Ministry of Higher Education and Scientific Research

University of Echahid Cheikh Larbi Tebessi

Faculty of Law and Political Science

وزارة التعـــليم العـــالي والبحـــث العلمي

جـــامعة الشهـــيد الشيخ العربي التبسي

كلية الحقـــوق والعلـــوم السيـــاسية

إذن بالإيداع

السنة الجامعية : 2024 / 2025

الكليـــة: كلية الحقوق والعلوم السياسية القسم: الحقوق

1/بيانات التعريف بالمشرف:

الاسم: عبير اللقب: بعشيش الرتبة العلمية: أستاذة محاضرة ب

العنوان الإلكتروني المهني:

2/معلومات خاصة بطالب / الطالبين

الاسم: أميمة اللقب: مباركية تاريخ ومكان الازدياد: 2000/01/19 - تبسة -

البريد الالكتروني : mebouamima7@gmail.com

الاسم: اللقب: تاريخ ومكان الازدياد:

البريد الالكتروني :

3/معلومات حول مذكرة الماستر

عنوان المذكرة: التعاون الدولي لمواجهة الجرائم السيبرانية

القسم: القانون الخاص التخصص: قانون جنائي وعلوم جنائية

بعد الاطلاع على المذكرة والتأكد من استيفائها لكل الشروط الشكلية والموضوعية أرخص للطالب/ الطلبة، المذكور/ المذكورون أعلاه استكمال إجراءات الإدارية لإيداع المذكرة.

التاريخ:

توقيع المشرف

Ministry of Higher Education and Scientific Research

University of Echahid Cheikh Larbi Tebessi

Faculty of Law and Political Science

وزارة التعـــليم العـــالي والبحـــث العلمي

جـــامعـة الشهـــيد الشيخ العربي التبسي

كليـة الحقـــوق والعلـــوم السيـــاسية

التزام بقواعد النزاهة والأمانة العلمية

(ملحق القرار الوزاري رقم 933 المؤرخ في 2016/07/28 المتعلق بالوقاية ومحاربة السرقة العلمية)

أنا الموقع أدناه / نحن الموقعين أدناه

الطالب ..مباركية أميمة.....

الحامل لبطاقة التعريف الوطنية رقم :..199247005.. والصادرة بتاريخ :..2020-12-30..

المسجّل(ة) بكلية :..الحقوق والعلوم السياسية.. قسم :..القانون الخاص..

الطالب .....

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

المسجّل(ة) بكلية :..... قسم :.....

و المكلف بإنجاز أعمال مشروع مذكرة الماستر

عنوانها :..التعاون الدولي لمواجهة الجرائم السيبرانية.....

.....

أصرح / نصرح بشرفي/ بشرفنا الالتزام بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية النزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

حرر بتبسة التاريخ .....

إمضاء الطالب

إمضاء الطالب

جامعة الشيخ العربي التبسي - تبسة -

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تخصص: قانون جنائي وعلوم جنائية

بعنوان

التعاون الدولي لمواجهة الجرائم السيبرانية

إعداد الطالب(ة)

مباركية أميمة

إشراف الأستاذ(ة)

الدكتور(ة) بعقيقي عبير

أعضاء لجنة المناقشة

الأستاذ	الرتبة العلمية	الصفة
د. دلول الطاهر	أستاذ	رئيسا
د. بعقيقي عبير	أستاذة محاضرة - ب -	مشرفا
د. عثماني عز الدين	أستاذ	مناقشا

السنة الجامعية: 2024 - 2025.

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

بسم الله الرحمان الرحيم ﴿ يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ ۚ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ﴾.

رب اشرح لي صدري ويسر لي أمري و احلل عقدة من لساني يفقهوا قولي.

رب أدخلني مدخل صدق و أخرجني مخرج صدق و اجعل لي من لدنك سلطانا نصيرا.

رب أوزعني أن أشكر نعمتك التي أنعمت علي وعلى والدي وأن أعمل صالحا ترضاه وأدخلني برحمتك في عبادك الصالحين.

أن تكون معلما فقد اخترت أن تحترق ولو كنت تضيء اخترت أن توزع قلبك في كل شتات الأرض.

شكر وعرفان

نؤمن بمقولة لكل بداية نهاية وها نحن نرى رحلتنا الجامعية قد شارفت على الإنتهاء من بعد تعب ومشقة لوقت طويل وها نحن نختم مشروع تخرجنا بكل ما لدينا من همة ونشاط.

فالحمد لله الذي علم بالقلم وأمرنا بالعلم فعلم الإنسان ما لم يعلم والصلاة والسلام على من أوتي جوامع الكلم وأفهم العرب والعجم فلكل نعمة من نعم الدنيا حد تنتهي إليه ومدى يوقف عنده وغاية من الشكر يسمو إليها الطرف عدا نعمت العلم التي فاقت الوصف وطالت الشكر وتجاوزت كل قدر وأتت من وراء كل غاية فكيف يشكر الشاكر؟ وأين يبلغ جهد المجتهد؟

نتقدم بالشكر للأساتذة الكرام إلى من علمنا الحرف، فالكلمة، فالجملة، فالدرس، فالمحاضرة إلى كل هؤلاء معلمين وأساتذة.

نتقدم بالشكر والعرفان إلى الأستاذة المشرفة بعقيقي عبير التي ساعدتني كثيراً وهيأت لي الجو النفسي قبل العلمي فكانت نعمة الأستاذة الكريمة حفظها الله وجزاها كل خير وأدام عليها الصحة والعافية وإرتقى بها إلى درجات أعلى وأسمى.

كما نشكر كل عمال المكتبة الجامعية وخاصة عمال جامعة الشيخ العربي التبسي الذين كانوا نعم الناس ونستطيع الإعتماد عليهم.

الإهداء

من قال أنا لها نالها لم يكن الحلم قريباً ولا الطريق كان محفوفاً بالتسهيلات .. لكني فعلتها أهدي بكل حب ثمرة تخرجي:

ـ إلى من كلله الله بالهيبة والوقار إلى من أحمل إسمه بكل فخر والذي بذل جهد السنين من أجل أن أعتلي سلالم النجاح من دعمني بلا حدود وأعطاني بلا مقابل داعمي الأول في مسيرتي وسندي لقد فعلتها يا أبي الغالي لتنم قرير العين فابنتك قد تخرجت وحققك حلمك: سعيد.

ـ إلى من جعل الله الجنة تحت أقدامها ومن قال فيها الرسول ﷺ أمك ثم أمك ثم أمك وإحتضنني قلبها قبل يداها وسهلت لي الشدائد بدعائها إلى القلب الحنون والشمعة التي كانت لي في الليالي المظلمات سر قوتي ونجاحي جنتي أمي: سعاد.

ـ إلى من وهبني الله نعمة وجودهم في حياتي إلى العقد المتين إلى من ساندوني بكل حب عند ضعفي وأزاحوا عن طريقي المتاعب ممهدين لي الطريق زارعين الثقة والإصرار بداخلي متابعين نجاحي خطوة خطوة إليكما قرة عيني أخواتي: زينب، تقوى.

ـ إلى من شدّ الله بهم عضدي إلى تلك النجوم التي تنير طريقي دوماً إلى ملهمي نجاحي وصناع قوتي إلى من إنتظروا قطاف ثمرة جهدي طويلاً وكانوا شركاء كل بسمة ودمعة وحسرة إلى أحباب قلبي إخوتي: محمد علي، أيوب.

ـ إلى ملائكة رزقني الله بهم لأعرف من خلالهم طعم الحياة الجميلة تلك الملائكة التي غيّرن مفاهيم الحب والصداقة والسند في حياتي أبناء أختي: بيان، ليان، محمد جود.

ـ إلى بركة العائلة وفرحتها وقوتها وجذعها الثابت الذل لا يميل إلى جدتاي الغاليتين: معيوفة، جمعة.

ـ إلى الغوالي العزيزات رمز الطيبة والحنان إلى من أكن لهن أوصال المحبة والأخوة: هيبة الرحمان، آية.

ـ إلى كل حوتهم ذاتي وتجاوزهم حبر كتاباتي.

ـ إلى كل دفعة 2025.

ـ ما كنت لأفعلها لولا توفيق من الله هاهو اليوم العظيم هنا الذي أجريت سنوات دراستي الشاقة حالمة به حتى توالت بمنه وكرمه لفرحة التمام فالحمد لله الذي ما تيقنت به خيراً وأملاً إلاّ وأغرقني سروراً وفرحاً.

قائمة المختصرات:

- ج ر ج ج: الجريدة الرسمية للجمهورية الجزائرية.
- د، ب: دون بلد.
- د، س: دون سنة.
- د، ط: دون طبعة.

مقدّمة

مقدمة:

إنّ مصطلح الجريمة مصطلح قديم إقترن بالإنسان منذ نشأته، فمع تطورها وإنتشارها عبر الأزمنة ظهرت لنا أنواع جديدة من الجرائم خاصة مع التطور التكنولوجي الذي وصلنا له اليوم، بفضل جهاز الحاسوب وشبكة الأنترنت التي سهلت التعاملات بين الأفراد وجعلت من العالم قرية صغيرة، فبالرغم من كل هذه التسهيلات والإيجابيات التي جاءت بها شبكة الأنترنت إلاّ أنّ بعض الأشخاص إستغلوها وأساءوا إستخدامها.

وهنا ظهر لنا نوع جديد من الجرائم يختلف تماماً عن الجرائم التقليدية يسمى الجرائم السيبرانية حيث أنّ هذه الجرائم جرائم ناعمة لا تحتاج إلى العنف أو لجهد عضلي بل تحتاج إلى جهد فكري، إتسمت هذه الجرائم أنها جرائم عابرة للحدود حيث يمتد الإجرام فيها إلى أكثر من دولة لذلك يصعب إكتشاف زمن وقوعها أو الشخص الذي قام بها.

فعادة ما يقوم بهذه الجرائم أشخاص مختصين في تقنيات نظام الحاسوب ولهم خبرة في إختراق الأنظمة المعلوماتية وهم من أطلق عليهم تسمية الهاكرز، حيث يتمتع هؤلاء بالمهارة والذكاء الذي يجعل منهم يحترفون في جرائمهم لذلك تنوعت الجرائم السيبرانية وإزدادت، ومن بينها جرائم السرقة الإلكترونية، النصب والإحتيال، الإتلاف المعلوماتي.... وغيرها.

ونظراً لخطورة هذه الجرائم وقيامها في أكثر من دولة وجب على هذه الدول التعاون فيما بينهم من خلال وضع إتفاقيات ومعاهدات إضافة إلى المساعدات القضائية المتمثلة في: تبادل المعلومات، وتسليم المجرمين... كل هذا لتعزيز التعاون الدولي من أجل التصدي لهذه الظاهرة التي أصبحت هاجس العصر.

حاولت الدول العربية والأجنبية جاهدة إستحداث قوانين ونصوص جديدة مواكبة لهذه الجرائم والتطور الحالي ومن بينهم المشرع الجزائري من خلال القوانين 15/04 و 04/09 والأمر 11/21 حيث سعى المشرع الجزائري للتصدي لهذه الجرائم من خلال فرض عقوبات صارمة لكل شخص يتعدى على الأنظمة الآلية للمعطيات.

ويكتسي هذا الموضوع أهمية بالغة علمية وعملية فتظهر الأهمية العلمية في أنّ الجرائم السيبرانية جرائم مستحدثة تتساير والتقدم التكنولوجي الذي وصلنا له اليوم، إضافة إلى طبيعة هذه الجرائم مقارنة

بالجرائم التقليدية من حيث مرتكب الجريمة ومكان وقوعها فهذه الجرائم عابرة للحدود أي أنّها تقع في أكثر من دولة حيث أضحت هذه الجرائم من مشكلات العصر التي وجب على الدول التعاون فيما بينهم للتصدي لها، ونظراً لكثرة هذه الجريمة حاولنا أن نقوم بدراسة شاملة حول أنواع هذه الجريمة وصولاً إلى المجرم المعلوماتي ودوافع إجرامه والأهمية العملية تتمثل في أنّ هذه الجرائم تشكل خطراً على المجتمع لذلك يجب القيام بتوعية الأفراد من مخاطر الجريمة السيبرانية.

ودافعنا لإختيار هذا الموضوع الذي يتمثل في جانبين هما الجانب الأوّل لأسباب ذاتية: والمتمثلة في حب التطلع والإكتشاف وزيادة الرصيد المعرفي في هذا الموضوع الذي يواجهنا في حياتنا نظراً لإرتباطه بشبكة الأنترنت والحاسوب اللذان أصبحا من الركائز الأساسية في حياة الفرد والمجتمع. والجانب الثاني لأسباب موضوعية لكون هذه الجرائم انتشرت بكثرة لأنّها جرائم مستحدثة ودائمة التطور وهذا ما يستدعي البحث فيها إضافة إلى معرفة الجهود الدولية التي قامت بها الدول بالتعاون فيما بينها للتصدي لهذا الخطر الذي نعيشه اليوم.

إنّ الجرائم السيبرانية جرائم سريعة الإنتشار والتطور نظراً لإرتباطها بشبكة الأنترنت المتطورة يوماً بعد يوم وهذا ما أدّى إلى تزايد الخطر على الأفراد والمؤسسات لذلك وجب على الدول التعاون فيما بينها من أجل الحد من هذه الظاهرة، **ومن هنا نطرح إشكالية بحثنا الرئيسية وهي:**

فيما تتمثل الآليات الدولية المبذولة لمجابهة الجرائم السيبرانية؟ وإلى أي مدى كان التعاون الدولي فعالاً للتصدي لهذا الخطر؟

ويندرج تحت هذا السؤال مجموعة أسئلة فرعية وهي:

- ماهي الجريمة السيبرانية؟ وفيما تتمثل خصائصها وأركانها؟
- ما الصفات التي يتمتع بها المجرم المعلوماتي؟ وما هي دوافعه؟
- فيما تكمن الجهود الأمنية للقضاء على الجرائم السيبرانية؟
- كيف ساهم المشرع الجزائري في الحد من الجرائم السيبرانية؟
- ما هي الصعوبات التي واجهت التعاون الدولي لمواجهة هذه الجرائم؟

وللإجابة على هذه الأسئلة **إعتمدنا على المنهج التحليلي الوصفي** الذي رأيناه صالحاً لهذه الدراسة، فالمنهج التحليلي الوصفي يتجلى في كونه يعمل على تحليل المواد القانونية وتفسير النصوص المتعلقة بالدراسة، ويهدف إلى إيضاح وتبيان آليات التعاون الدولي لمكافحة الجرائم السيبرانية.

يهدف الموضوع إلى التعريف بالجريمة السيبرانية وطرق مكافحتها، إضافة إلى الجهود الدولية والعربية التي سعت لها الدول من خلال التعاون فيما بينهم عن طريق الإتفاقيات والمعاهدات للحد من هذه الجرائم، وتهدف هذه الدراسة أيضاً إلى تعزيز التعاون الأمني والقضائي عن طريق الأنتربول والأفريبول من أجل أن يعم الأمن والإستقرار في الدول، إضافة إلى ذكر الصعوبات والمعوقات التي واجهها التعاون الدولي للتصدي لهذه الجرائم وسبل التغلب عليها.

ومن بين الدراسات السابقة التي تناولت الجرائم السيبرانية نذكر ما يلي:

بعقيقي عبير، "**مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإمارلتي ـ دراسة مقارنة**"، (رسالة دكتوراه)، بجامعة محمد خيضر بسكرة، قسم الحقوق، الجزائر، 2018/2017م.

طارق أحمد مسعود، "**دور التعاون الدولي في مكافحة الجرائم الإلكترونية**"، (رسالة ماجستير)، جامعة أبوظبي ـ كلية الحقوق ـ ، الإمارات، 2022/2021م.

حيث أنّ هذه الدراسات فيها تشابه كبير مع دراستنا إذ يكمن التشابه مع الدراسة الأولى في كوننا تطرقنا إلى تأصيل الأحكام العامة للجرائم السيبرانية والدراسة الثانية تحدثنا عن آليات التعاون الدولي لمواجهة هذه الجرائم إلاّ أنّ هذه الدراسات تميزت بالتوسع الكبير مقارنةً بدراستنا.

وكما أنّه لا يخلو أي بحث علمي مهما كان من بعض الصعوبات التي تقف في وجه الباحث عند إعداد بحثه، **فمن بين هذه الصعوبات** عدم توفر الوقت الكافي للتّوسع أكثر فيما يخص الإتفاقيات جميعاً وغيرها.

وكانت خطة بحثنا كالتالي:

مقدمة وفصلين وخاتمة حيث تناولنا في الفصل الأوّل الذي كان تحت عنوان "الإطار المفاهيمي والقانوني للجريمة السيبرانية" إلى ثلاث مباحث ومطلبين في كل مبحث، تحدثنا في المبحث الأوّل على

ماهية الجريمة السيبرانية، وفي المبحث الثاني تطرقنا إلى أركان وأنواع الجريمة السيبرانية، أمّا بالنسبة للمبحث الثالث فقد خصصناه للمجرم المعلوماتي.

وفصل ثاني كان بعنوان "الآليات والجهود الدولية لمكافحة الجرائم السيبرانية "، الذي تطرقنا فيه إلى ثلاث مباحث أيضاً ومطلبين لكل مبحث، حيث سلطنا الضوء في المبحث الأوّل على آليات التعاون الدولي لمكافحة الجرائم السيبرانية، أمّا فيما يخص المبحث الثاني فقد عرّجنا على آليات التعاون العربي لمكافحة الجرائم السيبرانية، والمبحث الثالث تعرضّنا فيه إلى الصعوبات التي تواجه الجهود الدولية وسبل التغلب عليها.

الفصل الأوّل

مقدمة الفصل الأول:

الجريمة السيبرانية من الجرائم المستحدثة التي أصبحت تشكل خطراً كبيراً على العالم فهي هاجس العصر نظراً لإرتباطها بالتطور التكنولوجي، فهي تمثل نوعاً جديداً من الجرائم حيث تتمثل خصائصها في أنها جرائم عابرة للحدود إضافة إلى صعوبة إكتشافها ومن الممكن أن يتعاون أكثر من شخص للقيام بها...، وهذا ما أدى إلى تنوعها مثل: جريمة السرقة الإلكترونية، الإحتيال والنصب، الإتلاف المعلوماتي...

وتقوم الجريمة السيبرانية على 3 أركان تتمثل في الركن الشرعي والركن المادي والمعنوي فالركن الشرعي يتمثل في الصفة غير المشروعة للفعل، والركن المادي يتمثل في السلوك الإجرامي والنتيجة المترتبة عليها والعلاقة السببية أما بالنسبة للركن المعنوي وهو توفر العلم والإرادة والقصد الإجرامي.

ولقيام هذه الجريمة لابد من وجود أشخاص مختصين لهم خبرة في إختراق الأنظمة المعلوماتية كما يتمتعون بالذكاء والمهارة، ولهم دوافع أدت بهم إلى القيام بهذه الجرائم الشنيعة ومن بين هذه الدوافع المتعة والتحدي والرغبة في قهر النظام المعلوماتي إضافة إلى تحقيق الأرباح والرغبة في الإنتقام، وفي هذا الفصل سنتعرض بالتفصيل إلى "تأصيل الأحكام العامة للجريمة السيبرانية" الذي قسمناه إلى المبحث الأوّل بعنوان ماهية الجريمة السيبرانية الذي يندرج تحته مطلبين وهما: المطلب الأول الذي سنتناول فيه الجانب التاريخي، أمّا المطلب الثاني سيكون مفاهيم حول الجريمة السيبرانية وخصائصها. وتطرقنا في المبحث الثاني إلى أركان وأنواع الجريمة السيبرانية الذي ذكرنا في مطلبه الأول أركان الجريمة السيبرانية، وفي مطلبه الثاني أنواع الجريمة السيبرانية. أمّا فيما يخص المبحث الثالث فقد خصصناه للمجرم المعلوماتي حيث تضمن مطلبين، تمثل المطلب الأول في التعريف بالمجرم المعلوماتي وسماته، والمطلب 2الثاني حول دوافع الإجرام المعلوماتي.

المبحث الأول: ماهية الجريمة السيبرانية:

تعد الجريمة السيبرانية من أخطر الجرائم التي شهدها عصر التطور التكنولوجي، لما شهدته من إعتداءات على الأفراد والمؤسسات، فقد ارتبطت بالحاسوب من جهة وشبكة الأنترنت من جهة أخرى، وإتسمت بمجموعة من الخصائص ميزتها عن الجريمة التقليدية كونها عابرة للحدود الجغرافية إضافة إلى صعوبة إكتشافها وإثباتها وغيرها، وفي هذا المبحث سنأتي بذكر التطور التاريخي للحاسوب وكذا الأنترنت ومفاهيم عامة حولهما وكذا الخصائص المميزة للجريمة السيبرانية.

المطلب الأول: الجانب التاريخي:

إن لكل شيء في هذه الحياة جانب تاريخي يتأصل منه وجانب متجدد يتطور بظهور التكنولوجيا وهذا ما سهل حياة الأفراد والمجتمعات، فمع تطور العلم شهد العالم اكتشافات واختراعات جديدة ساعدت الأفراد عى المضي قدما نحو عالم تكون فيه الأنترنت والحاسوب نقطة مضيئة ساعدت في تقارب الأفراد والتواصل فيما بينهم بأسهل وأسرع الطرق.

الفرع الأول: التطور التاريخي للحاسوب:

يعتبر الحاسوب أداة مهمة في حياة الفلرد نظرا لفوائده لذلك عمل الإنسان على تطويره وجعله أسهل أداة للتواصل بين الناس "فمنذ تصميم أول جهاز حاسب والذي استلزم مساحة ملعب صغير لاستيعابه، تطورت صناعة الحاسب باتجاه الحجم الأصغر والذاكرة الأوسع والفعالية الأعلى والكلفة الأقل"[1].

حيث مر هذا الجهاز بعدة مراحل إلى أن وصل إلى المرحلة المتقدمة والمتطورة التي هو عليها الآن، ويمكن تصنيف هذه المراحل أو هذه الأجيال التي مر بها كما يلي:

1. **الجيل الأول: (1951 ـ 1959):**

" في بداية عام 1951 تم تطوير أول جهاز حاسوب للأغراض التجارية يدعى (Univercal) على يد العالمان (Mauchly and Eckert) ومن خصائص حواسيب هذا الجيل إستخدام الصمامات المفرغة

[1] علي جعفر،"**جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة–دراسة مقارنة–**"،ط1،مكتبة زين الحقوقية والأدبية، (د،ب)، 2013 م، ص ـ ص :48، 49.

التي تتميز بأنها: غالية الثمن، وتولد حرارة عالية وبطيئة. كما أن حجم حواسيب هذا الجيل كبير وعملية البرمجة صعبة حيث استخدمت في هذا الجيل لغة الآلة التي تعتبر صعبة".[1] ومن هنا نرى أن الحاسوب في البداية كان يستخدم من أجل الأغراض التجارية أي أنه لا يستخدم للتواصل بين الناس وحجم الحواسيب في هذا الجيل كان كبيرا مقارنة بالحاسوب الذي نملكه الآن إضافة إلى أن لغته كانت صعبة ومعقدة جدا.

2. الجيل الثاني: (1959 ـ 1964):

" وتميز هذا الجيل بظهور الترانزيستور كإختراع جديد في عالم الإلكترونيات الذي يمتلك مزايا عديدة لا يمتلكها الصمام المفرغ، حيث زادة سرعة تنفيذ العمليات الحسابية، وكان هناك انخفاض نسبي في الحجم والكلفة. كذلك تم استخدام لغات برجمة مثل لغة فوتران ولغة كوبول بدلا من لغة الآلة".[2] ففي هذا الجيل كان هناك تطور في سرعة تنفيذ العمليات على عكس ما كان عليه في المرحلة السابقة وهنا تقلص حجمه قليلا وتغيرت لغات البرمجة تدريجيا من لغة الآلة إلى لغة فوتران.

