الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة غرداية UN .47.01

كلية الحقوق والعلوم السياسية
قسم العلوم السياسية

شهادة تصحيح المذكرة

يشهد الأستاذ فروحات سعيد بصفته (رئيسا أو مناقشا) في لجنة المناقشة

لمذكرة الماستر للطالب(ة): بلحاج عبد الرحمن رقم التسجيل: 141190547714

ميدان: الحقوق والعلوم السياسية **شعبة**: العلوم السياسية **التخصص**: تنظيم سياسي وإداري

الموسم الجامعي: 2025 - 2024

أن المذكرة المعنونة بـ:

سياسة مكافحة الجرائم السيبرانية في الجزائر

تم تصحيحها من طرف الطالب وهي صالحة للإيداع.

إمضاء الأستاذ المكلف بمتابعة التصحيح (رئيس اللجنة أو المتحن)

رئيس قسم العلوم السياسية
د. البير طارق

غرداية في: 2024/10/13

رئيس القسم

ملاحظة: تودع هذه الوثيقة على مستوى القسم

جامعة غرداية

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

سياسة مكافحة الجرائم السيبرانية في الجزائر

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في العلوم السياسية

تخصص سياسي وإداري

إعداد الطالب:

عبد الرحمان باعمارة

إشراف الأستاذ:

د. حمزة خير الناس

لجنة المناقشة:

لقب واسم الاستاذ	الرتبة	الجامعة	الصفة
د. فروحات سعيد	أستاذ محاضر أ	جامعة غرداية	رئيسا
د. خيار الناس حمزة	أستاذ محاضر أ	جامعة غرداية	مشرفا مقررا
د. صوالحي ليلى	أستاذ محاضر ب	جامعة غرداية	عضواً مناقشا

السنة الجامعية:

1445-1444 هـ/ 2024-2023


بسم الله الرحمن الرحيم

شكر وعرفان

أتقدم بخالص الشكر والعرفان إلى كل من ساهم في إنجاز هذه المذكرة، وأود أن أعبر عن امتناني العميق لمن كان له دور كبير في توجيهي ودعمي طوال فترة إعداد هذا العمل.

أولاً، أخص بالشكر الدكتور حمزة خير الناس، مشرف هذا البحث، على توجيهاته القيمة، صبره، ودعمه المتواصل، لقد كان لتوجيهاته العلمية والنقدية دور كبير في تحسين جودة هذا العمل والوصول به إلى هذا المستوى.

كما أتوجه بالشكر إلى كافة أساتذة الكلية الذين لم يبخلوا بتقديم النصح والإرشاد خلال سنوات الدراسة، وكذلك إلى زملائي وزميلاتي على دعمهم وتشجيعهم المستمر.

ولا أنسى أن أعبر عن امتناني العميق لعائلتي التي كانت مصدر دعم معنوي كبير طوال هذه الرحلة العلمية، والتي لولاها لما كنت لأصل إلى هذه المرحلة.

شكراً لكم جميعاً من القلب.

ختاماً، أشكر كل من ساهم من قريب أو بعيد في إنجاز هذا العمل، راجياً من الله عز وجل أن يوفقني في خطواتي المستقبلية، وأن يكون هذا البحث إضافة قيمة للمجال الذي أدرس فيه.

عبد الرحمان

قائمة المختصرات

ج: الجزء

د. إ. ن: دون اسم الناشر

د. ب. ن: دون بلد النشر

د. ج: دون جزء

د. د. ن: دون دار النشر

د. س. ن: دون سنة النشر

د. ط: دون طبعة

ص: الصفحة

ط: الطبعة

ع: عدد

ق: قانون

ق. إ. ج: قانون الإجراءات الجنائي

ق. ج. ج: قانون الجنائي الجزائر

ق، ع، ج: القانون العقوبات الجزائري

ق، م، ج: القانون المدني الجزائري

P: page

ملخص الدراسة:

تسعى سياسة الجزائر لمكافحة الجريمة السيبرانية إلى تعزيز الأمن السيبراني من خلال تطوير تشريعات وطنية تتماشى مع التحديات الراهنة حيث تركز هذه السياسة على تحليل التحديات الكبيرة التي تواجهها البلاد، بما في ذلك نقص الموارد التقنية، الحاجة إلى التدريب المتخصص، وصعوبة التعاون الدولي في هذا المجال.

حيث هذه الدراسة أهمية تعزيز التعاون مع الدول الأخرى وتحديث التشريعات لمواكبة التطورات التكنولوجية المستمرة حيث تهدف الجزائر إلى تحسين القدرات الأمنية والتقنية، مما يسهم في توفير حماية فعالة ضد الجرائم السيبرانية في عصر الرقمنة من خلال هذه الجهود تأمل الجزائر في تحقيق بيئة رقمية آمنة تعزز من ثقة الأفراد والشركات في التعاملات الإلكترونية.

الكلمات المفتاحية: مكافحة الجريمة السيبرانية، الأمن السيبراني، التعاون الدولي، تطوير التشريعات الوطنية.

Abstract :

Algeria's policy for combating cybercrime aims to enhance cybersecurity by developing national legislation in line with current challenges. This policy focuses on analyzing the significant challenges facing the country, including the lack of technical resources, the need for specialized training, and the difficulty of international cooperation in this field.

The study highlights the importance of strengthening cooperation with other countries and updating legislation to keep pace with ongoing technological advancements. Algeria seeks to improve its security and technical capabilities, contributing to effective protection against cybercrime in the digital age. Through these efforts, Algeria hopes to achieve a secure digital environment that fosters trust among individuals and businesses in electronic transactions .

Keywords: combating cybercrime, cybersecurity, international cooperation, developing national legislation.

مقدمة

مقدمة:

يشهد العالم اليوم طفرة نوعية في محال المعاملات السيبرانية، حيث شهدت الألفية الأخيرة تطورا إلكترونيا مذهلا صاحبه تداخل وتباين التعاملات الاقتصادية والشخصية والتجارية والإدارية بما يعني تحول العالم من نمط الفضاء المغلق إلى نمط الفضاء المفتوح في كل المجالات وعلى كل المستويات وتعتبر الجرائم السيبرانية إحدى أهم الهواجس التي أصبحت تؤرق المواطن في حياته الشخصية والدول في سيادتها وأمنها، باعتبار أن التطور التكنولوجي والرقمي الهائل وما صاحبه من تأثير على كل المستويات أثر بشكل أو بآخر على أمن واستقرار الشعوب من جهة بل وأصبحت تداعيات هذه الثورة التكنولوجية تمس حرمة وخصوصية المواطن من جهة أخرى.

في ظل هذا التحدي الرقمي التكنولوجي الجديد سعت الدول إلى من حزمة من التشريعات والآليات القانونية والمؤسساتية للتصدي لهذه الجريمة التي أضحت تسمى في الأدبيات الأكاديمية بالجريمة الإلكترونية أو الجريمة السيبرانية.

والجزائر إحدى هذه الدول التي لم تكن في منأى من تداعيات هذه الظاهرة، حيث انتشرت في الآونة الأخيرة جرائم تمس بالحياة الشخصية للمواطن وتمس أيضا بأمن واستقرار البلاد وبكل جوانب الحياة الأخرى اقتصاديا سياسيا ثقافيا، ومست حتى البناء المجتمعي في تركيبته وبنايته.

من هنا سعى المشرع الجزائري إلى سن العديد من التشريعات والقوانين للتصدي لهذه الجرائم السيبرانية وأهم هذه التشريعات القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وغيره من التشريعات التي تدعم الحد من انتشار هذه الجرائم.

ومنه نطرح الإشكالية التالية:

إلى أي مدى ساهمت الجهود الدولية والوطنية المبذولة في مكافحة الجريمة السيبرانية؟

وتثير هذه الإشكالية عدة تساؤلات منها:

ماهي الجريمة السيبرانية؟

هل للجريمة السيبرانية أنواع؟

هل يوجد آليات لمكافحة هذه الجرائم؟

الفرضيات:

1. **الفرضية الأولى:** الجريمة السيبرانية قد تعتبر نوعاً جديداً من الجرائم التي تطورت مع التطور التكنولوجي وتستهدف خصوصيات الأفراد والشركات.

2. **الفرضية الثانية:** قد تُصنَّف الجرائم السيبرانية بناءً على أهدافها مثل جرائم اقتصادية، سياسية، أو اجتماعية.

3. **الفرضية الثالثة:** قد تشمل آليات المكافحة التعاون بين الدول والمنظمات الدولية من خلال تبادل المعلومات والخبرات.

أهمية الموضوع:

أهمية هذا البحث تتجلى في تقديمه لأسلوب علمي وقانوني يسهم في وضع إطار قانوني لمواجهة الجرائم المعلوماتية عبر الإنترنت، بالإضافة إلى اقتراح وسائل وآليات عقابية لمكافحتها. يأتي ذلك في ظل التطور السريع للجريمة المعلوماتية الذي لا يوازيه دائمًا تطور في الأطر القانونية والتشريعية، مما يؤدي إلى قصور في التشريعات الحالية في مواجهة هذا التهديد المتزايد. لذا، يبرز ضرورة إعادة تقييم الوسائل التقليدية للمكافحة وابتكار أساليب جديدة تضمن مكافحة فعّالة لهذه الجرائم. بالإضافة إلى ذلك، يسهم هذا البحث في إثراء المكتبة الجامعية، وخصوصًا مكتبة الحقوق، بموضوع متخصص في دراسة الآليات العقابية للجرائم الإلكترونية في التشريع الجزائري.

أسباب اختيار الموضوع:

من بين الأسباب التي دفعتني لاختيار هذا الموضوع:

1. **استفحال وانتشار الجرائم المعلوماتية:** مع تزايد انتشار هذه الجرائم، أصبحت تشكل هاجسًا وخطرًا عالميًا لما تسببه من أضرار جسيمة على اقتصاديات الدول. هذا الوضع يستدعي تأسيس أجهزة متخصصة للإشراف على مكافحة هذه الجرائم ووضع آليات فعالة للتحقيق فيها.

2. **قلة العناية الأكاديمية:** على الرغم من أهمية الجريمة المعلوماتية في الدراسات والبحوث، إلا أنها لم تحظ بالاهتمام الكافي من قبل الباحثين. غالبًا ما تم التعامل معها بشكل سطحي وصُنفت ضمن الجرائم

الأخرى دون التعمق في تفاصيلها. لذلك، من الضروري تقديم توضيح شامل لهذه الجريمة، سواء للدارسين أو لأولئك الذين يعملون على تطبيق النصوص القانونية المتعلقة بالمساس بالأنظمة المعلوماتية في الميدان العملي.

3. **الدمج بين الجانب النظري والتطبيقي:** يسعى هذا البحث إلى الجمع بين ما هو نظري وما هو تطبيقي، نظرًا لعدم تناول الدراسات السابقة لهذا الجانب بشكل كافٍ.

الدراسات السابقة:

1. **Dan Craigen &Others, Defining Cybersecurity, Technology innovation Management Review (Octobre 2014)**

تطرق الباحث في هذه الورقة الى تعريف الامن السيبراني، حيث وجد انه يوجد العديد من التعريفات لهذا المصطلح الحديث، وقام في هذه الورقة بتقديم تعريف جديد للامن السيبراني، وبدأ الورقة بالتهديدات التي ظهرت جراء الثورة المعلوماتية الكبيرة التي وصل لها ا□تمع اليوم، ومع تزايد هذه الجرائم بدات الدول تبحث عن استراتيجيات لمواجهتها.

2. **محمد أمين الرومي، جرائم الكمبيورتر والانترنت، (الاسكندرية، دار المطبوعات الجامعية، 2004)**

انطلق الكاتب من الثورة المعلوماتية الهائلة، وكيف انها اصبحت سلاح ذو حدين، فقد اصحب تحدث جرائم داخل الفضاء المعلوماتي او ما يطلق عليها بالجرائم السيبرانية، واصبحت هذه التهديدات تشكل خطرا كبيرا على الدول خاصة التي امنها المعلوماتي ضعيف، لذلك تم التفصيل في انواع هذه الجرائم لمواجهتها من طرف الدول.

3. **إلهام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، مؤسسة المنشورات العسكرية العدد ،630 (جانفي 2016)**

فصلت الباحثة في الجانب القانوني لمحاربة الجرائم السيبرانية، حيث قامت الجزائر مثلها مثل بقية دول العالم بوضع العديد من التشريعات والقوانيين للحد من خطورة التهديدات الالكترونية، ومحاولة ردع الأطراف

التي تقوم بتهديد المصالح العليا للبلاد، وتعتبر هذه التشريعات احد اهم الاستراتيجيات التي تقوم بها الجزائر لمواجهة هذه الجرائم السيبرانية.

تتناول الأوراق الثلاث موضوع الأمن السيبراني وجرائم الإنترنت من زوايا مختلفة. ركزت ورقة Dan Craigen وآخرين على تقديم تعريف جديد للأمن السيبراني في ظل الثورة المعلوماتية وتزايد التهديدات الإلكترونية، مسلطة الضوء على الحاجة لوضع استراتيجيات لمواجهتها. أما محمد أمين الرومي فقد تناول بالتفصيل أنواع الجرائم الإلكترونية، مشيراً إلى أنها تشكل خطراً كبيراً على الدول ذات الأنظمة الأمنية الضعيفة. من جهتها، ركزت إلهام غازي على الجانب القانوني في التشريع الجزائري، موضحة الجهود التشريعية المبذولة للوقاية ومكافحة الجرائم الإلكترونية، باعتبارها استراتيجية أساسية لحماية المصالح الوطنية.

منهج البحث:

المنهج الوصفي التحليلي: تحليل نصوص التشريعات والقوانين الوطنية والدولية المتعلقة بالجرائم السيبرانية، ودراسة أثرها على مكافحة هذه الجرائم.

المنهج المقارن: مقارنة التشريعات الجزائرية بالتشريعات الدولية لمعرفة مدى فعالية القوانين الجزائرية في مواجهة الجرائم الإلكترونية.

أهداف البحث:

تحديد مفهوم الجرائم السيبرانية وأنواعها :تقديم تعريف دقيق وشامل للجرائم السيبرانية، مع تسليط الضوء على الأنواع المختلفة لهذه الجرائم.

تحليل التشريعات الجزائرية :دراسة التشريعات والقوانين الجزائرية المتعلقة بالجرائم السيبرانية، مع التركيز على قانون 09/04 وأهم النصوص القانونية المرتبطة.

تقييم فعالية التشريعات :تقييم مدى فعالية التشريعات الجزائرية في مكافحة الجرائم السيبرانية ومدى توافقها مع التطورات التكنولوجية المتسارعة.

الوقوف على الآليات الوقائية :استعراض الآليات المؤسساتية والقانونية التي تبنتها الجزائر للحد من انتشار الجرائم السيبرانية وحماية المجتمع من آثارها السلبية.

صعوبات البحث:

1. نقص المعلومات: قلة المصادر الموثوقة حول السياسات الوطنية.
2. تحديث التشريعات: صعوبة متابعة التغييرات السريعة في القوانين.
3. التعاون الدولي: تحديات في جمع المعلومات بسبب اختلاف الأنظمة القانونية.
4. نقص الموارد التقنية: قلة الأدوات والبرامج اللازمة للتحليل.
5. تعقيد الموضوع: الحاجة لفهم عميق للتقنيات والتشريعات.
6. تباين الآراء: اختلاف وجهات النظر حول فعالية السياسات.

هيكل الدراسة:

للإجابة على هذه الإشكالية المركزية والأسئلة الفرعية للدراسة ولاختبار مدى صحة الفرضيات المقترحة ستتم دراسة الموضوع باعتماد خطة مكونة من ثلاثة فصول، نتطرق في الفصل الأول المعنون الإطار المفاهيمي والنظري للدراسة، أين قسم إلى مبحثين خصصنا المبحث الأول للبحث حول الإطار المفاهيمي والقانوني للجريمة أما بالنسبة للمبحث الثاني إفطار القانوني للجريمة.

أما الفصل الثاني والذي عنوانه: الجهود الدولية والوطنية، قسم كذلك إلى مبحثين وهي كالاتي: المبحث الأول وتطرقنا فيه إلى الآليات الدولية لمكافحة الجريمة السيبرانية، كما عنون المبحث الثاني: الآليات الوطنية لمكافحة الجريمة السيبرانية، وسنحاول التطرق فيه إلى كيف كافحا أكبر دولتان هذه الظاهرة

أما الخاتمة فسنعرض فيها نتائج البحث، حيث سنحاول الإجابة على التساؤلات المكونة للإشكالية المطروحة في بداية الدراسة، وسبر مدى صدق الفرضيات التي قمنا باقتراحها

اقتراح تحسينات: تقديم توصيات واقتراحات لتحسين التشريعات الوطنية وتعزيز البنية المؤسساتية لمكافحة الجرائم السيبرانية بفاعلية أكبر.

بالرجوع إلى مختلف المراجع والمكتبات يمكن القول أن هذا البحث ليس بجديد ولقد تناولته العديد من الدراسات والأبحاث في تخصصات مختلف نذكر منها ما يأتي: حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب،

جامعة باتنة،2011/2012، وكذلك دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منثوري، قسنطينة، 2012-2013، كما وجدنا أطروحة دكتوراه لـ: نسيمة درار الامن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني- دراسة مقارنة، جامعة أبي بكر بلقايد تلمسان-الجزائر، كلية الحقوق والعلوم السياسية، 2017، فقد استفدنا من الأبحاث السابقة وغيرها إلا أنها كانت تركز على جانب وتهمل جوانب أخرى، وأنها لم تعاصر التدابير الأمنية المستحدثة مؤخرا، وهو ما يميز دراستنا عن مثل هاته الأبحاث السابقة ذكرها.

