

انعكاسات الجريمة السيبرانية على البيئة الرقمية:

دراسة في آليات واستراتيجيات مكافحتها

The implications of cybercrime on the digital environment:
a study of mechanisms and strategies to combat them

حكيمة جاب الله¹

¹ كلية علوم الإعلام والاتصال، جامعة الجزائر 3، (الجزائر)، Djaballah-hakima@univ-alger.dz

تاريخ النشر: سبتمبر/2021

تاريخ القبول: 2021/06/09

تاريخ الإرسال: 2020/07/15

الملخص:

تمثل الجريمة السيبرانية أحد المشكلات التي استفحلت في البيئة الرقمية، وهي جرائم حديثة النشأة ارتبط ظهورها بانتشار التكنولوجيات الحديثة للاتصال، نتيجة الإقبال الكبير على استخدام هذه التكنولوجيات عبر شبكة الانترنت مما أدى لظهور سلوكات و مشكلات لم تكن تعرف من قبل، لعل من أبرزها الجريمة التي تحدث في البيئة الرقمية و التي تعرف بالجريمة السيبرانية و قد تعددت أنواعها من سرقة واختراق وقرصنة معلومات إلى جرائم أخلاقية مثل الابتزاز والتهديد والاختطاف وغيرها كلها جرائم تجاوزت الحدود الجغرافية و أصبحت تهدد الحياة الاجتماعية وحتى الدولية. إن الانتشار الكبير للجرائم السيبرانية أصبح هاجسا يورق المجتمعات والدول نظرا لتسارع تطور هذه الجرائم ونمو الكثير من المشكلات و آثارها الوخيمة المهددة للمجتمع ولكيان الدولة مما دفع بالكثير من البلدان للتسارع في اتخاذ تدابير أمنية و وضع استراتيجيات، بالإضافة لسن تشريعات لمكافحة هذه الجرائم المهددة للبيئة الرقمية و كذا التقليل من آثارها السلبية و الوخيمة على المجتمع.

الكلمات المفتاحية: انعكاسات، الجريمة السيبرانية، البيئة الرقمية، آليات ، استراتيجيات.

Abstract:

Cybercrime is one of the problems that has increased in the digital environment, it's a new crime that has been linked to the proliferation of modern communication technologies, cybercrime has multiple types from theft and piracy information to ethical crimes such as threats, kidnapping and other crimes that have crossed geographical boundaries. The high prevalence of cybercrime has become a concern for societies due to the rapid development of these crimes and their serious effects, which has prompted many countries to accelerate security measures and strategies, in addition to enacting legislation to combat these crimes that threaten the digital environment and to minimize their negative effects on society.

Key words: cybercrime, digital environment, reflections, mechanisms, strategies.

المقدمة:

إن التطور الهائل لتكنولوجيا المعلومات والاتصال أدى إلى تحولات سريعة في جميع مناحي الحياة نتيجة الإقبال الكبير سواء من طرف المؤسسات المختلفة أو الأفراد على استخدام هذه الوسائل، وهذا ما أدى لظهور ما يعرف بالمجتمع المعلوماتي الذي لقي اهتماما كبيرا على الصعيد الدولي نظرا لآفاقه المصيرية على العلاقات الدولية نتيجة للعولمة. كما ظهرت أنواع جديدة من السلوكيات التي لم تعد مجرد أخطاء تقنية أو نقص في التجربة، بل هي غالب الأحيان تجاوزات ناتجة عن أطراف تتعمد استغلال الانترنت واستخدامها لأهداف غير قانونية وهذا ما يعرف بالجرائم السيبرانية أو الجرائم الالكترونية أو جريمة العصر نتيجة سوء استخدام النظم الحاسوبية والشبكات وفي طليعتها الانترنت، وهي جرائم حديثة لم تقتصر على اقتحام الشبكات وتخريبها أو سرقة معلومات فقط وإنما تعدت ذلك حيث ظهرت جرائم أخلاقية مثل الابتزاز والتهديد والاختطاف وغيرها. إن الانتشار الكبير للجرائم السيبرانية أصبح هاجسا يورق المجتمعات، مما دفع بالكثير من البلدان للتسارع في وضع استراتيجيات بالإضافة لسن تشريعات وقوانين لمكافحة هذا النوع من الجرائم، خاصة وأن الكثير من الجرائم تستهدف بعض الأشخاص ومصالح الدول والشركات والمؤسسات العملاقة من أجل الإطاحة بها من خلال الاختراقات الأمنية لشبكات معلوماتها. كل هذه المخاطر تتطلب تبني التفكير والتدبير الاستراتيجي في التعامل مع هذه الجرائم التي استفحلت نتيجة الإقبال الكبير على استخدام هذه التكنولوجيات. انطلاقا من ذلك سنحاول من خلال هذه الورقة البحثية التعرف على انعكاسات الجريمة السيبرانية على البيئة الرقمية و كذا آليات مكافحتها، و ذلك من خلال الإشكالية التالية: ما هي انعكاسات الجريمة السيبرانية على البيئة الرقمية ؟ وما هي الآليات والاستراتيجيات التي يمكن من خلالها مكافحتها والتقليل من آثارها الوخيمة؟

تساؤلات الدراسة:

- ما هي طبيعة الجريمة السيبرانية؟ - ما هي أسباب انتشار الجريمة السيبرانية في البيئة الرقمية؟
- ما هي الآثار و الاشكالات التي ترتبت على انتشار الجريمة السيبرانية في البيئة الرقمية؟
- ما هي الآليات والاستراتيجيات التي يمكن من خلالها التصدي والتقليل من خطورتها؟
- أهداف الدراسة: يمكن تلخيصها في النقاط التالية: -إبراز ماهية الجريمة السيبرانية. -توضيح الأسباب التي أدت إلى انتشار الجريمة السيبرانية في البيئة الرقمية. - طبيعية التهديدات التي تسببها الجريمة السيبرانية. - إبراز أهم الإشكالات التي تترتب عن الجريمة السيبرانية في البيئة الرقمية. - محاولة تقديم أهم الآليات و الاستراتيجيات التي يمكن الاعتماد عليها في التحدي و التصدي للجريمة السيبرانية و كذا التقليل من آثارها الوخيمة. -محاولة تقديم مجموعة من التوصيات.

أهمية الدراسة: تعالج هذه الدراسة أحد المشكلات الحديثة و الآنية التي ظهرت و انتشرت نتيجة الاستخدام الغير قانوني لمختلف التكنولوجيات الحديثة للاتصال، هذه المشكلة التي أصبحت تؤرق الدول و المجتمعات نظرا لآثار الوخيمة التي تتجر عنها خاصة في ظل صعوبة التحكم في البيئة الرقمية.

المنهج و أدواته: أما بشأن المنهج المعتمد في معالجة هذا الموضوع فيتمثل في المنهج الوصفي الذي يفيد في التعرف على الظاهرة المدروسة في وضعها الطبيعي الذي تنتمي إليه، من خلال مسح المعلومات ذات العلاقة بمكوناتها الأساسية وما يسودها من علاقات داخلية وخارجية، وقد استخدمنا المقابلة مع بعض الباحثين المختصين في هذا المجال بالإضافة للملاحظة العلمية وكذا الوثائق المكتبية و الالكترونية والقيام بمسح و وصف لمضامين الوثائق والدراسات المتوفرة في هذا المجال، من أجل الشرح والتفسير للوصول إلى استبصارات جديدة حول الموضوع لمعرفة كيف انعكست الجريمة الالكترونية على البيئة الرقمية و ماهي الآليات التي يمكن الاعتماد عليها لاحتواء والتقليل من مخاطر هذه الجرائم.

