وزارة التعليم العالي والبحث العلمي
جامعة عباس لغرور –خنشلة–
كلية الحقوق و العلوم السياسية

قسم الحقوق
نيابة العمادة للدراسات وشؤون الطلبة

الجرائم الإلكترونية والأمن السيبيراني في الأتفاقيات الدولية والتشريع الجزائري

مذكرة مكملة لنيل شهادة الماستر في الحقوق تخصص: قانون جنائي

إعداد الطلبة:
- لعور مرزوق
- تازولت أكرم سيف الإسلام

إشراف الأستاذ:
- أ/د. بولقواس سناء

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة الاصلية	الصفة
تافرونت عبد الكريم	أستاذ التعليم العالي	جامعة عباس لغرور –خنشلة–	رئيسا
بولقواس سناء	أستاذ التعليم العالي	جامعة عباس لغرور –خنشلة–	مشرفا و مقررا
عثماني مريم	أستاذ محاضر أ	جامعة عباس لغرور –خنشلة–	عضوا مناقش

السنة الجامعية:2024/2023


بسم الله الرحمن الرحيم

شكر وعرفان

أتقدم بداية بالشكر "هلل سبحانه وتعالى" الذي وفقني لإنجاز هذا

العمل كما أتقدم بالشكر الى الأستاذة المشرفة البروفيسورة "بولقواس سناء"

التي لم تبخل علينا بتوجيهاتها ونصائحها القيمة.

الى أعضاء لجنة المناقشة الذين تفضلوا علي بقراءة ومناقشة

وتصويب هذه المذكرة.

الى جميع من قدم لي يد المساعدة من قريب أو من بعيد.

المقدمة

مقدمة:

تعد الجرائم الإلكترونية والأمن السيبراني من أبرز التحديات التي تواجه المجتمعات الحديثة في ظل التطور التكنولوجي المتسارع والتحول الرقمي الكبير الذي يشهده العالم. فمع تزايد استخدام التكنولوجيا في الحياة اليومية، أصبحت الجرائم الإلكترونية تهدد الأمن والاستقرار الاجتماعي والاقتصادي للدول. إذ تشمل هذه الجرائم أنواعًا متنوعة مثل الاحتيال المالي، والاختراقات السيبرانية، وسرقة الهوية، والابتزاز الرقمي، ونشر البرمجيات الخبيثة، وغيرها، مما يؤدي إلى خسائر مالية هائلة وتأثيرات سلبية على الاقتصاد والثقة في النظم الرقمية.

وفي هذا السياق، يلعب الأمن السيبراني دورًا حيويًا في حماية الأنظمة الإلكترونية والبيانات من هذه التهديدات الإلكترونية. فهو يشكل الدرع الواقي الذي يسعى لتحسين قدرة الدول والمؤسسات على اكتشاف واحتواء ومكافحة الهجمات الإلكترونية. وبتطبيق استراتيجيات الأمن السيبراني الفعّالة، يمكن تقليل تأثير الجرائم الإلكترونية والحد من الاختراقات والاحتيالات السيبرانية.

إلى جانب ذلك، تعزز الاتفاقيات الدولية التعاون في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني عبر الحدود. فهي تسهم في تطوير إطار قانوني دولي يوفر أسسًا قانونية قوية لمكافحة الجرائم الإلكترونية وتعزيز التعاون بين الدول في هذا المجال. ومن خلال توحيد الجهود وتبادل المعلومات والخبرات، يمكن تعزيز فعالية الاستجابة للتهديدات السيبرانية وتعزيز الأمن الإلكتروني على المستوى العالمي.

بالتالي، يظهر أن الربط بين الأمن السيبراني والجرائم الإلكترونية لا يقتصر فقط على حماية الأنظمة والبيانات، بل يتعدى ذلك ليشمل التعاون الدولي وتطوير الإطار القانوني العالمي، مما يسهم في تعزيز الأمن والاستقرار الإلكتروني في عصر التكنولوجيا المتقدمة.

وفي هذه المذكرة تتناول دراسة شاملة للجرائم الإلكترونية والأمن السيبراني في الاتفاقيات الدولية والتشريع الجزائري. سيتم استعراض أبرز الاتفاقيات الدولية المتعلقة بهذا المجال، مع تحليل للتشريع الجزائري والجهود المبذولة لتعزيز الأمن السيبراني. سيتم أيضًا تقديم توصيات لتحسين وتطوير الإطار القانوني والمؤسسي في الجزائر لمواجهة هذه التحديات بفعالية.

الأهمية:

تتمثل أهمية هذه المذكرة في عدة نقاط:

- تسليط الضوء على مفهوم الجرائم الإلكترونية والأمن السيبراني: من خلال تحليل وتوضيح هذين المفاهيم، يتم فهم طبيعة التهديدات الإلكترونية وأهمية الحماية السيبرانية في العصر الرقمي.
- استعراض الاتفاقيات الدولية ذات الصلة: يسلط الضوء على الاتفاقيات الدولية المتعلقة بمكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني، مما يساهم في فهم كيفية التعاون الدولي في هذا المجال وتطوير إطار قانوني عالمي.
- تحليل التشريع الجزائري: يتيح فحص التشريع الجزائري الحالي وفهم مدى توافقه مع المعايير الدولية والتحديات التي تواجه البلاد في مجال مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني.
- تقديم التوصيات: بناءً على التحليل الشامل، يتم تقديم توصيات عملية لتحسين وتطوير الإطار القانوني والمؤسسي في الجزائر، مما يساهم في تعزيز القدرة على مكافحة التهديدات الإلكترونية وحماية الأنظمة والبيانات الحساسة.

الأهداف:

أهداف دراستنا تتمثل في:

- توضيح مفاهيم الجرائم الإلكترونية والأمن السيبراني: تهدف المذكرة إلى توضيح مفاهيم الجرائم الإلكترونية والأمن السيبراني بشكل دقيق وشامل.
- استعراض جهود الدولية والإقليمية: تقوم دراستنا بمراجعة وتحليل الجهود التي تبذلها الدول والمنظمات الإقليمية لمكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني.
- تقييم التشريعات والسياسات: تقدم المذكرة تقييمًا للتشريعات والسياسات المتعلقة بالجرائم الإلكترونية والأمن السيبراني في الاتفاقيات الدولية والتشريع الجزائري.
- تحليل التحديات والفرص: تسعى في دراستنا إلى تحليل التحديات التي تواجه جهود مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني، وتحديد الفرص المتاحة لتعزيز التعاون والتنسيق الدولي والإقليمي.
- تقديم التوصيات: تختتم المذكرة بتقديم توصيات عملية لتعزيز جهود مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني، بناءً على الدروس المستفادة من الخبرات الدولية والإقليمية والتشريعات المحلية.

أسباب إختيار الموضوع:

الأسباب الذاتية:

اختيارنا لموضوع دراستنا ينبع من اهتمامنا العميق بهذا المجال المتعلق بالظاهرة الإلكترونية والتطور السريع لها. تعتبر هذه الظاهرة إحدى أبرز سمات المجتمع المعلوماتي، حيث تفرض علينا معرفة كل ما يترتب عن هذا التطور من تبعات. من بين هذه التبعات، تبرز ظاهرة الجريمة الإلكترونية، التي تشكل تحديًا كبيرًا يستدعي الدراسة والتحليل لفهم أبعادها وتأثيراتها على الأفراد والمؤسسات والمجتمعات ككل. هذا الاهتمام يدفعنا للغوص في تفاصيل هذا المجال المعقد، واستكشاف الجهود المبذولة لمكافحته على المستويين الوطني والدولي، بهدف المساهمة في إثراء المكتبة القانونية وتقديم حلول عملية لمواجهة هذه التحديات.

الأسباب الموضوعية:

الأهمية العالمية: الجرائم الإلكترونية أصبحت تهديدًا عالميًا يؤثر على الأفراد والشركات والحكومات. دراسة هذا الموضوع تساعد في فهم التحديات العالمية وكيفية التصدي لها من خلال التعاون الدولي والتشريعات.

التطور التكنولوجي: التكنولوجيا تتطور بسرعة، مما يزيد من فرص ووسائل ارتكاب الجرائم الإلكترونية. البحث في هذا المجال يساهم في مواكبة التطورات التكنولوجية وتقديم حلول فعّالة لمكافحة هذه الجرائم.

التعاون الدولي: الجرائم الإلكترونية غالبًا ما تتجاوز الحدود الوطنية، مما يستدعي تعاونًا دوليًا لمكافحتها. دراسة الاتفاقيات الدولية توفر فهمًا لكيفية تنظيم التعاون الدولي وتنسيق الجهود بين الدول لمواجهة هذه التحديات بشكل موحد.

التشريعات الوطنية: البحث في التشريع الجزائري يقدم نظرة معمقة حول كيفية تعامل الجزائر مع الجرائم الإلكترونية وما هي القوانين والإجراءات المتبعة. هذا يمكن أن يكون مفيدًا لتقييم فعالية هذه التشريعات واقتراح تحسينات إذا لزم الأمر، مما يساهم في تطوير الأطر القانونية المحلية.

حماية الأفراد والمؤسسات: الفهم العميق لموضوع الجرائم الإلكترونية يساعد في تطوير استراتيجيات لحماية الأفراد والمؤسسات من هذه التهديدات. يمكن أن يساهم البحث في تحسين الوعي الأمني وتقديم توصيات عملية لتعزيز الأمن السيبراني على مستوى الأفراد والشركات.

الاهتمام الأكاديمي والبحثي: هذا الموضوع يجذب اهتمام الأكاديميين والباحثين نظرًا لتأثيره الكبير على مختلف مجالات الحياة. البحث في هذا المجال يساهم في تطوير المعرفة

الأكاديمية وإثراء الأدبيات العلمية المتعلقة بالجرائم الإلكترونية والأمن السيبراني، مما يعزز الفهم العام والتطور العلمي في هذا المجال.

التحديات القانونية والتنظيمية: فهم التحديات القانونية والتنظيمية المرتبطة بالجرائم الإلكترونية يساعد في تحليل الفجوات القانونية والبحث عن حلول لتطوير الأطر القانونية الحالية، مما يساهم في تعزيز الأمن السيبراني بشكل عام وتحقيق استقرار قانوني أكبر.

التوعية والتثقيف: دراسة هذا الموضوع يمكن أن تساعد في زيادة التوعية والتثقيف حول المخاطر السيبرانية وكيفية الوقاية منها، مما يؤدي إلى مجتمع أكثر أمانًا على المستوى الإلكتروني ويقلل من مخاطر التعرض للهجمات السيبرانية.

اختيار هذا الموضوع يعكس وعيًا بأهمية التحديات الراهنة ورغبة في المساهمة في إيجاد حلول لها على الصعيدين المحلي والدولي، مما يجعله موضوعًا ذا قيمة كبيرة من الناحية الأكاديمية والعملية.

الإشكالية:

وبهدف الرد على الاشكالية الاساسية لدراستنا والتي تتمثل في :

كيف يمكن للتشريعات مواجهة تحديات الجرائم الإلكترونية وضمان الأمن السيبراني في عصر التكنولوجيا المتقدمة؟

وللاجابة عن الاشكالية الجوهرية لابد من طرح بعض التساؤلات الفرعية المهمة المتمثلة في:

1.ماهو مفهوم الجريمة الالكترونية وماذا يقصد بالامن السيبراني؟

2.ما هي التحديات التي تواجه تطوير التشريعات الوطنية لمكافحة الجرائم الإلكترونية؟

3.كيف مواجهة التهديدات ومخاطر حوادث الامن السيبراني؟

المنهج المتبع:

بناء على ما تقدم فقد اعتمدنا في دراستنا هذه على مناهج نرى أنها تتلاءم وطبيعة الموضوع، حيث استعنا بالمنهج الإستقرائي والذي يظهر في استقراءنا للمواد القانونية ذات العلاقة التي تفرض بعد ذلك تحليلها من خلال استعانتنا بالمنهج التحليلي تباعا، أما المنهج الوصفي فيظهر في تناولنا الاطار المفاهيمي الموضوع الدراسة

الخطة:

للإجابة عن الإشكالية السابقة ارتأينا تقسيم مذكرتنا لفصلين تناولنا في الأول مفهوم الجريمة الالكترونية والامن السيبراني وقد أبرزنا في المبحث الأول مفهوم الجريمة الالكترونية، وتناولنا في المبحث الثاني مفهوم الامن السيبراني، اما في الفصل الثاني قم بتسليط الضوء على أليات مكافحة الجرائم الالكترونية وحماية الامن السيبراني وقد تناولنا في المبحث الاول الجهود الدولية والاقليمية في مكافحة الجرائم السيبرانية، وفي المبحث الثاني تطرقنا الى أليات مكافحة الجرائم السيبرانية في ظل التشريع الجزائري.

الفصل الأول

الإطار المفاهيمي للجرائم الإلكترونية والأمن السيبراني

المبحث الأول:

ماهية الجريمة الإلكترونية.

في ظل التطور التكنولوجي السريع الذي يشهده العالم اليوم، أصبحت الجريمة الإلكترونية واحدة من التحديات الرئيسية التي تواجه المجتمعات الحديثة. تنتشر هذه الجرائم بشكل واسع عبر الإنترنت، مستهدفة الأفراد والمؤسسات على حد سواء. مفهوم الجريمة الإلكترونية يشمل كافة الأنشطة غير القانونية التي تتم عبر الإنترنت أو باستخدام الأجهزة الرقمية، مثل الاختراق، والاحتيال الإلكتروني، وسرقة الهوية، ونشر البرمجيات الخبيثة. في هذا المبحث، سنستعرض مفهوم الجريمة الإلكترونية بشكل مفصل، مع تسليط الضوء على خصائصها، وأركانها في المطلب الاول، وأبرز أنواعها ومراحل تطورها في المطلب الثاني، لتوفير فهم شامل لهذه الظاهرة المتنامية وتأثيراتها على المجتمع.

المطلب الأول:

مفهوم الجريمة الإلكترونية .

أصبحت الجريمة الإلكترونية موضوعًا واسعًا ومعقدًا، ورغم صعوبة إيجاد تعريف شامل ودقيق لها، إلا أن اجتهاد الفقهاء والباحثين قد أدى إلى تطوير عدة تعريفات مختلفة. تتباين هذه التعريفات بناءً على منظور كل فئة؛ حيث ركز البعض على الجانب التقني والفني، بينما تناول الآخرون الجانب القانوني.ومن أجل مفهوم شامل للجريمة لا بد من تعريفها من كل هذه الجوانب وهذا ماسنبرزه الفرع الأول، وبيان أركانها الفرع الثاني والتطرق الى خصائصها في الفرع الثالث.

الفرع الأول:

تعريف الجريمة الإلكترونية.

في عصر الرقمنة الحديث، أصبحت التكنولوجيا جزءًا لا يتجزأ من حياتنا اليومية، حيث يعتمد الكثير من الأنشطة الحياتية والتجارية على الإنترنت والأنظمة الرقمية. ومع تزايد الاعتماد على التكنولوجيا، زادت أيضًا التحديات والتهديدات التي تواجهها المجتمعات الدولية والمؤسسات، ومن بين هذه التحديات تبرز الجريمة الإلكترونية كواحدة من أخطر الظواهر الجرمية التي تهدد الأمن السيبراني، ومنه نسعى في فرعنا هذا ابراز تعريف الجريمة الالكترونية، وفقا للفقهاء، وحسب ماعرفه المشرع الجزائري، وسنتطرق الى تعريف الجريمة الالكترونية حسب اتفاقية مجلس أوربا للجريمة الإلكترونية لعام 2001.

- **اولا: التعريف الفقهي**

تعرف الجريمة الالكترونية على انها(عبارة عن نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي. كما يعرفها البعض الآخر بأنها تصرف غير مشروع يؤثر في الاجهزة والمعلومات الموجودة عليها).[1] يعكس هذا التعريف اتساع نطاق الجرائم الإلكترونية، إذ يشمل ليس فقط الأفعال التي تستهدف الأنظمة الإلكترونية والأجهزة، ولكن أيضًا تلك التي تستخدم التكنولوجيا كأداة لتنفيذ جرائم تقليدية بطرق جديدة وأكثر تعقيدًا. من جهة أخرى، يعرّفها البعض بأنها تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها، مما يبرز الأثر الضار المباشر لهذه الجرائم على البيانات والتكنولوجيا. يوضح كلا التعريفين الأهمية البالغة لاتخاذ تدابير قانونية وتقنية فعالة لمكافحة هذه الأنشطة وحماية البنية التحتية الرقمية.

[1] عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية مصر 2006 ، ص ص 01 -02

كما يعرفها البعض الآخر بأنها(تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها).[1] إن هذا التعريف يسلط الضوء على جوانب محددة من الجرائم الإلكترونية، حيث لا يقتصر الضرر على سرقة المعلومات أو اختراق الأنظمة فحسب، بل يمتد ليشمل أي تأثير سلبي على سلامة الأجهزة والمعلومات.

لقد أنقسم أنصار تعريف الجريمة من الجانب التقني والفني فالبعض استند إلى موضوع الجريمة والبعض الآخر إلى وسيلة الجريمة

- **1- أهم التعريفات التي استندت على موضوع الجريمة**

انها "(نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب)[2] ، هذا التعريف يركز على الأفعال التي تستهدف البيانات المخزنة، مما يُبرز الحاجة إلى حماية المعلومات الرقمية من التلاعب والاختراق.

ويمكن تعريفها ايضا بانها (كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات او نقل هذه البيانات)"[3]، يقدم هذا التعريف نظرة أوسع للجرائم الإلكترونية، مشدداً على أهمية حماية العمليات الآلية للبيانات ووسائل نقلها من الأنشطة غير القانونية.

او تعرف ايضا (" أي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات) [4] ، يعزز هذا التعريف مفهوم أن الجرائم الإلكترونية يمكن أن

[1] نفس المرجع، ص ص 01- 02 .

[2] هشام محمد رستم: الجوانب الاجرائية للجرائم المعلوماتية – مكتبة الآلات الحديثة اسيوط 1994، ص 31 .

[3] هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، الطبعة الأولى، 1992 ، ص 20

[4]هشام محمد رستم: الجوانب الاجرائية للجرائم المعلوماتية مكتبة الآلات الحديثة اسيوط 1994، ص 30

تشمل الجرائم التقليدية عندما تُنفذ باستخدام تكنولوجيا المعلومات، مما يوضح التداخل بين الجرائم التقليدية والتكنولوجيا الحديثة.

او يمكن تعريفها انها (" الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة الى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر "). يركز هذا التعريف على الجوانب الفنية للجريمة الإلكترونية، ويبرز التحديات التقنية المرتبطة بإدخال البيانات المزورة والتلاعب بالأنظمة.

- **2/. أهم التعريفات التي استندت على وسيلة الجريمة**

فان أنصار هذا الاتجاه ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة، وبالتالي تعرف على أنها("فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" كما تعرف بأنها كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب")[1] وكذلك تعرف بأنها ("الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا")، وانها (" كل فعل او امتناع من شانه الاعتداء على الأمواج المادية او المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية")[2] يعتبر هذا التعريف الأخير الرأي الراجح لتبنيه من قبل العديد من الباحثين والدارسين[3] نظرا الشموليته بحيث يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية، وهذه التعريفات المتعددة تسلط الضوء على تنوع وتعقيد الجريمة الإلكترونية وتعكس تطورها في ظل تقدم التكنولوجيا. إن استخدام الحاسوب كأداة رئيسية في ارتكاب الجريمة يبرز أهمية البنية التحتية الرقمية كوسيلة للجرائم.

[1] هشام محمد رستم ، المرجع السابق، ص 31

[2] هدى قشقوش، المرجع السابق، ص22.

[3] هشام محمد رستم ، المرجع السابق ، ص 35

- **ثانيا: تعريف المشرع الجزائري للجريمة الالكترونية**

المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وعرفها بموجب المادة الثانية من القانون 09 – 04 [1]على أنها(جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية. ")[2]

ويلاحظ على هذا التعريف ما يلي:

يشير هذا التعريف إلى الجرائم التي تستهدف مباشرة الأنظمة المستخدمة في معالجة البيانات والمعلومات. هذه الأنظمة قد تشمل قواعد البيانات، الخوادم، والشبكات التي تدير عمليات

[1] القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجزائر

[2] القانون رقم 09-04 : المادة 2 : يقصد في مفهوم هذا القانون بما يأتي:

– 1الجرائم المتصلة بتكنولوجيات الإعلام والاتصال :

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين

ج – معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها،

د – مقدمو الخدمات:

1 – أي كيان عام أو خاص يقدم المستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و / أو نظام للاتصالات

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو المستعمليها

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

حيوية للمؤسسات والأفراد. الجرائم التي تتعلق بهذا الجانب قد تتضمن القرصنة، تدمير البيانات، أو تعطيل الخدمات.

وايضا يعكس هذا التعريف أن الجريمة الإلكترونية ليست محدودة فقط بالجرائم التي تستهدف الأنظمة التقنية بشكل مباشر، بل تشمل أيضاً الجرائم التقليدية التي يتم تسهيلها أو ارتكابها من خلال استخدام تكنولوجيا المعلومات والاتصالات. يشمل ذلك الاحتيال الإلكتروني، التصيد الاحتيالي، ونشر البرمجيات الضارة.

هذا التعريف يعزز الفهم الشامل للجريمة الإلكترونية بدمج الجرائم التي تستهدف البنية التحتية التقنية مباشرةً وتلك التي تستخدم هذه البنية التحتية كوسيلة لتحقيق أهداف غير قانونية.

- **ثالثا: تعريف الجريمة الالكترونية في اتفاقية مجلس أوربا للجريمة الإلكترونية لعام 2001**

تم التوقيع على هذه الاتفاقية في 23 نوفمبر 2001 في بودابست وتضم في عضويتها 45 دولة أوربية و18 دولة من خارج أوربا حتى تاريخ 5/10/2014 [1]، وعرفت الاتفاقية جرائم الحاسب الآلي في الفصل الثاني بأنها الجرائم ضد السرية والنزاهة وتوافر البيانات وأنظمة الحاسب الآلي في المواد من 2 إلى 16 حيث تم بالترتيب تعريف الدخول غير المشروع، الاعتراض غير القانوني، التدخل في البيانات التدخل في النظام إساءة استخدام أجهزة. [2]

ثانياً: الجرائم ذات الصنة بالحاسوب الجرائم المتعلقة بالتزوير والجرائم المتعلقة بالعش،

ثالثاً: الجرائم المتعلقة بالمحتوى الجرائم المتعلقة بالمواد الإباحية عن الأطفال.

[1] ز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتي ومكافحتها، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الوقاية و المكافحة، يومي 16-17 نوفمبر 2015 كلية الحقوق جامعة بسكرة، الجزائر

[2] يوسف صعيدي، الجريمة المرتكبة عبر الانترنيت، مذكرة ماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسة، جامعة مولود معمري، تيزي وزو، 2013، ص ص 40-41.

