الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi – Bordj Bou Arreridj
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون أعمال

الموسومة ب:

الإطار القانوني لحماية المؤسسات من الاحتيال الالكتروني

إعداد الطالبين:

✓ عماد الدين سماتي

✓ العياشي ميلودي

إشراف:

د. منى طواهرية

السنة الجامعية: 2025/2024

ملحق بالقرار رقم ....1082.... المؤرخ في ....27 ديسمبر 2020....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): العياشي ميلود ..... الصفة: طالب، أستاذ، باحث ..... طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: 112681378 والصادرة بتاريخ 2019/01/05

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم القانون الخاص

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: الإطار القانوني لحماية المؤسسات من الاحتيال الالكتروني

....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 27 ماي 2025

توقيع المعني (ة)

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،

السيد(ة): عماد الدين سماتي ..... الصفة: طالب، أستاذ، باحث ..... طالب .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 413888974 والصادرة بتاريخ ..... 2024.11.04 .....

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسة قسم القانون الخاص .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

عنوانها: الإطار القانوني لحماية المرضى من الإجهاض .....

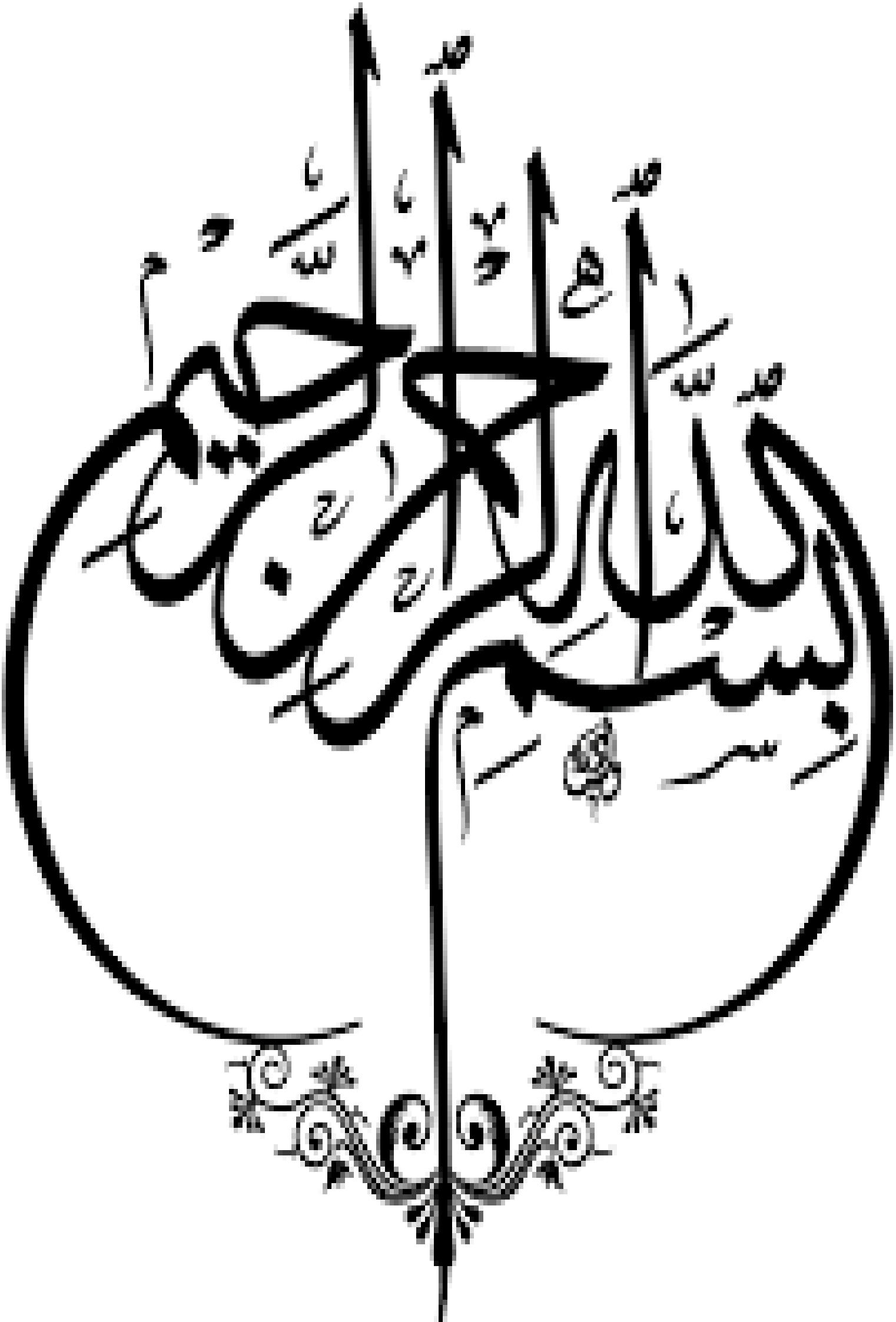
الإلكتروني .....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: ..... 2025.05.27 ..... 27 ماي 2025

توقيع المعني (ة)

نظرت للمصادقة على إمضاء
السيد: .....
رقم ب و ت أو رس: .....
الصادرة بتاريخ: .....
من طرف
من السيد(ة) بتفويض منه
عن رئيس للإدارة المركزية


بسم الله الرحمن الرحيم

شكر وعرفان

قال الله تعالى: "لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ"

ـ سورة إبراهيم، الآية 7 ـ

نتوجه بجميل الشـــكر والعرفان وخالص الثناء والامتنان للمولى عز وجل، الذي أنعم علينا بنعمة العلم والايمان، وحثنا على طلبه بلا حدود لزمان أو مكان، ووفقنا لإتمام هذا البحث، فله الحمد والمنة أولا وآخرا.

في خضم هذا الجهد العلمي، لا يسعنا إلا أن نعبر عن الإمتنان، فالشكر مفتاح البركة، وهو عربون وفاء لمن كان لهم الفضل بعد الله في إتمام هذه المذكرة.

نتوجه بأسمى آيات الشكر والعرفان إلى مشرفتنا الفاضلة الدكتورة طواهرية منى، التي كانت النور الذي أضـــاء لنا الطريق، والصـــوت الذي وجهنا، واليد التي إمتدت إلينا بعونها في كل مرحلة من مراحل هذا العمل. كلمات الشكر لا تفيها حقها، فقد كانت نعم السند والداعمة الحقيقية في أدق التفاصيل، فجزاها الله عنا كل خير، ورفع قدرها في الدارين.

كما لا يفوتنا أن نتقدّم بالشكر إلى أعضاء لجنة المناقشة، على قبولهم مناقشة هذا العمل وتقييمه.

والله وليّ التوفيق.

إهداء

إلى من كانت الدعوة الصادقة منها سرّ بركتي وتوفيقي،

إلى من سهرت لأجلي، وتحملت تعبي، وغمرتني بحنانها دون حدود...

ꕥ أمي العزيزة ꕥ

وإلى من كان السند والقدوة،

إلى من علّمني أن الطريق إلى النجاح لا يكون إلا بالعزيمة والإصرار...

ꕥ أبي الغالي ꕥ

إلى من تقاسمت معهم لحظات الحياة بحلوها ومرّها،

ꕥإلى إخوتي الأعزاء: أمين، سيرين، سلسبيل، فراس، دمتم لي خير رفيق،بكم أعتز و أفتخرꕥ

ꕥ ولا أنسى رفاق دربي وأصدقائي الأوفياء، جميعًا دون استثناءꕥ

لكم جميعا، أهدي هذا العمل، عرفانا بجميلكم، ووفاءً لحبكم، وامتنانًا لا ينتهي.

كنتم خير العون والدعم في كل المراحل

سماتي عماد الدين

إهداء

إلى من كانا سندي ودفئي في كل لحظة،

ﷺ والدي الغاليين، نبع الحنان والقوة ﷺ

الذين علموني معنى الصبر، وأضاءوا لي دربي.

ﷺ إخوتي الأعزاء ﷺ

الذين كانوا لي عونًا ورفاق درب لا يكلون،

ﷺ رفاق الشدة والفرح، وركائز لا تتزعزعﷺ

لكم جميعا، أهدي هذا العمل،

عرفانا بجميلكم، وفخرا بدعمكم، وإمتنانا لا ينضب.

ميلودي العياشي

المقدمة

المقدمة

عرف العالم في العقود الأخيرة ثورة معلوماتية هائلة نتج عنها تنامي استخدام الشبكة العنكبوتية في شتى المجالات، سواء في الإدارة، الاقتصاد أو حتى في التواصل بين الأفراد والمؤسسات. هذا التطور، وإن حمل في طياته فرصا غير مسبوقة للتنمية وحركية المجتمعات، إلا أنه طرح أنماطا جديدة من الجرائم الالكترونية التي وجدت في الفضاء الرقمي البيئة الأكثر خصوبة للنمو والتطور، مهددة أمن الدول والمجتمعات.

فقد أدى التوسع في استعمال هذه التكنولوجيا وارتباطها بأنظمة المؤسسات، إلى بروز جرائم إلكترونية معقدة، تستهدف المؤسسات المالية والاقتصادية وحتى الإدارات العمومية من خلال أساليب احتيالية متطورة تتم عن بعد، مستغلة في ذلك الثغرات القانونية، والتقنية لتحقيق مكاسبها غير المشروعة، يأتي في طليعة هذه الجرائم، الاحتيال الالكتروني، الذي تفاوتت أشكاله وآلياته بحسب الخصوصيات الثقافية والاجتماعية لكل مجتمع، فأصبح أكثر المجالات استقطابا للجماعات الاجرامية المنظمة، مستغلا تطور الوسائل المعلوماتية لخداع الضحايا سواء الأفراد أو المؤسسات، مما أفرز تحديات أمنية وقانونية معقدة نتيجة قدرته على تجاوز الحدود الجغرافية، واستغلال الثغرات في الأنظمة الرقمية.

فقد ساعدت الطبيعة اللامادية لجريمة الاحتيال الالكتروني، وتعقيداتها التقنية، والقدرة على إخفاء هويات الجناة، إلى جعلها تهديدا حقيقيا لجهود حماية المؤسسات، لما تطرحه من تحديات تتراوح بين النصب على الأفراد، وسرقة البيانات الشخصية، وصولا إلى استهداف المؤسسات المالية والاقتصادية، وحتى الإدارية، إذ لم تعد تداعياتها تقتصر على الجانب المالي فقط، بل تمتد إلى سمعة المؤسسات، وثقة المتعاملين والمستخدمين، خاصة وأن الأنظمة القانونية التقليدية لم تعد قادرة على مواجهة هذه التداعيات بفعالية في ظل التوسع الكبير لجريمة الاحتيال الالكتروني.

دفع هذا المشهد المتنامي، والمعقد لظاهرة الاحتيال الإلكتروني، وما تسببه من تداعيات جسيمة، بالدول على الصعيدين الدولي والوطني، إلى استشعار حجم الخطر، وضرورة التحرك الفوري من خلال إعادة النظر في الأطر التشريعية والقانونية القائمة، وتطويرها بما يسهم في بناء

المقدمة

منظومة قانونية ومؤسساتية تتسم بالديناميكية والمرونة، لتواكب التطورات المتسارعة في أساليب الاحتيال الالكتروني، وتعزيز الأمن السيبراني المؤسسي، وتنظيم التعاون الدولي، عبر إقرار أفضل الممارسات وتفعيل الاتفاقيات والتشريعات بما يسهم في حماية المؤسسات ومواجهة هذه الجريمة العابرة للحدود.

أهمية الدراسة: تنبع أهمية دراسة هذا الموضوع من جانبين: علمي وقانوني.

الأهمية العلمية: تكمن الجوانب العلمية في أن الدراسة تطرح موضوعا حديثا وهاما في حقل العلوم القانونية، خاصة وأن الاحتيال الالكتروني أضحى اليوم من المواضيع الحساسة والمهمة في سياسات الدول واستراتيجياتها، إذ رغم أن عديد الدراسات تناولت موضوع الجريمة الالكترونية، إلا أن مجالات البحث في جريمة الاحتيال الالكتروني لا تزال حديثة نسبيا، ومن ثمة تأتي هذه الدراسة كمساهمة في إثراء البحث العلمي بمثل هذه المواضيع الهامة، التي أضحت تشغل بال الدول أفرادا ومؤسسات.

كما تبرز أهمية الدراسة أيضا في كونها تسلط الضوء على واقع المؤسسات الدولية والوطنية في مواجهة الاحتيال الالكتروني، والدعوة إلى تطوير الاستراتيجيات والآليات القانونية والتقنية لحماية هذه المؤسسات.

الأهمية القانونية: تظهر أهمية الدراسة من الناحية القانونية في كونها تتناول الإطار القانوني المنظم لآليات الحماية، ومدى فعاليته في التصدي لجريمة الاحتيال الالكتروني، ومن ثمة تسهم الدراسة في إبراز الفجوات القانونية التي قد تعيق التصدي الفعال لهذه الجرائم، والحاجة إلى بناء منظومة تشريعية متكاملة، قادرة على الاستجابة الفعالة لطبيعة هذا النوع من الجرائم المستحدثة، وعلى حماية المؤسسات من المخاطر السيبرانية المتزايدة.

أهداف الدراسة: تسعى هذه الدراسة لتحقيق جملة من الأهداف، نوردها في ضوء النقاط التالية:

- توضيح مفهوم الاحتيال الالكتروني وتمييزه عن سابقه التقليدي.

- تحليل الآثار المترتبة عن تعرض المؤسسات للاحتيال الالكتروني.
- التعرف على الآليات القانونية والمؤسساتية الدولية والوطنية المستحدثة لمواجهة جريمة الاحتيال الالكتروني التي تستهدف المؤسسات.
- دراسة مدى فعالية الإطار القانوني والمؤسساتي الوطني، الإقليمي والدولي في التصدي لجريمة الاحتيال الالكتروني.
- إثراء النقاش العلمي حول هذا النمط من الجرائم المستحدثة. وتزويد المكتبة بالدراسات الحديثة.

أسباب اختيار الموضوع: يستند اختيارنا لهذا الموضوع من عدة أسباب، نلخصها في أسباب ذاتية وأخرى موضوعية.

1. الأسباب الذاتية

- اهتمامنا الخاص بمجال الجريمة الالكترونية عامة، والاحتيال الالكتروني بشكل خاص وتأثيرها على المؤسسات.
- محاولة ابراز أهمية الأطر القانونية في تأمين بيئة آمنة للمؤسسات من الاحتيال الالكتروني.
- تزايد حالات تعرض المؤسسات الوطنية والدولية للاحتيال الالكتروني دفعنا للبحث في الظاهرة والكشف عن خباياها وأدواتها.
- الاطلاع على الجهود الدولية والوطنية لمواجهة جريمة الاحتيال الالكتروني.

2. الأسباب الموضوعية

- غياب الوعي القانوني الكافي وعدم إلمام المؤسسات بخطورة هذه الجريمة.
- الحاجة إلى توفير حماية قانونية للمؤسسات من أجل اقتصاد وطني متماسك.
- المساهمة في إثراء المكتبة بدراسة تعالج موضوع هام، وقضية مستحدثة في القانون.

المقدمة

الدراسات السابقة

تناولت عديد الكتابات موضوع الاحتيال بشكله التقليدي سواء على المستوى الدولي أو الوطني، إلا أن ما كتب حول حماية المؤسسات من الاحتيال الالكتروني محدود جدا، فحسب اطلاعنا، وفي حدود علمنا لم نجد دراسة علمية أكاديمية ربطت بين موضوعي الاحتيال الالكتروني والمؤسسات بكافة متغيراتها، إذ أن معظم الدراسات المتعلقة بالاحتيال الالكتروني يغلب عليها الطابع التقني، أو تتناول جريمة الاحتيال الالكتروني بشكل عام، وعليه سيتم التركيز على الدراسات التي تخدم الموضوع بوصفها تعالج بعض جزئياته، نذكر منها مايلي:

1. حمد عبد الله يحي بوغانم السليطي، تجريم الاحتيال الالكتروني في القانون القطري والمقارن، رسالة ماجستير، كلية القانون، يونيو 2018.

ركزت هذه الدراسة على الاحتيال الالكتروني كجريمة تمس المال وترتكب عبر الحاسب الآلي والانترنت، متناولة تعريفها، أركانها، وخصائها القانونية، وذلك من خلال بعض القوانين المقارنة، كما ناقشت دور الشبكة العنكبوتية في ارتكاب الجريمة، وموقف الفقه والقضاء من هذه الجرائم، مشيرة إلى التحديات التي تواجه النصوص القانونية التقليدية.

من خلال ذلك، يتضح أن هذه الدراسة قد ركزت على جريمة الاحتيال الالكتروني بشكل عام، مع دراسة معمقة في القانون القطري والمقارن دون تخصيص نوع الضحايا المتستهدفين كالمؤسسات، وهو ما تركز عليها دراستنا، حيث كانت أكثر تخصيص من حيث الجانب المستهدف، بالإضافة إلى تناولنا للأثر القانوني والاقتصادي لهذا النوع من الاحتيال، وكذا جوانب الوقاية، والمسؤوليات التي تقع على عاتق المؤسسات، كما أن هذه الدراسة قد ركزت على القانون القطري أما دراستنا فقد تطرقت للقانون الجزائري والاقليمي وحتى الدولي.

2. أسماء مبارك الريامي، أحكام الاحتيال الالكتروني (دراسة مقارنة)، رسالة ماجستير، كلية القانون، جامعة أبوظبي ، 2021 – 2022 .

المقدمة

تناولت هذه الدراسة تحليلا قانونيا لجرائم الاحتيال الالكتروني في القانون الاماراتي مقارنة مع القانون السعودي ، حيث ركزت على ابراز الخصوصية القانونية لهذه الجريمة باعتبارها ظاهرة حديثة و متفردة تختلف عن الاحتيال التقليدي، نظرا لارتباطا بالتطورات التقنية، وأساليب التنفيذ المعقدة، وقد عالجت الدراسة مدى كفاية النصوص القانونية في مواجهة هذه الجريمة، ومدى توفر الأدلة التقنية اللازمة للإثبات، وتوصلت إلى أن التشريعين لم يحددا أساليب الاحتيال بدقة، مع وجود اختلافات في العقوبات، فمثلا قام المشرع الاماراتي بتجريم محاولة الاحتيال بنصف عقوبة بينما في التقليدي يعاقب المحاولة بسنتين كحد اقصى .

تختلف هذه الدراسة من حيث النطاق والتركيز، فهي دراسة مقارنة بين نظامين (الاماراتي والسعودي)، بينما تركز دراستنا على النطاق الوطني، والدولي على حد سواء، كما أن الاختلاف الجوهري يكمن في تركيز هذه الدراسة على الجانب القانوني فقط، بينما تركز دراستنا على الجانب التقني والجانب القانوني.

3. شركة مكافي، مركز الدراسات الاستراتيجية والدولية، التكاليف الخفية للجرائم الالكترونية، 07 ديسمبر 2020.

نشرت شركة مكافي تقريرا بعنوان "التكاليف الخفية للجريمة الالكترونية" بالتعاون مع مركز الدراسات الاستراتيجية الدولية، ومن أبرز ما جاء في هذا التقرير أن الجرائم السيبرانية تكلف الاقتصاد العالمي أكثر من تريليون دولار سنويا، وهو ما يمثل أكثر من 1% من الناتج المحلي العالمي، وأكد على أن الاضرار لا تقتصر على الخسائر المالية فقط، بل تشمل أضرارا خفية مثل تراجع ثقة العملاء ، فقدان البيانات الحساسة ، و تكاليف التعافي و اصلاح السمعة ، مما يجعل أثر الجريمة الالكترونية أعمق مما يبدو عليه.

تختلف هذه الدراسة في تركيزها على الجانب الاقتصادي العالمي وتأثره بالجرائم السيبرانية خاصة الشركات والبنى الاقتصادية بشكل عام، بينما ركزت دراستنا بشكل كبير على الإطار القانوني مع التركيز على حماية المؤسسات.

4. عبد الوهاب عبد الكريم محمد مبارك، إشـــكالية المســـؤولية القانونية عن جرائم النصب والاحتيال الواقعة على عملاء البنوك، المجلة القانونية، العدد 8، فيفري 2023.

تناولت هذه الدراسة اشكالية تتعلق المسؤولية القانونية عن جرائم النصب والاحتيال التي تقع على عملاء البنوك الذين يضـعون أموالهم بثقة في الانظمة الالكترونية، وقد أوضـحت المسـؤولية القانونية عند حدوث خلل تقني او احتيال الكتروني، كما تطرقت الدراسـة إلى الاحتيال الالكتروني كجريمة تلاعب بالمعلومات والبيانات باسـتخدام الانظمة المعلوماتية، وخطورة هذه الجريمة وسـرعة تنفيذها، وصعوبة كشفها، إلى جانب جهود بعض الدول في وضع قوانين للحد منها.

يكمن اختلاف هذه الدراسـة في تركيزها على المسـؤولية القانونية للاحتيال الالكتروني الذي يستهدف عملاء البنوك، خاصة في التعاملات المالية الالكترونية، بينما تستهدف دراستنا الحماية القانونية للمؤسسات من الاحتيال الالكتروني بشكل عام، و الاطار القانوني المنظم لها.

5. تقرير الانتربول، مجموعة اغمونت، مجموعة العمل المالي، التدفقات المالية غير المشروعة الناجمة عن الاحتيال الذي يسهل الانترنت ارتكابها، نوفمبر 2023.

جاء في هذه الدراسة أن الاحتيال الذي يسهل الانترنت ارتكابه بات يشكل تهديدا متسارعا و عابرا للحدود ، تقوده عصابات منظمة تتكون من مجموعات فرعية متخصصة ، أبرزها غاسلوا الاموال ، تستغل هذه العصابات التكنولوجيا الرقمية الحديثة ، مثل الخدمات المصرفية الافتراضية ومنصات الدفع عبر الانترنت ووسائل التواصل الاجتماعي ، لتنفيذ عمليات احتيال وجذب بغال المال، ثم تمرير المتحصلات عبر شبكات مالية معقدة تشمل شركات صورية ومؤسسات مالية مشـروعة ، و قد اكدت الدراسـة على خطورة هذا الاحتيال و ضـرورة تحسـين التنسـيق المحلي والدولي، وتفعيل آليات مثل مشـــروع I-GRIP التابع للانتربول لتعقب المدفوعات المشـــبوهة، إضافة إلى تشجيع الابلاغ عن الضحايا و المعاملات ، وتطوير أدوات تحليل متقدمة تحليل متقدمة ومؤشرات خطر تساعد على كشف ومنع هذه الانشطة الاجرامية .

المقدمة

تختلف هذه الدراسة في تسليطها الضوء على الاحتيال الالكتروني من منظور دولي واسع، مع التركيز عليه كجريمة عابرة للحدود، وتورط الشبكات الاجرامية المنظمة، بينما تركز دراستنا على المؤسسات التي تتعرض للاحتيال الالكتروني، وكيفية حمايتها من ذلك وطنيا، واقليميا، ودوليا.

إشكالية الدراسة

أدى الانتشار الواسع لتكنولوجيا الاعلام والاتصال إلى تغيير في أنظمة تسيير المؤسسات، غير أن هذا التغيير صاحبه تهديدات على هذه المؤسسات، من خلال تعرضها للاحتيال الالكتروني، الذي بات يهدد أمن واستقرار المؤسسات نظير اختراق المواقع، واستغلال الثغرات القانونية لتحقيق مكاسب غير مشروعة، وانطلاقا من ذلك نطرح الإشكالية التالية:

كيف يسهم الإطار القانوني الدولي والوطني في حماية المؤسسات من الاحتيال الالكتروني؟

لمناقشة الإشكالية، نطرح الأسئلة الفرعية التالية:

- **ما مفهوم الاحتيال الالكتروني؟ وفيما تتمثل أبرز خصائصه وأشكاله؟**
- **ما الآثار المترتبة على تعرض المؤسسات للاحتيال الالكتروني؟**
- **فيما تتمثل الأطر القانونية والمؤسساتية المعتمدة لحماية المؤسسات من الاحتيال الالكتروني على الصعيد الدولي والوطني؟**
- **ما مدى نجاح التعاون الدولي والإقليمي في دعم جهود المؤسسات للحماية من الاحتيال الالكتروني؟**

منهج الدراسة

يُعدّ المنهج العلمي بمثابة البوصلة الأكاديمية، والدليل الإرشادي الذي لا غنى عنه للباحث في مسعاه نحو تحقيق الأهداف المرجوّة والكشف عن الحقائق، وعليه فقد اعتمدنا في هذه الدراسة على المنهج الوصفي والمنهج التحليلي المناسبين لهذا الموضوع، حيث يساعد المنهج الوصفي في تشخيص الظاهرة محل الدراسة والربط بين متغيراتها بما يسمح بتقديم تفسيرات ملائمة تقود إلى

وصـــف عملي ملموس للظاهرة محل الدراســـة، وذلك من خلال جمع المعلومات الدقيقة حولها، ثم تحليلها وتفســـيرها بطريقة موضـــوعية تنســـجم مع المعطيات الفعلية للظاهرة، ومحاولة الربط بين المتغيرات واكتشـاف العلاقات المحتملة بينهما وإعطاء التفسـير الملائم الذي يسـمح بالوصـول إلى وصـــف عملي دقيق حول الظاهرة محل الدراســـة[1]، وقد اعتمدنا على هذا المنهج في كل مراحل الدراسة عبر تشـخيص واقع الاحتيال الالكتروني، وأثره على المؤسـسـات. ومن ثمة وصـف الوضـع القانوني الحالي المتعلق بحماية المؤسـسـات من الاحتيال الإلكتروني سـواء على المسـتوى الدولي أو الوطني.

كما اســـتعنا بالمنهج التحليلي المســـاعد على تفكيك الظاهرة المدروســـة إلى متغيراتها الأســاســية، ومن ثم دراســة كل متغير وعلاقته بالمتغيرات الأخرى، وقد تم توظيفه في دراســتنا من خلال تحديد مختلف النصوص القانونية والتشريعات الدولية والوطنية المتعلقة بحماية المؤسسات من الاحتيال الالكتروني، وكذا تحديد الجهات المعنية بتطبيق هذه القوانين ومن ثم تحليل مدى فعالية الآليات والإجراءات المعتمدة في الوقاية والتصدي لجريمة الاحتيال الالكتروني.

صعوبات الدراسة

يعترض الباحث في مختلف مراحل إعداد بحثه صعوبات جمة، خاصة إذا كان الموضوع يتسم بالتعقيد، وعليه فقد واجهتنا جملة من الصعوبات، يمكن ذكرها في ضوء النقاط التالية:

- ✓ ندرة المراجع التي تعالج الاحتيال الالكتروني في علاقته بالمؤسسات وخصائصه مقارنة بالدراسات في مجال الجرائم الالكترونية.
- ✓ تداخل الطابع التقني والقانوني للجريمة، ما تطلب منا جهدا مضاعفا في تحليلها وربط الجانبين معا.
- ✓ صعوبة الوصول إلى معطيات ميدانية واحصائية رسمية تخص الموضوع.

[1] عبد الغفار رشاد القصبي. مناهج البحث في علم السياسة الكتاب الأول التحليل السياسي ومناهج البحث، القاهرة: مكتبة الآداب، 2004، ص.263.

✓ ضيق الوقت المخصص لإعداد هذه المذكرة نظرا لما تتطلبه من تعمق وتحليل لمتغيراتها.

هندسة الدراسة

لدراسة هذا الموضوع ارتأينا وضع خطة من شأنها أن تلم بكل جوانبه، انطوت على فصلين، فضلا عن المقدمة والخاتمة.

يضم الفصل الأول الموسوم **بعنوان الاحتيال الالكتروني: مدخل مفاهيمي** ثلاث مباحث، تطرق المبحث الأول لمفاهيم عامة حول الاحتيال الالكتروني، من خلال التعرض لمفهوم الاحتيال الالكتروني بمفهومه التقليدي والحديث، وكذا خصائص الاحتيال الالكتروني لنعرج بعدها إلى المبحث الثاني الذي عرض أنواع الاحتيال الالكتروني من خلال تقديم مختلف أنواع وأشكال الاحتيال الالكتروني، ليعرض المبحث الثالث آثار الاحتيال الالكتروني على المؤسسات، عبر التطرق لمختلف الآثار والتداعيات التي تترتب على المؤسسات من الاحتيال الالكتروني.

وبالنسبة للفصل الثاني الموسوم ب **آليات حماية المؤسسات من الاحتيال الالكتروني**، فعالج من خلال **المبحث الأول** الاطار القانوني والمؤسساتي الدولي والإقليمي لحماية المؤسسات من الاحتيال الالكتروني، والذي انطوى على الصكوك القانونية والآليات المؤسساتية الدولية والإقليمية المعتمدة للتصدي لجريمة الاحتيال الالكتروني وحماية المؤسسات ، في حين درس المبحث الثاني التشريعات الوطنية لحماية المؤسسات من الاحتيال الالكتروني، والتي انطوت على القوانين العامة والخاصة الوطنية، وكذا الآليات المؤسساتية الوطنية لحماية المؤسسات من الاحتيال الالكتروني. أما المبحث الثالث فجاء بعنوان التحديات التي تواجه تطبيق الإطار القانوني لحماية المؤسسات من الاحتيال القانوني وآليات تفعيلها.

في الخاتمة قدمنا أهم النتائج التي خلصت إليها الدراسة، مع تقديم مجموعة من التوصيات التي يُمكن من خلالها تفعيل وتطوير الأطر القانونية لحماية المؤسسات من الاحتيال الالكتروني على المستوى الدولي والوطني.

الفصل الأول

الاحتيال الالكتروني: مدخل مفاهيمي

المبحث الأول: مفهوم الاحتيال الالكتروني

المبحث الثاني: خصائص الاحتيال الالكتروني

المبحث الثالث: آثار الاحتيال الالكتروني على المؤسسات

الفصل الأول: الإحتيال الإلكتروني: مدخل عام

تعتبر الجرائم الإلكترونية من أخطر التحديات، التي تواجه جميع مجتمعات العالم، على مستوى مؤسسات القطاع العام، والخاص، وحتى الأفراد ، وقد ظهر هذا النوع من الجرائم مع مرور الزمن، وتطور تكنولوجيا الإعلام والإتصال ، وبطبيعة الحال فقد صاحب هذا التطور سلبيات كثيرة، نذكر منها الجرائم المعلوماتية التي تتعدد وسائلها وآلياتها على نحو يتفنن المجرمون في إستخدامها، وهي تلك الجرائم الموجهة ضد نظام الحاسب الآلي، أو الأنظمة المعلوماتية للمؤسسات ، حيث يكون فيها الحاسوب، أو أي جهاز من الأجهزة الإلكترونية وسيلة لإرتكاب الجريمة .

ولا شك أن جريمة الإحتيال الإلكتروني، ما هي إلا إمتداد لجرائم الإحتيال التقليدية، مع إختلاف الوسيلة، فلجريمة الإحتيال الإلكتروني خصوصياتها عن باقي الجرائم الإلكترونية، فهي تتميز بإستنادها على مهارات ذهنية وطرق مبتكرة، ربما لا يستطيع معظم الأفراد وحتى المؤسسات التفطن لها، ولعل أهم مايميزها هو عنصر الخداع، الذي يمارس ضد الضحايا، وهو عنصر لا نجده في جرائم أخرى، كجريمة الإبتزاز الإلكتروني، والتشهير الإلكتروني.

المبحث الأول: مفهوم الإحتيال الإلكتروني

تمتاز جريمة الإحتيال الإلكتروني بوسائلها العديدة، وطرقها التي تتطور يوما بعد يوم، لذلك فقد تنوعت التعاريف بين الباحثين، وإختلفت بين التشريعات من بلد لآخر، لهذا فقد وجب علينا ضبط مفهوم هذه الجريمة.

المطلب الأول: تعريف الإحتيال الإلكتروني

قبل ضبط التعريف، لابد من التطرق إلى تعريف الإحتيال بشكله التقليدي.

