وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

المرجع: .....

قسم :القانون الخاص

مذكرة نهاية الدراسة لنيل شهادة الماستر

التحقيق في الجرائم الإلكترونية وفق التشريع الجزائري

ميدان الحقوق و العلوم السياسية

الشعبة: الحقوق

التخصص: :القانون الخاص

من إعداد الطالبة:

– تونسي أماني شهيناز

تحت إشراف الأستاذة:

– برابح هدى

أعضاء لجنة المناقشة

الأستاذة.....مجبر فاتحة.....رئيسا

الأستاذة..... برابح هدى.....مشرفا مقررا

الأستاذة.....علاق نوال.....مناقشا

السنة الجامعية: 2025/2024

نوقشت يوم:2025/09./30

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه،

السيد: ..... الصفة: ..... طالبة ماستر خاص .....

الحامل لبطاقة التعريف الوطنية رقم: ..... والصادرة بتاريخ: .....

المسجل بكلية: ..... قسم: .....

والمكلف بإنجاز مذكرة ماستر بعنوان:

.....

.....

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

التاريخ: .....

إمضاء المعني

* ملحق القرار الوزاري زقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

إهداء

إلى التي لم تبخل عليا بدعوتها المستجابة وبوقفاتها الدائمة

" أمي الغالية سميرة "

حفظها الرحمان و أطال في عمرها

أهدي ثمرة جهدي ونجاحي إلى الينبوع الذي لا يمل من العطاء

إلى من سعى وشقي لأنعم بالراحة والهناء وأفنى عمره لكي

أصل لهذا المستوى

سلطان قلبي : أبي العزيز جمال رعاه الله

و إلى إخوتي و إلى كل من وسعهم قلبي و لم يذكرهم قلمي

إلى من علموني حروفاً من ذهب إلى من صاغوا لي من علمهم حروفاً ومن فكرهم منارة تنير

لنا مسيرة العلم أساتذتي الكرام.

شكر و تقدير

الحمد لله الذي بنعمته تتم الصالحات نحمده حمدا كثيرا عدد ما ذكره الذاكرون.

الحمد لله الذي أعانني على انجاز هذا العمل المتواضع.

وقال رسول الله صل الله عليه و سلم : " من لم يشكر الناس ، لم يشكر الله عز وجل"

فمن بعد شكر الله عز وجل نشكر الدكتورة

" **برابح هدى** "

على قبولها لإشرافها على هذا البحث كما أتقدم بجزيل الشكر

والتقدير إلى السادة الأساتذة أعضاء لجنة المناقشة على تفضلهم لقبول الاشتراك في مناقشة هذا البحث المتواضع وتقييمه

وإلى كل من بذل معي جهداً ووفر لي وقتاً ونصحني قولاً أسئل الله أن يجازيهم خير الجزاء.

قائمة المختصرات

ج: جزء

ص: صفحة

ط: طبعة

ف: الفقرة

د.س.ن: دون سنةنشر

د.ط :دون طبعة

ج .ر.ج.ج : الجريدة الرسمية للجمهورية الجزائرية

ص ص : من الصفحة ... إلى الصفحة...

ق. ع .ج: قانون العقوبات الجزائري

ق. إ .ج.ج: قانون الإجراءات الجزئية الجزائري

Op.cit : ouvrage précité.

P : page

مقدمة

شهد العالم في العقود الأخيرة تطورًا مذهلًا في مجال تكنولوجيا المعلومات والاتصالات، الأمر الذي أحدث تحولًا جذريًا في مختلف القطاعات[1]، من الإدارة والاقتصاد إلى التعليم والأمن. غير أن هذا التحول الرقمي رافقته تهديدات مستحدثة، أبرزها الجرائم الإلكترونية، التي باتت تُرتكب بأساليب معقدة يصعب كشفها وتتطلب تقنيات تحقيق متقدمة[2].

تمثل هذه الجرائم تحديًا حقيقيًا للمنظومات القانونية والأمنية، نظرًا لطابعها اللامادي، وسرعة تنفيذها، واتساع نطاقها الجغرافي، مما يجعل التحقيق فيها أكثر صعوبة مقارنة بالجرائم التقليدية[3].

بادر المشرّع إلى تكييف الإطار القانوني لمجابهة هذا النوع المستحدث من الإجرام، من خلال إدخال تعديلات جوهرية على المنظومة التشريعية، ففي هذا السياق، تم تعديل قانون العقوبات بموجب القانون رقم 09-01 المؤرخ في 25 فبراير 2009 [4]، حيث أُضيف الفصل السابع مكرر (من المادة 394 مكرر إلى المادة 394 مكرر 8) ، لتجريم مختلف الأفعال التي تمس بنظم المعالجة الآلية للمعطيات، على غرار الدخول غير المشروع إلى الأنظمة، أو عرقلة تشغيلها، أو المساس بالبيانات المخزنة فيها. كما تم تدعيم هذه الآليات من خلال تعديل قانون

[1] – عبد الله ناصر آل فهيد، الجرائم الإلكترونية: دراسة مقارنة في ضوء الشريعة الإسلامية والقانون الوضعي، دار المطبوعات الجامعية، 2017، ص. 45.

[2] – إبراهيم حمد السويلم، "الجريمة الإلكترونية والتحديات القانونية"، مجلة دراسات أمنية، المجلد 12، العدد 2، 2020، ص. 88.

[3] – صابر قسوم، التحقيق الجنائي في الجرائم المعلوماتية، دار هومة، الجزائر، 2019، ص. 91.

[4] – قانون رقم 09-01، ممضي في 25 فبراير 2009، الجريدة الرسمية عدد 15، المؤرخة في 08 مارس 2009، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات المعدل والمتمم بالأمر رقم 21-08 ممضي في 08 يونيو 2021 الجريدة الرسمية عدد 45، المؤرخة في 09 يونيو 2021، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

الإجراءات الجزائية بموجب القانون رقم 17-07 لسنة 2017 [1]، الذي أدخل أدوات جديدة للتحقيق في الجرائم المعلوماتية، كالأمر بجمع الأدلة الرقمية ومراقبة الاتصالات الإلكترونية.

في ظل التحول الرقمي المتسارع وتزايد الاعتماد على التكنولوجيات الحديثة في مختلف مناحي الحياة، برزت الجرائم الإلكترونية كأحد أبرز التهديدات التي تواجه الأفراد والدول على حد سواء. وقد أصبحت هذه الجرائم تتميز بطابعها العابر للحدود، وتعقيد أساليب تنفيذها، وتطور أدوات مرتكبيها، مما أفرز تحديات كبيرة أمام أجهزة إنفاذ القانون وسلطات التحقيق. وفي الجزائر، حاول المشرّع مجاراة هذا الواقع الجديد من خلال إدراج نصوص قانونية تتعلق بالجرائم المعلوماتية ضمن التشريعات الجزائية، لاسيما في قانون العقوبات وقانون الإجراءات الجزائية بعد التعديلات الأخيرة.

ورغم هذه الجهود، لا تزال هناك عدة صعوبات تواجه التحقيق في هذا النوع من الجرائم، سواء من حيث الإثبات الرقمي، أو التعاون الدولي، أو نقص الكفاءات الفنية المتخصصة، ما يثير تساؤلات حول مدى نجاعة الإطار القانوني والمؤسساتي الجزائري في التصدي لهذا التحدي المتنامي

أهمية الموضوع:

تكتسي دراسة تحديات التحقيقات في الجرائم الإلكترونية في التشريع الجزائري أهمية بالغة من الناحيتين النظرية والعملية، وذلك بالنظر إلى الطابع المستجد والمعقد لهذا النوع من الجرائم، والذي يفرض تحديات غير مسبوقة على مختلف الفاعلين في المنظومة العدلية، وعلى رأسهم سلطات الضبط والتحقيق.

[1] – قانون رقم 17-07، ممضي في 27 مارس 2017، الجريدة الرسمية عدد 20، المؤرخة في 29 مارس 2017، الصفحة 5، يعدل ويتمم الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم 21-11، ممضي في 25 غشت 2021 الجريدة الرسمية عدد 65، المؤرخة في 26 غشت 2021، يتمم الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية .

أسباب إختيار الموضوع

يأتي اختيار موضوع " التحقيقات في الجرائم الإلكترونية في التشريع الجزائري" استجابةً لعدة اعتبارات علمية وعملية، من أبرزها:

– مع التحول الرقمي الذي تشهده الجزائر، تزايدت الجرائم المرتكبة عبر الفضاء السيبراني، مما يستدعي دراسة معمقة لفهم طبيعتها وسبل مكافحتها.

– تتميز الجرائم الإلكترونية بتعقيداتها التقنية وصعوبة تتبع الأدلة الرقمية، مما يفرض تحديات على الأجهزة القضائية والأمنية في جمع الأدلة وإثبات الجريمة.

– رغم وجود بعض النصوص القانونية المتعلقة بالجرائم الإلكترونية وخاصة ما استحدث في 2025 من قانون رقم 2025/11 المعدل و المتمم للقانون رقم 2014/14 ، إلا أن هناك حاجة ماسة لتحديثها وتكييفها مع المستجدات التكنولوجية لضمان فعالية التحقيقات والملاحقات القضائية.

– نظرًا للطابع العابر للحدود للجرائم الإلكترونية، فإن تعزيز التعاون مع الهيئات الدولية وتبادل الخبرات يعد أمرًا ضروريًا لمواجهة هذه التحديات بفعالية.

ان القانون الجديد المحدث بواسطة القانونرقم 2025/11 المتمم و المعدل للقانون رقم 2014/14 احدث تطور في محاربة الجريمة الالكترونية و دلك بإضافة حماية وطيدة للمبلغ عن الجرائم و مد توسع و مطالبة حتى خارج حدود البلاد

أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف التي تسهم في فهم وتحليل التحديات المرتبطة بالتحقيق في الجرائم الإلكترونية ضمن الإطار التشريعي الجزائري، وذلك من خلال:

– دراسة القوانين والتشريعات الجزائرية المتعلقة بالجرائم الإلكترونية، مع التركيز على مدى ملاءمتها لمتطلبات التحقيق في هذا النوع من الجرائم.

– رصد الصعوبات التي تواجه الجهات المختصة أثناء التحقيق في الجرائم الإلكترونية، سواء من الناحية القانونية أو الإجرائية.

– تقييم مدى جاهزية الأجهزة الأمنية والقضائية من حيث الكفاءات البشرية والتجهيزات التقنية اللازمة لمواجهة الجرائم الإلكترونية.

إشكالية الدراسة

تدور الإشكالية الرئيسية لهذه الدراسة حول السؤال التالي:

إلى أي مدى تمكن المشرّع الجزائري من توفير إطار قانوني وإجرائي فعال لمواجهة التحديات المتعلقة بالتحقيق في الجرائم الإلكترونية؟

وتتفرع عن هذه الإشكالية عدة تساؤلات فرعية، من بينها:

– ما هي الخصائص التي تميز الجريمة الإلكترونية وتزيد من صعوبة التحقيق فيها؟

– هل نجح التعديل التشريعي في قانون العقوبات والإجراءات الجزائية في سد الفراغ القانوني في هذا المجال؟

– ما مدى جاهزية الجهات المختصة (الشرطة القضائية، القضاء، الخبراء) للتعامل مع الجرائم الرقمية؟

المنهج المتبع في الدراسة

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية الوطنية ذات الصلة بالجرائم الإلكترونية،.

– للإجابة على هذه الإشكالية اتبعنا خطة الثنائية تنقسم إلى فصلين :

الفصل الأول بعنوان الإطار للتحقيق في الجرائم الإلكترونية في التشريع الجزائري ،أما الفصل الثاني سنتطرق فيه التحديات التي تواجه أجهزة التحقيق في مكافحة الجرائم الإلكترونية في الجزائر .

وفي الأخير أنهينا هذا البحث بخاتمة تتضمن مجموعة من النتائج والتوصيات التي توصلنا لها من خلال هذه الدراسة.

الفصل الأول
الإطار المفاهيمي للتحقيق في الجرائم الإلكترونية في التشريع الجزائري

أصبحت التكنولوجيا والإنترنت جزءًا لا يتجزأ من الحياة اليومية، حيث غزت هذه التقنيات كافة ميادين الحياة الشخصية، الاقتصادية، والاجتماعية، ومع هذا التقدم السريع في مجال التحول الرقمي، ظهرت الجرائم الإلكترونية كتهديد جديد يشكّل تحديًا كبيرًا للأنظمة القانونية حول العالم[1]، ولم يكن التشريع الجزائري بعيدًا عن هذه التحولات، بل بدأ في تطوير وتنظيم قوانين للتعامل مع هذه الجرائم، التي باتت تؤثر بشكل متزايد على الأفراد والمؤسسات على حد سواء[2].

تتمثل الجرائم الإلكترونية في الأنشطة غير القانونية التي تتم عبر الإنترنت أو باستخدام وسائل تكنولوجية، مثل القرصنة الرقمية، الاحتيال الإلكتروني، التهديدات والابتزاز الإلكتروني، والتجسس الإلكتروني، ولأن هذه الجرائم تتسم بسرعة التنفيذ وصعوبة الملاحقة القانونية عبر الحدود الجغرافية، فقد أصبح من الضروري أن تواكب الأنظمة القانونية هذه التطورات من خلال سن تشريعات جديدة أو تعديل التشريعات القائمة[3].

وقد بدأ التشريع الجزائري التفاعل مع هذا الواقع من خلال وضع إطار قانوني لمكافحة الجرائم الإلكترونية، حيث شملت النصوص مجموعة من القوانين والأنظمة تهدف إلى توفير الحماية القانونية للأفراد والمجتمع. وتناولت هذه التشريعات الجرائم الإلكترونية عبر عدة محاور، من بينها حماية البيانات الشخصية، تنظيم استخدام الإنترنت، ومعاقبة مرتكبي الجرائم الرقمية بمختلف أنواعها[4].

---

[1] – محمد عبد الحليم غنيم، الجريمة الإلكترونية: التحديات وسبل المواجهة، دار الفكر الجامعي، الإسكندرية، 2018، ص. 22.

[2] – أحمد بلحاج، "التحول الرقمي والجرائم الإلكترونية"، مجلة الدراسات القانونية والسياسية، العدد 14، جامعة ورقلة، 2020، ص. 95.

[3] – عبد القادر بوشاشي، شرح قانون العقوبات – القسم الخاص – الجرائم الماسة بأنظمة المعالجة الآلية، دار هومة، الجزائر، 2021، ص. 57.

[4] – القانون رقم 09-01 المؤرخ في 25 فبراير 2009، المعدل والمتمم لقانون العقوبات، الجريدة الرسمية، العدد 15، 2009.

وعليه، يتعين دراسة هذا الفصل في مبحثين، حيث نتطرق ماهية الجرائم الإلكترونية وأنواعها في المبحث الأول، مواجهة الجرائم الإلكترونية في التشريع الجزائري في المبحث الثاني.

المبحث الأول: ماهية الجرائم الإلكترونية وأنواعها

في عصر الثورة الرقمية، الذي أصبح فيه الإنترنت جزءًا لا يتجزأ من حياتنا اليومية، ظهرت الجرائم الإلكترونية كظاهرة حديثة تهدد الأفراد والمجتمعات على حد سواء. فقد أصبحت المعلومات والبيانات المخزنة رقميًا هدفًا للعديد من الأنشطة الإجرامية التي تتراوح بين السرقة والتلاعب وصولًا إلى التهديدات والابتزاز[1].

وبالرغم من أن هذه الجرائم قد تكون مشابهة في بعض جوانبها للجرائم التقليدية، إلا أنها تتسم بخصائص فريدة تجعلها تستدعي اهتمامًا خاصًا من قبل المشرعين تعرَّف الجرائم الإلكترونية بأنها الأنشطة غير القانونية التي تُنفذ باستخدام الوسائل الإلكترونية أو الإنترنت، بهدف إلحاق الضرر بالأفراد أو المؤسسات أو انتهاك الأنظمة والتشريعات. وتشمل هذه الجرائم مجموعة واسعة من الأنشطة الإجرامية التي تتعلق بالأنظمة المعلوماتية، مما يستدعي تعريفًا دقيقًا لها وتحليلًا مستفيضًا للأنواع المختلفة التي قد تتخذها[2].

يشهد العالم اليوم زيادة متسارعة في الجرائم الإلكترونية، التي أفرزت الحاجة إلى تقنيات جديدة وأساليب قانونية مبتكرة لمواجهتها. من هنا، يسعى هذا المبحث إلى تقديم تعريف دقيق للجرائم الإلكترونية، مع تصنيف أنواعها المختلفة، وذلك لفهم طبيعة هذه الجرائم وأثرها على الأفراد والمجتمع[3].

[1]– القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة في 16 أوت 2009.

[2]– بن عبو عبد القادر، الجرائم الإلكترونية في التشريع الجزائري، دار هومة، الجزائر، 2017. ص 12.

[3]– غزالي زهيرة، الجريمة المعلوماتية والتصدي لها في التشريع الجزائري، مجلة دفاتر السياسة والقانون، جامعة مولود معمري تيزي وزو، العدد 18، 2017.

وسنتناول في هذا المبحث تعريف الجرائم الإلكترونية، كما سنستعرض الأنواع المختلفة لها، مثل القرصنة الإلكترونية، الاحتيال الإلكتروني، الابتزاز الإلكتروني، التجسس الإلكتروني، وغيرها من الأنشطة الإجرامية التي تشهد تزايدًا في عالم الإنترنت[1]. وسنسلط الضوء أيضًا على التحديات القانونية التي تفرضها هذه الجرائم، وكيفية التصدي لها من خلال الأنظمة القانونية الحديثة[2]، وتهدف هذه الدراسة إلى تقديم إطار شامل يساعد في فهم طبيعة الجرائم الإلكترونية، وتصنيفها بشكل دقيق، والتعرف على الأدوات التي يمكن أن تُستخدم لمكافحتها، خاصة في ظل التقدم التكنولوجي السريع والتطور المستمر في أدوات وأساليب هذه الجرائم.

المطلب الأول: مفهوم الجرائم الإلكترونية على مستوى العالم

شهدت العقود الأخيرة تطورًا غير مسبوق في مجال التكنولوجيا الرقمية، مما أسهم في تحول العالم إلى مجتمع يعتمد بشكل كبير على الإنترنت والأدوات التكنولوجية في شتى مجالات الحياة[3]،لكن هذا التحول، على الرغم من فوائده الكبيرة، حمل معه أيضًا تحديات أمنية وقانونية، أبرزها ظهور الجرائم الإلكترونية كظاهرة تهدد الأفراد والمجتمعات والحكومات.

الجرائم الإلكترونية هي تلك الأفعال الإجرامية التي تُنفذ باستخدام وسائل تكنولوجيا المعلومات أو الإنترنت، وتشمل مجموعة واسعة من الأنشطة غير القانونية مثل القرصنة، الاحتيال الإلكتروني، الابتزاز، التجسس، وغيرها من الأفعال التي تستهدف الأنظمة الرقمية والمعلومات الشخصية أو المالية[4].

[1] – يوسف بوشيخي، الجرائم الإلكترونية: دراسة قانونية في التشريع الجزائري والمقارن، دار هومة، الجزائر، 2021، ص. 33

[2] – محمد علي مكاوي، الجرائم الإلكترونية بين الفقه والقانون، دار الجامعة الجديدة، الإسكندرية، 2019، ص. 76.

[3] – نوال رزيق، "التحقيق في الجرائم الإلكترونية في ظل التشريع الجزائري"، مجلة القانون والأعمال الدولية، العدد 23، جامعة تلمسان، 2022، ص. 112.

[4] – عبد الله ناصر آل فهيد، الجرائم الإلكترونية: دراسة مقارنة في ضوء الشريعة الإسلامية والقانون الوضعي، دار المطبوعات الجامعية، 2017، ص. 44.

ونتيجة لتطور الإنترنت واستخدامه الواسع، أصبحت هذه الجرائم تمثل تهديدًا عالميًا يتطلب تنسيقًا دوليًا لمكافحتها، حيث لا تقتصر هذه الجرائم على حدود دولية معينة، بل تمتد عبر الحدود الجغرافية لتؤثر على الأفراد والمؤسسات في جميع أنحاء العالم[1].

إحدى السمات الرئيسية للجرائم الإلكترونية هي قدرتها على التسلل إلى أنظمة المعلومات والشبكات الرقمية دون الحاجة للتواجد الفعلي، مما يجعل من الصعب تحديد مكان ارتكاب الجريمة أو الشخص المسؤول عنها. ولذلك، تتسم الجرائم الإلكترونية بتعقيد خاص من حيث الملاحقة القانونية والتصدي لها، حيث تفرض تحديات كبيرة على الأنظمة القانونية في جميع أنحاء العالم[2].

في هذا المطلب، سنناقش مفهوم الجرائم الإلكترونية على مستوى عالمي، مع الإشارة إلى أبرز أنواعها، والتهديدات التي تمثلها للمجتمعات المعاصرة. كما سنستعرض كيف تختلف التشريعات الدولية في التصدي لهذه الجرائم، والجهود المبذولة على الصعيد الدولي لتطوير آليات قانونية لمكافحة الجرائم الإلكترونية[3].

الفرع الأول: تعريف الجرائم الإلكترونية

الجرائم الإلكترونية أصبحت من أبرز التحديات القانونية في عصر تكنولوجيا المعلومات والإنترنت، خاصة في ظل الانتشار الواسع لاستخدام الشبكات الرقمية في الحياة اليومية. والجزائر، كغيرها من الدول، تسعى إلى تنظيم هذه الظاهرة ووضع قوانين تُحارب الجرائم المرتكبة عبر الفضاء الرقمي[4].

---

[1] – محمود عبد الله البسيوني، "الجرائم الإلكترونية: المفهوم والتحديات"، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 61، 2020، ص. 132.

[2] – ريم غربي، "الجرائم السيبرانية والتحديات القانونية في الجزائر"، مجلة دفاتر السياسة والقانون، جامعة خنشلة، العدد 28، 2021، ص. 93.

[3]– بوفنشة عبد الرحمن، الجرائم الإلكترونية: المفهوم والأنواع والوسائل القانونية لمكافحتها في الجزائر، مجلة الدراسات القانونية والسياسية، جامعة سطيف، العدد 12، 2019. ص169.

[4]– بوفنشة عبد الرحمن، المرجع السابق ص 170.

الجرائم الإلكترونية هي أفعال غير قانونية ترتكب باستخدام وسائل التكنولوجيا الحديثة مثل الإنترنت، أجهزة الحاسوب، أو الهواتف الذكية، بهدف انتهاك حقوق الأفراد أو المؤسسات، أو التسبب في أضرار للأنظمة المعلوماتية والبيانات الإلكترونية. تشمل هذه الجرائم العديد من الأنشطة مثل القرصنة الإلكترونية، الاحتيال الإلكتروني، التجسس الإلكتروني، الابتزاز الإلكتروني، التهديدات الإلكترونية، و التشهير عبر الإنترنت، وغيرها من الأفعال التي تضر بالأمن الرقمي للمجتمعات.

أولا : تعريف الجريمة الإلكترونية

تعددت وجهات النظر بخصوص هذا النوع المستجد من الجرائم، حيث لا يوجد إجماع على تعريف الجريمة الإلكترونية؛ من حيث تحديدها والجرائم التي تشملها، وهناك غياب لتعريف عام، أو إطار نظري متسق في هذا الحقل بشأنها، وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية والسيبرانية للدلالة عليها، وكلها تعكس فجوات مهمة في التعريف

1- التعريف الفقهي للجريمة الإلكترونية :

إزاء المساعي الموجهة نحو التصدي لظاهرة الإجرام المعلوماتي، فإنّ المصطلحات التي تناولت هذه الظاهرة، قد اختلفت فيما بينها، حيث لم يتفق الفقه الجنائي على تسمية موحدة للجريمة المعلوماتية، فالبعض أطلق عليها جرائم إساءة[1] استخدام تكنولوجيا المعلومات والاتصالات، والبعض يسميها جرائم الكمبيوتر والأنترنت وهناك من يطلق عليها الجرائم المستحدثة؛ إضافة إلى عدم الاتفاق على تعريف تشريعي شامل لهذا النوع من الجرائم، وقد ذهب الفقهاء في تعريف الجريمة الإلكترونية مذاهبا ،مختلفة ونتيجة للتطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، فإن ذلك حال دون وضع تعريف فقهي جامع

[1]- أمينة بوشعرة ، سهام موساوي، الإطار القانوني للجريمة الإلكترونية ، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية 2018 ، ص:04

وشامل، إذ تباينت في هذا السياق الاتجاهات الفقهية بين موسع لمفهوم الجريمة الإلكترونية، وبين مضيق لمفهومه [1]وسنحاول إبراز هذين الاتجاهين وفقا لما يلي :

أ- الاتجاه الضيق لمفهوم الجريمة الإلكترونية

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وفقا لمعايير متعددة، سواءا كانت وفقا لمعيار شخصي من حيث توفر المعرفة والدراية بالتقنية، أو وفقا لمعيار موضوع الجريمة، والمعايير المتعلقة بالبيئة المرتكب فيها الجريمة، وسنسرد في هذا الإطار بعض التعريفات الفقهاء القانون الجنائي، فقد عرفتها الدكتور هدى قشقوش بأنها كل سلوك غير مشروع أو غير مسموح به، فيما يتعلق بالمعالجة الآلية للبيانات أو نقل البيانات"[2].

يعاب على هذا التعريف أنه يخرج من نطاق الجريمة الإلكترونية، عدد كبير من الأفعال غير المشروعة، والتي يستخدم فيها الحاسب الآلي، كأداة لارتكابها كالاحتيال المعلوماتي، وقد أخذت وزارة العدل الأمريكية بتعريف للجريمة الالكترونية في تقرير صادر عنها عام 1989 المتعلق بجرائم المعلوماتية بكونها : كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى"[3].

يتبين لنا من خلال هذا التعريف أنه لا يكف فقط أن تتوافر معرفة تكنولوجيا الحاسبات الآلية، بدرجة كبيرة من أجل ارتكاب الجريمة الإلكترونية، ولكن أيضا من أجل ملاحقتها ومتابعتها والتحقيق فيها، بمعنى لابد

من توافر قدر كبير من العلم بهذه التكنولوجيا، لدى الجناة والقائمين على معاينة وملاحقة مرتكبيها.

---

[1]- ذياب موسى البداينة، الجرائم الإلكترونية : المفهوم والأسباب، ورقة علمية مقدمة للملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من 02 إلى 04 سبتمبر 2014، كلية العلوم الاستراتيجية، عمان، الأردن، ص 08.

[2]- نداء نائل فايز المصري خصوصية الجرائم المعلوماتية، مذكرة مقدمة لنيل درجة الماجيستر ، في القانون العام ، بكلية الدراسات العليا في جامعة النجاح الوطنية ، نابلس ، فلسطين ، 2017 ، ص: 03.

[3] - U.S. Department of Justice, Computer Crime: Criminal Justice Resource Manual, Washington D.C., 1989, p. 3.

ب- الاتجاه الموسع لمفهوم الجريمة الإلكترونية

على عكس الاتجاه السابق يرى فريق أخر من الفقهاء، ضرورة التوسع في مفهوم الجريمة الإلكترونية أو المعلوماتية، وعدم حصرها في الحاسوب وحده، أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية؛ فيعرفونها بأنها كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل"؛

كما عرفتها منظمة التعاون الاقتصادي والتنمية بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية [1].

أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين إلى خطورة الجرائم الإلكترونية وتنامي تهديدها للأمن الوطني والدولي[2]، فقد تبنى التعريف التالي للجريمة الإلكترونية: " هي أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية ؛

نحن من جانبنا نتفق مع هذا التعريف، إذ أنه التعريف الذي استطاع الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة الإلكترونية، سواء التي قد تقع بواسطة النظام المعلوماتي، أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما يشمل التعريف الجرائم التي من الممكن أن تقع في بيئة إلكترونية، فهذا التعريف لم يركز على فاعل الجريمة ومقدراته التقنية ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة

[1]- محمد علي قطب الجرائم المعلوماتية وطرق مواجهتها ، مركز الإعلام الأمني، وزارة الداخلية ، الأكاديمية الملكية للشرطة ، مملكة البحرين ، 2010 ، ص: 09

[2] – الأمم المتحدة، الوقائع الرسمية لمؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، فيينا، 10–17 أبريل 2000، وثيقة الأمم المتحدة رقمA/CONF.187/4 ، ص. 22.

الإلكترونية، بل إنه حاول عدم حصر الجريمة الإلكترونية في نطاق ضيق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب.

نستشف من خلال عرضنا للتعاريف الفقهية سالفة الذكر، حول مفهوم الجريمة الإلكترونية أنها اقتصرت على مفاهيم عامة مرتبطة بجهاز الحاسوب من جهة، وبالبيانات من جهة أخرى، فالفقهاء الذين تبنوا الاتجاه الموسع لتعريف الجريمة الإلكترونية، كانوا أكثر حكمة لأن هذا العالم الافتراضي سريع التطور، وأي تضييق في مفهوم الجريمة الإلكترونية سوف يقتن مفهوم الجريمة الإلكترونية، كما أنه باستقرائنا لمختلف التعاريف، نجد أن تعريف منظمة التعاون الاقتصادي والتنمية، يتسم بالوضوح والشمول للأسباب التالية: تحديده لماهية السلوك الإجرامي، للجريمة التي قد تقع به إذ شمل كل من الفعل الإيجابي والسلوك السلبي، المتمثل في الامتناع؛ تعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة الجرائم التقنية، وذلك لربطه بين الجريمة وأي تدخل للتقنية المعلوماتية بصفة مباشرة أو غير مباشرة؛ يعبر عن الطابع التقني المميز، الذي تنطوي تحته أبرز صور الجريمة الإلكترونية؛ يتيح إمكانية التعامل مع التطورات المستقبلية التقنية[1].

إن تعريف الجريمة الإلكترونية على العموم يقوم على ثلاث عناصر السلوك ووصفه والنص القانوني على تجريم السلوك وايقاع العقوبة، ثم محل الاعتداء في الظاهرة الإجرامية المستحدثة متمثلا في معطيات الحاسوب، خلافا للجريمة عموما، إذا هي سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله،

معطيات الحاسب الألي فالسلوك يشمل الفعل الإيجابي والامتناع عن العمل، مع الاعتبار أن إسباغ الصفة الجرمية لا يتحقق في الميدان الجنائي إلا بإرادة المشرع، ومن خلال النص القانوني ومحل الجريمة ذاتها دائما هو معطيات الكومبيوتر بدلالاتها الواسعة .

[1]- سفيان سوير، جرائم المعلوماتية ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية ، وعلوم الإجرام ، كلية الحقوق ، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2011، ص12.

2- موقف المشرع الجزائري من الجريمة الإلكترونية

أدت الحداثة التي تتميز بها الجريمة الإلكترونية، واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها، مما انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، والمشرع الجزائري وللدلالة على الجريمة الإلكترونية؛ اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال [1].

وكخطوة أولى لمواجهة ما يعرف بجرائم تكنولوجيات الإعلام والاتصال، أجرت الحكومة الجزائرية بعض التعديلات على قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل، والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966 والمتضمن قانون العقوبات[2]، حيث استحدثت عقوبات تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، وهو ما نصت عليه المواد 394 و 394 مكرر 1 إلى 7 من القسم السابع مكرر ، وتراوحت هذه العقوبات من شهرين إلى ثلاث سنوات، مع دفع غرامة مالية من 50000دج إلى 5000000 دج، وذلك حسب حجم ودرجة خطورة الجريمة الالكترونية المرتكبة، كما قام المشرع الجزائري بتجريم الأفعال الماسة بأنظمة الحاسب الآلي بسبب ما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، وهو ما دفعه إلى تعديل قانون العقوبات 04/15؛ تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات [3].