رابعاً: الجرائم المتعلقة بانتهاك حقوق الطبع والحقوق المجاورة: الجرائم المتعلقة بالتعدي على حقوق المؤلف والحقوق المجاورة،

خامساً: المسؤولية الإضافية المحاولة والعون والتحريض والمسؤولية المؤسسية في المادة (12).[1]

وترتيبا على كل هذه التعاريف الفقهية والتشريعية، يمكننا تعريف الجريمة الالكترونية بأنها كل سلوك غير مشروع يمس بالنظام المعلوماتي المادي أو المعنوي " او كل سلوك غير مشروع يقع على النظام المعلوماتي او بواسطته وبمس بالأشخاص او الاموال او امن الدولة أي أن الجريمة الالكترونية على سبيل الجرائم التقليدية تعرف من خلال أركانها أي توفر القصد الجنائي لارتكاب هذه الجريمة والركن المادي للجريمة وركنها القانوني

الفرع الثاني:

أركان الجريمة الإلكترونية:

من أجل فهم هذا النوع من الجرائم بعمق وتحديد الإجراءات القانونية اللازمة لمواجهتها، من الضروري تحليل أركان الجريمة الإلكترونية الأساسية. تتكون هذه الأركان عادةً من الركن المادي، والركن المعنوي، والركن القانوني.

يعكس كل ركن من هذه الأركان جانبًا مختلفًا من الجريمة، مما يساعد على تكوين صورة كاملة عن كيفية حدوثها وأثرها وأفضل السبل لمكافحتها.وهذا ما سنتناوله في فرعنا هذا.

- **اولا: الركن الشرعي**

يقصد بالركن الشرعي النص القانوني الذي يجعل النشاط الإجرامي غير مشروع. ووفقاً لمبدأ شرعية الجرائم والعقوبات، لا يمكن متابعة أي شخص عن أي فعل ما لم يكن

[1] اتفاقية بودابست المتعلقة بالاجرام المعلوماتيconvention sur la cybercriminalité Budapest ، الموقعة في23 نوفمبر 2001

هناك نص يجرمه، والذي ينص على أنه "لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون"[1]. هذا يثير التساؤل حول مدى تطبيق مبدأ الشرعية على الجرائم الإلكترونية[2].

مع تطور الأنظمة المعلوماتية، ظهرت أفعال غير مشروعة جديدة تختلف بخصائصها عن الجرائم التقليدية. لذلك، سعت العديد من الدول إلى وضع تشريعات عقابية لمكافحة الجرائم الإلكترونية، بهدف منع إفلات المجرمين من العدالة وضمان حماية الشبكات المعلوماتية. ومن بين هذه التشريعات، ما نص عليه المشرع الجزائري في قانون العقوبات في القسم المخصص لهذه الجرائم، تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، من المادة 394 مكرر إلى المادة 394 مكرر 7، بالإضافة إلى المادة 394 مكرر 8 التي أضيفت إثر تعديل قانون العقوبات.[3]

- **ثانيا: الركن المادي**

يُعرف الركن المادي للجريمة كالمظهر الظاهري للجريمة، ويتمثل في سلوك إجرامي معين مطلوب من القانون كشرط لتطبيق العقوبة على هذه الجريمة، مع اشتراط تحقيق نتيجة ضارة للسلوك الإجرامي كشرط أساسي لتوجيه العقوبة[4].

[1] مبدأ الشرعية هو مبدأ عالمي نصت عليه أغلب التشريعات، وقد نص عليه المشرع الجزائري في المادة الأولى من قانون العقوبات.انظر :

عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، الجزء الأول، ديوان المطبوعات الجامعية، الجزائر، 1996، ص 78.

[2] عبد النور بشان الجوانب الموضوعية المعالجة الجريمة المعلوماتية، أطروحة دكتوراه، تخصص قانون جنائي و علوم جنائية، كلية الحقوق جامعة الجزائر 1 2017-2018، ص 68

[3] عبد النور بشان، الرجع السابق ، ص68

[4] خالد ممنوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009، ص 98

أ- السلوك الاجرامي

بالنسبة للجريمة الإلكترونية، يشمل السلوك المادي وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الإنترنت، بالإضافة إلى معرفة بداية هذا النشاط والشروع فيه ونتائجه. على سبيل المثال، يمكن للمرتكب تجهيز الكمبيوتر لتحقيق الجريمة عبر تثبيت برامج اختراق، أو يمكنه إعداد هذه البرامج بنفسه. لذلك، يجب تحديد ومعرفة نقطة بداية السلوك الإجرامي أو الشروع فيه، بالإضافة إلى فهم النتائج التي يحققها هذا السلوك[1].

يثير النشاط أو السلوك المادي عبر الإنترنت العديد من التساؤلات، خاصة فيما يتعلق ببدايته أو الشروع في ارتكاب الجريمة. هذا النشاط يختلف عن العالم المادي، حيث يتطلب ارتكاب الجريمة عبر الإنترنت وجود منطلق تقني، ودون ذلك لا يمكن للشخص حتى الوصول إلى الإنترنت، سواء كان بقصد ارتكاب الجريمة أو بمجرد التصفح أو الدخول في الاتصال المباشر مثل المحادثات وغيرها[2]

ب- النتيجة الاجرامية

النتيجة الإجرامية تشكل العنصر الثاني من عناصر الركن المادي للجريمة، ويمكن تعريفها على أنها الضرر الذي ينجم عن السلوك الإجرامي، سواء كان فعليًا أو تركيًا، أو يمكن أن تكون الأثر الخارجي الذي يحدث تغييرًا يعتد به القانون[3].

ومع ذلك، يثير الاستفسار مسألة مدى اعتبار الجريمة الإلكترونية كسلوك ونتيجة في العالم الافتراضي، أو ما إذا كان هناك تأثير يمتد لتحقيق النتيجة في العالم المادي. على سبيل المثال، إذا دخل الطبيب العامل في مستشفى إلى قاعدة البيانات لتغيير جرعة الدواء لقتل

[1] يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية الجزائر، 2018، ص 110

[2] خالد ممنوح إبراهيم ، المرجع السابق، ص 98

[3] يوسف خليل يوسف العفيفي الجرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير في القانون العام، كلية الشريعة والقانون الجامعة الإسلامية غزة 2013، ص 53

أحد المرضى[1]، فإن الطبيب هنا قد ارتكب اعتداءً على النظام المعلوماتي بتغيير المعلومات، مما أدى إلى تحقيق نتيجة في العالم المادي وهو قتل المريض. لذلك، يتضمن النشاط الإجرامي سلوكًا حقق به نتيجة من العالم الافتراضي من خلال اعتداء على المعلومات داخل نظام المعلومات، وامتد هذا التأثير ليحقق نتيجة في العالم المادي[2].

- **ثالثا: الركن المعنوي**

الإكتمال الإجرامي في أي جريمة يتطلب وجود إرادة إجرامية من الجاني تصاحب السلوك أو النشاط المادي. فلا يكفي لتحديد المسؤولية الجنائية أن يقوم الجاني بالتصرف بطريقة إجرامية، بل يجب أيضًا توفر نية داخلية تكمن في دوافعه ونواياه، وتظهر هذه النية في العالم الخارجي من خلال سلوك مادي، ويُعرف هذا الجانب النفسي للجريمة بالركن المعنوي[3].

الركن المعنوي في الجريمة الإلكترونية يتجلى من خلال توضيح الحالة النفسية للجاني والعلاقة بين ماديات الجريمة وشخصيته. يستند هذا المبدأ على صورتين أساسيتين. الصورة الأولى تتمثل في الاعتداء على أنظمة المعالجة الآلية، وتشمل الدخول والبقاء غير المشروع في أنظمة المعالجة الآلية للبيانات، والنوع الثاني يتمثل في الاعتداء على منتجات الإعلام الآلي مثل التزوير المعلوماتي.

[1] عبد النور بشان، الرجع السابق ، ص76

[2] المرجع نفسه ، ص76

[3] يوسف خليل يوسف العفيفي، الرجع السابق ، ص54

يقوم الركن المعنوي للجريمة الإلكترونية على وجود الإرادة السائدة لدى الجاني وتوجيه هذه الإرادة نحو القيام بأعمال غير مشروعة جرمها القانون، مثل انتحال شخصية شخص آخر عبر الإنترنت أو سرقة أرقام بطاقات الائتمان[1].

بناءً على ذلك، يتضح أن الأركان الأساسية للجريمة الإلكترونية تعتمد على الركن المعنوي، حيث لا تكتمل الجريمة الإلكترونية بدون وجوده. تعتبر الجريمة الإلكترونية نتيجة للتطور التكنولوجي، وقد أظهرت تحديات جديدة للتشريعات القانونية التقليدية، لذا سعت معظم دول العالم إلى إصدار قوانين وتشريعات جديدة لمواجهة هذا النوع من الجرائم[2].

الفرع الثالث:

خصائص الجريمة الالكترونية

تتميز الجريمة الالكترونية بطبيعة خاصة تميزها عن الجريمة التقليدية، ولذا أضحت هذه الخاصية بهذا النوع من الجرائم عدة سمات وحقائق سواء تتعلق الأمر بمرتكبيها أو ما يسمى بالمجرم المعلوماتي أو بالنسبة لحدودها باعتبارها جريمة ذات بعد عالمي[3] وعليه سنحاول البحث في خصائص الجريمة فيما يلي:

- **أولا: الجريمة الالكترونية جريمة عالمية الحدود**

من أهم الخصائص التي تميز الجريمة الالكترونية أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الانترنيت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، وبسبب السرعة الهائلة في تنفيذها وحجم الأموال والأشخاص المستهدفة من خلالها.

[1] يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير تخصص قانون دولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو 06-03-2013، ص 66

[2] نفس المرجع، ص 66

[3] سميرة معاشي، الجريمة المعلوماتية مجلة المفكرة العدد 17 جامعة محمد خيضر بسكرة، 2006، ص 409

ومن أهم القضايا التي أكدت هذه الخاصية[1]، قضية عرفت باسم مرض نقص المناعة المكتسبة إيدز،

وتتلخص وقائعها عام 1989، حيث قام أحد الأشخاص وهو "جوزيف بيب" بنسخ أحد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض الإيدز، لكن في الحقيقة يحتوي هذا البرنامج على فيروس يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل فيقوم الفاعل أو الجاني بطلب مبلغ مالي للحصول على عنوان الكتروني مضاد للفيروس، وفي الثالث من فبراير تم إلقاء القبض على الجاني في أوهايو بالولايات المتحدة الأمريكية

وطلبت المملكة المتحدة تسليم الجاني لإرسال البرنامج على أراضيها، وبالفعل تمت محاكمته أمام القضاء الانكليزي، إلا أن إجراءات محاكمته لم تستمر بسبب حالته العقلية[2]

وتثير خاصية عالمية الحدود للجريمة الالكترونية عدة آثار قانونية أهمها القانون الواجب التطبيق عليها، والقضاء المختص بها، فهل هو قانون الدولة التي وقع فيها النشاط الإجرامي أم الدولة التي يقيم فيها الجاني أو الدولة التي أضرت بمصالحها هذا التلاعب.

لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إبرام الاتفاقيات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم.[3]

[1] عائشة بن قارة مصطفى حجية الدليل الإلكتروني في مجال الاثبات الجنائي في القانون الجزائري و القانون المقارن دار الجامعة الجديدة الاسكندرية 2010، ص 45

[2] سوبر سفيان، الجرائم المعلوماتية رسالة لنيل شهادة الماجيستير في العلوم الجنائية والقانون الجنائي، كلية الحقوق جامعة أبو بكر بلقايد، تلمسان . الجزائر 2010، ص 12

[3] محمد حماد مرهج الهيتي الجريمة المعلوماتية (نماذج من تطبيقاتها) دار الكتب القانونية، الامارات، 2014

- **ثانيا: جرائم صعبة الإثبات:**

توصف الجرائم الإلكترونية بأنها خفية ومستترة في معظم الحالات، إذ قد لا يدرك الضحية وقوعها رغم تواجده على الشبكة. يعود ذلك إلى المهارات الفنية المتقدمة التي يمتلكها الجاني، مما يسمح له بتنفيذ جريمته بدقة من خلال إرسال فيروسات، أو سرقة الأموال والبيانات الخاصة، أو إتلاف المعلومات، أو التجسس، أو سرقة المكالمات وغيرها من الجرائم[1].

عادةً ما يتم اكتشاف هذه الجرائم بمحض الصدفة، وتشير الإحصاءات إلى أن نسبة الاكتشاف لا تتجاوز 1% منها، بينما يبلغ عن 15% فقط، ويصدر أحكام إدانة في خمس هذه الحالات المبلغ عنها. هذا يوضح الحاجة الملحة إلى خبراء في مجال المعلوماتية في التحقيق الجنائي لتسهيل عملية اكتشاف هذه الجرائم، وهو ما بادرت به الجزائر مؤخرًا[2].

من الواضح أن عدد الجرائم الإلكترونية المكتشفة قليل جدًا مقارنة بالجرائم التقليدية.[3] ففي النهاية، هذه الجرائم غالبًا ما تترك أثرًا ضئيلًا أو لا تترك أثرًا إلا بعد وقوعها.

- **ثالثا: جرائم ناعمة**

ما يميز الجريمة الإلكترونية ويجعلها تختلف عن الجرائم التقليدية هو طبيعتها الهادئة وعدم وجود العنف فيها. تتميز الجريمة الإلكترونية بهذه الخاصية لأنها لا تحتاج إلى استخدام القوة أو العنف المطلوبين في بعض الجرائم التقليدية، مثل السرقة باستخدام العنف أو التهديدات[4].

---

[1] حماد مرهج الهيتي الجريمة المعلوماتية (نماذج من تطبيقاتها) دار الكتب القانونية، الامارات، 2014،ص 99

[2] نجاة بن مكي السياسة الجنائية لمكافحة الجرائم المعلوماتية، دار الخلدونية الجزائر، 2017، ص 21

[3] نهلا عبد القادر المومني الجرائم المعلوماتية، الطبعة الأولى دار الثقافة للنشر والتوزيع، عمان، 2008، ص 54

[4] محمد حماد مرهج الهيئي، المرجع السابق، من 100

فالوسائل التي تُرتكب بها الجرائم الإلكترونية لا تتطلب إلا بضع لمسات على الأزرار لتنفيذها، وهذا يمكن الجاني من ارتكاب جرائم خطيرة دون الحاجة إلى استخدام العنف أو القوة.[1]

المطلب الثاني

مراحل تطور الجريمة الالكترونية وانواعها

من المعلوم أن هناك صعوبة في تحديد بداية معينة لنشوء الجرائم الإلكترونية ، حيث أن الحواسيب الإلكترونية كانت موجودة منذ فترة بعيدة ، ولكن تختلف عما هي عليه الحواسيب الحالية سواء من حيث الشكل أو السرعة والدقة والتطور الحالي الذي يعتبر نتاج لتطور كبير، ومن خلال هذا المطلب سنتناول في الفرع الاول نشاءة الجريمة الالكترونية مبرزين مراحل تطورها، اما في الفرع الثاني سنتطرق الى انواع الجريمة الالكترونية

الفرع الاول

تطور الجريمة الالكترونية

شهدت الجريمة الإلكترونية تطورًا كبيرًا مع التقدم التكنولوجي. بدأت بعمليات اختراق بسيطة وسرقة المعلومات، وتطورت إلى هجمات معقدة تشمل الاحتيال المالي ونشر البرمجيات الخبيثة. فهم مراحل هذا التطور يساعد على تطوير استراتيجيات فعالة لمكافحة التهديدات الإلكترونية المتزايدة، وهذا ما سنتطرق اليه في فرعنا هذا.

- **مراحل تطور الجريمة الالكترونية**

يُرجع البعض حدوث أول جريمة متصلة بالحاسوب إلى عام 1701م، عندما صمم جوزيف جاكوارد، صاحب مصنع للنسيج في فرنسا، لوحة إلكترونية كانت أول نموذج للوحة

[1] المرجع نفسه، ص 100

الحاسوب الحالية. قامت هذه اللوحة بتكرار مجموعة من الخطوات المستخدمة في حياكة أنواع من المنسوجات، مما أثار مخاوف بعض العاملين في المصنع من تأثيرها على وظائفهم، فقاموا بتخريبها[1].

بينما يرى البعض الآخر أن البداية الحقيقية لظاهرة الجرائم الإلكترونية كانت في عام 1958م، حين بدأ معهد ستانفورد الدولي للأبحاث في الولايات المتحدة الأمريكية رصد حالات إساءة استخدام الحاسوب بصورة منظمة. خلال التسعينيات من القرن العشرين، ومع انتشار الحواسيب والاعتماد عليها في شتى مجالات الحياة والأعمال اليومية، بدأت الجريمة الإلكترونية في النمو والبروز بشكل أكبر[2]. من أبرز الحالات المسجلة خلال هذه الفترة كانت جريمة سرقة بنك مينيسوتا الأمريكي عام 1966م، التي اعتُبرت أول سرقة إلكترونية تقع على بنك.

توالت المقالات الصحفية التي تناولت حالات أُطلق عليها جرائم الحاسوب (Computer Crime)أو الجرائم ذات الصلة بالحاسوب .(Computer-related Crime)[3] ورغم استمرار تطور ظاهرة الجريمة الإلكترونية خلال السبعينيات، كانت الحالات المسجلة قليلة. يعود ذلك إلى أن مكمن الخطر كان داخليًا، حيث كان العاملون على الأنظمة الحاسوبية هم الوحيدين الذين يستطيعون الوصول إليها مباشرةً، ولم يكن هناك اتصال خارجي بتلك الأنظمة. كما أن عدم الإبلاغ عن العديد من تلك الجرائم، بسبب حرص الشركات والوكالات على عدم اهتزاز الثقة بها وبأنظمتها، ساهم في قلة الحالات المسجلة. شهدت تلك الحقبة أيضًا بداية ظهور التشريعات والقوانين التي تُجرم بعض الممارسات المتعلقة بإساءة استخدام

[1] غادة العربي نصار: الإرهاب والجريمة الإلكترونية، ط1، العربي للنشر والتوزيع، القاهرة 2017، ص: 09

[2] هشام بشير: الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية والاستراتيجية، 2012، ص:07.

[3] الأشقر جبور منى ،القانون والانترنت: تحدي التكيف والضبط، مكتبة صادر ناشرون، بيروت،2008، ص 70

الحاسوب، مثلما حدث في السويد، التي اعتُبرت أول دولة تصدر قانونًا يُجرم بعض الأفعال المرتبطة بالحواسيب[1].

في عقد الثمانينيات، حدث تغير ملحوظ في التعامل مع ظاهرة الجريمة الإلكترونية من جانب الباحثين والعامة على السواء، بسبب ارتفاع عدد القضايا المتعلقة بإساءة استخدام الحاسوب. ازداد اهتمام الصحافة بهذه القضايا، مما جعل بعضها يؤرق المجتمع الدولي، مثل قضايا الاختراق، قرصنة البرمجيات، التلاعب في أنظمة النقد الإلكتروني، وانتشار الفيروسات. شهدت تلك الفترة الانطلاقة الأولى للقوانين والتشريعات الخاصة بحماية البرامج الحاسوبية، والتي أطلق عليها قوانين حماية الملكية الفكرية، واعتُبرت من القوانين الأكثر وضوحًا ونضجًا[2].

في تلك الفترة الزمنية، ظهر اهتمام عربي بظاهرة الجريمة الإلكترونية. تمثل ذلك في صدور العديد من الدراسات العلمية والمؤلفات العربية المتعلقة بالجريمة الإلكترونية، وعقد الندوات ذات الصلة، مثل ندوة أمن المعلومات في الحاسبات الآلية التي عُقدت في عام 1986م، وتبناها مركز المعلومات الوطني التابع لوزارة الداخلية السعودية.

شهدت التسعينيات والسنوات الأولى من القرن الحادي والعشرين تحولات في مجال الجريمة الإلكترونية، نتيجة تحول شبكة الإنترنت من شبكة أكاديمية إلى شبكة تُعنى بخدمة المجالات التجارية والفردية. بلغ عدد مستخدمي الإنترنت في عام 1996 حوالي 40 مليون مستخدم، وفي عام 2014 تجاوز عدد المستخدمين الثلاثة مليارات، مما أدى إلى خلق عبء كبير على المختصين بمكافحة الجريمة الإلكترونية. أدى هذا الوضع إلى ظهور مفهوم جديد

[1] مجاني باديس المعالجة الصحفية الأخبار الجريمة مجلة الحضارة الإسلامية، جوان، 2015، ص 33

[2] نفس المرجع، ص33

يُعرف بالجرائم العابرة، حيث يمكن للمجرمين تنفيذ مخططاتهم الإجرامية في دول متعددة دون الاكتراث بالحدود الدولية[1].

الفرع الثاني

انواع الجريمة الالكترونية

اختلف الفقه الجنائي حول تقسيم الجرائم الالكترونية، حيث قد يكون النظام المعلوماتي هو نفسه موضوع أو محل الجريمة الالكترونية ومن ناحية أخرى، قد يكون النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها.[2]ومن خلال فرعنا هذا نبرز انواع الجريمة الالكترونية، وتقسيماتها.

- **أولا: الجرائم الواقعة بواسطة النظام المعلوماتي**

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة وتنقسم هذه الجرائم بدورها إلى:

1. الجرائم الواقعة على الأشخاص:

رغم تطور الحياة اليومية للأفراد والمجتمع بفضل استعمالهم للفضاء الافتراضي إلا أنه أصبح سلاحا فتاكا في يد المجرمين للدخول إلى المعلومات الخاصة للأشخاص، وعليه ظهرت عدة أنواع خاصة من الجرائم الالكترونية الواقعة على الاشخاص كجريمة التهديد والمضايقة والملاحقة، خاصة عن طريق البريد الالكتروني بإرسال رسالة خاصة للترويع

[1] حنين، جورج إسحاق .دراسة عن الجرائم المعلوماتية والإلكترونية عبر شبكة الإنترنت وسبل مواجهتها. الإدارة المركزية، مركز المعلومات والتوثيق، ص 20

[2] صالح شنين الحماية الجزائية لبرامج الحاسب الآلي، دراسة مقارنة رسالة لنيل شهادة الماجيستير، جامعة بسكرة كلية الحقوق والعلوم السياسية2007-2008، ص:107

والتهديد أو عن طريق وسائل الحوارات المختلفة على شبكة الانترنيت كالفاسبوك، والفايبر والواتساب.[1]

وكذلك جريمة القذف والسب وتشويه السمعة للمساس بشرف الغير وكرامتهم واعتبارهم عن طريق وسائل الاتصال المباشر أو الكتابة أو عن طريق المطبوعات أو المبادلات الالكترونية بريد الكتروني) صفحات الويب غرف المحادثة [2]

كما تعتبر من أهم الجرائم الالكترونية الواقعة على الأشخاص صناعة ونشر الإباحة والجنس سواء للبالغين والأطفال خاصة، حيث يتعرض الأطفال للاستغلال الجنسي على الانترنيت بأشكال متعددة انطلاقا من الصور إلى التسجيلات المرئية للجرائم الجنسية العنيفة، حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنيت ويضاف إلى الجرائم الالكترونية الشخصية جرائم انتحال الشخصية والتغرير والاستدراج باستخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحياته أو تتخذ هذه الجريمة وجهان انتحال شخصية الفرد وانتحال شخصية المواقع [3]

تتضمن المواد 296 و297 و298[4] من قانون العقوبات أحكامًا تتعلق بالمساس بشرف واعتبار الأشخاص والسب والقذف ومع ذلك، لم تتناول هذه المواد استخدام الوسائل المعلوماتية المختلفة لارتكاب هذه الجرائم. بدأت عملية تجريم هذه الأفعال من قبل المشرع

[1] يوسف صغير، الجرائم المرتكبة عبر الانترنيت مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة مولود معمري تيزي وزو الجزائر، ص: 50

[2] عبد الرحمن بن عبد الله السيد الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات والانترنيت)، دار الوراقين للنشر والتوزيع بيروت، الطبعة الأولى، 2004، ص 312

[3] عمرو عيسى الفقي: الجرائم المعلوماتية، جرائم الحاسب الآلي والانترنيت في مصر والدول العربية المكتب العربي الحديث، الاسكندرية 2006 ص102

[4] انظر للمواد 297،298،296 من قانون العقوبات الجزائري

بموجب القانون رقم 01-09[1] المؤرخ في 26 يونيو 2001، الذي أضاف المادة 144 مكر[2]ر، التي تنص على عقوبة الحبس من 3 أشهر إلى 12 شهرًا وغرامة من 50،000 دج إلى 250،000 دج، أو بإحدى هاتين العقوبتين فقط لكل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبًا أو قذفًا، سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.

تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيًا. في حالة العود، تضاعف عقوبات الحبس والغرامة المنصوص عليها في هذه المادة، والتي عدلت بموجب القانون رقم 11-14[3] المؤرخ في 2 أغسطس 2011، حيث تم التخلي عن فكرة مضاعفة عقوبة الحبس والاكتفاء بمضاعفة الغرامة. إذا كانت هذه العقوبات محصورة في الأفعال المرتكبة ضد بعض الشخصيات في الدولة، فإنه يمكن استخدامها قياسًا في الجرائم المرتكبة ضد باقي الأشخاص كما أن نصوص المواد الثلاث المذكورة سابقًا جاءت بصيغة عامة ولم تأتِ بتفصيل.

2. الجرائم الواقعة على الأموال

لقد صاحب تطور شبكة الإنترنيت تطور وسائل الدفع والوفاء، وأضحت جزء لا يتجزأ من المعاملات الإلكترونية وفي خضم هذه التداول المالي عبر الإنترنيت ظهرت عدة جرائم الكترونية على الأموال مثل:

---

[1] قانون رقم 01-09 مؤرخ في 4 ربيع الثاني عام 1422 الموافق 26 يونيو سنة 2001، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.،صادر في الجريد الرسمية عدد34 بتاريج 2001/06/27

[2] انظر للمادة 144 مكرر ،من قانون رقم 11-14.

[3] القانون 11-14 المؤرخ في 02/08/2011، المتضمن قانون العقوبات الجريدة الرسمية عدد 44 صادرة في: 10/08/2011.

السطو والسرقة، والتحويل الالكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة، حيث أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريقة الغير المشروعة ممكنة عبر قنوات شبكة الانترنيت.[1]

كما ظهرت جريمة القمار وغسيل الأموال عبر الانترنيت بظهور الكازينوهات الافتراضية أو أندية القمار الافتراضية التي أصبحت فيما بعد مسرحا كذلك لجريمة غسيل الأموال، حيث ساعدت الشبكة العنكبوتية في انتشارها وتطورها بنقل هذه الجريمة من دولة إلى دولة أخرى لاستثمارها في مجالات مشروعة.[2]

ومن أهم الجرائم الالكترونية على الأموال، نذكر جريمة المخدرات على الانترنيت حيث تتخذ المواقع الالكترونية للترويج للمخدرات وتسويقها للناشئ لاستخدامها، وتعليمه كيفية صناعتها بكافة أصنافها وأنواعها.[3]وايضا جريمة النصب الالكتروني ، وفقًا لتعريف المشرع الجزائري في المادة 372[4] من قانون العقوبات، فإن جريمة النصب تشمل كل من حصل أو حاول الحصول على أموال، منقولات، سندات، تصرفات، أوراق مالية، وعود، مخالصات، إبراءات من التزامات، أو أي من هذه الأشياء باستخدام الاحتيال بهدف سلب ثروة الغير كليًا أو جزئيًا. ويشمل هذا الاحتيال استخدام أسماء أو صفات كاذبة، سلطة خيالية، اعتماد مالي خيالي، إحداث الأمل في الفوز بشيء ما، الإيحاء بوقوع حادث أو واقعة وهمية، أو التسبب في الخشية من وقوع شيء وهمي.

يعاقب على جريمة النصب بالحبس لمدة تتراوح بين سنة وخمس سنوات، وبغرامة مالية تتراوح بين 500 و20،000 دينار. وإذا ارتكبت الجنحة من قبل شخص لجأ إلى الجمهور

[1] خالد ممدوح إبراهيم أمن الجريمة الالكترونية، الدار الجامعية الاسكندرية 2010، ص: 76 وما بعدها.

[2] صالحة العمري، جريمة غسل الأموال وطرق مكافحتها مجلة الاجتهاد القضائي، العدد الخامس مخبر اثر الاجتهاد القضائي على حركة التشريع جامعة محمد خيضر بسكرة، ص 179

[3] يوسف صغير، المرجع السابق، ص51

[4] انظر للمادة 372 من قانون العقوبات الجزائري

بغرض إصدار أسهم، سندات، أذونات، حصص، أو أية سندات مالية سواء كانت لشركات أو مشروعات تجارية أو صناعية، فيمكن أن تصل مدة الحبس إلى عشر سنوات والغرامة إلى 200،000 دينار[1].

وعليه، إذا لم يربط المشرع الجزائري جريمة النصب بالجريمة المعلوماتية ولم يحدد وسيلة معينة، يمكن تطبيقها إذا توفرت شروطها التالية:

وجود الاحتيال :يجب أن يكون هناك استخدام لوسائل احتيالية مثل الأسماء أو الصفات الكاذبة، السلطة الخيالية، أو الاعتماد المالي الوهمي.

تحقيق النتيجة :يجب أن يكون الاحتيال قد أدى إلى استلام أو تلقي أموال، منقولات، سندات، تصرفات، أوراق مالية، وعود، مخالصات، أو إبراءات من التزامات، أو محاولة الحصول على أي منها.

نية الاحتيال :يجب أن يكون الهدف من الاحتيال هو سلب كل أو بعض ثروة الغير.

وسائل إقناع وهمية :يمكن أن تشمل هذه الوسائل إحداث الأمل في الفوز بشيء ما، الإيحاء بوقوع حادث أو واقعة وهمية، أو التسبب في الخشية من وقوع شيء وهمي.

بالتالي، يمكن إسقاط جريمة النصب على الجرائم المعلوماتية إذا توفرت هذه الشروط، حيث أن الوسائل الاحتيالية يمكن أن تشمل التكنولوجيا الحديثة والوسائل الإلكترونية[2].

3. الجرائم الواقعة على أمن الدولة

تعد هذه الجرائم من أخطر الجرائم الالكترونية خاصة الارهاب المعلوماتي والجريمة المنظمة المعلوماتية، حيث أتاحت الانترنيت للكثير من المنظمات الارهابية الترويج لأفكارها

[1] يوسف صغير،المرجع السابق، ص53

[2] صالحة العمري،المرجع السابق،ص 181

ومعتقداتها وأدت إلى ظهور جريمة أخرى أخطر منها وهي جريمة التجسس الالكتروني على الدول بالاطلاع على مختلف الأسرار العسكرية والاقتصادية بين الدول المتصارعة، كما تعطى الشبكة العنكبوتية فرصا للتأثير على المعتقدات الدينية وتقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة والمساس بأمنها الداخلي وبنظامها العام[1]

قام المشرع الجزائري من خلال تعديله لقانون العقوبات لسنة 2004 بتخصيص بعض الهيئات العامة والمؤسسات الخاضعة للقانون العام بحماية جنائية لمعارضتها المعلوماتية. جاء هذا التعديل استجابة للتطورات التكنولوجية وانتشار الجرائم المعلوماتية، حيث أدرك المشرع أهمية حماية البيانات والمعلومات التي تتعامل معها هذه الهيئات من أي اختراق أو تعدٍ غير مشروع[2].

يهدف هذا التعديل إلى تعزيز الأمن المعلوماتي وضمان سلامة البيانات والمعطيات التي تعتبر حساسة ومهمة لاستمرار عمل المؤسسات العامة. من خلال توفير حماية قانونية قوية، يسعى المشرع إلى ردع الأفراد والجماعات عن ارتكاب الجرائم المعلوماتية وضمان مساءلة الجناة وتقديمهم للعدالة.

تضمنت هذه الحماية الجنائية تشديد العقوبات على الأفعال التي تستهدف المعلومات والبيانات التابعة لهذه الهيئات، بما في ذلك الدخول غير المشروع إلى الأنظمة المعلوماتية، أو التلاعب بالبيانات، أو استخدامها بشكل غير قانوني. كما تم إدراج مواد قانونية تنص

[1] أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته، ورقة مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، 31-32 سبتمبر 2014.ص 97

[2] الطاهر حرف الله، النخبة الحاكمة في الجزائر 6219-1982 بين التصور الإيديولوجي والممارسات السياسية، ج1، الجزائر: دار هومة، 2007.ص102

على عقوبات صارمة لهذه الجرائم، لضمان حماية فعالة وشاملة للمعطيات المعلوماتية الخاصة بالهيئات العامة والمؤسسات الخاضعة للقانون العام[1].

وقد نص المادة 394 مكرر 3[2] على انه تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد.

- **ثانيا: الجرائم الواقعة على النظام المعلوماتي**

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية يمس النظام المعلوماتي ويستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي

1. الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل للسرقة وخيانة الأمانة أو الاتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، مما يترتب عليها خسائر كبيرة، ولقد حدث هذا النوع من الجرائم في فرنسا، وأدى إلى إتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية، وقدرت الخسائر بـ 5 ملايين فرنك فرنسي.[3]

[1] ايسر محمد عطية،المرجع السابق، ص98

[2] انظر للمادة 394 مكرر 3 من قانون العقوبات الجزائري

[3] هواري عباش مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام. جامعة بسكرة كلية الحقوق – 2016 . ص . 3.

2. الجرائم الواقعة على البرامج الالكترونية

وتنقسم هذه الجرائم بدورها إلى الجرائم الواقعة على البرامج التطبيقية، عن طريق تحديد البرنامج أولا ثم التلاعب به أو تعديله، [1]ومن أمثلتها قيام أحد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بتقييد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick [2]

وكذلك تضم هذه الجرائم الجرائم الواقعة على برنامج التشغيل وهي البرامج المسؤولة عن عمل النظام المعلوماتي، ومن حيث قيامها بضبط ترتيب العمليات الخاصة بالنظام، وتقوم هذه الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشيفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام المعلوماتي ومثالها جريمة تصميم برنامج وهمي من خلاله تنفذ الجريمة، ومثاله ما قامت به إحدى الشركات التأمين الأمريكية في مدينة لوس انجلوس بواسطة مبرمجها تصميم برنامج يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 46000 بهدف تقاضي هذه الشركة لعمولات من اتحاد شركات التأمين. [3]

3. الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

لقد عرف القانون الفرنسي الصادر في 29 جويلية 1982 الخاص بالاتصالات السمعية والبصرية المعلومة <sons ou de message de toute : de données d'images de documents> بأنها .nature كما عرفها الفقيه الفرنسي Catala على

---

[1] حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، جامعة محمد خيضر، بسكرة، كلية الحقوق، 2016، ص 6.

[2] سوير سفيان المرجع السابق، ص: 42

[3] سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، بمحكمة سيدي محمد، ص 31.

أنها رسالة معبر عنها في الشكل يجعلها قابلة للنقل أو الإبلاغ للغير " . بينما عرفها القضاء الفرنسي بأنها: وسيلة للمعرفة قابلة لكي تحفظ أو تبلغ بواسطة الاصطلاحات"[1]

وتعد المعلومة المعالجة آليا ذات أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي، لما لها من قيمة اقتصادية، وتتم الجرائم عليها من خلال التلاعب فيها بصفة مباشرة أو غير مباشرة أو عن طريق اتلافها أو استبدالها أو محوها وهذا ما تسمى بجريمة الغش أو التزوير المعلوماتي ومثالها ما قام به شخص يدعى Vladimir loriblitt بإسرائيل باستخدام طريقة تدعى bluff وهو موظف بوزارة المالية، حيث قام بإدخال فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي قام بإنشائها.

[1] سالم عبد الرزاق، المرجع السابق، ص 34.

المبحث الثاني:

ماهية الامن السيبراني

في عالمنا الحديث المعتمد على التكنولوجيا، تعد الأنظمة الرقمية والشبكات الإلكترونية عمودًا فقريًا للكثير من الأنشطة اليومية، سواء كانت شخصية أو تجارية أو حكومية. ومع ذلك، يترافق هذا التطور التكنولوجي مع تزايد التهديدات السيبرانية التي تستهدف هذه الأنظمة والشبكات الأمن السيبراني يمثل تلك الحاجز الذي يحمينا من الهجمات الإلكترونية، سواء كانت قرصنة، اختراق، أو تجسس، والتي يمكن أن تترك آثارًا وخسائر كبيرة إذا لم يتم التصدي لها بفعالية في هذه المبحث سنتناول مفهوم الأمن السيبراني ، متناولين تعريفه ونشاته أهميته وتحدياته .

المطلب الاول:

مفهوم الامن السيبراني ونشأته

أصبح الأمن السيبراني ضروريًا لضمان سلامة البيانات والخصوصية والحفاظ على الثقة في الأنظمة الرقمية. يعد الفهم العميق لمفهوم الأمن السيبراني أساسياً لمواجهة التحديات الأمنية الحديثة في عالم متصل بشكل متزايد.ومنه سنتناول في هذا المطلب تعريف الامن السيبراني في الفرع الاول منه ونتطرق الى نشاءته في الفرع الثاني.

الفرع الاول:

تعريف الامن السيبراني

مع التوسع الهائل في استخدام التكنولوجيا، أصبحت الهجمات الإلكترونية تهديدًا متزايدًا. في هذا السياق، برز مفهوم الأمن السيبراني كضرورة لحماية الأنظمة والمعلومات الحساسة من التهديدات الرقمية،وفي هجا الفرع سنتناول تعريف الامن السيبراني.

تتعدد تعريفات الأمن السيبراني (المعلوماتي) فهناك من يقوم بتوزيعها لكي تعبر عن القدرة على حماية بيانات الدولة وشبكاتها مثل تعريف lwis.J.A بأنه ("القدرة على حماية والدفاع عن استخدام الفضاء السيبيراني من الهجمات السيبرانية".[1] ويعرف كذلك بأنه «المحافظة على المعلومات من تداخل استخدامها أو تخريبها أو استخدام معلومات مضللة أو تحريفها او استبدالها او سوء تفسيرها او الغائها او سوء استخدامها أو الفشل في استخدامها او الوصول اليها او اظهارها او مراقبتها او نسخها او سرقتها")[2].

تعريف الأمن السيبراني الذي أورده lwis.J.A يبرز أهمية حماية الفضاء السيبراني والمعلومات الرقمية من التهديدات السيبرانية المتنوعة. من خلال تعريفه، يتم تسليط الضوء على الجوانب القانونية للأمن السيبراني، حيث يشمل حماية البيانات والمعلومات من التداخل والتلاعب والوصول غير المصرح به والسرقة والتلف والاستخدام غير القانوني والتحريف والاستخدام المضلل والغير مصرح به[3].

ويشير "الاتحاد الدولي للاتصالات" على أن الأمن السيبراني هو (مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات والمبادئ ومناهج إدارة المخاطر والإجراءات والتدريبات وأفضل الممارسات والضمانات التكنولوجيا التي يمكن استخدامها لحماية البيئة السيبرانية والمستخدم والمنظمة بصورة عامة). تعريف "الاتحاد الدولي للاتصالات" للأمن السيبراني يعكس الشمولية والتنوع الذي يتمتع به هذا المجال. يُظهر التعريف أن الأمن السيبراني ليس مجرد تكنولوجيا، بل هو مجموعة من الأدوات والسياسات والمفاهيم

[1] إيهاب خليفة، "الأمن السيبراني: الماهية والاشكالات"، رؤى مصرية، ع. أكتوبر 2019، ص ص. 4_8.

[2] عمر بن محمد العتيبي، الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية والدولية، اطروحة دكتوراه، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، 2010، ص.15.

[3] محمد علي سالم، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 1، العدد 2، 2007، العراق، ص 21.

والضمانات والمبادئ والإجراءات والتدريبات وأفضل الممارسات التي تهدف إلى حماية البيئة السيبرانية والمستخدم والمنظمة بشكل عام.

وتعرفه "وزارة الداخلية الأمريكية" بأنه (النشاط او العملية، القدرة او الامكانية أو الحالة التي يمكن من خلالها حماية المعلومات ونظم الاتصالات والدفاع عنها من الضرر او التعديل او التجسس او التدمير او الدخول غير المصرح به).[1]

تعريف "وزارة الداخلية الأمريكية" للأمن السيبراني يتماشى مع التعريفات السابقة، حيث يركز على النشاط أو العملية التي تسهل حماية المعلومات ونظم الاتصالات والدفاع عنها من مختلف التهديدات السيبرانية. يُشير هذا التعريف إلى الضرورة الحاسمة لتطبيق التدابير والسياسات والتقنيات التي تُمكِّن من مواجهة التهديدات مثل التجسس والتدمير والاختراقات غير المصرح بها.

يشمل الأمن السيبراني في تعريفه كل الممارسات والتدابير والإجراءات التي تهدف الى حماية اجهزة الكمبيوتر والبرامج والبيانات والملفات الخاصة من التلف او السرقة أو التزوير وحماية فضاء الانترنت والمعلومات للمستخدمين والمستفيدين. ونستخلص من التعريفات السابقة مجموعة من العناصر والخصائص:

- الأمن السيبراني شبكه غير محدودة تختلف استخداماتها وتتفاوت درجات استعمالها
- يتميز بسرعه الإجراء، التغيير، والتفاعل.
- وجود جهات معينة ومتخصصة للحماية واستراتيجيات ملائمة ومناسبة لأمن المعلومات.[2]

[1] إيهاب خليفة، مرجع سابق، ص ص.4_8.

[2] إيهاب خليفة، مرجع سابق، ص ص.4_8.

الفرع الثاني

نشأة الامن السيبراني

يعتبر الأمن السيبراني مفهومًا حديثا نسبيًا، حيث بدا تاريخه في سبعينيات القرن الماضي. في تلك الفترة، كانت أجهزة الكمبيوتر واتصالها بالإنترنت لا تزال في مرحلة الإنشاء والتطوير، وكان من السهل تهديد أمن هذه الأجهزة، ومنه سنتطرق الى نشاءة الامن السيبراني، ومراحل تطوره.

- **نشأة الامن السيبراني**

نشأ مفهوم الأمن السيبراني بعد اختراع الحاسوب بعدة عقود، فلم يكن في البداية أي داعٍ للأمن السيبراني، إذ كان من الصعب حدوث هجمات إلكترونية، لأنّ الوصول لأجهزة الكمبيوتر كان مقتصرًا على أعداد محددة من المستخدمين، فقد كانت الأجهزة عملاقة محصورة في غرفة بمواصفات معينة ولم تكن مرتبطة بشبكات آنذاك[1]

- **اولا: النشأة في السبعينيات:**

في سبعينيات القرن العشرين، حيث كانت الحواسيب الأولى تستخدم بشكل أساسي في الأوساط الأكاديمية والعسكرية في تلك الفترة، ظهرت الحاجة إلى حماية المعلومات عندما تم تصميم أول فيروس كمبيوتر يُعرف باسم(Creeper) ، والذي كان ينتقل عبر شبكةARPANET[2]

---

[1] **شركة سيسكو**" .ما هو الأمن السيبراني؟ ."*سيسكو* .متاح على :
https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html#~types-of-threats تم الوصول في 31 مايو 2024. ساعة 22.30

[2] **كاسبرسكي**" .تاريخ موجز للفيروسات الكمبيوتر وما يخبئه المستقبل .*كاسبرسكي* .متاح على :
https://me.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds تم الوصول في 31 مايو 2024 22:40

- **ثانيا ؛التطور في الثمانينيات**

مع تزايد استخدام الحواسيب في الثمانينيات، ظهرت الحاجة الملحة البرامج مكافحة الفيروسات. في عام 1987، تم تطوير أول برنامج تجاري لمكافحة الفيروسات من قبل Andreas Lüningو .Kai Figgeوفي نفس الوقت، شهد ذلك العام أول إصدار من NOD antivirusفي الولايات المتحدة، والذي أدى إلى بداية صناعة الأمن السيبراني ، وظهرت مصطلحات جديدة مثل فيروسات الحاسوب (Trojan Horse)، لذا حدّدت وزارة الدفاع الأمريكية معايير لتقييم نظام الكمبيوتر الموثوق به عام 1985 م.[1]

- **ثالثا :التسعينيات والإنترنت**

. مع بداية فترة التسعينيات من القرن الماضي، بدأت خدمة الإنترنت تدخل في الكثير من المجالات، وازداد عدد المستخدمين لها بشكل ملحوظ، وأصبحوا يضعون معلوماتهم الشخصية والمهمة على المواقع الإلكترونية. الأمر الذي فتح المجال واسعًا أمام بعض الأشخاص لسرقة تلك المعلومات والبيانات، بهدف تحقيق بعض المكاسب المادية، ومع حلول منتصف التسعينات أصبحت التهديدات التي تواجه الشبكات الإلكترونية كثيرة ومتعددة.

وهو الأمر الذي دفع بالكثير من الباحثين في هذا المجال وكذلك من الشركات على اختلاف أنواعها إلى السعي إلى إنتاج جدران حماية فعالة بشكل عالي، وكذلك اختراع برامج عالية الكفاءة لمكافحة الفيروسات على نطاق أوسع[2].

---

[1] **ويكيبيديا**" .مضاد فيروسات (برمجة) .*ويكيبيديا* .متاح على : https://ar.wikipedia.org/wiki/%D9%85%D8%B6%D8%A7%D8%AF_%D9%81%D9%8A%D8%B1%D9%88%D8%B3%D8%A7%D8%AA_(%D8%A8%D8%B1%D9%85%D8%AC%D8%A9) تم الوصول في 31 مايو 2024، الساعة 22:45

[2] مها الدحام، تاريخ الامن السيبراني ،[2] تاريخ الأمن السيبراني – موضوع(mawdoo3.com) 10:30 01/04/2024

- **رابعا: القرن الحادي والعشرين**

مع بداية الألفية الجديدة، أصبح الأمن السيبراني أكثر أهمية مع تزايد الاعتماد على الأنظمة الرقمية. بحلول العقد الأول من القرن الحادي والعشرين تنوعت وتضاعفت التهديدات والاختراقات وكذلك الهجمات الإلكترونية التي بدأت كثير من الكيانات الإجرامية القيام بها وبشكل محترف باستخدام تقنيات عالية، الأمر الذي دفع الكثير من الدول والحكومات إلى اتخاذ العديد من القرارات من أجل تضييق الخناق على هذه الجهات[1].

المطلب الثاني

الامن السيبراني بين المخاطر والابعاد

نبغي دراسة الأمن السيبراني بعمق لفهم مدى تعقيد التحديات التي يواجهها، بما في ذلك الجوانب التقنية والقانونية والسياسية والاجتماعية. إذ يتعين على المجتمع الدولي والشركات والمؤسسات والأفراد اتخاذ التدابير اللازمة لتعزيز الأمن السيبراني وحماية البيانات الحساسة وضمان استدامة الأنظمة الرقمية.