3. الجيل الثالث: (1964 ـ 1670):

" شهد هذا الجيل ولادة الدوائر المتكاملة التي كان لها أثر كبير في تصغير حجم الحاسب، كما زادت سرعة العمليات وإنخفضت تكاليف جهاز الحاسب، كما تم تحسين أجهزة الإدخال والإخراج ".[3] في هذه المرحلة وبولادة الدوائر المتكاملة تم تصغير حجم الحاسوب كما ساهمت في تحسين أجهزة الإدخال والإخراج أيضا هنا لاحظنا بداية تطور الحاسوب للأفضل.

4. الجيل الرابع: (1971 ـ 1981):

" مع إستخدام السيليكون Silicon في التكنولوجيا الحديثة لصناعة الذواكر والمعالجات، حصلت قفزة جديدة في صناعة الحاسبات، حيث تم بناء الدارات التكاملية المختلفة على رقائق السيليكون بدءاً من الدارات المندمجة ثم عالية الإندماج (LSI) مروراً بعالية الإندماج جداً (VLSI) وأخيراً وليس آخراً فوق العالية (ELSI). وقد سميت المعالجات التي تصنع من هذه الدارات المندمجة المعالجات الدقيقة /.../

---

[1] نهلا عبد القادر المومني، "**الجرائم المعلوماتية**" ، ط2، دار الثقافة، الأردن، 2010م، ص 31.

[2] المرجع نفسه، الصفحة نفسها.

[3] علي جعفر، المرجع السابق، ص50.

وأصبح الحاسب ينجز عشرات إلى مئات الملايين من العمليات في الثانية".[1] نلاحظ هنا أن جهاز الحاسوب شهد تطورا كبيرا في هذه المرحلة حيث أضافة رقاقة السيليكون تحسينات على أجهزة الإدخال والإخراج وأصبح الجهاز سريعا مقارنة بالأجيال السابقة.

5. الجيل الخامس: (1981 ـ 1991):

" عقد مؤتمر دولي في طوكيو في عام 1891 حيث أعلن اليابانيون مشروع الجيل الخامس للحاسبات الإلكترونية والتطور الذكاء الإصطناعي وإنتاج الحاسبات الدقيقة".[2] حيث شهدت هذه المرحلة تكور مميز وسريع لهذا الجهاز بفضل الذكاء الصناعي الذي هو عبارة عن برامج حديثة تحاكي العقول الذهنية البشرية، إضافة إلى إمتياز هذه الفترة بالسرعة الفائقة في إنجاز العمليات.

6. الجيل السادس: (1991 ـ حتى الوقت الحاضر):

" ومن خصائصه تقليد الدماغ البشري والتشبه به، فهناك محاولات لتقريب الأسلوب المتبع في معالجة المعلومات مع الأسلوب البشري. وتتركز تقنيات حواسيب الجيل السادس على مفاهيم الشبكات العصبية والمعالجات المتوازية".[3]من مميزات هذا الجيل أنه حاول التوفيق بين العقل البشري ونظام الآلة كل هذه الجهود للوصول إلى جهاز سهل الإستعمال يتناسب أسلوبه مع الأسلوب البشري.

الفرع الثاني: التطور التاريخي للأنترنت:

" أنشأت وزارة الدفاع الأمريكي (Department Of Defense) DOD عام 1957 وكالة لمشاريع الأبحاث المتقدمة (ARPA Advanced Research Project Ajency) تهتم بتطوير العلوم التي تخدم الإحتياجات العسكرية/.../ ويشير هاردي Hardy إلى أنّ تاريخ انترنت بدأ في الولايات المتحدة الأمريكية في أعوام الستينات" [4].

---

[1] صلاح الدين نور الدين، "**المعلوماتية**"، (د،ط)، منشورات وزارة الثقافة، دمشق، سوريا، 2000م، ص ـ ص: 19 ـ 20.

[2] خالد ممدوح إبراهيم، " **أمن الجريمة الإلكترونية**"، (د،ط)، الدار الجامعية، الإسكندرية، مصر، 2008م، ص 17.

[3] نهلا عبد القادر المومني، المرجع السابق، ص32.

[4] نبال إدلبي، "**أنترنت**"، تر: منى ملحيس، ط2، الدار العربية للعلوم، بيروت، لبنان، 1998م، ص 37.

" نشأت الأنترنت كفكرة (دعمت بواسطة وزارة الدفاع الأمريكية) عام 1969م لإجراء تجارب نحو إنشاء شبكة لربط مراكز الأبحاث من خلال ربط أربعة أجهزة حاسب آلي في عدد من ولايات الولايات المتحدة الأمريكية أشرفت عليها وكالة مشروع الأبحاث المتقدمة (Advanced Research Project Aency – ARPANET) وإستخدم في ذلك بروتوكول خاص يضم أكثر من مائة بروتوكول لتنظيم حركة نقل وتبادل المعلومات بين أجهزة الحاسب الآلي المختلفة".[1]

ومن هنا نلاحظ أن بداية شبكة الأنترنت جاءت من أجل تحقيق أغراض عسكرية حيث حاولوا ربط أكثر من جهاز بهذه الشبكة عن طريق ARPANET التي حاولوا من خلالها تسهيل نقل المعلومات بينهم عن طريق الحاسوب.

" ثم ظهور شبكة جديدة عام 1984 سميت بإسم (MIL NET) تخدم المواقع العسكرية فقط وتتولى (ARPNET) أمر الإتصالات غير العسكرية"[2] في هذه المرحلة بدأ تطور هذه الشبكة تدريجيا لكثرة إستخدامها وهذا ما أدى إلى إنشاء شبكة جديدة تخدم الجهة العسكرية فقط.

ومع مرور الأعوام بقيت الأنترنت شاملة للمجال العلمي البحثي والجانب العسكري إلى " أن حل عام 1990، حتى اعترت الشبكة عدد من العيوب وبدأت تعاني البطء، ناهيك عن ظهور الحواسيب الصغيرة في حجمها والقوية في كفاءتها وأدائها، التي أدت إلى ضعف الشبكة".[3]

إن الحاسوب وتطوره أدى إلى ظهور عائق أمام هذه الشبكة لأن كل تطور يجب أن يصاحبه تطور من نفس مستواه، ومن هنا توسعت مجالات الأنترنت من كونها محدودة من الجانب العسكري والجامعي فقط لتشمل المجالات التجارية أيضا فظهرت عدة شبكات وتطورت من بينها مايكروسوفت التي تضم أكثر من ألفي حاسوب.

---

[1] منصور بن فهد صالح العبيد، "**الأنترنت Internet إستثمار المستقبل**"، ط1، مكتبة الملك فهد الوطنية، الرياض، 1996م، ص32 .

[2] سفيان رقيق وعلي عز الدين، "**تفعيل إدارة العلاقة مع الزبون من منظور تكنولوجيا الأنترنت**"، مجلة البديل الإقتصادي، العدد6، الجلفة، الجزائر، ص 247.

[3] عمار عباس الحسيني، "**جرائم الحاسوب والأنترنت الجرائم المعلوماتية**"، ط1، مكتبة زين الحقوقية والأدبية، بيروت، لبنان، 2017م، ص23.

" ومما تجدر إليه الإشارة إلى أن ملكية شبكة الأنترنت اليوم، لا تعود لأي مؤسسة محددة أو دولة محددة، فلا يمكن لأحد أي يدعي ملكيته لهذه الشبكة، إنما باتت ملكيتها، ملكية دولية تعاونية"[1] فشبكة الأنترنت اليوم أصبحت ملكا للجميع الذين تتوفر فيهم شروط الإتصال بها، وبها تحول العالم إلى قرية صغيرة يسهل تواصل الأفراد فيما بينهم.

الفرع الثالث: التطور التاريخي للجريمة السيبرانية:

إن الجريمة مصطلح موجود منذ القديم فبظهور جهاز الحاسوب والأنترنت ظهرت أنواع جديدة من الجرائم وهي الجرائم السيبرانية، ومع التطور التكنولوجي أصبحت هذه الجرائم تشكل خطراً على الأشخاص والمؤسسات حيث تطورت هذه الجرائم ومرت بعدة مراحل:

"المرحلة الأولى: بظهور إستخدام الكمبيوتر وربطه بالشبكة في الستينات إلى السبعينيات، حيث ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي"[2] شهدت المرحلة الأولى بداية ظهور الجرائم السيبرانية مع بداية إستخدام الحواسيب حيث كانت معظم الجرائم تقع على البيانات وتخريب الأنظمة إضافة إلى التزوير المعلوماتي.

" المرحلة الثانية: في بداية الثمانينات، في هذه المرحلة ظهر مفهوم جديد لجرائم الكمبيوتر والأنترنت يرتبط بعمليات إقتحام نظام الكمبيوتر عن بعد كما ظهرت أنشطة الفيروسات الإلكترونية التي تقوم بتدمير الملفات والبرامج، وشاع مصطلح "الهاكرز" المعبر عن مقتحمي نظام الكمبيوتر"[3].

من ظهور الثمانينات زادت الجرائم التي تقع في الفضاء السيبراني عن طريق إختراق نظام الكمبيوتر إضافة إلى إنشاء فيروسات إلكترونية تعمل على التخريب الكلي للملفات حيث يقوم بهذه الأعمال الخطيرة مجرمي المعلومات الذين يتمتعون بمهارة فائقة في هذا المجال.

---

[1] عمار عباس الحسيني، المرجع السابق، ص24.

[2] لامية طالة وكهينة سلام، " **الجريمة الإلكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الإجتماعي**"، مجلة الرواق للدراسات الإجتماعية والإنسانية، المجلد6، العدد2، الجزائر، 2020م، ص 70.

[3] عفاف بعون ونسيمة ولاد سالم، "**الجريمة الإلكترونية - قراءة سسيوتاريخية في النشأة والآثار**"، مجلة القبس للدراسات النفسية والإجتماعية، المجلد5، العدد20، الجزائر، 2023م، ص 73.

"المرحلة الثالثة: حيث شهدت فترة التسعينات تنامياً هائلاً في حقل الجرائم الإلكترونية وتغيير في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الأنترنت من تسهيلات لعمليات دخول الأنظمة /.../ وفي البداية لم يكن ثمة إهتمام بمسائل الأمن بقدر ما كان الإهتمام ببناء الشبكة وتوسيع نشاطها /.../ وهذه الثغرة التي شجعت تنامي الجريمة الإلكترونية وتسببت في أضرار بالغة"[1].

إن ظهور شبكة الأنترنت وتطورها جعل الجرائم تكثر وتتزايد، فهذه التطورات أدت إلى فتح الطريق خاصة أمام مجرمي المعلومات حيث سهلت عليهم عملية الدخول للأنظمة لأن بداية ظهور الأنترنت كان الغرض منها بناء هذه الشبكة وتوسيع نشاطها فلم تهتم بمسائل الأمن وهذا الفراغ جعل من المجرمين يتفننون في إرتكاب جرائمهم وهذا ما أدى لتزايد الجرائم السيبرانية بكافة أنواعها.

المطلب الثاني: مفاهيم حول الجريمة السيبرانية وخصائصها:

من خلال هذا المطلب حاولنا الإلمام بمجموعة من المفاهيم التي تدور حول الجريمة السيبرانية والمتمثلة في تعريف جهاز الحاسوب وشبكة الأنترنت والجريمة السيبرانية من الجانب اللغوي والفقهي والقانوني، كل هذا لكي نخلص إلى تعريف شامل لهذه المفاهيم إضافة إلى ذلك تحدثنا أيضاً عن الخصائص التي تميز الجريمة السيبرانية عن غيرها من الجرائم.

الفرع الأول: مفاهيم حول الجريمة السيبرانية:

أوّلا: تعريف جهاز الحاسوب:

تنوعت وتعددت تعاريف الحاسوب من عدة جوانب لما يحمله من مميزات وأهمية بالغة في حياة الأفراد، فالحاسوب لغة من الفعل " حَسَبَ و حَسَبَهُ أي عدّهُ وهو مأخوذ من الحِساب لقوله تعالى :﴿ أُولَٰئِكَ لَهُمْ نَصِيبٌ مِّمَّا كَسَبُوا ۚ وَاللَّهُ سَرِيعُ الْحِسَابِ﴾ [2]، فالحَسْبُ العدّ والإحصاء بمعنى التدبير أي حاسبه حساباً[3]، لقوله تعالى:﴿ وَالَّذِينَ يَصِلُونَ مَا أَمَرَ اللَّهُ بِهِ أَن يُوصَلَ وَيَخْشَوْنَ رَبَّهُمْ وَيَخَافُونَ سُوءَ الْحِسَابِ﴾ [4]، وقوله

---

[1] لامية طالة وكهينة سلام، المقال السابق، ص ـ ص: 70 ـ 71.

[2] سورة البقرة، الآية 202.

[3] محمد بن مكرم علي أبو الفضل جمال الدين إبن منظور الأنصاري، "**لسان العرب**"، ط3، ج3، دار إحياء التراث العربي، بيروت، لبنان، 1999م، ص 162.

[4] سورة الرعد، الآية 21.

تعالى:﴿ الشَّمْسُ وَالْقَمَرُ بِحُسْبَانٍ﴾ [1]. إرتبط مفهوم الحاسوب لغة بالعد والحساب والتدقيق، وهذا ما إتفقت عليه المعاجم العربية والقواميس في شرحهم لهذا المصطلح.

ويعرف إصطلاحاً على أنه:" جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية طبقاً للتعليمات المعطاة له بسرعة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية من الدقة، وله القدرة على التعامل مع كم هائل من البيانات وتشغيلها وإسترجاعها عند الحاجة إليها"[2].

والحاسوب Computer هو" آلة إلكترونية يمكن برمجتها لكي تقوم بمعالجة البيانات وتخزينها وإسترجاعها وإجراء العمليات الحسابية والمنطقية عليها. وجهاز الحاسوب يقوم بتحليل وعرض ونقل المعلومات Information بأشكالها المختلفة، والمعلومات لها أشكال متنوعة قد تتمثل على هيئة أرقام أو أحرف للنصوص المكتوبة أو المرسومة وصور وأصوات"[3].

وعرّف أيضاً بأنّه " جهاز إلكتروني يتكون من مجموعة متداخلة من الأجزاء تعمل فيما بينها بهدف مشترك هو إخراج العمليات الحسابية والمنطقية طبقاً لبرنامج يتم وضعه مسبقاً من خلال عدة عمليات هي الإدخال والمعالجة والإسترجاع والإخراج"[4].

وعرفه الفقه على أنّه: "عبارة عن جهاز إلكتروني، مكون من مجموعة من الأجزاء المستخدمة في معالجة البيانات وعرضها في أفضل شكل" [5].

نستخلص من هذه التعاريف أن جهاز الكمبيوتر أو الحاسوب جهاز إلكتروني سهل للإنسان العديد من العمليات بفضل تطوره، حيث أنه يتمتع بالعديد من الوظائف التي تساعد الأفراد على تخزين بياناتهم أو تصفحها أو إرسالها من خلال الأوامر المعطاة له بفضل تطور التقنيات التكنولوجية والبرامج، كما فتح

---

[1] سورة الرحمان، الآية 05.

[2] عمار عباس الحسيني، المرجع السابق، ص13.

[3] عبد الرحمان صالحي ولبنى سويقات،" **تكنولوجيا الحاسوب والعملية التعليمية الجامعية**"، الملتقى الوطني الثاني حول (الحاسوب وتكنولوجيا المعلومات في التعليم العالي)، ورقلة، الجزائر،05 ـ 06 مارس 2014م، ص612.

[4] خالد ممدوح إبراهيم، المرجع السابق، ص 15.

[5] قلات سومية، " **الأحكام الإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري**"، (أطروحة دكتوراه)، جامعة محمد خيضر بسكرة، قسم الحقوق، الجزائر، 2024/2023م، ص 41.

هذا الجهاز العديد من الآفاق في جميع المجالات التربوية العسكرية التجارية وغيرها أمام الأفراد والمؤسسات وهذا ما ساعد على تسهيل العلاقات بين المجتمعات، فالدول، فالعالم بأسره.

ثانياً: تعريف شبكة الأنترنت:

قبل الولوج إلى التعاريف المختلفة لشبكة الأنترنت لابد لنا أن نذكر أن الجهاز الإلكتروني تعدى من كونه جهازاً يخزن المعلومات إلى جهاز يربط بين الدول والعالم عن طريق هذه الشبكة العالمية التي من خلالها نستطيع الربط بين ملايين الأجهزة الآلية بعضها مع البعض الآخر حول العالم.

"فالأنترنت (Internet) لغويا مشتقة من شبكة المعلومات الدولية، إختصار للإسم الإنجليزي (Inter –National Net Work) فهي مركبة من كلمتين "Inter" وهي مأخوذة من الكلمة اللاتينية (Inter Conercter) ومعناها الربط أو الفصل، نت "Net" وهي مأخوذة من الكلمة اللاتينية (Net Works) ومعناها الشبكات"[1].

وعّرفت شبكة الأنترنت بأنها:" عبارة عن عدة ملايين من أجهزة الحاسب الآلي المرتبطة ببعضها والمنتشرة حول العالم وتعمل ضمن بروتوكول موحد عام يمكن التعامل معه من أي جهاز حاسب آلي بإستخدام برامج وأنظمة مفتوحة متداولة"[2].

وتعرف أيضا بأنها: " أكبر شبكة حواسيب موسعة تغطي جميع أنحاء العالم /.../ وهذه الشبكة بالرغم من عالميتها وخط سيرها عبر الدول والقارات، إلاّ أنها لا تخضع لملكية فرد أو مؤسسة أو دولة، ويمكن لأي شخص أن يتواصل مع شبكة الأنترنت بمجرد توافر مستلزمات الإتصال لديه"[3].

وهناك من عرفها بأنها: " شبكة الشبكات، وبتعبير آخر هو مجموعة الشبكات العالمية المتصلة بعضها ببعض. ليس هناك شبكةواحدة محددة تدعى الأنترنيت، كما يوجد مثلاً شبكات تدعى Suranet أو Prepnet /.../ إنّ كل هذه الشبكات المحلية متصل بعضها ببعض في أنحاء العالم المختلفة لتشكل

---

[1] محمد يسعد ليلى، " **أهمية الأنترنت لدى الطالب الجامعي في ظل العولمة**"، (مذكرة ماجستير)، جامعة سعد دحلب، قسم علم الإجتماع، البليدة، الجزائر، 2005م، ص52.

[2] منصور بن فهد صالح العبيد، المرجع السابق، ص 32. .

[3] علي جعفر، المرجع السابق، ص60.

شبكة واحدة ضخمة تنقل المعلومات من منطقة إلى منطقة حول الأرض بسرعة فائقة وبشكل دائم التطور"[1].

تبيّن لنا من خلال هذه التعاريف أن الأنترنت أو الشبكة العنكبوتية كما يطلق عليها تعد أكبر شبكة تواصل في العالم لأن بها أصبح العالم عبارة عن قرية صغيرة يتواصل فيها الأشخاص بسهولة فيما بينهم رغم بعد المسافات وإختلاف الثقافات، فبمجرد أن يكون الشخص مالكاً لجهاز الكومبيوتر ومزوداً بهذه الشبكة فإنها تتيح له الإطلاع على أخبار جميع الأفراد، في جميع المجالات سياسية كانت أو تربوية أو عسكرية وغيرها لأن الأنترنت لا تعود ملكيتها لأي شخص أو مؤسسة أو دولة فهي متاحة للجميع عبر أنحاء العالم.

ثالثاً: تعريف الجريمة السيبرانية:

إن مفهوم الجريمة السيبرانية واسع النطاق لإشتماله على مصطلحين أساسيين وهما الجريمة والسيبرانية، وهنا سنأتي بذكر التعريف اللغوي والإصطلاحي والقانوني لكل واحد منهما على حدى بعدها سنعرف الجريمة السيبرانية تعريفاً شاملاً من كلا الجانبين التشريعي والدولي.

الجريمة لغة: "من الجُرْمُ: بمعنى التعدّي، والجُرْمُ وهو الذنب والجمع أجْرامٌ وجُرُومٌ، وهو الجرِيمَةُ، وجَرَمَ يَجْرِمُ جَرْماً واجْتَرَمَ وأَجْرَمَ، فهو مُجْرِمٌ وجَرِيمٌ. وجَرَمَ إليهم وعليهم جَرِيمة وأَجْرَمَ: جنى جناية، وجرُم إذا عَظُمَ جُرْمُهُ أي أذنب" [2].

والجريمة هنا بمعنى التعدّي على حرمة الآخرين وقد ورد في القرآن الكريم ذكر لهذا المعنى في قوله تعالى: ﴿ وَيَجْعَلُونَ لِلَّهِ مَا يَكْرَهُونَ وَتَصِفُ أَلْسِنَتُهُمُ الْكَذِبَ أَنَّ لَهُمُ الْحُسْنَىٰ ۖ لَا جَرَمَ أَنَّ لَهُمُ النَّارَ وَأَنَّهُم مُّفْرَطُونَ﴾[3]، وقوله أيضا: ﴿ لَا جَرَمَ أَنَّهُمْ فِي الْآخِرَةِ هُمُ الْأَخْسَرُونَ﴾[4]، وقوله تعالى في آية أخرى: ﴿ إِنَّ الَّذِينَ أَجْرَمُوا كَانُوا مِنَ الَّذِينَ آمَنُوا يَضْحَكُونَ﴾ [5].

---

[1] راجي أبو شقرة، " **دليل إستعمال خدمات الأنترنيت لغير المختصين**"، ط1، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان، 1997م، ص ـ ص: 9 ـ 10.

[2] إبن منظور،" **لسان العرب**"، ط1، مجلد2، دار إحياء التراث العربي، بيروت، لبنان، 1988م، ص258.

[3] سورة النحل، الآية 62.

[4] سورة هود، الآية 22.

[5] سورة المطففين ، الآية 29.

والجريمة في نطاق القانون تعرف على أنها: " فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيراً إحترازياً"[1].

كما عرّفت أيضاً " كل فعل له بعد مادّي خرج بوعي عن القواعد القانونية الجنائية المعمول بها في المجتمع، وبهذا الخروج يكون مساس بأمن وسلامة وإستقرار المجتمع"[2].

فالجريمة عبارة عن أفعال وسلوكات مجرمة من طرف القانون ونظراً لإختلاف الجرائم وضع المشرع لكل جريمة عقوبة لمنع الأفراد من الإعتداء على بعضهم.

السيبرانية: إنّ هذا المصطلح مصطلح حديث النشأة ويعد الأمريكي "نوربير وينر" أوّل من نسب إليه هذا المصطلح فقد عرّفه بأنّه:" علم التحكم والتواصل عند الحيوان والآلة، لنقل الرسائل بين الإنسان والآلة، أو بين الآلة والآلة، كما يعتبره علم القيادة أو التحكم في كل منهما"[3].

حاول العالم الأمريكي تبسيط هذا المصطلح فهو ذلك العلم الذي يربط بين الإنسان والآلة عن طريق شبكات التواصل، ولذلك ارتبط هذا المصطلح بشبكة الأنترنت لأنها الشبكة الوحيدة التي يتصل بها أكثر من نصف سكان العالم.

" لقد دفع التقدم التكنولوجي وثورة المعلومات، بالدول الكبرى إلى توظيف الأدوات السيبرانية لتعزيز قدرتها خاصة العسكرية، فالولايات المتحدة الأمريكية تعتمد بدرجة كبيرة على الأنترنت في عمليات تنظيم الجيش وزيادة قدراته في أرض المعركة (القيادة، الهجوم، السيطرة)، وكذا تنظيم الإمدادات وشبكة الإتصالات، وأي إختراق محتمل من الممكن أن يقوّض قدراتها الهجومية أو الدفاعيّة"[4].

ومن هنا نستنتج أن الفضاء السيبراني والتطور التكنولوجي أدّى بالدّول لزيادة قدراتها في المجال العسكري خاصة وأصبح العالم مترابطاً من خلال الشبكة العالمية وهي شبكة الأنترنت.

---

[1] محمود نجيب حسني، " **شرح قانون العقوبات**"، (د،ط)، دار النهضة العربية، القاهرة، مصر، 1962م، ص36.

[2] بسّام محمد أبو عليان، "**الإنحراف الإجتماعي والجريمة (علم إجتماع الجريمة)**"، ط3، منشورات أي ـ كتب، (د،ب)، 2016م، ص16.

