دور الأمن السيبراني في مواجهة التهديدات الإلكترونية دراسة حالة الجزائر
The role of cybersecurity in confronting cyber threats, a case study of Algeria

د/إسماعيل جابوربي
كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح ،ورقلة – الجزائر.

تاريخ الإرسال	تاريخ القبول	تاريخ النشر
2020-11-15	2020-12-22	2020-12-31

ملخص الدراسة:

شهد العالم تطورا كبيرا في تقنيات الاتصالات وتداول المعلومات،ورافق ذلك زيادة كبيرة في عدد المستخدمين لهذه الاتصالات ونقل المعلومات،وتزامن كل هذا ظهور ممارسات سلبية لبعض المستخدمين تصل في بعض الأحيان إلى وصفها بالجرائم -وفق النص القانوني- تهدد أمن الدولة وسلامة المواطنين،مما اضطر الدول إلى البحث عن سبل وطرق لمواجهة هذه التهديدات الأمنية ذات المنبت الإلكتروني ،فصيغت تعريفات للجريمة الإلكترونية وهو لم يتفق التشريع والفقه الجنائيين على تسمية تعريف موحد لها ،فهناك من يطلق عليها تسمية جرائم المعلوماتية ،في حين يذهب آخرون إلى تسميتها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال،ويسميها آخرون جرائم الكومبيوتر والانترنيت ،وهناك من يطلق عليها الجرائم المستحدثة،كما لاقى موضوع الأمن السيبراني اهتمام الباحثين وقلق الدول لما له من آثار وتأثير على الأمن والسلامة العامة والنمو الاقتصادي.

الكلمات المفتاحية: الأمن السيبراني - الجريمة الكترونية- التهديد السيبراني- حماية الأنظمة.

Study Summary:

The world witnessed a great development in communication technologies and information circulation, accompanied by a significant increase in the number of users for these communications and information transfer, and all this coincided with the emergence of negative practices for some users that sometimes amount to being described as crimes - according to the legal text - threatening the security of the state and the safety of citizens, forcing Countries have sought to find ways and means to confront these security threats that have an electronic source. Definitions of cybercrime have been formulated, and criminal legislation and jurisprudence have not agreed to name a unified definition for it. There are those who call it information

crimes, while others refer to them as crimes of misuse of information and communication technology. Others call it computer and Internet crimes, and there are those who call it new crimes. The issue of cybersecurity has also met the interest of researchers and the concern of countries because of its tremendous implications for security, public safety and economic prosperity.
Keywords: Cyber Security- Internet Crime- Cyber threat.

مقدمة:

تستخدم الدول لضمان أمن الفضاء الإلكتروني مبادرات مختلفة ،مثل توفير المزيد من التمويل لتحسين التدابير الأمنية ،وإلزام الوكالات الحكومية أو المؤسسات التجارية بتنفيذ أنواع محدده من الممارسات الأمنية ،وزيادة العقوبات علي الحاسوب الجرائم ،والتصدي للتهديدات للبنية التحتية الحيوية وأكثر من ذلك حماية النظم المتصلة بالإنترنت،بما في ذلك المعدات والبرمجيات والبيانات، من الهجمات السيبرانية.

وتقع الجريمة الإلكترونية على المؤسسات أو الأفراد مستخدمي أجهزة الحاسب الآلي أو أجهزة الهواتف الذكية، وهي بلا شك سلوك لا أخلاقي وغير مصرح به وينكره القانون ويعاقب عليه ويدينه الشرع وينبذه المجتمع، حيث يتم ارتكاب الجريمة الإلكترونية باستخدام أدوات الاتصال الحديثة بالإضافة إلى مجموعة البرامج والتقنيات المعدة لهذا الأرض.

ويكمن تحدي الأمن السيبراني في الطبيعة المتطورة للتهديدات الحدودية والمخاطر الأمنية، وكيفيات معالجتها التي تعتمد على النهج التقليدي أي دون استراتيجية وطنية وعمل مؤسسي استباقي ومعالجة التهديد بالتركيز على مصدر الخطر ومكونات النظام من غير حصانة وعدم حماية النظم .

ومن هذا المنطلق فإن إشكالية هذه الدراسة تتمحور في التساؤل الأتي:**كيف يواجه الأمن السيبراني الجرائم الالكترونية في الجزائر؟**و للإجابة عن هذه الإشكالية اعتمدنا الخطة التي تشتمل على ثلاثة مطالب وفق الآتي:

المطلب الأول:مفهوم الجريمة الالكترونية

المطلب الثاني:خصائص الجرائم المعلوماتية

المطلب الثالث:الأمن السيبراني في مواجهة التهديد الإلكتروني

المطلب الأول: مفهوم الجريمة الالكترونية

مما لا شك فيه أن الجريمة بالمفهوم الوسع تعني كل مخالفة لقاعدة من القواعد تنظم سلوك الإنسان في الجماعة، أو هي سلوك إجرامي من خلال ارتكاب فعل يجرمه القانون، أو الامتناع عن فعل أمر به القانون، وعلى العموم فالجريمة بصورة عامة هي ذلك السلوك المضاد للمجتمع والذي يضر بصالحه، هذا بوجه عام،

فإذا ما تم هذا النشاط أو الفعل بواسطة الوسائل التكنولوجية الحديثة الممثلة في الكمبيوتر وباستخدام شبكات الاتصال الإلكترونية عبر وسائط تقنية علمية يمكن وصف النشاط أو الفعل حينئذ بالجريمة الإلكترونية.

