعالية المواجهة، وعلى الصعيد الوطني، بادر المشرّع إلى تكريس سياسة تجريمية واضحة تُعاقب على الأفعال الاحتيالية المرتكبة بوسائل تقنية، من خلال النص على جزاءات أصلية وتكميلية تتناسب مع خطورة جريمة الاحتيال المعلوماتي وآثاره المتعددة، وهو ما يعكس توجهاً تشريعياً نحو بناء منظومة قانونية حديثة قادرة على التصدي لجريمة الاحتيال المعلوماتي كصورة متطورة للجريمة في العصر الرقمي.

خاتمة

خاتمة :

أظهرت الدراسة أن جريمة الاحتيال باستخدام وسائل تقنية المعلومات تمثل نمطًا مستحدثًا من السلوك الإجرامي، يتميز بقدر عالٍ من التكيف مع البيئات الرقمية المختلفة، وهي جريمة تقوم على استغلال الوسائل التقنية بطرق احتيالية تهدف إلى تحقيق كسب غير مشروع، من خلال الاعتداء على نظم المعالجة الإلكترونية للمعطيات أو استدراج الضحية بطرق مموّهة رقمياً، مما منحها طابعًا خاصًا يميزها عن جرائم الاحتيال التقليدية من حيث الوسائل، الضحايا، طبيعة الاعتداء، و النتائج المترتبة عنها .

كما تبين أن هذه الجريمة أصبحت من أكثر صور الجرائم المعلوماتية تعقيدًا من الناحية القانونية والإجرائية، حيث لم تعد الأنظمة الوطنية التقليدية قادرة على مواجهتها دون التعاون الدولي والآليات المستحدثة في الإثبات والتحري، فهي جريمة لا تقتصر على النطاق المحلي، بل تتخطى الحدود الجغرافية والسيادية للدول، وتستهدف البنية الرقمية للأفراد والمؤسسات على حد سواء، ما يستوجب بناء منظومة قانونية حديثة ومتكاملة تستجيب لهذا النوع من التهديدات الرقمية.

1. النتائج:

- ✓ تبيّن أن جريمة الاحتيال المعلوماتي تختلف من حيث طبيعتها ووسائل تنفيذها عن صور الاحتيال التقليدي، إذ تقوم أساسًا على استغلال الأنظمة الإلكترونية والبيانات الرقمية بطرق معقدة ومموّهة.
- ✓ أظهرت الدراسة تنوع صور هذه الجريمة وتطورها المستمر، لاسيما من خلال استهداف بطاقات الائتمان، المواقع الإلكترونية، والتحويلات المالية، وهو ما يعكس قابليتها الدائمة للتجدد والامتداد.

- ✓ أثبت التحليل أن الآليات الإجرائية التقليدية لم تعد كافية للتصدي لهذه الجريمة، مما فرض استحداث وسائل تقنية جديدة مثل التسرب الإلكتروني واعتراض المراسلات والمراقبة الإلكترونية.
- ✓ برز الدليل الرقمي كوسيلة إثبات أساسية في هذا النوع من الجرائم، إلا أن طبيعته التقنية تفرض ضرورة وجود إطار قانوني يضمن حمايته ويضبط شروط استخدامه أمام الجهات القضائية.
- ✓ كشفت الدراسة عن تعدد السبل التشريعية المعتمدة لمكافحة الجريمة المعلوماتية، سواء على المستوى الوطني الإقيمي أو الدولي، مؤكدة على أهمية المواءمة بين التشريعات الداخلية والاتفاقيات الدولية لضمان نجاعة التصدي لهذا النوع من الجرائم.

