جـــامـعـــة الـــشـرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

الإطار القانوني لخدمات الأمن السيبراني
(دراسة مقارنة)

Legal Framework for Cybersecurity Services
(Comparative Study)

إعداد:

حنين جميل أبو حسين

إشراف:

الدكتور مأمون أحمد راشد الحنيطي

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير

في القانون الخاص

قسم القانون الخاص

كلية الحقوق

جامعة الشرق الأوسط

أيار، 2021

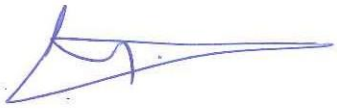
تفويض

أنا **حنين جميل أبو حسين**، أفوّض جامعة الشرق الأوسط بتزويد نسخ من رسالتي ورقيًا وإلكترونيا للمكتبات أو المنظمات أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: حنين جميل أبو حسين.

التاريخ: 31 / 05 / 2021.

التوقيع:



قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها: "**الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة)**".

وأجيزت بتاريخ: 31 / 05 / 2021.

للباحثة: **حنين جميل محمد ابو حسين.**

أعضاء لجنة المناقشة:

الإسم	الصفة	جهة العمل	التوقيع
د. مأمون أحمد الحنيطي	مشرفاً	جامعة الشرق الأوسط	.....
د. ياسين أحمد القضاة	مناقشاً داخلياً ورئيساً	جامعة الشرق الأوسط	.....
د. محمد عبدالمجيد الذنيبات	مناقشاً داخلياً	جامعة الشرق الأوسط	.....
أ.د. أحمد عدنان النعيمات	مناقشاً خارجياً	جامعة البلقاء التطبيقية	.....

شكر وتقدير

الحمد لله رب العالمين أهل المجد والثناء، والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد وعلى آله وصحبه أجمعين.

إنني **أشكر الله العلي القدير أولاً وأخيراً** على توفيقه بإتمام هذه الرسالة، فهو عز وجل أحق بالشكر والثناء وأولى بهما، فالحمد لله الذي وفقني بإنجاز هذا العمل المتواضع فإن أصبت فمن الله وإن أخطأت فمن نفسي، وما توفيقي إلا من الله تعالى

الشكر كل الشكر مقرون بالعرفان والاحترام الدكتور **مأمون أحمد راشد الحنيطي** الذي كان صاحب الفضل الأول بعد الله سبحانه وتعالى، في إنجاز هذه الرسالة وعلى سعة صدره وغزارة علمه.

وإذ أتقدم **لأساتذتي أعضاء لجنة المناقشة** بالشكر، والتقدير لقبول مناقشة الرسالة وتعهدي للأخذ بكل ملاحظاتهم الهادفة إلى تصويبها وإثرائها.

والمقام يتسع لأن أسجل لأهل الفضل فضلهم، وهم هنا **جامعة الشرق الأوسط برئاستها وكوادرها وهيئاتها المشرفة والتدريبية والإدارية.**

والله ولي التوفيق

الباحثة

حنين جميل أبو حسين

الإهداء

إلى **أبي وروح أبي وتراب أبي واسم أبي** .... الذي عرفنا به وكان شهادات نصرنا الأولى ،،،

إلى من **طرزوا بنيران أسلحتهم رايات النصر**، إلى من **حرروا ألفاً ويزيد من الأسر**

إلى **أشاوس القسام** الذين علموا الدنيا كيف يكون، الصبر وكيف يكون النصر

إلى **فلسطين الحبيبة**

الباحثة

حنين جميل أبو حسين

فهرس المحتويات

الموضوع **الصفحة**

الفصل الأول: خلفية الدراسة وأهميتها

الفصل الثاني: ماهية الأمن السيبراني وخدماته

الفصل الثالث: الهيكل التنظيمي لخدمات الأمن السيبراني

الفصل الرابع: التزامات أطراف مقدمي خدمات الأمن السيبراني

الفصل الخامس: الخاتمة، النتائج والتوصيات

قائمة المراجع

الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة)

إعداد: حنين جميل أبو حسين

إشراف: الدكتور مأمون أحمد راشد الحنيطي

الملخّص

هدفت هذه الدراسة إلى التعرف على الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة) ومعرفة مفهوم الفضاء السيبراني وتأثيرها على دول العالم، حيث اعتمدت الدراسة على المنهج الوصفي وتم الاستعانة لغايات الاستدلال، ويعتبر الأمن السيبراني هو مجال متغير باستمرار، مع تطوير التقنيات التي تفتح آفاقاً جديدة للهجمات الإلكترونية، وعلى الرغم من أن الانتهاكات الأمنية الكبيرة هي التي يتم الإعلان عنها فقط، إلا أنه لا يزال يتعين على المؤسسات الصغيرة أن تهتم بالانتهاكات الأمنية، حيث قد تكون غالباً هدفاً للفيروسات والتصيد الاحتيالي.

وقد خلصت الدراسة إلى مجموعة من النتائج كان من أبرزها:

1- ان الأمن السيبراني يقوم على حماية المنظمات والموظفين والأفراد، يجب على المنظمات والخدمات تنفيذ أدوات الأمن السيبراني والتدريب وأساليب إدارة المخاطر وتحديث الأنظمة باستمرار مع تغير التقنيات وتطورها.

2- تبين من الدراسة ان المشرّع الأردني لم يعالج في قانون الأمن السيبراني الأردني المسائل التقنية والفنية لحادث الأمن السيبراني من حيث الطبيعة والاثر والتصنيف. الأمر الذي من شأنه التأثير على ضمان الحماية المقررة أو المرجوة للأمن السيبراني وسلامة الفضاء السيبراني الأردني.

كما أوصت الدراسة بضرورة مُبادرة المشرّع الأردني لإيجاد قواعد قانونية خاصة ناظمة لالتزامات وحالات قيام مسؤولية مقدمي خدمات الأمن السيبراني: الجزائية، والمدنية، وحالات الإعفاء منها. وهو ما سيترك آثاراً إيجابيَّةً ستؤدي إلى زيادة حجم التبادل المعلوماتي الإلكتروني، وستُشجِّع الإقدام على الاستثمار في هذا القطاع الشرياني، فتعم المنفعة على اقتصادنا الوطني، واوصت أيضًا ضرورة أن تسمح التشريعات، في هذا المجال، باللجوء لدعاوى أو لطلبات وقف بثِّ المضمون الإلكتروني غير المشروع، وأن يتمَّ، بدقَّة، تحديد الإجراءات الواجب إتِّباعها لسحبه، أو لمنع وصوله لمستخدمي الشبكة.

الكلمات المفتاحية: الإطار القانوني، المخاطر، الفضاء السيبراني، الجرائم.

Legal framework for cybersecurity services (Comparative Study)

Prepared by: Hanin Jamil Abu Hussein

Supervised by: Dr. Mamoun Ahmed Rashid Al-Hunaity

Abstract

This study aimed to identify the legal framework for cybersecurity services (a comparative study) and to know the concept of cyberspace and its impact on the countries of the world, where the study relied on the descriptive approach and was used for the purposes of inference, and cybersecurity is a constantly changing field, with the development of techniques that open new horizons For cyber-attacks, although only major security breaches are reported, small organizations still have to take care of security breaches, as they can often be the target of viruses and phishing.

The study concluded a set of results, the most prominent of which are:

1- Cyber security is based on the protection of organizations, employees and individuals. Organizations and services must implement cyber security tools, training, risk management methods, and constantly update systems as technologies change and evolve.

2- The study showed that the Jordanian legislator did not deal in the Jordanian cyber security law the technical and technical issues of the cyber security incident in terms of nature, impact and classification. This would affect the guarantee of the planned or desired protection for cyber security and the safety of the Jordanian cyber space.