يأتي هذا المطلب لتطرق الى تهديدات، وتحليل المخاطر المحتملة المتعلقة بالامن السيبراني، وفهم الأبعاد المتعددة لهذا المجال، بغية تطوير استراتيجيات فعالة للوقاية من الهجمات السيبرانية والتعامل معها بكفاءة وفاعلية.وهذا ما سنتحدث عليه بالتفصيل في الفصل الثاني لاحقا.

الفرع الاول

تهديدات ومخاطر حوادث الامن السيبراني

في عصر التكنولوجيا الحديثة، تواجه المؤسسات والأفراد تحديات كبيرة في مجال الأمن السيبراني. يتزايد التكنولوجيا بسرعة مذهلة، ومعها تتزايد أيضًا التهديدات السيبرانية. تشمل

[1] مها الدحام، تاريخ الامن السيبراني تاريخ الأمن السيبراني – موضوع(mawdoo3.com) 10:40 01/04/2024

هذه التهديدات الهجمات الإلكترونية، والبرمجيات الخبيثة، وسرقة الهوية، والاختراقات السيبرانية، والاحتيال الإلكتروني، والتجسس، وغيرها الكثير. في هذا الفرع، سنستكشف عددًا من هذه المخاطر والتهديدات التي تواجه الأمن السيبراني وتأثيرها على المؤسسات والأفراد، وفي فرعنا هذا سنبرز هذه التهديدات والمخاطر.

صحيح أن التهديد السيبراني لا يحدث إلا عبر الحاسب الآلي وشبكة النت، لكنه يختلف من شكل لأخر حسب نوع ارتكابه، كما أن له عدة مجالات يمكن أن يقع فيها ويرتكب في حقها وهذا ما سيأتي معنا فيما يلي[1]:

أولا: أنواع التهديدات السيبرانية

تُصنف التهديدات السيبرانية إلى ثلاثة أنواع رئيسية:

1: التهديدات المتعلقة بالأجهزة

تشمل هذه التهديدات الأضرار التي قد تلحق بالمكونات الفيزيائية للكمبيوتر مثل وحدات الإدخال والإخراج، وأجهزة التخزين مثل الأقراص المرنة والصلبة، بالإضافة إلى الشاشات والطابعات. كما تشمل الأضرار التي قد تصيب البيانات والمعلومات المخزنة، والتي قد تؤدي إلى تدميرها كليًا أو جزئيًا، أو انتقالها إلى أجهزة أخرى، أو حتى محوها أو تلفها[2]. مثال على ذلك هو فيروس الفدية.

2: التهديدات المتعلقة بشبكات المعلومات:

تتضمن هذه التهديدات الأفعال غير القانونية التي تستهدف المواقع الإلكترونية بهدف تعطيلها، التشويش عليها، تعديل محتوياتها، أو الدخول غير المصرح به إلى مواقع خاصة.

---

[1] Kaspersky(لا تاريخ محدد). "أهم ٧ تهديدات سيبرانية .*كاسبرسكي* .متاحة عل : (https://me.kaspersky.com/resource-center/threats/top-7-cyberthreats تم الوصول إليها في 31 مايو 2024. 23.30

[2] نفس المرجع، 31 مايو 2024. 23.38

تشمل هذه الأفعال استخدام عناوين مزيفة للوصول إلى الشبكة، نقل الفيروسات، إرسال رسائل ضارة، وترويج محتويات غير مشروعة[1].

3: التهديدات المتعلقة بالبيانات والمعلومات:

تشمل هذه التهديدات الأفعال غير القانونية مثل الدخول غير المصرح به أو الاعتراض على وثائق أو نصوص موجودة في شبكة الكمبيوترات بهدف سرقتها، تعديلها، إتلافها، أو نشرها. تتضمن هذه التهديدات انتهاك الملكية الفكرية للبرمجيات، الإنتاج الفني، الأدبي، أو العلمي، وتمكن المتطفلين من المراقبة والتنصت على الاتصالات الإلكترونية. وقد أدى ذلك إلى ظهور مكتبات إلكترونية ضخمة في الدول المتقدمة تحتوي على بيانات ونصوص تم اعتراضها وتسجيلها من جميع أنحاء العالم[2].

ثانيا: المجالات التي تقع عليها التهديدات السيبرانية

1: الخصوصية الفردية :

في عصرنا الرقمي الحالي، أصبحت الحياة الشخصية للأفراد معرضة بشكل متزايد للتهديدات السيبرانية. هذه التهديدات تشمل، ولكن لا تقتصر على، الاختراقات الأمنية التي تسمح بالوصول غير المشروع إلى المعلومات الشخصية، مما يؤدي إلى استخدامات ضارة

[1]."Technology Reviewتهديد الأمن السيبراني والاستعداد له". متاح على :
https://technologyreview.ae/%d8%aa%d9%87%d8%af%d9%8a%d8%ab-%d8%a7%d9%84%d8%a3%d9%85%d9%86-%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a-%d9%88%d8%a7%d9%84%d8%a7%d8%b3%d8%aa%d8%b9%d8%af%d8%a7%d8%af-%d9%84%d9%87/ تاريخ الوصول: 2024/05/31 23:01

[2] إبراهيم أحمد عبد السامرائي، الجريمة الالكترونية السيبرانية في القانون الدولي مجلة جامعة جيهان أربيل للعلوم الإنسانية والاجتماعية، المجلد 6 ، العدد 2، 2022، ص147

مثل الابتزاز، التهديد، انتحال الشخصية، الاستدراج، ونشر المحتوى الإباحي. هذه الأفعال تنتهك الحق في الخصوصية وتشكل تهديدًا جسيمًا للأمان الشخصي والسلامة العاطفية[1].

يظهر أن التهديدات السيبرانية، مثل الاختراقات الأمنية والوصول غير المشروع إلى المعلومات الشخصية، ليست فقط مصدر إزعاج بل تتسبب في أضرار حقيقية.

2: الأمن المالي :مع التحول الرقمي السريع، تحولت المعاملات المالية إلى الفضاء السيبراني، مما أدى إلى زيادة في الجرائم المالية الإلكترونية. هذه الجرائم تشمل الاحتيال ببطاقات الائتمان، الاختلاسات المالية الإلكترونية، سرقة الأموال من البنوك، وغسيل الأموال. الأمر الذي يتطلب تعزيز الأمن السيبراني وتطوير القوانين لحماية الأصول المالية للأفراد والمؤسسات[2].

التحديات القانونية الناشئة عن التحول الرقمي السريع في المعاملات المالية وما يترتب عليه من جرائم مالية إلكترونية متزايدة مثل الاحتيال ببطاقات الائتمان، الاختلاسات المالية، وسرقة الأموال. من منظور قانوني، يتطلب هذا الوضع تعزيز الأطر القانونية والتنظيمية لمكافحة هذه الجرائم بشكل فعال. يجب تطوير التشريعات الحالية لتشمل عقوبات صارمة ورادعة للجرائم السيبرانية، مع تحديث القوانين لمواكبة التطورات التكنولوجية. كما يجب تعزيز التعاون الدولي لمكافحة الجرائم العابرة للحدود، وضمان تطبيق معايير عالية للأمن السيبراني في المؤسسات المالية لحماية الأصول المالية للأفراد والشركات.

[1] فتيحة ليتيم، ونادية ليتيم، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة"، جامعة بسكرة مجلة المفكر، العدد 12، (د.س.ن) ص 239

[2] فتيحة ليتيم، ونادية ليتيم، نفس المرجع، ص 239

3: الأمن القومي

الجرائم السيبرانية التي تستهدف الأمن القومي تعتبر من أخطر التهديدات لأنها تهدد البنية التحتية الحيوية للدول وتعرض سلامتها للخطر. تشمل هذه الجرائم الإرهاب الإلكتروني، التجسس، والجوسسة المضادة، وهي تمثل تحديات كبيرة للمؤسسات الحكومية وتتطلب استجابة متكاملة ومتعددة الأبعاد للحفاظ على الأمن القومي[1]

الجرائم السيبرانية التي تستهدف الأمن القومي تشكل تهديدات خطيرة للغاية لأنها تستهدف البنية التحتية الحيوية للدول، مما يعرض سلامتها واستقرارها للخطر. هذه الجرائم تشمل الإرهاب الإلكتروني، التجسس، والجوسسة المضادة، وتعتبر من أعقد التحديات التي تواجه المؤسسات الحكومية. للتصدي لهذه التهديدات، يتطلب الأمر استجابة متكاملة تشمل تعزيز القدرات التقنية للدفاع السيبراني، وتطوير التشريعات الصارمة، وتعزيز التعاون بين الوكالات الحكومية والدولية. كما يجب التركيز على بناء وعي مجتمعي بأهمية الأمن السيبراني وتشجيع الأبحاث والتطوير في هذا المجال لضمان استباق التهديدات المحتملة والحفاظ على الأمن القومي.

الفرع الثاني

ابعاد الامن الاسيبراني

مع تزايد التهديدات السيبرانية وتعقيدها، تتسع أبعاد الأمن السيبراني لتشمل جوانب تقنية وقانونية وإدارية واجتماعية. هذا الفرع يستعرض الأبعاد المختلفة للأمن السيبراني.

[1] رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة 443 العدد 41، 2018، ص ص449-444

اولا: البعد العسكري:

الإنترنت، الذي نشأ في الأصل كمشروع عسكري، قد تطور ليصبح أداة حاسمة في القدرات العسكرية والتفوق العلمي. الصراع بين القوى العظمى، كما شهدنا بين الاتحاد السوفياتي والولايات المتحدة، قد امتد إلى الفضاء السيبراني، مع التركيز على الوصول إلى الفضاء وتطوير الأسلحة النوويةو الهجمات السيبرانية.

كما رأينا في دول مثل جورجيا واستونيا وكوريا الجنوبية وإيران، يمكن أن تترجم إلى تداعيات مادية خطيرة[1]، من اندلاع صراعات مسلحة إلى انقطاعات في الاتصالات والخدمات الأساسية.

القوة السيبرانية تتميز بقدرتها على ربط الوحدات العسكرية وتنسيق العمليات عبر الشبكات العسكرية، مما يجعل الأمن السيبراني عنصرًا حيويًا في الدفاع الوطني[2].

أن القوة السيبرانية تتميز بقدرتها على ربط الوحدات العسكرية وتنسيق العمليات عبر الشبكات العسكرية، مما يجعل الأمن السيبراني عنصراً حيوياً في الدفاع الوطني. هذا يعني أن الدول تحتاج إلى تطوير استراتيجيات دفاع سيبرانية فعالة لحماية نفسها من الهجمات السيبرانية وضمان سلامة واستقرار بنيتها التحتية الحيوية[3].

منه، يمكننا أن ندرك أن الأمن السيبراني أصبح جزءاً لا يتجزأ من الأمن القومي، وأن التهديدات السيبرانية تشكل تحدياً معقداً يتطلب استجابة متعددة الأبعاد تشمل التقنية والقانونية والإدارية والاستراتيجية.

---

[1] عادل عبد الصادق "الحروب السيبرانية تصاعد القدرات والتحديات للأمن العالمي، المركز العربي لأبحاث الفضاء الإلكتروني، د.ش،2017،ص02

[2] سمير بارة، الأمن السيبراني في الجزائر السياسات والمؤسسات المجلة الجزائرية للأمن الإنساني.العدد 04 ،2007،.ص 260

[3] ب بوعلام، ملتقى حول الجيش الوطني الشعبي ورهانات تداول المعلومات عبر شبكات التواصل الاجتماعي، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016ص 6.

ثانيا: البعد الاقتصادي:

الاقتصاد العالمي أصبح معتمدًا بشكل كبير على التكنولوجيا الرقمية، من تخزين البيانات إلى تطوير الصناعات وتحريك الاقتصادات.

المعاملات المالية والاقتصادية الآن محوسبة ومترابطة عبر شبكات الكترونية، مما يجعل الإنترنت محورًا أساسيًا للتطور الاقتصادي في القرن الحادي والعشرين. [1]

هذا التطور يبرز أهمية الأمن السيبراني في حماية البنية التحتية الاقتصادية وضمان استمرارية الأعمال[2].

أي هجوم سيبراني يمكن أن يعطل العمليات التجارية والمالية، مما يؤدي إلى خسائر اقتصادية كبيرة. لذا، يجب على الشركات والحكومات الاستثمار في أنظمة أمان سيبراني متقدمة وتطوير سياسات فعالة لمواجهة التهديدات السيبرانية.

ثالثا: البعد الاجتماعي:

شبكات التواصل الاجتماعي فتحت آفاقًا جديدة للتعبير عن الآراء السياسية والطموحات الاجتماعية، وأصبحت وسيلة لتطوير المجتمعات من خلال تبادل الأفكار والمعلومات.

الانفتاح على الشبكة العالمية للمعلومات وتوسع المفاهيم لتشمل أساليب جديدة باستخدام تقنيات المعلومات والاتصالات، مثل إنشاء المدونات الإلكترونية والتجمعات على الإنترنت، يعزز الحاجة إلى الأمن السيبراني لحماية هذه الحقوق والحريات[3].

---

[1] عادل عبد الصادق، الحروب السيبرانية تصاعد القدرات والتحديات للأمن العالمي، المركز العربي لأبحاث الفضاء الإلكتروني، دبي، 2017. ص66

[2] عبد الفتاح حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت مصر: دار الكتب القانونية المحلة الكبرى ، الطبعة الأولى.2007،ص207

[3] منى الأشقر حور، الأمن السيبراني التحديات ومستلزمات المواجهة ،جامعة الدول العربية المركز العربي للبحوث القانونية والقضائية،2012، ص 30

مع توسع الوصول إلى الإنترنت وانتشار تقنيات المعلومات والاتصالات، زادت أهمية الأمن السيبراني لضمان حماية حقوق الأفراد وحرياتهم على الإنترنت. فإنشاء المدونات الإلكترونية والتجمعات الاجتماعية على الإنترنت يتطلب توفير بيئة آمنة وموثوقة تحمي من التهديدات السيبرانية مثل الاختراقات والتجسس والاحتيال[1].

بالتالي، يتعين تعزيز الأمن السيبراني لضمان استمرارية هذه الحقوق والحريات على الإنترنت. ويجب أن تعمل الحكومات والشركات والمجتمعات المدنية سويًا على وضع سياسات وتشريعات تعزز الأمان السيبراني وتحمي البيانات الشخصية وتضمن الحرية والخصوصية الرقمية للأفراد.

رابعا: البعد السياسي:

التسريبات الوثائقية والحملات الانتخابية والحركات الاحتجاجية الإلكترونية تدل على الأهمية المتزايدة للأمن السيبراني في السياسة.

الحكومات تستغل شبكات التواصل الاجتماعي لتمرير سياساتها والتأثير على الرأي العام، مما يجعل الأمن السيبراني محورًا رئيسيًا في الحفاظ على الاستقرار السياسي والنظام العام[2].

أن استغلال الحكومات لشبكات التواصل الاجتماعي يجعل الأمن السيبراني أمراً بالغ الأهمية للحفاظ على الاستقرار السياسي والنظام العام. فالتسريبات الوثائقية والحملات الانتخابية والحركات الاحتجاجية الإلكترونية يمكن أن تتسبب في اضطرابات سياسية واضطرابات اجتماعية إذا لم يتم التعامل معها بشكل فعال.

[1] عبد الفتاح حجازي ،المرجع السابق،ص 210

[2] عطية إدريس ،مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري مجلة مصداقية، المجلد 01 ،2009 ، ص 105

لذا، يتعين على الحكومات والمنظمات السياسية اتخاذ إجراءات لتعزيز الأمن السيبراني، بما في ذلك تطوير سياسات وإجراءات لحماية البيانات ومكافحة التسريبات الوثائقية، وتعزيز الوعي بأهمية الأمن السيبراني بين المواطنين[1].

[1] فتيحة ليتيم، ونادية ليتيم، نفس المرجع، ص 244

الفصل الثاني

آليات مكافحة الجرائم الإلكترونية وحماية الأمن السيبراني

المبحث الاول

الجهود الدولية والإقليمية في مواجهة الجريمة السيبرانية

إن هناك العديد من الهيئات والمنظمات والمجالس الدولية التي تلعب دورا ملحوظا في إطار إبرام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة الجرائم السيبرانية. وعلى رأس هذه المنظمات هيئة الأمم المتحدة، والمجلس الأوروبي وبعض الهيئات الأخرى، وعليه فإن هذا الموضوع ستتم معالجته عبر مطالب ثلاثة يخصص الأول منها لدور الجهود الدولية ، ويخصص الثاني للجهود الإقليمية كاتفاقية بودابست والاتفاقية العربية، ويخصص الثالث لعرض الصعوبات التي تواجه الجهود الدولية وكيفية القضاء عليها.

المطلب الأول

الجهود الدولية في مكافحة الجريمة السيبرانية

تشهد العصر الحالي تطورًا هائلًا في التكنولوجيا الرقمية، مما أدى إلى زيادة التعرض لتهديدات الجريمة السيبرانية على مستوى العالم. في هذا السياق، بات التعاون الدولي ضرورة ملحة لمكافحة هذه الظاهرة المتزايدة التعقيد والخطورة. تعتبر الجهود الدولية في هذا المجال أحد السبل الفعّالة للتصدي للجريمة السيبرانية وحماية البنية التحتية الرقمية للدول والمجتمعات.

سنتناول في هذا المطلب مراجعة للجهود الدولية المبذولة في مجال مكافحة الجريمة السيبرانية، بما في ذلك التعاون القائم بين الدول والمنظمات الدولية، والاتفاقيات والاتفاقيات الدولية المتعلقة بالأمن السيبراني.

الفرع الأول

جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية

تنشط الجريمة السيبرانية على نطاق عالمي، مما يشكل تحديًا كبيرًا للأمن والاستقرار الدوليين. تعمل الأمم المتحدة بجدية على مكافحة هذا الظاهرة المتزايدة، ومن خلال فرعنا هذا سنسلط الضوء على جهوداً هامة لتعزيز التعاون الدولي وتطوير القوانين والسياسات اللازمة لمواجهة التهديدات السيبرانية.

قام المجلس الاقتصادي والاجتماعي للأمم المتحدة بإصدار توصية تقضي بأن تتولى المنظمة الدولية مسؤولية رئيسية في تطوير سياسات للوقاية من الجريمة وتعزيز العدالة الجنائية على المستوى الدولي. وقد تم تبني هذه التوصية من قبل الجمعية العامة للأمم المتحدة في عام 1950، مما أدى إلى تأسيس لجنة استشارية من الخبراء مكلفة بمهام مكافحة الجريمة وتقديم الاستشارات للأمين العام، وتطوير البرامج والخطط وصياغة السياسات للتدابير الدولية في مجال الوقاية من الجريمة ومعاملة المجرمين. [1]

وعقب انعقاد مؤتمر الأمم المتحدة حول الوقاية من الجريمة ومعاملة المجرمين في كيوتو، اليابان، في عام 1970، تم استبدال اللجنة الاستشارية بلجنة متخصصة في الوقاية من الجريمة ومكافحتها، بناءً على توصية من المجلس الاقتصادي والاجتماعي في عام 1971. تهدف مؤتمرات الأمم المتحدة المتعلقة بالوقاية من الجريمة ومعاملة المجرمين، التي تُعقد كل خمس سنوات، إلى تحفيز تبادل المعارف والخبرات بين الخبراء من مختلف الدول وتعزيز التعاون الدولي والإقليمي في مجال مكافحة الجريمة، مما يجعلها منصة أساسية للتعاون

[1] يوسف صغير. المرجع السابق، ص93

الدولي. وتركز هذه الدراسة على جهود الأمم المتحدة من خلال مؤتمراتها المخصصة للوقاية من الجريمة ومعاملة المجرمين، خاصة فيما يتعلق بالجرائم التقنية أو جرائم الحاسوب. [1]

ويُشار هنا إلى أن المؤتمر السابع للأمم المتحدة حول الوقاية من الجريمة ومعاملة المجرمين، الذي عُقد في ميلانو، إيطاليا، في عام 1985[2]، أسفر عن مجموعة من القواعد التوجيهية التي تمت صياغتها بشكل كامل في الاجتماعات التحضيرية الإقليمية للمؤتمر الثامن، الذي أُقرت فيه هذه المبادئ والذي عُقد في هافانا، كوبا، في عام 1990. كما شدد المؤتمر على ضرورة تطبيق التطورات الحديثة في مجال العلم والتكنولوجيا لصالح العامة وبالتالي للوقاية من الجريمة بشكل فعال، وأكد على أنه نظرًا لأن التكنولوجيا قد تؤدي إلى ظهور أشكال جديدة من الجرائم، يجب اتخاذ تدابير مناسبة ضد سوء استخدام هذه التكنولوجيا.

وأشار المؤتمر إلى مسألة الخصوصية التي قد تتعرض للخطر من خلال الوصول إلى البيانات الشخصية المخزنة في أنظمة الحاسوب، والتي تُعد انتهاكًا لحقوق الإنسان وتعديًا على الحياة الخاصة، وأكد على ضرورة وجود ضمانات كافية لحماية السرية وإقرار أنظمة تضمن للأفراد الوصول إلى هذه البيانات وتصحيح الأخطاء فيها. وأكد المؤتمر من خلال قواعده التوجيهية على أهمية تشجيع التشريعات الحديثة التي تجرم وتعالج جرائم الحاسوب، باعتبارها نوعًا من أنواع الجرائم المنظمة مثل غسيل الأموال والاحتيال المنظم وإنشاء حسابات وتشغيلها باسماء وهمية. ويمكن تلخيص توصيات مؤتمر هافانا لعام 1990 وفقًا للمبادئ التالية[3]:

---

[1] نفس المرجع ،ص94

[2] محمود أحمد عبابنة ،جرائم الحاسوب وأبعادها الدولية الأردن: دار الثقافة للنشر والتوزيع الإصدار الثاني المجلد الأولى، عمان،2009.ص 156

[3] محمود أحمد عبابنة. المرجع الشابق . ص157

1. تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية.
2. تحسين أمن الحاسوب والتدابير الوقائية.
3. اعتماد إجراءات تدريب كافية للموظفين والوكالات المسؤولة عن التعامل مع الجريمة الاقتصادية والجرائم المتعلقة بالحاسوب والتحقيق والادعاء فيها.
4. تضمين آداب الحاسوب كجزء من المناهج الدراسية للاتصالات والمعلومات واعتماد سياسات تعالج المشكلات المتعلقة بالضحايا في هذه الجرائم[1].
5. زيادة التعاون الدولي لمكافحة هذه الجرائم. وقد عُقد المؤتمر التاسع للأمم المتحدة حول الوقاية من الجريمة ومعاملة المجرمين في القاهرة في عام 1995، حيث أكدت توصياته أيضًا على ضرورة حماية الأفراد في حياتهم الخاصة وفي ملكيتهم الفكرية من المخاطر المتزايدة للتكنولوجيا وضرورة التنسيق والتعاون بين الدول لاتخاذ الإجراءات المناسبة للحد منها.

وربما تكون أفضل استراتيجية طويلة الأجل لمكافحة الجريمة الإلسيبرانية[2] قد تكون الاستراتيجية الأمثل للتصدي للجريمة الإلكترونية على المدى الطويل هي عبر تعزيز التعاون الدولي وصياغة اتفاقيات متينة تضمن محاسبة مرتكبي جرائم الإنترنت. نظرًا للطبيعة العالمية للإنترنت، يمكن أن تظهر الجريمة الإلكترونية في أي مكان وتستهدف أي دولة تتواجد بها شبكة الإنترنت.