2. التوصيات:

- ✓ ضرورة تحديث المنظومة التشريعية الوطنية بصفة دورية لمواكبة التغيرات التقنية التي تستغل في جرائم الاحتيال باستخدام وسائل تقنية المعلومات .
- ✓ تعزيز الكفاءة المؤسسية من خلال تكوين متخصص للقضاة، ضباط الشرطة القضائية، وأعوان الرقابة الإلكترونية في مجال مكافحة الجريمة المعلوماتية.
- ✓ تفعيل الانضمام إلى الاتفاقيات الدولية ذات الصلة وتوسيع مجالات التعاون القضائي والتقني العابر للحدود.
- ✓ إطلاق حملات توعوية وتحسيسية تستهدف فئات المجتمع المختلفة، لاسيما مستخدمي الخدمات البنكية والإلكترونية، لتعزيز الوعي بمخاطر الاحتيال باستخدام وسائل تقنية المعلومات وطرق التوقي منه.

قائمة المراجع

قائمة المراجع:

I. المراجع باللغة العربية :

أولا: المعاجم

1. ابن منظور، لسان العرب، ج 12، د.ط. دار صادر للطباعة، بيروت، 1998.
2. عبد الغفور عبد الفتاح قاري، معجم مصطلحات المكتبة والمعلومات: انجليزي- عربي، مكتبة الملك الوطنية، الرياض، 2000.

ثانيا: الكتب

1. أحمد بن محمد بن علي الفيومي المقرئ، المصباح المنير في غريب الشرح الكبير، مكتبة لبنان، 2009.
2. أيمن عبد الله فكري ، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية و الاجنبية ، الطبعة الاولى، مكتبة القانون و الاقتصاد ، الرياض، 2015.
3. باسم شهاب، جرائم المال والثقة العامة (السرقة، خيانة الامانة، الاحتيال، اصدار شيك دون رصيد) مع الجرائم الملحقة بها او القريبة منها في ظل التشريعات الجزائرية و المقارنة، دون طبعة، دار بيرتي للنشر، الجزائر، 2013.
4. خالد بن سليمان الغثبر، سليمان عبد العزيز الهيشة، الاصطياد الالكتروني الاساليب و الاجراءات المضادة ، الطبعة الاولى ، الرياض ، السعودية 2009.
5. رشيدة بوكر، الحماية الجزائية للتعاملات الالكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020.

6. زبيحة زيدان، "الجريمة المعلوماتية في التشريع الجزائري و الدولي"، دون طبعة، دار الهدى، الجزائر، 2011.
7. سامر سليمان الجبوري، "جريمة الاحتيال الالكتروني دراسة مقارنة"، مكتبة زين الحقوقية، الطبعة الاولى، 2018.
8. عبد العزيز بن إبراهيم بن محمد الشبل، الاعتداء الإلكتروني: دراسة فقهية، دون طبعة، دار كنوز اشبيليا للنشر والتوزيع، السعودية، 2022.
9. عبد الله سليمان ، شرح قانون العقوبات الجزائري القسم العام، الجزء الأول ، ديوان المطبوعات الجامعية الجزائرية ، الجزائر ،2005.
10. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الانترنيت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2007.
11. علم الدين، محمود، تكنولوجيا المعلومات وصناعة الاتصال الجماهيري، العربي للنشر والتوزيع، 1990.
12. علي عدنان الفيل، "اِجراءات التحري و جمع الأدلة و التحقيق الاِبتدائي في الجريمة المعلوماتية (دراسة مقارنة)"، دون طبعة، دار الكتب و الوثائق العلمية، مصر، 2012.
13. عادل ابراهيم العاني، جرائم الاعتداء على الاموال في قانون العقوبات ؛ السرقة - الاحتيال - اساءة الإئتمان، دون طبعة، دار الثقافة للنشر، عمان1997.
14. غادة نصار ، الارهاب و الجريمة الالكترونية ، الطبعة الاولى، العربي للنشر والتوزيع ،القاهرة ،2017.
15. فريد رستم هشام، قانون العقوبات ومخاطر تقنية المعلومات، دون طبعة، مكتبة الآلات الكاتبة، القاهرة، ،1995.

16. كريم منشد خنياب الأسدي ، جرائم النصب و الاحتيال و علاقتها بالجرائم المشابهة لهما في القانون الجنائي ،الطبعة الأولى، دار النشر الان ناشرون و موزعون، عمان ، الاردن ، سنة 2015.

17. كميت طالب البغدادي ، "الاستخدام غير المشروع لبطاقات الائتمان" ، دون طبعة، دار الثقافة للنشر و التوزيع، عمان ، 2008 .