الفرع الأول: تعريف الإحتيال

سوف نتناول تعريف الإحتيال لشكله التقليدي من الناحية اللغوية ومن الناحية الإصلاحية

أولا: الإحتيال لغة: الإحتيال في اللغة، مأخوذ من –حيل – وهو من –الحيلة– وتطلق على ما يتوصل به الانسان الى غرضه، من الوسائل والتدابير، وغالبا ما تقترن بالمكر، والخداع، والدهاء وقد ورد أن الحيلة تدل على القوة والتصـــرف، ويقال –لا حيلة له– أي لا قوة ولا تدبير ولا مخرج له وعليه فيفهم الإحتيال لغويا على أنه:" إســتخدام الوســائل الملتوية لتحقيق غرض ما، وقد يكون ذلك بالطرق المشروعة أو غير المشروعة ".[1]

ثانيا : الإحتيال إصطلاحا

هي جرائم الذهن والفكر، بغية الحصول على أموال الغير بطريقة غير مشروعة، وذلك من خلال الخداع، والمكر، والحيلة، والدهاء، بالاضافة إلى إستخدام الكذب وتبديل الحقائق، إذا إستد على الأمر ذلك.[2]

وجريمة الإحتيال هي الاستيلاء غير المشروع على أموال الغير بخداعه، وحمله على تسلي م ذلك المال بإرادته، وهي وسيلة من وسائل التدليس، التي يستعملها الجاني ليقوم المجني عليه بتسليم المال بإرادته.

الإحتيال هو مصطلح قانوني، يضم مجموعة واسعة من السلوكيات التي تتضمن شكلا من أشكال الخداع، أو التحايل، بهدف تحقيق مكاسب شخصية، وغالبا ما ينطوي الإحتيال على حرمان الضحية من المال، أو ممتلكات مادية، ما يجعله شكلا من أشكال جرائم الممتلكات، وقد يرتكب الإحتيال كذلك لتحقيق مكاسب غير مادية، مثل الحصول على معلومات، أو وثائق ذات قيمة، ومن ثمة يعرف الإحتيال من خلال ثلاث طرق رئيسية لإرتكابه: [3]

- الإحتيال عبر التمثيل الزائف؛
- الاحتيال عبر الإخفاق في الكشف عن معلومات؛

[1] إبن منظور ، لسان العرب ، مادة "حيل" ، طبعة جديدة ، مكتبة نور الالكترونية ، ص 1073.

[2] أحسن مبارك طالب، جرائم الاحتيال والعوامل الاجتماعية والنفسية المهيئة لها، كلية القانون، الرياض: جامعة نايف العربية للعلوم الأمنية، 2007 ص 23.

[3] Michael Skidmore, The A Natomy Of Online Fraud, Perspectives On Policing:Paper 10, April 2024 ,P02.

- الإحتيال عبر إساءة إستغلال الموقع الوظيفي.

وقد جرّم المشـرع الجزائري فعل الإحتيال، في المادة (372) من قانون العقوبات، حيت جاء فيه: كل من توصل إلى إستلام أو تلقي أموال ، أو منقولات ، أوسندات ، أو تصرفات ، أو أوراق مالية أو وعود ، أو مخالصـات ، أو إبراء من التزامات ، أو الحصـول على أي منها أو شـرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير، أو بعضها، أو الشروع فيه، إما بإستعمال أسماء أو صـفات كاذبة، أو سـلطة خيالية ، أو إعتماد مالي خيالي، أو بإحداث الأمل في الفوز بأي شـيء، أو في وقوع حادث أو أية واقعة وهمية أخرى، أو الخشـية من وقوع شـيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر، وبغرامة مالية من 500 إلى 20.000 دينار جزائري".[1]

الفرع الثاني: تعريف الإحتيال الإلكتروني

إن تطور تكنولوجيا الإعلام والإتصـال، سـاهم في ظهور نوع جديد من الإحتيال، ألا هو الإحتيال الإلكتروني.

أولا: التعريف الفقهي لجريمة الإحتيال الإلكتروني

يشـير مفهوم الإحتيال الإلكتروني (E-Fraud) إلى جميع أشـكال الخداع التي ترتكب عبر الإنترنت. وقد طرحت عدة تعريفات لهذا المفهوم في أدبيات الجرائم الإلكترونية.

يعرف غراهام الاحتيال الإلكتروني بأنه: "سلوك إحتيالي مرتبط بعمليات الحوسبة، يهدف من خلاله شـخص ما إلى تحقيق منفعة غير مشـروعة" في حين يرى سميث أن الإحتيال الإلكتروني هو:" أي نشاط غير نزيه يتضمن الإنترنت كهدف أو كوسيلة للحصول على مكافأة مالية ".[2]

كما عرّف الإحتيال الإلكتروني على أنه: "إسـتعمال خدمة أو برنامج من برامج الأنترنت، للوصـول إلى ضـحايا محتملين يتم التحايل عليهم بغية سـلبهم أموالهم، أوإجراء معاملات إحتيالية

[1] الجمهورية الجزائرية الديمقراطية الشـعبية، القانون رقم 66-156 المؤرخ في 08 يونيو 1966، المتضـمن قانون العقوبات المعدل والمتمم، المادة 372.

[2] Deaconescu, Ionuț Cosmin, et al, E-Fraud, Studia z nauk technicznych. N° 2, DWSPiT Polkowice, 2013, p03.

وذلك، عن طريق وسائط كالبريد الإلكتروني، أو مواقع الويب، أو غرف الدردشة، أو لوحات الرسائل".[1]

وقد وصفه بعض الفقهاء، على أنه الغش والخداع الذي يستعمله الجاني للحصول، على فائدة من أموال أو بيانات دون أحقيته بذلك، و كذلك حصوله على ميزات غير مشروعة، وصنفه بعض الباحثين كإساءة لإستخدام الحاسب الآلي، من أجل الوصول، أو النقل غير القانوني للأموال، أو الأصول، أو الخدمات، و يكون ذلك ضمن نظام المعالجة الإلكترونية للبيانات، ويتميز عن الإحتيال التقليدي العادي بأنه معقد في صعوبة كشفه، والوصول إلى دلائل تقود للجاني وهذا راجع للشفرات، والمفاتيح، وكذا الطرق المستحدثة التي يستعملها المجرمون في هذه الجريمة لإخفاء هوياتهم."[2]

كما ذهب بعض الفقهاء، إلى "أن الإحتيال المعلوماتي يتحقق إذا كانت نية الجاني تحقيق ربح مادي، غير مشروع، تصحبه خسارة تلحق بالمجني عليه، بإستعمال الحاسوب كوسيلة للجريمة"[3]

ثانيا: تعريف الإحتيال الإلكتروني في مختلف التشريعات

عرفت هيئة الأمم المتحدة الاحتيال الإلكتروني بشكل صريح على أنه:"إدخال البيانات أو محوها أو تعديلها أو كَتبِها، أو برامج الحاسوب، أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة إقتصادية أو فقد حيازة ملكية شخص آخر، بقصد الحصول على كسب إقتصادي غير مشروع له أو لشخص آخر."[4]

وبالنسبة للمشرع الجزائري فلم يعرّف بشكل صريح جريمة الإحتيال الإلكتروني، وذلك لعدم وجود مفهوم دقيق، لما لهذه الجرائم من طرق ووسائل تتطور بشكل مستمر، لكن يمكننا إستنباط

[1] أحمد محمد عبد الرؤوف المنيفي، الإحتيال عبر الانترنت، شبكة الألوكة، ص06.

[2] أحمد عبد اللـه حي بوغانم السليطي، تجريم الاحتيال الإلكتروني في القانون القطري والمقارن، رسالة ماجستير، كلية القانون، جامعة قطر،2018، ص7.

[3] نهلى عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، عمان، دار الثقافة، 2010، ص 188.

[4] نهلى عبد القادر المومني، المرجع نفسه، ص 188.

أن القانون الجزائري يعترف بجريمة الإحتيال الإلكتروني ويعاقب عليها، وذلك من خلال قانون العقوبات لاسيما في نص المواد 394 مكرر إلى 394 مكرر 7، حيث جاء في نص المادة 394 مكرر على سبيل المثال: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. [1]

أما في التشريعات العربية، فقد إختلفت في تسمية هذه الجريمة، حيث سمتها بعض التشريعات بجريمة النصب الإلكتروني، أو الإحتيال المعلوماتي، ولم تعرف معظم التشريعات جريمة هذه الجريمة.

فقد أشار المشرع الإماراتي للإحتيال الإلكتروني في نص المادة (34) من المرسوم بقانون إتحادي رقم (34) لسنة 2021، في شأن مكافحة الشائعات والجرائم الإلكترونية إلى أنه: يعاقب بالحبس مدة لا تقل عن سنة وغرامة لا تقل عن مائتين وخمسين ألف درهم، ولا تزيد عن مليون درهم، أو بإحدى هاتين العقوبتين، كل من إستولى لنفسه، أو لغيره بغير حق على مال منقول أو منفعة، أو على سند، أو توقيع هذا السند، وذلك بالإستعانة بأي طريقة من الطرق الإحتيالية أو بإتخاذ إسم كاذب، أو إنتحال صفة غير صحيحة، عن طريق الشبكة المعلوماتية أو نظام معلوماتي إلكتروني، أو إحدى وسائل تقنية المعلومات .[2]

أما المشرع السعودي، فقد ذكر جريمة الإحتيال الإلكتروني في المادة (04) من نظام مكافحة جرائم المعلوماتية لعام 1428 هـ، التي نصت على أنه: يعاقب بالسجن لمدة لا تزيد على ثلاثة سنوات، وبغرامة لا تزيد عن مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أي من الجرائم الآتية... وقد ذكر في نفس المادة الكثير من أنواع الإحتيال الإلكتروني كالإستيلاء على مال منقول. "[3]

[1] القانون رقم 66-156، مرجع سابق، المواد 394 مكرر-394 مكرر7.

[2] أسماء مبارك الريامي، أحكام الاحتيال الالكتروني، رسالة ماجستير، كلية القانون، جامعة أبو ظبي،2021-2022، ص 16.

[3] أسماء مبارك الريامي، المرجع نفسه، ص16.

كما عرّف المشرع الفرنسي الإحتيال الإلكتروني ضمن المادة 313/1 من قانون العقوبات وقد ذكر أنه :" إستعمال الخداع لإقناع شخص طبيعي، أومعنوي، لتسليم أموال أو أشياء أو تقديم خدمة، أو منح ميزة، وذلك بإستخدام وسيلة إلكترونية أو معلوماتية".[1]

أما وزارة العدل الأمريكية فتعرف الإحتيال الإلكتروني من منظور إستخدام الإنترنت بقولها: "مخطط إحتيالي يستخدم أحد مكونات الإنترنت – مثل غرف الدردشة، البريد الإلكتروني، المنتديات، أو المواقع الإلكترونية – من أجل تقديم عروض إحتيالية للضحايا المحتملين، أو لإجراء معاملات إحتيالية، أو لتحويل عائدات الإحتيال إلى مؤسسات مالية أو إلى أطراف أخرى مرتبطة بالمخطط"[2]

وعرف بدوره المشرع التونسي جريمة الإحتيال الإلكتروني، ضمن قانون مكافحة الجرائم الإلكترونية، عدد5 لسنة 2004 المتعلق بالأنظمة المعلوماتية وإعتبرها :"كل من يستعمل نظام معلوماتي، أو برنامج معلوماتي بقصد التلاعب بالبيانات، والحصول على مكاسب غير مشروعة، لنفسه أو غيره".[3]

كما أشار المشرع المصري لجريمة الإحتيال الإلكتروني، حيث قال أنها: "كل إستيلاء على مال منقول، أو سند، أو توقيع بإستخدام تقنية معلومات، وكان ذلك بالاحتيال، وإنتحال صفة كاذبة، يعاقب بالحبس"حسب المادة (13) من قانون مكافحة جرائم تقنية المعلومات 175 لسنة 2018.[4]

---

[1] Article 313-1 du Code pénal français : "L'escroquerie est le fait, soit par l'usage d'un faux nom…", www.legifrance.gouv.fr consulté le 27 /05/2025، 20:22.

[2] Deaconescu, Ionuţ Cosmin, et al, op-cit,p03.

[3] القانون العدد 05 لسنة 2022 المؤرخ في 2022/09/27، المتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتصال، الرائد الرسمي لجمهورية التونسية، عدد 105، بتاريخ:2023/09/30، المادة 02، ص2346.

[4] القانون رقم 175 لسنة 2008، بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية للقانون المصري، لسنة 2018، المادة 13.

بناءً عما سبق، يمكن تعريف الإحتيال الإلكتروني بأنه:" سيطرة الجاني على أموال أو بيانات شخص آخر، طبيعي أو معنوي، بهدف الحصول على ربح مادي (مال- معلومات- إمتيازات)، بإستخدام الحاسوب، أو أي جهاز إلكتروني ضمن قاعدة بيانات معلوماتية."

أو هو "فعل خداعي يُمارس عمدًا بغرض تحقيق مكاسب غير مشروعة، يتم فيه استخدام شبكة حاسوبية كوسيلة تواصل بين الضحية والمحتال، أو يُنفذ جزء من الأفعال (سواء من قبل الضحية أو المحتال) عبر شبكة حاسوبية"

المطلب الثاني: خصائص الإحتيال الإلكتروني

يتميز الإحتيال الإلكتروني بمجموعة من الخصائص، تفرّده عن باقي جرائم الحاسب الآلي وأيضا على جميع الجرائم الإلكترونية الأخرى، والتي نقوم بتقسيمها إلى فرعين:

الفرع الأول: الخصائص المتعلقة بالجانب التقني

يتميز الإحتيال الإلكتروني بجملة من الخصائص التقنية التي تنبع من طبيعة البيئة الرقمية وهي:

أولا: البيئة الإلكترونية

يستلزم لقيام هذه الجريمة التعامل مع بيئة إلكترونية تتمثل في وسيلة الإرتكاب التي تكون جهازا إلكترونيا كالحاسب الآلي عادة، وكذا التعامل مع كم من البيانات قصد تصحيحها أو تعديلها والتلاعب بها، من أجل خداع المجني عليه، ولابد أن يكون الجاني ملما، ومتمكنا في المجال الإلكتروني.[1]

فهذه الجريمة تقع كثيرا عبر منصات التواصل الإجتماعي المعروفة كالفايسبوك، والأنستقرام التي وفرت بيئة خصبة لهؤلاء المجرمين، للقيام بأفعالهم الإحتيالية، بعيدا عن أي رقابة تحول بينهم، وبين تحقيق رغباتهم، فقد شهد الإحتيال عبر مواقع التواصل الإجتماعي، إنتشارا واسعا، حيث يقدم

[1] سعد فهد سعد ادبيس المطيري، مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية، العدد 05، 2023، ص 1258.

المجرم على هذه الجريمة، لمعرفه السابقة بأنه محمي من الرقابة، ويرجع ذلك لتواجده في بيئة إلكترونية بعيدة عن مسرح الجريمة."[1]

ثانيا: سرعة التنفيذ

تتسم جريمة الإحتيال الإلكتروني بسرعة تنفيذها، حيث يستخدم الجاني مهاراته، وقدراته في الجانب التقني، ليوقع بالضحية في وقت وجيز، فالضحية، لا يلاحظ الجريمة رغم أنها قد تقع في وقت وجوده على الشبكة، وربما على مرأى عينيه، هذا الذي جعلها جريمة مخفية ومستترة.[2]

تزداد سرعة تنفيذ هذه الجريمة، نتيجة إستعمال أدوات تقنية متطورة كالبرمجيات، الصفحات المزيفة، و كذا إيهام الضحية بتحقيق هدفها من مال، أو صلاحيات، هذا الذي يتيح للجاني الإحتيال في وقت وجيز جدا، وذلك خلال دقائق معدودة، أو حتى ثوان، خصوصا عند إستهدافه لأنظمة ضعيفة الحماية، دون الحاجة إلى التنقل، أو المواجهة المباشرة مع الضحية.

و لا تقتصر السرعة، على سرعة التنفيذ فقط، بل يشمل أيضا سرعة التخلص من الأدلة الرقمية التي تشير إليه، فقبل قيام المحتال بجريمة يقوم بكل الخطوات اللازمة لإخفاء هويته الحقيقية إما بتزييفها، وإنتحال شخصية وهمية، أو حتى حقيقية، أو التخفي وراء شخصية مجهولة، و بعد إنتهائه، من القيام بجريمته، يقوم بإخفاء أي دليل يدينه، وذلك بشكل سريع يجعل من الصعب إكشافه في الوقت المناسب بسبب أن المحتال يستطيع التنقل بين عدة شبكات في لحظات، ويعتبر عنصر الوقت أيضا عاملا حاسما في نجاح الجريمة، التي ترتكب في عديد المرات خلال ثوان فقط بمجرد تفاعل الضحية مع المحتوى الإحتيالي، وقد يستعمل الجاني أدوات الشفير أو يلجأ الى أدوات إخفاء الهوية،كمنصات الدارك ويب (DARK WEB)، ذلك الذي يحول دون تدخل الجهات المختصة في الوقت المناسب.

---

[1] محمد الأمين بن خيرة، أسباب ودوافع إنتشار السلوكات الإجرامية عبر الفايسبوك بين الشباب الجزائري، مداخلة مقدمة للملتقى الوطني حول الجرائم الإلكترونية في المجتمع الجزائري تشخيص الواقع و تحديات الأمن السيبراني، 2022/03/15، ص 427،428.

[2] وائل محمد نصيرات،غادة عبد الرحمن الطريف، جريمة الاحتيال عبر شبكة المعلومات الدولية، مجلة دفاتر السياسة والقانون،العدد19، 2018، ص 98.

ثالثا: التنفيذ عن بعد

تتم جريمة الإحتيال الإلكتروني على الأشـــخاص، والمؤســـســـات عن بعد، حيث لا يتواجد الجاني في مكان إرتكابها ، بل يستطيع القيام بالجريمة وهو بعيد عن المكان الذي تحققت فيه نتيجة الجريمة، ســـواءا كان ذلك عبر الدخول لمنصـــات إلكترونية، أو إعتراض عمليات تحويل مالية أو الإستلاء على معلومات بطاقات الدفع إئتمانية .[1]

فجريمة الإحتيال الإلكتروني تتم عبر شبكة الأنترنت، أثناء عملية معالجة البيانات، وإستخدام أليات الحاسـوب، ويعتبر شـرطا أسـاسـيا لقيام الجريمة، وقد أدى هذا الإرتباط الوثيق بين شـبكة الأنترنت، والحاســـوب إلى جعلها ترتكب دون الحاجة إلى التواجد الفعلي قرب الضـــحية ماديا فالإحتيال الإلكتروني يختلف عن الإحتيال التقليدي، في كونه لا يتطلب إتصـــالا مباشـــرا بين الأطراف، بل يمكن أن يتم من دولة إلى أخرى في غضـــون لحظات، وهي خاصـــية فرضـــتها البيئة الإلكترونية لهذا السلوك الإجرامي.[2]

الفرع الثاني: الخصائص المتعلقة بالجانب الإجرامي

إضـــافة إلى الخصـــائص التقنية هناك خصـــائص أخرى إجرامية، معقدة تضـــفي عليه طابعا خاصا ضمن الجرائم الحديثة نذكر منها:

أولا: صعوبة الإثبات

يصعب إثبات جريمة الإحتيال الإلكتروني، ومعرفة هوية الجاني، وكذا إيجاد أي دليل يقود إلى معرفة الفاعل لدى سلطات الأمن، وأجهزة التحقيق، والملاحقة، وحتى بالنسبة إلى آليات المكافحة ضمن المؤسسات العمومية والخاصة، ولكون هذه البيئة الإلكترونية مجموعة من البينات، والمعلومات الإلكترونية غير المرئية، فقد بات من الســـهل طمس الأدلة، والقيام بمحوها كليا، كأنها لم تكن

[1] عبد السـلام محمد المايل، عادل محمد الشـريجي، علي قابوسـة، الجريمة الإلكترونية في الفضـاء الإلكتروني، مجلة آفاق، العدد 04، 2019، ص 251.

[2] عبد الله دغش العجمي، المشـكلات العملية والقانونية للجرائم الإلكترونية–دراسـة مقارنة– رسـالة ماجسـتير في القانون العام، جامعة الشـرق الأوسط ، 2014، ص ص 20،24.

موجودة مطلقا، إذ يتم ذلك في بضغطة زر واحدة، على لوحة المفاتيح في جهاز الحاسوب، هذا ما صعب عملية إثبات الجريمة على الجاني، فعلى إعتبار أن هذه الجريمة تتم في شكل أوامر تصدر للحاسوب، فما إن ينتهي المحتال من جريمته حتى يبادر بمحو كل ماسبق من أدلة.

وبذلك تكمن صعوبة الإثبات في هذه الجريمة، أنها لاتترك أثار مادية على مكان إرتكابها والتي هي مجموعة من النبضات الإلكترونية وقواعد بيانات، أو منصات تواصل، وتشير الدراسات في هذا السياق، أن ما يتم إكتشافه من جرائم النصب، والإحتيال، هو بعض الحالات فقط من بين آلاف المحاولات، التي تحدث يوميا وفي كل وقت، وأيضا ما يتم الإبلاغ عنه، هو نسبة 5% فقط من إجمالي الحالات التي تكتشف، وهذه مشكلة أخرى، نضيفها إلى التحديات التي تشكل عائقا دون إثبات هذه الجريمة.[1]

ثانيا: عنصر الخداع

يعد الخداع أحد الخصائص الرئيسية لجريمة الاحتيال الإلكتروني، وهو الوسيلة الرئيسية التي يستخدمها الجاني لتنفيذ مخططه، دون الحاجة إلى إستعمال العنف أو القوة المادية، وتتميز هذه الجريمة بكون مرتكبيها من ذوي الذكاء الحاد، والدهاء إذ يعتمدون على مهارات عقلية، وتقنية متقدمة، لتضليل الضحية وإستغلال ثغرات النظام الإلكتروني.[2]

فالجاني في الإحتيال الإلكتروني غالبا ما يكون شخصا يمتلك قدرة عالية على تحليل الأنظمة الرقمية، وفهم تفاصيلها و محتوياتها، وكذا إكتشاف نقاط ضعفها، مما يتيح له التسلل من خلالها كما يكون قادرا على صياغة رسائل أو عروض إلكترونية مزيفة، تحاكي الواقع بدرجة عالية من الدقة، حيث يدفع ضحيته إلى إتخاذ قرارات غير مدروسة، كإفشاء بياناته الشخصية أو البنكية أو تحويل أموال لحساب الجاني، بحيث يخاطب الضحية بأسلوب يلامس إحتياجاتها أو يثير فضولها، مستغلا في ذلك قلة الوعي الرقمي لدى بعض الأشخاص.[3]

[1] عبد الله دغيش العجمي، مرجع سابق، ص 21.

[2] محمد هشام صالح عبد الفتاح، مرجع سابق، ص 11.

[3] محمد هشام صالح عبد الفتاح، المرجع نفسه، ص 12.

ثالثا: جريمة عابرة للحدود

يتميز الإحتيال الإلكتروني بالطابع الدولي، أي أنه عابر للحدود ، حيث يتجاوز الحدود الجغرافية للدولة الواحدة، فهذه الجريمة تتم عبر الشـــبكة الإلكترونية، ومواقع الويب التي لاتعترف بالحدود الجغرافية وهو مايثير بشكل كبير تحديات قانونية، وصعوبات سياسية في سبيل مواجهتها خاصـــة فيما يتعلق بإجراءات الملاحقة الجنائية، وكذا الإختلاف الحاصـــل بين الأنظمة القانونية للدول، وتباين درجات التعاون القضـائي والأمني الدولي، كما تنشـأ صـعوبات عند مرتكب الجريمة من دولة لاتربطها أي إتفاقيات دولية للتعاون القضائي، وتسليم المجرمين أوحتى لاتقوم بتجريم بعض السلوكيات الإلكترونية. [1]

سـاهم التطور المتسـارع للتكنولوجيا، في إلغاء الحدود الجغرافية للدول في المجال المعلوماتي، مما أتاح إرتكاب الجرائم الإحتيالية في دولة معينة، بينما تمتد أثارها إلى دول أخرى، وقد تشـــمل أضـرارها المحتملة عدة بلدان في آن واحد، إن هذه الطبيعة العالمية للجريمة، تمكن الفاعل من القيام بفعله بعيدا عن موقع الضـرر، مما يخلق صـعوبات كبيرة أمام رجال القانون، والسـلطات في تحديد الإختصـاص الإقليمي، وتثير إشـكالات تتعلق بالتعاون الدولي، تبادل المعلومات وتسـليم المجرمين وعليه فإن جريمة الإحتيال الإلكتروني تعد شـــكلا من أشـــكال الجريمة العابرة للحدود الوطنية والإقليمية، الأمر الذي يســـتوجب مراجعة الإطار القانوني التقليدي، والعمل على تطوير آليات قانونية دولية، قادرة على مواكبة هذا النوع من الإحتيال.[2]

رابعا: تحقيق الربح

يعد الدافع المادي، أحد الأســباب التي تحفز الجاني على إرتكاب جريمة الإحتيال الإلكتروني حيث شـكل الربح السـريع حافزا قويا يجعله يسـعى لتطوير قدراته، ومهاراته التقنية بشـكل مسـتمر حتى يواكب كل جديد في عالم التكنولوجيات المعلوماتية، فالمحتال هنا أصبح يدرك أن تحقيق أرباح

[1] إسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث، العدد 11، سبتمبر 2018، ص 335.

[2] شوقي يعيش تمام، الجريمة المعلوماتية، محاضرات موجهة لطلبة السنة الثانية ماستر قانون الاعلام الآلي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، جانفي 2019، ص28.

ضخمة بات أمرا ممكنا، من خلال الإحتيال على المؤسسات، والأفراد، بأقل جهد ممكن، ودون ترك أي أثر، ومن جهة أخرى فتطوير المؤسسات للمواقع الإلكترونية، وأساليب الدفع الإلكتروني وحتى إستعمال الأفراد، ووسائل التواصل الإجتماعي، جعل من الشبكة المعلوماتية أرضا خصبة للمحتالين، لإكتشاف ثغرات جديدة يستغلوها لتحقيق مصالحهم الخاصة سواء كانت مالا، أو معلومات شخصية تقودهم إلى أرباح مادية[1]

يقوم الجاني بالتلاعب بقيم مالية تمثلها بيانات داخل نظام إلكتروني، سواء تعلق الأمر بمعالجة المعلومات، أو تخزينها، أو نقلها، وتستغل هذه البيانات في أهداف مالية غير مشروعة كما هو الحال في الإحتيال المتعلق بكشوف الرواتب، مستحقات مالية، والحسابات البنكية، أو عبر فواتير عمل وهمية أو مزورة، ويأدي هذا الإحتيال إلى مكاسب مالية مباشرة، غلبا ماتكون كبيرة لتعدد ضحايا الجاني، ويبرز هذا الإحتيال بشكل خاص في المعاملات البنكية، خاصة في إطار مايعرف بنظام "المجتمع غير النقدي "، حيث أصبحت معضم علميات الدفع تعتمد على التحويلات البنكية الإلكترونية، سواءا كانت في القطاعات التجارية، أوضمن العلاقات المالية بين الأفراد، ويتم ذلك غالبا من خلال "أوامر تحويل الأموال"، التي باتت بمثابة الوسيلة الأساسية لتحريك الأموال.[2]

المبحث الثاني: أنواع الإحتيال الإلكتروني

يعتبر الإحتيال الإلكتروني من الجرائم المستحدثة التي فرضها التحول الرقمي، وتوسع إستخدام الوسائط التكنولوجية في مختلف مجالات الحياة، لا سيما في ميدان المال والأعمال، وقد ساهمت سهولة الوصول إلى الشبكة العنكبوتية، وتطور وسائل الإتصال الحديثة في تنوع صور هذا الإحتيال، سواء من حيث الأساليب المستعملة أو الأهداف المنشودة، إذ لم يعد الأمر مقتصرا على الإستيلاء غير المشروع على الأموال، بل تعداه إلى المساس بالبيانات الرقمية الحساسة للأفراد والمؤسسات على حد سواء، وعليه، سيتم في هذا المبحث تصنيف أبرز أنواع الإحتيال الإلكتروني

[1] طارق قادري، الجريمة الالكترونية وحجية الدليل الرقمي والاثبات الجنائي، المركز المغاربي –شرق أدنى للدراسات الاستراتجية، جانفي 2024، ص 74،75.

[2] طارق قادري، المرجع نفسه، ص 66.

من خلال مطلبين رئيسيين، يتناول أولهما الإحتيال الذي يستهدف الأموال، بينما يركز الثاني على الاحتيال الموجه نحو البيانات.

المطلب الأول: الإحتيال الإلكتروني الذي يستهدف الأموال

يعد الإحتيال الإلكتروني الذي يستهدف الأموال من أكثر الجرائم الرقمية تعقيدا وتأثيرا على الأفراد والمؤسسات، حيث يمارس عبر وسائل متعددة تتنوع وفقا للأساليب التقنية المستخدمة ومن بين هذه الأساليب نذكر:

الفرع الأول: الإحتيال عبر وسائل الدفع الإلكترونية

شهدت المعاملات التجارية تحولا جذريا في ظل التطورات الكبيرة التي صاحبت ظهور شبكة الإنترنت، حيث أصبحت تتم معظمها عبر هذه الشبكة، خاصة ما تعلق بعمليات البيع والشراء مما أدى إلى تطور وسائل الدفع والوفاء، لتصبح جزءا لا يتجزأ من هذه المعاملات، غير أن هذا التطور صاحبه بروز ظاهرة الإحتيال الإلكتروني، إذ إستغل بعض المجرمين هذا الفضاء الرقمي لإرتكاب أفعال غير مشروعة تمس الجانب المالي، من خلال أساليب متعددة كقرصنة أرقام البطاقات البنكية، والتحويل غير المشروع للأموال، إلى جانب أنشطة أخرى كغسل الأموال والسطو على أموال البنوك، مما جعل هذه المعاملات عرضة دائمة لمخاطر الإحتيال الإلكتروني.[1]

وقد أشار موقع الإنتربول إلى تعدد أنماط الإحتيال الإلكتروني، المرتبطة ببطاقات الدفع ونظم الدفع الإلكتروني، والتي إستفادت من إنتشار المعاملات المالية عبر الإنترنت، مما أتاح فرصا جديدة للمجرمين، وتشمل هذه الجرائم إعتداءات مباشرة على أجهزة الصراف الآلي، عبر هجمات تقنية متطورة مثل هجوم "الصندوق الأسود"، حيث يتم إرسال أوامر غير مصرح بها إلى الجهاز، كما يمارس الإحتيال سواء بوجود بطاقة الدفع أو دونها، من خلال سرقة بياناتها عبر وسائل متعددة كالتصوير أو التصيد، ما يؤدي إلى إستنساخ بطاقات مزورة أو إستعمالها في عمليات شراء

[1] إسمهان بوضياف، مرجع سابق، ص 385.

إحتيالية، وغالبا ما تباع البيانات المصرفية المسروقة عبر الشبكة المظلمة(Darknet) ، ويتم إستغلالها في بلدان أخرى، مما يصعب تتبع مصدرها ويعقد من جهود المكافحة.[1]

الفرع الثاني: التصيد الإحتيالي

ينفذ الإحتيال الإلكتروني بأساليب متنوعة، من بينها إنتحال الصفة، حيث ينشئ الجناة مواقع مزيفة تشبه مواقع الشركات التجارية الكبرى، ويستقبلون من خلالها المعاملات والخدمات التي يقدمها الموقع الأصلي، مما يتيح لهم الوصول إلى رسائل البريد الإلكتروني، وسرقة بيانات بطاقات الإئتمان، والدفع الإلكتروني.[2]

يمثل في ذلك التصيد الإحتيالي أخطر أنواع الإحتيال الإلكتروني، حيث يتم فيه خداع الشخص ليعطي بياناته المالية الشخصية (مثل أرقام بطاقات الإئتمان، أرقام الحسابات، رموزPIN كلمات المرور، وغيرها) للمحتال الذي يقوم بإقناع الضحية بتسليم هذه البيانات عبر رسائل بريد إلكتروني مزورة ومواقع إلكترونية مزيفة تستخدم علامات تجارية موثوقة.[3]

أما أسلوب التجسس فيعتمد على إستخدام برامج إختراق لأنظمة المعلومات الخاصة بالشركات، مما يمكن الجاني من الحصول على بيانات البطاقات الصحيحة، وإستعمالها عبر الإنترنت، في حين يتمثل أسلوب الشفط، في تركيب جهاز يسمى "Skimmer" على الصراف الآلي، لمسح بيانات البطاقة ضوئيا وتخزينها، مما يتيح إنشاء نسخة مطابقة للبطاقة الأصلية وإستخدامها في المعاملات الإلكترونية.[4]

الفرع الثالث: الإحتيال عبر المواقع والتطبيقات المزيفة

يستغل المحتالون في هذا النوع الوسائل الرقمية للإيقاع بضحاياهم، ومن أبرز هذه الأساليب الإحتيال عبر البريد الإلكتروني، حيث يتضمن إرسال رسائل غير مرغوب فيها (Spam)

---

[1] Interpol, Social engineering scams, Available at the link: https://www.interpol.int/en/Crimes/Financial-crime/Social-engineering-scams, accessed on27/05/2025, at08:10.