الفصل الأول:

الإطار المفاهيمي و النظري للدراسة

تمهيد:

لقد شهد العالم في الآونة الأخيرة تطور ملحوظ في مجال التقنية، مما نتج عنه استعمال الحاسب الألي وشبكة الأنترنت في جميع الميادين، لكن قد يتم استخدام هذه الوسائل بطرق غير مشروعة، الأمر الذي قد ينجر عنه ارتكاب جرائم لها علاقة بهذا المجال، وهو ما يعرف بالجريمة السيبرانية، ونظرا لحداثة هذه الجريمة، فقد اختلف الفقهاء في وضع تعريف موحد لها، كما اتسمت بمجموعة من الخصائص، وعرفت نوع جديد من المجرمين لهم عدة دوافع لارتكاب هذه الجريمة، وسأحاول التطرق في هذا الفصل إلى مفهوم الجريمة السيبرانية وأنواعها في المبحث الأول، التشريعات الوطنية والدولية الجريمة السيبرانية في القانون الجزائري من خلال المبحث.

المبحث الأول: الإطار المفاهيمي والقانوني للجريمة

لقد تطورت أساليب ارتكاب الجرائم عما هو معروف سابقا، فلم تعد الاعتداءات تهدف النفس والمال فقط، بل تعدتها إلى المعلومات والبيانات الخاصة بمتعاملي البيئة الرقمية، إذ أصبح بإمكان المجرمين ارتكاب أبشع الجرائم في هدوء تام دون إراقة للدماء، وذلك بسبب ظهور نوع جديد من الجرائم لم تكن معروفة سابقا. يطلق عليها بالجرائم.

وبناء على ذلك سنخصص المبحث الأول للتعرف على هذا النوع الجديد من الجرائم من خلال التطرق إلى تعريفها وإلى أنواعها وذلك في (المطلب الأول) وإلى إطارها القانوني (المطلب الثاني).

المطلب الأول: مفهوم الجريمة السيبرانية

لغرض الإحاطة بماهية الجريمة السيبرانية، سنقسم هذا المطلب على فروع، سنبني في الفرع الأول التعريف اللغوي للجريمة والتعريف الشرعي لها، وفي الفرع الثاني تعريف الجريمة السيبرانية.

الفرع الأول: تعريف الجريمة المعلوماتية

أولا: التعريف الفقهي

اختلفت تعريفات الفقهاء والاساتذة تبعا للدولة صاحبة الانتماء وتبعا لمعيار التعريف ذاته، ونحاول في هذا الصدد جمع غالبية التعريف التي وضعت في هذا الحقل.

من التعريفات التي تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك محل التجرم، تعريف الأستاذ ROSENBALT بأنه نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقة أو هي كما عرفها الفقيه سولاربز أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات[1].

أما التعريفات التي تعتمد على وسيلة ارتكاب الجريمة، فيرى أصحابها أن الجرائم المعلوماتية تحدث عندما يُستخدم الكمبيوتر كأداة لتنفيذ الجريمة. ومن هذه التعريفات نجد:

[1] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لاستكمال شهادة الماستر المهني الطور الثاني، جامعة قاصي مرباح، الجزائر، 2018-2019، ص03.

تعريف الأستاذ جون فور ستر " **فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية وبعرفها تادمان بأنها كل أشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب**"[1].

ومن التعريفات كذلك نجد أنها الجريمة التي تقوم على أساس سمات شخصية لدى مرتكب الفعل، تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية أي جريمة لفاعلها معرفة فنية بالحاسبات تمكن من ارتكابها.

كما عرفها الأستاذ" دافيد تومسن "**أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي**"[2].

تباينت تسميات الجريمة الالكترونية عبر مراحل تطورها والذي ارتبط أساسا بتقنية المعلومات، فقد أصطلح على تسميتها في البداية بإساءة استخدام الكمبيوتر ثم احتيال الكمبيوتر، فالجريمة المعلوماتية ثم جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر ثم جرائم التقنية العالية إلى جرائم الهاكر، فجرائم الانترنت وأخيرا السايبركرايم.

وتعرف الجريمة الإلكترونية بأنها: "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكات الانترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها"[3].

واتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية للجريمة المعلوماتية في اجتماع باريس سنة 1983 م على أنها: "**كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها**"[4].

ويمكن تعريف الجريمة الإلكترونية بأنها: "**كل أشكال السلوك غير المشروع والمتعمد الذي يرتكب باستخدام الحاسب الآلي المرتبط بالإنترنت والتي تمس به أو بمحتوياته أو بالعمليات التي تتم بواسطته**

[1] هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص120.

[2] هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة، 2000، ص 20.

[3] ياسمينة بونعارة، "الجريمة الإلكترونية"، جامعة: الأمير عبد القادر للعلوم الإسلامية، د س ن، ص 03.

[4] ياسمينة بونعارة، نفس المرجع، ص 04.

بغرض إلحاق الضرر بالضحية أو الكسب المادي أو غير ذلك من الأغراض من طرف أفراد على دراية كاملة بتقنيات التكنولوجيا المعلوماتية وأسرارها"[1].

الفرع الثاني: التعريف القانوني للجريمة

لم يعرف المشرع الجزائري شأنه شأن جل التشريعات العقابية المقارنة الجريمة، ولعل سبب يرجع في كون أن وضع التعاريف للمفاهيم القانونية العامة هو عمل فقهي وليس من عمل المشرع، لذلك يعرف الفقه القانوني الجريمة بصفة عامة على أنها "**فعل غير مشروع صادر عن إرادة جرمية يقرر له القانون العقوبة أو التدبير احترازيا**"، كما تعرف على أنها "**كل تصرف جرمه القانون سواء كان إيجابيا أو سلبيا كالامتناع ما لم يرد نص على خلاف ذلك**"[2].

أما بالنسبة لمفهوم الجريمة فلم يتفق الفقهاء والباحثون على تعريف موحد لهذه الأخيرة فمنهم من ينظر إلى موضوع الجريمة في حد ذاتها، وهناك من ينظر إلى الوسيلة المستعملة في ارتكابها، هذا على غرار أنهم لم يتفقوا على تسمية موحد لهذا النوع الجديد من الجرائم التي تباينت تسمياتها عبر مراحل زمنية ارتبطت بتقنية المعلومات[3]، فهناك من يطلق عليها بتسمية الجرائم cybre crime " وهناك من يطلق عليها بتسمية الجرائم السيبرانية وجانب أخر من الفقه يطلق عليها بتسمية إساءة استخدام تكنولوجيا المعلومات والاتصال، كما يطلق عليها أيضا بجرائم الكومبيوتر والأنترنت.

وعلى العموم يتراوح تعريف الجريمة بين الجرائم التي ترتكب عبر الحاسب الآلي وبين الجرائم التي ترتكب عبر مختلف المعدات الرقمية، غير انه يمكن تعريفها على أنها "**نشاط إجرامي تستخدم فيه التقنية السيبرانية (الحاسب الآلي وشبكة الأنترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي**"[4].

---

[1] ياسمينة نوعارة، نفس المرجع، ص 04.

[2] فريد روابح، محاضرات في القانون الجنائي العام، مطبوعة الدروس السنة الثانية ليسانس، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، 2018/2019، ص 29.

[3] رامي متول القاضي، مكافحة الجرائم المعلوماتية، دون طبعة، دار النهضة العربية، مصر، 2011، ص 17.

[4] جدو بن علية، تحديات الأمن السيبراني في مواجهة الجريمة السيبرانية، المجلة الجزائرية للأمن الإنساني، جامعة الحاج الخضر، باتنة، المجلد 07، العدد 02 جويلية 2022، ص 304.

كما يمكن تعريفها على أنها "**سلوك غير قانوني يتم باستخدام الأجهزة السيبرانية، ينتج عنها حصول المجرم الرقمي على فوائد مادية ومعنوية، وغالبا ترتكب هذه الجرائم عبر القرصنة أو الاختراق للأنظمة المعلوماتية**"[1].

وتعرف أيضا على أنها "**السلوك غير المشروع والمنافي للأخلاق أو غير المسموح به المرتبطة بالشبكات المعلوماتية العالمية فهي تعد من الجرائم العصر الرقمي التي تطال بالمال والمعرفة والثقة والسمعة وهي كلها تنفذ عن طريق التقنية**" [2].

أما بالنسبة للمشرع الجزائري نجده أنه لم يستقر على استخدام مصطلح واحد للدلالة على هذه الجرائم حيث أطلق عليها تسمية: "**الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات**" وذلك بموجب القانون رقم 04/15 المتعلق بقانون العقوبات[3]، كما أن استخدم مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[4] بموجب القانون رقم 09/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. وتعتبر هذه التسميات التي اعتمد عليها المشرع الجزائري دلالة على الجرائم حيث عرفها على أنها جرائم الماسة بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصال السيبرانية"[5].

المطلب الثاني: أنواع الجرائم في القانون الجزائري

تصنف الجريمة التقليدية بحسب خطورتها إلى جناية وهي أخطر الجرائم، وجنحة وهي متوسطة الخطورة، ثم مخالفة وهي أقل خطورة، وتصنف بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية[6]. على خلاف هذه الجريمة، فإن الجريمة السيبرانية عرفت اختلاف حول تقسيماتها،

---

[1] علي قويدري، أمال العيش، الجريمة السيبرانية مفهومها وسبل الوقاية منها، مجلة نوميرس الاقتصادية، المجلد الثالث، العدد01، 2022، ص194.

[2] روان بنت عطية الله الصحفي الجرائم السيبرانية، المجلة السيبرانية الشاملة متعددة التخصصات، العدد 24 ماي 2020، ص 08.

[3] القانون رقم 15/04، المؤرخ في 10/11/2004، المعدل والمتمم للقانون رقم 66/156، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، لسنة 2004.

[4] القانون رقم 09/04 المؤرخ في 05/08/2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، الجريدة الرسمية، العدد 47، الصادر بتاريخ 1/08/2009

[5] المادة 01 من القانون رقم 09/04، السابق ذكره.

[6] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية،2002 ط،01 ص 24.

وذلك بسبب الاختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة، والبعض الآخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيما على تعدد محل الاعتداء وتعدد الحق المعتدى عليه[1]. أما بالنسبة للمشرع الجزائري فقد قسم الجريمة السيبرانية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال، أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات، وهذا ما سيتم بيانه في الفرعين الموالين.

الفرع الأول: الجريمة المرتكبة باستخدام النظام المعلوماتي.

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص[2]، الجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار، وسأوضح كل نوع منها تاليا:

أولا: الجريمة السيبرانية الواقعة على الأشخاص الطبيعية

تنقسم هذه الجرائم بدورها إلى جرائم واقعة على حقوق الملكية الفكرية، وجرائم واقعة على حرمة الحياة الخاصة.

1- الجريمة السيبرانية الواقعة على حقوق الملكية الفكرية:

يُعتبر النظام المعلوماتي أداةً يمكن استخدامها في انتهاك حقوق الملكية الفكرية، من خلال عمليات مثل سرقة البيانات وتخزينها واستخدامها دون الحصول على إذن من مالكها. يُعد استخدام المعلومات بدون إذن من أصحابها اعتداءً على حقوقهم المعنوية، بالإضافة إلى أنها قد تشكل اعتداءً على قيمتها المالية، حيث تكتسب المعلومات قيمة أدبية بجانب قيمتها المادية. تشمل حقوق الملكية الفكرية أيضاً براءات الاختراع، التي تعبر عن أفكار للمخترع وتحمل حقوقاً معنوية ومالية له. وقد نظم المشرع الجزائري حقوق الملكية الفكرية من خلال

[1] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، -2011 ص 69.

[2] سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبوبكر بلقايد، تلمسان، -2010 ص 33.

تشريعات محددة، وهي الأمر رقم 03-05 الصادر في 2003 بشأن حقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الاختراع[1].

2- الجريمة السيبرانية الواقعة على حرمة الحياة الخاصة:

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الاعتداء على هذه الحرمة.

ولما كان الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين أكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الآلي دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص أخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها باطلاع الغير عليها دون إذن صاحبها، أو أن يقوم شخص باختراق معلومات هي بمثابة أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص آخر.

ثانياً: الجريمة السيبرانية الواقعة على النظم المعلوماتية الأخرى

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدام البطاقة الائتمانية.

بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الاستيلاء على المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة، أو استخدام شاشة النظام، أو الاطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، أما الحالة الثانية تكون في حالة اساءة استخدام العميل البطاقة الائتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الائتمانية شروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة ائتمانية انتهت مدة صلاحيتها أو تم إلغاؤها[2]، أما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة ائتمانية للحصول على السلع والخدمات[3].

[1] سوير سفيان، رسالة الماجستير السابقة الذكر، ص 35.

[2] سوير سفيان، رسالة الماجستير السابقة الذكر، ص -35.37-36

[3] سوير سفيان، رسالة الماجستير السابقة الذكر، ص -35.

ثالثاً: الجريمة السيبرانية الواقعة على الأسرار

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة ويتخذ هذا النوع من الجرائم صورتين[1]، الأولى تتعلق بالجرائم الواقعة على أسرار الدولة، حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الامتناع عن القيام بعمل[2].

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة61 إلى المادة 96 مكرر من قانون العقوبات، بالإضافة إلى المادة394 مكرر 03 التي تنص على: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد[3]".

الفرع الثاني: الجريمة السيبرانية الواقعة على النظام المعلوماتي.

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 15-04 الصادر في 10 نوفمبر2004 المتضمن قانون العقوبات بتجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر إلى 394 مكرر،07 وتأخذ صور الاعتداء صورتين وهما: الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش، وهذا ما سأتناوله تالياً:

أولاً: جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتية

[1] سوير سفيان، نفس الرسالة، ص 38.

[2] سوير سفيان، رسالة الماجستير السابقة الذكر، ص.38

[3] القانون رقم 15-04 الصادر في 10 نوفمبر2004 يعدل ويتمم الأمر رقم،66/156 الصادر في 08 جوان 1966 المتضمن قانون العقوبات.

تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الألية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام[1].

1- فعل الدخول غير المشروع:

لا نعني هنا الدخول بالمعنى المادي، أي الدخول إلى مكان معين كمنزل أو غيره، وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الألية للمعطيات، وتقع هذه الجريمة من كل إنسان أيا كانت صفته سواء كان شخص يعمل في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع أن يستفيد من الدخول أم لا، فيكفي أن يكون الجاني ممن ليس له الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط، أي أن الجريمة تقوم بفعل الدخول إلى النظام مجردا عن أي نتيجة أخرى، ولا يشترط لقيامها التقاط أو حصول الشخص على المعلومات الموجودة داخل النظام أو البعض منها، بل أن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام، ففعل الدخول يتسع ليشمل كل فنيات الدخول الاحتيالي في منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لا حق له في ذلك المفتاح للدخول إلى المنظومة[2].

2- فعل البقاء غير المشروع:

يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في النظام وقد يجتمعان، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، وهنا يجب على المتدخل أن يقتطع وجوده داخل النظام وينسحب، فإذا بقي رغم

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة،2011/2012 ص،13 نقلا عن قورة نائلة، جرائم الحاسب الاقتصادية القاهرة، ص 182.

[2] حمزة بن عقون، نفس المرجع، ص 182-183.

ذلك فإنه يعاقب على جريمة البقاء غير المشروع، ويكون البقاء جريمة في الحالة التي يطبع الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الاطلاع فقط، ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، والتي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على مدة أطول من المدة التي دفع مقابلها، ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد، وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية[1].

ثانياً: جريمة المساس بمنظومة معلوماتية

نصت المادة 394 مكرر 01 من قانون العقوبات رقم 04/15 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش. هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي، وأفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها[2].

ثالثاً: أفعال إجرامية أخرى.

جرمت المادة 394 مكرر02 من قانون العقوبات السابق الذكر الأعمال الأتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابقة الذكر[3]، ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية،

[1] حمزة بن عقون، رسالة الماجستير، ص183.

[2] دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منثوري، قسنطينة، 2012،2013- بدون صفحة.

[3] حمزة بن عقون، رسالة الماجستير، ص 184.

أو المعطيات المعلوماتية في حد ذاتها، كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لأي غرض.

من خلال التعرض إلى ماهية الجريمة السيبرانية، يتضح بأن لهذا النمط من الجرائم طبيعة خاصة ومتميزة، وهي جريمة ناعمة حال ارتكابها، تتجاوز حد الخشونة في نتائجها، إذ بمجرد ملامسة الجاني لزر أو أكثر من لوحة المفاتيح، قد ترتكب أخطر الجرائم في بضعة ثواني، ودون التقاء بين الجاني والمجني عليه، وهذا ما يؤدي إلى صعوبة في مكافحتها، ويعاب على المشرع الجزائري أنه اهتم بالجريمة السيبرانية بالنص على بعض الجرائم السيبرانية وليس كلها وأهمل المجرم الإلكتروني، إذ لم يتعرض له في أي نص قانوني، بالإشارة إلى تعريفه أو سماته. كما أن التطرق لماهية الجريمة السيبرانية والتعرف عليها بعمق يفيدنا في إيجاد الحلول لمواجهتها[1].