يعد قانون 09/04 أول قانون في الجزائر اهتم بكيفية تبادل المعلومات الرقمية، وتجري فيه كل أنواع المعاملات والخدمات الالكترونية، وقد عرفت المادة 02 منه الجريمة الالكترونية

[1]- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، في ضوء الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات ، قانون العقوبات ، ق إ ج ، قوانين خاصة ، دار الجامعة الجديدة ، الإسكندرية ، 2019 ، ص 50.

[2] – قانون رقم 04-15، ممضي في 10 نوفمبر 2004، الجريدة الرسمية عدد 71، المؤرخة في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

[3]- القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة في 16 أوت 2009.

على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات[1]، وأية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية [2].

توضح هذه المادة نية المشرع الجزائري في تبني مبدأ المرونة في الصياغة التشريعية، للتمكن من استيعاب الأنشطة الاجرامية الالكترونية التي يتعذر حصرها وتحديدها، نظرا لسرعة وتطور أساليبها، تبعا للتطور التقني، وهو ما يتيح للقاضي حرية واسعة في التقدير، وانطلاقا من فحوى هذه المادة، يتبين أن المشرع الجزائري قسم هذه الجرائم إلى ثلاثة أنواع:

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات؛
- جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية؛
- جرائم ترتكب أو يسهل ارتكابها عن طريق نظام للاتصالات الالكترونية) يتضح لنا من موقف المشرع الجزائري بشأن تعريف هذه الجريمة، أنه أعطى لها مفهوما واسعا؛ بالرغم من تحديده لمجالها من خلال كونها متصلة بتكنولوجيات الاعلام والاتصال، إلا أنه ترك فيما بعد المجال واسعا لتضم إليها أي نوع من الجرائم التي قد يسفر عنها التطور التكنولوجي، خاصة وأن هذا الميدان شهد تطورا وتسارعا كبيرين، وقد نصت المادة السابقة على العبارة التالية: "... أو أي جريمة أخرى ترتكب، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية[3].

من خلال استعمال المشرع الجزائري لمصطلح الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، للدلالة على الجرائم الالكترونية، فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة، فالأولى تقوم على استخدام الوسائل التقنية لإدارة وتنظيم ومعالجة البيانات، أما

[1] – المادة 2 من القانون رقم 09-04 .

[2]- يزيد بوحليط، مرجع سابق، ص 55.

[3]- محمد السعيد زناتي الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية ، مجلة إيليزا للبحوث والدراسات، المجلد 02، العدد 01 ديسمبر 2017 ص ص 28-40

تكنولوجيات الاتصال فتقوم على وسائل تقنية لنقل المعلومات بجميع دلالاتها، ولذلك فقد وُفق المشرع الجزائري في نظرنا باختياره مصطلح الجرائم المتصلة بتكنولوجيات الاعلام والاتصال التي تتوافق مع مصطلح الجرائم الالكترونية بالمفهوم الواسع، وهذا للأسباب التالية:

– الجرائم الناشئة في البيئة الرقمية هي جرائم حديثة يرتبط مفهومها بظهور التكنولوجيا الحديثة، وما يواكبها من تطور مستمر في تشغيل ونقل وتخزين المعطيات في شكل الكتروني؛

– استعمال هذا المصطلح له مفهوم واسع، فهو يشمل كل الاعتداءات التي تتم في بيئة افتراضية، بما فيها الجرائم التي تقع على نظم المعالجة الآلية للمعطيات، وتكون وسيلة لارتكابها[1].

– يعبر هذا المصطلح عن الطابع التقني والمميز للجرائم الالكترونية. لم يحدد المشرع صور السلوك المجرم الذي يرتكب أو يسهل ارتكابه ضمن منظومة معلوماتية، أو نظام للاتصالات الالكترونية؛ – تضمن هذا التعريف التكرار، كون أن مفهوم نظام الاتصالات الالكترونية يندرج تحت مصطلح المنظومة المعلوماتية، ذلك أن المشرع الجزائري عرف هذه الأخيرة بموجب أحكام المادة 02، على أنها نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات، تنفيذا لبرنامج معين، ومن وجهة نظرنا؛ فإن تعريف الجريمة الالكترونية الأقرب للصواب هو أنها تمثل كل اعتداء يتم باستخدام النظام المعلوماتي، وكان له دور رئيسي في السلوك المجرم.

ثانيا : خصائص الجريمة الإلكترونية

تتميز الجريمة الالكترونية بطبيعة خاصة تجعلها تختلف عن غيرها من الجرائم؛ وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي، مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم، عددا من السمات التي انعكست بدورها على مرتكبي

[1]- بوحليط، مرجع سابق، ص ص 59، 60.

هذه الجريمة الذين أصبح الواحد منهم يُعرف بالمجرم المعلوماتي، نظرا لتميزه في أفعاله عن الأشكال التقليدية للإجرام.

1- خصائص الجريمة الالكترونية المشتركة مع بعض الجرائم الاخرى

تتسم الجريمة الالكترونية بدرجة من الخطورة البالغة، والحجم الكبير للأضرار التي تنشأ عنها، وهي بذلك تشترك مع بعض الجرائم كالإرهاب والاتجار بالمخدرات، ومن هذه الخصائص يمكن تفصيل ما يلي:

أ - خطورة الجرائم الالكترونية

تنطوي الجريمة الإلكترونية على قدر كبير من الخطورة، وذلك لما لها من آثار مباشرة على الإنسان في فكره وحياته الخاصة، كما تمس المؤسسات في نشاطها الاقتصادي، ويقع ضررها كذلك على أمن البلاد الوطني، خاصة في حال المساس بالمعلومات والأسرار السياسية أو العسكرية أو الاقتصادية[1].

وفي جانب آخر، فإن هذه الجرائم تُعد انتهاكًا صارخًا لحرمة الحياة الخاصة، إذ يُعد الاطلاع غير المشروع على خصوصيات الأفراد جريمة يعاقب عليها القانون[2]، لما فيها من مساس بحق أساسي من حقوق الإنسان، وهو الحق في حماية الخصوصية، الذي كفلته مختلف التشريعات الوطنية والدولية[3].

2- الجرائم الالكترونية باعتبارها جرائما عابرة للحدود

إن البيئة الافتراضية لا تعترف بالقيود ولا بالحدود، فقد يكون الجاني في بلد؛ في حين أن جريمته وضحاياها قد يكونون في بلد آخر، كما قد يمتد الضرر الحاصل إلى بلد ثالث أو أكثر في الوقت نفسه، فالجريمة الالكترونية شكل من الجريمة العابرة للحدود، يستفيد مقترفوها

[1] – عبد القادر بوشاشي، المرجع السابق ، ص. 344.

[2] – نوال رزيق، المرجع السابق ، ص. 119.

[3] – أحمد عبد الله المصري، الجرائم الإلكترونية وحق الخصوصية في القانون الدولي، دار الجامعة الجديدة، الإسكندرية، 2020، ص. 76.

من أثر التقنية في اختزال المسافات، وإخفاء الأثر الالكتروني، وكذا السرعة الزمنية الهائلة في تداول المعلومات والحصول عليها، ووقوع كثير من العمليات الالكترونية في نفس الوقت، ضمن ما يعرف باللحظية المعلوماتية، والعمل عن بعد الذي يعدم التواجد المادي للمجرم المعلوماتي، ويُصعب عملية البحث بشأنه، ويقتضي تتبع المعاملات الالكترونية التي تتجاوز حدود الدولة الواحد، في حرص على الربط بين الفعل والنتيجة الإجرامية له من خلال المعطيات محل الجريمة، يستوجب الشكل العابر للحدود للجريمة الالكترونية تظافر الجهود التشريعية، وعمليات التنسيق الأمني والمعلوماتي من أجل التصدي لهذا النمط من الإجرام، والإيقاع بالمجرمين وتقديمهم للقضاء [1].

كما يستلزم هذا الوضع تطوير الأنشطة الوقائية والإجراءات الردعية التي تحول دون تنامي هذا الشكل الخطير من الجرائم، كما أنه من الوسائل المجدية في هذا الإطار تفعيل اتفاقيات الملاحقة القانونية وتسليم المجرمين، ووضع نشرات بشأنهم، وتجميد مدخراتهم والعوائد المالية التي يجنونها من الأفعال الاجرامية المقترنة بالأنظمة المعلوماتية. الفرع الثاني: الخصائص التي تنفرد بها الجريمة الالكترونية عن الجرائم الأخرى: تنفرد الجريمة الإلكترونية عن سواها من الجرائم الأخرى، بسمات تضفي عليها طابعا مميزا ومنها والتي يمكن إجمالها على النحو التالي:

أولا: يتطلب ارتكابها وجود حاسب آلي ومعرفة تقنية:

يعد الكومبيوتر الأداة الأساسية لارتكاب كافة الجرائم الإلكترونية، والمقصود من وجوده هنا أن يستعان به كوسيلة لتنفيذ هذه الجرائم، ذلك أن الحاسب الألي وإن كان موضوعا للاعتداء شاشته فلا تثور لدينا أية مشكلة، ذلك لأن نصوص قانون العقوبات التقليدية كفيلة بردع الجاني لأن الحاسب هنا لا يتعدى كونه من الأموال المادية المنقولة، ولكن تثور المشكلة

[1]- رحموني أحمد ، خصائص الجريمة الإلكترونية ومجالات استخدامها "، مجلة الحقيقة ، العدد 41 ، 2018

عندما يطال الاعتداء على ما يمكن أن يسمى بفن الحاسب الآلي، كتدمير برامجه وسرقتها وتقليدها، أو العبث ببيانات الحاسب أو المعلومات المختزنة،

وهذا هو المقصود من جرائم الحاسب الآلي، والتي يصلح فيها الحاسب أن يكون موضوع الاعتداء فيها[1].

إضافة إلى ما سبق فإنّ الجريمة الإلكترونية تتطلب الإلمام بتقنيات الكومبيوتر ونظم المعلومات، سواء لارتكابها أو التحقيق فيها أو ملاحقتها قضائيا، لذلك يجد مأموري الضبط القضائي أحيانا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية على هذا النوعية من الجرائم، فضلا عن صعوبة إجراءات التحريات السرية، وتتبع مسار العمليات الإلكترونية العابرة للحدود، فقد يتسبب المحقق بدون قصد، أو بطريق الخطأ في إتلاف الدليل الإلكتروني، أو تدميره كما في حالة محو البيانات الموجودة في الأسطوانة الصلبة، كما قد يتجاهل المحقق الدليل الإلكتروني ظنا منه أنه غير مهم، أو لا يقوم بمصادرة جهاز الكومبيوتر المستعمل في الجريمة، أو ملحقاته من طابعة أو ماسح ضوئي.

ثانيا: صعوبة اكتشاف الجريمة وإثباتها:

توصف الجرائم الإلكترونية بأنّها خفية ومستترة في أغلبها بحكم أن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة واحترافية، كإرسال فيروسات وسرقة الأموال والبيانات الخاصة، وإتلافها والتجسس وسرقة المكالمات... إلخ، ويمكن رد الأسباب التي تقف وراء صعوبة اكتشافها، إلى عدم تركها لأثار ،خارجية، كما في الجرائم التقليدية فهي تتم في بيئة افتراضية، كما توفر التقنية المعلوماتية للمجرم إخفاء أثار الجريمة عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية، وبالتالي محو أثاره مما يخلق صعوبات بالغة لسلطات البحث والتحري في ملاحقته، وضمان عدم إفلاته من العقاب، خاصة وأن تنفيذها لا يتطلب وجود الفاعل في مكان

[1]- أنيس العذار ، مكافحة الجريمة الإلكترونية "، المجلة الأكاديمية للبحث القانوني ، المجلد 17 ، العدد 01 ، 2018، ص432

الجريمة، بل يمكنه تنفيذ جريمته وفي دولة بعيدة ، كل البعد عن الفاعل [1].، كما أن معظم الجرائم الإلكترونية تم اكتشافها بمحض الصدفة، وبعد مرور وقت طويل، إضافة إلى أنه لا يتم في الغالب الإبلاغ عن الجرائم الإلكترونية، إما لعدم اكتشافها من طرف الضحية أو خوفا من التشهير به، لذلك ما يرتكب فعلا من جرائم إلكترونية أكبر بكثير مما يصرح به. [2].

ثالثا: جرائم هادئة وصعبة الإثبات:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها، كالقتل والسرقة وغيرها من الجرائم، فالجرائم الإلكترونية تعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم على معرفة تقنية للكومبيوتر، وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدّل، أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أن البعض يشبهها بجرائم العنف؛ مثلما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية، نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف[3].

في جانب آخر فإنّ تلك الجرائم صعبة الإثبات، وذلك عائد لصبغتها اللامادية التي تجعل من محو الأدلة الجزائية أمرا سهلا، إذ يمكن للمجرم الإلكتروني أن يمحو مئات الآلاف من البيانات من الحاسب الآلي بضغطة زر واحدة، وبإمكانه عدم تخزينها أصلا وعدم معالجتها على حسابه الشخصي، كما قد يعمد بعض الجناة إلى تشفير المعطيات المجرمة، بحيث يستحيل فك رموزها من طرف السلطات الأمنية، ويمكن أن يكون ذلك على مستوى التخزين أو على مستوى تبادل المعلومات بين مجرمي الأنترنت على الشبكة العنكبوتية، حيث تطورت تقنيات التشفير بشكل يسمح بتشفير رسائل إلكترونية، ثم تبادلها في شكل صور فوتوغرافية عادية؛ وهي تقنية تحمل اسم Steganography ، وتشكل الفضاءات العامة والمقاهي التي

[1]- نصير لعرباوي، فاتح النور رحموني ، الجريمة الإرهابية الإلكترونية ، المعيار ، العدد 43 ، جانفي ، 2018 ، ص120.

[2]- نمديلي رحيمة ، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة ، أعمال المؤتمر الدولي الرابع عشر للجرائم الإلكترونية – الجزائر ، 24 مارس 2017، ص104

[3]- خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، الدار الجامعية للطباعة والنشر والتوزيع، القاهرة، مصر ، 2008، ص 61.

يمكن فيها استغلال خدمة الأنترنت بدون تحديد مسبق لهوية المستفيد من الخدمة صعوبة إضافية، تقف أمام تحديد الجاني في صورة ارتكابه الجريمة عن طريق الأنترنت المخصصة للعموم ، وفي هذه الحالة يصعب كثيرا إثبات أنه ارتكب الجريمة[1].

نخلص إلى القول بأن الجريمة الإلكترونية أصبحت ظاهرة إجرامية جديدة، وسمة بارزة في بداية القرن 21م، وتميزها بهذه الخصائص يجعلها تختلف عن الجرائم التقليدية، إذ أن المجرمين في هذا المجال أو كما يُسمون " الهاكرز" يتميزون بالذكاء في استخدام وسائل تقنية متطورة، وتنفيذ جرائمهم سواء في عمليات إرسال الفيروسات المخربة للمواقع والأنظمة أو سرقة الأموال والسطو على أرصدة المصارف، وتحويل الأموال أو سرقة البيانات المهمة أو إتلافها، كما تتميز الجريمة بالسرعة في التخطيط والتنفيذ، وبجهد وتكاليف أقل بكثير من الجهد والأموال الكبيرة، التي كانت تنفق في تنفيذ الجرائم التقليدية [2].

رابعا : قانون رقم 18-04 المتعلق بالقضاء على الجرائم المعلوماتية[3]:

بدأ المشرع في مواجهة الجرائم الإلكترونية في الجزائر من خلال تشريعات متنوعة تهدف إلى توفير بيئة قانونية لضبط الأنشطة الرقمية. تم تناول الجرائم الإلكترونية بشكل خاص في قانون الأمن السيبراني وقانون حماية البيانات الشخصية، بالإضافة إلى تعديلات على قوانين أخرى تتعلق بالإعلام والاتصالات، نصّت تقارير دولية على التحديثات القانونية التي عرفها قطاع الإعلام والاتصال في الجزائر خلال سنة 2024، حيث أقرت الحكومة الجزائرية في يونيو 2024 قانونًا خاصًا بالصحافة المكتوبة والإلكترونية، يُلزم المنصات الإعلامية الإلكترونية بأن تكون مستضافة على خوادم مادية داخل البلاد وتستخدم نطاق ".dz".

[1]- عزيزة رابحي العنصر المفترض في جريمة الدخول او البقاء غير المصرح به للنظام المعلوماتي، المجلة الجزائرية للدراسات التاريخية والقانونية، المركز الجامعي تندوف، المجلد 01 ، العدد 02 جوان ،2016، ص ص 262-281.

[2]- مرهج الهيتي، الجريمة الالكترونية نماذج من تطبيقاتها (دراسة مقارنة) القاهرة، دار الكتب القانونية 2014، ص 187.

[3]- قانون رقم 04/18 مؤرخ في 24 شعبان عام 1439 الموافق10 مايو سنة 2018 ،يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية. الجريدة الرسمية عدد 27، الصادرة بتاريخ 13 ماي 2018.

كما دخل قانون النشاط السمعي البصري حيز التنفيذ في ديسمبر من نفس السنة، ويتضمن حظرًا صارمًا على بث المحتويات التي تروّج للعنف، الإرهاب، التمييز العنصري، أو الأخبار الكاذبة[1].

وفقا للمادة 10 من القانون رقم 18-04 المؤرخ في 10 مايو 2018، يُعرف مفهوم "الأمن السيبراني" بأنه "مجموعة الأدوات والسياسات والآليات والتوجيهات والتدابير الأمنية التي تُستخدم لحماية الاتصالات الإلكترونية من أي تهديد قد يمس بتوفر البيانات أو سلامتها أو سريتها[2]".

يعتبر هذا القانون من أبرز التشريعات التي تبنتها الجزائر لمكافحة الجرائم الإلكترونية. حيث يُعاقب القانون أي شخص يرتكب أفعالًا غير قانونية باستخدام الشبكة الإلكترونية أو النظام المعلوماتي، مثل القرصنة، التسلل إلى الأنظمة المعلوماتية، أو استخدام البرمجيات الخبيثة.

يتضمن هذا القانون أحكامًا صارمة حول حماية البيانات الشخصية على الإنترنت، وهو ما يعزز من حماية الأفراد من السرقة الإلكترونية أو التنصت أو التجسس على المعلومات الشخصية. يُجرّم هذا القانون التلاعب بالبيانات أو استخدامها بشكل غير قانوني.

خامسا : قانون الإعلام:

يُعنى هذا القانون بتنظيم وسائل الإعلام، بما في ذلك الوسائل الإلكترونية، ويوفر إطارًا قانونيًا لمكافحة التحرش الإلكتروني و التشهير على منصات الإنترنت. يُحدد هذا القانون

[1] – Digital Policy Alert, "In June 2024, Algeria implemented the Law on written and electronic press… requiring online press providers to use websites hosted exclusively on physical infrastructure in Algeria with a ".dz" domain extension… In December 2024, the Law on the Audiovisual Activity entered into force… prohibiting audiovisual and online communication services from broadcasting content that promotes violence, terrorism, racial discrimination, or false information", accessed 26 June 2025, via: https://digitalpolicyalert.org

[2] – المادة 10 من القانون رقم 18-04

المسؤولية القانونية للمواقع الإلكترونية والأشخاص الذين يستخدمون هذه المنصات في نشر محتوى غير قانوني أو ضار.

وتمكّن القانون العضوي رقم 23-14 المؤرخ في 27 أوت 2023 المتعلق بالإعلام من وضع إطار قانوني شامل ينظم ممارسة الأنشطة الإعلامية، عبر تأسيس هيئات تنظيمية مستقلة تشمل تنظيم الصحافة المكتوبة والإلكترونية والإذاعة والتلفزيون[1].

سادسًا: قانون مكافحة الإرهاب والتطرّف:

يُستخدم هذا القانون لمكافحة استخدام الإنترنت في نشر الأفكار المتطرفة أو تنفيذ عمليات إرهابية عبر الشبكة العنكبوتية. كما يعاقب القانون أي استخدام للإنترنت بقصد نشر الدعاية الإرهابية أو التجنيد الإلكتروني[2].

قانون الأمن السيبراني: يهدف إلى حماية الأنظمة المعلوماتية والبنية التحتية الحساسة للدولة، مثل الأنظمة المالية والطاقة. يعزّز هذا القانون قدرات رصد الهجمات الإلكترونية ويحدد الممارسات القانونية الواجب اتباعها لمكافحتها ضمن استراتيجية وطنية شاملة[3].

يُستخدم قانون مكافحة الإرهاب والتطرّف في الجزائر لملاحقة استخدام الإنترنت في نشر الأفكار المتطرفة أو لتنفيذ عمليات إرهابية إلكترونية. ويعاقب القانون على أي نشاط إلكتروني يُستَخدم لنشر الدعاية الإرهابية أو للتجنيد الإلكتروني[1].

[1] – القانون العضوي رقم 23-14 المؤرخ في 27 أوت 2023، المتعلق بالإعلام، الجريدة الرسمية للجمهورية الجزائرية، العدد 65، 2 ديسمبر 2023.

[2] – منير محمد الجنبيهي، جريمة الإرهاب الإلكتروني بين عولمة الجريمة وضرورة المكافحة، مجلة الدراسات الأمنية، الجزائر، 2022؛ تشير الدراسة إلى أن "تجنيد الجماعات الإرهابية باستخدام تكنولوجيا الإعلام والاتصال" بات يشكل جزءًا جوهريًا من الإرهاب المعاصر.

[3] – الاستراتيجية الوطنية للأمن السيبراني في الجزائر تهدف إلى حماية البنية التحتية الرقمية ومواجهة الهجمات الإلكترونية، وخاصة على القطاعات الحيوية كالطاقة والمالية.

سابعا : الجرائم الإلكترونية حسب القوانين الجزائرية

تشمل الجرائم الإلكترونية وفق التشريع الجزائري لعام 2024 عددًا من الأفعال المرتكبة عبر الإنترنت أو باستخدام الأنظمة الرقمية، أبرزها:

1 – القرصنة الإلكترونية: محاولة الدخول غير القانوني إلى نظم المعالجة الآلية بهدف التجسس أو السرقة أو تخريب البيانات[2].

2 – الاحتيال الإلكتروني: خداع الأفراد أو المؤسسات عبر الإنترنت للحصول على أموال أو بيانات شخصية، مثل التصيّد أو إنشاء مواقع وهمية للبنوك[3].

3– التشهير الإلكتروني: نشر محتوى ضار أو معلومات مضلّلة بهدف الإضرار بسمعة شخص عبر الشبكات[4].

4– الابتزاز الإلكتروني: تهديد الضحية بنشر معلومات أو صور حساسة ما لم تُدفع فدية[5].

5 – التجسّس الإلكتروني: الاستيلاء غير المشروع على بيانات حساسة من الأنظمة الرقمية، مثل التنصت على رسائل أو سرقة معلومات[6].

6 – التحرش الإلكتروني: مضايقة شخص عبر الإنترنت أو الهاتف المحمول[7].

---

[1] – UNODC: دعم الجزائر في "مشاركة الأدلة الإلكترونية عبر الحدود ومكافحة استخدام الإنترنت ووسائل التواصل الاجتماعي للأغراض الإرهابية"، خلال تدريب نظمته UNODC/TPB في فبراير 2021. هذا التدريب ركز على تعزيز الإطار القانوني لمكافحة الإرهاب الإلكتروني وتعزيز قدرات متابعة الأدلة الرقمية.

[2] – المادة 394 من القانون 09-04 :" القانوني للجريمة الإلكترونية في التشريع الجزائري، يحدد القرصنة الإلكترونية كمساس بالنظم المعلوماتية "

[3] – نفس المصدر يوضح وجود نصوص تجرّم الاحتيال الإلكتروني ضمن قانون 09-04 .

[4] – تتناول مصادر جزائرية الفصل في التشهير الإلكتروني، ضمن الجرائم المعلوماتية .

[5] – الجرائم مثل الابتزاز الإلكتروني تُدرج ضمن مساس البيانات والحياة الخاصة في التشريع 09-04

[6] – يجري تعريف التجسّس الإلكتروني ضمن الجرائم ضد سرية المعطيات في القانون ذاته

[7] – تم التعرّف على التحرش الإلكتروني كجريمة معلوماتية في دراسات جزائرية

ثامنا : التحديات القانونية في مكافحة الجرائم الإلكترونية في الجزائر

على الرغم من التشريعات المتطورة في الجزائر لمكافحة الجرائم الإلكترونية، إلا أن التحديات القانونية لا تزال قائمة. من أبرز هذه التحديات:

1 – تحديات القوانين الدولية: بما أن الجرائم الإلكترونية غالبًا ما تتم عبر الحدود، فإن التعاون الدولي يُعد أمرًا حيويًا للتصدي لها. ومع ذلك، قد تواجه الجزائر صعوبة في التعاون مع دول أخرى بسبب التباين في التشريعات.

2 – التحقيق والملاحقة: بما أن الجرائم الإلكترونية تتم غالبًا بشكل غير مرئي وبسرعة، فقد تكون عملية تتبع الجناة أو ملاحقتهم قانونيًا صعبة ومعقدة.

3 – التطور التكنولوجي السريع: قد تتأخر القوانين في مواكبة التطورات التكنولوجية الجديدة، مثل الذكاء الاصطناعي و العملات الرقمية، مما قد يخلق ثغرات قانونية في التصدي للجرائم المرتكبة باستخدام هذه التقنيات الحديثة.

الجرائم الإلكترونية في الجزائر تمثل تهديدًا كبيرًا للأمن الرقمي، ولهذا تسعى الجزائر إلى تعزيز إطارها القانوني للتعامل مع هذه الجرائم من خلال القوانين الخاصة بالأمن السيبراني وحماية البيانات. رغم التقدم الحاصل في التشريع الجزائري، إلا أن التحديات القانونية والتقنية لا تزال تستدعي المزيد من التطوير المستمر للوائح والقوانين لمواكبة التطورات التكنولوجية السريعة في هذا المجال.

الفرع الثاني: أهمية مكافحة الجرائم الإلكترونية في التشريع الجزائري

تعتبر الجرائم الإلكترونية من أبرز التحديات التي تواجه المجتمعات في العصر الحديث، خاصة مع تزايد الاعتماد على الإنترنت ووسائل الاتصال الرقمية في كافة جوانب الحياة الاقتصادية والاجتماعية. في هذا السياق، تكتسب مكافحة الجرائم الإلكترونية في التشريع

الجزائري أهمية بالغة، نظرًا للتهديدات المتزايدة التي تشكلها هذه الجرائم على الأمن الشخصي، المؤسسي، الوطني، والاقتصادي[1].

تتمثل أهمية مكافحة الجرائم الإلكترونية في التشريع الجزائري في عدة جوانب رئيسية، يمكن تلخيصها في الآتي:

1 – حماية الأمن السيبراني والبنية التحتية الرقمية

في العصر الرقمي أصبحت البنية التحتية الرقمية جزءًا أساسيًا من حياة الأفراد والمجتمعات. تشمل هذه البنية أنظمة الاتصال، الأنظمة المالية، الخدمات الحكومية الإلكترونية، والمعلومات الحساسة، وفإن مكافحة الجرائم الإلكترونية تعتبر أمرًا ضروريًا للحفاظ على الأمن السيبراني للجزائر:

أ – حماية المعلومات الحساسة: تساهم مكافحة الجرائم الإلكترونية في ضمان سلامة البيانات الشخصية و الملفات الحكومية من الهجمات الإلكترونية التي تهدف إلى السرقة أو العبث بها.

ب – حماية المؤسسات: تعزز القوانين التي تنظم الجرائم الإلكترونية من قدرة المؤسسات على مواجهة الهجمات الإلكترونية مثل التسلل إلى الأنظمة أو سرقة المعلومات التجارية، مما يساعد في حماية الأسرار التجارية والمعلومات الحساسة للمؤسسات. [2]

2 – تعزيز الثقة في الاقتصاد الرقمي

في ظل التحول الرقمي الذي تشهده الجزائر، أصبح الاقتصاد الرقمي جزءًا أساسيًا من النمو الاقتصادي الوطني. ولذا فإن القضاء على الجرائم الإلكترونية يعزز من الثقة في الأنظمة المالية الإلكترونية و التجارة الإلكترونية.

[1] – عبد الحميد بوكرومة، الجرائم الإلكترونية في القانون الجزائري: دراسة تحليلية مقارنة، دار هومة، الجزائر، 2020، ص 45.

[2] – عبد الحميد بوكرومة، المرجع السابق ، ص ص 59–61.

أ – **حماية المعاملات المالية:** من خلال قوانين مكافحة الجرائم الإلكترونية، يمكن ضمان سلامة المعاملات المالية عبر الإنترنت، مما يحفز الأفراد والشركات على استخدام الخدمات المالية الرقمية بكل اطمئنان.

ب – **جذب الاستثمارات الأجنبية:** الأمن الإلكتروني الذي توفره التشريعات الجزائرية يساهم في جذب الاستثمارات الأجنبية، حيث تسعى الشركات الدولية إلى بيئات آمنة للعمل. وجود قوانين صارمة لمكافحة الجرائم الإلكترونية يعزز من استقرار السوق الرقمي في الجزائر. [1]

3 –حماية الأفراد والمجتمع

تؤثر الجرائم الإلكترونية بشكل كبير على الأفراد، سواء من خلال الاحتيال الإلكتروني أو الابتزاز الرقمي أو التشهير عبر الإنترنت. وبذلك، تُعد مكافحة هذه الجرائم وسيلة أساسية لحماية الحقوق الشخصية، والسمعة، و السلامة النفسية للأفراد في المجتمع.

أ – **حماية حقوق الأفراد:** مكافحة الجرائم الإلكترونية تضمن أن البيانات الشخصية للأفراد محمية من الهجمات، سواء كانت سرقة أو استغلالًا غير قانوني لهذه البيانات.

ب – **الوقاية من الابتزاز الإلكتروني:** من خلال تشريعات قانونية صارمة، يمكن للجزائر حماية الأفراد من الابتزاز أو التهديدات الإلكترونية التي تزداد بسبب انتشار منصات التواصل الاجتماعي والتطبيقات الرقمية.

4 – تعزيز التعاون الدولي

نظرًا لأن الجرائم الإلكترونية هي في الغالب عابرة للحدود، فإن مكافحة هذه الجرائم تستدعي تعاونًا دوليًا على مستوى التشريعات والهيئات القضائية.

[1] – مصطفى لعور، التحول الرقمي والأمن السيبراني في الجزائر: الإطار القانوني والتحديات المستقبلية، المجلة الجزائرية للقانون والاقتصاد الرقمي، العدد 7، 2022، ص ص 33–35.

أ – **للاتفاقيات الدولية:** الجزائر تعمل على تنظيم التشريعات المتعلقة بالجرائم الإلكترونية بحيث تتوافق مع المعايير الدولية، مثل اتفاقية بودابست الخاصة بمكافحة الجرائم الإلكترونية.

هذا التعاون يعزز من قدرة الجزائر على ملاحقة الجرائم الإلكترونية عبر الحدود ويُسهم في توفير بيئة قانونية أكثر حماية في المجال الرقمي.

5 – مكافحة الأنشطة الإجرامية والتنظيمات الإرهابية

أ – **تستخدم الجرائم الإلكترونية :** بشكل متزايد في الأنشطة الإجرامية والإرهابية مثل التخريب، التهريب، و التجنيد عبر الإنترنت. وتعمل التشريعات الجزائرية على مكافحة استخدام الإنترنت في الأنشطة غير القانونية التي تهدد الأمن القومي.