[1] المكتب الأممي المعني بالمخدرات والجريمة" .(UNODC) ،تقرير الامين العام ، مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية متاح على : https://www.unodc.org/documents/Cybercrime/SG_report/V1908180_A.pdf، تاريخ الوصول: 04:36 2024/05/31

[2] محمود أحمد عبابنة. نفس المرجع . ص158

تكمن التحديات في تعدد الاختصاصات القضائية التي تتجاوزها هذه الجرائم، وغالبًا ما تُبذل الجهود لمكافحتها عبر تدابير أمنية تقنية كمكافحة الفيروسات، فلترة البريد الإلكتروني غير المرغوب فيه، والتشفير. هذه التدابير قد تحول دون نجاح الهجمات الإلكترونية، لكنها لا تمنع الجناة من إيجاد أهداف أخرى. لذا، يُعتقد أن الحل الأكثر فعالية للقضاء على هجمات الإنترنت قد يكون من خلال تطبيق القانون بشكل صارم وضمان محاكمة الجناة.[1]

في ضوء التحديات المستمرة، تشدد المؤتمرات الدورية التابعة للأمم المتحدة على ضرورة تحديث القوانين الجنائية، وتعزيز أمن الحواسيب، وتطوير القدرات التحقيقية والتدريبية لمواجهة التهديدات السيبرانية. وتشير التوصيات الحديثة إلى أهمية تعزيز التعاون الدولي وتبادل المعرفة والخبرات لمكافحة الجريمة عبر الحدود، وضمان حماية الخصوصية وحقوق الإنسان في العصر الرقمي.

بشكل عام، يُعتبر تطبيق القوانين وتعزيز التعاون الدولي أساسيًا لمكافحة الجريمة السيبرانية، مع التركيز على تطوير السياسات الجديدة وتحديث القوانين لمواجهة التحديات المستمرة في العصر الرقمي.

الفرع الثاني

جهود المنظمات الدولية في مجال مكافحة الجريمة السيبرانية

تُعتبر المنظمات الدولية من أبرز الجهات التي تسعى لمكافحة هذا النوع من الجرائم بشكل فعّال، وفي فرعنا هذا سنتطرق الى اهم هذه المنضمات.

لقد أطلقت العديد من المنظمات الدولية مبادرات لمواجهة التحديات الناشئة عن الجريمة السيبرانية وتعزيز الأمن الإلكتروني[2]. من بين هذه المنظمات:

[1] االمجلس الأوروبي، المذكرة التفسيرية الاتفاقية بودابست 2001 النسخة المترجمة بالعربية،2014/05/12

[2] محمود أحمد عبابنة. المرجع السابق . ص166

1. **الاتحاد الدولي للاتصالات :(ITU)** يعمل على تطوير وتنسيق السياسات الدولية في مجال الاتصالات، ويهدف إلى تعزيز الاتصالات وتقنيات المعلومات على الصعيدين الوطني والدولي.
2. **الإنتربول / يوروبول** :يقدمان الدعم في مكافحة الجرائم العابرة للحدود، بما في ذلك الجرائم السيبرانية، من خلال التعاون الدولي وتبادل المعلومات والخبرات بين الدول الأعضاء[1].
3. **منظمة التعاون الاقتصادي والتنمية :(OECD)** تعمل على تعزيز السياسات التي تحسن الرفاهية الاقتصادية والاجتماعية حول العالم، بما في ذلك دعم استراتيجيات الأمن السيبراني وتعزيز التعاون الدولي في هذا الصدد.
4. **مؤسسة الإنترنت للأسماء والأرقام المخصصة :(ICANN)** تدير تخصيص مساحات العناوين على الإنترنت، وتعمل على تطوير وتنظيم نظام أسماء النطاقات والعناوين على شبكة الإنترنت بطريقة تضمن أمنها واستقرارها[2].
5. **المنظمة الدولية لتوحيد المقاييس (ISO) واللجنة الكهروتقنية الدولية :(IEC)** تطوران المعايير الدولية للتقنيات، بما في ذلك معايير الأمان السيبراني، لتعزيز التوافق وتبادل المعلومات بين الدول والمؤسسات الدولية.
6. **فرق عمل هندسة الإنترنت** :تعمل على تطوير وترويج معايير الإنترنت، بما في ذلك البروتوكولات والتقنيات الخاصة بالأمان السيبراني، لضمان تشغيل شبكة الإنترنت بكفاءة وأمان.

[1] منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، مذكرة ماجستير، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، 2012.ص 73

[2] زيدان، ربيعة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة – الجزائر، 2011، ص 44.

7. **المنظمات الإقليمية والدولية** :تعمل هذه المنظمات على تعزيز التعاون الإقليمي والدولي في مختلف المجالات، بما في ذلك الأمن السيبراني، وتضمن استمرارية الجهود المشتركة لمكافحة التهديدات السيبرانية على مستوى العالم[1].

تعمل هذه المنظمات على تعزيز التعاون الإقليمي والدولي في مختلف المجالات، بما في ذلك الأمن السيبراني. وسنأخذ في دراستنا منظمتين على سبيل المثال:

أولا: منظمة التعاون الاقتصادي والتنمية (OECD)

منظمة التعاون الاقتصادي والتنمية (OECD) تسعى لتحقيق التنمية الاقتصادية المستدامة والرفاه الاجتماعي. منذ عام 1978، أولت المنظمة اهتمامًا خاصًا بالجريمة السيبرانية، مُطلقةً مجموعة من الأدلة والقواعد الإرشادية المتعلقة بتكنولوجيا المعلومات. في عام 1980، اعتمد مجلس المنظمة دليلًا يركز على حماية الخصوصية وقواعد نقل البيانات، موصيًا الأعضاء بالالتزام به[2].

في عام 1983، أصدرت OECD تقريرًا بعنوان "الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية"، الذي استعرض السياسات الجنائية القائمة والمقترحات في الدول الأعضاء. التقرير حدد الأفعال التي يجب تجريمها[3]، مثل:

- الدخول غير المصرح به إلى أنظمة ومصادر الحاسب.
- الإفشاء غير المصرح به للمعلومات المعالجة آليًا، النسخ، الإتلاف، التخريب للبيانات والبرامج.

[1] زيدان، ربيعة،المرجع السابق،ص47

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 49.

[3] مراد مشوش، الجهود الدولية لمكافحة الاجرام السيبراني مجلة الواحات للبحوث والدراسات. المجلد 12، العدد726-703،01، 2017.ص710

- الإعاقة غير المشروعة للوصول إلى مصادر الحاسب.

في عام 1992، قدمت OECD توصيات وإرشادات خاصة بأنظمة المعلومات، مؤكدة على مبادئ عامة يجب أن تتبناها التشريعات الجنائية للدول الأعضاء، مثل:

1. حدود التجميع :فرض قيود على تجميع البيانات لحماية الخصوصية.
2. نوعية البيانات :البيانات يجب أن تكون مرتبطة بالغرض المحدد لاستخدامها.
3. تعيين الغرض :تحديد الغرض من استخدام البيانات الشخصية مسبقًا.
4. حدود الاستخدام :الالتزام بعدم إفشاء البيانات الشخصية لغير المصرح لهم.
5. الوقاية الأمنية :اتخاذ تدابير أمنية لحماية البيانات.
6. المشاركة الفردية :حق الأفراد في الوصول إلى بياناتهم والتحقق من صحتها.
7. المسائلة والمحاسبة :محاسبة المسؤولين عن البيانات في حالة الإخلال بالإجراءات الوقائية[1].

هذه المبادئ تعكس التزام OECD بتطوير إطار قانوني وسياسي يعزز الأمن السيبراني ويحمي الخصوصية والبيانات الشخصية[2].

ثانيا: الاتحاد الدولي للاتصالات(ITU)

في عام 2006، اعتمد المؤتمر العالمي لتنمية الاتصالات القرار رقم (45)، الذي دعا إلى تنظيم اجتماع حول الأمن المعلوماتي ومكافحة الرسائل الاقتحامية. وكان من المقرر أن يقدم مدير مكتب تنمية الاتصالات تقريرًا يتضمن نتائج هذا الاجتماع إلى مؤتمر المندوبين

[1] مراد مشوش،المرجع نفسه،ص 711

[2] الأشقر جبور منى،المرجع السابق،ص210

المفوضين في نفس العام. تم تبني عدة توصيات تتعلق بالأمن المعلوماتي والرسائل الاقتحامية، وفي مايو 2007، أطلق الأمين العام للاتحاد جدول أعمال الأمن المعلوماتي العالمي لمواجهة التحديات المتزايدة لأمن الإنترنت وإيجاد حلول لتعزيز الثقة والأمن في مجتمع المعلومات[1].

في أكتوبر 2007، تم تشكيل فريق من الخبراء رفيع المستوى (HLEG) يضم أكثر من مائة خبير، والذين قدموا تقاريرهم وتوصياتهم في يونيو 2008. وفي 12 نوفمبر 2008، تم نشر الإستراتيجية العالمية التي تضمنت مجالات متعددة مثل[2]:

- التدابير القانونية :تطوير الأطر القانونية لتعزيز الأمن المعلوماتي.
- التدابير التقنية :استخدام التكنولوجيا لحماية الأنظمة والشبكات.
- التدابير الإجرائية :تنفيذ السياسات والإجراءات للحفاظ على الأمن المعلوماتي.
- الهياكل التنظيمية :إنشاء هياكل تنظيمية لإدارة الأمن المعلوماتي.
- بناء القدرات :تطوير المهارات والقدرات اللازمة لمواجهة التحديات الأمنية.
- التعاون الدولي :تعزيز التعاون بين الدول لمكافحة التهديدات السيبرانية.

هذه الإستراتيجية تمثل جهودًا دولية متكاملة لتحسين الأمن المعلوماتي ومكافحة الجرائم الإلكترونية على مستوى العالم[3].

[1] عبد الإله النوايسة، جرائم تكنولوجيا المعلومات – شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية الأردن دار وائل للنشر والتوزيع، المجلد الأولى عمان.،2017،ص104

[2] عبد الإله النوايسة،نفس المرجع،ص104

[3] عبد الإله النوايسة،نفس المرجع،ص104

المطلب الثاني

الجهود الإقليمية في مكافحة الجريمة السيبرانية

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

الفرع الأول

المجلس الأوروبي

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

يجب على القوانين تحديد الإجراءات الدقيقة لتفتيش أجهزة الكمبيوتر والتحفظ على المعلومات المخزنة بها، بالإضافة إلى مراقبة المعلومات خلال عملية الانتقال من نقطة إلى أخرى.

[1] الأشقر جبور منى،المرجع السابق،ص217

- ينبغي للإجراءات الجزائية الوطنية أن تمنح السلطات المختصة الحق في ضبط البرمجيات والمعلومات الموجودة على الأجهزة تحت نفس الشروط المطبقة على التفتيش العادي، مع ضرورة إبلاغ صاحب الجهاز بأن النظام قد خضع للتفتيش وتحديد المعلومات التي تم ضبطها.
- خلال عملية التفتيش، يجب السماح للسلطات المنفذة بالوصول إلى أنظمة الكمبيوتر الأخرى ضمن نطاق اختصاصها والمتصلة بالنظام المفتش، وضبط المعلومات الموجودة بها إذا كان ذلك ضروريًا ومبررًا[1].
- يجب أن ينص قانون الإجراءات الجزائية على أن الإجراءات المتبعة مع الوثائق التقليدية تنطبق أيضًا على المعلومات المخزنة على أجهزة الكمبيوتر، ويجب تطبيق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي عند الضرورة في مجال تكنولوجيا المعلومات، مع الحفاظ على سرية المعلومات المحمية بموجب القانون.
- يجب على العاملين في المؤسسات الحكومية والخاصة التي تقدم خدمات الاتصال التعاون مع السلطات القضائية في إجراءات المراقبة والتسجيل[2].
- يجب تعديل القوانين الإجرائية لتمكين إصدار أوامر للأشخاص الذين يمتلكون معلومات متعلقة بأجهزة الكمبيوتر، سواء كانت برامج أو قواعد بيانات، لتسليمها والكشف عن الحقيقة.
- يجب منح سلطات التحقيق القدرة على إصدار أوامر للأشخاص الذين لديهم معلومات خاصة للدخول إلى أنظمة المعلومات أو الاطلاع على المعلومات المخزنة بها، واتخاذ الإجراءات اللازمة للسماح للمحققين بالوصول إليها.

[1] سالم عبد الرزاق، المرجع السابق، ص 32.

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

- يجب تطوير وتوحيد الأنظمة المتعلقة بالأدلة الإلكترونية لضمان الاعتراف بها عالميًا، وتطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.
- يجب إنشاء وحدات خاصة لمكافحة جرائم الكمبيوتر وتطوير برامج لتأهيل العاملين في مجال العدالة الجنائية لتحسين معرفتهم بتكنولوجيا المعلومات.
- قد تتطلب إجراءات التحقيق الوصول إلى أنظمة كمبيوتر خارج الدولة، ولتجنب اعتداء على سيادة الدول والقانون الدولي، يجب وضع قاعدة قانونية تسمح بمثل هذه الإجراءات، ولذلك تُعد الاتفاقيات الدولية ضرورية لتنظيم كيفية وتوقيت اتخاذ هذه الإجراءات.
- يجب وجود إجراءات سريعة ومناسبة ونظام اتصال يسمح للمحققين بالتواصل مع السلطات الأجنبية لجمع الأدلة، ويجب على السلطة الأجنبية السماح بإجراءات التفتيش والضبط[1].

الفرع الثاني

اتفاقية بودابست لمكافحة جرائم السيبرانية 2001

في أواخر عام 2001، شهدت بودابست، العاصمة المجرية، توقيع أول معاهدة دولية [2]تهدف إلى مكافحة جرائم الإنترنت، وذلك في إطار جهود المجلس الأوروبي لمواكبة التطورات التكنولوجية. تم إبرام الاتفاقية في 8 نوفمبر 2001 وفُتحت للمصادقة في 23 نوفمبر من نفس العام. هذه الاتفاقية[3]، المعروفة باسم اتفاقية بودابست، قدمت تعريفًا واضحًا لأهدافها وأدرجت قائمة بالجرائم الإلكترونية التي يجب على الدول الموقعة تجريمها ضمن

[1] شيخه حسين الزهراني ، نفس المرجع . ص753

[2] اتفاقية بودابست حول التعاون الدولي في مجال مكافحة الفساد،تم .توقيعها في 25نوفمبر 2010في بودابست، المجر.

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

تشريعاتها الوطنية، وتشمل جرائم مثل الإرهاب، تزوير بطاقات الائتمان، واستغلال الأطفال جنسيًا.

تُعتبر اتفاقية بودابست الأولى من نوعها في مجال مكافحة جرائم الإنترنت وتهدف إلى تنسيق القوانين الجديدة بين الدول المختلفة. تم صياغة نص الاتفاقية بعد مشاورات مكثفة بين الحكومات، أجهزة الشرطة، والمتخصصين في قطاع الكمبيوتر، بمساعدة خبراء من مجلس أوروبا ودعم من دول عدة، بما في ذلك الولايات المتحدة[1].

بعد دخولها حيز التنفيذ في الأول من يوليو 2004، أصبحت اتفاقية بودابست ركيزة أساسية في مكافحة الجرائم الإلكترونية على أعلى مستوى بين دول مجلس الاتحاد الأوروبي. وقد وقعت عليها العديد من الدول غير الأعضاء في مجلس أوروبا، مثل كندا، اليابان، جنوب إفريقيا، وصادقت عليها الولايات المتحدة. تُعد هذه الاتفاقية دعوة مفتوحة لدول العالم للانخراط في جهود مكافحة الجرائم الإلكترونية، وهي نتيجة لمحاولات استمرت منذ ثمانينيات القرن العشرين حتى تم تقديمها بشكلها النهائي في بودابست وتوقيعها من قبل ثلاثين دولة أوروبية، بما في ذلك الدول الأربع غير الأعضاء في المجلس الأوروبي التي شاركت في إعداد الاتفاقية، إلى جانب كندا، اليابان، جنوب إفريقيا، والولايات المتحدة. وقد تضمنت هذه الاتفاقية الأقسام التالية[2]

القسم الأول: تحديد المصطلحات

القسم الثاني: الخطوات الواجب اتخاذها في إطار التشريع الوطني

القسم الثالث: التعاون الدولي

القسم الرابع: الشروط النهائية حول الانضمام إلى الاتفاقية.

[1] نسيمة درار ،نفس المرجع،ص 275

[2] نسيمة درار .نفس المرجع .ص274

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

- الجرائم المتعلقة بأمن الشبكات الدخول والمراقبة غير المشروعة والعدوان على الثقة في البيانات أو على النظام والإساءة إليه : الجرائم المعلوماتية كما هو الشأن في الاختلاق والانتحال والنصب والاحتيال المعلوماتي... الخ[1]
- جرائم الأخلاق مثل إنتاج أو بث أو حيازة ما يتعلق بدعارة الأطفال
- جرائم العدوان على حقوق الملكية الأدبية والفكرية كاستنساخ المصنفات المشمولة الي بالحماية
- المسؤولية الجنائية للأشخاص المعنوية، وكذلك الاهتمام بالإجراءات الجنائية لاسيما في مرحلة التحقيق والملاحقة القضائية مثل التحفظ على الأدلة والتفتيش والضبط وما إلى ذلك وقد حملت هذه الاتفاقية الطابع التوجيهي للخطوات التي يلزم اتخاذها في إطار التشريع الوطني[2] في كل دولة فيما يتعلق بالأحكام الموضوعية والإجرائية كما أشرنا أعلاه وألزمت الدول الأعضاء بمراعاة حقوق الإنسان وحرياته الأساسية التي تضمنتها الاتفاقيات الدولية والتشريعات الوطنية على حد سواء والالتزام بعدم انتهاكها، مع إمكانية الدول الأخرى غير الأعضاء في الاتفاقية الاستعانة بهذه الاتفاقية، عند إعداد التشريعات الوطنية باعتبارها مصدر تاريخي في مجال مكافحة الجريمة على الانترنت.[3]
- كما تضمنت الاتفاقية جانب آخر من التعاون انصب هذه المرة حول تدريب أعوان الأمن الإكسابهم خبرات عملية كما ورد في التوصية الصادرة عن اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم السيبرانية، وتعد الولايات المتحدة الأمريكية

[1] نسيمة درار .نفس المرجع .ص278

[2] شيخه حسين الزهراني ، نفس المرجع . ص766

[3] التقرير التفسيري الاتفاقية بودابست الصادر خلال الدورة 109 عن لجنة الوزراء للمجلس الأوروبي

من الدول المتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية والشبكات وهى تساعد على تدريب أجهزة الشرطة وقضاة الدول الأخرى، بتمكينها من تعزيز قدراتها على ضبط مشاكل هذه الجرائم، قبل أن تفلت منها زمام الأمور فقد أوجدت وزارة العدل الأمريكية مكتب للمساعدة والتدريب لتطوير أجهزة الادعاء العام في الدول الأخرى، ويعمل إلى جانبه البرنامج الدولي للمساعدة والتدريب (ICITAP) التوفير المساعدات لأجهزة الشرطة بالدول النامية[1]

جامعة الدول العربية، في إطار جهودها لمكافحة الجرائم السيبرانية، أصدرت قانونًا استرشاديًا يهدف إلى توحيد الجهود العربية في هذا المجال. تم التوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في 21 ديسمبر 2010، وهي تسعى لتعزيز التعاون بين الدول العربية للحفاظ على أمن وسلامة مجتمعاتها من خلال تجريم الأعمال غير المشروعة التي تُرتكب عبر الفضاء السيبراني.

تدعو الاتفاقية الدول العربية المصدقة عليها إلى مواءمة تشريعاتها مع أحكام الاتفاقية، وتجريم الجرائم الإلكترونية الجديدة لمنع استخدام الإنترنت في الأنشطة الإرهابية. كما تشدد على أهمية التعاون الدولي والإقليمي لمواجهة جرائم الإرهاب الإلكترونية وتعزيز الأمن في المناطق الحيوية مثل المطارات والموانئ.

بالإضافة إلى ذلك، تحث الاتفاقية الدول العربية على التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات في أنشطتهم الإرهابية، وتؤكد على أهمية بناء القدرات اللازمة لمواجهة هذا الخطر.

[1] جمال بوازدية الاستراتيجية الجزائرية في مواجهة الجريمة السيبرانية" التحديات والأفاق المستقبلية"، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 3 أفريل2019،ص13

هذه الجهود تأتي في سياق دولي يشهد تعاونًا متزايدًا لمكافحة الجرائم السيبرانية، والتي تتجاوز الحدود الجغرافية، مما يستدعي تعاونًا دوليًا مكثفًا ومتواصلًا. اتفاقية بودابست تُعتبر مثالًا على هذا التعاون، حيث تُشكل دعوة للدول لتحديث تشريعاتها والانخراط في جهود مكافحة الجرائم الإلكترونية على مستوى عالمي.

الفرع الثالث

إتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية

أصدرت جامعة الدول العربية قانونًا إرشاديًا يهدف إلى محاربة الجرائم الإلكترونية في الفضاء السيبراني[1]، حيث عملت الدول العربية على تنظيم وتجريم الأفعال غير القانونية المنفذة عبر الفضاء السيبراني من خلال التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 21/12/2010[2]، بهدف تعزيز التعاون العربي في مجال مكافحة الجرائم السيبرانية وضمان الأمن وحماية المجتمعات. وقد حث المجلس الدول العربية الموقعة على الاتفاقية على إبلاغ الأمانة الفنية للمجلس بالخطوات المتخذة لتوافق تشريعاتها مع مقتضيات الاتفاقية، وتجريم الأشكال الجديدة من الجرائم الإلكترونية لمنع الإرهابيين من استغلال الإنترنت، وتشجيع التعاون مع الهيئات الدولية والإقليمية لمواجهة جرائم الإرهاب الإلكتروني بكافة أنواعها. كما شدد المجلس على ضرورة التعاون العربي لمنع الإرهابيين من استخدام تقنيات المعلومات والاتصالات والإنترنت في التحريض وتمويل وتخطيط أعمالهم الإرهابية، وأكد على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة لتطوير القدرات اللازمة لمواجهة خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، وتأمين

[1] اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية .تبنيتها في 21 ديسمبر 0201 من قبل الجامعة العربية

[2] محمد عبد الجواد أميرة عبد العظيم ، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام. مجلة الشريعة والقانون الجزء 03، العدد 35 361-541. 2020 ،ص 499

المطارات والموانئ والحدود. وعلى الرغم من هذه الجهود الدولية، سواء على مستوى الأمم المتحدة أو المنظمات الدولية أو على المستوى الإقليمي، وخصوصًا اتفاقية بودابست التي تمثل دعوة للدول لمراجعة تشريعاتها الوطنية والتعاون الدولي لمكافحة الجرائم السيبرانية التي تتجاوز الحدود الجغرافية. . إلا هناك صعوبات تواجه هذه الجهود سنتطرف إلى هذه الصعوبات وكيفية القضاء عليها في هذا المطلب.

المطلب الثالث:

الصعوبات والتحديات التي تواجه الجهود الدولية كيفية القضاء عليها

رغم الجهود التي تبذلها المنظمات والهيئات الدولية في مكافحة الجرائم السيبرانية إلا هناك عوائق وصعوبات تقف في كعارض في نفاذ هذه الاتفاقيات الدولية والإقليمية سوف نتطرق لها في هذا المطلب ونتناول كيفية القضاء عليها.