1-مدخل مفاهيمي:

1.1-تعريف الجريمة السيبرانية: "بداية تعرف الجريمة بأنها تمثل سلوك سيئ متعمد يتسبب في إلحاق الضرر بالضحية أو يعرض الضحية إلى ضرر محتمل، أو ينتج عنه حصول الجاني أو محاولته الحصول على كسب فائدة لا يستحقها". أما الجريمة السيبرانية فقد تعددت تسميات المفكرين والباحثين في هذا المجال ولا يوجد إجماع على تعريف الجريمة السيبرانية من حيث كيف تعرف وما هي الجرائم التي تتضمنها الجريمة السيبرانية وفي أغلب الأحيان فهناك من يسميها: جريمة العصر، الجريمة الالكترونية، استخدام نظم المعلومات¹. فهي تمثل مختلف السلوكات التي ترتكب ضد الأفراد بدافع إلحاق الضرر بالطرف الآخر باستخدام الحاسوب وشبكات الاتصال المختلفة، فالجرائم السيبرانية بشكل عام هي جميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصال دورا أساسيا وتتكون الجريمة السيبرانية من كلمتين: هما الجريمة crime السيبرانية cyber وهو مصطلح مشتق من المصطلح الإغريقي Kubernan الذي يعني التسيير والقيادة، مع الإشارة إلى ان الجريمة السيبرانية لم يبيث في تعريفها من طرف رجال القانون باستثناء ما نصت عليه إجراءات الاتحاد الأوروبي الخاصة بمذكرة التوقيف، و قد عرفت هيئة الأمم المتحدة الجريمة السيبرانية: "أنها جميع السلوكات الغير قانونية التي تستخدم عمليات الكترونية تستهدف امن النظام المعلوماتي و المعطيات التي يعالجها"².

- "إنها جميع الأفعال المخالفة للقانون والشرعية والتي ترتكب بواسطة الحاسوب من خلال شبكة الانترنت، وهي تتطلب إلمام خاص بتقنيات ونظم المعلومات سواء لارتكابها أو للتحقيق فيها، ويقصد بها أيضا أي نشاط غير مشروع ناشئ من مكونات الانترنت وتسمى أيضا بالجرائم السيبرية أو السيبرانية لارتباطها بالعالم الافتراضي"³. كما "تتمثل في تلك الهجمات التي تستهدف أشخاصا وحتى المؤسسات والإدارات،

وتسعى للحصول على معلومات خاصة وشخصية (معلومات بنكية، كلمات مرور للمستخدمين للمواقع التجارية، من أجل استغلالها أو استخدامها أو بيعها) وقد تطورت وازدادت حدة ابتداء من عام 2017 حيث تحولت إلى ظاهرة مؤرقة⁴. كما عرفت أنها "تتمثل في استخدام التقنيات المرتبطة بشبكات المعلومات والاتصالات، التي تعد من الوسائط المستخدمة في هذا النوع من الجرائم، كما تقوم على استغلال مصداقية المستخدمين لسرقة المعلومات واستخدامها بشكل غير قانوني"⁵. وقد تبين من خلال الاستبيان الدولي الموجه للبلدان لتحديد معنى الجريمة الالكترونية أنه قد استخدمت أقل من 5 بالمائة من الدول كلمة جرائم إلكترونية في التشريعات التي استشهدت بها البلدان، وكان الاستخدام الأكثر شيوعاً هو جرائم الكمبيوتر أو الجريمة ذات التقنية العالية والتي تشترك كلها في الدخول غير المرخص به لنظام الكمبيوتر والمعلومات⁶. فالجريمة السيبرانية تتمثل في جميع الأفعال المخالفة للقانون والتي يتم ارتكابها بواسطة التكنولوجيات الحديثة و الانترنت بهدف الحصول على حقوق غير مشروعة من جهة مع إلحاق ضرراً أو تهديداً للطرف الآخر.

2.1- تعريف البيئة الرقمية:

-**تعريف البيئة:** تعرف بأنها مجموعة العناصر البشرية المتفاوتة المهام والاختصاصات والدرجات الوظيفية والقناعات والكفاءات العلمية، المتفاعلة فيما بينها وفق منظومة إدارية لإنجاز مهام محددة.

-**تعريف البيئة الرقمية:** تعرف أيضاً "بالبيئة التكنولوجية وهي عبارة عن البعد الإنساني للتطبيقات التكنولوجية المختلفة في المؤسسات، فضلاً عن تفاعل الإنسان وقناعاته ومدى تقبله للتغيرات التكنولوجية الجديدة"⁷. فالبيئة الرقمية تعكس ذلك الانتشار والاستخدام الكبير للتكنولوجيات الحديثة في جميع المجالات وهذا يؤدي لظهور بيئة افتراضية يتفاعل فيها الأفراد والدول إلكترونياً بعيداً عن الحواجز الجغرافية والزمنية فهي وليدة استخدام الإنسان لهذه التكنولوجيات.

2- مقارنة نظرية للجريمة السيبرانية في البيئة الرقمية:

1.2-**خصائص الجريمة السيبرانية:** تتميز الجريمة في البيئة الرقمية بخصائص تختلف عن الجريمة العادية بسبب خصائص أطراف الجريمة السيبرانية وطبيعة البيئة التي تحدث فيها، من أهمها نذكر:

-**جرائم عابرة للدول:** إنها جرائم لا تعترف بالحدود الجغرافية باعتبارها تنفذ عبر الشبكة المعلوماتية، مما يتطلب تحديات قانونية وسياسية لمواجهتها مثل جرائم غسيل الأموال والمخدرات وغيرها.

-**جرائم صعبة الإثبات:** يستخدم فيها الجاني وسائل معقدة وسريعة في كثير من الأحيان قد لا تستغرق أكثر من ثواني، بالإضافة لسهولة محو الدليل والتلاعب والاهم هو عدم تقبل القضاء في الكثير من الدول التقنية المعلوماتية التي تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة بالحواس.

- **جرائم مغرية للمرتكبين:** إن سرعة تنفيذها دون التواجد في مسرح الجريمة تجعلها مغرية لأنها توفر مبالغ مالية ضخمة. - **جرائم سهلة الارتكاب:** فهي جرائم ناعمة وعند توفر التقنية اللازمة تصبح سهلة⁸. كما يتميز مرتكب الجريمة يتميز بالذكاء والدهاء وذو مهارات عليا ودراية في استخدام الأجهزة الالكترونية، مع إمكانية تبادل الخبرات الإجرامية بين الهاركرز من خلال المواقع والمنديات و يتم اكتشافها بعد وقت طويل من ارتكابها مع صعوبة التوصل للجاني في ظل غياب الأدلة.

2.2- أهداف الجريمة السيبرانية: يمكن توضيح أهدافها في النقاط التالية:

- الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات وتعطيلها أو تخريبها وذلك عبر الانترنت.
- الوصول إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو تخريبها. -الحصول على عناوين تغيير مواقع الانترنت بهدف تخريب المؤسسات العامة. -الوصول إلى الأشخاص أو الجهات المستخدمة للتكنولوجيا بغرض التهديد أو الابتزاز. -الاستفادة من تقنية المعلومات من أجل كسب مادي أو معنوي أو سياسي كعمليات تزوير بطاقات الائتمان وعمليات اختراق المواقع الالكترونية. -استخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة⁹. يتضح مما سبق أن الجريمة السيبرانية ذات أهداف غير مشروعة تمارس ضغوطات لإلحاق الضرر بالطرف الآخر من خلال التهديد و الابتزازه أو السرقة المعلوماتية أو تخريب نظم المعلومات لتحقيق مكاسب خاصة مما ينعكس سلبا على البيئة الرقمية.

3.2-أنواع الجرائم السيبرانية: تعددت أنواعها وأشكالها لعل من أبرزها يمكن ذكر:

أ- **الجريمة المادية:** تسبب أضرار مادية على المستهدف من عملية النصب من بينها: السرقة الالكترونية كالاستيلاء على ماكينات الصرف الآلي والبنوك، إنشاء صفحة انترنت مماثلة جدا لموقع أحد البنوك الكبرى، الرسائل البريدية الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج مع الوعد بنسبة من المبلغ.

ب- **الجريمة الثقافية:** تتم من خلال استيلاء المجرم على الحقوق الفكرية ونسبتها له بدون موافقة الضحية مثل قرصنة البرمجيات من خلال نسخ لبرامج إحدى الشركات العالمية على أسطوانات وبيعها للناس بسعر أقل، وكذا التعدي على القنوات الفضائية بالإضافة لجريمة نسخ المؤلفات العلمية والأدبية.

