جامعة عمار ثليجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

الجريمة السيبرانية والإستراتيجيات الدولية لمكافحتها

مذكرة مكملة لنيل شهادة الماستر في القانون الدولي العام

تخصص: قانون دولي العام

إعداد الطالب:
- خروبي يسين

إشراف الأستاذ:
د/ عبد المالك الدح

لجنة المناقشة:

الإسم واللقب	الرتبة	الجامعة	الصفة
عطاء الله خضرون	دكتور	جامعة عمار ثليجي - الأغواط	رئيسا
عبد المالك الدح	دكتور	جامعة عمار ثليجي - الأغواط	مشرفا
جيلالي شويرب	دكتور	جامعة عمار ثليجي - الأغواط	مناقشا

السنة الجامعية : 2025 /2026

شكر وتقدير

قال الله تعالى: *فاذكروني أذكركم واشكروا لي ولا تكفرون"* ،

وقال رسول الله صلى الله عليه وسلم" :*من لا يشكر الناس لا يشكر الله."*

الحمد لله الكريم المنّان، نحمده ونشكره ونستعين به، فهو الذي وفقنا وأعاننا لإتمام هذا العمل المتواضع، ونسأله أن يجعله خالصًا لوجهه الكريم.

نتقدم بجزيل الشكر وخالص الامتنان إلى أستاذنا المشرف **شويرب جيلالي** ، الذي لم يدّخر جهدًا في توجيهنا وإرشادنا، وكان لنا نعم السند في كل المراحل، فله منا كل التقدير والاحترام.

كما نوجه الشكر إلى كافة أساتذة قسم قانون دولي، لما بذلوه من جهود في تعليمنا وتكويننا، وإلى كل من ساعدنا من قريب أو بعيد في إنجاز هذا العمل، فلكم جميعًا منا أسمى عبارات الشكر والامتنان.

إهداء

﴿ وَقَضى رَبُّكَ أَلّا تَعبُدوا إِلّا إِيّاهُ وَبِالوالِدَينِ إِحسانًا ﴾

إهداء

إلى من هي الأولى بصحبتي، ونبع الحنان في حياتي،

"أمي الغالية"

إلى من ربتني صغيرًا، وأشفقت علي كثيرًا، وكانت سندي في كل مراحل حياتي، إلى اخوتي الأعزاء، الذين كانوا دائمًا عونًا وسندًا لي في حياتي عامة، وفي تحصيلي العلمي خاصة، كل واحد باسمه ومكانته في

قلبي.

إلى كل من ساعدني من قريب أو بعيد، ولو بكلمة طيبة أو دعاء صادق، أسأل الله أن يجزيهم عني خير الجزاء.

فنسأل الله أن ييسر لنا هذا العمل، ويوفقنا فيه، ويجعله في ميزان حسناتنا.

مقدمة

مقدمة:

شهد العالم خلال العقود الأخيرة ثورة رقمية غير مسبوقة، كان لها أثر بالغ في إعادة تشكيل مختلف مجالات الحياة الإنسانية، حيث أصبحت تكنولوجيا المعلومات والاتصال عنصرا أساسيا في إدارة المؤسسات وتسيير المرافق العامة والخاصة. غير أن هذا التطور التكنولوجي، رغم ما يحمله من مزايا، أفرز في المقابل تحديات خطيرة تمثلت في بروز أنماط جديدة من الجرائم تُعرف بالجرائم الإلكترونية أو السيبرانية، والتي تتميز بقدرتها على تجاوز الحدود الجغرافية واستهدافها لمصالح حيوية تمس أمن الدول واستقرارها و حتى الأفراد على اختلاف مسؤولياتهم و مجالات أعمالهم .

قد أدى الانتشار الواسع للإنترنت وتزايد الاعتماد على الأنظمة الرقمية إلى اتساع نطاق هذه الجرائم، مما جعلها تشكل تهديدًا حقيقيًا للأمن الدولي، خاصة في ظل صعوبة تعقب مرتكبيها وتعدد وسائل تنفيذها. الأمر الذي دفع المجتمع الدولي إلى تبني استراتيجيات وآليات قانونية لمكافحتها، من خلال الاتفاقيات الدولية والتعاون الأمني والقضائي.

إشكالية الدراسة:

إلى أي مدى نجحت الجهود الدولية والتشريعات الوطنية، خاصة التشريع الجزائري، في مكافحة الجريمة السيبرانية وتحقيق الأمن السيبراني؟

التساؤلات الفرعية:

- ما المقصود بالجريمة الالكترونية أو السيبرانية وما أركانها وخصائصها؟
- كيف تطورت الجرائم السيبرانية و ما أنواعها؟
- ما مفهوم الأمن السيبراني وما أبعاده؟
- ما هي أهم الآليات الدولية والوطنية لمكافحة هذه الجرائم؟

أسباب اختيار الموضوع:

يرجع اختيار هذا الموضوع إلى:

- حداثته وأهميته في القانون الدولي
- تزايد الجرائم السيبرانية عالميًا
- الحاجة إلى دراسة فعالية التشريعات الجزائرية

أهمية الدراسة:

تتمثل في:

- إبراز خطورة الجرائم السيبرانية
- تحليل الجهود الدولية لمكافحتها
- تقييم فعالية التشريع الجزائري

أهداف الدراسة:

- تحديد مفهوم الجريمة السيبرانية
- تحليل أركانها وخصائصها
- دراسة الآليات الدولية والوطنية

الدراسات السابقة:

تناولت عدة دراسات هذا الموضوع، منها:

- عبد الفتاح بيومي حجازي حول الجريمة المعلوماتية
- محمد حسين منصور حول المسؤولية الجنائية

وقد ركزت هذه الدراسات على الجانب القانوني دون الربط الكافي بالبعد الدولي .

قالمنهج المعتمد:

تم الاعتماد على:

اعتمدت على المنهجين الوصفي و التحليلي و ذلك للتعريف بالجريمة السيبرانية و خصائصها و أنواعها و طبيعة كرتطبي هذه الجريمة و تبيان خطورتها على الافراد و الدول

كما لجأت في جوانب ضيقة لاعتماد المنهج المقارن لتبيان كيف عولجت هذه الظاهرة محليا و دوليا

الصعوبات:

- قلة المراجع العربية المتخصصة
- تطور الظاهرة بشكل سريع
- صعوبة الحصول على نصوص تطبيقية حديثة

هيكلة البحث:

تم تقسيم الدراسة إلى فصلين:

- فصل أول: الإطار المفاهيمي
- فصل ثاني: آليات المكافحة الدولية والوطنية

الفصل الأول

الإطار المفاهيمي للجرائم الإلكترونية والأمن السيبراني

المبحث الأول: ماهية الجريمة السيبرانية

تمهيد:

الجريمة السيبرانية من أبرز الظواهر القانونية المستحدثة التي فرضت نفسها بقوة في ظل التطور التكنولوجي المتسارع، حيث لم يعد النشاط الإجرامي مقتصرا على الأفعال التقليدية التي تتم في نطاق مادي محسوس، بل امتد ليشمل الفضاء الرقمي الذي يتميز بعدم خضوعه للقيود الجغرافية أو الزمنية، وقد أدى هذا التحول إلى بروز إشكاليات قانونية معقدة تتعلق بتحديد مفهوم الجريمة الإلكترونية، وبيان عناصرها، ومدى خضوعها لمبدأ الشرعية الجنائية.

كما أن الطبيعة التقنية لهذه الجرائم جعلت من الصعب على الأنظمة القانونية التقليدية مواكبتها، الأمر الذي استدعى تدخل المشرعين لوضع نصوص خاصة تُجرّم هذه الأفعال، كما هو الحال في التشريع الجزائري من خلال القانون رقم 09-04 ومن جهة أخرى، سعى المجتمع الدولي إلى توحيد الجهود من خلال إبرام اتفاقيات دولية، أبرزها اتفاقية بودابست، بهدف مكافحة هذا النوع من الجرائم.

وعليه، فإن دراسة ماهية الجريمة السي تقتضي الوقوف على مفهومها القانوني، وتحليل أركانها، واستعراض خصائصها، وهو ما سيتم تناوله في هذا المبحث.

---

1. انون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 أوت سنة 2009

المطلب الأول: مفهوم الجريمة السبرانية

تمهيد:

إن تحديد مفهوم الجريمة الإلكترونية يعد من المسائل الجوهرية في الدراسات القانونية، نظرا لارتباطه بتحديد نطاق التجريم وتطبيق النصوص القانونية، غير أن هذا الأمر يواجه صعوبات كبيرة، بسبب الطبيعة المتغيرة للتكنولوجيا، وتعدد صور الجرائم المرتبطة بها، وقد أدى ذلك إلى اختلاف الفقهاء في وضع تعريف موحد، حيث اتجه البعض إلى التعريف الضيق، بينما تبنى آخرون تعريفا واسعا يشمل كل استخدام غير مشروع للتكنولوجيا.

الفرع الأول: ماهية الجريمة السبرانية

تعد الجريمة السيبرانية من الظواهر الحديثة التي ظهرت نتيجة التطور التكنولوجي السريع وانتشار استخدام الحواسيب والإنترنت في مختلف مجالات الحياة. فقد أدى التحول الرقمي واعتماد المؤسسات والأفراد على الأنظمة الإلكترونية إلى ظهور بيئة جديدة استغلها بعض الأشخاص لارتكاب أفعال غير مشروعة، مثل اختراق الأنظمة وسرقة البيانات والاحتيال الإلكتروني. وقد بدأت هذه الجرائم بشكل بسيط ومحدود مع بدايات استخدام الحواسيب، ثم تطورت تدريجيا مع تطور وسائل الاتصال والشبكات المعلوماتية.

ومع توسع شبكة الإنترنت خلال تسعينيات القرن الماضي، ازدادت خطورة الجريمة السيبرانية وتعقدت أساليبها، حيث ظهرت جماعات منظمة تستغل الفضاء الرقمي لتحقيق أهداف مالية أو سياسية أو حتى تخريبية. كما ساهم الانتشار الواسع للهواتف الذكية ووسائل التواصل الاجتماعي في توفير فرص أكبر للمجرمين الإلكترونيين للوصول إلى الضحايا بسهولة. وأصبحت الهجمات السيبرانية تستهدف الأفراد والشركات والمؤسسات الحكومية، مما جعلها تمثل تهديدا حقيقيا للأمن المعلوماتي والاقتصادي للدول.

وقد دفعت هذه التطورات العديد من الدول والمنظمات الدولية إلى سن قوانين وتشريعات خاصة بمكافحة الجرائم السيبرانية، إضافة إلى إنشاء هيئات متخصصة في الأمن الرقمي وحماية البيانات. كما تم تعزيز التعاون الدولي لمواجهة هذا النوع من الجرائم العابرة للحدود، نظرا لصعوبة تعقب مرتكبيها بالوسائل التقليدية. وعليه، فإن نشأة الجريمة السيبرانية ترتبط ارتباطا وثيقا بالتطور

التكنولوجي، الأمر الذي يفرض ضرورة مواكبة الوسائل القانونية والتقنية لمواجهة أخطارها المتزايدة.تعريف الجريمة السيبرانية لغة:

الجريمة لغة: مأخوذة من **الجريمة** بمعنى **الذنب أو الفعل المخالف للقانون.**[1]

الجريمة اصطلاحا : تعرف الجريمة في الفقه الجنائي الجزائري الحديث بأنها : ً كل سلوك خارجي ، إيجابي كان أو سلبي يرتكبه شخص أهلا لتحمل المسؤولية الجنائية ، بموجب نص قانوني سابق الوضع يجرم السلوك و يقرر له عقوبة أو تدبيرا أمنيا ، مستهدفا به الاعتداء على مصلحة أو حق يحميه القانون ً [2]

السيبرانية : كلمة معربة مشتقة من اللفظ اليوناني : (Cybernetes - كيوبيرنيتيس) و تعني في أصلها اللغوي : (الموجه أو القائد ، أو ربان السفينة ،أة الشخص الذي يملك القدرة على التوجيه و التحكم ، وقد دمجت في اللغات المعاصرة كسابقة تعني (الالكتروني)أو كل ما يرتبط بشبكات الحاسوب و الفضاء الالكتروني أو كل ما يرتبط بشبكات الحاسوب و الفضاء الالكتروني)[3] وبالتالي: الجريمة السيبرانية لغةً هي **:كل فعل خاطئ أو محظور يحدث في فضاء الإنترنت أو باستخدام الحاسوب.**

تعريف الجريمة السيبرانية اصطلاحا:

.1ابن منظور، لسان العرب، جزء 7، ص 123، دار صادر، بيروت، 2002.

2 . د.منصور رحماني، الوجيز في القانون الجنائي الجزائري: القسم العام ،ط4, ، ص45، دار العلوم للنشر و التوزيع ، عنابة 5 الجزائر ، 2021

3 . د . ممدوح عبد الحميد ، الأمن السيبراني، المركز القومي للإصدارات القانونية، ص18،ط1، القاهرة،2022

في **مصطلحات القانون**، يعرفها العلماء والباحثون القانونيون على النحو التالي:

التعريف العام :

الجريمة السيبرانية **هي كل فعل أو امتناع يُرتكب بواسطة الحاسوب أو الشبكات المعلوماتية، ويخالف أحكام القانون الجنائي**، ويترتب عليه **ضرر مادي أو معنوي على الأفراد أو الدولة أو المجتمع**[1].

2. **تعريف بعض المختصين :**

- **د. محمد خليل**" :الجريمة السيبرانية هي الأعمال التي تُرتكب ضد الأنظمة المعلوماتية أو من خلالها، بغرض إلحاق الضرر بالآخرين أو انتهاك الحقوق القانونية ."
- **الأمم المتحدة** :تعتبر الجريمة السيبرانية **كل جريمة تقترف باستخدام الإنترنت أو نظم المعلومات الإلكترونية .**

تعرف الجريمة الإلكترونية في الفقه القانوني بأنها كل فعل غير مشروع يتم باستخدام نظام معلوماتي أو شبكة إلكترونية، ويستهدف الاعتداء على البيانات أو الأنظمة أو الحقوق المرتبطة بها، ويلاحظ أن هذا التعريف يجمع بين عنصرين أساسيين: الوسيلة (التكنولوجيا) والهدف الاعتداء غير المشروع.

وقد ذهب جانب من الفقه إلى تعريفها بأنها "كل سلوك إجرامي يكون الحاسوب أو الشبكة وسيلة لارتكابه أو هدفًا له"، وهو تعريف يبرز الطبيعة المزدوجة للجريمة الإلكترونية، حيث يمكن أن

1ابن منظور، لسان العرب، جزء 7، ص 123، دار صادر، بيروت، 2002.

2 . د.منصور رحماني، الوجيز في القانون الجنائي الجزائري: القسم العام ،ط4, ، ص45، دار العلوم للنشر و التوزيع ، عنابة 5 الجزائر ، 2021

3 . د . ممدوح عبد الحميد ، الأمن السيبراني، المركز القومي للإصدارات القلنونية، ص18،ط1، القاهرة،2022

تكون الوسيلة أو المحل. وفي هذا السياق، يرى الفقيه عبد الفتاح بيومي حجازي أن الجريمة المعلوماتية هي "كل فعل غير مشروع يستخدم فيه الحاسوب كأداة رئيسية.[1]

أما على المستوى الدولي، فقد تناولت **اتفاقية بودابست لسنة 2001** الجريمة الإلكترونية من خلال تحديد الأفعال المجرمة، حيث نصت:

- **المادة 2** :تجريم الدخول غير المشروع إلى نظام معلوماتي
- **المادة 3** :تجريم اعتراض البيانات دون وجه حق
- **المادة 4** :تجريم الإضرار بالبيانات
- **المادة 5** :تجريم الإضرار بالأنظمة

أما في التشريع الجزائري، فقد نص القانون رقم 09-04 على مجموعة من الجرائم، من بينها:

- الدخول غير المشروع إلى نظام معلوماتي
- المساس بسلامة البيانات
- إساءة استخدام وسائل الاتصال

كما نص قانون العقوبات الجزائري في **المادة 394 مكرر** على معاقبة كل من يدخل أو يبقى في نظام معلوماتي دون ترخيص.