[2] مريم عبد الكافي، صورية بوربابة، جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الالكترونية، مجلة القانون والعلوم السياسية، العدد01، 2022، ص415.

[3] Deaconescu, Ionuț Cosmin, Et Al, op-cit,P05

[4] مريم عبد الكافي، صورية بوربابة، مرجع سابق، ص 415.

تُستخدم أحيانا للتنكر كجهات مالية رسمية، وهي ممارسة قد تتطلب فرض تكاليف إضافية على المرسلين كوسيلة ردع فعّالة، أو القيام بإعادة توجيه الضحايا من مواقع شرعية إلى أخرى مزيفة لجمع البيانات الشخصية، كما قد يلجأ المحتال إلى أسلوب إحتيال الرسوم المسبقة الذي يقوم على خداع الضحايا بإيهامهم بأنهم سيحصلون على مكاسب مالية كبيرة مقابل دفع رسوم بسيطة مسبقة. وتشمل هذه الممارسات: إحتيال اليانصيب، الإرث الوهمي، التبرعات الكاذبة والمخططات الهرمية.[1]

كما قد يدير المحتال موقعا إلكترونيا يقدم سلعا بأسعار مخفضة للغاية ويشحن السلع قبل إستلام الدفع، حيث يجب على العملاء تقديم أسمائهم وأرقام بطاقاتهم الإئتمانية عند الشراء. عندما يقدم العميل طلبا، يقوم المحتال بطلب نفس المنتج (بإسم العميل) من موقع قانوني آخر بإستخدام بيانات بطاقة الإئتمان المسروقة. بعد فترة تُستخدم بيانات بطاقة الإئتمان الخاصة بالعميل لشراء سلع.[2]

المطلب الثاني: الإحتيال الإلكتروني الذي يستهدف البيانات

يشكل الإحتيال الإلكتروني الذي يستهدف البيانات تهديدا بالغ الأهمية، لا يقل في خطورته عن الإحتيال المالي، إذ يتعرض كل من المستخدمين والمؤسسات لخطر إنتهاك خصوصيتهم وسرقة معلوماتهم الحساسة، علاوة على ذلك، قد يلجأ المجرمون إلى التلاعب أو إتلاف البيانات المخزنة وهذا ما سنتطرق إليه في هذا المطلب.

الفرع الأول: بيانات المستخدمين

تعد بيانات المستفيدين الحساسة، هدفا رئيسيا لمجرمي الإنترنت، حيث يسعون إلى الحصول عليها، من خلال هجمات التصيد الإحتيالي أو الهندسة الإجتماعية التي تم التطرق لها سابقا وذلك عن طريق إنتحال صفة مؤسسات رسمية، أو أفراد موثوقين، تشمل هذه البيانات معلومات

[1] Shewangu Dzomira, Electronic Fraud (Cyber Fraud) Risk In The Banking Industry, Zimbabwe, Risk Governance & Control: Financial Markets & Institutions, Vol 4, Issue 2, 2014, P17.
[2] Deaconescu, Ionuț Cosmin, et al, op-cit,p05

تسجيل الدخول، التفاصيل المالية، وأرقام بطاقات الهوية، بمجرد الحصول على هذه المعلومات يمكن إستخدامها لإنشاء هويات مزيفة، أو حسابات إحتيالية تستغل، في تنفيذ عمليات نصب وإحتيال رقمي، كما يمكن دمج هذه البيانات، مع معلومات مسروقة أخرى، لتجاوز الإجراءات الأمنية، مما يعرض الأفراد لمخاطر كبيرة، قد تطال حساباتهم المصرفية، وسمعتهم الرقمية.[1]

ومن التقنيات الإحتيالية أيضا "هجوم السلامي"، حيث تُبرمج أنظمة إلكترونية لسرقة مبالغ صغيرة من حسابات متعددة، يصعب إكتشافها نظرًا لصغر حجمها، فضلا عن إستخدام الفيروسات والديدان وأحصنة طروادة لنشر البرامج الخبيثة والتحكم في أنظمة الضحايا. وتُمكّن هذه البرمجيات المجرمين من الوصول إلى بيانات المستخدم أو تخريب الأنظمة. وقد عرفت فترة الركود المالي العالمي تنامي جريمة غسيل الأموال السيبراني، حيث تُحوَّل الأموال إلكترونيا دون المرور بإجراءات تحقق صارمة، مما يُغري المجرمين بإستخدام الفضاء السيبراني كقناة تبييض للأموال. [2]

الفرع الثاني: بيانات المؤسسات

تمثل بيانات المؤسسات، هدفا ثمينا للمجرمين الإلكترونيين، حيث يسعون لإختراق أنظمة الشركات، والوصول إلى قواعد بياناتها، بهدف سرقة معلومات مالية، تجارية، أو بيانات، قد يتم ذلك عن طريق إستغلال الثغرات الأمنية، أو شن هجمات موجهة كالهندسة الإجتماعية ضد الموظفين حيث تستخدم هذه البيانات لاحقا في إرتكاب جرائم إحتيال مالي، أو بيعها في السوق السوداء الرقمية، أو حتى تنفيذ هجمات تخريبية تمس إستقرار المؤسسة، إن إختراق بيانات المؤسسات لا يؤثر فقط على سمعتها، بل قد يؤدي أيضا إلى خسائر مالية جسيمة وتعطيل نشاطها التجاري.[3]

فضلا عن الإبتزاز الإلكتروني الذي يستند إلى تهديد يُوجه لشركة، حيث يُطلب من الشركة دفع مبلغ مالي للمحتال، وإلا سيقوم المحتال بشن هجوم رفض خدمة (Denial of Service) على موقع الشركة الإلكتروني.[4]

---

[1] هيئة الحكومة الرقمية، الاحتيال الرقمي، دراسة بحثية، الإصدار 1.0، أوت 2023، ص ص 10-11.

[2] Shewangu Dzomira, op-cit, P17.

[3] هيئة الحكومة الرقمية، المرجع نفسه، ص 10.

[4] Deaconescu, Ionuț Cosmin, et al, op-cit,p05

الفرع الثالث: الإضرار بالبيانات المخزنة

تعد جرائم الإضـــرار بالبيانات، من أخطر أنواع الإحتيال الإلكتروني لما تســـببه من خســـائر جســـيمة للأفراد والمؤســـســـات، وتتمثل في حذف، أو تعديل، أو ســـرقة، أو إتلاف، أو تعطيل البيانات المخزنة رقميا على الحواسيب، سواء المتصلة أو غير المتصلة بالشبكات، وتشمل أيضا محاولات الدخول غير المشروع دون إحداث ضرر فعلي، ويعرف مرتكبو هذا النوع بـ"ذوي القبعات البيضاء"، الذين يستغلون الثغرات بغرض الإختبار أو التبليغ، أما الإضرار الفعلي كالمحو، أو السرقة أو التعطيل، فيقوم به "ذوو القبعات الســـوداء" بدافع مادي أو معنوي، كالإضـــرار بشـــخص أو مؤسسة، أو بهدف المنافسة، وتحدث هذه الجرائم رغم وجود أنظمة الحماية مثل الجدران النارية وأنظمة كشـــف ومنع الإختراق، وكلمات الســـر، مما يعكس تطور أســـاليب الإحتيال وصـــعوبة مكافحتها.[1]

يتضـــح من خلال دراســـة أنواع الإحتيال الإلكتروني، أن هذا النمط الإجرامي، يتخذ صـــورا متعددة تختلف بإختلاف الأهداف، ما بين المساس بالأموال، أو التعدي على البيانات، فقد بينت الأمثلة المعروضـــة أن الأســـاليب الإحتيالية، التي تســـتهدف الأموال تتنوع بين التصـــيد الإلكتروني بمختلف أشكاله، والإحتيال عبر الهاتف، وإنتحال الصفة، والتجسس التقني، إضافة إلى الهجمات الموجهة نحو نظم الدفع، وبطاقات الإئتمان، بما في ذلك تقنيات "الشـــفط" وإســـتنســـاخ البطاقات وهي أساليب تعكس توجه المجرمين نحو الإستيلاء المباشر على موارد مالية، بإستخدام أدوات رقمية يصـــعب تتبعها أو إثباتها، في المقابل، نجد أن الإحتيال الموجه نحو البيانات يكتســـي طابعا أكثر تعقيدا، إذ يســـتهدف الجناة الوصـــول إلى معلومات حســـاســـة، ســـواء تعلق الأمر ببيانات الأفراد أو المؤســـســـات، وتشـــمل هذه الإعتداءات، ســـرقة معلومات تســـجيل الدخول، التفاصـــيل البنكية أو المعطيات التجارية والتقنية للمؤســـســـات، بهدف إســـتغلالها لاحقا في عمليات نصـــب، أو بيعها في الأسواق السوداء الإلكترونية، وقد أظهرت الدراسة أن بعض الأفعال، تدخل في نطاق الإضرار

[1] نوال شايل، الجريمة الالكترونية في التشريع الجزائري، مجلة سيسيولوجيا، العدد02،2022، ص 65.

بالبيانات، مثل حذف، أو التعديل، أو التعطيل المتعمد، وهو ما يصنف ضمن أشد صور الإحتيال ضررا، لا سيما عندما تنفذ ضد مؤسسات حيوية.

المبحث الثالث: آثار الإحتيال الإلكتروني على المؤسسات

تعد المؤسسات سواء كانت مصرفية تجارية، أو إدارية من أبرز الضحايا المحتملين للإحتيال الإلكتروني، إذ تمتد آثاره لتشمل أبعادا مالية، وإقتصادية، وتنظيمية، نظرا لإرتباطه الوثيق بالأنظمة المعلوماتية التي تستخدم في إدارة المعاملات المالية، وتخزين البيانات، ويتم تناول هذه الآثار في مطلبين.

المطلب الأول: الآثار المالية للإحتيال الإلكتروني على المؤسسات

يخلف الإحتيال الإلكتروني آثارا مالية جسيمة على المؤسسات، من خلال الخسائر المباشرة الناتجة عن سرقة الأموال، إضافة إلى التكاليف التي تنفقها من أجل تعزيز أمنها السيبراني و هذا ما سنتناوله في هذا المطلب

الفرع الأول: الخسائر المالية

أصبح الإحتيال الإلكتروني يشكل تهديدا متزايدا على الإقتصاد العالمي، و المؤسسات العمومية والتجارية، حيث خلّف خسائر مالية باهضة، في مختلف القطاعات، حيث أفادت شركة cyber security ventures، المختصة في أبحاث الأمن السيبيراني، عن بلوغ هذه الخسائر 6 تريليونات دولار، خلال سنة 2024، و هو ضعف الرقم المسجل سنة 2015، والذي كان في حدود 3 تريليونات دولار فقط، ورجحت أن ترتفع هذه الخسائر بشكل متسارع بمعدل 15% سنويا خلال السنوات الخمس القادمة، وبحسب هذه التقديرات فإن الخسائر العالمية الناجمة عن الهجمات الإحتيالية ستصل إلى نحو10,50 تريليونات دولار سنويا خلال العام 2025، و هو رقم يعكس حجم الضرر الهائل الذي تسببه مثل هذه الجرائم بالنسبة للمؤسسات المالية، والتجارية.[1]

[1] بلال عقل الصنديد، الاحتيال الإلكتروني وتحدياته المستمرة، 2024-12-08، متوفر على الرابط:

كبّدت الولايات المتحدة الأمريكية سنة 2003 خسائر تجاوزت 70مليون دولار، نتيجة هجمات تعطيل نظم المعلومات، المعروفة بهجمات "الحرمان من الخدمة" (Denial of Service Attack)، والتي تعتمد على إغراق الخوادم بطلبات وهمية تفوق قدرة المكونات المادية والبرمجية على المعالجة، مما يؤدي إلى شلل تام في النظام المعلوماتي، وتعرض موقع "ياهو" في سنة 2000 لهجوم مشابه تسبب في تعطيله لمدة ثلاث ساعات، إلى أن تمكن المهندسون من تحديد مصدر الهجوم واستعمال "فلاتر" على أجهزة التوجيه (Routers) لحجب مناطق الإتصال وتعطيلها، وتعد هذه الهجمات مثالا واضحا على الإحتيال الإلكتروني، الذي يستهدف المؤسسات ويسبب خسائر مالية وتقنية جسيمة.[1]

كما تعرضت النمسا لعمليات الإحتيال الإلكتروني، المعتمد على التصيد(Phishing) حيث نجح مجرمون سيبيرانيون في تنفيذ هجمات دقيقة إستهدفت الضحايا عبر الانترنت حيث قاموا بخداعهم لتحميل برامج خبيثة مموهة، تمكنهم من التحكم الكامل عن بعد في أجهزتهم، هذه البرمجيات المعروفة بأدوات الوصول عن بعد (Remote Access Tool) ، مكنتهم من التسلل إلى معلومات حساسة، وشخصية، إستخدمت فيما بعد لفتح حسابات جديدة، لدى مزودي خدمات الأصول الإفتراضية (VASP) مثل محافظ العملات المشفرة، حيث تم تسجيل الحسابات بأسماء الضحايا الحقيقيين دون علمهم أو إذنهم.[2]

وفي كثير من الحلات قاموا بتوجيه الضحايا مباشرة أثناء عملية التسجيل إلى مواقع زائفة، تحاكي واجهات المواقع الرسمية، ما مكنهم من تخطي مراحل التحقيق الأمني بسهولة هذا الخداع المتقن سمح للمجرمين بإخفاء أنشطهم الحقيقة، وجعل عمليات التسجيل تبدو وكأنها نفذت من قبل الضحايا أنفسهم، بعد إنشاء هذه الحسابات، أستخدمت كقنوات تمرير

//www.google.com/amp/s/www.aljarida.com/article/83723/amp:https أطلع عليه يوم 10 ماي 2025 الساعة 11:00.

[1] نوال شايل، مرجع سابق، ص 65.

[2] مجموعة العمل المالي الأنتربول، مجموعة إنكونت، تدفقات المالية غير المشروعة الناجمة عن الاحتيال الذي سهل الانترنات ارتكابها، نوفمبر 2023، ص 23.

لغسل الأموال العائدة من جرائم إلكترونية أخرى، فبفضل الواجهة الإفتراضية لهذه الخدمات صار تتبع حركة الأموال أصعب على السلطات، ونشير إلى أن القيمة الإجمالية للأموال التي تم الإحتيال عليها خلال هذه السلسلة تجاوزت 600.000 ألف أورو، وهو رقم يعكس مدى الإحترافية والتنظيم الذي تتسم به هذه الشبكات الإجرامية، خاصة مع إستغلالها لفجوات الحماية الرقمية في المنصات المالية عبر الأنترنت.[1]

من المثال السابق، نجد أن الاحتيال الإلكتروني على المؤسسات، لا يعتمد فقط على الإحتيال التقني المباشر، بل يوظف أيضا أدوات الوصول عن بعد، ما يجعل الأمر أكثر صعوبة على المؤسسات، وهو ما يرجع بخسائر فادحة في الجانب المالي.

الفرع الثاني: تكاليف حماية الأنظمة ومكافحة الإحتيال

يشكل الإحتيال الإلكتروني تحد كبير تواجهه المؤسسات، نظرا لما يترتب عنه من أعباء مالية جسيمة تتكبدها هذه الأخيرة، سواءً في إطار الوقاية، أو عند وقوع الهجوم الإلكتروني، وتشير الإحصائيات إلى أن ما يقارب 26% من الشركات الكبيرة، تجد نفسها مضطرة لدفع فدية مقابل إسترجاع بياناتها التي تم الإستلاء عليها من طرف الجناة، حيث يبلغ متوسط الفدية المدفوعة في هذه الحالات بحوالي 404.170 دولار أمريكي، وهو ما يعكس بشكل واضح الأثر المالي الباهظ الذي يسببه الإحتيال الإلكتروني على المؤسسات، لاسيما عند غياب تدابير الحماية الكافية، مما يفرض عليها تخصيص ميزانيات معتبرة لتعزيز نظم الأمن السيبراني، و تفادي أي خسائر محتملة.[2]

ووفقا لما ورد في تقرير The Hidden Costs OF Cyber crime فإن الوقت الذي تستغرقه المؤسسات في المتوسط، للإنتقال من مرحلة إكتشاف الإحتيال إلى معالجته، يبلغ حوال 19 ساعة، و رغم أن العديد من الحوادث الأمنية، يمكن التعامل معها داخليا، من قبل

[1] مجموعة العمل المالي الأنتربول، المرجع نفسه، ص 23.

[2] أبوبكر أحمد همام عبد المجيد، الأثار الإقتصادية للجرائم المعلوماتية وسبل مكافحتها، مجلة جامعة جنوب الوادي الدولية للدراسات القانونية، العدد 06، 2021، ص360.

الفرق التقنية التابعة للمؤسسة، إلا أن الحوادث الأكبر والأكثر تعقيدا، غالبا ما تستلزم الإستعانة بخبرات وإستشارات خارجية، والتي تعد ذات تكلفة مرتفعة ، إذ تشكل جزءا جوهريا من التكاليف الإجمالية التي تتحملها المؤسسة، نتيجة حوادث الإحتيال المعلوماتي واسعة النطاق، ويترتب عن ذلك عبئ مالي إضافي يفرض على هذه المؤسسات.[1]

وقد شهد إقتصاد الأمن السيبراني، خلال عامي 2022 و2023 نموا لافتا، حيث تضاعف معدله ليبلغ أربعة أضعافه في 2023 مقارنة بسنة 2022، ورغم هذا التطور السريع إلا أن التوسع في الإستثمارات التقنية لم يترجم إلى توزيع التكافؤ بين المؤسسات في مجال الأمن السيبراني بل ساهم في خلق فجوة واضحة بين هذه المؤسسات، في قدرتها على التكيف مع محاولات الإحتيال الإلكتروني، وتأكد البيانات أن هنالك إختفاء تدريجي لما يعرف بالطبقة المتوسطة من المؤسسات، التي تمتلك حدا أدنى من المرونة السيبرانية، حيث إنخفضت بنسبة 31 % منذ عام 2022.[2]

ترجع أسباب هذا التفاوت إلى عاملين رئيسيين يتمثلان في:

- إرتفاع تكلفة الحصول على الأدوات، والخدمات، والمهارات السيبرانية المتخصصة؛
- إعتماد المؤسسات الكبرى على التكنولوجيات المتقدمة، مما يمنحها أفضلية تنافسية يصعب على غيرها مجاراتها، حيث تشير الإحصائيات إلى أن المؤسسات الصغيرة، أكثر عرضة للتصريح بعدم قدرتها على تلبية الحد الأدنى من متطلباتها التشغيلية، من حيث الأمن السيبراني، بينما تظهر المؤسسات ذات الإيرادات المرتفعة حدا أعلى بـــ 22 %، حيث تتمتع بمرونة تفوق تلك الإحتياجات، ويزداد القلق بالنظر إلى الطبيعة المعقدة للمنظومة السيبرانية العالمية، حيث يعتمد الأداء السيبراني لكل مؤسسة على سلامة شركائها، وقد أظهرت إحدى الدراسات أن 98% من المؤسسات العالمية ترتبط بطرف ثالث تعرض للإختراق خلال الأعوام الماضية،

[1] شركة حاكافي MCAFEE، مركز الدراسات الاستراتيجية والدولية، التكاليف الخفية للجرام الالكترونية، 7 ديسمبر 2020، https://www.mcafee.com، تم الاطلاع في 20 ماي2025، على الساعة 01:46.

[2] تقرير المنتدى الإقتصادي العالمي، التوقعات العالمية للأمن السيبراني، جانفي 2024، ص9.

وبالمقابل نجد أن نسبة المؤسسات الصغيرة المؤمنة لا تتجاوز 25 % مقارنة بنسبة 75 % للمؤسسات الكبرى وتتسع الفجوة كذلك عند النظر إلى حجم المؤسسة من حيث عدد الموظفين، إذ يبلغ معدل التغطية 85 % في المؤسسات من أصل (100.000 موظف) مقابل 21 % فقط للمؤسسات الصغيرة التي تضم 250 موظف أو أقل، وتشير التوقعات إلى تزايد هذا التفاوت الذي يحد من القدرة المؤسسات الصغيرة على الوقاية ومكافحة الإحتيال الإلكتروني.[1]

المطلب الثاني: الآثار غير المالية للإحتيال الإلكتروني على المؤسسات

لا تقتصر تداعيات الإحتيال الإلكتروني على الجوانب المالية فحسب، بل تمتد لتشمل آثارا غير مباشرة تهدد إستقرار المؤسسة وموثوقيتها. ومن أبرز هذه الآثار:

الفرع الأول: تسريب البيانات والمعلومات الحساسة

مما لاشك فيه أن المعلومات والبيانات، التي يسعى المجرمون الإلكترونيون للإستيلاء عليها من خلال أساليب الإحتيال، تعد من الأصول ذات القيمة العالية، ذلك أنها لا تمثل مجرد معطيات على الشاشة، بل تترجم مباشرة إلى قيم مالية ملموسة، ومع الإعتماد على الأنظمة الرقمية في تسيير مختلف مجالات العمل في المؤسسات، أصبحت البيانات هدفا رئيسيا للهجمات الإحتيالية، لما تحمله من إمكانيات كبيرة للإستغلال غير المشروع. وتتجلى خطورة الإحتيال على هذه البيانات في حساسيتها، حيث تشمل على سبيل المثال معلومات بنكية، معلومات شخصية، حسابات إلكترونية، سجلات تجارية، مراسلات خاصة، هذه البيانات تستخدم من قبل الجناة، إما بشكل مباشر عن طريق السحب غير المشروع للأموال باستعمال هذه المعلومات أو إنتحال الهويات، أو بشكل غير مباشر عبر بيعها في الأسواق السوداء، أو توظيفها في عمليات إحتيال مستقبلية.[2]

[1] –المنتدى الاقتصادي العالمي، مرجع سابق، ص9.

[2] عبد الله دغش العجمي، مرجع سابق، ص 63.

فالإحتيال الإلكتروني لم يعد يقتصر على الإستيلاء على أموال المؤسسات، ومستخدميها فقط، بل تعدى ذلك إلى إنتهاك الخصوصية الرقمية، والهيمنة على المعلومات الحساسة، سواء المعلومات الشخصية، أو البنكية الخاصة بالمستخدمين، أو معلومات وبيانات المؤسسة، وهو ما يعكس التحول الجوهري، في مفهوم المال والقيمة في هذه الجريمة، لأنه وبالنظر للأهداف التي يعتمدها المحتالون، والتي ليست محصورة على المال المادي فقط، وإنما المعلومات أيضا، وفي كثير من الأحيان لا يعطي الجاني إهتماما للمال بنفس درجة إهتمامه بالهيمنة على البيانات، فهذا ما يدل على أن قيمة هذه البيانات، أصبحت في بعض المرات أكثر من قيمة النقود، لإمكانية تحويل هذه المعلومات، وإستخدامها في مكاسب غير مشروعة بشكل متواصل.

لقد إستغلت الجماعات الإجرامية السيبرانية، بشكل جيد الثغرات في سلاسل التوريد الرقمية (Digital Supply Chains)،حيث كشفت الهجمات الأخيرة عن ضعف واضح في قدرة المؤسسات على رصد المخاطر الأمنية المرتبطة بالجهات الخارجية التي تتعامل معها، و يعتبر الهجوم السيبراني (MOVEIT TRANSFER ATTACK)، الذي وقع في منصف عام 2023، مثالا على هذا النوع من الإحتيال، حيث إستهدفت خدمات النقل الآمن للبيانات، وهو تطبيق تستخدمه آلاف المؤسسات لنقل ملفاتها الحساسة، مما أتاح للمهاجمين الإحتيال على عدد كبير من المؤسسات عن طريق ثغرة واحدة، ما يميز هذا الهجوم ليس فقط نطاقه، بل طبيعته المركبة، لأنه إمتد إلى العملاء وشركاء المؤسسات، فقد أثر تسلسليا وإستولى على جميع معلومات المؤسسات بالاضافة إلى متعامليها ومستخدميها، ليصل الجناة في هذا الهجوم إلى معلومات شديدة الحساسية تضمنت بينات تعريف شخصية، وأرقام الضمان الإجتماعي، وسجلات طبية خاصة، ومعلومات مالية، ومصرفية، وهو ما يمثل خرقا خطيرا للخصوصية الرقمية، ووضع المؤسسات في مواجهة مع أعباء قانونية.[1]

[1] – المنتدى الاقتصادي العالمي، مرجع سابق، ص33.

الفرع الثاني: تدهور سمعة المؤسسات

تُعد السمعة الإلكترونية للمؤسسة أحد أبرز الأصول غير الملموسة التي تؤثر بشكل مباشر على مكانتها التنافسية واستمراريتها، لاسيما في ظل التطور الكبير لوسائل التواصل الإجتماعي وإنتشار الفضاء الرقمي. إذ تعكس السمعة الإلكترونية تصورات الجمهور وأصحاب المصلحة حول المؤسسة، وتشكل إنطباعاً عاماً يؤثر على قرارات العملاء والمستثمرين والشركاء.

غير أن هذه السمعة أصبحت معرضة بشكل متزايد لمخاطر الإحتيال الإلكتروني، الذي يمس بصورة المؤسسة ويقوّض ثقة المتعاملين معها. فالإعتداءات السيبرانية مثل إنتحال هوية الشركة إختراق قواعد بيانات العملاء، أو نشر معلومات كاذبة على المنصات الرقمية، قد تؤدي إلى تدهور حاد في السمعة الإلكترونية، مما ينعكس سلباً على الأداء المالي وفُرص التوظيف والتوسع في السوق.

أشارت في ذلك عدة دراسات مثل (Davies Chun، وCastellano وDutot) إلى أن السمعة الإلكترونية ترتبط بشكل وثيق بمدى قدرة المؤسسة على حماية نفسها من الهجمات الإلكترونية، حيث يرى أصحاب المصلحة أن السمعة الإيجابية تعكس مصداقية وأمان التعامل الرقمي، وفي المقابل فإن تعرض المؤسسة لهجمات إحتيالية عبر الأنترنت، قد يفسر على أنه ضعف في الحوكمة الرقمية، وقصور في إدارة المخاطر، ما يؤدي إلى فقدان الثقة وتراجع تنافسية المؤسسة. لذلك، أصبحت حماية السمعة الإلكترونية اليوم لا تقتصر على التسويق الرقمي، أو التفاعل مع الجمهور، بل تشمل أيضا الإستثمار في نظم الأمن السيبراني وتطوير إستراتيجيات إستباقية لرصد الإحتيال والتصدي له قبل تفاقمه.[1]

[1] سهيلة بن يحي، أمينة مرابط، السمعة الإلكترونية للمؤسسات، دفاتر MECAS، العدد 01، 2018، ص 218.

خلاصة وإستنتاجات

من خلال دراستنا لهذا الفصل، يبدو جليا أن الإحتيال الإلكتروني يشكل أخطر التهديدات التي تواجه المؤسسات، نظرا لخصائصه المعقدة مثل سرعة التنفيذ، وصعوبة الإثبات، وطبيعته العابرة للحدود، بالإضافة إلى كونه موجها غالبا لتحقيق مكاسب مالية، وتكمن خطورته في إستخدام وسائل تقنية يصعب تتبعها، مما يعيق الوصول إلى الجاني، أو إثبات الجريمة بسهولة.

كما تتعدد أنواع الإحتيال الإلكتروني، وأبرزها الإحتيال على البيانات مثل سرقة المعلومات أو إختراق الأنظمة، والإحتيال على الأموال كالتصيد الإلكتروني، والتحويل غير المشروع للأموال أما آثاره، فهي تشمل خسائر مالية مباشرة، وتكاليف إضافية للحماية والوقاية، فضلا عن تدهور سمعة المؤسسة وفقدان ثقة العملاء، إلى جانب سرقة بيانات حساسة، قد تستغل لاحقا لأغراض غير مشروعة، مما يؤثر على إستقرار المؤسسة وقدرتها التنافسية.

الفصل الثاني

آليات حماية المؤسسات من الاحتيال الالكتروني

المبحث الأول: الإطار القانوني والمؤسساتي الدولي والإقليمي لحماية المؤسسات من الاحتيال الالكتروني

المبحث الثاني: الآليات القانونية والمؤسساتية الوطنية لحماية المؤسسات من الاحتيال الالكتروني

المبحث الثالث: التحديات وآليات تفعيل الإطار القانوني لحماية المؤسسات من الاحتيال الالكتروني

الفصل الثاني: آليات حماية المؤسسات من الإحتيال الإلكتروني

في ظل التطور التكنولوجي المتسارع، وخاصة في مجالات الإعلام والإتصال. برزت الجريمة الإلكترونية كأحد أكثر التحديات التي رافقت الثورة التكنولوجية المعاصرة، والتي تنوعت صورها ومجالاتها، يعد في ذلك الإحتيال الإلكتروني من أخطر الجرائم التي تهدد المؤسسات في الوقت الراهن، ما جعل مواجهته تتطلب إعتماد آليات قانونية، وتنظيمية فعالة على المستويات الدولية والوطنية. فعلى الصعيد الدولي، تؤدي المعاهدات والإتفاقيات الدولية دورا محوريا في تنسيق الجهود الدولية لمكافحة الإحتيال الإلكتروني، إلى جانب المؤسسات الدولية المتخصصة في هذا المجال، أما على الصعيد الوطني، فقد تنوعت وسائل الحماية بين القوانين العامة والخاصة، إضافة إلى الآليات المؤسساتية الوطنية التي تسعى إلى تعزيز الأمن في البيئة الرقمية. وهذا ما نهدف لإبرازه في هذا الفصل، من خلال تسليط الضوء على مختلف هذه الآليات، وإستعراض مدى فعاليتها في حماية المؤسسات من التهديدات الإلكترونية المتزايدة.

المبحث الأول: الإطار القانوني والمؤسساتي الدولي والإقليمي لحماية المؤسسات من الإحتيال الإلكتروني

تتميز غالبا الجرائم الإلكترونية بكونها جرائم عابرة للحدود الوطنية، فقد ترتكب الجريمة الإلكترونية في بلد لتتحقق النتيجة في بلد آخر، وقد تستهدف عدة ضحايا من بلدان مختلفة، كما يمكن أن يعتمد الجاني على معطيات وبيانات لخوادم تقع في بلدان أجنبية، هذا الطابع الدولي للجرائم السيبرانية يشكل تحديا قانونيا معقدا، يستدعي تنسيقا دوليا فعالا وإطارا قانونيا شاملا لمكافحتها والحد من آثارها العابرة للحدود[1].

لذا أصبح من الضروري تظافر الجهود، وتعزيز التعاون بين الدول من خلال وضع آليات قانونية ومؤسساتية، سواء كانت إقليمية، أو دولية تسعى لتوحيد الجهود بينها، من خلال وضع

[1] عبد اللطيف جمل، عبد الغاني طرايش، الحماية الجنائية للمستهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري: دراسة تحليلية ومقارنة على ضوء القانون الفرنسي، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد 01، 2025/03/20، ص1396

معايير موحدة لمكافحة الجرائم السيبرانية من جهة، وتوفير الحماية الازمة للمؤسسات من جهة أخرى، ومن خلال ما تطرقنا إليه آنفا سوف نتناول هذا المبحث في مطلبين، المطلب الأول يتضمن الآليات القانونية الدولية والإقليمية لحماية المؤسسات من الإحتيال الإلكتروني، والمطلب الثاني يتطرق إلى الآليات المؤسساتية الدولية والإقليمية لحماية المؤسسات من الإحتيال الإلكتروني.

