السنة: 2020 المجلد: 05 العدد: 02 ص ص: 125 - 145
EISSN 2676-1645 ISSN 2543-375X

الأمن الفضائي السيبراني –التحديات والحلول–

Cyberspace Security - Challenges and Solutions-

حورية بن سيدهم[1]، جامعة سطيف2،
bensidhoumhouria@gmail.com
رقية عواشرية، جامعة باتنة1 rokayamoi@yahoo.fr

تاريخ الإرسال: 2020/03/14 تاريخ القبول: 2020/05/24

ملخص:

تهدف هذه الدراسة إلى الوقوف عند أهم التحديات التي تواجه الأمن الفضائي السيبراني، بعد أن أصبح اختراقه من أهم التحديات التي تجعل أمن الأفراد والشركات والدول في خطر، والبحث على أهم الحلول التي يمكن بتجسيدها للوقاية أو مواجهة الأخطار التي تهدد الأمن السيبراني، وكذا ملاحقة وتعقب مرتكبي الجرائم الواقعة في هذا الفضاء الافتراضي.

وقد خلصت هذه الدراسة إلى أن الجرائم السيبرانية ذات طبيعة خاصة، وخصوصيتها تفرض وجود جهاز تحقيق وقضاة مختصين على درجة عالية من التأهيل كما تتطلب تخصيص غرف على مستوى المحاكم والمجالس القضائية تختص في هذا النوع من الجرائم. وتتطلب من جهة أخرى نصوص عقابية وإجرائية خاصة. كما أن البعد الدولي لهذه الجريمة يفرض ضرورة التعاون القضائي وتسليم المجرمين.

الكلمات المفتاحية: -الأمن السيبراني– الجريمة السيبرانية– الإنترنت– المعلومة – المجرم السيبراني.

Abstract:

This study aims to identify the most important challenges facing cyberspace security, after its penetration has become one of the most important challenges that make the security of

[1] -المؤلف المراسل

individuals, companies and countries at risk, and look at the most important solutions that can be embodied to prevent or address threats to cybersecurity, as well as Prosecuting and tracking perpetrators of crimes in this virtual space.

This study concluded that cybercrime is of a special nature, and its specificity requires the existence of an investigative body and competent judges with a high degree of qualification, as well as requiring the allocation of rooms at the level of courts and judicial councils specialized in this type of crime. The international dimension of this crime also dictates the need for judicial cooperation and the extradition of the criminal.

Keywords: Cybersecurity1, Cybercrime2, Internet3, Information4, Cyber criminal5.

مقدمة:

أدى التطور التكنولوجي الواسع في مجال الإتصالات إلى أن يصبح الحاسوب أداة للتعامل بين الأشخاص والشركات والمؤسسات، وبالرغم مما وفرته شبكات المعلومات الإلكترونية من وفرة في الوقت والجهد، إلا أنها تواجه من جانب أخر أخطارا يصعب تعقبها، إذ ظهرت العديد من أنماط الإعتداء لم تعد تغطيها الجرائم التقليدية، وإن كان القاسم المشترك بينها أنها تشكل أضرارا كبرى للمؤسسات.

إن الجريمة السيبرانية تختلف عن الجريمة التقليدية فمكان ارتكابها مسرحا افتراضيا وخصوصيتها تؤدي في الكثير من الحالات إلى التكتم عليها حفاظا على سمعة المؤسسة، وثقة العملاء بها، كما أن هذه الجريمة تتميز بعالميتها، فضلا أنها صعبة الإثبات. ومن جهة أخرى فإن مرتكبوها ليسوا بحاجة إلى مهارات وتدابير معقدة. كما أن مسألة استخدام تكنولوجيا الأمن السيبراني إذا كانت ممكنة في الشركات الكبرى فإنها ليست كذلك بالنسبة للشركات الصغيرة والمتوسطة، لأن ذلك يتطلب أموالا كثيرة ترهق ميزانيتها.

إن تنامي الجرائم السيبرانية يتزامن مع تزايد عدد المتعاملين بالأنترنت، وهذا مادعا البعض للقول بأن هناك دولة جديدة ظهرت هي دولة المتعاملين بالأنترنت ويبلغ عدد سكانها حوالي 40 مليون مواطن يتزايدون بنسبة خمسة بالمائة شهريا، ويوقع أن يصل في المستقبل القريب إلى 720 مليون، ويعود ذلك إلى أن الأنترنت لم تعد قاصرة على الباحثين وموظفي المؤسسات، وإنما طالت الأفراد والشركات الخاصة وأصبحت عصب عالم التجارة. ".(علي، 38، 2009).

مما سبق بات ضروريا البحث في جملة التحديات التي تواجه الأمن الفضائي السيبراني لغرض وضع حلول لها، وهو يشكّل معالم مشكلة البحث والدافع الرئيسي لدراسة ومعالجة هذا الموضوع.

وتندرج ضمن هذه الإشكالية تساؤلات فرعية تتمثل:

- ماهي أهم مهددات الأمن السيبراني؟

- كيف يمكن الوقاية من هذه المهددات؟ وما السبل الكفيلة بمكافحتها في حالة وقوعها؟

وتظهر أهمية هذه الدراسة في اعتماد الأفراد والمؤسسات والدول في تعاملاتهم على شبكة الأنترنت التي وإن وفرت الوقت والمسافات والمال، إلا أنها كلفتهم من جانب آخر مخاطر لا يحمد عقباها لمن لم يتبع أنظمة حمائية متطورة، وهو مالا يكون متاحا عند الأفراد بل وعند الكثير من المؤسسات الصغيرة والمتوسطة خصوصا في الدول النامية.