ويلاحظ أن المشرع الجزائري، شأنه شأن العديد من التشريعات، لم يضع تعريفا صريحا، بل اعتمد على تعداد الأفعال، وهو ما يتيح مرونة في مواجهة التطورات التقنية.

ومن جهة أخرى، تتميز الجريمة الإلكترونية بكونها جريمة غير مادية، حيث لا تترك آثارًا ملموسة، بل تكون في شكل بيانات رقمية، مما يطرح إشكالات في الإثبات. كما أنها قد تُرتكب عن بعد، دون الحاجة إلى التواجد في مكان الجريمة، وهو ما يجعلها جريمة عابرة للحدود.

---

1 عبد الفتاح بيومي حجازي، الجريمة المعلوماتية، دار الفكر الجامعي، مصر، 2006، ص 25 .

2 محمد حسين منصور، المسؤولية الجنائية عن الجرائم الإلكترونية، دار الجامعة الجديدة، مصر، 2010، ص 48 .

3 أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، 2013، ص 115 .

كما أن هذه الجرائم قد تكون فردية أو منظمة، حيث ظهرت في السنوات الأخيرة شبكات إجرامية متخصصة في الهجمات السيبرانية، مما يزيد من خطورتها[1].

الفرع الثاني: أركان الجريمة السيبرانية

إن أركان الجريمة الإلكترونية هو الأساس الذي تقوم عليه المسؤولية الجنائية، حيث لا يمكن تصور قيام جريمة دون توافر عناصرها القانونية. ورغم أن الجريمة الإلكترونية تشترك مع الجرائم التقليدية في أركانها العامة، إلا أنها تتميز بخصوصيات ناتجة عن طبيعتها التقنية والافتراضية، مما يفرض تحليلًا معمقًا لهذه الأركان في ضوء التشريعات الحديثة والاتفاقيات الدولية.

أولا: الركن المادي للجريمة السيبرانية

يتمثل الركن المادي في السلوك الإجرامي الذي يصدر عن الجاني، والذي قد يأخذ صورًا متعددة في البيئة الرقمية، مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، أو اعتراض البيانات، أو تدميرها أو تعديلها. ويتميز هذا الركن في الجرائم الإلكترونية بكونه يتم عبر وسائل تقنية، مما يجعله غير ملموس في أغلب الأحيان.

وقد نصت **اتفاقية بودابست لسنة 2001** في المادة (2) على أن:

تتخذ كل دولة طرف التدابير التشريعية اللازمة لتجريم الدخول العمدي وغير المشروع إلى نظام معلوماتي.

كما نصت المادة (4) من نفس الاتفاقية على[2]:

1 اتفاقية بودابست لمكافحة الجرائم المعلوماتية، 2001، المواد 2–5 .

2 القانون رقم 09–04، الجزائر، 2009، المادة 2 .

3 قانون العقوبات الجزائري، المادة 394 مكرر.

تجريم إتلاف البيانات أو حذفها أو تعديلها دون وجه حق.

وفي التشريع الجزائري، نص قانون العقوبات في **المادة 394 مكرر** على:

يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة كل من يدخل أو يبقى عن طريق الغش في نظام معلوماتي.

ويلاحظ أن الركن المادي في الجريمة الإلكترونية قد يتحقق بمجرد الفعل دون الحاجة إلى تحقق نتيجة، كما في جريمة الدخول غير المشروع، وهو ما يعكس اتجاها نحو **تجريم الخطر** وليس فقط النتيجة.

كما أن إثبات هذا الركن يطرح صعوبات كبيرة، نظرا لاعتماده على الأدلة الرقمية، التي تتطلب خبرة تقنية خاصة، مثل تحليل السجلات الإلكترونية (Logs) وتتبع عناوين IP.

ثانيا: الركن المعنوي للجريمة السيبرانية

يقوم الركن المعنوي على القصد الجنائي، الذي يتمثل في علم الجاني بالفعل الإجرامي وإرادته في ارتكابه. وتُعد الجرائم الإلكترونية في الغالب جرائم عمدية، حيث يتطلب تنفيذها معرفة تقنية مسبقة.

وقد نصت العديد من التشريعات على ضرورة توافر القصد الجنائي، حيث جاء في الفقه أن "الجريمة المعلوماتية لا تقع غالبًا بطريق الخطأ، بل تتطلب نية إجرامية واضحة"[4].

غير أن بعض الجرائم قد تقع نتيجة الإهمال، مثل تسريب البيانات بسبب ضعف الحماية، مما يثير إشكالية المسؤولية غير العمدية في المجال السيبراني.

ثالثا: الركن الشرعي للجريمة السيبرانية

يقصد بالركن الشرعي وجود نص قانوني يجرّم الفعل، تطبيقًا لمبدأ "لا جريمة ولا عقوبة إلا بنص"، وهو مبدأ أساسي في القانون الجنائي.

وقد عملت التشريعات الحديثة على سد الفراغ القانوني في هذا المجال، حيث:

-أصدر المشرع الجزائري القانون رقم 09-04

-اعتمد المجتمع الدولي اتفاقية بودابست

كما نصت المادة (1) من قانون العقوبات الجزائري على مبدأ الشرعية.

وتبرز أهمية هذا الركن في مواجهة التطور السريع للجريمة الإلكترونية، حيث يجب على المشرع مواكبة المستجدات التقنية باستمرار[1].

1قانون العقوبات الجزائري، المادة 394 مكرر .

2 د الله سليمان، شرح قانون العقوبات، الجزائر، 2015، ص 89 .

الفرع الثالث: خصائص الجريمة السيبرانية

أدى التطور السريع في مجال تكنولوجيا المعلومات والاتصال إلى ظهور نمط جديد من الجرائم يختلف بصورة واضحة عن الجرائم التقليدية المعروفة في القوانين الجنائية الكلاسيكية، وهو ما يعرف بالجريمة الإلكترونية أو السيبرانية وقد أصبحت هذه الجرائم تشكل تهديدا حقيقيا للأفراد والمؤسسات والدول، بالنظر إلى اتساع نطاق استخدامها واعتماد المجتمعات الحديثة بشكل متزايد على الأنظمة الرقمية والشبكات المعلوماتية في مختلف المجالات الاقتصادية والاجتماعية والإدارية والأمنية.

وتتميز الجريمة الإلكترونية بخصائص فريدة تجعلها أكثر تعقيدا وصعوبة من الجرائم التقليدية، سواء من حيث أساليب ارتكابها أو وسائل اكتشافها أو طرق إثباتها ومتابعة مرتكبيها. فهي جرائم تعتمد أساسا على التكنولوجيا الحديثة، وتتم غالبا في بيئة افتراضية لا تعترف بالحدود الجغرافية، الأمر الذي يمنح المجرمين قدرة كبيرة على التخفي وسرعة تنفيذ أفعالهم الإجرامية. كما أن طبيعتها التقنية تجعل من الصعب أحيانا تحديد الجاني أو جمع الأدلة الرقمية المرتبطة بالجريمة.

ومن جهة أخرى، فإن الجرائم الإلكترونية تتميز بسرعة تطورها وتنوع صورها، حيث تتغير أساليب ارتكابها باستمرار تبعا للتطور التكنولوجي، مما يفرض على التشريعات الجنائية والأجهزة الأمنية والقضائية مواكبة مستمرة لهذه التغيرات. كما أن آثارها قد تكون واسعة وخطيرة، إذ يمكن أن تستهدف الأفراد من خلال سرقة بياناتهم الشخصية أو الاحتيال عليهم، وقد تمتد إلى المؤسسات الاقتصادية والمالية أو حتى البنى التحتية الحيوية للدول[1].

وعليه، فإن دراسة خصائص الجريمة الإلكترونية تكتسي أهمية كبيرة لفهم طبيعتها القانونية والتقنية، وإبراز أوجه الاختلاف بينها وبين الجرائم التقليدية، بما يساعد على تطوير آليات فعالة لمكافحتها وتعزيز الحماية القانونية والأمنية في الفضاء الرقمي[2].

[1] عبد الفتاح بيومي حجازي، *الجرائم الإلكترونية في التشريع المقارن*، دار الفكر الجامعي، الطبعة الأولى، 2010، ص 45-48.

[2] عبد الله سليمان، نفس المرجع، ص 90 .

أولا: الطابع غير المادي للجريمة السيبرانية

من أبرز خصائص الجريمة الإلكترونية أنها ذات طبيعة غير مادية، حيث ترتكب في بيئة رقمية افتراضية تعتمد على البيانات والمعلومات الإلكترونية بدلا من الوسائل المادية التقليدية. ففي الجرائم التقليدية يكون محل الجريمة غالبا شيئا ماديا ملموسا، مثل الأموال أو الممتلكات أو الأشخاص، بينما تستهدف الجريمة الإلكترونية البيانات والمعلومات والأنظمة الرقمية، وهي عناصر غير مادية يصعب إدراكها بالحواس المباشرة.

ويظهر هذا الطابع غير المادي في كون الجاني يستخدم وسائل إلكترونية كالحاسوب أو الهاتف الذكي أو الشبكات المعلوماتية لارتكاب أفعاله الإجرامية، دون الحاجة إلى الحضور المادي في مكان الجريمة. فقد يتمكن شخص موجود في دولة معينة من اختراق نظام معلوماتي في دولة أخرى وسرقة بيانات أو تعطيل خدمات دون أن يغادر مكانه.

كما أن الطابع غير المادي للجريمة الإلكترونية ينعكس أيضا على الأدلة المرتبطة بها، إذ تعتمد هذه الجرائم على الأدلة الرقمية التي تتمثل في البيانات الإلكترونية والسجلات الرقمية والرسائل الإلكترونية وآثار الاستخدام المعلوماتي. وتتميز هذه الأدلة بسهولة محوها أو تعديلها أو إخفائها، مما يجعل عملية الإثبات أكثر تعقيدا مقارنة بالجرائم التقليدية.

وقد أدى ذلك إلى ظهور الحاجة إلى وسائل حديثة للتحقيق الجنائي الرقمي، تعتمد على الخبرة التقنية وتحليل البيانات الإلكترونية واسترجاع المعلومات المحذوفة، إضافة إلى تطوير قواعد قانونية تنظم حجية الأدلة الرقمية في الإثبات الجنائي[1].

ثانيا: الطابع العابر للحدود

تعتبر الجريمة **السيبرانية** من الجرائم ذات الطبيعة العابرة للحدود، وذلك بسبب ارتباطها بشبكة الإنترنت التي تسمح بانتقال المعلومات والبيانات بين مختلف دول العالم دون قيود جغرافية. ويعني ذلك أن الجريمة قد ترتكب في دولة معينة بينما تكون آثارها أو ضحاياها أو وسائل تنفيذها موجودة في دول أخرى.

فالمجرم الإلكتروني يستطيع تنفيذ هجوم معلوماتي على أنظمة مصرفية أو مؤسسات حكومية أو شركات أجنبية وهو موجود في مكان بعيد تماما عن موقع الضحية، مستفيدا من سهولة الاتصال بالشبكات

[1] عبد الله سليمان، نفس المرجع، ص 91.

العالمية. كما قد تستخدم خوادم إلكترونية موزعة في عدة دول لإخفاء مصدر الهجوم أو تعقيد عملية تتبع الجاني.

ويؤدي هذا الطابع الدولي إلى إثارة العديد من الإشكالات القانونية، خاصة فيما يتعلق بتحديد الاختصاص القضائي الواجب التطبيق، والقانون الجنائي المختص، وآليات التعاون بين الدول في مجال التحقيق والمتابعة وتسليم المجرمين. كما أن اختلاف التشريعات الوطنية من دولة إلى أخرى قد يشكل عائقا أمام مكافحة هذا النوع من الجرائم.

ولذلك أصبحت مكافحة الجريمة **السيبرانية** تتطلب تعاونا دوليا وإقليميا واسعا، يقوم على تبادل المعلومات والأدلة الرقمية وتوحيد التشريعات وتعزيز آليات المساعدة القضائية بين الدول.

ثالثا: السرعة الفائقة في التنفيذ

من الخصائص المهمة للجريمة **السيبرانية** السرعة الكبيرة التي تتم بها، حيث يمكن تنفيذ عمليات الاختراق أو الاحتيال أو سرقة البيانات خلال ثوان أو دقائق قليلة، بفضل التطور التكنولوجي والقدرات الهائلة التي توفرها الأنظمة المعلوماتية الحديثة.

فالجرائم التقليدية غالبا ما تحتاج إلى وقت وجهد وتحضير مادي، بينما يستطيع المجرم الإلكتروني تنفيذ هجوم واسع النطاق باستخدام برامج متطورة أو فيروسات معلوماتية دون الحاجة إلى تنقل أو احتكاك مباشر بالضحية. وقد تؤدي ضغطة زر واحدة إلى اختراق آلاف الأجهزة أو تعطيل أنظمة إلكترونية كاملة.

كما أن سرعة تنفيذ الجريمة **السيبرانية** تقابلها سرعة انتشار آثارها، خاصة في ظل الترابط الكبير بين الشبكات المعلوماتية العالمية. فالهجمات **السيبرانية** قد تؤثر في وقت قصير على قطاعات حيوية مثل البنوك والمطارات وشبكات الكهرباء والاتصالات والخدمات الحكومية[1].

وتزيد هذه السرعة من صعوبة تدخل الأجهزة الأمنية في الوقت المناسب لمنع وقوع الجريمة أو الحد من آثارها، الأمر الذي يتطلب تطوير وسائل تقنية متقدمة للرصد المبكر والاستجابة السريعة للهجمات السيبرانية[2].

[1] محمود حسنين، *الجرائم الإلكترونية ومخاطرها على الأمن المعلوماتي*، دار النهضة العربية، 2015، ص 88-92.

[2] عبد الله سليمان، نفس المرجع، ص 92.

رابعا: سهولة إخفاء الهوية

تتميز الجريمة **السيبرانية** بإمكانية إخفاء هوية الجاني بدرجة كبيرة، حيث يستطيع المجرمون استخدام وسائل تقنية متعددة لإخفاء مواقعهم الحقيقية أو هوياتهم الشخصية، مثل الشبكات الافتراضية الخاصة وبرامج التشفير والخوادم الوسيطة والحسابات الوهمية.

ويعد هذا الأمر من أخطر التحديات التي تواجه أجهزة الأمن والتحقيق، لأن اكتشاف الفاعل الحقيقي يتطلب خبرات تقنية عالية وتعاونا دوليا بين الجهات المختصة. كما أن بعض المجرمين يستخدمون تقنيات متطورة تسمح بتغيير عناوين الإنترنت الخاصة بهم أو تنفيذ الهجمات عبر أجهزة مخترقة تعود لأشخاص آخرين.

وقد أدى ذلك إلى ارتفاع نسبة الجرائم **السيبرانية** التي تبقى مجهولة المصدر، خاصة عندما ترتكب من قبل جماعات إجرامية منظمة أو شبكات دولية متخصصة في الجرائم السيبرانية.

كما أن سهولة إخفاء الهوية تمنح المجرمين شعورا بالأمان والثقة في الإفلات من العقاب، مما يشجع على تكرار هذه الجرائم وانتشارها بصورة أوسع.[1]

خامسا: صعوبة اكتشاف الجريمة وإثباتها

تعتبر الجريمة **السيبرانية** من الجرائم التي يصعب اكتشافها وإثباتها مقارنة بالجرائم التقليدية، وذلك بسبب طبيعتها التقنية وتعقيد الوسائل المستخدمة في ارتكابها. ففي كثير من الأحيان قد تتعرض الأنظمة المعلوماتية للاختراق أو سرقة البيانات دون أن يلاحظ الضحية ذلك إلا بعد مرور فترة زمنية طويلة.