ج- **الجريمة السياسية الاقتصادية:** مثلما تستخدمه المجموعات الإرهابية من اتصالات و بث أخبار مغلوطة، وتحويل بعض الأموال مع الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات ونشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان لا فساد الدولة لأسباب سياسية و اقتصادية. د- **الجريمة الجنسية:** تشمل الابتزاز والتعريض والاستدراج¹⁰. كانت هذه بشكل عام أهم أنواع الجرائم التي انتشرت بشكل كبير في البيئة الرقمية التي كانت نتيجة انتشار التطبيقات

التكنولوجية المختلفة بالإضافة للبعد الإنساني، فتفاعل الإنسان مع هذه الآليات الجديدة أوجد مشكلات وجرائم لم تكن معروفة من قبل مع الإشارة إلى أن الانتشار الكبير والإقبال الكبير على استخدام التكنولوجيات الحديثة بشكل عام و الانترنت بشكل خاص أدى لبروز مظاهر تميز البيئة الرقمية تختلف باختلاف ردود الأفعال في هذا المجال منها: -التحديات الفكرية والاجتماعية والإعلامية والسياسية والاقتصادية، لان التكنولوجيا جعلت المجتمعات تعيش في بيئة اجتماعية وظيفية معقدة.

-التناقضات والتعقيدات الإيجابية والسلبية معا. -هناك انبهار شديد وتحمس واندفاع نحو هذا النوع من التكنولوجيا من جانب البعض، يقابلها مقاومة شديدة مستمرة أو متقطعة من جانب آخر، كما هناك إعجاب شديد أو متوسط أو حتى قناعة مشوبة بالحرر من جانب، يقابله خوف وتردد من الجانب الآخر¹¹. هذا بشكل عام ما يميز البيئة الرقمية وكذا الجريمة السيبرانية. و يرى وول Wall إن الفضاء الرقمي قد خلق فرصا جديدة لارتكاب الجرائم من خلال خصائص فريدة تميز بها هذا الفضاء الرقمي مقارنة بالبيئة الواقعية من أهمها نذكر: -العولمة: التي تمكن الجناة على تجاوز الحدود الجغرافية التقليدية حتى الزمنية. -الإجمالية والشمولية: مكنت الجناة من إذلال ضحاياهم عن بعد دون التنقل والتواجد في مسرح الجريمة. - شبكات التوزيع: التي ولدت فرصا جديدة لتكوين الضحايا عبر الدول دون حدود. - مسارات البيانات: والتي خلقت فرصا جديدة للجاني لارتكاب سرقة الهوية¹². فالبيئة الرقمية وخصائصها ساهمت في نمو الجريمة السيبرانية سواء كانت تهديدا أو تخريبا، مع توفر الأمن و الفرار نتيجة غياب الأثر و صعوبة المتابعة في ظل غياب الرقابة الأمنية. فهذه الجريمة أكثر أمنا مقارنة بالجريمة التقليدية.

4.2-أسباب انتشار الجريمة السيبرانية: يمكن أن نلخص أسباب انتشارها في النقاط التالية:

- الرغبة في التعلم: بهدف الحصول على معلومات و سبر أغوار هذه التقنية المتسارعة التطور، ويفضل هؤلاء البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة و تعلم أكثر كيفية اختراق المواقع الممنوعة و التقنيات الأمنية الحاسوبية.

-الدوافع المادية "الربح و كسب المال": تتمثل في الرغبة في تحقيق مكاسب مادية في زمن قياسي.

- المتعة والتحدي والرغبة في قهر النظام المعلوماتي وإثبات الذات: إن اختراق الأنظمة الالكترونية و كسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة و تسلية كبيرة لمرتكبيها تغطي أوقات الفراغ... لإظهار تفوقهم والشعور بالقوة وجنون العظمة¹³. بالإضافة لعوامل أخرى مثل: - الرغبة في الانتقام من شخص مثلا أو من رب العمل أو من مؤسسة أو حتى من بعض الأنظمة السياسية في بعض الدول. -افتقاد ثقافة التعامل الآمن مع شبكة الانترنت. -عوامل اجتماعية أسرية تتعلق بطبيعة الحياة الاجتماعية المعاصرة التي نتج عنها الكثير من المشاكل التي أثرت على العلاقات الأسرية و زاد من العزلة و أدى لغياب المشاعر و الأحاسيس الأسرية. -عدم الاهتمام بتطبيق إجراءات التأمين والحماية الخاصة لجهاز الحاسوب¹⁴. بالإضافة للكثير من الأسباب الأخرى التي تختلف من بيئة لأخرى.

3- انعكاسات الجريمة السيبرانية على البيئة الرقمية: تسببت الجريمة السيبرانية في الكثير من المشكلات أو التهديدات في البيئة الرقمية التي بات من الصعب حصرها أو إيجاد استراتيجيات محكمة لمواجهتها خاصة مع تنوع أشكالها ومصادرها وتطورها المتسارع والمستمر. "ويقصد بالتهديدات في هذا المجال تلك الهجمات التي تتم باستخدام آليات وشبكات إلكترونية كالانترنت وأجهزة الحاسوب الآلي وهي تهدف لإلحاق الضرر بأجهزة أو شبكات أو حتى معلومات، وهي هجمات لا تستهدف الأفراد بصورة مباشرة وإنما التأثير في الفضاء الإلكتروني على الشبكات والأجهزة التي يستخدمها الأفراد وتعتمد عليها الدول مما يؤثر على أمن الدول،¹⁵ وسنوضح انعكاسات وتهديدات الجريمة من خلال ما يلي:

1.3-تهديدات الجريمة السيبرانية: إن الانتشار الكبير للتكنولوجيات الجديدة على نطاق العالم أدى لظهور أشكال من الجرائم المتصلة بالحواسيب والتي تشكل خطرا على سرية النظم الحاسوبية أو سلامتها أو توافرها، بل يتعدى ذلك ليشكل خطرا على أمن البنى الأساسية لأنظمة الدول لذا تحرص معظم الدول في العالم على النهوض بتكنولوجيا المعلومات والاتصالات حتى تتخطى المشكلات والتهديدات التي تحيط بهذا الاستخدام في البيئة الرقمية. "وتنقسم هذه الهجمات إلى هجمات تكنولوجية من خلال تركيب برامج التجسس وتثبيت برامج القراصنة وسرقة المعلومات وتدمير المواقع والحرمان من الخدمة، بالإضافة إلى هجمات هادفة تتم من خلال جمع المعلومات وفحص الشبكة لمعرفة النقائص مع استخدام الهندسة الاجتماعية بالتركيز على الإنسان عوض التقنية للوصول إلى المعلومات حول الهيئة المستهدفة¹⁶. لعل من أهم التهديدات التي تسببها الجريمة السيبرانية يمكن ذكر ما يلي:

1.1.3-الجرائم التي تستهدف الأفراد والهيئات: تستهدف فرد أو مجموعة من الأفراد وتتمثل في:

أ-**انتحال الشخصية أو سرقة الهوية:** يسميها بعض المختصين في أمن المعلومات بجريمة الألفية الجديدة، نظرا لخطورتها وسرعة انتشار ارتكابها خاصة في الأوساط التجارية والمصرفية تستهدف هذه الجريمة من وراء انتحال هوية الضحية، الاستفادة من مكانة صاحبها أو إخفاء هوية شخصية المجرم لتسهيل ارتكاب جرائم أخرى. ونظرا لخطورتها اتجهت الكثير من المعاملات على الشبكة الدولية إلى الاعتماد على وسائل أكثر أمنا لتوثيق الهوية كالتوقيع الرقمي من أجل التضييق على مرتكب هذه الجرائم.

ب-**التشهير وتشويه السمعة:** من خلال قيام الجاني بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن المجني عليه، الذي يمكن أن يكون فردا أو مؤسسة أو مجتمعا بأسره، مثل إنشاء موقع على الشبكة يتضمن المعلومات المطلوب نشرها وإرسالها عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين.