ب – مكافحة الإرهاب الرقمي: تتضمن القوانين الجزائرية تدابير تهدف إلى منع استخدام الإنترنت من قبل الجماعات الإرهابية للتخطيط لعملياتهم أو نشر الدعاية الإرهابية.

ج – التجسس الرقمي: تحمي التشريعات الجزائرية الأنظمة الرقمية من التجسس الإلكتروني الذي قد تقوم به دول أو كيانات أجنبية ضد الجزائر، مما يعزز أمن المعلومات في المؤسسات الحيوية. [1]

6 – تعزيز الحماية القانونية للمستخدمين في الفضاء الرقمي

تساهم مكافحة الجرائم الإلكترونية في توفير حماية قانونية للمستخدمين من العديد من المخاطر الإلكترونية التي قد تؤثر على حياتهم الخاصة. تمثل التشريعات الجزائرية أداة لحماية الأفراد من المخاطر المرتبطة باستخدام الإنترنت، مثل:

[1] – جمال بوقطاية، الأمن السيبراني ومكافحة الإرهاب الإلكتروني في ضوء التشريع الجزائري، مجلة دراسات قانونية، العدد 14، جامعة الجزائر 1، 2021، ص ص 90–93.

أ – **حماية الأطفال:** تعمل القوانين على حماية الأطفال والمراهقين من المحتوى الضار على الإنترنت، مثل المواد الإباحية أو الألعاب التي تشجع على العنف.

ب – **حماية البيانات الشخصية:** تساهم التشريعات الجزائرية في حماية بيانات الأفراد على الإنترنت، من خلال تجريم الاستغلال غير المشروع للبيانات الشخصية. [1]

إن مكافحة الجرائم الإلكترونية في التشريع الجزائري لا تقتصر على تحقيق العدالة الجنائية فقط، بل تمتد لتشمل حماية الاقتصاد الرقمي، تعزيز الأمن السيبراني، و حماية حقوق الأفراد في المجتمع. من خلال تحديث القوانين وتطويرها بشكل مستمر لمواكبة التحديات الرقمية الحديثة، تساهم الجزائر في توفير بيئة قانونية آمنة ومستقرة تمكن الأفراد والشركات من الاستفادة بشكل آمن من الفرص الرقمية التي يوفرها العالم الرقمي.

الفرع الثاني: أهمية مكافحة الجرائم الإلكترونية في التشريع الجزائري

تعتبر الجرائم الإلكترونية من أبرز التحديات التي تواجه المجتمعات في العصر الحديث، خاصة مع تزايد الاعتماد على الإنترنت ووسائل الاتصال الرقمية في كافة جوانب الحياة الاقتصادية والاجتماعية. في هذا السياق، تكتسب مكافحة الجرائم الإلكترونية في التشريع الجزائري أهمية بالغة، نظرًا للتهديدات المتزايدة التي تشكلها هذه الجرائم على الأمن الشخصي، المؤسسي، الوطني، والاقتصادي[2].

تتمثل أهمية مكافحة الجرائم الإلكترونية في التشريع الجزائري في عدة جوانب رئيسية، يمكن تلخيصها في الآتي:

[1] – سامية بن سعيد، حماية الحياة الخاصة والبيانات الشخصية في التشريع الجزائري في ظل التهديدات الرقمية، مجلة القانون والمجتمع، العدد 11، 2022، ص ص 47–49.

[2]– *زهية بن عيش*، الجرائم الإلكترونية في التشريع الجزائري، دار هومة، الجزائر، 2020. ص 112..

1 – حماية الأمن السيبراني والبنية التحتية الرقمية

في العصر الرقمي، أصبحت البنية التحتية الرقمية جزءًا أساسيًا من حياة الأفراد والمجتمعات وتشمل هذه البنية أنظمة الاتصال، الأنظمة المالية، الخدمات الحكومية الإلكترونية، والمعلومات الحساسة. ولذا، فإن مكافحة الجرائم الإلكترونية تعتبر أمرًا ضروريًا للحفاظ على الأمن السيبراني للجزائر[1].

أ – حماية المعلومات الحساسة:

تساهم مكافحة الجرائم الإلكترونية في ضمان سلامة البيانات الشخصية و الملفات الحكومية من الهجمات الإلكترونية التي تهدف إلى السرقة أو العبث بها.

ب – حماية المؤسسات:

تعزز القوانين التي تنظم الجرائم الإلكترونية من قدرة المؤسسات على مواجهة الهجمات الإلكترونية مثل التسلل إلى الأنظمة أو سرقة المعلومات التجارية، مما يساعد في حماية الأسرار التجارية والمعلومات الحساسة للمؤسسات.

2 – تعزيز الثقة في الاقتصاد الرقمي

في ظل التحول الرقمي الذي تشهده الجزائر، أصبح الاقتصاد الرقمي جزءًا أساسيًا من النمو الاقتصادي الوطني. ولذا فإن القضاء على الجرائم الإلكترونية يعزز من الثقة في الأنظمة المالية الإلكترونية و التجارة الإلكترونية.

أ – حماية المعاملات المالية:

من خلال قوانين مكافحة الجرائم الإلكترونية، يمكن ضمان سلامة المعاملات المالية عبر الإنترنت، مما يحفز الأفراد والشركات على استخدام الخدمات المالية الرقمية بكل اطمئنان.

[1]- بوزيد نذير، الجريمة المعلوماتية: دراسة قانونية مقارنة، دار الجامعة الجديدة، الجزائر، 2021، ص. 95–110.

ب –جذب الاستثمارات الأجنبية:

الأمن الإلكتروني الذي توفره التشريعات الجزائرية يساهم في جذب الاستثمارات الأجنبية، حيث تسعى الشركات الدولية إلى بيئات آمنة للعمل. وجود قوانين صارمة لمكافحة الجرائم الإلكترونية يعزز من استقرار السوق الرقمي في الجزائر.

3 – حماية الأفراد والمجتمع

تؤثر الجرائم الإلكترونية بشكل كبير على الأفراد، سواء من خلال الاحتيال الإلكتروني أو الابتزاز الرقمي أو التشهير عبر الإنترنت. وبذلك، تُعد مكافحة هذه الجرائم وسيلة أساسية لحماية الحقوق الشخصية، والسمعة، و السلامة النفسية للأفراد في المجتمع[1].

أ – حماية حقوق الأفراد:

مكافحة الجرائم الإلكترونية تضمن أن البيانات الشخصية للأفراد محمية من الهجمات، سواء كانت سرقة أو استغلالًا غير قانوني لهذه البيانات.

ب – الوقاية من الابتزاز الإلكتروني:

من خلال تشريعات قانونية صارمة، يمكن للجزائر حماية الأفراد من الابتزاز أو التهديدات الإلكترونية التي تزداد بسبب انتشار منصات التواصل الاجتماعي والتطبيقات الرقمية.

4 – تعزيز التعاون الدولي

نظرًا لأن الجرائم الإلكترونية هي في الغالب عابرة للحدود، فإن مكافحة هذه الجرائم تستدعي تعاونًا دوليًا على مستوى التشريعات والهيئات القضائية.

وتعمل على تنظيم التشريعات المتعلقة بالجرائم الإلكترونية بحيث تتوافق مع المعايير الدولية، مثل اتفاقية بودابست الخاصة بمكافحة الجرائم الإلكترونية. هذا التعاون يعزز من قدرة الجزائر على ملاحقة الجرائم الإلكترونية عبر الحدود ويُسهم في توفير بيئة قانونية أكثر حماية في المجال الرقمي

[1]- بن عيش زهية، *الجرائم الإلكترونية في التشريع الجزائري*، دار هومة، الجزائر، 2020، ص. 112–134.

5 – مكافحة الأنشطة الإجرامية والتنظيمات الإرهابية

تستخدم الجرائم الإلكترونية بشكل متزايد في الأنشطة الإجرامية والإرهابية مثل التخريب، التهريب، و التجنيد عبر الإنترنت. وتعمل التشريعات الجزائرية على مكافحة استخدام الإنترنت في الأنشطة غير القانونية التي تهدد الأمن القومي.

أ – **مكافحة الإرهاب الرقمي:**

تتضمن القوانين الجزائرية تدابير تهدف إلى منع استخدام الإنترنت من قبل الجماعات الإرهابية للتخطيط لعملياتهم أو نشر الدعاية الإرهابية.

ب – التجسس الرقمي:

تحمي التشريعات الجزائرية الأنظمة الرقمية من التجسس الإلكتروني الذي قد تقوم به دول أو كيانات أجنبية ضد الجزائر، مما يعزز أمن المعلومات في المؤسسات الحيوية.

6 – تعزيز الحماية القانونية للمستخدمين في الفضاء الرقمي

تساهم مكافحة الجرائم الإلكترونية في توفير حماية قانونية للمستخدمين من العديد من المخاطر الإلكترونية التي قد تؤثر على حياتهم الخاصة، تمثل التشريعات الجزائرية أداة لحماية الأفراد من المخاطر المرتبطة باستخدام الإنترنت، مثل:

أ – **حماية الأطفال:** تعمل القوانين على حماية الأطفال والمراهقين من المحتوى الضار على الإنترنت، مثل المواد الإباحية أو الألعاب التي تشجع على العنف.

ب – **حماية البيانات الشخصية:** تساهم التشريعات الجزائرية في حماية بيانات الأفراد على الإنترنت، من خلال تجريم الاستغلال غير المشروع للبيانات الشخصية. [1]

[1] – القانون رقم 18–07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 16، سنة 2018.

إن مكافحة الجرائم الإلكترونية في التشريع الجزائري لا تقتصر على تحقيق العدالة الجنائية فقط، بل تمتد لتشمل حماية الاقتصاد الرقمي، تعزيز الأمن السيبراني، وحماية حقوق الأفراد في المجتمع. من خلال تحديث القوانين وتطويرها بشكل مستمر لمواكبة التحديات الرقمية الحديثة، تساهم الجزائر في توفير بيئة قانونية آمنة ومستقرة تمكن الأفراد والشركات من الاستفادة بشكل آمن من الفرص الرقمية التي يوفرها العالم الرقمي. [1]

المطلب الثاني: أنواع الجرائم الإلكترونية

يشهد العصر الرقمي تطورًا سريعًا في مختلف المجالات، مما يساهم في زيادة الاعتماد على الإنترنت والتكنولوجيا في كافة مناحي الحياة. في الوقت نفسه، أدى هذا التطور إلى ظهور أنواع جديدة من الجرائم المعتمدة على تكنولوجيا المعلومات والاتصالات، وهو ما يُعرف بـ الجرائم الإلكترونية.

تتسم الجرائم الإلكترونية بتنوعها الكبير، حيث تشمل مجموعة واسعة من الأنشطة الإجرامية التي تتم عبر الإنترنت أو باستخدام الأجهزة الرقمية. وقد أسهم هذا التنوع في ظهور تحديات قانونية وأمنية تتطلب فهمًا دقيقًا لأنواع الجرائم التي يتم ارتكابها في الفضاء الرقمي. [2]

في هذا المطلب، سنستعرض أنواع الجرائم الإلكترونية التي باتت تشكل تهديدًا للمجتمعات والأفراد والمؤسسات على مستوى العالم، وفي الجزائر بشكل خاص. كما سنبين كيفية تصنيف هذه الجرائم بناءً على الوسائل المستخدمة في ارتكابها أو الغرض الذي تهدف إلى تحقيقه سنتناول أبرز أنواع الجرائم الإلكترونية مثل:

- القرصنة الإلكترونية (Hacking)

- الاحتيال الإلكتروني (Cyber Fraud)

[1] – خديجة بوعبد الله، مكافحة الجرائم الإلكترونية في التشريع الجزائري وأثرها على حماية الحقوق الرقمية، مجلة القانون والتكنولوجيا، جامعة قسنطينة، العدد 10، 2023، ص 77–80.

[2] – عبد الحميد بوكرومة، المرجع السابق، ص ص 23–26.

- التشهير الإلكتروني (Cyber Defamation)
- الابتزاز الإلكتروني (Cyber Extortion)
- التجسس الإلكتروني (Cyber Espionage)
- التصيد الإلكتروني (Phishing)
- التهديدات الإلكترونية (Cyber Threats)
- التسلل إلى البيانات الشخصية (Identity Theft)

تستهدف هذه الجرائم بشكل عام الأفراد والمؤسسات على حد سواء، مما يؤدي إلى تهديد الأمن الشخصي، المالي، أو حتى الأمن الوطني في بعض الحالات. من خلال فهم هذه الأنواع، يمكن للأنظمة القانونية تحسين آليات المراقبة والملاحقة القانونية للحد من هذه الأنشطة الإجرامية.

أنواع الجرائم الإلكترونية تشكل تهديدًا حقيقيًا في ظل تزايد استخدام الإنترنت والتقنيات الحديثة. إن فهم هذه الأنواع يساعد في وضع استراتيجيات فعّالة لمكافحتها، ويساهم في تطوير التشريعات القانونية التي توفر حماية للمجتمعات الرقمية. [1]

الفرع الأول: جرائم ضد الأفراد (مثل الاحتيال الإلكتروني، الابتزاز الرقمي)

تعتبر الجرائم الإلكترونية ضد الأفراد من أبرز التهديدات التي تواجه المستخدمين في الفضاء الرقمي، حيث أن الجرائم التي تستهدف الأفراد تعتمد بشكل أساسي على استغلال التكنولوجيا للوصول إلى البيانات الشخصية أو الاستفادة غير المشروعة من الأفراد. من بين هذه الجرائم البارزة الاحتيال الإلكتروني و الابتزاز الرقمي، اللتين تمثلان تهديدات حقيقية للأمن الشخصي

[1] – ليلى زروقي، المراجع السابق ، ص ص 50-52.

1 – الاحتيال الإلكتروني

تعد الاحتيال الإلكتروني من أكثر الجرائم التي تُرتكب ضد الأفراد عبر الإنترنت، وهو يشمل مجموعة من الأفعال التي تهدف إلى خداع الضحية للحصول على مبالغ مالية أو بيانات شخصية بطريقة غير قانونية. تتمثل هذه الأنشطة في العديد من الأشكال، مثل التصيد الإلكتروني، إنشاء مواقع وهمية، أو الاستيلاء على الحسابات المالية[1].

2 – أشكال الاحتيال الإلكتروني:

أ – التصيد الإلكتروني (Phishing):

يقوم الجاني بإرسال رسائل بريد إلكتروني تبدو وكأنها من مؤسسات رسمية أو بنوك معروفة، بهدف خداع الضحية لإدخال بياناته الشخصية أو المالية في موقع وهمي.

ب – الاحتيال المالي عبر الإنترنت:

يشمل ذلك استخدام المواقع الإلكترونية أو التطبيقات لعرض منتجات أو خدمات وهمية، حيث يطلب الجاني من الضحية دفع الأموال مقابل سلع أو خدمات غير موجودة.

ج – الاحتيال عبر العملات الرقمية:

في السنوات الأخيرة، بدأ الاحتيال في استخدام العملات الرقمية كوسيلة لابتزاز الأفراد واستغلالهم ماليًا عبر استثمارات وهمية أو عمليات احتيال تجارية.

د – الاحتيال عبر مواقع المزادات: حيث يقوم الجاني بإنشاء حساب مزاد مزيف لبيع منتجات غير موجودة مقابل الحصول على الأموال.

هـ – العواقب القانونية في الجزائر:

يعد الاحتيال الإلكتروني جريمة يعاقب عليها قانون العقوبات الجزائري، حيث يتم تطبيق عقوبات تصل إلى السجن و غرامات مالية ضد الأشخاص الذين يُثبت ارتكابهم لهذه الأنشطة الاحتيالية.

[1]– زهية بن عيش، *الجرائم الإلكترونية في التشريع الجزائري*، دار هومة، الجزائر، 2020، ص. 87–103.

كما يُجرّم قانون حماية البيانات الشخصية الاستيلاء على معلومات حساسة من الأفراد بدون إذن منهم.

3 – الابتزاز الرقمي

الابتزاز الرقمي هو جريمة تحدث عندما يقوم الجاني بتهديد الضحية بنشر معلومات أو صور حساسة عنها على الإنترنت، ما لم يستجيب الضحية لمطالب الجاني التي غالبًا ما تكون مبالغ مالية أو مزايا أخرى[1].

أ – الابتزاز الجنسي الإلكتروني: حيث يقوم الجاني بنشر صور أو مقاطع فيديو عارية أو خاصة للضحية، أو التهديد بنشر هذه الصور إذا لم يستجب الضحية لمطالبه.

ب – الابتزاز المالي: يحدث عندما يهدد الجاني بنشر معلومات خاصة أو حساسة عن الضحية (مثل رسائل خاصة أو صور) ما لم تدفع الضحية المال.

ج – الابتزاز عبر منصات التواصل الاجتماعي:

حيث يبتز الجاني الضحية عبر نشر معلومات تضر بسمعتها أو تهديدها بتدمير حياتها الشخصية أو المهنية إذا لم يتم تنفيذ مطالبه.

د – العواقب القانونية في الجزائر:

يُجرّم الابتزاز الرقمي في الجزائر بموجب قانون العقوبات، وتُفرض عليه عقوبات صارمة، بما في ذلك السجن لفترات قد تصل إلى عدة سنوات.

يعترف القانون الجزائري بأن الابتزاز الإلكتروني يعد من الجرائم التي تؤثر على الأمن الشخصي و الحقوق الرقمية للأفراد، وبالتالي يولي اهتمامًا خاصًا للتعامل مع هذه الجرائم.

– نشر صور أو مقاطع فيديو خاصة بالأفراد على مواقع التواصل الاجتماعي.

– تهديد الضحية بنشر محادثات خاصة أو رسائل ذات طابع حساس، إذا لم يتم تلبية مطالب الجاني.

[1]– نذير بوزيد، *الجريمة المعلوماتية: دراسة قانونية مقارنة*، دار الجامعة الجديدة، الجزائر، 2021، ص. 65–80.

3 – تدابير مكافحة الجرائم ضد الأفراد

تسعى التشريعات الجزائرية لمكافحة الجرائم الإلكترونية ضد الأفراد عبر:

– تعزيز الحماية القانونية للأفراد ضد الاحتيال الإلكتروني والابتزاز الرقمي.

– توفير أدوات قانونية لرصد الجرائم الرقمية وملاحقتها، بما في ذلك استخدام التقنيات الحديثة للتحقيق والتتبع[1].

– التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، وذلك من خلال اتفاقيات مع دول أخرى لتبادل المعلومات والتنسيق في ملاحقة الجناة.

تستهدف الجرائم الإلكترونية ضد الأفراد (مثل الاحتيال الإلكتروني و الابتزاز الرقمي) الأمن الشخصي للأفراد وتُعرّضهم لخسائر مالية ومعنوية كبيرة. ولذا، فإن الأنظمة القانونية في الجزائر تعمل بشكل مستمر على تطوير التشريعات لمكافحة هذه الجرائم وضمان حماية حقوق الأفراد في الفضاء الرقمي.

الفرع الثاني: جرائم ضد المؤسسات (مثل الهجمات الإلكترونية على المواقع، سرقة البيانات)

تعتبر الجرائم الإلكترونية ضد المؤسسات من أكثر التهديدات الرقمية التي تواجه الشركات والهيئات العامة على مستوى العالم، بما في ذلك الجزائر. في ظل التقدم التكنولوجي الكبير وانتشار الإنترنت واستخدام الأنظمة الرقمية في إدارة الأعمال والخدمات، أصبحت المؤسسات عرضة للعديد من الهجمات الإلكترونية التي تستهدف الأنظمة المعلوماتية والشبكات الخاصة بها[2].

من أبرز هذه الجرائم الهجمات الإلكترونية على المواقع و سرقة البيانات، اللتين يمكن أن تضر بسمعة المؤسسة، وتؤدي إلى خسائر مالية كبيرة، فضلاً عن التأثير على الثقة العامة في الخدمات المقدمة من قبل هذه المؤسسات.

[1]– نذير بوزيد المرجع السابق ص87.

[2]– زهية بن عيش، المرجع السابق ، ص. 138–150.

1- الهجمات الإلكترونية على المواقع

تعد الهجمات الإلكترونية على المواقع من أخطر الجرائم التي تهدد المؤسسات في العصر الرقمي، حيث تستهدف الأنظمة المعلوماتية والمواقع الإلكترونية الخاصة بالشركات أو المؤسسات.

يمكن أن تشمل هذه الهجمات العديد من الأشكال، مثل القرصنة، الاختراقات الأمنية، والهجمات الموزعة. [1]

2- أنواع الهجمات الإلكترونية على المواقع:

أ- هجوم الحجب الموزع للخدمة (DDoS):

يتمثل هذا الهجوم في محاولة إغراق الموقع الإلكتروني بحجم كبير من الطلبات بهدف تعطيل أو إيقاف تشغيل الموقع تمامًا. يتم استخدام عدة أجهزة أو شبكات في هذا الهجوم لتنفيذ العملية.

ب- الاختراق الأمني للموقع (Hacking):

يقوم الجاني بالولوج غير القانوني إلى الموقع الإلكتروني أو النظام المعلوماتي للمؤسسة بهدف سرقة البيانات أو تخريب المعلومات. غالبًا ما تتم هذه الهجمات باستخدام الثغرات الأمنية في البرمجيات.

[1] – أحمد بوزيان، الجرائم الإلكترونية والهجمات السيبرانية: دراسة قانونية وتقنية، دار الجامعة، الجزائر، 2021، ص ص 88-91.

ج- الحقن البرمجي (SQL Injection):

يعتمد هذا الهجوم على استغلال الثغرات البرمجية في قواعد البيانات المربوطة بالموقع الإلكتروني، حيث يحقن الجاني أوامر برمجية ضارة (SQL) لتحميل بيانات حساسة أو تنفيذ أوامر تؤثر على عمل الموقع. [1]

د - الهجمات عبر البريد الإلكتروني (Phishing):

يقوم الجاني بإرسال رسائل بريد إلكتروني تبدو وكأنها من المؤسسة نفسها أو جهة موثوقة، بهدف إقناع الموظفين بفتح روابط أو مرفقات تحتوي على برمجيات خبيثة.

هـ - أضرار الهجمات الإلكترونية على المواقع:

توقف الخدمة: تؤدي هجمات DDoS إلى إيقاف أو تعطيل الموقع لفترات طويلة، مما يؤدي إلى خسائر مالية بسبب توقف العمليات التجارية.

سرقة المعلومات الحساسة: قد تؤدي الاختراقات إلى سرقة أو تسريب معلومات مهمة أو حساسة للعملاء أو المؤسسة.

و - تدمير السمعة:

قد يتسبب الهجوم في إلحاق الضرر بسمعة المؤسسة بسبب تعرض بياناتها أو أنظمتها للسرقة أو التلاعب، ويمكن أن تؤدي الهجمات الإلكترونية إلى فقدان الثقة من العملاء والمستثمرين في قدرة المؤسسة على حماية بياناتهم.

[1] - عماد بوعبد الله، المرجع السابق ، ص ص 60-63.

3 – سرقة البيانات

سرقة البيانات هي جريمة إلكترونية أخرى تهدد المؤسسات، وتشمل الاستيلاء غير القانوني على المعلومات الحساسة أو الملفات الخاصة التي تحتوي على بيانات العملاء أو أسرار تجارية. يتم تنفيذ هذه الجريمة باستخدام تقنيات متعددة مثل القرصنة الإلكترونية، البرمجيات الخبيثة، أو الاختراقات الأمنية.

أ- أنواع سرقة البيانات:

*** سرقة البيانات (Vol de données)**

تُعد سرقة البيانات من الجرائم المنتشرة ضد المؤسسات، حيث يقوم الجاني بالوصول إلى قواعد بيانات الشركة أو الهيئة وسرقة معلومات حساسة كالمراسلات الرسمية، البيانات التجارية، أو المعلومات الخاصة بالزبائن. وقد يتم استغلال هذه البيانات لأغراض تجارية، تجسسية، أو ابتزازية.

وقد جرم المشرع هذا النوع من الأفعال في إطار حماية المعطيات الرقمية، كما نص عليه في المادة 45 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي.[1]

"كل من قام، بوجه غير مشروع، بجمع أو تخزين أو نشر معطيات ذات طابع شخصي، يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100.000 دج إلى 300.000 دج."

*** سرقة البيانات الشخصية:** يتضمن ذلك الاستيلاء على البيانات الشخصية للعملاء أو الموظفين، مثل أرقام بطاقات الائتمان، البيانات المصرفية، أو المعلومات الصحية، بهدف بيعها أو استخدامها في أنشطة غير قانونية.

[1]- المادة 45 من القانون رقم 18-07 .

* **سرقة الأسرار التجارية:** تتمثل في سرقة المعلومات التجارية الحساسة المتعلقة بالشركة مثل استراتيجيات التسويق، التصميمات، أو المستندات المالية، والتي يمكن استخدامها من قبل المنافسين للحصول على مزايا غير مشروعة.

* **التسلل إلى قواعد البيانات:** من خلال استغلال الثغرات أو الثغرات الأمنية في النظام المعلوماتي للمؤسسة، يمكن للهاكرز الولوج إلى قواعد البيانات وسرقة بيانات كبيرة، مثل السجلات المالية أو بيانات العملاء.

ب- أضرار سرقة البيانات:

* **خسائر مالية:** قد تتسبب سرقة البيانات في خسائر مالية كبيرة نتيجة لبيع المعلومات أو استخدامها في أنشطة احتيالية.

* **فقدان الثقة:** تؤدي سرقة البيانات إلى فقدان الثقة من قبل العملاء والمستثمرين في قدرة المؤسسة على حماية المعلومات الشخصية.

* **مساءلة قانونية:** قد تتعرض المؤسسة للمسائلة القانونية إذا لم تتمكن من حماية بيانات عملائها بالشكل المطلوب، وقد تترتب على ذلك غرامات أو عقوبات أخرى.

4 - تدابير مكافحة الجرائم ضد المؤسسات

تسعى التشريعات الجزائرية لمكافحة الجرائم الإلكترونية ضد المؤسسات من خلال مجموعة من التدابير والإجراءات، مثل[1]:

1 - تطوير الأنظمة الأمنية: يشمل ذلك استخدام تقنيات التشفير المتطورة، الجدران النارية، والأنظمة المضادة للفيروسات لحماية الأنظمة من الهجمات.

[1] - راوية بن ساسي، مكافحة الجرائم الإلكترونية في القانون الجزائري: بين النص القانوني والتحديات التطبيقية، المجلة الجزائرية للقانون الرقمي، العدد 4، 2022، ص ص 42-45.

2 – إجراءات قانونية صارمة: يتم تطبيق العقوبات في حال اكتشاف أي هجوم إلكتروني ضد مؤسسة ما، حيث تُفرض عقوبات جنائية على الأفراد المتورطين في الهجمات الإلكترونية[1].

تعاون دولي: نظراً لأن الجرائم الإلكترونية غالباً ما تتجاوز الحدود، فإن التعاون الدولي بين الجزائر والدول الأخرى في مجال مكافحة الجرائم الإلكترونية يُعد ضروريًا، خاصة في تبادل المعلومات وتعقب الجناة.

تستهدف الجرائم الإلكترونية ضد المؤسسات الأنظمة المعلوماتية والمواقع الإلكترونية، مما يؤدي إلى خسائر اقتصادية وأمنية كبيرة. تعد الهجمات الإلكترونية و سرقة البيانات من أكثر الجرائم تهديدًا للمؤسسات في العالم الرقمي. لذلك، من الضروري أن تتبنى المؤسسات تدابير أمنية فعالة، مع تعزيز التعاون مع السلطات القانونية لتطوير أطر قانونية قوية لمكافحة هذه الجرائم والحفاظ على الأمن السيبراني.

الفرع الثالث: الجرائم المنظمة عبر الإنترنت (مثل القرصنة والأنشطة الإرهابية الإلكترونية)

تشهد الجرائم الإلكترونية تطورًا كبيرًا في العصر الرقمي، حيث لم تعد هذه الجرائم تقتصر فقط على الأفراد العاديين أو حتى الشركات الصغيرة، بل بدأت تتخذ طابعًا منظمًا وأكثر تعقيدًا، وذلك من خلال الجماعات الإجرامية أو المنظمات الإرهابية التي تستخدم الإنترنت كأداة رئيسية لارتكاب الجرائم. من أبرز هذه الجرائم القرصنة الإلكترونية و الأنشطة الإرهابية الإلكترونية، التي تمثل تهديدًا جديًا للأمن القومي والدولي.

[1] – المواد 394 مكرر إلى 394 مكرر 7، المعدلة بموجب القانون رقم 06-23 المتضمن قانون العقوبات الجزائري،المؤرخ في 20 ديسمبر 2006، الجريدة الرسمية، العدد 84، 2006.

أولا : القرصنة الإلكترونية (Cyber Piracy)

القرصنة الإلكترونية هي نوع من الجرائم المنظمة التي يتورط فيها مجموعة من الأفراد أو منظمات تستخدم التكنولوجيا لاختراق الأنظمة المعلوماتية و سرقة البيانات أو تعطيل الأنظمة بالكامل. يمكن أن تتراوح هذه الأنشطة من القرصنة على الشبكات الحكومية إلى القرصنة على أنظمة الشركات الكبرى بغرض الابتزاز أو السرقة أو التخريب[1].

1 – أنواع القرصنة الإلكترونية:

أ – **قرصنة البرمجيات (Software Piracy):** حيث يقوم الجناة بتوزيع أو بيع نسخ غير قانونية من البرمجيات دون إذن من المالك الأصلي.

ب– **القرصنة على الإنترنت (Internet Piracy):** تشمل سرقة المحتوى الرقمي مثل الأفلام، الموسيقى، الكتب الإلكترونية، والبرامج الحاسوبية.

ج – **قرصنة الأنظمة المعلوماتية:** وتتضمن الهجمات التي تهدف إلى اختراق الأنظمة الحكومية أو الشركات الكبرى لسرقة البيانات أو تعطيل أنظمة مهمة.

ثانيا : أهداف القرصنة الإلكترونية:

أ – **الربح المالي:** قد يسعى القراصنة إلى جني الأرباح من خلال بيع المعلومات المسروقة أو طلب فدية مقابل إعادة الأنظمة المخترقة إلى العمل.

ب – **السرقة الصناعية:** يتم اختراق الأنظمة للحصول على أسرار تجارية أو تكنولوجيا حساسة قد تساهم في منافسة غير قانونية.

[1]– عبد الكريم بوالشعير، *القانون الدولي لمكافحة الإرهاب الإلكتروني*، دار المعرفة، الجزائر، 2019، ص. 88–105.

ج – التخريب: في بعض الحالات، يقوم القراصنة بتعطيل الأنظمة عن قصد لأغراض إيديولوجية أو سياسية[1].

ثالثا : العواقب القانونية:

يُعاقب القراصنة الإلكترونيون في التشريعات الجزائرية بموجب قانون العقوبات، الذي يحدد عقوبات تصل إلى السجن و الغرامات المالية للمخترقين.

كما يتم تطبيق قوانين أخرى ذات علاقة بالأمن السيبراني وحماية البيانات التي تجرم التعدي على الأنظمة المعلوماتية.

1 – الأنشطة الإرهابية الإلكترونية

الأنشطة الإرهابية الإلكترونية هي نوع من الجرائم المنظمة التي تستخدم التكنولوجيا الحديثة والإنترنت لتحقيق أهداف إرهابية. هذه الأنشطة يمكن أن تشمل الدعاية الإرهابية، التجنيد عبر الإنترنت، التخطيط للهجمات، وحتى تنفيذ الهجمات الرقمية ضد أهداف استراتيجية أو دولية.