المطلب الأول: الآليات القانونية الدولية والإقليمية لحماية المؤسسات من الإحتيال الالكتروني

أصبح تعاون الدول سواء كان إقليميا أو دوليا، من أهم آليات السياسة الجنائية في مجال حماية المؤسسات من خطر الإحتيال الإلكتروني، بالنظر إلى ما يترتب عليه من تحقيق تقارب بين النصوص والتشريعات الجنائية من جهة، وتدعيم صور المساعدة القانونية والقضائية المتبادلة بين الدول من جهة أخرى، وذلك من أجل كشفها وملاحقة مرتكبيها.[1] لذا تعتبر الصكوك القانونية سواء كانت إقليمية أو دولية، أحد الآليات لتحقيق هذه الأهداف.

الفرع الأول:الصكوك القانونية الدولية

تعتبر الصكوك القانونية الدولية من قرارات الأمم المتحدة، إتفاقيات، والمعاهدات، الإطار قانوني الذي تسعى من خلالها المنظمات الدولية لتعزيز الأمن السيبراني، و توحيد الجهود لتعاون بفعالية ضد الإحتيال الإلكتروني و التي نذكر منها:

أولا: قرارات وإتفاقيات الجمعية العامة للأمم المتحدة

بذلت الأمم المتحدة جهودا كبيرة في مواجهة الجرائم المعلوماتية، بما فيها جريمة الاحتيال الإلكتروني الذي تتعرض له المؤسسات، مشددة على أهمية التعاون بين الدول الأعضاء للحد من إنتشارها وتفاقم آثارها، ولقيت هذه القضية إهتماما بارزا في مؤتمرات الأمم المتحدة نذكر منها:[2]

[1] محمد صفاء الدين علي شرشر محمود، الجهود الدولية لمكافحة جرائم الأنترنت، مجلة البحوث القانونية والاقتصادية جامعة المنوفية، العدد 03، أكتوبر 2021، ص 525

[2] فاروق خلف، مرجع سابق، ص11.

1- **إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية:** تم التوقيع على هذه الاتفاقية في مدينة باليرمو بإيطاليا عام 2000، وتهدف بشكل رئيسي إلى تعزيز التعاون الدولي في مكافحة الجريمة المنظمة العابرة للحدود، بما في ذلك الجرائم المرتكبة باستخدام الحواسيب أو شبكات الاتصالات السلكية واللاسلكية أو غيرها من التقنيات الحديثة ، وقد تضمنت مجموعة من التدابير لتعزيز التعاون الدولي، كتبادل المساعدات القانونية، تسليم المجرمين، إجراء تحقيقات مشتركة، والتعاون في المسائل الجنائية، كما تدعو جميع الدول إلى إبرام إتفاقيات إضافية تهدف إلى تعزيز هذا التعاون الدولي في مواجهة التحديات المتزايدة للجريمة المنظمة.[1]

2- **قرارات وتوصيات الأمم المتحدة:** أصدرت الجمعية العامة للأمم المتحدة مجموعة من القرارات والتوصيات المهمة في مجال مكافحة الجرائم المعلوماتية وتعزيز الأمن السيبراني، من أبرزها:[2]

- القرار (121/45) عام 1990، الذي شمل نشر دليل خاص بمنع الجرائم المرتبطة بأجهزة الكمبيوتر ومكافحتها، وذلك عام 1994.
- القرار (63/55) الصادر في 4 ديسمبر 2000، والقرار (121/56) الصادر في 19 ديسمبر 2001، حيث ركزا على إستخدام نظم المعلومات الجنائية الإدارية لمكافحة الجرائم المعلوماتية.
- القرار (239/57) الصادر في 31 يناير 2003، والقرار (199/58) الصادر في 30 يناير 2004، اللذان ساهما في تعزيز ثقافة الأمن السيبراني على المستوى العالمي.

وسعيا منها لبلوغ الهدف المنشود من خلال تضافر الجهود الدولية، في هذا المجال أكدت بعض هذه القرارات و التوصيات مايلي:

[1] نادر عبد الكريم الغزوالي، الحماية الجنائية من جرائم الأنترنت دراسة مقارنة، سويسرا: دار نور للنشر الأكاديمي، 2017، ص 157.

[2] فاروق خلف، مرجع سابق، ص11.

أ- توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات، بشأن جرائم الكومبيوتر، الذي تم التطرق من خلاله إلى جانبين:[1]

➢ **الجانب الموضوعي**

نص على قائمة الحد الأدنى للأفعال التي صنفت كجرائم إلكترونية، والمتمثلة في الإحتيال والغش المرتبط بالكومبيوتر، تزويد الكومبيوتر أو التزويد المعلوماتي، الإضرار بالبيانات والبرامج الدخول غير المصرح به؛

➢ **الجانب الإجرائي**

- وضع تحت سلطة التحقيق والتحري، ما يكفي لتحقيق حماية حقوق وخصوصية الأفراد؛
- يجب أن تكون القيود التي ترد على الأفراد متماشية والمعايير الدولية لحقوق الأنسان ولا تكون مقبولة إلا إذا كانت بسند قانوني؛
- على ضوء المبادئ العامة يجب أن تحدد بوضوح السلطات المختصة بالقيام بإجراءات التفتيش في بيئة رقمية ووضع القواعد المتعلقة بالإثبات، وواجب التعاون الفعال من طرف أطراف القضية، إضافة بالسماح للسلطات العامة بإعتراض الإتصالات داخل الحاسب وتقديم ما تم التوصل إليه من أدلة للقضاء؛
- إعتماد الأدلة الرقمية في التشريعات الدول؛

ب – قرار الجمعية العامة للأمم المتحدة لمكافحة إستغلال تكنولوجيا المعلومات لأهداف إجرامية يحث الدول الأعضاء على:[2]

- تنسيق أجهزة الردع بين الدول وتبادلها المعلومات بشأن المشاكل التي تواجههم في مكافحة الجرائم الإلكترونية؛
- العمل على تعزيز نظام المساعدة القانونية بين الدول لما توفره من سرعة في إجراء التحقيقات؛

---

[1] أمال بيدي، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية، مجلة البحوث في الحقوق والعلوم الإنسانية، العدد 01، 2022/06/03، ص307.

[2] نادر عبد الكريم الغزوالي، مرجع سابق، ص 157-159

- جمع وتبادل عناصر الأدلة المتعلقة بهذه القضايا بشكل سريع.

ومن أهم التوصيات التي أقرها المؤتمر في مكافحة الجريمة السيبرانية:[1]

- إستحداث أدوات وبرامج لتسهيل مكافحة ومنع الجريمة السيبرانية؛
- تكوين أفراد الأجهزة المعنية بمكافحة الجرائم الإلكترونية في مجال التحقيق والتحري عمليات الإستدلال الجنائي الرقمية وكيفية التعامل مع الأدلة؛
- تعاون الدول فيما بينها وتمكين بعضها، من الوصول إلى البيانات الموجودة خارج إقليمها بحيث يكون محددا، خاضعا للرقابة، ومتناسبا مع طبيعة الجريمة في ظل إحترام القانون، حماية حقوق الإنسان وخصوصية الأفراد؛
- إشراك القطاع الخاص في مجال الأمن السيبراني، وإعتماد الجهات المختصة إستراتيجيات جديدة كأن يعملوا على تدعيم الشركات مع فرق بحث أكاديمية في مجالات متنوعة؛

لاتزال جهود الأمم المتحدة مستمرة في هذا المجال بإصدارها دليلا عاما إرشاديا حول الجرائم السيبرانية تعمل على تعديله وتنقيحه كل ما إستلزم الأمر ذلك.

ثانيا: معاهدة بودابست لمكافحة جرائم الانترنت

أول معاهدة متعلقة بمكافحة الجرائم الإلكترونية تتكون من 48 مادة، أكدت الإتفاقية على الحاجة إلى إتخاذ تدابير تشريعية لمكافحة الجرائم السيبرانية، ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء لمكافحة الجريمة المعلوماتية، وتعتبر مرجعا لا يستهان به في ميدان محاربة الإجرام السيبراني، سواء بالنسبة لبعض الإتفاقيات اللاحقة ذات الصلة أو بالنسبة للتشريعات الداخلية، هي في الأصل أوروبية المنشئ إلا أنها دولية الطابع حيث تنص المادة(48)

[1] أمال بيدي، مرجع سابق، ص 310،309.

منها، على أنها مفتوحة للإنضـــمام لكل دول العالم وقد تم التوقيع عليها، من قبل 30 دولة في نوفمبر 2001 بالعاصة المجرية بودابست. [1] وقد تضمنت المعاهدة مايلي:[2]

1- التدابير الواجب إتخاذها على الصعيد الوطني:

أ- في الجانب الموضـــوعي: نص على الأفعال التي يجب على الدول الأعضـــاء تجريمها في تشريعاهم الوطنية وتم تقسمها إلى خمسة أنواع:

- الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الحاسوب وهي النفاذ والإعتراض غير المشروع، التدخل في البيانات، التدخل في النظام، إساءة إستخدام الأجهزة الرقمية؛
- جرائم الحاســـوب والمتمثلة في التزوير والإحتيال الإلكتروني خصـــوصـــا الذي تتعرض له المؤسسات؛
- الجرائم ذات صلة بالمحتوى؛
- الجرائم المتعلقة بإنتهاكات حقوق النشر والتأليف والحقوق ذات صلة؛
- المسؤولية الإضافية من خلال تجريم أفعال المحاولة والمساعدة والتحريض على هذه الأفعال المنصوصة في المعاهدة، وكذلك مسائلة الشخص الإعتباري، الذي أرتكب هذه الأفعال لمصلحته دون الإخلال بالمسؤولية الجنائية للشخص الطبيعي الذي قام بهذا الفعل، على أن تكون العقوبات والإجرءات رادعة ومتناسبة وطبيعة الجرم إضافة إلى العقوبات المالية؛

ب- أما الجانب الإجرائي فنص على:

- الأحكام المشـتركة في الجرائم الإلكترونية والمتضـمن نطاق الأحكام الإجرائية، بإقرار من خلال تشـــريعات الوطنية للدول الأطراف، على الســـلطات والإجراءات المتعلقة بالتحقيقات

[1] ناشف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، العدد 01، 2022/06/03، ص 443.

[2] مجلس أوروبا، الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست) 2001/11/23، متوفر على الرابط: https://rm.coe.int/budapest-convention-in-arabic/1680739173 أطلع عليها يوم:2025/05/22 على الساعة 23:53

والدعاوى الجنائية السيبرانية إضافة إلى الشروط والضمانات التي يجب أن توفر الحماية لحقوق الأفراد وخصوصياتهم؛

- التعجيل في حفظ بيانات الحاسوب المخزنة من خلال السلطات المختصة، خاصة إذا كانت هذه البيانات قابلة للحذف والتعديل، وكذا حفظ بيانات الحاسوب والكشف الجزئي عن بيانات الحركة، من خلال الإسراع في حفظ بيانات الحركة للمجرم، مع ضمان تعجيل الكشف للدولة الطرف، عن البيانات بالقدر الذي يمكنها من تحديد المسار الذي نقل من خلاله الإتصال؛
- الأمر بإبراز البيانات، من خلال النص على تدابير تشريعية لتمكين السلطات المختصة إصدار أمر تسخر فيه، أي شخص داخل إقليمها بتقديم بيانات الحاسوب بحوزته أو تحت سيطرته كيف ما كان تخزينها، أو طلب معلومات عن المشترك من أي مزود خدمة على أراضيها؛
- البحث عن بيانات الكومبيوتر المخزنة ومصادرتها، من خلال إعتماد تشريعات تتيح للدولة الطرف توسيع نطاق التحري، من خلال السماح لها بالنفاذ إلى أجهزة الحاسوب أو أي دعامة مخزنة للمعلومات على أراضيها، إذا تأكدت بأن البيانات المطلوبة مخزنة عليها وتمكين السلطات المختصة من مصادر نظام الكومبيوتر، أو جزء منه أو دعامة تخزين البيانات، أونسخها مع الحفاظ على سلامتها وجعلها غير قابلة للنفاذ أو الإزالة.

2- أما فيما يخص التعاون الدولي، فتضمن:

- حث الدول الأطراف تسليم مرتكبي الجرائم السيبرانية فيما بينهم ؛
- تبادل الدول الأطراف المساعدة فيما بينهم، لأغراض التحقيقات والمتابعات المتصلة بالجرائم الجنائية السيبرانية، إضافة إلى تبادل المعلومات التلقائية وذلك دون إذن مسبق، إذا حصلت عليها في إطار التحقيقات المنجزة، وعلمت أن الإفصاح عنها للدولة الطرف يساعدها في تحقيقاتها أو متبعاتها مع الحفاظ على السرية، وإستعمالها وفق شروط النص على الإجراءات المتعلقة بطلبات المساعدة المتبادلة، في حالة عدم وجود إتفاقيات دولية واجبة التطبيق، والتي تتم وفق مراحل منصوص عليها في المادة (27) مع السرية، والقيود المستخدمة، والمنصوص عليها في المادة (28).

تعد الإتفاقية الإطار المرجعي لمكافحة الجرائم المعلوماتية ولها صـــبغة دولية بحيث يمكن لأي دولة الإنضمام إليها.[1]

الفرع الثاني : الصكوك القانونية الإقليمية

تشـــكل الإتفاقيات والمعاهدات، بين الدول ذات الحدود المشـــتركة، أو/و ذات التجانس الديمغرافي، أو التي تجمعها مصـــالح إســـتراتيجية، إحدى أهم الأدوات القانونية التي تنتهجها الدول في مجال تعزيز تعاونها لمكافحة الإحتيال الإلكتروني و أهم هذه الصكوك:

أولا إتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

وافق مجلس وزراء الداخلية والعدل العرب في إجتماعه المشـــترك، المنعقد بمقر الأمانة العامة لجامعة الدول العربية، في القاهرة بتاريخ 21ديســمبر2010، على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي تهدف إلى تعزيز التعاون بين الدول العربية في التصـــدي للجرائم الإلكترونية، بما يسهم في حماية أمن الدول العربية ومصالحها، وضمان سلامة مجتمعاتها وأفرادها.[2] وقد أصبحت الإتفاقية ســارية المفعول، بعد تصــديق مصــر عليها عام 2015، ليكتمل نصــاب الدول الســبع المطلوبة لسريانها.[3]

كما صـــادقت الجزائر على هذه الاتفاقية بموجب المرســـوم الرئاســـي رقم 14-252[4] بتاريخ:2014/09/08 والذي نص في المادة (03) على مجالات تطبيق الإتفاقية لمنع الجرائم التقنية والمعلومات ، التحقيق فيها، وملاحقة مرتكبيها وذلك في حالة ما إذا: [5]

- أرتكبت في دولة وتم الإعداد، التخطيط لها، توجيهها أو الإشراف عليها في دولة أخرى؛

---

[1] أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، العدد 01، 2018، ص 740.

[2] فلاح عبود، هالة لبرارة، "الجريمة الإلكترونية وآليات مكافحتها وطنيا ودوليا"، في: ارتباس نذير، دياولو محمد نجيب، طارق قادري (محررا)، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، بريطانيا، المركز المغاربي شرق أدنى للدراسات الإستراتيجية، جانفي 2024، ص 376.

[3] آسيا لعمراني، التعاون الدولي في مواجهة الجرائم السيبرانية: الجزائر نموذجا، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، العدد3، 2012، ص 79.

[4] الجمهورية الجزائرية الديمقراطية الشعبية المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة 21 ديسمبر 2010، الجريدة الرسمية العدد 57 الصادرة بتاريخ 28 سبتمبر 2014.

[5] المرسوم الرئاسي رقم 14-252، المرجع نفسه، المادة 03

- قامت بإرتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة؛
- كانت لها أثار شديدة في دولة أخرى، أو أرتكبت في أكثر من دولة.

كما جاء في المادة (04) منه بتحديد الإلتزامات التي نصـــت عليها الإتفاقية، وقد تمثلت في إلتزام أطراف الاتفاقية بـ:[1]

- تنفيذ إلتزاماتها الناشـــئة عن تطبيق هذه الاتفاقية بما يتفق مع مبدأ الســـيادة، والمســـاواة في السيادة الإقليمية للدول، وعدم التدخل في الشؤون الداخلية للدول الأخرى؛
- عدم التدخل في الممارســـة الولائية القضـــائية، وأداء الوظائف التي هي من إختصـــاص سلطات الدولة الأخرى، بمقتضى قانونها الداخلي؛

في حين تضـــمنت المادة (05) إلزام الدول الأطراف بتجريم الأفعال المبينة في هذا الفصـــل وذلك وفقا لتشريعاتها وأنظمتها الداخلية، والمتمثلة في الجرائم التي تستهدف تقنية المعلومات، حيث نصـــت الإتفاقية، على الجرائم التي تســـتهدف التقنية في المواد من (06) الى (11)[2]. وقد حمت هذه الاتفاقية المؤسسات من الإحتيال الإلكتروني، فقد نص المشرع على ذلك في نص المادة (11) منه، فعرفها على أنها: "التسبب بإلحاق ضـرر بالمستفيد، والمستخدمين عن قصـد، أو بدون وجه حق، بدافع الإحتيال لتحقيق المصالح، والمنافع بطريقة غير مشروعة للفاعل أو للغير بواسطة:[3]

- إدخال تعديلات حجب أو حذف للمعلومات والبيانات؛
- التدخل في أنظمة التشغيل والإتصالات أو محاولة تعطيلها أو تغيرها؛
- تعطيل الأجهزة، البرامج والمواقع.

في حين تضـمن الفصـل الرابع من هذا المرسـوم التعاون القانوني والقضـائي بين الدول الأطراف في مثل هذا النوع من الجرائم:

---

[1] المرسوم الرئاسي رقم 14-252، المرجع نفسه، المادة 04

[2] ليلى لعمريوي، سعد صليح، آليات مواجهة المخاطر السيبرانية في المجتمع الجزائري مقارنة بالنظام الدولي، مداخلة مقدمة ضمن الملتقى الافتراضي الجرائم الإلكترونية في المجتمع الجزائري: تشخيص الواقع وتحديات الأمن السيبراني، المنعقد بتاريخ 03/15/ 2022، ص283.

[3] المرسوم الرئاسي رقم 14-252 مرجع سابق، المادة 11.

- إلتزام كل دولة طرف تبني الإجراءات الضـــرورية لمد الإختصـــاص على أي من الجرائم المنصوص عليها في الإتفاقية إذا ارتكبت الجريمة في إقليم الدولة الطرف[1]؛
- تسليم المجرمين بين الدول الأطراف؛
- المساعدة المتبادلة فيما يخص التحقيقات، أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة الإلكترونية؛
- تبادل المعلومات بين هذه الدول فيما يخص هذا النوع من الجرائم بدون طلب مسبق إذا حصـلت عليها من خلال تحقيقاتها، وإعتبرت أن كشـف هذه المعلومات يمكن مسـاعدة الدول الطرف والإلتزام بسريتها وحدود إستخدامها؛
- الحفظ العاجل للمعلومات المخزنة في أنظمة المعلومات؛
- الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة، الخاصة بإتصالات معينة؛
- التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة؛
- الوصـــول إلى معلومات تقنية المعلومات عبر الحدود للدول الأطراف، فيما بينهم بدون الحصول على تفويض من تلك الدولة إذا كان المصدر مفتوح؛
- إنشـاء جهاز متخصـص في كل دولة من هذه الدول يعمل بشـكل متفرغ لضـمان توفير المساعدة الفورية اللازمة في مجال جرائم تقنية المعلومات، وذلك بهدف ضمان إستمرارية الإجراءات والتحقيقات المتعلقة بهذه الجرائم، وجمع الأدلة الرقمية بطريقة قانونية سليمة.[2]

وقد تم تصـنيف الجزائر عام 2018 ضـمن الدول العربية التي بدأت بتنفيذ إلتزاماتها في مجال الأمن السـيبراني، بينما أظهرت خمس دول عربية مسـتويات عالية من الإلتزام بكافة ركائز المؤشـر العالمي للأمن السـيبراني، من ناحية أخرى، عملت الكويت، الأردن، تونس، والمغرب على تطوير إسـتراتيجيات أكثر تعقيدا، وإنخرطت في برامج ومبادرات لتعزيز الأمن في هذا المجال، أما على

[1] المرسوم الرئاسي رقم 14-252 مرجع سابق، المواد من 30-40

[2] المرسوم الرئاسي 14-252 المرجع نفسه، المادة 43.

مستوى التصنيف الإقليمي، فقد إحتلت السعودية، عمان، وقطر المراتب الثلاث الأولى بين الدول العربية وفقًا لمعايير المؤشر العالمي للأمن السيبراني.[1]

ثانيا: إتفاقية الإتحاد الافريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي

سعت الدول الإفريقية على غرار باقي المجتمعات الدولية، لتعزيز أمنها المعلوماتي، فكانت إتفاقية الإتحاد الافريقي حول الأمن السيبراني، وحماية البيانات ذات الطابع الشخصي هي ثمرة جهود وزراء الإتحاد الإفريقي المسؤولين عن تكنولوجيا المعلومات والإتصال خلال المؤتمر الإستثنائي لهم، في جنوب إفريقيا في الفترة الممتدة من 02 إلى 05 نوفمبر2009، حيث طلبوا من مفوضية الإتحاد الإفريقي، إعداد إتفاقية حول التشريع القضائي فيما يخص، المتطلبات القانونية والتنظيمية للمعاملات والأمن الإلكترونيين وحماية البيانات الشخصية، مع ضرورة توفير الحماية للأنظمة المعلوماتية وذلك بالإشتراك مع لجنة الأمم المتحدة.[2]

ليطرح المشروع الأولي للإتفاقية سنة 2013، ويعتمده رؤساء البلدان الأعضاء في الدورة العادية رقم 23 لمؤتمر الإتحاد الإفريقي، حيث أصبحت الإتفاقية مفتوحة للمصادقة عليها والتي تسمى إختصارا بإتفاقية مالابو.[3]

تضمنت المعاهدة ديباجة تحتوي على شرح بعض المصطلحات، وفصل أول يتضمن المعاملات الإلكترونية، أما الفصل الثاني فتضمن حماية البيانات ذات الطابع الشخصي، لينص الفصل الثالث على تعزيز الأمن الإلكتروني، ومكافحة الجريمة الإلكترونية بما فيها الإحتيال الإلكتروني على المؤسسات، وقد تضمن هذا الفصل ما يلي:[4]

---

[1] فتيحة سويسي، التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها، مداخلة مقدمة ضمن الندوة البحثية المنظمة من مركز البحوث القانونية والقضائية، بتاريخ 18 جانفي 2022، ص 30.

[2] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد 02، ديسمبر 2015، ص14.

[3] مريم لوكال، قراءة في الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة2014، مجلة الدراسات القانونية والإقتصادية، العدد 03، 2021/12/30، ص 660.

[4] إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، متوفرة على الرابط: African Union Convention on Cyber Security and Personal Data Protection | African Union تم الإطلاع يوم 2025/05/18 على الساعة 18:40.

1- تدابير الأمن الإلكتروني الواجب إتخاذها على المستوى الوطني

- تأمين الفضاء الإلكتروني الوطني، من خلال وضع سياسة وإستراتيجيات وطنية لتأمينه لاسيما فيما يخص الإصلاح التشريعي والهياكل التنظيمية؛
- إتخاذ التدابير القانونية من خلال إعتماد تدابير تشريعية و/أو تنظيمية لتجريم الأفعال التي تؤثر على سلامة أنظمة تكنولوجيا المعلومات، وإتخاذ تدابير إجرائية لمتابعة المخالفين، على أن تكون العقوبة في الجرائم الإلكترونية التي تستهدف القطاعات الحساسة من مؤسسات للدولة كالأمن والإقتصاد الوطني أكثر صرامة؛
- إعداد وتنفيذ برامج ومبادرات توعوية بالأمن لمستخدمي الأنظمة، والشبكات الإلكترونية؛
- إلزام الدول الأطراف بإنشاء آلية مؤسساتية مسؤولة عن حوكمة أمن الفضاء الإلكتروني وقادر على معالجة القضايا المتعلقة بهذا المجال؛
- إشراك المجتمعات المدنية والأكاديمية، وحتى القطاع الخاص في تعزيز الأمن السيبراني؛
- تكفل الدول بتكوين الأفراد المكلفين بالأمن السيبراني وتطوير خبراتهم؛

2- **تدابير الأمن الإلكتروني الواجب إتخاذها على مستوى الإتحاد الإفريقي:** إنشاء الآلية التنفيذية لهذه الاتفاقية التي ستسعى لتحقيق ما يلي:

- تعزيز إعتماد وتنفيذ التدابير لتعزيز الأمن السيبراني؛
- جمع الوثائق والمعلومات بشأن إحتياجات أمن الفضاء الإلكتروني؛
- العمل على نشر التوعية بين الجمهور بشأن الآثار السلبية لهذه الظواهر؛
- تقديم المشورة للحكومات الإفريقية بشأن أفضل السبل لتعزيز الأمن السيبراني؛
- تحليل السلوكات الإجرامية وجمعها وتقديمها كمعلومات للسلطات الوطنية المختصة.

3- تدابير الأمن الإلكتروني الواجب اتخاذها على المستوى الدولي

- المواءمة حيث تلزم الدول الأطراف بضمان أن التدابير التشريعية و/أو التنظيمية

المعتمدة لمكافحة الجريمة الإلكترونية سوف تعزز إمكانية المواءمة الإقليمية لهذه التدابير وتحترم مبدأ المسؤولية الجنائية المزدوجة؛

- المساعدة القانونية من خلال تشجيع توقيع الإتفاقيات المتعلقة بالمساعدة القانونية المتبادلة، وتعزيز تبادل المعلومات والبيانات فيما يخص الجرائم الإلكترونية؛
- تبادل المعلومات بتشجيع إنشاء المؤسسات لتبادل المعلومات بشأن التهديدات السيرانية، والإستفادة من وسائل التعاون الدولي في هذا الخصوص؛
- إلتزام الدول الأطراف بالاستفادة من وسائل التعاون الدولي القائمة بهدف الإستجابة للتهديدات الإلكترونية وتحسين أمن الفضاء الإلكتروني.

الأحكام الجنائية: تم النص على الأفعال التي يجب أن تأتى صبغة التجريم كجنايات على مستوى تشريعات الدول الأطراف والمتمثلة في:

- الهجمات على أنظمة الكومبيوتر؛
- الخروقات على البيانات الحوسبية؛
- الجرائم ذات صلة بالمحتوى؛
- الجرام المتعلقة بإجراءات تأمين الرسائل الإلكترونية.

غير أن هذه الاتفاقية لم تدخل حيز التنفيذ لأنها لم تبلغ النصاب المقدر عدده بـ 15 دولة مصادقة، إذ لم يتم التوقيع عليه إلا من طرف 09 دول ، أما الدول المصادقة عليها فهي 10 دول من أصل 55 دولة إفريقية، لتكون الجزائر من بين الدول التي لم توقع و لم تصادق على الإتفاقية فموقف الجزائر لا يبدو واضحا، حيث صادقت على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، بموجب المرسوم الرئاسي 14-252 المؤرخ في 2014/09/08، بعد أن وقعت عليها في 21 ديسمبر 2010، في حين أن الإتفاقيتين تدرسان الموضوع ذاته لماذا تتأخر في المصادقة أو التوقيع عليها؟.[1]

[1] مريم لوكال، مرجع سابق، ص 670.

ثالثا: توصـــيات المجلس الاوروبي بشـــأن المشـــاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات

إن التطور التكنولوجي في مجال الإعلام والاتصـــال الذي أدى إلى تطور الجرائم الإلكترونية، بما فيها الاحتيال الإلكتروني على المؤسسات الذي هو موضوع بحثنا، دفع بالدول الأوروبية لإعادة النظر في الإجراءات الجزائية المطبقة من طرفها في مثل هذا النوع من الجرائم، حيث أصـــدر المجلس الأوروبي التوصـية رقم 95/13 المؤرخة في 1995/09/11 بشـأن مشـاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، وحث أعضـــائه على مراجعة هذه القوانين الإجرائية الوطنية كي تتلائم والتطور الحالي في هذا المجال[1]. وأهم ما جاء فيه[2]:

- توضـيح الإجراءات المتعلقة بتفتيش أجهزة الكمبيوتر، وضـبط البيانات المخزنة عليها، بالإضافة إلى مراقبة المعلومات أثناء إنتقالها،
- سن إجراءات جزائية وطنية تسمح لسلطات التفتيش ضبط برامج الحاسوب والمعلومات المخزنة به وفقا لنفس شروط التفتيش العادية، مع إعلام الشخص القائم عليه بأن النظام كان محل تفتيش وما تم ضبطه من معلومات؛
- السماح أثناء عملية التفتيش، للجهات المعنية، مع إحترام الضمانات المقررة لهذا الإجراء بمد التفتيش إلى أنظمة حاسـوب، تكون على إتصـال بالنظام محل تفتيش في دائرة إختصـاصـهم وضبط ما بها من معلومات إذا كان ذلك ضروريا؛
- أن يوضح قانون الإجراءات الجزائية أن الإجرءات الخاصة بالوثائق التقليدية هي نفسها التي تطبق على المعلومات المخزن بالحاسوب؛

[1] جيلالي شـــويرب، فائزة مراد، الاليات الدولية و الوطنية لمكافحة الجريمة الســـيرانية ، مجلة الدراســـات القانونية و الســـياســـية ، العدد02 ، 2023/06/05، ص159.

[2] ســـليمان قطاف، عبد الحليم بوقرين، مواجهة الجرائم الســـيرانية في ضـــوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصـــادية، العدد 02 ،2022 ، ص ص 77-79.

- تطبيق إجراءات المراقبة والتسجيل الخاصة بالتحقيق الجنائي في حالة الضرورة، بالنسبة لجرائم تكنولوجيا الإعلام والإتصال مع السرية للمعلومات التي يحميها القانون؛
- إلزام العاملين بالمؤسسات التي توفر خدمات الإتصال، إجراء المراقبة والتسجيل، بالتنسيق مع سلطة التحقيق؛
- تطبيق النصوص الإجرائية، المتعلقة بالأدلة التقليدية، على الأدلة الرقمية، مع توحيد وتطوير أنظمة التعامل معها والإعتراف بها بين الدول؛
- تدريب وتأهيل العاملين في مجال العدالة الجنائية لتطوير خبراتهم في مجال الأمن السيبراني وإنشاء وحدات خاصة لمكافحة هذا النوع من الجرائم؛
- وضع قاعدة قانونية، إلى جانب إبرام إتفاقيات بين الدول لضمان عدم المساس بسيادة الدول أو مخالفة القانون الدولي، لتنفيذ إجراءات التحقيق التي تتطلب تدخلاً سريعًا، للوصول إلى أنظمة كمبيوتر خارج إقليمها؛
- يجب أن تكون هنا سرعة في الإجراءات، وقنوات إتصال تربط الجهات المعنية بالتحقيق مع نظيرتها في الدولة الأجنبية لجمع الأدلة، والسماح لها بإجراءات التفتيش والضبط.

لقد اعتمد المجلس الأوروبي الطابع الدولي، لجرائم الحاسوب من سنة 1976، لينشئ سنة 1996 اللجنة الأوروبية لمشاكل الجريمة (CDPC)، تتكون من خبراء للتعامل مع مشاكل الجرائم السيبرانية بما فيها الإحتيال الإلكتروني الذي تتعرض له المؤسسات.[1]

المطلب الثاني: الآليات المؤسساتية الدولية والإقليمية لحماية المؤسسات من الإحتيال الإلكتروني

عمدت عديد من المنظمات الدولية، إلى صياغة أطر قانونية وتأسيس أجهزة متخصصة لمكافحة الجريمة السيبرانية، كما أنشأت عدة تكتلات إقليمية مؤسسات، تُعنى بالتعاون الأمني والتقني

[1] فاروق خلف، مرجع سابق، ص14.