ت- **التغريب والاستدراج:** وهي جريمة تؤثر على العلاقات الإنسانية بشكل عام¹⁷.

ث-**الجرائم المالية والاقتصادية أو جرائم الاحتيال:** حيث تشمل جرائم السطو على أرقام البطاقات الائتمانية والتزوير وغسيل الأموال، و قد ظهرت مع انتشار مفهوم التجارة الإلكترونية وأصبح لصوص

البطاقات يستطيعون سرقة مئات الآلاف من بطاقات الائتمان من خلال شبكة الانترنت، بالإضافة لجرائم غسيل الأموال التي تستخدم الانترنت لتوسيع وتسريع أعمالها في غسيل الأموال غير المشروعة¹⁸.

ج- المضايقة والملاحقة: وتشمل وسائل تخويف وتهديد أو ملاحقة، قصد محاولة التحكم في الضحية.

ح- حقوق الملكية الفكرية: تعني حقوق التأليف والنشر الإلكتروني وتمثل شكل مهم من الحماية التي تكفلها الأنظمة والقوانين للأشخاص والجهات المسؤولة عن الإنتاج الفكري، لكن نظم المعلومات المعاصرة جعلت من السهل جدا تجاوز حقوق الملكية الفكرية وإعادة إنتاجها من دون ترخيص رسمي صادر عن أصحابها الأصليين¹⁹. بالإضافة للعديد من الجرائم الأخرى مثل الشغب والبرنامج الخبيثة والتجسس والجرائم الغير أخلاقية التي انتشرت بشكل كبير عبر مختلف دول العالم.

2.1.3- جرائم تهدد نظم المعلوماتية: تنقسم هذه الجرائم إلى نوعين:

- جرائم تقع على المكونات المادية للنظام المعلوماتي: يتم من خلال الاعتداء على المكونات المادية للنظام المعلوماتي ويتحقق ذلك بإتلاف الأجهزة وتدميرها أو بحرقها وغير ذلك من الأفعال المجرمة.

- وقوع الجريمة على المكونات المعنوية للنظام المعلوماتي: من خلال الاعتداء على المعلومات بكل صورها حيث يتم سرقتها أو إتلافها والعبث بها وهذه تعد أخطر أنواع الجرائم²⁰. بشكل عام هذه الجرائم جديدة ترتبط بالتكنولوجيا تقع في أغلب الحالات في بيئة المعالجة الآلية للبيانات، حيث تكون المعلومات محل الاعتداء عبارة عن نبضات إلكترونية، وتتنوع خطورة تهديدات هذه الجرائم من نوع لآخر من أهمها:

أ- الهجمات الشبكية: تتم عبر الشبكة الدولية للمعلومات وبإمكانها أن تسبب تباطؤ أداء الشبكة وتقلل فاعلية عمل البريد الإلكتروني والخدمات الإلكترونية الأخرى وتسبب أضرار بملايين الدولارات.

ب- صناعة ونشر الفيروسات: "وهي أكثر الجرائم انتشارا وتأثيرا والفيروس الإلكتروني عبارة عن برنامج غير مرغوب فيه من طرف المستعملين يحشر خلسة ضمن المعلومات المتبادلة عبر الشبكة (التراسل الإلكتروني مثلا) أو على حوامل مغناطيسية (القرص المرن عادة) وينفذ هذا البرنامج بدون إرادة المستفيد لفسخ أو تغيير أو سرقة المعلومات المخزنة على جهاز الحاسب، وتتسبب الفيروسات في أضرار وخيمة فتؤدي إلى تعطيل الشبكة أو الحاسب خاصة عندما يتم مهاجمة نظام التشغيل"²¹. ترجع خطورة الجريمة السيبرانية إلى ثلاث عناصر أساسية: -استنادها إلى تقنيات متقدمة ومتطورة: غالبا ما تكون تلك التقنيات حkra على دول معدودة وشركات كبرى تتحكم في هذه التكنولوجيات، خاصة وأن كثيرا من تلك التقنيات سرية وغير متاحة للتصدير مما يجعلها مصدرا لتهديدات إضافية.

-سرعة وسهولة انتشارها: إن عملية نشر الفيروسات الخبيثة أو شن هجمات لإعاقة الخدمات وغيرها من الأخطار السيبرانية يحدث بسرعة فائقة وسهولة تامة عبر الحدود من أي مكان و بأرخص التكاليف.

-**اتساع نطاق تأثيرها:** يكون التأثير بشكل مباشر أو غير مباشر على البنى التحتية وما قد يتبعه من أضرار أو خسائر، والتأثير يمكن أن يكون خاص أو عام بصورة مفاجئة وفي وقت قصير وعن بعد.²²

3.1.3- جرائم تهدد أمن الدولة: من أهم الجرائم التي تهدد أمن الدولة يمكن ذكر:

أ-**الجماعات الإرهابية:** حيث استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للانترنت من أجل بث معتقداتها وأفكارها، بل يتعدى الأمر إلى ممارسات تهدد أمن الدولة المعتدي عليها.

ب-**الجريمة المنظمة:** حيث استغلت عصابات الجريمة المنظمة الإمكانات المتاحة في وسائل الاتصال والانترنت في تخطيط وتمير وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة.

ت-**الجرائم الماسة بالأمن الفكري:** يعتبر الأمن الفكري من أخطر الجرائم المرتكبة عبر الانترنت، حيث توفر فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة لطمس الهوية المحلية.

ث-**جريمة التجسس الالكتروني:** سهلت أعمال الجوسسة على الأشخاص والدول أو مختلف المنظمات على القيام بعملية الجوسسة مثل التجسس العسكري، التجسس السياسي و التجسس الاقتصادي.²³

2.3- آليات الجريمة السيبرانية: يمكن ان نلخصها في النقاط التالية:

1.2.3-**"الحرمان من الخدمة:** يتمثل في ذلك الهجوم الذي يستهدف إيقاف قدرة الهدف على تقديم الخدمات المعتادة أو المفترض تقديمها، عن طريق إغراق الحاسب الآلي المقدم للخدمة بكم كبير من الأوامر تؤدي إلى توقفه عن العمل، أو الحد بصورة طبيعية نتيجة لهذا الكم من الأوامر وقد ينتج عن ذلك أيضا إيقاف الاتصال بين جهازين أو منع شخص معين من الوصول إلى الخدمة. ولقد شهدت الساحة الدولية أكبر موجة من هجمات الحرمان من الخدمة عام 2000 والتي نتج عنها إيقاف عدد من المواقع.

2.2.3-**البرامج الخبيثة:** تستخدم لإلحاق الضرر بأجهزة الحاسب الآلي ونظم المعلومات ومن بين الأضرار التي تنتج عن ذلك: فقدان الملفات من الذاكرة الخاصة بجهاز الحاسوب أو ملأ الذاكرة بالنفائات أو ببطء تشغيل الجهاز وبطأ عملية تبادل المعلومات أو إتلافها جزئيا من أهم آلياتها:

- **الفيروسات:** وهو برنامج قادر على تجديد نفسه وإن كان غير قائم بذاته، بمعنى أنه لابد أن يتم إلحاقه ببرنامج أو ملف آخر حتى ينتقل ولا يشغل الفيروس إلا بفتح البرنامج المصاب.

-**الديدان:** هي برامج قادرة على إعادة إنتاج نفسها بنفسها بمعنى لا تحتاج الى برامج أو ملفات ليتم إلحاقها حيث تقوم بتنفيذ نفسها تلقائيا، ويقوم هذا البرنامج باستغلال أي فجوة في نظم التشغيل كي ينتقل من حاسب لآخر أو من شبكة لأخرى عبر المواصلات التي تربط بينهما، وتتكاثر أثناء عملية الانتقال بإنتاج نسخ منها وتعمل على تقليل كفاءة الشبكة أو التخريب الفعلي للملفات والبرامج.²⁴

-**حصان طراودة:** هي برامج تبدو كما لو كانت آمنة ولكن بمجرد تحميلها تقوم بإلحاق الضرر بالجهاز المستهدف، وكثيرا ما تستخدم في التجسس الإلكتروني لأنها تستخدم كلمة السر التي تم الاستلاء عليها.