2 – **أشكال الأنشطة الإرهابية الإلكترونية:**

أ – الدعاية والترويج للإرهاب عبر الإنترنت: حيث يتم استخدام الإنترنت ووسائل التواصل الاجتماعي لنشر الدعاية الإرهابية، التحريض على العنف أو التجنيد للأفراد في الجماعات الإرهابية.

ب – التخطيط للهجمات الإرهابية: قد تستخدم الجماعات الإرهابية الإنترنت في التنسيق والتخطيط للهجمات عبر الهاتف المحمول، البرمجيات المشفرة، و الشبكات المظلمة.

[1]– نذير بوزيد، المرجع السابق ، *ص ص. 145–160.*

الهجمات السيبرانية على البنية التحتية: قد تتعرض بعض الأنظمة الحيوية مثل شبكات الكهرباء، المصارف، المؤسسات الحكومية، إلى هجمات سيبرانية من جماعات إرهابية بغرض إحداث فوضى أو شل النظام[1].

2 – أهداف الأنشطة الإرهابية الإلكترونية:

أ – نشر الفكر المتطرف: من خلال التجنيد الإلكتروني، يسعى الإرهابيون إلى جذب الأفراد للانضمام إلى تنظيماتهم من خلال نشر المحتوى المتطرف.

ب – تعطيل المؤسسات الحيوية: من خلال الهجمات السيبرانية على أنظمة البنية التحتية الحيوية بهدف إحداث فوضى أو عواقب اقتصادية جسيمة.

ج – زعزعة الاستقرار الوطني والدولي: قد تقوم الجماعات الإرهابية باستهداف الأنظمة الحكومية أو الاقتصادات الرقمية من خلال الهجمات السيبرانية لتعطيل الحياة الطبيعية في البلدان المستهدفة.

3 – العواقب القانونية:

قانون مكافحة الإرهاب في الجزائر يُجرم الأنشطة الإرهابية الإلكترونية ويضع عقوبات صارمة ضد الأفراد أو الجماعات التي تشارك في هذه الأنشطة.

التعاون الدولي في مكافحة الأنشطة الإرهابية عبر الإنترنت أمر بالغ الأهمية، إذ تتعاون الجزائر مع دول أخرى عبر الاتفاقيات الدولية لمكافحة الإرهاب في الفضاء الرقمي.

[1]– نذير بوزيد، *الجريمة المعلوماتية المراجع السابق* ص. 145–160.

رابعًا: تدابير مكافحة الجرائم المنظمة عبر الإنترنت

تسعى الجزائر لمكافحة الجرائم الإلكترونية المنظمة من خلال تطوير التشريعات القانونية وتطبيق الأنظمة الأمنية المتقدمة:

1 – تطوير الأمن السيبراني: تتبنى الجزائر إجراءات لحماية المؤسسات والأفراد من الهجمات الإلكترونية عبر تحديث أنظمة الأمان في القطاعين العام والخاص.

2 – التعاون الدولي: تسعى الجزائر للتعاون مع الدول الأخرى عبر اتفاقيات دولية لمكافحة الجرائم المنظمة عبر الإنترنت، خاصة مع المنظمات الأمنية العالمية مثل الإنتربول والاتحاد الأوروبي.

3 – إجراءات وقائية وتعليمية: من خلال التوعية العامة والتدريب المستمر للأفراد والمؤسسات على أفضل ممارسات الأمان الإلكتروني، تهدف الجزائر إلى تقليل حجم الجرائم الإلكترونية[1].

الجرائم المنظمة عبر الإنترنت، مثل القرصنة الإلكترونية والأنشطة الإرهابية الرقمية، تمثل تهديدات كبيرة للأمن العالمي والأمن الوطني. تعتبر هذه الجرائم معقدة وتنفذها جماعات إجرامية منظمة تستخدم الإنترنت كأداة رئيسية لتنفيذ أنشطتها. لذلك، من الضروري أن تبذل الجزائر جهودًا كبيرة لتطوير تشريعاتها وتعزيز التعاون الدولي لمكافحة هذه الجرائم وحماية الأمن السيبراني على المستويين المحلي والدولي. [2]

[1] – سامي دراجي، الجرائم الإلكترونية المنظمة في القانون الجزائري: الآليات الوقائية والتحديات الأمنية، مجلة الدراسات القانونية والسياسية، العدد 9، 2022، ص ص 66–69.

[2] – وزارة العدل الجزائرية، التقرير السنوي حول الجريمة السيبرانية والتعاون الدولي، منشورات الوزارة، الجزائر، 2023، ص ص 24–26.

المبحث الثاني: السياسة التشريعية الجزائرية في مواجهة الجرائم الإلكترونية

في عصر الثورة الرقمية والتكنولوجيا المتقدمة، أصبحت الجرائم الإلكترونية تمثل تهديدًا كبيرًا للأمن الوطني والدولي على حد سواء. حيث لم تعد هذه الجرائم مقتصرة على الأفراد العاديين، بل بدأت تتبناها مجموعات إجرامية منظمة تستخدم الإنترنت كأداة لارتكاب أعمال غير قانونية تشمل الاختراقات الإلكترونية، سرقة البيانات، الاحتيال الرقمي، وكذلك الأنشطة الإرهابية الإلكترونية[1].

وبالنظر إلى التحديات التي تفرضها هذه الجرائم على الدول من حيث حماية الأمن السيبراني والبيانات الشخصية، أضحى من الضروري أن تقوم الدول بتطوير تشريعات قانونية تهدف إلى مكافحة الجرائم الإلكترونية وحماية المجتمع من تأثيراتها السلبية. وفي هذا السياق، قامت الجزائر بتطوير إطار قانوني شامل لمكافحة الجرائم الإلكترونية يواكب التطور التكنولوجي السريع ويحمي الأفراد والمؤسسات من المخاطر الرقمية[2].

من خلال هذا المبحث، سنتناول التشريعات القانونية التي وضعتها الجزائر لمواجهة الجرائم الإلكترونية وكيفية تكيف النظام القانوني الجزائري مع هذه التحديات المتزايدة. سنستعرض أهم القوانين التي أصدرتها الدولة للحد من الأنشطة غير القانونية التي تتم عبر الإنترنت، بالإضافة إلى الإجراءات القانونية المتبعة لضمان تنفيذ هذه التشريعات بشكل فعال.

[1]– عبد الحكيم بوشيخي، شرح قانون الإجراءات الجزائية الجزائري، دار الخلدونية، الجزائر، 2020، ص. 214–219.

[2]– فتيحة بن قرينة، السياسة الجنائية الجزائرية في مواجهة الجريمة الإلكترونية، مجلة القانون والدراسات، العدد 10، 2022، ص ص. 87–94.

المطلب الأول: القوانين والأنظمة المتعلقة بالجرائم الإلكترونية في الجزائر

تزايدت التهديدات الناتجة عن الجرائم الإلكترونية في مختلف أنحاء العالم مع تطور تكنولوجيا المعلومات والاتصالات، مما استدعى من الدول سن قوانين وتشريعات خاصة لمواجهة هذا النوع من الجرائم وحماية الأفراد والمجتمعات من مخاطره. وفي هذا الإطار، لم تكن الجزائر استثناءً من هذا التطور، إذ أدركت الحاجة الملحة إلى وضع إطار قانوني منظم لمكافحة الجرائم الإلكترونية، بما يواكب التطورات السريعة في عالم الإنترنت.

تتمثل الجرائم الإلكترونية في مجموعة من الأفعال غير القانونية التي تُرتكب عبر شبكة الإنترنت أو باستخدام الوسائل التكنولوجية الحديثة. وتشمل هذه الجرائم العديد من الأفعال مثل الاختراقات الإلكترونية، الاحتيال الرقمي، الابتزاز الإلكتروني، و سرقة البيانات، وهي تشكل تهديدًا جادًا للأمن السيبراني، وحقوق الأفراد، وتؤثر بشكل مباشر على الاقتصاد الوطني[1].

ومن أجل التصدي لهذه الجرائم، قامت الجزائر بتطوير مجموعة من القوانين والأنظمة التي تهدف إلى تنظيم التعاملات الإلكترونية وحماية الحقوق الرقمية. وتشمل هذه التشريعات قانون العقوبات، قانون حماية البيانات الشخصية، قانون مكافحة الجرائم السيبرانية، بالإضافة إلى القوانين الخاصة بالأمن السيبراني و التعاون الدولي في مجال مكافحة الجرائم الإلكترونية.

يتناول هذا المطلب القوانين والأنظمة التي وضعتها الجزائر لمواجهة الجرائم الإلكترونية، وسبل تنظيم هذه الأفعال المعاقب عليها، مع إلقاء الضوء على أهم النصوص القانونية التي تتعلق بالحماية من هذه الأنواع من الجرائم وتحديد المسؤوليات والعقوبات المترتبة على ارتكابها.

[1]– عبد الحكيم بوشيخي، المرجع السابق ، ص218.

الفرع الأول: عرض لأهم القوانين والأنظمة الجزائرية المتعلقة بالجرائم الإلكترونية

في ظل تزايد المخاطر المرتبطة بالجرائم الإلكترونية في الجزائر، وضعت الدولة مجموعة من القوانين والأنظمة التي تهدف إلى مواجهة هذا التحدي، وحماية الأمن السيبراني وحفظ البيانات الشخصية.

وتشمل هذه التشريعات مختلف الجوانب القانونية المتعلقة بالجرائم الإلكترونية، مثل الاختراقات الرقمية، الاحتيال الإلكتروني، التشهير الرقمي، و الجرائم المرتبطة بالأنظمة المعلوماتية. [1].

في هذا الفرع، سنعرض أهم القوانين والأنظمة الجزائرية التي تتعلق بالجرائم الإلكترونية، وتوضح كيفية تنظيم الدولة لهذه الجرائم وآليات معاقبة مرتكبيها.

أولا : قانون العقوبات الجزائري (قانون رقم 66-156 المعدل والمتمم)

يعد قانون العقوبات الجزائري من القوانين الأساسية التي تعالج الجرائم الإلكترونية في الجزائر. تم تعديل هذا القانون ليتناسب مع التحديات الجديدة التي فرضتها تكنولوجيا المعلومات. ويشمل هذا القانون عدة مواد تجرم الأفعال الإلكترونية التي تمس بأنظمة المعلومات.

المادة 392 مكرر: تتعامل مع الاختراقات الإلكترونية، حيث يُعاقب كل من يحاول اختراق الأنظمة المعلوماتية أو الاستيلاء على البيانات الرقمية دون إذن قانوني. هذه المادة تجرم التلاعب أو العبث بالبيانات الشخصية أو المؤسسية المخزنة إلكترونيًا[2].

[1]- عبد الحكيم بوشيخي، المرجع السابق ، ص 219.

[2]- المادة 392 مكرر من قانون العقوبات الجزائري.

المادة 403: تختص بالاحتيال الإلكتروني، ويشمل التزوير الإلكتروني و المواقع المزيفة، حيث يعاقب القانون من يستخدم الإنترنت أو البرمجيات الرقمية لارتكاب الاحتيال، مثل التلاعب بالمعاملات المالية أو سرقة المعلومات الشخصية[1].

ثانيا : قانون حماية البيانات الشخصية (قانون رقم 18-07)

صدر هذا القانون في 2018 بهدف حماية البيانات الشخصية للأفراد من الاستخدام غير المشروع أو التسريب. في عصر الإنترنت، أصبحت البيانات الشخصية هدفًا رئيسيًا للعديد من الجرائم الإلكترونية، مثل الاحتيال و السرقة الرقمية.

1 - أهم النقاط التي يتناولها هذا القانون:

أ - تعريف البيانات الشخصية وكيفية جمعها، تخزينها، ومعالجتها.

- حق الأفراد في حماية بياناتهم الشخصية، بما في ذلك الحق في الوصول إلى بياناتهم أو تصحيحها.

- إنشاء لجنة وطنية لحماية البيانات الشخصية لضمان تنفيذ القانون ومراقبة انتهاكاته.

- عقوبات قانونية تشمل الغرامات و السجن في حالة استخدام البيانات الشخصية بشكل غير قانوني.

ثالثا : قانون مكافحة الجرائم السيبرانية (قانون رقم 20-06)

يعد قانون مكافحة الجرائم السيبرانية من أحدث التشريعات التي أصدرتها الجزائر لمكافحة الجرائم التي تحدث عبر الإنترنت. يشمل هذا القانون القرصنة الإلكترونية، الهجمات الرقمية، و الابتزاز الإلكتروني[2].

[1]- المادة 403 من قانون العقوبات الجزائري.

[2]- القانون رقم 20-06 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 27، سنة 2020.

أبرز ملامح هذا القانون:

أ – **القرصنة:** يُعاقب كل من يخترق أنظمة المعلومات الخاصة بالمؤسسات أو الأفراد.

ب – **الهجمات الرقمية:** مثل الفيروسات والبرمجيات الخبيثة التي تُستخدم لتعطيل الأنظمة المعلوماتية أو سرقة البيانات.

ج – **الابتزاز الرقمي:** يعاقب القانون على التهديدات أو المطالبات المالية التي تتم عبر الإنترنت باستخدام معلومات شخصية أو حساسة.

يتضمن القانون عقوبات مشددة على مرتكبي الجرائم الإلكترونية، مثل السجن لفترات طويلة و غرامات مالية ضخمة.

رابعا : قانون مكافحة الإرهاب (قانون رقم 04-06)

نظرًا لأن بعض الجرائم الإلكترونية قد تكون مرتبطة بأنشطة إرهابية، فإن قانون مكافحة الإرهاب في الجزائر يشمل نصوصًا تتعلق بالأفعال الإرهابية التي تُرتكب عبر الإنترنت، وقد عمل المشرع الجزائري على تطوير الإطار القانوني لمواجهة التحديات الرقمية، بدءًا من القانون رقم 04-06 المتعلق بالأمن المعلوماتي، وصولًا إلى القانون رقم 20-06 الذي يُعنى بشكل مباشر بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1]

النصوص القانونية المتعلقة بالجرائم الإلكترونية تشمل:

أ – **الدعاية الإرهابية عبر الإنترنت:** يُحظر نشر أفكار إرهابية أو تحريض على العنف عبر الشبكات الرقمية.

ب – **التجنيد الرقمي:** يعاقب على التجنيد الإلكتروني للانضمام إلى جماعات إرهابية.

[1] – القانون رقم 04-06 المؤرخ في 23 يونيو 2004، المتعلق بالقواعد المطبقة على الممارسات المتعلقة بالأمن المعلوماتي، الجريدة الرسمية، العدد 41، سنة 2004.

ج – التمويل الإلكتروني للإرهاب: يُجرم القانون استخدام الوسائل الإلكترونية لجمع الأموال أو تمويل الأنشطة الإرهابية.

خامسا : قانون الأمن السيبراني (قانون رقم 21-01)

في إطار تعزيز الأمن السيبراني[1]، أصدرت الجزائر قانونًا خاصًا ينظم حماية الأنظمة المعلوماتية في القطاعين العام و الخاص، ويهدف إلى ضمان حماية البنية التحتية الرقمية للدولة والمؤسسات من الهجمات الإلكترونية محتويات القانون تشمل:

تعزيز الأمن السيبراني: من خلال توفير إجراءات حماية للأنظمة الإلكترونية الوطنية من التهديدات الرقمية.

فرض مسؤولية على الأفراد والمؤسسات في حماية بياناتهم وأنظمتهم المعلوماتية.

التعاون الدولي: يسعى القانون إلى تعزيز التعاون مع الدول الأخرى في مكافحة الجرائم الإلكترونية عبر الإنترنت.

سادسا : القانون الخاص بالمعاملات الإلكترونية

مع تطور التجارة الإلكترونية والمعاملات الرقمية في الجزائر، تم إصدار قانون المعاملات الإلكترونية لتنظيم استخدام التوقيع الرقمي و العقود الإلكترونية[2].

أبرز محتويات هذا القانون:

– الاعتراف بالمعاملات الإلكترونية كأدوات قانونية معترف بها من قبل السلطات القضائية.

– تنظيم التوقيع الرقمي وتحديد شروطه القانونية.

– تعزيز الثقة في التجارة الإلكترونية من خلال توفير إجراءات أمنية لضمان سلامة المعاملات.

[1] – القانون رقم 21-01 المؤرخ في 8 مارس 2021، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 16، سنة 2021.

[2] – القانون رقم 18-05 المؤرخ في 10 مايو 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 28، سنة 2018.

سابعا : الاتفاقيات الدولية لمكافحة الجرائم الإلكترونية

أدركت الجزائر أن الجرائم الإلكترونية لا تعرف الحدود، ولذلك فهي جزء من التعاون الدولي لمكافحة هذه الجرائم عبر الإنترنت. ومن أبرز الاتفاقيات التي انضمت إليها الجزائر:

– اتفاقية بودابست لمكافحة الجرائم الإلكترونية التي أقرها مجلس أوروبا في عام 2001. [1]

– التعاون الثنائي مع دول أخرى في مجالات التحقيق والتبادل القانوني لمكافحة الجريمة الإلكترونية العابرة للحدود.

– لقد وضعت الجزائر مجموعة من القوانين والأنظمة التي تتعامل مع الجرائم الإلكترونية، وتستهدف حماية البيانات الشخصية، الأمن السيبراني، والحقوق الرقمية للأفراد والمؤسسات.

تُمثل هذه القوانين خطوة هامة نحو مكافحة الجرائم التي تهدد النظام الرقمي في البلاد، إلا أن التطور السريع في تكنولوجيا المعلومات يستدعي تحديث هذه التشريعات بشكل دوري لضمان فعاليتها في مواجهة التهديدات الإلكترونية المتزايدة.

الفرع الثاني: تحليل كيفية تكييف التشريع الجزائري لمواجهة تطور الجرائم الإلكترونية

تواجه الجزائر تحديات كبيرة في مواجهة الجرائم الإلكترونية، إذ يظل هذا المجال عرضة للتطور المستمر في ظل التقدم التكنولوجي السريع وظهور أدوات جديدة للجرائم الإلكترونية. وعليه، فإن التشريع الجزائري في هذا المجال بحاجة إلى التكيف المستمر لضمان التصدي بفعالية لهذه الجرائم التي تتسم بالحداثة والتعقيد. من خلال هذا الفرع، سنقوم بتحليل كيفية تكييف التشريع الجزائري لمواجهة تطور الجرائم الإلكترونية، مع التركيز على التحولات القانونية التي اتخذتها الدولة في السنوات الأخير.

[1] – اتفاقية بودابست بشأن الجرائم المعلوماتية، المعتمدة في 23 نوفمبر 2001، من قبل مجلس أوروبا، ودخلت حيز التنفيذ في 1 يوليو 2004.

أولا : التعديل المستمر لقانون العقوبات الجزائري

أحد أبرز التكيفات التي قام بها المشرع الجزائري في مواجهة الجرائم الإلكترونية هو التعديل المستمر لقانون العقوبات الجزائري. ففي بداية الأمر، كان القانون العقابي الجزائري يفتقر إلى أحكام خاصة بالجرائم الإلكترونية، لكنه بدأ يدمج هذه الجرائم تدريجياً في إطار النصوص القانونية المتعلقة بالجريمة.

1 – إضافة مواد جديدة: تم إدخال مواد خاصة بالجرائم الإلكترونية، مثل المادة 392 مكرر و المادة 403، اللتين تجرمان القرصنة الإلكترونية و الاحتيال الرقمي على التوالي. هذا التعديل كان خطوة هامة لمواكبة التحولات التكنولوجية.

2 – التوسع في التعريفات: تم تحديث التعريفات الخاصة بالمخالفات الإلكترونية بما يتناسب مع تطور أدوات الجريمة الإلكترونية. كما أن التوسع في مفهوم البيانات الشخصية و الأنظمة المعلوماتية ساعد في توفير حماية قانونية أفضل ضد المخاطر الرقمية المتزايدة.

ثانيا : تشديد العقوبات على الجرائم الإلكترونية

إن تشديد العقوبات على الجرائم الإلكترونية كان من أبرز التكييفات التي أُدخلت على التشريع الجزائري. إذ تعكس العقوبات الواردة في التشريعات مدى خطورة الأفعال الإلكترونية التي تُرتكب في عالمنا المعاصر، فضلاً عن تأثيرها المباشر على الأفراد والمؤسسات.

أ – العقوبات الثقيلة: جرى تحديد عقوبات السجن و الغرامات المالية بشكل صارم لمن يقوم باختراق أنظمة المعلومات أو استخدام الإنترنت في عمليات الاحتيال أو الابتزاز. على سبيل المثال، يمكن أن تصل العقوبة إلى السجن لفترات طويلة أو غرامات مالية كبيرة.

ب – الجرائم المرتبطة بالأنظمة الحساسة: في حال كانت الجريمة الإلكترونية تستهدف المؤسسات الحكومية أو البنية التحتية الحيوية للدولة، تكون العقوبات أشد، مما يعكس اهتمام الجزائر بحماية الأنظمة الحساسة من الهجمات الإلكترونية.

ثالثا : إنشاء هيئة متخصصة في حماية البيانات الشخصية

أقرّ قانون حماية البيانات الشخصية رقم 18-07 المؤرخ في 10 يونيو 2018 (المفعّل اعتبارًا من 12 أغسطس 2023) إطارًا قانونيًا شاملاً لحماية الأشخاص الطبيعيين في مجال معالجة البيانات الشخصية[1] وقد أنشأت الجزائر بموجب هذا القانون الهيئة الوطنية المستقلة لحماية البيانات الشخصية(ANPDP) ، التي تشرف على احترام المعايير التشريعية، وتعمل على مراقبة استخدام البيانات وضمان حقوق الأفراد، من خلال مهامها التي تشمل إصدار التراخيص، استقبال التصريحات، فرض العقوبات الإدارية أو الجنائية، والقيام بعمليات تفتيش ميدانية.

أ – الموافقة المسبقة: ينص القانون على ضرورة الحصول على موافقة الأفراد قبل جمع أو استخدام بياناتهم الشخصية. هذا يشكل خطوة مهمة لضمان حماية الأفراد من الاحتيال الرقمي أو الاستغلال غير المشروع لبياناتهم.

ب – عقوبات صارمة: تفرض اللجنة عقوبات قانونية ضد الجهات التي تنتهك حقوق الأفراد في خصوصية البيانات الشخصية، مثل الغرامات أو السجن، مما يعكس جدية الجزائر في حماية خصوصية الأفراد.

[1]– قانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، 10 يونيو 2018؛ ودخول القانون حيّز التنفيذ في 12 أغسطس 2023 بإصدار نماذج التصريح لدى الهيئة الوطنية؛ انظر أيضًا ANPDP) National Data Protection Authority establishment)، أغسطس 2023.

رابعا : تطوير القوانين المتعلقة بالأمن السيبراني

بسبب تصاعد المخاطر المتعلقة بالأمن السيبراني، أقرّت الجزائر قانون الأمن السيبراني رقم 21-01 لعام 2021 لتعزيز حماية الأنظمة المعلوماتية والبيانات الوطنية من الهجمات الإلكترونية. ويهدف القانون إلى رفع قدرة الدولة على رصد الهجمات الإلكترونية وتحديد الإجراءات القانونية الواجب اتباعها لمكافحتها، خصوصًا في القطاعات الحساسة مثل الأنظمة المالية والطاقة[1].

أ – **الاحتياطات التقنية:** ينص القانون على إلزام المؤسسات بتطبيق معايير أمنية لحماية أنظمتها المعلوماتية من الهجمات المحتملة، مثل البرمجيات الخبيثة و الفيروسات.

ب – **التعاون مع الشركاء الدوليين:** يعزز هذا القانون من التعاون بين الجزائر والدول الأخرى في مجال مكافحة الجرائم السيبرانية، بما في ذلك التبادل المعلوماتي بشأن الهجمات الإلكترونية والتهديدات.

خامسا : التكييف مع التحديات العالمية والتعاون الدولي

إن الجرائم الإلكترونية عادة ما تتعدى حدود الدول، ولهذا تسعى الجزائر إلى تعزيز التعاون الدولي لمكافحة هذه الجرائم. تنخرط الجزائر في الاتفاقيات الدولية الخاصة بمكافحة الجرائم الإلكترونية، مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية، بالإضافة إلى الاتفاقيات الثنائية مع بعض الدول العربية والأوروبية.

أ – **التعاون القضائي:** تشمل هذه الاتفاقيات تبادل المعلومات القضائية والتعاون بين السلطات القضائية لدول مختلفة من أجل مكافحة الجرائم العابرة للحدود.

[1]– أيمن بارّة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر، جامعة ورقلة، 2022؛ يشير إلى أن القانون رقم 21-01 يضع "برامج وآليات تقنية وقدرات بشرية لمواجهة أي تعدٍّ على المعلومات الإلكترونية.

ب- التعاون في التحقيقات: بالإضافة إلى التعاون القضائي، يشمل التعاون الدولي أيضًا تبادل الخبرات والمساعدة في التحقيقات المتعلقة بالجرائم الإلكترونية، مما يساهم في تحقيق العدالة للضحايا بشكل أسرع وأكثر فاعلية.

سادسا : تنظيم المعاملات الإلكترونية

مع ازدهار التجارة الإلكترونية واستخدام الوسائل الرقمية في المعاملات اليومية، تم تعديل التشريعات الجزائرية لتشمل صرامة أكبر في الإجراءات. أبرزها:

- قانون رقم 15-04 الصادر في 1 فبراير 2015، الذي يحدد القواعد العامة للتوقيع والتصديق الإلكترونيين، ما يعزز الاعتماد القانوني على التواقيع الرقمية في الوثائق والمعاملات[1].

- تعديلات لاحقة اعترفت بالتوقيع الرقمي في الإجراءات المدنية، حيث أصبح معترفًا به مساويًا للتوقيع التقليدي وفقًا للمادة 327 من القانون المدني (بعد تعديل 2020) [2].

- كما تقر التشريعات الحديثة في قانون 18-05 (2018) الخاص بالتجارة الإلكترونية بضرورة التسجيل في السجل التجاري، واحتياج المواقع الإلكترونية للامتثال القانوني[3].

تأتي هذه التطورات لتعزيز الثقة القانونية في المعاملات الإلكترونية، وتوفير حماية قانونية فعّالة عند حدوث نزاعات أو تلاعب، عبر ضمان سلامة العقود الرقمية وسريتها.

---

[1]- قانون رقم 15-04 المؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد 06، الصادرة بتاريخ 8 فبراير 2015.

[2]- القانون المدني الجزائري، الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، الجريدة الرسمية للجمهورية الجزائرية، العدد 78 لسنة 1975، مع التعديلات الأخيرة لا سيما بموجب القانون رقم 05-10 المؤرخ في 20 يونيو 2005، والقانون رقم 07-05 المؤرخ في 13 مايو 2007.

[3]- قانون رقم 18-05 الصادر في نوفمبر 2018 بشأن التجارة الإلكترونية، الذي يفرض تسجيل المتعاملين ورقمنة العمليات مع ضرورة امتلاك نطاق ".dz" والسجل التجاري.

أ – **الاعتراف بالتوقيع الرقمي:** يعترف القانون بالتوقيع الرقمي كأداة قانونية معترف بها، مما يسهم في حماية الأطراف المتعاملة من الاحتيال والتزوير.

ب – **القوانين المتعلقة بالحماية في المعاملات التجارية:** تتضمن هذه القوانين حماية لحقوق الأفراد في حال حدوث خداع أو استغلال في المعاملات الإلكترونية، مثل استخدام المواقع المزيفة أو سرقة الأموال.

من خلال استعراض الإجراءات المتخذة من قبل التشريع الجزائري لمواجهة تطور الجرائم الإلكترونية، يتضح أن الجزائر قد قامت بتكييف قوانينها بشكل تدريجي للتعامل مع هذا النوع من الجرائم. فالتشريعات الجزائرية تتسم بالمرونة والتحديث المستمر، سواء من خلال تشديد العقوبات أو إدخال قوانين جديدة أو التعاون الدولي، مما يعكس رغبة الدولة في حماية الأمن السيبراني والحقوق الرقمية للمواطنين. ومع استمرار تطور التكنولوجيا، تبقى الحاجة قائمة لتحديث وتطوير هذه التشريعات بشكل مستمر لضمان مواجهة التحديات المستقبلية في هذا المجال.

المطلب الثاني: التعاون الدولي في مكافحة الجرائم الإلكترونية

تُعتبر الجرائم الإلكترونية جرائمًا عابرة للحدود حيث تتجاوز الدول والقارات، مما يعقّد معالجتها على المستوى الوطني[1]، وعلى الرغم من الجهود المحلية، أصبح التعاون الدولي عنصرًا أساسيًا في أي استراتيجية فعالة، وذلك عبر تنسيق الجهود بين الدول والهيئات الدولية.

يتناول هذا المطلب آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مع عرض أهم الاتفاقيات الدولية المبرمة. نبرز أيضًا دور الجزائر في تعزيز أمنها السيبراني من خلال الانخراط في شبكات التعاون ومبادرات التكوين، مثل التعاون مع مكتب الأمم المتحدة لمكافحة

[1]– أبحاث أكاديمية تؤكد أن الجرائم الإلكترونية، لطابعها العابر للحدود، لا يمكن مكافحتها دون تعاون دولي.

الإرهاب (UNODC) للتبادل الفوري للأدلة الرقمية عبر الحدود[1]، والمشاركة في برامج CyberSouth+ التابعة لمجلس أوروبا لتدريب القضاء على معالجة الأدلة الإلكترونية[2]، رغم أن الجزائر لم توقع حتى الآن اتفاقية بودابست 2001[3]، فإنها تعتمد على المساعدة القانونية المتبادلة بموجب قانون 09-04 (مادة 27) لتسريع تبادل البيانات وتطبيق network 7/24 في الحالات العاجلة.

الفرع الأول: دور الجزائر في الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية

تعتبر الجرائم الإلكترونية من التحديات الكبرى التي تواجهها الدول في العصر الرقمي، مما يستدعي تعزيز التعاون الدولي لمكافحة هذه الأنواع من الجرائم العابرة للحدود. الجزائر، كما هو الحال مع العديد من الدول الأخرى، تدرك أهمية التعاون الدولي لمكافحة هذه الجرائم على المستوى العالمي، وتعمل على الانضمام إلى مختلف الاتفاقيات الدولية التي تهدف إلى تعزيز الأمن السيبراني وحماية البيانات الشخصية، بالإضافة إلى ضمان التحقيق الفعّال في الجرائم الإلكترونية.

في هذا الفرع، سنستعرض دور الجزائر في الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية، ونلقي الضوء على التزامها بالقوانين الدولية وتعاونها مع دول العالم في هذا المجال.

[1]– منظمة UNODC دعمت الجزائر لمشاركة الأدلة الإلكترونية عبر الحدود ومكافحة الإرهابيين الإلكترونيين، ضمن تدريب (فبراير 2021).

[2]– مشروع 2026–2024) +CyberSouth) يعزز قدرات القضاء الجزائري على التعامل مع الأدلة الإلكترونية في إطار تعاون بين الاتحاد الأوروبي ومجلس أوروبا.

[3]– الجزائر لم توقع على اتفاقية بودابست لكنها تعتمد على قانون 09-04 لتنظيم المساعدة القانونية المتبادلة وتفعيل شبكة الطوارئ 7/24 تبعًا للمواد 27 و35 من القانون ذاته.

1 –انضمام الجزائر إلى اتفاقية بودابست لمكافحة الجرائم الإلكترونية

تُعتبر اتفاقية بودابست، التي أُبرمت عام 2001 من قبل مجلس أوروبا، واحدة من أبرز الاتفاقيات الدولية الخاصة بمكافحة الجرائم الإلكترونية. وتهدف هذه الاتفاقية إلى وضع إطار قانوني موحد لملاحقة الجرائم المعلوماتية على المستوى الدولي، بما في ذلك القرصنة الإلكترونية، الاحتيال الرقمي، التزوير الإلكتروني، والتهديدات السيبرانية العابرة للحدود. كما تشجع على التعاون الدولي بين الدول الأطراف وتيسير تبادل الأدلة الرقمية عبر الحدود[1].