وعليه تهدف هذه الدراسة إلى إبراز أهم الجهود المبذولة على المستويين الوطني والدولي، لمواجهة الأخطار المحدقة بالأمن السيبراني سواء تعلق الأمر بالآليات التشريعية أو المؤسساتية. ولفت انتباه صناع القرار خصوصا السلطة التشريعية إلى ضرورة إعادة النظر في الكثير من تشريعاتها وخصوصا التشريع الجنائي، لأن قواعده لم تعد تستوعب هذه الصور المستحدثة من الإجرام السيبراني، نظرا لخصوصيتها مما يجد مرتكبوها في مبدأ شرعية التجريم والعقاب ملاذا للفرار.

لدراسة هذا الموضوع تم الإعتماد على المنهج التحليلي بصفة أساسية، كما اعتمد المنهج الوصفي لوصف حجم الظاهرة وأهم مهدداتها لتصل الدراسة في الختام إلى وضع تصور متكامل يعتقد أنه قادر على معالجة كل سلوك غير مشروع يرتكبه فرد لحسابه الخاص أو لحساب شخص معنوي بواسطة جهاز الحاسب الآلي عبر شبكة الإنترنت مخترقا بذلك الزمان والمكان، ابتغاء الحصول على منفعة مادية أو معنوية أو سياسية.

1-مهددات الأمن الفضائي السيبراني

إن الأمن الفضائي السيبراني باتت تحدق به أخطارا عدة بعضها تقني راجع إلى تعدد استخداماته، وبعضها قانوني، وهو ما يتم تناوله على النحو الآتي:

1.1-المهددات التقنية

بلغ عدد الموصلين بالأنترنت عام2011 ما لا يقل عن 2.3 بليون نسمة، أي ما يعادل أكثر من ثلث مجموع سكان العالم، ويتوقع عام2020 أن يفوق عدد الأجهزة المتصلة بالشبكة عدد الناس بنسبة ستة إلى واحد.(فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، 2013). مما يعنى أنه من المنتظر أن تتم أغلب المعاملات بين الأفراد والشركات والمنظمات عبر هذا العالم الافتراضي مرتبا أثارا إيجابية، إلا أنه من ناحية أخرى قد تكون له أثارا كارثية اجتماعية واقتصادية في غياب تدابير حمائية، ويمكن أن نورد أهم بعض هذه المهددات:

1.1.أ-التسويق الالكتروني: يواجه المستهلك فردا كان أم شركة أثناء عملية التسوق الالكتروني مجموعة من الأخطار سواء قبل إبرام العقد، حيث يواجه المستهلك في هذه المرحلة التضليل فيما يخص شخص المتعاقد أو مواصفات البضاعة أو الخدمات أو ثمنها. ولا تتوقف المخاطر عند هذه المرحلة، وإنما تتعدى مرحلة إبرام العقد، وذلك بشأن غموض شروط التعاقد أو ضمانات التسليم، وقد يتعرض إلى اختراق طرف ثالث أثناء تبادل الإيجاب والقبول. وتستمر المخاطر إلى مرحلة تنفيذ العقد وتتعلق بالتسليم أو التزويد أو عدم تطابق السلعة أو الخدمة للمواصفات المتفق عليها.(الطويل، 77، 2017).

يعد المستهلك الطرف الضعيف في العلاقة ولذا خصته التشريعات بالحماية حتى في العقود العادية، وقد اختلفت التشريعات في تحديد شخص المستهلك، حيث يذهب التشريع المصري إلى أن الشخص الذي يقوم بالشراء أو التزود بالخدمة لأغراض مهنته لا يعتبر مستهلكا بدعوى أن هذا الشخص يعتبر خبيرا في مجال الأنشطة التي تدخل في مجال مهنته.(الطويل، 80، 79، 2017). وبالرغم من وجاهة هذا الرأي في بعض جوانبه، إلا أنه في اعتقادي يجب أن لا يأخذ على إطلاقه، لأن هناك من المؤسسات الصغيرة التي لا تتوفر على الخبرة اللازمة في هذا المجال، ولا تمكنها ميزانيتها من الاستعانة بمن يملكون الخبرة الكافية.

لقد بات الإعلان المضلل سيف مسلطا على المستهلك بوصفه يحتوي على معلومات تهدف إلى إيقاع المتعاقد عبر الانترنت في خلط أو خداع في عنصر أو عناصر جوهرية في السلعة أو الخدمة المعلن عنها. وقد عرف الإشهار المضلل بأنه: "الإعلان الذي من شأنه خداع المستهلك، أو من الممكن أن يؤدي إلى ذلك". (Pllimen,2010/2011,241). وعليه فالإعلان يعتبر مضللا عندما يخلف فكرة خاطئة في ذهن المستهلك، وهو ما يتحقق في حالتين: حالة الإعلان الكاذب، وحالة الإعلان الذي يدفع إلى الوقوع في الغلط سواء بسبب تركيبته أو إغفال ذكر المعلومات كإعلان شركة الطيران مثلا عن أسعار منخفضة تستقطب المستهلك، مع إغفال ذكر أن هذه الأسعار قبل الخضوع للرسوم. (Delphine,2015,48). وللإشارة فان المبالغة في الإعلان لا تعد تضليلا، نظرا لأن العبارات والألفاظ التي تستخدم في المبالغة عبارات بالغة العمومية وغير محددة. (الناشف، 95، 1999). ومع ذلك حتى وإن كان الإعلان المبالغ فيه غير محظور إلا أنه يتعين على الأعوان الاقتصاديين عدم التعسف في استعمال المبالغات مع عدم تجاوز حدود المعقول، وهي الحدود التي يرجع إخضاعها لمعيار المستهلك المتوسط. (Chandeb,2012,81).