The study also recommended the necessity of the Jordanian legislator's initiative to find special legal rules regulating the obligations and cases of liability of cybersecurity service providers: criminal and civil, and cases of exemption from them. This will leave positive effects that will lead to an increase in the volume of electronic information exchange, and will encourage investment in this arterial sector, thus benefiting our national economy. It also recommended that legislation, in this field, allow recourse to lawsuits or requests to stop the transmission of illegal electronic content, and that the procedures to be followed to withdraw it or to prevent its access to network users should be precisely defined.

Keywords: Legal Framework, Risks, Cyberspace, Crimes.

الفصل الأول
خلفية الدراسة وأهميتها

المقدمة

يعتبر الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيداً عن تحققه، سواء أكان ذلك، على المستوى التقني، أم على المستوى القانوني. وقد تحول الأمن، مع بروز مجتمع المعلومات، والفضاء السيبراني، إلى واحد من قطاع الخدمات، التي تشكل قيمة مضافة، ودعامة أساسية، لأنشطة الحكومات والأفراد، على السواء، كما هو الحال، مع التطبيقات الخاصة بالحكومة الإلكترونية، والصحة الإلكترونية، والتعليم عن بعد، والاستعلام، والتجارة الإلكترونية، وغيرها الكثير. إلا ان الوجوه المتعددة للأمن السيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الاساءة إلى الأفراد، والمؤسسات، بل تتعداها إلى تعريض سلامة الدول والحكومات، تزيد مهمة القيمين على الموضوع تعقيداً وصعوبة، وتستدعي مقاربة، شاملة، ومتكاملة، لجميع التحديات، التي يطرحها الفضاء السيبراني، بحيث تأتي الردود، والحلول المقترحة، ناجعة وفاعلة. فتحقيق الأمن، وبناء الثقة في الفضاء السيبيري، من أساسيات تسخير تقنيات المعلومات والاتصالات، في مجالات التنمية خدمة للمجتمعات الانسانية، على ما جاء في التوصيات الصادرة عن القمة العالمية لمجتمع المعلومات ومع مرور الوقت وتشابك العلاقات على الواقع السيبراني { والذي لا يجب أن نسميه افتراضياً لكونه واقع يؤثر فينا ونتأثر به ونؤثر فيه ولكنه واقع سيبراني ذا دلالة خاصة يمكن قياسها وتحديد أبعادها } ومن خلال ذلك التشابك السيبراني بأشكاله المختلفة من تواصل اجتماعي بمختلف شبكاته وأشكاله ومن خلال عرض وتداول المعلومات وكيفية الوصول اليها ومن خلال العلاقات الاقتصادية بين الأفراد والشركات والدول بدأت تزيد الخلافات

والانزعة بين تلك الاطراف المتباينة الوجود في عدد من اقاليم الدولة الواحدة أو بين عدة دول مما دعا إلى الحاجة إلى وجود إطار قانوني ينظم تلك العلاقات وتدخل تشريعي ينهي وجود هذه الانزعة.

الأمر الذي دعا الأمم المتحدة إلى تخصيص أحد أفرقتها العاملة لهذا الأمر وتسابقت الدول في حماية فضائها السيبراني من تعديات الآخرين لما في ذلك من خطورة قصوى قد تؤدي للانهيار الاقتصادي كما حدث في عدد من الدول بسبب عمليات القرصنة المنظمة على بنيتها السيبرانية أو الانهيار الأمني بمعناه السياسي كما حدث في مصر من خلال شبكات التواصل الاجتماعي فيسبوك وتويتر مما أدى لانهيار نظام الحكم القائم واستبداله بآخر كما يمكن ان تؤدي تلك التداعيات إلى انهيار أخلاقي واجتماعي تواجهه العديد من الدول بسياسات الحجب والمنع للمواقع الإباحية والجنسية وبعض شبكات التواصل الاجتماعي.

تنبهت جامعة الدول العربية وهي المظلة الحامية والأم الرؤوم لأمن وسلامة الفضاء السيبراني في وقت مبكر دعاها إلى إقامة العديد من الاجتماعات وصدور التوصيات التي تم الأخذ بها في العديد من الدول العربية وإصدار القوانين الاسترشادية المتعلقة بالموضوع سواء في مجال الملكية الفكرية أو استخدام التقنيات الحديثة في الاثبات " الاثبات الإلكتروني " وفي التجارة الإلكترونية ولم ينته ذلك المجهود وما زال حتى اجتماعنا هذا.

وتوفر البيئة السيبرانية أرضية لأنشطة اقتصادية مهمة وأداة ضرورية للقيام بجميع المعاملات التجارية على المستوى الدولي توفر للإنسان في كل زمان ومكان [1]. لا تقتصر منطقة

(1) الحربي، عبدالرحمن حراب (2008) الوقاية من الاحتيال المنظم وتجريمه، ص9، www.almoslim.net/node/16321، تم الحصول على المعلومات بتاريخ: 2014/11/24.

المستخدمين على الحدود المادية لمنزل وحتى حدود بلد ما، وبمستوى تكلفة منخفضة، يمكن لأي مستخدم مقابلة أشخاص حول العالم والتعامل مع المعلومات، دون معرفة هوية المكان الحقيقي للأشخاص. [1]

لذلك، لا بد من التوقف بداية، عند ماهية الأمن السيبراني، والأخطار السيبرانية، لنستعرض بعدها أبعاد هذا الأمن، وما يرتبط به من تحديات، مع التركيز على الإطارين التشريعي والتنظيمي في العالم العربي، والصعوبات الاكثر بروزا، لنصل إلى أساسيات المواجهة، والمقترحات.

وعلى الرغم من المخاطر المتزايدة التي تشكلها الهجمات الإلكترونية، فإن التداعيات القانونية، وعلى وجه التحديد، لا تزال المسؤولية المدنية الناتجة عن مثل هذه الهجمات غير واضحة وتثير قضايا قانونية معقدة، خاصة بسبب تنوع عمليات إعادة تنظيم المسؤولية القابلة للتطبيق (والتي تشمل البيانات الشخصية ولوائح مسؤولية المنتج). وبالتالي، قد يكون هناك ما يبرر اتخاذ إجراء تشريعي بشأن هذه المسألة في وقت ما في المستقبل، لذلك تأتي هذه الدراسة للتعرف على الإطار القانوني الخدمات الأمن السيبراني.

مشكلة الدراسة

تتمثل مشكلة الدراسة معرفة آثار الإطار القانوني لخدمات الأمن السيبراني وذلك يرجع للوضع الذي نعيشه حالياً يسمى "فلات لايت"، هو إحدى مصطلحات الملاحة الجوية والذي يشير للمناطق التي تبدو منها جميع الاتجاهات متشابهة، وهذا وضعنا حالياً، فنحن لا نعرف ما يجب القيام به

(1) Clasessens, J., Dem,V., De Cock and Van de walle, J. (2002) on the Security of Today's Online Electronic Banking System, Computer and Security. 253-265.

من أجل الحد من مشاكل الأمن السيبراني والحفاظ على أمن معلوماتنا وبيان الالتزامات القانونية والعلاقات بين أطراف خدمات الأمن السيبراني.

أهداف الدراسة

تهدف هذه الدراسة إلى ما يلي:

1- بيان ماهية الأمن السيبراني.

2- بيان ماهية الخدمات للأمن السيبراني.

3- بيان الهيكل التنظيمي لخدمات الأمن السيبراني.

4- بيان الطبيعة القانونية لخدمات الأمن السيبراني.

5- بيان التزامات أطراف الأمن السيبراني.