لمواجهة الإحتيال الإلكتروني. وذلك بهدف تعزيز قدرات الدول والمؤسسات على التصدي لجرائم الإحتيال الرقمي، ومن أبرز هذه المؤسسات، نذكر:

الفرع الأول: المنظمة الدولية للشرطة الجنائية الأنتربول

تعتبر المنظمة الدولية للشـــرطة الجنائية الأنتربول من أهم الأجهزة التابعة لهيئة الأمم المتحدة المعنية بمكافحة الجرائم السيبرانية.[1] وقد تأسست سنة 1923 وإتخذت مدينة ليون بفرنسا مقرا لها وهي تعمل على التنسيق بين أجهزة الشـرطة في العالم والتي تضـم 192 دولة عضـو.[2] وقد كان إنضـمام الجزائر إليها سنة 1963.[3] وتسعى المنظمة لمكافحة الجرائم وفق المهام المحددة في نظامها الأساسي بغية تحقيق أهدافها المسطرة.

تتمثل مهامها في:

- العمل على إدارة شبكة اتصالات آمنة بين الدول الأعضاء، مما يتيح للجهات المختصة متابعة الجرائم الإلكترونية، طلب المعلومات، وإحالتها بســـرعة وأمان، حيث تعمل هذه الشـــبكة كحلقة وصل بين أنظمة الشرطة المختلفة؛
- توفير خدمات الإســـناد الميداني من خلال تأمين الموارد اللازمة لمكافحة الإجرام المالي المرتبط بالتكنولوجيا المتقدمة، لما له من تأثيرات كبيرة على المؤسسات؛
- تدريب وتطوير أجهزة الشـــرطة في الدول الأعضـــاء لتعزيز قدرتها على مكافحة الجرائم السيبرانية العابرة للحدود، بما فيها الإحتيال الإلكتروني الذي تتعرض له المؤسسات؛
- حماية الأمن الدولي عبر تحذير الدول من إحتمالات وقوع جرائم، بناءً على المعلومات المستخلصة من عمليات تحليل البيانات.[4] حيث أسفرت عملية **Africa Cyber Surge 2**

---

[1] هشام بشير، الآليات الدولية لمكافحة الرجيمة الإلكترونية، المركز الدولي للدراسات المستقبلية والإستراتيجية، مصر، 2012، ص 21.

[2] أسماء بوعكاز، الأنتربول ودوره في تنفيذ إتفاقيات تسليم المجرمين في إطار مكافحة الجريمة المنظمة، مجلة الباحث للدراسات الكاديمية، العدد 03، 2021، ص 129.

[3] رابح نهائلي، سـعاد قيرة، دور المنظمات الدولية في مكافحة الجريمة المنطمة (منظمة الأمم المتحدة، المنطمة الدولية للشـرطة الجنائية نموذجا)، مجلة البحوص القانونية، العدد 02، 2021، ص 134.

[4] أسـامة غري، المنظمة الدولية للشـرطة الجنائية (الأنتربول) ودورها في مكافحة الجريمة المنظمة، دراسـات وأبحاث، العدد 03، 2011/03/15، ص 164.

التي نسقها الإنتربول والأفريبول، عن تحديد 14 مشتبهًا بهم في جرائم سيبرانية وكشف 20674 شبكة مشبوهة، كما ساعدت بيانات الإستخبار والتعاون الدولي في منع العديد من عمليات الإحتيال الإلكتروني والتصيد الإحتيالي، إضافة إلى التحقيق فيها وتعطيلها.[1]

- تحليل المعلومات والبيانات المرتبطة بالجريمة ومرتكبيها، بناءً على المعطيات المتاحة ضمن نطاقها، ومشاركتها بين الدول الأعضاء لتعزيز التنسيق في مكافحة الجرائم السيبرانية، إلى جانب التعاون مع المؤسسات البرمجية في تعقب الجناة بدعم أجهزة الشرطة في تلك الدول.[2] فقد قامت الأنتربول بتبادل بيانات إستخباراتية مع شركة Group-IB وشركة Orange من خلال عملية نورفون Nervone بتعقب عصابة إجرامية معروفة باسم OPERA1ER حيث كانت هذه العصابة تستهدف مؤسسات مالية وخدمات مصرفة نقالة ببرامج خبيثة وحملات تصيد إحتيالي واسعة النطاق بإصدار أوامر زائفة لتحويل الأموال.[3]
- تسهيل التحقيقات المتعلقة بالجرائم السيبرانية التي تجريها الجهات القضائية والأمنية، من خلال تبادل المعلومات، والقيام بالتفتيشات العابرة للحدود لمنظومة الإعلام والإتصال للدول الأعضاء دون مساس بسيادة هذه الدول، بحثا عن الأدلة الرقمية لهذه الجرائم وتعاقب مرتكبيها.[4]
- تدريب وحدات الشرطة للدول الأعظاء على كيفية التحقيق والتحري عن الجريمة ومرتكبيها بإعداد برامج ودورات تدريبية ملتقيات والمؤتمرات وغيرها.[5]

الأهداف المسطرة:

- تعزيز التعاون بين الدول الأعضاء لمحاربة الجرائم السيبرانية وفق الأطر القانونية الوطنية المعتمدة، بما يضمن تكامل الجهود بين سلطات الشرطة الجنائية؛

---

[1] الانتربول، برنامج الإنتربول لدعم الاتحاد الأفريقي فيما يتصل بأفريبول (ISPA)، متوفر على الرابط: https://www.interpol.int/ar/3/Our-partners/3/1 ، أطلع عليه يوم 2025/05/26 على الساعة 09:52

[2] عيسى محمد أحمد سليمان، التعاون الدولي لمواجهة الجرائم الإلكترونية المجلة الأكاديمية للبحث القانوني، العدد 02، 2016، ص 53.

[3] برنامج الإنتربول لدعم الاتحاد الأفريقي فيما يتصل بأفريبول (ISPA)، مرجع سابق.

[4] خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية: دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث، كلية الحقوق والعلوم السياسية، جامعة أدرار، 2021/2020، ص ص 210،211.

[5] عبد النور تمائلي، سعاد قيرة، دور المنظمات الدولية في مكافحة الجريمة المنظمة، (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجا)، مجلة الصراط، العدد 02، 2021، ص 136.

- إنشاء وتطوير المؤسسات المختصة بمكافحة الجرائم السيبرانية، مع التركيز على كشف الجرائم الإلكترونية الدولية التي تستهدف المؤسسات والحد منها عبر آليات تحقيق متقدمة؛
- جمع وتحليل البيانات والمعلومات المتعلقة بالجرائم الإلكترونية ومرتكبيها، من خلال مكاتبها المنتشرة في الدول الأعضاء، مما يتيح تعقب الجناة وإتخاذ الإجراءات القانونية بحقهم.
- تعزيز الأمن السيبراني الدولي، من خلال التنسيق مع الدول الأعضاء لضبط وملاحقة مرتكبي الجرائم الإلكترونية الفارين وتسليمهم وفقاً للطلبات القانونية.[1]
- تنسيق العمل بين المكاتب المركزية الوطنية، التي تلتزم الدول الأعضاء بإنشائها على أراضيها، مما يسهم في توحيد الإستجابة لمكافحة الجريمة السيبرانية العابرة للحدود،
- تطوير وتنمية التعاون الأمني الدولي، من خلال تبادل الخبرات والموارد التقنية، لضمان فعالية المنظومة الأمنية في التصدي للتهديدات السيبرانية المتنامية.[2]

فالمنظمة تسعى جاهدة لتوحيد الجهود مع مختلف الأجهزة الشرطية حول العالم، حيث أطلقت برنامج الأنتربول لدعم الإتحاد الإفريقي فيما يتصل بأفريبول (ISPA) وهو من بين أهم البرامج التي تم أطلاقها بهدف إنماء قدرات أجهزة الشرطة للدول الأعضاء وتحسين أدائهم من خلال الإطلاع على أفضل الممارسات فيما يخص التحقيقات والتحليل الجنائي وتبادل المعلومات وتحقيق الدعم التقني وتوسيع نطاق الوصول إلى منظومتها العالمية للإتصالات الشرطية المأمونة.[3]

الفرع الثاني: هيئات الإتحاد الأوروبي

يعد الإتحاد الأوروبي من أبرز المنظمات الإقليمية، التي نجحت في تحقيق التكامل والاندماج بهدف تعزيز الأمن عبر تبني سياسة أمنية أوروبية مشتركة، فقد كانت معاهدة ماستريخت نقطة الانطلاق الرسمية لهذه السياسة، محددة بذلك أهدافها ومبادئها الأساسية.[4] وقد أنشأ الإتحاد

[1] هشام بشير، مرجع سابق، ص 22.

[2] محمد عبسة، معمر فرقاق، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الجرائم، مجلة القانون، العدد09، ديسمبر 2017، ص 256.

[3] برنامج الانتربول لدعم الاتحاد الأفريقي فيما يتصل بأفريبول (ISPA)، مرجع سابق.

[4] مراد مسعودي، السياسة الأمنية الأوروبية المشتركة: الواقع والتحديات، مجلة صوت القانون، العدد 02 ،2022/03/31، ص627.

الأوروبي لمحاربة الجريمة وتجسيد أهداف و مبادئ الاتفاقية وكالتي الأوروبول والأوروجيست، اللتان تعدان أهم الوكالات التي يعتمد عليها الإتحاد الأروبي لمحاربة الجرائم الإلكترونية.

أولا : وكالة الإتحاد الأوروبي للتعاون في مجال إنفاذ القانون الأوروبول(Europol)

هو جهاز يعمل على مكافحة الجرائم السيبرانية، في كامل إقليم القارة الأوروبية أنشأت الوكالة سنة 2015، وإتخذت مدينة لاهاي بهولاندا مقرا ،حيث تعد كمركز عمليات تعمل على التنسيق الأمني، و تبادل المعلومات، بين وحدات الشرطة للدول الأعضاء في الإتحاد الأوروبي فيما بينهم، وحتى مع الدول المجاورة له.[1] وتتمثل مهام الوكالة فيما يلي:

- مكافحة الجرائم الإلكترونية عبر تحليل البيانات والإستخبارات، وتوفير التدريب والتنسيق بين الجهات الوطنية، مما يعزز التعاون الأوروبي في هذا المجال؛
- جمع المعلومات الإستخباراتية حول الإحتيال الذي تتعرض له المؤسسات على الإنترنت ودعم التحقيقات عبر توفير الأدلة الرقمية وتحليلها بإستخدام تقنيات متطورة،
- التنبؤ بالهجمات المستقبلية وتحليل أنماط سلوك المجرمين الإلكترونيين من خلال الذكاء الإصطناعي وخوارزميات التعلم الآلي.
- دعم التحقيقات في الجرائم السيبرانية وتسهيل الإجراءات القانونية ضد المجرمين الرقميين.

منذ إنشاء مركز الجرائم الإلكترونية الأوروبي (EC3) عام 2013، عزز يوروبول إستجابته لتهديدات الإحتيال الإلكتروني على المؤسسات، وساهم في عمليات بارزة تضمنت الإعتقالات وتحليل الملفات الضارة، مما يجعله أحد الأعمدة الأساسية في حماية النظم الرقمية داخل الاتحاد الأوروبي.[2]

---

[1] آسيا لعمراني ، مرجع سابق، ص 86.

[2] محمد تذير بن عريفة، يوسف حوري، اليوروبول كآلية لمكافحة الجريمة الإلكترونية، مجلة الدراسات القانونية والسياسية، العدد 01 ،2025، ص41.

- دعم وتشجيع سلطات التحقيق، وذلك بتكميل وسائلهم، وتحديثاتها من أجل مكافحة جميع أنواع الإجرام السيبراني.[1]

ثانيا: وكالة الإتحاد الأوروبي للتعاون في مجال العدالة الجنائية الأوروجيست (Eurojust)

تلعب الوكالة هي الأخرى دورًا هاما في مكافحة الجريمة الإلكترونية، تأسست عام 2002 بهدف تعزيز التعاون القضائي بين الدول الأعضاء في الإتحاد الأوروبي. ينعقد إختصاصها عندما تمتد الجريمة عبر دولتين أو أكثر داخل الإتحاد الأوروبي، أو عندما تشمل دولة عضو ودولة من العالم الثالث، أو دولة عضو ودولة من الرابطة الأوروبية[2]. حيث تعمل الوكالة على:

- تعزيز التنسيق والتعاون القضائي بين الدول الأعضاء في الاتحاد الأوروبي؛
- تسهيل تنفيذ طلبات التعاون القضائي والقرارات المتعلقة بالتحقيقات؛
- تساهم في دعم التحقيقات المتعلقة بالاحتيال الإلكتروني عبر إتخاذ تدابير قانونية خاصة وتشكيل فرق تحقيق مشتركة لملاحقة الجناة عبر الحدود؛
- إعداد تحليلات قانونية حول الجرائم الإلكترونية بالتعاون مع اليوروبول ومكتب المدعي العام الأوروبي، ويعقد إجتماعات دولية لمناقشة التهديدات السيبرانية، مثل الإحتيال المالي
- يساهم الأوروجيست في تذليل الصعوبات الإجرائية التي تواجه الدول الأعضاء، لضمان إستجابة قانونية فعالة ضد الجرائم الإلكترونية، لاسيما تلك التي تستهدف المؤسسات مما يعزز الأمن السيبراني الأوروبي[3].

يسعى الاتحاد الأوروبي من خلال هيئاته إلى تجسيد سياسة أمنية أوروبية موحدة، من خلال تعزيز تنسيق الجهود سواء مع الدول الأعضاء، أو الدول الأخرى، بهدف حماية المؤسسات من الجرائم الإلكترونية بما فيها الإحتيال الإلكتروني.

---

[1] هشام بشير، مرجع سابق، ص 23

[2] هشام بشير، المرجع نفسه، ص 23.

[3] خضرة شنتير، مرجع سابق، ص 253.

الفرع الثالث: الإتحاد الإفريقي للتعاون الشرطي(الأفريبول)

هو آلية إقليمية أمنية أنشأت سنة 2017، وتعتبر أكبر منظمة شرطية في إفريقيا، تتكون من قوات الشرطة لـــ(41) دولة، مقرها الجزائر العاصمة، حيث تعد أداة تعاون إقليمية، لمحاربة الجرائم التي تهدد أمن القارة، بما فيها الأمن السيبراني .[1]

يهدف الاتحاد الإفريقي للتعاون الشرطي "أفريبول "إلى تعزيز التعاون بين مؤسسات الشرطة في الدول الأعضاء على مختلف المستويات الوطنية والإقليمية والقارية والدولية، بما يضمن تكامل الجهود الأمنية في مكافحة الجريمة، كما يسعى إلى تطوير قدرات أجهزة الشرطة عبر برامج تدريب متخصصة، وإنشاء مراكز إمتياز إفريقية لتأهيل الكوادر الشرطية وتحديث أساليب التحقيق، إضافة إلى ذلك، يعمل "أفريبول" على دعم إستراتيجية منع ومكافحة الجريمة من خلال تعزيز التنسيق بين الهياكل والمؤسسات الأمنية المماثلة، لضمان إستجابة فعالة للتهديدات الأمنية، وفي إطار حماية الأمن السيبراني، يسعى الإتحاد إلى إعداد إستراتيجية إفريقية متكاملة لمكافحة الجرائم الخطيرة، بما في ذلك الجريمة الإلكترونية والجرائم المنظمة العابرة للحدود، لضمان بيئة رقمية آمنة ومستقرة داخل الدول الأعضاء.[2]

تضطلع آلية الإتحاد الإفريقي للتعاون الشرطي "أفريبول "بعدد من المهام الأساسية في مجال مكافحة الجرائم الإلكترونية:

- المتابعة والتحقيق في الجرائم السيبرانية، مثل القرصنة والتجسس الإلكتروني، مع تطوير إستراتيجيات ردع عبر وحدات متخصصة في التصدي لهذه التهديدات؛
- تنسّق الجهود الإقليمية والدولية لضمان تسليم المجرمين، وفقًا للإتفاقيات القانونية المعتمدة. وفي إطار تعزيز الأمن السيبراني؛

[1] أسيا لعمراني، مرجع سابق، ص 87.

[2] خديجة خالدي، آلية الإتحاد الإفريقي للتعاون الشرطي "أفريبول"، مجلة العلوم الإجتماعية والإنسانية، العدد 15، 2018، ص 69.

- في تطبيق إتفاقية الإتحاد الإفريقي بشـــأن أمن الفضـــاء الإلكتروني وحماية البيانات الشـخصـية، وتحليل الهجمات السـيبرانية التي تسـتهدف الأنظمة المعلوماتية، بما في ذلك عمليات الإحتيال الإلكتروني الذي تتعرض له المؤسسات؛
- تطوير تقنيات رقابية وقائية، وإعتماد سياسات أمنية تهدف إلى حماية البنية التحتية الرقمية للدول الإفريقية من الإختراقات والهجمات السيبرانية العابرة للحدود.[1]
- تعزيز التعاون بين أجهزة الشـرطة في الدول الأعضـاء على مختلف المسـتويات، بما يضـمن تطوير القدرات الأمنية عبر برامج تدريب متقدمة وإنشاء مراكز إمتياز إفريقية؛
- دعم الجهود الرامية إلى مكافحة الجرائم الإلكترونية، خاصـــة الاحتيال الإلكتروني، من خلال تبادل المعلومات الاستخباراتية وتعزيز التنسيق بين الجهات الأمنية المختصة؛
- تسـهيل المسـاعدة القانونية المتبادلة، لا سـيما في ملاحقة مرتكبي هذه الجرائم وتسـليمهم وفق الأطر القانونية الدولية؛
- تطوير أنظمة الإتصـال وقواعد البيانات لضـمان إسـتجابة فعالة لمكافحة الجريمة السـيبرانية على مســـتوى القارة[2]. حيث تم إقامة مركز بيانات على مســـتوى مقر الأفريبول، لتعزيز إمكانية تبادل المعلومات عبر المنظومة الإفريقية للإتصالات الشرطية(AFSECOM). [3]

المبحث الثاني: الآليات القانونية والمؤسـساتية الوطنية لحماية المؤسـسـات من الإحتيال الإلكتروني

أصـبحت أغلب المؤسـسـات تعتمد على أجهزة الاعلام الآلي، وشـبكة الأنترنت لما توفره لها من ســـرعة في إنجاز مهامها، وربطها بعملائها، غير أن هذا التطور الحاصـــل في مجال تكنولوجيا

[1] عبد العزيز لزعر، رشـيد زياني، آلية الإتحاد الإفريقي للتعاون الشـرطي "أفريبول" ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، العدد 03، 2021/09/15، ص 263-265.

[2] خضرة شنتير، مرجع سابق، ص 246.

[3] الانتربول، برنامج الإنتربول لدعم الاتحاد الأفريقي فيما يتصل بأفريبول (ISPA)، مرجع سابق.

الإعلام والإتصال أدى إلى تطور الجريمة المعلوماتية، ومنها جريمة الإحتيال الإلكتروني الموجهة ضد المؤسسات.

الأمر الذي دفع المشرّع الجزائري يواكب التطورات الحاصلة في هذا المجال، والسعي لمواجهة هذه الظاهرة عبر تجريم الإحتيال الإلكتروني، وذلك بتعديل القواعد القانونية العامة والإجرائية من جهة، وإستحداث قوانين خاصة من جهة أخرى، إضافة إلى إنشاء آليات مؤسساتية لإنفاذ هذه القوانين، ولمناقشة ذلك قسمنا هذا المبحث إلى مطلبين، تضمن المطلب الأول حماية المؤسسات بموجب القوانين العامة و الخاصة الوطنية، في حين تطرق المطلب الثاني إلى الهيئات الوطنية التقليدية والحديثة لمكافحة الإحتيال الإلكتروني.

المطلب الأول: حماية المؤسسات بموجب القوانين العامة والخاصة

أصدر المشرع الجزائري مجموعة من الأحكام التشريعية العامة، والخاصة بهدف التصدي لجرائم الإحتيال الإلكتروني، وعززها بمؤسسات لتطبيق هذه القوانين وللحد من الإنتشار الواسع لهذا النوع من الجرائم، بعد أن تحولت إلى هاجس يؤرق المؤسسات، وهو ما سوف نتطرق اليه من خلال هذا المطلب.

الفرع الأول: القوانين العامة

قام المشرع الجزائري بتعديل القوانين العامة لجعلها هي الأخرى تواكب التطورات التي تشهدها الجريمة الإلكترونية حيث سنتطرق في هذا الفرع إلى كل من قانو العقوبات و قانون الإجراءات الجزائية.

أولا قانون العقوبات

يعتبر قانون العقوبات الأساس الذي تبنى عليه مختلف القوانين التي تكتسي الطابع الجنائي فبموجبه توضع المبادئ العامة التي تنظم الجرائم والعقوبات، كمبدأ الشرعية، وعدم رجعية القوانين وعليه فقد جرّم المشرع الجزائري الإحتيال الإلكتروني، قصد حماية الأشخاص سواء الطبيعيين

أو المعنويين، وتعتبر المؤسسات أحد هذه الأشخاص المعنية بالحماية، وفي هذا الإطار. فقد إشتمل قانون العقوبات نصوصا عامة يمكن تطبيقها على بعض صور الإحتيال الإلكتروني.[1]

إستحدث المشرع الجزائري موادا تتعلق بالجرائم الإلكترونية بموجب القانون 15/04[2] المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري في قسمه السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات المتضمنة ثمانية مواد من (394) مكرر الى (394) مكرر7، حيث أقرّ فيها المشرع على عقوبة الحبس لمدة أدناها شهرين، وأقصاها ثلاث سنوات، بالإضافة إلى غرامة مالية من 50.000دج الى5.000.000 دج و تضاعف العقوبة إذا إستهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد.

ويمكن تصنيف هذه الجرائم إلى :[3]

- الغش أو الشروع فيه في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات؛
- حذف أو تغيير لمعطيات المنظمة؛
- إدخال أو تعديل في نظام المعطيات؛
- تصميم أو بحث أو تجميع أو توفير أو نشر أو إتجار؛
- حيازة أو إفشاء أو نشر أو إستعمال المعطيات؛
- تكوين جمعية أشرار وعليه يمكن تكييف هذه الأفعال الإجرامية بأنها جرائم ضد أموال الغير والمضرة بالمجتمع.

[1] عبد اللطيف جمل، عبد الغاني طرايش، الحماية الجنائية للمستهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري: دراسة تحليلية ومقارنة على ضوء القانون الفرنسي، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد 01، 2025/03/20، ص 1385.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004 ، يعدل و يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.المواد 394مكرر-394 مكرر7.

[3] راضية عيمور، الجريمة الإلكترونية وآلية مكافحتها، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد الأول، 2022/03/31، ص 105.

ليقوم المشرع بتعديله مرة أخرى بموجب القانون 16-02[1]حيث تم إدراج ثلاث مواد جديدة بهدف تعزيز الإطار القانوني، وتحديث الأحكام بما يتماشى مع المستجدات والتطورات الحديثة حيث تم إستحداث المادتين (87) مكرر 11 [2]ومكرر 12[3] في القسم الرابع مكرر1 المتعلق بالجرائم الموصوفة بأفعال إرهابية أو تخريبية، حيث تضمنتا المعاقبة بالسجن لمدة تتراوح بين خمس (05) وعشر سنوات (10) وبغرامية مالية من (100.000 دج) الى (500.000دج)، كل من يقوم بأعمال إرهابية، أو يساهم فيها، في الخارج بطريقة مباشرة أو غير مباشرة لإرتكابها، سواء بطريقة كلاسيكية، أو بإستخدام تكنولوجيا الإعلام والإتصال، ولكل من يستخدم هذه الأخيرة لتجنيد الأشخاص لصالح الأعمال الإرهابية أو نشر أفكارها بطريقة مباشرة أو غير مباشرة. في حين تضمنت المادة (394) مكرر8 [4] إضافة الى العقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول يعاقب بالحبس من سنة (01) الى ثلاث (03) سنوات وبغرامة مالية من (2.000.000دج) الى (10.000.000دج) أو بإحدى العقوبتين، مزودي خدمة الأنترنت الذين لا يمتثلون لأوامر السلطات المختصة فيما يخص إزالة أو حجب المحتويات، أو وضع ترتيبات تقنية تسمح بسحب، أو تخزين المحتويات التي تشكل جرائم منصوص عليها.

يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث من الجرائم بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى[5]. غير أن الأحكام العامة تطرح تحديًا عند تطبيقها على الجرائم الإلكترونية التي تتعرض لها المؤسسات، فالمادة (372) من قانون العقوبات تنص على تجريم فعل النصب كجريمة كلاسيكية، وتعاقب عليه بالحبس من سنة(01) إلى عشر (10) سنوات وبغرامة من 500دج الى 200.000دج، كما يجوز الحرمان من الحقوق الوطنية والمدنية، والعائلية

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 16-02 المؤرخ في 19 يونيو 2016 يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 37 الصادرة بتاريخ 22 يونيو 2016.

[2] القانون رقم 16-02، المرجع نفسه، المادة (87) مكرر11

[3] القانون رقم 16-02، المرجع نفسه، المادة (87) مكرر 12

[4] القانون رقم 16-02، المرجع نفسه، المادة (394) مكرر 8

[5] راضية عيمور، مرجع سابق، ص 96.

لمدة لا تتجاوز خمس (5) سنوات. ونكون أمام جريمة نصب وإحتيال عندما يتم الإستيلاء على أموال أو ممتلكات الغير عن طريق وسائل إحتيالية، مثل إنتحال هوية أو صفة غير صحيحة، أو خداع الضحية بوجود مشروع غير حقيقي، أو سلطة خيالية.[1]

تأسيسا بمقتضيات تطبيق هذه المادة يستلزم تحليل العناصر المكونة للجريمة على الإحتيال الإلكتروني وهي:[2]

1- الركن المادي: يتمثل في فعل الإستلاء على مال الغير (أو أي من العناصر المذكورة في المادة 372) بإستعمال طرق إحتيالية.

2- الركن المعنوي: تفترض جريمة النصب توافر القصد الجنائي بعنصريه، العام، والخاص فبالنسبة للقصد العام فيتجلى في إنصراف إرادة المتهم إلى تحقيق الجريمة بأركانها الكاملة كما حددها القانون وهو عالم بذلك، في حين يتمثل القصد الخاص في نية المتهم في الإستلاء على مال الغير، وتنتفي الجريمة في ركنها المعنوي إذا كان الغرض من الفعل الإحتيالي مجرد المزاح أو المداعبة، أو تحقيق منفعة عابرة.[3]

وقد حددت المادة (372) الطرق الإحتيالية على النحو التالي:[4]

- بإستعمال أسماء أو صفات كاذبة؛
- بإستعمال سلطة أو إعتماد مالي خيالي؛
- إعطاء الأمل بالفوز بأي شيء، أو حدوث واقعة ما أو خشية وقوعها.

يثير تطبيق هذه المادة على وقائع الإحتيال الإلكتروني إشكالية حول مفهوم الطرق الإحتيالية في الفضاء الرقمي. ويتجلى السؤال في مدى إعتبار إنشاء موقع إلكتروني وهمي لبيع

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم، المادة 372.

[2] عبد اللطيف جمل، عبد الغاني طرايش، مرجع سابق، ص 1389.

[3] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الجزائر: دار هومة،2007، ص 327.

[4] القانون رقم 66-156، مرجع سابق، المادة 372.

سلع غير موجودة نصبا؟ وما إذا كان إرسال رسائل التصيد الإحتيالي (Phishing) للحصول على بيانات بنكية يشكل فعلا من أفعال النصب المعاقب عليها قانونيا؟.[1]

لذلك، يتطلب تطبيق هذه العناصر على الإحتيال الإلكتروني تفسيرا واسعا لمفهوم "الطرق الإحتيالية"، بحيث يشمل الأساليب التي يستخدمها المحتالون في الفضاء الرقمي، حيث نجد أن الإجتهاد القضائي الجزائري في هذا المجال لا يزال لم يبلور بعد تفسيرا واضحا لمفهوم "الطرق الإحتيالية" في سياق الجرائم الإلكترونية. ومع ذلك يمكن القول بأن العديد من صور الإحتيال الإلكتروني يمكن أن تندرج تحت مفهوم النصب، متى توافرت أركانه. [2]

فالمشرع أبدى نيته من خلال تحيينه للقوانين، تعديلها وصياغتها لتتماشى ومقتضيات التطور التكنولوجي لحماية المؤسسات. فعلى سبيل المثال قبل تعديل قانون العقوبات سنة 2016 تبنى رؤية تهدف إلى تجريم أفعال توصف في ظاهرها بالإرهاب، مستخدما في ذلك عبارات ذات دلالة شمولية آنذاك، مما أتاح المجال لإستيعاب وسائل جديدة قد تستعمل في إرتكاب مثل هذه الجرائم مستقبلا، مثلما كان يستعمل عبارات مثل (بأي وسيلة كانت) أو (بأي طريقة)... إلا أنه وتكريسا لمبدأ الشرعية، وتجاوزا لإشكالية إصطدام القضاء بقاعدة عدم جواز القياس في المواد الجزائية من جهة، ومن جهة أخرى تحقيقا للتوافق مع نص المادة 15 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تجرم الأفعال المرتبطة بالإرهاب والمرتكبة بواسطة التقنية، عمد المشرع الجزائري إلى تعديل قانون العقوبات لسنة 2016 بإضافة المادتين 87 مكرر11 و 87 مكرر12 بهدف إدراج كل الأفعال المرتبطة بالإرهاب المرتكبة بواسطة تكنولوجيا الإعلام والإتصال، تجسيدا لمبدأ الشرعية الجنائية المنصوص عليها في المادة الأولى من قانون العقوبات."[3]

---

[1] عبد اللطيف جمل، عبد الغاني طرايش، مرجع سابق، ص 1385.

[2] عبد اللطيف جمل، عبد الغاني طرايش، المرجع نفسه، ص 1389.

[3] عبد النور بشان، الإرهاب المعلوماتي في ضوء قانون العقوبات الجزائري، مجلة صوت القانون، العدد01، 2021/11/30، ص961.

ثانيا: قانون الإجراءات الجزائية

بإعتبار أن قانون الإجراءات الجزائية هو مجموعة القواعد القانونية التي تنظم كيفية تطبيق العدالة الجنائية، بدءً من التحقيق في الجرائم، وجمع الأدلة، وتحديد إختصاص الجهات القضائية وصولًا إلى المحاكمة وإصدار الأحكام وتنفيذها، بحيث يهدف هذا القانون إلى ضمان تحقيق العدالة، وفقا للإجراءات القانونية السليمة، مع حماية حقوق المتهمين والضحايا لذا وجب على المشرع أن يحيّنه هو الآخر، ويعدل نصوصه القانونية لضمان توافقها مع الأحكام التشريعية الواردة في القوانين الأخرى، فقد عدّل في نص المادة (37) من قانون الإجراءات الجزائية[1] حيث منح المشرع لوكيل الجمهورية صلاحية تمديد الإختصاص في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما تضمن التعديل الجديد للمادة (45)[2]، وبالتحديد في فقرتها السابعة إستثناء هذا النوع من الجرائم من إجراءات التفتيش المنصوص عليها في نفس المادة، وذلك مراعاة لما تتسم به هذه الجرائم من خصوصية، فهي تختلف عن الإجراءات الشكلية والموضوعية المطبقة في الجرائم الكلاسيكية لكونها تحتاج إلى قواعد خاصة، كما تم تعديل المادة (51)[3] حيث تم النص في فقرتها السادسة، على إمكانية تمديد أجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية، المختص مرة واحدة إذا تعلق الأمر بهذا النوع من الجرائم.

كما قام المشرّع بتتمة الباب الثاني من الكتاب الأول من قانون الإجراءات الجزائية بالقانون 06-22[4] وذلك بالفصل الرابع بعنوان في إعتراض المراسلات، وتسجيل الأصوات وإلتقاط الصور، حيث نصت المادة (65) مكرر 5 منه على أنه إذا إقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الإبتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 ، المؤرخ في 8 يونيو 1966 ، المتضمن قانون الإجراءات الجزائية المعدل و المتمم، المادة (37).

[2] الأمر رقم 66-155، المرجع نفسه المادة (45)

[3] الأمر رقم 66-155، المرجع نفسه، المادة (51).

[4] الجمهورية الجزائرية الديمقراطية الشعبية القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84 الصادرة بتاريخ 24 ديسمبر 2006.