أ – الجزائر وانضمامها إلى الاتفاقية: الجزائر كانت من الدول الموقعة على اتفاقية بودابست، وهي واحدة من الدول غير الأوروبية التي انضمت إلى هذا الاتفاق. انضمام الجزائر إلى هذه الاتفاقية يعكس التزامها بتطوير التشريعات الوطنية لمكافحة الجرائم الإلكترونية وضمان تعاون دولي فعال في هذا المجال.

ب – أهداف الجزائر من الانضمام:

* **توحيد التشريعات:** الانضمام إلى هذه الاتفاقية يساهم في توحيد التشريعات الجزائرية مع تلك المعمول بها في الدول الأوروبية وغيرها من الدول الموقعة، مما يعزز من فعالية مكافحة الجرائم الإلكترونية.

* **التعاون القضائي والتبادل المعلوماتي:** تتيح الاتفاقية للجزائر فرصة التعاون القضائي مع الدول الأخرى من خلال تبادل المعلومات والبيانات المتعلقة بالجرائم الإلكترونية، بما يعزز التحقيقات العابرة للحدود.

[1] – اتفاقية بودابست لمكافحة الجرائم الإلكترونية، مجلس أوروبا، 23 نوفمبر 2001، تم فتحها للتوقيع في بودابست ودخلت حيز التنفيذ في 1 يوليو 2004. وهي أول اتفاقية دولية تهدف إلى مواجهة الجرائم المرتكبة عبر الإنترنت وتعزيز التعاون الدولي في هذا المجال.

*** تطبيق أحكام الاتفاقية في الجزائر:** بعد انضمام الجزائر إلى اتفاقية بودابست، قامت بتعديل بعض من قوانينها الوطنية، بما في ذلك قانون العقوبات و قانون حماية البيانات الشخصية، بما يتناسب مع المعايير الدولية التي نصت عليها الاتفاقية. هذا التعديل يساهم في تحسين قدرة الجزائر على مواجهة التهديدات الرقمية بشكل قانوني وفعال[1].

ثانيا : التعاون مع الشرطة الدولية (الإنتربول) في مكافحة الجرائم الإلكترونية

يعتبر الإنتربول أحد أبرز المنظمات الدولية التي تساهم في مكافحة الجرائم الإلكترونية على مستوى العالم. تهدف الشرطة الدولية إلى تعزيز التعاون بين الأجهزة الأمنية في الدول الأعضاء من أجل مكافحة الجرائم السيبرانية التي قد تهدد الأمن العام العالمي.

1 – دور الجزائر مع الإنتربول: الجزائر تعد من الدول الأعضاء في الإنتربول، وتشارك في مختلف المبادرات التي تهدف إلى تعزيز التعاون الدولي في مجال الأمن السيبراني.

2 – المساهمات الجزائرية:

أ – تبادل المعلومات: الجزائر تتعاون مع الإنتربول في تبادل المعلومات المتعلقة بالتهديدات الإلكترونية مثل الهجمات الإلكترونية و القرصنة.

ب الاستفادة من الدورات التدريبية: الجزائر تشارك في ورش العمل والدورات التدريبية التي ينظمها الإنتربول، مما يعزز من قدرة الأجهزة الأمنية الجزائرية على مواجهة التهديدات الرقمية الحديثة.

[1] –Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, Budapest, 23.XI.2001.

ثالثا : اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية

اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية تسعى إلى إنشاء إطار قانوني دولي لمكافحة الجرائم الإلكترونية، خاصة تلك التي تستهدف البنية التحتية الحساسة، مثل أنظمة الطاقة والاتصالات[1].

1 – دور الجزائر في هذه الاتفاقية: الجزائر تعد من الدول التي تدعم هذه الاتفاقية من خلال تفعيل القوانين المحلية التي تلتزم بها الدول الأعضاء، مما يساهم في تعزيز حماية الأمن السيبراني وحماية المؤسسات الحكومية من الهجمات الإلكترونية.

2 – أهداف الاتفاقية بالنسبة للجزائر:

أ – حماية الأنظمة الحكومية: تتيح الاتفاقية للجزائر تقوية تدابير الأمن السيبراني على المستوى الوطني، مما يساعد في حماية المؤسسات الحكومية والخدمات الحيوية.

ب – التعاون الدولي: تعزز هذه الاتفاقية التعاون بين الجزائر والدول الأخرى في مواجهة الجريمة الإلكترونية العابرة للحدود، وهو أمر بالغ الأهمية في ظل تزايد التهديدات الرقمية العالمية.

رابعا : التعاون الإقليمي مع الدول العربية والاتحاد الإفريقي

إلى جانب التزامات الجزائر الدولية، تشارك الجزائر في التعاون الإقليمي لمكافحة الجرائم الإلكترونية مع الدول العربية والدول الإفريقية، وذلك من خلال المشاركة في مؤتمرات ومنظمات مختصة في الأمن السيبراني.

[1]– الأمم المتحدة، Convention on Cybercrime, تبنّت من قبل الجمعية العامة في ديسمبر 2024؛ يفرض الاتفاق إحلال تشريعات وطنية تتناول "الولوج غير المصرّح به إلى نظام معلوماتي، والمساس بالبيانات أو أنظمة البنية التحتية الحساسة"، ويشدد على آليات التعاون الدولي وتبادل الأدلة الإلكترونية.

أ – **الجزائر والمنظمات العربية:** الجزائر عضو فعال في منظمة التعاون الإسلامي (OIC) و جامعة الدول العربية، حيث تشارك في مبادرات إقليمية تهدف إلى تعزيز الأمن السيبراني في منطقة الشرق الأوسط وشمال إفريقيا[1].

ب – مركز التعاون العربي للأمن السيبراني: الجزائر تساهم في هذه المبادرات الإقليمية التي تهدف إلى رفع مستوى الوعي وتعزيز التعاون بين الدول العربية في مواجهة التهديدات الإلكترونية[2].

ج – التعاون مع الاتحاد الإفريقي: الجزائر تشارك في الجهود التي تبذلها الاتحاد الإفريقي في مجال الأمن السيبراني، حيث يتم تبادل الخبرات والمعلومات بين الدول الأعضاء بهدف التصدي للتهديدات الإلكترونية التي تؤثر على الأنظمة المعلوماتية في المنطقة.

خامسا : التحديات التي تواجه الجزائر في تطبيق الاتفاقيات الدولية : رغم التقدم الذي أحرزته الجزائر في مجال التعاون الدولي لمكافحة الجرائم الإلكترونية، إلا أن هناك تحديات تواجهها في تطبيق هذه الاتفاقيات، ومنها:

1 – الفجوة التقنية: لا يزال هناك تفاوت بين الجزائر وبعض الدول المتقدمة من حيث التكنولوجيا و القدرات التقنية لمكافحة الجرائم الإلكترونية، مما قد يشكل تحديًا في تنفيذ بعض جوانب الاتفاقيات الدولية.

2 – التنسيق المحلي والدولي: رغم وجود الآليات القانونية، إلا أن التنسيق بين الجهات المحلية والدولية لا يزال يحتاج إلى تعزيز ليكون أكثر فاعلية في التعامل مع الجرائم الإلكترونية المتطورة.

[1]– استضافت الجزائر القمة السابعة للأمن السيبراني الإفريقي عام 2019، بمشاركة خبراء أفارقة وأجانب، تحت شعار "أفريقيا الرقمية الآمنة.

[2]– المركز العربي الإقليمي للأمن السيبراني نظم "تمرينًا سيبرانيًا" بمراكش عام 2024 بمشاركة 80 متخصصًا من 18 دولة عربية وإفريقية، في إطار تعاون مشترك مع الاتحاد الدولي للاتصالات وواشنطن للمعلومات السيبرانية.

3 – القوانين المحلية: قد تواجه الجزائر بعض الصعوبات في تحديث التشريعات الوطنية لتتناسب مع الاتفاقيات الدولية، خاصة فيما يتعلق بتكييف قانون العقوبات مع التحديات المتزايدة في مجال الجرائم الإلكترونية[1].

تعتبر الجزائر من الدول الفاعلة في التعاون الدولي لمكافحة الجرائم الإلكترونية، من خلال انضمامها إلى اتفاقية بودابست ومشاركتها في الشرطة الدولية و اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية. تسهم هذه الجهود في تعزيز الأمن السيبراني في الجزائر، وتساعد في تعزيز التعاون الإقليمي والدولي لمكافحة الجرائم الإلكترونية العابرة للحدود. ومع ذلك، تواجه الجزائر تحديات في تطبيق هذه الاتفاقيات على أرض الواقع، مما يتطلب تعزيز التعاون بين الدول والأجهزة المعنية لضمان مكافحة فعّالة لهذه الجرائم.

الفرع الثاني: التحديات التي تواجه الجزائر في تطبيق هذه الاتفاقيات

رغم الجهود التي تبذلها الجزائر في مجال التعاون الدولي لمكافحة الجرائم الإلكترونية، فإن هناك العديد من التحديات التي قد تؤثر على قدرتها في تطبيق الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية. هذه التحديات تتنوع بين التحديات القانونية، التقنية، و الإدارية، مما قد يعوق فعالية تطبيق الاستراتيجيات الدولية لمكافحة الجرائم الإلكترونية على مستوى البلاد.

في هذا الفرع، سنتناول أهم التحديات التي تواجه الجزائر في تطبيق الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية، وكيفية التأثير المحتمل على جهودها في هذا المجال[2].

[1] – شاركت الجزائر في ورشات) CyberSouth سيبروسوث) التي تنظمها مجلس أوروبا، مثل المؤتمر الوطني حول الجرائم الإلكترونية (سبتمبر 2023، الجزائر العاصمة).

[2] – محمد عبد الحليم غنيم، المرجع السابق ، ص44.

1 – الفجوة التقنية وعدم التطور التكنولوجي

تعتبر التكنولوجيا من أبرز العوامل التي تؤثر في قدرة الدول على مكافحة الجرائم الإلكترونية. الجزائر، على الرغم من تقدمها في العديد من المجالات، تواجه تحديًا كبيرًا في الاستثمار في البنية التحتية الرقمية المتطورة، وهو ما يحد من قدرتها على تنفيذ الاتفاقيات الدولية المتعلقة بالأمن السيبراني.

أ – نقص في البنية التحتية الرقمية: الجزائر لا تزال تواجه تحديات في بناء بنية تحتية رقمية متقدمة وقوية تكفل حماية الأنظمة المعلوماتية من الهجمات الإلكترونية المعقدة. التهديدات السيبرانية الحديثة تتطلب أنظمة أمنية حديثة ومتطورة لمواكبة الهجمات المستمرة.

ب – نقص في الخبرات الفنية المتخصصة: هناك نقص في المتخصصين في مجال الأمن السيبراني و التقنيات الحديثة التي تسمح بالتطبيق الفعال للأدوات والأطر القانونية الدولية. التعامل مع الجرائم الإلكترونية يتطلب وجود كفاءات تقنية قادرة على مواكبة التحديثات المستمرة في هذا المجال.

ج – صعوبة التأقلم مع التكنولوجيات الحديثة: التحديات التكنولوجية تتزايد مع التطور السريع للتقنيات الحديثة مثل الذكاء الاصطناعي و البيانات الضخمة، والتي يمكن أن تستغل في ارتكاب الجرائم الإلكترونية، بينما تظل الأجهزة الوطنية في الجزائر بحاجة إلى التكيف مع هذه التطورات.

2 – الفجوة التشريعية والقانونية

إن إنشاء إطار قانوني متكامل لمكافحة الجرائم الإلكترونية يعد أمرًا بالغ الأهمية لمكافحة هذه الجرائم بكفاءة. ولكن الجزائر تواجه بعض التحديات فيما يتعلق بتكييف التشريعات الوطنية مع المعايير الدولية الواردة في الاتفاقيات العالمية، مثل اتفاقية بودابست وغيرها من الاتفاقيات الدولية.

أ- **تحديات التحديث التشريعي:** رغم أن الجزائر قد قامت بتحديث بعض من تشريعاتها، مثل قانون العقوبات و قانون حماية البيانات الشخصية، إلا أن القوانين المحلية قد لا تكون محدثة بما يتماشى مع التطور السريع للجرائم الإلكترونية وأساليبها الحديثة. مثلًا، هناك حاجة إلى تكييف قوانين الخصوصية و حماية البيانات بما يتماشى مع أحدث المعايير الدولية.

ب - **تباين التشريعات بين الدول:** بالرغم من توقيع الجزائر على اتفاقية بودابست، إلا أن هناك تفاوتًا في تطبيق بعض بنود الاتفاقية بشكل يتماشى مع القوانين الوطنية، مما يعوق التنسيق الفعّال بين الجزائر ودول أخرى، خاصة في المسائل المتعلقة بـ التعاون القضائي و تبادل المعلومات. [1]

ج - **تحديات التوفيق بين حقوق الخصوصية والأمن:** تطبيق الاتفاقيات الدولية قد يواجه تحديًا في ما يتعلق بـ حقوق الخصوصية وحماية البيانات الشخصية. في بعض الأحيان، قد يتعارض المطلب الأمني لمكافحة الجرائم الإلكترونية مع القوانين المحلية التي تضمن حماية الأفراد من التجاوزات في مراقبة البيانات.

3 - التحديات الإدارية واللوجستية

تطبيق الاتفاقيات الدولية يتطلب وجود آليات إدارية فعّالة وقادرة على التنسيق بين مختلف الجهات المعنية في مكافحة الجرائم الإلكترونية. الجزائر تواجه تحديات في هذا السياق، حيث يتطلب التعاون الدولي التنسيق بين الجهات الحكومية و القطاع الخاص و الهيئات الدولية.

[1] - عبد القادر بوشاشي، المرجع السابق ، ص66.

أ – عدم وجود آليات متكاملة للتنسيق بين الجهات: في بعض الأحيان، يواجه التنسيق بين الأجهزة الحكومية الجزائرية المختلفة تحديات، مثل الشرطة، القضاء، و هيئات حماية البيانات. هذا يعوق سرعة تنفيذ التشريعات الخاصة بالأمن السيبراني والجرائم الإلكترونية.

ب – قصر في الوعي المؤسساتي: تحتاج المؤسسات الحكومية في الجزائر إلى مزيد من التوعية والتدريب لضمان فهمها الكامل لأبعاد الاتفاقيات الدولية وأثرها على تشريعات مكافحة الجرائم الإلكترونية. كما يحتاج بعض المسؤولين إلى التدريب المستمر لمواكبة التغيرات التقنية في هذا المجال[1].

ج – تحديات التنسيق الدولي: الجزائر، على الرغم من مشاركتها في العديد من الاتفاقيات الدولية، قد تواجه صعوبة في التنسيق الفعّال مع الدول الأخرى بسبب الاختلافات في الأنظمة القانونية والممارسات القضائية، مما يؤثر على سرعة الإجراءات والتعاون في مكافحة الجرائم الإلكترونية العابرة للحدود.

4 – التحديات المتعلقة بالتمويل والموارد

تعتبر الموارد المالية من العوامل التي قد تؤثر في تطبيق الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية في الجزائر.

أ – نقص التمويل اللازم:

تحتاج الجزائر إلى استثمارات مالية ضخمة لبناء أنظمة أمن سيبراني متطورة، وتدريب الكوادر، وتحديث التشريعات، مما قد يحد من قدرة الدولة على التنفيذ الفعّال لهذه الاتفاقيات.

[1]– أحمد بلحاج، المرجع السابق ، ص98.

ب – صعوبة تخصيص الموارد بشكل كافٍ:

في ظل التحديات الاقتصادية التي قد تواجهها الجزائر، قد يكون تخصيص الموارد الكافية لمكافحة الجرائم الإلكترونية أمرًا صعبًا. يحتاج تطبيق الاتفاقيات إلى تمويل مستمر لإنشاء البنية التحتية المتقدمة لمكافحة هذه الجرائم[1].

5 – التحديات المتعلقة بالوعي المجتمعي

إن الوعي المجتمعي بالجرائم الإلكترونية وأثرها يعد من العوامل الأساسية في تحسين فعالية مكافحة هذه الجرائم، وهو ما قد يواجه تحديات في الجزائر.

أ – نقص الوعي الجماهيري:

بالرغم من تطور مفهوم الأمن السيبراني عالميًا، إلا أن العديد من الأفراد والمؤسسات في الجزائر قد يفتقرون إلى الوعي الكافي حول التهديدات الإلكترونية وأهمية اتخاذ إجراءات وقائية للحماية من هذه الجرائم.

ب – أهمية التوعية والتعليم:

من الضروري أن تعمل الجزائر على رفع الوعي من خلال البرامج التثقيفية التي تستهدف مختلف فئات المجتمع، بدءًا من الأفراد وصولًا إلى الشركات والمرافق الحكومية، لتعريفهم بأهمية تطبيق الاتفاقيات الدولية لمكافحة الجرائم الإلكترونية.

على الرغم من أن الجزائر قد أحرزت تقدمًا في تعزيز تعاونها الدولي لمكافحة الجرائم الإلكترونية، إلا أن هناك العديد من التحديات التي قد تواجهها في تطبيق الاتفاقيات الدولية المتعلقة بالأمن السيبراني. تشمل هذه التحديات الفجوة التقنية، التحديات التشريعية، المشاكل الإدارية واللوجستية، بالإضافة إلى الموارد المالية ونقص الوعي المجتمعي. هذه التحديات

[1]– محمد علي مكاوي، المرجع السابق، ص. 76.

تستدعي تطوير استراتيجيات محلية فعالة لمواجهة الجرائم الإلكترونية بالتوازي مع الاستمرار في تعزيز التعاون الدولي.

الفصل الثاني
العوائق والتحديات التي تواجه أجهزة التحقيق في مكافحة الجرائم الإلكترونية

أضحت الجرائم الإلكترونية تشكل تهديدًا متزايدًا ليس فقط للأفراد والمجتمعات، بل أيضًا للأنظمة الاقتصادية والسياسية في الدول. في الجزائر، ومع تزايد استخدام الإنترنت والتطور السريع للتكنولوجيا، أصبحت التحقيقات في الجرائم الإلكترونية أمرًا بالغ الأهمية لضمان الأمن السيبراني وحماية الحقوق الشخصية و الاقتصاد الرقمي، تشهد الجريمة الإلكترونية تطورًا متسارعًا يتزامن مع تطور تكنولوجيا المعلومات والاتصال، مما أدى إلى بروز تحديات كبيرة أمام أجهزة التحقيق التقليدية، التي لم تُصمم أساسًا لمواجهة هذا النوع المستحدث من الجرائم.

تتميز الجرائم الإلكترونية بالتعقيد الفني، والتطور المستمر في أدواتها وأساليب ارتكابها، فضلًا عن الطابع العابر للحدود الذي يصعّب من تحديد الاختصاص القضائي وملاحقة الجناة. كما أن نقص التكوين المتخصص، وصعوبة جمع الأدلة الرقمية، تعد من أبرز المعوقات التي تواجه المحققين في هذا المجال[1]، لذلك فإن أجهزة التحقيق في الجزائر، وعلى غرار دول العالم، مطالبة بتحديث أدواتها، وتعزيز التعاون الدولي، وتطوير مهارات الموارد البشرية، من أجل التصدي الفعّال لهذا النوع من الجريمة الحديثة. [2]

ومع ذلك، يواجه التحقيق في الجرائم الإلكترونية العديد من التحديات التي تعيق فعاليته في الجزائر. تتنوع هذه التحديات بين المشاكل التقنية، القانونية، و الإدارية، وتؤثر بشكل كبير على قدرة السلطات القضائية والأمنية على ملاحقة مرتكبي الجرائم الإلكترونية بشكل فعال.

في هذا الفصل، سنتناول أبرز التحديات التي تواجه التحقيقات في الجرائم الإلكترونية في الجزائر، وكيفية تأثير هذه التحديات على سرعة وكفاءة العمليات الجنائية في هذا المجال.

[1] – أحمد فلاق، التحقيق في الجرائم الإلكترونية: التحديات القانونية والتقنية، مجلة الدراسات القانونية، جامعة الجزائر 1، العدد 7، 2021، ص 55.

[2] – القانون رقم 20–06 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 27، سنة 2020.

كما سنستعرض كيفية تأثير التكنولوجيا الحديثة و التعاون الدولي في مواجهة هذه الجرائم، ومدى قدرة النظام القضائي الجزائري على التكيف مع التطورات الرقمية السريعة

المبحث الأول: العوائق القانونية والتقنية في الجرائم الإلكترونية في الجزائر

تُعد الجرائم الإلكترونية من أبرز التهديدات التي تواجه الأنظمة القانونية والأمنية في العديد من الدول، بما في ذلك الجزائر، في ظل الانتشار المتسارع للتكنولوجيا الرقمية والإنترنت، أصبحت الجرائم الإلكترونية أكثر تعقيدًا، وأدى ذلك إلى ظهور تحديات جديدة في مجال التحقيق و الملاحقة القضائية [1].

تتمثل أبرز التحديات التي تواجه الجزائر في الجرائم الإلكترونية في جانبين أساسيين هما: التحديات القانونية و التحديات التقنية. هذه التحديات تتداخل في العديد من الأحيان، مما يجعل التصدي لهذه الجرائم أمرًا معقدًا ويتطلب تحديث التشريعات وتطوير البنية التحتية التقنية في البلاد.

في هذا المبحث، سنستعرض التحديات الرئيسية التي يواجهها التشريع الجزائري و الأجهزة الأمنية في التعامل مع الجرائم الإلكترونية، وكيفية تأثير التطورات التقنية و القصور القانوني على فعالية التحقيقات والملاحقات القضائية. كما سنتناول التحديات المتعلقة بمواءمة القوانين المحلية مع المعايير الدولية لمكافحة هذه الجرائم، وكذلك صعوبة استخدام الأدوات التقنية المتطورة التي تواكب الجرائم الرقمية الحديثة.

[1]– بلعزوز، فاطمة الزهراء. الجرائم الإلكترونية في القانون الجزائري. مجلة الدراسات القانونية والسياسية، جامعة محمد خيضر بسكرة، العدد 17، 2020، ص. 122.

المطلب الأول: العوائق القانونية في التحقيقات في الجرائم الإلكترونية في الجزائر

تواجه الجزائر، كغيرها من الدول، العديد من التحديات القانونية في التحقيقات المتعلقة بالجرائم الإلكترونية، التي أصبحت تهدد الأمن السيبراني والمصالح الاقتصادية والاجتماعية. مع النمو المتسارع في استخدام التكنولوجيا الرقمية و الإنترنت، أصبح من الضروري تحديث القوانين الوطنية لتواكب التهديدات السيبرانية الجديدة والمستحدثة. ولكن، بالرغم من الجهود المبذولة لتطوير التشريعات، لا تزال هناك العديد من الثغرات القانونية التي تؤثر في قدرة النظام القضائي الجزائري على التحقيق الفعال في الجرائم الإلكترونية[1].

إن التحديات القانونية التي تواجه الجزائر في مجال التحقيقات في الجرائم الإلكترونية تتعدد وتشمل جوانب متعددة من النظام القانوني، مثل تحديد المسؤولية الجنائية، تطبيق القوانين الدولية، التعامل مع الأدلة الرقمية، بالإضافة إلى الخصوصية وحماية البيانات الشخصية. هذه التحديات تجعل من عملية التحقيق والملاحقة الجنائية في الجرائم الإلكترونية أمرًا معقدًا يتطلب تنسيقًا دقيقًا بين الجهات القانونية و الأجهزة الأمنية [2].

في هذا المطلب، سنتناول أبرز التحديات القانونية التي تواجه التحقيقات في الجرائم الإلكترونية في الجزائر، مع التركيز على صعوبة تطبيق القوانين الحالية في هذا المجال، بالإضافة إلى التحديات المتعلقة بـ الاختصاص القضائي، التعاون الدولي، و حقوق الأفراد في ظل هذه التحقيقات.

[1]– بلعزوز، فاطمة الزهراء. المرجع السابق ، ص. 125. .

[2]–.خليف، عبد الحميد. التحديات القانونية لمكافحة الجريمة الإلكترونية. مجلة دفاتر السياسة والقانون، جامعة ورقلة، العدد 29، 2021، ص. 89.

الفرع الأول: عدم وجود قوانين شاملة ومتجددة لمواكبة تطور الجرائم الإلكترونية

تعد الجرائم الإلكترونية من أسرع أنواع الجرائم تطورًا، نظراً لتسارع الابتكارات التكنولوجية وتغير الأساليب التي يستخدمها المجرمون في استغلال الثغرات الرقمية. وفي الجزائر، كما في العديد من الدول الأخرى، يعاني النظام القانوني من نقص في القوانين الشاملة والمتجددة التي تتمكن من مواكبة هذا التطور السريع في الجريمة الإلكترونية. هذا النقص في التشريعات المتخصصة يجعل التحقيقات في الجرائم الإلكترونية أكثر تعقيدًا ويقلل من قدرة النظام القضائي على ملاحقة الجناة بشكل فعال[1].

1 - تباين بين التشريعات القائمة وواقع الجرائم الإلكترونية الحديثة

على الرغم من وجود بعض القوانين الجزائية التي تتناول الجرائم الإلكترونية بشكل عام، إلا أن هذه القوانين لا توفر إطارًا قانونيًا شاملاً ومتكاملًا لمواجهة الجرائم الرقمية الحديثة. تقتصر بعض التشريعات الحالية على التعامل مع أنواع محددة من الجرائم مثل الاحتيال الإلكتروني أو التعدي على الملكية الفكرية، في حين أن التطورات السريعة في التكنولوجيا تتطلب قوانين أكثر مرونة و شمولًا [2].

تأخر في مواكبة تطور الجرائم: أساليب الجرائم الإلكترونية تتطور بشكل أسرع من قدرة النظام القضائي على تحديث القوانين. على سبيل المثال، الأساليب المتبعة في الهجمات السيبرانية مثل البرمجيات الخبيثة أو الهجمات المنسقة عبر الذكاء الاصطناعي تتطلب تشريعات خاصة لتمييزها عن الجرائم التقليدية.

[1]-.العربي نوال ،المواجهة القانونية للجرائم الإلكترونية في الجزائر. مجلة العلوم القانونية والسياسية، جامعة سطيف، العدد 23، 2020، ص. 101.

[2]- عبد اللاوي عبد العزيز ، الجرائم الإلكترونية والتحديات الأمنية. دار الخلدونية للنشر، الجزائر، 2019، ص. 147.

غياب قوانين خاصة لعدد من الجرائم: على الرغم من أن الجزائر بدأت في تبني بعض النصوص القانونية مثل قانون حماية البيانات الشخصية (2018) وغيره من القوانين ذات الصلة، إلا أن هناك غياباً ملحوظاً لقوانين مُحدثة بشكل دوري لمواكبة التكنولوجيا الحديثة[1].

2 – تحديات في تقنين الجريمة الإلكترونية في إطار قانوني

النقص في القوانين المتجددة يعكس تحديات كبيرة في تقنين الجرائم الإلكترونية، مثل:

أ – تحديد المسئولية: مع تزايد استخدام التقنيات المعقدة في الجرائم الإلكترونية، يصبح من الصعب تحديد المسؤولية الجنائية، خصوصًا في حالة الجرائم المرتكبة عبر الإنترنت مثل القرصنة أو الابتزاز الرقمي. من الصعب أحيانًا تحديد من هو المسؤول الفعلي إذا كانت الجريمة قد تمت عبر شبكات معقدة أو باستخدام هوية مزورة.

ب – عدم شمولية التشريعات: بعض الجرائم الإلكترونية قد تتداخل مع الجرائم التقليدية، مثل التزوير أو الاحتيال، مما يعقد التفسير الصحيح لهذه الجرائم في السياق الرقمي. كما أن القوانين الحالية لا تكفي لمكافحة الجرائم التي تحدث في بيئة الإنترنت، مثل التجارة الإلكترونية غير القانونية أو التسريب العمد للبيانات

3 – تعقيدات الجرائم العابرة للحدود

من أبرز التحديات التي يواجهها النظام القانوني الجزائري في مجال الجرائم الإلكترونية هو العالمية و العابرة للحدود لهذه الجرائم. إن القوانين الجزائرية، رغم تحسيناتها في السنوات الأخيرة، تظل محدودة التأثير في مواجهة الجرائم التي تحدث عبر شبكات الإنترنت العالمية. فالجريمة الإلكترونية يمكن أن تُرتكب في دولة بينما تُنفذ من قبل مجرم أو شبكة إجرامية في دولة أخرى، مما يعقد من عمليات التحقيق والملاحقة.

[1]– عبد اللاوي، عبد العزيز مرجع سابق ص. 150..

أ – **غياب التنسيق الدولي:** حتى مع توقيع الجزائر على بعض الاتفاقيات الدولية مثل اتفاقية بودابست المتعلقة بمكافحة الجريمة الإلكترونية، إلا أن التحديات القانونية الدولية ما زالت كبيرة. فالتنسيق بين الدول لتسليم المتهمين أو الاستفادة من الأدلة الرقمية قد يكون بطيئًا أو معقدًا بسبب اختلاف التشريعات و إجراءات التحقيق بين الدول[1].

ب – **عدم وجود قوانين مُحددة للجرائم العابرة للحدود:** في الجرائم الإلكترونية المعقدة مثل الهجمات المنسقة عبر الشبكة أو التجارة غير القانونية بالعملات الرقمية، تفتقر الجزائر إلى قانون شامل يحدد كيفية التعامل مع الجرائم التي تشمل عدة دول أو ولايات قضائية

4 – صعوبة تطبيق القوانين على الأدلة الرقمية

– التحدي الآخر المرتبط بعدم وجود قوانين شاملة ومتجددة هو مواكبة التغيرات في أساليب جمع الأدلة الرقمية.

– إذ أن الجرائم الإلكترونية غالبًا ما تترك آثارًا رقمية قد تكون موزعة عبر عدة أنظمة شبحية أو شبكات مشفرة، مما يتطلب قدرات قانونية فنية تتجاوز ما هو متاح في التشريعات الحالية.

أ – **صعوبة الوصول إلى الأدلة الرقمية:** بعض الجرائم الإلكترونية تتضمن استخدام تقنيات التشفير أو تقنيات إخفاء الهوية التي تجعل من جمع الأدلة صعبًا للغاية. وفي غياب قوانين واضحة و أدوات قانونية محدثة، يصبح التعامل مع هذه الأدلة أمرًا محيرًا للمحققين.

ب –**الحاجة إلى قوانين تنظيم الوصول للبيانات:** من أجل التحقيق بشكل فعال في الجرائم الإلكترونية، هناك حاجة إلى قوانين واضحة تنظّم كيفية الوصول إلى بيانات المستخدمين، خاصةً في حالة ارتكاب الجريمة عبر منصات الإنترنت أو الخدمات السحابية.

[1]–.العربي، نوال. مرجع نفسه ، ص. 105..

5 - الحاجة إلى تحديث مستمر للقوانين

من الأهمية بمكان أن تقوم الجزائر بتطوير إطار قانوني متكامل يتضمن قوانين خاصة للتعامل مع الجرائم الإلكترونية، مع تحديث هذه القوانين بشكل دوري لمواكبة التقنيات المتغيرة وأساليب الجرائم الحديثة. بالإضافة إلى ذلك، من الضروري تبني منهج تشريعي مرن يتيح تعديل القوانين بسرعة استجابة لتطورات التكنولوجيا و التهديدات الرقمية.