18. محمود الكيلاني، "الموسوعة التجارية و المصرفية"، المجلد الرابع، عمليات البنوك، دراسة مقارن، دون طبعة، دار الثقافة للنشر و التوزيع، 2008.

19. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دون طبعة، دار الثقافة للنشر والتوزيع، الأردن، 2005.

20. محمد أحمد الشوابكة، جرائم الحاسوب والانترنيت، الطبعة الأولى، مكتبة دار الثقافة و التوزيع، عمان، 2004.

21. محمد بن ابي بكر بن عبد القادر الرزاي، مختار الصحاح، دون طبعة، دار الكتاب العربي، لبنان، 1981.

22. محمد الشوابكة، جرائم الحاسوب و الانترنيت الجريمة المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة 2007.

23. محمود محمد طه، المواجهة التشريعية الجرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر والقانون، القاهرة، 2013 .

24. محمود نجيب حسني، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، المجلد الأول، منشورات الحلبي الحقوقية، بيروت، لبنان، 1998.

25. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1992.

26. محمد الامين البشرى، التحقيق في الجرائم المستحدثة، مركز الدراسات و البحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

27. محمد محمد الهادي، تكنلوجيا المعلومات و تطبيقاتها، دون طبعة، دار الشروق، القاهرة ،1989.

28. منصور رحماني، القانون الجنائي للمال و الاعمال الجزء الاول، دون طبعة، دار العلوم للنشر و التوزيع، الجزائر، 2019.

29. نهلا عبد القادر المومني ، الجرائم المعلوماتية، دون طبعة، دار الثقافة، عمان، الاردن، 2010.

30. هدى قشقوش، "جرائم الحاسب في التشريع المقارن"، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992.

ثالثا: الرسائل والمذكرات الجامعية

أ/ رسائل الدكتوراه

1. أحمد حمي، جرائم تقنية المعلومات وآليات مكافحتها وفقا لاتفاقية العربية لمكافحة جرائم المعلومات- دراسة مقارنة -، أطروحة دكتوراه في الحقوق، تخصص القانون الجنائي، المركز الجامعي أمين العقال الحاج موسى أق اخموك تامنغست، معهد الحقوق والعلوم السياسية، الجزائر، 2020/2019.

2. بلال بن جامع، الجرائم المعلوماتية على شبكة الأنترنيت دراسة حالة جامعة عبد الحميد مهري قسنطينة 2، أطروحة دكتوراة في علم المكتبات و التوثيق، معهد علم المكتبات و التوثيق، جامعة قسنطينة 2 عبد الحميد مهري، الجزائر، 2017/2016.

3. بدري فيصل ، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي ، أطروحة دكتوراة تخصص قانون عام ، كلية الحقوق ، جامعة الجزائر 01 -بن يوسف بن خدة- ، 2018/2017.
4. حسين ربيعي ، آليات البحث و التحقيق في الجرائم المعلوماتية، أطروحة مقّدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص قانون العقوبات و العلوم الجنائية، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2016.
5. رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية و السياسية، المجلد 03، العدد 05، جامعة قاصدي مرباح، ورقلة، الجزائر، 2012.
6. عبد الرحمان نشادي، الجرائم المعلوماتية في وسائل الاتصال الحديثة، اطروحة دكتوراه في علوم الاعلام و الاتصال، كلية الاعلام و الاتصال، جامعة الجزائر 3، 2017.
7. عبد القادر عميمر، اليات اثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه علوم في القانون العام تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1(بن يوسف بن خدة)، 2020/2019.
8. عبير بعقيقي ، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإمراتي -دراسة مقارنة-، أطروحة دكتوراه في الحقوق تخصص النظام الجزائي و السياسة الجزائية المعاصرة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر،2018/2017.
9. نسيمة درار ، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد، الجزائر ، 2016-2015.

10. هدى رابح ، بطاقة الائتمان البنكية و الجرائم المتعلقة بها، اطروحة لنيل شهادة دكتوراه علوم تخصص قانون بنكي و مالي، كلية الحقوق و العلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2022.