يجوز لوكيل الجمهورية المختص أن يأذن بإعتراض المراسلات التي تتم عن طريق الوسائل السلكية واللاسلكية، ووضع الترتيبات التقنية دون موافقة المعنيين لإلتقاط الصور، وتسجيل الأصوات في أماكن خاصة أو عمومية. [1]

تخوّل هذه المادة لسلطات التحقيق والإستدلال في حال التلبس بجريمة، أو عند التحقيق في جريمة إلكترونية، صلاحيات اللجوء إلى إجراءات خاصة تتضمن إعتراض المراسلات السلكية واللاسلكية، وتسجيل المحادثات، والأصوات، وإلتقاط الصور، والإستعانة بكل الترتيبات التقنية اللازمة، وذلك بهدف تسهيل الكشف عن ملابسات الجريمة، وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة. ومع هذا فإن المشرع الجزائري لم يمنح هذا الحق بشكل مطلق، بل أقّر له ضمانات قانونية تحد من تعسف سلطات الإستدلال والتحري، وتصون الحقوق، والحريات العامة والحياة الخاصة للأفراد.[2]

الفرع الثاني: القوانين الخاصة

إن إستفحال جريمة الإحتيال الإلكتروني، وإستهدافها للمؤسسات دفع بالمشرع الجزائري إلى سن قوانين جديدة لحمايتها من هذه الجرائم، حيث أصدر عدة قوانين نذكر منها:

أولا: القانون رقم 18-04 المتعلق بالبريد والإتصالات الإلكترونية

في ظل التطورات التكنولوجية الراهنة، ومع تطور وسائل الإتصال قام المشرع الجزائري بإلغاء القانون رقم 2000-03[3] المتعلق بالبريد والمواصلات السلكية واللاسلكية، بموجب القانون رقم 18-04[4] المحدد للقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، وقد

---

[1] القانون رقم 06-22، المرجع نفسه، المادة (65) مكرر6.

[2] إسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية العدد 11، سبتمبر 2018، ص 364.

[3] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 2000-03 مؤرخ في 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمراسلات السلكية والاسلكية، الجريدة الرسمية، عدد 48، الصادرة بتاريخ 06 غشت 2000.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 18-04 مؤرخ في 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية ، الجريدة الرسمية، عدد 27، الصادرة بتاريخ 13 مايو 2018.

حرص على أن تكون الدولة المسؤول الأول عن أمن وسلامة شبكات الإتصال الإلكترونية حيث تضمنت المادة (04)[1] منه على سهر الدولة في إطار صلاحياتها على أمن وسلامة شبكات الإتصالات الإلكترونية، خاصة في ظل دخول نمط جديد من التحويلات المالية، ألا وهي التحويل عن طريق الإتصالات الإلكترونية، وقد نص عليها المشرع في المادة (60)[2] " يمكن أن ترسل الأموال...أو عن طريق الإتصالات الإلكترونية"، لينص في الباب المتعلق بالأحكامه الجزائية على مجموعة من العقوبات حيث نصت المادة (164)[3] على الحبس من سنة (1) إلى خمس (5) سنوات و بغرامة من 500.000دج إلى 1.000.000دج كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الإتصالات الإلكترونية أو يفشي مضمونها، أو بنشره، أو يستعمله دون ترخيص من المرسل أو المرسل إليه، أو يخبر بوجودها. أما المادة (165)[4] في فقرته الثانية فقد نصت على الحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج أو بإحدى هاتين العقوبتين، كل متعامل للإتصالات الإلكترونية، يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الإتصالات الإلكترونية، أو أمر أو ساعد في إرتكاب هذه الأفعال، و يمكن الحكم بواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة (9)[5] من قانون العقوبات. لتتضمن المادة (166)[6] في فقرته الثانية أيضا الحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 500.000دج إلى 1.000.000دج أو بإحدى العقوبتين، كل شخص مستخدم لدى متعامل الإتصالات الإلكترونية، يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الإتصلات الإلكترونية، أو أمر أو ساعد

[1] قانون رقم 18-04، مرجع سابق، المادة 04.
[2] قانون رقم 18-04، المرجع نفسه، المادة 60.
[3] قانون رقم 18-04، المرجع نفسه، المادة 164.
[4] قانون رقم 18-04، المرجع نفسه، المادة 165.
[5] القانون رقم 66-156، مرجع سابق، المادة 09.
[6] قانون رقم 18-04، مرجع سابق، المادة 166.

في إرتكاب هذه الأفعال. وبعاقب كل شخص غير الأشخاص المذكورين في المادتين (165)و(166) أرتكب أحد الأفعال المذكورة في المادتين السابقتين، بالحبس من شهرين (2) إلى سنة (1) و بغرامة من 200.000دج إلى 500.000دج حسب المادة (167)[1]. و قد حاول المشرع من خلال النص على هذه الأحكام الجزائية، خلق فضاء آمن، خاصة لنشاط المؤسسات كونها المستهدف الأول من خلال عمليات الإحتيال الإلكتروني، فشبكات الإتصالات الإلكترونية تعد البيئة الخصبة لتنفيذ المجرمين لعملياتهم الإحتيالية، فأغلب معاملات المؤسسات تقوم على شبكات الإتصال الإلكترونية.

ثانيا: القانون رقم 08-01 المتعلق بالتأمينات الإجتماعية

نص المشرع على هذا القانون ليتمم به القانون 83-11[2]بعد أن إعتمد قطاع التأمينات الإجتماعية وسيلة البطاقات والمفاتيح الإلكترونية في معاملتها مع المؤمنين لهم إجتماعيا، حيث عرف قطاع الضمان الإجتماعي تحولا رقميا في إطار عصرنة هذا القطاع، مواكبة لمستجدات الإدارة الإلكترونية، والإنتقال للهوية الرقمية بدلا من التعامل بالهوية المتعارف عليها تقليديا وفق ما أقرته الدولة، وسعت لتطبيقه وزارة العمل والتشغيل والضمان الإجتماعي.[3]

لذلك تطرق هذا القانون إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الإجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج، وهي صالحة في كامل التراب الوطني، وكذلك للجزاءات المقررة في حالة الإستعمال غير المشروع.[4]

---

[1] قانون رقم 18-04، مرجع سابق، المادة 167.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، قانون 83-11 مؤرخ في 2 يوليو سنة 1983، المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، عدد 28، الصادرة بتاريخ 5 يوليو 1983 .

[3] سعاد بن خذير، ميمونة قويدر، الحماية القانونية للهوية الرقمية للمؤمن له اجتماعيا في إطار رقمنة خدمات الضمان الاجتماعي – بطاقة الشفاء نموذجا-، مجلة البحوث في الحقوق و العلوم السياسية العدد 03، 2025/04/22، ص 300.

[4] فضيلة عاقلي، مرجع سابق، ص 132.

فقد إستحدث المشرع عن طريق القانون 08-01[1] باب خامس متعلق بالأحكام الجزائية، حيث نصت المادة (93) مكرر3 على معاقبة كل من يقوم عن طريق الغش، بتعديل أوحذف كلي أو جزئي للمعطيات التقنية و/أو الإدارية المدرجة في البطاقة الإلكترونية، للمؤمن له إجتماعيا، أو المفتاح الإلكتروني لهيكل العلاج، أو لمهني الصحة، أو القيام بإعداد أو تعديل أو نسخ بطريقة غير مشروعة، البرمجيات التي تسمح بالوصول وإستعمال المعطيات المدرجة عليها، بعقوبة الحبس من (2) سنتين إلى (5) سنوات وبغرامة مالية من 500.000 دج الى 1.000.000 دج، كما تعاقب المحاولة فيها أيضا بنفس العقوبة. [2]

أما المادة (93) مكرر4 فقد نصت على تجريم كل نسخ أو صنع او حيازة أو توزع بطريقة غير مشروعة للبطاقة الإلكترونية للمؤمن له إجتماعيا أو المفاتيح الإلكترونية لهيكل العلاج أو لمهني الصحة بعقوبة الحبس من (2) سنتين إلى (5) سنوات و بغرامة مالية من 500.000 دج إلى 5.000.000 دج دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به[3]. لينص المشرع في المادة (93) مكرر5 ،على معاقبة كل شخص، معنوي يرتكب الجنح المذكورة في المادتين سالفتي الذكر، بغرامة تساوي خمس أضعاف المبلغ الأقصى للغرامة المقررة للشخص الطبيعي.[4] في حين أن المادة (93) مكرر 6 [5] تتضمن مصادرة الأجهزة والوسائل المستعملة، و كذلك غلق أماكن الإستغلال التي تكون محل الجنح المنصوصة في المواد 93 مكرر3و مكرر4 في حالة ما إذا كان مالكها على علم بذلك مع عدم الإخلال بحقوق الغير حسن النية.

وعليه، فإن هذا القانون يعزز من مصداقية أنظمة الضمان الإجتماعي، من خلال ضمان إستخدامها وفق إطار قانوني واضح، مما يرسخ الثقة في العمليات الرقمية ويؤمن البيانات ضد أي إستغلال غير مشروع.

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 08-01 مؤرخ في 23 يناير سنة 2008، المتعلق بالتأمينات الاجتماعية، ج ر، عدد 04، الصادرة بتاريخ 27 يناير 2008 .

[2] القانون رقم 08-01 ، المرجع نفسه، المادة (93) مكرر3.

[3] القانون رقم 08-01، المرجع نفسه، المادة (93) مكرر4.

[4] القانون رقم 08-01 ،المرجع نفسه، المادة (93) مكرر5.

[5] القانون رقم 08-01، المرجع نفسه، المادة (93) مكرر6.

ثالثا: القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

أصدر المشرع هذا القانون بهدف مكافحة الجرائم الإلكترونية، حيث خصه حصريًا بهذا النوع من الجرائم نظرًا لطبيعتها الإجرائية التي تختلف عن باقي الجرائم، ويأتي هذا الإطار القانوني إستجابةً للتحديات المتزايدة التي تفرضها الجرائم المعلوماتية.

تتجلى أهمية هذا القانون في جمعه بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية، وبين القواعد الوقائية التي تتيح إمكانية الرصد المبكر للاعتداءات المحتملة، والتدخل السريع لتحديد مصدرها وكشف هوية مرتكبيها، كما أنه جرّم الأفعال المخالفة للقانون، والتي ترتكب عبر وسائل الإتصال عامة، ما يجعله قابلا للتطبيق على جميع التكنولوجيات الجديدة والقديمة بما في ذلك شبكة الأنترنت، وعلى كل تقنية تظهر مستقبلا.[1] وهي كما يلي:

1- التدابير الوقائية

نص القانون 04/09 على مجموعة من التدابير الوقائية التي يتم إتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع الجرائم معلوماتية، أو الكشف عنها، وعن مرتكبيها في وقت مبكر. وهي كالتالي:[2]

- مراقبة الاتصالات الإلكترونية التي نصت عليها المادة (04) من القانون 09-04؛
- إقحام مزودي خدمات الإتصالات الإلكترونية في مسار الوقاية من الجرائم الإلكترونية من خلال فرض مجموعة من الالتزامات المذكورة في المواد 10، 11و12 من نفس القانون أعلاه.

أ- فالمادة (10) تنص على إلزام مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها، ووضعها تحت تصرف المحققين، وكتمان سرية العمليات

[1] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد الثاني، سنة 2015، ص 18.

[2] راضية عيمور، مرجع سابق، ص 105.

التي ينجزونها بطلب منهم، وكذا المعلومات المتصـــلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.[1]

ب- كما تضمنت **المادة (11)** إلتزام مقدمي الخدمات بحفظ: [2]

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة؛
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال؛
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال؛
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها؛
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها.
- تحدد مدة الحفظ المعطيات المذكورة في المادة بسنة واحدة ابتداءً من تاريخ التسجيل.

أما **المادة (12)** فتنص على: [(3)]

- التدخل الفوري لســـحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة او غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن؛
- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالف للنظام العام وإخبار المشتركين لديهم بوجودها.

2- التدابير الإجرائية

تبنى المشـــرع إجراءات جديدة تدعم تلك المنصـــوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجيا الإعلام والإتصال، تتلخص فيما يلي: [4]

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 مؤرخ في 5 غشت سنة 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، الصادرة بتاريخ 16 غشت 2009 ، المادة 10.

[2] القانون رقم 09-04، المرجع نفسه، المادة 11.

[3] القانون رقم 09-04، مرجع سابق، المادة 12.

[4] راضية عيمور، مرجع سابق، ص 105.

– السماح للجهات القضائية المختصة وضباط الشرطة بالدخول لغرض التفتيش ولو عن بعد للمنظومة المعلوماتية، أو جزء منها، والمعطيات المعلوماتية المخزنة فيها وإستنساخها مع إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى، والتي يمكن التوصل إليها بواسطة المنظومة الأصلية، بشرط إخطار السلطات المختصة مسبقا.

– إمكانية الإستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل بحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للإتفاقيات الدولية ومبدأ المعاملة بالمثل.

3– العقوبات

تم النص في المادة (11) الفقرة 9 على العقوبات المقررة لمقدمي الخدمات في حالة عدم تقيدهم بالإلتزامات المنصوص عليها في هذا القانون، وذلك دون الإخلال بالعقوبات الإدارية المترتبة على ذلك، والمتمثلة في: [1]

- الحبس من ستة (06) أشهر الى خمس (05) سنوات بالنسبة للشخص الطبيعي، وبغرامة مالية من50.000دج الى 500.000دج؛
- يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

يمثل النص على هذا القانون خطوة نوعية، اتخذها المشرّع الجزائري في إطار تعزيز التدابير الوقائية ضد المخاطر الناجمة عن إستخدام تكنولوجيا الإعلام والإتصال، فهو يهدف إلى الحد من الإحتيال الإلكتروني الذي تتعرض له المؤسسات، مما يسهم في توفير بيئة قانونية أكثر أمانًا وتنظيمًا لهذا المجال المتنامي.

رابعا: القانون 15–03 المتعلق بعصرنة العدالة

فقد تناول هذا القانون، المنظومة المعلوماتية المركزية لوزارة العدل، والتصديق الإلكتروني وتأمينه من طرفها، إضافة إلى إرسال الوثائق، والإجراءات القضائية بالطريق الالكتروني والكيفيات، والمصاريف كما تطرق إلى الأحكام الجزائية.[2]

---

[1] القانون رقم 09–04، مرجع سابق، المادة (10).

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 15–03 مؤرخ في 01 فبراير سنة 2015، المتعلق بعصرنة العدالة، الجريدة الرسمية، عدد06، الصادرة بتاريخ 10 فبراير2015.

حيث تضـــمنت المادة (17)، على معاقبة كل شـــخص، يســـتعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر، أما المادة (18) فتنص على معاقبة كل شـــخص حائز شـــهادة إلكترونية يواصـــل إســـتعمالها رغم علمه بإنتهاء صـــلاحيتها، أو إلغائها حيث تنص المادتان على عقوبة الحبس من ســـنة (1) إلى خمس (5) سنوات وغرامة مالية تتراوح بين 100.000دج الى 500.000دج.[1]

لينص المشـــرع على الأمر 21-09[2] المتعلق بحماية المعلومات، والوثائق المصـــنفة. فهي المحرك الأســـاســـي والحيوي، والســـبيل الوحيد التي تســـلكه الدولة، ومؤســـســـاتها للقيام بمهامها وتجســـدها على أرض الواقع، وهي في ذلك تتوصـــل إلى معلومات وتحرر وثائق تتســـم بالســـرية والأهمية، فهي تعبر عن مبدأ السـيادة، الذي يقضـي أن يبقى التعامل فيها وتداولها تحت سـلطة المؤسسة المعنية بها، وتحت إشرافها وبترخيص منها، وأي خروج عن ذلك يشكل إنتهاكا خطيرا لحرمة هذه المعلومات، والوثائق ومساسا بهيبة الدولة وبمؤسساتها.[3]

بالمقابل، أدى تبني مبدأ الرقمنة في كل المؤســـســـات، وضـــرورة إســـتعمال وســـائل الإعلام والاتصـــال في تحرير الوثائق الإدارية، وتخزينها وتبادلها فيما بينها، جعلها هي الأخرى عرضـــة للإحتيال الإلكتروني، لذا نص المشـــرع في هذا الأمر، على جملة من الأحكام، حيث يتناول الفصـــل الأول منه الأحكام العامة المتعلقة بحماية المعلومات والوثائق الإدارية الخاصـــة بالســـلطات العمومية ، حيث أعطى تعريف لبعض المصـــطلحات كالموظف العمومي، الوثائق والوثائق المصنفة، أما الفصل الرابع ، فتطرق فيه إلى المسؤولية المدنية والتأديبية حيث نص على المتابعة الجزائية وطلب التعويض، في حين نص على القواعد الإجرائية في فصله الخامس ، ليشغل الفصـل السـادس بالأحكام الجزائية، فالمادتين(37) و(38) تنص على معاقبة كل دخول دون

---

[1] القانون رقم 15-03، مرجع سابق، المادة 17، 18.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 21-09 مؤرخ في 08 يونيو سنة 2021، المتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية، عدد 45، الصادرة بتاريخ 09 يونيو 2021.

[3] محمد الحبيب عباســـي، الحماية الجزائية للمعلومات والوثائق الإدارية من خلال الأمر 21-09، مجلة القانون والعلوم الســـياســـية، العدد 01، 2023، ص414.

ترخيص إلى وسائل تكنولوجيا الإعلام والاتصال، للحصول على معلومات أو وثائق مصنفة لتضاعف العقوبة إذا تم نشرها، قصد الإضرار بالسلطات المعنية أو الحصول على منافع، وكل إنشاء أو إشراف أو ادارة لمواقع أو حساب أو برنامج لنشر المعلومات والوثائق المصنفة كليا أو جزئيا بأحد وسائل تكنولوجيا الإعلام والإتصال بعقوبة الحبس من خمس (5) سنوات إلى عشر (10) سنوات، وبغرامة مالية تتراوح بين 50.000دج الى 1.000.000دج.[1]

كما نصت المادة (42) بتطبيق العقوبات المنصوص عليها في قانون العقوبات على الشخص المعنوي المرتكب للجرائم التي نص عليها هذا الأمر. أما المادة (44)[2] فتنص على مصادرة كل شيء أستخدم في إرتكاب الجرائم، المنصوص عليها في هذا الأمر، والأموال المتحصل عليها، إضافة إلى إغلاق الموقع أو الحساب الإلكتروني، الذي أرتكب الجرم من خلاله، والمحل مكان الإستغلال إذا أرتكبت الجريمة بعلم مالكه، دون المساس بحقوق الغير حسن النية في هذه المادة. ليمنح المشرع للجهة القضائية المختصة، من خلال نص المادة (45)[3]، الحكم على مرتكبي الجرائم المنصوص عليها في هذا الأمر، بعقوبة أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات، كما يمكن الحكم على الموظف العمومي بالمنع من ممارسة وظيفة عليا نهائيا أو لمدة لا تقل عن (5) سنوات، ولا تفوق (10) سنوات، ليعاقب المحرض بأي وسيلة بنفس عقوبة الفاعل الأصلي حسب المادة (46) ، أما في حالة الشروع فيعاقب بنفس عقوبة الجريمة التامة حسب المادة (47) لينص على مضاعفة العقوبة في حالة العود في المادة (48).[4]

سعى المشرع من خلال إصدار كل من القانون 15-03 والأمر 21-09، إلى ضمان سلامة البيانات والتعاملات الإلكترونية للمؤسسات والمتعلقة بالوثائق الإدارية، بحيث أصبح

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 21-09 مؤرخ في 08 يونيو سنة 2021، المتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية، عدد 45، الصادرة بتاريخ 09 يونيو 2021، المادة 37، 38.

[2] القانون رقم 21-09، المرجع نفسه، المادة42، 44.

[3] القانون رقم 21-09 ،المرجع نفسه، المادة 45.

[4] القانون رقم 21-09 ، المرجع نفسه، المادة 46،47،48.

هناك إطار قانوني صـارم، سـعيا منه لتكريس التزام الدولة بمواكبة التطورات، وتوفير بيئة قانونية آمنة.

المطلب الثاني: الهيئات الوطنية التقليدية والحديثة لمكافحة الإحتيال الإلكتروني

دعّم المشـرع الجزائري الآليات القانونية السـابقة بأخرى مؤسـساتية، لتحقيق تكامل فعال يسـعى للقضـاء على مثل هذه الجرائم، وتقوم بتطبيق القوانين من أجل تعزيز الأمن الرقمي وحماية البنية التحتية التكنولوجية للمؤسـسـات، وهذا ما يعكس حرص المشـرع الجزائري على مواجهة التحديات التي تفرضـها التكنولوجيا الحديثة، وضـمان بيئة رقمية آمنة للمؤسسات مما يسهم في تعزيز إستقرارها الإقتصادي، وحماية مصالحها من التهديدات الإلكترونية المتزايدة.

الفرع الأول: الهيئات الوطنية التقليدية

إعتمد المشـرع الجزائري في البداية، على آليات قانونية تقليدية قائمة لمواجهة الجرائم الإلكترونية، والجرائم الكلاسيكية على حد سواء و المتمثلة في:

أولا: الجهات القضائية ذات الإختصاص الموسع 04-14

ظهرت الجهات القضائية ذات الإختصاص الموسع بعد أن نص المشرع على القانون رقم 04-14 المؤرخ في 10 نوفمبر2004 المعدل والمتمم لقانون الإجراءات الجزائية[1]، فقد سعى المشرّع الجزائري من خلال هذه التعديل، إلى تطوير المنظومة القانونية لمواكبة المستجدات وحماية المؤسـسـات من الإحتيال الإلكتروني، من خلال التصـدي للجرائم الماسـة بأنظمة المعالجة الآلية للمعطيات، نظرًا لما تمثله هذه الجرائم من تهديد خطير للإقتصاد الوطني والأمن السيبراني. حيث نص القانون 04-14[2] على توسـيع الإختصـاص المحلي ليشـمل محاكم أخرى، وفقًا للتنظيم لكل من وكيل الجمهورية حسـب المادة (37)[3] الفقرة 2 وقاضـي التحقيق الذي نص عليه هو

[1] نورة عبد الله، الاختصاص القضائي الموسع في المادة الجزائية وفق القانون الجزائري، مجلة الفكر القانوني والسياسي، العدد01، 2022، ص971

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 04-14 مؤرخ في 10 نوفمبر سنة 2004، يعدل و يتمم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية، عدد 71، الصادرة بتاريخ 10 نوفمبر 2004 .

[3] القانون رقم 04-14، المرجع نفسه، المادة 37.

الآخر في المادة (40)[1] من نفس الأمر، حيث ذكر فيها الجرائم التي يتم فيها تمديد الإختصاص على سبيل الحصر، وهي الجرائم ذات التعقيد التقني مثل الجرائم المرتبطة بأنظمة المعالجة الآلية للمعطيات، إضافة إلى جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية تبييض الأموال، الإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف.

في حين جاءت المادة (329) الفقرة 5 من نفس الأمر بجواز تمديد الاختصاص المحلي للمحاكم ليشمل محاكم أخرى وفقًا للتنظيم، وذلك بهدف ضمان معالجة فعالة للجرائم الإلكترونية والمتعلقة بأنظمة المعلومات، إلى جانب الجرائم ذات الأثر الإقتصادي والأمني.[2]

وتجسيدا لهذا المسعى، تم إصدار النصوص التنظيمية سنة 2006، ممثلة في المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006، والذي يهدف إلى تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق. فقد تم تحديد المحاكم ذات الإختصاص الموسع، ومحاكم المجالس القضائية التابعة لها، وهي محكمة سيدي أمحمد الجزائر العاصمة، محكمة قسنطينة، محكمة ورقلة، محكمة وهران.[3] ليتم تعديله بموجب المرسوم التنفيذي رقم 16-267 الذي ينص على تعديل دائرة إختصاص هذه المحاكم، حيث مس هذا التعديل كل المحاكم ما عدا محكمة سيدي أمحمد.[4]

لقد جاءت هذه التعديلات الإجرائية التي قام بها المشرع نتيجة حرصه الدائم على حماية المؤسسات من خطر الجرائم الإلكترونية التي تهددها، إضافة إلى سعيه لمواكبة التطورات الحاصلة في هذا النوع من الجرائم، وضمان فاعلية المتابعة القضائية، لكونها تختلف عن الجرائم الكلاسيكية، فهو يسعى جاهدا على جعل هذه الإجراءات تضمن إستجابة فعالة للتحديات

---

[1] القانون رقم 04-14، مرجع سابق، المادة 40.

[2] القانون رقم 04-14، المرجع نفسه، المادة (329).

[3] نورة عبد الله، مرجع سابق، ص971.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم التنفيذي رقم16-267 مؤرخ في 17 أكتوبر سنة 2016، يعدل المرسوم التنفيذي رقم 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق ، الجريدة الرسمية،عدد 62، الصادرة بتاريخ 23 أكتوبر 2016 .

الناشـــئة عن الإحتيال الإلكتروني الذي تتعرض له المؤســـســـات، وهو ما يعزز دور العدالة في الحفاظ على الأمن القانوني والإقتصادي للدولة.

ثانيا: المعهد الوطني للأدلة الجنائية وعلم الإجرام

يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام، أحد الآليات المؤسساتية التي تؤدي دورا مهما في مكافحة الجرائم الســـيبرانية، بما في ذلك جريمة الإحتيال الإلكتروني التي تســـتهدف المؤسسات بصفة خاصة، فهذه الآلية تعتبر دعم للعدالة لما توفره من أدلة. "فالدليل هو الواقعة التي يســـتمد منها القاضـــي البرهان على إثبات إقناعه بالحكم الذي ينتهي إليه"[1]. ولأن هذه الجرائم، تستعمل أساليب تختلف عن تلك المستعملة في الجرائم التقليدية، وجب بالضرورة تقديم دليل يتماشـــى وطبيعة الجريمة المقترفة، وقد أنشـــئ هذا المعهد بموجب المرســـوم الرئاســـي 04-183[2] المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، وهو عبارة عن مؤسسة عمومية ذات طابع إداري يتمتع بالشخصية المعنوية يوضع تحت وصاية وزير الدفاع الوطني.[3]

تتمثل مهامه وفق ما جاء في الفصل الثاني من الأمر:[4]

- إجراء الخبرات والفحوص العلمية بناءً على طلب القضـــاة، المحققين، أو الســـلطات المؤهلة كل حسب إختصاصه في إطار التحريات الأولية، والتحقيقات القضائية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكب الجريمة الإلكترونية؛
- العمل على الوقاية والحد من كل أشـــكال الإجرام بما فيها الإحتيال الإلكتروني من خلال المشاركة في الدراسات، والتحاليل المتعلقة بهذه الجرائم؛

---

[1] نصر الدين مروك، محاضرات في الإثبات الجنائي، الجزء الثاني أدلة الإثبات الجنائي، الجزائر: دار هومة، 2004، ص 09 .

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 04-183 مؤرخ في 26 يونيو سنة 2004، متضمن إحداث المعهد الوطني للأدلة الجنائية و تحديد قانونه الأساسي، الجريدة الرسمية، عدد 41، الصادرة بتاريخ 27 يونيو 2004.

[3] سميرة بارة، الأمن السيبراني في الجزائر السياسات و المؤسسات، المجلة الجزائرية للأمن الإنساني، العدد04، جويلية 2017 ، ص271.

[4] القانون رقم 04-183، مرجع سابق، المادة (04)

- تصـميم بنوك معطيات وإنجازها طبقا للقانون، و جعلها في متناول القضـاة و المحققين بغرض وضـع مقاربات وإسـتخلاص الروابط المحتملة بين المجرمين و أسـاليب النشـاط الإجرامي الإلكتروني ؛
- المشاركة بصفته هيئة، تضمن الفحوص والخبرات في مجال علم الإجرام؛
- إجراء البحوث المتعقة بالإحتيال الإلكتروني من خلال اللجوء إلى التكنولوجيا الدقيقة؛
- ترقية البحث التطبيقي وأسـاليب التحريات التي تثبت فعاليتها في ميادين علم الإجرام والأدلة الجنائية للجرائم الإلكترونية؛
- المشـاركة في الملتقيات والمحاضـرات والندوات المتعلقة بالأمن السـيبراني على الصـعيدين الوطني والدولي الضرورية في تطوير مستخدمي المعهد.

فالمعهد يتولى مهمة دعم السـلطات القضـائية والتنفيذية من خلال إجراء الخبرات الفنية وتحليل الأدلة والآثار المرتبطة بالجريمة، بهدف إضـفاء الطابع القانوني عليها وتحويلها إلى أدلة موثوقة تسـتخدم في الإثبات القضـائي، كما يسـهم في تعزيز قدرات المحققين عبر توفير النتائج المستخلصة من التجارب السابقة، مما يمكنهم من تحسين أساليب التحقيق وإعتماد منهجيات أكثر دقة وكفاءة في الكشف عن الحقيقة.

ثالثا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها

أنشـئ المركز سـنة 2008، ويعتبر الجهاز الوحيد المختص في جرائم الإعلام الآلي والجرائم المعلوماتية بالجزائر، يوجد مقره ببئر مراد رايس الجزائر العاصمة، تتمثل مهامه في:[1]

- تأمين منظومة المعلومات لخدمة الأمن العمومي؛
- يعتبر مركز توثيق،
- تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها؛

[1] سمير بارة، مرجع سابق، ص271.

- تأمين الأنظمة المعلوماتية والحفاظ عليها لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك.

كما أنه يساعد الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال والبحث عن الأدلة، والمشاركة في عمليات التحري والتسرب عبر شبكة الأنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية، إضافة إلى المشاركة في قمع الجرائم المعلوماتية من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.[1]

بناءً على ما تم ذكره، يختص هذا المركز في الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات، حيث يتولى عمليات البحث، التحري والتحقيق في هذا المجال. بالإضافة إلى ذلك يقوم بحماية ومراقبة شبكات الإتصال وأنظمة المعالجة الآلية التابعة للمؤسسات، مما يسهم في تعزيز الأمن السيبراني لها ضد مختلف التهديدات، مثل الإحتيال الإلكتروني.

الفرع الثاني: الهيئات الوطنية الحديثة

في إطار التكيّف مع التطورات الحاصلة في مجال الجريمة، خاصة منها المتعلقة بالتكنولوجيا أنشأ المشرع الجزائري مؤسسات حديثة، تهدف إلى حماية البنية التحتية الرقمية وتعزيز الأمن السيبراني نذكر منها:

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته

جاء تنظيم الهيئة المختصة بمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من سعيا لتعزيز الآليات القانونية لمكافحة الجرائم السيبرانية التي تمس المؤسسات بآليات أخرى مؤسساتية وقد تم النص عليها لأول مرة بموجب القانون 09-04[2] المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها في المادة (13)[3] منه ، ليتم النص

[1] سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، العدد 1، جوان 2021 ص 281.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 مؤرخ في 5 غشت سنة 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، الصادرة بتاريخ 16 غشت 2009.

[3] القانون رقم 09-04، المرجع نفسه، المادة 13.

على تشكيلتها وتنظيمها وكيفيات سير الهيئة بعدة مراسيم رئاسية، أولها المرسوم الرئاسي رقم 15-261 [1]، ليتم النص على آخر مرسوم رئاسي 21-439 المتضمن إعادة تنظيم الهيئة ومن خلال مواده تعرف الهيئة على أنها سلطة مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي توضع لدى رئيس الجمهورية، تمارس مهامها تحت رقابة السلطة القضائية، طبقا لأحكام قانون الإجراءات الجزائية. [2]

وقد تضمنت **المادة (14)** من **القانون 09-04** مهام الهيئة والمتمثلة في: [3]

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وتحديد مكان تواجدهم.

ليعيد النص على معظم المهام مرة أخرى عن طريق **المرسوم الرئاسي 21-439** في **مادته (04)** والمتمثلة في: [4]

- تحديد الإستراتيجيات الوطنية لوقاية المؤسسات من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال؛
- تنشيط عمليات وقاية المؤسسات من الجرائم الإلكترونية والتنسيق بين الهيئات المعنية؛

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 15-261، المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 53، الصادرة بتاريخ 08 أكتوبر 2015.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 21-439، المؤرخ في 07 نوفمبر 2021، يتضمن أعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 86، الصادرة بتاريخ 11 نوفمبر 2021.

[3] القانون 09-04، مرجع سابق، المادة 14.

[4] المرسوم الرئاسي رقم 21-439، مرجع سابق، المادة 04.