أهمية الدراسة

تتمثل أهمية الدراسة في بيان الهيكل التنظيمي لخدمات الأمن السيبراني ومعرفة الطبيعة القانونية لخدمات الأمن السيبراني وماهية الخدمات للأمن السيبراني لمزودي في ظل تطور الخدمات خاصة أن هناك تطوراً في الخدمات التي يقدمها مزود الانترنت في ضوء الأمن السيبراني. ومعرفة التدابير في الأمن السيبراني بناء سياسات وضوابط وأنظمة مثل إنشاء جدران الحماية وبرامج مكافحة الفيروسات والأنظمة.

أسئلة الدراسة

ستقوم الدراسة من الإجابة عن التساؤلات التالية:

1. ماهية الأمن السيبراني؟

2. ماهية الخدمات للأمن السيبراني؟

3. ما هو الهيكل التنظيمي لخدمات الأمن السيبراني؟

4. ما هي الطبيعة القانونية لخدمات الأمن السيبراني؟

5. ما هي الالتزامات أطراف الأمن السيبراني؟

حدود الدراسة

الحدود المكانية:

الحدود المكانية للدراسة محددة بتشريعات المملكة الأردنية الهاشمية مع المقارنة بالتشريعات العربية والغربية.

الحدود الزمانية:

القانون المدني الأردني رقم 43 لسنة 1976 وقانون المعاملات الإلكترونية رقم 15 لسنة 2015 وتعديلاته والقوانين المقارنة بالقانون المصري رقم 120 لسنة 2008 وهي المختصة حصرياً دون غيرها بنظر القضايا المتعلقة بالجرائم السيبرانية، القانون الأردني الخاص بالأمن السيبراني رقم 16 لسنة 2019.

محددات الدراسة

لا توجد أي محددات تمنع من تعميم نتائج هذه الدراسة على المجتمع الأكاديمي والمجتمع القانوني بشكل عام.

مصطلحات الدراسة

قامت الباحثة بتعريف بعض مصطلحات الدراسة من خلال العودة إلى المراجع التي عرفتها، ولتسهل على القارئ فهم هذه المصطلحات.

- **الإطار القانوني:** هو القانون أو التشريع الذي ينص على قوانين الأمن السيبراني أو الفضاء السيبراني من تشريعات وقوانين واتفاقيات دولية تعمل على حماية الأمن السيبراني.

- **الأمن السيبراني:** والذي يعرف أيضًا باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكتروني، وهو ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة.

- **مزودي خدمات الأمن السيبراني:** هم مزودو خدمات الأمن الذي يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية وخاصة الإنترنت، حيث يعمل مختصو الأمن السيبراني على حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والاختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى وشبكة الإنترنت بشكلٍ عام. [1]

الأدب النظري والدراسات السابقة

أولا: الأدب النظري

تتضمن الدراسة وعنوانها عدة فصول:

الفصل الأول: مقدمة عامة للدراسة تعالج خلفية الدراسة وأهميتها نتناول فيها مشكلة الدراسة وأهدافها وأسئلتها ومصطلحات الدراسة انتهاء بمنهجية الدراسة.

الفصل الثاني: ماهية الأمن السيبراني وخدماته.

الفصل الثالث: الهيكل التنظيمي لخدمات الأمن السيبراني.

الفصل الرابع: التزامات أطراف خدمات الأمن السيبراني.

الفصل الخامس: الخاتمة والنتائج والتوصيات.

(1) Clasessens, J., Dem, V., De Cock and Van de walle, J. (2002) on the Security of Today's Online Electronic Banking System, Computer and Security. 253-265.

ثانيا: الدراسات السابقة

دراسة الشهري، علي (2019) [1]. الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية.

هدفت هذه الدراسة إلى الوقوف الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، والتعرف على طبيعة الجرائم الإلكترونية وأسبابها، والاستبصار للمهددات والمخاطر التي تعترض الأمن السيبراني في المملكة العربية السعودية للوصول إلى الإطار القانوني التي تحد من الجرائم الإلكترونية وتعزز الأمن السيبراني. منهج الدراسة وأدواتها: استخدم الباحث في هذه الدراسة المنهج الوصفي واستخدم أداة الاستبانة لجمع البيانات واستخدم أيضًا أداة S.W.O.Tللتحليل الرباعي للإطار القانوني. أهم النتائج: 1. تبين أن الجرائم الإلكترونية لا تعترف بأي حدود زمانية أو مكانية وهذه الخاصية تمثل أهم السمات المميزة لطبيعة الجرائم الإلكترونية. 2. تبين أن التقنيات الحديثة والانترنت وفرت فرصًا غير مسبوقة لانتشار الجرائم الإلكترونية. 3. تبين أن انتهاك السياسات الأمنية الخاصة بالأمن السيبراني تمثل أهم التهديدات التي تواجه الفضاء السيبراني في المملكة العربية السعودية. حيث اوصت الدراسية إلى انفاذ التشريعات والأنظمة في مواجهة الجريمة الإلكترونية من خلال انشاء المزيد من المحاكم المختصة وتفعيل دورها الرقابي والتشريعي.

تتفق هذه الدراسة الحالية مع الدراسة السابقة في أنها اقتصرت على الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني حيث سأقوم الاستفادة منها في الاتفاقيات والقوانين التي

---

(1) الشهري، علي زايد محمد الجبيري، (2019). الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة (دكتوراه)–جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية، تخصص دراسات استراتيجية.

تعمل على المحافظة على الأمن بشكل عام بينما ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

دراسة جبور، منى، (2012). الإطار القانوني للأمن السيبراني والتحديات

هدفت هذه الدراسة إلى بيان الإطار القانوني للأمن السيبراني والتحديات حيث بينت الدراسة العديد من الحكومات العربية، إلى موارد بشرية ومالية، كما إلى ارادة واضحة وحازمة، تساعد على متابعة ما يجري في الفضاء السيبراني، من نشاطات غير شرعية، تنطلق من اراضيها. وفي هذا المجال، لا بد من التشديد، على ضرورة التعاون، بين القطاعين العام والخاص والمجتمع المدني، للتوصل إلى نشر ثقافة احترام القانون في الفضاء السيبراني، وحماية الحقوق والحريات الأساسية.[1]

وتوصلت الدراسة إلى النتائج التالية لابد للقوانين ان تحوي قواعد الملزمة، ورادعة، تطال فيما تطال، ليس فقط إقرار عقوبات وأصول محاكمات وتحقيق خاصة، بل أيضًا، مجموعة من الالتزامات القانونية الخاصة بالأمن، كاعتماد المقاييس والمعايير الدولية، الصادرة عن المنظمات والهيئات الدولية المتخصصة، في كل ما يتعلق بحماية الأنظمة المعلوماتية، والبنى التحتية، والبيانات والمعلومات الحساسة وبينت الدراسة وجود ثغرات تشريعية في الأنظمة القانونية العربية، لجهة المواضيع التي تتصل بتحقيق الأمن والثقة في الفضاء السيبراني. حيث أوصى الباحث اتخاذ تدابير تعتمد الأمن كعنصر ضروري في الانتاج، لا سيما ما يخص البرامج والأجهزة المستخدمة

(1) جبور، منى الأشقر (2012). الإطار القانوني للامن السيبراني والتحديات، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت 27 – 28 أغسطس (آب) 2012

في تقنيات الاتصال. وضع إطار تعاون، يضمن تبادل المعلومات، ونقل الممارسات الفضلى، في المجال الأمني.