لقد أدت كثرة المواقع الالكترونية التي تسوق للسلع والخدمات واشتداد التنافس بين الشركات لتقديم السلعة بشكل مغري، مما فتح المجال لتسويق بضائع مقلدة أو مغشوشة في كثير من الأحيان. (الجريدلي، 80، 2008).

إن ضرورة ضمان مبدأ حسن النية والشفافية في مجال التسوق الإلكتروني يتطلب سن نصوص قانونية رادعة، فقد أوصى دليل منظمة التعاون الاقتصادي والتنمية OCED إلى ضرورة سن نصوصا واضحة توجب على مقدم السلعة أو الخدمة تقديم بيانات كافية تحدد شخصية المتعاقد وتحدد طبيعة السلعة أو الخدمة أو مواصفاتها ومخاطرها، وكذلك بيان واضح لكيفية حل أي نزاع قد ينشأ نتيجة إبرام مثل هذه الصفقات، والقانون الواجب التطبيق على النزاع. (Perez.2008.700).

1.1.ب-غسيل الأموال: تعد الأنترنت الأداة المثالية لغسل الأموال نظراً لطبيعتها الافتراضية وسرعة التحويل وتحررها من القيود الإقليمية (طبيعتها العابرة للحدود، وتعارض الاختصاصات والولايات القضائية). وهو ما تعلم عملاء غسل الأموال استغلاله. والإنترنت تجعل من الممكن تحويل الأموال ذات المنشأ الإجرامي إلى دوائر اقتصادية قانونية وذلك باستخدام الحوالات المالية والاستثمار والرسملة. فالاستثمارات والمقامرة والتجارة على شبكة الإنترنت، كبيع سلع وخدمات خيالية مقابل نقود حقيقية، تجعل في المستطاع توليد دخول تبدو مشروعة ويصعب رصدها ويكاد يستحيل مقاضاتها. فالعمليات المصرفية الإلكترونية والعمليات العقارية عبر الشبكة، واستخدام شركات كواجهات خيالية والنقد الإلكتروني يمكن استخدام كل ذلك في غسل غنائم الجريمة. والمستعملون العاديون قد يدعمون عن جهل غسل الأموال عندما يستخدمون خدمات وهمية معينة. كما أن المنظمات التجارية قد تصبح دون قصد ضالعة في ذلك بكل ما يرافق ذلك من تداعيات كارثية من الناحيتين القانونية والتجارية. وهذا مصدر رئيسي للمخاطر بالنسبة للشركات. ويوجد الآن عدد قليل من الوسائل الفعالة للتحكم في هذه الظاهرة الخاصة بغسل الأموال المتصل

بتكنولوجيا المعلومات. (دليل الأمن السيبراني للدول النامية، 32، 33، 2007).

لقد أشار التقرير الذي أعدته الأمم المتحدة وصندوق النقد الدولي إلى أن28.5 مليار دولار من الأموال القذرة تطير سنويا عبر الأنترنت لتخترق حدود67 دولة لغسلها. (رصاع، 83، 2011، 2012،).

وعليه تشكل جريمة غسيل الأموال أحد مهددات الأمن الفضائي السيبراني خصوصا في الدول النامية، ومنها البنوك الجزائرية لعدم توفرها على نظام معلوماتي متطور من شأنه أن يعرقل عملية مكافحة تبيض الأموال التي تتم عبر الوسائط الالكترونية، مما يقتضي ضرورة استخدام أنظمة التبادل الالكتروني التي توفر أمنا أكثر سواء بالنسبة للبنوك أو بالنسبة للزبائن، وذلك للحد من ارتكاب جريمة تبيض الأموال الكترونيا، وبالرغم من تتكبده البنوك من تكلفة لأعمال هذه الأنظمة، إلا أن الخسائر الناجمة عن عملية التبييض تفوق بكثير تكلفة استخدام أنظمة التحويل الآمنة. (عبد الله، 186، 2017).

1.1.ج-خصوصية مرتكب الجريمة السيبرانية: يتميز المجرم السيبراني بمميزات خاصة تميزه عن المجرم العادي، وربما تعود هذه الخصوصية إلى خصوصية محل الفعل غير المشروع. فهذا المجرم وعلى خلاف المجرم العادي لا يحتاج إلى العنف لارتكاب فعله الجرمي ولا إلى مجهود عضلي، فهو مجرم متخصص ومحترف، ولذلك يطلق على الجرائم السيبرانية الجرائم الناعمة (عاقلي، 122، 2017). كما أن المجرم السيبراني مجرم عائد إلى الإجرام (موسى، 219، 2017). فهو مجرم لا يقهر.

وفي غالب الحالات تكون الرغبة في تحقيق العائد المادي الباعث من وراء ارتكاب هذا النوع من الإجرام، وقد يكون الباعث منها الانتقام من رب العمل، أو مجرد الرغبة في قهر نظام الحاسب واختراق حاجزه الأمن. (موسى، 219، 2017).

إن مرتكب الفعل الجرمي في هذا النوع من الجرائم قد يكون فاعلا أصليا أو شريكا في ارتكابها، فالفاعل الأصلي غالبا ما يكون أحد العاملين أو المستخدمين في منشأة تدار بالنظام المعلوماتي بصرف النظر عن المستفيد من وراء ارتكاب مثل هذا الفعل. ونظرا لكون هذا النوع من الإجرام يتطلب الدقة في التنفيذ، فانه قد يستلزم مشاركة أو مساعدة أشخاص آخرين، سواء أكانوا فنيين أم مجرد وسطاء وذلك بفعل أو امتناع عن فعل وقد يلعب هؤلاء الشركاء الدور الرئيس في نجاح العملية غير المشروعة أو المستهدفة. (المقصودي، 109، 2017). وللأسباب السابقة فقد ساوى المشرع الجزائري بين عقوبة الفاعل الأصلي وعقوبة الشريك، وهو ما نصت عليه المادة 394 مكرر5 من قانون العقوبات القسم السابع مكرر1 والخاص بالمساس بأنظمة المعالجة الآلية للمعطيات. كما ساوى كذلك بين الشروع في ارتكاب هذه الجرائم بنفس العقوبة للجريمة الكاملة، وهو ما نصت عليه المادة 394 مكرر 7من ذات القانون.