إن مسألة وضع تعريف للجريمة المعلوماتية كانت محلا خصبا لاجتهادات الفقهاء ،لذا ذهب الفقهاء في تعريف الجريمة الالكترونية مذاهب شتى ووضعوا تعريفات مختلفة ،ومن ثم فلا نجد تعريفا محددا للجريمة الالكترونية نتيجة للاجتهادات الفقهية المتشعبة في هذا المجال ،فمن يتصدى لتعريف هذه الجريمة قد يتناول تعريفها من زاوية تقنية فنية أو من زاوية قانونية أو زاوية تشريعية، وقد أخذ تحديد مفهوم الجريمة الالكترونية حيزا كبيرا ،وذلك ما سنتناوله في النقاط الآتية:

أولا:التعريف التقني للجريمة الالكترونية

يذهب هذا التعريف إلى القول بأن الجريمة المعلوماتية هي:"نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود "[1]. ويعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا. ويركز في تعريفه على الوسيلة المرتكبة بها الجريمة"[2]. وفي تعريف آخر هي:"مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب"[3].

ثانيا:التعريف الفقهي

يذهب أنصار هذا الاتجاه الفقهي إلى القول بأن تعريف الجرائم الإلكترونية من الناحية القانونيةوتصنيف صورها يتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جريمة الكترونية وهي: الكمبيوتر، برنامج الكمبيوتر، البيانات، الممتلكات، الدخول، الخدمات، الخدمات الحيوية.[4] وهناك جانب آخر من الفقه يذهب إلى تعريف الجريمة الإلكترونية بأنها" الجريمة التي تقع بواسطة الكمبيوتر أو عليه أو بواسطة شبكة الانترنيت"[5]. ويرى أنصار هذا الاتجاه أن من سمات هذه الجريمة أنها جريمة مستترة ، وتتسم بالسرعة والتطور في وسائل ارتكابها ، وهي أقل عنفا في التنفيذ من الجرائم التقليدية ، وعابرة للحدود القطرية، ويصعب إثباتها إلا بوسائل تقنية خاصة تتوفر للحكومات غالبا ، كما يسهل إتلاف الأدلة الخاصة بها إضافة إلى نقص الخبرة العلمية لدى الجهات القائمة على ضبطها ، وعدم كفاية القوانين القائمة التي تعالجها.[6]وهناك اتجاه في الفقه يذهب إلى تعريف الجريمة المعلوماتية اعتمادا على وسيلة ارتكاب الجريمة

،لذلك عرفها الفقيه الألماني تاديمان بأنها : هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي[7].

ويمكن تعريف الجريمة الالكترونية وفق ما سبق بأنها" كل فعل مجرم قانونا مضر بالآخرين عبر استعمال الوسائط الالكترونية" ونقصد بالوسائط الحواسيب ،وأجهزة الهاتف النقال،شبكات الاتصالات الهاتفية،أو شبكات نقل المعلومات كشبكة الانترنيت أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الالكترونية عموما.

ثالثا:التعريف التشريعي

أ - تعريف الجريمة الإلكترونية في التشريع الجزائري وفق القانون04- 15 .[8]

أقر له القسم السابع مكرر منه تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات ، فقد أثار المشرع الجزائري استخدامه لمصطلح لدلالة على كلمة المعلومات والنظام الذي يحتوي عليها ويخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة ارتكابها وحصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي ، أي الجرائم التي يكون النظام المعلوماتي محلا لها،وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها ، فقام بحماية هذه المعطيات من أوجه عدة.

تم في مرحلة لاحقة اختيار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 09-04 المتضمن هذه الجرائم ومكافحتها[9].

ونجد المشرع الجزائري تطرق إلى تعريف الجريمة المساس بأنظمة المعالجة الآلية للمعطيات في المادة2 من قانون رقم 09-04 وجرم الأفعال الماسة بأنظمة المعالجة الآلية لمعطيات في مواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات ،وقد حددت المادة 394 مكرر مفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث بالآتي:

- الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.

- حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكرر1 فقد أشارت إلى ما يأتي:

- إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إ زلة أو تعديل

بطريق الغش المعطيات التي يتضمنها.

وبالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من الآتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

ب -تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون

حددت المادة 2 من القانون رقم 09-04 الجريمة الإلكترونية بقولها :يقصد في مفهوم هذا القانون بما يأتي:

-الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:الجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

-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.

-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.