[1] حمزة بن عقون، رسالة الماجستير السابقة الذكر، ص 184-185.

المبحث الثاني: الإطار القانوني للجريمة

في العديد من الأنظمة القانونية، يتم تقسيم القوانين الجنائية إلى أنواع مختلفة مثل القوانين التي تتعلق بالجرائم العادية مثل السرقة والاعتداء، والقوانين التي تتعلق بالجرائم الخاصة مثل الجرائم الإلكترونية والجرائم الاقتصادية. هذا التصنيف يساعد في تخصيص الموارد القانونية بطريقة فعالة وتقديم عقوبات مناسبة لكل نوع من الجرائم.[1]

في السياق الحديث، يتزايد اهتمام الأنظمة القانونية بالجريمة الإلكترونية بسبب الانتشار الواسع للتكنولوجيا وتزايد الجرائم المرتبطة بها، مما يتطلب تحديث القوانين بانتظام لمواكبة التغيرات التكنولوجية وتحدياتها، وعليه تم تقسيم المبحث إلى مطلبين، المطلب الأول التشريعات الوطنية، المطلب الثاني: التشريعات الدولية.

المطلب الأول: التشريعات الوطنية

هي مجموعة القوانين واللوائح التي تصدرها السلطة التشريعية في دولة معينة لتنظيم العلاقات والأنشطة داخل حدود تلك الدولة. تهدف هذه التشريعات إلى تحقيق النظام والعدالة، وتوفير إطار قانوني ينظم حقوق وواجبات الأفراد والمؤسسات. تشمل التشريعات الوطنية القوانين المتعلقة بالجرائم والعقوبات، الحقوق المدنية، قوانين الأسرة، العمل، والتجارة، وغيرها من المجالات. تعتبر هذه التشريعات الأساس الذي يقوم عليه النظام القانوني في البلاد، وهي تعكس القيم والمبادئ التي تنظم الحياة الاجتماعية والاقتصادية والسياسية في الدولة.[2]

الفرع الأول: واقع الجريمة في الجزائر

شهدت الجزائر في السنوات الأخيرة ارتفاعاً كبيراً في معدلات الجرائم السيبرانية، حيث سُجلت أكثر من 500 حالة مُبلغة في عام 2016، لكن من المؤكد أن العدد الفعلي أكبر بكثير، نظرًا لامتناع بعض الضحايا

[1] غازي إلهام، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، (جانفي 2016)، ص 30.

2 بوعلام، ملتقى حول " الجيش الوطني الشعبي ورهانات تداول المعلومات عبر شبكات التواصل الاجتماعي "مجلة الجيش، العدد 630، (جانفي 2016)، ص 50.

عن التبليغ لأسباب اجتماعية وثقافية. في هذا السياق، كثفت مصالح الدرك الوطني جهودها لحماية مستخدمي الإنترنت، خاصة رواد مواقع التواصل الاجتماعي الذين يمثلون شريحة كبيرة من المستخدمين[1].

في عام 2017، سجلت مصالح الدرك والشرطة حوالي 2500 جريمة إلكترونية شملت جرائم مثل القرصنة، الابتزاز، التشهير، والتحرش الإلكتروني. وكانت نسبة 80% من هذه الجرائم مرتبطة بموقع "فيسبوك"، حيث تعرض العديد من الأشخاص للابتزاز والتهديد بنشر صور مفبركة.

أكد هواري قدور، رئيس الرابطة الجزائرية للدفاع عن حقوق الإنسان، أن الرابطة تعمل بجدية على مواجهة هذه الظاهرة، داعيًا إلى فرض عقوبات صارمة على مرتكبي الجرائم السيبرانية. وفي عام 2020، شهدت الجزائر طفرة في عدد الجرائم السيبرانية، حيث تجاوز عدد القضايا المسجلة 8 آلاف جريمة، ما جعل هذه الجرائم تنافس الجرائم التقليدية من حيث الانتشار والخطورة.[2]

وفي تقرير حديث، أشارت المديرية العامة للأمن الوطني إلى أن عدد الجرائم السيبرانية المسجلة قفز من 500 جريمة في عام 2015 إلى 5200 قضية في عام 2020، فيما سجلت قيادة الدرك الوطني 1362 جريمة سيبرانية تورط فيها 1028 شخصًا. وأظهرت التحليلات أن الجرائم المتعلقة بالقذف والسب عبر الإنترنت كانت الأكثر شيوعًا بنسبة تجاوزت 55%.

أما على صعيد استخدام الإنترنت، فقد ارتفع عدد مستخدمي الإنترنت في الجزائر بمقدار 3.6 مليون مستخدم خلال عام واحد، ليصل العدد الإجمالي إلى 26.35 مليون مستخدم بحلول يناير 2021. كما زاد عدد مستخدمي مواقع التواصل الاجتماعي بنسبة 13.6% خلال نفس الفترة، ليصل إلى 25 مليون مستخدم، يمثلون 56.5% من سكان البلاد. وفي مواجهة التهديدات السيبرانية، نجحت شركة "كاسبرسكي" في إحباط 95 ألف هجوم إلكتروني على الجزائر خلال عام 2020، ما جعل الجزائر في المرتبة الأولى عربياً والـ 14 عالمياً من حيث التعرض للهجمات السيبرانية[3].

---

[1] سعيدة بوزنون مكافحة الجريمة السيبرانية في التشريع الجزائري مجلة العلوم الانسانية، 2019، ص 5.

[2] خديجة بودومي، الجريمة السيبرانية بالجزائر. DW عربية 2018، تاريخ المعاينة 14 أوت 2024.

[3] المديرية العامة للأمن الوطني مصالح شرطة مكافحة الجرائم السيبرانية تسجل 567 قضية تتعلق بجرائم الأنترنت. تاريخ المعاينة 07 جويلية 2024، من موقع الشرطة الجزائرية https://www.algeriepolice dz.

من بين الجرائم السيبرانية التي هزت الجزائر في عام 2021، برزت قضية النصب على الطلبة باستخدام المؤثرين (يوتيوبرز)، وهي قضية أثارت جدلاً واسعاً حيث لا يزال التحقيق جارياً فيها. وقد تم حبس 11 متهمًا، فيما وُضع باقي المتورطين تحت الرقابة.

وعلى صعيد آخر، سجلت المديرية العامة للأمن الوطني، المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، 567 قضية متعلقة بجرائم الإنترنت خلال الأشهر الثمانية الأولى من العام نفسه. تورط في هذه القضايا 543 شخصًا. وقد تمكنت الفرق المتخصصة في مكافحة الجرائم السيبرانية من معالجة 385 جريمة إلكترونية من إجمالي القضايا المسجلة، وذلك من خلال تحليل كافة المعطيات التقنية والأدلة المادية المرتبطة بهذه القضايا[1].

هذه الأرقام تعكس التحديات المتزايدة التي تواجهها الجزائر في مواجهة الجريمة السيبرانية، وتؤكد على الحاجة الملحة لتعزيز الجهود الأمنية والتقنية لمكافحة هذه الظاهرة المتنامية.

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الأنترنت	430	289	365	68%
جرائم الإعتداء على سلامة الأنظمة المعلوماتية	57	31	39	55%
جرائم الإحتيال عبر الأنترنت	25	17	32	68%
جرائم التحريض والتطرف عبر الأنترنت	14	14	31	100%
الجرائم المخلة بالحياء	12	08	22	67%
جرائم بيع السلع المحضورة عبر الأنترنت	06	05	15	84%

[1] آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007 ص102.

جرائم مختلفة(نسخ البرامج دون حق، القرصنة)	23	21	39	92%
المجموع	567	385	543	68%

المصدر: المديرية العامة للأمن الوطني، مصالح شرطة مكافحة الجرائم السيبرانية تسجل 567 قضية تتعلق بجرائم الأنترنت 2021

واستنادا على ما سبق، وبعد التعرض إلى واقع الجريمة السيبرانية في الجزائر الذي هو في تزايد مستمر نظرا لسهولتها واختلاف فئات المجرمين شرع المشرع الجزائر قوانين موضوعية واجرائية ووقائية بداية من 2004 لاحتواء الجريمة السيبرانية والتصدي لها وهذا ما يتضح في تعريفه لها هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات السيبرانية[1].

الفرع الثاني: قوانين الجريمة السيبرانية الموضوعية والإجرائية والوقائية في التشريع الجزائري

في التشريع الجزائري، تشمل قوانين الجريمة السيبرانية ثلاثة جوانب رئيسية:

1. **القوانين الموضوعية:** تحدد الجرائم السيبرانية وأنواع الأفعال غير القانونية المرتبطة بالتكنولوجيا، مثل الاختراقات الإلكترونية والاحتيال الرقمي، وتحدد العقوبات المناسبة لها.

2. **القوانين الإجرائية:** تتناول الإجراءات المتبعة للتحقيق في الجرائم السيبرانية وتقديم الجناة للعدالة، بما في ذلك طرق جمع الأدلة الرقمية والمحاكمات.

3. **القوانين الوقائية:** تهدف إلى تعزيز الأمان السيبراني والوقاية من الجرائم الإلكترونية من خلال نشر الوعي والتدابير الأمنية.

تسعى هذه القوانين إلى مواكبة التطورات التكنولوجية وحماية الأفراد والمؤسسات من المخاطر الرقمية.

1. القانون رقم 04/15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، ج.ر، عدد 71:

لقد جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي (الحاسوب والشبكة) في قانون العقوبات بموجب القانون 04/15 تحت عنوان ": المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن، وباعـتباره

[1] خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر،،2010 ص.

القانون الأول في هذا القسم الـسابع ستة مواد من المادة 394 مكرر إلى 394 مـكرر 6 مجال الجريمة السيبرانية سنعرض مواده بالتفصيل[1]، وجاء فيه:

المادة 394 مكرر:

– يعاقب بالحبس من ثلاثة أشهر إلى ستة أشهر، وبغرامة من 50.000 إلى 100.000 دينار جزائري، كل من يدخل أو يبقى بشكل غير مشروع في كل أو جزء من منظومة المعالجة الآلية للمعطيات، أو يحاول ذلك.

– تضاعف العقوبة إذا نتج عن هذا الفعل حذف أو تغيير في المعطيات المخزنة في المنظومة.

– إذا أدى هذا الفعل إلى تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من سنة إلى سنتين، وغرامة من 50.000 إلى 150.000 دينار جزائري.

– تشمل هذه المادة الجرائم المتعلقة بالحاسوب وبيانات شبكة الإنترنت.[2]

المادة 394 مكرر 1:

– يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من 500.000 إلى 2.000.000 دينار جزائري، كل من يدخل معطيات بشكل غير مشروع في نظام المعالجة الآلية للمعطيات، أو يقوم بإزالة أو تعديل المعطيات الموجودة فيه بطرق غير مشروعة.

– تم تشديد العقوبة في هذه المادة نظرًا لخطورة الجرائم السيبرانية المرتبطة بالدخول غير المصرح به، واستخدام تقنيات متقدمة مثل القنابل المعلوماتية أو الفيروسات.[3]

المادة 394 مكرر 2:

– يعاقب بالحبس من شهرين إلى ثلاث سنوات، وبغرامة من 1.000.000 إلى 5.000.000 دينار جزائري، كل من يقوم عمدًا بواحد أو أكثر من الأفعال التالية بطرق غير مشروعة:

1. تصميم، بحث، تجميع، توفير، نشر، أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عبر منظومة معلوماتية يمكن استخدامها في ارتكاب الجرائم المنصوص عليها في هذا القسم.

---

[1] القسم السابع مكرر: المساس بأنظمة المعالجة الآلية للمعطيات الجريدة الرسمية، 2004، ص 11–12 –14.

[2] Maras, M.–H. Cybercriminology. Oxford University Press. 2016. P 132 16

[3] قانون رقم 22 – 06 المعدل والمتمم للأمر 15566 المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية، ص 87

2. حيازة، إفشاء، نشر، أو استخدام لأي غرض كان، المعطيات المتحصل عليها عبر الجرائم المنصوص عليها في هذا القسم.

المادة 394 مكرر 3:

– تضاعف العقوبات المنصوص عليها في هذا القسم إذا كانت الجريمة تستهدف الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون المساس بتطبيق عقوبات أشد، نظرًا لخطورة هذه الجرائم السيبرانية على الأمن القومي واستقرار البلاد.[1]

المادة 394 مكرر 4:

– يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

– يقصد بالشخص المعنوي المؤسسات والمنظمات، بينما الشخص الطبيعي هو الفرد.

المادة 394 مكرر 5:

– يعاقب بالعقوبات المقررة للجريمة ذاتها كل من شارك في مجموعة أو اتفاق يهدف إلى الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدًا بفعل أو عدة أفعال مادية.

– وهنا، يوضح المشرع أن العقوبة لا تقتصر على مرتكب الجريمة فقط، بل تشمل أيضًا كل من شارك في التخطيط أو التحضير لها.

المادة 394 مكرر 6:

– تُصادر الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجرائم المنصوص عليها في هذا القسم، مع الاحتفاظ بحقوق الغير حسن النية.

– تغلق المواقع التي تكون محلًا للجريمة، كما يغلق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه.

[1] 12 قانون رقم 09-04 المؤرخ في 2009 الجريدة الرسمية 2009، ص 12

– هذه المادة تشير إلى أن صاحب المقهى الإلكتروني (مقهى الإنترنت) يمكن أن يعاقب إذا ارتكبت جريمة إلكترونية في محله بعلمه.

تحليل عام للقانون:

يُعتبر هذا القانون من القوانين الموضوعية التي تركز على جوهر الجريمة، حيث تشمل عناصر الجريمة الفعل المحظور (الفعل الإجرامي) والنية الجرمية (العقل المذنب). يتضمن القانون أيضًا عقوبات للسلوكيات المحظورة المرتبطة بالجرائم السيبرانية.

الجرائم السيبرانية تشمل جرائم تقليدية يمكن ارتكابها عبر الإنترنت مثل الاحتيال والتزوير وغسل الأموال، بالإضافة إلى جرائم "جديدة" تعتمد على التكنولوجيا الرقمية.

العديد من الدول، مثل ألمانيا واليابان والصين، قامت بتعديل قوانينها لمكافحة الجرائم السيبرانية، واستخدمت القوانين القائمة لمعالجة هذه الجرائم. وفي العراق، يُستخدم القانون المدني الحالي وقانون العقوبات لمحاكمة الجرائم المرتكبة عبر الإنترنت.

القوانين الإجرائية:

يتضمن هذا القانون قواعد وإجراءات تحدد كيفية تطبيق القانون الموضوعي وإنفاذه، مع التركيز على حقوق الأشخاص المتهمين والتعامل معهم في إطار نظام العدالة.[1]

يشمل قانون الجرائم السيبرانية الإجرائي أحكامًا بشأن الاختصاص القضائي وسلطات التحقيق، وقواعد جمع الأدلة والإجراءات الجنائية المتعلقة بالبحث والمصادرة وحفظ البيانات.

قام المشرع الجزائري بتعديل القانون الإجرائي في عام 2006 لمواكبة تطورات الجرائم السيبرانية، حيث تم تحديد مدد توقيف النظر وإجراءات التحري والتحقيق في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

كما أصدر المشرع قانونًا وقائيًا في عام 2009 لمكافحة الجرائم السيبرانية بشكل أكثر فعالية.

2. القانون الوقائي رقم 09/04، الصادر بتاريخ 5 أغسطس 2009

[1] وتوغي نبيل، زيوش عبد الرؤوف الجريمة المعلوماتية في التشريع الجزائري. مجلة العلوم القانونية 139–127 والاجتماعية، 2019، ص20 .

ينظم القواعد المتعلقة بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات ومكافحتها. يهدف هذا القانون إلى تحديد معايير خاصة لمواجهة هذه الجرائم، مع استبدال مصطلح "جرائم منظومة المعالجة الآلية للمعطيات" بعبارة "الجرائم المتعلقة بتكنولوجيات المعلومات والاتصال"، التي تعتبر مرادفًا لمصطلح الجريمة السيبرانية.

في الفصل الثالث، يحدد القانون شروط اللجوء إلى المراقبة السيبرانية كإجراء وقائي ضد الأفعال الإرهابية والتهديدات للأمن الوطني وحماية الحياة الخاصة. بينما يتناول الفصل الرابع الإجراءات المتعلقة بتفتيش المنظومات المعلوماتية، موضحًا كيفية تعامل ضباط الشرطة مع الجرائم السيبرانية، بما في ذلك تفتيش الأنظمة والوصول إلى الحسابات وتخزين البيانات كأدلة، مع النص على ضرورة التعاون مع السلطات الأجنبية إذا كانت المعلومات خارج حدود البلاد.

كما يفرض القانون في الفصل الخامس التزامات على مقدمي الخدمات، مثل جمع وتسجيل بيانات الاتصالات، والحفاظ على السرية تحت طائلة العقوبات. يشمل ذلك أيضًا كيفية التعرف على مصدر الاتصال وتحديد موقعه، وتحديد العقوبات للمخالفين[1].