الفرع الأول

الصعوبات التي تواجه الجهود الدولية

يُطالب البعض بإنشاء وحدات متخصصة في مكافحة الجرائم المعلوماتية على غرار الأجهزة الجنائية الوطنية والدولية مثل الإنتربول، لتوثيق الجرائم عند حدوثها وتحديد الأدلة والجناة، مما يستدعي تطوير نموذج تعاون دولي فعّال لمكافحة الاعتداءات على المعلومات الخاصة وتبادل الخبرات والمعلومات حول هذه الجرائم ومرتكبيها وكيفية مواجهتها. وعلى الرغم من الدعوات للتعاون الدولي في هذا المجال، تواجه عدة تحديات تعيق هذا التعاون، ويمكن تلخيصها في النقاط التالية:

أولًا :غياب نموذج موحد للنشاط الإجرامي، نظرًا لعدم توافق الأنظمة القانونية العالمية على تعريفات محددة لما يُعتبر إساءة استخدام لنظم المعلومات، وهذا يعود إلى قصور التشريعات

الحالية التي لا تواكب التطور السريع في مجال تكنولوجيا المعلومات وبالتالي الجريمة المعلوماتية[1].

ثانيًا :نقص المعاهدات الثنائية أو الجماعية التي تسمح بتعاون فعّال في مكافحة هذه الجرائم، وحتى في حال وجودها، فإنها تظل غير كافية لتوفير الحماية المطلوبة في ظل التقدم المتسارع لتكنولوجيا الحاسوب والإنترنت.

ثالثًا :عدم وجود تنسيق بين الدول في الإجراءات الجنائية المتعلقة بالجريمة المعلوماتية، خاصة فيما يتعلق بالتحقيق وجمع الأدلة، مما يجعل الحصول على الدليل في هذه الجرائم خارج حدود الدولة أمرًا صعبًا للغاية[2].

رابعًا :مشكلة الاختصاص في الجرائم الإلكترونية، حيث تُثار مسألة الاختصاص بشكل متكرر بسبب التداخل والترابط بين شبكات المعلومات، وهذا يعقد الحصول على الأدلة ويؤثر على تطبيق الإجراءات الجنائية.

تُظهر هذه التحديات الحاجة الماسة إلى تشريعات جنائية أكثر مرونة تواكب التقدم التكنولوجي وعصر المعلوماتية، وتسهيل التحقيقات في بيئة تكنولوجيا المعلومات وفقًا للمعايير الدولية. ومن الضروري وضع قواعد قانونية واضحة تسمح بالتدخل السريع والفعّال عبر الحدود الوطنية دون انتهاك سيادة الدول أو القانون الدولي.

---

[1] ليندا شرابسة ، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية مجلة دراسات وأبحاث المجلد 01 . العدد24101-253. 2009،ص250

[2] محمد عبد الرحمان نصيرات وائل. الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC – جامعة الإمام محمد بن سعود الإسلامية المملكة العربية السعودية2015،.ص 134

الفرع الثاني

كيفية القضاء على الصعوبات التي تواجه الجهود الدولية في مكافحة جرائم السبرانية

تشهد التقنيات الرقمية والاتصالات الحديثة تطورًا سريعًا، مما يفتح أبوابًا جديدة للفرص والتحديات على حد سواء. تتضمن هذه التطورات تزايدًا ملحوظًا في جرائم السبرانية، التي تشكل تهديدًا خطيرًا على المستوى الدولي.

تعد مكافحة جرائم السبرانية تحديًا كبيرًا للمجتمع الدولي، حيث تعاني الجهود الدولية في هذا الصدد من العديد من الصعوبات.وهذا ما سنتطرق اليه في فرعنا هذا.[1]

أولًا :لحل العقبات المتعلقة بالمساعدات القضائية الدولية:

1. تبادل المعلومات :يشمل هذا تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها السلطات القضائية الأجنبية أثناء التحقيق في جريمة ما، بما في ذلك الاتهامات الموجهة إلى رعاياها في الخارج والإجراءات المتخذة ضدهم.
2. نقل الإجراءات :يعني هذا أن دولة ما، بناءً على اتفاقية أو معاهدة، تتخذ إجراءات جنائية بشأن جريمة ارتُكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، شريطة توافر شروط معينة[2].

ثانيًا :لحل عقبة عدم وجود نموذج موحد للنشاط الإجرامي:

يتمثل الحل في توحيد النظم القانونية وتقليل الفوارق بين الأنظمة العقابية الداخلية، من خلال تحديث التشريعات المحلية المتعلقة بالجرائم المعلوماتية وإبرام اتفاقيات خاصة تأخذ في الاعتبار هذا النوع من الجرائم[3].

---

[1] جمال بوازدية ،المرجع السابق،ص87

[2] إلهام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016،ص71.

[3] بكر أبو بكر، الإرهاب الالكتروني من الدعاة والاستقطاب إلى اكتساح المجال الافتراضي، المغرب، مجلة ذوات، العدد 46، 2018.ص39

ثالثًا :لحل عقبة تنوع واختلاف النظم القانونية الإجرائية:

تشجع الصكوك الدولية الصادرة عن الأمم المتحدة الدول على استخدام تقنيات التحقيق الخاصة، مما يخفف من اختلاف النظم القانونية والإجرائية ويفتح المجال لتعاون دولي فعّال. على سبيل المثال، تشير المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية إلى التسليم المراقب والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة[1].

رابعًا :لحل عقبة عدم وجود قنوات اتصال:

تشجع الصكوك الدولية الدول على إنشاء قنوات اتصال بين السلطات المختصة والوكالات والدوائر المتخصصة لتسهيل الحصول على المعلومات وتبادلها، كما هو الحال في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة[2].

[1] منى الأشفر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، مذكرة ماجستير، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، 2012.،ص89

[2] محمد عبد الرحمان نصيرات وائل ، الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC – جامعة الإمام محمد بن سعود الإسلامية المملكة العربية السعودية،2015، ص135.

المبحث الثاني:

الآليات مكافحة الجرائم السبرانية في ضل التشريع الجزائري.

شهدت الجزائر، كغيرها من الدول، تزايدًا في الجرائم السيبرانية مع تقدم التكنولوجيا وتوسع استخدام الإنترنت ووسائل التواصل الاجتماعي. لمواجهة هذا التحدي، يتعين على الدول أن تعمل على تحديث تشريعاتها ووضع آليات فعّالة لمكافحة الجرائم السيبرانية وتطبيقها بفعالية.

سنستعرض في هذا المبحث الآليات التي وضعتها الجزائر لمكافحة الجرائم السيبرانية وفقًا للتشريعات المعمول بها في البلاد. سنتناول استعراضًا للقوانين والتشريعات ذات الصلة، وكيفية تطبيقها على أرض الواقع،. ففي المطلب الاول سنتطرق الى الاليات التشريعية لمواجهة هذا النوع من الجرائم ونتناول في في المطلب الثاني الجهات المختصة في البحث والتحري ومكافحة الجريمة السيبرانية

المطلب الأول:

الآليات التشريعية لمواجهة الجرائم السبرانية .

مواجهة الجرائم السيبرانية تتطلب إطاراً قانونياً قوياً وفعّالاً. في السياق الجزائري، تم تبني عدة آليات تشريعية لمكافحة الجرائم السيبرانية، هذه الآليات تشكل جزءًا من الجهود المبذولة لمكافحة الجرائم السيبرانية في الجزائر، وتعكس التزام الحكومة بتعزيز الأمن السيبراني وحماية المعلومات والبنية التحتية الرقمية للبلاد.، وعليه قسمنا المطلب الأول الى فرعين، يتناول الفرع الاول القواعد الموضوعية المنظمة للجرائم السيبرانية اما الفرع الثاني فجاء تحت عنوان القواعد الاجرائية لمكافحة الجريمة السيبرانية.

الفرع الأول :

القواعد الموضوعية المنظمة للجرائم السيبرانية.

تأثر المشرع الجزائري باتفاقية بودابست 2001 يعكس التزام الدول بتعزيز التعاون الدولي في مكافحة الجرائم السيبرانية. من خلال التعديلات التي أدخلها على قانون العقوبات والنصوص القانونية الأخرى، يسعى المشرع إلى توفير الحماية اللازمة للأفراد والمؤسسات من التهديدات السيبرانية وتوفير آليات فعالة لمكافحتها.ففي هذا الفرع سنتطرق الى الاليات الموضوعية لمكافحة الجريمة السيبرانية في اطار القواعد العامة والقواعد الخاصة.

أولا: الآليات الموضوعية في إطار القواعد العامة

تدخل المشرع بأليات قانونية لمواجهة الجريمة السيبرانية حيث عمد إلى الحماية بموجب الدستور والقانون المدني وقانون العقوبات ونستعرضها على النحو التالي:

1/: الحماية بموجب الدستور والقانون المدني

الدستور الجزائري لسنة 2020 يضمن حماية حقوق الأساسية والحريات الفردية للمواطنين، ويُلزم الدولة بعدم انتهاك حرمة الإنسان. يتجلى هذا التأكيد على الحقوق الأساسية والحريات الفردية في مختلف جوانب الحياة العامة، ويتطلب تطبيق هذه المبادئ تبني نصوص تشريعية تحظر أي تجاوز على هذه الحقوق[1].

ومن أهم المبادئ الدستورية العامة التي تجسد هذه الحماية:

- **المادة 35** :الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.
- **المادة 47** : لكل شخص الحق في حماية حياته الخاصة وشرفه.

[1] بوضياف إسمهان الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، المجلد 03، العدد 03 سبتمبر 2018، ص 362

- لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت .
- لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.
- حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي
- يعاقب القانون على كل انتهاك لهذه الحقوق".
- **المادة 54/6:** الحق في نشر الأخبار والأفكار والصور والآراء في إطار القانون، واحترام ثوابت الأمة وقيمها الدينية والأخلاقية والثقافية. "

ترتيباً على الأهمية الدستورية لحرمة الحياة الخاصة، فقد سارع المشرع إلى وضع تشريعات تحمي هذا الحق المهم. وقد نص المشرع على أن كل من يتعرض لاعتداء غير مشروع في حق أي من الحقوق المتعلقة بشخصيته يحق له طلب وقف هذا الاعتداء والمطالبة بالتعويض عن الضرر الناجم عنه.

تجد هذه الحماية المباشرة في المادة 124 من التشريع المدني الجزائري، التي تنص على ان :**(كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض.")**[1]

ثانيا : المكافحة بموجب قانون العقوبات

يعتبر قانون العقوبات وسيلة ردعية للكف عن ارتكاب الجرائم بصفة عامة، وبما أن الجرائم المعلوماتية تلحق أضرارًا بالغير فقد أقر المشرع عقوبات ردعية لتلك الجرائم وهي كالتالي:

[1] بوضياف إسمهان ، المرجع السابق،ص363

1. المساس بأنظمة المعالجة الآلية للمعطيات

وهي من أبرز الجرائم التي عالجتها المحاكم الجزائرية، وذلك بموجب القانون رقم 04-15[1] المتعلق بقانون العقوبات، من خلال المواد 394 مكرر إلى 394 مكرر 7[2]. من خلال استقراء هذه النصوص، حاول المشرع الجزائري حصر الجرائم والعقوبات المقررة لها، على النحو التالي:

أ- جريمة دخول معالجة آلية للمعطيات:

عن طريق الغش نصت عليها المادة 394 مكرر [3] من قانون العقوبات، حيث تعاقب بالحبس والغرامة عند الدخول أو البقاء بالغش في المنظومة. وقد فرق المشرع في هذه الحالة بين ما إذا كانت الجريمة بسيطة، إذ تُضاعف العقوبة إذا ترتب عنها حذف أو تغيير في المنظومة، أو إذا أدى ذلك إلى تخريب النظام أو تعطيل اشتغال المنظومة.

ب-جريمة إزالة أو تعديل معطيات في نظام المعالجة الآلية بطرق تدليسية:

نصت عليها المادة 394 مكرر 1[4] من قانون العقوبات. اعتبر المشرع الجزائري أن إزالة أو تعديل المعطيات التي يتضمنها النظام بطرق تدليسية عملان إجراميان. يقصد بإزالة المعطيات، سواء جزئياً أو كلياً، محوها أو إتلافها أو تخريبها من أجل منع النظام من القيام بمهامه أو تعطيل النظام المعلوماتي. وتشمل الطرق المتعددة لتحقيق ذلك نشر الفيروسات.

---

[1] قانون رقم 15-04 مؤرخ في 10/11/2004 وعدل و يتمم الأمر رقم 66 - 156 يتضمن قانون العقوبات، جريدة 12 رسمية عدد 71، صادر بتاريخ 10/11/2004 معدل و متمم

[2] القانون 04-15 المؤرخ في 10 نوفمبر 2004 الصادر في الج. رج رقم 71 المتضمن تعديل قانون العقوبات لسنة 2004 ص ص 11 و 12، والذي أضيفت بموجبه المواد من 394 مكرر إلى 394 مكرر 07

[3] أنظر المادة 394 مكرر من القانون 04-15 ، المرجع السابق.

[4] نظر المادة 394 مكرر 2من القانون 04-15 ، المرجع نفسه

أما تعديل المعطيات فيشمل إدخال معلومات وهمية أو تزوير البيانات الموجودة في النظام المعلوماتي.

ج- جرائم نشر، حيازة، أو الاتجار بالمعطيات المخزنة أو المعالجة:

نصت عليها المادة 394 مكرر 02 من قانون العقوبات. تعتبر هذه الجريمة من أكثر الجرائم شيوعًا في العالم الافتراضي. اعتبر المشرع الجزائري أن عملية اصطناع برنامج مخصص لارتكاب فعل الغش المعلوماتي أو إعداد برنامج ناقص من الناحية الفنية، وخاصة المبرمج من أجل خلق فجوات وثغرات فيه لتمكين ممارسة فعل الغش أو تجميع أو التقاط البيانات بغرض استغلالها أو نشرها خاصة عن طريق الإنترنت أو الاتجار فيها، من الجرائم المعاقب عليها. تُعاقب جريمة الإنشاء والنشر بشكل خاص نظرًا لما تشكله من خطورة على الحياة الخاصة.

د. جرائم المعالجة الآلية الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام:

نصت عليها المادة 394 مكرر 3[1] من قانون العقوبات. اعتبر المشرع الجزائري أن الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي مؤسسة رسمية تشكل ظرف تشديد للعقوبة. وتستخلص من نص المادة 394 مكرر 3 من قانون العقوبات أن العقوبات المشددة تطبق على جميع الجرائم المنصوص عليها في المادة 394 مكرر والمادة 394 مكرر1 ومكرر 2 من قانون العقوبات. حرص المشرع الجزائري على ضمان حماية مطلقة لهيئات الدفاع

[1] نظر المادة 394 مكرر 3من القانون 04-15 ، المرجع السابق

الوطني ومؤسسات الدولة الجزائرية، وتوسع في هذه الحماية بإدراج جميع الجرائم المنصوص عليها في المادة 394 مكرر من قانون العقوبات[1].

هـ. الجرائم المعلوماتية للشخص المعنوي:

نصت عليها المادة 394 مكرر 4[2] من قانون العقوبات. أقر المشرع الجزائري المسؤولية الجزائية للأشخاص المعنوية وشدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية. تتراوح الغرامة المطبقة على الشخص المعنوي بين واحد إلى خمس أضعاف الغرامة المقررة على الشخص الطبيعي.

و. جريمة تكوين جمعية أشرار المعلوماتيين لغرض التحضير للجرائم الماسة بأنظمة المعالجة الآلية

نصت عليها المادة 394 مكرر 5[3] من قانون العقوبات. يتضح من خلال نص المادة أن العقوبة تطال من يشارك في أي مجموعة أو اتفاق يهدف إلى التحضير أو الإعداد لارتكاب الجرائم المعلوماتية مع توفر القصد الجنائي. كما يستخلص أن مجرد المشاركة أو الاتفاق المجسد بفعل مادي يوحي بالتحضير للجريمة، خاصة أن ذلك يمكن أن يتم عبر الشبكات المعلوماتية.

ك. العقوبات التكميلية

وفقا للمادة 394 مكرر6 [4] من قانون العقوبات، نص المشرع في هذه المادة على العقوبات التكميلية للجرائم السالفة الذكر، وتتمثل في المصادرة للأجهزة المستعملة والبرامج والوسائل المستعملة، مع إلحاق ذلك بغلق المواقع وأماكن الاستغلال شريطة أن تكون بعلم صاحبها.

---

[1] فاروق خلف الآليات القانونية لمكافحة الجريمة المعلوماتية مجلة الحقوق والحريات كلية الحقوق جامعة محمد خيضر بسكرة المجلد 03، العدد 02، 2015، ص16

[2] نظر المادة 394 مكرر 4من القانون 04-15 ، المرجع السابق.

[3] نظر المادة 394 مكرر 5من القانون 04-15 ، المرجع نفسه.

[4] نظر المادة 394 مكرر 6من القانون 04-15 ، المرجع السابق.

ل. العقاب على الشروع في الجريمة المعلوماتية

طبقا لنص المادة 394 مكرر 7[1] من قانون العقوبات، فإن فعل الشروع أو البدء في ارتكاب الجريمة يعاقب عليه بنفس العقوبة المقررة للجريمة ذاتها. ونظرا لكون جرائم الاعتداء على نظام المعالجة الآلية ذات وصف جنحوي، أقر المشرع العقاب لها بنفس العقوبة المقررة للجريمة المكتملة.

م. استعمال تكنولوجيا الإعلام لارتكاب أفعال إرهابية

نصت عليها المادة 87 مكرر 11[2] من قانون العقوبات. تُعتبر جناية يعاقب عليها بالسجن من 10 إلى 15 سنة وبغرامة من 100،000 إلى 500،000 د.ج عند استعمال تكنولوجيا الإعلام والاتصال بغرض ارتكاب أفعال إرهابية، تدبيرها، الإعداد لها، المشاركة فيها، التدريب على ارتكابها، أو لتلقي التدريب عليها.

كما تضمنت المادة 394 مكرر 8[3] صور الأفعال التي يعاقب عليها القانون مقدم خدمات الإنترنت عند رفضه لإعذارات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أو صدور أوامر وأحكام قضائية[4].

2. حماية حرمة الحياة الخاصة

جاء القانون رقم 06-23[5] المتعلق بقانون العقوبات ليحمي حرمة الحياة الخاصة. حيث تنص المادة 303 مكرر[6] من قانون العقوبات على معاقبة كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت، سواء بالتقاط أو تسجيل أو نقل صور أو

[1] نظر المادة 394 مكرر 7من القانون 04-15 ، المرجع انفسه.

[2] انظر المادة 87 مكرر 11 من القانون 16-02 المتضمن تعديل قانون العقوبات.

[3] انظر المادة 394 مكرر 8 من القانون رقم 15-04 المرجع السابق

[4] مشوش مراد الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال مجلة القانون المجلد 09 ، العدد 01 ، سنة 2020، ص ص 118- 119

[5] القانون 06-23 المؤرخ في 20/12/2006 المتضمن قانون العقوبات ،الجريدة الرسمية عدد 48، الصادرة 2006/12/24

[6] نظر المادة 303 مكرر، المرجع نفسه.

مكالمات خاصة أو سرية، بالحبس والغرامة. أما المادة 303 مكرر 1[1] من قانون العقوبات، فتعاقب بالعقوبة ذاتها على من يحتفظ دون إذن أو يضع في متناول الجمهور الصور أو الوثائق بأية وسيلة كانت.

3.حماية حرمة رموز الدولة

تم تعديل قانون العقوبات من خلال القانون رقم 11-14[2] المؤرخ في 02 أغسطس 2011، حيث نصت المادة 144[3] مكرر منه على معاقبة كل من أساء لرئيس الجمهورية بأي وسيلة كانت، بما في ذلك الوسائل الإلكترونية، بعقوبة الغرامة المالية فقط. وفي حالة العود، تتضاعف الغرامة.

ثانيا: الآليات الموضوعية في إطار القواعد الخاصة

1. الحماية المتعلقة بالأطفال القصر

تضمن القانون رقم 14-01 المؤرخ في 4 فبراير 2014، الذي يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، إضافة المادة 333 مكرر 1 من القسم الثاني في ترك الأطفال والعاجزين وتعريضهم للخطر وبيع الأطفال. تنص هذه المادة على تجريم تصوير قاصر لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة حقيقية أو غير حقيقية، أو تصوير الأعضاء الجنسية للقاصر لأغراض جنسية. كما يعاقب على إنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر[4].

---

[1] أنظر المادة 303 مكرر1 امن القانون 06/23 ، المرجع السابق .

[2] القانون 11-14 المؤرخ في 02/08/2011، المتضمن قانون العقوبات الجريدة الرسمية عدد 44 صادرة في: 10/08/2011.

[3] أنظر المادة 144 مكرر، المرجع نفسه.

[4] شرف الدين وردة د. بلجراف سامية الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية جامعة يحي فارس المدية، العدد 03، ديسمبر 2017 ،ص37

2. الحماية المتعلقة بالبريد والاتصالات الإلكترونية

الحماية المتعلقة بالبريد والاتصالات الإلكترونية تضمن القانون رقم 18-04[1] القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية جملة من التدابير الجديدة المنظمة، منها إدراج الانفتاح في القطاع وهذا بموجب المواد 101 إلى 105 بخصوص العديد من النقاط على غرار التوصيل البيني، كما يلزم المتعامل التاريخي صاحب رخصة إقامة واستغلال شبكة اتصالات إلكترونية ثابتة مفتوحة للجمهور بالاستجابة وفق شروط موضوعية وشفافة ، التوصيل البيني والنفاذ إلى الشبكات، بما فيه التفكيك والنفاذ إلى المصادر ذات الصلة والتمركز المشترك.

كما ينص القانون في مادته الـ104 على إلزام كل متعامل مستفيد من تفكيك الحلقة المحلية، في حدود قدراته الموضوعية، تقاسم منشأته الكامنة مع باقي المتعاملين، لاسيما منها القنوات ومواقع المحطات الهيرتزية والمحلات التقنية .[2]

وجاء هذا القانون تكميلية للقانون رقم : 2000-03[3] المتعلق بالبريد والمواصلات السلكية واللاسلكية يحدد مفهوم المواصلات السلكية واللاسلكية، ولقد تضمن الفصل الثاني من الباب الرابع من هذا القانون الأحكام الجزائية المترتبة في حالة مخالفة النظام القانوني، فالأشخاص المرخص لهم بتقديم خدمة المواصلات السلكية واللاسلكية والعمال لدى متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق

---

[1] القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج. ر.ج العدد 27 بتاريخ 13 مايو 2018، ص 03

[2] نسرين العراش، صدور القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، 6 يونيو 2018 ، على الموقع الإلكتروني التالي https://www.aljazairalyoum.dz :، تاريخ التصفح 31مايو2021 على الساعة 22:49

[3] القانون 2000-03 المؤرخ في 05/08/2000 الذي يحدد القواعد العامة المتعلقة بالبريد السلكية واللاسلكية، الجريدة الرسمية عدد 48، المؤرخة في2000/08/06

المواصلات السلكية واللاسلكية أو الذين يأمرون أو يساعدون في ارتكاب هذه الأفعال فيعاقبون طبقا لما يقضي به نص المادة 137[1] من قانون العقوبات.[2]

3. الحماية المتعلقة بالتأمينات الاجتماعية

جاء القانون رقم 08-01[3] المؤرخ في 23 يناير 2008، ليعدل القانون 83-11 المؤرخ في 2 يوليو 1983، بإضافة "أحكام جزائية" تتضمن المواد 93 مكرر 2 إلى 93 مكرر 6. يجرم هذا القانون تسليم أو استلام البطاقة الإلكترونية للمؤمن له اجتماعياً أو المفتاح الإلكتروني لهيكل العلاج أو مهني الصحة بهدف الاستعمال غير المشروع، وكذلك تعديل أو حذف المعطيات المدرجة في البطاقة بطرق غير مشروعة[4].