فالمشرع الجزائري من خلال النصين القانونيين السابقين لم يعرف الجريمة الإلكترونية وإنما تبنى للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة.

المطلب الثاني: خصائص الجرائم المعلوماتية

تعد جرائم المعلوماتية إفرازا ونتاجاً لتقنية المعلومات،فهي ترتبط بها وتقوم عليها ، وهذا ما اكسبها لوناً وطابعاً قانونياً خاصاً يميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من الصفات قد يتطابق بعضها مع صفات طوائف أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فأن اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية اكسبها خصوصية غير عادية، وهذا ماحدا بنا إلى بيان بعض أهم خصائص جرائم المعلوماتية وهي:

أولا: صعوبة الكشف عن الجريمة المعلوماتية وإثباتها لا تحتاج جرائم الاعتداء على برامج ومعلومات الحاسب الالكتروني إلى أي عنف أو جثث أو سفك للدماء أو آثار اقتحام لسرقة الأموال ، وإنما هي بيانات ومعلومات تغير أو تعدل أو تمحي كلياً أو جزئياً من السجلات المخزونة في ذاكرة الحاسب الالكتروني ، لذا يكون من الصعب اكتشافها ومن ثم تطبيق الجزاء الجنائي على مرتكبها[10].وهناك صعوبة أخرى تتعلق بإثبات الجرائم المعلوماتية حيث أن هذه الجرائم لا تترك أي اثر خارجي ومرئي لها ، ومما يزيد من صعوبة إثباتها ارتكابها في الخفاء وعدم وجود أي اثر كتابي ملموس لما يجري خلال تنفيذها من عمليات وأفعال إجرامية حيث يتم استخدام النبضات الالكترونية في نقل المعلومات[11].

كما توجد صعوبات أخرى تكتنف إثبات هذه الجرائم تكمن في المجرمين الذين يخططون لمثل هذا النوع من الجرائم هم دائماً أصحاب ذكاء ودهاء وخبرة ودراية واحتراف في مجال تقنية المعلومات وبالتالي فهم يخططون لهذه الجرائم بطرق محكمة تكفل نجاحهم في ارتكاب الجريمة وفرارهم من أعين السلطات كما يستخدم المجرمون المخططون لهذه الجريمة وسائل تقنية متطورة يصعب على الغير معرفتها والتعامل معها[12].

ثانيا: تتطلب خبرة وتحكما في تكنولوجيا المعلوماتية عند متابعتها.

إن جريمة المعلوماتية لها طبيعة تقنية وبذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري ، لذلك لابد أن يكون المحقق متخصص في جريمة المعلوماتية حتى لا يتسبب في إتلاف الدليل الالكتروني[13]. بالإضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي لإثبات هذه الجرائم ،بالشكل الذي يوجب البحث عن أدلة جديدة وحديثة ناتجة من ذات الحاسب الآلي، وهنا تبدأ صعوبات البحث والتحري عن الدليل ، وجمع هذا الدليل ، وتبدأ إشكالية قبوله أن وجد ومدى مصداقيته على إثبات جريمة تنصب على عناصر غير مادية أي معلومات وبرامج[14].

ثالثا:طبيعة الجاني في جرائم المعلوماتية

قد يكون الجاني في جرائم المعلوماتية شخصاً طبيعياً يعمل لحسابه، ويسعى إلى تحقيق مصلحة خاصة به من وراء الجريمة التي يرتكبها عن طريق الاستعانة بأحد نظم المعالجة الآلية للبيانات والمعلومات،أو ضد أحد نظم المعالجة الآلية للبيانات والمعلومات، غير انه غالباً ما يرتكب الشخص الطبيعي السلوك الإجرامي ليس لحسابه الخاص وإنما لحساب احد الأشخاص المعنوية كشركة عامة أو خاصة تعمل في ميدان المعلوماتية أو أي ميدان آخر[15].

رابعا: الدافع إلى ارتكاب جرائم المعلوماتية :

هناك عدة دوافع إلى ارتكاب الجريمة المعلوماتية، قد يقف وراءها مصدر واحد هو الرغبة الإجرامية الشخصية أو الخارجية.

1. الدوافع الشخصية :

يمكن رد الدوافع الشخصية لدى مرتكب الجريمة المعلوماتية إلى السعي لتحقيق الربح ، فهذا الدافع المادي يعد من أهم البواعث إلى ارتكاب الجريمة المعلوماتية لما يحققه من ثراء شخصي فاحش ، وقد تكون الرغبة في إثبات الذات وتحقيق انتصار شخصي على نفس الأنظمة المعلوماتية من بين الدوافع الذهنية والنمطية لارتكاب الجريمة[16].