وفي الباب الخامس، ينص القانون على إنشاء هيئة وطنية للوقاية من الجرائم السيبرانية ومكافحتها، وتوضيح مهامها في التنسيق والبحث وتبادل المعلومات. كما يركز الباب السادس على التعاون الدولي في مكافحة الجريمة السيبرانية، متضمنًا إجراءات تبادل الأدلة والمساعدة القضائية الدولية، مع التأكيد على عدم المساس بالسيادة الوطنية.

يظل هذا القانون ساري المفعول حتى اليوم ويعد مرجعًا قانونيًا مهمًا في معالجة الجرائم السيبرانية في الجزائر.

في سياق الجرائم السيبرانية، يركز القانون الوقائي الجزائري على تنظيم وإدارة المخاطر المتعلقة بالتكنولوجيا والاتصالات. تسعى التشريعات الوقائية إلى تحقيق هدفين رئيسيين: الأول، منع الجرائم السيبرانية بقدر الإمكان، والثاني، تقليل الأضرار الناجمة عن حدوثها. مثالاً على ذلك، هناك قوانين مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي لعام 2016، واتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية

[1] قانون رقم 09-04 المؤرخ في 2009 الجريدة الرسمية 2009، ص 22.

البيانات الشخصية لعام 2014، بالإضافة إلى قوانين الأمن السيبراني مثل قانون أوكرانيا بشأن المبادئ الأساسية لضمان الأمن السيبراني لأوكرانيا لعام 2017.[1]

تساهم هذه القوانين في تقليل الأضرار المادية الناتجة عن الانتهاكات الجنائية للبيانات الخاصة، كما تهدف إلى تقليل تعرض القطاع الخاص للخطر. كما تساهم التشريعات في تحديد الجرائم السيبرانية، وتوفير الأدوات والتدابير اللازمة للتحقيق ومقاضاة مرتكبيها، من خلال ضمان وجود البنية التحتية المناسبة لمزودي خدمات الاتصالات السيبرانية، بما في ذلك التنصت على المكالمات الهاتفية والبيانات.

مع صدور القانون رقم 09/04 والقانون رقم 20-06، تم تعزيز الجهود في مكافحة الجرائم السيبرانية في الجزائر. وقد تضمن هذا التطور إنشاء القطب الجزائي الوطني لمحاربة الجريمة السيبرانية، والذي يهدف إلى تشديد العقوبات على الجرائم وتعزيز الإجراءات القانونية لملاحقة الجناة. سيتم تناول تفاصيل هذا الأمر في القسم التالي[2].

3. الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021 المتعلق بإنشاء القطب الجزائي الوطني المتخصص في محاربة الجريمة السيبرانية:

لتكملة الجهود التشريعية في مجال مكافحة الجرائم السيبرانية، قام المشرع الجزائري بتعديل الكتاب الأول من الأمر رقم 66-155 الصادر في سنة 1966 بإضافة باب سادس يحمل عنوان "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، ويشمل المواد من 211 مكرر 22 إلى 211 مكرر 29.[3]

المادة 211 مكرر 22: تنص على إنشاء القطب الجزائي الوطني على مستوى محكمة مقر مجلس قضاء الجزائر، وهو هيئة متخصصة في متابعة وتحقيق الجرائم السيبرانية، مع اختصاصه في الحكم عليها إذا كانت تشكل جنحًا.

المادة 211 مكرر 23: تحدد صلاحيات وكيل الجمهورية، وقاضي التحقيق، ورئيس القطب، حيث يمارسون صلاحياتهم على مستوى كامل الإقليم الوطني.

---

[1] وتوغي نبيل، زيوش عبد الرؤوف، مرجع سابق، ص 18.

[2] القانون رقم 09/04 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال، والقانون رقم 20-06 المتعلق بمحاربة الجريمة السيبرانية، الجريدة الرسمية للجمهورية الجزائرية، 2009 للقانون 09/04 و2020 للقانون 20-06

[3] الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021.

المادة 211 مكرر 24: توضح أن القطب يختص حصريًا بالجرائم السيبرانية التي تمس أمن الدولة، والدفاع الوطني، ونشر الأخبار الكاذبة التي تهدد الأمن والاستقرار، وجرائم متعلقة بالإدارات العامة، والأنشطة المنظمة العابرة للحدود، وجرائم التمييز وخطاب الكراهية، وجرائم الاتجار بالأشخاص أو تهريب المهاجرين.

المادة 211 مكرر 25: تشير إلى اختصاص القطب في التعامل مع الجرائم السيبرانية المعقدة، والتي تشمل تعدد الفاعلين، أو الشركاء، أو المتضررين، أو اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة، أو جسامة الأضرار.[1]

المادة 211 مكرر 26: تؤكد على صلاحيات القطب في جميع الجوانب المتعلقة بالجرائم السيبرانية، وتؤكد المادتان 211 مكرر 27 و211 مكرر 28 على اختصاص الهيئات القضائية في تخصصاتهم وإلغاء هذه الاختصاصات بشكل إلزامي إذا كانت متعلقة بالجريمة السيبرانية.

المادة 211 مكرر 29: تدعم هذا الباب بوجوب زوال كل اختصاص مرتبط بالجريمة السيبرانية ليكلف به القطب حتى لو كان الاختصاص متعلقًا بمحكمة مقر مجلس قضاء الجزائر.

بهذا الشكل، يعتبر القطب الجزائي الوطني أداة فعالة في التصدي للجرائم السيبرانية، مع الحفاظ على حرية الرأي والتعبير والنشر ضمن حدود عدم الإضرار. ويعد هذا خطوة هامة في تعزيز قطاع العدالة ومكافحة الجريمة السيبرانية في الجزائر.[2]

الأمر رقم 21-11 الصادر في 25 أغسطس 2021 يعزز جهود الجزائر في مكافحة الجريمة السيبرانية عبر إنشاء "القطب الجزائي الوطني المتخصص". هذا القطب، الذي يتخذ من محكمة مقر مجلس قضاء الجزائر مقرًا له، يُفوض بمسؤوليات واسعة تشمل الجرائم السيبرانية المعقدة والخطيرة التي تمس أمن الدولة، الدفاع الوطني، والإدارات العامة. [3]يضمن القطب توحيد الجهود عبر إلغاء اختصاصات الهيئات القضائية الأخرى في هذا المجال، ويعزز من قدرة النظام القضائي على التعامل مع التهديدات الإلكترونية بفعالية. تعتبر هذه الخطوة مهمة في تعزيز قدرة الجزائر على التصدي للتحديات السيبرانية المتزايدة، مع الحفاظ على التوازن بين حماية الأمن القومي وحرية التعبير.

[1] القسم السابع مكرر: المساس بأنظمة المعالجة الآلية للمعطيات الجريدة الرسمية، 2004، ص 11-12 -14.

[2] القانون رقم 20-06 المعدل والمتمم لقانون العقوبات الجريدة الرسمية، 2020، ص 3.

[3] الأمر رقم 21-11 الصادر في 25 أغسطس 2021.

المطلب الثاني: التشريعات الدولية

الاتفاقيات والمعاهدات الدولية هي واحدة من أهمها أشكال التعاون الدولي بشكل عام وفي مجال المكافحة الجرائم الناتجة عن الجرائم لإلكترونية على وجه الخصوص بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال المكافحة الجرائم السيبرانية، ومعاهدة بودابست لمكافحة جرائم الإنترنت واتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية وتوصيات المجلس الأوروبي بشأن المشاكل الجنائية الإجراءات المتعلقة تكنولوجيا المعلومات التي نوضحها تالياً.

الفرع الأول: توصيات المجلس الأوروبي

أدى التطور السريع في مجال الحاسبات وتقنية الإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية مما عجل إلى إصدار المجلس الأوروبي التوصية رقم: 13/95 بتاريخ:1995/09/11 بخصوص مشاكل الإجراءات الجنائية المتعلقة بالتكنولوجيا وتكنولوجيا المعلومات، وعقوبات وطنية لتتناسب مع التنمية في هذا المجال [1]، ومن بين أهم الأمور المذكورة في التوصية لأوروبية المجلس هم:

- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.
- أن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محلا للتفتيش مع بيان المعلومات التي تم ضبطها.
- أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة اختصاصهم والتي

تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط ان يكون هذا الإجراء ضروريا.

- أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.

---

[1] Al-Khafagy, B. (2020). International Efforts to Combat Cybercrime. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(6), 1-12.

- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية والاحترام للمعلومات التي يفرض القانون لها حماية خاصة.
- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.
- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء أكانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.
- يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحتويه من معلومات باتخاذ اللازم للسماح لرجال التحقيق بالاطلاع عليها[1].
- يجب تطوير وتوحيد أنظمة التعامل مع الأدلة السيبرانية، وحتى يتم الاعتراف بها بين الدول المختلفة ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة السيبرانية.
- يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة التأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.
- قد تتطلب إجراءات التحقيق من الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات.
- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع ادله معينة ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط [2].

الفرع الثاني: اتفاقية بودابست لمكافحة جرائم السيبرانية 2001

شهدت العاصمة المجرية بودابست، في أواخر عام 2001 أولى المعاهدات الدولية التي تكافح جرائم الانترنت. ومواكبة للتطور فقد أبرم المجلس الأوروبي اتفاقية ببودابست في: 8/11/2001 ووضعت للمصادقة في: 23/11/2001، والتي تضمنت التعريف بأهدافها ووضعت قائمة للجرائم التي يجب على الدول المصادقة

1 شيخه حسين الزهراني، "التعاون الدولي في مواجهة الهجوم السيبراني"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 01، 2020، ص 752.

2 شيخه حسين الزهراني، نفس المرجع، ص، 753.

عليها أن تحرمها في قوانينها الداخلية، وتعد الأولى في مجال مكافحة جرائم الانترنت وشملت العديد من جرائم الانترنت منها: الإرهاب، تزوير بطاقات الائتمان، دعارة الأطفال وتعمد الاتفاقية إلى تنسيق القوانين الجديدة في دول عديدة، وجاءت نتيجة مشاورات طويلة بين الحكومات واجهزة الشرطة وقطاع الكمبيوتر وصاغ نصها عدد من الخبراء في مجلس أوروبا بمساعدة عدة دول منها الولايات المتحدة [1].

كما تعد الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر وباستخدام شبكة الانترنت، وهي تمثل ركيزة أساسية منذ دخولها حيز النفاذ، في الأول من جويلية لعام 2004 اعلى مستوى الدول أعضاء مجلس الاتحاد الأوروبي وكما سبق الإشارة، فلقد وقعت عليها العديد من الدول من غير أعضاء مجلس اوروبا مثل كندا واليابان وجنوب إفريقيا، كما صادقت عليها الولايات المتحدة الأمريكية، كما أن هذه الاتفاقية بمثابة دعوة موجهة إلى دول العالم للتفاعل مع الانترنت جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها النهائي في2001/11/23 م في بودابست وقعت عليها ثلاثون دولة أوروبية بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوروبي المشاركة في إعداد هذه الاتفاقية وفي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية، وقد تضمنت هذه الاتفاقية الأقسام التالية[2]:

القسم الأول: تحديد المصطلحات.

القسم الثاني: الخطوات الواجب اتخاذها في إطار التشريع الوطني. **القسم الثالث:**

التعاون الدولي.

القسم الرابع: الشروط النهائية حول الانضمام إلى الاتفاقية.

كما حددت الجرائم التي يجب أن تتضمنها التشريعات الوطنية، للدول الأعضاء وذلك على النحو التالي:

- الجرائم المتعلقة بأمن الشبكات الدخول والمراقبة غير المشروعة والعدوان على الثقة في البيانات أو على النظام والإساءة إليه.
- الجرائم المعلوماتية كما هو الشأن في الاختلاق والانتحال والنصب والاحتيال المعلوماتي... الخ.
- جرائم الأخلاق مثل إنتاج أو بث أو حيازة ما يتعلق بدعارة الأطفال.

---

[1] نسيمة درار الامن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني دراسة مقارنة. أطروحة دكتوراه. جامعة أبي بكر بلقايد تلمسان–الجزائر، كلية الحقوق والعلوم السياسية، 2017، ص 273.

2 نسيمة درار، نفس المرجع، ص 274.

- جرائم العدوان على حقوق الملكية الأدبية والفكرية كاستنساخ المصنفات المشمولة الي بالحماية.
- المسؤولية الجنائية للأشخاص المعنوية، وكذلك الاهتمام بالإجراءات الجنائية لاسيما في مرحلة التحقيق والملاحقة القضائية مثل التحفظ على الأدلة والتفتيش والضبط وما إلى ذلك وقد حملت هذه الاتفاقية الطابع التوجيهي للخطوات، التي يلزم اتخاذها في إطار التشريع الوطني في كل دولة فيما يتعلق بالأحكام الموضوعية والإجرائية كما أشرنا أعلاه. وألزمت الدول الأعضاء بمراعاة حقوق الإنسان وحرياته الأساسية، التي تضمنتها الاتفاقيات الدولية والتشريعات الوطنية على حد سواء والالتزام بعدم انتهاكها، مع إمكانية الدول الأخرى غير الأعضاء في الاتفاقية الاستعانة بهذه الاتفاقية، عند إعداد التشريعات الوطنية باعتبارها مصدر تاريخي في مجال مكافحة الجريمة على الانترنت. [1]

كما تضمنت الاتفاقية جانب آخر من التعاون انصب هذه المرة حول تدريب أعوان الأمن لإكسابهم خبرات عملية كما ورد في التوصية الصادرة عن اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم السيب رانية، وتعد الولايات المتحدة الأمريكية، من الدول المتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية والشبكات، وهي تساعد على تدريب أجهزة الشرطة وقضاة الدول الأخرى، بتمكينها من تعزيز قدراتها على ضبط مشاكل هذه الجرائم، قبل أن تفلت منها زمام الأمور فقد أوجدت وزارة العدل الأمريكية مكتب للمساعدة والتدريب لتطوير أجهزة الادعاء العام في الدول الأخرى، ويعمل إلى جانبه البرنامج الدولي للمساعدة والتدريب (ICITAP) لتوفير المساعدات لأجهزة الشرطة بالدول النامية[2].

الفرع الثالث: اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

صدر عن جامعة الدول العربية قانونا استرشاديا لمكافحة جرائم تقنية الفضاء السيبراني سعت الدول العربية لتقنين وتجريم الأعمال الغير مشروعة المرتكبة من خلال استخدام الفضاء السيبراني بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010/12/21 لتعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على أمنها وسلامة مجتمعاتها[3].

ودعا المجلس، الدول العربية المصدقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى موافاة الأمانة الفنية للمجلس باتخاذه من إجراءات المواءمة تشريعاتها مع أحكام الاتفاقية وتجريم الصور المستحدثة

1 شيخه حسين الزهراني، مرجع سابق، ص، 755

[2] نسيمة درار، مرجع سابق، ص 278.

[3] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية،،2004 ص28

من الجرائم السيبرانية لمنع الإرهابيين من استخدام الإنترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال جرائم الإرهاب السيبرانية.

كما دعا المجلس، الدول العربية إلى التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات والإنترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها، وأكد المجلس على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، ودعم أمن المطارات والموانئ والحدود[1].

بالرغم من كل هذه الجهود الدولية سواء على مستوى الأمم المتحدة والمنظمات الدولية وعلى المستوى الإقليمي وخاصة اتفاقية بودابست التي تعتبر بمثابة دعوة للدول لإعادة النظر في تشريعاتها الداخلية والدعوة إلى التعاون الدولي لأجل مكافحة الجرائم السيبرانية التي لا تعرف الحدود الجغرافية.

المطلب الثالث: انعكاسات السلوكيات الإجرامية السيبرانية

بغض النظر عن نوع الجرائم الإلكترونية (الرقمية) وحجمها، فهي دائمًا تمس النظام المعلوماتي، سواء كانت موجهة إليه مباشرة أو تُنفذ من خلاله. يمكن أن تحدث في مراحل مختلفة، سواء في مرحلة إدخال البيانات، أو إخراجها، أو جمعها. ومع ذلك، فإن تأثير هذه الجرائم يختلف بناءً على نوع الجريمة، وطبيعة الأنظمة المعلوماتية المستهدفة، أو أهمية البيانات المتأثرة. لهذا السبب، تتنوع وتتفاوت الخسائر والأضرار الناجمة عن الجرائم الإلكترونية.

الفرع الأول: تأثير السلوك الإجرامي الرقمي على الاقتصاد

يتغير الأثر الاقتصادي المترتب عن السلوكيات الإجرامية الرقمية باختلاف نوع الجريمة ونوع الأنظمة المعلوماتية أو بحسب أهمية البيانات المستهدفة، ولهذا تتفاوت الخسائر الاقتصادية الناجمة عن الإجرام الرقمي حيث يمكن أن يكون ضررها مرتبط بقيمة التجهيزات والبرمجيات موضوع الجريمة، كما قد ترتبط بالأثر الناجم عن توقف هذه المنظومات عن العمل مثل اختراق منظومات عمل معينة أو شركات أو مؤسسات التي تؤدي

[1] محمد عبد الجواد أميرة عبد العظيم، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، الجزء03، العدد35، 2020، ص 499.