كما أن آثار الجريمة **السيبرانية** قد تكون غير ظاهرة ماديا، إذ يمكن نسخ البيانات أو سرقتها دون إتلاف الأصل، وهو ما يجعل الضحية أحيانا غير مدرك لوقوع الجريمة. ويضاف إلى ذلك أن الأدلة الرقمية تكون عرضة للتغيير أو المحو بسرعة كبيرة، سواء بفعل الجاني أو نتيجة الاستخدام العادي للأنظمة الإلكترونية[2].

وتتطلب عملية الإثبات في الجرائم **السيبرانية** خبرة تقنية متخصصة لتحليل الأنظمة المعلوماتية واستخراج الأدلة الرقمية وربطها بالجاني. كما تحتاج السلطات القضائية إلى الاستعانة بخبراء في مجال الأمن السيبراني والتحليل الجنائي الرقمي لفهم الجوانب التقنية المرتبطة بالقضية.

[1] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 95-99.
[2] محمد أمين البشري، *التحقيق في الجرائم المعلوماتية*، دار الجامعة الجديدة، 2013، ص 102-106.

وقد أدى ذلك إلى تطور مفهوم الدليل الرقمي واعتماد العديد من التشريعات الحديثة لقواعد خاصة تتعلق بحفظ الأدلة الإلكترونية وضمان سلامتها القانونية.

سادسا: التطور المستمر والتجدد

من الخصائص الأساسية للجريمة **السيبرانية** أنها تتطور باستمرار مع تطور التكنولوجيا الحديثة، حيث تظهر بشكل متواصل أساليب وتقنيات جديدة لارتكاب الجرائم السيبرانية. فكلما تطورت وسائل الحماية والأمن الإلكتروني، يسعى المجرمون إلى ابتكار طرق أكثر تعقيدا لتجاوزها[1].

ويشمل هذا التطور استخدام تقنيات الذكاء الاصطناعي، والبرمجيات الخبيثة المتقدمة، وهجمات الفدية الإلكترونية، ووسائل التصيد الاحتيالي الحديثة، إضافة إلى استغلال العملات الرقمية في عمليات غسل الأموال والابتزاز الإلكتروني.

كما أن تطور الجريمة **السيبرانية** يؤدي إلى تنوع صورها واتساع مجالاتها، بحيث لم تعد تقتصر على اختراق الأنظمة وسرقة البيانات، بل أصبحت تشمل جرائم تمس الاقتصاد والأمن القومي والحياة الخاصة وحقوق الملكية الفكرية.

ويفرض هذا التطور المستمر على الدول ضرورة تحديث تشريعاتها الجنائية بصورة دائمة، وتطوير قدرات أجهزتها الأمنية والقضائية، وتعزيز التعاون الدولي لمواجهة التهديدات السيبرانية المستجدة[2].

سابعا: ضخامة الأضرار والخسائر

تتميز الجريمة **السيبرانية** بإمكانية إحداث أضرار جسيمة قد تتجاوز بكثير آثار الجرائم التقليدية، سواء من الناحية الاقتصادية أو الأمنية أو الاجتماعية. فالهجمات السيبرانية قد تؤدي إلى خسائر مالية ضخمة نتيجة سرقة الأموال أو تعطيل الأنظمة البنكية والتجارية، كما قد تؤثر على سمعة المؤسسات وثقة العملاء فيها.

وقد تمتد آثار الجريمة **السيبرانية** إلى البنى التحتية الحيوية للدول، مثل شبكات الطاقة والمياه والاتصالات والمطارات والمستشفيات، الأمر الذي قد يهدد الأمن القومي والاستقرار العام. كما يمكن أن تؤدي بعض الهجمات الإلكترونية إلى تسريب معلومات حساسة أو بيانات شخصية، مما يشكل انتهاكا خطيرا للخصوصية.

---

[1] عبد الفتاح بيومي حجازي، *الجرائم الإلكترونية في التشريع المقارن*، دار الفكر الجامعي، الطبعة الأولى، 2010، ص 52-56.

[2] عبد الله سليمان، نفس المرجع، ص 93.

ومن الناحية الاجتماعية، ساهمت الجرائم **السيبرانية** في انتشار ظواهر خطيرة مثل الابتزاز الإلكتروني والتنمر الرقمي والاحتيال عبر الإنترنت، وهي جرائم تؤثر بشكل مباشر على الأفراد وخاصة فئة الشباب والأطفال.

ولذلك أصبحت الجريمة **السيبرانية** تمثل تحديا أمنيا وقانونيا عالميا يستوجب تضافر جهود الدول والمنظمات الدولية والإقليمية من أجل الحد من آثارها وتعزيز الأمن السيبراني.

وهناك خصائص تبعية أخرى كالاتي:

أولا: الطابع العابر للحدود

وتعد الجريمة **السيبرانية** جريمة دولية بطبيعتها، حيث يمكن أن يرتكبها شخص في دولة معينة، بينما تقع آثارها في دولة أخرى. وهذا ما أكدت عليه **اتفاقية بودابست** التي دعت إلى التعاون الدولي في هذا المجال.

ويطرح هذا الطابع إشكالات تتعلق بالاختصاص القضائي وتنازع القوانين.

ثانيا: صعوبة الاكتشاف والإثبات

ترتكب الجرائم **السيبرانية** في بيئة رقمية، مما يجعل اكتشافها صعبًا، خاصة مع استخدام تقنيات التشفير وإخفاء الهوية. كما أن الأدلة تكون رقمية وقابلة للتغيير، مما يتطلب خبرات تقنية متقدمة.

وقد نص القانون الجزائري 09-04 على إجراءات خاصة للتحري، مثل تفتيش الأنظمة المعلوماتية.

ثالثا: السرعة والتطور المستمر

تتميز هذه الجرائم بسرعة تنفيذها، حيث يمكن اختراق نظام في ثوانٍ، كما أنها تتطور باستمرار مع تطور التكنولوجيا، مما يجعل مكافحتها تحديا دائما.

رابعا: انخفاض التكلفة وارتفاع العائد

لا تتطلب الجريمة **السيبرانية** موارد كبيرة، بل يكفي حاسوب واتصال بالإنترنت، في حين قد تحقق أرباحًا كبيرة، كما في جرائم الاحتيال الإلكتروني

خامسا: الطابع التقني

تعتمد الجريمة **السيبرانية** على مهارات تقنية، مما يجعل مرتكبيها غالبًا من ذوي الخبرة في مجال تكنولوجيا المعلومات[1].

15. مير عبد السيد تناغو، الجرائم المعلوماتية، دار الفكر، مصر، 2012، ص 102 .

المطلب الثاني: مراحل تطور الجريمة السيبرانية وأنواعها

تمهيد:

شهد العالم خلال العقود الأخيرة ثورة تكنولوجية هائلة مست مختلف مجالات الحياة، حيث أصبح الاعتماد على الحواسيب والأنظمة الرقمية وشبكات الإنترنت أمرا ضروريا في المعاملات الاقتصادية والإدارية والاجتماعية والأمنية. وقد ساهم هذا التطور التقني في تسهيل الاتصال وتبادل المعلومات وتحسين الخدمات، إلا أنه في المقابل أفرز تحديات جديدة تمثلت في ظهور أنماط إجرامية حديثة استغلت البيئة الرقمية والتقنيات المعلوماتية لتحقيق أهداف غير مشروعة.

ولم تنشأ الجريمة **السيبرانية** في صورتها الحالية بشكل مفاجئ، بل مرت بعدة مراحل تطورية ارتبطت ارتباطا وثيقا بالتقدم التكنولوجي وتوسع استخدام الحواسيب والشبكات المعلوماتية. ففي بدايات ظهور الحاسوب كانت الجرائم المعلوماتية محدودة وبسيطة، وتقتصر غالبا على بعض الأفعال الفردية التي تستهدف اختراق الأنظمة أو العبث بالبرمجيات بدافع الفضول أو التحدي التقني. غير أن التطور المتسارع للتكنولوجيا وانتشار الإنترنت على نطاق عالمي أدى إلى توسع نطاق هذه الجرائم وتحولها إلى ظاهرة إجرامية معقدة تمارسها أحيانا جماعات إجرامية منظمة تمتلك قدرات تقنية عالية.

ومع دخول العالم عصر الاقتصاد الرقمي والتجارة الإلكترونية والخدمات البنكية عبر الإنترنت، ازدادت فرص استغلال التكنولوجيا في ارتكاب جرائم متنوعة تمس الأفراد والمؤسسات والدول، مثل الاحتيال الإلكتروني، وسرقة البيانات، والتجسس السيبراني، وغسل الأموال الرقمية، والهجمات على البنى التحتية الحيوية. كما ساهم ظهور تقنيات حديثة كالذكاء الاصطناعي والعملات الرقمية والحوسبة السحابية في تعقيد المشهد الإجرامي السيبراني وظهور أساليب أكثر تطورا وخطورة[1].

وأمام هذا التنوع الكبير في صور الجريمة **السيبرانية** ، أصبح من الضروري تصنيف هذه الجرائم وفق معايير قانونية وتقنية متعددة، بهدف فهم طبيعتها وتحديد خصائصها وآليات مكافحتها. فالتصنيف يساعد على وضع سياسات جنائية متخصصة، وتطوير التشريعات الملائمة، وتعزيز قدرات أجهزة الأمن والقضاء في التعامل مع هذا النوع من الجرائم.

[1] عبد الفتاح بيومي حجازي، *أمن المعلومات والجرائم الإلكترونية*، دار الفكر الجامعي، الطبعة الأولى، 2007، ص 143-149.

وعليه، فإن دراسة تطور الجريمة **السيبرانية** وتصنيفاتها تكتسي أهمية كبيرة لفهم التحولات التي عرفها هذا النوع من الإجرام، وإبراز مختلف صوره وأشكاله، بما يسهم في بناء منظومة قانونية وأمنية قادرة على مواجهة التهديدات السيبرانية المتزايدة[1].

الفرع الأول: مراحل تطور الجريمة السيبرانية

أولا: مرحلة الظهور الأول للحواسيب

تعود البدايات الأولى للجريمة **السيبرانية** إلى الفترة التي ظهر فيها استخدام الحواسيب الإلكترونية في المؤسسات الحكومية والعسكرية والجامعات خلال ستينيات وسبعينيات القرن العشرين. ففي تلك المرحلة كانت الحواسيب تستخدم بصورة محدودة جدا، وكانت تكلفتها مرتفعة، الأمر الذي جعل استخدامها مقتصرا على جهات معينة تمتلك الإمكانيات التقنية والمالية.

وخلال هذه المرحلة، لم تكن الجرائم المعلوماتية تمثل خطرا كبيرا، إذ اقتصرت غالبا على بعض الأفعال الفردية التي يقوم بها موظفون أو مبرمجون داخل المؤسسات، مثل التلاعب بالبيانات أو استخدام الحاسوب لأغراض غير مشروعة. كما ظهرت بعض محاولات الاختراق البسيطة بدافع الفضول والرغبة في اكتشاف الأنظمة المعلوماتية أكثر من كونها تهدف إلى تحقيق مكاسب مالية أو إجرامية[2].

وكانت أغلب الجرائم في هذه الفترة تتم داخل نفس المؤسسة التي يوجد بها النظام المعلوماتي، نظرا لعدم وجود شبكات اتصال واسعة تربط الحواسيب ببعضها. ولذلك كانت الجرائم المعلوماتية ذات طابع محلي ومحدود الأثر مقارنة بما هو عليه الحال في الوقت الراهن.

كما أن التشريعات الجنائية في تلك المرحلة لم تكن تتضمن نصوصا خاصة بالجرائم المعلوماتية، لأن المشرعين لم يكونوا يتوقعون حجم التطور الذي ستشهده التكنولوجيا مستقبلا. ولهذا كانت بعض الأفعال الإجرامية المرتبطة بالحاسوب تواجه صعوبات قانونية فيما يتعلق بالتكييف الجنائي والإثبات[3].

---

[1] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 54-59.
[2] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 31-35.
[3] ممدوح إبراهيم، *الجرائم المعلوماتية*، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص 91.

ثانيا: مرحلة انتشار الشبكات المعلوماتية

مع بداية الثمانينيات والتسعينيات، شهد العالم تطورا ملحوظا في مجال الاتصالات والشبكات المعلوماتية، حيث بدأت الحواسيب ترتبط فيما بينها من خلال شبكات داخلية وخارجية، مما أدى إلى توسيع نطاق استخدام التكنولوجيا في المؤسسات الاقتصادية والإدارية والتعليمية[1].

وقد ساهم هذا التطور في ظهور أشكال جديدة من الجرائم **السيبرانية** ، خاصة مع تزايد عدد المستخدمين وارتفاع حجم البيانات المتبادلة عبر الشبكات. وأصبحت عمليات الاختراق المعلوماتي أكثر انتشارا، كما ظهرت الفيروسات والبرمجيات الخبيثة التي تستهدف الأنظمة الإلكترونية وتعمل على تعطيلها أو إتلاف بياناتها.

وفي هذه المرحلة، بدأ المجرمون يدركون الإمكانيات الكبيرة التي توفرها التكنولوجيا لتحقيق مكاسب غير مشروعة، فظهرت جرائم سرقة المعلومات البنكية والتلاعب بالأنظمة المالية، بالإضافة إلى استخدام الحواسيب في عمليات الاحتيال والتزوير الإلكتروني.

كما ساهم انتشار الشبكات المعلوماتية في انتقال الجريمة **السيبرانية** من الطابع المحلي إلى الطابع العابر للحدود، حيث أصبح بإمكان الجاني تنفيذ هجمات إلكترونية ضد أهداف موجودة في دول أخرى دون الحاجة إلى التنقل الجغرافي[2].

وأمام تزايد هذه الجرائم، بدأت الدول تدرك ضرورة تطوير تشريعات خاصة بالجرائم المعلوماتية، وإنشاء وحدات أمنية متخصصة في مكافحة الجرائم **السيبرانية** والتحقيق في الأدلة الرقمية[3].

ثالثا: مرحلة انتشار الإنترنت والعولمة الرقمية

تعتبر مرحلة انتشار الإنترنت خلال نهاية التسعينيات وبداية الألفية الجديدة نقطة تحول أساسية في تطور الجريمة **السيبرانية** ، إذ أدى الاستخدام الواسع لشبكة الإنترنت إلى توسع غير مسبوق في حجم المعاملات الإلكترونية والخدمات الرقمية.

---

[1] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 40-44.
[2] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 78-83.
[3] ممدوح إبراهيم، نفس المرجع، ص 92.

فقد أصبحت التجارة الإلكترونية والخدمات البنكية والتعليم الإلكتروني ووسائل التواصل الاجتماعي جزءا أساسيا من الحياة اليومية، وهو ما وفر للمجرمين فرصا جديدة لاستغلال الفضاء الرقمي في ارتكاب جرائم متنوعة.

وخلال هذه المرحلة، ظهرت جرائم أكثر تعقيدا مثل الاحتيال الإلكتروني، والتصيد الاحتيالي، وسرقة الهوية الرقمية، والابتزاز الإلكتروني، إضافة إلى الهجمات **السيبرانية** التي تستهدف المواقع الحكومية والمؤسسات المالية الكبرى.

كما شهدت هذه الفترة بروز جماعات إجرامية منظمة تعمل في مجال الجرائم السيبرانية، حيث أصبحت بعض الشبكات الإجرامية تعتمد على التكنولوجيا الرقمية كمصدر رئيسي لتحقيق الأرباح غير المشروعة، سواء من خلال سرقة البيانات أو ابتزاز الضحايا أو الاتجار بالمعلومات المسروقة[1].

وقد دفعت خطورة هذه الجرائم المجتمع الدولي إلى تعزيز التعاون الدولي في مجال مكافحة الجريمة **السيبرانية** ، وهو ما تجسد في اعتماد العديد من الاتفاقيات الدولية والإقليمية، وعلى رأسها اتفاقية بودابست لمكافحة الجريمة **السيبرانية**[2].