-**برامج التجسس** تقوم بنقل معلومات من جهاز المستخدم إلى مكان آخر دون علمه، عبر مراقبة الكتابة أو المواقع الإلكترونية التي يزورها وتجميع المعلومات الشخصية عنه بهدف سرقة المعلومات أو التجسس لأغراض تجارية. -**المراقبة:** تقوم بمراقبة الهدف و إرسال معلومات عنه وعن المواقع الإلكترونية التي يدخل عليها. -**سرقة كلمة السر والتصيد:** من خلال استخدام برامج التجسس²⁵.

3.3- الإشكالات المترتبة عن الجريمة السيبرانية: لعل ما يميز الجرائم السيبرانية أنها تحدث في الفضاء الرقمي مما يخلق صعوبة في ضبط المجرم وإخضاعه للعقاب، خاصة وأنها جرائم تتجاوز الحدود وتختلف الرؤى بشأنها من بلد لآخر ولعل من أهم المشكلات التي تترتب عنها يمكن ذكر:

-**تخريب المعلومات وإساءة استخدامها:** وتعد من أخطر الجرائم ويتم فيها التخريب بمحو الملفات أو تدمير الوسائط التي تحتويها، ولعل من أهم وسائل التدمير أن يقوم المجرم بتشفير هذه المعلومات والاحتفاظ بمفتاح الشفرة وعدم الكشف عنه. كما تتضمن جرائم إساءة استخدام المعلومات والمقصود بها الأذى الذي يتم تحقيقه باستخدام هذه المعلومات مثل عدم تمكين المستفيد من الوصول إليها أو كشفها أو استغلالها في إلحاق الضرر بمصالح صاحب المعلومات.²⁶

-**تزوير وتزييف البيانات:** بإدخال بيانات مغلوطة إلى قواعد البيانات أو القيام بتعديلها بشكل مقصود باستخدام بعض البرامج المساعدة الجاهزة المصممة خصيصا لتعديل البيانات في أماكنها بالإضافة لتزييف الوثائق ووضع وثائق مقلدة مثل الشيكات المصرفية والسندات وكذا تزوير العلامات التجارية.²⁷

-**انتهاك الخصوصية:** يتم بجمع البيانات وتخزينها على نحو غير مشروع مع إساءة استعمال البيانات أو المعلومات الاسمية والإفشاء غير المشروع لها وكذا الاعتداء على سرية الاتصالات والمراسلات.²⁸

-**التجسس المعلوماتي:** لقد أصبحت المعلومة تمثل سلاح جديد في حياة الشعوب ومختلف مؤسسات إدارة الدولة و تجاوزت أهمية الموارد الطبيعية كمصدر للقوة الاقتصادية والصناعية والعسكرية، فالحرية المتاحة في البيئة الرقمية تتيح إمكانية الوصول للمعلومات السرية التي قد تخفيها الهيئات والدول، مع الإشارة إلى أن التجسس المعلوماتي أصبح يشمل جميع مجالات الحياة الصناعية والعسكرية والاقتصادية والأمنية، ولعل من أبرز المعلومات التي يمكن أن تكون مجالا للتجسس المعلوماتي نجد المعلومة العسكرية التي تمثل أسرار الدولة الحربية والتي تتعلق بالجانب الاستراتيجي والأمني وهي معلومات سرية، لكن استخدام نظم المعلومات ساعد المخترقين في الوصول إليها مما يهدد الأمن القومي للدولة.²⁹

-**القرصنة والاختراق:** حيث يستغل القرصنة نقاط الضعف المتوفرة في الجوانب الأمنية لمواقع الشبكة، ليحصلوا على فرص للدخول إلى البيانات الخاصة بالمواقع من خلال استخدام برمجيات متنوعة لتحقيق

أغراض غير مشروعة مثل السرقة والتخريب عن طريق نقل أو مسح ملفات وبرامج أو إضافة برامج أخرى³⁰. بالإضافة للكثير من المشكلات الأخرى التي تهدد الأمن السيبراني.

4- آليات واستراتيجيات مكافحة الجريمة السيبرانية في البيئة الرقمية.

ان المواجهة الفاعلة للهجمات السيبرانية تستلزم التعاون والتنسيق على المستوى الدولي وكذا على المستوى الإقليمي والوطني، لتحقيق الأمن الإلكتروني والكشف عن التهديدات الأمنية المختلفة والتفاعل معها والتخفيف من الآثار السلبية المحتملة. والتصدي لمثل هذه الأضرار يتطلب العمل في اتجاهين:

-الاتجاه الأول: يكون بشكل داخلي حيث تقوم الدول المختلفة بسن القوانين الملزمة لمكافحتها في مختلف بلدان العالم³¹، و تعد السويد أول دولة أصدرت قانونا خاصا بالجرائم المعلوماتية حيث صدر قانون البيانات السويدي عام 1973 والذي عالج قضايا الاحتيال عن طريق الحاسب الآلي، كما أدركت الولايات المتحدة أهمية الموضوع حيث أصدرت أول تشريع على المستوى الفيدرالي خاص بجرائم الحاسوب عام 1977، ثم صدر قانون غش الحاسوب و إساءة استخدامه عام 1984 وقد خضع للتعديل عام 1986 و عام 1994، كما تم وضع مشروع القانون الأمريكي لجرائم الكمبيوتر و الانترنت عام 1998 بالإضافة إلى قوانين أخرى. كما اهتمت بريطانيا بالموضوع و اقرت قانون مكافحة التزوير و التزيف عام 1981 ثم سنت قانون إساءة استخدام الحاسوب لعام 1990³². أما في الوطن العربي فتعتبر الإمارات العربية المتحدة من الدول الأولى التي أولت الموضوع عناية خاصة حيث أصدرت القانون الاتحادي رقم 2 عام 2006 الخاص بمكافحة الجرائم الإلكترونية، كما أصدرت تونس مجموعة من التشريعات المتعلقة بالأمان السيبراني منها القانون رقم 5 لعام 2014 المتعلق بتنظيم مجال السلامة المعلوماتية وضبط القواعد العامة لحماية النظم المعلوماتية، بالإضافة للقانون رقم 89 لعام 1999 المتعلق بتنقيح و إتمام بعض أحكام المجلة الجنائية و إضافة فصل خاص بالجرائم المعلوماتية بالإضافة للقانون الأساسي رقم 63 لعام 2004 المتعلق بحماية المعطيات الشخصية³³.

أما في الجزائر فقد قام المشرع الجزائري باصدار القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، حيث تضمن في القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات ثمان مواد(من المادة 394مكرر الى المادة 394مكرر 7) إذ نصت المادة 394مكرر على "يعاقب بالحبس من ثلاثة أشهر (3) إلى سنة (1) و بغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة(6) أشهر إلى سنتين(2) و الغرامة من 50.000 دج إلى 150.000 دج³⁴". كما تؤكد