إلى إلحاق خسائر تقدر بآلاف الدولارات، وهذا ما أكدته دراسة عنيت بالجرائم الالكترونية في المملكة البريطانية. والتي أكدت نتائجها أن هذا النوع من الإجرام يستهدف أكثر القطاع المالي[1].

حيث أن أغلبها تمس البنوك وشركات التأمين في قطاعها وبنسب أقل في القطاع العام والتعليمي. كما أن الأثر الاقتصادي للسلوك الإجرامي الرقمي لا يستهدف في حقيقة الأمر التجهيزات والمؤسسات فقط أنما هو يمس بدرجة الأولى الأفراد، فالجريمة الاقتصادية المستحدثة مست كل فئات المجتمع فأثرت بذلك على الأفراد والجماعات كما أثرت على الشركات والمؤسسات وذلك نتاج الاستعمال المفرط للأنترنت التي يسرت ودعمت ونوعت من السلوكيات الإجرامية وأصبحت تمارس بطرق أسرع وأسهل، ومن بين الجرائم التي تؤثر على الجانب المادي والاقتصادي نجد جرائم نقل ملكية الأسهم، نقل أو تحويل الحسابات المصرفية، سرقة بطاقة الائتمان الخاصة، عمليات الاحتيال على الشركات، عمليات الابتزاز والتهديد وسرقة الهوية[2].

كما أن المؤسسات المالية والمؤسسات التجارية الرقمية والمؤسسات الحكومية والاتصالات تأتي في طليعة المؤسسات المستهدفة من قبل القرصنة الرقمية على مستوى العالم، ومن الجرائم التي تتعرض لها المؤسسات ذات الطابع المالي والاقتصادي، الاطلاع على معلومات أو بيانات سرية خاصة بصفقات هامة العبث بمخازن البيانات الخاصة بمؤسسة معينة قصد تخريبها أو التعديل فيها أو حذفها وكل هذه الممارسات من شأنه أن تعود بصرر على أصحاب هذه المؤسسات ومن ثمة على اقتصاد الوطن[3].

الفرع الثاني: تأثير السلوك الإجرامي الرقمي على المجال الثقافي

ساهمت العولمة الثقافية، من خلال تسريباتها عبر الأقمار الصناعية وما تقدمه من منتجات سينمائية، معلوماتية، فنية وفكرية، في انتشار مظاهر سلبية عديدة داخل المجتمعات، منها تعزيز ثقافة الرذيلة، العنف، والإدمان. كما لعبت دوراً في تسريب القيم الإجرامية وتعليم السلوكيات غير القانونية، مما أدى إلى ظهور أشكال جديدة من الجرائم المرتبطة بالبيئة الرقمية. وفي هذا السياق، يشكل تأثير العولمة الثقافية على المجتمع الجزائري خطراً كبيراً، حيث أسهمت في الترويج للأفكار المتطرفة ومحاولة استقطاب الشباب عبر منصات إلكترونية مصممة لنشر ثقافة الغلو والتطرف.

---

[1] حورية قويقح، الابعاد الاقتصادية للجريمة الإلكترونية، مجلة الاصلاحات الاقتصادية والاندماج الاقتصادي العالمي، جامعة الجزائر 1، سنة 2020، ص 245.

[2] رقية محمودي، نور الهدى قدوح، الجرائم الالكترونية في المجتمع الجزائري "تشخيص الواقع وتحديات الأمن السيبراني، جامعة يحي فارس، المدية، الجزائر، سنة 2022، ص 341.

[3] رقية محمودي، نور الهدى قدوح، نفس المرجع، ص342.

إلى جانب ذلك، كان للعولمة دور واضح في تفكيك الروابط الاجتماعية والعائلية داخل المجتمع الجزائري، من خلال نشر قيم الانحلال والتدهور الأخلاقي، والتي تتعارض مع النمط الثقافي السائد. هذه القيم تُروج كبدائل للنظام الأخلاقي والثقافي التقليدي، مما يؤدي إلى تآكل القيم المجتمعية الأصيلة. كما يعزز الاستخدام الفردي للوسائل التكنولوجية العزلة الاجتماعية، حيث يقلل من فرص التفاعل الطبيعي والنمو الاجتماعي والانفعالي السليم، مما ينعكس سلباً على التنشئة الاجتماعية الصحية للأفراد، خاصة في ظل غياب التواصل الأسري والمجتمعي[1].

وفي النهاية، تبرز ضرورة مواجهة هذه التأثيرات السلبية من خلال تعزيز الوعي الثقافي والاجتماعي، وتقوية الروابط الأسرية والتعليمية لمواجهة هذه التيارات الفكرية التي تهدد الاستقرار المجتمعي، كما بينت بعض الدراسات أن الاستخدام الغير مدروس لبعض المواقع بسهم في تنمية بعض الأفكار غير العقلانية خصوصا ما يتصل منها بنمط العلاقات الشخصية وأنماط الحياة والعادات والتقاليد السائدة في المجتمع مما يؤدي إلى تدمير نسيج الموروث الاجتماعي الوطني إضافة إلى تمجيد وتشجيع الثقافات الفرعية المعارضة لثقافة المجتمع الأصلية والتي تسعى لنشر قيمها ومعاييرها الجديد على حساب الثقافة الأصلية، كما كثيرا ما يسهم السلوك الإجرامي في خلق اختلال معياري داخل المجتمع مما يضعف بدوره القيم المجتمعية ويفقد المعايير سلطتها على المجتمع فيحتل ببذلك السير وتنتشر الجريمة.

الفرع الثالث: تأثير السلوك الإجرامي الرقمي على المجال الأمني

من أبرز الجرائم التي تمثل تهديداً خطيراً للأمن الوطني هي ما يُعرف بالإرهاب الإلكتروني، والذي يعتمد على توظيف القدرات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية لإلحاق الضرر بدولة معينة. هذا النوع من الجرائم لا يقل خطورة عن الإرهاب التقليدي، إذ يمتلك آثاراً سلبية سواء على الأفراد أو المجتمع. من خلاله، يتم استقطاب الأفراد والتغرير بهم للعمل ضد أوطانهم، عبر غسل أدمغتهم بأفكار متطرفة تستهدف أساساً أمن الفرد والمجتمع. كذلك، تؤدي الممارسات الإرهابية إلى زعزعة الأمن العام وإثارة الفوضى.

في هذا السياق، ظهرت العديد من المواقع الإلكترونية المشبوهة التي تُستخدم لتعليم صناعة المتفجرات، وطرق اختراق وتدمير المواقع من بين هذه المواقع، تلك التي أنشأتها تنظيمات إرهابية، مثل موقع "النداء"

[1] نورة فتاش، الجريمة المنظمة عبر الوطنية نموذجا، مجلة الدراسات القانونية، جامعة المدية، المجلد 7، العدد 2، جوان 2021، ص 815.

المرتبط بتنظيم القاعدة، والذي يستهدف جذب الأفراد للانضمام إلى صفوفها أو تكوين مجموعات دعم توفر الدعم المالي واللوجستي للجماعات الإجرامية الإرهابية.

هذه الأنشطة الإرهابية الإلكترونية تشكل تهديداً مباشراً لأمن الوطن والأفراد، وتساهم في خلق حالة من الفوضى واللانظام داخل المجتمع بالإضافة إلى الأضرار النفسية والاقتصادية التي قد تترتب على هذه السلوكيات، فإنها تزيد من تفكك النسيج الاجتماعي وتهدد استقراره على المدى الطويل[1].

كما تُعتبر الجوسسة من أخطر الجرائم التي تنتشر في الفضاء الرقمي، ويعني التجسس السيبراني تلك المحاولات المتعمدة لاختراق أجهزة الكمبيوتر والمواقع الإلكترونية التابعة للدولة المناوئة أو الخصم بهدف سرقة معلومات سرية[2]، ويهدف للحصول على بنك معلومات هائلة عن المنظومات والأسرار العسكرية والسياسية والأمنية والاقتصادية والصناعية، والتي تعتمد بشكل كامل في عملها على وسائل ومنظومات التواصل والاتصال التكنولوجي الحديث داخل الدول[3]، حيث أن التجسس المعتمد على المجال السيبراني يؤثر سلبا على المعلومات وأنظمة المعلومات، مما يتيح إمكانية تسريب أسرار ومعلومات حساسة للدول الأخرى، وتجدر الإشارة إلى أن أجهزة الاستخبارات السيبرانية لا يقتصر على وجهة النظر الرسمية للدول والحكومات، بل يتعدى ذلك لدور الأفراد في إنتاج المعلومات وترويجها، وفي توفير كم كبير للملفات السياسية والاقتصادية مع تعدي الحدود الدولية، عكفت أجهزة استخبارات الدول للحصول عليها أولا، والبحث فيها ثانيا، وتوظيف نتائجها ثالثا[4].

في الوقت الحالي، نواجه نوعاً جديداً من الحروب يعتمد على التكنولوجيا والحروب السيبرانية، مع ظهور حروب الجيل الرابع والخامس، التي تستهدف أمن الدول من خلال استغلال الثغرات وإثارة الفوضى. هذه الحروب تعتمد على ضرب استقرار الدولة عبر نشر الشائعات المغرضة، خلق البلبلة، وزعزعة الثقة بمؤسسات الدولة، مما يشكل تهديداً مباشراً لأمن الوطن ومصالحه الحيوية[5].

---

[1] رقية محمودي، نور الهدى قدوح، مرجع سابق، ص342.

[2] شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب "التفجير من الداخل" على الساحة الدولية، العربي للنشر والتوزيع، القاهرة، سنة 2019، ص106.

[3] نضال ناجي بدوي بريوش، الصراع السيبراني مع العدو الصهيوني، دراسة منشورة مقدمة للحصول على دبلوم الدراسات الفلسطينية من أكاديمية دراسات اللاجئين، 2019-2018 ، ص 14.

[4] أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، ج 3، ع 35، سنة 2020، ص415-416.

[5] رقية محمودي، نور الهدى قدوح، مرجع سابق، ص342.

خلاصة الفصل:

قمنا في هذا الفصل بالتركيز على مفهوم الجريمة السيبرانية في إطار التشريعات الجزائرية وكذا في إطار التشريعات الأجنبية والاتفاقيات الدولية، حيث أشرنا إلى أنها تمثل نوعًا جديدًا من الجرائم يتجاوز الحدود التقليدية من حيث الطبيعة والأساليب على عكس الجرائم التقليدية، تعتمد الجرائم السيبرانية بشكل رئيسي على التكنولوجيا الرقمية والإنترنت كوسيلة لارتكاب الجريمة، هذا التطور التكنولوجي السريع أدى إلى ظهور تحديات قانونية جديدة تتطلب استحداث تشريعات متخصصة.

في الجزائر، اتخذ المشرع خطوات مهمة لتحديث المنظومة القانونية لمواكبة هذه التطورات، من خلال إصدار قوانين جديدة تهدف إلى التصدي للجرائم السيبرانية، ورغم هذه الجهود إلا أن هناك نقصًا في بعض النصوص القانونية التي تغطي الجوانب المتنوعة لهذه الجرائم. على سبيل المثال، يفتقر القانون إلى تعريف دقيق للمجرم الإلكتروني وسماته الخاصة، وهو ما يفتح الباب أمام ثغرات يمكن استغلالها.

علاوة على ذلك، تطور طبيعة الجرائم السيبرانية يجعل من الصعب تكييف القوانين التقليدية معها، مما يستدعي ضرورة مراجعة مستمرة وتحديث متواصل للإطار القانوني. المشرع الجزائري مطالب اليوم بتعزيز القوانين الحالية وتوسيع نطاقها لتشمل جميع الأبعاد المرتبطة بالجريمة السيبرانية، بما في ذلك تعزيز الحماية القانونية للضحايا وتحديد مسؤوليات الجهات الفاعلة في الفضاء الرقمي.

الفصل الثاني:

الجهود الدولية والوطنية لمكافحة الجرائم السيبرانية

تمهيد:

يتسم الإجرام السيبراني بطبيعته الدولية، مما يتطلب جهودًا وطنية ودولية متكاملة للتصدي له. تقوم الدول بالتعاون عبر اتفاقيات ومعاهدات دولية لمكافحة الجرائم السيبرانية وتبادل المعلومات والخبرات، وتعمل على إنشاء وحدات شرطة متخصصة وتدريب كوادر قادرة على التعامل مع هذه الجرائم.

على المستوى الدولي، تشمل المبادرات معاهدات مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية، التي تهدف إلى توحيد التشريعات والإجراءات القضائية لتسهيل ملاحقة المجرمين عبر الحدود.

محليًا، تقوم الدول بتحديث تشريعاتها لتغطية جرائم الفضاء السيبراني، وتأسيس وحدات متخصصة في التحقيق وملاحقة الجرائم السيبرانية، وتعزيز التعاون بين السلطات الوطنية والدولية لضمان تنفيذ العدالة ومنع استغلال الفجوات القانونية بين الدول.

وللتعرف أكثر على الآليات والإجراءات على المحققين الكشف عن هاته الجرائم التي تتخذ للكشف عن هذه الجريمة، سنتطرق إلى مبحثين، المبحث الأول الآليات الدولية لمكافحة الجرائم السيبرانية، والمبحث الثاني الآليات الوطنية لمكافحة الجرائم السيبرانية.

المبحث الأول: الآليات الدولية لمكافحة الجرائم

هناك العديد من الهيئات والآليات الدولية التي تلعب دوراً ملحوظاً في إطار الاتفاقيات المختلفة التي تسعى لترسيخ وجوب التعاون الدولي لمواجهة الجرائم السيبرانية، وعلى رأس هذه الآليات هيئة الأمم المتحدة، والمجلس الأوروبي وبعض الهيئات الأخرى. وعليه، سيتم معالجة هذا الموضوع عبر مطلبين، يُخصص الأول منها على المستوى الدولي، ويُخصص الثاني على المستوى الإقليمي، مثل اتفاقية بودابست.

المطلب الأول: على المستوى الدولي

إذا كان التعاون الدولي هو الآلية الفعال لمكافحة الإجرام السيبراني، فإن هذا التعاون يقتضي التخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية لأن التباعد بين هذه الأنظمة يجعل المجرم المعلوماتي يبحث عن الأنظمة الأكثر تسامحاً (قضية دو غوزمان التي أشرنا إليها)، ولذلك أبرمت العديد من الاتفاقيات الدولية في مجال التعاون الدولي من أجل مكافحة الإجرام السيبراني وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ اجراءات التحقيق وجمع الأدلة وتسليم والاعتراف بالأحكام الجنائية، بحيث أن هذا القانون الدولي لا ينال من سيادة الدولة، بل بالعكس عدم التعاون يزيد من التباعد بين الأنظمة العقابية مما يساعد على تزايد هذه النوعية من الجرائم[1].

الفرع الأول: جهود الأمم المتحدة في مجال مكافحة الإجرام السيبراني

بذلت الأمم المتحدة جهوداً كبيرة في سبيل العمل على مكافحة الإجرام السيبراني، وذلك لما تسببه هذه الجرائم من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء، وإيماناً منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به.[2]

توصلت منظمة الأمم المتحدة في مؤتمرها الثامن المنعقد بهافانا 1990 حول منع الجريمة ومعاملة المجرمين United Nations Congress on the Revention of Crime and the Treatement of the Offenderإلى اصدار قانون خاص بالجرائم المتعلقة بالحاسوب، وأشار القرار إلى أن الأجرام الدولي لمواجهة الجرائم المستحدثة يتطلب من الدول الأعضاء اتخاذ عدة إجراءات تتلخص فيما يلي:

---

[1] حسين سعيداني، آليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص 181.

[2] عواطف محمد عثمان عبد الحليم،جرائم المعلوماتية، مجلة العدل، العدد الرابع والعشرون، ص 69

- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة من تحقيق وقبول الأدلة على نحو ملائم وإدخال التعديلات إذا دعت الضرورة لذلك.
- اتخاذ تدابير أمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان
- رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة على مكافحة هذا النوع من الجرائم.
- التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتخذة في استخدام الحاسوب في المناهج التعليمية.
- حماية مصالح الدولة وحقوق ضحايا جرائم الحاسوب.

لكن تزايد الجريمة السيبرانية وما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية ديسمبر سنة 2000، رقم 55/63 الجلسة العامة، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بالإضافة الذي يمكن أن تقوم به المنظمة والمنظمات الإقليمي الأخرى.

عقدت كذلك الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية بالبرازيل أيام 12 إلى 19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخير في استخدام التكنولوجيا من طرف المجرمين والسلطات المختصة في مكافحة الجريمة.

تبقى منظمة الأمم المتحدة الإطار الأمثل لمكافحة الإجرام السيبراني حيث وضعت مجموعة من القواعد الموضوعية وإجرائية[1] لمواجهة هذه النوعية من الجرائم.

أولاً: القواعد الموضوعيـة

تتضمن هذه القواعد النص على قائمة الحد الادنى للأفعال المتعين تجريمها واعتبارها من قبيل الإجرام السيبراني وتحديثها دورياً والمتضمنة:

[1] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، 2007، ص111.

- **جريمة الاحتيال أو الغش المرتبط بالكمبيوتر:** ويشمل ذلك الادخال والاتلاف والمحو لمعطيات الكمبيوتر أو برامجه أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى الحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.