تتفق هذه الدراسة الحالية مع الدراسة السابقة في أنها اقتصرت على الالتزامات القانونية الخاصة بالأمن وتتصل بتحقيق الأمن والثقة في الفضاء السيبراني بينما ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

دراسة فرح، أحمد قاسم (2007)" النظام القانوني لمقدمي خدمات الإنترنت

هدفت هذه الدراسة إلى بيان مُنذ بدايات ظهور الإنترنت، ثار الجدل حول المركز القانوني لمقدمي الخدمات، ودورهم في الوصول الأمثل لاستخدام الشبكة. وتذرَّع مقدمو الخدمات كثيراً من أجل التخفيف من الالتزامات التي ألقاها القضاء، في بداياته، على عاتقهم، وضغطوا، في نفس الوقت، لإرساء نظامٍ خاصٍّ يُعفيهم من المسؤولية، سواء عن إخلالهم بتقديم الخدمة أو عن عدم مشروعيَّة المضمون المعلوماتي المتداول عبر أجهزتهم، الأمر الذي أثار الكثير من الإشكاليات القانونية والفنية. تدخَّلت التشريعات المعاصرة، كالتشريعين الأُوروبي والفرنسي، لحسم الجدل، ولوضعِ نظامٍ قانونيٍّ خاصٍّ بمقدمي خدمات الإنترنت، فحدَّدت، من خلاله بدقَّة، الالتزامات الملقاة على عاتقهم، والأحكام الخاصة بمسؤوليتهم عمَّا يحدث من مخالفات عبر الشبكة. [1]

قوانين بعض الدول، كالقانون الأردني، لم تُرسِ بعد مثل هذا النظام، فثار التساؤل الهام حول مدى جدوى أعمال القواعد العامة، لإيجاد حلول متوازنة تتفق مع الطبيعة الخاصة لآلية عمل مقدمي خدمات الإنترنت.

---

(1) فرح، أحمد قاسم (2007) النظام القانوني لمقدمي خدمات الإنترنت–دراسة تحليليَّة مقارنة –قسم الدراسات القانونية، كلية الدراسات الفقهية والقانونية، جامعة آل البيت.

تتفق هذه الدراسة الحالية مع الدراسة السابقة في أنها اقتصرت على خدمات الانترنت بينما تناولت ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

دراسة ابو الهيجاء، الخصاونة (2009)" المسؤولية التقصيرية لمزودي خدمات الانترنت عن المحتة الغير مشروع –" [1]

هدفت الدراسة ان ظهور الحاسوب ووسائل الاتصال الحديثة، والانترنت إلى حدوث تطور تكنولوجي هائل في جميع جوانب الحياة إلا أن ذلك لم يخلو من بعض المصاعب التي نتجت عن إساءة استخدام البعض لشبكة الانترنت لبث ونشر معلومات غير مشروعية ومضرة بالغير لذلك يثار التساؤل حول مدى إمكانية إقامة المسؤولية عن هذه المعلومات وهل يمكن مساءلة مزودي الانترنت عن ذلك وما هو الأساس الذي يمكن ان تستند إليه مسؤوليتهم كما يثور التساؤل حول المعيار الذي يضبط حالات المسؤولية على شبكة الانترنت كل ذلك من أجل التعرف على الشروط التي تقوم بموجبها مسؤولية مزودي الانترنت وآثار هذه المسؤولية.

تتفق هذه الدراسة الحالية مع الدراسة السابقة في أنها اقتصرت المسؤولية التقصيرية لمزودي الانترنت بينما تناولت ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

---

(1) ابو الهيجاء، محمد، الخصاونة، علاء (2009) المسؤولية التقصيرية لمزودي خدمات الانترنت عن المحتة الغير مشروع. جامعة اليرموك.

الدراسات الأجنبية:

EVELYNE, JACQUES (2020) REGULATING CYBERSECURITY What civil liability in case of cyber-attacks [(1)]

هدفت هذه الدراسة إلى تنظيم الأمن السيبراني ما هي المسؤولية المدنية في حالة الهجمات السيبرانية وبنت الدراسة قضايا الأمن السيبراني والهجمات الإلكترونية التي وصلت بشكل نشط إلى صدارة جدول أعمال الشركات والحكومات على حد سواء بسبب الموجات العالمية الأخيرة من الهجمات الإلكترونية الشديدة. ولم تعد الهجمات الإلكترونية فقط عبر الإنترنت محتملة ومخاطر أو تهديدات مستقبلية ولكن أحداث حقيقية جدًا تؤثر على كل من الشركات والأفراد نتيجة لتزايد مجتمعنا والاعتماد على تكنولوجيا المعلومات والاتصالات خاصة فيما يتعلق بالأعمال التجارية مما يؤدي مشاكل تقع على عاتق المسؤولية المدنية لمثل هذه الحالات، وتوصلت الدراسة إلى المشاكل المسؤولية المدنية لمزودي الأمن السيبراني ولكن لم يوجد قانون صريح يمكن اللجوء له في حل مثل هذه المشكلة.

وتتفق هذه الدراسة مع الدراسة الحالية على أنها تناولت تنظيم الأمن السيبراني ما هي المسؤولية المدنية في حالة الهجمات السيبرانية أما الدراسة الحالية بينما تناولت ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

On June 21, (2018) over 130 participants attended the Geneva Cybersecurity Law & Policy [(2)]

هدف هذا المؤتمر إلى توضيح: ما هي المسؤولية المدنية عن الهجمات الإلكترونية ؟، المنعقد في إطار بحث مشروع بين جامعة جنيف والجامعة العبرية في القدس. هذا المؤتمر يهدف إلى

(1) EVELYNE, JACQUES (2020) REGULATING CYBERSECURITY What civil liability in case of cyber-attacks.

(2) On June 21, (2018) over 130 participants attended the Geneva Cybersecurity Law & Policy.

عرض الجوانب القانونية والسياساتية المختارة للأمن السيبراني في نهج شامل. شارك في تنظيمه البروفيسور ونائب الجامعة جاك دي ويرا ويانيف بنهامو من كلية الحقوق بجامعة جنيف، وكذلك أ.د Guy Pessach .والدكتور Tamar Berenblum من مركز أبحاث الأمن السيبراني في الجامعة العبرية في القدس.

افتتح المؤتمر ببعض الملاحظات التمهيدية الذي أشار إلى أن جنيف هي واحدة من عواصم الأمن السيبراني والتكنولوجيا الرقمية، مما يجعلها المكان المثالي لعقد المؤتمر. بالإضافة إلى ذلك، فإن كانت كانتون قد نشرت للتو، قبل يوم من المؤتمر، سياستها الجديدة بشأن الاقتصاد الرقمي الذي يتضمن أحكامًا بشأن الأمن السيبراني. وشدد على أهمية الاستثمار في التدريس والبحث حول هذا الموضوع سريع التغير وإنشاء منصة مناقشة السماح للخبراء التقنيين وواضعي السياسات بالعمل معًا. وذلك يدل على ان جميع الدول تعامي من مشكلة مزودي الأمن السيبراني والمسؤولية المدنية التي تقع عليه.

وتتفق هذه الدراسة مع الدراسة الحالية على أنها تناولت المسؤولية المدنية عن الهجمات الإلكترونية. بينما تناولت ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

By Wayne M. Alder (2018). **Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend A Claim** [(1)]

بينت هذه الدراسة بأن العالم اليوم، انه لا أحد في مأمن من خطر اختراق البيانات. لا يكاد يمر أسبوع عندما يكون الخبر بشكل عام عن شركة أو كيان حكومي يعاني من خسارة فادحة في الممتلكات الخاصة والمتميزة البيانات الشخصية السرية. وهذه الخسائر لا تحدث فقط للأشخاص

(1) By Wayne M. Alder (2018) Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend A Claim.

غير المتمرسين، ولكن للشركات الكبرى والمنظمات. في العالم، حيث عانى مكتب إدارة شؤون الموظفين التابع للحكومة الفيدرالية من أخرق البيانات الذي كشف البيانات الشخصية لما لا يقل عن 4 ملايين موظف اتحادي حالي وسابق خسارة من المعلومات من Sony Pictures و Target والعديد من الآخرين يسلطون الضوء على أنه لا توجد منظمة محصنة لاحظت وزارة الدفاع الأمريكية أن في العام ذاته، مقدار الملكية الفكرية أكبر من تلك الموجودة في مكتبة الكونجرس تمت سرقتها من الشبكات التي تحتفظ بها الشركات والجامعات الأمريكية والإدارات والوكالات الحكومية " بالنسبة لأي شخص يقوم بأعمال تجارية اليوم، فهم أساس الإمكانات المسؤولية – القانونية والمدنية – عن مثل هذه الخسائر من المعلومات الضرورية، ليس فقط للحد من المسؤولية أو للحفاظ على تنظيم الأخبار، ولكن لحماية الاختراق الأمني.