2. الدوافع الخارجية:

الإنسان بطبيعته مخلوق هش من الناحية السيكولوجية، يمكن في بعض المواقف أن يستسلم للمؤثرات الخارجية، ولعل من أبرزها الحاجة إلى اختصار عنصر الزمن وتوفير سنوات عدة من البحث، وتحاشي استثمار الملايين من الدولارات في مجال البحث العلمي، إذ تدفع الحاجة بعض المنشآت بل وحتى بعض الدول إلى الاتصال بالأفراد الذين يشغلون أماكن حساسة في إحدى المنشآت كي يعملوا لصالح منشآت أخرى منافسة بهدف الاطلاع على بعض المعلومات والتقنيات المتوفرة لديها للاستفادة منها ، وتستخدم في ذلك عدة أساليب منها الرشوة أو الاقتناع والإغراء المقترن بالتهديد ، والذي قد يصل في بعض الأحيان إلى زرع جواسيس في تلك المنشآت وقد يكون دافع جنون العظمة أو الطبيعة التنافسية هي التي تدفع بعض العاملين في المنشأة لإظهار قدراتهم الفنية الخارقة لإدارة المنشأة فيفضي به ذلك إلى ارتكاب مثل هذه الجرائم حتى ينافس زملائه للوصول إلى أعلى المراكز المرموقة. وأخيرا قد يكون دافع الانتقام من رب العمل أو احد الزملاء أو الأصدقاء من بين البواعث الدافعة إلى ارتكاب الجريمة.

خامسا: استهداف مراحل تشغيل نظام المعالجة الآلية للبيانات

على الرغم من إمكانية ارتكاب الجريمة المعلوماتية في أية مرحلة من مراحل تشغيل نظام المعالجةالآلية للبيانات في الكمبيوتر ، غير أن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن بالنظر لطبيعتها ارتكاب الجريمة المعلوماتية إلا في وقت محدد يعتبر هو الأمثل بالنسبة لمراحل التشغيل . ففي مرحلة الإدخال حيث تترجم المعلومات إلى لغة مفهومه من قبل الآلة، يسهل إدخال معلومات غير صحيحة أو عدم إدخال الوثائق الأساسية والمعلومات المطلوبة، وفي هذه المرحلة يتم ارتكاب أكثر الجرائم المعلوماتية. أما في

مرحلة المعالجة الآلية ل لبيانات فيمكن إدخال أي تعديلات على برامج الحاسب الآلي تحقق الهدف الإجرامي عن طريق التلاعب في برامج النظام المعلوماتي كدس تعليمات غير مصرح بها أو تشغيل برامج جديدة تلغي كلياً أو جزئياً عمل البرامج الأصلية ، وتتطلب الجرائم المرتكبة في هذه المرحلة معرفة فنية عميقة لدى الجاني بتلك التقنية ، كما أن اكتشافها يكون صعب للغاية ، وكثيراً ما تقف الصدفة وراء اكتشافها .

أما في المرحلة الأخيرة المتعلقة بالمخرجات وفيها يقع التلاعب في النتائج التي يخرجها النظام المعلوماتي بشأن بيانات صحيحة أدخلت فيه وعالجها بطريقة صحيحة[17].

سادسا: وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات

يشترط لقيام الجريمة المعلوماتية التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي وذلك من أجل معالجتها الكترونياً بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة والتي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها أو طباعتها وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية ، ولا بد من فهم وإتقان الفاعل لها أثناء ارتكابها وخاصة في جرائم التزوير والتقليد[18].

سابعا: تعدد الأطراف على الإضرار

يكون التعاون والتواطؤ على الإضرار أكثر تكراراً في الجرائم المعلوماتية منه في الأنماط الأخرى للجرائم المستحدثة أو الخاصة أو جرائم أصحاب الياقات البيضاء

فغالباً ما ترتكب هذه الجرائم من متخصص في الأنظمة المعلوماتية يقوم الجانب الفني من المشروع الإجرامي ، وشخص آخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب المالية إليه ، وقد اعتاد المتلصصون على الأنظمة المعلوماتية والحواسيب على تبادل المعلومات بصفة منتظمة حول أنشطتهم[19].

ثامنا: أضرار جرائم المعلوماتية

ترتكب الجرائم المعلوماتية في نطاق تقنية وتكنولوجيا متقدمة يتزايد استخدامها يوماً بعد آخر في إدارة مختلف المعاملات الاقتصادية والمالية حيث تمس هذه الجرائم المركز الحسابي والإداري وتنقلات الأموال والاستثمارات سواء في المنشآت العامة أو الخاصة ، كما تمس المعلومات الشخصية المخزونة في ذاكرة الحواسيب الآلية للبنوك وشركات التأمين ولدى المحامين والمستشفيات ومراكز الشرطة والأحزاب ،وقد تهدد هذه الاعتداءات مباشرة قدسية وسرية الحياة الخاصة أو الحرية السياسية ، ناهيك عن الخطورة التي

تشكلها هذه الجرائم إذا ما تعلقت بالمعلومات الخاصة بإدارة الدولة وعمل الحكومة وخاصة في ميادين الأمن والدفاع والمشروعات النووية والتصنيع الحديث للأسلحة [20].