- **جريمة التزوير التي تطال برامج الكمبيوتر أو التزوير المعلوماتي:** ويشمل ذلك ادخال أو الاتلاف أو المحو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى العادي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد فيما لو ارتكبت بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.

- **جريمة تخريب واتلاف الكمبيوتر:** ويشمل ذلك ادخال أو الاتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات والشبكات.

- **جريمة الدخول غير المصرح به:** وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن.

- **جريمة الاعتراض غير المصرح به:** وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات.

ثانيًا: القواعد الإجرائية

تتضمن بعض الأسس الواجب مراعاتها:[1]

- وجوب تحديد السلطات التي تقوم بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، وخاصة ضبط الأشياء المتعلقة بها وتفتيش الحاسب.

- وجوب أن يكون هناك قدر كبير من التعاون الفعال بين الأطراف لكي تكون المعلومات متاحة في صورة يمكن استخدامها للأغراض القضائية في حل هذه الجرائم

- السماح للسلطات العامة باعتراض الاتصالات داخل البيئة المعلوماتية مه استخدام الأدلة التي يمكن ان يتحصل عليها.

[1] عبد الله عبد الكريم عبد الله، المرجع السابق، ص 114

- ادخال بعض التعديلات التشريعية في حالة الضرورة ما يتماشى مع طبيعة الإجرام السيبراني داخل القانون الوطني وكذلك القواعد القائمة في مجال الإثبات الالكتروني من حيث مصداقية الأدلة وما يمكن أن تثيره من مشاكل عند تطبيقها.

- يجب أن يوضع في الاعتبار كل المسائل المرتبطة ببيئة تكنولوجيا المعلومات، مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسارة الاقتصادية، كلفة إعادة بناء قواعد البيانات كما كانت وإعادتها إلى الواضع السابق قبل اجراء أي تفتيش أو تحقيق.

الفرع الثاني: جهود المنظمات الدولية في مجال مكافحة الإجرام السيبراني

تم اتخاذ مبادرات من قبل العديد من المنظمات كالاتحاد الدولي للاتصالات(ITU) ، الإنتربول/يوروبول، منظمة التعاون الاقتصادي والتنمية (OECD)، مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) والمنظمة الدولية لتوحيد المقاييس(ISO) ، واللجنة الكهروتقنية الدولية (IEC) وفرق عمل هندسة الإنترنت وFIRST منتدى الاستجابة للأحداث ومجموعات الأمن لآسيا والمحيط الهادئ، ومنظمة التعاون الاقتصادي للمحيط الهادئ وآسيا (APEC) ومنظمة الدول الأميركية (OAS) ورابطة دول جنوب شرق آسيا (ASEAN) وجامعة الدول العربية، والاتحاد الأفريقي[1].

أولاً: منظمة التعاون الاقتصادي والتنمية (OECD)

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية، بدأت هذه المنظمة الاهتمام بالجريمة السيبرانية منذ عام 1978، حيث وضعت مجموعة من الأدلة وقواعد إرشادية تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها.[2]

---

[1] – Malcom Anderson : " Policing the world : Interpol the Politics of International Police Co-Operation " , Clarendon press.Oxford,1989,p 168

[2] يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير حقوق، جامعة مولود معمري تيزي وزو، الجزائر، 2013، ص 96

فأصدرت سنة 1983 تقريراً بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى من لأفعال سوء استخدام الحاسوب والتي على الدول تجريمها وتشمل هذه الأفعال[1]:

- الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به
- الإفشاء غير مصرح به للمعلومات المعالجة آلياً والنسخ والإتلاف أو التخريب ما يحتويه من بيانات وبرامج والإعاقة غير المشروعة للوصول لمصادر الحاسب من منع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة داخله.

وفي عام 1992 وضعت المنظمة توصيات وإرشادات خاصة بأنظمة المعلومات وأوصت بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء مبادئ عامة [2]تتمثل في:

- **حدود التجميع:** يتعين فرض قيود على تجميع البيانات.
- **نوعية البيانات:** حيث تنص على أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله.
- **تعيين الغرض:** بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورة ومحددة سلفا.
- **حدود الاستخدام:** يقتضي الالتزام بعدم إفشاء البيانات الشخصية ونشرها لغير المصرح لهم بذلك.
- **الوقاية الأمنية:** ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة وحازمة في إحاطة البيانات.
- **الانفتاح:** أن تكون السياسة العامة للتطوير والخطط والتطبيقات معلنة فيما يتعلق بالبيانات ذات الطبيعة الشخصية.
- **المشاركة الفردية:** حق الأشخاص المعنية في الوصول والتعرف على البيانات التي تخصهم فضلاً عن رقابة مدى صحتها.

[1] غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الانترنت)،مذكرة دكتوراه، الجامعة الإسلامية، لبنان،2004، ص92.

[2] د علي جبار الحسناوي، جرائم الحاسوب والأنترنت، دار اليازوي العلمية للنشر والتوزيع، عمان، 2009، ص 154.

- **المسائلة والمحاسبة:** التي تقتضي محاسبة الأشخاص والجهات المرخص لهم الوصول والاطلاع على البيانات والتعامل معها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة.

ثانياً: الإنتربول

وضعت منظمة الإنتربول نظاما خاصا للتعاون، وهو النظام الوطني الخاص بالنقطة المرجعية المركزية NCRP[1] ويوجد في كل دولة من الدول الأعضاء في الإنتربول مكتب مركزي وطني يُعد نقطة الاتصال مع الإدارات الأجنبية التي تجري تحقيقات خارج حدودها وتضم شبكة من المحققين العاملين في الوحدات الوطنية المعنية بجرائم لتيسير الاتصالات الميدانية بين البلدان الأعضاء وتسريعها قدر الإمكان ومن مهامها هذا النظام إنماء الاستراتيجيات والتقنيات والمعلومات بشأن أحدث الأساليب الجرمية في مجال جرائم تكنولوجيا المعلومات وهناك فرق عاملة إقليمية لإفريقيا والأمريكيتين وآسيا وجنوب المحيط الهادئ وأوروبا والشرق الأوسط وشمال إفريقيا[2].

كما قامت منظمة الإنتربول بوضع برنامجاً خاصاً لمكافحة الإجرام المعلوماتي يرتكز على التدريب والعمليات ويعمل على مواكبة التهديدات الناشئة مبادرات ويهدف هذا البرنامج:[3]

- توفير دورات تدريبية لوضع معايير مهنية والتقيد بها.
- تعزيز تبادل المعلومات بين البلدان الأعضاء عن طريق الأفرقة العاملة والمؤتمرات الإقليمية.
- تنسيق العمليات الدولية ودعمها
- إعداد قائمة عالمية بأسماء ضباط الاتصال ووضعها بتصرف المحققين في مجال الإجرام السيبيري على مدار الساعة

[1] جان فرنسوا هنروت، أهمية التعاون الدولي بين عناصر الشرطة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 جوان 2007، المملكة المغربية، ص 100

[2] الأنتربول، الإجرام السبراني، 2024/05/14، مجالات-الإجرام/الإجرام-السيبيري/الإجرام-السيبيري http://www.interpol.int/ar

[3] الإنتربول، المرجع نفسه، ص1.

- مساعدة البلدان الأعضاء على التحقيق في الهجمات أو الجرائم السيبرانية عن طريق توفير خدمات في مجال التحقيق وقواعد البيانات
- إقامة شراكات استراتيجية مع المنظمات الدولية الأخرى وهيئات القطاع الخاص.
- تحديد التهديدات الناشئة وتبادل معلومات الاستخبار في هذا المجال مع البلدان الأعضاء.
- توفير بوابة آمنة على الويب لنشر معلومات ووثائق عملياتية.

المطلب الثاني: على المستوى الإقليمي (اتفاقية بودابست)

تعد الاتفاقية الأوربية بمثابة دعوة موجهه إلى دول العالم للتفاعل مع الجرائم المستحدثة والتي جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها، فبتاريخ 20 أفريل 2000 تقدمت اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية، بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من اصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001 (اتفاقية الجرائم السيبرانية – سايبر كرايم) وكان قد طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات وأطلق ضمن مواقع عديدة أوروبية وأمريكية على شبكة الأنترنت لجهة التباحث وإبداء الرأي. وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ اكثر من عشرة أعوام[1].

الفرع الأول: القانون الجنائي الموضوعي

يعد موضوع القسم الأول من هذه الاتفاقية (المواد من 2 إلى 13) دليلاً ارشادياً لتحسن أو اصلاح وسائل منع وقمع الإجرام المعلوماتي Améliorer les moyens de prévenir et de réprimer la criminalité informatique، بتحديد أدنى القواعد العامة التي تسمح باتخاذ بعض التصرفات القانونية اتجاه هذه الجرائم ويسهل مكافحتها على المستوى الوطني والدولي، ويحدد قائمة تسمح بتجريم بعض الأفعال

[1] د. يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، 2-4 ابريل 2006، مسقط، ص15.

والتصرفات غير المشروعة التي ترتكب على بيئة معلوماتية، بعبارة أخرى حصر الإجرام السيبراني بتحديد الحد الأدنى في بعض الأفعال غير المشروعة التي تعد من قبيل الجريمة السيبرانية[1].

فإذا كانت هذه الاتفاقية تنطبق على التصرفات التي توصف على أنها جرائم مرتكبة عن طريق تكنولوجيا المعلومات، فإن المذكرة التفسيرية حرصت على ايضاح أن الاتفاقية تستخدم تكنولوجيا محايدة Neutreأي التكنولوجيا الآنية والمستقبلية، كما ركزت المذكرة التفسيرية على ضرورة ارتكاب الجرائم المحصاة دون حق وذلك عندما نصت (يشترط في تجريم الأفعال في هذه الاتفاقية أن يكون القيام بالفعل دون حق(Sans droit) ، كما أن كل الجرائم المدرجة يجب ان تكون مرتكبة بطريقة عمدية Facon Intentionnelle[2]

أولاً: الأفعال غير المشروعة

تناولت المواد من 2 إلى 10 الجرائم الواردة في هذه الاتفاقية

- **جرائم ضد سرية وسلامة وتوافر البيانات والنظم المعلوماتي** Infraction contre la : L'intégrité et la disponibilité des données et systèmes ،confidentialité informatique، إن الغرض من الجرائم التي تناولها هذا العنوان هو حماية سرية وسلامة واتاحة أو تهيئة البيانات ونظم الحاسب للعمل أو التشغيل، وبالتالي يخرج من نطاق التجريم الأنشطة المشروعة والعادية والمرتبطة بتصميم الشبكات وكذلك الممارسات الاستثمارية أو التجارية المشروعة والعادية، وقد تناولتها[3] المواد من 2 إلى 6.

- **الولوج غير القانوني (المادة2)**Accès Illégal : والذي يعد الجريمة الرئيسية التي تهدد سرية وأمن وسلامة المعلومات وتوفرها وعلى ذلك فإن مجرد التدخل غير المصرح به بمعنى القرصنة Le * piratage، أو الدخول غير المشروع في النظام يعتبر تصرفاً غير مشروع

[1]" مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، المنعقد في بانكوك في الفترة من 18 إلى 25 أبريل 2005، وثيقة رقم 14/203"./A.CONF.

[2] د طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، ص302.

[3] د هلالي عبد اللاه أحمد، جرائم المعلوماتية وأساليب المواجهة وفقاً لاتفاقية بودابست،ط1، دار النهضة، القاهرة، 2007، ص68.

- **الاعتراض غير القانوني (المادة3)** :تهدف هذه المادة لحماية الحق في احترام نقل البيانات وأن هذه الجريمة تمثل انتهاكاً للحق في احترام الاتصالات مثل التصنت والتسجيل التقليدي للمحادثات والمراسلات بين بين الأشخاص.

- **الاعتراض على سلامة البيانات (المادة4)** :الغرض من هذه المادة هو أن تكون بيانات وبرامج الحاسب مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمداً من اتلاف الأجهزة المادية والمنطقية المكونة للحاسب ومحو البيانات والبرامج.

- **الاعتداء على سلامة النظام (المادة5)** :تهدف هذه المادة إلى تجريم عرقلة الاستخدام الشرعي لنظام المعلومات، أو التأثير على سيرها العادي والتي تمنع أو تبطئ بشكل ملموس سير عمل النظام.

- **إساءة استخدام أجهزة الحاسب (المادة6)** :تشير هذه المادة أن الأعمال غير المشروعة التي تندرج تحت النوع أ من الجرائم المذكورة أعلاه تكون في الغالب عند حيازة وسائل الدخول كحصول المجرم على معدات التشويش أو أجهزة تحاليل الشبكات التي هي في الأصل تستعمل للتحقيق من إمكانية عمل الشبكات أو أجهزة مراقبة أمن الشبكات كما قد يكون جهاز الكمبيوتر نفسه أداة المزود بالأنترنت أداة لاختراق بعض المواقع أو الحسابات السيبرانية [1] كما تشمل الإنتاج المتعمد أو بيع أو شراء أو استيراد أو توزيع الأجهزة والأدوات بهدف ارتكاب أي فعل المنصوص عليه في المواد 2 إلى 5 من هذه الأتفاقية.[2]

- **الجرائم المتصلة بالحاسب**Infractions Informatiques : وهي المادتين 7و8 والتي تتعلق بجرائم عادية يمكن في الغالب ان ترتكب عن طريق الحاسب الآلي:

- **التزوير المعلوماتي (المادة7)** :الغرض من هذه المادة في إنشاء جريمة موازية لجريمة تزوير المستندات الورقية كما تهدف إلى استكمال أوجه النقص [3]التي تعتري قانون العقوبات بالنسبة للتزوير التقليدي، والتزوير المعلوماتي يتكون من خلق Créer أو تعديلModifier .

[1] د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 319

[2] عبد الله عبد الكريم عبد الله، المرجع السابق، ص 133.

[3] د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 323.

- **الغش المعلوماتي (المادة8)** :مع حدوث ثورة تكنولوجية تضاعفت إمكانية ارتكاب جرائم اقتصادية كالغش وبالأخص النصب ببطاقات الائتمان والمعاملات البنكية أو الودائع التي أصبحت هدفاً للنصب من خلال التلاعبات بمدخلات النظام بمعنى ادخال على النظام ببيانات غير صحيحة.

- **الجرائم المتصلة بالمضمون** Infraction se rapportant au contenu :هذه الجرائم المرتبطة بالمحتوى والتي تربط بإنتاج أو نشر غير المشروع للمواد الإباحية الطفولية عير النظم المعلوماتية.

- **الجرائم المتصلة بالمواد الاباحية (المادة9)** :تسعى هذه المادة إلى تدعيم الإجراءات التي تحمي الأطفال خاصة من الاستغلال الجنسي من خلال تحديث قانون العقوبات تشمل على استخدام الحاسب الآلي في اطار ارتكاب الجرائم الجنسية ضد الأطفال كما تجرم مختلف جوانب الإنتاج والحيازة والنشر للمواد الإباحية الطفولية.

- **الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة** Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : وهي الأفعال التي تعتبر عن انتهاكات واقعة على الملكية الفكرية وخاصة المؤلف من خلال المادة 10 من متخصصي النظام المعلوماتي وخصوصاً شبكة الانترنت والأفعال[1] هي: إن إعادة إنتاج وبث الأعمال المحمية عبر الأنترنت دون موافقة حائز الحق هو أمر غير شرعي وهذه الأعمال المحمية تشمل الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية.

تتناول المواد المذكورة من هذه الاتفاقية جوانب مختلفة من الجريمة السيبرانية، حيث تهدف إلى توسيع نطاق القوانين لمواكبة التحديات الرقمية. المادة 7 تتناول التزوير المعلوماتي، مُعالجة التزوير الرقمي الذي يعادل التزوير التقليدي، من خلال خلق أو تعديل المعلومات بطرق غير قانونية. المادة 8 تتعامل مع الغش المعلوماتي، حيث تسعى لمكافحة التلاعب بالبيانات في المعاملات المالية والنصب باستخدام بطاقات الائتمان. الجرائم المتصلة بالمضمون تركز على الجرائم المرتبطة بنشر المواد الإباحية الطفولية عبر الأنظمة الرقمية، في حين تعزز المادة 9 حماية الأطفال من الاستغلال الجنسي عبر تحديث القوانين لتشمل جميع جوانب المواد الإباحية الطفولية. أخيرًا، المادة 10 تتناول انتهاكات الملكية الفكرية عبر الإنترنت، مُعاقبة إعادة إنتاج وتوزيع الأعمال المحمية دون إذن، مثل الأعمال الأدبية والموسيقية.

ثانياً: تقرير العقوبات

أشارت المادة 13 من هذه الاتفاقية على ضرورة خضوع المنصوص عليها في المواد من 2 إلى 10 لعقوبات جزائية وبالنظر للالتزامات التي تفرضها هذه المواد فإنه يجب على الاطراف المتعاقدة استخلاص النتائج الخطيرة المترتبة على ارتكاب تلك الجرائم وإقرار عقوبات جزائية فعالة، مناسبة ورادعة تتضمن عقوبات سالبة للحرية.