رابعا: مرحلة الجرائم السيبرانية المنظمة

مع التطور المتسارع للتكنولوجيا الحديثة خلال السنوات الأخيرة، دخلت الجريمة **السيبرانية** مرحلة أكثر خطورة وتعقيدا، حيث أصبحت تمارس من قبل جماعات إجرامية منظمة تمتلك خبرات تقنية عالية وإمكانات مالية كبيرة.

وقد ارتبطت هذه المرحلة بظهور تقنيات حديثة مثل الذكاء الاصطناعي، والعملات الرقمية، والحوسبة السحابية، وإنترنت الأشياء، وهي تقنيات ساهمت في تطوير أساليب الجرائم السيبرانية وجعلها أكثر تعقيدا وصعوبة في الاكتشاف[3].

[1] عبد الفتاح بيومي حجازي، *أمن المعلومات والجرائم الإلكترونية*، دار الفكر الجامعي، الطبعة الأولى، 2007، ص 154-158.
[2] سعيد نمور، *شرح الجرائم الواقعة على نظم المعلومات*، دار الثقافة، عمان، الأردن، 2014، ص 88.
[3] عبد الفتاح بيومي حجازي، *الجرائم الإلكترونية في التشريع المقارن*، دار الفكر الجامعي، الطبعة الأولى، 2010، ص 171-176.

ومن أبرز الجرائم التي ظهرت في هذه المرحلة هجمات الفدية الإلكترونية، التي تقوم على تشفير بيانات الضحايا ومطالبتهم بدفع مبالغ مالية مقابل استرجاعها، بالإضافة إلى الهجمات السيبرانية التي تستهدف البنى التحتية الحيوية للدول، مثل شبكات الكهرباء والمياه والمطارات والمؤسسات الصحية.

كما أصبحت بعض الدول تستخدم الفضاء السيبراني في عمليات التجسس الإلكتروني والهجمات الرقمية التي تستهدف دولا أخرى، مما أدى إلى تحول الجريمة الإلكترونية إلى تهديد للأمن القومي والدولي.

وأدى هذا الوضع إلى تزايد الاهتمام بمفهوم الأمن السيبراني، وضرورة تطوير استراتيجيات وطنية ودولية لحماية الفضاء الرقمي ومواجهة التهديدات السيبرانية المتزايدة[1].

الفرع الثاني: أنواع الجريمة السيبرانية

أولا: الجرائم الماسة بالأنظمة المعلوماتية

يقصد بهذا النوع من الجرائم الأفعال التي تستهدف الأنظمة والشبكات المعلوماتية ذاتها، مثل عمليات الاختراق غير المشروع، وتعطيل الأنظمة الإلكترونية، وإتلاف البيانات أو تعديلها دون ترخيص.

وتشمل هذه الجرائم أيضا نشر الفيروسات والبرمجيات الخبيثة، والهجمات التي تهدف إلى شل عمل المواقع الإلكترونية أو الخوادم الرقمية. وتعتبر هذه الجرائم من أخطر الجرائم الإلكترونية لأنها قد تؤدي إلى تعطيل مؤسسات حيوية وإلحاق خسائر اقتصادية وأمنية جسيمة.

ثانيا: الجرائم الماسة بالأموال والمعاملات الإلكترونية

تشمل هذه الفئة الجرائم التي تستهدف الأموال والمعاملات المالية المنجزة عبر الوسائط الإلكترونية، مثل الاحتيال الإلكتروني، وسرقة البطاقات البنكية، والتلاعب بالحسابات المصرفية، وغسل الأموال باستخدام الوسائل الرقمية.

[1] عبد الفتاح بيومي حجازي، *أمن المعلومات والجرائم الإلكترونية*، دار الفكر الجامعي، الطبعة الأولى، 2007، ص 201-206.

وقد ازدادت هذه الجرائم بشكل كبير مع انتشار التجارة الإلكترونية والخدمات البنكية عبر الإنترنت، حيث يستغل المجرمون ضعف الوعي الأمني لدى بعض المستخدمين للحصول على بياناتهم المالية واستعمالها بطرق غير مشروعة[1].

كما أن تطور العملات الرقمية ساهم في ظهور أساليب جديدة لغسل الأموال والابتزاز المالي عبر الفضاء السيبراني[2].

ثالثا: الجرائم الماسة بالأشخاص

يقصد بها الجرائم التي تستهدف الأفراد وحقوقهم الشخصية عبر الوسائل الإلكترونية، مثل انتهاك الخصوصية، وسرقة الهوية الرقمية، والتشهير الإلكتروني، والابتزاز الرقمي، والتنمر عبر الإنترنت.

وقد أصبحت هذه الجرائم منتشرة بشكل واسع بسبب الاستخدام المكثف لوسائل التواصل الاجتماعي والتطبيقات الرقمية، حيث يمكن للمجرمين استغلال البيانات والصور والمعلومات الشخصية للإضرار بالضحايا أو ابتزازهم.

كما تشمل هذه الفئة الجرائم المتعلقة باستغلال الأطفال عبر الإنترنت ونشر المحتويات غير المشروعة، وهي من الجرائم التي تحظى باهتمام دولي كبير نظرا لخطورتها على المجتمع.

رابعا: الجرائم الماسة بأمن الدولة والمجتمع

تعد هذه الجرائم من أخطر أنواع الجرائم الإلكترونية، لأنها تستهدف المؤسسات الحكومية والبنى التحتية الحيوية والأمن القومي للدول، وتشمل عمليات التجسس الإلكتروني، والهجمات السيبرانية على الأنظمة العسكرية أو الأمنية، ونشر المعلومات السرية، إضافة إلى استخدام الإنترنت في دعم الإرهاب أو التحريض على العنف.[2]

وقد أصبحت الدول تعتبر الأمن السيبراني جزءا أساسيا من أمنها القومي، خاصة في ظل تزايد الهجمات الإلكترونية التي قد تؤدي إلى تعطيل الخدمات الأساسية أو تهديد الاستقرار السياسي والاقتصادي.

---

[1] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 119-124.

[2] علي عبد القادر القهوجي، *القانون الجنائي والتكنولوجيا الحديثة*، منشورات الحلبي الحقوقية، بيروت، لبنان، 2015، ص 109.

كما أن الجماعات الإرهابية والتنظيمات الإجرامية أصبحت تستغل الفضاء الرقمي في التجنيد والتواصل ونشر الدعاية المتطرفة، مما يزيد من خطورة الجرائم السيبرانية على الأمن الدولي.

المبحث الثاني: ماهية الأمن السيبراني

المطلب الأول: مفهوم الأمن السيبراني ونشأته

تمهيد

أصبح الأمن السيبراني من أهم المفاهيم المرتبطة بالعصر الرقمي، نظرا للتطور الكبير الذي شهدته وسائل الاتصال الحديثة واعتماد الأفراد والمؤسسات والدول على الأنظمة المعلوماتية في مختلف المجالات. فمع تزايد استخدام الإنترنت والخدمات الرقمية، ظهرت تهديدات إلكترونية متعددة تستهدف البيانات والشبكات والأنظمة الحساسة، مما جعل الحاجة إلى توفير الحماية الرقمية ضرورة حتمية للحفاظ على الأمن والاستقرار[1].

ولم يعد الأمن السيبراني مجرد مسألة تقنية تقتصر على حماية الحواسيب والبرمجيات، بل أصبح يشمل أبعادا قانونية واقتصادية وأمنية واستراتيجية، بالنظر إلى خطورة الهجمات السيبرانية وتأثيرها على الأفراد والمؤسسات وحتى الأمن القومي للدول. وقد دفعت هذه التحديات الدول والمنظمات الدولية إلى تطوير سياسات واستراتيجيات متخصصة تهدف إلى تعزيز حماية الفضاء الرقمي ومواجهة التهديدات الإلكترونية المتزايدة.

وعليه، فإن دراسة مفهوم الأمن السيبراني ونشأته تكتسي أهمية كبيرة لفهم طبيعة هذا المجال وتحديد أهدافه ووسائل تحقيقه، وهو ما سيتم تناوله من خلال تعريف الأمن السيبراني وبيان مراحل نشأته وتطوره.

الفرع الأول: تعريف الأمن السيبراني

يعد الأمن السيبراني من المفاهيم الحديثة التي ارتبط ظهورها بالتطور التكنولوجي المتسارع وانتشار استخدام الأنظمة الرقمية وشبكات الإنترنت في مختلف مجالات الحياة. ويقصد بالأمن السيبراني مجموعة التدابير والإجراءات التقنية والقانونية والتنظيمية التي تهدف إلى حماية الأنظمة المعلوماتية والشبكات والبيانات من الاختراق أو الهجمات أو أي استعمال غير مشروع[2].

ويعرف الأمن السيبراني لغة بأنه الأمن المرتبط بالفضاء السيبراني، أي البيئة الرقمية التي تضم الحواسيب والشبكات والأنظمة الإلكترونية المتصلة ببعضها عبر وسائل الاتصال الحديثة. أما

[1] سامي الشريف، *الأمن السيبراني وحماية المعلومات في العصر الرقمي*، دار التعليم الجامعي، الطبعة الأولى، 2021، ص 22-27.
[2] خالد ممدوح إبراهيم، *أمن المعلومات والشبكات*، دار الفكر الجامعي، 2019، ص 18-22.

اصطلاحا، فيقصد به حماية المعلومات والأنظمة الرقمية من التهديدات الإلكترونية التي قد تؤثر على سريتها أو سلامتها أو استمرارية عملها.

وقد عرفت المنظمة الدولية للاتصالات الأمن السيبراني بأنه مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات والتقنيات المستخدمة لحماية البيئة السيبرانية والمستخدمين والأصول الرقمية. كما عرفه بعض الفقه بأنه جميع الوسائل الرامية إلى حماية البيانات والشبكات من الوصول غير المشروع أو التدمير أو التعديل أو التعطيل.

ويقوم الأمن السيبراني على مجموعة من المبادئ الأساسية، تتمثل في:

- السرية: وتعني حماية المعلومات من الوصول غير المصرح به.
- السلامة: أي ضمان عدم التلاعب بالبيانات أو تعديلها بطريقة غير مشروعة.
- التوافر: ويقصد به ضمان استمرار عمل الأنظمة والخدمات الرقمية بصورة طبيعية.

كما يشمل الأمن السيبراني عدة مجالات، من بينها حماية الشبكات، وأمن المعلومات، وأمن التطبيقات، وحماية البنية التحتية الرقمية، إضافة إلى مكافحة الجرائم السيبرانية والهجمات الإلكترونية.

وتبرز أهمية الأمن السيبراني في كونه يمثل وسيلة أساسية لحماية الأفراد والمؤسسات والدول من المخاطر الإلكترونية، خاصة في ظل الاعتماد المتزايد على الاقتصاد الرقمي والخدمات الإلكترونية. كما أصبح يشكل جزءا مهما من الأمن القومي للدول، بالنظر إلى خطورة الهجمات التي قد تستهدف البنى التحتية الحيوية[1].

الفرع الثاني: نشأة الأمن السيبراني

ارتبطت نشأة الأمن السيبراني بتطور استخدام الحواسيب والأنظمة المعلوماتية خلال النصف الثاني من القرن العشرين، حيث ظهرت الحاجة إلى حماية البيانات الإلكترونية من التلاعب أو الاختراق مع بداية استخدام الحواسيب في المؤسسات الحكومية والعسكرية.

وفي المراحل الأولى، كانت وسائل الحماية بسيطة ومحدودة، نظرا لكون استخدام الحواسيب كان مقتصرا على عدد محدود من الجهات. غير أن التطور السريع في مجال الاتصالات وظهور

[1] سامي الشريف، *الأمن السيبراني وحماية المعلومات في العصر الرقمي*، دار التعليم الجامعي، الطبعة الأولى، 2021، ص 33-38.

الشبكات المعلوماتية أدى إلى اتساع نطاق المخاطر الإلكترونية، مما استدعى تطوير وسائل أكثر فعالية لحماية الأنظمة الرقمية.

ومع انتشار شبكة الإنترنت خلال التسعينيات، ازدادت التهديدات السيبرانية بصورة كبيرة، حيث ظهرت الفيروسات الإلكترونية وبرامج الاختراق وعمليات سرقة البيانات، وهو ما دفع المؤسسات والدول إلى الاهتمام بشكل أكبر بأمن المعلومات وحماية الشبكات.

كما شهدت بداية الألفية الجديدة تطورا كبيرا في مجال الأمن السيبراني، نتيجة تصاعد الهجمات الإلكترونية التي استهدفت المؤسسات المالية والحكومية، إضافة إلى ظهور جماعات متخصصة في الجرائم السيبرانية. وقد أدى ذلك إلى إنشاء هيئات ومراكز متخصصة في الأمن السيبراني، وإصدار تشريعات وطنية واتفاقيات دولية تهدف إلى تعزيز حماية الفضاء الرقمي.

وفي السنوات الأخيرة، أصبح الأمن السيبراني من الأولويات الاستراتيجية للدول، خاصة مع تطور تقنيات الذكاء الاصطناعي والحوسبة السحابية وإنترنت الأشياء، وهي تقنيات ساهمت في تعقيد التهديدات الإلكترونية وظهور أنماط جديدة من الهجمات السيبرانية.

كما سعت العديد من الدول إلى وضع استراتيجيات وطنية للأمن السيبراني تهدف إلى حماية البنية التحتية الرقمية وتعزيز قدرات المؤسسات والأفراد على مواجهة المخاطر الإلكترونية، وهو ما يعكس الأهمية المتزايدة لهذا المجال في العصر الحديث.

المطلب الثاني: الأمن السيبراني بين المخاطر والأبعاد

تمهيد

أدى التطور الهائل في مجال التكنولوجيا الرقمية إلى بروز تحديات جديدة فرضت نفسها على مختلف الدول والمؤسسات، حيث أصبحت الأنظمة المعلوماتية والشبكات الإلكترونية عرضة لهجمات وتهديدات متزايدة تمس أمن البيانات والمعلومات والخدمات الرقمية. وقد نتج عن هذا الواقع تنامي الاهتمام بالأمن السيبراني باعتباره وسيلة أساسية لحماية الفضاء الرقمي وضمان استمرارية الأنشطة الإلكترونية.

غير أن الأمن السيبراني لا يقتصر فقط على الجانب التقني المرتبط بحماية الأنظمة والشبكات، بل يمتد ليشمل أبعادا اقتصادية واجتماعية وقانونية وأمنية وسياسية، نظرا لتأثير الهجمات السيبرانية

على مختلف القطاعات الحيوية. كما أن المخاطر الإلكترونية أصبحت أكثر تعقيدا مع تطور وسائل الاختراق والهجمات الرقمية، الأمر الذي يستوجب تطوير آليات فعالة للوقاية والاستجابة.

وعليه، فإن دراسة الأمن السيبراني تقتضي التطرق إلى أهم التهديدات والمخاطر المرتبطة به، إضافة إلى بيان مختلف أبعاده وانعكاساته على الأفراد والمؤسسات والدول.

الفرع الأول: تهديدات ومخاطر حوادث الأمن السيبراني

تشهد البيئة الرقمية في الوقت الراهن تزايدا مستمرا في حجم التهديدات السيبرانية، نتيجة الاعتماد المتزايد على الأنظمة المعلوماتية والشبكات الإلكترونية في مختلف مجالات الحياة. وتتمثل هذه التهديدات في مجموعة من الهجمات والأفعال غير المشروعة التي تستهدف البيانات والأنظمة والخدمات الرقمية، مما قد يؤدي إلى أضرار اقتصادية وأمنية واجتماعية خطيرة.

ومن أبرز هذه التهديدات الهجمات الإلكترونية التي تستهدف اختراق الأنظمة المعلوماتية وسرقة البيانات الحساسة، سواء تعلق الأمر بالبيانات الشخصية للأفراد أو المعلومات السرية الخاصة بالمؤسسات والدول. كما تشمل هذه الهجمات نشر البرمجيات الخبيثة والفيروسات الإلكترونية التي تعمل على تعطيل الأنظمة أو إتلاف البيانات.