- إحباط الجرائم التي تمس بأمن الدولة من خلال حماية مؤسساتها، بالكشف المبكر عنها عن طريق المراقبة الوقائية للاتصالات الإلكترونية؛
- جمع الأدلة الرقمية من خلال تسجيل وحفظ هذه المعطيات للأنظمة المعلوماتية وتحديد مصدرها لإستعمالها في الإجراءات القضائية؛
- تكوين المحققين المتخصصين في مجال الجرائم السيبرانية؛
- الإسهام في تحديث المعايير القانونية في مجال إختصاصها؛
- مد يد المساعدة للسلطات المعنية في مجال مكافحة الجرائم الإلكترونية عن طريق تزويدهم بالمعلومات وانجاز الخبرات؛
- تعزيز التعاون بين المؤسسات والهئيات الوطنية المعنية بالأمن السيراني، وتطوير المعارف في هذا المجال؛
- العمل على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية، وتطوير التعاون الدولي وتبادل المعلومات فيما يخص الأمن السيبراني وفقا لأحكام المادتين (17) و(18) من القانون 04-09.

بناءً على ما سبق تفصيله بشأن مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، يتبين أن غالبية إختصاصاتها ذات طبيعة إستشارية ورقابية وإدارية، مع إستبعاد أي صلاحيات قمعية. وعليه، يمكن القول إن الدور الأساسي لهذه الهيئة هو الوقاية وليس العقاب[1]، ومع ذلك فهي تعمل على وقاية المؤسسات من الجرائم الإلكترونية بما فيها الإحتيال الإلكتروني من خلال الكشف المبكر عنها قبل وقوعها، وبهذا يعزز الأمن السيبراني للمؤسسات.

ثانيا: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

جاء إنشاء القطب الجزائي الوطني لمكافحة الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال كإستجابة مباشرة للنهج التشريعي الرامي إلى تعزيز التخصص القضائي في مواجهة التحديات

[1] سهيلة بوزبرة، الهئية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بين سرية المعطيات الشخصية الإلكترونية و مكافحة الجرائم الإلكترونية، المجلة النقدية للقانون و العلوم السياسية، العدد 02 ، 2022/12/10، ص 571

المستجدة، خاصة بعد أن بات الإحتيال الإلكتروني من أبرز الجرائم التي تفرض تهديدات إقتصادية كبيرة، نظراً لجسامة الخسائر المالية التي تسببها للمؤسسات، فضلاً عن تأثيره السلبي على مستوى ثقة المتعاملين معها، ولا يقتصر تأثير هذه الجرائم على الجانب الاقتصادي فحسب، بل يمتد ليشمل الأبعاد الأمنية، مما يستوجب تبني آليات قانونية أكثر دقة وفعالية لضمان حماية المصالح الوطنية وتعزيز الإستقرار الإقتصادي والقانوني.

من خلال إستقراء المواد القانونية المتعلقة بالأقطاب المتخصصة، يمكن تعريفه على أنه عبارة عن هيئة نوعية جزائية وطنية مختصة بالنظر في نوع معين من الجرائم، التي تهدد أركان الدولة مما تتطلب أساليب بحث وتحري خاصة أو تعاون دولي.[1]

وحسب ما جاء في نص المادة (211) مكرر22 من الأمر 21-11[2]، فإن له إختصاص وطني، فوكيل الجمهورية وقاضي التحقيق، ورئيس ذات القطب، يمارسون مهامهم في كامل الإقليم الوطني حسب نص المادة (211) مكرر23[3] من نفس الأمر، والمتمثلة في:

- الحكم في الجرائم المنصوص عليها في الأمر 21-11 إذا كانت تشكل جنحا؛
- المتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيا الإعلام والإتصال والجرائم المتصلة بها التي تمس بأمن الدولة ودفاعها، أو تلك التي تنشر وتروج لأخبار كاذبة ومغرضة للمساس بالأمن والسكينة العامة، سواء كانت ذات طابع منظم أو عابر للحدود الوطنية، أو تمس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية والجرائم التي تتاجرة بالبشر أو أعضائهم إضافة الى جرائم التحريض على التمييز والكراهية كما جاء في نص المادة 211 مكرر24. [4]

---

[1] فاطمة الزهراء عون، الإجراءات التشريعية المستحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري –القطب الجزائي الوطني نموذجا– مجلة حقوق الإنسان و الحريات العامة، العدد 02 ، 2022/12/26، ص 558.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 21-11 مؤرخ في 25 غشت سنة 2021 ،يتمم الأمر 66-155 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية، عدد 65، الصادرة بتاريخ 26 غشت 2021 .

[3] الأمر رقم 21-11، المرجع نفسه، المادة (211) مكرر 23

[4] الأمر رقم 21-11، مرجع سابق، المادة (211) مكرر 24

- المتابعة والتحقيق في الجرائم المتصـــلة بتكنولوجيا الإعلام و الإتصـــال الأكثر تعقيدا[1] و الجرائم المرتبطة بها كما جاء في نص المادة (211) مكرر 25.[2]

فمهام القطب تندرج كلها حول المتابعة، والتحقيق، والمحاكمة. فخلال مرحلة المتابعة الجزائية على مستوى هذا القطب، منح المشرع لوكيل الجمهورية على مستوى القطب طبقا لأحكام المادة (211) مكرر من الأمر 21-11، متابعة كل الجرائم المتصـــلة بتكنولوجيا الإعلام، والإتصـــال والجرائم المرتبطة بها، سواء كانت القضية في طور البحث والتحري، أو تم إيداع المحاضر الخاصة بها على مستوى النيابة، أما في مرحلة التحقيق، فيختص قاضـي التحقيق على مسـتوى القطب طبقا لنفس المادة بالتحقيق في كافة تلك الجرائم، أما في مرحلة المحاكمة فخلافا لوكيل الجمهورية وقاضـي التحقيق، فإن قاضـي الحكم لدى هذا القطب الجزائي، يختص بالنظر في الجرائم المتصـلة بتكنولوجيا الإعلام والإتصـــال، والجرائم المرتبطة بها الموصـــوفة بالجنح، حســـب المادة (211) مكرر22 من نفس الأمر، لكون الجرائم الموصـــوفة بالجنايات من إختصـــاص محكمة الجنايات الإبتدائية، و يتم الفصل فيها من طرف محكمة الجنايات لمجلس قضاء الجزائر.[3]

إن التخصـص القضـائي بما فيه القطب الجزائي الوطني لمكافحة الجرائم المتصـلة بتكنولوجيا الإعلام والإتصـــال يأتي في سـياق السـعي إلى تطوير آليات المكافحة القانونية، من خلال تمكين الهيئات القضائية المختصة من التعامل بفعالية مع هذه الجرائم، كما يسـهم في تعزيز الأمن القانوني والإقتصـادي، والحد من التداعيات السـلبية التي قد تهدد الإسـتقرار المؤسـساتي بما فيها الإحتيال الإلكتروني، لما ينجم عنه، من أضرار جسيمة تلحق بالمؤسسات والدولة على حد سواء.

---

[1] يقصـــد بالجريمة المتصـــلة بتكنولوجيا الإعلام والاتصـــال الأكثر تعقيدا، بمفهوم هذا القانون الجريمة التي بالنظر الى تعد الفاعلين او الشـــركاء أو المتضررين، أو بسبب إتساع الرقعة الجغرافية لمكان إرتكاب الجريمة أو جسامة أثارها أو الأضرار المترتبة عليها أو لطابعها المنظور او العابر للحدود الوطنية أو لمســاســها بالنظام العام و الأمن العمومية، تتطلب وســائل تحري خاصــة أو خبرة فنية متخصــصــة أو اللجوء الى تعاون قضــائي دولي المادة 211 مكرر 25 فقرة 2.

[2] الأمر رقم 21-11 ، مرجع سابق، المادة (211) مكرر 25.

[3] جمال الدين بوقرة، جمال الدين عنان، القطب الجزائي الوطني لمكافحة الجرائم المتصـــلة بتكنولوجيا الإعلام والاتصـــال، مجلة الأســـتاذ الباحث للدراسات القانونية والسياسية، العدد01، 2022/06/10، العدد01، ص 1684-1685.

ثالثا: المصلحة المركزية لمحاربة الجرائم الإلكترونية مديرية الأمن الوطني

يشكل التعاون بين السلطة القضائية والسلطة التنفيذية، ممثلة في جهاز مديرية الأمن الوطني أحد الركائز لضمان مكافحة الجرائم الإلكترونية التي تستهدف المؤسسات. فهي إحدى المديريات الرئيسة لوزارة الداخلية والجماعات المحلية، تقوم بحفظ الأمن والنظام العام بالمناطق الحضرية والشبه حضرية[1]. من بين مهامها، مساعدة السلطة القضائية في مباشرة التحقيق. وقد نظم المشرع الإجراءات التي تسبق تحريك الدعوى العمومية والتي تسمى بالمرحلة الإستدلالية، حيث يتم فيها تثبيت وقوع الجريمة، والبحث عن مرتكبيها، وجمع الدلائل.[2]

في هذا الإطار، وقصد مواكبة التطورات العلمية، والتكنولوجية الحديثة، والإستفادة منها في سبيل مكافحة الجريمة، سواء من الشق الوقائي، أو من الشق الردعي[3]. قامت المديرية العامة للأمن الوطني، بإنشاء المصلحة المركزية للجريمة الإلكترونية، لأول مرة سنة 2011، حيث كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية على مستوى المديرية، ليتم إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال بقرار من مدير الأمن الوطني، وأضيفت للهيكل التنظيمي لمديرية الشرطة القضائية سنة 2015.[4] وتمثلت مهامها فيما يلي[5]:

- دعم مصالح الشرطة القضائية في تنفيذ التحريات التقنية، عبر تحليل الأدلة الرقمية المتعلقة بالجرائم الإلكترونية، بما فيها الإحتيال الإلكتروني الذي يستهدف المؤسسات ويتسبب في خسائر مالية جسيم؛

---

[1] محمد السعيد زناتي، أحمد بنيني، دور الشرطة الجزائرية في الوقاية من الجريمة ومكافحتها، مجلة تحولات، العدد01، يناير2019، ص 375.

[2] عبد الرحمان بخيري، مقدم حمر العين، تنظيم جهاز الشرطة واختصاصاتهم على ضوء تعديل قانون الإجراءات الجزائية بالقانون 10/19، مجلة البحوث في الحقوق والعلوم السياسية، العدد 8 ،2023/04/04، ص 169.

[3] محمد السعيد زناتي، أحمد بنيني، مرجع سابق، ص 385.

[4] سمير بارة، مرجع سابق، ص273.

[5] سميحة بلقاسم، حميد بوشوشه، الجريمة الإلكترونية بعد جديد للأجرام في الجزائر واقعها وآليات مجابهتها، مجلة العلوم الإنسانية، العدد 1، جوان 2023، ص 549.

- المساهمة الفعالة في حماية الأنظمة المعلوماتية والفضاء السيبراني الوطني، من خلال تعزيز التدابير الأمنية التي تهدف إلى الوقاية من الهجمات الإلكترونية، خاصة الإحتيال الرقمي الذي يهدد إستقرار المؤسسات؛
- التنسيق والتعاون المشترك في التحقيقات والتحريات ذات الطابع الوطني والدولي، لمكافحة الجرائم الإلكترونية، بما في ذلك عمليات الإحتيال الممنهج التي تستهدف الأنظمة المصرفية والمؤسسات التجارية من خلال تأكيد عضويتها الفعالة في الشرطة الدولية INTERPOL؛
- تعزيز اليقظة المعلوماتية ورصد الشبكات المفتوحة، للكشف عن المحتويات غير المشروعة ومن بينها الأساليب الإحتيالية التي تُستخدم لخرق البيانات وسرقة المعلومات المالية والتجارية مما يُشكل تهديدًا مباشرًا للأمن الإقتصادي؛
- المشاركة في برامج التكوين المتخصص لعناصر الشرطة العاملة ضمن فرق مكافحة الجريمة المعلوماتية على مستوى أمن الولايات، لضمان تطوير مهاراتهم في التعامل مع الإحتيال الإلكتروني سواء من حيث التحقيق الرقمي أو حماية المؤسسات من الإستغلال السيبراني.
- سنة 2007 إستحدثت المديرة العامة للأمن الوطني بمخابر الشرطة العلمية بالجزائر العاصمة، وهران وقسنطينة أقسام متخصصة في تتبع الأدلة الرقمية، لتقوم بإنشاء خلايا مكافحة الجرائم الإلكترونية على مستوى جميع مديريات الأمن الولائية.[1]

وفق ما سبق، يظهر جليا إن دور الأمن الوطني في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال يأتي ضمن إستراتيجية شاملة تهدف إلى تطوير آليات التصدي لهذه التهديدات المستجدة، فمن خلال تعزيز قدرات الأجهزة الأمنية، يتم التعامل بفعالية مع الجرائم الإلكترونية بما في ذلك الإحتيال الرقمي الذي يشكل تحديا متزايدا للمؤسسات والدولة على حد سواء.

[1] عبد الرحمان حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، مداخلة مقدمة ضمن الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة ،2015، ص 08.

المبحث الثالث: التحديات وآليات تفعيل الإطار القانوني لحماية المؤسسات من الإحتيال الإلكتروني

أدى تزايد الإعتماد على التكنولوجيا الرقمية في تسيير شؤون المؤسسات إلى تنامي مخاطر الإحتيال الإلكتروني، الأمر الذي إستدعى تطوير أطر قانونية لضمان الحماية اللازمة، غير أن فعالية هذه الأطر ما تزال تواجه تحديات متعددة تعيق تنفيذها بشكل ناجع، ومن ثمة لابد من تجاوز هذه التحديات عبر إعتماد مقاربة شاملة تدمج بين القانون، التقنية، والإدارة المؤسساتية لضمان بيئة رقمية آمنة ومستقرة.

المطلب الأول: تحديات تطبيق الإطار القانوني لحماية المؤسسات من الإحتيال الإلكتروني

أصبح الإحتيال الإلكتروني من أبرز التهديدات التي تواجه المؤسسات، ورغم وجود أطر قانونية ومؤسساتية دولية ووطنية تهدف إلى حماية هذه المؤسسات من الهجمات الرقمية، إلا أن تطبيق هذه القوانين يواجه جملة من التحديات على جميع المستويات، الوطنية، الإقليمية والدولية نبرزها في ضوء النقاط التالية:

الفرع الأول: قصور وإختلاف التشريعات الوطنية والدولية

تختلف الأنظمة القانونية من بلد إلى آخر، ولا يوجد إتفاق عالمي على تعريف موحد لسوء إستخدام نظم المعلومات، مما يخلق ثغرات قانونية يستغلها مرتكبو الجرائم الإلكترونية، وتشمل هذه الجرائم أشكالا متعددة، مثل الإختراق، والبرمجيات الخبيثة، والإحتيال الإلكتروني الذي يستهدف المؤسسات، حيث يعتمد المهاجمون على وسائل متطورة لخداع الأنظمة وسرقة البيانات المالية والإدارية مما يعرض الإقتصاد الرقمي لمخاطر كبيرة. [1]

[1] سليمان قطاف، عبد الحليم بوقرين، مرجع سابق، ص 82.

وفي ظل هذا التطور السريع للجرائم الإلكترونية، تواجه التشريعات القانونية صعوبة في مواكبة التحديات المستجدة، حيث تختلف الدول في تصنيف الأفعال التي تعتبر جرائم إلكترونية، مما يترك المجال مفتوحا أمام مرتكبي هذه الجرائم لإستغلال الثغرات القانونية، ومن بين هذه التحديات، يأتي قصور التشريعات الجزائرية، إذ لم يتم بعد إصدار قانون خاص بالجريمة الإلكترونية رغم توجه الدولة نحو الرقمنة، وهو ما يستدعي ضرورة سنّ تشريعات حديثة، تتماشى مع التطورات الرقمية المتسارعة لضمان حماية المؤسسات وتقليل المخاطر الناجمة عن الإحتيال الإلكتروني.[1]

الفرع الثاني: الميزات الخاصة للجرائم الإلكترونية

تنفرد الجرائم الإلكترونية بخصائص تميزها عن غيرها من الجرائم، سواء من حيث تعقيد مسألة الإختصاص القضائي أو من حيث طبيعتها المختلفة عن الجرائم التقليدية.

أولا: إشكالية الإختصاص في الجرائم الإلكترونية

تعد جرائم الإحتيال الإلكتروني ضد المؤسسات، من أكثر القضايا القانونية تعقيدا، فمعظم التشريعات الجنائية تعتمد على الصفة الإقليمية، مما يحد من قدرة السلطات على ملاحقة المجرمين عبر الحدود، فالاتفاقيات الثنائية، والمتعددة تساعد في تجاوز هذه الإشكالية، لكن لا تزال غير كافية لمعالجة مشكلات تبادل الأدلة وتسليم المجرمين.[2] فمعظم أجهزة إنفاذ القانون تفتقر إلى الخبرة الفنية والصلاحيات التنظيمية، والمعدات اللازمة للتحقيق في الجرائم الرقمية، وجمع الأدلة في بيئة إفتراضية يصعب تتبعها، ومن ثم، فإن غياب تشريعات خاصة بالفضاء السيبراني يتيح بيئة آمنة للمجرمين الإلكترونيين، ومن جهة أخرى، فإن رغبة الشركات في الحفاظ على سمعتها وثقة المستثمرين والجمهور تجعلها مترددة في الإبلاغ عن الأنشطة الإجرامية الإلكترونية[3].

[1] خضرة شنتير، مرجع سابق، ص 278.

[2] سليمان قطاف، عبد الحليم بوقرين، مرجع سابق، ص 83.

[3] Shewangu Dzomira, ELECTRONIC FRAUD (CYBER FRAUD) RISK IN THE BANKING INDUSTRY, ZIMBABWE, Risk governance & control: financial markets & institutions, Vol 4, Issue 2, 2014, P19.

إن غياب التنسيق بين الدول والحكومات من أبرز التحديات في مواجهة الإحتيال الإلكتروني ضد المؤسسات، بإعتبار أن هذا النوع من الجرائم يتسم بطابع عابر للحدود، فمرتكبو الإحتيال الإلكتروني، قد ينفذون هجماتهم على أنظمة الحاسوب في دولة معينة، بينما يتم التلاعب بالبيانات أو إختراقها في دولة أخرى، وتسجل النتائج أو تستغل في دولة ثالثة، بل وقد تخزن أدلة هذا الإحتيال على خوادم، أو أجهزة تقع في دول لا علاقة لها مباشرة بمكان إرتكاب الجريمة، ونتيجة لذلك تصبح عدة جهات قضائية، وأنظمة قانونية، وقواعد تشريعية، معنية بنفس الجريمة، مما يبرز تداخل في الإختصاص بين الدول. [1]

ناهيك عن العقبات الكبيرة المترتبة عن إختلاف الإجراءات المتبعة في التحقيق الجنائي بين الدول، والحصول على الأدلة في الجرائم المعلوماتية، خاصة تلك التي تتجاوز حدود الدولة يشكل تحديا صعبا نظرا لتعقيد عمليات الضبط والتفتيش الإلكتروني، الشيء الذي يعيق جهود مكافحتها، ومن هنا، فإن التصدي الفعال للإحتيال الإلكتروني ضد المؤسسات، يتطلب تعاونا دوليا وثيقا، سريعا وفعالا، يتميز بأعلى درجات التنسيق بين مختلف الدول والهيئات. [2]

ثانيا: طبيعة الجريمة الإلكترونية المختلفة عن الجرائم التقليدية

تواجه مكافحة الجرائم الإلكترونية العديد من العقبات، حيث تعتمد المؤسسات على أنظمة معلومات مصممة لتسهيل الخدمات، دون إيلاء الإهتمام الكافي للجوانب الأمنية، مما يترك المجال مفتوحا أمام مرتكبي الجرائم الإلكترونية لإستغلال الثغرات التقنية، ويلاحظ في هذا المجال ضعف الإبلاغ عن الجرائم الإلكترونية، إذ يتجنب بعض الضحايا، خصوصا المؤسسات والمتعاملين التوجه إلى السلطات المختصة، رغم تعرضهم للإحتيال الإلكتروني، بسبب ضعف الوعي القانوني، حيث يعتقد البعض أن هذه الأفعال لا تندرج ضمن الجرائم التي تستوجب العقوبات القانونية، وفقا للأنظمة الوطنية والدولية إضافة إلى الخوف من التداعيات التجارية فقد تفضل بعض المؤسسات

[1] سمير بارة، الأمن السيبراني في الجزائر، المجلة الجزائرية للأمن السيبراني، العدد 04، 2017، ص 276.

[2] سليمان قطاف، عبد الحليم بوقرين، مرجع سابق، ص 82 .

عدم الإبلاغ خشية التأثير السلبي على سمعتها، أو التعرض لتعطيل نشاطها بسبب التحقيقات ناهيك عن إرتباطها بجرائم أخرى لكون الجرائم الإلكترونية متداخلة مع جرائم مالية، أو أخلاقية مما يدفع بعض الأطراف إلى تجنب الإبلاغ خشية العواقب الإجتماعية[1].

يعد جمع الأدلة الرقمية في الجرائم الإلكترونية، وخاصة في حالات الإحتيال الإلكتروني ضد المؤسسات، من أكبر التحديات التي تواجه جهات التحقيق، حيث يتمتع مرتكبو هذه الجرائم بمهارات متقدمة تُمكّنهم من إخفاء نشاطهم والتلاعب بالبيانات، مما يجعل عملية الكشف عن الأدلة أكثر تعقيدًا، إضافة إلى ذلك، فإن الطبيعة الفريدة للجرائم الإلكترونية مقارنةً بالجرائم التقليدية تعيق تطبيق الأساليب المعتادة في التحقيق، إذ تعمل هذه الجرائم ضمن بيئة رقمية غير ملموسة يصعب تتبعها بالوسائل التقليدية. ولذلك، يتطلب التعامل مع الإحتيال الإلكتروني ضد المؤسسات تطوير إستراتيجيات تحقيق متقدمة تعتمد على التكنولوجيا الحديثة، وتعزيز التعاون بين الجهات القانونية والتقنية لضمان الكشف الفعّال عن هذه الجرائم وضبط مرتكبيها.[2]

كما يواجه التحقيق الجنائي في الجرائم الإلكترونية، ولا سيما الإحتيال الإلكتروني ضد المؤسسات، تحديات جوهرية تتعلق بصعوبة الإثبات، ونقص الأدلة الرقمية القاطعة، فلا تزال هذه القضايا محور نقاش قانوني مكثف، حيث يرى بعض الباحثين ضرورة الإعتراف بالأدلة الرقمية كإثبات قانوني قوي، إضافة إلى صعوبة جمع الأدلة الرقمية، وضبطها وفق إجراءات قانونية سليمة كما أن ضعف التشريعات التي تنظم إستخدام الأدلة الرقمية يزيد من تعقيد التحقيقات الجنائية ويؤخر إجراءات إثبات الجريمة.[3]

فضلا عن تعدد مصادر المعلومات وتحديات التنسيق، فقد كانت تقارير الشرطة سابقا تُعد المصدر الرسمي الأوحد لإحصائيات الجريمة، مما وفر صورة موحدة وموثوقة للواقع الأمني. أما اليوم فقد أصبحت هذه التقارير مجرد "رؤية" واحدة ضمن فسيفساء متعددة من الحقائق والروايات حول الجريمة، ويظهر هذا التعدد بوضوح في مجال الإحتيال والجرائم السيبرانية، حيث تصدر البيانات عن طيف واسع من المؤسسات، بما في ذلك:

---

[1] أمال بيدي، جهود الأمم المتحدة في مكافحة الجرائم السيبرانية، بمجلة البحوث في الحقوق والعلوم السياسية، العدد 01، 2022، ص 312.

[2] خضرة شنتيرة، مرجع سابق، ص 279.

[3] أمال بيدي، مرجع سابق، ص313.

- مؤسسات القطاعين العام والخاص المتضررة من الإحتيال أو المعنية بمكافحته مثل : البنوك شركات الأمن الخاصة .... الخ.
- منظمات المجتمع المدني التي تدافع عن حقوق الضحايا، سواء كانوا أفرادا أو مؤسسات[1].

الفرع الثالث: ضعف تكوين الإطارات الإدارية

يعد تدريب القيادات الإدارية على تكنولوجيا المعلومات ضرورة لمكافحة الإحتيال الإلكتروني ضد المؤسسات، إذ تؤثر المهارات الرقمية بشكل مباشر على كفاءة الأمن السيبراني، إلا أن العديد من المؤسسات تواجه تحديات، أبرزها ضعف تأهيل الإطارات في التقنيات الحديثة، مما يعرض أنظمتها للمخاطر الإلكترونية، كما تؤدي الفوارق الفردية بين المتدربين إلى تفاوت في إستيعاب إستراتيجيات الحماية الرقمية، حيث يجد بعض الأفراد صعوبة في التعامل مع التهديدات السيبرانية بينما يمتلك آخرون خبرة متقدمة، وللتغلب على هذه التحديات، يجب تطوير برامج تدريبية متخصصة تراعي إختلاف مستويات المعرفة، مع التركيز على تطبيقات الأمن السيبراني كما يتطلب الأمر تعزيز التعاون بين الجهات الحكومية والخاصة، لضمان تنفيذ إستراتيجيات تدريبية فعالة تحمي المؤسسات من الإحتيال الإلكتروني.[2]

المطلب الثاني: آليات تفعيل الإطار القانوني لحماية المؤسسات من الإحتيال الإلكتروني

أمام التحديات التي تواجه التطبيق الفعلي للإطار القانوني لحماية المؤسسات من الإحتيال الإلكتروني، فقد أصبح الأمر يتطلب جملة من الآليات لتقوية منظومة الحماية القانونية والمؤسساتية على حدّ سواء نذكر أهمها فيمايلي:

الفرع الأول: دعم الإطار القانوني وتعزيز الإنسجام القضائي الدولي

يعد توحيد الجهود بين الدول، في مجال محاربة الإحتيال الإلكتروني ضد المؤسسات من خلال، تحديث التشريعات الوطنية عاملا محوريا، لتحقيق تعاون قضائي فعال، يرسخ سيادة

[1] Michael Skidmore, The Anatomy Of Online Fraud, Perspectives On Policing : Paper 10, April 2024, P03

[2] محمد صفاء الدين علي شرشر محمود، الجهود الدولية لمكافحة جرائم الأنترنت، جلة البحوث القانونية والاقتصادية جامعة المنوفية، العدد 03، المجلد 54، أكتوبر 2021، ص 567.

القانون على المستوى الدولي، كما يشكل دعم الإطار القانوني وتعزيز الإنسجام القضائي الدولي ركيزة أساسية ويتحقق ذلك عبر عدة إجراءات، أبرزها:

أولا تعزيز التشريعات والأنظمة: وذلك من خلال:[1]

- إعطاء جرائم التقنية حقها من الأهمية في مؤسسات التشريع الوطنية، وإدراجها ضمن التشريعات الوطنية المختلفة؛
- مبدأ الوقاية في جريمة الإحتيال الإلكتروني خير من العلاج، وبشكل خاص فيما يختص بالتشريعات، والتدريب؛
- تعديل بعض التشـــريعات الحالية بما يتلاءم مع طبيعة جرائم الإنترنت، والتقنية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح؛
- إيضاح الحكم الشرعي الإسلامي تجاه جرائم الحاسب، والأنترنت، ونشرها ضمن برامج التوعية العامة.

ثانيا: تعزيز التعاون بين الدول في المجال القضائي

يتم ذلك من خلال حل عقبة المساعدات القضائية، وتبادل المعلومات بين الدول لضمان توفير الوثائق والبيانات اللازمة لدعم التحقيقات في الجرائم السيبرانية، إضافة إلى نقل الإجراءات القضائية، وتوفير أدوات قانونية لتسهيل الكشف عن البيانات المخزنة ضمن التحقيقات إستنادا إلى الإتفاقيات الدولية، مما يسمح بملاحقة الجناة خارج الحدود الوطنية، وتوحيد النظم القانونية من خلال تحديث التشـــريعات المحلية المتعلقة بالجرائم المعلوماتية، وفق المعاهدات الدولية، مما يقلل الفوارق بين الأنظمة العقابية، وجعل المعاهدات مرجع تشريع دولي في مجال الأمن السيبراني وتحيينها لتراعي خصوصية هذه الجرائم ومستجداتها، إضافة إلى إنشاء قنوات إتصال بين الجهات المختصة

[1] وائل محمد نصيرات، جريمة الاحتيال عبر شبكة المعلومات الدولية: دراسة مقارنة النظام السعودي والقانون الأردني، دفاتر السياسة والقانون، العدد19، جوان 2018، ص122.

للدول، بحيث تسهل تبادل المعلومات بين أجهزة إنفاذ القانون، مما يسهم في سرعة الإستجابة والتصدي للجرائم الإلكترونية بفاعلية أكبر.[1]

الفرع الثاني: إعتماد اللامركزية في عملية تحصيل المعطيات الخاصة بمزودي الخدمة

لتحقيق كفاءة أعلى في تحصيل البيانات المرتبطة بالجرائم الإلكترونية، يمكن إعتماد نهج لامركزي يساهم في تسريع الوصول إلى المعلومات وتحسين آلية التحقيقات. يتمثل هذا النهج في توزيع مراكز جمع البيانات على عدة مناطق بدلًا من تركيزها في العاصمة فقط، مما يسمح للجهات المختصة بالوصول إليها بشكل أسرع وأكثر فعالية. إضافة إلى ذلك، يمكن إستخدام أنظمة سحابية لتخزين البيانات ومشاركتها عبر منصات رقمية آمنة، مما يتيح الوصول الفوري إليها من أي مكان، دون قيود جغرافية، كما أن إنشاء بوابات إلكترونية لمزودي الخدمة يسهل عملية إرسال البيانات المطلوبة تلقائيًا إلى الجهة المختصة، ما يقلل الحاجة إلى إجراءات طويلة ومعقدة مما يضمن إستجابة سريعة وفعالة للتحقيقات الإلكترونية.[2]

الفرع الثالث: بناء القدرات المؤسسية في المنظومة القضائية والبحثية

في ظل التحولات المتسارعة التي يشهدها العالم في مجال العدالة والتكنولوجيا، أصبح من الضروري تعزيز البنية المؤسسية للمنظومة القضائية والبحثية، من خلال تطوير الكفاءات وتوفير بيئة ملائمة للنمو المعرفي والتقني.

أولا: تدريب وتأهيل الجهات القضائية وأفراد الضبطية

يتطلب تفعيل القوانين الخاصة بالجرائم الإلكترونية، توفير تدريب وتأهيل متخصص للجهات المعنية، لضمان تعامل فعال مع هذه القضايا المتزايدة التعقيد، وفي هذا السياق، يجب إعداد برامج تدريبية شاملة تستهدف النيابة العامة، والضبطية القضائية ، بحيث تتناول تقنيات التحقيق الرقمي طرق جمع الأدلة الإلكترونية، وآليات تحليل البيانات بإستخدام أحدث البرمجيات والأدوات المتاحة كما أن الجرائم الإلكترونية غالبا ما تتطلب خبرة تقنية متقدمة في مجالات مثل أنظمة التشغيل

[1] سليمان قطاف، عبد الحليم بوقرين، مرجع سابق ص ص 83-85.

[2] شهرزاد بولحية، رشيد خلوفي، تحديات الجريمة الإلكترونية في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 02، 2019، ص 1999.

الشبكات، وأمن المعلومات، الأمر الذي يستدعي تعزيز التعاون بين الجهات القضائية والمتخصصين في الأمن السيبراني، عبر فرق عمل مشتركة، تسهم في سرعة معالجة القضايا وتحليل المعطيات بدقة وكفاءة.[1] فقد أصبحت الحاجة ملحة لتحديث التشريعات الجنائية لتكون أكثر مرونة، بما يتماشى مع سرعة التطور التكنولوجي، لضمان تحقيق العدالة ومكافحة الجرائم المعلوماتية بفعالية.

الأمم المتحدة والإتحاد الأوروبي توصيان بضرورة تدخل سريع يتجاوز الحدود الجغرافية، بشرط وجود إطار قانوني يحمي سيادة الدول.