وفي الأخير تجدر الإشارة إلى أن المجرم السيبراني قد يكون فردا وقد يكون شخصا معنويا كالشركات والمؤسسات، وقد خص المشرع الجزائري الجرائم السيبرانية المرتكبة من قبل هذا الأخير وعلى خلاف التشريعات المقارنة بنص خاص وذلك في المادة 394مكرر4 من قانون العقوبات بنصه: " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في القسم بغرامة تعادل خمس(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

2.1-المهددات القانونية

تمتاز الجرائم السيبرانية بخصوصيات تميزها عن الجرائم العادية وتجعل من قوانين العقوبات وقوانين الإجراءات الجزائية غير قادرة على استيعابها، لأن تطورهما لا يتم بنفس الوتيرة. فالجرائم السيبرانية تقع في بيئة افتراضية ولا تترك أثارا مادية، وكونها تقع في بيئة افتراضية فهي جريمة لا تعرف الحدود مما يتصور معها أن تتأثر عدة أماكن في دول مختلفة في آن واحد.

2.1.أ-مظاهر السلوك الإجرامي المكون للجرائم السيبرانية: صنفت اتفاقية بودابست بشأن الجرائم الالكترونية لعام 2001 هذه الجرائم إلى:

-الجرائم التي تستهدف سرية وسلامة وتوفر المعطيات.

-الجرائم المرتبطة بالكومبيوتر، أي الجرائم التي يلعب فيها الكومبيوتر أو الحاسب الآلي دور الوسيلة كجرائم الاحتيال والتزوير الالكتروني.

-الجرائم المرتبطة بالمحتوى، أي يلعب فيها الكومبيوتر دور البيئة الجرمية، كجرائم القمار وغسيل الأموال والمخدرات.

-الجرائم المتعلقة بحقوق الملكية الفكرية كحقوق المؤلف.

أما المشرع الجزائري فقد تناول هذه الجرائم في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات. في المواد من 394مكرر إلى 394مكرر7، وقسمها إلى الطوائف التالية:

-جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير، وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات.

-الجرائم الإلكترونية بواسطة النظام المعلوماتي، وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي، كجرائم التحويل الالكتروني والسطو والنصب والاحتيال والسلب وغيرها.

-الجرائم المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب.

-الجرائم الإلكترونية للشخص المعنوي.

2.1.ب-الجريمة السيبرانية جريمة عالمية: يعد البعد الدولي في الجريمة السيبرانية أهم التحديات التي تواجه الأمن السيبراني، مما يجعل آثارها تتعدى حدود الدولة الواحدة وتترتب على عالمية الجريمة السيبرانية عدة أثار قانونية أهمها القانون الواجب التطبيق عليها، فضلا عن الجهة التي يؤول إليها

الاختصاص في مثل هذه القضايا لتتداخل قوانين عدة دول. وهو الأمر الذي يستدعي التعاون والمساعدة القضائية. (ديلمي، 100، 2017).

ويسوق الفقه للتأكيد على البعد الدولي لهذه الجريمة القضية المعروفة بإسم نقص المناعة المكتسبة(الأيدز)، وتتلخص وقائعها التي حدثت عام 1989 بقيام شخص يدعى جوزيف يوب بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي في ظاهره عبارة عن نصائح خاصة بمرض نقص المناعة المكتسبة، غير أن هذا البرنامج في حقيقته يحتوي على فيروس(حصان طروادة)، حيث يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة من خلالها يطلب الفاعل مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس. وفي الثالث من فبراير من عام1990 تم إلقاء القبض على المتهم جوزيف يوب في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي على أساس أن البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليمه، وتم توجيه إحدى عشرة تهمة ابتزاز إليه، وقعت معظمها في دول مختلفة، غير أن إجراءات محاكمته لم تتم بسبب حالته العقلية. (صغير، 22، 2013).

2.1.ج-صعوبة إثبات الجريمة السيبرانية: يعد إثبات السلوك غير المشروع الماس بالأمن السيبراني من أهم التحديات، وذلك بفعل طبيعة الجاني والمجني عليه، وكذلك وسيلة تنفيذها. فالمجرم في غالب الحالات محترفا ذكيا لا يترك أثارا لاقترافه الجرم، والمجني عليه في غالب الحالات مؤسسات عامة أو خاصة تفضل الإحجام عن الإبلاغ حفاظا على سمعتها وثقة عملائها ومركزهم الاجتماعي، فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية. (ديلمي، 102، 2017) ولهذه الأسباب اقترح في الولايات المتحدة الأمريكية بأن تفرض النصوص المتعلقة بجرائم الحاسوب التزاما على عاتق موظفي الجهة المجني عليه بالإبلاغ عما يقع عليها من جرائم متى وصل إلى علمهم ذلك مع تقرير جزاء في حالة إخلالهم بهذا الالتزام. (عاقلي، 122، 2017).