[3] آسيا العمراني، "**التعاون الدولي في مواجهة الجرائم السيبرانية ـ الجرائم نموذجاً ـ** "، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد3، العدد2، الجزائر، 2010م، ص 57.

[4] المقال نفسه، ص58.

الجريمة السيبرانية: (المعلوماتية أو الإلكترونية):

مصطلح الجريمة المعلوماتية مصطلح شامل فيقصد به الجرائم المعلوماتية أو جرائم الحاسوب أو جريمة تقنية المعلومات، لذلك تعدّدت تعريفاته فالبعض عرفها بأنّها: " كل فعل أو امتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجاً، بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[1].

" ويتبنّى الخبير الأمريكي (Parker) مفهوماً واسعاً للجريمة المعلوماتية حيث يشير إلى أنها: " كل فعل إجرامي متعمّد أيّا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل"[2]، هنا توصل الخبير الأمريكي إللى أنّ الجريمة السيبرانية جريمة عمديّة فبحدوث الفعل الإجرامي تنشأ الجريمة.

تبنى الفقه الجزائري عدّة تعاريف للجريمة السيبرانية " إذ عرّف الجريمة المعلوماتية بأنها جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثّل من ناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[3].

أمّا بالنسبة للمشرع الجزائري فقد أطلق على هذه الجرائم تسمية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وذلك بموجب القانون رقم 15/04 المتعلق بقانون العقوبات [4].

كما استخدم مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال بموجب القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال:

" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى

---

[1] سامى على حامد عياد، " **الجريمة المعلوماتية وإجرام الأنترنت**"، (د، ط)، دار الفكر الجامعي، الإسكندرية، مصر، 2007م، ص 42.

[2] فتوح الشاذلي وعفيفي كامل عفيفي، "**جرائم الكمبيوتر (حقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون) دراسة مقارنة**، (د،ط)، منشورات الحلبي الحقوقية، لبنان، 2003م، ص 32.

[3] راضية عيمور، "**الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري**"، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد6، العدد1، الجزائر، 2022م، ص 91.

[4] القانون رقم 15/04، الصادر في 27 رمضان 1425هـ الموافق لـ10 نوفمبر 2004م، المعدل والمتمم للأمر 66/ 156 المتضمن استحداث قسم جديد في قانون العقوبات هو القسم السابع من المواد 394 مكرر حتى 394 مكرر7، الجريدة الرسمية، العدد 71، المؤرخة في 10 نوفمبر 2004م.

ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظم الإتصال الإلكترونية" [1].

وكذلك عرّفها من خلال الأمر رقم 11/21 في المواد من المادة 211 مكرر22 على أنّها: "أي جريمة ترتكب أو يسهل إرتكابها إستعمال منظومة معلوماتية أو نظام للإتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيا الإعلام والإتصال"[2].

ارتبطت الجريمة السيبرانية بالإعتداء على الأنظمة المعلوماتية والأموال سواء كانت مادية أو معنوية، وذلك عن طريق الأساليب المعلوماتية التي سهلت لها الأفق للقيام بتلك الجرائم، ومن هذه التعاريف نخلص إلى أن الجرائم السيبرانية ارتبطت بشكل كبير بالحاسوب وشبكة الأنترنت فبمجرد توفر هذه الأدوات تقوم هذه الجريمة.

الفرع الثاني: خصائص الجريمة السيبرانية:

أولا: الجريمة السيبرانية جريمة عابرة للحدود:

الجريمة السيبرانية عادة ما تتسم بالطابع الدولي إضافة إلى أن الأنترنت قد سهلت إرتكاب الجرائم من دولة إلى دولة أخرى، لذا فهذه الجريمة أصبحت عابرة للقارات " فهي تعتبر شكلاً جديداص من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل، جرائم التعدّي على قواعد البيانات، وتزوير وإتلاف المستندات الإلكترونية، والإحتيال المعلوماتي، وسرقة بطاقات الإئتمان، والقرصنة، وغسيل الأموال"[3].

ونلاحظ هنا أنه عن طريق الأنترنت أصبح التعدّي على الآخرين أسهل من قبل، فالشخص وهو في بيته من خلال حاسوبه يستطيع إرتكاب أشنع الجرائم وأبشعها في أي دولة من دول العالم.

---

[1] القانون رقم 04/09 المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد47، الصادر بتاريخ 16 أوت 2009م.

[2] الأمر رقم 11/21 المؤرخ في 16 محرم عام 1443هـ، الموافق 25 غشت سنة 2021م، يتمم الأمر رقم 155/66 المؤرخ في 18 صفر عام 1386هـ، الموافق لـ8 يونيو سنة 1966م، والمتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص 44.

ثانيا: صعوبة إكتشاف الجريمة السيبرانية:

الجريمة السيبرانية جريمة هادئة لذلك يعصب إكتشاف زمن وقوعها أو الشخص الذي قام بها حيث تعود " الأسباب التي تقف وراء الصعوبة في إكتشاف الجريمة الإلكترونية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، فلا يوجد جثث لقتلى ولا لآثار للدماء، كما أنّ المجرم يمكنه إرتكاب هذه الجريمة في دول وقارات مختلفة إذ أنّ الجريمة الإلكترونية كما سبق وأشرنا جريمة عابرة للحدود وكذلك فإنّ قدرة المجرم تدمير دليل الإدانة في أقل من ثانية الواحدة يشكل عاملاً إضافياً في صعوبة إكتشاف هذا النوع من الجرائم "[1]. ومن هنا فهذه الجريمة تحدث في سرية تامة لأنّ مجرمي المعلومات يتمتعون بتقنيات عالية تمكنهم من عدم كشف الجريمة التي قاموا بها.

ثالثا: صعوبة إثبات الجريمة السيبرانية:

صعوبة إثبات الجريمة السيبرانية راجع إلى: " أنّها كجريمة لا تترك أيّ آثار مادية لها بعد إرتكابها، فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية ولا توجد مستندات ورقية.

صعوبة الإحتفاظ الفني بدليل الجريمة المعلوماتية، إذ يستطيع المجرم المعلوماتي في أقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكمبيوتر"[2]. نستنتج مما سبق أنّ الجريمة السيبرانية يصعب إثباتها نظراً لأنها تحدث في بيئة إلكترونية غير مرئية تسهّل على الفاعل إخفاء دليله.

رابعا: الجريمة السيبرانية جريمة مستحدثة:

تعد الجريمة السيبرانية من الجرائم الجديدة الخطيرة التي شاعت في عصرنا في ظل وجود شبكة الأنترنت والعولمة، " حيث أنّ التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل أنه أضعف من

---

[1] رضا عسّال وعماد عبد الرزاق، "**الجريمة الإلكترونية والمجرم المعلوماتي: مقاربة مفاهيمية**"، مجلة ببليوفيليا، العدد5، تبسة، الجزائر، 2020م، ص 154.

[2] كوثر مازوني، "**الجريمة المعلوماتية**"، ط1، دار الخلدونية، الجزائر، 2022م، ص 452.

قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها"[1].نرى هنا أنّ الأنترنت سلاح ذو حدّين فرغم منافعها إلاّ أنّها شكلت خطورة كبيرة على المجتمع فارتبطت بالجرائم السيبرانية، ومن أبرز الجرائم التي تقع على هذه الشبكة: تهريب المخدرات، غسيل الأموال، الرشوة... إلخ.

خامسا: تعاون وتواطئ أكثر من شخص على إرتكاب الجريمة السيبرانية:

تعدّ هذه الجريمة من الجرائم التي يستطيع القيام بها شخص بعينه كما يمكن أن يقوم بها مجموعة من الأشخاص بالتعاون فيما بينهم، " وغالباً ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفنّي من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التّلاعب وتحويل المكاسب إليه" [2].

نستخلص هنا أنّه لإرتكاب الجريمة يجب على الشخص أن يتمتع بخصائص تمكنه من إنجاح هذه الجريم، لذلك لا يكفي شخص واحد لها بل بالتعاون مع مجموعة من الأشخاص وأبرز هؤلاء الأشخاص الذين يجيدون إستخدام تقنيات الحاسوب، وآخرون متواجدون في البيئة المحيطة بهذه العملية الإجرامية لتشتيت الإنتباه حتى تنتهي عمليتهم.

سادسا: الجريمة السيبرانية جريمة ناعمة:

" إذا كانت الجرائم التقليدية تحتاج من مرتكبها إلى قوة عضلية لتنفيذها، فإنّ جرائم المعطيات لا تحتاج إلى مثل تلك القوة العضلية، وإنّما تحتاج إلى قوة علمية وقدرة من الذكاء ومهارة في توظيف ذلك، والجاني في سبيل تنفيذها لا يحتاج من الوقت إلاّ ثوان أو دقائق معدودات، ولا يحتاج من القوة العضلية غير تحريك الأنامل على جهاز الكمبيوتر"[3].

يقصد بالجريمة السيبرانية أنها جريمة ناعمة وهادئة لأنّها عادة لا تحتاج لبذل مجهود عضلي بل تقوم على الكفاءات الذهنية للأفراد وهذا ما يتسم به مجرمي المعلومات إذ يتمتعون بذكاء فائق.

---

[1] عبد الله دغش العجمي، "**المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة**"، (مذكرة ماجستير)، جامعة الشرق الأوسط، قسم القانون العام، 2014م، ص 25.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 58.

[3] كوثر مازوني، المرجع السابق، ص 250.

المبحث الثاني: أركان وأنواع الجريمة السيبرانية:

الجريمة السيبرانية جريمة حديثة النشأة نظراً لإرتباطها بالشبكة العنكبوتية ومع التطور التكنولوجي وما صاحبه من أجهزة ذكية كالحاسوب والهواتف النقالة الذكية، أدّى ذلك إلى ظهور العديد من الجرائم حيث تنوعت هذه الأخيرة بأساليب مختلفة مسّت بالأفراد والمؤسسات أيضاً، وفي هذا المبحث سنتحدّث عن أركانها المتمثلة في الركن الشرعي والمادّي والمعنوي وذكر بعض أنواعها كالإحتيال والسرقة الإلكترونية والإتلاف المعلوماتي...

المطلب الأول: أركان الجريمة السيبرانية:

إنّ الجريمة ناتجة عن الأفعال الصادرة عن الإنسان حيث تختلف الجرائم من حيث طبيعة القيام بها فلكل جريمة أركان تميزها عن غيرها، ومن خلال هذا المطلب سنذكر أهم هذه الأركان وهي ثلاث والمتمثلة في الركن الشرعي والركن المادي والركن المعنوي.

الفرع الأوّل: الركن الشرعي:

" معناه إعتراف المشرع والنص على تجريم الفعل المرتكب، "لا جريمة ولا عقوبة إلاّ بنص"، بالنسبة للتشريع الجزائري فقد أحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث خاص بجرائم الجنايات والجنح ضدّ الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات "[1].

ويقصد هنا بالركن الشرعي للجريمة أنّه يوجد نص يجرّم هذه الأفعال ويوقع العقاب على مرتكبي هذه الجرائم، ومن هنا نلاحظ أنّ الجرائم السيبرانية تأخذ شرعيتها من التشريعات الوطنية التي تسعى جاهدة من أجل وضع تشريعات لمواجهتها.

الفرع الثاني: الركن المادي:

" يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية علماً أنّه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها" [2].

---

[1] كوثر مازوني، المرجع السابق، ص 344.

[2] راضية عيمور، المقال السابق، ص95.

يقوم الركن المادي للجريمة السيبرانية على صورتين أساسيتين:

" الأولى متمثلة في الإعتداءات على نظام المعالجة الآلية وهذه الأخيرة تحتوي على نوعين من الأعتداء الأول وهو الدخول والبقاء غير المشروع في نظام المعالجة الآلية /.../ أمّا النوع الثاني متمثل في الإعتداء العمدي على نظام المعالجة الآلية للمعطيات/.../ والصورة الثانية متمثلة في الإعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي" [1].

وهنا يرتكز الركن المادي على صورتين المتمثلة في الإعتداء على نظام المعالجة الآلية من جهة والإعتداء على منتجات الإعلام الآلي من جهة أخرى.

وقد نصّت المواد 394 مكرر و394 مكرر2 من قانون العقوبات على أنّه:

"يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000دج[2].

من خلال هذه المادة نستنتج وجود صورتين لفعل الدخول أو البقاء الغير مشروع لنظام المعالجة الآلية للمعطيات وكذا تخريب نظام إشتغال المنظومة فالأولى تعتبر صورة بسيطة أمّا الثانية فهي صورة مشددة. كما نصت المادة 394 مكرر2 من قانون العقوبات الجزائري على أنّه:

" يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج، كل من يقوم عمداً وعن طريق الغش بما يأتي:

[1] إيمان بغدادي،"**أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية**"، مجلة آفاق للبحوث والدراسات السياسية، العدد4، الجزائر، 2019م ، ص 189.

[2] القانون 15/04 المتضمت إستحداث قسم جديد في قانون العقوبات، المرجع السابق.

1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
2. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم" [1].

يتضح لما من خلال هذه المادة أنّ الفعل الثاني لتحقق الركن المادي للجريمة السيبرانية يتمثل في الإعتداءات على منتجات الإعلام الآلي فهذا الفعل يعتبر من أخطر صور الغش المعلوماتي.

ثالثا: الركن المعنوي:

" من المتصور غالباً أن لا تقع الجريمة الإلكترونية إلاّ بصورة عمديّة سبقها التفكير في الحصول على المعلومة أو إختراق الشبكة. والأصل في الجرائم هو العمدية إلاّ ما إستثني بنص، وهناك من الجرائم ما يتطلب المشرع إرادة إرتكاب السلوك وتحقق النتيجة، حيث يكتفي بتوافر القصد الجنائي العام بصورتيه العلم والإرادة كالدخول إلى أنظمة المعلومات وتدمير المعلومات الموجودة بها /.../لكن قد يتطلب المشرع إضافة إلى القصد الجنائي العام قصداً جنائياً خاصّاً كضرورة توافر نية التملك للأموال" [2].

وهنا نرى أن الجرائم السيبرانية الأصل فيها أنّها جرائم عمدية تتطلب قصد جنائي عام والمتمثل في العلم والإرادة، من خلال ما سبق ذكره أنّ الركن المعنوي للجريمة السيبرانية يختلف بإختلاف أشكالها ولقيام هذا الركن يكفي توفر العلم والإرادة ولكن في بعض الأحيان قد ترتكب هذه الجرائم من غير قصد، وهنا تبين لنا أنّ الدخول الغير المشروع للأنظمة دون علم الجاني ينفي القصد الجنائي للجريمة.

المطلب الثاني: أنواع الجرائم السيبرانية:

تعددت أنواع الجرائم السيبرانية حيث إتسمت بأنّها خرق للأنظمة الإلكترونية لذلك وجب على المشرع وضع قوانين صارمة للحد من هذه الجرائم ومن هنا سنذكر بعض من هذه الأنواع:

---

[1] قانون رقم 15/04 المتضمن إستحداث قسم جديد في قانون العقوبات، المرجع السابق.

[2] غنية باطلي، "**الجريمة الإلكترونية دراسة مقارنة**"، (د،ط)، الدار الجزائرية، الجزائر، 2016م، ص 48.

الفرع الأول: جريمة السرقة الإلكترونية:

تعد السرقة من أكبر الجرائم التي يعاقب عليها القانون فهي وفقاً للقواعد العامة لقانون العقوبات الجزائري " كل من إختلس شيئا غير مملوك له يعد سارقاً"[1]. من خلال قانون العقوبات نرى أنّه يجب أن يكون هناك شيئاً ملموساً يستطيع الإنتقال من مالكه الأصلي إلى شخص آخر، وهنا تقوم جريمة السرقة.

"وجريمة سرقة المعلومات والبرامج هي كل فعل من شأنه الإستيلاء على برامج المعلومات مملوكة للغير في داخل جهاز الكمبيوتر المرتبطة بشبكة الأنترنت وذلك عبر إرسال برامج فيروس من شأنه نسخ هذه البرامج والمعلومات والحصول عليها /.../ من خلال إستغلال وجود ضعف أمني في النظام التشغيلي يسهل عملية السرقة أو من خلال إعتداءات مادية على الرقابة ذاتها"[2].

تقوم جريمة السرقة هنا من خلال إختراق البرامج عن طريق إرسال الفيروسات التي تساعدهم على نسخ البرامج والحصول على المعلومات المراد الوصول إليها وهذا نظراً لوجود ضعف أمني في النظام فيسهل على مجرمي المعلومات القيام بعملياتهم.

الفرع الثاني: جريمة الإحتيال والنصب:

عرفت جريمة النصب والإحتيال في العديد من التشريعات الجزائري والمصري والأرني والكويتي حيث عرّفها المشرع الجزائري في المادة 372 من قانون العقوبات على أنّها: " كل من توصل إلى إستيلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من إلتزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالإحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إمّا بإستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو إعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخِشية من وقوع أي

[1] القانون رقم 06/ 23 الصادر في 20 ديسمبر 2006 لقانون العقوبات الجزائري، الجريدة الرسمية، العدد 89، المؤرخة في 20 ديسمبر 2006م، المعدل والمتمم.

[2] حسين طاهري، " **الجرائم الإلكترونية**"، ط1، دار الخلدونية، الجزائر، 2021م، ص ـ ص: 41 ـ 42.

شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500دج إلى 20.000دينار"[1].

حيث قام المشرع الجزائري بوضع "قانون خاص جديد 05/18 يتعلق بالتجارة الخارجية الذي يحدد القواعد العامة المتعلقة بالتجارة الإلكترونية للسلع والخدمات" [2]. من خلال هذه المادتين يتبين لنا أنّ جريمة النصب والإحتيال تقوم على خداع الأشخاص وذلك عن طريق إستخدام طرق إحتيالية للإستيلاء على أموال أو منقولات أو سندات لنزع بعض أو كل ملكيتها، ويعتمد الجاني هنا على إستعمال صفات وأسماء كاذبة لإقناع الأشخاص للقيام بجريمته.

"وقد تطورت هذه الجريمة من طابعها التقليدي من الجاني المجني عليه إلى وسيلة أكثر ذكاء وتصرفا من خلال شبكة الأنترنيت وإنه من الإنتشار الواسع لشبكة الأنترنيت وسهولة إستخدامها في مجالات واسعة كبيع السلع والتبادل التجاري وتحويل الأسواق إلكترونياً والدفع عبر بطاقات الإئتمان، كان من الطبيعي إستخدام هذه الوسائل المتطورة في عمليات نصب وإحتيال. كإنتحال، إسم كاذب أو صفة غير صحيحة"[3].

أحدثت الأنترنت مع ظهورها آفاقاً للمجرمين للتمادي في جرائمهم من خلال الأنظمة المتطورة والحديثة التي سهلت للجاني وساعدته في الإحتيال على الأشخاص عن طريق المواقع الوهمية المتمثلة في الأسواق الإلكترونية من خلال إيهامهم بوجود شركات أصلية يصعب على الأشخاص إكتشافها نظراً للتطور التكنولوجي الذي وصلنا إليه اليوم.

الفرع الثالث: جريمة الإتلاف المعلوماتي:

إنّ جريمة الإتلاف المعلوماتي "تتمثل بالإعتداء على سير نظام المعالجة الآلية للبيانات بمختلف

---

[1] الأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، الجريدة الرسمية، العدد 84، صادرة بتاريخ 10 جوان 1966م، المعدل والمتمم.

[2] القانون رقم 05/18 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد 28، مؤرخة في 16 ماي 2018م.

[3] حسين طاهري، المرجع السابق، ص 44.

التصرفات التدليسية المتمثلة بالدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه، وبما يترتب عليه من إتلاف للبيانات والبرامج أو بما يؤدي إليه من تعطيل أو إفساد نظام التشغيل.

ويقع الإتلاف على النظام المعلوماتي، سواء أكان ذلك بالدخول العمدي للنظام المعلوماتي أو بإستخدام الجاني الطرق التقنية والفنية للإتلاف كالفيروسات "Virus"[1].

تقع جريمة الإتلاف المعلوماتي على أنظمة الحاسوب حيث يقوم الجاني بالدخول عمداً لهذا النظام وتعطيله أو قد يلجأ إلى ذكائه ويستخدم تقنيات فنية كإرسال الفيروسات والبرامج التي تساعده لإفساد هذا النظام.

"تتنوع الطرق الفنية والتقنية المستخدمة لأتلاف البيانات والبرامج بدءاً من فيروسات الحاسب الآلي (Programmes Virus) ومروراً ببرنامج الدودة (Worm Software) وإنتهاءاً بالقنبلى المنطقية أو الزمنية (Logic Bomb). ويتفق الفقهاء في كل من إنجلترا والولايات المتحدة على أن المشكلات القانونية التي تنشأ عن جميع الفيروسات تكاد تكون واحدة، فلا وجه للتفرقة بين الفيروس والدودة وحصان طروادة، فهي نفس الفيروسات ويترتب عليها نفس المشكلات القانونية"[2]. والملاحظ هنا أنه مهما إختلفت الطرق والتقنيات التي يستخدمها الجاني سواء كانت فيروسات أو برامج كالدودة وحصان طروادة إلاّ أنّ النتيجة في كل هذا هي واحدة والتي تتمثل في إتلاف الأنظمة المعلوماتية.

الفرع الرابع: جريمة تزوير البيانات:

"تعتبر جرائم تزوير البيانات من أكثر الجرائم شيوعاً من بين كافة أنواع الجرائم التي ترتكب سواء على شبكة الأنترنت أو ضمن جرائم الحاسب الآلي نظراً لأنّه لا تخلو جريمة من الجرائم إلاّ ويكون من بين تفاصيلها جريمة تزوير البيانات بشكل أو بآخر"[3]. إنّ جريمة تزوير البيانات من الجرائم الخطيرة والأكثر إنتشاراً لذلك وضع لها القانون عقوبات مشددة حيث أنها ترتكب على شبكة الأنترنت إذ لا تقوم الجريمة إلاّ وكان التزوير جزءاً منها.

---

[1] محمد أمين الشوابكة، " **جرائم الحاسوب والأنترنت الجريمة المعلوماتية**"، ط1، دار الثقافة، عمان، 2007م، ص 222.

[2] المرجع نفسه، ص ـ ص: 237 ـ 238.

[3] منير محمد الجنبيهى وممدوح محمد الجنبيهى، " **جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها**"، ط2، دار الفكر الجامعي، الإسكندرية، مصر، (د، س)، ص90.

" وتزوير البيانات (Forgery Of Data) يكون بالدخول ـ سواء بطريقة شرعية أو غير شرعية ـ على قاعدة البيانات DATA BASE الموجودة وتعديل تلك البيانات سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل"[1].

ويعني هنا أن التزوير هو إضافة بيانات أو محو أخرى بما يتناسب مع مصالح الجاني وقد يستخدم كافة الطرق المسموحة والغير مسموحة ليتم الولوج داخل الأنظمة كل هذا لإنجاح عمليته الإجرامية.

الفرع الخامس: جريمة غسيل الأموال:

إرتبطت جريمة غسيل الأموال الإلكتروني بمصطلح الغسيل الرقمي "الذي هو عبارة عن تحويلات نقدية عبر شبكة الأنترنيت ومن مزايا هذه الطريقة تسهيل عمليات الدفع للمتعاملين في الأموال والتجارة الإلكترونية ولكن في المقابل زادت إحتمالات القرصنة وصعوبة الرقابة على المتعاملين في ظل الإلتزام بسرية المعلومات المصرفية"[2].

نرى هنا أنّ الغسيل الرقمي سهل عملية الدفع إلكترونياً وهذا ما ساعد المجرمين الإلكترونيين من خلال القرصنة عبر شبكة الأنترنت القيام بهذه الجريمة، ومن مميزات هذه الجريمة أنها تتسم بالسرية وإخفاء المصدر الغير شرعي الذي أتت منه هذه الأموال، فالإنسان بطبعه يسعى إلى الربح السريع وبطرق شرعية أو غير شرعية حتى وإن كان هذا ناتج عن أعمال غير مشروعة ومجرّمة من طرف القانون كالمتاجرة بالمخدرات والسلاح وغيرها من الجرائم التي تمس إقتصاد الدولة.