وتتفق هذه الدراسة مع الدراسة الحالية على أنها تناولت خلاق المعلومات والبيانات. بينما تناولت ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

(Zhang, 2013) **Audit Committee Quality، Auditor Independence، and Internal Control Weakness** "Journal of Accounting and Public Policy", Volume 26, Issue 3, p: 300 – 327. (1)

هدفت هذه الدراسة بيان طبيعة العلاقة بين جودة لجنة التدقيق وضعف نظام الرقابة الداخلية، واستقلالية المراجع بعد صدور قانون (Sarbances Oxly). وقد تكونت عينة الدراسة من (208) شركات تعاني من تحريفات مادية في نظام الرقابة الداخلية في سنغافورة. وقد تناولت الدراسة تعريف المتغيرات، ثم إجراء مقارنة بين مجموعة من الشركات التي تعاني من ضعف في الرقابة الداخلية على أساس القطاع الصناعي الذي تنتمي إليه الشركة، وحجمها، ومستوى أدائها مع

(1) Zhang Y. (2013) "Audit Committee Quality, Auditor Independence, and Internal Control Weakness, "Journal of Accounting and Public Policy", Volume 26, Issue 3, p: 300 – 327.

مجموعة أخرى لا تعاني من ضعف في الرقابة الداخلية، وتوصلت الدراسة إلى عدد من النتائج من أبرزها: وجود علاقة بين جودة التدقيق، وضعف نظام الرقابة الداخلية، واستقلالية المدقق، إذ أن الشركة تعاني من ضعف الرقابة الداخلية.

وتتفق هذه الدراسة مع الدراسة الحالية على أنها تناولت الرقابة على عمليات غسل الأموال في مجال الصرافة الإلكترونية. بينما تناولت ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

Oqab (2012). **The Role of the Audit Committee in Raising the Efficiency of the Internal Control System to Combat Money Laundering in Jordanian Banks**,[(1)] "Journal of Accounting and Public Policy", Volume 26, Issue 3, p: 300 – 327

هدفت هذه الدراسة بيان دور لجان التدقيق في مكافحة عمليات غسل الأموال وذلك من خلال مهامها الموكلة إليها وتقييم النظم الرقابية الداخلية لمكافحة عملية غسل الأموال، بالإضافة إلى وضع آلية مناسبة من آجل التأكد من التزام المصارف بتطبيق التعليمات الخاصة غسل الأموال، استخدم المنهج الاستقرائي وذلك بتجميع المعلومات الخاصة بعناصر الدراسة وتحليلها، كما تم تصميم الدراسة ووزعت على مجتمع الدراسة الذي تألف من البنوك الأردنية والبالغة (13) بنكاً، وبينت النتائج أن لجان التدقيق تساهم بشكل مرتفع في مكافحة عمليات غسل الأموال خلال الأنشطة في تقييم نظام الرقابة الداخلي.

(1) Oqab, R, (2012) The Role of the Audit Committee in Raising the Efficiency of the Internal Control System to Combat Money Laundering in Jordanian Banks. "Journal of Accounting and Public Policy", Volume 26, Issue 3, p: 300 – 327.

وتتفق هذه الدراسة مع الدراسة الحالية على أنها تناولت الرقابة على عمليات غسل الأموال في مجال الصرافة الإلكترونية. بينما تناولت ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

Arthur J. Wylene (2012). **PRESENTED AT THE TWENTY THIRD ANNUAL NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE** [(1)]

بينت هذه المقالة لمحة عامة عن التعرض المحتمل للمسؤولية المدنية التي يواجهها أي فرد أو شركة أو وكالة حكومية لاستخدامها أو عدم استخدامها أمن نظم المعلومات. حيث تم تضمين تحليل المسؤولية الناشئة عن مطالبات الفشل في حماية المعلومات الحساسة بشكل كاف في رعاية المرء، والفشل في منع النظام الخاضع لسيطرة الفرد من استخدامه لتسهيل السلوك الملتوي أو الإجرامي، والمسؤولية الناشئة عن توفير منتجات وخدمات أمنية للآخرين. ويهدف فقط إلى فحص المسؤولية الناتجة عن الوصول غير المصرح به إلى نظام معلومات. المسؤولية المحتملة الناتجة عن استخدام نظام من قبل المرخص لهم المستخدم، الذي يتصرف في نطاق تفويضه حسب مصدر المسؤولية المحتمل، كل منها مقدم بواسطة توضيح، نمط الحقيقة الافتراضي.

وتتفق هذه المقالة مع الدراسة الحالية على أنها تناولت المسؤولية المدنية لنظم المعلومات. بينما تناولت ستتناول دراستي على الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة.

(1) Arthur J. Wylene (2012) PRESENTED AT THE TWENTY THIRD ANNUAL NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE

منهجية الدراسة

اتبعت الباحثة في هذه الدراسة باستخدام المنهج الوصفي وقانون المعاملات الإلكترونية رقم 15 لسنة 2015 وتعديلاته وقانون الأمن السيبراني رقم (16) لسنة 2019، محاولاً إزالة الغموض الذي اكتنف موضوع المسؤولية المدنية لمزودي خدمات الأمن السيبراني، عمل بتحليل آراء الفقه القانوني بخصوص المسائل المثارة في هذه الدراسة، وكذلك الأحكام القضائية بهذا الخصوص إن وجدت في الأردن والمنهج المقارن مقارنة النصوص التشريعية بين القوانين الوضعية والقانون المقارن.

الفصل الثاني
ماهية الأمن السيبراني وخدماته

تمهيد

الأمن السيبراني أتى من كلمتي (Cyber security)، وكلمة سيبر لاتينية الأصل ومعناها الأمن المعلوماتي فيصبح المقصود بالأمن السيبراني أمن الأمن المعلوماتي وهو تعبير أشمل وأعم من أمن المعلومات .لذا يمكن القول أن الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم إستخدامها لمنع الإستخدام غير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين. [1]

يشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث .لقد أصبح الأمن السيبراني ركزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول لموجهة الحروب الإلكترونية. ولذلك جاء هذا الفصل لتوضيح ماهية الأمن السيبراني حيث تم تقسميه إلى مبحثين:

المبحث الأول: الأمن السيبراني: تعريفاته وأبعاده.
المبحث الثاني: خدمات الأمن السيبراني في الدول والاتفاقيات.

---

(1) خاطر، نوري حمد(2012). حماية المصنفات والمعلومات ذات العلاقة بالحاسوب بقانون حماية حقوق المؤلف، بحث منشور في مجلة المنارة العدد (2) كانون ثاني جامعة آل البيت، المفرق، ص 35.

المبحث الأول
الأمن السيبراني: تعريفاته وأبعاده

جاء هذا المبحث لدراسة مفهوم الأمن السيبراني وأبعاده وتم تقسيمة لمطلبين:

المطلب الأول: يوضح تعريفات الأمن السيبراني.
المطلب الثاني: يقوم بتوضيح أبعاد الأمن السيبراني.

المطلب الأول
تعريفات الأمن السيبراني

يمكن تعريف الأمن السيبراني، بأنه أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت. وعليه؛ فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية، المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقسى وأسوأ الأحوال.