فضلا عما سبق فإن صعوبة إثبات هذه الجرائم يرجع إلى كونها تعتمد على قمة الذكاء في ارتكابها، مما يصعب على المحقق التقليدي التعامل مع هذا النوع من الجرائم، فالوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى. (المقصود، 115، 114، 2017) كما أن مرتكبيها قد يلجؤون لتشفير التعليمات لمنع إيجاد أي دليل يدينه. (رستم، 24، 1999) بعبارة أخرى فان الجريمة السيبرانية لا تترك أثارا ملموسة، وهي بذلك لا تترك شهودا يمكن الاستدلال بأقوالهم، ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية. (عاقلي، 125، 2017) كل هذا يتطلب احترافية عالية عند رجال الضبطية القضائية حتى يتمكنوا من الكشف على هذه الجرائم، وحتى لا يتسببون في إتلاف الدليل الالكتروني. كما يجعل من تدريب القضاة وتأهيلهم وسن نصوص إجرائية تتلاءم والجريمة السيبرانية أكثر من ضرورة.

إن ما سبق يؤكد أن معظم الجرائم السيبرانية يتم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، وهذا ما يؤكد أن حجم الجرائم التي لم تكتشف أكبر بكثير من تلك التي كشف عنها على أساس أنها تفتقر إلى الدليل المادي التقليدي كالبصمات. (عاقلي، 122، 2017).

2.1.د-عدم تطورأحكام قانون العقوبات بنفس السرعة التي تتطوربها التكنولوجيا: تعد الجرائم السيبرانية ظاهرة إجرامية حديثة ارتبطت بظهور الحاسبات، وهذا ما يجعل تطبيق النصوص التقليدية يثير مشكلات عديدة في مقدمتها مسألة الإثبات التي تتطلب الحصول على أثر مادي، لإمكانية محوها في ثواني، كما أن البيانات التي يجرى البحث عنها قد تكون مشفرة، ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة، ومن هنا تثور مسألة مدى مشروعية إجباره على فك الشفرة، كما أن عناصر هذه الجرائم ترتكب في أكثر من دولة مما يطرح صعوبة ملاحقتهم خاصة إذا كانت هذه الدول لا تربطها اتفاقيات تعاون في هذا المجال. (المقصودي، 113، 2017).

إن هذا النوع من الجرائم سيجعل مبدأ الشرعية في أزمة وهو الضامن لمصلحة الأفراد، كما أنه السور الحقيقي لحماية حقوق الأفراد وكفالة

حرياتهم الفردية، فتطبيقه بحذافيره سيقف عائقا أمام مكافحتها. خصوصا وأن المرونة التي طرأت على مبدأ شرعية التجريم والعقاب، قد وردت في شقه الثاني المتعلق بتقدير العقوبة دون الشق الأول الخاص بإنشاء الجرائم، فقد بقي هذا الشق جامدا مما يمنع القاضي من أية سلطة تقديرية في هذا الشأن، الأمر الذي يتطلب نصوص جديدة تستوعب هذه السلوكات غير المشروعة والمهددة لجميع المعاملات التي تتم في هذا العالم السيبراني.

2.1.هـ-غيابالتعاون الدولي أوبطئه: تعد الجريمة السيبرانية جريمة عالمية، وعليه تتطلب مكافحتها تكاثف جهود الدول في هذا المجال، سواء من حيث تدريب وتأهيل القائمين على التحقيق والمتابعة، أو من حيث الاتفاق على مفهوم الأفعال المكونة لهذه الجرائم، لأن عدم وجود تعريف موحد وتعدد التشريعات في هذا المجال هو الذي يؤدي يطرح مشكلة تنازع القوانين والجهة المختصة. وللإشارة فإن مبدأ السيادة يقف عائق أمام جهود التعاون في هذا المجال.

أشار الاستبيان الذي قدمه فريق خبراء معني بإجراء دراسة شاملة عن الجريمة السيبرانية إلى التباين في نطاق الأحكام المتعلقة بالتعاون في الصكوك المتعددة الأطراف والثنائية، وعدم فرض أجال ملزم للاستجابة للطلبات، وعدم الاتفاق على إتاحة النفاذ المباشر إلى البيانات التي توجد خارج الولاية القضائية، وتعدد شبكات سلطات إنفاذ القانون غير الرسمية، والتباين في ضمانات التعاون، أمور تمثل تحديات كبيرة في وجه التعاون الدولي الفعال فيما يتعلق بالأدلة الالكترونية في المسائل الجنائية. (فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، 14، 15، 16، 2013).

2-الحلول المقترحة لمواجهة تحديات الأمن السيبراني

إن الأمن السيبراني لا يمكن تحقيقه إلا من خلال وضع حلول لمعالجة ومواجهة التحديات التي تحدق به، وذلك من خلال:

1.2-الحلول التقنية

يتعين على المتعاملين عبر شبكة الأنترنت اعتماد كلمة سر صعبة الاختراق وتغييرها بصورة دورية. فضلا عن ضرورة اعتماد نموذج الأرشيف الاحتياطي

للبيانات، وضمان الحماية والخصوصية باستخدام تقنيات التشفير. فضلا عن استعمال ما يطلق عليه جدار الحماية Frrewelوالذي يضاهي الدور الذي تقوم به جمارك الحدود للحيلولة دون دخول الأجسام الغريبة والضارة. كما يتعين من جهة أخرى استخدام تقنية التوقيع الرقمي لمنع تزوير الرسائل الالكترونية. (قوراري، راحلي، 56، 55، 2017). ونظرا لأن المصارف والبنوك وشركات البطاقات الائتمانية من أكثر المؤسسات استهدافا من قبل الجرائم السيبرانية، فانه يتعين عليها تطبيق إجراءات وقائية ضد الاحتيال، وتنصيب برمجيات مراقبة خاصة على خوادمها لتعقب النشاطات غير المعتادة على حسابات العملاء ووضع أنظمة لتنبيه العميل على كل عملية تتم على حسابه. (حفوظة، غرادين، 99، 2017).