11. ياسين بن عمر ، "جريمة النصب المعلوماتي(دراسة مقارنة)"، اطروحة مقدمة لنيل شهادة الدكتوراه العلوم في الحقوق، جامعة الحاج لخضر -1-باتنة، 2022/2021.

ب/ مذكرات الماجستير

1. أسماء مبارك الريامي، احكام الاحتيال الالكتروني، رسالة ماجيستر في القانون العام، قسم القانون، جامعة ابو ظبي، الامارات، 2022.
2. خديجة دحمان صبايحية ، جرائم السرقة و الاحتيال عبر الانترنيت، دراسة بين الفقه الاسلامي و القانون الجزائري، رسالة الماجستير في العلوم الاسلامية، كلية العلوم الاسلامية، جامعة الجزائر، 2013.
3. عبير علي محمد النجار، جرائم الحاسب في الفقه الاسلامي، رسالة الماجستير في الفقه المقارن، كلية الشريعة و القانون، الجامعة الاسلامية غزة، فلسطين،2009.
4. محمد هشام صالح عبد الفتاح، جريمة الاحتيال دراسة مقارنة، أطروحة نيل شهادة الماجيستر في القانون، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2008.
5. نعيم سعيداني ، اليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة الماجستير في العلوم القانونية، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013.

6. يوسف صغير ، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

ج/ مذكرات الماستر

1. حنان ديلمي، "الدليل العلمي الالكتروني في القانون الجنائي الجزائري"، مذكرة ماستر ، كلية الحقوق و العلوم السياسية،جامعة محمد البشير الإبراهيمي برج بوعريريج ، الجزائر،2022/2021.

رابعا: المقالات

1. أسامة بن يطو، حمزة عبدلي، حماية برامج الحاسب الالي في ضوء التشريع الجزائري والمواثيق الدولية، مجلة المعارف جامعة اكلي محند الحاج، البويرة، العدد 19، ديسمبر 2015.
2. اسمهان بن مالك، خصائص الجريمة المعلوماتية و اسباب ارتكابها، مجلة البيبان للدراسات القانونية والسياسية، جامعة البشري الابراهيمي، برج بوعريريج، الجزائر، العدد 1، جوان 2019.
3. جمال براهيمي، مكافحة الجرائم الالكترونية في التشريع الجزائري ، المجلة النقدية ، المجلد 11 ، العدد 2 ، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيـزي وزو، 2016
4. حسين العيساوي ، الإنابة القضائية في القانون الخاص الجزائري، مجلة الاستاذ الباحث للدراسات القانونية و السياسية، المجلد 06، العدد 02، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، جانفي 2022.
5. حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، دراسات وأبحاث العدد جامعة زيان عاشور الجلفة، الجزائر، 2009.

6. حليم رامي، "اجراءات استخلاص الدليل في الجرائم المعلوماتية"، دفاتر البحوث العلمية، المجلد 09، العدد 01، جامعة البليدة 2 -لونيسي علي-، الجزائر، 2021.
7. خالد حامد مصطفى، المسؤولية الجنائية لناشري الخدمات التقنية و مقدميها عن سوء استخدام شبكات التواصل الاجتماعي، مجلة رؤى استراتيجية، مركز الامارات للدراسات و البحوث الاستراتيجية، مجلد 1، عدد 2، أبو ظبي،2013.
8. دنيا عبد العزيز فهمي ، المسؤولية الناشئة عن اساءة استخدام مواقع التواصل الاجتماعي ، مجلة الحقوق للبحوث القانونية و الاقتصادية ، المجلد 2 ، العدد2، جامعة الاسكندرية ، مصر، 2019.
9. رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية و السياسية، المجلد 03، العدد 05، جامعة قاصدي مرباح، ورقلة، الجزائر، 2012.
10. سامية العايب، منار عراية، "الحماية الجزائية للمستهلك من جريمة النصب الالكتروني"، مجلة هيرودوت للعلوم الانسانية و الاجتماعية، جامعة 8 ماي 1945 قالمة، الجزائر، ، 2021.
11. شهيرة ولحيت ، صويح دنيا زاد، الاحتيال الالكتروني، مجلة الدراسات القانونية و الاقتصادية، العدد 4، الجزائر، ديسمبر 2019.
12. صالح شنين، "إجراءات التحري و التحقيق في جرائم تكنولوجيات الاعلام و الاتصال في التشريع الجزائري - القانون 09/04"، مجلة الدراسات الحقوقية، المجلد 01، العدد 01، جامعة عبد الرحمان ميرة، بجاية، الجزائر، 2014.
13. صورية بوربابة ، عبد الكافي مريم، جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الالكترونية، مجلة القانون والعلوم السياسية، مجلد 8، عدد 01، جامعة طاهري محمد بشار، الجزائر، 2022.