ويرتبط هذا الأمن، ارتباطاً وثيقاً، بأمن المعلومات. فالوصول إلى هذه الأخيرة، أو بثها أو الاطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها، هو ما يقف غالب الأحيان، وراء عمليات الاعتداء على الشبكات، وعلى الإنترنت.[1]

فالاعتماد على المعلومة، حقيقة لا لبس فيها، تفرض اعتماداً أكثر، على الأنظمة الإلكترونية التي تعالجها والحديث عن الأمن، يستدعي تعريف الخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف، أو الثغرات التي تعتريه، ومن ثم الإجراءات المفروض اتخاذها، لدفع الخطر.[2]

---

(1) جبور، منى الاشقر، (2018). السيبرانية، هاجس العصر، جامعة الدول العربية، ص 241.

(2) رستم، هشام محمد خليل (2012). الجوانب الإجرامية للجوانب المعلوماتية، مجلة الأمن والقانون، عدد 2، شرطة دبي.

فالتهديد هو نوع الأعمال العدائية، التي يمكن أن تمارس ضد النظام، بينما نقاط الضعف هي مستوى الانكشاف على هذا التهديد، في سياق معين. والإجراءات التي يفترض اتخاذها، لا يمكن أن تقتصر في أي حال من الأحوال على التقنية، بل أنها تتناول بناء القدرات، والتوعية، والتدريب، ونقل الخبرات، عدا عن مجموعة من القواعد المحددة والواضحة، التي يفترض إتباعها.[1]

فالخطر يتناول أمن الشبكات وأمن الإنترنت، لناحيتين: الأولى، هي البنية التحتية، وما عليها من نقاط دخول وخروج وتخزين، واعتراض للمعلومات. والثانية، عمليات التخريب والتدمير والتعطيل، التي تطاولها، وتطاول الأموال، والأشخاص من خلالها.

ولأن للشبكة العالمية للمعلومات، مواصفات تقنية وفنية خاصة، تؤسس لمخاطر معينة، فإن اتصال الشبكات بها، يعرض هذه الأخيرة للمخاطر عينها. وبذلك، يمكن تصوّر تعرض النظام لاعتداء، يجعله يتوقف عن تأدية الخدمات التي كان يقدمها، أو يجعله يعرض أسرار المؤسسات والأفراد، سواء منها الشخصية أو الصناعية والمهنية، أو بما يؤدي إلى تلف البيانات الحساسة، أو بث معلومات مغلوطة.[2]

وهنا لا بد أن نشير إلى ضرورة التمييز، بين المعلومات وبين التكنولوجيا وأدواتها. فالمعلومة هي ما ينتج عن معالج البيانات والمعطيات بشكل معين، تستخدم فيه التكنولوجيا، سواء للتجميع، أو للوصول، أو للتخزين، والمعالجة.[3]

---

(1) دليل الأمن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات، لعام 2010، ص 314.

(2) الرومي، محمد أمين، (2013). جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، الإسكندرية، ص 7.

(3) الشهري، حسن بن أحمد (1423هـ). قانون دولي موحد لمكافحة الجرائم الإلكترونية، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، تصدر عن جامعة نايف للعلوم الأمنية، العدد 27، العدد 53، رجب 1432هـ.

لذا فإن أولى خطوات تحقيق الأمن، هي مراقبة هذه التكنولوجيا، لا سيما في شقتها الذي يمثل الاتصالات، ومراقبة حركة انتقال المعلومات، بما يضمن إزالة العوائق أمام الوصول إليها، وانسيابها، ويمنع التنصت، سواء من جانب الطرف المنافس، أو من قبل الطرف الذي يسعى إلى الاعتداء. [1]

من هنا ضرورة سعي المؤسسات، كما الأفراد، إلى تحقيق أمن الاتصالات، عبر الحفاظ على سريتها، مع ما يمكن أن يطرحه هذا الأمر من إشكاليات، تتعلق بمكافحة الجرائم، والحفاظ على الأمن. وبهذا المعنى، يكون الأمن، هو عدم السماح باستخدام النظام، إلا فيما هو معد لأجله، وفي الإطار المسموح به.[2]

فالأمن السيبراني، بحسب التعريف المعطى له، في التقرير الصادر عن الاتحاد الدولي للاتصالات، حول "اتجاهات الإصلاح في الاتصالات للعام 2010–2011"، هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين.[3]

وتهدف الحماية، إلى جعل المعتدين يحجمون عن خطتهم، أو إلى منعهم من تحقيقها، وإلى ضمان حد مقبول من الأخطار، وذلك عبر وضع خطة أمن، تتلاءم والمحيط التقني، البشري، التنظيمي، والقانوني.

---

(1) معاشي، سميرة (2011). ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة، الجزائر.

(2) فورة، نائلة عادل، (2014). جرائم الحاسب الإقتصادية (دراسة نظرية وتطبيقية) دار النهضة العربية، القاهرة، ص9.

(3) دليل الأمن السيبراني للبلدان النامية الاتحد الدولي للاتصالات، لعام 2010، ص 421.

إلا أن الأمن بصورة شاملة، وأكيدة، ومضمونه، بعيد المنال. فلكل نظام نقاط ضعف وثغرات خاصة به، جعلت البعض يعتبرون قوة أي نظام، إنما تُقاس بقوة أضعف نقطة فيه. ومما لا شك فيه، أن اهتمامات الأمن، تختلف باختلاف المواد والموارد المعرضة للتهديد. فالمواقع التجارية الخاصة، غير المواقع الحكومية، وهذه الأخيرة، تختلف عن المواقع المالية، والعقارية، كما تختلف عن مواقع التسلية والمقامرة. (1)

تأسيساً على ذلك، يمكن تعريف الأمن السيبراني، انطلاقا من أهدافه، بأنه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار، إلى خسائر دائمة. (2)

في مدلوله العام، يعطى الأمن تعريفات عديدة، تنطلق من الإمكانات العسكرية، مروراً بالحفاظ على استقرار النظام، وصولاً إلى حماية القيم الجوهرية لمجتمع ما. لكن، وبغض النظر عن تقارب أو اختلاف النظرات الفلسفية والسياسية حول الموضوع، فإن الراسخ، هو الخشية التي تبديها معظم الدول حالياً، من تعرض أمنها القومي، نتيجة الاعتداءات السيبرانية، لا سيما وأن تقنيات المعلومات والاتصالات، قد رفعت منسور الخطر، عبر إتاحتها مصادر جديدة، متشعبة ومتعددة، وإمكانات هائلة، لتحقيقه، مقابل انخفاض نسبة المخاطر وإمكانات الانكشاف، في جانب الجهة

(1) By Wayne M. Alder (2018). Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim. P. 114.

(2) حسن، سعيد عبد اللطيف (2017). إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، ط.4، ص 214.