2.2-ضرورةالتدخل التشريعي لمواجهة الجرائم السيبرانية

إن السرعة المذهلة لتكنولوجيا المعلومات والاتصال، أدى إلى فراغ تشريعي بخصوص الجرائم المستحدثة في الفضاء السيبراني والتي لا يمكن بأي حال من الأحوال إخضاعها إلى القواعد التقليدية الخاصة بقانون العقوبات وقانون الإجراءات الجزائية، الأمر الذي يستتبع ضرورة سن تشريعات جديدة تطبق على هذا النوع من الإجرام. وهناك عدة أنماط تشريعية أو كيفيات يلجأ إليها المشرع لصياغة نصوص الحماية الجزائية لنظم المعلومات مع إمكانية الجمع بينها، إما بإتباع أسلوب الإضافة، أو أسلوب وضع نصوص جديدة، أو وضع نص رئيس ينطبق على الأوجه المختلفة للجريمة السيبرانية، وأخيرا أسلوب الجمع بين الأنماط السابقة. (عباوة، 281، 2017).

واختيار نمط من هذه الأنماط يتوقف إلى حد كبير بالوقت الذي يتدخل في المشرع لمواجهة هذا النوع من الإجرام، وكذا طبيعة النظام القانوني في كل دولة.

أما بالنسبة للمشرع الجزائري فقد اعتمد أسلوب خص بموجبه الجرائم السيبرانية بقسم خاص من قانون العقوبات هو القسم السابع مكرر أضيق بعد

تعديل هذا القانون، المتضمن المساس بأنظمة المعالجة الآلية للمعطيات، ويحتوي على سبع مواد تهتم بشتى أنواع الاعتداء على الأنظمة المعلوماتية.

الملاحظ على المشرع الجزائري وعلى غرار المشرع الفرنسي جعل المادة المجرمة للتلاعب داخل أنظمة المعلوماتية من المرونة بحيث يستوعب شتى أنواع التلاعب بالمعطيات ليساير التطور المتواصل في هذا المجال، وان كان قد خص بعض أنواع البطاقات بنصوص مستقلة كالقانون 01/08 المتعلق بالتأمينات الاجتماعية الذي يحرم الاعتداء على بطاقة الشفاء الالكترونية. (عباوة، 288، 2017).

وللإشارة فان الجرائم السيبرانية تترك مشكلة أساسية تتعلق بالمصطلحات، وهو ما يخلق تضاربا في تشريعات الدول، حيث أن ما يكون مشروعا في دولة قد لا يكون كذلك في أخرى، مما يقتضي الدقة والوضوح عند تحديد أنماط السلوك الإجرامي.

3.2-ضرورة الشراكة بين القطاع العام والخاص

تستخدم الشراكات من أجل تيسير تبادل المعلومات عن التهديدات والاستراتيجيات المتخذة والحلول الاستباقية، ولا يمكن لأي عمل تشاركي أن يؤتي ثماره في غياب التنسيق، لأن التنسيق يؤدي إلى إزالة سياسة التناقضات ويمنع التعارض في الاختصاصات.

4.2- ضرورة التعاون الدولي

نظرا للآثار الذي تتركه ارتكاب الجرائم خاصة ذات الطبيعة العالمية على المجتمعات والذي يؤدي إلى إهدار حقوق الإنسان فإن المجتمع الدولي ككل اقتنع بضرورة التعاون الثنائي والإقليمي والدولي من أجل تحقيق القضاء على الجريمة ونشر العدالة، حيث جاء هذا الكلام في مقدمة إعلان فيينا بشأن الجريمة والعدالة الصادر عن مؤتمر الأمم المتحدة العاشر المتعلق بمنع الجريمة ومعاملة المجرمين المنعقد في فيينا من 10إلى 17 أفريل 2000. هذا الإعلان يقر ويشدد على مكافحة هذه الظاهرة في إطار التعاون الدولي المكثف، وذلك من خلال المبدأين 4 و12.

وبذلك فإن الإعلان يقر صراحة أن التعاون لدولي هو الوسيلة الأنجع لمكافحة الجريمة ذات البعد الدولي كالجرائم السيبرانية خصوصا في مجال المساعدة القضائية وتسليم المجرمين، خصوصا وأن هذه الجرائم تحتاج الى السرعة في التحقيق لإمكانية محو الدليل في ثواني وعليه فان عدم الاستجابة في الوقت المناسب تؤدي إلى ضياع الدليل.

وفي الأخير تجدر الإشارة إلى أن تعزيز التعاون الدولي يقتضي الانضمام إلى الاتفاقيات الدولية والإقليمية الخاصة بحماية البيانات والمعلومات.

5.2- نشرالوعي الرقمي بين المستخدمين

لا ينبغي أن تقتصر التوعية بمخاطر مهددات الأمن السيبراني على المؤسسات والشركات في القطاعين العام والخاص، وإنما يجب أن تتعدى إلى الأفراد بصفتهم الحلقة الضعيفة في هذا النوع من الإجرام الذي يتطلب ثقافة عالية بتقنيات المعلومات والاتصال، فالمواطن العادي أصبح متعاملا عبر هذا الفضاء السيبراني، مما يقتضي الأمر توعيته بدوره الممكن في حماية نفسه من الوقوع ضحية للجرائم السيبرانية باقتنائه برمجيات الحماية من الفيروسات. ولذلك يجب أن تلعب الأسرة دورها التوعوي في هذا المجال بعد أن أصبح الأطفال ضحايا الجرائم السيبرانية كجرائم المواد اللاأخلاقية للأطفال، وكذا المدرسة مؤسسة الإنتاج الثانية التي تكمل عمل الأسرة، .كما يتعين على المؤسسات الأكاديمية القيام بدورها في مجال تثقيف المهنيين وتدريبهم والمساهمة في اقتراح القوانين والسياسات والعمل على تطوير الحلول التقنية. كما يتعين استحداث ماستر أكاديمي ومهني يختص بالأمن السيبراني ومهدداته وسبل حمايته، وإدخال الأمن السيبراني إلى صلب المناهج العلمية في الكليات ذات العلاقة.