14. عبد الرحمن محمد قدري حسن، جرائم الاحتيال الالكتروني، مجلة الفكر الشرطي، العدد 79، المجلد 20، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الامارات، اكتوبر. أبوظبي، 2011.

15. عبد الوهاب مخلوفي ، هوام علاوة، "اثر الاستخدام غير المشروع لبطاقات الائتمان و علاقته بجريمة تبييض الاموال"، مجلة العلوم الانسانية ، جامعة باتنة 1 الحاج لخضر ، باتنة ، الجزائر ، العدد 46، 2017.

16. علي اسلام العلمي ، عبد القادر بومسلة، برامج الحاسب الالي ومدى خضوعها لاحكام الامر رقم 03-05، مجلة الفكر القانوني والسياسي، العدد الثالث، جامعة عمار ثليجي، الاغواط، الجزائر، 2018.

17. عز الدين عثماني، "إجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الاتصال و المعلوماتية"، مجلة دائرة البحوث و الدراسات القانونية و السياسية-محبر المؤسسات الدستورية و النظم السياسية، المجلد02، العدد04، جامعة العربي تبسي، تبسة، الجزائر، 2018.

18. فيصل عماري ، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مجلة افاق العلوم، المجلد 7، العدد 1، جامعة الجزائر 01، 2022.

19. كلثوم قراوي ، "مشروعية الجليل الالكتروني في الاثبات الجزائي"، مجلة طبنة للدراسات العلمية الاكاديمية، المجلد 5، العدد 01، جامعة الجزائر 1، 2021.

20. ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية، الاتجاهات الدولية في مكافحة الجريمة الالكترونية، دراسات وأبحاث، المجلد 1، العدد1، جامعة زيان العاشور، الجلفة، الجزائر، 2009.

21. مختار دويني ، وسائل الدفع الإلكتروني ومدى مساهمتها في تطور التجارة الإلكترونية في الجزائر، مجلة القانون العام الجزائري والمقارن، المجلد 7، العدد 1، جامعة جيلالي ليابس، سيدي بلعباس، الجزائر، 2021.

22. مريم لوكال، قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني و حماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والاقتصادية، المجلد 4، العدد 3، جامعة احمد بوقرة، بومرداس، الجزائر،2021.

23. محمود محمد صفاء الدين على شرشر ، الجهود الدولية والتشريعية لمكافحة جرائم الأنترنيت ، مجلة البحوث القانونية و الاقتصادية -المنوفية ، كلية الحقوق ، جامعة المنوفية ، مصر، 2021.

24. نضال سالمي ، الإطار التنظيمي للدليل الرقمي في الإثبات، مجلة القانون والمجتمع، المجلد 10، العدد 01، جامعة وهران 2- محمد بن احمد-، الجزائر، 2022.

25. نبيل بن عودة ، درعي العربي ، الإنابات القضائية الدولية في المجال الجزائي، مجلة القانون الدولي و التنمية، المجلد 7 ، العدد 2 ، جامعة عبد الحميد بن باديس ، مستغانم ، 2020.

26. نوال مجدوب ، "الآليات الإجرائية للكشف عن الجريمة المعلوماتية"، مجلة البحوث القانونية والاقتصادية، المجلد 06، العدد 03، المركز الجامعي مغنية، الجزائر، 2022.