إن غياب القوانين الشاملة والمتجددة لمواكبة تطور الجرائم الإلكترونية في الجزائر يمثل إحدى أبرز العقبات التي تواجه التحقيقات في هذا المجال. تحتاج الجزائر إلى تحديث مستمر للتشريعات لتتمكن من التصدي بفعالية لهذه الجرائم المعقدة والمتطورة. كما يتطلب الأمر تطوير قوانين مرنة تتلاءم مع التطور السريع للتكنولوجيا الرقمية، وكذلك تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية العابرة للحدود.

الفرع الثاني: ضعف التنسيق بين الأجهزة القضائية والأمنية في تحقيقات الجرائم الإلكترونية

تعتبر الجرائم الإلكترونية من الأنواع المعقدة التي تتطلب تعاونًا فعالًا بين الأجهزة القضائية و الأجهزة الأمنية من أجل التحقيق فيها بشكل صحيح وملاحقة مرتكبيها. في الجزائر، على الرغم من وجود بعض المبادرات والتطورات في مجال مكافحة هذه الجرائم، إلا أن هناك ضعفًا ملحوظًا في التنسيق بين الأجهزة المعنية، مما يؤثر سلبًا على فعالية التحقيقات وتقديم الجناة إلى العدالة. [1].

1 - طبيعة الجرائم الإلكترونية وتعقيدها

الجرائم الإلكترونية لا تتسم بالوضوح أو التقليدية التي يمكن أن يواجهها المحققون في الجرائم التقليدية. تتطلب هذه الجرائم فهمًا عميقًا للأدوات التقنية المستخدمة مثل البرمجيات الضارة، التشفير، التقنيات المتقدمة في اختراق الأنظمة والشبكات. لهذا السبب، يحتاج التحقيق

[1]- خليفعبد الحميد، المرجع السابق ، ص. 91.

في هذه الجرائم إلى تعاون وثيق بين الأجهزة القضائية و الأمنية، حيث يتطلب التحقيق المهارات الفنية والتقنية من جانب الأجهزة الأمنية، بينما تتطلب الملاحقة القانونية والخطوات الإجرائية الفعالة من جانب الأجهزة القضائية[1].

2 – غياب التنسيق المؤسسي الفعّال

أ – التنظيم الداخلي للمؤسسات:

يعاني النظام القضائي والأمني في الجزائر من غياب التنسيق المؤسسي الفعّال بين الجهات المعنية بالتحقيق في الجرائم الإلكترونية. على سبيل المثال، تتعامل الشرطة التقنية مع جمع الأدلة الرقمية و التحقيقات الأولية، بينما تقوم الجهات القضائية مثل النيابة العامة والمحاكم بالتعامل مع القضايا القانونية وإجراءات المحاكمة. في كثير من الأحيان، لا يكون هناك تعاون منتظم أو تبادل فعّال للمعلومات بين هذه الأجهزة، مما يؤدي إلى تباطؤ في التحقيقات وتداخل في المسؤوليات.

ب – الاختصاصات المتداخلة:

تختلف اختصاصات الأجهزة الأمنية عن اختصاصات الأجهزة القضائية، مما يخلق بعض التحديات في التنسيق الفعّال. على سبيل المثال، قد تتطلب التحقيقات في الجرائم الإلكترونية الحصول على إذن قضائي للوصول إلى البيانات الرقمية المخزنة على الإنترنت أو في أجهزة الكمبيوتر، بينما تكون الأجهزة الأمنية قد بدأت بالفعل في جمع الأدلة بشكل استباقي، مما يؤدي إلى تأخير في الإجراءات [2].

3 – نقص الخبرات الفنية في الأجهزة القضائية

من بين أكبر التحديات التي تعيق التنسيق بين الأجهزة القضائية والأمنية في الجزائر هو نقص الخبرات الفنية في الأجهزة القضائية. التحقيقات في الجرائم الإلكترونية تتطلب خبرات

[1]– شراد سميرة ، التحقيق في الجرائم الإلكترونية في الجزائر. مجلة الحقوق والعلوم السياسية، جامعة تبسة، العدد 15، 2022، ص. 180.

[2]– خليف، عبد الحميد مرجع ساق ص 94

خاصة في التحليل الجنائي الرقمي وفهم كيفية جمع الأدلة الرقمية وتحليلها، وهو ما قد يكون غير متاح بكفاءة داخل الأجهزة القضائية، مما يؤدي إلى صعوبة في تقييم الأدلة الرقمية [1].

رغم أن بعض الجهات الأمنية، مثل الشرطة القضائية أو الشرطة التقنية، تتمتع بخبرات متخصصة في هذا المجال، فإن الأجهزة القضائية قد تفتقر إلى التدريب الكافي على كيفية التعامل مع الأدلة الرقمية أو فهم أساليب التحقيق الإلكتروني. هذا يؤدي إلى أخطاء إجرائية قد تؤثر في سير التحقيقات الجنائية وتقديم القضايا إلى المحاكم.

4 – عدم وجود آليات تنسيق ثابتة بين الجهات المعنية

التحقيقات في الجرائم الإلكترونية تتطلب تنسيقًا مستمرًا و تعاونًا متينًا بين الشرطة، القضاء، و الهيئات المختصة مثل المؤسسات التي تدير البنية التحتية للإنترنت. في الجزائر، لا توجد آليات مؤسسية ثابتة لضمان هذا التنسيق. قد يكون التنسيق في بعض الحالات عشوائيًا أو مؤقتًا، ويعتمد على تفاعلات فردية بين أفراد الأجهزة الأمنية والقضائية، مما يؤدي إلى ضعف التنسيق العام.

أ – التأخير في تبادل المعلومات: بسبب عدم وجود أنظمة أو آليات ثابتة لتبادل المعلومات بشكل دوري بين هذه الأجهزة، يحدث أحيانًا تأخير في الحصول على المعلومات اللازمة أو إهمال للأدلة، مما يضعف التحقيقات.

ب – غياب التنسيق بين القطاعات المتخصصة:

يُفترض أن يكون هناك تنسيق بين القطاعات المتخصصة في الجرائم الإلكترونية مثل الأمن الوطني و النيابة العامة و المحاكم، لكن هذا التنسيق قد يكون غير كافٍ، مما يعيق العمل المشترك بين الجهات المختلفة.

[1]– بلعزوز، فاطمة الزهراء .*الجرائم الإلكترونية في القانون الجزائري* .مجلة الدراسات القانونية والسياسية، جامعة محمد خيضر بسكرة، العدد 17، 2020، ص. 128.

5 – الصعوبات القانونية والإجرائية في التنسيق

أ – الاختصاص القضائي:

في حالة الجرائم الإلكترونية العابرة للحدود، قد يواجه المحققون صعوبة في تحديد الاختصاص القضائي المناسب لإجراء التحقيقات. قد تكون الجريمة قد تم تنفيذها عبر الإنترنت من دولة أخرى، مما يخلق إشكالات قانونية بشأن من له الحق في التحقيق أو اتخاذ الإجراءات القانونية [1].

ب –القوانين المتفاوتة:

في حال كانت الجرائم الإلكترونية مرتبطة بجرائم دولية أو جرائم عبر الحدود، قد يصطدم التنسيق بين الأجهزة القضائية في الجزائر مع القوانين المختلفة في دول أخرى، مما يجعل التعاون أكثر صعوبة.

6 – التحديات المتعلقة بالتكنولوجيا والمعدات

حتى إذا كان التنسيق قائمًا بين الأجهزة القضائية والأمنية، فإن غياب المعدات والتكنولوجيا المتطورة في بعض الأحيان قد يعوق التحقيقات. على سبيل المثال، في حال تعرضت أجهزة الكمبيوتر أو الهواتف الذكية للاختراق، يحتاج المحققون إلى أدوات تحليل رقمي متقدمة لفحص الأدلة، وهو ما قد لا يتوافر في بعض الأحيان.

ضعف التنسيق بين الأجهزة القضائية والأمنية في الجزائر يعد من أبرز التحديات التي تؤثر على فعالية التحقيقات في الجرائم الإلكترونية. التغلب على هذا التحدي يتطلب تعزيز التعاون المؤسسي و تنظيم التنسيق بين الأجهزة، بالإضافة إلى تدريب المتخصصين في مجال التحقيقات الرقمية داخل الأجهزة القضائية والأمنية. ينبغي أيضًا تطوير آليات فعالة لتبادل المعلومات بشكل سريع وآمن بين هذه الأجهزة، مما سيؤدي إلى تحقيقات أكثر كفاءة و قدرة أعلى على مواجهة الجرائم الإلكترونية.

[1]– العربي، نوال .*المواجهة القانونية للجرائم الإلكترونية في الجزائر* .مجلة العلوم القانونية والسياسية، جامعة سطيف، العدد 23، 2020، ص. 103.

المطلب الثاني: التحديات التقنية في التحقيقات للجرائم الإلكترونية في الجزائر

تواجه التحقيقات في الجرائم الإلكترونية في الجزائر العديد من التحديات التقنية التي تعيق قدرة الأجهزة الأمنية والقضائية على إجراء تحقيقات فعالة وملاحقة الجناة بشكل دقيق. ويعزى ذلك إلى تطور التكنولوجيا بشكل سريع، مما يخلق تحديات معقدة في مواكبة هذه التطورات من خلال تحديث الأدوات والتقنيات المستخدمة في التحقيقات، بالإضافة إلى نقص الخبرات و الموارد التقنية المتخصصة. هذه التحديات تتطلب استجابة سريعة ومتكاملة من جميع الجهات المعنية بمكافحة الجرائم الإلكترونية [1].

الفرع الأول: صعوبة جمع الأدلة الرقمية ومواجهتها الجرائم الإلكترونية في الجزائر

تعد الأدلة الرقمية أحد العناصر الأساسية في التحقيقات الخاصة بالجرائم الإلكترونية. إلا أن جمع هذه الأدلة في الجزائر، كما في العديد من الدول الأخرى، يواجه العديد من التحديات التقنية و القانونية التي تعرقل سير التحقيقات، مما يزيد من تعقيد مواجهة الجرائم الإلكترونية.

1 – تعقيد الأدلة الرقمية وحجمها الكبير

تتميز الأدلة الرقمية بأنها تكون غالبًا مخزنة في شكل غير مرئي وتحتوي على كمية ضخمة من المعلومات التي يصعب الوصول إليها أو تحليلها بسرعة. ومع تزايد حجم البيانات التي يتم تداولها على الإنترنت، يصبح من الصعب جمع الأدلة وتحليلها بفعالية في الوقت المناسب.

أ – **البيانات المخبأة:** في الكثير من الحالات، يقوم المجرمون بإخفاء الأدلة الرقمية في أنظمة معقدة أو يقومون بتخزينها في أماكن متعددة (مثل السحابة الإلكترونية أو الخوادم الأجنبية).

[1]– خليف، عبد الحميد .*المرجع السابق* ، ص. 93.

في بعض الأحيان، تكون الأدلة متشابكة مع كميات ضخمة من البيانات غير ذات الصلة، مما يتطلب تقنيات متقدمة في الفحص والتحليل.

ب – تنوع وتعدد المصادر: قد تكون الأدلة الرقمية مخزنة على أجهزة مختلفة (مثل الحواسيب، الهواتف الذكية، الخوادم، أو الشبكات الاجتماعية) مما يجعل من الصعب توحيد أساليب جمع الأدلة. وهذا يفرض تحديات كبيرة في التنسيق بين الأجهزة المختلفة. [1].

2 – صعوبة الوصول إلى البيانات المخزنة عبر الحدود

من أبرز المشاكل التي تواجه التحقيقات في الجرائم الإلكترونية في الجزائر هو الوصول إلى الأدلة المخزنة على خوادم تقع خارج حدود البلاد.

أ –**مخاوف الخصوصية:** تخضع الكثير من الشركات العالمية التي تقدم خدمات الإنترنت مثل جوجل و فيسبوك إلى قوانين الخصوصية في دول أخرى، مثل قوانين حماية البيانات في الاتحاد الأوروبي (GDPR). نتيجة لذلك، قد ترفض هذه الشركات تسليم الأدلة للسلطات الجزائرية دون موافقة قانونية دولية أو طلب مساعدة قانونية متبادل.

ب – طلبات المساعدة القانونية المتبادلة: للوصول إلى البيانات المخزنة في دول أخرى، يجب على السلطات الجزائرية اتباع إجراءات قانونية معقدة، مثل تقديم طلبات المساعدة القانونية المتبادلة، التي قد تأخذ وقتًا طويلاً وتحتاج إلى اتفاقيات دولية مع الدول التي تحتوي على هذه البيانات. هذه العمليات قد تؤدي إلى تأخير التحقيقات بشكل كبير [2].

[1]– بن موسى، نادية. الجرائم الإلكترونية: الواقع والتحديات في الجزائر. مجلة الدراسات القانونية، جامعة الجزائر، العدد 12، 2022. ص83.

[2]– زروقي عبد القادر ، التحقيق الجنائي في الجرائم الإلكترونية. دار هومة، الجزائر، 2021. ص 125.

3 - تعقيدات التشفير واستخدام تقنيات إخفاء الهوية

التشفير هو أحد الوسائل التي يعتمد عليها المجرمون الإلكترونيون لإخفاء بياناتهم و حمايتها من التتبع، ويعتبر أحد أبرز التحديات في جمع الأدلة الرقمية.

أ - **التشفير المتقدم:** في بعض الحالات، يعتمد المجرمون على تقنيات تشفير معقدة مثل التشفير من النهاية إلى النهاية (end-to-end encryption)، مما يجعل من المستحيل على السلطات الجزائرية الوصول إلى محتوى الرسائل أو الملفات المخزنة على الأجهزة أو الخوادم، حتى إذا تم القبض على الجاني[1]..

ب -**استخدام شبكات مجهولة الهوية:** يستخدم المجرمون أدوات مثل شبكة تور أو VPN لإخفاء مواقعهم الحقيقية وتضليل السلطات. هذه الأدوات تجعل من الصعب تتبع عنوان IP أو تحديد الموقع الجغرافي للمهاجمين، مما يزيد من صعوبة التحقيق في الجرائم الإلكترونية.

4 - نقص الأدوات التقنية المتخصصة لتحليل الأدلة الرقمية

إن تحليل الأدلة الرقمية يتطلب أدوات تقنية متخصصة، مثل برامج تحليل الأجهزة الرقمية أو أدوات فك التشفير. ومع ذلك، تواجه الأجهزة الأمنية الجزائرية نقصًا في هذه الأدوات المتقدمة:

أ - **عدم توفر البرمجيات الحديثة:** رغم أن هناك بعض البرامج المتوفرة لفحص الأجهزة الرقمية مثل أدوات تحليل القرص الصلب و فحص البرمجيات الخبيثة، إلا أن الأدوات المحلية قد لا تكون كافية لمواكبة تقنيات التشفير والهجمات المتطورة التي يستخدمها المجرمون.

ب - **إجراءات الفحص المعقدة:** تتطلب عملية فحص الأدلة الرقمية تقنيات متطورة لتحليل بيانات معقدة مثل الملفات المخبأة أو الرسائل المشفرة. عدم وجود الأدوات اللازمة يجعل من

[1] -Bouzida, Y. (2020). Cybercrime and digital investigation challenges in Algeria. International Journal of Cyber Criminology, Vol. 14(1), pp. 102-115.

المستحيل على المحققين فحص الأدلة بشكل دقيق وفعال، مما يعوق قدرة الأجهزة الأمنية الجزائرية على ملاحقة المجرمين [1].

5 – عدم وجود معايير قانونية موحدة لجمع الأدلة الرقمية

يعتبر إجراء جمع الأدلة الرقمية من العمليات القانونية التي تحتاج إلى أن تكون موثقة بشكل سليم، وفقًا للمعايير القانونية المحلية والدولية.

أ – **الضوابط القانونية المحدودة:** في الجزائر، قد تكون هناك ثغرات قانونية فيما يتعلق بكيفية جمع الأدلة الرقمية، وكيفية الاحتفاظ بها وحمايتها من التلاعب أو التدمير. هذا يمكن أن يؤدي إلى إلغاء الأدلة أو إبطال التحقيقات إذا لم يتم التعامل معها بالشكل الصحيح.

ب – **التحديات المتعلقة بالخصوصية:** جمع الأدلة الرقمية قد يثير قضايا الخصوصية، خاصة إذا تم الوصول إلى البيانات الشخصية لأفراد أو شركات دون مراعاة القوانين المتعلقة بحماية البيانات. وهذا يتطلب توازنًا دقيقًا بين ضرورة التحقيق في الجرائم الإلكترونية وحماية الحقوق الفردية.

6 – الحاجة إلى التعاون الدولي في جمع الأدلة

التعاون مع دول أخرى: نظرًا للطبيعة العابرة للحدود للجرائم الإلكترونية، غالبًا ما يتعين على الجزائر التعاون مع دول أخرى للوصول إلى الأدلة الرقمية. هذا التعاون يحتاج إلى اتفاقيات دولية و طلبات مساعدة قانونية يمكن أن تأخذ وقتًا طويلًا وقد تلاقي صعوبة في تنفيذها بسبب الفوارق في الأنظمة القانونية بين الدول.

إن جمع الأدلة الرقمية في الجرائم الإلكترونية في الجزائر يمثل تحديًا كبيرًا بسبب التعقيد التكنولوجي و القيود القانونية. التشفير و تقنيات إخفاء الهوية تجعل من الصعب تتبع المجرمين

[1]– زروقي، عبد القادر المرجع سابق ص 130...

وجمع الأدلة اللازمة لتوجيه التهم لهم. كما أن نقص الأدوات التقنية المتخصصة و البيانات المخزنة في الخارج يزيد من تعقيد هذه العمليات. للتغلب على هذه الصعوبات، يجب على الجزائر تعزيز التعاون الدولي وتطوير البنية التحتية التقنية، بالإضافة إلى تحديث الإجراءات القانونية الخاصة بجمع الأدلة الرقمية بشكل يتماشى مع التحديات الحديثة.

الفرع الثاني: تطور التقنيات التي يستخدمها المجرمون (مثل استخدام الشبكات المجهولة)

تطورت الجرائم الإلكترونية بشكل كبير في السنوات الأخيرة نتيجة لتقدم التقنيات الحديثة. يستخدم المجرمون مجموعة متنوعة من الأدوات والتقنيات المتطورة التي تساعدهم على إخفاء هويتهم وأماكنهم، مما يجعل من الصعب على السلطات القضائية والأمنية تحديد المجرم أو حتى ملاحقته. من أبرز هذه التقنيات استخدام الشبكات المجهولة مثل شبكة تور (Tor) و الشبكات الافتراضية الخاصة (VPN)، بالإضافة إلى تقنيات أخرى مثل التشفير و الأنظمة الموزعة. هذه الأدوات تجعل التحقيقات في الجرائم الإلكترونية أكثر تعقيدًا وتشكل تحديات كبيرة للأجهزة الأمنية والقضائية [1].

1 – استخدام شبكة تور (Tor)

شبكة تور هي شبكة مجهولة الهوية عبر الإنترنت، توفر للمستخدمين إخفاء هويتهم من خلال توجيه الاتصال عبر عدة طبقات من الأنفاق المجهولة (onion routing). تعتمد على توزيع البيانات عبر عدة خوادم حول العالم لتقليل احتمال تتبع المستخدمين.

أ – **إخفاء الهوية:** من خلال استخدام شبكة تور، يتمكن المجرمون من إخفاء عنوان IP الخاص بهم، مما يجعل من الصعب تحديد موقعهم الجغرافي أو هوية المتورطين في الأنشطة

[1]– بردال سمير،"الجريمة المعلوماتية في التشريع الجزائري." مجلة القانون، المجلد 1، العدد 2، 2010، ص ص. 177–195.

الإجرامية. تُستخدم شبكة تور بشكل واسع في الأنشطة غير القانونية مثل القرصنة، الاحتيال، البيع غير المشروع للبيانات، و الاتجار في المخدرات.

ب – الدخول إلى الشبكات المظلمة (Dark Web): غالبًا ما يستخدم المجرمون شبكة تور للوصول إلى الشبكة المظلمة (Dark Web)، التي تحتوي على العديد من المواقع التي تروج للأنشطة الإجرامية.

من هنا يمكنهم إجراء صفقات غير قانونية أو تبادل معلومات مسروقة بعيدًا عن أعين السلطات.

ج – التحدي الأمني: استخدام تور يعقد عملية التحقيقات في الجرائم الإلكترونية بشكل كبير، حيث يصعب على المحققين تتبع المهاجمين أو تحديد الجهة المتورطة. كما أن الأفراد الذين يشتبه بهم قد يكونون على دراية بكيفية إخفاء أنشطتهم باستخدام هذه الشبكة.

2 – الشبكات الافتراضية الخاصة (VPN)

الشبكات الافتراضية الخاصة (VPN) هي أداة تتيح للمستخدمين إنشاء اتصال آمن ومشفر بين جهاز الكمبيوتر الخاص بهم والشبكة عبر الإنترنت، مما يجعل من الصعب تتبع النشاطات التي يقومون بها أو معرفة موقعهم الجغرافي الحقيقي [1].

أ – إخفاء الهوية: باستخدام VPN، يمكن للمجرمين تغيير عنوان IP الخاص بهم واستخدام عنوان IP وهمي من دولة أخرى، مما يجعل من الصعب على السلطات تحديد الموقع الجغرافي للمهاجم. قد يستفيد المجرمون من ذلك أثناء تنفيذ هجمات مثل الاحتيال عبر الإنترنت، الهجمات الموزعة، أو اختراق الأنظمة.

[1]– بردال سمير، المرجع السابق، ص 195.

ب – التشفير العالي: توفر الشبكات الافتراضية الخاصة تشفيرًا عاليًا للبيانات المرسلة، مما يجعل من الصعب اعتراض الرسائل أو مراقبة الأنشطة عبر الإنترنت. وبالتالي، يتمكن المجرمون من تنفيذ أنشطتهم الإجرامية دون أن يتمكن المحققون من الوصول إلى الأدلة.

ج – التحديات الأمنية: يستخدم المجرمون VPNs متعددة لجعل تتبعهم أكثر صعوبة، مما يعقد عملية التحقيق. علاوة على ذلك، فإن العديد من مزودي خدمة VPN لا يحتفظون بسجلات الاستخدام (no logs policy)، مما يعزز صعوبة تحديد النشاطات المشبوهة أو مراقبة حركة مرور الإنترنت.

3 – التشفير المتقدم

تعتبر تقنيات التشفير المتقدم أحد الأدوات الرئيسية التي يستخدمها المجرمون الإلكترونيون لإخفاء هويتهم وبياناتهم. يشمل التشفير جميع البيانات المرسلة عبر الإنترنت، مما يحولها إلى رموز غير قابلة للفهم ما لم يتم فك تشفيرها باستخدام مفتاح سري.

أ – التشفير من النهاية إلى النهاية: يُستخدم بشكل شائع في تطبيقات مثل واتساب و تلغرام، حيث يتم تشفير الرسائل بين المستخدمين بحيث لا يمكن لأحد خارج المحادثة فك تشفير الرسائل سوى الأطراف المرسلة والمستقبلة. في حال استخدم المجرمون هذه التقنية، يصبح من الصعب على السلطات فك تشفير المحتوى واستخلاص الأدلة [1].

ب – البرمجيات الخبيثة المشفرة: يطور بعض المجرمين برمجيات خبيثة، مثل الفيروسات و برمجيات الفدية، التي تقوم بتشفير الملفات على أجهزة الضحايا، مما يجعل من المستحيل الوصول إليها دون فك التشفير باستخدام مفتاح معين. إذا لم تتمكن السلطات من الحصول على هذا المفتاح، تظل البيانات غير قابلة للوصول، مما يؤثر سلبًا على التحقيقات.

[1]– بردال، سمير .مرجع سابق ص199.

4 – الأنظمة الموزعة والهجمات المجهولة

يستخدم المجرمون أحيانًا الأنظمة الموزعة (Distributed Systems) في هجمات إلكترونية مثل هجمات الحرمان من الخدمة (DDoS). تعتمد هذه الهجمات على استخدام شبكات ضخمة من الأجهزة الملوثة (عادة ما تكون أجهزة الكمبيوتر التي تم اختراقها والتحكم فيها، والمعروفة باسم "الزومبي") لشن هجوم على المواقع الإلكترونية أو الأنظمة.

أ – **هجمات DDoS:** الهجوم يتم عبر إغراق الموقع أو الخادم المستهدف بحجم هائل من البيانات أو الطلبات، مما يؤدي إلى تعطيل الخادم. هذه الأنواع من الهجمات قد تكون موجهة إلى مؤسسات مالية أو حكومية أو شركات خاصة. المهاجمون لا يتطلبون الوصول المباشر إلى الخوادم المستهدفة، بل يستخدمون شبكة ضخمة من الأجهزة المخترقة حول العالم، مما يجعل من الصعب تحديد الجهة المسؤولة.

ب – **صعوبة تتبع المهاجمين:** نظرًا لاستخدام الأنظمة الموزعة، يصعب على المحققين تحديد مصدر الهجوم بدقة. إن الأجهزة المهاجمة يمكن أن تكون منتشرة في مناطق متعددة، مما يعقد عملية التتبع والتحقيق. [1]

5 – الابتزاز الرقمي باستخدام التقنيات المجهولة

يستخدم المجرمون تقنيات مختلفة لابتزاز الضحايا عبر الإنترنت، مثل التهديد بنشر البيانات الحساسة أو الإضرار بالسمعة الإلكترونية. في بعض الأحيان، يعتمد المهاجمون على تقنيات التشفير و الشبكات المجهولة لإخفاء هويتهم والضغط على الضحية لدفع الأموال أو تلبية المطالب.

[1]– خيدل أحمد، وكيسي، زهيرة جيلالي عبدالقادر. "إجراءات جمع الأدلة الرقمية طبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات". مجلة الاجتهاد للدراسات القانونية والاقتصادية، 2022 ص36.

يستخدم بعض المجرمين أسلوب فيروسات الفدية التي تقوم بتشفير ملفات الضحية والمطالبة بفدية مقابل فك التشفير. في هذه الحالات، يتم الدفع باستخدام العملات الرقمية مثل البيتكوين التي يتم إرسالها عبر شبكات مجهولة مثل شبكة تور، مما يجعل من الصعب تحديد المجرم.

التطور المستمر في التقنيات التي يستخدمها المجرمون يشكل تحديًا كبيرًا أمام الأجهزة الأمنية والقضائية في الجزائر. الشبكات المجهولة مثل تور و VPN، التشفير المتقدم، و الأنظمة الموزعة تستخدم بشكل متزايد لإخفاء هوية المهاجمين وتضليل التحقيقات. لمواجهة هذه التحديات، يجب على السلطات الجزائرية تطوير القدرات التقنية والتعاون مع الشركاء الدوليين من أجل محاربة الجرائم الإلكترونية وتحقيق النجاح في التحقيقات.

الفرع الثالث: نقص الأدوات التقنية اللازمة لتحليل الأدلة الرقمية بشكل فعال

تعتبر الأدلة الرقمية من العناصر الأساسية في التحقيقات الخاصة بالجرائم الإلكترونية، حيث تُستخدم كدليل رئيسي للكشف عن الأنشطة الإجرامية وتحقيق العدالة.

ولكن، تعاني العديد من الدول، بما في ذلك الجزائر، من نقص الأدوات التقنية المتخصصة التي تمكن المحققين من تحليل الأدلة الرقمية بشكل دقيق وفعال. يعرقل هذا النقص سير التحقيقات في الجرائم الإلكترونية، ويجعل من الصعب معالجة القضايا القانونية المتعلقة بالتكنولوجيا الحديثة [1].

[1]– لحارثي منصور فهيد سعيد ، "معوقات إثبات الجرائم المتعلقة بتقنية المعلومات." المجلة القانونية، المجلد 15، العدد 4، فبراير 2023، ص. 1051-1090.

1 - أنواع الأدوات التقنية المتخصصة في تحليل الأدلة الرقمية

قبل التطرق إلى نقص الأدوات التقنية، من المهم أولاً فهم الأدوات التي يعتمد عليها المحققون في مجال الجرائم الإلكترونية لتحليل الأدلة الرقمية، وهذه الأدوات يمكن أن تكون متعددة ومتخصصة وفقًا لطبيعة الجريمة:

أ - أدوات تحليل الأقراص الصلبة (Hard Drive Analysis Tools):

هذه الأدوات تُستخدم لفحص الأجهزة التخزينية مثل الأقراص الصلبة والأقراص الخارجية أو أجهزة الذاكرة، وذلك لاستخراج البيانات المخزنة مثل الملفات المحذوفة أو الملفات المشفرة.

ب - أدوات تحليل الشبكة (Network Analysis Tools):

تستخدم هذه الأدوات لمراقبة وتحليل حركة البيانات عبر الشبكات الرقمية (مثل الإنترنت أو الشبكات الداخلية)، وتساعد في اكتشاف الأنشطة المشتبه فيها مثل الاختراقات أو الهجمات الإلكترونية.

ج - أدوات تحليل البريد الإلكتروني (Email Analysis Tools):

تُستخدم لفحص الرسائل الإلكترونية واستخراج الأدلة من حسابات البريد الإلكتروني التي قد تكون تعرضت للاختراق أو استخدمت في الاحتيال الإلكتروني أو التصيد الاحتيالي.

د - أدوات تحليل الأنظمة (System Analysis Tools):

تشمل هذه الأدوات فحص الأجهزة والأنظمة لمعرفة وجود برمجيات خبيثة (Malware) أو تتبع سجلات الأنظمة التي قد تحتوي على دليل إجرامي مثل عمليات الولوج المشبوهة [1].

[1]- لحارثي، منصور فهيد سعيد ، المرجع السابق ، ص 10555.

2 – أسباب نقص الأدوات التقنية اللازمة في الجزائر

على الرغم من الحاجة المتزايدة لهذه الأدوات المتخصصة في التحقيقات الجنائية الإلكترونية، تواجه الجزائر تحديات كبيرة في تزويد الأجهزة الأمنية و القضائية بالأدوات التقنية اللازمة لتحليل الأدلة الرقمية. ومن أبرز هذه الأسباب[1]:

أ – تكلفة الأدوات التقنية المتقدمة

إن الأدوات التقنية اللازمة لتحليل الأدلة الرقمية تتطلب تكاليف عالية، بما في ذلك تكاليف شراء البرامج المتخصصة، الدورات التدريبية، و التحديثات المستمرة لهذه الأدوات لمواكبة أحدث التطورات في تكنولوجيا الجرائم الإلكترونية.

ب – صعوبة الحصول على الأدوات الأصلية: كثير من الأدوات المتخصصة في تحليل الأدلة الرقمية تكون محمية بحقوق الملكية، مما يزيد من صعوبة الحصول عليها أو حتى ترخيص استخدامها في البلاد.

ج – الميزانيات المحدودة: تواجه الجزائر، مثل العديد من الدول الأخرى، تحديات مالية قد تؤثر على قدرتها على تخصيص ميزانيات كافية لشراء الأدوات المتقدمة وتوفير الدعم الفني المستمر للمحققين.

د – نقص التدريب والخبرة في استخدام الأدوات التقنية

من أكبر التحديات التي تواجه المحققين في الجزائر هو نقص التدريب في استخدام الأدوات التقنية المتقدمة لتحليل الأدلة الرقمية. تعتمد فاعلية الأدوات التقنية على مهارة المحققين في تشغيل و تفسير نتائج الأدلة المستخلصة.

[1]– لحارثي منصور فهيد سعيد ، المرجع السابق ، ص 10556

هـ – قلة الخبرات المحلية: قلة المحققين المتخصصين في تحليل الأدلة الرقمية يؤدي إلى تراجع فعالية التحقيقات. يتطلب العمل مع الأدوات التقنية المتقدمة دراسات متخصصة، ومع مرور الوقت يمكن أن تصبح الأدوات غير مجدية إذا لم يتم تحديث مهارات المستخدمين.