" ويصف أحد الباحثين العلاقة بين الأنترنت وغسيل الأموال بأنّها حركة سريعة ولا توقفها الحدود الجغرافية والجودة ذاتها تجعل الأنترنت والبطاقات الذكية محل ترحيب من الجمهور، وكذلك محل جاذبية من المجرمين الذين هم في شوق لغسل أموالهم بهدوء وسرعة، فالنقود الإلكترونية وسيلة سهلة في التحويل والنقل من مكان لآخر" [3].

---

[1] مبير محمد الجنبيهى وممدوح محمد الجنبيهى، المرجع السابق، ص 90.

[2] حسين طاهري، المرجع السابق، ص 40.

[3] أمير فرج يوسف، "**الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت**"، ط1، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2011م، ص 39.

ونرى هنا أنّ شبكة الأنترنت سهلت للمجرمين عملية غسيل الأموال في سرية تامة وبما أنّها جرائم عابرة للحدود فسحت مجال لتحويلها لأي مكان من هذا العالم.

المبحث الثالث: المجرم المعلوماتي:

بعد تطرقنا لماهية الحاسوب والأنترنت والجريمة السيبرانية وأنواع وخصائص هذه الجريمة، يجدر بنا الإشارة في هذا المبحث إلى التعريف بالمجرم المعلوماتي وأهم السمات التي تميزه وأبرز الدوافع التي أدت به لإرتكاب مثل هذه الجرائم.

المطلب الأول: التعريف بالمجرم المعلوماتي وسماته:

الجريمة السيبرانية كغيرها من الجرائم تقوم من طرف المجرمين المعلوماتيين الذين لهم خبرة في إختراق الأنظمة المعلوماتية فعادةً ما يقوم بهذه الجرائم أشخاص طبيعيين ولكن هذا لا يمنع أن كون المجرم المعلوماتي شخصاً معنوياً، إضافة إلى أنه يتسم بسمات تميزه عن غيره مثل: الذكاء، المهارة، وغيرها كل هذه السمات جعلت منه محترفاً في جرائمه حيث يصعب على رجال القضاء كشفه في بعض الأحيان ومن خلال هذا المطلب سنتعرف على المجرم المعلوماتي وسماته.

الفرع الأول: تعريف المجرم المعلوماتي:

تعددت مفاهيم المجرم المعلوماتي وتنوعت بحسب المجالات المنتمية إليه، فالمجرم في اللغة: من" أَجْرَمَ، فهو مُجْرِمٌ و جَرِيمٌ، والجَارِمُ هو الجاني والمُجْرِمُ: المُذْنِبُ"[1]، وقد أورد الله في قرآنه الكريم المجرمين في عدّة سور منها قوله تعالى: ﴿ فَمَنْ أَظْلَمُ مِمَّنِ افْتَرَىٰ عَلَى اللَّهِ كَذِبًا أَوْ كَذَّبَ بِآيَاتِهِ ۚ إِنَّهُ لَا يُفْلِحُ الْمُجْرِمُونَ﴾ [2]، وأيضاً: ﴿ وَرَأَى الْمُجْرِمُونَ النَّارَ فَظَنُّوا أَنَّهُم مُّوَاقِعُوهَا وَلَمْ يَجِدُوا عَنْهَا مَصْرِفًا﴾ [3]، وقال أيضاً: ﴿يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تُحِلُّواْ شَعَٰٓئِرَ ٱللَّهِ وَلَا ٱلشَّهۡرَ ٱلۡحَرَامَ وَلَا ٱلۡهَدۡيَ وَلَا ٱلۡقَلَٰٓئِدَ وَلَآ ءَآمِّينَ ٱلۡبَيۡتَ ٱلۡحَرَامَ

[1] إبن منظور، المعجم السابق، ص 258.

[2] سورة يونس، الآية 17.

[3] سورة الكهف، الآية 53.

يَبْتَغُونَ فَضْلًا مِّن رَّبِّهِمْ وَرِضْوَٰنًا ۖ وَإِذَا حَلَلْتُمْ فَٱصْطَادُوا۟ ۚ وَلَا يَجْرِمَنَّكُمْ شَنَـَٔانُ قَوْمٍ أَن صَدُّوكُمْ عَنِ ٱلْمَسْجِدِ ٱلْحَرَامِ أَن تَعْتَدُوا۟ ۘ وَتَعَاوَنُوا۟ عَلَى ٱلْبِرِّ وَٱلتَّقْوَىٰ ۖ وَلَا تَعَاوَنُوا۟ عَلَى ٱلْإِثْمِ وَٱلْعُدْوَٰنِ ۚ وَٱتَّقُوا۟ ٱللَّهَ ۖ إِنَّ ٱللَّهَ شَدِيدُ ٱلْعِقَابِ﴾ [1].

المجرم المعلوماتي هو " شخص يجيد إستخدام الكمبيوتر والأنترنت بإحتراف لذا يتسنى له تدمير وإختراق وسرقة البرامج والمعلومات المخزنة على الحاسب ولما كان جهاز الكمبيوتر موجود داخل كل منزل كان من السهل على كل مجرم معلوماتي أن يرتكب الجرائم المعلوماتية وهو داخل منزله دون أن يراه أحداً ويمسك به"[2].

" يطلق خبراء أمن المعلومات الإلكترونية مصطلح "Hackers" وهي جمع لكلمة هاكر وهو الإنسان الذي يقوم بعمليات الإختراق والتخريب عبر شبكة الأنترنيت كما يطلقون مصطلح كراكرز "Crackers" على المتخصصين بفك شفرات البرامج، وليس تخريب الشبكات فهم نوع من الهاكرز المتخصص" [3].

" فيما يميل البعض إلى تسمية المجرم المعلوماتي ب"المجرم الإلكتروني الرقمي" ويعرفه بأنّه " من لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها وإسترجاعها بإستخدام الحاسوب الإلكتروني أو الرقمي وملحقاته ووسائل الإتصال الرقمية، وذلك بأداء فعل أو إمتناع عنه مما يحدث إضطرابات في المجتمع الدولي أو المحلي نتيجة مخالفة قواعد الضبط الإجتماعي محلياً أو دولياً" [4].

نلاحظ من خلال التعاريف المذكورة أعلاه أن الشخص الذي يطلق عليه المجرم المعلوماتي هو تقني المعلومات وذلك لإمتلاكه مهارات تمكنه من التعدّي على الأنظمة بإستخدام الحاسوب، حيث نرى أن العديد من المختصين في المجال القانوني ذهبوا إلى أنّ المجرم المعلوماتي ليس بالضرورة أن خلفية إجرامه بحتة إنّما يفعل ذلك لإثبات قدرته على إختراق نظم الحاسوب، وهناك من يقوم به بدافع الإنتقام أو ردّ الإعتبار، لذلك فالمجرم المعلوماتي يشكل خطراً على المجتمعات يجب الحذر منه لأنّه يستطيع أن يستخدم الحاسوب والأنترنت لحسابه الخاص ولصالحه.

---

[1] سورة المائدة، الآية 02.

[2] نسرين عبد الحميد نبيه، "**الجريمة المعلوماتية والمجرم المعلوماتي**"، (د،ط)، دار المعارف، الإسكندرية، مصر، 2008م، ص 4.

[3] خليلي سهام، "**خصوصية المجرم الإلكتروني**"، مجلة المفكر، العدد 15، سطيف، الجزائر، 2017م، ص 405.

[4] عمار عباس الحسيني، المرجع السابق، ص 58.

الفرع الثاني: سمات المجرم المعلوماتي:

هناك مميزات تميز المجرم المعلوماتي عن المجرم التقليدي لأن هناك سمات أساسية متواجدة في شخصيته لا يمكن الإستغناء عنها، وسنتطرق هنا لذكر أهم هذه السمات:

أولا: الذكاء والمهارة في مجال التعامل مع التقنية المعلوماتية:

إن الجريمة السيبرانية جريمة تحدث في فضاء الأنترنت عن طريق الحاسوب لذلك وجب وجود أشخاص مختصين ويتمتعون بصفات محددة لكي تنجح عمليتهم الإجرامية حيث أنّ المجرم المعلوماتي " يتمتع بالذكاء والمهارة في مجال إستخدام والتعامل مع تقنية المعلوماتية فهو:

ـ يتميز بالقدرة على إختراق النظم المعلوماتية (حواسيب وشبكة إتصال) والتلاعب بأنظمتها الأمنية.

ـ يبتكر أساليب متطورة لإرتكاب أفعاله.

ـ لديه قدرة فائقة على المعالجة الإلكترونية للنصوص والكلمات، والتعامل مع البرامج"[1].

ونرى هنا أنّ المجرم المعلوماتي يتميز بالذكاء والمهارة مقارنة بالمجرم التقليدي الذي يكون العنف سلاحه، عكس المجرم المعلوماتي الذي يسعى إلى معرفة كل جديد بهدف إختراقه حيث يستخدم معرفته وتصوره الكامل لإنجاع عمليته الإجرامية.

ثانيا: المجرم العلوماتي إنسان إجتماعي:

إنّ المجرم المعلوماتي إنسان عادي بالدرجة الأولى وبذلك فهو إنسان إجتماعي، فهو يتميز بقدرته على ملائمة بيئته المحيطة به فكما سبق وذكرنا أنه يتميز بالذكاء، وهذا الذكاء سلاح ذو حدين فمن جهة يساعده على الإنخراط داخل المجتمع ومن جهة أخرى تكثر خطورته الإجرامية.

[1] ربيعي حسين، "**المجرم المعلوماتي ـ شخصيته وأصنافه ـ** "، مجلة العلوم الإنسانية، العدد40، بسكرة، الجزائر، 2015م، ص ـ ص: 288 ـ 289.

" فشعور المجرم أنه محل ثقة من مجتمعه وشعوره بأنه خارج إطار الشبهات قد يدفعه إلى التمادي في إرتكاب جرائمه التي قد لا تكتشف، وإذا إكتشفت فإنها تواجه صعوبة الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء"[1].

وهنا يتبين أن المجرم يستغل ثقة المجتمع المحيط به للقيام بعمليات إجرامية يعصب إكتشافها وإثباتها من طرف القضاة، لأن المجرمين المعلوماتيين يستخدمون ذكائهم في الإنخراط في المجتمع وهذا ما يؤدي بهم في التمادي في إرتكاب هذه الجرائم.

ثالثا: المجرم المعلوماتي يتمتع بالسلطة تجاه النظام المعلوماتي:

" تشير السلطة إلى حقوق أو إمتيازات الإستخدام التي يتمتع بها المجرم، أو التي يحتاج الحصول عليها من أجل إرتكاب الجريمة، ويحصل المجرمون على السلطة اللازمة لإساءة إستخدام ملفات معلومات الكمبيوتر أو إساءة إستخدامها من خلال الحصول على معرفة مستخدم وكلمة المرور أو الرمز المميز لكلمة المرور " [2].

وهنا يتمتع المجرم المعلوماتي بصفات ومزايا بفضلها يستطيع القيام بالدخول للأنظمة وتفحصها وهذا ما يسهل عليه ويساعده على إرتكاب مثل هذه الجرائم.

المطلب الثاني: دوافع الإجرام المعلوماتي:

إنّ لكل جريمة سبباً ودافعاً يؤدي إلى وقوعها والجريمة السيبرانية أحد هذه الجرائم وكما سبق وتحدثنا عن المجرم المعلوماتي وأهم صفاته التي تميزه، يجب علينا أن نتطرق إلى الدوافع التي من خلالها تقع الجريمة السيبرانية، والملاحظ أن الدوافع عامةً هي نفسها لأن الجرائم مهما إختلفت تبقى شيئاً مخالفاً للقانون ويجب مكافحتها، ومن أبرز هذه الدوافع:

[1] نهلا عبد القادر المومني، المرجع السابق، ص 79.

[2] كوثر مازوني، المرجع السابق، ص 135.

الفرع الأول: تحقيق الربح المادي:

يعتبر المال شيئاً ضرورياً في حياة الفرد لأن به تتحقق الرفاهية التي يسعى لها الجميع لذلك يعد تحقيق الأرباح المادية من أقوى الدوافع التي تؤدي إلى حدوث الجريمة السيبرانية.

" فحب الفرد للمال هو عصب الحياة يدفعه للقرصنة أو السرقة أو الإختلاس عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع الغير المكلف" [1].

نستخلص من هنا أنه ومن أجل الربح السريع يلجأ مجرمو المعلومات إلى إيجاد طرق ووسائل للوصول إلى غايتهم لأنهم وفي وقت وجيز قد يكسبون أموالاً طائلة تضمن لهم العيش الكريم وهذا ما يسعون إليه حتى وإن كانت طرقهم خارقة للقانون.

الفرع الثاني: الأحقاد الشخصية والرغبة في الإنتقام:

إن المشاعر الكامنة عند الإنسان قد تولد عنده الرغبة في الإنتقام وهذا ما يدفع به لإرتكاب الجريمة بغرض إطفاء حقده وغضبه المتسبب من قبل شخص أو مؤسسة أو غيرها.

لذا نرى أن مجرمي المعلومات إنقسموا "إلى قسمين أولهم المجرمين الذين يعملون في المؤسسة فيعمدون إلى إختراق أنظمتها الإلكترونية إمّا بسبب سوء التعامل معهم أو بسبب قلة أجورهم أو رواتبهم وماشابه وثانيهم أولئك الذين يكونون خارج المؤسسة كأولئك الموظفين المطرودين من عملهم والذين يعمدون إلى الإساءة إلكترونياً إلى المؤسسات التي إستغنت عن خدمتهم"[2].

إنّ الباعث على إرتكاب الجريمة السيبرانية شخص يرغب بالإنتقام من مؤسسة أساءة إليه أو شخص طرده من مهنته أو قلل إحترامه وبذلك تنعدم الثقة لديه، فيذهب إلى الفضاء الإلكتروني ويرتكب جريمته الشنيعة لإسكات غضبه خاصة إذا كان ملماً بأسرار هذه المؤسسة وبذلك فهو يشكل خطراً عليه.

---

[1] نسرين عبد الحميد نبيه، المرجع السابق، ص 44.

[2] عمار عباس الحسيني، المرجع السابق، ص 65.

الفرع الثالث: دوافع سياسية وأيديولوجية:

تعد شبكة الأنترنت من الشبكات العالمية التي تضم جميع مجالات الحياة سواء إجتماعية أو سياسية أو ثقافية وغيرها وكما يوجد بها مواقع فعالة تخدم المجتمع، بها أيضاً مواقع غير مرغوب بها ففي بعض الأحيان نرى أن بعض المواقع تضرب مصالح دول أخرى.

" حيث تعد الدوافع السياسية من أبرز المحاولات الدولية لإختراق شبكات حكومية في مختلف دول العالم، كما أنّ الأفراد قد يتمكنون من إختراق الأجهزة الأمنية الحكومية، كذلك أصبحت شبكة الأنترنت مجالاً خصباً لنشر أفكار العديد من الأفراد والمجموعات، ووسيلة للترويج لأخبار وأمور أخرى قد تحمل في طياتها مساساً بأمن الدولة أو بنظام الحكم أو قدحاً في رموز دولية أو سياسية والإساءة لها بالذم"[1].

إن الإختلاف السياسي بين الدول جعل من الأشخاص يرتكبون الجرائم السيبرانية التي تتمثل في الجوسسة عبر الأنترنت وهذه الأخيرة أصبحت من أبرز الطرق المخابرتية التي تستخدمها الحكومات ضد الدول المعادية لها.

الفرع الرابع: المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذّات:

" على صعيد آخر قد يكون الدافع وراء إرتكاب الجرائم المعلوماتية هو الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة"[2].

هناك بعض المجرمين الذين يملؤون أوقات فراغهم بإستخدام الحاسوب والأنترنت وبالتالي ينجرون إلى تحدي أنفسهم بإختراق الأنظمة أو تحدي النظام المعلوماتي وهذا للوصول إلى المتعة والشعور بالقوة، وبذ لك تدفعهم هذه القوة إلى إرتكاب الجرائم السيبرانية.

الفرع الخامس: الرغبة في التعلم:

إنّ الإنسان بطبعه يتطلع دائماً إلى إكتشاف الجديد وتعلم كل شيء حتى وإن كان غير مباح والحاسوب والأنترنت من أكثر الأشياء الملمّة بالمعلومات لذلك قد يدفع حب الإطلاع بالإنسان إلى إرتكاب جرائم يعاقب عليها القانون .

---

[1] رضا عسّال وعماد عبد الرزاق، المقال السابق، ص 156.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 92.

" إنّ قراصنة الأنظمة لديهم إهتمام شديد بأجهزة الكمبيوتر وبالتعلم، ويدخل العديد منهم على أنّهم محترفون ويختار بعض القراصنة الأنظمة لتعلم المزيد عن كيفية عملها. ويقول لاندريس أنّ " القراصنة يحبذون البقاء مجهولين ليتمكنوا من الإستمرار في التواجد داخل الأنظمة لأطول وقت ممكن. والكثير منهم يكرس وقته في تعلم كيفية إختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة"[1].

ونستنتج من هنا أنه في بعض الأحيان قد يؤدي الوصول إلى التعلم ومسايرة العصر والرغبة في معرفة أخبار العالم دون قيود وعبر طرق غير شرعية، كل هذا يدفع بالإنسان للوقوع في الخطأ وبذلك يسمى مجرماً معلوماتياً.

[1]غنية باطلي، المرجع السابق، ص 26.

ملخص الفصل الأول:

لقد مر كل من الحاسوب والأنترنت والجريمة السيبرانية بعدت مراحل إلى أن وصلوا على ماهم عليه اليوم وكل هذا نتيجة التطور التكنولوجي المتقدم يوماً بعد يوم، ففي القديم كان إستخدامهم صعباً عكس ما هو عليه اليوم إذ أصبحوا في متناول الجميع وهذا ما أدى إلى زيادة الجرائم على الفضاء السيبراني.

والجريمة السيبرانية هي كل فعل إجرامي متعمد يمكن إرتكابها بواسطة نظام حاسوبي وقد أطلق المشرع الجزائري على هذه الجرائم تسمية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم المتصلة بتكنولوجيا الإعلام والإتصال وقد وضع عقوبات صارمة لكل من تعدّى على هذه الأنظمة.

وتتميز هذه الجريمة بأنها عابرة للحدود إذ يمتد نطاق إجرامها إلى أكثر من دولة لذلك يصعب إكتشاف زمن وقوعها وكذلك إثباتها فعادة ما تكتشف عن طريق الصدفة فهي تتسم بأنها جرائم ناعمة وقد يقوم بها أكثر من شخص لذا يصعب على القضاة إيجاد الأدلة الكافية لمقاضاة مرتكبي هذه الجرائم.

أما فيما يتعلق بالمجرم المعلوماتي أو الهاكر كما يطلق عليه فهو الشخص الذي يمتلك القدرة على التعدي على الأنظمة بإستخدام الحاسوب وذلك لتمتعه بالذكاء والمهارة كل هذا لكي يحقق أرباحاً ماديةً أو رغبة في إثبات ذاته أو التعلم فيؤدي به كل هذا إلى إرتكاب أشنع الجرائم كالتزوير المعلوماتي والنصب والإحتيال إلى غير ذلك من أنواع الجرائم.

الفصل الثّاني

مقدمة الفصل الثاني:

سعت الدول بالتعاون فيما بينها من أجل القضاء على الجرائم السيبرانية التي أصبحت من مشكلات العصر الحالي إلى وضع إتفاقيات ومعاهدات من خلال الجهود العربية والدولية إضافة إلى التعاون الأمني الذي بات من الضروري وجوده لمجابهة هذه الظاهرة ومن بين هذه الإتفاقيات إتفاقية بودابست والإتفاقية العربية لمكافحة جرائم تقنيات المعلومات وغيرها...

تعتبر الجزائر من الدول التي تأثرت بهذه الجرائم حيث سعى المشرع الجزائري لإستحداث قوانين ونصوص جديدة تتساير والإعتداءات التي تقع في الفضاء السيبراني من خلال القانون 15/04 والقانون 04/09 كل هذا للتصدي لهذه الظاهرة الخطيرة التي هي في تطور دائم نظراً لإتصالها بالتطور التكنولوجي.

كما حاولت الدول العربية والأجنبية من خلال التعاون والجهود التي بذلوها وضع حد لهذه الجرائم إلاّ أنهم تعرضوا للعديد من الصعوبات من بينها إختلاف النظم الإجرائية القانونية، التجريم المزدوج..... فمن أجل القضاء على هذا الخطر يجب أولاً إيجاد حلول لهذه الصعوبات مثل إبرام إتفاقيات دولية وتسهيل الإتصال بين الدول إضافة إلى المساعدات القضائية كل هذا لمواجهة الجرائم السيبرانية.

وفي هذا الفصل تطرقنا إلى "الآليات والجهود الدولية لمكافحة الجرائم السيبرانية وإشكالاته وسبل التغلب عليها وقد تم تقسيمه مما يلي تناولنا في المبحث الأوّل آليات التعاون الدولي لمكافحة الجرائم السيبرانية الذي يندرج فيه المطلب الأوّل بعنوان الإتفاقيات والمعاهدات الدولية في مواجهة الجرائم السيبرانية، والمطلب الثاني الذي تضمن الآليات الأمنية والقضائية لمواجهة الجرائم السيبرانية، أمّا في المبحث الثاني تطرقنا إلى آليات التعاون العربي لمكافحة الجرائم السيبرانية من خلال المطلب الأوّل المتمثل في الجهود العربية لمكافحة الجرائم السيبرانية، والمطلب الثاني المتمثل في سياسة المشرع الجزائري لمكافحة الجرائم السيبرانية، أمّا فيما يخص المبحث الثالث تحدثنا عن الصعوبات التي تواجه الجهود الدولية لمكافحة الجرائم السيبرانية وسبل التغلب عليها حيث تناولنا في المطلب الأوّل الإشكالات التي تواجه الجهود الدولية لمكافحة الجرائم السيبرانية، وفي المطلب الثاني سبل التغلب على الإشكالات التي تواجه الجهود الدولية.

المبحث الأوّل: آليات التعاون الدولي لمكافحة الجرائم السيبرانية:

تعتبر الجرائم السيبرانية من أكثر الجرائم شيوعاً في هذا العصر لإرتباطها بتطور شبكة الأنترنت والتكنولوجيا التي وصلنا لها اليوم ولمكافحة هذه الجرائم لا يكون هناك أي أساس يذكر إلاّ إذا كان هناك تعاوناً دولياً فعالاً وذلك لأن هذه الجرائم تتّسم بأنها عابرة للحدود فهي لا تقع في دولة واحدة بل يمتد ذلك إلى أكثر من دولة لهذا وجب على الدول وضع معاهدات وإتفاقيات والتنسيق فيما بينهم للحد من هده الجرائم وهذا ما يسمى بالتعاون الدولي ومن أبرز هذه المعاهدات التي ساعدت في مكافحة الجرائم السيبرانية إتفاقية بودابست والمعاهدة الأوروبية ...إلخ إضافة إلى الجهود الدولية المتثلة في التعاون الأمني الذي بات من الضروري وجودها للحد من هذه الجرائم وفي هذا المبحث سنتطرق بالتفصيل إلى هذه الإتفاقيات والآليات الأمنية.

المطلب الأول: الإتفاقيات والمعاهدات الدولية في مكافحة الجرائم السيبرانية:

حاولت الدول بالتعاون فيما بينها من أجل القضاء على الجرائم السيبرانية التي أضحت من مشكلات العصر الحالي وضع مجموعة نت المعاهدات والإتفاقيات التي حاولت من خلالها إتخاذ تدابير تشريعية موضوعية وهذا ما جاءت به إتفاقية بودابست ومساعدة الدول بعضها البعض في جمع الأدلة و هذا ما جاءت به المعاهدة الأوروبية أمّا الأمم المتحدة فقد نادت بضرورة العمل المشترك بين الدول وتهتم أيضاّ بحماية حقوق الملكية الفكرية ومن خلال هذا المطلب سنوضح أكثر كل ما جاءت به الإتفاقيات للقضاء على هذه الجرائم التي أصبحت خطيرة جداً.

الفرع الأول: إتفاقية بودابست:

" شهدت العاصمة المجرية بودابست في أواخر عام2001م ميلاد أولى المعاهدات الدولية التي تكافح جرائم الأنترنت Internet Crimes وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات" [1].