27. نور الهدى محمودي، "حجية الدليل الرقمي في اثبات الجريمة المعلوماتية"، مجلة الباحث للدراسات الاكاديمية، المجلد 02، العدد 11، جامعة باتنة 1 الحاج لخضر، الجزائر، 2017.

28. هاجر اميرة بورايو، واقع استخدام البطاقات البنكية في الجزائر -دراسة مقارنة لعينة من البنوك العمومية الجزائرية- ، مجلة الابحاث الاقتصادية لجامعة البليدة2، المجلد13، العدد18، جامعة "لونيسي علي"، البليدة ، الجزائر، 2018.

خامسا: النصوص القانونية

1. الاتفاقيات الدولية :

1. معاهدة نموذجية بشأن نقل الاجراءات في المسائل الجنائية، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/118 المؤرخ في 14 كانون الأول / ديسمبر 1990.
2. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني / نوفمبر 2000، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 02-55، المؤرخ في 22 ذي القعدة عام 1422، الموافق 5 فبراير سنة 2002، الجريدة الرسمية العدد 09.
3. مشروع قانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات، المعتمد من طرف مجلس وزراء العدل العرب، الدورة التاسعة عشرة، القرار رقم 495 بتاريخ 8 أكتوبر 2003.
4. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المبرمة يوم 2010.12.21 والمصادق عليها بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 08/09/2014 الجريدة الرسمية 57 لسنة 2014.

2- النصوص التشريعية :

1. أمر رقم 66-156 المؤرخ في 18 صفر الموافق 8 يونيو سنة 1966، الذي يتضمن قانون العقوبات المعدل و المتمم ج.ر.ج.ج، العدد 49 لسنة 1966.
2. أمر رقم 15-02 المؤرخ في 23 جويلية 2015 المعدل و المتمم للأمر رقم 66-155 المؤرخ في 8 جوان 1966، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 40، الصادر بتاريخ 23 جويلية 2015.
3. قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966، والمتضمن قانون العقوبات الجزائري، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.
4. قانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية. الجريدة الرسمية، العدد 84، المؤرخة في 24 ديسمبر 2006
5. قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، ج.ر.ج.ج، عدد 47، 2009.
6. قانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر في 16 غشت 2009.

7. قانون رقم 18-04 المؤرخ في 10 مايو 2018 المتعلق بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 27، الصادر بتاريخ 13 مايو 2018.
8. قانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 هـ الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 35، الصادرة بتاريخ 13 يونيو 2018.

ب/ النصوص التنظيمية

1. مرسوم رئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 المتضمن تحديد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، الصادر في الجريدة الرسمية عدد 53 بتاريخ 08 أكتوبر 2015.

سادسا: الاتفاقيات الدولية الإقليمية

1. اتفاقية مجلس أوروبا رقم 108 لسنة 1981 بشأن حماية الأشخاص تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي، الموقعة في ستراسبورغ بتاريخ 28 يناير 1981.
2. اتفاقية بودابست المتعلقة بالجريمة المعلوماتية، المعتمدة من طرف مجلس أوروبا في 23 نوفمبر 2001، ودخلت حيز التنفيذ في 1 يوليو 2004.
3. اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية، المعتمدة في الدورة العادية الثالثة والعشرين لمؤتمر الاتحاد الأفريقي، مالابو، غينيا الاستوائية، 27 يونيو 2014.

سابعا: المؤتمرات الدولية

1. مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين، ميلانو، إيطاليا، 26 آب/أغسطس – 6 أيلول/سبتمبر 1985، الوثيقة A/CONF.121/22، منشورات الأمم المتحدة، نيويورك، 1980، الرابط: Previous Congresses
2. مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، كوبا، 27 آب/أغسطس – 7 أيلول/سبتمبر 1990، الوثيقة A/CONF.144/28/Rev.1، منشورات الأمم المتحدة، نيويورك، 1991، الرابط: EIGHTH UNITED NATIONS CONGRESS ON THE PREVENTION OF CRIME AND THE TREATMENT OF OFFENDERS | Office of Justice Programs
3. الجمعية الدولية لقانون العقوبات، أعمال المؤتمر الخامس عشر – ريو دي جانيرو، 4– 10 أيلول/سبتمبر 1994: الجريمة الاقتصادية وجرائم الكمبيوتر، منشورات AIDP، باريس، 1995. الرابط: XVe Congrès international de droit pénal (Rio de Janeiro, 4 – 10 septembre 1994) | Cairn.info