المطلب الثالث: الأمن السيبراني في مواجهة التهديد الإلكتروني

الأمن السيبراني هي تقنيات حماية أجهزه الكمبيوتر والشبكات والبرامج والبيانات من الوصول غير المصرح به أو الهجمات التي تهدف إلى الاستغلال،ويغطي الأمن السيبراني هي: تطبيق الأمن،أمن المعلومات، التعافي من الكوارث، أمن الشبكات[21]،ويشمل أمن التطبيق تدابير أو تدابير مضادة تتخذ خلال دوره حياه التطوير لحماية التطبيقات من التهديدات التي يمكن أن تأتي من خلال العيوب في تصميم التطبيقات أو تطويرها أو نشرها أو ترقيتها أو صيانتها. بعض التقنيات الأساسية المستخدمة لضمان التطبيق المتمثلة في التحقق من صحة معلمه الإدخال ،ومصادقة المستخدم،و معالجه المعلمات وأداره الاستثناء ،والتدقيق والتسجيل.

ويعد التخطيط للتعافي من الكوارث عمليه تشمل إجراء تقييم للمخاطر،وتحديد الأولويات ، ووضع استراتيجيات للإنعاش في حاله وقوع كارثة. وينبغي أن يكون لأي عمل خطه ملموسة للتعافي من الكوارث لاستئناف العمليات التجارية العادية في أسرع وقت ممكن بعد وقوع كارثة.

ويتضمن أمان الشبكة أنشطه لحماية قابليه الشبكة وموثوقيها وسلامتها. ويستهدف أمن الشبكات الفعال مجموعه متنوعة من التهديدات ويمنعها من الدخول أو الانتشار علي الشبكة. تتضمن مكونات أمان الشبكة:

- المضادة للفيروسات ومكافحه التجسس.
- جدار الحماية ، لمنع الوصول غير المصرح به إلى الشبكة الخاصة.
- أنظمه منع التسلل ،لتحديد التهديدات السريعة الانتشار ، مثل الهجمات التي لا تستغرق يوما أو سفرا،و الشبكات الخاصة ،لتوفير الوصول الأمن عن بعد.

أولا:استراتيجية مواجهة التهديد السيبراني

في ظل هذا التوسع الهائل في استخدام تكنولوجيا الاتصالات ارتفعت الرقابة ووسائل التجسس على الأفراد وليس على المؤسسات فقط، فأصبحت عمليات الرقابة على الاتصالات ووسائل التواصل الاجتماعي لا تصدق فمن اختراقات الأفراد للأمن الشخصي إلى اختراقات الأجهزة الأمنية، وهذا جعل حياة البشر وخصوصياتهم مخترقة بشكل لا يصدق، وكثرت عمليات الابتزاز والجرائم الالكترونية من خلال ذلك، فلم يعد يسلم فرد من هذه العمليات القذرة، سواء كان مسئولا أو مواطنا.

ومن هنا توجهت العديد من الدول لوضع استراتيجية وطنية شاملة من أجل ضمان أمن المعلومات في الفضاء السيبراني، فأمن المعلومات مهمة تعتبر ضمن مفهوم الأمن الوطني العام والشامل للدول مؤسسات وأفراد، وبدأت الكثير من الدول تدرك أن التغيرات المتسارعة في التكنولوجيا تؤدي الى تهديدات ليست بالسهلة لأمن الوطن والمواطن، ولذا لا بد من ضرورة العمل على ضمان أمن المعلومات من خلال خطوات مهمة للأمن السيبراني لحماية الأمن الوطني بمفهومه الشامل، فالأمن السيبراني يعتمد على مجموعة كبيرة من وسائل قانونية وتقنية لمقاومة الاستخدام الغير قانوني للشبكة العنكبوتية ومن أجل حماية نظم المعلومات ووسائل الاتصالات لحماية الوطن والمواطن والمؤسسات من أخطار الفضاء السيبراني.

إن العمل على بناء جدران الحماية لمنع الهجمات الالكترونية وتقليل تأثير رقابة واختراقات الحسابات وأنظمة المعلومات الحكومية والخاصة مسألة في غاية الأهمية، فلا يمكن حماية الوطن والأمن الوطني بمفهومه الشمولي والاقتصاد الوطني والمؤسسات المصرفية ومعلومات الدولة بدون ذلك، وبدون زيادة الثقة بأنظمة المعلومات الوطنية، وإنشاء هيئات وطنية للأمن السيبراني، فالفضاء السيبراني هو عالم غير مادي ولكن لأن وسائل الاتصالات وخزن المعلومات تستخدمه من خلال شبكات الانترنت والشبكة العنكبوتية في العالم وفي الفضاء، فالمعلومات يتم تخزينها ولذا من الضروري حمايتها من الاختراق والسرقة والتجسس، ومن خلال إنشاء الهيئات الوطنية للأمن السيراني يكون بالإمكان من خلالها الإستجابة والمساعدة للمؤسسات والأفراد والقطاع الخاص والعام لمواجهة حوادث الاختراق والتجسس والقرصنة والتقليل من تأثيرها وزيادة الوعي والفهم للتهديدات التي تفرضها التطورات الهائلة في وسائل التواصل والاتصال في الفضاء السيبراني، وخصوصا أن إنشاء الحكومات الالكترونية أصبحت تسير قدما وبتطور جيد في العديد من الدول، وهذا يستدعي اهتماما أكبر في عمليات الحماية كون هذه الحكومات الالكترونية تقدم الخدمات الالكترونية للمواطن وهذا يستدعي أداء جيد مشمولا بالحماية حفاظا على أمن الأفراد والمؤسسات والدولة، ويحتاج إلى بناء معايير لتطوير سياسات أمن وحماية المعلومات[22].