" توزعت بنود الإتفاقية، على محاور ثلاثة:

[1] منير محمد الجنبيهى وممدوح محمد الجنبيهى، المرجع السابق، ص 180.

- الإنسجام بين التشريعات الوطنية، التي تجرم الأعمال غير القانونية في الفضاء السيبراني.
- تحديد وسائل التحقيق والملاحقة الجزائية، التي تنسجم مع الطبيعة العالمية للشبكة.
- وضع نظام تعاون بين الدول، يتصف بالسرعة والفعالية"[1].

إتفاقية بودابست من أوّل الإتفاقيات الدولية التي جاءت للقضاء على الجرائم السيبرانية لأنّ هذه الجرائم من أصعب وأخطر الجرائم التي تمس بالأشخاص وممتلكاتهم حيث قامت هذه الإتفاقية على توحيد التشريعات الوطنية وعملت على وضع أنظمة تعاون بين الدول تتناسب مع سرعة الأنترنت.

" وزعت الإتفاقية الجرائم التي ترتكب بواسطة الأنترنت، على أربع مجموعات كبرى، تضم الأولى: الجرائم التي تتعرض لخصوصية وسلامة وتوفر الأنظمة والبيانات؛ مثل النفاذ غير الشرعي، والإعتراض غير الشرعي وتشويه البيانات، وسلامة النظام. وتضم المجوعة الثانية: جرائم التزوير والإحتيال، بينما تندرج في الثالثة، الجرائم المتصلة بالمحتوى، مثل: إنتاج، وتوزيع، وحيازة مواد إباحية يستخدم فيها الأطفال، وفي المجكوعة الرابعة، جرائم الإعتداء على الملكية الفكرية، والحقوق المجاورة"[2].

تنوعت الجرائم المرتبطة بشبكة الأنترنت حيث عملت الإتفاقية على توزيع هذه الجرائم وتقسيمها إلى أربع مجموعات كل مجموعة تضم الجرائم المتشابهة كالتزوير والإحتيال مثلاً وضعتها في مجموعة واحدة وننس الشيء بالنسبة للمجموعات الأخرى.

" أكدت الإتفاقية على الحاجة إلى إتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء لمكافحة الجريمة المعلوماتية، وإعتبرت مرجعاً لا يستهان به في ميدان محاربة الإجرام السيبراني، سواء بالنسبة لبعض الإتفاقيات اللاحقة ذات الصلة أو بالنسبة للتشريعات الداخلية لبعض الدول"[3].

نستنتج من هنا أنّ إتفاقية بودابست عملت على إتخاذ تدابير تشريعية لمكافحة الجرائم التي تقع على الحاسوب ومدى خطورتها على العالم وتضمنت أيضاً الكثير من التوصيات للدول الأعضاء وتعد هذه

---

[1] منى الأشقر جبور، "**السيبرانية هاجس العصر**"، (د،ط)، المركز العربي للبحوث القانونية، بيروت، لبنان، 2017م، ص 105.

[2] المرجع نفسه، الصفحة نفسها.

[3] آسيا العمراني، المقال السابق، ص 77.

الإتفاقية مرجعاً أساسياً لأنّها جاءت لمكافحة ومحاربة الجرائم السيبرانية بكل أنواعها.

وترتكز أهمية هذه الإتفاقية بفعاليتها على إقرار إجراءات عملية، تلتزم الدول المنظمة بإدراجها في قوانينها الوطنية، فقد لاحظت المعاهدة في المادة 23،

"المادة 23 – المبادئ العامة المتعلقة بالتعاون الدولي

يتعاون الطرفان، وفقًا لأحكام هذا الفصل، ومن خلال تطبيق الصكوك الدولية ذات الصلة بالتعاون الدولي في المسائل الجنائية، والترتيبات المتفق عليها على أساس تشريعات موحدة أو متبادلة، والقوانين المحلية، إلى أقصى حد ممكن لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة وبيانات الحاسوب، أو لجمع الأدلة في شكل إلكتروني عن جريمة جنائية."[1].

نلاحظ هنا أنّ الإجراءات التي أقرتها هذه الإتفاقية ألزمت الدول الأطراف بإدراجها في قوانينها الوطنية ونادت إلى التعاون بين الدول كتبادل الأدلة والمعلومات، تسليم المجرمين ... إلى غير ذلك من أشكال التعاون.

تتميز هذه الإتفاقية " بالمتابعة التي تحظى بها، من قبل المجلس الأوروبي الذي يعقد إجتماعات وندوات بشكل مستمر، سواء بتعديلها، بما يتلائم أكثر مع واقع الجريمة السيبرانية /.../ حيث ركزت على: التعاون بين السلطات القضائية ومزودي الخدمات، ومتابعة آثار عمليات تبييض الأموال على الأنترنت،/.../ وقد أوردت هذه المعاهدة بنوداً خاصةً لحماية الحريات والحقوق، وسمحت بوصول المحققين إلى المعلومات المتاحة للعموم، أو بموافقة وإرادة الطرف المعني، بالحفاظ على البيانات"[2].

نرى أنّ إتفاقية بودابست تحظى بالمراقبة الدائمة من قبل المجلس الأوروبي وهذا نظراً للتطور التكنولوجي السريع لذلك وجب مواكبته ومواكبة الجرائم التي يصاحبها يوماً بعد يوم، حيث أكدت على ضرورة التعاون بين السلطات القضائية ومتابعة الجرائم التي تقوم على شبكة الأنترنت، كما تصّت أيضاً على حماية الحريات والحقوق.

---

[1] إتفاقية بودابيست لمكافحة الجرائم المعلوماتية، المجلس الأوربيي ببودابيست، رقم 185، بتاريخ 21 نوفمبر 2001م.
. CONVENTION ON CYBERCRIME, Budapest,2001, European Treaty Series No. 185,p 14.

[2] منى الأشقر جبور، المرجع السابق، ص ـ ص : 105 ـ 106.

وفي الأخير نستنتج أنّ إتفاقية بودابست من أوّل الإتفاقيات التي سعت جاهدة في محاربة الجرائم السيبرانية ودعت إلى التعاون الدولي خاصة بين محموعة من الدول كالولايات المتحدة، كندا جنوب إفريقيا، واليابان... كل هذه الدول تعمل على الحد من هذه الجرائم التي أصبحت تشكل خطورة عليهم.

الفرع الثاني: الجهود المبذولة على مستوى هيئة الأمم المتحدة:

تسعى هيئة الأمم المتحدة جاهدة لمكافحة الجرائم التي تقع على الحاسوب وتعمل على تعزيز التعاون بين الدول " حيث بذلت الأمم المتحدة جهوداً كبيرةً في سبيل العمل على مكافحة الإجرام السيبراني، وذلك لما تسببه هذه الجرائم من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء، وإيماناً منها بأنّ منع هذه الجرائم ومكافحتها يتطلبان إستجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة إستخدام الكمبيوتر والجرائم المتعلقة به"[1].

ومن بين المؤتمرات التي تحت إشراف الأمم المتحدة " حضيت جرائم الحاسب الآلي بإهتمام وفير من خلال مؤتمرات الأمم المتحدة لمنع الجريمة ومعاملة المجرمين (United Nation Congress On The Rrevention Of Crime And The Treatment Of The Offenders)"[2].

تعد منظمة الأمم المتحدة من أهم المنظمات التي تسعى إلى تحقيق العدالة دولياً لذلك وضعت مؤتمر لمنع الجريمة ومعاملة المجرمين وذلك من أجل الحد من الجرائم السيبرانية.

" إنّ مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تم إنعقاده في مدينة ميلانو بإيطاليا في عام 1985، إنبثقت عنه مجموعة من القواعد التوجيهية والتي إكتملت صياغتها في الإجتماعات الإقليمية التحضيرية للمؤتمر الثامن الذي أجاز هذه المبادئ والذي عقد في هافانا بكوبا في 1990 /.../ أكد المؤتمر على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان لصالح الجمهور وبالتالي لمنع الجريمة على نحو فعّال"[3].

---

[1] مراد مشوش، " **الجهود الدولية لمكافحة الإجرام السيبراني**"، مجلة الواحات للبحوث والدراسات، المجلد12، العدد2، الجزائر، 2019م، ص 706.

[2] محمود أحمد عبابنة، "**جرائم الحاسوب وأبعادها الدولية**"، ط1، دار الثقافة، عمان، الأردن، 2009م، ص 155.

[3] المرجع نفسه، ص ـ ص : 156 ـ 157.

تقوم هيئة الأمم المتحدة بعقد مؤتمر بشكل دائم حرصاً على الإلمام بالقوانين والقواعد التي تحد من الجرائم ومن بين هذه المؤتمرات المؤتمر الثامن المنعقد بهافانا الذي ناد بضرورة تطبيق التطورات الجديدة لمنع وقوع الجرائم.

ويمكن إجمال توصيات مؤتمر هافانا 1990م في المبادئ التالية:

"1. تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسساتية.

2. تحسين أمن الحاسب الآلي والتدابير المعنية.

3. إعتماد إجراءات تدريب كافية للموظفين والوكالات المسؤولة عن منع الجريمة الإقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والإدعاء فيها.

4. تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الإتصالات والمعلومات.

5. إعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم.

6. زيادة التعاون الدولي من أجل مكافحة هذه الجرائم "[1].

نصّ المؤتمر على مجموعة من المبادئ التي تمثلت في تجديد القوانين الجنائية الوطنية، إيجاد أشخاص مختصين في أمن الكمبيوتر وذلك من أجل زيادة التدابير الوقائية إضافة إلى تلقين آداب الحاسب وتقديمه كجزء من مقررات الإتصال، إضافة إلى النداء لضرورة التعاون الدولي من أجل مجابهة الجرائم السيبرانية.

" لكن تزايد الجريمة السيبرانية وما تثيره من مشاكل أدّى بمنظمة الأمم المتحدة إلى عقد الإتفاقية الخاصة بمكافحة إساءة إستعمال التكنولوجيا لأغراض إجرامية /.../ أين أكّدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول /.../ تبقى منظمة الأمم المتحدة الإطار الأمثل لمكافحة الإجرام السيبراني حيث وضعت مجموعة من القواعد الموضوعية والإجرائية لمواجهة هذه النوعية من الجرائم" [2].

[1] علي جبار الحسيناوي، "**جرائم الحاسوب والأنترنت**"، الطبعة العربية، دار اليازوري العلمية، عمان، الأردن، 2009م، ص 148.

[2] مراد مشوش، المقال السابق، ص 77.

"وأجرت الأمم المتحدة في عام 2024 إتفاقية جديدة من أجل مكافحة الجرائم الإلكترونية. ويمثل هذا الصك الجديد أداة ناجعة من أجل مساعدة الدول في مكافحة الجرائم الإلكترونية، عبر تعزيز آلياتها التشريعية الوطنية والتعاون الدولي" [1]

نظراً لتطور الجرائم السيبرانية لم يعد المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين كافياً للحد من أخطارها لذلك عقدت منظمة الأمم المتحدة الإتفاقية الخاصة لمكافحة إساءة إستخدام التكنولوجيا لأغراض إجرامية والعديد من المؤتمرات أيضاً كل هذه المحاولات لوضع حد لهذه الجرائم لذلك سعت منظمة الأمم المتحدة لسن قوانين وقواعد إجرائية وموضوعية لمكافحة هذه الجرائم التي أصبحت هاجساً لهذا العصر.

الفرع الثالث: المعاهدة الأوروبية لمكافحة الجرائم السيبرانية:

" نظراً للتطور السريع في مجال تكنولوجيا الكمبيوتر والأنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية في هذا المجال، فقد أصدر المجلس الأوروبي التوصية رقم 13/95 في 11 سبتمبر 1995 في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات لحث الدول الأعضاء بمراجعة قوانين الإجراءات الجنائية الوطنية لتلاؤم التطور في هذا المجال "[2].

عملت الدول الأوروبية على وضع توصيات لمجابهة جرائم الأنترنت حيث تمثلت هذه التوصيات في:

"ـ وضع التشريعات الملائمة وتعزيز التعاون الدولي سيما مع تزايد الجرائم المرتبطة بالتقنية من جرائم شبكات الحاسب الآلي.

ـ يتوجب إضافة نصوص قانونية خاصة بالإعتراض غير الشرعي /.../ وأخرى خاصة بإتلاف المعطيات وإتلاف الأنظمة ووجوب تبني نصوص تجرم التعطيل البالغ لوظائف الحاسب الآلي"[3].

---

[1] **أنشطة فرنسا في مجال مكافحة الجرائم الإلكترونية (9 كانون الثاني/ يناير 2025)**، تاريخ الإطلاع: 2025/05/24م، على الساعة: 9:51.

https//: www.diplomatie.gouv.fr

[2] محمد أحمد سليمان عيسى، "**التعاون الدولي لمواجهة الجرائم الإلكترونية**"، المجلة الأكاديمية للبحث القانوني، المجلد14، العدد2، المملكة العربية السعودية، 2016م، ص 58.

[3] محمد أحمد عبابنة، المرجع السابق، ص ـ ص: 165 ـ 166.

ناد المجلس الأوروبي بضرورة التعاون الدولي لمحاربة الجرائم السيبرانية والتي باتت من أصعب الجرائم لأنّها تستدعي جهوداً مكثفة للوصول إلى من قام بها لذلك عملت الدول الأوروبية على إتخاذ التدابير اللازمة لردع هذه الظاهرة حيث قامت بإضافة نصوص قانونية تمس كل أنواع الجرائم السيبرانية، كما نصت أيضاً على:

"أ ـ توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

ب ـ توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونياً.

ج ـ جمع معلومات عن حركة البيانات وعن إمكان وجود تدخل في محتواها.

د ـ تتضمن الإتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية"[1].

وهنا عملت على وضع قوانين موحدة تتلاؤم وتساير الأحكام المتعلقة بالجرائم السيبرانية إضافة إلى التعاون بين الدول في جمع المعلومات والأدلة التي تسهل عملية التحقيق وإجراءات التحري لإكتشاف الفاعلين وتوقيع العقاب عليهم، ويعد المجلس الأوروبي مثله مثل جميع الإتفاقيات التي تضمنت المبادئ العامة للتعاون الدولي المتمثلة في: تسليم المجرمين وتبادل المساعدات الدولية لأنّ الجرائم ترتكب في العديد من الدول.

" وتعد هذه الإتفاقية وإن كانت مسودة أو مشروعاً بمثابة القانون بين الدول الأعضاء والتي وبموجبها تلتزم الدول الأعضاء في المجلس والموقعون على هذه المسودة بضرورة العمل على تنفيذ أحكامها والخضوع لها وإحترام تنفيذها وتطويع النصوص القانونية بالشكل الذي يضمن عدم التعارض مع أحكامها"[2].

المعاهدة الأوروبية كغيرها من المعاهدات التي حاولت القضاء على الجرائم السيبرانية من خلال فرضها لعدة قوانين وإجراءات لذلك على الدول الأعضاء إحترام هذه القوانين والتعاون دولياً فيما بينهم من خلال تطبيق هذه القوانين وعدم التعارض عليها خاصة أنّ الأنترنت التي تعتبر هي الوسيلة لقيام هذه

[1] فاروق خلف، "**الآليات القانونية لمكافحة الجريمة المعلوماتية**"، مجلة الحقوق والحريات، العدد2، الجزائر، 2015م، ص 13.

[2] محمود أحمد عبابنة، المرجع السابق، ص 169.

الجرائم إضافة إلى جهاز الحاسوب اللذان هما في تطور ملحوظ، سعت الإتفاقيات جاهدة للوصول إلى هذا التطور ومواكبته من أجل القضاء بشكل كلي على هذه الجرائم التي أصبحت تهدد حياة الأفراد إضافة إلى التعدي على ممتلكاتهم.

المطلب الثاني: الآليات الأمنية والقضائية في مواجهة الجرائم السيبرانية:

تطرقنا من خلال المطلب الأوّل إلى أهم الأتفاقيات التي حاولت جاهدة بالإلمام بكل الوسائل والطرق من أجل مكافحة الجرائم السيبرانية من خلال وضع قوانين وإجراءات جزائية وموضوعية للحد من هذه الجرائم إلاّ أنّ كل هذه الجهود لت تعد كافية لوحدها لمجابهة هذا الخطر الأمر الذي إستدعى إلى إنشاء مؤسسات وأجهزة تعاون دولية أمنية تتضامن من خلالها أجهزة الشرطة في مختلف الدول من أجل تبادل المعومات وتسليم المجرمين ..إلى غير ذلك من أساليب التعاون، وفي هذا المطلب سنلم بكل هذه الأشكال التعاونية التي هدفها القضاء على الجرائم السيبرانية.

الفرع الأوّل: جهود المنظمة الدولية للشرطة الجنائية (الأنتربول):

"المنظمة الدولية للشرطة الجنائية (أنتربول) هي منظمة حكومية دولية خاضعة للقانون الدولي ولديها هدفان هما ربط أجهزة الشرطة ومنع ومحاربة الجريمة وتعد أكبر منظمة دولية في العالم حيث تضم 195 من البدان الأعضاء" [1]

" تهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعّال في مكافحة الجريمة /.../ أمّا في مجال الجرائم المعلوماتية، فقد أنشأت المنظمة الدولية للشرطة الجنائية " الأنتربول" خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) بوضع إستراتيجيات لمواجهة هذا النوع من الجرائم"[2].

[1] **الإدارة العامة للشرطة الدولية**، تاريخ الإطلاع 2025/04/10م، على الساعة: 21:36.
https://www.moi.gov.sa

[2] الطاهر ياكر، "**مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والإتفاقيات الدولية**"، مجلة الصدى لدراسات القانونية والسياسية، المجلد4، العدد4، الجزائر، 2022م، ص ـ ص: 15 ـ 16.

نستنتج من هنا أنّ المنظمة جاءت من أجل تعزيز التعاون الدولي من خلال التنسيق بين أجهزة الشرطة للدول الأطراف عن طريق المساعدات المتبادلة بينهم مثل تجميع المعلومات من أجل تسهيل طرق التحقيق والمحاكمة، وفي عام 2004م خصص الأنتربول فرع خاص لمكافحة جرائم التكنولوجيا وإستعانت على ذلك بمجموعة الدول الثمانية الكبرى فوضعت إستراتيجيات للحد من هذه الجرائم وتمثلت هذه الإستراتيجيات في:

"ـ إنشاء مركز إتصالات أمني عبر الشبكة يعمل على مدار (24) ساعة و(7) أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف.

ـ إستخدام وسائل حديثة في تلك المكافحة، كإستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف والتي تستخدم برنامج EXCALIBUR للتحليل والمقارنة الأوتوماتيكية لتلك الصور.

ـ تزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها" [1].

سعت المنظمة لتحديد مجموعة من الإستراتيجيات تمثلت في العمل على مدار 24 ساعة من خلال وضع قناة إتصال بين مركز الشرطة في الدول الأعضاء وهذا حرصاً على البقاء متيقظين لأي طارئ قد يحدث لأنّ المجرمين لا يفلتون أي فرصة للقيام بجرائمهم، إضافة إلى ذلك تحديث الوسائل لتسهيل إكتشاف هذه الجرائم والعمل على تدريب أعوان الشرطة وتجهيزهم لأي خطر قد يأتيهم من خلال إعطائهم كتب مفصلة تتحدث عن الجرائم السيبرانية بكل أنواعها وكيفية التصدّي لها.

حيث قامت أيضاً بوضع برنامج يرتكز على التدريب لمكافحة الإجرام المعلوماتي ويعمل على مواكبة التهديدات الناشئة ويهدف هذا البرنامج إلى:

ـ توفير دورات تدريبية لوضع معايير مهنية والتقيد بها.

ـ تعزيز تبادل المعلومات بين البلدات الأعضاء عن طريق الأفرقة العاملة والمؤتمرات الإقليمية.

[1] عادل عبد العال إبراهيم خراشي، " **إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**"، (د،ط)، دار الجامعة الجديدة، القاهرة، مصر، (د،س)، ص 198.

ـ تنسيق العمليات الدولية ودعمها.

ـ إعداد قائمة عالمية بأسماء ضباط الإتصال ووضعها في تصرف المحققين في مجال الإجرام السيبيري على مدار الساعة"[1].

من مميزات هذا البرنامج ضرورة تبادل المعلومات والعمل على تنظيم العمليات بين الدول والتواصل المستمر بين الضباط والمحققين لكشف الحقائق والعمليات الإجرامية.

" وبهذا فإنّ شرطة الأنتربول تعد منظومة عالمية تختص بمكافحة الجرائم الدولية والعابرة للحدود الوطنية للدول، بما فيها الجرائم المعلوماتية /.../ حيث دعى الأمين العام للأنتربول السيد " بونالد نوبل" جميع الحكومات والدول لدعم وتطوير نظم تبادل المعلومات /.../ وقد نجحت المنظمة الدولية للشرطة الجنائية خلال الأعوام الأخيرة في جعل إسمها من أكثر الأسماء التي يخشاها المجرمون"[2].

وفي الأخير نرى أنّ الدول كافة تسعى عن طريق التعاون فيما بينها من خلال الإتفاقيات والمنظمات الأمنية إلى إيجاد حل يتوافق مع كل الدول لمجابهة هذا الخطر ألا وهو الجرائم السيبرانية.

الفرع الثاني: تسليم المجرمين:

إنّ تسليم المجرمين يعد من دروب التعاون الدولي في مجال مكافحة الإجرام لذلك " يجب على الدول أن تتعاون بعضها مع البعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي"[3].

عُرّف تسليم المجرمين بأنّه " عبارة عن إجراء وصورة من صور التعاون الدولي بحيث تقوم الدولة المطلوب منها التسليم بتسليم شخص يوجد داخل إقليمها إلى دولة أخرى أو تقديمه إلى جهة قضائية دولية بهدف ملاحقته عن جريمة إتُّهم برتكابها أو لأجل تنفيد حكم جنائي صادر ضدّه" [4].

---

[1] مراد مشوش، المقال السابق، ص 711.

[2] عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 199.

[3] عبد العال الديربي ومحمد صادق إسماعيل، "**الجرائم الإلكترونية دراسة قانونية قضائية مقارنة** "، ط1، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012م، ص 349.

[4] خرشي عثمان، "**تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية**"، مجلة البحوث القانونية والسياسية، العدد10، الجزائر، 2018م، ص 929.

يقصد هنا أنّ تسليم المجرمين إجراء تقوم به الدول فيما بينها لتحقيق العدالة ذلك أنّ هؤلاء المجرمين قد قاموا بارتكاب جرائم سيبرانية في غير دولتهم فتقوم الدولى التي ينتمي إليها المجرم بالتفاوض مع دولة أخرى وتطلب منها تسليم ذلك الشخص من أجل معاقبته والغرض هنا من تسليم هذا المجرم هو عدم إفلات المتهم من العقاب.

" شروط التسليم: أهمية شروط التسليم تكمن في كونها تفصل حدود العلاقة بين الدول الأطراف في عملية التسليم، وتضع الأحكام العامة التي على أساسها سيتم التسليم من عدمه /.../ التجريم المزدوج: ويقصد به أن يكون الفعل المطلوب التسليم من أجله مجرّماً في تشريع الدولة طالبة التسليم، وكذلك في تشريع الدولة المطلوب إليها التسليم/.../ ويشترط في جميع الأحوال أن تكون الجريمة المطلوب من أجلها التسليم جناية أو جنحة معاقباً عليها بالسجن مدة لا تقل عن سنة" [1].

من أهم شروط تسليم المجرمين التجريم المزدوج والذي يجب أن يكون الفعل المعاقب عليه مجرّم في كلتا الدولتين وأساسه يكون في الدولة التي تطلب التسليم من أجل المحاكمة وتوقيع العقاب على ذلك المجرم، أمّا بالنسبة لدرجة جسامة الجريمة فيقصد به أنّ الدول أثناء سنّها للقوانين تحدّد الحد الأدنى للعقوبة المقررة للجرائم التي يتم التسليم لأجلها، ومن بين الشروط المتعلقة بالأشخاص المطلوب تسليمهم:

" أ ـ عدم جواز تسليم الرعايا، حيث من المبادئ السائدة والمستقر عليها في المجتمع الدولي والتي نصّت عليها معظم التشريعات الوطنية والإتفاقيات الدولية /.../ أيّاً كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولهم.