وتعد هجمات الفدية الإلكترونية من أخطر التهديدات الحديثة، حيث يقوم المهاجمون بتشفير بيانات الضحايا ومنعهم من الوصول إليها، ثم مطالبتهم بدفع مبالغ مالية مقابل استرجاعها. وقد استهدفت هذه الهجمات العديد من المؤسسات الصحية والمالية والإدارية في مختلف دول العالم.

كما تبرز مخاطر الاحتيال الإلكتروني والتصيد الاحتيالي، حيث يستغل المجرمون الوسائل الرقمية لخداع المستخدمين والحصول على بياناتهم البنكية أو معلوماتهم الشخصية. وقد ساهم انتشار وسائل التواصل الاجتماعي والخدمات البنكية الإلكترونية في زيادة هذا النوع من الجرائم.

ومن جهة أخرى، تشكل الهجمات التي تستهدف البنى التحتية الحيوية خطرا كبيرا على الأمن القومي للدول، خاصة إذا استهدفت شبكات الكهرباء أو المياه أو الاتصالات أو الأنظمة العسكرية. كما أن استخدام الفضاء الرقمي في التجسس الإلكتروني ونشر المعلومات المضللة يزيد من تعقيد التهديدات السيبرانية[1].

[1] عبد الرؤوف مهدي، *الأمن السيبراني وحماية الأنظمة المعلوماتية*، المركز القومي للإصدارات القانونية، 2021، ص 112-118.

وتؤدي هذه المخاطر إلى خسائر مالية ضخمة، إضافة إلى التأثير على الثقة في الأنظمة الرقمية والخدمات الإلكترونية. ولذلك أصبح من الضروري تطوير استراتيجيات فعالة للأمن السيبراني تقوم على الوقاية والكشف المبكر والاستجابة السريعة للهجمات الإلكترونية.

الفرع الثاني: أبعاد الأمن السيبراني

لا يقتصر الأمن السيبراني على البعد التقني فقط، بل يشمل مجموعة من الأبعاد المتكاملة التي ترتبط بحماية المجتمع والدولة والاقتصاد في البيئة الرقمية.

أولا: البعد الأمني

يتمثل البعد الأمني في حماية الأنظمة المعلوماتية والبنى التحتية الرقمية من الهجمات الإلكترونية والاختراقات التي قد تهدد استقرار الدول والمؤسسات .وقد أصبح الأمن السيبراني جزءا أساسيا من الأمن القومي، خاصة في ظل تصاعد الهجمات التي تستهدف القطاعات الحيوية.

ثانيا: البعد القانوني

يقوم البعد القانوني على وضع تشريعات وقوانين تنظم استخدام الفضاء الرقمي وتجرم الأفعال غير المشروعة المرتبطة به. كما يشمل تطوير آليات التعاون القضائي الدولي لمواجهة الجرائم السيبرانية العابرة للحدود.

ثالثا: البعد الاقتصادي

يرتبط الأمن السيبراني بحماية الأنشطة الاقتصادية والمعاملات الإلكترونية من المخاطر الرقمية، حيث إن أي اختراق أو هجوم إلكتروني قد يؤدي إلى خسائر مالية كبيرة ويؤثر على استقرار الأسواق وثقة المستثمرين.

رابعا: البعد الاجتماعي

يهدف هذا البعد إلى حماية الأفراد والمجتمع من المخاطر المرتبطة باستخدام الإنترنت ووسائل التواصل الاجتماعي، مثل الابتزاز الإلكتروني والتنمر الرقمي وانتهاك الخصوصية. كما يشمل نشر الوعي الرقمي وتعزيز ثقافة الاستخدام الآمن للتكنولوجيا[1].

[1] عبد الرؤوف مهدي، *الأمن السيبراني وحماية الأنظمة المعلوماتية*، المركز القومي للإصدارات القانونية، 2021، ص 146-150.

خامسا: البعد التقني

ويتمثل في استخدام الوسائل والتقنيات الحديثة لحماية الأنظمة والشبكات والبيانات، مثل برامج الحماية والتشفير وأنظمة كشف الاختراق والجدران النارية. كما يعتمد على تطوير الكفاءات والخبرات التقنية القادرة على مواجهة التهديدات السيبرانية[1].

سادسا: البعد الدولي

نظرا للطابع العابر للحدود الذي تتميز به الجرائم والهجمات السيبرانية، أصبح التعاون الدولي أمرا ضروريا لمواجهة التهديدات الرقمية. ويشمل ذلك تبادل المعلومات والخبرات بين الدول، وإبرام الاتفاقيات الدولية المتعلقة بالأمن السيبراني ومكافحة الجرائم الإلكترونية.

ومن خلال ما سبق، يتضح أن الأمن السيبراني يمثل منظومة متكاملة تتداخل فيها الجوانب التقنية والقانونية والأمنية والاقتصادية والاجتماعية، الأمر الذي يفرض على الدول والمؤسسات اعتماد سياسات شاملة وفعالة لضمان حماية الفضاء الرقمي وتعزيز الأمن والاستقرار في العصر الرقمي.

المبحث الثالث ": التكييف القانوني للمجرم السيبراني

يتميز المحرم السيبراني بطبيعة افتراضية عابرة للحدود ، لا يستند إلى أي حضور مادي حينما يرتكب حرائمه باعتباره مستند إلى الوسائل الرقمية و الوسائل التكنولوجية الحديثة حيث يمتاز بالذكاء التقني الكبير و القدرة على التخفي تحت هويات وهمية يصعب الوصول إليها مما يتيح له التفلة من المتابعة الأمنية ، تثير هذه الطبيعة إشكالية في تحديد هوية هذا النوع من المجرمين و تنازع الاختصاص القضائي الدولي ، مما يخرجه من من النمط التقليدي من المجرمين و يفرضه كفاعل ذي خصوصية جنائية مستقلة

المطلب الأول: المجرم السيبراني في عرف القانون الدولي :

هو مجرم يتمتع بقدر عال من الذكاء يمكنه من اختراق أي شبكة الكترونية و فك الشفرات و كلمات المرور بما لديه من تقنيات تخزين الالبيانات و التحكم في أنظمة الشبكات ، و تثبت الدراسات النفسية الجنائية أن المحرم السيبراني ليس لديه أي شعور بشناعة ما يرتكبه من الجرائم مثله مثل أي مجرم تقليدي و الغريب أنهم في الكثير من الحالات يحوزون على مكانة اجتماعية [2]

[1] خالد ممدوح إبراهيم، *أمن المعلومات والشبكات*، دار الفكر الجامعي، 2019، ص 73-78.

المطلب الثاني: خصائص المجرم السيبراني :

يتميز المجرم السيبراني بالعديد من الخصائص نذكر أهمها :

1. **الذكاء الحاد :** يحوز هذا النوع من المجرمين على قدرة غير تقليدية من الذكاء أهلته لبلوغ هذا المستوى من التقنية الحديثة و هو ما يتيح له التحكم فبما يريده من شبكات مهما تعقدت صعوبتها
2. **مجرم مدمن على ارتكاب جرائم مماثلة متجددة :** تحقيق نجاحات في فك شبكات جديدة تجعله دائم السعي إلى تحقيق المزيد من العمليات الإجرامية المماثلة و الأعقد تحديا .
3. **مجرم متخصص محترف :** هذه الجرائم تتطلب جانب عال من الخبرة التقنية و الإلمام بعالم البرمجة في أرقى درجاتها و لا يكون هذا إلا لمن تصف بدرجة التخصص و الاحتراف

المطلب الثالث : أصناف المجرم السيبراني

تتنوع أصناف المجرم السيبراني حسب الأهداف و ما يصبون إلى تحقيقه ومن هذه الأصناف نميز خمسة أصناف مهمة :

1. **الهواة :** وهو من يرتكبون هذه الجرائم بغرض التسلية لا أكثر و قد نجد منهم حتى صغار السن
2. **القراصنة (Hacker) :** على اختلاف مسمياتهم و درجاتهم في مقدمتهم

أ. الهاكرز : المتطفلون على أنظمة المعلومات لغرض كسر الحواجز الأمنية و هدفهم إثبات الذات

ب . الكراكرز : يتسللون إلى أنظمة المعالجة للاطلاع على المعلومات المخزنة و إلحاق الضرر بها لهدف السرقة أو العبث بها وهم على إطلاع بأخر التطورات و على تواصل فيما بينهم .

ج . القراصنة الخبثاء و المؤذين (Malicious hacker): هدفهم إلحاق خسائر بالطرف المستهدف و ليس مكاسب مادية ، و من بينهم مخترعو الفيروسات الالكترونية و مروجوها

3. **الجماعات المتطرفة :** وهم جماعات تعمل تحت معتقدات و أفكار سياسية و اجتماعية و دينية بغرض فرض معتقداتهم ومن هنا يلجؤون إلى اختراق الأنظمة المعلوماتية و الشبكات محليا و عالميا
4. **جواسيس الصناعة :** تعتبر فئة فرعية من الجماعات الاجرامية و أهدافها مقصورة على الأسرار التجارية و الابتزاز لأسباب تتعلق بالمصلحة الاقتصادية أو تدمير المنافس

الفصل الثاني:

آليات المكافحة الدولية للجرائم

الإلكترونية وحماية الأمن السيبراني

تمهيد:

أصبحت الجريمة السيبرانية في ظل العولمة الرقمية ظاهرة تتجاوز قدرة الأنظمة القانونية الوطنية على احتوائها، نظرا لطبيعتها العابرة للحدود واعتمادها على بيئة افتراضية لا تعترف بالسيادة الإقليمية بالمعنى التقليدي. وقد أفرز هذا الواقع تحديات قانونية عميقة، لعل أبرزها صعوبة تحديد الاختصاص القضائي، وتعقيد إجراءات تسليم المجرمين، واختلاف التجريم بين التشريعات الوطنية، فضلًا عن التطور السريع في وسائل ارتكاب الجريمة مقارنة ببطء تطور القواعد القانونية.

وفي هذا الإطار، لم يعد من الممكن الاكتفاء بالحلول الداخلية، بل أصبح من الضروري إرساء منظومة دولية قائمة على التعاون والتنسيق بين الدول، من خلال الاتفاقيات الدولية والآليات المؤسسية التي تضمن تبادل المعلومات وتوحيد الجهود، كما برزت الحاجة إلى تطوير تشريعات وطنية منسجمة مع هذه الجهود، وهو ما حاولت الجزائر تجسيده من خلال مجموعة من النصوص القانونية والمؤسسات المتخصصة.

وعليه، سيتم في هذا الفصل تحليل الجهود الدولية والإقليمية في مكافحة الجريمة السيبرانية، مع تقييم فعاليتها، ثم دراسة الآليات الوطنية في التشريع الجزائري، من خلال تحليل النصوص القانونية والمؤسسات المختصة.

المبحث الأول: الجهود الدولية في مواجهة الجريمة السيبرانية

تمهيد:

تستند الجهود الدولية في مكافحة الجريمة السيبرانية إلى مبدأ التعاون الدولي، باعتباره الآلية الوحيدة القادرة على مواجهة الجرائم العابرة للحدود. غير أن هذا التعاون يصطدم بعدة إشكالات، منها اختلاف الأنظمة القانونية، وتباين المصالح السياسية، وغياب تعريف موحد للجريمة السيبرانية. ورغم ذلك، فقد بذلت المنظمات الدولية والإقليمية جهودًا معتبرة لتجاوز هذه الصعوبات، من خلال وضع أطر قانونية وتنظيمية تهدف إلى توحيد السياسات الجنائية في هذا المجال.[1]

المطلب الأول: الجهود الدولية في مكافحة الجريمة السيبرانية

تمهيد:

تتمثل الجهود الدولية أساسًا في المبادرات التي تقودها المنظمات العالمية، وعلى رأسها الأمم المتحدة، والتي تسعى إلى إرساء قواعد عامة لمكافحة الجريمة السيبرانية، وإن كانت هذه الجهود تتسم في الغالب بالطابع التوجيهي غير الملزم.

الفرع الأول: جهود الأمم المتحدة في مكافحة الجريمة السيبرانية

1. اضطلعت الأمم المتحدة بدور محوري في معالجة ظاهرة الجريمة السيبرانية، حيث سعت منذ نهاية التسعينيات إلى إدراج هذا الموضوع ضمن أولوياتها، إدراكا منها لخطورة التهديدات المرتبطة باستخدام تكنولوجيا المعلومات في الأنشطة الإجرامية، وقد تجسد هذا الدور في إصدار الجمعية العامة القرار رقم 63/55 لسنة 2000، الذي دعا الدول إلى التعاون في مكافحة إساءة استخدام تكنولوجيا المعلومات، مؤكدا على ضرورة تبادل المعلومات وتعزيز القدرات الوطنية[2].

[1] عبد الفتاح بيومي حجازي، *الجرائم الإلكترونية في التشريع المقارن*، دار الفكر الجامعي، الطبعة الأولى، 2010، ص 211-216.
[2] الجمعية ال العامة للأمم المتحدة، القرار 63/55، 2000

كما جاء القرار رقم 121/56 لسنة 2001 ليعزز هذا التوجه، حيث نص على "ضرورة تطوير استراتيجيات وطنية شاملة لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات، وتعزيز التعاون الدولي في هذا المجال.[1]

ويلاحظ أن هذه القرارات، رغم أهميتها، لا تتمتع بقوة إلزامية، مما يجعل فعاليتها مرهونة بمدى التزام الدول بها.

ومن جهة أخرى، عملت لجنة منع الجريمة والعدالة الجنائية التابعة للأمم المتحدة على إعداد دراسات وتقارير تحليلية حول الجريمة السيبرانية، كما تم إنشاء فريق خبراء حكومي لدراسة إمكانية وضع اتفاقية دولية شاملة في هذا المجال. غير أن هذه الجهود لا تزال تواجه صعوبات، بسبب اختلاف مواقف الدول، خاصة فيما يتعلق بمسائل السيادة الرقمية وحرية الإنترنت.

ويستنتج من ذلك أن دور الأمم المتحدة، رغم أهميته في وضع الإطار العام، يظل محدودا من حيث الإلزام، مما يستدعي دعمه بآليات أكثر فعالية.

1. الجمعية العامة للأمم المتحدة، القرار 121/56، 2001 .
2. تقرير لجنة منع الجريمة والعدالة الجنائية، الأمم المتحدة، 2019، ص 35 .

الفرع الثاني: جهود المنظمات الدولية

إلى جانب الأمم المتحدة، تلعب المنظمات الدولية المتخصصة دورًا مهمًا في مكافحة الجريمة السيبرانية، حيث تعتمد هذه المنظمات على آليات عملية أكثر فعالية، مثل التنسيق الأمني وتبادل المعلومات. ومن أبرز هذه المنظمات المنظمة الدولية للشرطة الجنائية (الإنتربول)، التي تعد أداة أساسية في مكافحة الجرائم العابرة للحدود.

وقد عملت الإنتربول على إنشاء مراكز متخصصة في الجرائم السيبرانية، تقدم الدعم التقني للدول الأعضاء، كما تسهم في تنسيق العمليات الأمنية المشتركة. غير أن دورها يظل مرتبطًا بإرادة الدول، حيث لا تملك سلطة تنفيذية مستقلة.

كما ساهم الاتحاد الدولي للاتصالات في تعزيز الأمن السيبراني، من خلال تطوير مؤشرات عالمية لقياس جاهزية الدول، وتقديم الدعم الفني للدول النامية. ويُلاحظ أن هذه الجهود تركز على الجانب الوقائي، أكثر من الجانب الردعي.

ومن خلال ذلك، يتضح أن المنظمات الدولية تلعب دورا تكميليا، لكنها لا تستطيع بمفردها مواجهة هذه الظاهرة دون تعاون الدول[1].

1. الإنتربول، تقرير الجرائم السيبرانية، 2020 .
2. الاتحاد الدولي للاتصالات، تقرير الأمن السيبراني، 2018 .