4. الحماية من خلال قانون الملكية الأدبية والفنية

وسع المشرع الجزائري قائمة المؤلفات المحمية في قانون حقوق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم 03-05[5] المؤرخ في 23 يوليو 2003، ليشمل برامج المعلوماتية وقواعد البيانات. ينص القانون على عقوبات تصل إلى الحبس من 6 أشهر إلى 3 سنوات وغرامات تصل إلى مليون دينار جزائري للمخالفين. يمكن أن تتضاعف العقوبات في حالة العود، وتتضمن العقوبات التكميلية مصادرة المبالغ المتأتية من الاستغلال غير الشرعي ومعدات النسخ غير المشروعة[6].

---

[1] أنظر المادة 137، المرجع السابق.

[2] . بوعناد فاطمة زهرة مكافحة الجريمة الالكترونية في التشريع الجزائري مجلة الندوة للدراسات القانونية، كلية الحقوق والعلوم السياسية جامعة سيدي بلعباس .العدد 01، 2013، ص 67.

[3] القانون 08-01 المؤرخ في 23/01/2008 المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، عدد 04، صادرة في 27/01/2008

[4] الأمر 03-05 المؤرخ في 19/07/2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 44، صادرة بتاريخ 2003/07/23

[5] فاروق خلف، المرجع السابق، ص 18

[6] المادة 153 من القانون 03-05 المرجع السابق.

5. استحداث نصوص جديدة في التشريع الجزائري

استحدث القانون رقم 15-04[1] المؤرخ في 1 فبراير 2015 القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، مما يضمن بيئة إلكترونية آمنة للمعاملات عبر الإنترنت. لتعزيز حماية المستهلك الإلكتروني، صدر القانون رقم 18-05[2] المؤرخ في 10 مايو 2018 المتعلق بالتجارة الإلكترونية. كما عزز القانون رقم 18-07[3] المؤرخ في 10 يونيو 2018 حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وجاء المرسوم التنفيذي رقم 20-233 المؤرخ في 22 نوفمبر 2020 ليعزز الإعلام الإلكتروني بحق الرد وحق التصحيح الإلكتروني، مما يدعم الصحافة الإلكترونية ويتماشى مع أهداف القانون العضوي رقم 12-05 المتعلق بالإعلام.

الفرع الثاني

القواعد الإجرائية المنظمة لمكافحة الجرائم السبرانية .

تضمنت التعديلات المختلفة لقانون الإجراءات الجزائية الجزائري عدة قواعد إجرائية جديدة لمواجهة الجريمة المعلوماتية شأنها شأن الجريمة المنظمة وأشكالها، حيث خص المشرع الجزائري هذه الجرائم بجملة من الإجراءات الخاصة تمس كل من مرحلة البحث والتحري التحقيق والمحاكمة. وتكمن خصوصية إجراءات المتابعة في الجريمة الالكترونية، وهذا ما سيتناوله فرعنا فيما يلي:

---

[1] رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين المنشور بالج ر . ج عدد 6 مؤرخة في 10 فبراير 2015، ص 6

[2] القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018، المتعلق بالتجارة الإلكترونية، المنشور بالج. ر. ج رقم 28، الصادرة يوم 16 ماي 2018

[3] القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الصادر في الج. رج العدد 34 بتاريخ 10 يونيو 2018، ص 11.

أولا: تمديد الاختصاص المحلي.

تمديد الاختصاص المحلي لكل من ضباط الشرطة القضائية وقاضي التحقيق ووكيل الجمهورية المادة 37من ق إ ج[1] إذا تعلق الأمر بالجريمة المنظمة وجرائم المعالجة الآلية للمعطيات، الإرهاب، تبييض الأموال وجرائم الصرف، ولعل اعتماد الاختصاص الإقليمي الموسع هو المواجهة الفعالة لطائفة من الجرائم المنظمة الخطيرة التي تتسم بالتعقيد حتى ولو كان في ذلك خروج عن معايير الاختصاص الأصلية المتمثلة في مكان وقوع الجريمة أو مكان القبض على المتهم أو مكان إقامته، فهي في الأصل معايير موضوعية تبرر ردة فعل المجتمع اتجاه المجرم الذي اخل بالنظام العام[2].

كذلك نظم المشرع الجزائري في القانون رقم 04/09[3] المؤرخ في 5 أوت 2009، أحكاما جديدة خاصة بالاختصاص في مجال بالجريمة المعلوماتية تتماشى والتطور الذي لحق الجريمة، من هذه القواعد ما نصت عليه المادة الثالثة التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات من ترتيبات تقنية بالإضافة إلى ذلك، قررت المادة 15[4] من القانون 04/09" أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني."[5]

---

[1] انظر للمادة7 من قانون الاجراءات الجزائية الجزائري.

[1] – يتحدد الاختصاص الإقليمي لوكيل الجمهورية وقاضي التحقيق عادة بمكان وقوع الجريمة او مكان إقامة المتهم أو مكان القبض عليه، لمزيد من التفاصيل انظر المواد 37و40 من قانون الاجراءات الجزائية.

[3]قانون رقم 09-04 المؤرخ في 2009/8/16 : وهو القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، صدر هذا القانون في الجريدة الرسمية رقم 47 الصادرة بتاريخ 16/8/ 2009

[4] انظر للمادة 15من القانون04/09،نفس المرجع

إضافة إلى ذلك تم سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و144مكرر 1 و144 مكرر 2 [1]من قانون العقوبات المعدل والمتمم بالقانون رقم 09[2]/01 المؤرخ في 26 يونيو 2000.

ثانيا : أساليب التحري الخاصة.

إن أهمية جهاز الشرطة القضائية في الكشف عن الجريمة الالكترونية والتعرف على المجرمة الالكتروني تبعه استحداث المشرع الجزائري أساليب التحري الخاصة المستعملة بما تتناسب ومتطلبات ضبط الوجه الجديد للإجرام حتى يسمح للقضاء والشرطة أن تتكيف بدورها في مهامها مع الإجرام الجديد مستمدة شرعيتها من المواثيق الدولية التي صادقت عليها الجزائر وخاصة المادة 20 من اتفاقية باليرمو المكافحة الجريمة المنظمة عبر الحدود الوطنية[3] التي أدرجت الجريمة الالكترونية كشكل من أشكال الجريمة المنظمة.

ما تجدر الإشارة إليه أن هذه الأساليب لا يرخص بها إلا في بعض الجرائم المعينة من طرف المشرع الجزائري على سبيل الحصر لا المثال بما فيها الجريمة الالكترونية

[1] انظر للمادة 144 مكرر و مكرر 1و2 من القانون رقم 09/01 المعدل و المتم للقانون العقوبات

[2] قانون رقم 01-09 مؤرخ في 4 ربيع الثاني عام 1422 الموافق 26 يونيو سنة 2001، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.،صادر في الجريد الرسمية عدد34 بتاريخ 2001/06/27

[3] الأمم المتحدة. (2000). اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية. تم اعتمادها في 15 نوفمبر 2000، ودخلت حيز التنفيذ في 29 سبتمبر 2003. الأمم المتحدة، تمت مصادقة الجزائر في 9 نوفمبر

استدركها المشرع بموجب تعديل قانون الإجراءات الجزائية القانون رقم 22-06 [1]والتي تتمثل في[2]:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام.

جواز التسرب أو الاختراق للكشف عن الجريمة الالكترونية بمقتضى المادة 65 مكرر 12[3] من القانون 22-06 المتضمن قانون العقوبات، ولأنه إجراء غير مألوف وخطير في عمل سلطات الضبط القضائي احاطه المشرع بجملة من الضوابط أهمها: الإذن القضائي بالتسرب من وكيل الجمهورية أو قاضي التحقيق المادة 65 مكرر 11 وأيضا احترام المدة القانونية التسرب.[4]

ثالثا: التفتيش.

تتميز الجريمة الالكترونية عن غيرها من الجرائم كونها من الجرائم التي يصعب إثباتها لذلك يجيز المشرع الجزائري التفتيش في المنظومة المعلوماتية ضد كل جريمة يحتمل وقوعها وتتقلص معه الضمانات التي يشترطها المشرع عادة في الجرائم الأخرى نظرا لسرعة ارتكابها ومحو آثارها وتخطيها الحدود الوطنية[5] .

وإذا كان التفتيش يقصد به البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها وكل ما له علاقة بها أو بفاعلها، فإن عالم التقنية قد يتميز عن الجرائم العادية

---

[4] الجمهورية الجزائرية الديمقراطية الشعبية. (2006). قانون رقم 06-22 مؤرخ في 20 ديسمبر 2006، يتضمن قانون الإجراءات الجزائية. معدل ومتمم للأمر رقم 66-155.الجريدة الرسمية، عدد 84، 24 ديسمبر 2006،

[2] - كور طارق، آليات مكافحة جريمة الصرف، دار هومة ،الجزائر، الطبعة الثانية 2014

[3] انظر للمادة 65 مكرر12 من القانون22-06،المرجع السابق.

[4] انظر للمادة 65 مكرر11 من القانون22-06،المرجع السابق.

[5] -المادة 05 من الأمر 04- 09

بكونه يتكون من شقين هما الكيانات المادية والتي تنطبق عليها القواعد العامة للتفتيش من حيث مكان تواجدها بحسب ما إذا كان مكان عام أو خاص كمسكن المتهم مثلا، أما إذا تعلق الأمر بتفتيش الكيانات المعنوية كالبرامج ونظم التشغيل وقواعد البيانات وبعيدا عن الآراء الفقهية التي قيلت حولها فقد نص المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن القاضي التحقيق أن يقوم باية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك".

التوقيف تحت النظر .

من الإجراءات المستحدثة لمواجهة الجريمة الالكترونية في التشريع الجزائري تمديد التوقيف تحت النظر الممنوح لضباط الشرطة القضائية مرة واحدة إذا تعلق بالجريمة الالكترونية طبقا لنص المادة 5/51 من الأمر 15-02[1] المؤرخ في 23 جويلية 2015 مع العلم أن هذا الإجراء بوليسي يقوم به الضابط ضد كل شخص تتوافر دلائل قوية على ارتكابه الجريمة في الجريمة المتلبس بها بوضع شخص في مركز الشرطة أو الدرك لمدة يحددها المشرع كلما دعته الضرورة لذلك، على أنه لا يجوز أن تتجاوز مدة التوقيف للنظر ثمان وأربعون ساعة ماعدا بعض الجرائم الخطيرة التي خصها المشرع باستثناءات [2].

[1] الأمر رقم 15 – 02 المؤرخ في 23 جويلية 2015 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 40،الصادرة في 2015/07/23

[2] – عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري ،دار بلقيس ، 2015 ص 91.

المطلب الثاني:

الهيئات المتخصصة في البحث والتحري ومكافحة الجرائم السبرانية.

تتزايد التهديدات السيبرانية بشكل مستمر مع تطور التكنولوجيا واعتماد المجتمع على الأنظمة الرقمية في مختلف المجالات. هذا التطور جعل من الجرائم السيبرانية تهديدًا جديًا للأمن الوطني، مما يستدعي تكوين هيئات متخصصة في البحث والتحري لمكافحة هذه الجرائم. تلعب هذه الهيئات دورًا حاسمًا في الكشف عن الأنشطة غير القانونية التي تستهدف الأفراد والمؤسسات والبنية التحتية الحيوية. من خلال تزويدها بأحدث التقنيات وأفضل الكفاءات، تسعى الدول إلى تعزيز قدراتها على مواجهة الجرائم السيبرانية، حماية أمنها القومي، وضمان سلامة الفضاء الرقمي[1] في هذا المطلب، سنتناول أهمية ودور الهيئات المتخصصة في مكافحة الجرائم السيبرانية، مع التركيز على التشريعات والسياسات التي تنظم عمل هذه الهيئات.

الفرع الأول

الهيئة الوطنية لمكافحة الجرائم المتعلقة بالتكنولوجية الإعلام.

استحدث المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب القانون رقم 09/04[2]، الذي يتضمن القواعد الخاصة بالوقاية من هذه الجرائم ومكافحتها. حيث نصت المادة 13[3] من هذا القانون على إنشاء

[1] – ربيعي حسين المرجع السابق ، ص 171

[2] قانون رقم 09/04 المؤرخ في 14 شعبان 1430 الموافق 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية، العدد 47، الصادرة بتاريخ 25 شعبان 061430 الموافق لـ 16 أوت 2009، ص06

[3] انظر للمادة 13 من القانون09/04،نفس المرجع.

هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أن يتم تحديد تشكيلتها وتنظيمها وكيفية سير عملها عن طريق التنظيم.

وفيما يتعلق بتنظيم الهيئة وتشكيلتها وكيفية سيرها، أحال المشرع الجزائري ذلك إلى التنظيم من خلال نص المادة 13 المذكور أعلاه، وقد تم ذلك من خلال المرسوم الرئاسي رقم 19-172 [1]الذي ألغى المرسوم الرئاسي رقم 15/261[2]. واعتبر المشرع الجزائري الهيئة بموجب هذا المرسوم مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية، وتوضع تحت سلطة وزارة الدفاع الوطني.

وفيما يخص تنظيم الهيئة، أشارت المادة 4 [3]من المرسوم الرئاسي رقم 19-172 إلى أن الهيئة تتشكل من مجلسين: مجلس توجيه ومديرية عامة. يترأس مجلس التوجيه وزير الدفاع أو ممثله، وتتألف الهيئة من ممثلين عن الوزارات التالية: وزارة الدفاع الوطني، الوزارة المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالمواصلات السلكية واللاسلكية.

أما عن كيفية سير عمل الهيئة، فقد نصت المادة 7[4] من المرسوم الرئاسي رقم 19-172 على أن مجلس التوجيه يجتمع في دورة عادية مرتين في السنة بناءً على استدعاء من رئيسه، ويمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضروريًا بناءً على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

[1] مرسوم رئاسي رقم 19-172 مؤرخ في 06-06-2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام و الإتصال و مكافحتها و تنظيمها و كيفيات سيرها .جريدة رسمية رقم ،37 لسنة 2019

[2] مرسوم رئاسي 15-261 مؤرخ في 08/10/2015، تعدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والمكافحة الجريدة الرسمية، العدد 53 الصادرة بتاريخ 08/10/2015

[3] انظر للمادة 4 من المرسوم الرئاسي 19-172،نفس المرجع.

[4] نظر للمادة 7 من المرسوم الرئاسي 19-172،نفس المرجع.

وبخصوص مهام الهيئة، تمارس الهيئة المهام المنصوص عليها في المادة 14 [1]من القانون رقم 09/04 تحت رقابة السلطة القضائية، وفقًا لأحكام قانون الإجراءات الجزائية والقانون رقم 09/04. وتشمل هذه المهام:

1. مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات المتعلقة بالجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

2. تبادل المعلومات مع نظيراتها في الخارج لجمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الإلكترونية وتحديد مكان تواجدهم.

ولمزيد من التفصيل، تم تقسيم هذه المهام بين مجلس التوجيه والمديرية العامة للهيئة في المرسوم الرئاسي رقم 19-172، حيث تم تحديدها في المواد 6، 9، 11، 13، و14 من المرسوم[2].

الفرع الثاني

الوحدات التابعة لسلك الأمن الوطني والقيادة العامة للدرك الوطني

تصدى المشرع الجزائري للجريمة الالكترونية من خلال مجموعة من النصوص القانونية التي منحت بدورها الاختصاص لمجموعة من الهياكل الخاصة تتولى مكافحة الجرائم الالكترونية والوقاية منها، ومن خلال هذه الجزئية من دراستنا في هذا الفرع سنحاول التطرق لهذه الهياكل والهيئات .

[1] نظر للمادة 14 من القانون 04-09،المرجع السابق.

[2] نظر للمادة 6.9.11.13.14 من المرسوم الرئاسي 19-172،المرجع السابق

أولا. مركز الوقاية من الجرائم في الإعلام الآلي والجرائم المعلوماتية للدرك الوطني :

أنشئ هذا المركز في عام 2008 ويعتبر الجهاز الوحيد المختص في مجال تأمين منظومة المعلومات في الجزائر. يهدف المركز أساسًا إلى تأمين الأنظمة المعلوماتية لخدمة الأمن العام، ويعمل كمركز توثيق مقره في بئر مراد رايس. يقوم هذا المركز بتحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية مرتكبيها سواء كانوا أفرادًا أو جماعات، وذلك بهدف تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستخدمة في المؤسسات الرسمية والبنوك والمنازل. كما يسعى إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها[1].

استطاعت قيادة الدرك الوطني، من خلال التكوين المستمر والمتميز لأفرادها، والملتقيات الدولية والوطنية، وتبادل الخبرات مع دول أخرى، أن توفر القوى المؤهلة والكفاءة من مهندسي الإعلام الآلي ورجال القانون. يأتي ذلك بهدف الفهم الصحيح للجريمة المعلوماتية والتصدي لها بفعالية[2].

وفي هذا السياق، تمكن المركز من معالجة العديد من الجرائم الإلكترونية والرقمية، بالإضافة إلى تلك المتعلقة بوسائل التواصل الاجتماعي والجرائم المتعلقة باختراق مواقع رسمية لمؤسسات عامة وخاصة. استهدف مرتكبو هذه الجرائم أنظمة المعالجة الآلية للمعطيات، مما يعزز أهمية دور المركز في حماية وتأمين البنية التحتية المعلوماتية الوطنية[3] .

[1] عز الدين عز الدين "الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها"، قيادة الدرك الوطني، مداخلة بالملتقى الوطني حول :الجريمة المعلوماتية بين الوقاية والمكافحة ،جامعة محمد خيضر بسكرة 16 نوفمبر 1015 ، ص 30

[2] عز الدين عز الدين، مرجع سابق، ص 39

[2] – سمير بارة،المرجع السابق ، ص271.

.ب . المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاؤه بموجب الرئاسي رقم 04- 183[1] المؤرخ بتاريخ 26 جوان 2004، وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة، والمدعومة بالتكنولوجيات المناسبة. ولعل الخدمة الأساسية التي يقدمها هذا المعهد هي خدمة العدالة ودعم وحدات التحري في إطار الشرطة القضائية الاجرام، ولهذا فإن مكلف المعهد الوطني للأدلة الجنائية وعلم بالمهام الآتية:

القيام بالخبرات العلمية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح .[2]

مساعدة المحققين للسير الحسن للمعاينات خاصة عن طريق الوضع تحت تصرف الأفراد المؤهلين أثناء الحاجة.

المبادرة وإجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة.

العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعالياتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.

ج . المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني :

تم إنشاء المصلحة المركزية لمكافحة الجريمة المعلوماتية كاستجابة لمطلب الأمن المعلوماتي ولمحاربة التهديدات الأمنية المنبثقة عن الجرائم الإلكترونية. بدأت هذه الجهود بتكوين فصيلة في إطار المديرية الشرطية القضائية، والتي كانت النواة الأولى لتطوير قدرات مكافحة الجرائم الإلكترونية. وفي عام 2011، تم إنشاء المديرية العامة للأمن الوطني، وبعد

[1] مرسوم رئاسي رقم 183-04 ، المؤرخ في 26 يونيو سنة 2004 ،يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسيا. الجريدة الرسمية41 ، الصادرة قي 2004/06/27

[2] عز الدين عز الدين، مرجع سابق، ص 39

ذلك، تم تكييف التشكيل الأمني لهذه المديرية لمواجهة التحديات المتزايدة في مجال الجرائم الإلكترونية[1].

وفي يناير 2015، بناءً على قرار من المدير العام للأمن الوطني[2]، تمت إضافة المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إلى الهيكل التنظيمي للمديرية الشرطية القضائية. هذه الخطوة تعكس الالتزام بتعزيز القدرات في مجال مكافحة الجريمة المعلوماتية وتحسين الأمن السيبراني في البلاد[3].

الفرع الثالث

الهيئات القضائية الخاصة للبث في الجرائم الالكترونية.

لقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000 والذي انصب على دراسة ثلاث نقاط أساسية دعم حقوق الإنسان وتسهيل حق اللجوء إلى القضاء وإعادة الاعتبار لنظام التكوين والتأهيل، بإحداث تغييرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة. ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائي بشقيه الموضوعي والإجرائي لمواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد مخاطر التقنية والمعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهددة بذلك اقتصاديات الدول وأمنها، حيث

[1] عز الدين عز الدين، مرجع سابق، ص 41

[2] إمام غازي الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، حالفي 44 2016، ص44

[3] إمام غازي، نفس المرجع، ص

شهدت السنوات الأخيرة تزايدا في العمليات الإرهابية وتزايدا في أعمال المنظمات الإجرامية واستعمالها الفضاء الافتراضي للاستفادة من خصائص الجريمة المعلوماتية[1].

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 14 – 04 [2]المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل الحصر وتوصف أنها خطيرة وعلى درجة عالية من التعقيد والتنظيم وهي جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف[3].

ولقد تم بالفعل صدور مرسوم التنفيذي رقم 16–280[4] المؤرخ في 02–11–2016 .[1]هذا المرسوم يعدل ويكمل المرسوم التنفيذي رقم 08–04 المؤرخ في 19–01–2008، الذي يتعلق بالقانون الأساسي الخاص بالموظفين المنتمين للأسلاك المشتركة في المؤسسات والإدارات العمومية. الذي تم بموجبه تمديد الاختصاص لأربع جهات قضائية:[5]

[1] سمير بارة،المرجع السابق ، ص273.

[2] لقانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية ،الجريدة الرسمية عدد 71 بتاريخ 10 نوفمبر 2004

[3] – كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11 عدد 01–2015،ص 17

[4] لمرسوم التنفيذي رقم 16–280 المؤرخ في 02–11–2016 المعدل والمتمم للمرسوم التنفيذي رقم 08–04 المؤرخ في 19–01–2008 المتضمن القانون الاساسي الخاص بالموظفين المنتمين للأسلاك المشتركة في المؤسسات والإدارات العمومية.الجريد الرسمية العدد66، الصادر بتاريخ 2016/11/09

[5] – كور طارق، المرجع السابق، ص154

- محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: الجزائر، الشلف الأغواط البليدة، تيزي وزو الجلفة المدية المسيلة وبومرداس.
- محكمة قسنطينة ويمتد اختصاصها للمجالس القضائية قسنطينة وام البواقي وباتنة وبجاية وتبسة وجيجل وسطيف وسكيكدة وعنابة وقائمة وبرج بوعريريج والطارف وخنشلة وسوق اهراس وميلة .
- محكمة ورقلة ويمتد اختصاصها للمجالس القضائية التالية : ورقلة وأدرار وتمنراست وإليزي وبسكرة والوادي وغرداية .
- محكمة وهران ويمتد اختصاصها الى المجالس القضائية التالية :وهران وبشار وتلمسان وتيارت وتندوف وسعيدة وسيدي بلعباس ومستغانم ومعسكر والبيض وتسمسيلت والنعامة وعين تموشنت وغليزان .
- بحيث يشمل اختصاص كل جهة قضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا جنوبا شرقا وغربا وذلك لدى أربع محاكم تسمى أقطابا جزائية، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيها الجريمة الإلكترونية. [1]

[1] كريمة علة، المرجع السابق، ص 20

خاتمة

خاتمة:

في ختام هذه الدراسة التي تناولت الإطار المفاهيمي للجريمة الإلكترونية والأمن السيبراني وآليات مكافحة الجريمة الإلكترونية وحماية الأمن السيبراني في ظل الاتفاقيات الدولية والتشريع الجزائري، نجد أن هذه الموضوعات تتشابك بشكل وثيق لتشكّل تحديات معقدة في عصر الرقمنة المتسارعة.