ثانيا:مظاهر التهديدات الأمنية الالكترونية

إن التقدم التكنولوجي أفرز أنماطا جديدة من الجريمة، وكذا من المجرمين، فكان للتقدم في العلوم المختلفة أثره على نوعية الجرائم، واستغل المجرم ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة لتشريعاته.

ويمكن أن يساعد استخدام الأمن السيبراني في منع الهجمات الكترونية وانتهاكات البيانات وسرقه الهوية ، ويمكنه المساعدة في أداره المخاطر.وعندما يكون لدي المنظمة إحساس قوي بأمن الشبكات وبخطه فعاله للاستجابة للحوادث ، فإنها تكون أقدر علي منع هذه الهجمات والتخفيف من حدتها. علي سبيل المثال،حماية المستخدم النهائي يدافع عن المعلومات والحراس ضد الضياع أو السرقة بينما أيضا مسح أجهزه الكمبيوتر للتعليمات البرمجية الضارة،ومن مظاهره:

1. **الاستيلاء على بيانات الضحية** من خلال استخدام برامج قادرة على استرجاع البيانات المحذوفة عن ذاكرة الهاتف النقال أو الكمبيوتر، لذلك يجب عدم بيع أو إعطاء الهاتف الخلوي أو جهاز الحاسوب لأي كان، لأنه باستخدام برامج قادرة على استعادة البيانات المحذوفة سوف يقوم الجاني باستعادة كل ما يخص الضحية من ملفات ومعلومات، لذلك يفضل عدم بيع جهاز الهاتف أو جهاز الكمبيوتر وإذا حصل وتعطل كل من الهاتف الخلوي أو جهاز الحاسوب فعليك إرساله إلى شخص مختص تثق به ومشهود له بالخير والصلاح[23].
2. **الحصول على بيانات الضحية** من خلال فقدان جهاز الهاتف النقال أو الكمبيوتر، بهذا يتم الاستيلاء على بيانات الضحية وانتهاك خصوصيته، لذلك ينصح بعدم الاحتفاظ بصور أو مقاطع فيديو ذات طابع خاص،في حساب الفيسبوك ويتم ذلك بطرق كثيرة بطلب البريد الإلكتروني والرقم السري لنموذج وهمي احتيالي،أو عمليات الابتزاز بالصور الخاصة ومعلومات شخصية حصلت بسبب اختراق الحساب.
3. **الجريمة الإلكترونية الإرهابية**

مما لا شك فيه أن ظاهرة الإرهاب أضحت عالمية، حيث ظهرت الكثير من التنظيمات التي تتبنى هذا الفكر في مختلف دول العالم وبمختلف التسميات،وتظهر العلاقة بين الإرهاب والجريمة الإلكترونية من خلال تجنيد وتجييش أعضاء جدد في التنظيم أو حشد الهمم بواسطة استخدام مختلف وسائل التواصل الإلكتروني.كما يتم تبني العمليات الإرهابية والدعاية لهذه التنظيمات وأعمالها من خلال مختلف الوسائط والمواقع الإلكترونية بما يحقق أهدافها[24]. ومن أهم مظاهرها ما يسمى بهجمات الفدية التي أصبحت من التقنيات الأساسية التي يستخدمها الكثير من مجموعات المجرمين الإلكترونيين في العالم،وما توصف به هو سهولة تنفيذ هذا النوع من الهجمات.

إن سهولة القيام بهجمات الفدية ليست الأمر الوحيد الذي يقف وراء انتشارها ،لكن بعض الوسائل ساعدت على انتشارها مثل ظهور العملة الرقمية التي تعتمد على مبادئ التشفير في كثير من جوانبها لتوفر بذلك قدرا عاليا من عدم الاطلاع، ومن ثم ،فإن الدفعات المالية عبرها يصعب تعقبها من قبل الأجهزة الأمنية.