المطلب الثاني: الجهود الإقليمية في مكافحة الجريمة السيبرانية

تمهيد:

أصبحت الجريمة السيبرانية من أبرز التحديات التي تواجه الدول في العصر الرقمي، بالنظر إلى طبيعتها العابرة للحدود وسرعة تطور وسائل ارتكابها. وقد أثبتت التجربة العملية أن الجهود الوطنية وحدها غير كافية لمواجهة هذا النوع من الجرائم، مما دفع الدول إلى تعزيز التعاون الإقليمي باعتباره آلية فعالة للتنسيق وتبادل الخبرات والمعلومات. وتتميز الجهود الإقليمية بقدرتها على تحقيق درجة أكبر من الانسجام القانوني والمؤسساتي بين الدول الأعضاء، نتيجة تقارب الأنظمة السياسية والتشريعية والثقافية، الأمر الذي يسهم في تسهيل عمليات الملاحقة القضائية وتبادل الأدلة الرقمية.

وفي هذا الإطار، برزت العديد من المنظمات الإقليمية التي لعبت دورا محوريا في وضع استراتيجيات وآليات متخصصة لمكافحة الجريمة السيبرانية، ومن أبرزها المجلس الأوروبي، والاتحاد الأوروبي، والاتحاد الإفريقي، وجامعة الدول العربية. وقد سعت هذه الهيئات إلى تطوير أطر قانونية وتنظيمية مشتركة، وتعزيز التعاون الأمني والقضائي، بالإضافة إلى دعم بناء القدرات التقنية والبشرية للدول الأعضاء[1].

ويعد المجلس الأوروبي من أهم النماذج الإقليمية الرائدة في هذا المجال، حيث نجح في وضع أول اتفاقية دولية ملزمة لمكافحة الجرائم المعلوماتية، والمعروفة باتفاقية بودابست لسنة 2001، والتي أصبحت مرجعا دوليا تعتمد عليه العديد من الدول حتى خارج القارة الأوروبية. كما ساهمت مؤسسات الاتحاد الأوروبي في تطوير سياسات أمن سيبراني متقدمة، وإنشاء وكالات متخصصة لمواجهة التهديدات الرقمية وتعزيز الأمن الإلكتروني داخل الفضاء الأوروبي[2].

ومن جهة أخرى، سعت المنظمات الإقليمية العربية والإفريقية إلى مواكبة هذه التطورات من خلال اعتماد اتفاقيات واستراتيجيات تهدف إلى مواجهة الجرائم الإلكترونية وحماية البنية التحتية الرقمية، وإن كانت هذه

[1] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 221-226.

[2] محمد حسين منصور، المسؤولية الجنائية عن الجرائم الإلكترونية، مصر، 2010، ص 135 .

الجهود لا تزال تواجه بعض التحديات المتعلقة بضعف الإمكانيات التقنية والتفاوت التشريعي بين الدول الأعضاء.

وعليه، فإن دراسة الجهود الإقليمية في مكافحة الجريمة السيبرانية تبرز أهمية التعاون الجماعي في مواجهة المخاطر الرقمية، وتوضح مدى مساهمة المنظمات الإقليمية في تطوير قواعد قانونية وآليات عملية تعزز الأمن السيبراني وتحد من انتشار الجرائم المعلوماتية.

الفرع الأول: المجلس الأوروبي

يعد المجلس الأوروبي من أبرز المنظمات الإقليمية التي لعبت دورا رياديا في مكافحة الجريمة السيبرانية، حيث أدرك منذ وقت مبكر خطورة التطور التكنولوجي وما يرافقه من تهديدات تمس أمن الدول والأفراد والمؤسسات. ومع التوسع الكبير في استخدام شبكات الإنترنت والأنظمة المعلوماتية خلال نهاية القرن العشرين، ظهرت أشكال جديدة من الجرائم التي تستهدف البيانات الإلكترونية والأنظمة الرقمية، وهو ما دفع المجلس الأوروبي إلى التحرك من أجل وضع إطار قانوني موحد يضمن مواجهة فعالة لهذه الجرائم[1].

وقد انطلقت جهود المجلس الأوروبي في هذا المجال من خلال عقد العديد من المؤتمرات واللقاءات بين الخبراء القانونيين والتقنيين، بهدف دراسة التحديات المرتبطة بالجريمة المعلوماتية ووضع حلول مشتركة للتصدي لها وتميزت هذه الجهود بالتركيز على ضرورة توحيد التشريعات الجنائية بين الدول الأوروبية، باعتبار أن اختلاف القوانين الوطنية يشكل عائقا أمام ملاحقة مرتكبي الجرائم الإلكترونية، خاصة وأن هذه الجرائم غالبا ما ترتكب عبر حدود متعددة وفي وقت قصير جدا[2].

وفي هذا السياق، قام المجلس الأوروبي بإعداد اتفاقية بودابست حول الجريمة الإلكترونية سنة 2001، والتي تعتبر أول معاهدة دولية ملزمة تهدف إلى مكافحة الجرائم المرتبطة باستخدام الحاسوب وشبكات الإنترنت، وقد شكلت هذه الاتفاقية نقلة نوعية في مجال مكافحة الجريمة السيبرانية، لأنها وضعت تعريفا

[1] عبد الفتاح بيومي حجازي، *الجرائم الإلكترونية في التشريع المقارن*، دار الفكر الجامعي، الطبعة الأولى، 2010، ص 235-240.

[2] محمد حسين منصور، نفس المرجع، ص 136 .

موحدا لأهم الجرائم الإلكترونية، وحددت آليات التعاون الدولي والإجراءات القانونية اللازمة للتحقيق والمتابعة القضائية.

وتكتسي اتفاقية بودابست أهمية كبيرة لكونها لم تقتصر على الدول الأوروبية فقط، بل أصبحت مرجعا عالميا انضمت إليه عدة دول من خارج أوروبا، مثل الولايات المتحدة الأمريكية وكندا واليابان وأستراليا، مما ساهم في توسيع نطاق التعاون الدولي في مكافحة الجرائم السيبرانية. كما أن الاتفاقية عكست وعيا متزايدا بضرورة مواجهة التهديدات الرقمية من خلال مقاربة جماعية تقوم على التنسيق بين الدول وتبادل المعلومات والخبرات التقنية والقانونية.

وقد تضمنت الاتفاقية مجموعة من الجرائم التي يجب على الدول الأعضاء تجريمها في قوانينها الداخلية، ومن أبرزها جرائم الدخول غير المشروع إلى الأنظمة المعلوماتية، واعتراض البيانات الإلكترونية، وإتلاف أو تعديل البيانات دون ترخيص، بالإضافة إلى جرائم الاحتيال والتزوير المعلوماتي، وجرائم نشر واستغلال المواد الإباحية المتعلقة بالأطفال، فضلا عن الجرائم المرتبطة بانتهاك حقوق الملكية الفكرية عبر الوسائط الرقمية.

كما أولت الاتفاقية أهمية خاصة للإجراءات الإجرائية المتعلقة بالتحقيق في الجرائم الإلكترونية، حيث نصت على تمكين السلطات المختصة من تفتيش الأنظمة المعلوماتية، وحجز البيانات الإلكترونية، وحفظها بصورة مستعجلة، واعتراض الاتصالات الرقمية عند الضرورة، مع مراعاة الضمانات القانونية المتعلقة بحماية حقوق الإنسان والحريات الأساسية. وقد ساهمت هذه الأحكام في تطوير وسائل الإثبات الرقمي وتعزيز فعالية التحقيقات الجنائية في الجرائم المعلوماتية.

ومن بين الجوانب المهمة التي ركز عليها المجلس الأوروبي كذلك تعزيز التعاون القضائي الدولي، إذ نصت الاتفاقية على مجموعة من آليات المساعدة القانونية المتبادلة بين الدول، مثل تبادل المعلومات، وتسليم المجرمين، وتبادل الأدلة الرقمية، وإنشاء قنوات اتصال سريعة تعمل على مدار الساعة لتسهيل التدخل الفوري في القضايا المستعجلة المتعلقة بالجرائم الإلكترونية. وقد ساعدت هذه الآليات على تجاوز العديد من الصعوبات المرتبطة بالطابع العابر للحدود الذي تتميز به الجرائم السيبرانية[1].

[1] محمد حسين منصور، نفس المرجع، ص137.

إلى جانب اتفاقية بودابست، عمل المجلس الأوروبي على تطوير استراتيجيات وبرامج تدريبية تهدف إلى دعم قدرات الدول الأعضاء في مجال الأمن السيبراني والتحقيق الرقمي. وتم تنظيم العديد من الدورات التكوينية وورشات العمل لفائدة القضاة وأعوان الشرطة والخبراء التقنيين، وذلك من أجل تحسين مهاراتهم في التعامل مع الأدلة الإلكترونية وفهم التقنيات الحديثة المستخدمة في ارتكاب الجرائم السيبرانية.

كما قام المجلس الأوروبي بإنشاء برامج للتعاون مع دول خارج أوروبا، خاصة الدول النامية، بهدف مساعدتها على تطوير تشريعاتها الوطنية المتعلقة بالجريمة الإلكترونية وتدعيم قدراتها التقنية والمؤسساتية. وقد ساهم هذا التوجه في تعزيز البعد الدولي للجهود الأوروبية وجعل المجلس الأوروبي فاعلا أساسيا في مجال الحوكمة الرقمية والأمن السيبراني على المستوى العالمي.

ومن الناحية العملية، ساهمت الجهود التي قادها المجلس الأوروبي في تحقيق قدر من الانسجام التشريعي بين الدول الأوروبية، حيث قامت أغلب الدول الأعضاء بتعديل قوانينها الجنائية والإجرائية بما يتوافق مع أحكام اتفاقية بودابست. كما أدى ذلك إلى تحسين فعالية التعاون بين الأجهزة الأمنية والقضائية، وتسريع إجراءات التحقيق والمتابعة في القضايا المتعلقة بالجرائم الإلكترونية.

ورغم الأهمية الكبيرة لاتفاقية بودابست، إلا أنها تعرضت لبعض الانتقادات، خاصة من قبل بعض الدول التي اعتبرت أن الاتفاقية تعكس بصورة أساسية الرؤية الأوروبية والغربية لمكافحة الجريمة السيبرانية، دون مراعاة كافية لاختلاف الأنظمة القانونية والثقافية للدول الأخرى. كما أثيرت مخاوف تتعلق بحماية السيادة الرقمية للدول وبإمكانية المساس بالخصوصية وحقوق الأفراد نتيجة توسيع صلاحيات السلطات المختصة في مجال المراقبة الرقمية واعتراض الاتصالات.

ومع ذلك، تبقى تجربة المجلس الأوروبي من أنجح التجارب الإقليمية في مجال مكافحة الجريمة السيبرانية، نظرا لقدرتها على الجمع بين الجانب التشريعي والتقني والتعاوني، إضافة إلى مساهمتها في وضع أسس قانونية دولية أصبحت تعتمد عليها العديد من الدول والمنظمات الإقليمية الأخرى. وقد أثبتت

هذه التجربة أن مواجهة التهديدات السيبرانية تتطلب تعاونا إقليميا ودوليا قائما على التنسيق المستمر وتبادل الخبرات والمعلومات[1].

وفي ظل التطورات المتسارعة للتكنولوجيا الحديثة، مثل الذكاء الاصطناعي والحوسبة السحابية والعملات الرقمية، يواصل المجلس الأوروبي تحديث آلياته القانونية وتعزيز استراتيجياته الأمنية لمواكبة الأشكال الجديدة للجرائم السيبرانية. كما يسعى إلى تعزيز التعاون مع المنظمات الدولية والإقليمية الأخرى من أجل بناء فضاء رقمي أكثر أمنا واستقرارا.

وعليه، فإن الدور الذي قام به المجلس الأوروبي في مجال مكافحة الجريمة السيبرانية يمثل نموذجا متقدما للتعاون الإقليمي، حيث نجح في وضع إطار قانوني ومؤسساتي متكامل ساهم في تطوير التشريعات الوطنية وتعزيز التعاون القضائي والأمني بين الدول، الأمر الذي جعله مرجعا أساسيا في الجهود الدولية الرامية إلى مكافحة الجرائم الإلكترونية وحماية الأمن السيبراني.

الفرع الثاني: اتفاقية بودابست

تعد اتفاقية بودابست لسنة 2001 حجر الأساس في النظام القانوني الدولي لمكافحة الجريمة السيبرانية، حيث تضمنت إطارا متكاملا يشمل التجريم والإجراءات والتعاون الدولي.

فمن حيث التجريم، نصت المادة (2) على تجريم الدخول غير المشروع، والمادة (3) على اعتراض البيانات، والمادة (4) على الإضرار بالبيانات. أما من حيث الإجراءات، فقد نصت المادة (16) على حفظ البيانات، والمادة (19) على التفتيش الإلكتروني.

كما نصت المادة (23) على التعاون الدولي، حيث ألزمت الدول الأطراف بتقديم المساعدة القانونية المتبادلة[2].

[1] محمد حسين منصور، نفس المرجع، ص 138.

2الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، 2010.

غير أن هذه الاتفاقية تعرضت لانتقادات، منها:

-عدم انضمام العديد من الدول النامية

-هيمنة الدول الأوروبية على صياغتها

الفرع الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

في إطار الجهود الإقليمية الرامية إلى مواجهة التحديات المتزايدة للجرائم السيبرانية، برزت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي تم اعتمادها سنة 2010 في نطاق جامعة الدول العربية، باعتبارها محاولة لتوحيد الرؤية القانونية بين الدول العربية في هذا المجال، وقد جاءت هذه الاتفاقية استجابة لتنامي التهديدات المرتبطة باستخدام تكنولوجيا المعلومات في الأنشطة الإجرامية، خاصة في ظل التفاوت التشريعي بين الدول العربية، وغياب إطار قانوني مشترك يضمن التنسيق الفعال في مواجهتها[1].

وتتميز هذه الاتفاقية بطابعها الشامل، حيث لم تقتصر على تجريم الأفعال المرتبطة بالجرائم السيبرانية، بل امتدت لتشمل الجوانب الإجرائية وآليات التعاون القضائي بين الدول الأعضاء، ففيما يتعلق بالتجريم، نصت الاتفاقية على مجموعة من الأفعال التي تُعد جرائم، من بينها الدخول غير المشروع إلى الأنظمة المعلوماتية، والاعتداء على سلامة البيانات، واستخدام الشبكات في الاحتيال أو نشر المحتويات غير المشروعة. ويُلاحظ أن هذه الأحكام تتقاطع إلى حد كبير مع ما ورد في اتفاقية بودابست، وهو ما يعكس تأثر المشرع العربي بالنموذج الأوروبي.

كما نصت الاتفاقية على تجريم الأفعال المرتبطة بالإرهاب الإلكتروني، حيث اعتبرت استخدام تكنولوجيا المعلومات في دعم الأنشطة الإرهابية جريمة تستوجب العقاب، وهو ما يعكس إدراكًا متزايدًا لخطورة هذا النوع من الجرائم على الأمن القومي للدول العربية. وفي هذا السياق، يمكن اعتبار الاتفاقية خطوة متقدمة في ربط الجريمة السيبرانية بالأمن الاستراتيجي.

1. محمد حسين منصور، المسؤولية الجنائية عن الجرائم الإلكترونية، مصر، 2010، ص 140 .

أما من الناحية الإجرائية، فقد تضمنت الاتفاقية أحكامًا تتعلق بجمع الأدلة الرقمية، وتفتيش الأنظمة المعلوماتية، وضبط البيانات، وهي مسائل ذات أهمية كبيرة في ظل الطبيعة الخاصة للأدلة الإلكترونية. كما نصت على ضرورة توفير الضمانات القانونية لحماية الحقوق والحريات، مما يعكس محاولة لتحقيق التوازن بين متطلبات الأمن واحترام حقوق الإنسان.