الجريمة الإلكترونية باتت تشكل تهديداً حقيقياً للأفراد والمؤسسات والدول، نظراً لتنوعها وتطور أساليبها، مما يستدعي تكاتف الجهود لمواجهتها بفعالية. الإطار المفاهيمي للجريمة الإلكترونية يوفر الأساس لفهم طبيعة هذه الجرائم، ودوافع مرتكبيها، وأساليب تنفيذها، مما يسهم في تطوير استراتيجيات فعالة لمكافحتها.

الأمن السيبراني، من جانبه، يعد الركيزة الأساسية لحماية الأنظمة المعلوماتية والبنية التحتية الرقمية من التهديدات السيبرانية. تكامل الأمن السيبراني مع التشريعات الوطنية والدولية يساهم في خلق بيئة آمنة ومستقرة لتبادل المعلومات والخدمات الإلكترونية.

آليات مكافحة الجريمة الإلكترونية تتنوع بين الإجراءات التقنية، مثل استخدام برامج الحماية وجدران النار، والإجراءات القانونية التي تشمل سن القوانين وتطبيقها بصرامة. كما أن التعاون الدولي، من خلال الاتفاقيات والمعاهدات، يلعب دوراً محورياً في تبادل المعلومات والخبرات وتعزيز القدرات على مواجهة الجرائم العابرة للحدود.

في السياق الجزائري، يعكس التشريع الوطني التزام الحكومة بمكافحة الجريمة الإلكترونية وحماية الأمن السيبراني، من خلال تطوير قوانين متخصصة وتحديثها بما يتماشى مع التطورات العالمية. ورغم ذلك، تظل هناك حاجة لتعزيز التنفيذ الفعلي لهذه القوانين وتوفير التدريب اللازم للجهات المعنية.

ختاماً، يظل التصدي للجريمة الإلكترونية وحماية الأمن السيبراني مسؤولية مشتركة تتطلب تضافر جهود الحكومات والمؤسسات والأفراد. ومن خلال الالتزام بالاتفاقيات الدولية وتطوير التشريعات الوطنية، يمكن تحقيق بيئة رقمية أكثر أماناً واستقراراً. يجب أن نبقى يقظين ومبتكرين في مواجهة التحديات الجديدة التي تفرضها التطورات التقنية المستمرة.

في ختام دراستنا لموضوع الجرائم الالكترونية والامن السيبراني في الاتيفاقيات الدولية والتشريع الجزائري توصلنا لجملة من النتائج والاقتراحات نوجزها على النحو التالي:

أولا: النتائج

1. تزايد الجرائم الإلكترونية :شهد العقدان الأخيران نمواً كبيراً في وتيرة الجرائم الإلكترونية، مما يستدعي استجابات قانونية وتقنية فعالة لمواجهتها. هذا الازدياد يبرز الحاجة الملحة لتعزيز الأمن السيبراني لحماية الأفراد والمؤسسات.
2. الاتفاقيات الدولية :لعبت الاتفاقيات الدولية، مثل اتفاقية بودابست، دوراً هاماً في وضع معايير عالمية لمكافحة الجرائم الإلكترونية، مما يعزز التعاون بين الدول لمواجهة هذه التحديات المشتركة. هذه الاتفاقيات تسهم في تعزيز الأمن السيبراني من خلال وضع أسس قانونية موحدة تسهل تبادل المعلومات والتنسيق بين الدول.
3. التشريع الجزائري :يحتوي التشريع الجزائري على قوانين لمكافحة الجرائم الإلكترونية، ولكن بعضها قديم ويحتاج إلى تحديثات لمواكبة التطورات التكنولوجية السريعة وضمان فعالية الحماية القانونية. تحديث هذه القوانين يعد ضرورياً لتعزيز الأمن السيبراني الوطني والقدرة على التصدي للتهديدات الإلكترونية المتزايدة.
4. تطور الأمن السيبراني :يُعَدُّ تطوير الأمن السيبراني أحد الأولويات الرئيسية في الدول المتقدمة، ويعتمد على التحديث المستمر للتقنيات والسياسات لضمان حماية فعالة

ضد التهديدات السيبرانية. تعزيز الأمن السيبراني يتطلب استجابات قانونية وتقنية متكاملة للتصدي للجرائم الإلكترونية بفعالية.

5. أهمية التعاون الدولي :يُعَدُّ التعاون الدولي أساسياً لمكافحة الجرائم الإلكترونية العابرة للحدود، ويتطلب تبادل المعلومات والتنسيق المستمر بين الدول لضمان استجابة فعالة وشاملة. هذا التعاون يسهم في تعزيز الأمن السيبراني العالمي من خلال الجهود المشتركة لمواجهة التهديدات الإلكترونية وتطوير استراتيجيات موحدة.

ثانيا: الاقتراحات

1. حديث التشريعات الجزائرية :يجب على الجزائر تحديث قوانينها المتعلقة بالجرائم الإلكترونية بما يتماشى مع المعايير الدولية والتطورات التقنية، لضمان فعالية التصدي للتهديدات السيبرانية وحماية الأمن السيبراني.

2. تعزيز التعاون الدولي :توسيع نطاق التعاون مع الدول الأخرى والمنظمات الدولية لتبادل المعلومات والخبرات في مجال مكافحة الجرائم الإلكترونية، مما يعزز الجهود المشتركة في تعزيز الأمن السيبراني العالمي وتنسيق الاستجابات للتهديدات العابرة للحدود.

3. تطوير البنية التحتية للأمن السيبراني :الاستثمار في البنية التحتية للأمن السيبراني وتوفير التقنيات الحديثة لحماية الأنظمة والشبكات، مما يقلل من نقاط الضعف ويساهم في حماية البيانات والمعلومات الحساسة من الهجمات الإلكترونية.

4. التوعية والتدريب :تنظيم حملات توعية وتدريب متواصل لمختلف فئات المجتمع حول مخاطر الجرائم الإلكترونية وكيفية الوقاية منها، مما يعزز الوعي الأمني ويشجع على تبني ممارسات أمنية أفضل على مستوى الأفراد والمؤسسات.

5. إنشاء وحدات متخصصة :إنشاء وحدات متخصصة داخل أجهزة الأمن والقضاء للتعامل مع الجرائم الإلكترونية بفعالية وكفاءة، لضمان استجابة سريعة ومخصصة لهذا النوع من الجرائم وتعزيز الأمن السيبراني.

6. تشجيع البحث والتطوير :دعم البحوث والدراسات المتعلقة بالأمن السيبراني وتطوير حلول مبتكرة لمواجهة التحديات الجديدة، مما يسهم في تحسين تقنيات الحماية والاستجابة للتهديدات الإلكترونية المتجددة.

7. تعزيز الأطر القانونية والتنظيمية :وضع أطر قانونية وتنظيمية واضحة تحدد مسؤوليات الجهات المختلفة وتعزز من إجراءات الوقاية والاستجابة الفعالة للجرائم الإلكترونية، مما يساهم في توفير بيئة قانونية وتنظيمية متكاملة تدعم الأمن السيبراني وتعزز من قدرات التصدي للهجمات الإلكترونية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

اولا:المصادر

1. الاتفاقيات الدولية:

2. اتفاقية بودابست المتعلقة بالإجرام المعلوماتي (Convention sur la cybercriminalité Budapest)، الموقعة في 23 نوفمبر 2001.
3. اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية, الموقعة في 21 ديسمبر 2010.

4. القوانين:

5. قانون رقم 01-09 مؤرخ في 4 ربيع الثاني عام 1422 الموافق 26 يونيو سنة 2001، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، صادر في الجريدة الرسمية عدد 34 بتاريخ 2001/06/27.
6. القانون رقم 15-04 مؤرخ في 10/11/2004 وعدل و يتمم الأمر رقم 66 - 156 يتضمن قانون العقوبات، جريدة 12 رسمية عدد 71، صادر بتاريخ 10/11/2004 معدل و متمم.
7. قانون رقم 06-22 :يتضمن قانون الإجراءات الجزائية، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات،، الجريدة الرسمية، عدد 84، 24 ديسمبر 2006.
8. القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 أغسطس 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،الصادرة في الجريدة الرسمية العدد 84, في تاريخ:2009/09/16 الجزائر.
9. القانون 11-14 المؤرخ في 02/08/2011، المتضمن قانون العقوبات، الجريدة الرسمية عدد 44 صادرة في: 10/08/2011.

10. القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج. ر.ج العدد 27 بتاريخ 13 مايو 2018.

11. الاوامر :

12. الأمر 03-05 المؤرخ في 19/07/2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 44، صادرة بتاريخ 2003/07/23.

13. المراسيم:

14. مرسوم رئاسي رقم 183-04 :يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، جريدة رسمية رقم 37 لسنة 2019.

15. مرسوم رئاسي رقم 16-280 :المعدل والمتمم للمرسوم التنفيذي رقم 08-04 المؤرخ في 19-01-2008 المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك المشتركة في المؤسسات والإدارات العمومية، الجريد الرسمية العدد66، الصادر بتاريخ 2016/11/09.

16. مرسوم رئاسي رقم 19-172 :يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وتنظيمها وكيفيات سيرها، جريدة رسمية رقم 37 لسنة 2019.

17. مرسوم رئاسي رقم 16-280 :المعدل والمتمم للمرسوم التنفيذي رقم 08-04 المؤرخ في 19-01-2008 المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك المشتركة في المؤسسات والإدارات العمومية، الجريد الرسمية العدد66، الصادر بتاريخ 2016/11/09.

ثانيا: المراجع

1. الكتب

18. عبد الفتاح بيومي حجازي، "الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت"، دار الكتب القانونية، مصر، 2006.

19. هشام محمد رستم، "الجوانب الإجرائية للجرائم المعلوماتية"، مكتبة الآلات الحديثة، أسيوط، 1994.

20. هدى قشقوش، "جرائم الحاسب الإلكتروني في التشريع المقارن"، دار النهضة العربية، القاهرة، الطبعة الأولى، 1992.

21. خالد ممنوح إبراهيم، "فن التحقيق الجنائي في الجرائم الإلكترونية"، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009.

22. يوسف مناصرة، "جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، دار الخلدونية، الجزائر، 2018.

23. محمد حماد مرهج الهيتي، "الجريمة المعلوماتية (نماذج من تطبيقاتها)"، دار الكتب القانونية، الإمارات، 2014.

24. نجاة بن مكي، "السياسة الجنائية لمكافحة الجرائم المعلوماتية"، دار الخلدونية، الجزائر، 2017.

25. كور طارق آليات مكافحة جريمة الصرف دار هومة، الجزائر، الطبعة الثانية 2014.

26. عبد الرحمان خلفي .الإجراءات الجزائية في التشريع الجزائري .دار بلقيس، 2015.

27. نهلا عبد القادر المومني، "الجرائم المعلوماتية"، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.

28. غادة العربي نصار، "الإرهاب والجريمة الإلكترونية"، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2017.

29. هشام بشير، "الآليات الدولية لمكافحة الجريمة الإلكترونية"، المركز الدولي للدراسات المستقبلية والاستراتيجية، 2012.

30. الأشقر جبور منى، "القانون والإنترنت: تحدي التكيف والضبط"، مكتبة صادر ناشرون، بيروت، 2008.

31. عبد الرحمن بن عبد الله السيد، "الأحكام الفقهية للتعاملات الالكترونية (الحاسب الآلي وشبكة المعلومات والانترنيت)"، دار الوراقين للنشر والتوزيع، بيروت، الطبعة الأولى، 2004.

32. عمرو عيسى الفقي، "الجرائم المعلوماتية: جرائم الحاسب الآلي والانترنيت في مصر والدول العربية"، المكتب العربي الحديث، الإسكندرية، 2006.

33. خالد ممدوح إبراهيم، "أمن الجريمة الإلكترونية"، الدار الجامعية، الإسكندرية، 2010.

34. الطاهر حرف الله، "النخبة الحاكمة في الجزائر 1962-1982 بين التصور الإيديولوجي والممارسات السياسية"، ج1، الجزائر: دار هومة، 2007.

35. عادل عبد الصادق. "الحروب السيبرانية تصاعد القدرات والتحديات للأمن العالمي". المركز العربي لأبحاث الفضاء الإلكتروني، (د.ش)، 2017،

36. عبد الفتاح حجازي. "مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت". مصر: دار الكتب القانونية، المحلة الكبرى، الطبعة الأولى، 2007.

37. محمود أحمد عبابنة. "جرائم الحاسوب وأبعادها الدولية". الأردن: دار الثقافة للنشر والتوزيع، الإصدار الثاني، المجلد الأول، عمان، 2009.

38. زيدان، ربيعة. "الجريمة المعلوماتية في التشريع الجزائري والدولي". دار الهدى، عين مليلة – الجزائر، 2011.

39. عبد الإله النوايسة. "جرائم تكنولوجيا المعلومات – شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية الأردن". دار وائل للنشر والتوزيع، المجلد الأولى عمان، 2017.

2. الاطروحات والمذكرات:

40. يوسف صعيدي، "الجريمة المرتكبة عبر الإنترنت"، مذكرة ماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

41. عبد النور بشان، "الجوانب الموضوعية المعالجة للجريمة المعلوماتية"، أطروحة دكتوراه، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق، جامعة الجزائر 1، 2017-2018.

42. يوسف خليل يوسف العفيفي، "الجرائم الإلكترونية في التشريع الفلسطيني"، رسالة ماجستير في القانون العام، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2013.

43. يوسف صغير، "الجريمة المرتكبة عبر الإنترنت"، مذكرة لنيل شهادة الماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 6 مارس 2013.

44. سوبر سفيان، "الجرائم المعلوماتية"، رسالة لنيل شهادة الماجستير في العلوم الجنائية والقانون الجنائي، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010.

45. صالح شنين، "الحماية الجزائية لبرامج الحاسب الآلي، دراسة مقارنة"، رسالة لنيل شهادة الماجستير، جامعة بسكرة، كلية الحقوق والعلوم السياسية، 2007-2008.

46. عمر بن محمد العتيبي، "الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية والدولية"، أطروحة دكتوراه، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، 2010.

47. منى الأشفر جبور. "الأمن السيبراني: التحديات ومستلزمات المواجهة". مذكرة ماجستير، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، 2012.

48. محمد عبد الرحمان نصيرات وائل. "الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ."ICACC – جامعة الإمام محمد بن سعود الإسلامية المملكة العربية السعودية، 2015.

3. المقالات البحثية والأوراق العلمية:

49. الدين عز الدين، "الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها"، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الوقاية والمكافحة، كلية الحقوق، جامعة بسكرة، الجزائر، 16–17 نوفمبر 2015.

50. سميرة معاشي، "الجريمة المعلوماتية"، مجلة المفكرة، العدد 17، جامعة محمد خيضر، بسكرة، 2006.

51. مجاني باديس، "المعالجة الصحفية لأخبار الجريمة"، مجلة الحضارة الإسلامية، جوان، 2015.

52. حنين جورج إسحاق، "دراسة عن الجرائم المعلوماتية والإلكترونية عبر شبكة الإنترنت وسبل مواجهتها"، الإدارة المركزية، مركز المعلومات والتوثيق.

53. صالحة العمري، "جريمة غسل الأموال وطرق مكافحتها"، مجلة الاجتهاد القضائي، العدد الخامس، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة.

54. أيسر محمد عطية، "دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته"، ورقة مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، 31–32 سبتمبر 2014.

55. إيهاب خليفة، "الأمن السيبراني: الماهية والاشكالات"، رؤى مصرية، ع. أكتوبر 2019.

56. محمد علي سالم، "الجريمة المعلوماتية"، مجلة جامعة بابل للعلوم الإنسانية، المجلد 1، العدد 2، 2007، العراق.

57. هواري عباش، "مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية"، المعهد الوطني للأدلة الجنائية وعلم الإحرام، جامعة بسكرة، كلية الحقوق، 2016._حملاوي عبد الرحمان، "مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية"، جامعة محمد خيضر، بسكرة، كلية الحقوق، 2016.

58. سالم عبد الرزاق، "ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية"، بمحكمة سيدي محمد.

59. مها الدحام، "تاريخ الأمن السيبراني"، موضوع(mawdoo3.com) ، 01/04/2024.

60. إبراهيم أحمد عبد السامرائي. "الجريمة الالكترونية السيبرانية في القانون الدولي". مجلة جامعة جيهان أربيل للعلوم الإنسانية والاجتماعية، المجلد 6، العدد 2، 2022.

61. فتيحة ليتيم، ونادية ليتيم. "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة". جامعة بسكرة، مجلة المفكر، العدد 12، (د.س.ن).

62. رحموني محمد. "خصائص الجريمة الإلكترونية ومجالات استخدامها". مجلة الحقيقة، العدد 41، 2018.

63. سمير بارة. "الأمن السيبراني في الجزائر: السياسات والمؤسسات". المجلة الجزائرية للأمن الإنساني، العدد 04، 2007.

64. بوعلام. "ملتقى حول الجيش الوطني الشعبي ورهانات تداول المعلومات عبر شبكات التواصل الاجتماعي". مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016.

65. عطية إدريس. "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري" مجلة مصداقية، المجلد 01، 2009.

66. مراد مشوش. "الجهود الدولية لمكافحة الاجرام السيبراني". مجلة الواحات للبحوث والدراسات. المجلد 12، العدد726-703،01، 2017.

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

68. جمال بوازدية. "الاستراتيجية الجزائرية في مواجهة الجريمة السيبرانية: التحديات والأفاق المستقبلية". مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 3 أفريل2019.

69. محمد عبد الجواد أميرة عبد العظيم. "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام". مجلة الشريعة والقانون، الجزء 03، العدد 35 361-541. 2020.

70. ليندا شرابسة. "السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية". مجلة دراسات وأبحاث المجلد 01. العدد253-24101. 2009.

71. إلهام غازي. "الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري". مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، جانفي 2016.

72. بكر أبو بكر. "الإرهاب الالكتروني من الدعاة والاستقطاب إلى اكتساح المجال الافتراضي". مجلة ذوات، العدد 46، 2018.

73. بوضياف إسمهان" .الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر ."مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف المسيلة، المجلد 03، العدد 03، سبتمبر 2018.

74. فاروق خلف" .الآليات القانونية لمكافحة الجريمة المعلوماتية ."مجلة الحقوق والحريات، كلية الحقوق، جامعة محمد خيضر بسكرة، المجلد 03، العدد 02، 2015.

75. مشوش مراد" .الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال "مجلة القانون، المجلد 09، العدد 01، سنة 2020.

76. شرف الدين وردة د. بلجراف سامية" .الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري ."مجلة المنار للبحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة يحي فارس المدية، العدد 03، ديسمبر 2017.

77. بوعناد فاطمة زهرة" .مكافحة الجريمة الالكترونية في التشريع الجزائري ."مجلة الندوة للدراسات القانونية، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، العدد 01، 2013.

78. عز الدين عز الدين" .الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها"، قيادة الدرك الوطني، مداخلة بالملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر بسكرة 16 نوفمبر 2015.

79. إمام غازي" .الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، جانفي 16 . 2016.

80. كريمة علة" .الجهات القضائية الجزائية ذات الاختصاص الموسع"، المجلة الأكاديمية للبحث القانوني، المجلد 11، عدد 2015-01.

4. المواقع الالكترونية:

81. https://www.cisco.com

82. https://me.kaspersky.com

83. https://ar.wikipedia.org

84. https://me.kaspersky.com

85. https://technologyreview.ae

86. https://www.unodc.org

فهرس الموضوعات

فهرس الموضوعات

الفصل الثاني

آليات مكافحة الجرائم الإلكترونية وحماية الأمن السيبراني

فهرس الموضوعات

الملخص:

المجتمع الدولي يواجه تحديات متزايدة في مجال الجريمة الإلكترونية وأمن المعلومات، حيث تعد الجريمة السيبرانية تهديدًا خطيرًا على المستوى العالمي. تشمل هذه التهديدات الاختراقات السيبرانية، وسرقة الهوية، واختراق البيانات، والاحتيال الإلكتروني، والتجسس الصناعي، والهجمات الإلكترونية على البنية التحتية الحيوية.

يعتبر الأمن السيبراني جزءًا حيويًا من استراتيجيات الأمن الوطني، حيث تقوم الحكومات بتطوير إطار قانوني وتشريعات تهدف إلى مكافحة الجريمة السيبرانية وحماية المعلومات الحساسة. تسعى الجزائر، كدولة عضو في المجتمع الدولي، إلى تعزيز جهودها لمكافحة الجريمة الإلكترونية من خلال التعاون مع الشركاء الدوليين والانضمام إلى الاتفاقيات الدولية ذات الصلة.

تعتبر الاتفاقيات الدولية مثل اتفاقية مجلس أوروبا لمكافحة الجريمة السيبرانية (قانون مجلس أوروبا رقم 185) وبروتوكول الأمم المتحدة الخاص بمكافحة استخدام الكمبيوتر للجرائم غير القانونية وبروتوكول الاتحاد الدولي للاتصالات (ITU) لمكافحة الجريمة السيبرانية، أدوات فعالة لتعزيز التعاون الدولي في مجال مكافحة الجريمة الإلكترونية.

من جانبها، تعتمد الجزائر على تحديث تشريعاتها الجنائية والقانونية لمواجهة التحديات الناشئة من جريمة الإنترنت والأمن السيبراني. وتقوم بتطوير آليات مكافحة الجريمة السيبرانية عبر توفير التدريب المستمر للقوات الأمنية وتعزيز التعاون بين الجهات المختصة داخلياً وخارجياً.

Abstract:

The international community is facing increasing challenges in the field of cybercrime and information security, as cybercrime is a serious threat at the global level. These threats include cyber intrusions, identity theft, data breach, electronic fraud, industrial espionage, and cyber attacks on critical infrastructure.

Cybersecurity is a vital part of national security strategies, as governments are developing a legal framework and legislation aimed at combating cybercrime and protecting sensitive information. Algeria, as a member state of the international community, seeks to strengthen its efforts to combat cybercrime through cooperation with international partners and accession to the relevant international conventions.

International conventions such as the Council of Europe Convention on combating cybercrime (Council of Europe Law No. 185), the UN Protocol on combating the use of computers for illegal crimes and the ITU protocol on combating cybercrime are effective tools for strengthening international cooperation in the fight against cybercrime.

For its part, Algeria is counting on updating its criminal and legal legislation to meet the emerging challenges of cybercrime and cybersecurity. It is developing mechanisms to combat cybercrime by providing continuous training to the security forces and enhancing cooperation between the competent authorities internally and externally.