وفي حالة الاشخاص الاعتباريين أن يخضعوا أيضاً لعقوبات فعالة ومناسبة ورادعة والتي يمكن أن تكون جزائية، مدنية أو ادارية، كما تركت نفس المادة المجال مفتوحاً لإمكانية فرض عقوبات أخرى أو إجراءات تتناسب مع خطورة الجرائم المرتكبة مثل قرار الحظر أو المصادرة.

الفرع الثاني: قانون الإجراءات

إن المواد في القسم الراهن نصت بعض الإجراءات التي يجب اتخاذها على الصعيد الوطني، والتي تخدم التحريات الجنائية التي ترتكب عن طريق المنظومة المعلوماتية، وجمع الادلة ذات الطابع الالكتروني.

فتكمن أحد أصحاب المشاكل في مجال مكافحة الإجرام السيبراني في صعوبة تحديد هوية مرتكب الجريمة ومداها وتأثيرها والمشكلة الأخرى تكمن في ضياع البيانات السيبرانية التي يمكن نقلها أو تعديلها أو محوها في ثواني معدودة[1]، فمثلاً يستطيع الشخص الذي يتحكم في البيانات أن يستخدم المنظومة المعلوماتية بمحوها مدمراً بذلك جميع الأدلة التي يقوم عليها التحقيق الجنائي، لذا تعتبر في أغلب الأحيان السرعة والسرية من المكونات الأساسية لنجاح التحريات.

تُقر الاتفاقية إجراءات تقليدية مع المناخ التكنولوجي الحديث مثل التفتيش والمصادرة وبالتوازي وضعت إجراءات جديدة[2]، كالحفظ السريع للبيانات خلال مدة زمنية محدودة وذلك بهدف إتاحة الفرصة للحصول أو جمع البيانات التي تخدم التحريات أو الإجراءات الجنائية التي يجب القيام بها، والتي بموجبها يجري الإعداد والاتفاق على نظم حماية تسمح بالسيطرة على هذا المناخ التكنولوجي الجديد وتطوير سلطات إجرائية جديدة.

---

[1] د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص496

[2] دليل "Guide to Cybercrime Legislation" الصادر عن الاتحاد الدولي للاتصالات (ITU) في عام 2009، الطبعة الأولى، ص 94.

كما تشير هذا القسم إلى مجال تطبيق بنود هذه الاتفاقية من خلال المادة 14، حيث تلزم كل دولة طرف في الاتفاقية بإقرار الإجراءات التشريعية بما يسمح القانون الداخلي بها لخدمة التحريات والإجراءات الجنائية الخاصة على:

- الجرائم الجنائية المنصوص عليها في القسم الأول من الاتفاقية.
- جميع الجرائم الجنائية الأخرى التي ترتكب عن طريق المنظومة المعلوماتية.
- جمع الأدلة السيبرانية[1] لكل جريمة من أجل التحريات أو إجراءات جنائية معينة.

وتشير الاتفاقية بوضوح إلى أنه يجب ان تقر الأطراف بان القانون الداخلي يتضمن معلومات رقمية أو الكترونية قد تستخدم كأدلة[2] أما القضاء وذلك في إطار الجنائي أياً كان طبيعة الجريمة المطلوب متابعتها.

[1] الدليل الالكتروني هو كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسب من إنجاز مهمة ما، عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات، دار الجامعة الجديدة، الاسكندرية، 2010، ص53

[2] علماً أن القانون المدني الجزائري قد انتبه إلى مسألة حجية الدليل الرقمي والتوقيعات الالكترونية وقبولها من طرف القاضي في مادتيه 1/223 و327 من قانون 10/05 المتعلق بالمنافسة، محمد فولان، الحماية القانونية لتكنولوجيات الإعلام، مجلة المحكمة العليا، الجزائر، العدد01، 2010، ص 41.

المبحث الثاني: الآليات الوطنية لمكافحة الجرائم السيبرانية

في إطار إصلاح المنظومة التشريعية والقضائية وضماناً لفعالية وسرعة التحقيق في القضايا المتعلقة بالجرائم المستحدثة، سارع المشرع الجزائري إلى تعديل قانون الإجراءات الجزائية تماشياً مع التطور المعلوماتي. وقد شمل هذا الإصلاح وضع قواعد خاصة لسلطة التحري والمتابعة، بالإضافة إلى إنشاء هياكل خاصة لمكافحة الجرائم، بهدف التصدي لهذه الجرائم ومواجهتها بفعالية[1]، ومنه سنطرق إلى مطلبين، حيث سنتناول في المطلب الأول الآليات القانونية الإجرائية، أما المطلب الثاني فسنتحدث فيه عن الهياكل الخاصة لمكافحة الجرائم.

المطلب الأول: الآليات القانونية الإجرائية

أدرك المشرع الجزائري جيدا بان المواجهة الفعالة للإجرام السيبراني لا تكون بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية فقط، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى اجرائية وقائية وتحفظية.

الفرع الأول: في قانون الإجراءات الجزائية

أولا: الاختصاص:

تمديد الاختصاص المحلي:

حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الاخيرة "على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجريمة الماسة بأنظمة المعالجة الآلية للمعطيات ولعل اعتماد الاختصاص الاقليمي الموسع هو للمواجهة الفعالة لطائفة من الجرائم المنظمة الخطيرة ومنها الجرائم السيبرانية الماسة بأنظمة المعالجة الآلية للمعطيات.[2]

كما انشئت الاقطاب القضائية الجزائية المتخصصة بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية[3] من بين الجرائم التي تختص بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المواد 37 و40 و329 من قانون الإجراءات الجزائية).

---

[1] الملتقي الوطني، اليات مكافحة الجريمة الإلكترونية في التشريع الجزائري. الجزائر العاصمة 29 مارس 2017 ص 67

[2] قانون 06-22، مؤرخ في 20 ديسمبر 2006، يتم الأمر 66 156 المتضمن قانون الاجراءات الجزائية.

[3] القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الاجراءات الجزائية

كذلك نظم المشرع الجزائري في القانون رقم 04-09 المؤرخ في 05 اوت 2009 احكاما جديدة خاصة بالاختصاص في مجال الجريمة المعلوماتية تتماشى والتطور الذي لحق الجريمة، ومن هذه القواعد ما نصت عليه المادة 03 التي تضمنت اجراءات جديدة التي تتطلبها التحريات والتحقيقات من ترتيبات تقنية بالإضافة الى ذلك قررت المادة 05 من ق 09-04 " انه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبيها اجنبيا ويستهدف مؤسسات الدولة الجزائرية والدفاع الوطني، أو المصالح الاستراتيجية للاقتصاد الوطني.[1]

توسيع مجال اختصاص النيابة العامة:

بموجب المادة 37 من قانون الإجراءات الجزائية تم توسيع اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها بها من قبل، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية الى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات، والجريمة المنظمة، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبيض الأموال، والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

ثانيا: التسرب

عرف المشرع الجزائري التسرب بموجب المادة 65 مكرر 12 من قانون العقوبات على انه " قيام ضباط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الاشخاص المشتبه في ارتكابهم جناية، أو وجنحة بإيهامهم انه فاعل معهم أو شريك"[2].

ويمكن تصور عملية التسرب في نطاق جرائم الاعتداء على نظم المعالجة الآلية في دخول ضابط أو عون الشرطة القضائية الى العالم الافتراضي واشراكه مثلا في محادثات غرفة الدردشة أو حلقات النقاش

[1] القانون رقم 09-04 مؤرخ في 05 اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها الجريدة الرسمية 47 الصادرة بتاريخ 16 اوت 2009.

[2] قانون 06-22 مؤرخ في 20 ديسمبر 2006 يتم الأمر 66 156 المؤرخ في 08 يونيو 1966 المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية العدد 84 الصادر بتاريخ 24 ديسمبر 2006.

والاتصال المباشر في كيفية قيام أحدهم باختراق شبكات أو بث فيروسات مستخدما في ذلك اسماء وصفات هيئات مستعارة ووهمية ظاهرا فيها بمظهر طبيعي.

شروط صحة عملية التسرب لما كان التسرب ممارسة غير مألوفة للضابط أو عون الشرطة القضائية، بل أخطر الإجراءات انتهاكا لحرمة الحياة الخاصة للمتهم، احاطه المشرع بشروط يمكن ايجازها في نوعين وهي كما يلي:

الشروط الشكلية:

أ. صدور بإذن قضائي وهذا ما نصت عليه المادة 56 مكرر من قانون الإجراءات الجزائية. يجوز لوكيل الجمهورية أو قاضي التحقيق بعد اخطار وكيل الجمهورية أن يأذن تحت [1]..... والجهة المختصة لإصداره كما هو مبين من نص المادة اما وكيل الجمهورية أو قاضي التحقيق، وذلك حماية للحقوق الاساسية المكرسة دستوريا.

ب. ان يكون مكتوبا وهذا ما نصت عليه المادة 65 مكرر 15 من قانون الإجراءات الجزائية بقولها " يجب ان يكون الاذن مسلما طبقا للمادة 65 مكرر 11 اعلاه مكتوبا تحت طائلة البطلان".

ج. ذكر اسم الضابط المشرف على العملية وهويته الكاملة.

د. المدة المطلوبة لعملية التسرب وقد جاءت حسب نص المادة 65 مكرر 15 الفقرة الثالثة من قانون الإجراءات الجزائية على ان لا تتجاوز اربعة اشهر، ويمكن ان تجدد حسب مقتضيات التحري أو التحقيق، وفي نفس الوقت اجاز القانون للقاضي الذي رخص بإجرائها ان يأمر في اي وقت بوقفها قبل انقضاء المدة المحددة.

هـ. ابقاء الاذن بالتسرب خارج ملف الإجراءات الى غاية الانتهاء من العملية حفاظ على السرية المطلوبة التي حصرها المشرع بين القاضي الأمر بها وكيل الجمهورية أو قاضي التحقيق وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب

و. وجود تقرير مسبق محرر من طرف الضابط عن الجريمة بشكل مفصل للاطلاع القاضي بشكل تام عن ظروف القضية ومتطلباتها.

[1] قانون رقم 05-22 مؤرخ في 20 ديسمبر 2006، يتم الأمر 66 -156 المؤرخ في 08 يونيو 1966، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية، العدد 84، الصادر بتاريخ: 24 ديسمبر 2006

ز. الصفة: يستشف من نص المادة 65 مكرر 12 المادة 65 مكرر 14 من قانون الإجراءات الجزائية ان المخولين قانون للعمل بنظام التسرب هم ضباط وكذا أعوان الشرطة القضائية وكذا الاشخاص المسخرين لذلك.[1]

الشروط الموضوعية:

أ. تسبيب عملية التسرب يعتبر التسبيب شرط جوهري لمشروعية عملية التسرب لذلك اشترط القانون عند اصدار الاذن بالتسرب من السلطات المختصة ذكر السبب أو الدافع الحقيقي الجاد الذي يبرر اللجوء الى هذا الإجراء تحت طائلة البطلان المادة 65 مكرر 15 من قانون الإجراءات الجزائية

ب. محل التسرب بمعني أن عملية التسرب يجب ان تنصب على إحدى الجرائم السبعة المنصوص عليها في المادة 65 مكرر 5 وهي جرائم المخدرات، الجريمة المنظمة، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبيض الأموال، وجرائم المتعلقة بالتشريع الخاص بالصرف وفيما عدى ذلك يعتبر التسرب إجراء باطلا.[2]

يشترط القانون أن يكون لتسبيب عملية التسرب سببًا حقيقيًا وجادًا، حيث يتعين على السلطات المختصة توضيح الدافع وراء اللجوء لهذا الإجراء، وإلا سيكون التسرب باطلاً وفقًا للمادة 65 مكرر 15 من قانون الإجراءات الجزائية. بالإضافة إلى ذلك، يجب أن يركز التسرب على الجرائم المحددة في المادة 65 مكرر 5، مثل جرائم المخدرات والجريمة المنظمة وجرائم الكمبيوتر وتبيض الأموال، وإلا يعتبر التسرب إجراءً باطلاً.

الفرع الثاني: في قانون الإجراءات المدنية

حيث تنص المادة 32 من قانون الإجراءات المدنية والإدارية الاختصاص النوعي والإقليمي للمحكمة حيث ان المشرع الجزائري نص على جريمة المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات

[1] بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن طبعة 2012 منشورات الحلبي الحقوقية، مستغانم الجزائر، ص436.

[2] بوكر رشيدة، مرجع سابق، 437,

من خلال المواد 394 مكرر 7 واعتبرها جنحا في جميع الأحوال ولم يقم المشرع الجزائري بتعريفها كما وضحنا سابقا واكتفى فقط بالإشارة الى بعض الأفعال التي تبلور الركن المادي للجريمة.[1]

الاختصاص الإقليمي للمحكمة: وعليه وتطبيقا لنص المادة 328 من قانون الإجراءات الإدارية تختص المحكمة بالنظر في الجنح والمخالفات وتنص المادة 329 منه على انه تطبق نفس قواعد الاختصاص المحلي في الحالات العادية وهي: مكان وقوع الجريمة محل إقامة احد المتهمين أو شركائهم، محل القبض عليهم ولو كان هذا القبض قد وقع لسبب اخر ويجوز تمديد الاختصاص المحلي للمحكمة الى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم منصوص عليها على سبيل الحصر بما فيها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ما وضحناه سابقا اذا طلبه النائب العام المحاكم المتخصصة (كما ان هناك اختصاصا حصريا للقطب الجزائي الوطني لمكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال.

تختص الأقطاب المتخصصة المنعقدة في بعض المحاكم بالنظر دون سواها في المنازعات المتعلقة بالتجارة الدولية، والإفلاس والتسوية القضائية والمنازعات المتعلقة بالبنوك ومنازعات الملكية الفكرية والمنازعات البحرية والنقل الجوي ومنازعات التأمينات تحدد مقرات الأقطاب المتخصصة والجهات القضائية التابعة لها، عن طريق التنظيم تفصل الأقطاب المتخصصة بتشكيلة جماعية من ثلاث قضاة تحدد كيفيات تطبيق هذه المادة عند الاقتضاء عن طريق التنظيم.

تنص المادة 32 من قانون الإجراءات المدنية والإدارية على تنظيم الاختصاص النوعي والإقليمي للمحاكم في الجزائر فيما يخص جريمة المساس بأنظمة المعالجة الآلية للمعطيات، التي تعتبر جنحًا بموجب المواد 394 مكرر 7 من قانون العقوبات، لا يوجد تعريف محدد لها بل يقتصر النص على توضيح بعض الأفعال التي تشكل الركن المادي للجريمة. وفقًا للمادة 328 من قانون الإجراءات الإدارية، تختص المحاكم بالنظر في الجنح والمخالفات، ويحدد الاختصاص المحلي بناءً على مكان وقوع الجريمة أو محل إقامة المتهمين. يمكن أيضًا توسيع الاختصاص إلى محاكم أخرى حسب التنظيم. علاوة على ذلك، يوجد اختصاص حصري للقطب الجزائي الوطني لمكافحة الجريمة المرتبطة بتكنولوجيات الإعلام والاتصال،

[1] قرية سيد علي، عصماني سعيد، الطبيعة القانونية للأقطاب الجزائية المتخصصة واجراءات سير الدعوى أمامها مذكرة لنيل شهادة الماستر في القانون تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية قسم القانون العام، جامعة العقيد اكلي محمد اولحاج البويرة، 2019، ص 47.

بينما تفصل الأقطاب المتخصصة في قضايا معينة مثل التجارة الدولية والإفلاس والمنازعات المتعلقة بالبنوك والتأمينات، بتشكيلة جماعية من ثلاث قضاة.[1]

المطلب الثاني: الهياكل الخاصة لمكافحة الجرائم

الفرع الأول: الوحدات التابعة لسلك الأمن الوطني

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها ألجل التصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجرائم المعلوماتية، والتي تعتبر نتاج التطور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات.[2]

أولا: على مستوى المركزي

بادرت المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية بغية خلق وحدات متخصصة تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها، ولذلك قامت المديرية العامة للشرطة القضائية باستحداث مصلحة مختصة في المكافحة الجريمة المعلوماتية سميت بنيابة مديرية مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالإضافة الى نيابة مديرية الشرطة العلمية والتقنية، هذه الأخيرة التي تضع لخدمة هذا الهدف مصالح عملية مختصة بذلك، تتولى أعمال البحث والتحري والتحقيق بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذه الوحدة هي المخبر المركزي للشرطة العلمية والكائن مقره بالجزائر العاصمة.

يتولى كل المخبر المركزي، مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها، ولأجل ذلك يضم المخبر دائرة تقنية وتتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي

[1] عادل عبد العال إبراهيم خراشي، "إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها"، دار الجامعة الجديدة، جامعة الأزهر، مصر، ص. 42.

[2] عادل عبد العال إبراهيم خراشي، نفس المرجع، ص 63.

تستعمل فيها الأسلحة والقذائف بمختلف أنواعها، وكذلك جرائم التزوير، إضافة إلى الجرائم المعلوماتية وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى.[1]

ثانيا: على المستوى الجهوي

قامت بإنشاء مخابر جهوية للشرطة العلمية في كل من ولايتي قسنطينة ووهران، بالإضافة إلى ثلاث مخابر أخرى قيد الإنجاز على مستوى – ورقلة – بشار – تمنراست ينتظر تسليمها قريبا لأجل تعميم هذا النوع من النشاط على كافة ربوع الوطن.