وفيما يتعلق بالتعاون الدولي، أكدت الاتفاقية على ضرورة تبادل المعلومات بين الدول الأعضاء، وتقديم المساعدة القضائية، وتسليم المجرمين، وهو ما يُعد عنصرًا أساسيًا في مكافحة الجرائم العابرة للحدود. غير أن فعالية هذه الآليات تظل رهينة بمدى التزام الدول بتنفيذها، فضلًا عن وجود تفاوت في القدرات التقنية والقانونية بين الدول العربية.

ورغم أهمية هذه الاتفاقية، إلا أنها تواجه عدة انتقادات، من أبرزها ضعف آليات التنفيذ، وغياب هيئة رقابية تضمن تطبيق أحكامها، إضافة إلى محدودية الانسجام بين التشريعات الوطنية للدول الأعضاء. كما أن التطور السريع للتكنولوجيا يفرض ضرورة تحديث نصوصها بشكل دوري، وهو ما لم يتحقق بالقدر الكافي.

ومن خلال ذلك، يمكن القول إن الاتفاقية العربية تمثل خطوة مهمة نحو توحيد الجهود الإقليمية، لكنها لا تزال بحاجة إلى تعزيز من خلال تطوير آليات التنفيذ، وتحديث النصوص، وتعزيز التعاون الفعلي بين الدول.

المطلب الثالث: الصعوبات والتحديات التي تواجه الجهود الدولية وسبل معالجتها

تمهيد:

رغم تعدد الجهود الدولية والإقليمية المبذولة في مجال مكافحة الجرائم السيبرانية، إلا أن هذه الجهود لا تزال تواجه مجموعة من التحديات المعقدة، التي تعيق تحقيق فعالية حقيقية في هذا المجال. ويعود ذلك إلى طبيعة هذه الجرائم، التي تتسم بالديناميكية والتطور المستمر، فضلًا عن تعارض بعض المصالح الوطنية مع متطلبات التعاون الدولي. ومن هنا، فإن تحليل هذه الصعوبات يُعد خطوة أساسية لفهم حدود فعالية الجهود الدولية، واقتراح سبل لتجاوزها.[1]

الفرع الأول: الصعوبات التي تواجه الجهود الدولية

تتمثل إحدى أبرز الصعوبات التي تواجه الجهود الدولية في اختلاف التشريعات الوطنية بين الدول، حيث لا يوجد تعريف موحد للجريمة السيبرانية، ولا اتفاق شامل حول الأفعال التي ينبغي تجريمها. ويؤدي هذا الاختلاف إلى ظهور ما يُعرف بـ"الملاذات الآمنة"، حيث يستغل المجرمون الدول التي تفتقر إلى تشريعات صارمة لممارسة أنشطتهم دون خوف من الملاحقة[2].

كما تبرز مشكلة الاختصاص القضائي كأحد أهم التحديات، إذ قد ترتكب الجريمة في فضاء افتراضي يشمل عدة دول، مما يثير تساؤلات حول الجهة المختصة بالنظر في الدعوى. وقد حاولت اتفاقية بودابست معالجة هذه الإشكالية من خلال إقرار مبدأ التعاون الدولي، غير أن التطبيق العملي لا يزال يواجه صعوبات.

ومن جهة أخرى، يعد التطور التكنولوجي السريع من أبرز التحديات، حيث تتطور أساليب ارتكاب الجرائم بشكل يفوق قدرة التشريعات على مواكبتها، مما يؤدي إلى وجود فجوة قانونية يستغلها المجرمون. كما أن نقص الكفاءات التقنية لدى بعض الدول، خاصة النامية، يحد من قدرتها على مواجهة هذه الجرائم.

---

[1] عبد الفتاح بيومي حجازي، *الجرائم الإلكترونية في التشريع المقارن*، دار الفكر الجامعي، الطبعة الأولى، 2010، ص 252-257.
[2] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 248-252.

ولا يمكن إغفال العوائق السياسية، حيث قد تتردد بعض الدول في التعاون، بسبب اعتبارات تتعلق بالسيادة أو الأمن القومي، وهو ما يضعف فعالية الجهود الدولية[1].

الفرع الثاني: سبل تجاوز الصعوبات في مكافحة الجرائم السيبرانية

في مواجهة هذه التحديات، تبرز الحاجة إلى تبني مجموعة من الحلول التي من شأنها تعزيز فعالية الجهود الدولية في مكافحة الجرائم السيبرانية. ويأتي في مقدمة هذه الحلول العمل على توحيد التشريعات الوطنية، من خلال تبني نماذج قانونية موحدة، مثل اتفاقية بودابست، بما يضمن تقارب الأنظمة القانونية وتقليل الفجوات التي يستغلها المجرمون.

كما يعد تعزيز التعاون الدولي أمرًا ضروريًا، من خلال تطوير آليات تبادل المعلومات، وتبسيط إجراءات المساعدة القضائية، وتسريع عمليات تسليم المجرمين. وفي هذا السياق، يمكن الاستفادة من التجارب الناجحة لبعض الدول والمنظمات الدولية.

ومن جهة أخرى، يجب الاستثمار في تطوير القدرات التقنية، من خلال تدريب الكوادر الأمنية والقضائية، وتوفير الوسائل التكنولوجية اللازمة لمكافحة الجرائم السيبرانية. كما يُعد نشر الوعي الأمني بين المستخدمين عنصرًا مهمًا في الوقاية من هذه الجرائم.

كما ينبغي تعزيز الشراكة بين القطاعين العام والخاص، نظرًا للدور الكبير الذي تلعبه الشركات التكنولوجية في إدارة الفضاء السيبراني وأخيرا، يتعين العمل على تحديث التشريعات بشكل مستمر، بما يواكب التطور التكنولوجي.

1. تقرير الأمم المتحدة حول الجرائم السيبرانية، 2019، ص 45 .
2. أحمد فتحي سرور، الوسيط في قانون العقوبات، مصر، 2008، ص 260 .

المبحث الثاني: آليات مكافحة الجرائم السيبرانية في ظل التشريع الجزائري

تمهيد:

في مواجهة التحديات المتزايدة للجرائم السيبرانية، سعى المشرع الجزائري إلى تطوير منظومة قانونية ومؤسساتية تهدف إلى مكافحة هذه الجرائم، من خلال تبني مقاربة شاملة تجمع بين التجريم والعقاب من جهة، والوقاية والتأهيل من جهة أخرى. وقد تجسد هذا التوجه في إصدار القانون رقم 09-04، الذي يُعد الإطار الأساسي لمكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، إلى جانب إدخال تعديلات على قانون العقوبات، وإنشاء هيئات متخصصة في هذا المجال.

المطلب الأول: الآليات التشريعية لمواجهة الجرائم السيبرانية

الفرع الأول: القواعد الموضوعية المنظمة للجرائم السيبرانية

اعتمد المشرع الجزائري على مجموعة من النصوص القانونية التي تهدف إلى تجريم الأفعال المرتبطة بالجرائم السيبرانية، حيث نص قانون العقوبات في المادة 394 مكرر على تجريم الدخول غير المشروع إلى الأنظمة المعلوماتية، كما نص القانون 09-04 على تجريم الاعتداء على البيانات، ونشر المحتويات غير المشروعة.

وتظهر هذه النصوص توجهًا نحو توسيع نطاق التجريم ليشمل مختلف صور الجريمة الإلكترونية، مع مراعاة خصوصيتها[1].

1. الاتحاد الدولي للاتصالات، تقرير الأمن السيبراني، 2018 .
2. عبد الله سليمان، الأمن المعلوماتي، الجزائر، 2016، ص 85 .

الفرع الثاني: القواعد الإجرائية لمكافحة الجرائم السيبرانية

تتميز الجرائم السيبرانية بطبيعة خاصة تختلف عن الجرائم التقليدية، فهي ترتكب في بيئة رقمية تعتمد على الأنظمة المعلوماتية والشبكات الإلكترونية، الأمر الذي يجعل وسائل الإثبات التقليدية غير كافية للكشف عنها أو تعقب مرتكبيها، لذلك سعى المشرع الجزائري من خلال القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إلى وضع قواعد إجرائية تتلاءم مع خصوصية هذا النوع من الجرائم، وذلك بهدف تمكين السلطات المختصة من الوصول إلى الأدلة الرقمية والحفاظ عليها قبل ضياعها أو إتلافها.

ومن بين أهم الإجراءات التي نص عليها المشرع الجزائري إجراء تفتيش الأنظمة المعلوماتية، حيث يختلف هذا النوع من التفتيش عن التفتيش التقليدي باعتبار أن محل التفتيش هنا لا يتعلق بمكان مادي فقط، وإنما يمتد إلى الحواسيب وقواعد البيانات والهواتف الذكية والخوادم الإلكترونية وكل الوسائط الرقمية التي يمكن أن تحتوي على بيانات مرتبطة بالجريمة، ويكتسي هذا الإجراء أهمية كبيرة لأن المجرم السيبراني يعتمد غالبًا على إخفاء آثاره الرقمية أو تشفير البيانات المستعملة في ارتكاب الجريمة، وهو ما يستدعي تدخلًا سريعًا من قبل الضبطية القضائية المختصة[1].

كما يهدف تفتيش الأنظمة المعلوماتية إلى الوصول إلى الأدلة الرقمية المتعلقة بالجريمة، مثل الرسائل الإلكترونية، وسجلات الاتصال، والبرمجيات المستعملة، وملفات التخزين، إضافة إلى التعرف على هوية الفاعلين والشركاء المحتملين. ويستلزم هذا النوع من التفتيش وجود خبرة تقنية متخصصة، لأن التعامل مع الأدلة الرقمية يتطلب المحافظة على سلامتها وعدم تغيير محتواها أثناء عملية الفحص أو النسخ[2].

وقد منح القانون الجزائري للسلطات القضائية صلاحية الأمر بتفتيش الأنظمة المعلوماتية متى وجدت دلائل جدية على ارتكاب جريمة سيبرانية، مع ضرورة احترام الضمانات القانونية المتعلقة بحرمة الحياة الخاصة وسرية المراسلات. ويعد هذا التوازن بين حماية الحقوق الفردية ومتطلبات

[1] محمد أمين البشري، *التحقيق في الجرائم المعلوماتية*، دار الجامعة الجديدة، 2013، ص 174-179.

[2] عبد الله سليمان، نفس المرجع، ص 86 .

الأمن الإلكتروني من أهم المبادئ التي يقوم عليها التشريع الجزائري في مجال مكافحة الجرائم السيبرانية.

ومن الإجراءات المهمة كذلك ضبط البيانات المعلوماتية، حيث تتمثل هذه العملية في حجز أو نسخ أو حفظ المعطيات الرقمية التي يمكن أن تشكل دليلًا على ارتكاب الجريمة. وتكتسب هذه العملية أهمية خاصة بالنظر إلى سهولة حذف البيانات الإلكترونية أو تعديلها في وقت قصير، الأمر الذي قد يؤدي إلى ضياع الدليل الرقمي بشكل نهائي.

ويشمل ضبط البيانات مختلف أنواع المعطيات الإلكترونية، سواء كانت مخزنة داخل أجهزة الحاسوب أو على الخوادم الإلكترونية أو في خدمات التخزين السحابي. كما يمكن أن يشمل البرامج والتطبيقات المستخدمة في تنفيذ الجريمة، إضافة إلى بيانات المستخدمين وسجلات الولوج إلى الأنظمة المعلوماتية.

ويقتضي التعامل مع الأدلة الرقمية مراعاة مجموعة من القواعد التقنية والإجرائية، من بينها توثيق عملية الضبط وتحديد تاريخ وساعة استخراج البيانات، مع ضمان عدم المساس بمحتوى الدليل الإلكتروني. ويهدف ذلك إلى الحفاظ على حجية الدليل الرقمي أمام الجهات القضائية، لأن أي تغيير في البيانات قد يؤدي إلى الطعن في مصداقيتها.

ومن جهة أخرى، نص القانون على إمكانية اعتراض الاتصالات الإلكترونية، وهو إجراء يسمح للسلطات المختصة بمراقبة أو تسجيل الاتصالات الرقمية التي يشتبه في ارتباطها بجرائم سيبرانية. ويشمل ذلك البريد الإلكتروني، والمحادثات الإلكترونية، والاتصالات عبر تطبيقات التواصل الاجتماعي، وغيرها من وسائل الاتصال الحديثة.

ويعتبر اعتراض الاتصالات من أخطر الإجراءات التي تمس بالحريات الفردية، لذلك أحاطه المشرع الجزائري بمجموعة من الضمانات القانونية، من بينها ضرورة الحصول على إذن قضائي

مسبق يحدد مدة الاعتراض وطبيعته والأشخاص المعنيين به. كما يجب أن يكون هذا الإجراء مبررا بوجود ضرورة حقيقية للكشف عن الجريمة أو تحديد هوية مرتكبيها[1].

وتبرز أهمية اعتراض الاتصالات في الجرائم السيبرانية المنظمة، خاصة تلك المتعلقة بالاختراق الإلكتروني والاحتيال الرقمي والإرهاب الإلكتروني، حيث يعتمد المجرمون على وسائل اتصال مشفرة يصعب تتبعها بالطرق التقليدية. ولذلك فإن تمكين الجهات المختصة من مراقبة هذه الاتصالات يساعد في إحباط العديد من المخططات الإجرامية قبل تنفيذها.

كما اعتمد المشرع الجزائري على أسلوب التعاون بين مختلف الجهات الأمنية والقضائية من أجل تسهيل تبادل المعلومات المتعلقة بالجرائم السيبرانية، باعتبار أن هذا النوع من الجرائم يتسم بالطابع العابر للحدود. فالجريمة قد ترتكب في دولة، بينما توجد الخوادم المستعملة في دولة أخرى، في حين يكون الضحايا موزعين عبر عدة دول، الأمر الذي يجعل التعاون الدولي ضرورة حتمية.

ومن بين القواعد الإجرائية المهمة كذلك إمكانية اللجوء إلى الخبرة التقنية، حيث أصبح الخبير المعلوماتي عنصرًا أساسيًا في التحقيقات المتعلقة بالجرائم الإلكترونية. ويقوم هذا الخبير بتحليل الأنظمة المعلوماتية وفحص الأدلة الرقمية والكشف عن طرق الاختراق المستعملة، إضافة إلى استرجاع البيانات المحذوفة وتحديد مصدر الهجمات الإلكترونية.

وتساعد الخبرة التقنية القاضي على فهم الجوانب الفنية المعقدة المرتبطة بالجريمة السيبرانية، خاصة وأن العديد من الجرائم الإلكترونية تعتمد على تقنيات متطورة يصعب استيعابها دون الاستعانة بالمختصين. ولذلك فإن فعالية مكافحة الجرائم السيبرانية ترتبط بشكل كبير بمدى توفر الكفاءات البشرية المؤهلة في مجال الأمن السيبراني والتحليل الجنائي الرقمي[2].

كما أن الطبيعة الخاصة للجرائم السيبرانية فرضت على السلطات القضائية اعتماد السرعة في اتخاذ الإجراءات، لأن التأخر في التدخل قد يؤدي إلى اختفاء الأدلة أو انتقالها إلى أنظمة معلوماتية

[1] عبد الله سليمان، نفس المرجع، ص 87.

[2] عبد الفتاح بيومي حجازي، *الدليل الجنائي الرقمي وجرائم الإنترنت*، دار الفكر الجامعي، الطبعة الأولى، 2008، ص 164-168.

أخرى خارج نطاق الاختصاص الوطني. ولهذا السبب منح القانون للجهات المختصة صلاحيات عاجلة تسمح بالحفاظ على البيانات الرقمية وضمان عدم ضياعها[1].

ويلاحظ كذلك أن التشريع الجزائري حاول مواكبة التطورات التكنولوجية الحديثة من خلال إدراج نصوص قانونية مرنة تسمح بالتعامل مع الجرائم المستحدثة، إلا أن التحدي يبقى قائمًا بسبب التطور المستمر لوسائل الجريمة الإلكترونية، الأمر الذي يتطلب تحديثًا دوريًا للنصوص القانونية وتكييفها مع المستجدات التقنية.