ب ـ عدم جواز ممنوحي حق اللجوء السياسي، فمن المبادئ السائدة في أغلب التشريعات /.../ المتعلقة بتسليم المجرمين عدم جواز تسليم ممنوحي حق اللجوء السياسي"[2] .

نلاحظ هنا في أغلب الإتفاقيات ومعظم التشريعات أنّه لا يسمح بتسليم المجرمين أيّاً كان نوع الجريمة بالنسبة للرعايا وممنوحي حق اللجوء السياسي.

[1] أمير فرج يوسف، المرجع السابق، ص/ص: 452 / 453.

[2] عادل عبد العال إبراهيم خراشي، المرجع السابق، ص ـ ص: 122 ـ 123.

وهناك نوع آخر والمتمثل في " عدم جواز تسليم من تمّت محاكمتهم عن ذات الجريمة المطلوب التسليم من أجلها/.../ فطالما أنّ الشخص سبق له أن حوكم عن الجريمة المطلوب التسليم من أجلها وبرّء منها أو عوقب عليها فلا يجوز تسليمه، بل لا يجوز أيضاً التسليم عن الجريمة المنظورة أمام القضاء الوطني ولم يصدر فيها حكم بعد"[1].

وهنا نرى أنّه لايسمح أيضاً تسليم من تم محاكمته عن جريمة سواء وقع عليه العقاب أة برّء منها وأيضاً من تكون جريمته قدمت أمام القضاء حتى ولم يصدر الحكم فيها، كل هذه الشروط لا يجوز فيها التسليم.

الفرع الثالث: المساعدة القضائية الدولية:

" تعرف المساعدة القضائية الدولية بأنّها " كل إجراء قضائي تقوم به دولة من شأنها تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم. وتتعلق المساعدة القضائية بالمعاونة في مكافحة الجرائم في المجال الجنائي من خلال الإتفاقيات"[2].

" كما تعرف أيضاً بأنها "تقديم الدول الأطراف المساعدة القانونية في التحقيق والملاحقة والإجراءات القضائية المتعلقة بأي جريمة من الجرائم المشمولة بالإتفاقيات الدولية بالطرق التي تطلبها بشأن جريمة من تلك الجرائم التي قامت بها جماعة إجرامية منظمة" [3]

تعمل المساعدة القضائية على تسهيل مهام المحاكمة بين الدول وأهميتها تكمن في القضاء على الجرائم بواسطة المعاهدات والإتفاقيات وتتخذ المساعدة القضائية صوراً عدة منها:

" تبادل المعلومات ويتم بواسطة تبادل البيانات والوثائق والمواد الإستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الإتهامات التي وُجّهت إلى رعاياها في الخارج والإجراءات التي إتّخذت ضدّهم، وقد يشمل التبادل السوابق القضائية للجناة"[4].

---

[1] ، عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 123.

[2] المرجع نفسه، ص 202.

[3] طارق أحمد مسعود، " **دور التعاون الدولي في مكافحة الجرائم الإلكترونية**"، (رسالة ماجستير)، جامعة أبوظبي ـ كلية القانون ـ ، الإمارات، 2022/2021م، ص91.

[4] محمد أحمد سليمان عيسى، المقال السابق، ص 55.

والملاحظ هنا أنّ تبادل المعلومات يكون في صالح الدولة التي تقوم بالمحاكمة لإثبات أو نفي جريمة عن شخص إستناداً على البيانات والأدلة الموجودة وأيضاً السوابق لهذا الشخص.

" نقل الإجراءات وهو يقضي بقيام دولة ما بمقتضى إتفاقية أو معاهدة بإتخاذ إجراءات جنائية وهي بصدد التحقيق في جريمة معلوماتية إرتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من الشروط"[1].

إنّ نقل الإجراءات يتمثل في إتخاذ إجراءات من أجل التحقيق في واقعة جرمية وقعت في إقليم دولة أخرى ولمصلحة الدولة المطالبة بنقل هذه الإجراءات وفق شروط معينة أهمها:

" ـ أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والمطلوب منها.

ـ أن تكون الإجراءات المطلوب إتخاذها مقررة في قانون الدولة المطلوب منها عن ذات الجريمة.

ـ أن يكون الإجراء المطلوب إتخاذه يؤدي إلى الوصول إلى الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب منها[2].

من أجل نقل الإجراءات من دولة إلى دولة يجب توفر شروط وهي أن يكون الجرم الذي قام به الشخص مجرما في تشريع كلا الدولتين، ضرورة وجود الإجراءات المطلوبة في تشريع الدولة التي تطالب بهذه المعلومات، وأن يكون الهدف من هذه الإجراءات يسعى إلى تحقيق العدالة والوصول إلى الحقائق .

" الإنابة القضائية ويقصد بها إتخاذ إجراء قضائي من إجراءات الدعوة الجنائية لأثره المباشر من أجل الفصل في مسألة معروضة على السلطة القضائية تعذر على الدولة التي تقدمت بطلب الإنابة القيام به بنفسها وتهدف الإنابة القضائية إلى تسهيل الإجراءات الجنائية بين الدول بما يضمن إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة"[3].

---

[1] شوارب جيلاني ومراد فايزة، "**الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية**"، مجلة الدراسات القانونية والسياسية، المجلد9، العدد2، الجزائر، 2023م، ص 165.

[2] عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 207.

[3] قزران مصطفى وزرقين عبد القادر، "**الآليات الدولية لمكافحة الجريمة الإلكترونية**"، مجلة صوت القانون، المجلد8، العدد2، الجزائر، 2022م ، ص 1228.

نرى هنا أنّ الإنابة القضائية عبارة عن إتخاذ إجراء قضائي تتقدم به الدولة الطالبة إلى الدولة المطلوب منها من أجل وضع حل للقضية المعروضة أمام السلطة القضائية فمن مميزاتها أنّها تعمل على تسهيل الإجراءات بين الدول حيث أنّ هذا الإجراء يتسم بالبطئ وهذا ما أدى بالدول تعيين سلطة مركزية تستقبل الطلبات مباشرة وهذا من أجل تسريع وصول الإجراءات لإتخاذ القرارات تجاه القضايا المعروضة أمام القضاء.

المبحث الثاني: آليات التعاون العربي لمكافحة الجرائم السيبرانية:

هناك جهود دولية أخرى مبذولة على مستوى وطننا العربي حيث حاولوا وضع إتفاقيات وإجراءات ومن بين هذه الإتفاقيات الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذلك سعت المملكة العربية السعودية وكذلك الإمارات من خلال الجهود التي بذلوها للحد من هذا الخطر، وسنتطرق أيضاً في هذا المبحث على موقف المشرع الجزائري من الجرائم المعلوماتية حيث حاول إنشاء عدة نصوص وأطر تنظيمية لمواجهة الجرائم السيبرانية وإستحداثها بما يتلائم والتطور التكنولوجي الذي وصلنا له اليوم.

المطلب الأوّل: الجهود العربية في مكافحة الجرائم السيبرانية:

إنّ الدول العربية حاولت التصدّي للجرائم السيبرانية وعملت على مكافحتها ونظراً لطبيعة وخصائص هذه الجرائم فهي عابرة للحدود فقد سعت الدول العربية ونادت بضرورة التعاون بينها من خلال إبرام إتفاقيات ومعاهدات تهدف إلى توحيد الجهود والتشريعات للحد من هذا الخطر الذي أصبح يهدد البشرية، ومن خلال هذا المطلب سنأتي بذكر الإتفاقية العربية لمكافحة جرائم تقنية المعلومات وإلى جهود بعض الدول العربية

الفرع الأوّل: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات:

قامت جامعة الدول العربية بإصدار قانون يحد من الجرائم السيبرانية من خلال الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، ومن أهداف هذه الإتفاقية ما يلي: " تعزيز التعاون الدولي وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرأ أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها"[1]. أشارت الإتفاقية إلى تعزيز التعاون الدولي من أجل محاربة

[1] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية، العدد58.

هذا الخطر الذي نعيشه اليوم وهذا للحفاظ على إستقرار الدول والمحافظة على أفرادها.

" نصّت الإتفاقية عن بعض الأفعال المجرمة ومن ذلك جريمة الإعتراض غير المشروع والإعتداء على سلامة البيانات، جريمة إساءة إستخدام وسائل تقنية المعلومات، جريمة التزوير، جريمة الإحتيال /.../ الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بإنتهاك حق المؤلف والحقوق المجاورة" [1].

حاولت الإتفاقية الإلمام بمعظم الجرائم التي لها علاقة بشبكة الأنترنت وتجريمها كل هذا لوضع حد لها من خلال إنشاء قولنين وإجراءات متلائمة معها لمحاولت مكافحتها.

ونصّت الإتفاقية "في المادة الحادية والعشرون: تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات:

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال إرتكابها بواسطة تقنية المعلومات "[2].

سعت الإتفاقية مثلها مثل الإتفاقيات التي سبقتها إلى ضرورة تحقيق العدالة عن طريق فرض عقوبات صارمة على مرتكبي هذه الجرائم.

" يرى الدكتور عادل مشموشي بالرغم من الدعوات إلى تطوير التشريعات الوطنية الخاصة بجرائم المعلوماتية الموضوعية والإجرائية بقيت التداخلات غير كافية /.../ لذا ينبغي تغيير جذري في أسلوب التعاطي مع جرائم المعلوماتية عما هو معتمد حيال الجرائم التقليدية، وذلك بإقرار وإبتكار نصوص وإجراءات ملاحقة قادرة على مواكبة التطورات ومستجدات الجرائم المعلوماتية ومكافحتها بكفاءة تقنية عالية"[3].

إنّ طبيعة الأنترنت وتطورها المستمر جعل من الإتفاقيات والمعاهدات غير قادرة على مواكبتها لذلك من رأي الدكتور عادل مشموشي لابد من تغيير جذري لكافة القوانين المتعلقة بالجرائم السيبرانية وليس فقط تعديل هذه القوانين لأنّ مكافحة هذه الجرائم تستلزم تقنيات عالية وإجراءات مسايرة لتطورات الجرائم السيبرانية.

---

[1] حسين طاهري، المرجع السابق، ص ـ ص: 567 ـ 568.

[2] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق.

[3] حسين طاهري، المرجع السابق، ص ـ ص: 568 ـ 569.

الفرع الثاني: جهود دولة الإمارات العربية المتحدة:

" حرصت دولة الإمارات العربية المتحدة ـ منذ نشأتها ـ على التعاون والتنسيق مع المجتمع الدولي ممثلة في منظمة الأمم المتحدة في إرساء وتعزيز مبادئ وقواعد العدالة الجنائية من خلال المشاركة الفعّالة في المؤتمرات والإجتماعات واللقاءات العلمية المعنية بنظم العدالة الجنائية/.../ والأخذ بالمعايير والمواجهات التي إتخذتها الأمم المتحدة لتكون دولة الإمارات العربية المتحدة في مقدمة الدول المنفذة للمعاهدات والمواثيق الدولية" [1]. من بين الدول العربية التي كانت حريصة على مكافحة الجرائم السيبرانية نجد دولة الإمارات العربية المتحدة حيث حاولت من خلال مشاركاتها في الإجتماعات على تعزيز التعاون الدولي.

ومن الأشكال التي قامت بها دولة الإمارات لمحاربة هذا الخطر المستحدث مايلي:

"1 ـ مشاركتها وإحتضانها للمؤتمرات والإجتماعات ذات الصلة بهذه الجرائم، مما عكس ذلك جلياً بتبني جامعة الدول العربية القانون الإتحادي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات كقانون إسترشادي.

2 ـ التركيز على الجانب الوقائي في مكافحة الجريمة وإقرار الأمن والإستقرار والسلامة العامة بين المواطنين والمقيمين على أرض الدولة مع التسلح بالخبرات اللازمة، وإنشاء إدارة الأدلة الإلكترونية ونظام الشرطي الإلكتروني وتدريب الكوادر الفنية للتصدي لهذا النوع من الجرائم عند وقوعها" [2].

عملت دولة الإمارات العربية على إشتراكها الدائم في المؤتمرات وكل ما يخص الجرائم السيبرانية وهذا ما جعل جامعة الدول العربية تتخذ القانون الإتحادي الخاص بها كقانون إسترشادي كل هذا لحرص الإمارات الكبير وسعيها لمجابهة هذه الجرائم، إضافة إلى إهتمامها بالجانب الوقائي حيث عملت على إقرار

---

[1] جمال محمد خلفان محمد النقبي وسلطان محمد سالم عوض هيسان المعصبي، "**التعاون الوطني والدولي في الجرائم الإلكترونية المشكلات والحلول**"، مجلة المعهد العالي للدراسات النوعية، المجلد3، العدد16، 2023م، ص ـ ص: 5488 ـ 5489.

[2] وائل محمد عبد الرحمان نصيرات، "**الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها**"، (د،ط)، دار المنظومة، الرياض، السعودية، 2016م، ص 131.

الأمن من خلال تدعيم مراكز الشرطة وتدريبهم لمواجهة هذه الجرائم بشتى أنواعها كل هذا من أجل توفير الأمن والإستقرار لمواطنيها.

وعملت أيضاً على:

"3 ـ تدريب الشرطة من أجل التعامل مع هذه السلوكيات.

4 ـ كما قامت بدراسات متواصلة فيما يتعلق بالمواقع الإلكترونية /.../ وتجري البحوث اللازمة لمعرفة الثغرات وإغلاقها قبل وصول المحتالين وقراصنة الأنترنت لها، بما يؤدي في النهاية إلى حماية العملاء وضمان المعاملات المصرفية الإلكترونية بصورة آمنة" [1]. حيث قامت أيضاً بدراسة وفهم كل ما يدور حول المواقع الإلكترونية وعملت أيضاً إيجاد الثغرات ومحاولة إغلاقها قبل تفطن مجرمي المعلومات لها، كل هذا من أجل أن تجرى المعاملات الإلكترونية بآلية صادقة تتسم بالأمان.

" إنّ قانون دولة الإمارات العربية المتحدة يمنع نسخ برامج الكمبيوتر بدون إذن وكا من يقبض عليه متلبساً بقرصنة البرامج سيخضع هو وشركته للمحاكمة، بموجب القانون المدني أو الجنائي وتشمل العقوبات حسب قانون الغرامة المالية بالإضافة إلى مصادرة المنتجات والحبس لمدة تصل 3 سنوات" [2].

وضعت دولة الإمارات العربية عقوبات صارمة لمرتكبي هذه الجرائم كما وضعت مبادئ لا يجب على أحد أن يتخطاها كل هذا لمنع وقوع الجرائم السيبرانية.

الفرع الثالث: جهود المملكة العربية السعودية لمكافحة الجرائم السيبرانية:

" أدركت المملكة السعودية العربية خطورة الجرائم السيبرانية على المصالح الوطنية، وعلى القيم والتقاليد والعادات الإسلامية التي تسود في المجتمع السعودي، لذلك سارعت المملكة في إصدار نظاماً خاصاً لمكافحة جرائم تقنية المعلومات حيث وافق مجلس الوزراء على نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (17) لعام 1428هـ" [3].

---

[1] وائل محمد عبد الرحمان نصيرات، المرجع السابق، ص ـ ص: 131 ـ 132.

[2] الطاهر ياكر، المقال السابق، ص 24.

[3] رانا مصباح عبد المحسن عبد الرزاق، "**آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية "دراسة تحليلية""**، المجلة القانونية، (د، س)، ص 1386.

نظراً لخطورة الجرائم السيبرانية ومساسها بالقيم والعادات السائدة في المجتمعات قررت المملكة العربية السعودية وضع نظام يختص بهذه الجرائم وحدها دون سواها وقد نال موافقة من قبل مجلس الوزراء لأن الجميع يسعى لمكافحة هذه الجرائم، ومن أهداف نظام مكافحة جرائم تقنية المعلومات ما يلي:

"- إرساء قواعد نظامية موحدة لإستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بواسطة سجلات إلكترونية يعول عليها إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإلكترونية وسلامتها.

- إزالة العوائق أمام إستخدام التعاملات الإلكترونية " [1].

حيث دعت أهداف هذا النظام إلى العمل على إنشاء قواعد نظامية موحدة لتسهيل معاملاتها في القطا ع العام والخاص ومنح الثقة للمتعاملين عن طريق تسهيل التعاملات والعمل أيضاً على حل الصعوبات التي تواجه المتعاملين الإلكترونيين.

وهناك أهداف أخرى أيضاً تمثلت في:

"- تيسير إستخدام التعاملات والتوقيعات الإلكترونية على الصعيدين المحلي والدولي للإستفادة منها في جميع المجالات، كالإجراءات الحكومية والتجارة والطب والتعليم والدفع المالي الإلكتروني.

- منع إساءة الإستخدام والإحتيال في التعاملات والتوقيعات الإلكترونية"[2].

نستنتج من هنا أنّ المملكة العربية السعودية وضعت جهداً كبيراً للحد من الجرائم السيبرانية من خلال أهداف وضحتها في نظامها حيث حاولت تسهيل التعاملات في جميع المجالات التجارية والتعليمية ... إلخ مع مراعاة سوء الإستخدام لهذه التعاملات ومن يرتكب ذلك سيعاقب بالحبس إضافة إلى غرامة مالية.

سعت الدول العربية جاهدة للقضاء على جرائم العصر التي ارتبطت بالأنترنت ألا وهي الجرائم السيبرانية التي أصبحت خطراً كبيراً يهدد الجميع على المستوى الإقليمي والدولي، فعملت كل من دولة الإمارات والمملكة العربية السعودية على مجابهة هذا الخطر من خلال وضعهم لقوانين وأنظمة كان الهدف

[1] وائل محمد عبد الرحمان نصيرات، المرجع السابق، ص 131.

[2] المرجع نفسه، الصفحة نفسها.

منها وضع مبادئ جديدة تتلائم مع التطور التكنولوجي للحد من هذه الظاهرة، حيث بات من الصعب مواجهة هذا الخطر من قبل دزلة لوحدها هذا ما استدعى إلى التعاون الدولي الذي بفضله يمكن الوصول إلى الحقائق وفرض العقوبات على مرتكبي هذه الجرائم.

الفرع الرابع: جهود المنظمة الدولية للشرطة القضائية (الأفريبول):

" ظهرت فكرة إنشاء أفريبول في المؤتمر الإقليمي الإفريقي الثامن والعشرين في 10 إلى 12 سبيمبر 2013 بوهران والتي شهدت بالإجماع إنضمام قادة الشرطة الأفارقة الواحد والأربعون الحاضرون. ويساهم هذا الهيكل الشرطي الجديد في تعزيز القدرة التحليلية للشرطة الإفريقية على تقييم التهديدات الإجرامية وتطوير الإستجابات الملائمة وتقرير تنسيق قوات الشرطة في سياق عمليات دعم السلام" [1].

" فالأفريبول مؤسسة تقنية شرطية دائمة ذات طابع إقليمي تتمتع بالشخصية القانونية الدولية والأهلية القانونية اللازمة للقيام بمهامها المنوطة بها، تهدف إلى التنسيق والتعاون بين الدول الأعضاء في الإتحاد الإفريقي بغرض مكافحة الجريمة المنظمة العابرة للحدود الوطنية بمختلف صورها وأشكالها" [2].

تعتبر منظمة الشرطة الجنائية الإفريقية من المنظمات التي حاولت الوقوف ضد التهديدات الإجرائية من خلال التنسيق بين قوات الشرطة وتدعيم قدرتها ومحاولة تجديد هياكل الإستجابة لديها، كل هذا لكي يعم السلام داخل الوطن ومن هنا جاءت فكرة الأفريبول التي تتمتع بشخصية قوية قانونية التي تقوم بمهامها على أكمل وجه، حيث تهدف إلى تعزيز التعاون الدولي بين الدول الإفريقية من أجل التصدي للجرائم العابرة للحدود بكل أنواعها.ومن الأهداف التي يسعى الأفريبول في تحقيقها ما يلي:

". العمل على إنشاء أطر ناظمة تضبط التعاون بين مؤسسات شرطة الدول الأعضاء على المستوى الإستراتيجي والعملياتي، قصد الكشف عن الجريمة المنظمة العابرة للحدود الوطنية والتحقيق فيها.

تشجيع المساعدة الفنية بين مؤسسات الشرطة بالدول الأعضاء في مجالات هامة كالتدريب تبادل الخبرات"[3].

---

[1] حسين طاهري، المرجع السابق، ص 556.

[2] فتيحة حيمر ، "**تأثير الجريمة الإلكترونية على الأمن في إفريقيا**"، مجلة أبحاث قانونية وسياسية، المجاد9، العدد1، الجزائر، 2024م، ص ـ ص: 559 ـ 560.

[3] المقال نفسه، ص 560.

مما سبق يتضح أنّه من أهداف الأفريبول وضع أطر ناظمة من أجل التعاون بين هيئات شرطة الدول الأعضاء لكشف الجرائم السيبرانية وتعزيز المساعدة بين مؤسسات الشرطة.

" إنّ الإنتشار السريع للجريمة الإلكترونية وتعدد وسائلها ونطاق إستعمالها أصبح يشكل تهديداً حقيقياً لأمن شبكات الحاسوب وتطور مجتمع المعلومات في إفريقيا /.../ وعلى إثر ذلك فقد تم إبرام إتفاقية بين الدول الأعضاء في الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني /.../ وقد تم تحديد التوجهات العامة والإستراتيجية لمكافحة الجريمة الإلكترونية في إفريقيا"[1].

إنّ شبكة الأنترنت وما وصلت إليه اليوم من تقدم وتطور في جميع المجالات جعل من الجرائم السيبرانية المتعلقة بها أكثر خطورة لذا إستلزم على دول إفريقيا مواكبة هذا التطور الهائل من خلال إبرام إتفاقية بين الدول الأعضاء الهدف منها وضع إستراتيجيات لمجابهة هذه الجرائم ولا يتحقق هذا إلاّ من خلال " تنسيق بين الدول الأعضاء في الإتحاد الإفريقي في التصدي للجريمة الإلكترونية وتبادل المعلومات، كما دعوا إلى معالجة الثغرات التي تحول دون ذلك من خلال توحيد التشريعات /.../ يتماشى مع سرعة الربط بالقارة الإفريقية التي تعرف في الآونة الأخيرة طفرة نوعية في تحديث منظومتها الإلكترونية"[2].

نستنتج من هنا أنه بفضل التعاون والتنسيق بين الدول يمكن الحد من الجرائم السيبرانية ويكون هذا التعاون من خلال تبادل البيانات، الأدلة، المعلومات ... أيضاً توحيد التشريعات وكل هذا يجب أن يتماشى مع التطور الذي وصلت إليه المنظومات الإلكترونية اليوم.

تسعى الدول جمعاء إلى مواكبة سرعة الأنترنت التي إنجر عليها الكثير من الجرائم التي تهدد أمن البلاد والبشرية فبات من الضروري على الدول إنشاء منظمات وعقد مؤتمرات للحد من هذه الجرائم من أمثلة ذلك: الأنتربول، إتفاقية بودابست، الأفريبول، الجامعة العربية لمكافحة تقنية المعلومات كل هذه الجهود وبالتعاون دولياً فيما بينهم عملو على مكافحة هذه الجرائم من خلال إصدار قوانين وتوحيد التشريعات كل هذا لكشف الحقائق والوصول إلى المجرمين المعلوماتيين من خلال تبادل المعلومات فيما بينهم وتسليم المجرمين وغير ذلك من أساليب التعاون.

---

[1] عبد العزيز لزعر ورشيد زياني، "**آلية الإتحاد الإفريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية**"، مجلة متون، الجزائر، 2021م، ص 256.

[2] المقال نفسه، ص 257.