المعتدية. والدليل على ذلك، هو التنسيق المتزايد بين إدارات الأمن والاقتصاد، إضافة إلى الترابط الذي يراه قادة العالم، بين أمن الأمن السيبراني، والاقتصاد والأمن القومي. [3]

ويلامس الأمن السيبراني الأمن القومي، بشكل جد وثيق. فالتقنيات التي وسعت الآفاق، وأثرت الثقافة، وسمحت للثقافة المحلية بالامتداد إلى المجال العالمي، باتت تهدد الهوية الوطنية والقومية، مع تأثر الأجيال الصاعدة بما يصلها وبما تصل إليه عبر الإنترنت، حيث تبدو الهوية وكأنها خاضعة لعملية إعادة تشكيل، من خلال تكنولوجيا المعلومات، وحرص الغالبية العظمى من الناس، على استخدامها في تكوين مجتمعهم الخاص، وبيئتهم المميزة. [1]

فالأمن السيبراني، كأي مجال آخر، فضاء سيبراني يستحضر الناس فيه قيمهم ومصالحهم، واهتماماتهم المختلفة، التي يمكن أن تتأثر وتؤثر. وبتنا نلاحظ، على سبيل المثال، أن بعض مجموعات المصالح الخاصة، تهدد بالحلول كبديل لهوية يندمج تحت مظلتها، مجموعات أكبر من الناس.[2]

وكان بدهاهات، المسؤول السابق عن الأمن الوطني الأميركي، قد اعتبر، أن الإنترنت قد رفعت مستوى الأخطار التي يتعرض لها النظام، بشكل غير مسبوق. وذلك، في إشارة واضحة، إلى التهديدات الجديدة، التي تستهدف الأمن القومي، والتي يمكن أن تتخذ أشكالاً غير متوقعة، وتطاول مجالات أساسية وحيوية. كذلك، أعلن الرئيس الأميركي الحالي، باراك أوباما، أن أمن الأمن السيبراني، يأتي في مقدمة اهتماماته، معتبراً التهديد الآتي من الأمن السيبراني، من أخطر

---

(3) فورة، نائلة عادل، مرجع سابق، ص 32.

(1) EVELYNE, JACQUES (2020) REGULATING CYBERSECURITY What civil liability in case of cyber-attacks p . 231.

(2) حجازي، عبد الفتاح بيومي، (2003). النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى.

المسائل، التي تطرح على المستوى الاقتصادي، كما على مستوى الأمن القومي. وقد ترجم هذا عملياً، بتعيين مسؤول عن أمن الأمن السيبراني، يكون على اتصال وتنسيق دائمين معه، ويكون عضواً في الأمن القومي، وفي المجلس الاقتصادي الوطني.

في هذا الإطار، حددت التوصية الأوروبية الصادرة في العام 2002، الأمن القومي، بأنه: "أمن الدولة، والدفاع، والسلامة العامة ...". وعليه، فالأمن القومي هو جميع الإجراءات القانونية، والإدارية، والعسكرية والأمنية، التي تهدف إلى حماية بلد معين، ضد أي نوع من التهديدات والأخطار، التي يمكن أن تعرض سلامة مواطنيه أو أراضيه، أو سيادته، بما فيها سلامة بنيته الحساسة، وبنية الاتصالات والمعلومات.[1]

أما على المستوى العربي، وبالرغم من غياب تعريف واضح للأمن القومي، إلا أن هنالك محاولة، قامت بها الأمانة العامة لجامعة الدول العربية، بإعدادها دراسة في العام 1992، جاء فيها: إن الأمن القومي، هو قدرة الأمة على الدفاع على أمنها، وحقوقها، وصيانة استقلالها، وسيادتها على أراضيها، وتنمية القدرات والإمكانات العربية، في مختلف المجالات السياسية، والاقتصادية، والثقافية والاجتماعية، مستندة إلى القدرة العسكرية والدبلوماسية، آخذة في الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والإمكانات المتاحة، والمتغيرات الداخلية والاقليمية والدولية، والتي تؤثر على الأمن القومي العربي.[2]

---

(1) دليل الأمن السيبراني للبلدان النامية الاتحد الدولي للاتصالات، لعام 2010، ص 441.

(2) الشهري، علي زايد محمد الجبيري، (2019). الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة (دكتوراه)–جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية، تخصص دراسات استراتيجية.

وهكذا، يبدو واضحاً، أنه من تحول الأنظمة، وتغير أنماط الحروب، وموازين القوى، وتطور مفهوم دور الدولة، اتسع مفهوم الأمن القومي، ليشمل السلامة المادية للمواطنين والوطن، والأمن الاقتصادي، والاجتماعي، والإنساني. [1]

وترى الباحثة على أن الأمن السيبراني يعد أهم القضايا التي تعتمد فيها القيادات العليا في أي دولة على استخدام أساليب التخطيط الاستراتيجي في إدارتها، ورسم سياساتها الداخلية والخارجية، وفقاً لتداخل المصالح التي تربطها بالبيئة الداخلية والإقليمية والدولية، دون إغفال أية تحديات وتهديدات قد تمس المصالح الحيوية للأمن الوطني للدولة، ما يستوجب رسم سياسات وخطط استراتيجية ممنهجة تواجه تلك التحديات، كي يتم تحقيق المكاسب وتفادي أكبر ما يمكن تفاديه من الخسائر.

المطلب الثاني
مجلات الأمن السيبراني

أن الأمن السيبراني يخص جميع المسائل الاقتصادية، والاجتماعية والسياسية، والإنسانية، وذلك انطلاقاً من التعريف المعطى له، على أنه قدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم، بأمان، من جهة أولى، ومن كونه يرتبط ارتباطاً وثيقاً بسلامة مصادر الثروة في العصر الحالي، ونعني بها، البيانات، والمعلومات، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكون حوله الإنتاج، والإبداع، والقدرة على المنافسة، من جهة ثانية.[2] لذا، لا بد من التوقف عند أبعاد الأمن السيبراني، على أن نستعرضها كما يلي:

(1) محمود، عبد الله حسين (2020). سرقة المعلومات المخزنة بالحاسوب _ رسالة دكتوراه، جامعة عين شمس.

(2) شمدين، عفاف (2013): الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات، دمشق، ص 311.

الفرع الأول: الأبعاد العسكرية

تتراكم الأمثلة التي يمكن سوقها، في هذا المجال، لتوضيح الأبعاد العسكرية للأمن السيبراني، وخطورة الهجمات السيبرانية، حيث يمكن إيراد ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وإيران، كمثال على بعض الهجمات والاختراقات، التي ترجمت مادياً، سواء باندلاع صراع مسلح لاحق، كذلك الذي وقع بين روسيا وجورجيا، أو بانقطاع الاتصال بالإنترنت في استونيا، بين الدولة والمواطنين، والتشويش على الإدارات الحكومية.

كذلك، ترد هنا اختراقات أنظمة المنشآت النووية في إيران، وتحقق إمكانات التلاعب بها، مع ما يعنيه ذلك من تهديد للأمن القومي، للدولة المعنية، ومن تعرض السلام الدولي للاهتزاز. في هذا المجال أيضًا، يمكن إيراد الاختراق الذي حصل في البرازيل، والمملكة المتحدة، للبنية التحتية للطاقة، حيث انقطع التيار الكهربائي، ما طال بآثاره السلبية ملايين الأشخاص، والمؤسسات والمصالح.[1]

في هذا السياق، وجه خبراء أميركيون، خطاباً مفتوحاً إلى الرئيس الأميركي، جورج بوش، في أيلول 2007، محذرين إياه، من خطر الهجمات السيبرانية على البنية التحتية الأميركية، التي تضم إلى الدفاع، امدادات الطاقة الكهربائية والمياه والاتصالات السلكية واللاسلكية والخدمات الصحية والنقل والإنترنت.[2]

فإلى جانب سيناريو هجمة سيبرانية على مثال بيرل هاربور، يبقى السيناريو الذي تخيله حمدون توريه حول النتائج الكارثية، التي يمكن أن تتجسد فيها التهديدات، هي أفضل ما يمكن أن

(1) ستيفن إليوت، "Analysis on Defense and Cyberwarfare," *Infosec Island*, 8 July (2010) https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html

(2) قورة، نائلة عادل (2015). جرائم الحاسب الاقتصادية، رسالة دكتوراه منشورة، ط1، دار النهضة العربية، القاهرة.

يعبر عن جدية الأمر وحاجتنا إلى العمل معاً، لتحقيق هذا الأمن، لا سيما وأن كلفة التقاعس وانتظار وقوع الكارثة يجعلان نتائجها أكثر دراماتيكية.

وترى الباحثة على ضرورة وجود إطار قانوني في حماية الأمن السيبراني الذي من خلالها يمكن حماية المواقع العسكرية ولذلك يجب ان يكون هناك قانون صريح في حماية هذه الاماكن التي تعد ذات اهمية كبيرة في الدولة.