المطلب الثاني: الهيئات المتخصصة في البحث و التحري

حرصت الجزائر على إنشاء هيئات وأجهزة متخصصة لمكافحة الجرائم السيبرانية، إدراكًا منها لخطورة هذه الجرائم وتأثيرها على الأمن الوطني والاقتصاد والاستقرار الاجتماعي. وقد تمثلت هذه الجهود في إنشاء فرق متخصصة داخل أجهزة الأمن والدرك والجهات القضائية، مع توفير التكوين اللازم للعاملين في هذا المجال.

وتعد وحدات الأمن الوطني من أهم الجهات المكلفة بمكافحة الجرائم السيبرانية، حيث تم إنشاء مصالح متخصصة تعنى بالتحقيق في الجرائم الإلكترونية ومتابعة النشاطات الإجرامية المرتبطة بالأنظمة المعلوماتية وتعمل هذه الوحدات على رصد الهجمات الإلكترونية وتعقب مرتكبيها، إضافة إلى استقبال شكاوى المواطنين المتعلقة بالابتزاز الإلكتروني والاحتيال الرقمي واختراق الحسابات الإلكترونية.

وقد ساهمت هذه الوحدات في كشف العديد من الشبكات الإجرامية التي تستغل الوسائط الإلكترونية لارتكاب جرائمها، خاصة جرائم النصب الإلكتروني وسرقة المعطيات الشخصية والقرصنة المعلوماتية. كما تعتمد مصالح الأمن الوطني على تقنيات حديثة في التحليل الرقمي ومراقبة الفضاء السيبراني، ما يعزز قدرتها على مواجهة التهديدات الإلكترونية.

[1] عبد الله سليمان، نفس المرجع، ص 88.

أما الدرك الوطني فيلعب بدوره دورًا مهمًا في مكافحة الجرائم السيبرانية، خاصة في المناطق الريفية والنائية التي تدخل ضمن نطاق اختصاصه الإقليمي. وقد أنشأ الدرك الوطني وحدات تقنية متخصصة في الجرائم المعلوماتية، تعمل على التحقيق في الجرائم المرتبطة باستخدام التكنولوجيا الحديثة.

ويقوم الدرك الوطني كذلك بحملات توعوية تهدف إلى نشر الثقافة الأمنية الرقمية بين المواطنين، من خلال التحذير من مخاطر الاحتيال الإلكتروني وضرورة حماية البيانات الشخصية. كما يساهم في التعاون الدولي في مجال مكافحة الجرائم العابرة للحدود، من خلال تبادل المعلومات والخبرات مع مختلف الأجهزة الأمنية الأجنبية.

ومن جهة أخرى، تلعب الجهات القضائية المختصة دورًا محوريًا في متابعة الجرائم السيبرانية والفصل فيها، حيث تم تخصيص قضاة ووكلاء جمهورية تلقوا تكوينًا متخصصًا في مجال الجرائم الإلكترونية. ويهدف هذا التخصص إلى تمكين القضاة من فهم الطبيعة التقنية لهذه الجرائم وكيفية التعامل مع الأدلة الرقمية[1].

كما تعمل الجهات القضائية على ضمان التطبيق السليم للقوانين المتعلقة بمكافحة الجرائم السيبرانية، مع الحرص على تحقيق التوازن بين متطلبات الأمن الإلكتروني واحترام الحقوق والحريات الأساسية ويظهر ذلك من خلال الرقابة القضائية على إجراءات التفتيش والمراقبة واعتراض الاتصالات[2].

وقد ساهم إنشاء الفرق المتخصصة في رفع فعالية مكافحة الجرائم السيبرانية، حيث أصبح التعامل مع هذا النوع من الجرائم يتم بوسائل أكثر احترافية ودقة. كما أدى ذلك إلى تحسين سرعة الاستجابة للهجمات الإلكترونية وتقليص حجم الأضرار الناتجة عنها.

[1] محمد أمين البشري، *التحقيق في الجرائم المعلوماتية*، دار الجامعة الجديدة، 2013، ص 209-213.

[2] عبد الله سليمان، نفس المرجع، ص 91.

ورغم الجهود المبذولة، إلا أن الهيئات المختصة ما تزال تواجه عدة تحديات، من بينها النقص في الكفاءات التقنية المتخصصة، والتطور السريع لأساليب الجريمة الإلكترونية، إضافة إلى صعوبة التعاون الدولي في بعض الحالات بسبب اختلاف التشريعات الوطنية[1].

كما أن مكافحة الجرائم السيبرانية تتطلب توفير تجهيزات تقنية متطورة وبرمجيات حديثة قادرة على تحليل البيانات الضخمة وتتبع الأنشطة الإجرامية عبر الإنترنت. ولذلك فإن نجاح الهيئات المختصة يرتبط بمدى توفير الإمكانيات المادية والبشرية اللازمة[2].

وتبرز أهمية التكوين المستمر لأعوان الأمن والقضاة والخبراء في مجال الأمن السيبراني، لأن الجرائم الإلكترونية تشهد تطورًا متسارعًا يتطلب مواكبة دائمة للمستجدات التقنية والقانونية. كما أن تعزيز التعاون مع الجامعات ومراكز البحث يمكن أن يساهم في تطوير القدرات الوطنية في هذا المجال.

[1] محمد أمين البشري، *الجرائم المعلوماتية والتحقيق فيها*، دار الجامعة الجديدة، 2012، ص 255-259.
[2] عبد الفتاح بيومي حجازي، *أمن المعلومات والجرائم الإلكترونية*، دار الفكر الجامعي، الطبعة الأولى، 2007، ص 244-248.

خلاصة الفصل

يتضح من خلال دراسة الجهود الدولية والإقليمية والوطنية لمكافحة الجرائم السيبرانية أن هذه الظاهرة أصبحت تشكل تحديًا حقيقيًا يهدد أمن الدول واستقرار المجتمعات، الأمر الذي دفع مختلف الهيئات الدولية والإقليمية إلى وضع اتفاقيات وآليات قانونية تهدف إلى تعزيز التعاون في مجال الوقاية والمكافحة.

ورغم أهمية هذه الجهود، إلا أنها ما تزال تعاني من عدة نقائص، من بينها اختلاف التشريعات الوطنية، وصعوبة توحيد المفاهيم القانونية المتعلقة بالجرائم الإلكترونية، إضافة إلى محدودية التعاون الدولي في بعض الحالات. كما أن التطور السريع للتكنولوجيا يجعل القوانين أحيانًا غير قادرة على مواكبة الأساليب الإجرامية الحديثة.

أما على المستوى الوطني، فقد خطت الجزائر خطوات مهمة في مجال مكافحة الجرائم السيبرانية من خلال إصدار القانون 09-04 وإنشاء هيئات متخصصة وتطوير آليات التحقيق الرقمي. ويعكس ذلك إدراك المشرع الجزائري لخطورة التهديدات السيبرانية وضرورة التصدي لها بوسائل قانونية وتقنية حديثة.

غير أن فعالية مكافحة الجرائم السيبرانية تتطلب مزيدًا من الجهود، خاصة في مجال التكوين المتخصص، وتطوير البنية التحتية الرقمية، وتعزيز التعاون الدولي، إلى جانب تحديث التشريعات بشكل دوري لمواكبة المستجدات التقنية. كما أن نشر الوعي المجتمعي بأهمية الأمن السيبراني يعد عنصرا أساسيا في الحد من الجرائم الإلكترونية وحماية الأفراد والمؤسسات من مخاطرها.

الخاتمة

الخاتمة:

بناء على ما تقدم ذكره في هذه الدراسة و تفصيلا لماهية الجريمة السيبرانية و سبل التصدي لها دوليا بشكل خاص ، و في ظل المنظومة القانونية الدولية و الوطنية الكلاسيكية ، و بالنظر إلى تسارع المد التكنولوجي المذهل و عدم انحصار موقع الجريمة و لا بقائها بشكلها المادي الكلاسيكي كل هذا جعل المجتمع الدولي عامة أمام تحد بالغ التعقيد يتطلب إعادة النظر في ألية التجريم و الملاحقة و الإثبات .

و استنادا إلى ما سبق فإننا نخلص إلى مايلي :

أولا . نتائج الدراسة:

- الجريمة السيبرانية جريمة عابرة للحدود و مهما اختلفت وسائلها و أهدافها فإنها أفة خطيرة تؤثر على استقرار الدول السياسي و الاقتصلدي و حتى السيادي للدول و الحكومات
- الجريمة السيبرانية متعددة الأوجه و الوسائل
- الجريمة السيبرانية تتصاعد خطورتها بتطور التقنية و فردية المكافحة
- أفرزت هذه الدراسة أن الأمن السيبراني لم يعد مجرد خيار تقني، بل أصبح ضرورة استراتيجية تمس الأمن الوطني والدولي، حيث يقوم على حماية الأنظمة المعلوماتية وضمان سرية البيانات وسلامتها وتوافرها. كما تبين أن هذا المفهوم تطور تدريجيًا استجابة لتزايد التهديدات الرقمية، وأصبح اليوم يشكل أحد أهم محاور السياسات الأمنية للدول.
- أما على مستوى الاستراتيجيات الدولية، فقد خلصت الدراسة إلى أن المجتمع الدولي قد بذل جهودا معتبرة من خلال الأمم المتحدة والمنظمات الدولية والإقليمية، وعلى رأسها اتفاقية بودابست لسنة 2001، التي شكلت مرجعا أساسيا في مجال تجريم الأفعال السيبرانية وتنظيم التعاون الدولي.

غير أن هذه الجهود ما تزال تعاني من محدودية الفعالية بسبب غياب الإلزام في بعض الآليات، وتباين التشريعات الوطنية، وضعف التنسيق الدولي في بعض الحالات.

- وفي السياق الإقليمي، برزت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كخطوة مهمة نحو توحيد الجهود العربية، إلا أن فعاليتها تبقى محدودة بسبب ضعف آليات التنفيذ وتفاوت الإمكانيات التقنية بين الدول الأعضاء.
- أما على المستوى الوطني، فقد تبنى المشرع الجزائري مقاربة قانونية متطورة نسبيًا من خلال القانون رقم 09-04 وتعديل قانون العقوبات، إلى جانب إنشاء هيئات أمنية وقضائية متخصصة، وهو ما يعكس إدراكًا متزايدًا لخطورة هذه الجرائم. ومع ذلك، فإن فعالية هذه المنظومة تبقى مرتبطة بمدى مواكبتها للتطور التكنولوجي وتعزيز التعاون الدولي والتكوين المتخصص.

ثانيا . اقتراحات الدراسة :

بناءا على ما سبق، يمكن استخلاص أن مكافحة الجريمة السيبرانية لا يمكن أن تتحقق بفعالية إلا من خلال مقاربة شاملة من خلال :

- تطوير التشريعات الوطنية بشكل مستمر من خلال الاهتمام بالبحث في العلوم القانونية الجنائية
- تعزيز التعاون الدولي والإقليمي في مجال مكافحة الجريمة العابرة للقارات و تفعيل اتفاقيات تسليم المجرمين
- دعم القدرات التقنية والبشرية من خلال الاهتمام و تشجيع البحث العلمي الذي بات ضرورة وجودية
- رفع مستوى الوعي الأمني لدى المستخدمين
- وتوحيد الجهود القانونية على المستوى الدولي

وفي الأخير، يمكن القول إن الجريمة السيبرانية ستظل في تطور مستمر ما دام التطور التكنولوجي قائمًا، مما يجعل مواجهتها عملية ديناميكية تتطلب يقظة دائمة وتحديثًا مستمرًا للأطر القانونية والتقنية، لضمان تحقيق التوازن بين حماية الأمن السيبراني وصون الحقوق والحريات في الفضاء الرقمي.

قائمة المراجع

قائمة المراجع:

أولا: الكتب

1. عبد الفتاح بيومي حجازي، الجريمة المعلوماتية في ظل الثورة التكنولوجية الحديثة، دار الفكر الجامعي، الإسكندرية، مصر، 2006 .
2. محمد حسين منصور، المسؤولية الجنائية عن الجرائم الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2010 .
3. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، 2013 .
4. أحمد فتحي سرور، الوسيط في قانون العقوبات، دار النهضة العربية، القاهرة، مصر، 2008 .
5. عبد الله سليمان، شرح قانون العقوبات الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2015 .
6. سمير عبد السيد تناغو، الجرائم المعلوماتية وأمن المعلومات، دار الفكر العربي، القاهرة، مصر، 2012 .
7. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، دار النهضة العربية، القاهرة، مصر، 1998 .
8. علي عبد القادر القهوجي، القانون الجنائي والجرائم المستحدثة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014 .

ثانيا: المذكرات الجامعية

1. بوعزة محمد، الجرائم الإلكترونية في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2017 .
2. حماني فاطمة، الأمن السيبراني في ظل التطور التكنولوجي، مذكرة ماستر، جامعة وهران، الجزائر، 2020 .
3. بن عيسى عبد القادر، آليات مكافحة الجريمة المعلوماتية في القانون الجزائري، مذكرة ماستر، جامعة باتنة، الجزائر، 2019 .
4. لعروسي أسماء، الجرائم السيبرانية وأثرها على الأمن الوطني، مذكرة ماستر، جامعة تلمسان، الجزائر، 2021 .
5. الدام محمد ، الأمن السيبراني ، مذكرة ماستر ، كلية الحقوق ، جامعة حمة لخضر، الجزائر ، 2023

ثالثا: المجلات العلمية والمقالات

1. مجلة القانون والعلوم السياسية، الجرائم الإلكترونية وإشكالية الإثبات، العدد 12، الجزائر، 2020 .
2. مجلة الفكر القانوني والسياسي، الأمن السيبراني بين الحماية والتحديات، العدد 7، الجزائر، 2019 .
3. مجلة الدراسات القانونية، التعاون الدولي في مكافحة الجرائم المعلوماتية، العدد 5، مصر، 2018 .

رابعا: القوانين والتشريعات

1. قانون العقوبات الجزائري، الأمر رقم 66-156، المعدل والمتمم .
2. القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .
3. اتفاقية بودابست لمكافحة الجريمة السيبرانية، مجلس أوروبا، 2001 .
4. قرارات الجمعية العامة للأمم المتحدة رقم 63/55 و121/56 بشأن مكافحة الجريمة المعلوماتية .
5. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، 2010 .

خامسا: التقارير الدولية

1. الأمم المتحدة، تقرير الجريمة السيبرانية والأمن الرقمي، نيويورك، 2019 .
2. الاتحاد الدولي للاتصالات(ITU) ، تقرير مؤشر الأمن السيبراني العالمي، جنيف، 2018 .
3. الإنتربول، تقرير الجرائم السيبرانية العالمية، .2020

فهرس المحتويات

Abstract

This study addressed a legal topic of an international nature to analyze the phenomenon of "cybercrime," whose gravity and indicators of difficulty in combating are steadily increasing among governments, nations, and legal and judicial systems worldwide. It has become evident that the transition from the locus of conventional, physical crime to non-tangible virtual spaces has created a vast legal vacuum between classic legislative texts formulated to adjudicate physical, tangible facts and crimes committed outside the observable, transboundary spectrum.

Through this study, an endeavor was made to demonstrate that safeguarding cybersecurity has become an existential imperative and a critical pillar of state sovereignty. This requires the concerted efforts of all nations through international cooperation to update laws and draft modern legislation capable of keeping pace with this accelerating cyber-criminal influx. Such a goal can be achieved by engaging in security and legal frameworks and conventions at both regional and global levels.

Furthermore, the study demonstrated that cybercrime is characterized by complex attributes, most notably its non-material nature, the difficulty of proof, and its rapid evolution, in addition to the feasibility of remote commission across global networks. These factors fundamentally distinguish it from conventional crimes. It has also been revealed that the diversity of its forms—ranging from crimes targeting systems and data to financial, terrorist, and targeted crimes against individuals and states—reflects its expanding scope and ramified impacts. Consequently, this necessitates a comprehensive reconsideration of classical criminal law concepts .