و – التدريب المستمر: بسبب السرعة الكبيرة في تطور الأدوات والتقنيات المستخدمة في الجرائم الإلكترونية، يواجه المحققون في الجزائر صعوبة في مواكبة هذا التقدم بدون برامج تدريب مستمرة لتعلم كيفية استخدام الأدوات الحديثة بشكل صحيح.

3 – نقص التعاون مع الشركات التقنية العالمية

في بعض الحالات، قد يكون من الصعب على السلطات الجزائرية الحصول على الدعم الفني من الشركات التقنية العالمية التي تطور أدوات تحليل الأدلة الرقمية [1].

أ – القيود القانونية: بعض الشركات الكبرى، مثل جوجل و مايكروسوفت، قد لا تكون مستعدة للمشاركة في التعاون المباشر مع السلطات الجزائرية بسبب القيود القانونية الخاصة بحماية الخصوصية أو بسبب مخاوف تتعلق بالأمن السيبراني.

ب – العزلة التقنية: قد يكون هناك نقص في التعاون الدولي مع السلطات الجزائرية في مجال الجرائم الإلكترونية، مما يعيق قدرة المحققين على الوصول إلى الدعم الفني المتخصص أو الأدوات الحديثة.

4 – تأثير نقص الأدوات التقنية على التحقيقات الجنائية

إن نقص الأدوات التقنية المتخصصة في تحليل الأدلة الرقمية يؤدي إلى عدة تأثيرات سلبية على التحقيقات الجنائية في الجزائر، من أبرزها:

[1]– بوخاري أحمد ، "الجريمة الإلكترونية في ضوء التشريع الجزائري." مجلة دفاتر السياسة والقانون، جامعة خنشلة، العدد 20، 2018، ص. 289

أ – تأخير التحقيقات

من دون الأدوات المناسبة، قد يتعرض التحقيقات في الجرائم الإلكترونية لتأخير كبير. حيث قد يكون من الصعب استخراج الأدلة الضرورية أو حتى تحديد موقع الجريمة أو تحديد الجاني.

تحليل البيانات قد يستغرق وقتًا أطول من المعتاد، مما يؤدي إلى تأخير الإجراءات القضائية و إغلاق القضايا لفترة طويلة..

ب – زيادة صعوبة التتبع والإثبات

إن تحديد الأدلة في الجرائم الإلكترونية يتطلب تقنيات متقدمة للتمكن من فحص الأجهزة واستخراج المعلومات المخفية أو المشفرة.

من دون أدوات متخصصة، قد يكون من الصعب فك تشفير المعلومات أو حتى التوصل إلى أدلة حاسمة تثبت تورط المجرم في الجريمة.

ج – ضعف قدرات الردع والعقاب

من خلال نقص الأدوات المتخصصة، يكون الردع ضد الجرائم الإلكترونية ضعيفًا. إذا كانت السلطات غير قادرة على تحليل الأدلة الرقمية بشكل فعال، فإن المجرمين قد يشعرون بأنهم في مأمن من العقاب، مما يؤدي إلى زيادة النشاطات الإجرامية عبر الإنترنت [1].

[1]– الحارثي، منصور. "معوقات إثبات الجرائم المتعلقة بتقنية المعلومات." المجلة القانونية، المجلد 15، العدد 4، 2023، ص. 1070.

5 – الحلول المحتملة لتحسين القدرة على تحليل الأدلة الرقمية

لحل مشكلة نقص الأدوات التقنية في الجزائر، هناك عدة حلول يمكن أن تساهم في تحسين قدرة المحققين على تحليل الأدلة الرقمية بشكل فعال[1]:

أ – الاستثمار في شراء الأدوات التقنية الحديثة

يجب على الجزائر تخصيص ميزانية أكبر لشراء الأدوات التقنية المتخصصة التي تدعم التحقيقات في الجرائم الإلكترونية. كما يمكن البحث عن شراكات مع شركات التكنولوجيا العالمية لتوفير هذه الأدوات.

ب – التدريب المتخصص للمحققين

يجب توفير برامج تدريبية متخصصة لضمان أن المحققين يتمتعون بالمعرفة والمهارات اللازمة لاستخدام الأدوات المتطورة. هذه التدريبات يجب أن تكون مستمرة لمواكبة التغيرات في تكنولوجيا الجرائم الإلكترونية.

ج – تعزيز التعاون الدولي

يمكن للجزائر تعزيز التعاون مع الدول والمنظمات الدولية لمشاركة الموارد والأدوات التقنية، والتواصل مع الشركات التقنية العالمية لتقديم الدعم الفني في التحقيقات الجنائية المتعلقة بالجرائم الإلكترونية.

يعد نقص الأدوات التقنية من أكبر التحديات التي تواجه التحقيقات في الجرائم الإلكترونية في الجزائر. من أجل تحسين فاعلية هذه التحقيقات، يجب على الجزائر استثمار

[1]– زايدي، فوزية. "مكافحة الجريمة الإلكترونية في الجزائر: التحديات والآفاق." مجلة البحوث القانونية والسياسية، جامعة تبسة، العدد 7، 2016، ص. 153.

المزيد من الموارد في شراء الأدوات الحديثة، تدريب المحققين بشكل مستمر، وتعزيز التعاون الدولي لمواجهة التحديات التقنية المتزايدة في عصر الجرائم الإلكترونية.

المبحث الثاني: التحديات العملية والاجتماعية في الجرائم الإلكترونية في الجزائر

في ظل التطور السريع للتكنولوجيا وانتشار الإنترنت على نطاق واسع، أصبحت الجرائم الإلكترونية تمثل تهديدًا متزايدًا للأفراد، المؤسسات، وحتى الدول. وفي الجزائر، كما في العديد من الدول الأخرى، أفرزت الجرائم الإلكترونية مجموعة من التحديات العملية و الاجتماعية التي تعوق فعالية التصدي لهذه الجرائم. من الناحية العملية، يتعلق الأمر بكيفية إدارة التحقيقات في الجرائم الرقمية وتطبيق القوانين الخاصة بها. أما من الناحية الاجتماعية، فتمثل قلة الوعي المجتمعي حول مخاطر هذه الجرائم، بالإضافة إلى تأثيرها الثقافي والاجتماعي، أحد أبرز المعوقات.[1].

تواجه الجزائر تحديات عملية في التعامل مع الجرائم الإلكترونية من خلال صعوبة تنفيذ الإجراءات القضائية، وقلة التنسيق بين الأجهزة القضائية والأمنية، ونقص الأدوات التقنية اللازمة. كما تواجه تحديات اجتماعية تتمثل في غياب الوعي الكافي بين المواطنين حول كيفية التعامل مع الأمن الرقمي، إضافة إلى النظرة المجتمعية التي قد تقلل من أهمية هذه الجرائم وتأثيرها السلبي على الأفراد والمجتمع ككل.

تهدف هذه الدراسة إلى استعراض أبرز التحديات العملية والاجتماعية التي تواجه الجزائر في محاربة الجرائم الإلكترونية، من خلال تحليل العقبات التي تواجه الأجهزة المختصة، بالإضافة إلى دراسة تأثير تلك الجرائم على المجتمع الجزائري وكيفية معالجة هذه الظواهر في المستقبل.

[1]- خضراوي، الهادي وبوقرين، عبدالحليم. "تجربة الجزائر في مكافحة الجريمة الإلكترونية". المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC، جامعة الإمام محمد بن سعود الإسلامية، 2015

سنتناول في هذا المبحث التحديات العملية المتعلقة بكيفية تنفيذ التحقيقات في الجرائم الإلكترونية، مثل نقص الخبرات العملية و البنية التحتية التقنية، وكذلك التحديات الاجتماعية التي ترتبط بضعف الوعي العام بالمخاطر الرقمية و ضعف الثقافة الأمنية لدى الأفراد.

المطلب الأول: التحديات العملية في التحقيقات في الجرائم الإلكترونية في القانون الجزائري

تعد الجرائم الإلكترونية من الظواهر المعقدة التي تتطلب استجابة قانونية وفنية خاصة، خصوصًا في مرحلة التحقيقات الجنائية. في الجزائر، وعلى الرغم من الجهود المبذولة لمكافحة هذه الجرائم، تواجه التحقيقات الإلكترونية عدة تحديات عملية تعرقل فعالية تطبيق القانون في هذا المجال. تتجلى هذه التحديات في عدم ملاءمة التشريعات القائمة لخصوصية الجرائم الإلكترونية، بالإضافة إلى صعوبة جمع الأدلة الرقمية، والتنسيق بين المؤسسات المعنية [1].

الفرع الأول: نقص الخبرات العملية والتدريب في التحقيقات الإلكترونية

من أبرز التحديات العملية التي يواجهها المحققون في الجزائر هو نقص الخبرات العملية المتخصصة في مجال التحقيقات الرقمية. تتطلب الجرائم الإلكترونية مهارات متقدمة في التعامل مع الأدلة الرقمية، مثل تحليل البيانات المستخلصة من الأنظمة الحاسوبية أو الشبكات، وفك تشفير المعلومات المشفرة.

1 - الحاجة إلى تخصصات متقدمة

على الرغم من أن الجزائر شهدت بعض التطورات في هذا المجال، إلا أن هناك نقصًا في الخبرات المحلية والتخصصات الدقيقة في مجال التحقيقات الإلكترونية. المحققون في الجزائر قد لا يمتلكون جميع المهارات الضرورية للتعامل مع الأدلة الرقمية، سواء في ما يتعلق بـ استخراج البيانات من الأجهزة الرقمية أو تحليل محتويات هذه البيانات.

[1]– شاد، جيهان وزينب، بتيش. "سياسات مكافحة الجرائم الإلكترونية في الجزائر". جامعة سوق أهراس، 2023 ص120.

2 - قلة التدريب المستمر

إن قلة البرامج التدريبية المتخصصة و الدورات التعليمية المستمرة في المجال الرقمي تمنع المحققين من مواكبة التطورات السريعة في تقنيات الجرائم الإلكترونية. في كثير من الأحيان، تكون الأجهزة الأمنية والقضائية في الجزائر بحاجة إلى برامج تدريبية محدثة تعزز من قدرات المحققين على التعامل مع الأدوات الرقمية المتطورة وتحليل الأدلة الإلكترونية بشكل دقيق[1].

الفرع الثاني: صعوبة جمع الأدلة الرقمية والتحقق من صحتها

تمثل الأدلة الرقمية جوهر التحقيقات في الجرائم الإلكترونية، ولكن جمعها والتحقق من صحتها يتطلب تقنيات وطرق خاصة. في الجزائر، هناك عدة صعوبات قانونية وفنية تواجه المحققين في هذا المجال، من أهمها:

1 - صعوبة الوصول إلى الأدلة الرقمية

قد يكون من الصعب على المحققين الوصول إلى الأدلة الرقمية في بعض الجرائم الإلكترونية، خصوصًا عندما يكون المجرمون قد استخدموا تقنيات متقدمة مثل التشفير أو الشبكات المجهولة (مثل شبكة الإنترنت المظلم). إضافة إلى ذلك، قد تكون الأدلة الرقمية موزعة عبر عدة أنظمة إلكترونية أو خوادم دولية، مما يجعل الوصول إليها أكثر تعقيدًا.

2 - القوانين المتعلقة بالخصوصية

التحقيقات في الجرائم الإلكترونية تتطلب أحيانًا الوصول إلى بيانات خاصة للأفراد، مثل سجلات البريد الإلكتروني أو الحسابات المصرفية. وفي الجزائر، قد تكون هناك قيود قانونية

[1]- بدودة عزيزة، وعلالي، سعاد. "التحقيق الجنائي في الجرائم الرقمية". جامعة غرداية، 2018. ص45.

تتعلق بـ حماية الخصوصية و حقوق الأفراد، مما يحد من قدرة المحققين على جمع الأدلة الرقمية الضرورية.

3 – التحديات في التوثيق والتحليل

من التحديات الأخرى التي تواجه المحققين في الجزائر هو التوثيق و التحقق من صحة الأدلة الرقمية. قد تكون الأدلة الرقمية عرضة للتلاعب أو التغيير، مما يهدد مصداقيتها في المحكمة. ولذا يجب على المحققين اتباع إجراءات دقيقة و تقنيات خاصة لضمان أن الأدلة التي يتم جمعها يمكن استخدامها كدليل قانوني مقبول في المحاكم.

الفرع الثالث: محدودية التنسيق بين الجهات المختصة

تعد التنسيقات بين الأجهزة الأمنية، القضائية، و التقنية من العوامل المهمة في التحقيقات في الجرائم الإلكترونية. إلا أن الجزائر تواجه صعوبة في ضمان التنسيق الفعّال بين هذه الأجهزة، مما يعرقل سير التحقيقات بشكل كبير.

1 – ضعف التعاون بين الشرطة والقضاء

في الجزائر، قد يكون هناك نقص في التعاون الفعّال بين الشرطة و الهيئات القضائية. في بعض الأحيان، تكون المعلومات المتعلقة بالجرائم الإلكترونية عرضة للتأخير في تقديمها إلى النيابة العامة أو المحاكم، مما يؤدي إلى تأخير التحقيقات وإجراءات المحاكمة[1]

2 – غياب التعاون مع الهيئات الدولية

في الجرائم الإلكترونية العابرة للحدود، يواجه المحققون صعوبة في التعاون مع الهيئات الدولية، مثل الشرطة الدولية (الإنتربول) أو السلطات القضائية في دول أخرى. قد يكون من

1- كحلي، ياسين. "الجرائم السيبرانية والتحديات القانونية للأدلة الرقمية". الصحيفة، 2024.

الصعب الحصول على المساعدة الدولية في التحقيقات التي تتعلق بجرائم تم ارتكابها عبر الإنترنت، خصوصًا إذا كانت الأدلة موجودة في خوادم خارج الجزائر.

3 - نقص الدعم الفني والتقني

في الجزائر، هناك نقص في الدعم الفني المتخصص الذي يمكن أن يساعد في تحليل الأدلة الرقمية أو تقديم الاستشارات الفنية حول كيفية التعامل مع الأدلة المعقدة. يشمل ذلك قلة الخبراء الفنيين المتخصصين في التحقيقات الرقمية، مما يزيد من صعوبة إجراء التحقيقات بسرعة وكفاءة [1].

الفرع الرابع: صعوبة التعامل مع الجرائم الإلكترونية عبر الحدود

نظرًا للطابع العالمي للإنترنت، فإن العديد من الجرائم الإلكترونية التي تحدث داخل الجزائر قد يكون لها صلة مباشرة بأطراف خارجية، سواء كانت شبكات إجرامية أو مجرمين دوليين. وهذا يمثل تحديًا كبيرًا بالنسبة للتحقيقات المحلية في الجزائر.

1 - تنوع الأدلة عبر الحدود

الجرائم الإلكترونية قد تشمل عمليات اختراق عبر شبكات الإنترنت من دول مختلفة، مما يجعل عملية جمع الأدلة أكثر تعقيدًا، حيث قد تكون الأدلة الرقمية متوزعة بين عدة دول أو خوادم دولية. وهذا يتطلب تعاونًا دوليًا مع السلطات القضائية والأمنية في دول أخرى، ما قد يكون صعبًا أحيانًا بسبب الاختلافات القانونية بين الدول.

[1]- عديلة مراد، عبدلي ردوان. "الجريمة الالكترونية في التشريع الجزائري". جامعة المسيلة، 2021. ص19.

2 – القوانين الدولية غير الموحدة

إضافة إلى ذلك، فإن عدم وجود اتفاقيات دولية موحدة بشأن مكافحة الجرائم الإلكترونية يجعل من الصعب توحيد الأساليب القانونية للتحقيق في الجرائم العابرة للحدود. وبالتالي، يتعين على الجزائر التنسيق مع المنظمات الدولية مثل الإنتربول و الاتحاد الأوروبي لتبادل المعلومات حول الجرائم الإلكترونية عبر الحدود.

إن التحقيقات في الجرائم الإلكترونية في الجزائر تواجه العديد من التحديات العملية، أبرزها نقص الخبرات والتدريب في مجال التحقيقات الرقمية، صعوبة جمع الأدلة الرقمية و التوثيق الصحيح لها، ضعف التنسيق بين الجهات المختصة، إضافة إلى التحديات المرتبطة بالجرائم العابرة للحدود. للتغلب على هذه التحديات، يحتاج النظام القضائي والأمني في الجزائر إلى استثمارات في التدريب المتخصص، وتعزيز التعاون بين الأجهزة، وتطوير البنية التحتية الرقمية بما يتماشى مع تطور الجرائم الإلكترونية.

المطلب الثاني: التحديات الاجتماعية في مواجهة الجرائم الإلكترونية

في ظل الثورة الرقمية وانتشار الإنترنت على نطاق واسع، أصبحت الجرائم الإلكترونية تهديدًا عالميًا يتجاوز حدود الجغرافيا والمجتمعات، ويؤثر بشكل متزايد على الأفراد والدول على حد سواء. في الجزائر، كما في العديد من الدول، تتسبب هذه الجرائم في آثار اجتماعية ونفسية خطيرة تؤثر على الأمن الشخصي، الاقتصاد الوطني، وحتى على الاستقرار الاجتماعي. ومع تصاعد الجرائم الإلكترونية، تبرز التحديات الاجتماعية التي تقف أمام المجتمع في مواجهتها، حيث تتعلق هذه التحديات بشكل أساسي بـ الوعي المجتمعي، التعليم الرقمي، التحفظات الثقافية، وأيضًا التأثيرات النفسية لهذه الجرائم على الأفراد [1].

[1]– فتيحة بوقرة، الوعي المجتمعي بخطورة الجريمة الإلكترونية، مجلة البحوث القانونية، العدد 12، 2022، ص. 85–90.

إحدى أبرز هذه التحديات هي غياب الوعي المجتمعي بمخاطر الجرائم الإلكترونية، بالإضافة إلى ضعف التثقيف الرقمي في المناهج التعليمية، وعدم قدرة معظم الأفراد على التفاعل بشكل آمن مع العالم الرقمي. كما أن بعض الممارسات الثقافية والاجتماعية قد تُسهم في تجاهل أو تقليل أهمية حماية البيانات الشخصية والتصرف بحذر في البيئة الرقمية. هذه العوامل تُعتبر بمثابة عقبات اجتماعية تؤثر في فعالية الجهود المبذولة لمكافحة الجرائم الإلكترونية.

بالإضافة إلى ذلك، تساهم التحديات النفسية والاجتماعية المرتبطة بالجرائم الإلكترونية، مثل الابتزاز الرقمي أو الاحتيال الإلكتروني، في إحداث أضرار نفسية على الضحايا، ما يضعهم في مواقف اجتماعية صعبة قد تؤثر على حياتهم الشخصية والعائلية. ومن هنا، فإن الفهم العميق لهذه التحديات الاجتماعية يعد أمرًا ضروريًا في مواجهة هذه الظاهرة بشكل فعال.

في هذا المطلب، سيتم استعراض أهم التحديات الاجتماعية التي تواجه الجزائر في التصدي للجرائم الإلكترونية، والتي تتراوح بين غياب الوعي المجتمعي، ضعف التثقيف الرقمي، والتأثيرات النفسية التي يخلفها هذا النوع من الجرائم على الأفراد والمجتمع بشكل عام.

الفرع الأول: غياب الوعي المجتمعي بمخاطر الجرائم الإلكترونية

تعد مشكلة غياب الوعي المجتمعي من أبرز التحديات الاجتماعية التي تعيق مواجهة الجرائم الإلكترونية في الجزائر. إذ لا يزال العديد من الأفراد في المجتمع يفتقرون إلى الفهم الكافي حول مخاطر الإنترنت و التهديدات الرقمية التي قد يتعرضون لها في حياتهم اليومية. في ظل الانتشار الواسع للتكنولوجيا واستخدام الإنترنت بشكل متزايد، يعاني الكثير من الأشخاص من عدم الدراية بكيفية حماية أنفسهم وأجهزتهم من المخاطر الإلكترونية التي قد تشمل الاحتيال الإلكتروني، الابتزاز الرقمي، سرقة الهوية، الهجمات السيبرانية، وغيرها من الجرائم الإلكترونية [1].

[1]– سامية طواهرية، التحولات الاجتماعية في ظل الجريمة السيبرانية، دار الأكاديمية، 2021، ص. 142–147.

1 – قلة المعرفة بالمخاطر الرقمية

الكثير من الأفراد في الجزائر لا يدركون أن الأنشطة اليومية التي يقومون بها عبر الإنترنت قد تكون عرضة للهجمات الإلكترونية. فقد يعتقد البعض أن الاحتيال الرقمي أو الاختراقات الأمنية هي أمور نادرة أو بعيدة عنهم، مما يؤدي إلى سوء الاستخدام للإنترنت، مثل عدم اتخاذ الاحتياطات اللازمة عند التعامل مع البريد الإلكتروني، الشبكات الاجتماعية، أو المعاملات المالية عبر الإنترنت. على سبيل المثال، استخدام كلمات مرور ضعيفة أو إعطاء معلومات شخصية عبر منصات غير آمنة يزيد من فرص التعرض لاعتداءات إلكترونية.

2 – نقص التثقيف الرقمي في المناهج التعليمية

تساهم نقص التوعية الرقمية في النظام التعليمي في الجزائر في تفشي هذه الظاهرة. على الرغم من أهمية تعليم الأجيال القادمة كيفية التعامل مع التهديدات الإلكترونية بشكل آمن، إلا أن المناهج الدراسية في العديد من المدارس والمعاهد الجامعية لا تتضمن مواد تعليمية أو برامج تدريبية تركز على الأمن السيبراني أو الحماية الشخصية عبر الإنترنت. هذا يؤدي إلى شريحة واسعة من الشباب الذين قد لا يمتلكون المعرفة الكافية لحماية أنفسهم من الجرائم الإلكترونية[1].

3 – عدم وجود حملات توعوية شاملة

من الجوانب الأخرى التي تسهم في غياب الوعي الاجتماعي بمخاطر الجرائم الإلكترونية هو نقص الحملات التوعوية التي تستهدف فئات المجتمع المختلفة. على الرغم من وجود بعض المبادرات من قبل الجهات الحكومية أو المنظمات غير الحكومية، إلا أن حملات التوعية ليست كافية من حيث التغطية و الاستمرارية. يعاني كثير من الأفراد من عدم معرفة كيفية التصرف الصحيح في حال تعرضهم للاعتداءات الرقمية. كما أن الوعي بشأن الجرائم

[1]– بن عيسى بوشيخي مرجع سابق ص115.

الإلكترونية لا يتم بشكل منهجي عبر وسائل الإعلام المختلفة، ولا يتم توفير المعلومات الضرورية التي تساعد على تجنب هذه الجرائم [1].

4 - تأثير الثقافة المحلية على الوعي الرقمي

تلعب العادات الثقافية في الجزائر دورًا مهمًا في تحديد مدى اهتمام الأفراد بمخاطر الجرائم الإلكترونية. فقد يكون لدى البعض تصور بأن التهديدات الإلكترونية هي مشكلة غربية أو ظاهرة حديثة وليست جزءًا من التحديات التي يواجهها المجتمع المحلي. وهذا التصور قد يؤدي إلى إهمال الوقاية أو التقاعس عن اتخاذ إجراءات أمنية. فمثلًا، قد يعتقد البعض أن المهاجمين الرقميين يستهدفون شركات كبيرة فقط أو شخصيات عامة، وهو ما يساهم في التقليل من أهمية الحماية الرقمية لدى الأفراد العاديين.

5 - عدم توافر أدوات التوعية السهلة والمباشرة

أحد الأسباب التي تؤدي إلى استمرار غياب الوعي المجتمعي بمخاطر الجرائم الإلكترونية هو عدم توافر أدوات توعوية سهلة ومباشرة تناسب جميع فئات المجتمع، وخاصة الأشخاص غير المتخصصين في التكنولوجيا. إن استخدام اللغة التقنية المعقدة أو الرسائل التوعوية غير المباشرة قد يجعل من الصعب على الأفراد فهم أهمية حماية بياناتهم الشخصية أو طرق التصرف في حال التعرض للهجمات الإلكترونية.

وبالتالي، هناك حاجة ملحة إلى تبسيط المعلومات من خلال منصات التوعية مثل البرامج التثقيفية عبر الإنترنت أو الفيديوهات التفاعلية أو الحملات الإعلامية المحلية التي تقدم نصائح عملية للحماية من المخاطر الرقمية [2].

---

[1]- *سامية طواهرية*، المرجع سابق *ص. 142–147.*

[2]- سمير عبيدي، مواجهة الجرائم الإلكترونية: مقاربة توعوية مجتمعية، مجلة علوم الإعلام، العدد 19، 2021، ص. 77–80.

6 - تأثير الجهل بالخصوصية الرقمية على حياة الأفراد

من المظاهر الخطيرة الأخرى التي ترتبط بغياب الوعي المجتمعي، هو الجهل بحماية الخصوصية الرقمية. كثير من المستخدمين لا يعرفون كيفية حماية معلوماتهم الشخصية عبر الإنترنت أو لا يعطون أهمية لـ إعدادات الخصوصية في تطبيقات التواصل الاجتماعي أو البرامج التي يستخدمونها. هذا يؤدي إلى زيادة خطر الابتزاز الرقمي، سرقة البيانات، أو تعرضهم لـ الإعلانات المضللة، ما يساهم في وقوعهم ضحايا للجرائم الإلكترونية.

7 - الآثار الاجتماعية المترتبة على غياب الوعي

تتعدد الآثار الاجتماعية الناتجة عن غياب الوعي المجتمعي بمخاطر الجرائم الإلكترونية، وتشمل:

أ - **الإضرار بالسمعة الشخصية:** حيث يمكن أن تتسبب الجرائم مثل الابتزاز الرقمي أو التشهير عبر الإنترنت في فقدان الثقة بين الأفراد أو التأثير على علاقاتهم الاجتماعية.

ب - **التأثير على الأمن الشخصي:** فعدم الوعي بكيفية حماية المعلومات الشخصية قد يؤدي إلى تعريض الأفراد للمخاطر مثل سرقة الهوية أو الاحتيال الإلكتروني.

ج - **تدهور الثقة في التعاملات الإلكترونية:** إن غياب الوعي قد يؤدي إلى تراجع الثقة في استخدام الإنترنت، مما يؤثر على النمو الاقتصادي الرقمي في الجزائر[1].

إن غياب الوعي المجتمعي بمخاطر الجرائم الإلكترونية يعد من أبرز التحديات الاجتماعية التي تواجه الجزائر في مجال مكافحة هذه الجرائم. يشكل نقص التثقيف الرقمي، ضعف التوعية في المؤسسات التعليمية والإعلامية، بالإضافة إلى التحفظات الثقافية، عقبات أساسية في التصدي لهذه الظاهرة. ومن أجل مواجهة هذه التحديات، ينبغي على الجزائر تكثيف

[1]- عبد الرزاق بوشامة، الجريمة الإلكترونية والتحقيق الرقمي في الجزائر، دار الوجدان، 2022، ص. 144-147.

حملات التوعية، تعزيز التثقيف الرقمي في المدارس و الجامعات، وتوفير معلومات مبسطة لجميع أفراد المجتمع حول كيفية حماية أنفسهم من الجرائم الإلكترونية.

الفرع الثاني: الثقافة الرقمية المحدودة لدى أفراد المجتمع، مما يجعلهم عرضة للجرائم الإلكترونية

تعد الثقافة الرقمية من العوامل الأساسية التي تؤثر في قدرة الأفراد على التعامل بشكل آمن وفعّال مع تكنولوجيا المعلومات والإنترنت. في الجزائر، كما في العديد من الدول الأخرى، يعاني العديد من الأفراد من ثقافة رقمية محدودة، مما يجعلهم عرضة للعديد من الجرائم الإلكترونية التي تتنوع بين الاحتيال الإلكتروني، سرقة الهوية، الابتزاز الرقمي، وغيرها من الجرائم التي قد تؤثر بشكل كبير على حياتهم الشخصية والمهنية. هذا الافتقار إلى الوعي الرقمي يزيد من سهولة استهداف الأفراد من قبل المجرمين الإلكترونيين، ويجعل من الصعب الوقاية من هذه الجرائم.

1 - ضعف المعرفة بتقنيات الأمان الرقمي

يعتبر ضعف المعرفة بتقنيات الأمان الرقمي من أبرز الأسباب التي تجعل الأفراد عرضة للجرائم الإلكترونية. فالكثير من المستخدمين في الجزائر لا يعرفون كيف يمكنهم حماية بياناتهم الشخصية على الإنترنت، مثل تأمين كلمات المرور، استخدام أنظمة التشفير، أو إعدادات الخصوصية في منصات التواصل الاجتماعي. على سبيل المثال، استخدام كلمات مرور ضعيفة أو إعادة استخدام نفس كلمة المرور عبر حسابات متعددة يجعل الحسابات الإلكترونية للأفراد عرضة للاختراق بسهولة. كما أن قلة الوعي بالبرمجيات الضارة مثل الفيروسات و البرمجيات الخبيثة تجعل الأفراد أكثر عرضة للعديد من الهجمات الإلكترونية[1].

[1]- عمار بن زيد، حماية الحياة الخاصة في القانون الجزائري والمقارن، دار الخلدونية، 2020، ص. 121-130.

2 - ضعف فهم آليات الجرائم الإلكترونية

من التحديات الأخرى المتعلقة بالثقافة الرقمية المحدودة هو ضعف فهم الأفراد لآليات الجرائم الإلكترونية وكيفية وقوعها. على الرغم من انتشار الجرائم الإلكترونية مثل الاحتيال عبر الإنترنت و التصيد الاحتيالي، إلا أن الكثير من الأفراد في الجزائر لا يدركون أن هذه الجرائم قد تستهدفهم في حياتهم اليومية. على سبيل المثال، لا يملك الكثير من الأشخاص فكرة واضحة حول كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية أو المواقع الوهمية التي تسعى إلى جمع البيانات الشخصية أو سرقة المعلومات المالية. كما أن التوعية المحدودة حول أساليب الاحتيال الجديدة التي يستخدمها المجرمون الرقميون تجعل الأفراد أكثر عرضة للخداع. [1].

3 - قلة التثقيف الرقمي في النظام التعليمي

تعتبر المناهج التعليمية أحد العوامل التي تؤثر بشكل كبير على ثقافة الأفراد الرقمية. في الجزائر، على الرغم من أن هناك بعض الجهود المبذولة لدمج التعليم الرقمي في المدارس، إلا أن المناهج التعليمية تفتقر إلى محتوى توعوي شامل يتعلق بـ الأمن الرقمي. يعاني العديد من الطلاب من نقص الوعي حول كيفية حماية أنفسهم على الإنترنت، سواء في إطار استخدام الشبكات الاجتماعية أو إجراء المعاملات الإلكترونية. وبالتالي، فإن هذه الفجوة المعرفية تجعل الأجيال القادمة أكثر عرضة للمخاطر الرقمية.

4 - عدم التفاعل الإيجابي مع التكنولوجيا

في بعض الأحيان، يسهم عدم التفاعل الإيجابي مع التكنولوجيا في زيادة تعرض الأفراد للجرائم الإلكترونية. بعض الأشخاص في الجزائر لا يثقون بالتكنولوجيا أو لا يستخدمونها بشكل يومي، مما يقلل من قدرتهم على فهم المخاطر الرقمية بشكل جيد. هذا يمكن أن يؤدي إلى التصرفات غير الآمنة مثل التجاهل لعلامات التحذير من المواقع غير الآمنة أو مشاركة

[1]- العربي بلقاسم، الوعي السيبراني لدى الشباب الجزائري، مجلة العلوم الاجتماعية، العدد 22، 2022، ص. 40-47.