وفي سبيل التوعية الأمنية عكفت المؤسسات الأمنية الجزائرية منذ2002 على عقد الأيام المفتوحة في مختلف ولايات الوطن والمقدرة ب48ولاية، وذلك في إطار تجسيد سياستها الخاصة بعصرنة قطاع الأمن وفقا لما يفرضه واقع الوقاية من الانحراف والجريمة من ضرورة التكامل بينها وغيرها من مؤسسات

المجتمع، وقد كانت المؤسسات التربوية أحد الشركاء الذين راهنت عليهم في هذه العلاقة التكاملية، نظرا للدور والوظائف المنوطة بها في تربية النشء وكذا توعيته.

6.2-إنشاءهياكل خاصة بالتصدي للجرائم السيبرانية

وهو ما نصت المادة 14 من اتفاقية بودابست للإجرام المعلوماتي. وتحقيقا لذلك وأمام تزايد الإجرام السيبراني وعجز أجهزة الضبطية القضائية عن التحقيق فيها وكشف مرتكبيها، قامت الأنظمة المقارنة باستحداث أجهزة متخصصة. ويمكن في هذا المجال استعراض التجربة الجزائرية: (نمديلي، 132، 2017).

-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: أنشئت بموجب القانون 04-09 المؤرخ في 5أوت 2009 والخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

-المعهد الوطني للأدلة الجنائية وعلم الإجرام: يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن انجاز خبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات.

-المديرية العامة للأمن الوطني: تتصدى هذه المديرية للجريمة الالكترونية من عدة جوانب، ومنها الجانب التوعوي.

وفي الأخير نقترح على المشرعين إنشاء شرطة جنائية على غرار شرطة العمران والمياه وغيرها محاكاة لما هو معمول به في بعض الدول.

7.2-تأهيل وتدريب المعنيين: يتطلب مكافحة الجرائم السيبرانية خبراء ذوي مؤهلات وقدرات فنية عالية، ومعرفة بتركيب الكومبيوتر وكذا المعرفة الشاملة لشبكة الأنترنت، وكذا كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف.(عاقلي، 126، 2017).

إن خصوصية الجرائم السيبرانية تقتضي تأهيل وتدريب العاملين في جهاز التحري والتحقيق في هذا النوع من الجرائم التي لا تعتمد على القوة البدنية – على خلاف الجرائم التقليدية-بقدر ما تعتمد على المهارة الفنية والتقنية في مجال تكنولوجيا المعلومات والاتصال. كما ينبغي أن يطال التأهيل القضاة والنيابة العامة، كما يقتضي الوضع استحداث غرف متخصصة على مستوى المحاكم الابتدائية والمجالس القضائية للفصل في هذا النوع من المنازعات.

ونظرا لأن عملية التدريب والتأهيل تحتاج إلى خبراء وأموال، فانه يجب على الدول المتقدمة تقديم الدعم الدولي في مجال تمويل الدورات التدريبية. وتحقيقا لذلك ولغرض تأهيل الأجهزة الضبطية والقضائية أشرف خبراء من الاستخبارات الأمريكية، وعملاء من مكتب التحقيقات الفيدرالي سنة2010على ورشة تكوينية بالجزائر حول "مكافحة الجريمة المعلوماتية" لفائدة ضباط الشرطة القضائية والقضاة، وقد ركز التدريب على الجانب النظري والعملي واستفاد منه عشرة ضباط من الشرطة القضائية وستون متخصصا في الجريمة المنظمة. (الدبور، 224، 2017).

خلاصة القول بأن هذا النوع من الإجرام يحتاج إلى تقنية عالية لا تكون متاحة لدى الدول النامية، الأمر الذي يتطلب تعزيز التعاون الدولي في هذا مجال تدريب وتأهيل وتمكين المؤسسات المتخصصة في هذه الدول من اللازمة.

خاتمة:

توصلت الدراسة للنتائج والتوصيات التالية :

1-النتائج:

أ-حماية أمن الفضاء السيبراني مسؤولية الجميع، مما يقتضي التعاون الدولي لحمايته.

ب- يواجه الأمن الفضائي السيبراني تحديات تقنية وقانونية على رأسها الجرائم السيبرانية.

ج-تخلف الجرائم السيبرانية أثارا اقتصادية واجتماعية كارثية.

د-تتميز الجرائم السيبرانية بخصوصية راجعة لصفة مرتكبها، وطبيعة المجني عليها، كما أنها ذات بعد دولي مما يجعل أمر مكافحتها ليس بالأمر السهل.

و-تتميز تكنولوجيا المعلومات بسرعة في التطور، هذه السرعة تتزامن مع أشكال جديدة من الجرائم التي تعجز النصوص العقابية التقليدية على استيعابها، خصوص في ظل المبدأ العريق مبدأ شرعية التجريم والعقاب.

ز-صعوبة إثبات الجرائم السيبرانية لغياب الدليل المادي.

2-التوصيات :

أ-ضرورة سن نصوص عقابية وإجرائية تتلاءم مع طبيعة الجرائم السيبرانية، لعدم تواءم تطبيق النصوص التقليدية عليها.