بقية المواد على مختلف الأفعال التي يعاقب عليها الجاني وطبيعة العقوبة التي تطبق عليه. بالإضافة للقانون رقم 09-04 المؤرخ في 5 أوت عام 2009 والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها الذي تضمن مجموعة من التدابير الوقائية التي يمكن الأخذ بها من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر، مثل مراقبة الاتصالات الالكترونية و الالتزام بالتعاون مع مصالح الأمن و المكلف بالتحقيق القضائي³⁵. من اهم القوانين التي فرضتها البيئة الرقمية نجد ايضا قانون رقم 18-07 مؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي³⁶ بهدف حماية الحياة الخاصة للأفراد والحفاظ على حقوقهم وكرامتهم، خاصة مع توفر وسائل التسجيل والتخزين والاسترجاع التي تتم بطريقة آلية مما يستدعي توفر قواعد عقابية لأي تجاوزات وجرائم في هذا المجال. كما أصدرت الجزائر القانون رقم 18-05 مؤرخ في 10 ماي 2018 يتعلق بالتجارة الالكترونية³⁷ حيث تضمن 50 مادة، يحدد هذا القانون القواعد العامة و الشروط المتعلقة بالتجارة الالكترونية للسلع و الخدمات من أجل تأطير مختلف المعاملات التجارية المختلفة المحلية و الخارجية القائمة على الاتصال الالكتروني. بالإضافة لقانون رقم 15-04 مؤرخ في 1 فبراير 2015 يحدد القواعد المتعلقة بالتوقيع والتصديق الالكترونيين مبرزا ماهية و وآليات إنشاء التوقيع الالكتروني الموصوف والتحقق منه، و كذا دور مختلف سلطات التصديق الالكتروني مع الإشارة في الباب الرابع للعقوبات الجزائية في حالة عدم احترام قواعد التصديق الالكتروني³⁸، بعد أن أصبحت مختلف المعاملات تتم إلكترونيا مما يستدعي ضبط مسؤولية كل طرف في حالة حدوث تجاوزات. و يعتبر في هذا المجال الأستاذ ب. لطفي لمين "أن الجزائر أثبتت جدارتها في التعاطي مع الأشكال الجديدة من الإجرام و قد سبق لها أن صدرت تجربتها في مكافحة البعض منها كما هو الشأن بالنسبة للظاهرة الارهابية وقد أضفى ذلك على الجزائر مكانة جعلتها مدرسة يحتذى بها في مجال مكافحة الإرهاب، وكذلك الشأن بالنسبة للجريمة الالكترونية التي أدت بالجزائر إلى إعادة النظر في ترسانتها القانونية وهندسة ميكانيزمات وآليات تسهر على تنفيذها هيئات وطنية مخولة قانونا، بما يمكن من مواجهة التحديات والتهديدات التي تترص بالأمن القومي مع توظيف تكنولوجيا حديثة في هذا الشأن لا سيما الهندسة الاجتماعية والذكاء الاصطناعي"³⁹. كما يعتبر الأستاذ أحمد عظيمي "ان المشكل في الجريمة السيبرانية أنها ترتبط بالتطور التكنولوجي لذلك فان ظهور الجرائم يسبق وجود نصوص تشريعية تمنعها و تمنح القاضي الأداة القانونية لمعالجتها، فجريمة القذف مثلا عبر الفضاء الالكتروني لم تكن مقننة قبل الانتشار الواسع الذي عرفته المنصة الاجتماعية الفيسبوك، لذلك يمكن القول ان ما هو متوفر من قوانين لحد الآن يعتبر كافيا للتعامل مع الجريمة السيبرانية بالوسائل المتاحة الآن، غير انه على المشرع الجزائري كما هو الشأن في العالم كله أن ينتظر انتشار تكنولوجيات جديدة وظهور ممارسات غير شرعية ليقتن كيفية التعامل معها، مع الإشارة إلى أن البلدان الكبرى تملك مراكز بحث تتابع كل ما يحدث في المجتمع مع محاولة استباق نتائج كل جديد مؤثر على المجتمع أو

الدولة بصفة عامة بينما لا تتوفر على مثل هذه المراكز عندنا⁴⁰. يتضح مما سبق أن هناك عناية بسن مجموعة من القوانين الخاصة بالجريمة السيبرانية مع الإشارة إلى أنها جاءت موزعة بين عدة قوانين مثل قوانين العقوبات، قوانين تكنولوجيا المعلومات وقوانين أخرى، مع ذلك فإن تأطير الجريمة السيبرانية من الناحية القانونية يبقى من المواضيع الشائكة نظرا للتطور التكنولوجي السريع و صعوبة مسايرة مستجدات هذه الجرائم.

-الاتجاه الثاني: يكون ذات بعد دولي من خلال عقد اتفاقيات دولية، حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج وآثار هذه الجرائم⁴¹. مع الإشارة إلى أن الدول الكبرى هي الأكثر اهتماما بالأمن الإلكتروني نتيجة لامتلاكها لقدرات تكنولوجية هائلة وكذا اعتمادها بشكل كبير على أنظمة المعلومات في إدارة شؤون الدولة، ولذا نجد أن اهتمامها بهذه القضايا يأتي في إطار استراتيجيات وسياسات واستخدام الفضاء الإلكتروني كـ مجال لإدارة التفاعلات الدولية، في حين يظل اهتمام دول الجنوب بقضايا الأمن الإلكتروني محدودا ومقصورا فقط على محاولة التصدي للتهديدات الأمنية المرتبطة به.⁴² "إن الأمن المعلوماتي يمكن أن يلعب دورا هاما في تطوير تكنولوجيا المعلومات و خدماتها المختلفة عبر الخط، و جميع دول العالم اليوم في حاجة لتقوية أمنها المعلوماتي وحماية الهيئات الأساسية القائمة على المعلومات، و تحقيق ذلك يتطلب تعاون محلي و دولي مع الهيئات المعنية في ضبط استراتيجيات قائمة على مقاربة شاملة"⁴³.

1.4-الاتفاقيات الدولية: من أهم صور التعاون الدولي في هذا المجال يمكن ذكر إستراتيجية بلدان مجموعة 8 سنة 1997 وهي استراتيجية رائدة في محاربة الجريمة السيبرانية وتطوير طرق تحديد هجمات الكمبيوتر والمتسللين ومساعدة بعضهم البعض، والمشكل الكبير أمام تحقيق إستراتيجية دولية مثل إستراتيجية الدول الثمانية الكبرى هو افتقاد بعض الدول للخبرة في مجال التكنولوجيا و غياب تشريع خاص بهذا المجال، مما يمثل عقبة في مجال التعاون الدولي في هذا المجال⁴⁴. يمكن ذكر أيضا اتفاقية بودابست في 23 نوفمبر 2001 ودخلت حيز التنفيذ في عام 2004 حيث أكد مجلس أوروبا والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة أدت لظهور فضاء جديد يسمى بالفضاء المعلوماتي الذي يستخدم لأغراض شرعية، ولكن يمكن أن يستخدم هذا الفضاء في ارتكاب أعمال إجرامية، مما يتطلب مواكبة هذا التطور بقوانين جنائية تسير تطور هذه التكنولوجيات واستخداماتها في البيئة الرقمية⁴⁵. كما تناولت الاتفاقية الإرهاب الإلكتروني وعمليات التزوير لبطاقات الائتمان كما تحدد أفضل الطرق الواجب إتباعها في جرائم الانترنت التي تعهدت الدول الموقعة بالتعاون من أجل محاربتها، وقد وقعت على الاتفاقية 30 دولة كما انضم إليها أعضاء من خارج المجلس الأوروبي وأبرزها الولايات المتحدة الأمريكية سنة 2006، وألمانيا سنة 2009 أما فرنسا فقد صادقت عليها سنة 2006، وقد اشتملت الاتفاقية على عدة جوانب من جرائم الانترنت بالإضافة للعديد من الاتفاقيات والمعاهدات الدولية