ثامنا: المواقع الالكترونية

1. الهام هواري، "تحذير عاجل لمستخدمي "بريدي موب" من الاحتيال الالكتروني"، منشور على موقع تحذير عاجل لمستخدمي "بريدي موب"من الاحتيال الإلكتروني ، تاريخ الاطلاع 08/04/2025 على الساعة 15:49.
2. احمد الشريف، احترس من عصابات المتاجر الوهمية لسرقة بيانات بطاقات الائتمان، منشور على احترس من عصابات المتاجر الوهمية لسرقة بيانات بطاقات الائتمان .. ما القصة؟ ، تاريخ الاطلاع 2025/04/09، على الساعة 14:52

3. "التحويل الإلكتروني: تحويل الأموال الإلكتروني: التحويل الإلكتروني وRTGS: فهم أنظمة الدفع الإلكترونية"، منشور على موقع التحويل الإلكتروني: تحويل الأموال الإلكتروني: التحويل الإلكتروني و RTGS: فهم أنظمة الدفع الإلكترونية - FasterCapital ، تم الاطلاع في تاريخ 11/04/2025 على الساعة 08:26.
4. الاحتيال أثناء تقديم البطاقة: مكافحة الأنشطة الاحتيالية باستخدام تقنية EMV، منشور على الموقع الإلكتروني تقنية EMV: كيف تمنع تقنية EMV الاحتيال أثناء تقديم البطاقة - FasterCapital ، تم الاطلاع عليه في تاريخ 2025/04/09، على الساعة 14:22.
5. الاحتيال على بطاقة الائتمان: كيفية منع الاحتيال على بطاقة الائتمان واكتشافه وماذا تفعل إذا كنت ضحية، منشور على الموقع الالكتروني الاحتيال على بطاقة الائتمان: كيفية منع الاحتيال على بطاقة الائتمان واكتشافه وماذا تفعل إذا كنت ضحية - FasterCapital، تم الاطلاع في تاريخ 2025/04/09، على الساعة14:18.
6. بشار خليل، ما هو هجوم الباب الخلفي؟ المعنى، التعريف، الأمثلة، مقال منشور على Syrian Computer Society ، تاريخ الاطلاع 17 مارس 20225، على الساعة 18:20.
7. خالد سيف الدين، الاحتيال المتغير في عالم بطاقات الائتمان، منشور على موقع الاحتيال المتغير في عالم بطاقات الائتمان ، تاريخ الاطلاع: 09/04/2025 على الساعة 14:56.
8. سمير منصوري، "محتالون يستولون على اربعة ملايير باستعمال "بريدي موب"، منشور على الموقع: محتالون يستولون على أربعة ملايير باستعمال "بريدي موب – "الشروق أونلاين ، تاريخ الاطلاع: 09/04/2025 على الساعة 15:14.

9. ستان كامينسكي، كيف يسرق مجرمو الإنترنت الأموال من البطاقات المصرفية — وكيفية حماية نفسك من هذه السرقة، منشور على مدونة كاسبرسكي الرسمية | كيفية حماية الأموال المسروقة من البطاقات المصرفية باستخدام شريحة وتقنية اتصال المجال القريب (NFC) ، تم الاطلاع في تاريخ 09/04/2025،على الساعة 14:37

10. شيرين عبد السلام، اهم برامج الحاسب الالي، 2 سبتمبر 2023، مقال منشور على الموقع الالكتروني أهم برامج الحاسب الآلي ووظائفها - موسوعة، تاريخ الاطلاع 12 مارس 2025، على الساعة 22:09.