و قد لا يكفي دفع الفدية أحيانا لتحرير البيانات التي يسيطر عليها قرصان الإنترنت، حيث إن تسديد الدفعة لا يضمن أن يسلم المجرم مفتاح فك تشفير البيانات إلى الضحية،وهذا ماستبقى هذه الهجمات من أهم أشكال جرائم الإنترنت لفترة أخرى، ويتطلب على الأغلب التعامل معها وتقليص تأثيرها السيطرة على العديد من التقنيات التي تعتمد عليها، وتحديدا عملة بتكوين، من خلال إخضاعها لرقابة رسمية.[25]

4. الجريمة المنظمة والجريمة الإلكترونية

غني عن البيان أن أعضاء الجريمة المنظمة يستفيدون من التطور التكنولوجي في مجال المعلومات الإلكترونية، وذلك من خلال استغلال الإمكانات المتاحة إلكترونياً في التخطيط والتوجيه وتنفيذ المخططات الإجرامية بسهولة مخترقة حدود الدول بأقل تكلفة ممكنة ودون مخاطرة،كما أن التطور في المجال الإلكتروني المعلوماتي سهل من مهمة التجسس، فالمجرم الإلكتروني سواء كان شخص واحد أو تنظيم يمكنه التجسس سواء على الأشخاص أو المنظمات وحتى الدول أو أجهزتها، ويأخذ التجسس عدة صور، فقد يكون تجسس اقتصادي أو سياسي أو عسكري[26].

ثالثا:المواجهة الوطنية للجرائم الإلكترونية

إن الاستراتيجية الجزائرية تجاه الجرائم الالكترونية تعتمد على مجموعة من الإجراءات بهدف حماية النظام العام في الدولة وفقا لقوانين الدولة مع وضع ترتيبات لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها ،والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية .

وتمارس عمليات المراقبة من قبل الجهات المختصة في حالات عديدة أهمها :

– الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحته إذن لمدة ستة أشهر قابلة للتجديد على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها توضع الترتيبات التقنية وتوجه حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني

أو مؤسسات الدولة أو الاقتصاد الوطني أو في حال صعب الوصول إلى نتيجة تهم الأبحاث الجارية متعلقة بمقتضيات التحريات والتحقيقات القضائية .

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة حيث يمكن للسلطات المختصة الجزائرية تبادل المساعدة القضائية في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم وكشف مرتكبيها ولجمع الأدلة لخاصة بالجريمة الالكترونية . تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية بناءا على الاتفاقيات الدولية ذات الصلة و الاتفاقيات الثنائية وحسب مبدأ المعاملة بالمثل بينما يتم رفض طلبات المساعدة الدولية إذا كان من شانها المساس بالسيادة الوطنية أو النظام العام،وتضطلع هيئات وطنية وقضائية متخصصة و المعهد الوطني للأدلة الجنائية وعلم الجرائم لهذه المهام التي سنوردها في الإيجاز الآتي:

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

أنشئت هذه الهيئة بموجب لقانون 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السابق ذكره، ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقاية، ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية،في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية أللاقتصاد الوطني[27].

2. الهيئات القضائية الجزائية المتخصصة

أنشئت بموجب القانون 14/04المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد329،37،و40 من ق.إ.ج.ج.وتتمتع اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في 2006/01/05.بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04.

3. المعهد الوطني للأدلة الجنائية وعلم الجرائم .

يقوم المعهد بتقديم المساعدات التقنية ،و دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات[28]،وملاحقة تطور أشكال جرائم القرصنة و فيروسات البرمجيات على مستوى شبكة التي تعد من التحديات المعهد في المدى المتوسط والبعيد.

كما أن المديرية العامة للأمن الوطني تضطلع المديرية للجريمة الإلكترونية بالجانب الوقائي من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

وأيضا في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم ،فأكدت الجزائر عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين ، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا[29].

الخاتمة:

بعد أن أصبح المجتمع المعلوماتي ومنذ أواخر القرن الماضي ومطلع هذا القرن حقيقة واقعة لا تجريد فيها،وبعد أن تم استعراض موقف التشريعات المقارنة في معظم الأنظمة القانونية لمواجهة أو التصدي لهذه الظاهرة الإجرامية الخطيرة المتمثلة بالجرائم المعلوماتية بات واضحا مدى قصور التشريعات الجزائري والإستراتيجية في التصدي لهذا النمط من الجرائم،ومن هذا المنطلق نورد أهم النتائج:

- في الوقت الذي قامت فيه التكنولوجيا بتقريب المسافات بين الشعوب، من خلال توفيرها للعديد من وسائل الاتصالات ووسائل التنقل التي لم تكن معروفة من قبل، نجد أن تلك التكنولوجيا أفرزت الكثير من السلبيات، لعل أهمها كان صعوبة احتفاظ الفرد بخصوصياته جراء انتشار الكثير من الوسائل السهلة، والتي يستخدمها أشخاص يعرفون باسم قراصنة الشبكة العنكبوتية.
- المشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة لتشريعاته.
- عدم الاقتصار عند التجريم والعقاب على أنماط السلوك المحظور المرتكبة حاليا بل يجب مراعاةالأبعاد المستقبلية لأن تكنولوجيا المعلومات والحواسيب في تطور سريع بل يكاد يكون مذهل .
- إن للأمن الإلكتروني عمل مؤسسي وليس عمل مجموعة من الأفراد لذا يجب التخطيط لتنفيذ إستراتيجية وطنية للأمن الإلكتروني الهدف منها تأمين جميع معلومات واتصالات الدولة.
- تعزيز مستوى التعاون بين الجهات الوطنية والدولية لتحفيز إيجاد بيئة تعاونية ينصب تركيزها على تحقيق الأهداف وتعزيز مستوى أمن أصول الفضاء الإلكتروني للدولة والحد من مستويات المخاطر،وإدارة الحوادث الإلكترونية الخطيرة للحد من أثرها على أمن الدولة والمجتمع والاقتصاد.