وكذا المؤتمرات الدولية مثل قمة المؤتمر السيبراني بالولايات المتحدة الأمريكية عام 2014 الذي ناقش التدابير المضادة للتهديدات السيبرانية وتعزيز أمن القطاع العام والخاص في مواجهة الجريمة الالكترونية.⁴⁶ بالإضافة للمعاهدة الأوروبية لمكافحة جرائم الانترنت التي وقعت اللجنة الخاصة بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية لمعاهدة شاملة تهدف لمساعدة البلدان على مكافحة جرائم الانترنت، وعلى إلزام الدول الموقعة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية⁴⁷. كما طالب المختصون أيضا بضرورة "تبني إستراتيجية عربية لمكافحة هذه الجريمة وتتمثل الخطوط العامة لهذه الإستراتيجية: أن تقوم الحكومات العربية بتطوير لوائح وقوانين وفقا لخصائص شبكة الانترنت والعمل على إدخال نظم الدفع الالكتروني إلى البنوك العربية، وضرورة تقديم ضمانات خاصة لحماية المستهلك مع إصدار قوانين وتشريعات تقوم بتجريم سرقة المكونات الصلبة لأجهزة الكمبيوتر مع التنسيق بين الأجهزة الأمنية في الوطن العربي وتوحيد الجهود العربية في هذا المجال واستخدام التكنولوجيا في مجال مكافحة الجريمة والتقليص من حجمها⁴⁸. فهذه الاتفاقيات بشكل عام تهدف لمواجهة مختلف أشكال التهديدات السيبرانية مع تكثيف التعاون الدولي، و السؤال الذي يطرح نفسه في هذا المجال هل يمكن الاكتفاء بالجانب القانوني و المعاهدات في التحدي للجريمة السيبرانية؟ يعتبر الأستاذ زغلامي العيد في هذا المجال "أن معالجة أو التقليل من هذه المشاكل يتطلب التعامل مع الأسباب و ليس مع الجريمة في حد ذاتها، و هذا يتطلب تظافر الجهود بين مختلف المجالات من خلال القيام بدراسة شاملة وعميقة بين مختلف التخصصات (علم الاجتماع، الاقتصاد، السياسة، الإعلام، القانون، علم النفس الخ) بهدف التوصل لمعرفة الأسباب الحقيقية لانتشارها و اتخاذ الآليات المناسبة، لان معالجة المشكلة لا يرتبط فقط بالجانب القانوني وإنما بمعرفة الأسباب الحقيقية"⁴⁹. كما يعتبر الأستاذ عظيمي أحمد "انه لا بد من إنشاء مراكز وخلايا بحث تعنى بآثار استخدام تكنولوجيا الإعلام و الاتصال و تهتم بالدراسات المستقبلية و التغيرات التي تحدث في المجتمع و إدخال ثقافة "الاستخدام الرقمي" في مستويات التعليم ليتعرف الشباب على طبيعة الجريمة الالكترونية التي لا تختلف عن الأنواع الأخرى من الجرائم، مع العمل على قمع الجريمة من خلال تطوير آليات عمل الأجهزة المكلفة بتتبع واكتشاف واقتياد القائمين بها إلى القضاء".⁵⁰

2.4- أهمية الأمن الرقمي من خلال البرمجيات المضادة للاعتداءات الالكترونية: بداية يتمثل أمن المعلومات في تلك التدابير الوقائية التي تستخدم للمحافظة على المعلومات وسريتها من السرقة و الاختراق و يشمل: حماية المعلومات من الضرر بمختلف أشكاله سواء كان مصدر هذا الضرر أشخاص أو برامج كالفيروسات، حماية المعلومات من الوصول غير المصرح به أو السرقة أو سوء الاستخدام، تمكين أنظمة تقنية المعلومات والبرامج من العمل بشكل آمن. ويقوم أمن المعلومات على ثلاثة عناصر أساسية: السرية، التكامل وسلامة المحتوى، التوافر والإتاحة⁵¹. هناك آليات أخرى تتمثل في:

-في الجانب التكنولوجي: يجب التأكد من استخدام Logiciels securises توفر أكبر قدر من الحماية والسرية للمعلومات. -في الجانب الانساني: توعية العملاء بأخطار الجريمة وأشكالها وعوقبها الوخيمة و كذا التدريب و التعود على الممارسات الايجابية لضمان سرية المعلومات. -استخدام برنامج wimi Armored الذي يمثل منصة تعاونية سهلة الاستخدام وأمنة للغاية تسمح بالتعاون بفعالية في جميع المشاريع الحساسة مع ضمان السرية".⁵² الأمن الرقمي يتيح لنا باتخاذ إجراءات أمنية احترازية توفر القدرة على التحكم بالمخاطر والتهديدات السيبرانية، وتعد البرمجيات المضادة للاعتداءات السيبرانية من أهم الآليات التي يمكن أن تركز الأمن المعلوماتي من خلال اتخاذ بعض الإجراءات الوقائية التي تعمل على تدمير البرامج الخبيثة التي يمكن أن تتواجد بذاكرة الحاسوب، كما تعمل على منع تحميل هذه البرامج على الحاسب وعلى إيقاف أغلب الاعتداءات باستعمال برمجيات وبرامج الجوسسة ولعل من أهم هذه البرمجيات يمكن ذكر Nettools و acunetix و coffre fort و antisniffer بالإضافة للعديد من البرمجيات الأخرى التي يمكن أن تساعد بالقضاء على البرامج الخبيثة، كونها تتضمن وسائل متطورة تسمح باكتشاف وتحطيم البرامج الخبيثة خصوصا عند الارتباط بشبكة الانترنت من أهمها نذكر:

-الجدران النارية FireWalls: كواحد من الاستراتيجيات المتبعة لمنع عمليات الدخول غير الشرعية من الأنترنت، ويعتبر بمثابة ممر إلكتروني يراقب الدخول إلى الشبكة والخروج منها، وأصبحت تقوم بعمل فعال في مجال التحقق من هوية المستخدمين واكتشاف البرامج الخبيثة ومواجهة مختلف التهديدات الإلكترونية، كما يعتبر كحارس بوابة الذي يقوم بحماية الشبكات الحاسوبية المختلفة من التطفل والتدخل.⁵² -التشفير Encryption: حيث يتم تشفير البيانات المتبادلة مع التأكد عند حل التشفير من أن الرسالة الإلكترونية لم تتعرض للتغيير أو التعديل. وتعتمد عملية التشفير على تغيير محتوى الرسالة باستخدام ما يسمى بمفتاح التشفير وذلك قبل إرسال الرسالة على أن تكون لدى المستقبل القدرة على استعادة المحتوى في صورتها الأصلية باستعمال مفتاح فك الشفرة. وبشكل عام هناك أسلوبين:

أ-أسلوب الشبكة الخاصة الافتراضية: يوفر ممر أمان من خلال تشفير كل البيانات والرسائل قبل تبادلها.
ب-أسلوب الأمان من خلال نظام SSL الذي يسمح بتشفير كل البيانات الخاصة مع توفر ما يسمى بشهادات الموثوقية أو الرقمية المدعمة ببروتوكول SSL التي يمكن أن يتحصل عليه الموقع ليصبح جديرا بالثقة.⁵³ مثل هذه الإجراءات الوقائية يمكن أن تقلل من الآثار الوخيمة للجريمة السيبرانية بالإضافة للعديد من الآليات الأخرى مثل: حماية الملكية الفكرية بإبرام معاهدات وكذا حماية القصر.

خاتمة

إذا كانت تكنولوجيا المعلومات والاتصال قد وفرت وسهلت الكثير من الإجراءات العملية، فإنها في المقابل قد فتحت الأبواب أمام انتشار الكثير من المشكلات والجرائم التي باتت تهدد البيئة الرقمية، خاصة في المجتمعات النامية التي مازالت تعاني من الفجوة الرقمية نتيجة انتشار الأمية الرقمية وعدم التحكم في استخدام هذه التقنيات الحديثة مما يستدعي اتخاذ إجراءات مشتركة بين الدول المختلفة بهدف التصدي لهذه التهديدات التي تحيط بالأفراد والدول للتقليل من آثارها الوخيمة. إن مواجهة انعكاسات الجريمة السيبرانية تعد من أصعب التحديات التي تتطلب تضافر الجهود خاصة وأن استخدام هذه التكنولوجيات في تزايد مستمر في إدارة مختلف الشؤون الأمنية والاقتصادية والعسكرية مما يتطلب التعاون بين الدول في مجال أمن المعلومات ومواجهة الجريمة السيبرانية. و من أهم التوصيات التي يمكن أن نقدمها في هذا المجال: -مواكبة تطورات هذه الجريمة وهذا يتطلب القيام ببحوث ودراسات لمعرفة الأسباب الكامنة وراء انتشار مثل هذه المشكلات وكذا محاولة إيجاد الآليات التي يمكن أن تقلص من آثارها الوخيمة. -نشر ثقافة الوعي في استخدام هذه التكنولوجيات لتجنب مخاطر الجريمة السيبرانية. -نشر المعرفة التكنولوجية ومحاربة الأمية التكنولوجية التي تعد سبب رئيسي في انتشار الجريمة. -التأكيد على مخاطر الجريمة السيبرانية من خلال وسائل الإعلام التي يمكن أن تقوم بدور تحسيسي و توعوي في هذا المجال. -تعزيز التعاون على المستوى العربي. -توفير الآليات الخاصة بالاستخبارات التي يمكن أن تساهم في استشعار التهديدات قبل وقوعها من خلال الكشف المبكر. -التأكيد على دور التربية الإعلامية في التعامل مع المضامين التي توفرها هذه الوسائل. -التأكيد على أهمية تبني استراتيجية أمنية مجتمعية تساهم فيها مختلف الأطراف. -تشجيع التكوين في هذا المجال من خلال الاستفادة من تجارب البلدان المتطورة. تكثيف جهود التعاون على المستوى الدولي والمحلي لمحاربة مختلف مظاهر الجريمة السيبرانية.