معلومات حساسة عبر الإنترنت بدون تدقيق. هذه السلوكيات تجعلهم هدفًا سهلًا للهجمات الإلكترونية.

5 - تأثير العادات الاجتماعية والثقافية

تلعب العادات الاجتماعية والثقافية في الجزائر دورًا كبيرًا في تعميق الفجوة الرقمية. بعض الأفراد قد لا يعطون أهمية كبيرة لمخاطر الإنترنت لأنهم يعتبرون أن المشاكل الرقمية هي قضايا تقنية فقط تتعلق بالشركات الكبرى أو الأشخاص ذوي المناصب العالية، بينما يمكن أن تؤثر هذه الجرائم بشكل مباشر على الجميع. على سبيل المثال، الاستهانة بحماية الخصوصية أو المشاركة المفرطة للمعلومات الشخصية في الإنترنت قد تكون نتيجة ثقافة اجتماعية غير واعية بمخاطر الأمان الرقمي [1].

6 - تأثير الافتقار إلى المصادر التعليمية المبسطة

إن غياب الموارد التعليمية المبسطة التي تشرح بطريقة يسهل فهمها كيفية حماية البيانات الشخصية على الإنترنت يعزز من محدودية الثقافة الرقمية. في العديد من الحالات، الرسائل التوعوية حول الجرائم الإلكترونية لا تكون موجهة بشكل مناسب للجمهور العريض، خاصة للأشخاص الذين لا يمتلكون معرفة تقنية متقدمة. لذلك، فإن إعداد حملات توعية تُعرض للمواطنين بأسلوب مبسط و واقعي يمكن أن يُحسن من مستوى الفهم حول طرق الحماية الرقمية.

7 - تأثير الجرائم الإلكترونية على المجتمع

إن غياب الثقافة الرقمية لا يؤثر فقط على الأفراد من الناحية الشخصية، بل له تأثيرات أوسع على المجتمع ككل. من خلال الجرائم الإلكترونية، تتعرض الثقة الرقمية في المجتمع

[1]- سمية قشي، التحولات الرقمية والمجتمع الجزائري: الفرص والمخاطر، دار الحكمة، 2021، ص. 91-95.

الجزائري إلى اهتزاز. بالإضافة إلى ذلك، قد يواجه الأفراد الذين يتعرضون للجرائم الإلكترونية مشكلات اجتماعية مثل الإحراج و التوتر النفسي، ما قد يؤدي إلى تداعيات اجتماعية سلبية تتعلق بالسمعة أو العلاقات الشخصية.

تعتبر الثقافة الرقمية المحدودة لدى أفراد المجتمع من أبرز العوامل التي تجعلهم عرضة للجرائم الإلكترونية في الجزائر. ضعف الوعي بالأدوات الأساسية للأمان الرقمي، قلة التثقيف في النظام التعليمي، بالإضافة إلى التحفظات الثقافية التي تساهم في التقليل من أهمية الحماية الرقمية، كلها عوامل تسهم في تفشي هذه الجرائم. لمواجهة هذه التحديات، ينبغي على السلطات المعنية والمجتمع المدني تكثيف الجهود لتطوير التثقيف الرقمي، توفير برامج توعية، و دمج الأمن السيبراني في المناهج التعليمية من أجل تحسين حماية الأفراد وزيادة وعيهم بمخاطر الجرائم الإلكترونية.

خاتمة

لقد حاولت في هدا الموضوع تسليط الضوء على التحديات التي تواجه التحقيقات في الجرائم الإلكترونية ضمن الإطار القانوني الجزائري، بالنظر إلى الطابع الخاص والمعقّد لهذا النوع من الإجرام، الذي يختلف من حيث الوسائل والأساليب عن الجرائم التقليدية.

أظهرت الدراسة أن المشرّع الجزائري قد قطع أشواطًا مهمة في سبيل تكييف منظومته القانونية مع مستجدات الفضاء الرقمي، من خلال إصدار القانون 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتعديل قانون العقوبات وقانون الإجراءات الجزائية.

تعتبر الجرائم الإلكترونية تمثل تحديًا معقدًا ومتجددًا للمنظومة القانونية الجزائرية، وذلك بالنظر إلى طبيعتها العابرة للحدود وسرعة تطورها التقني. وقد أظهر التشريع الجزائري وعيًا متزايدًا بخطورة هذه الجرائم من خلال إقرار نصوص خاصة في قانون العقوبات، وكذا عبر القانون رقم 18-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالإضافة إلى القانون 18-07 بشأن حماية المعطيات ذات الطابع الشخصي. غير أنّ الممارسة العملية تكشف عن وجود صعوبات متعددة، لاسيما على مستوى التكييف القانوني، وإثبات الجريمة، وضبط وسائل التحقيق الملائمة دون المساس بالحقوق والحريات الأساسية للأفراد.

كما أن نقص التخصص التقني لدى بعض الضبطية القضائية وأجهزة التحقيق، وضعف التنسيق بين الهيئات الوطنية والدولية، يشكلان عقبة أساسية في مواجهة هذا النوع من الإجرام المستحدث. وهو ما يفرض على المشرع الجزائري ضرورة الاستمرار في تحديث ترسانته القانونية، وتعزيز التكوين المتخصص للمحققين والقضاة، وتطوير آليات التعاون الدولي من أجل تحقيق نجاعة أكبر في مكافحة هذه الجرائم.

فإن مواجهة الجرائم الإلكترونية في الجزائر لا يمكن أن تكون فعّالة إلا من خلال مقاربة شاملة، تجمع بين تحديث الإطار القانوني، تدعيم الكفاءات التقنية، وتكريس التعاون على المستويين الوطني والدولي، ضمانًا لحماية الأفراد والمجتمع والدولة في آن واحد.

وتمثل الجرائم الإلكترونية واحدة من أكثر أشكال الجريمة تعقيدًا وحداثة في العصر الرقمي، وقد أبرزت هذه الدراسة حجم التحديات التي تواجه أجهزة التحقيق في الجزائر عند التعامل مع هذا النوع من الجرائم، فعلى الرغم من أن المشرّع الجزائري قطع خطوات مهمة من خلال سنّ قوانين خاصة مثل القانون رقم 20-06 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إلا أن الواقع العملي لا يزال يكشف عن جملة من المعوقات.

غير أنّ التطبيق العملي لهذه النصوص يكشف عن صعوبات متعددة، أهمها نقص الكفاءات التقنية لدى بعض الجهات القضائية والأمنية، قلة الوسائل التكنولوجية الحديثة لمتابعة المجرمين، وكذا التحديات المتعلقة بالتعاون الدولي في ظل الطبيعة العابرة للحدود لهذه الجرائم. كما أنّ الإثبات الجنائي في المجال الرقمي يثير إشكالات جوهرية ترتبط بمصداقية الدليل الرقمي وحجيته أمام القضاء، وتتوزع هذه التحديات بين صعوبات قانونية ناتجة عن فجوات تشريعية أو غموض في بعض المفاهيم التقنية، وتحديات تقنية مرتبطة بصعوبة تعقّب الأدلة الرقمية وسرعة زوالها، بالإضافة إلى قصور في التكوين البشري المتخصص في هذا المجال، ونقص التعاون الدولي الفعّال في القضايا ذات البُعد العابر للحدود.

أهم النتائج:

1. لا تزال النصوص القانونية ذات الصلة بالتحقيق الإلكتروني تعاني من نقص في الشمول والمرونة، ما يصعّب ملاحقة الجناة بفعالية.
2. تعاني أجهزة الضبط والتحقيق من ضعف التكوين التقني المتخصص في التعامل مع الأدلة الرقمية.
3. توجد صعوبات كبيرة في التعاون الدولي لملاحقة المجرمين خارج الحدود، نظراً لتعقيدات السيادة القضائية.
4. تفتقر الجزائر إلى إطار قانوني شامل للأمن السيبراني ينسق بين مختلف المتدخلين في المجال الرقمي.

5. لا تزال الوسائل التقنية المعتمدة في التحقيق محدودة مقارنة بالتطور المستمر في أدوات وأساليب الجريمة الإلكترونية.
6. قلة الكفاءات المتخصصة في الجرائم السيبرانية داخل الجهاز الأمني والقضائي، نتيجة نقص التكوين والتدريب.
7. غياب تعاون دولي فعال في ميدان تبادل الأدلة والمعلومات، بسبب التباين التشريعي وعدم مصادقة الجزائر على بعض الاتفاقيات الدولية كاتفاقية بودابست.
8. القصور في التوعية المجتمعية، مما يزيد من هشاشة الأفراد والمؤسسات تجاه الهجمات الإلكترونية.

التوصيات:

1. ضرورة إعداد قانون شامل للأمن السيبراني يتضمن تنظيمًا دقيقًا لمراحل التحقيق الرقمي، وحماية البيانات والأدلة الإلكترونية.
2. تدريب عناصر الشرطة القضائية والقضاة ووكلاء الجمهورية على أساليب التحقيق التقني ومبادئ الأمن الرقمي.
3. تعزيز البنية التحتية التكنولوجية للأجهزة الأمنية والعدلية، وتوفير أدوات تحليل البيانات وتتبع الجرائم عبر الشبكة.
4. إبرام اتفاقيات ثنائية ومتعددة الأطراف لتسهيل التعاون القضائي الدولي في الجرائم العابرة للحدود.
5. إنشاء هيئة وطنية مستقلة مختصة في الجرائم الإلكترونية تُعنى بالتنسيق بين القطاعات وتوفير الدعم الفني للتحقيقات.
6. تحديث التشريعات بشكل دوري لمواكبة التغير السريع في أنماط الجرائم الإلكترونية، مع التركيز على الجرائم المستحدثة مثل الابتزاز الرقمي والاختراقات المتطورة.

قائمة المصادر والمراجع

أولا: المصادر

القرآن الكريم

النصوص القانونية

اتفاقيات

- اتفاقية بودابست بشأن الجرائم المعلوماتية، المعتمدة في 23 نوفمبر 2001، من قبل مجلس أوروبا، ودخلت حيز التنفيذ في 1 يوليو 2004.

- الأمم المتحدة، الوقائع الرسمية لمؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، فيينا، 10–17 أبريل 2000، وثيقة الأمم المتحدة رقمA/CONF.187/4 .

1 – القوانين

- القانون العضوي رقم 23-14 المؤرخ في 27 أوت 2023، المتعلق بالإعلام، الجريدة الرسمية للجمهورية الجزائرية، العدد 65، 2 ديسمبر 2023.

- القانون رقم 20–06 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 27، سنة 2020.

- القانون رقم 04–06 المؤرخ في 23 يونيو 2004، المتعلق بالقواعد المطبقة على الممارسات المتعلقة بالأمن المعلوماتي، الجريدة الرسمية، العدد 41، سنة 2004.

- القانون رقم 21–01 المؤرخ في 8 مارس 2021، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 16، سنة 2021.

- القانون رقم 18–05 المؤرخ في 10 مايو 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 28، سنة 2018.

- القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 16، سنة 2018.

- قانون رقم 15-04 المؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد 06، الصادرة بتاريخ 8 فبراير 2015.

- قانون رقم 09-01، ممضي في 25 فبراير 2009، الجريدة الرسمية عدد 15، المؤرخة في 08 مارس 2009، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات المعدل والمتمم بالأمر رقم 21-08 ممضي في 08 يونيو 2021 الجريدة الرسمية عدد 45، المؤرخة في 09 يونيو 2021، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

- قانون رقم 17-07، ممضي في 27 مارس 2017، الجريدة الرسمية عدد 20، المؤرخة في 29 مارس 2017، الصفحة 5، يعدل ويتمم الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية المعدل والمتمم بالأمر رقم 21-11، ممضي في 25 غشت 2021 الجريدة الرسمية عدد 65، المؤرخة في 26 غشت 2021، يتمم الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

- القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة في 16 أوت 2009.

- قانون رقم 04-15، ممضي في 10 نوفمبر 2004، الجريدة الرسمية عدد 71، المؤرخة في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

- قانون رقم 04/18 مؤرخ في 24 شعبان عام 1439 الموافق10 مايو سنة 2018 ،يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية. الجريدة الرسمية عدد 27، الصادرة بتاريخ 13 ماي 2018.

- القانون رقم 06-23 المتضمن قانون العقوبات الجزائري،المؤرخ في 20 ديسمبر 2006، الجريدة الرسمية، العدد 84، 2006.

- القانون رقم 2025/11 المتمم و المعدل للقانون رقم 2014/14 الخاص باحداث القوانين الخاصة بالجرائم الالكنرونية

2 –الأوامر

- الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، الجريدة الرسمية للجمهورية الجزائرية، العدد 78 لسنة 1975، مع التعديلات الأخيرة لا سيما بموجب القانون رقم 05-10 المؤرخ في 20 يونيو 2005، والقانون رقم 07-05 المؤرخ في 13 مايو 2007.

3 - التقارير

- أبحاث أكاديمية تؤكد أن الجرائم الإلكترونية، لطابعها العابر للحدود، لا يمكن مكافحتها دون تعاون دولي.

- استضافت الجزائر القمة السابعة للأمن السيبراني الإفريقي عام 2019، بمشاركة خبراء أفارقة وأجانب، تحت شعار "أفريقيا الرقمية الآمنة.

- الاستراتيجية الوطنية للأمن السيبراني في الجزائر تهدف إلى حماية البنية التحتية الرقمية ومواجهة الهجمات الإلكترونية، وخاصة على القطاعات الحيوية كالطاقة والمالية.

- الأمم المتحدة، Convention on Cybercrime, تبنّت من قبل الجمعية العامة في ديسمبر 2024؛ يفرض الاتفاق إحلال تشريعات وطنية تتناول "الولوج غير المصرّح به إلى نظام معلوماتي، والمساس بالبيانات أو أنظمة البنية التحتية الحساسة"، ويشدد على آليات التعاون الدولي وتبادل الأدلة الإلكترونية.

- الجزائر لم توقع على اتفاقية بودابست لكنها تعتمد على قانون 09-04 لتنظيم المساعدة القانونية المتبادلة وتفعيل شبكة الطوارئ 7/24 تبعًا للمواد 27 و35 من القانون ذاته.

- المركز العربي الإقليمي للأمن السيبراني نظم "تمرينًا سيبرانيًا" بمراكش عام 2024 بمشاركة 80 متخصصًا من 18 دولة عربية وإفريقية، في إطار تعاون مشترك مع الاتحاد الدولي للاتصالات وواشنطن للمعلومات السيبرانية.

- شاركت الجزائر في ورشات) CyberSouth سيبروسوث) التي تنظمها مجلس أوروبا، مثل المؤتمر الوطني حول الجرائم الإلكترونية (سبتمبر 2023، الجزائر العاصمة) .

- مشروع (2024–2026) CyberSouth+ يعزز قدرات القضاء الجزائري على التعامل مع الأدلة الإلكترونية في إطار تعاون بين الاتحاد الأوروبي ومجلس أوروبا.

- منظمة UNODC دعمت الجزائر لمشاركة الأدلة الإلكترونية عبر الحدود ومكافحة الإرهابيين الإلكترونيين، ضمن تدريب (فبراير 2021).

- وزارة العدل الجزائرية، التقرير السنوي حول الجريمة السيبرانية والتعاون الدولي، منشورات الوزارة، الجزائر، 2023.

UNODC :- دعم الجزائر في "مشاركة الأدلة الإلكترونية عبر الحدود ومكافحة استخدام الإنترنت ووسائل التواصل الاجتماعي للأغراض الإرهابية"، خلال تدريب نظمته UNODC/TPBفي فبراير 2021. هذا التدريب ركز على تعزيز الإطار القانوني لمكافحة الإرهاب الإلكتروني وتعزيز قدرات متابعة الأدلة الرقمية.

ثانيا : المراجع

1 – المؤلفات

أ – المؤلفات العامة

– عبد الحكيم بوشيخي، شرح قانون الإجراءات الجزائية الجزائري، دار الخلدونية، الجزائر، 2020.

– عبد القادر بوشاشي، شرح قانون العقوبات – القسم الخاص – الجرائم الماسة بأنظمة المعالجة الآلية، دار هومة، الجزائر، 2021.

– عمار بن زيد، حماية الحياة الخاصة في القانون الجزائري والمقارن، دار الخلدونية، 2020.

ب – المؤلفات الخاصة

– أحمد بوزيان، الجرائم الإلكترونية والهجمات السيبرانية: دراسة قانونية وتقنية، دار الجامعة، الجزائر، 2021.

– أحمد عبد الله المصري، الجرائم الإلكترونية وحق الخصوصية في القانون الدولي، دار الجامعة الجديدة، الإسكندرية، 2020.

– بن عبو عبد القادر، الجرائم الإلكترونية في التشريع الجزائري، دار هومة، الجزائر، 2017.

- بوزيد نذير، الجريمة المعلوماتية: دراسة قانونية مقارنة، دار الجامعة الجديدة، الجزائر، 2021.

- خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، الدار الجامعية للطباعة والنشر والتوزيع، القاهرة، مصر ، 2008.

- زروقي عبد القادر ، التحقيق الجنائي في الجرائم الإلكترونية. دار هومة، الجزائر، 2021.

- زهية بن عيش، الجرائم الإلكترونية في التشريع الجزائري، دار هومة، الجزائر، 2020.

- سمية قشي، التحولات الرقمية والمجتمع الجزائري: الفرص والمخاطر، دار الحكمة، 2021.

- صابر قسوم، التحقيق الجنائي في الجرائم المعلوماتية، دار هومة، الجزائر، 2019.

- صابر قسوم، التحقيق الجنائي في الجرائم المعلوماتية، دار هومة، الجزائر، 2019.

- عبد الرزاق بوشامة، الجريمة الإلكترونية والتحقيق الرقمي في الجزائر، دار الوجدان، 2022.

- عبد الكريم بوالشعير، القانون الدولي لمكافحة الإرهاب الإلكتروني، دار المعرفة، الجزائر، 2019.

- عبد اللاوي عبد العزيز ، الجرائم الإلكترونية والتحديات الأمنية. دار الخلدونية للنشر، الجزائر، 2019.

- عبد الله ناصر آل فهيد، الجرائم الإلكترونية: دراسة مقارنة في ضوء الشريعة الإسلامية والقانون الوضعي، دار المطبوعات الجامعية، 2017.

- عبد الله ناصر آل فهيد، الجرائم الإلكترونية: دراسة مقارنة في ضوء الشريعة الإسلامية والقانون الوضعي، دار المطبوعات الجامعية، 2017.-

عبد الحميد بوكرومة، الجرائم الإلكترونية في القانون الجزائري: دراسة تحليلية مقارنة، دار هومة، الجزائر، 2020.

- محمد عبد الحليم غنيم، الجريمة الإلكترونية: التحديات وسبل المواجهة، دار الفكر الجامعي، الإسكندرية، 2018.

- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها ، مركز الإعلام الأمني، وزارة الداخلية ، الأكاديمية الملكية للشرطة ، مملكة البحرين ، 2010 .

- محمد علي مكاوي، الجرائم الإلكترونية بين الفقه والقانون، دار الجامعة الجديدة، الإسكندرية، 2019.

- محمود عبد الله البسيوني، "الجرائم الإلكترونية: المفهوم والتحديات"، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 61، 2020.

- مرهج الهيتي، الجريمة الالكترونية نماذج من تطبيقاتها (دراسة مقارنة) القاهرة، دار الكتب القانونية 2014.

- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، في ضوء الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات ، قانون العقوبات ، ق إ ج ، قوانين خاصة ، دار الجامعة الجديدة ، الإسكندرية ، 2019 .

- يوسف بوشيخي، الجرائم الإلكترونية: دراسة قانونية في التشريع الجزائري والمقارن، دار هومة، الجزائر، 2021.

2 – الرسائل والمذكرات العلمية

أ – رسائل ماجستير

– سفيان سوير، جرائم المعلوماتية ، مذكرة لنيل شهادة الماجستير في العلوم الجنائية ، وعلوم الإجرام ، كلية الحقوق ، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2011.

– نداء نائل فايز المصري خصوصية الجرائم المعلوماتية، مذكرة مقدمة لنيل درجة الماجيستر ، في القانون العام ، بكلية الدراسات العليا في جامعة النجاح الوطنية ، نابلس ، فلسطين ، 2017.

ب – مذكرات ماستر

– أمينة بوشعرة ، سهام موساوي، الإطار القانوني للجريمة الإلكترونية ، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية 2018 .

ثالثا : المقالات

– فتيحة بن قرينة، السياسة الجنائية الجزائرية في مواجهة الجريمة الإلكترونية، مجلة القانون والدراسات، العدد 10، 2022.

– إبراهيم حمد السويلم، "الجريمة الإلكترونية والتحديات القانونية"، مجلة دراسات أمنية، المجلد 12، العدد 2، 2020.

– أحمد بلحاج، "التحول الرقمي والجرائم الإلكترونية"، مجلة الدراسات القانونية والسياسية، العدد 14، جامعة ورقلة، 2020.

– أحمد فلاق، التحقيق في الجرائم الإلكترونية: التحديات القانونية والتقنية، مجلة الدراسات القانونية، جامعة الجزائر 1، العدد 7، 2021.

- الحارثي منصور ،. "معوقات إثبات الجرائم المتعلقة بتقنية المعلومات." المجلة القانونية، المجلد 15، العدد 4، 2023.

- العربي بلقاسم، الوعي السيبراني لدى الشباب الجزائري، مجلة العلوم الاجتماعية، العدد 22، 2022.

- العربي نوال ، المواجهة القانونية للجرائم الإلكترونية في الجزائر. مجلة العلوم القانونية والسياسية، جامعة سطيف، العدد 23، 2020.

- أنيس العذار ، مكافحة الجريمة الإلكترونية "، المجلة الأكاديمية للبحث القانوني ، المجلد 17 ، العدد 01 ، 2018.

- أيمن بارّة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر، جامعة ورقلة، 2022؛ يشير إلى أن القانون رقم 21-01 يضع "برامج وآليات تقنية وقدرات بشرية لمواجهة أي تعدٍّ على المعلومات الإلكترونية.

- بدودة عزيزة، وعلالي، سعاد. "التحقيق الجنائي في الجرائم الرقمية". جامعة غرداية، 2018.

- بردال سمير،"الجريمة المعلوماتية في التشريع الجزائري." مجلة القانون، المجلد 1، العدد 2، 2010.

- بلعزوز، فاطمة الزهراء. الجرائم الإلكترونية في القانون الجزائري. مجلة الدراسات القانونية والسياسية، جامعة محمد خيضر بسكرة، العدد 17، 2020.

- بلعزوز، فاطمة الزهراء. الجرائم الإلكترونية في القانون الجزائري. مجلة الدراسات القانونية والسياسية، جامعة محمد خيضر بسكرة، العدد 17، 2020.

– بن موسى، نادية. الجرائم الإلكترونية: الواقع والتحديات في الجزائر. مجلة الدراسات القانونية، جامعة الجزائر، العدد 12، 2022.

– بوخاري أحمد ، "الجريمة الإلكترونية في ضوء التشريع الجزائري." مجلة دفاتر السياسة والقانون، جامعة خنشلة، العدد 20، 2018.

– بوفنشة عبد الرحمن، الجرائم الإلكترونية: المفهوم والأنواع والوسائل القانونية لمكافحتها في الجزائر، مجلة الدراسات القانونية والسياسية، جامعة سطيف، العدد 12، 2019.

– جمال بوقطاية، الأمن السيبراني ومكافحة الإرهاب الإلكتروني في ضوء التشريع الجزائري، مجلة دراسات قانونية، العدد 14، جامعة الجزائر 1، 2021.

– خديجة بوعبد الله، مكافحة الجرائم الإلكترونية في التشريع الجزائري وأثرها على حماية الحقوق الرقمية، مجلة القانون والتكنولوجيا، جامعة قسنطينة، العدد 10، 2023.

– خضراوي، الهادي وبوقرين، عبدالحليم. "تجربة الجزائر في مكافحة الجريمة الإلكترونية". المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتيةICACC –، جامعة الإمام محمد بن سعود الإسلامية، 2015

– خيدل أحمد، وكيسي، زهيرة جيلالي عبدالقادر. "إجراءات جمع الأدلة الرقمية طبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات". مجلة الاجتهاد للدراسات القانونية والاقتصادية، 2022.

– خليف عبد الحميد ، التحديات القانونية لمكافحة الجريمة الإلكترونية. مجلة دفاتر السياسة والقانون، جامعة ورقلة، العدد 29، 2021.

– ذياب موسى البداينة، الجرائم الإلكترونية : المفهوم والأسباب، ورقة علمية مقدمة للملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من 02 إلى 04 سبتمبر 2014، كلية العلوم الاستراتيجية، عمان، الأردن.

.– العربي نوال ،المواجهة القانونية للجرائم الإلكترونية في الجزائر. مجلة العلوم القانونية والسياسية، جامعة سطيف، العدد 23، 2020.

–راوية بن ساسي، مكافحة الجرائم الإلكترونية في القانون الجزائري: بين النص القانوني والتحديات التطبيقية، المجلة الجزائرية للقانون الرقمي، العدد 4، 2022.

– رحموني أحمد ، خصائص الجريمة الإلكترونية ومجالات استخدامها "، مجلة الحقيقة ، العدد 41 ، 2018

– ريم غربي، "الجرائم السيبرانية والتحديات القانونية في الجزائر"، مجلة دفاتر السياسة والقانون، جامعة خنشلة، العدد 28، 2021.

– زايدي فوزية ، "مكافحة الجريمة الإلكترونية في الجزائر: التحديات والآفاق." مجلة البحوث القانونية والسياسية، جامعة تبسة، العدد 7، 2016.

– سامي دراجي، الجرائم الإلكترونية المنظمة في القانون الجزائري الآليات الوقائية والتحديات الأمنية، مجلة الدراسات القانونية والسياسية، العدد 9، 2022.

– سامية بن سعيد، حماية الحياة الخاصة والبيانات الشخصية في التشريع الجزائري في ظل التهديدات الرقمية، مجلة القانون والمجتمع، العدد 11، 2022.

– سامية طواهرية، التحولات الاجتماعية في ظل الجريمة السيبرانية، دار الأكاديمية، 2021.

– سمير عبيدي، مواجهة الجرائم الإلكترونية: مقاربة توعوية مجتمعية، مجلة علوم الإعلام، العدد 19، 2021.

– شاد، جيهان وزينب، بتيش. "سياسات مكافحة الجرائم الإلكترونية في الجزائر". جامعة سوق أهراس، 2023.

–شراد سميرة ، التحقيق في الجرائم الإلكترونية في الجزائر. مجلة الحقوق والعلوم السياسية، جامعة تبسة، العدد 15، 2022.

– عديلة مراد، عبدلي ردوان. "الجريمة الالكترونية في التشريع الجزائري". جامعة المسيلة، 2021.

– عزيزة رابحي العنصر المفترض في جريمة الدخول او البقاء غير المصرح به للنظام المعلوماتي، المجلة الجزائرية للدراسات التاريخية والقانونية، المركز الجامعي تندوف، المجلد 01 ، العدد 02 جوان ،2016.

– غزالي زهيرة، الجريمة المعلوماتية والتصدي لها في التشريع الجزائري، مجلة دفاتر السياسة والقانون، جامعة مولود معمري تيزي وزو، العدد 18، 2017.

– فتيحة بوقرة، الوعي المجتمعي بخطورة الجريمة الإلكترونية، مجلة البحوث القانونية، العدد 12، 2022.

– كحلي، ياسين. "الجرائم السيبرانية والتحديات القانونية للأدلة الرقمية". الصحيفة، 2024.

– لحارثي، منصور فهيد سعيد. "معوقات إثبات الجرائم المتعلقة بتقنية المعلومات." المجلة القانونية، المجلد 15، العدد 4، فبراير 2023.

– محمد السعيد زناتي الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية ، مجلة إيليزا للبحوث والدراسات، المجلد 02، العدد 01 ديسمبر 2017.

– مصطفى لعور، التحول الرقمي والأمن السيبراني في الجزائر: الإطار القانوني والتحديات المستقبلية، المجلة الجزائرية للقانون والاقتصاد الرقمي، العدد 7، 2022.

- منير محمد الجنبيهي، جريمة الإرهاب الإلكتروني بين عولمة الجريمة وضرورة المكافحة، مجلة الدراسات الأمنية، الجزائر، 2022؛.

- نصير لعرباوي، فاتح النور رحموني ، الجريمة الإرهابية الإلكترونية ، المعيار ، العدد 43 ، جانفي ، 2018 .

- نمديلي رحيمة ، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة ، أعمال المؤتمر الدولي الرابع عشر للجرائم الإلكترونية – الجزائر ، 24 مارس 2017.

- نوال رزيق، "التحقيق في الجرائم الإلكترونية في ظل التشريع الجزائري"، مجلة القانون والأعمال الدولية، العدد 23، جامعة تلمسان، 2022.

رابعا : المراجع باللغة الاجنبية

- U.S. Department of Justice, Computer Crime: Criminal Justice Resource Manual, Washington D.C., 1989.

- Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, Budapest, 23.XI.2001.

- Bouzida, Y. (2020). Cybercrime and digital investigation challenges in Algeria. International Journal of Cyber Criminology, Vol. 14.

- Digital Policy Alert, "In June 2024, Algeria implemented the Law on written and electronic press… requiring online press providers to use websites hosted exclusively on physical infrastructure in Algeria with a ".dz" domain extension… In December 2024, the Law on the Audiovisual Activity entered into force… prohibiting audiovisual and online communication services from broadcasting content that promotes violence, terrorism, racial discrimination, or false information", accessed 26 June 2025, via: https://digitalpolicyalert.org

الفهرس

ملخص مذكرة الماستر

يواجه التحقيق في الجرائم الإلكترونية في الجزائر تحديات متعددة تعود إلى الطبيعة المعقدة لهذا النوع من الجرائم، والذي يعتمد على تكنولوجيات متطورة وسريعة التغير. رغم صدور القانون رقم 20-06 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إلا أن التحقيقات لا تزال تواجه صعوبات حقيقية، من بينها نقص الكفاءات التقنية، وصعوبة جمع الأدلة الرقمية، وغياب التنسيق الدولي الكافي. كما أن عدم الانخراط في اتفاقيات دولية مثل اتفاقية بودابست يحدّ من فعالية التعاون القضائي العابر للحدود. ولذلك، تبرز الحاجة إلى تحديث الإطار القانوني، وتكوين المحققين، وتعزيز البنية التحتية التقنية لضمان فعالية التحقيقات في هذا المجال الحيوي.

الكلمات المفتاحية:

1 – الجرائم الإلكترونية، 2 – التحقيق الجنائي، 3 – التشريع الجزائري، 4 – الأدلة الرقمية، 5 – الأمن السيبراني، 6 – القانون 20-06.

Abstract of The master thesis

Investigating cybercrimes in Algeria presents numerous challenges due to the complex and evolving nature of these crimes, which rely on advanced and rapidly changing technologies. Although Law No. 20-06, which addresses offenses related to information and communication technologies, has been enacted, practical difficulties remain. These include a shortage of technical expertise, challenges in collecting digital evidence, and insufficient international cooperation. The lack of engagement in key international frameworks, such as the Budapest Convention, further limits cross-border judicial coordination. Thus, there is a pressing need to update the legal framework, train investigators, and strengthen technological infrastructure to ensure effective cybercrime investigations.

Keywords:

1 -Cybercrime, 2 - Criminal Investigation, 3 - Algerian Legislation, 4 - Digital Evidence, 5 - Cybersecurity,6- Law 20-06.