– بناء قدرات وطنية واحترافية في مجال الأمن السيبراني والبرمجة من خلال التوعية والتأهيل والدعم المبني على أفضل الممارسات والمعايير العالمية.

قائمة المراجع:

[1]- عبد الفتاح بيومي حجازي ،مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي ،دار الفكر الجامعي ، الإسكندرية،2006،ص20.

[2]- سامي على حامد عياد ، الجريمة المعلوماتية وإجرام الانترنت ، دار الفكر الجامعي ،الإسكندرية ، طبعة 2008 ،ص 24.

[3]- نهلا عبد القادر المومني ، الجرائم المعلوماتية،دار الثقافة للنشر والتوزيع ،الأردن، الطبعة الأولى ،1429 هـ 2008 م ،ص20.

[4]- محمد الأمين البشري،التحقيق في جرائم الحاسب الآلي ،مؤتمر القانون والكومبيوتر،والانترنيت،كلية القانون والشريعة ،جامعة الإمارات،ماي 2005،ص6.

[5]- محمد عبد الرحيم سلطان العلماء ، جرائم الانترنيت والاحتساب عليها ،مؤتمر القانون والكمبيوتر والانترنيت ، كلية القانون والشريعة ،جامعة الإمارات ،ماي2005،ص5.

[6]- نائلة عادل محمد فريد قورة،جرائم الحاسب الاقتصادية دراسة نظرية وتطبيقه ،دار النهضة العربية،القاهرة،2004،ص25.

[7]- علي عبد القادر القهوجي ،الحماية الجنائية لبرامج الحاسب ،دار الجامعة الجديدة للنشر، الإسكندرية ،1997،ص7.

[8]- القانون04- 15 المؤرخ في 10 نوفمبر، يعدل ويتمم الأمر 66 - 156المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71 لسنة 2004.

[9]- القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 لسنة 2009.

[10]- شمس الدين إبراهيم أحمد ،وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري دراسة مقارنة ،دار النهضة العربية ،القاهرة ،الطبعة الأولى،2005 ،ص100.

[11]- المرجع نفسه،ص51.

[12]- محمد عبد الله أبو بكر سلامة،موسوعة جرائم المعلوماتية جرائم الكمبيوتر والانترنت ،منشأة المعارف ،الإسكندرية ،2006، ص95.

[13]- عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة،كلية الحقوق ،جامعة الإسكندرية،2006،ص27.

[14]- أحمد خليفة الملط ،الجرائم المعلوماتية ،دار الفكر الجامعي،الاسكندرية،الطبعة الثانية،2005،ص 98 .

[15]- محمد عبد الله أبو بكر سلامة ،المرجع السابق،ص51.

[16]- محمد سامي الشوا ،ثورة المعلومات وانعكاساتها على قانون العقوبات ،مطابع الهيئة المصرية العامة للكتاب،2003،ص19.

[17]- أحمد خليفة الملط، المرجع السابق،ص102.

[18]- حاتم عبد الرحمن منصور الشحات ، الإجرام المعلوماتي ،دار النهضة العربية ، القاهرة ،الطبعة الأولى ،2003،ص37.

[19]- أحمد خليفة الملط، المرجع السابق،ص103.

[20]- محمد سامي الشوا ،المرجع السابق،ص67.

[21]- https://www.cisco.com/ تاريخ الإطلاع2018/12/03م.

[22]- حول هذه الأفكار أنظر:https://is.com.sa تاريخ الإطلاع2018/12/07م

[23]- أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الانترنت،دار المطبوعات الجامعية ، الإسكندرية ، 2009 ،ص 106.

[24]- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل درجة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013 ،ص44.

[25]- https://www.aljazeera.net/ تاريخ الإطلاع03 /2018/12م.

[26]- حاتم عبد الرحمن منصور الشحات،المرجع السابق،ص41.

[27]- صغير يوسف،المرجع السابق،ص96.

[28]- المرسوم الرئاسي رقم 04- 183 المؤرخ في 26 جوان 2004 يتضمن استحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي ،الجريدة الرسمية،العدد41 لسنة2004.

[29]- فضيلة عاقلي،الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري،كتاب أعمال مؤتمر الجرائم الإلكترونية ،مركز جيل البحث العلمي،طرابلس، لبنان، 2017، ص 115.