11. عبد الرحمان الحاج، "تحذير عاجل من أندرويد بسبب برامج خبيثة تتسلل إلى الحسابات المصرفية"، منشور على موقع: الأمان المصرفي في خطر: تسلل البرامج الخبيثة إلى الهواتف - مجلة هي، تاريخ الاطلاع 09/04/2025 على الساعة 16:20.

12. عايض راشد المري، التحويل الالكتروني للأموال دراسة مقارنة، مارس 2024، مقال منشور على الموقع الالكتروني التحويل الإلكتروني للأموال – دراسة مقارنة – Kilaw Journal ، تاريخ الاطلاع 2025/04/10، على الساعة 11:36

13. كتبت هبة السيد، "برمجيات خبيثة متطورة تضرب نظام أندرويد وتستهدف الخدمات المصرفية"، منشور على تقرير يكشف.. ثلاث برمجيات خبيثة قادرة على سرقة البيانات والأموال - اليوم السابع ، تاريخ الاطلاع 09/04/2025 على الساعة 16:28.

14. ليندة عبد الله ، تبييض الاموال عن طريق الاعتماد المستندي للأموال" ، مجلة جيل البحث العلمي ، عدد خاص عن اعمال المؤتمر الدولي الرابع عشر ، طرابلس 25-24 مارس 2017 متوفر على موقع تبييض الأموال عن طريق الاعتماد المستندي الالكتروني | ليندة عبد اللهJiL.Center – ، تاريخ الاطلاع 11/04/2025 ، على الساعة 15:12

15. نهال نعواش، وسائل الدفع الإلكترونية، منشور على الموقع وسائل الدفع الإلكترونية - موضوع، تاريخ الاطلاع 04/09/2025، على الساعة 8:21.

II. المراجع باللغة الأجنبية

أولا: باللغة الفرنسية

1. code pénal français, article 313-1, sur le site officiel du gouvernement français « Legifrance ».
2. Code pénal, art. 323-1, al. 1 (France). (n.d.). Accès ou maintien frauduleux dans un système de traitement automatisé de données.

ثانيا: باللغة الانجليزية

1. AfricanUnion’s Malabo Convention on Cyber Security and Personal Data Protection Entersinto Force منشور على الموقع الالكتروني، African Union’s Malabo Convention on Cyber Security and Personal Data Protection Enters into Force يوم الاطلاع 2025/22/04، ساعة الاطلاع 17:42.
2. U.S. Code § 2703 - Requireddisclosure of customer communications or record, 18 U.S. Code § 2703 – Require d disclosure of customer communications or records | U.S. Code | US Law | LII / Legal Information Institute.

3. Lukas Stefanko, Fakebankingapps on Google Play leakstolencreditcard data منشور على الموقع الالكتروني ,Bogus apps found on Google Play leak stolen credit card credentials, 2025/04/0815:30 ، تاريخ الاطلاع، ساعة الاطلاع
4. Louis DeNicola, What Is Card Skimming and How Can You Avoid It?, منشور على الموقع What Is Card Skimming and How Can You Avoid It? - Experian14:15 على الساعة ,2025/04/09 تاريخ الاطلاع,
5. Nihadhassan, Social media phishing: Attacktactics and mitigation strategiesمنشور على الموقع الاكتروني , Social media phishing: Attack tactics and mitigation strategies | Barracuda Networks Blog تاريخ الاطلاع 04/ 08 / 2025، على الساعة 15:50.

6. Perbhdevsingh, URL manipulation techniques: Puny code, typosquatting, and more, منشور على الموقع الالكتروني URL manipulation techniques: Punycode, typosquatting, and more | Barracuda Networks Blog17:00 على الساعة 2025 / 08 /04، تاريخ الاطلاع ، .
7. Parliamentarians for Global Action. PGA Congratulates Grenada on becoming the 72nd State Party to the Budapest Convention on Cybercrime. منشور على الموقع الاكتروني PGA Congratulates Grenada on becoming the 72nd State Party to the Budapest Convention on

، تاريخ الاطلاع 04/20/2025 ، على الساعة Cybercrime - News Center
18:40

الفهرس

الفهرس