على مستوى كل مخبر مصلحة تسمى دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية، تتولي هذه المصلحة أعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية، وذلك تحت تسمية دائرة الأدلة الرقمية والآثار التكنولوجية والتي لم تكن عند استحداثها سنة 2004 سوى قسم، غير أن الارتفاع الملحوظ لعدد القضايا الناتجة عن الجرائم المعلوماتية، بسبب الانتشار المتزايد لتقنية المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية[2] هي:

1. قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.
2. قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
3. قسم تحليل الأصوات.

تضم الدائرة في صفوفها ثمانية 08 أعضاء محققين أربع 04 منهم عناصر شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية، والبقية هم أعوان شبيهون يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي، إضافة إلى إلمامهم بالجانب القانوني، ومما يزيد من فعاليتهم في مجال مباشرتهم المختلف

[1] مساهمة المخبر الجهوي للشرطة العلمية في كل من قسنطينة ووهران في إدارة الدليل ضمن التقنيات الخاصة للتحقيق – وثيقة خاصة صادرة عن نيابة مديرية الشرطة العلمية والتقنية – مديرية الشرطة القضائية – المديرية العامة للأمن الوطني – ص 02-03.

[2] مساهمة الشرطة العلمية والتقنية في مجال التحقيقات الجنائية– وثيقة خاصة صادرة عن مديرية الشرطة القضائية– المديرية العامة لألمن الوطني ص 46.

إجراءات البحث والتحقيق في الجرائم المعلوماتية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الاطلاع على كل المستجدات القانونية منها والتقنية في مجال الإجرام المعلومات.[1]

ثالثا: على المستوى المحلي

في سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية، خلقت المديرية العامة لألمن الوطني سنة 2016 ما يقارب 48 فرقة لمكافحة الجرائم المعلوماتية على مستوى مصالحها بأمن والواليات، يتمثل دورها في تلقي الشكوى والبحث والحقيق في الجرائم المعلوماتية وتقريب الإدارة من المواطن.

الفرع الثاني: الوحدات التابعة للدرك الوطني

تضع قيادة الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية وهي تباعا:

- قيادة الدرك الوطنية.
- الوحدات الإقليمية.
- الوحدات المشكلة.
- الوحدات المتخصصة وحدات الإسناد.
- هياكل التكوين.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام.
- المصالح والمراكز العلمية والتقنية.
- المصلحة المركزية للتحريات الجنائية.

[1] حسين ربيعي آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدّمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص – قانون العقوبات العلوم الجنائية، جامعة باتنة 1، السنة الجامعية 2015/2016،ص 180.

– المفرزة الخاصة للتدخل.[1]

تعمل مؤسسة الدرك الوطني جادة إلى التطلع بمختلف الجرائم المرتكبة على شبكة الإنترنت وهذا لتسهيل مهمة البحث والمعاينة والتفتيش في أنظمة الحواسيب والعمل على مراقبة مختلف الشبكات وبالتالي:

فقد تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، وذلك حسب الاختصاص والصالحيات وطبيعة الجريمة إلى ثالث 03 مستويات مركزية، جهوية، محلية.

1. المستوى المركزي:

– **مديرية الأمن العمومي والاستغلال:** تنسق بين الوحدات الإقليمية والمركز التقني العلمي في مجالات البحث والتحري.

– **المصلحة المركزية للتحريات الجنائية:** تتولى مكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال على مستوى وطني.

– **المعهد الوطني للأدلة الجنائية وعلم الإجرام:** يقدم خبرات وتحليلات في الجرائم المعلوماتية، ويساعد في توجيه التحقيقات وتوفير الدعم العلمي.

– **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية:** يقدم المساعدة التقنية ويوجه التحقيقات المتعلقة بتكنولوجيا المعلومات، ويشارك في مراقبة الإنترنت والاتصالات السيبرانية.[2]

2. المستوى الجهوي:

– المصالح الجهوية للشرطة القضائية تنسق بين الوحدات وتدعمها في التحريات المعقدة، مثل الجرائم المعلوماتية.

3. المستوى المحلي:

[1] الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 جويلية 2024 – الرابط الإلكتروني : http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

[2] بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة 16 و17 نوفمبر،2015 كلية الحقوق جامعة بسكرة، ص2.

– يتوفر للدرك الوطني فصائل متخصصة في مكافحة الجرائم المنظمة، بما في ذلك الجرائم المعلوماتية، وتساهم في دعم الأبحاث والتحقيقات على المستوى الإقليمي.[1]

[1] معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني – البيض – الجزائر، معلومات مهمة حول قضايا وجوانب مختلفة تتعلق بالأمن والنظام العام، بما في ذلك مكافحة الجريمة الإلكترونية.

خلاصة الفصل:

في هذا الفصل، تم تناول الجهود الدولية والوطنية المبذولة لمكافحة الجريمة السيبرانية، حيث تم استعراض الاستراتيجيات والآليات المتبعة على مختلف المستويات. شمل ذلك التحليل العميق للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التي تلعب دورًا حيويًا في التنسيق بين الجهات المختلفة لمكافحة الجرائم الرقمية. كما تم تناول دور الأجهزة الأمنية على المستويات الوطنية، الجهوية، والمحلية في تطبيق الإجراءات الأمنية والتقنية اللازمة لمكافحة هذه الجرائم.

تم التركيز أيضًا على الإجراءات القانونية المتبعة في التحقيقات الجنائية المتعلقة بالجرائم السيبرانية، بما في ذلك الأساليب والتقنيات المستخدمة للتحري والكشف عن الجناة. تم توضيح كيف تساعد هذه الإجراءات المحققين في جمع الأدلة وتحديد هويات المشتبه بهم، وتقديمهم إلى العدالة لمحاسبتهم وفقًا للقوانين المعمول بها .

بالإضافة إلى ذلك، تم استعراض التحديات التي تواجهها السلطات في هذا المجال، مثل تطور أساليب الجريمة السيبرانية وتعدد الجهات المتورطة، وطرق تعزيز التعاون الدولي والمحلي لمواجهة هذه التحديات بفعالية .

كما تم تناول أهمية تطوير الإطار القانوني والتشريعي لضمان توافقه مع التطورات التكنولوجية، وتحسين الإجراءات والآليات لمواكبة الابتكارات في عالم الجريمة السيبرانية.

الخاتمة

خاتمة:

نستخلص من خلال ما قد سبق دراسته نجد أن موضوع الجريمة السيبرانية يعد من المواضيع البالغة في الأهمية نظرا لخطورتها، مما يتطلب دراسة دقيقة وعميقة حولها، الأمر الذي جعلنا نلاحظ وجود آليات معتمدة لمكافحة هذه الجريمة في التشريع الجزائري وفقا لمجهودات قد قامت بها أجهزة الدولة من جهة. فنرى أن المشرع سعيا منه لتدارك الفراغ التشريعي الذي وقع فيه بخصوص مجال مكافحة الجرائم السيبرانية، وقد اتضح لنا أن الجرائم السيبرانية ظاهرة اجرامية مستجدة تستهدف الاعتداء على المعلومات المخزنة أو المعالجة في نظام الحاسب الآلي او المتبادلة عبر الشبكات، فان طبيعتها المنفردة ادت الى صعوبة ادراجها ضمن الاوصاف التقليدية في القوانين الجنائية الوطنية نظرا للتطور السريع للجريمة السيبرانية من جهة، وللطابع العالمي والعابر للحدود من جهة اخرى، يتعين معه مواجهة هذه الجريمة بنصوص تجريمية جديدة.

ومن خلال من تم دراسته لقد توجت هذه الدراسة بمجموعة من النتائج يمكن أن تستخلصها فيما يلي:

– تعتبر الجريمة السيبرانية من الآثار السلبية التي خلفتها الثورة التكنولوجية الهائلة التي يشهدها العالم.

– يلاحظ عدم الاستقرار سواء على مستوى الفقه القانوني أو على المستوى مختلف التشريعات حول تسمية موحدة للجريمة السيبرانية، فهناك من أطلق عليها تسمية " الجريمة السيبرانية " وجانب آخر أطلق عليها " بالجريمة التي تتم عبر الأنترنت "، ويعود سبب ذلك في إمكانية ظهور جرائم جديدة متصلة بالتكنولوجيات الحديثة.

– تتميز الجريمة السيبرانية في أنها من جرائم التي يصعب اكتشافها وإثباتها أمام القضاء، كما تعد من الجرائم عابرة للحدود لا تعترف بالحدود الزمانية والمكانية.

لقد عمل المشرع الجزائري على مكافحة الجريمة السيبرانية، من خلال استحداثه قسم خاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

توصيات:

لقد منح المشرع الجزائري لسلطات المختصة في إطار مكافحة الجريمة السيبرانية مجموعة من صلاحيات الواسعة كالمراقبة السيبرانية والتفتيش الأنظمة السيبرانية وحجزها، ومع ذلك يمكن القول إنها غير

كافية في ظل ظهور جرائم جديدة تتماشى والتطورات التكنولوجية الحديثة، ومن خلال مشروع مذكرتنا هذا توصلنا إلى جملة من التوصيات:

- تكوين كوادر من الفنيين والتقنيين يمتلكون الخبرة والمهارة العالية في المجال السيبراني .
- الاستعانة أكثر بخبراء معنيين في مجال الاستدلال والتحقيق السيبراني .
- اعتماد المحاضر والضبوط والموثقة من الهيئة الناتجة من التحقيق كأوراق رسمية تقدم لدى المحكمة المختصة.
- الاهتمام أكثر بالكفاءات الجزائرية وعدم الاعتماد على المصادر الأجنبية في التشريع حيث أن هناك العديد من الخبرات الجزائرية التي يجب الاستفادة منها في وضع التشريعات الوطنية.
- الاستفادة من التجارب الدولية الرائدة في هذا المجال لكسب المهارات اللازمة لمكافحة الجريمة السيبرانية.
- التأكيد على مسايرة التحديثات عن طريق الانضمام إلى الاتفاقيات الدولية والعربية للتعاون في مكافحة الجريمة الإلكترونية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

1.القرآن الكريم

2.النصوص القانونية

1. القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الاجراءات الجزائية.
2. القانون رقم 04-15 الصادر في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم،66/156 الصادر في 08 جوان 1966 المتضمن قانون العقوبات.
3. قانون 06-22، مؤرخ في 20 ديسمبر 2006، يتم الأمر 66 156 المتضمن قانون الاجراءات الجزائية.
4. القانون رقم 20-06 المعدل والمتمم لقانون العقوبات.
5. قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

3. الكتب

1. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، ط 1، س 2002.
2. آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر،2007.
3. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، س 2004.
4. بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، مستغانم الجزائر، سنة 2012.
5. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010.
6. رامي متول القاضي، مكافحة الجرائم المعلوماتية، دون طبعة، دار النهضة العربية، مصر، س 2011.
7. شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب "التفجير من الداخل" على الساحة الدولية، العربي للنشر والتوزيع، القاهرة، سنة 2019.

8. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، س 2015.
9. عادل عبد العال إبراهيم خراشي، "إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها"، دار الجامعة الجديدة، جامعة الأزهر، مصر، 2008.
10. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، 2007.
11. علي جبار الحسناوي، جرائم الحاسوب والأنترنت، دار اليازوي العلمية للنشر والتوزيع، عمان، 2009.
12. هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.
13. هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة، 2000.
14. هلالي عبد اللاه أحمد، جرائم المعلوماتية وأساليب المواجهة وفقاً لاتفاقية بودابست، ط1، دار النهضة، القاهرة، 2007.

4. المراجع الأجنبية:

1. Al-Khafagy, B. (2020). International Efforts to Combat Cybercrime. PalArch's Journal of Archaeology of Egypt/Egyptology.
2. Malcom Anderson : " Policing the world : Interpol the Politics of International Police Co- Operation " , Clarendon press.Oxford,1989.
3. Maras, M.-H. Cybercriminology. Oxford University Press. 2016.

5. الرسائل الجامعية:

1. حسين ربيعي آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدّمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص -قانون العقوبات العلوم الجنائية، جامعة باتنة 1، السنة الجامعية 2015/2016.
2. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة، 2011/2012.

3. دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منثوري، قسنطينة، 2012-2013.
4. رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2011.
5. سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية – تخصص علوم جنائية، جامعة الحاج لخضر باتنة، سنة 2012.
6. سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبوبكر بلقايد، تلمسان، 2010.
7. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لاستكمال شهادة الماستر المهني الطور الثاني، جامعة قاصي مرباح، الجزائر 2018-2019.
8. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الانترنت)، مذكرة دكتوراه، الجامعة الإسلامية، لبنان، 2004.
9. قرية سيد علي. عصماني سعيد، الطبيعة القانونية للأقطاب الجزائية المتخصصة واجراءات سير الدعوى أمامها مذكرة لنيل شهادة الماستر في القانون تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية قسم القانون العام، جامعة العقيد اكلي محمد اولحاج البويرة، 2019.
10. نسيمة درار الامن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني دراسة مقارنة. أطروحة دكتوراه. جامعة أبي بكر بلقايد تلمسان-الجزائر، كلية الحقوق والعلوم السياسية، 2017.
11. يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير حقوق، جامعة مولود معمري تيزي وزو، الجزائر، 2013.

6. الملتقيات:

1. جان فرنسوا هنروت، أهمية التعاون الدولي بين عناصر الشرطة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 جوان 2007، المملكة المغربية.

2. جدو بن علية، تحديات الأمن السيبراني في مواجهة الجريمة السيبرانية، المجلة الجزائرية للأمن الإنساني، جامعة الحاج الخضر، باتنة، المجلد 07، العدد 02، جويلية 2022.
3. قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، 2-4 ابريل 2006، مسقط.
4. الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة 16 و17 نوفمبر 2015 بكلية الحقوق جامعة بسكرة.
5. الملتقي الوطني اليات مكافحة الجريمة الإلكترونية في التشريع الجزائري. الجزائر العاصمة 29 مارس 2017.
6. مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، المنعقد في بانكوك في الفترة من 18 إلى 25 أبريل 2005.

7.المجلات والمقالات القانونية:

1. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، ج 3، ع 35، سنة 2020.
2. اهمية الشرطة العلمية والتقنية في مجال التحقيقات الجنائية –وثيقة خاصة صادرة عن مديرية الشرطة القضائية– المديرية العامة للأمن الوطني.
3. حورية قويقح، الابعاد الاقتصادية للجريمة الإلكترونية، مجلة الاصلاحات الاقتصادية والاندماج الاقتصادي العالمي، جامعة الجزائر 1، سنة 2020.
4. دليل "Guide to Cybercrime Legislation" الصادر عن الاتحاد الدولي للاتصالات (ITU) في عام 2009، الطبعة الأولى.
5. رقية محمودي، نور الهدى قدوح، الجرائم الالكترونية في المجتمع الجزائري "تشخيص الواقع وتحديات الأمن السيبراني، جامعة يحي فارس، المدية، الجزائر، سنة 2022.
6. روان بنت عطية الله الصحفي الجرائم السيبرانية، المجلة السيبرانية الشاملة متعددة التخصصات، العدد 24 ماي 2020.
7. سعيدة بوزنون مكافحة الجريمة السيبرانية في التشريع الجزائري مجلة العلوم الانسانية، 2019.

8. شيخه حسين الزهراني، "التعاون الدولي في مواجهة الهجوم السيبراني"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 01، 2020.
9. علي قويدري، أمال العيش، الجريمة السيبرانية مفهومها وسبل الوقاية منها، مجلة نوميرس الاقتصادية، المجلد الثالث، العدد01، 2022.
10. عواطف محمد عثمان عبد الحليم، جرائم المعلوماتية، مجلة العدل، العدد الرابع والعشرون.
11. فريد روابح، محاضرات في القانون الجنائي العام، مطبوعة الدروس السنة الثانية ليسانس، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، 2018/2019.
12. محمد عبد الجواد أميرة عبد العظيم، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، الجزء03، العدد35، 2020.
13. نضال ناجي بدوي بريوش، الصراع السيبراني مع العدو الصهيوني، دراسة منشورة مقدمة للحصول على دبلوم الدراسات الفلسطينية من أكاديمية دراسات اللاجئين، 2019-2018.
14. نورة فتاش، الجريمة المنظمة عبر الوطنية نموذجا، مجلة الدراسات القانونية، جامعة المدية، المجلد 7، العدد 2، جوان 2021.
15. وتوغي نبيل، زيوش عبد الرؤوف الجريمة المعلوماتية في التشريع الجزائري. مجلة العلوم القانونية 139-127 والاجتماعية، 2019.
16. ياسمينة بونعارة، "الجريمة الإلكترونية"، جامعة: الأمير عبد القادر للعلوم الإسلامية، د س ن.

8.موقع إلكتروني:

1. الأنتربول، الإجرام السبراني، 2024/05/14، مجالات-الإجرام/الإجرام-السيبيري/الإجرام-السيبيري http://www.interpol.int/ar
2. موقع الشرطة الجزائرية تاريخ المعاينة 07 جويلية 2024، https://www.algeriepolice.dz.
3. الموقع الرسمي لقيادة الدرك الوطني - تاريخ التصفح 31 جويلية- 2024 http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

الفهرس

الفهرس