المطلب الثاني: سياسة المشرع الجزائري لمكافحة الجرائم السيبرانية:

نظراً لتطور الجرائم السيبرانية وتزايدها فقد أصبحت هذه الجرائم تشكل خطراً على المجتمعات لذلك وجب وضع حد لها والجزائر من الدول التي تأثرت بهذه الجرائم فوضعت لها قوانين محاولةً من خلالها ردعها ومن خلال التطور التكنولوجي الحاصل اليوم وإزدياد الجرائم السيبرانية يوماً بعد يوم إضطر المشرع الجزائري لإستحداث قوانين ونصوص جديدة لقمع الإعتداءات الواقعة على الفضاء السيبراني ضمن نصوص قانون العقوبات وقانون الإجراءات الجزائية، ومن خلال هذا المطلب سنأتي بذكر النصوص التي أقرتها الجزائر للتصدي للجرائم السيبرانية:

الفرع الأوّل: الحماية بموجب الدستور:

" لقد كفل دستور الجزائر لسنة 2020 حماية حقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم إنتهاك حرمة الإنسان وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق"[1].

عمل الدستور الجزائري على حماية حقوق الإنسان وفرض عقوبات صارمة لكل من ينتهكها بوضع قوانين وإجراءات الموجودة في قانون العقوبات وقانون الإجراءات الجزائية وغيرها من القوانين ومن أهم المبادئ الدستورية ما يلي:

" ـ المادة 35: تضمن الدولة الحقوق الأساسية والحريات.

ـ المادة 47: لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرية مراسلاته وإتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلاّ بأمر معلل من السلطات القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

---

[1] قطاف سليمان وبوقرين عبد الحليم،"**مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية**"، مجلة البحوث القانونية والإقتصادية، المجلد 5، العدد2، الأغواط، الجزائر، 2022م، ص 344.

يعاقب القانون على كل إنتهاك لهذه الحقوق.

ـ المادة 6/54: الحق في نشر الأخبار والأفكار والصور والآراء في إطار القانون، وإحترام ثوابت الأمة وقيمها الدينية والأخلاقية والثقافية "[1].

حرص الدستور على حماية حرمة الحياة الخاصة للأفراد فقام بسن قوانين تحميهم وتدافع عن حقوقهم من الإعتداءات التي تقع من طرف المجرمين فعلى كل إنسان وقع عليه إعتداء في حق من حقوقه أي يلجأ لأطلب وقف هذا الإعتداء إضافة إلى طلب التعويض عن الضرر الذي لحقه وهذا ما جاء به الدستور الجزائري.

الفرع الثاني: الآليات القانونية الموضوعية:

" سعياً من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني ومايصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولةً منه تدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والإتصال"[2]، حاول المشرع الجزائري تدارك الفراغ لمواجهة الجرائم السيبرانية من خلال تعديل القوانين المتعلقة بهذه الجرائم كل هذا لمواكبة التطورات التي وصلت إليها الجريمة الإلكترونية اليوم.

" قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 15/04 من أجل تجريم الأفعال الماسة بأنظمة الحاسب الآلي، وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، حيث جاء التعديل في المواد 394 مكرر إلى المادة 394 مكرر 7 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات"[3].

أجرى المشرع هنا تعديلات للمواد من 394 مكرر إلى 394 مكرر 7 حيث قام بتبيان كل ما يخص

---

[1] دستور الجمهورية الجزائرية الديمقراطية الشعبية وفقا للتعديل الدستوري لسنة 2020م، صادر بموجب المرسوم الرئاسي رقم 20 ـ 442، مؤرخ في 30 ديسمبر سنة 2020م، ج ر ج ج ، عدد 82، الصادرة في 30 ديسمبر 2020م.

[2] راضية عيمور، المقال السابق، ص 95.

[3] القانون 15/04 المتضمن إستحداث قسم جديد في قانون العقوبات، المرجع السابق.

العقوبات والغرامات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات بالنسبة للشخص الطبيعي والمعنوي كل هذا من أجل التصدي لهذا الخطر الكبير الذي أصبح بمثابة هاجس للعصر الذي نعيشه.

أضاف المشرع الجزائري في سنة 2006 تعديلات جديدة مست القسم السابع مكرر منه، ومن بين الجرائم المعدلة في قانون العقوبات ما يلي: جريمتا الدخول والبقاء غير المصرح بهما: نصت المادة 394 مكرر ما يلي:

" يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة . يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي" [1].

نلاحظ هنا أنّ المشرع الجزائري جرّم الدخول والبقاء في أي منظومة غير مصرح بها أو حتى جزء منها وفرض العقاب عليها بالحبس وغرامة مالية محددة في المادة 394 مكرر من قانون العقوبات، هذا بالنسبة للشخص الطبيعي أمّا الشخص المعنوي فقد تحدثت عنه المادة 394 مكرر4 ، وهنا أوقع المشرع الجزائري العقاب عليه أيضاً حيث تمثلت العقوبة بغرامة تعادل خمس مرات للمقررة للشخص الطبيعي.

الفرع الثالث: الآليات القانونية الإجرائية:

" كخطوة جديدة قام المشرع الجزائري بسن القانون 04/09 المتعلق بالوقاية من تكنولوجيا الإعلام والإتصال ومكافحتها، وإن كان تجسيد بنوده على أرض الواقع ما زال ضعيفاً إلى حد الساعة نتيجة إهمال الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وفي تحديد العقوبة المناسبة في حق مرتكبيها، حيث تقتصر العقوبات في غالبية الأحيان على الغرامة المالية فقط" [2].

[1] القانون 15/04 المتضمن إستحداث قسم جديد في قانون العقوبات، المرجع السابق.

[2] مهدي رضا، "**الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري**"، مجلة إليزا للبحوث والدراسات، المجلد6، العدد2، الجزائر، 2021م، ص 118.

إضافة إلى قانون العقوبات وضع المشرع الجزائري قانوناً آخر يختص بالجرائم السيبرانية كل هذه الجهود للحد من هذا الخطر وردع المجرمين الذين يقومون بهذه الجرائم من خلال العقوبات التي أقرها المشرع الجزائري في هذا القانون رقم 04/09 فمن التدابير الوقائية والإجرائية التي وضعها نذكر ما يلي:

تمثلت التدابير الوقائية في الإستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية من خلال المادة 11 والمراقبة الإلكترونية في المادة 4 وغيرها، فتحدثت المادة 11 عما يلي:

" ـ المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ـ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

ـ الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال.

ـ المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

ـ المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليه"[1].

وهنا يقوم مزودي الخدمات بتقديم مساعدات للسلطات من أجل التحقيقات الجنائية عن طريق جمع المعطيات وتسليمها لهم وأيضاً يجب على مزودي الخدمات الإتصاف بالأمانة لأنهم يحتفظون بهذه المعلومات ومن خلال المادة 11 نستطيع معرفة نوع الإتصال ووقته ومدته والطريق الذي سلكه كل هذا لمساعدة الجهات المختصة للوصول إلى الأدلة والبراهين لإثبات الجرائم السيبرانية ومن ثمة معرفة العقوبات الواجب إتخاذها لتوقيع العقاب على المجرمين.

وهناك أيضاً تدابير إجرائية مذكورة في قانون 04/09 من بينها إجراءات تفتيش وحجز المنظومة المعلوماتية والذي ذكر في المادتين 03 و07 بالإضافة إلى تبادل المساعدة القضائية الدولية...إلخ من الإجراءات وجاءت المادة 03 و07 بما يلي:

[1] القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المرجع السابق.

" المادة 3: وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

المادة 7: إذا إستحال إجراء الحجز وفقاً لما هو منصوص عليه في المادة 06 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة"[1]. نلاحظ هنا أنّ القانون أجاز اللجوء إلى التفتيش حتى وإن كان عن بعد، كما يستلزم على السلطة أن تقوم بالتفتيش من خلال إستخدام تقنيات من أجل عدم الوصول إلى المعطيات المتواجدة داخل المنظومة.

وحرصاً من المشرع الجزائري قام بإستحداث قطب جزائي وطني متخصص في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال في ظل الأمر رقم 11/21 في الباب السادس من خلال المواد من 211 مكرر22 إلى 211 مكرر 29 [2].

وفي الأخير نرى أنّ المشرع الجزائري بذل قصار جهده للتصدي لظاهرة الإجرام السيبراني وما خلّفه من أضرار على الأفراد والمؤسسات حيث حاول من خلال قانون العقوبات وقانون الإجراءات الجزائية والعديد من النصوص الأخرى إستحداث وتعديل القوانين لجعلها تتناسب والتطورات الإجرامية خاصة مع التطور التكنولوجي الذي وصلنا له اليوم، كل هذا من أجل الحماية الجنائية للمعاملات الإلكترونية والتصدي للإعتداءات التي تقع عليها من خلال فرض عقوبات جد صارمة على مرتكبي هذه الأفعال.

المبحث الثالث: الصعوبات التي تواجه التعاون الدولي لمكافحة الجرائم السيبرانية وسبل التغلب عليها:

حاولت الدول العربية والأجنبية بالتعاون فيما بينهم من خلال الإتفاقيات كإتفاقية بودابست والإتفاقية العربية لمكافحة جرائم تقنية المعلومات إضافة إلى الجهود التي قاموا بها للحد من الجرائم السيبرانية إلاّ أنهم

[1] القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المرجع السابق.

[2] الأمر رقم 11/21 المتضمن قانون الإجراءات الجزائية المعدل والمتمم، المرجع السابق.

واجهوا العديد من العقبات والإشكاليات التي صعبت عليهم تحقيق ذلك وفي هذا المبحث سنحاول الإحاطة بأهم هذه الصعوبات وكيفية الحد منها والقضاء عليها.

المطلب الأول: مشكلات التعاون الدولي لمكافحة الجرائم السيبرانية:

تختلف التشريعات في مضامين النصوص القانونية بإختلاف الفلسفة القانونية لكل دولة، فهناك جرائم تعد مباحة في تشريعات دولة ما عكس الدول الأخرى تعتبر فيها أنها أفعال غير مشروعة، ونظراً لإختلاف هذه النظم واجه التعاون الدولي الكثير من العوائق والصعوبات ومن بين هذه الصعوبات ما يلي:

الفرع الأول: عدم وجود نموذج موحد للنشاط الإجرامي:

" عدم وجود نموذج موحد للجرائم المعلوماتية، إذ أنّ لكل دولة تصنيفها الخاص لتلك الجرائم فبعض من الدول يجرم كل الصور والبعض الآخر يجرم فقط البعض منها، وبالتالي ما يكون مباحاً في دولة يكون مجرماً في دولة أخرى"[1].

نرى هنا أنّه نظراً لإختلاف الأنظمة القانونية المتعلقة بالجرائم السيبرانية أنه لا يوجد تفاهم في كيفية إستخدام نظم المعلومات بين الدول حيث يعود ذلك لإختلاف السياسات والبيئات والعادات من دولة لأخرى.

الفرع الثاني: تنوع وإختلاف النظم القانونية الإجرائية:

" بسبب تنوع وإختلاف النظم القانونية الإجرائية، نجد أنّ طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهة فإذا ما إعتبرت طريقة ما من طرق جمع الإستدلالات أو التحقيق أنّها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى"[2].

---

[1] بعقيقي عبير، "**مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي ـ دراسة مقارنة** ـ"، (أطروحة دكتوراه)، تخصص النظام الجزائي والسياسة الجزائية المعاصرة، كلية الحقوق والعلوم السياسة، جامعة محمد خيضر بسكرة، الجزائر، 2017 ـ 2018م ، ص306.

[2] وائل محمد عبد الرحمان نصيرات، المرجع السابق، ص 133.

فمن الصعوبات التي واجهها التعاون الدولي إضافة إلى إختلاف الأنظمة القانونية فإنّ حتى الطرق وأساليب التحري والتحقيق والمحاكمة قد تختلف من دولة إلى أخرى لأنّ لكل دولة الأساليب الخاصة بها قي التحري والتحقيق في مثل هذه الجرائم.

الفرع الثالث: التجريم المزدوج:

" التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتتسليم المجرمين، وبالرغم من أهميته تلك، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية سيما وأن معظم الدول لا تجرم هذه الجرائم" [1].

يقصد بالتجريم المزدوج هنا آليات تسليم المجرمين وهذا يختلف بإختلاف التشريعات لكل دولة خاصة وأنّ هناك بعض الدول لا تجرم بعض هذه الجرائم وهذا ما يشكل عائق أمام التعاون الدولي.

الفرع الرابع: عدم وجود معاهدات ثنائية أو جماعية:

وهنا نرى أنه لا يوجد معاهدات تسمح " بالتعاون المثمر في مجال هذه الجرائم وحتى في حالة وجودها فإن هذه المعاهدات تبقى قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب الآلي وشبكة الأنترنت، ومن ثم تطور الجريمة المعلوماتية بذات السرعة على نحو يؤدي إلى إرباك المشرع وسلطات أمن الدول" [2].

أن التقدم الذي وصلنا له اليوم من خلال التطور التكنولوجي عبر شبكة الأنترنت ساعد في القيام على الجرائم السيبرانية لأن النظم والبرامج في تقدم سريع مقارنة بالجهود التي تقوم بها الدول للحد منها لذلك وجب وضع معاهدات وإتفاقيات دولية تعمل جاهدة على تحقيق الحماية ويجب أن تكون مواكبة لهذا التقدم لمكافحة هذه الجرائم الخطيرة.

---

[1] أمير فرج يوسف، المرجع السابق، ص 437.

[2] قطاف سليمان وبوقرين عبد الحليم، المقال السابق، ص 82.

الفرع الخامس: إشكالية الإختصاص القضائي:

" في أغلب الأحيان تتم الجرائم الإلكترونية من خلال أفعال ترتكبها أشخاص من خارج الحدود كما يتم تنفيذها عبر شبكات وأنظمة معلومات خارج الحدود أيضاً، وما يثير التساول حول الإختصاص القضائي لهذه الجرائم بالإضافة إلى حقيقة إمتداد أنشطة الملاحقة والضبط والتحري والتفتيش خارج الحدود الوطنية أمر يتطلب تعاوناً دولياً شاملاً يهدف إلى تحقيق مكافحة مثل هذه الجرائم وذلك مع إحترام السيادة الوطنية للدول المعنية" [1].

من خصائص الجرائم السيبرانية أنها عابرة للحدود أي يمكن أن يقوم الأشخاص بالجرائم من خارج دولتهم وهنا يقع إشكال مَن الدولة المختصة قضائياً عن توقيع العقاب لهذا المجرم؟ هل هي الدولة التي ينتمي إليها؟ أم الدولة التي وقعت فيها الجريمة؟ وهذا الأمر يستدعي تعاوناً دولياً وإتفاق بين الدول على إحترام الجهة المختصة بتوقيع العقاب لأن جميع الدول تسعى جاهدة لمكافحة هذه الجرائم.

الفرع السادس: الصعوبات التي تواجه الجهود الدولية في مجال قنوات الإتصال:

" أهم الأهداف المرجوة من التعاون الدولية في مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لازماً أن يكون هناك نظام إتصال يسمح للجهات القائمة على التحقيق بالإتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالباً ما تكون مفيدة في التصدّي لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون"[2].

نرى هنا أنّ نظام الإتصال يسهل على الجهات القائمة بالتحقيق على جمع الأدلة الهامة لإستكمال التحقيق في الجرائم وهذا ما تسعى إليه الجهود الدولية وهو الحصول على المعلومات التي تخص المجرمين من أجل وضع حد لهم لأن المهمة الأصعب هي الوصول إلى هذه الأدلة خاصة أن هذه النوعية من الجرائم قد تقع في أكثر من دولة لذا وجب أن يكون هناك إتصال بين الدول للعمل على القضاء على الجرائم السيبرانية.

---

[1] مبروك فاطيمة وذيب محمد، "**التعاون الدولي لمكافحة الجريمة الإلكترونية، الأشكال والإشكالات**"، مجلة الحقوق والعلوم السياسية، المجلد11، العدد1، الجزائر 2024م، ص 121.

[2] أمير يوسف فرج، المرجع السابق، ص 436..

الفرع السابع: الصعوبات الخاصة بالمساعدات القضائية الدولية:

"نعلم أنّ الأصل بالنسبة لطلبات الإنابة القضائية الدولية والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطريق الديبلوماسية وهذا بالطبع يجعلها تتسم بالبطئ والتعقيد والذي يتعارض مع طبيعة الأنترنت وما تتميز به من سرعة، وهو الأمر الذي إنعكس على الجرائم المتعلقة بالأنترنت" [1].

يقصد بالمساعدة القضائية هنا الإجراءات التي تسهل المحاكمة حيث تقوم بها دولة ما لمساعدة دولة أخرى وصور المساعدة تقوم على الطريق الديبلوماسية وعادة ما تتسم بالبطئ وهذا ما يعقد الأمر لأن الأنترنت تتميز بالسرعة الفائقة وهذا ما يسهل على المجرمين القيام بالجرائم.

المطلب الثاني: سبل التغلب على مشكلات التعاون الدولي:

من أجل القضاء على الجرائم السيبرانية ومكافتها بفعالية، يجب معالجة الصعوبات والعراقيل التي واجهة الجهود الدولية من خلال مجموعة من الإجراءات وفي هذا المطلب سنحاول أن نلم بأهم الحلول والإجراءات المتوصل إليها.

الفرع الأوّل: حل عقبة عدم وجود نموذج موحد للنشاط الإجرامي:

" يتم حل هذه العقبة نتوحيد النظم القانونية وتخفف من غلو الفوارق بين الأنظمة العقابية الداخلية، وذلك من خلال تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية وإبرام إتفاقيات خاصة يراعى فيها هذا النوع من الجرائم" [2]، حاولوا هنا وضع نظام موحد للأنظمة الداخلية حيث قاموا بتجديد التشريعات المحلية وتكوين معاهدات وإتفاقيات لمكافحة الجرائم السيبرانية.

الفرع الثاني: حل عقبة تنوع وإختلاف النظم الإجرائية:

" إن الصكوك الدولية الصادرة عن الأمم المتحدة غالباً ما تشجع الأطراف فيها على السماح بإستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غلو وإختلاف النظم القانونية والإجرائية

---

[1] أمير فرج يوسف، المرجع السابق، ص ـ ص: 437 ـ 438.

[2] وائل محمد عبد الرحمان نصيرات، المرجع السابق، ص 134.

ويفتح المجال أمام نعاون دولي فعّال، فمثلاً المادة 20 من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقب والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة" [1].

إنّ الأمم المتحدة من الدول المشجعة على إستخدام التقنيات الخاصة وهذا ما يفتح المجال أمام الدول الأخرى لتعاون دولي الغرض منه الحد من الجرائم المعلوماتية المنتشرة بكثرة وهذا ما نصّت عليه المادة 20 من إتفاقية الأمم المتحدة كالتسليم المراقب والمراقبة الإلكترونية التي تعتبر من أهم العمليات التي تقوم بها الدول بالتعاون فيما بينها.

حيث هذه الأشكال " تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة المحنكة بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لإستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة" [2].

نلاحظ من هنا أنّ هذه التقنيات والأشكال جاءت للتصدي للعمليات الإجرامية التي يقوم بها مجرمو المعلومات ولتجميع الأدلة والمعلومات الكامنة لمساعدتهم أثناء التحقيق وكل هذا يرجع لتعاون الدول فيما بينهم للحد من هذه العمليات الإجرامية.

الفرع الثالث: ضرورة إبرام إتفاقيات دولية ثنائية كانت أو جماعية:

" يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الإختصاص القضائي خاصةً بالنسبة للجرائم المتعلقة بالأنترنت بالإضافة إلى تحديد القوانين الجنائية الموضوعية منها والإجرائية لما يتناسب والتطور الكبير الذي تشهده تكنولوجيا المعلومات والإتصالات" [3].

إنّ إختلاف وجهات النظر يجعل لكل دولة قواعد خاصة بها لكن في بعض الأحيان ومن أجل الكشف عن الجرائم التي تقع بين الدول خاصة الجرائم المتعلقة بالأنترنت والحاسوب يجب توحيد وجهات النظر في الإختصاص القضائي فيكون هناك مساعدة وتعاون بين الدول لكشف الحقيقة والقبض على

[1] قطاف سلسمان وبوقرين عبد الحليم، المقال السابق، ص 84.
[2] وائل محمد عبد الرحمان نصيرات، المرجع السابق، ص 134.
[3] محمد أحمد سليمان عيسى، المقال السابق، ص 63.

المجرمين فهنا على الدول إبرام إتفاقيات خاصة بالقوانين الجنائية ويجب أن نكون هذه القوانين تواكب التطور التكنولوجي الذي هو عليه اليوم.

الفرع الرابع: حل عقبة الإختصاص في الجرائم الأنترنتية:

" بالنسبة لمشكل الإختصاص في الجرائم الأنترنتية فثمة حاجة ملحة إلى

1. إتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الإختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالأنترنت.

2 . بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير التي تشهده تكنولوجيا المعلومات والإتصالات" [1].

هنا نرى أنه لحل هذه العقبة ضرورة إبرام إتفاقيات تتعلق بقواعد الإختصاص القضائي إلى جانب تجديد القوانين الجنائية إجرائية كانت أو موضوعية تتناسب من التطور التكنولوجي الذي تشهده تكنولوجيا المعلومات لأن العلم يكتشف الجديد كل يوم وفي سرعة فائقة لذا يجب مجاراته والسعي دائما لمواكبته االحد من الجرائم السيبرانية التي أصبحت تشكل خطورة على المجتمع.

الفرع الخامس: حل عقبة عدم وجود قنوات إتصال:

" للحد من ظاهرة عدم وجود قنوات إتصال بين جهات إنفاذ القانون فنلاحظ أنّه غالباً ما تشجع الصكوك الدولية الدول إلى التعاون فيما بينها وتدعوها إلى إنشاء قنوات إتصال بين سلطاتها المختصة ووكالاتها ودوائرها المختصة بغية التيسير في الحصول على هذه المعلومات وتبادلها" [2].

لحل هذه العقبة يجب أن تتعاون الدول فيما بينها بإنشاء قنوات إتصال بين السلطة المختصة والدول التي وقعت فيها الجريمة من أجل الحصول على الأدلة والمعلومات وتبادلها لتوقيع العقاب على مرتكبي هذه الجرائم.

---

[1] وائل محمد عبد الرحمان نصيرات، المرجع السابق، 135.

[2] قطاف سليمان وبوقرين عبد الحليم، المقال السابق، ص 84.

الفرع السادس: حل العقبة المتعلقة بالمساعدات القضائية الدولية:

" 1 ـ تبادل المعلومات: وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الإستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما عن الإتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي إتخذت ضدهم.

2 ـ نقل الإجراءات: ويقصد به قيام دولة ما بناءاً على إتفاقية أو معاهدة بإتخاذ إجراءات جنائية وهي بصدد جريمة إرتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة" [1].

نستنتج مما سبق لكي يكون هناك تعاون دولي فعّال يجب تبادل المعلومات بين الدول فمثلاً إذا طلبت دولة أجنبية وثائق أو بيانات تخص قضية ما وقعت في دولة أخرى فعلى هذه الدولة تلبية الطلب وإعطائها كل الأدلة التي تملكها إضافة إلى نقل الإجراءات حيث يقصد بها إتخاذ إجراءات من المعاهدات حيث تقوم الجريمة في إقليم دولة أخرى ويكون هذا الإجراء لمصلحة هذه الدولة.

[1] قطاف سليمان وبوقرين عبد الحليم، المقال السابق ، ص 83.

ملخص الفصل الثاني:

قامت الدول الأجنبية بإبرام إتفاقيات ومعاهدات من خلال التعاون الدولي حيث كانت إتفاقية بودابست من أوّل الإتفاقيات التي وضعت نظام تعاون بين الدول إضافة إلى تحديد وسائل التحقيق والملاحقة الجزائية وغيرها وسعت هيئة الأمم المتحدة إلى تحديث القوانين الجنائية وتعزيز أمن الكمبيوتر وغيرها إضافة إلى التعاون الأمني المتمثل في الأنتربول الذي قام بإنشاء مركز إتصالات أمني عبر الشبكة وسعى إلى التنسيق بين أجهزة الشرطة عن طريق المساعدات المتبادلة بينهم وتسليم المجرمين لعدم الإفلات من العقاب.