ب-ضرورة وضع تدابير حمائية من قبل المؤسسات والشركات والدول، لأن أيا كانت تكلفتها فإنها لا يمكن أن تضاهي حجم الخسائر التي تنتج عن اختراق الفضاء السيبراني.

ج-ضرورة تأهيل رجال الضبطية القضائية والقضاة ورجال النيابة العامة وتدريبهم على التقنيات الحديثة في مجال التحقيق والحكم في مثل هذه القضايا عن طريق دورات تدريبية بالاستعانة بخبراء مشهود لهم في هذا المجال.

د-على الأسرة والمدرسة والمسجد والمؤسسات الأكاديمية القيام بدورها التوعوي المنوط بها في هذا المجال، لأن استخدام الأنترنت لم يعد حكرا على طائفة معينة، بل الكل معني في العملية فكل المعاملات أصبحت الكترونية.

ه-تخصيص غرف على مستوى المحاكم والمجالس القضائية للفصل في مثل هذا النوع من المنازعات.

و-استحداث جهاز شرطة الجرائم السيبرانية.

ز-ضرورة التعاون الدولي لمواجهة الجرائم السيبرانية سواء في مجال التحقيق أو تسليم المجرمين أو التدريب والتأهيل.

توثيق الهوامش والمراجع:

قائمة المراجع:

أولا: المراجع باللغة العربية

أ-الكتب:

1-الجريدلي، جمال زكي، (2008)، البيع الالكتروني للسلع المقلدة عبر شبكة الأنترنت، دار الفكر العربي، الإسكندرية.

2-دليل الأمن السيبراني للبلدان النامية، الاتحاد الدولي للاتصالات، ط2007.

3-رستم، هشام محمد، (1999)، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، العدد 2، دبي، الإمارات العربية المتحدة.

4-رصاع، فتيحة، (2011-2012)، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر.

5-صغير، يوسف، (2013)، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر.

6-علي، رشيدي محمد علي محمد عيد، (2009)، الحماية الجنائية للمعلومة على شبكة الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة.

7-العريان، محمد علي، (2004)، الجرائم المعلوماتية، دار الجامعة الجديد للنشر الناشف، أنطوان، (1999)، الإعلانات والعلامات التجارية بين القانون والاجتهاد، منشورات الحلبي الحقوقية، بيروت.

8-UNODC/CCPCJ/EG.4/2013/2-(2013) فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية

ب-الدوريات والملتقيات

1-بوشعور الغازي، رضية، طويل أحمد، (2017)، التكلفة الاقتصادية والاجتماعية لوسائل الدفع الالكتروني، تحليل التجربة الجزائرية وآفاقها، ورقة مقدمة للمؤتمر الدولي الربع عشر حول "الجرائم الالكترونية، 24، 25 مارس، مركز جيل للبحث العلمي، طرابلس، لبنان.

2-حفوظة، عبد القادر، غرادين، حسام، الجريمة الالكترونية والية التصدي لها، ورقة مقدمة للملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 29 مارس، الجزائر، مركز جيل للبحث العلمي.

3-الدبور، عمر عبد العزيز موسى، (2017)، آليات تفعيل الحماية والوقاية من الجرائم الالكترونية، (إنشاء ضبطية خاصة بالجرائم الالكترونية)، ورقة مقدمة للمؤتمر الدولي الربع عشر حول "الجرائم الالكترونية، 24، 25 مارس، مركز جيل للبحث العلمي، طرابلس، لبنان.

4-الطويل، أنور جمعة علي، الحماية المدنية للمستهلك في عملية التسوق الالكتروني في القانون الفلسطيني -دراسة مقارنة-، ورقة مقدمة للمؤتمر الدولي الربع عشر حول "الجرائم الالكترونية، 24، 25 مارس، مركز جيل للبحث العلمي، طرابلس، لبنان.

5-عاقلي، فضيلة، (2017)، الجرائم الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، ورقة مقدمة للمؤتمر الدولي الربع عشر حول "الجرائم الالكترونية، 24، 25 مارس، مركز جيل للبحث العلمي، طرابلس، لبنان.

6-عباوة، نجاة، (2017)، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، العدد 16.

7-عبد الله، ليندة، (2017)، تبييض الأموال عن طريق الاعتماد المستندي الالكتروني، ورقة مقدمة للملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 29 مارس، الجزائر، مركز جيل للبحث العلمي.

8-قواري، سليمان، رحلي، سعاد، دور التربية والتوجيه في الحماية والوقاية من الجرائم الالكترونية، ورقة مقدمة للملتقى الوطني حول اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، 29 مارس، الجزائر، مركز جيل للبحث العلمي.

9-المقصودي، محمد بن أحمد علي، (2017)، الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونيا، المجلة العربية للدراسات الأمنية، المجلد 33، العدد 70. جامعة نايف العربية للعلوم الأمنية.

10- نمديلي، رحيمة، (2017)، خصوصية الجريمة الالكترونية في القانون الجزائري والقانون المقارن، ورقة مقدمة للمؤتمر الدولي الربع عشر حول "الجرائم الالكترونية، 24، 25 مارس، مركز جيل للبحث العلمي، طرابلس، لبنان.

ثانيا: المراجع باللغة الأجنبية

1- Bellimen Yamina. Le droit et la Publicité commerciale, Thèse de doctorat en droit, Université Mentouri Constantine, Faculté de droit et science politiques

2- Chandeb, Rabih, (2012), Le régime juridique du contrat de consommation, Alpha édition .Lebanon

3- Delphine Bazing-Beust,(2015), L'essentiel du droit de la consommation, 1re éd, Lextenso. France.

4- Perez.AntonioF, (2008) Consumer protection in the Americas Asecond ware of american revolutions, The catholic University of America, 5U.ST.THOMASL.T, 698.