الهوامش

- 1- منال هلال زهرة، تكنولوجيا الاتصال والمعلومات، ط1، دار أسامة، الأردن، 2014، ص 374.
- 2- Romain Beas, **La lutte contre la cybercriminalité au regard de l'action des états**, doctorat de droit prive et sciences criminelles, université de lorraine, Faculté de droit, Paris, 2016, p 25-26.
- 3- المركز الديمقراطي العربي، "الجرائم الالكترونية: الأهداف، الأسباب، طرق الجريمة ومعالجتها"، أوت 2016، ص4، تاريخ زيارة الموقع: 4-02-2019، انظر الموقع: democraticac.de
- 4-10 Bonnes pratiques anticybercriminalite, FIDSUD CDBA, Fidsudedba.fr, visite le 12/10/2019.
- 5-Amber Finey, Les différentes forme de cybercriminalité, site visite 3/9/2019. [http : // cybercriminalite-penal.fr](http://cybercriminalite-penal.fr)
- 6-عباس لحر، البعد الاستراتيجي لتكنولوجيا المعلومات، دار هومة، الجزائر، 2018، ص 224.
- 7-عامر إبراهيم قنديلجي، الحكومة الالكترونية، ط1، دار المسيرة، الأردن، 2015، ص 332-333.
- 8- ناجي ملاعب، الأمن السيبراني: تعريف الجرائم السيبرانية وتطورها، موقع مجلة الأمن والدفاع العربي زيارة الموقع 6-2-2019 أنظر الموقع sdarabia.com .
- 9-طارق أحمد الطيبي، الجرائم الالكترونية عبر الإعلام الالكتروني، ندوة علمية عن "الإعلام الأمني الالكتروني"، السعودية، جامعة نايف للعلوم الأمنية، 2012، ص 3. أنظر الموقع tarek@ictp.edu.eg
- 10- منال هلال زهرة، مرجع سابق، ص 374-375.
- 11-عامر إبراهيم قنديلجي، الحكومة الالكترونية، مرجع سبق ذكره، ص 333.
- 12-ذياب موسى الذيابنة، الجرائم الالكترونية: المفهوم والأسباب، ورقة مقدمة في الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية" الأردن، 2014، ص2 .
- 13-نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر و التوزيع، ص الاردن، ص 90-93
- 14-محمود الرشيد، العنف في جرائم الانترنت، اهم القضايا: الحماية و التامين، الدار المصرية اللبنانية، القاهرة، 2011، صص 66.
- 15- شفيق نوران، أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني، ط1، المكتب العربي للمعارف القاهرة، 2016، ص 19-20.
- 16-Amber Fiiney, opcit.-
- 17- منال هلال زهرة، مرجع سبق ذكره، ص 304.
- 18-عامر إبراهيم قنديلجي، الحكومة الالكترونية، ط1، دار المسيرة، 2015، ص 312.
- 19-نفس المرجع السابق، ص 316.
- 20-نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، عمان، ص 97.
- 21- منال هلال زهرة، مرجع سبق ذكره، ص 308-309.
- 22-هبة السيد، عناصر وراء خطورة التهديدات السيبرانية، 12-12-2018، انظر الموقع: www.youm,

- 23-حفوظة الأمير عبد القادر، حسام غرداين، **الجريمة الالكترونية و آليات التصدي لها**، مركز جيل البحث العلمي، أنظر الموقع، jilrc.com تاريخ زيارة الموقع، 1-2-2019.
- 24- محمد أمين الشوابكة، **جرائم الحاسوب والانترنت** دار الثقافة للنشر والتوزيع، الأردن، 2009، ص 240.
- 25- شفيق انوران، مرجع سبق ذكره، ص 21-27.
- 26- نوال هلال زهرة، مرجع سبق ذكره، ص 376.
- 27- نفس المرجع، ص 36.
- 28- نهلا عبد القادر المومني، مرجع سبق ذكره، ص 177-178.
- 29- نفس المرجع السابق، ص 211.
- 30- عامر إبراهيم قندليجي، **الإعلام الإلكتروني**، ط1، دار المسيرة، الأردن، 2015، ص 355.
- 31- نهلا عبد القادر المومني، مرجع سبق ذكره، 2010، ص 53.
- 32- دليلة العوفي، **آليات مكافحة الجريمة المعلوماتية، دراسة حالة الجزائر 2009-2016**، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية علوم الإعلام و الاتصال، جامعة الجزائر 2019-2020، صص 196-199.
- 33- نفس المرجع السابق، ص 205.
- 34- الجمهورية الجزائرية، **قانون العقوبات**، رئاسة الجمهورية، 2015، ص 157.
- 35- اسمهان بوضياف **"الجريمة الالكترونية و الإجراءات التشريعية لمواجهتها في الجزائر"** مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 11 ديسمبر 2018، ص 367.
- 36- الجمهورية الجزائرية، **الجريدة الرسمية عدد 34**، القانون رقم 18-07 مؤرخ في 10 يونيو 2018 يتعلق بحماية الاشخاص الطبيعيين و معالجة المعطيات ذات الطابع الشخصي.
- 37- الجمهورية الجزائرية، **الجريدة الرسمية عدد 28**، القانون رقم 18-05 مؤرخ في 10 ماي 2018 يتعلق بالتجارة الالكترونية، ص 5.
- 38- الجمهورية الجزائرية، **الجريدة الرسمية عدد 06**، القانون رقم 15-04 المؤرخ في 10 فيفري 2015 يتعلق بالتوقيع والتصديق الالكتروني، ص 6.
- 39- مقابلة مع الاستاذ ب. لطفي لمين، كلية علوم الاعلام و الاتصال، جامعة الجزائر، يوم 29/10/2020.
- 40- مقابلة الكترونية مع أ.د. عظيمي أحمد، كلية علوم الإعلام والاتصال، جامعة الجزائر 01/11/2020، ص 11 صباحا.
- 41- شفيق نوران، مرجع سبق ذكره، ص 7.
- 42-union internationale des télécommunications, **comprendre la cybercriminalité : guide pour les pays en développement**-Département de politique et stratégies, projet de document, 2009, p 13
- 43- **Lutter contre la criminalité sur le net**, Dixième congrès des nation unies pour la prévention du crime et le traitement des délinquants, ODCCP, www.un.org presse 2000, Site visite le 3/9/2019.
- 44- شفيق نوران، مرجع سبق ذكره، ص 53.
- 45- ليلى الجنابي، **فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية**، دراسات وأبحاث قانونية، 2017، أنظر الموقع: www.m.ahewar.org في 20\02\2019

- 46-ربيعة فندوشي، الإعلان الإلكتروني، دار هومة، الجزائر، 2011، ص 120.
- 47- شريف درويش اللبان، تكنولوجيا الاتصال، المخاطر و التحديات والتأثيرات الاجتماعية، الدار المصرية اللبنانية، القاهرة، 2005، ص 162-163.
- 48- Lionel Roux, CEO Wimi, **Cybercriminalités : exemples et mesures pour protéger les projets sensibles** 2018. Visité le 10/10/2019. www.appvizer.fr
- 49-مقابلة مع د. العيد زغلامي، كلية علوم الاعلام والاتصال، جامعة الجزائر3، يوم 2020/10/26، سا. 11.
- 50-مقابلة مع أ.د. أحمد عظيمي، مرجع سبق ذكره.
- 51-عباس لحمر، مرجع سبق ذكره، ص 236.
- 52- المرجع نفسه 237. 53-المرجع السابق ص 237.