ثانيا: تعزيز مجال البحث والتعليم والتدريب

يعد التعليم والبحث العلمي من أهم الأدوات التي تسهم في مكافحة جريمة الإحتيال الالكتروني، وذلك من خلال:

- تشجيع البحث في دراسة جريمة الإحتيال عبر شبكة المعلومات الدولية وتقييم فعالية التدابير المتخذة لمكافحتها؛ حيث يمكن لهذا البحث أن يسهم في إنشاء قاعدة من المعلومات تصلح أساسا لإنطلاق البرامج الوقائية؛
- إدراج مادة جريمة الإحتيال المعلومات ضمن مناهج الدراسات القضائية، ومناهج الدراسة في الكليات والمعاهد الأمنية وكلية الدراسات العليا، وذلك بإستحداث تدريس" مادة تأمين نظم المعلومات على شبكة الإنترنت" والتعريف بالأساليب الإجرامية التي يتبعها قراصنة الحاسب الآلي لإختراقها نظراً لما تمثله جريمة النصب المعلوماتي من خطر على الإقتصاد القومي؛
- حث الجامعات والمراكز البحثية لدراسة جريمة الإحتيال المعلوماتي، ومحاولة إنشاء دراسة متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجريمة؛
- إجراء تدريبات متخصصة في جرائم الإحتيال المعلوماتية للقضاة والمحامين وأفراد الضبطية القضائية للإطلاع على أساليب إرتكابها، وكيفية ضبطها وقائيا أو علاجيا؛
- إنشاء مركز وطني إستشاري وتوجيهي للتوعية بمخاطر جرائم المعلومات والإستفادة من بعض كوادر "الهاكرز" وإعادة توجيههم والإستفادة منهم في القرصنة البيضاء؛
- ضرورة نشر الوعي بين المواطنين حول خطورة هذه الجرائم وسبل الوقاية منها. وتفعيل دور مؤسسات المجتمع المحلي في مجال التوعية المجتمعية.[2]

[1] خالد علي نزار الشعار، التحقيق الجنائي في الجرائم الإلكترونية، مجلة البحوث القانونية والإقتصادية، العدد 79، 2022، ص 33.

[2] وائل محمد نصيرات، مرجع سابق، ص123.

خلاصة وإستنتاجات

من خلال دراستنا لهذا الفصل، يتضح أن جريمة الإحتيال الإلكتروني التي تستهدف المؤسسات تمثل نمطا إجراميا مستحدثا، وقد إستجابت الدول لهذا التحدي من خلال تبني أطر قانونية ومؤسساتية متعددة المستويات، حيث مثّلت إتفاقية بودابست لعام 2001 وثيقة مرجعية أساسية في مجال مكافحة الجرائم الإلكترونية بشكل عام، حيث إستندت إليها العديد من الدول والمنظمات الإقليمية والدولية في صياغة تشريعاتها وتطوير آلياتها المؤسساتية بهدف تعزيز الجهود الرامية إلى مكافحة جريمة الإحتيال الإلكتروني التي تلحق بالمؤسسات أضرارًا مادية وإقتصادية كبيرة مما ينعكس سلبًا على إقتصادات الدول.

على الصـــعيدين الدولي والإقليمي، تم تناولنا هذه الجريمة من خلال معاهدات وإتفاقيات ثنائية ومتعددة الأطراف، صاحب ذلك إنشاء مؤسسات متخصصة مكلفة بإنفاذ القانون في هذا المجال. وقد ظهرت وكالات دولية وإقليمية متخصصة في هذا النوع من الجرائم.

وإنطلاقا من الطبيعة العابرة للحدود لجريمة الإحتيال الإلكتروني، إستلزم الأمر تدخل المشرع الجزائري الذي قام بدوره بتضمين الجرائم الإلكترونية، بما فيها الإحتيال الإلكتروني، ضمن منظومته القانونية. وقد تجلى ذلك في تعديل القوانين العامة، وإســـتحداث قوانين خاصـــة تعالج هذا النوع من الجرائم، بالإضـــافة إلى دعم جهود المكافحة من خلال مؤســـســـات تابعة للســـلطتين التنفيذية والقضائية.

ومع ذلك، لا تزال هذه الآليات القانونية والمؤســـســـاتية، على مختلف مســـتوياتها، تواجه تحديات تطبيقها الفعلي، سواء كان ذلك ناتجا عن الطبيعة المعقدة والمتغيرة لهذه الجرائم، أو بسبب الإختلافات القائمة بين تشـــريعات وإجراءات الدول. لذا، تبرز الحاجة إلى تطوير آليات لتفعيل هذه الأطر، والحد من عمليات الإحتيال الإلكتروني التي تستهدف المؤسسات.

خاتمة

خاتمة

تناولنا في هذه المذكرة الاحتيال الإلكتروني، وكيفية حماية المؤسسات من هذا النوع من الجرائم، وذلك خلال فصلين، تطرقنا في الفصل الأول للإطار المفاهيمي للاحتيال الإلكتروني، وعالجنا في الفصل الثاني آليات ووسائل حماية المؤسسات من الاحتيال الإلكتروني.

تبيّن لنا من هذه الدراسة أن الاحتيال الإلكتروني يعد من أكبر التهديدات التي تواجه المؤسسات بمختلف أنواعها، اقتصادية كانت وإدارية، وتتجلى خطورة هذا التهديد في الخسائر الجسيمة التي يحدثها، ليس فقط على الجانب المالي، بل تمس الأمن الاقتصادي، وزعزعة ثقة المتعاملين، الأمر الذي فرض على الدول اعتماد أطر قانونية وآليات مؤسساتية لمواجهة هذا النوع من الجرائم، خاصة وأن ضعف الأنظمة المعلوماتية التي تعتمدها المؤسسات، وغياب الثقة الرقمية لدى الفاعلين داخل المؤسسة، والمتعاملين معها، ساهم في تفشي هذا النوع من الاحتيال، ما جعل التصدي له أمرا معقدا في ظل البيئة الرقمية التي تمثل بيئة خصبة لنمو وتطور هذا النوع من الجرائم الالكترونية.

لذلك، تبرز الأهمية البالغة للإطار القانوني الذي يضمن حماية المؤسسات من الاحتيال الإلكتروني، سواء على الصعيد الدولي أو الوطني، فقد أظهرت الدراسة وجود إطار قانوني وآليات مؤسساتية تسهم بلا شك في الحماية، وهو ما يبرز ضرورة التعاون الدولي كحتمية لمواجهة الاحتيال الإلكتروني، وضمان ملاحقة مرتكبي هذه الجريمة العابرة للحدود التي أصبحت تحتاج لأطر قانونية حديثة ومواكبة للتطور الرقمي المتسارع كسبيل يسهم في تعزيز حماية هذه المؤسسات ومكافحة هذه الجريمة.

تبعا لما سبق، وفي ضوء ما تقدم في هذه الدراسة، فقد توصلنا لجملة من النتائج نذكرها في ضوء النقاط التالية:

- يشكل الاحتيال الالكتروني أبرز التحديات المعاصرة التي تواجه المؤسسات في العصر الرقمي الحديث.

خاتمة

- التطور المتسارع لأساليب الاحتيال الإلكتروني في ظل بطء عملية تحديث التشريعات يسهم في وجود ثغرات قانونية تستغلها العصابات الإجرامية.
- تتسم جرائم الاحتيال الإلكتروني بالتعقيد وصعوبة جمع الأدلة الرقمية وتقديمها بشكل مقبول أمام المحاكم، مما يشكل تحديا كبيرا أمام جهات إنفاذ القانون.
- يترتب على الاحتيال الإلكتروني آثار وخسائر متعددة تطال المؤسسات، لذا، أصبحت حماية المؤسسات من الاحتيال الإلكتروني أولوية قصوى للتشريعات الحديثة، نظرا للتهديدات المباشرة التي تشكلها هذه الجرائم.
- أظهرت التشريعات الإقليمية تقدما في مكافحة الاحتيال الإلكتروني عبر اتفاقيات وآليات تعاون، مما يوفر إطارا مهما لتطوير القوانين الوطنية.
- تتوقف حماية المؤسسات من الاحتيال الإلكتروني بشكل أساسي على تحديث التشريعات الوطنية والدولية، وتدعيم التعاون الدولي بما يتلاءم مع تطور الوسائل الاحتيالية الإلكترونية.
- تعتمد الحماية الفعالة للمؤسسات من الاحتيال الإلكتروني على أكثر من مجرد الجانب القانوني؛ إذ تتطلب أيضا تعزيز الثقافة السيبرانية الداخلية، ودمج آليات قوية للوقاية والكشف المبكر عن محاولات الاحتيال.

انطلاقا من النتائج، نقدم الاقتراحات التالية:

✓ ضرورة تعزيز الإطار القانوني لمكافحة الاحتيال الإلكتروني، وذلك من خلال إصدار نصوص قانونية متخصصة تجرم الأفعال الاحتيالية الموجهة ضد المؤسسات، مع التطبيق الفعلي لها بما يحقق الحماية الفعالة للمؤسسات من هذه الجريمة.

✓ ضرورة التدريب المستمر للمؤسسات والجهات القضائية على الاحتيال الإلكتروني قصد توعيتهم بالجوانب التقنية لهذه الجرائم.

✓ العمل على توعية المؤسسات، خاصة الصغيرة، والمتوسطة، بمخاطر الاحتيال الإلكتروني، وطرق الوقاية منه، وذلك من خلال تنظيم حملات تشرف عليها هيئات مختصة.

خاتمة

- ✓ تشـجيع المؤسـسـات على اعتماد وتطوير أنظمة أمن معلوماتي، وإنشـاء وحدات داخلية متخصـصـة في الأمن السـيبراني، بهدف رصـد محاولات الاحتيال والاسـتجابة لها بسـرعة وفعالية.
- ✓ تفعيل التعاون الدولي في مكافحة الاحتيال الإلكتروني من خلال الانضـمام للآليات الدولية ذات الصلة، وتطوير سبل تبادل الخبرات بين الدول، خصوصا في التتبع والتحقيق الرقمي العابر للحدود.
- ✓ توسيع صلاحيات الهيئات الوطنية لمكافحة الجرائم الإلكترونية، لتشمل الإشراف وتقديم الدعم الفني للمؤسسات الاقتصادية بهدف حمايتها.

قائمة المراجع

قائمة المصادر والمراجع

أ. باللغة العربية

أولا: النصوص القانونية

القوانين

1. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84 الصادرة بتاريخ 24 ديسمبر 2006.

2. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 04-14 مؤرخ في 10 نوفمبر سنة 2004، يعدل و يتمم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية، عدد 71، الصادرة بتاريخ 10 نوفمبر 2004 .

3. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004 ، يعدل و يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

4. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 04-183 مؤرخ في 26 يونيو سنة 2004، متضمن إحداث المعهد الوطني للأدلة الجنائية و تحديد قانونه الأساسي، الجريدة الرسمية، عدد 41، الصادرة بتاريخ 27 يونيو 2004.

5. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 08-01 مؤرخ في 23 يناير سنة 2008، المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، عدد 04، الصادرة بتاريخ 27 يناير 2008.

6. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 مؤرخ في 5 غشت سنة 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، الصادرة بتاريخ 16 غشت 2009.

7. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 15-03 مؤرخ في 01 فبراير سنة 2015، المتعلق بعصرنة العدالة، الجريدة الرسمية، عدد06، الصادرة بتاريخ 10 فبراير2015.

8. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 16-02 المؤرخ في 19 يونيو 2016 يتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 37 الصادرة بتاريخ 22 يونيو 2016.

9. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 2000-03 مؤرخ في 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمراسلات السلكية والاسلكية، الجريدة الرسمية، عدد 48، الصادرة بتاريخ 06 غشت 2000.

10. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 18-04 مؤرخ في 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، الجريدة الرسمية، عدد 27، الصادرة بتاريخ 13 مايو 2018.

11. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 21-09 مؤرخ في 08 يونيو سنة 2021، المتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية، عدد 45، الصادرة بتاريخ 09 يونيو 2021

12. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات المعدل والمتمم.

13. الجمهورية الجزائرية الديمقراطية الشعبية، قانون 83-11 مؤرخ في 2 يوليو سنة 1983، المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، عدد 28، الصادرة بتاريخ 5 يوليو 1983 .

14. الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 18-04 مؤرخ في 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد وبالمراسلات السلكية واللاسلكية، الجريدة الرسمية، عدد 27، الصادرة بتاريخ 13 مايو 2018.

15. القانون العدد 05 لسنة 2022 المؤرخ في 2022/09/27، المتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات والإتصال، الرائد الرسمي لجمهورية التونسية ،عدد 105، بتاريخ:2023/09/30.

16. القانون رقم 175 لسنة 2008، بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية للقانون المصري، لسنة 2018.

قائمة المصادر والمراجع

المراسيم

1. الجمهورية الجزائرية الديمقراطية الشعبية المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر 2014، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة 21 ديسمبر 2010، الجريدة الرسمية العدد 57 الصادرة بتاريخ 28 سبتمبر 2014.
2. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 15-261، المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 53، الصادرة بتاريخ 08 أكتوبر 2015.
3. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 21-439، المؤرخ في 07 نوفمبر 2021، يتضمن أعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 86، الصادرة بتاريخ 11 نوفمبر 2021.
4. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم التنفيذي رقم16-267 مؤرخ في 17 أكتوبر سنة 2016، يعدل المرسوم التنفيذي رقم 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية و قضاة التحقيق، الجريدة الرسمية،عدد 62، الصادرة بتاريخ 23 أكتوبر 2016.

الأوامر

1. الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 21-11 مؤرخ في 25 غشت سنة 2021، يتمم الأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 65، الصادرة بتاريخ 26 غشت 2021 .
2. الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 ، المؤرخ في 8 يونيو 1966 ، المتضمن قانون الإجراءات الجزائية المعدل و المتمم.

ثانيا: الكتب

1. إبن منظور، لسان العرب، مادة "حيل" ، طبعة جديدة ، مكتبة نور الالكترونية.
2. بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الأول، الجزائر: دار هومة،2007.

3. طالب أحسن مبارك،جرائم الاحتيال والعوامل الاجتماعية والنفسية المهيئة لها، الرياض: جام عة نايف العربية للعلوم الأمنية،2007.

4. عبود فلاح، هالة لبرارة، "الجريمة الإلكترونية وآليات مكافحتها وطنيا ودوليا"، في: ارتباس نذير، ديابلو محمد نجيب، طارق قادري (محررا)، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، بريطانيا، المركز المغاربي شرق أدنى للدراسات الإستراتيجية، جانفي 2024.

5. مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الثاني أدلة الإثبات الجنائي، الجزائر: دار هومة، 2004.

6. المنيفي أحمد محمد عبد الرؤوف، الاحتيال عبر الانترنت، شبكة الألوكة.

7. المومني نهلى عبد القادر، الجرائم المعلوماتية، الطبعة الثانية، عمان، دار الثقافة، 2010.

8. نادر عبد الكريم الغزوالي، الحماية الجنائية من جرائم الأنترنت دراسة مقارنة، سويسرا: دار نور للنشر الأكاديمي، 2017.

ثالثا: المقالات والأبحاث

1. أبوبكر أحمد همام عبد المجيد، الأثار الإقتصادية للجرائم المعلوماتية وسبل مكافحتها، مجلة جامعة جنوب الوادي الدولية للدراسات القانونية، العدد 06، 2021.

2. بارة سمير، الأمن السيبراني في الجزائر السياسات و المؤسسات، المجلة الجزائرية للأمن الإنساني، العدد04، جويلية 2017.

3. بخيري عبد الرحمان ، مقدم حمر العين، تنظيم جهاز الشرطة واختصاصاتهم على ضوء تعديل قانون الإجراءات الجزائية بالقانون 10/19، مجلة البحوث في الحقوق والعلوم السياسية، العدد 8، 2023/04/04.

4. بشان عبد النور ، الإرهاب المعلوماتي في ضوء قانون العقوبات الجزائري، مجلة صوت القانون، العدد01، 2021/11/30.

5. بلقاسم سميحة، حميد بوشوشه، الجريمة الإلكترونية بعد جديد للأجرام في الجزائر واقعها وآليات مجابهتها، مجلة العلوم الإنسانية، العدد 1، جوان 2023.

6. بن خذير ســـعاد، ميومونة قويدر، الحماية القانونية للهوية الرقمية للمؤمن له اجتماعيا في إطار رقمنة خدمات الضمان الاجتماعي – بطاقة الشفاء نموذجا–، مجلة البحوث في الحقوق و العلوم السياسية العدد 03، 2025/04/22

7. بن خيرة محمد الأمين، مداخلة بعنوان أســباب ودوافع إنتشــار الســلوكات الإجرامية عبر الفايسبوك بين الشباب الجزائري، ملتقى بعنوان الجرائم الإلكترونية في المجتمع الجزائري تشخيص الواقع و تحديات الأمن السيبراني، 2022/03/15.

8. بن يحي سهيلة، أمينة مرابط، السمعة الإلكترونية للمؤسسات، دفاتر MECAS، العدد 01، 2018، ص 218.

9. بوزبرة سـهيلة، الهئية الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيا الإعلام والاتصـال، بين سـرية المعطيات الشـخصـية الإلكترونية و مكافحة الجرائم الإلكترونية، المجلة النقدية للقانون و العلوم السياسية، العدد 02 ، 2022/12/10.

10. بوضـــياف إسمهان ، الجريمة الإلكترونية والإجراءات التشـــريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث، العدد 11، سبتمبر 2018.

11. بوعكاز أسماء ، الأنتربول ودوره في تنفيذ إتفاقيات تسـليم المجرمين في إطار مكافحة الجريمة المنظمة، مجلة الباحث للدراسات الكاديمية، العدد 03، 2021.

12. بوقرة جمال الدين، جمال الدين عنان، القطب الجزائي الوطني لمكافحة الجرائم المتصـــلة بتكنولوجيا الإعلام والاتصـال، مجلة الأسـتاذ الباحث للدراسـات القانونية والسـياسـية، العدد01، 2022/06/10، العدد01.

13. بولحية شـهرزاد، رشـيد خلوفي، تحديات الجريمة الإلكترونية في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 02، 2019.

14. بيدي أمال ، جهود الأمم المتحدة في مكافحة الجريمة السـيبرانية، مجلة البحوث في الحقوق والعلوم الإنسانية، العدد 01، 2022/06/03.

15. تقرير المنتدى الإقتصادي العالمي، التوقعات العالمية للأمن السيبراني، جانفي 2024.

16. جمل عبد اللطيف، عبد الغاني طرايش، الحماية الجنائية للمستهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري: دراسة تحليلية ومقارنة على ضوء القانون الفرنسي، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد 01، 2025/03/20.

17. حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، مداخلة مقدمة ضمن الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة ،2015.

18. خالد علي نزار الشعار، التحقيق الجنائي في الجرائم الإلكترونية، مجلة البحوث القانونية والإقتصادية، العدد 79، 2022.

19. خالدي خديجة، آلية الإتحاد الإفريقي للتعاون الشرطي "أفريبول"، مجلة العلوم الإجتماعية والإنسانية، العدد 15، 2018.

20. خلف فاروق، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد 02، ديسمبر 2015.

21. راضية عيمور، الجريمة الإلكترونية وآلية مكافحتها، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد الأول، 2022/03/31.

22. زناتي محمد السعيد، أحمد بنيني، دور الشرطة الجزائرية في الوقاية من الجريمة ومكافحتها، مجلة تحولات، العدد01، يناير2019.

23. سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، العدد 1، جوان 2021.

24. سويسي فتيحة، التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها، مداخلة مقدمة ضمن الندوة البحثية المنظمة من مركز البحوث القانونية والقضائية، بتاريخ 18 جانفي 2022.

25. شايل نوال، الجريمة الالكترونية في التشريع الجزائري، مجلة سيسيولوجيا، العدد02،2022.

26. شـوقي يعيش تمام، الجريمة المعلوماتية، محاضـرات موجهة لطلبة السـنة الثانية ماسـتر قانون الاعلام الآلي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، جانفي 2019.

27. شـويرب جيلالي ، فائزة مراد ، الاليات الدولية و الوطنية لمكافحة الجريمة السـيرانية ، مجلة الدراسات القانونية و السياسية ، العدد02 ، 2023/06/05.

28. عاقلي فضيلة، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، أعمال المؤتمرات، الجرائم الإلكترونية، طرابلس لبنان: مركز جيل البحث العلمي، 2017

29. عباسـي محمد الحبيب، الحماية الجزائية للمعلومات والوثائق الإدارية من خلال الأمر 21-09، مجلة القانون والعلوم السياسية، العدد 01، 2023.

30. عبد الكافي مريم، صـــورية بوربابة ، جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الالكترونية، مجلة القانون و العلوم السياسية، العدد01، 2022.

31. عبد اللطيف جمل، عبد الغاني طرايش، الحماية الجنائية للمســـتهلك من جرائم الاحتيال الإلكتروني في القانون الجزائري: دراســة تحليلية ومقارنة على ضــوء القانون الفرنســي، المجلة الأكاديمية للبحوث القانونية والسياسية، العدد 01، 2025/03/20.

32. عبسة محمد، معمر فرقاق، المنظمة الدولية للشرطة الحنائية ودورها في مكافحة الجرائم، مجلة القانون، العدد09، ديسمبر 2017.

33. العذار أنيس ، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، العدد 01، 2018.

34. عون فاطمة الزهراء، الإجراءات التشـــريعية المســـتحدثة في مواجهة الجريمة الإلكترونية في القانون الجزائري –القطب الجزائي الوطني نموذجا– مجلة حقوق الإنسـان و الحريات العامة، العدد 02 ، 2022/12/26.

35. عيسـى محمد أحمد سـليمان، التعاون الدولي لمواجهة الجرائم الإلكترونية ـــالمجلة الأكاديمية للبحث القانوني، العدد 02، 2016.

36. غري أسامة، المنظمة الدولية للشرطة الجنائية (الأنتربول) ودورها في مكافحة الجريمة المنظمة، دراسات وأبحاث، العدد 03، 2011/03/15.

37. فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد الثاني، سنة 2015.

38. قادري طارق، الجريمة الالكترونية وحجية الدليل الرقمي والاثبات الجنائي ، المركز المغاربي – شرق أدنى للدراسات الاستراتجية، جانفي 2024.

39. قطاف سليمان ، عبد الحليم بوقرين، مواجهة الجرائم السيرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، العدد 02 ،2022.

40. لزعر عبد العزيز، رشـيد زياني، آلية الإتحاد الإفريقي للتعاون الشـرطي "أفريبول" ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، العدد 03، 2021/09/15.

41. لعمراني آسـيا ، التعاون الدولي في مواجهة الجرائم السـيبرانية: الجزائر نموذجا، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، العدد3، 2012.

42. لعمريوي ليلى، سعد صليح، آليات مواجهة المخاطر السيبرانية في المجتمع الجزائري مقارنة بالنظام الدولي، مداخلة مقدمة ضـــمن الملتقى الافتراضـــي الجرائم الإلكترونية في المجتمع الجزائري: تشخيص الواقع وتحديات الأمن السيبراني، المنعقد بتاريخ 03/15/ 2022.

43. لوكال مريم، قراءة في الإتحاد الإفريقي حول الأمن السـيبراني وحماية المعطيات ذات الطابع الشخصي لسنة2014، مجلة الدراسات القانونية والإقتصادية، العدد 03، 2021/12/30

44. المايل عبد السلام محمد، عادل محمد الشريجي، علي قابوسة، الجريمة الإلكترونية في الفضاء الإلكتروني، مجلة آفاق، العدد 04، 2019.

45. مجموعة العمل المالي الأنتربول، مجموعة إنكونت، تدفقات المالية غير المشـروعة الناجمة عن الاحتيال الذي سهل الانترنات ارتكابها، نوفمبر 2023.

قائمة المصادر والمراجع

46. محمد تذير بن عريفة، يوســـف حوري، اليوروبول كآلية لمكافحة الجريمة الإلكترونية، مجلة الدراسات القانونية والسياسية، العدد 01 ،2025.

47. محمد صـــفاء الدين علي شـــرشـــر محمود، الجهود الدولية لمكافحة جرائم الأنترنت، جلة البحوث القانونية والاقتصادية جامعة المنوفية، العدد 03، المجلد 54، أكتوبر 2021.

48. مسعودي مراد، السياسة الأمنية الأوروبية المشتركة: الواقع والتحديات، مجلة صوت القانون، العدد 02 ،2022/03/31.

49. المطيري سعد فهد سعد ادبيس ، مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية، العدد 05، 2023.

50. ملاك وردة، إشـــكالات تقويض جهود التعاون الدولي في مكافحة الجرائم الدولية، مجلة النبراس للدراسات القانونية، العدد 02، 2025.

51. ناشـــف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، العدد 01، 2022/06/03.

52. نصـــيرات وائل محمد، الطريف غادة عبد الرحمن ، جريمة الاحتيال عبر شـــبكة المعلومات الدولية، مجلة دفاتر السياسة والقانون،العدد19، 2018.

53. نهائلي رابح، ســـعاد قيرة، دور المنظمات الدولية في مكافحة الجريمة المنطمة (منظمة الأمم المتحدة، المنطمة الدولية للشرطة الجنائية نموذجا)، مجلة البحوص القانونية، العدد 02، 2021.

54. نورة عبد اللـــه، الاختصاص القضائي الموسع في المادة الجزائية وفق القانون الجزائري، مجلة الفكر القانوني والسياسي، العدد01، 2022/05/12.

55. هائلي عبد النور ت، ســـعاد قيرة، دور المنظمات الدولية في مكافحة الجريمة المنظمة، (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجا)، مجلة الصراط، العدد 02، 2021.

56. هشـــام بشـــير، الآليات الدولية لمكافحة الرجيمة الإلكترونية، المركز الدولي للدراســـات المستقبلية والإستراتيجية، مصر، 2012.

57. هيئة الحكومة الرقمية، الاحتيال الرقمي، دراسة بحثية، الإصدار 1.0، أوت 2023.

رابعا: الرسائل الجامعية

1. شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية: دراسة مقارنة، أطروحة شهادة الدكتوراه الطور الثالث، كلية الحقوق والعلوم السياسية، جامعة أدرار، 2021/2020.

2. الريامي أسماء مبارك ، أحكام الاحتيال الالكتروني، رسالة ماجستير، كلية القانون، جامعة أبو ظبي،2021-2022.

3. السليطي حمد عبد الله حي بوغانم، تجريم الاحتيال الإلكتروني في القانون القطري و المقارن، رسالة ماجستير، كلية القانون، جامعة قطر،2018.

4. العجمي عبد الله دغش، المشكلات العملية والقانونية للجرائم الإلكترونية-دراسة مقارنة- رسالة ماجستير في القانون العام، جامعة الشرق الأوسط ، 2014.

خامسا: المواقع الالكترونية

1. الصنديد بلال عقل، الاحتيال الإلكتروني وتحدياته المستمرة، 2024-12-08، متوفر على الرابط: //www.google.com/amp/s/www.aljarida.com/article/83723/amp:https تم الاطلاع عليه يوم 10 ماي 2025 الساعة 11:00.

2. شركة حاكافي MCAFEE، مركز الدراسات الاستراتيجية و الدولية، التكاليف الخفية للجرام الالكترونية، 7 ديسمبر 2020، https://www.mcafee.com، تم الاطلاع في 20 ماي2025، على الساعة 01:46.

3. إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، متوفرة على الرابط: African Union Convention on Cyber Security and Personal Data Protection | African Union تم الإطلاع يوم 2025/05/18 على الساعة 18:40.

4. مجلس أوروبا، الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست) 2001/11/23، متوفر على الرابط: https://rm.coe.int/budapest-convention-in-arabic/1680739173 أطلع عليها يوم:2025/05/22 على الساعة 23:53

الانتربول، برنامج الإنتربول لدعم الاتحاد الأفريقي فيما يتصل بأفريبول (ISPA)، متوفر على الرابط:

قائمة المصادر والمراجع

https://www.interpol.int/ar/3/Our-partners/3/1 ، أطلع عليه يوم 2025/05/26 على الســـاعة 09:52

ب. باللغة الأجنبية

1. Skidmore Michael, The A Natomy Of Online Fraud, Perspectives On Policing:Paper 10, April 2024.
2. Ionuț Deaconescu, Cosmin, et al, E-Fraud, Studia z nauk technicznych. N° 2, DWSPiT Polkowice, 2013.
3. Article 313-1 du Code pénal français : “L'escroquerie est le fait, soit par l’usage d’un faux nom…”, www.legifrance.gouv.fr consulté le 27 /05/2025، 20:22.
4. Interpol, Social engineering scams, Available at the link: https://www.interpol.int/en/Crimes/Financial-crime/Social-engineering-scams, accessed on27/05/2025,at08:10.
5. Shewangu Dzomira, Electronic Fraud (Cyber Fraud) Risk In The Banking Industry, Zimbabwe, Risk Governance & Control: Financial Markets & Institutions, Vol 4, Issue 2, 2014.

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

ملخص

يعتبر الاحتيال الإلكتروني في عصر التكنولوجيا الرقمية تهديدا خطيرا للغاية، يهدد أمن وإستقرار المؤسسات العامة، والخاصة على حد سواء، الأمر الذي إستدعى تحركا تشريعيا ومؤسساتيا، دوليا ووطنيا لمواجهة هذه الجريمة والتصدي لها، حيث وضعت التشريعات، والمنظمات الدولية، والإقليمية، آليات وقوانين، للوقوف في وجه هذا الخطر المستمر، وقد كان لهذه الآليات، دور في حماية المؤسسات من الاحتيال الإلكتروني.

خلصت الدراسة إلى أن الإطار القانوني القائم، على الرغم من احتوائه على عديد النصوص القانونية والآليات المؤسساتية المتعلقة بمكافحة جريمة الاحتيال الإلكتروني، إلا أنه ما يزال يواجه عديد التحديات في سبيل التطبيق الفعلي لها، بالنظر إلى الطبيعة المعقدة والمتزايدة لهذه الجرائم التي تواجهها المؤسسات في الفضاء الرقمي. وعليه هناك حاجة ملحة إلى تطوير التشريعات الدولية والوطنية، بما يشمل تحديث القوانين الجنائية، وتعزيز آليات التحقيق والتعاون الدولي، إلى جانب ضرورة رفع مستوى الوعي القانوني والتقني داخل المؤسسات، وتفعيل دور الهيئات الرقابية في الوقاية من هذا النوع من الجرائم.

Abstract

Electronic fraud in the era of digital technology constitutes a highly serious threat that endangers the security and stability of both public and private institutions alike. This has necessitated legislative and institutional responses at both international and national levels to confront and counter this crime. Accordingly, international, regional, and national legislations and organizations have established legal mechanisms and frameworks to combat this persistent threat. These mechanisms have played a significant role in protecting institutions against electronic fraud.

The study concluded that the existing legal framework, despite encompassing numerous legal provisions and institutional mechanisms aimed at combating electronic fraud, still faces several challenges in terms of effective implementation. This is largely due to the complex and evolving nature of cyber fraud crimes confronting institutions in the digital space. Therefore, there is an urgent need to develop both international and national legal systems, including the modernization of criminal laws, the strengthening of investigative procedures, and the enhancement of international cooperation. Additionally, raising legal and technical awareness within institutions and activating the role of regulatory bodies are crucial steps in preventing this category of crimes.

Résumé

La fraude électronique à l'ère de la technologie numérique représente une menace particulièrement grave, mettant en péril la sécurité et la stabilité des institutions publiques et privées. Cette situation a nécessité une réaction législative et institutionnelle, tant au niveau international que national, afin de faire face à ce type de criminalité. Ainsi, des cadres juridiques et des mécanismes ont été mis en place par les législations et les organisations internationales et régionales pour lutter contre ce danger persistant. Ces mécanismes ont joué un rôle important dans la protection des institutions contre la fraude électronique.

L'étude a conclu que le cadre juridique en vigueur, bien qu'il comprenne de nombreux textes législatifs et mécanismes institutionnels relatifs à la lutte contre la fraude électronique, continue de faire face à de nombreux défis en matière de mise en œuvre effective. Cela s'explique notamment par la nature complexe et en constante évolution de ces crimes dans l'espace numérique. Par conséquent, il est impératif de développer les législations internationales et nationales, en modernisant les lois pénales, en renforçant les mécanismes d'enquête et la coopération internationale, et en élevant le niveau de sensibilisation juridique et technique au sein des institutions. Il est également essentiel d'activer le rôle des instances de régulation dans la prévention de ce type de criminalité.