كما حاولت الدول العربية بالتعاون فيما بينها للحد من هذه الجرائم بوضع إتفاقيات كالإتفاقية العربية لمكافحة جرائم تقنيات المعلومات التي سعت إلى ضرورة تحقيق العدالة عن طريق فرض عقوبات صارمة كما نادت إلى تعزيز التعاون القضائي من خلال المساعدات القضائية المتمثلة في تبادل المعلومات والأدلة إضافة إلى جهود دولة الإمارات والسعودية وغيرها الذين نادوا بضرورة التعاون الدولي من أجل تحقيق العدالة.

والجزائر أيضاً من الدول التي تسعى جاهدة لمكافحة هذه الجرائم فقام المشرع بإستحداث قوانين لقمعها من خلال القانون 15/04 و04/09 عن طريق فرض عقوبات لكل شخص يتعدّى على الأنظمة الآلية للمعطيات.

رغم كل هذه الجهود إلاّ أنّها تتعرض لصعوبات كعدم وجود قنوات إتصال تسمح بتبادل المعلومات والأدلة، ونظراً للتطور التكنولوجي السريع تبقى المعاهدات والإتفاقيات قاصرة عن تحقيق الحماية المطلوبة لذا وجب وضع حلول لهذه الصعوبات تتناسب والتطور الحاصل للقضاء على الجرائم السيبرانية.

خاتـــمة

خاتمة:

وختاماً لموضوع دراستنا يمكننا القول أنّ الجرائم السيبرانية جرائم مستحدثة سريعة الإنتشار لما يتلاؤم والتطور التكنولوجي الذي في تقدم يوماً بعد يوم، لذلك فهي من الجرائم الخطيرة التي أصبحت تهدد أمن وإستقرار الدول التي سعت جاهدة للتصدّي لها، فبالرغم من الجهود والمحاولات التي قاموا بها لقمع هذه الإعتداءات إلاّ أنّهم واجهوا العديد من الصعوبات التي وقفت عائقاً لمواجهة هذا الخطر.

ولقد خلصنا بعد دراستنا لهذا البحث إلى مجموعة من النتائج نوجزها فيما يلي:

- إنّ إساءة إستخدام التكنولوجيا ولّدت لنا الجرائم السيبرانية التي أضحت هاجس العصر الحالي.
- تتّسم الجرائم السيبرانية بأنّها جرائم عابرة للحدود لذلك يصعب إكتشاف زمن وقوعها وإثبات من قام بها.
- يتصف المجرم المعلوماتي بالذكاء والمهارة وهذا ما يجعل منه فرداً خطيراً على المجتمع نظراً لشغفه بعالم التكنولوجيا التي من خلالها يستطيع تطوير تقنياته الإجرامية.
- تعزيز التعاون الدولي قضائياً وإجرائياً للقضاء على الجرائم السيبرانية.
- عمل المشرع الجزائري على إستحداث بعض النصوص والمواد القانونية من أجل مكافحة هذه الظاهرة.
- ضرورة التنسيق بين الدول من أجل تبادل المعلومات وغيرها من الإجراءات التي تمكّنهم من الإمساك بالمجرمين وعدم إفلاتهم من العقاب.

ومن خلال هذه النتائج التي توصلنا إليها نقترح مجموعة من التوصيات التي تتمثل في:

- ✓ ضرورة إصدار نصوص قانونية جديدة تعمل على مكافحة هذه الجرائم وفرض عقوبات صارمة لمرتكبيها.
- ✓ تكثيف التعاون الدولي من خلال تنظيم دورات تكوينية لضباط الشرطة القضائية من أجل التعمق في فهم التقنيات التكنولوجية.

- ✓ العمل على تنظيم حملات تحسيسية وملتقيات تحت عنوان "السلبيات والمخاطر التي تخلفها شبكة الأنترنت" لنشر الوعي في المجتمع من أجل تفادي هذه الجرائم الخطيرة والدعوة إلى الإستخدام الأمثل لهذه التقنيات المعلوماتية.
- ✓ ضرورة التعاون الدولي من خلال مساندة الدول لبعضها والتنسيق فيما بينهم كالمساعدات القضائية وتسليم المجرمين وغيرها كل هذا لمجابهة هذا الخطر.

قائـــمة المصـــادر والمراجـــع

قائمة المصادر والمراجع:

❖ القرآن الكريم برواية ورش عن نافع.

أولاً: قائمة المصادر:

- **الدستور:**

1- دستور الجمهورية الجزائرية الديمقراطية الشعبية وفقاً للتعديل الدستوري سنة 2020م، صادر بموجب المرسوم الرئاسي رقم 20 ـ 442، مؤرخ في 30 ديسمبر سنة 2020م، ج ر، ج ج، عدد 82، الصادرة في 30 ديسمبر 2020م.

- **الإتفاقيات:**

1- إتفاقية بودابيست لمكافحة الجرائم المعلوماتية، المجلس الأوروبي ببودابيست، رقم 185، بتاريخ 21 نوفمبر 2001م.

2- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية، العدد58.

- **النصوص التشريعية:**

1- الأمر رقم 11/21 المؤرخ في 16 محرم عام 1443هـ، الموافق 25 غشت سنة 2021م، يتمم الأمر رقم 155/66 المؤرخ في 18 صفر عام 1386هـ، الموافق لـ8 يونيو سنة 1966م، والمتضمن قانون الإجراءات الجزائية المعدل والمتمم.

2- الأمر 156/66 المؤرخ في 8 جوان 1966م، المتضمن قانون العقوبات ، الجريدة الرسمية، العدد 84، الصادرة بتاريخ 10 جوان 1966م، المعدل والمتمم.

3ـ القانون رقم 04/09 مؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد47، الصادر في 16 أوت 2009م.

4ـ القانون رقم 05/18 المؤرخ في 10 ماي 2018م، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد28، المؤرخة في 16 ماي 2018م.

ثانياً: قائمة المراجع:

✓ الكتب العربية:

1ـ أمير فرج يوسف،" **الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت**"، ط1، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2011م.

2ـ بسام محمد أبو عليان، "**الإنحراف الإجتماعي والجريمة (علم إجتماع الجريمة)**"، ط3، منشورات أي ـ كتب، (د،ب)، 2016م.

3ـ حسين طاهري، "**الجرائم الإلكترونية**"، ط1، دار الخلدونية، الجزائر، 2021م.

4ـ خالد ممدوح إبراهيم، "**أمن الجريمة الإلكترونية**"، (د،ط)، الدار الجامعية، الإسكندرية، مصر، 2008م.

5ـ راجي أبو شقرة، "**دليل إستعمال خدمات الأنترنيت لغير المختصين**"، ط1، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان، 1997م.

6ـ سامى على حامد عياد، "**الجرائم المعلوماتية وإجرام الأنترنت**"، (د،ط)، دار الفكر الجامعي ، الإسكندرية، مصر، 2007م.

7ـ صلاح الدين نور الدين، "**المعلوماتية**"، (د،ط)، منشورات وزارة الثقافة، دمشق، سوريا، 2000م.

8ـ عادل عبد العال إبراهيم خراشي، "**إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**"، (د،ط)، دار الجامعة الجديدة، القاهرة، مصر، (د،س).

9- عبد العال الديربي ومحمد صادق إسماعيل، "**الجرائم الإلكترونية دراسة قانونية قضائية مقارنة**"، ط1، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012م.

10- علي جبار الحسيناوي، "**جرائم الحاسوب والأنترنت**"، الطبعة العربية، دار اليازوري العلمية، عمان، الأردن، 2009م.

11- علي جعفر، "**جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة ـ دراسة مقارنة ـ**"، ك1، مكتبة زين الحقوقية والأدبية، (د،ب)، 2013م.

12- عمار عباس الحسيني، "**جرائم الحاسوب والأنترنت الجرائم المعلوماتية**"، ط1، مكتبة زين الحقوقية والأدبية، بيروت، لبنان، 2017م.

13- غنية باطلي، "**الجريمة الإلكترونية دراسة مقارنة**"، (د،ط)، الدار الجزائرية، الجزائر، 2016م.

14- فتوح الشاذلي وعفيفي كامل عفيفي، "**جرائم الكمبيوتر (حقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون) دراسة مقارنة**"، (د،ط)، منشورات الحلبي الحقوقية، لبنان، 2033م.

15- كوثر مازوني، "**الجريمة المعلوماتية**"، ط1، الدار الخلدونية، الجزائر، 2022م.

16- محمد أمين الشوابكة، "**جرائم الحاسوب والأنترنت الجريمة المعلوماتية**"، ط1، دار الثقافة، عمان، الأردن، 2007م.

17- محمود أحمد عبابنة، "**جرائم الحاسوب وأبعادها الدولية**"، ط1، دار الثقافة، عمان، الأردن، 2009م.

18- محمود نجيب حسني، "**شرح قانون العقوبات**"، (د،ط)، دار النهضة العربية، القاهرة، مصر، 1962م.

19- منى الأشقر جبور، "**السيبرانية هاجس العصر**"، (د،ط)، المركز العربي للبحوث القانونية، بيروت، لبنان، 2017م.

20- منصور بن فهد صالح العبيد، "**الأنترنت Internet إستثمار المستقبل**"، ط1، مكتبة الملك فهد الوطنية، الرياض، 1996م.

21ـ منير محمد الجنبيهى ومحمود محمد الجنبيهى، "**جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها**"، ط2، دار الفكر الجامعي، الإسكندرية، مصر، (د،س).

22ـ نبال إدلبي، "**أنترنت**"، تر: منى ملحيس، ط2، الدار العربية للعلوم، بيروت، لبنان، 1998م.

23ـ نسرين عبد الحميد نبيه، "**الجريمة المعلوماتية والمجرم المعلوماتي**"، (د،ط)، دار المعارف، الإسكندرية، مصر، 2008م.

24ـ نهلا عبد القادر المومني، "**الجرائم المعلوماتية**"، ط2، دار الثقافة، الأردن، 2010م.

25ـ وائل محمد عبد الرحمان نصيرات، "**الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها**"، (د،ط)، دار المنظومة، الرياض، السعودية، 2016م.

✓ الرسائل الجامعية:

1ـ بعقيقي عبير، "**مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإمارلتي ـ دراسة مقارنة** ـ."، (رسالة دكتوراه)، بجامعة محمد خيضر بسكرة، قسم الحقوق، الجزائر، 2018/2017.

2ـ قلات سومية، " **الأحكام الإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري**"، (أطروحة دكتوراه)، جامعة محمد خيضر بسكرة، قسم الحقوق، الجزائر، 2024/2023م.

3ـ طارق أحمد مسعود، "**دور التعاون الدولي في مكافحة الجرائم الإلكترونية**"، (رسالة ماجستير)، جامعة أبوظبي ـ كلية الحقوق ـ ، الإمارات، 2022/2021م.

4ـ عبد الله دغش العجمي، "**المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة**"، (مذكرة ماجستير)، جامعة الشرق الأوسط، قسم القانون العام، 2014م.

5ـ محمد يسعد ليلى، "**أهمية الأنترنت لدى الطالب الجامعي في ظل العولمة**"، (مذكرة ماجستير)، جامعة سعد دحلب، قسم علم الإجتماع، البليدة، الجزائر، 2005م.

✓ المجلات:

1- آسيا العمراني، "**التعاون الدولي في مواجهة الجرائم السيبرانية - الجزائر نموذجاً -**"، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد3، العدد2، الجزائر، 2010م.

2- الطاهر ياكر، "**مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والإتفاقيات الدولية**"، مجلة الصدى للدراسات القانونية والسياسية، المجلد4، العدد4، الجزائر، 2022م.

3- إيمان بغدادي، "**أثر تعديل قانون العقوبات الجزائري في التصدّي للجريمة الإلكترونية**"، مجلة آفاق للبحوث والدراسات السياسية، العدد4، الجزائر، 2019م.

4- جمال محمد خلفان محمد النقبي وسلطان محمد سالم عوض هيسان المعصبي، "**التعاون الوطني والدولي في الجرائم الإلكترونية المشكلات والحلول**"، مجلة المعهد العالي للدراسات النوعية، مجلد3، عدد16، 2023م.

5- خرشي عثمان، "**تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية**"، مجلة البحوث القانونية والسياسية، العدد10، الجزائر، 2018م.

6- خليلي سهام، "**خصوصية المجرم الإلكتروني**"، مجلة المفكر، العدد15، سطيف، الجزائر، 2017م.

7- راضية عيمور، "**الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري**"، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد6، العدد1، الجزائر، 2022م.

8- رانا مصباح عبد المحسن عبد الرزاق، "**آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية "دراسة تحليلية""**، المجلة القانونية، (د،ب)، (د،س).

9- ربيعي حسين، "**المجرم المعلوماتي - شخصيته وأصنافه -**"، مجلة العلوم الإنسانية، العدد40، بسكرة، الجزائر، 2015م.

10- رضا عسّال وعماد عبد الرزاق، "**الجريمة الإلكترونية والمجرم المعلوماتي مقاربة مفاهيمية**"، مجلة بيبليوفيليا، العدد5، تبسة، الجزائر، 2020م.

11- سفيان رقيق وعلي عز الدين، "**تفعيل إدارة العلاقة مع الزبون من منظور تكنولوجيا الأنترنت**"، مجلة البديل الإقتصادي، العدد6، الجلفة، الجزائر.

12- شوارب الجيلاني ومراد فايزة، "**الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية**"، مجلة الدراسات القانونية والسياسية، المجلد9، العدد2، الجزائر، 2023م.

13- عبد العزيز لزعر ورشيد زياني، "**آلية الإتحاد الإفريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية**"، مجلة متون، الجزائر، 2021م.

14- عفاف بوعون ونسيمة ولاد سالم، "**الجريمة الإلكترونية قراءة سسيوتاريخية في النشأة والآثار**"، مجلة القبس للدراسات النفسية والإجتماعية، المجلد5، العدد20، الجزائر، 2023م.

15- فاروق خلف، "**الآليات القانونية لمكافحة الجريمة المعلوماتية**"، مجلة الحقوق والحريات، العدد2، الجزائر، 2015م.

16- فتيحة حيمر، "**تأثير الجريمة الإلكترونية على الأمن في إفريقيا**"، مجلة أبحاث قانونية وسياسية، المجلد9، العدد1، الجزائر، 2024م.

17- قزران مصطفى وزرقين عبد القادر، "**الآليات الدولية لمكافحة الجريمة الإلكترونية**"، مجلة صوت القانون، المجلد8، العدد2، الجزائر، 2022م.

18- قطاف سليمان وبوقرين عبد الحليم، "**مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية**"، مجلة البحوث القانونية والإقتصادية، المجلد5، العدد2، الجزائر، 2022م.

19- لامية طالة وكهينة سلام، "**الجريمة الإلكترونية بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الإجتماعي**"، مجلة الرواق للدراسات الإجتماعية والإنسانية، المجلد6، العدد2، الجزائر، 2020م.

20- مبروك فطيمة وذيب محمد، "**التعاون الدولي لمكافحة الجريمة الإلكترونية الأشكال والإشكاليات**"، مجلة الحقيق والعلوم السياسية، المجلد11، العدد1، الجزائر، 2024م.

21- محمد أحمد سليمان عيسى، "**التعاون الدولي لمواجهة الجرائم الإلكترونية**"، المجلة الأكاديمية للبحث القانوني، المجلد14، العدد2، المملكة العربية السعودية، 2016م.

22- مراد مشوش، "**الجهود الدولية لمكافحة الإجرام السيبراني**"، مجلة الواحات للبحوث والدراسات، المجلد12، العدد2، الجزائر، 2019م.

23- مهدي رضا، "**الجرائم السيبرانية وآليات مكافحتهل في التشريع الجزائري**"، مجلة إليزا للبحوث والدراسات، المجلد6، العدد2، الجزائر، 2021م.

✓ الملتقيات:

1- عبد الرحمان صالحي ولبنى سويقات، "**تكنولوجيا الحاسوب والعملية التعليمية الجامعية**"، الملتقى الوطني الثاني حول الحاسوب وتكنولوجيا المعلومات في التعليم العالي، ورقلة، الجزائر، 5 ـ 6 مارس 2014م.

✓ المواقع الإلكترونية:

1- أنشطة فرنسا في مجال مكافحة الجرائم الإلكترونية (9 كانون الثاني/ يناير 2025)، تاريخ الإطلاع: 2025/05/24م، على الساعة: 9:51.

https//: www.diplomatie.gouv.fr

2- الإدارة العامة للشرطة الدولية، تاريخ الإطلاع 2025/04/10م، على الساعة: 21:36.

https://www.moi.gov.sa

✓ المعاجم:

1- محمد بن مكرم علي أبو الفضل جمال الدين إبن منظور الأنصاري، "لسان العرب"، ط1، المجلد2، دار إحياء التراث العربي، بيروت، لبنان، 1988م.

ـ إبن منظور، "لسان العرب"، ط3، الجزء3، دار إحياء التراث العربي، بيروت، لبنان، 1999م.

فهرس المحتويات

المحتوى	رقم الصفحة
شكر وعرفان	/
إهداء	/
مقدمة	أ - ج
الفصل الأول: الإطار المفاهيمي والقانوني للجريمة السيبرانية:	6 - 36
المبحث الأول: ماهية الجريمة السيبرانية	8 - 21
المطلب الأول: الجانب التاريخي	8 - 13
الفرع الأول: التطور التاريخي للحاسوب	8 - 10
الفرع الثاني: التطور التاريخي للأنترنت	10 - 12
الفرع الثالث: التطور التاريخي للجريمة السيبرانية	12 - 13
المطلب الثاني: مفاهيم حول الجريمة السيبرانية وخصائصها	13 - 21
الفرع الأول: مفاهيم حول الجريمة السيبرانية	13 - 19
الفرع الثاني: خصائص الجريمة السيبرانية	19 - 21
المبحث الثاني: أركان وأنواع الجريمة السيبرانية	22 - 28
المطلب الأول: أركان الجريمة السيبرانية	22 - 24
الفرع الأول: الركن الشرعي	22
الفرع الثاني: الركن المادي	22 - 24
الفرع الثالث: الركن المعنوي	24
المطلب الثاني: أنواع الجريمة السيبرانية	24 - 29
الفرع الأول: جريمة السرقة الإلكترونية	25
الفرع الثاني: جريمة الإحتيال والنصب	25 - 26
الفرع الثالث: جريمة إتلاف المعلومات	26 - 27
الفرع الرابع: جريمة تزوير المعلومات	27 - 28
الفرع الخامس: جريمة غسيل الأموال	28 - 29
المبحث الثالث: المجرم المعلوماتي	29 - 35
المطلب الأول: التعريف بالمجرم المعلوماتي وسماته	29 - 32
الفرع الأول: تعريف المجرم المعلوماتي	29 - 30
الفرع الثاني: سمات المجرم المعلوماتي	31 - 32

المطلب الثاني: دوافع الإجرام المعلوماتي	32 ـ 35
الفرع الأول: تحقيق الربح المادي	33
الفرع الثاني: الأحقاد الشخصية والرغبة في الإنتقام	33
الفرع الثالث: دوافع سياسية وأيديولوجية	34
الفرع الرابع: المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات	34
الفرع الخامس: الرغبة في التعلم	34 ـ 35
الفصل الثاني: الآليات والجهود الدولية لمكافحة الجرائم السيبرانية:	37 ـ 71
المبحث الأول: آليات التعاون الدولي لمكافحة الجرائم السيبرانية	39 ـ 52
المطلب الأول: الإتفاقيات والمعاهدات الدولية في مكافحة الجرائم السيبرانية	39 ـ 46
الفرع الأول: إتفاقية بودابست	39 ـ 42
الفرع الثاني: الجهود المبذولة على مستوى هيئة الأمم المتحدة	42 ـ 44
الفرع الثالث: المعاهدة الأوروبية لمكافحة الجرائم السيبرانية	44 ـ 46
المطلب الثاني: الآليات الأمنية والقضائية في مواجهة الجرائم السيبرانية	46 ـ 52
الفرع الأول: جهود المنظمة الدولية للشرطة الجنائية "الأنتربول"	46 ـ 48
الفرع الثاني: تسليم المجرمين	48 ـ 50
الفرع الثالث: المساعدة الدولية القضائية	50 ـ 52
المبحث الثاني: آليات التعاون العربي لمكافحة الجرائم السيبرانية	52 ـ 63
المطلب الأول: الجهود العربية في مكافحة الجريمة السيبرانية	52 ـ 58
الفرع الأول: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات	52 ـ 53
الفرع الثاني: جهود دولة الإمارات العربية المتحدة	44 ـ 55
الفرع الثالث: جهود المملكة العربية السعودية لمكافحة الجرائم السيبرانية	55 ـ 57
الفرع الرابع: جهود المنظة الدولية للشرطة القضائية "اللإريبول"	57 ـ 58
المطلب الثاني: سياسة المشرع الجزائري لمكافحة الجرائم السيبرانية	59 ـ 63
الفرع الأول: الحماية بموجب الدستور	59 ـ 60
الفرع الثاني: الآليات القانونية الموضوعية	60 ـ 61
الفرع الثالث: الآليات الموضوعية الإجرائية	61 ـ 63
المبحث الثالث: الصعوبات التي تواجه التعاون الدولي لمكافحة الجرائم السيبرانية وسبل التغلب عليها	63 ـ 70
المطلب الأول: مشكلات التعاون الدولي لمكافحة الجرائم السيبرانية	64 ـ 67

الفرع الأول: عدو وجود نموذج موحد للنشاط الإجرامي	64
الفرع الثاني: تنوع وإختلاف النظم القانونية الإجرائية	64 ـ 65
الفرع الثالث: التجريم المزدوج	65
الفرع الرابع: عدم وجود معاهدات ثنائية أو جماعية	65
الفرع الخامس: إشكالية الإختصاص القضائي	66
الفرع السادس: الصعوبات التي تواجه الجهود الدولية في مجال قنوات الإتصال	66
الفرع السابع: الصعوبات الخاصة بالمساعدات القضائية الدولية	67
المطلب الثاني: سبل التغلب عى مشكلات التعاون الدولي	67 ـ 70
الفرع الأول: حل عقبة عدم وجود نموذج موحد للنشاط الإجرامي	67
الفرع الثاني: حل عقبة تنوع وإختلاف النظم الإجرائية	67 ـ 68
الفرع الثالث: ضرورة إبرام إتفاقيات دولية ثنائية كانت أو جماعية	68 ـ 69
الفرع الرابع: حل عقبة الإختصاص في الجرائم الأنترنتية	69
الفرع الخامس: حل عقبة عدم وجود قنوات إتصال	69
الفرع السادس: حل العقبة المتعلقة بالمساعدات القضائية الدولية	70
خاتمة	72 ـ 74
قائمة المصادر والمراجع	75 ـ 82
الفهرس	83 ـ 85
الملخص	/

الملخص:

تعد الجرائم السيبرانية من الجرائم المستحدثة التي عرفها عصرنا الحالي لإرتباطها بالحاسوب وشبكة الأنترنت التي هي في تطور سريع إذ أصبحت هذه الجرائم تشكل خطراً على حياة الأفراد والمؤسسات حيث تميزت هذه الجريمة بأنها عابرة للحدود إضافة إلى أنّها صعبة الإكتشاف والإثبات حيث يقوم بهذه الجرائم مجرمو المعلومات الذين يتمتعون بالذكاء والمهارة، ونظراً لطبيعة هذه الجرائم التي تتسم بالهدوء لم تعد الدولة لوحدها قادرة على مجابهة هذا الخطر لذا وجب على الدول أن تتعاون فيما بينها من خلال التعاون الأمني والقضائي ووضع إتفاقيات وإستحداث قوانين جديدة كل هذا للتصدي للجرائم السيبرانية التي أصبحت هاجس العصر.

Summary:

Cybercrimes are newly emerging crimes that have come to be recognized in our current era due to their association with computers and the rapidly evolving internet. These crimes pose a threat to the lives of individuals and institutions as they are characterized by their cross-border nature, making them difficult to detect and prove. Cybercriminals, who are skilled and intelligent, perpetrate these offenses. Given the quiet nature of these crimes, it is no longer possible for a state to confront this danger alone; therefore, countries must cooperate through security and judicial collaboration, establishing agreements and creating new laws, all to combat cybercrimes that have become a concern of our time.