الفرع الثاني: الأبعاد الاجتماعية

تسمح طبيعة الإنترنت المفتوحة، عبر المدونات والشبكات الاجتماعية بشكل خاص، لكل مواطن، بأن يعبر عن تطلعاته السياسية، وطموحاته الاجتماعية، بأشكالها كافة. كذلك، تشكل مشاركة جميع شرائح المجتمع ومكوناته، وسيلة لإغناء هذا المجتمع وتطويره، بما تتيحه من فرص للاطلاع على الأفكار، والمعلومات، المختلفة، وبما تكونه من حاجة لدى الجميع، في الحفاظ على استقرار الأمن السيبراني، والمجتمع الذي يرتكز إليه. والمعلوم، إن انفتاح مجتمع ما، على مجتمع آخر، يؤسس لتبادل خبرات، وأفكار، وتكون حاجات جديدة، وآفاق تعاون وتكامل.[1]

يضاف إلى ذلك، ما تقدمه الإنترنت، من إمكانات وقدرات، للمجالات العلمية، والثقافية، والخدماتية، حيث تسمح بالوصول إلى مناطق بعيدة، وإلى فئات محددة، ككبار السن، والمرضى، وغيرهم من ذوي الاحتياجات الخاصة. هذا عدا عن الدور الذي يمكن أن تؤديه، في تبادل المعلومات، في أوقات الأزمات الإنسانية والكوارث، بحيث تتأمن المساعدات، وتوزع بالسرعة المطلوبة. ولا تقف الأبعاد الاجتماعية، عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والإفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها إلى

(1) العنزي، سليمان (2013): وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

صيانة القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات، إضافة إلى العادات والتقاليد، عبر إنشاء المجموعات، التي تهتم بنشر الوعي حول هذه المسائل.[1]

في هذا السياق، يأتي التشديد من قبل المنظمات والهيئات الدولية، على نشر ثقافة الأمن في الأمن السيبراني، وضرورة تعاون المجتمع، بكل مكوناته، على تحقيقه وضمانه. فمما لا شك فيه، أن المخاطر السيبرانية، تطاول المجتمع ككل، سواء، بسبب ارتكاز الخدمات الحيوية، كالطاقة، والنقل، والصحة، والاتصالات، وغيرها، على ما تقدمه تقنيات الاتصالات والمعلومات، من إمكانات، أو عبر ما يضخ من محتوى في الأمن السيبراني. فالمحتويات غير المشروعة، وغير المرغوب بها، ذات تأثير سلبي أكيد، على أخلاقيات مجتمع معين، وعلى ارتفاع نسبة الممارسات الجرمية. أما الأمثلة التي تستاق هنا فكثيرة، ونذكر منها: الإباحية، والترويج للاتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين. وعليه، لا بد من بناء مجتمع مسؤول، ومدرك لمخاطر القضاء السيبراني، قادر على التعامل بحد أدنى من قواعد السلامة، مع إدراك للعواقب القانونية، التي يمكن أن تترتب على بعض التصرفات، التي تمارس في الأمن السيبراني.[2]

وترى الباحثة أن على مزوّدي الأمن السيبراني وضع حماية وقوانين تعمل على حماية المجتمعات من جميع مظاهر الاحتيال ومظاهر الاختراق.

الفرع الثالث: الأبعاد السياسية

تتمثل الأبعاد السياسية للأمن السيبراني، بشكل أساسي، في حق الدولة في حماية نطاقها السياسي، وكيانها، ومصالحها الاقتصادية، التي تعني، حقها وواجبها في السعي إلى تحقيق رفاه

(1) النقروز، علي (2017) جرائم نظم المعلومات، دار السناء للنشر، الأردن، عمان، ص 114.

(2) النقروز، علي، المرجع سابق، ص 120.

شعبها، في وقت تؤثر التقنيات، في موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان المواطن، أن يتحول إلى لاعب أساسي، في اللعبة السياسية. كما أصبح بإمكانه الاطلاع، على خلفيات ومبررات القرارات السياسية، التي تتخذها حكومته، عبر الكم الهائل من المعلومات، التي يمكنه الوصول إليها، أو التي يمكن أن توزع وتنشر على الإنترنت، وبقية الأجهزة التي توصل بها.[1]

بالمقابل، لا يتوانى العاملون في الشأن السياسي، عن الإفادة مما تقدمه هذه التقنيات، للوصول إلى أكبر شريحة ممكنة من المواطنين، والترويج لسياساتهم، في العالم. وغني عن البيان، مدى التأثير الذي يتركه هذا الأمر، بغض النظر عن صحة السياسات، والمبادئ والمواقف، التي يروج لها، فقد استخدم أوباما، مثلاً، الشبكات الاجتماعية بشكل كثيف، خلال حملته الانتخابية. كما تركت التسريبات، لآلاف الوثائق الدبلوماسية السرية، عبر الويكيليكس، أثراً سلبياً على العلاقات بين الدول، وعلى مصداقيتها. [2]

وترى الباحثة ان على الأمن السيبراني وضع الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمان والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية والتنظيم والمستخدمين.

الفرع الرابع: الأبعاد الاقتصادية

يرتبط الأمن السيبراني، ارتباطاً وثيقاً بالاقتصاد، فالتلازم واضح، بين اقتصاد المعرفة، وتوسع استخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة،

---

(1) البشري، محمد أمين (2014): التحقيق في الجرائم المستحدثة، الرياض: جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث

(2) طوالبة، علي (2015). التفتيش الجنائي على نظم الحاسوب والإنترنت، رسالة دكتوراة، جامعة عمان العربية، منشورة، ط1، عالم الكتب الحديث، إربد.

والمخزنة، والمستخدمة، على كل المستويات. كذلك، تتيح تقنيات المعلومات والاتصالات، تعزيز التنمية الاقتصادية لبلدان كثيرة، عبر إفادتها، من فرص الاستخدام، التي تقدمها الشركات الدولية، والشركات الكبرى، التي تبحث عن إدارة كلفة إنتاجها، بأفضل الشروط. إلا أن هذا الواقع المشرق، يطرح مسائل مختلفة، سواء منها ما يتعلق بحماية مقدم الخدمة، والعمل، أو بحماية المستهلك على الإنترنت.[1]

ويضاف إلى ذلك، دخول العالم عصر المال الإلكتروني، ضمن بيئة تقنية متحركة، بعد إطلاق خدمات المحفظة الإلكترونية، إذ تتزايد استثمارات المصارف، والمؤسسات المالية، في مجال المال الرقمي، وتتنافس الشركات، على إصدار تطبيقات، تسمح بآليات دفع أمنة، ويحفظ المال في المحفظة الإلكترونية، وبالإيفاء من خلالها، وباستخدامها كرصيد افتراضي. وقد وضعت بعض الدول تشريعات خاصة بهذا المال. وغنيّ عن القول، ما يمكن أن يثيره هذا الأمر، من صعوبات، وما يتطلبه من تشريعات، للحد من بعض الجرائم الاقتصادية والمالية الخطرة، والعابرة للحدود، كتبييض الأموال، والتهرب من الضريبة.[2]

ويربط المسؤولون عن مقدرات الحكومات، وسياساتها، بين الأمن والنمو الاقتصادي، يشكل واضح. فالأمن السيبراني، يضمن ركوب الجمهور، إلى الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الإقبال عليها، بما يترجم عملياً، بتطوير أسس اقتصاد سليم.[3]

---

(1) انظر أبراهام د. سوفاير وسيمور ي. جودمان، *The Transnational Dimension of Cyber Crime and Terrorism,* 2001 at 14, http://media.hoover.org/documents/0817999825_1.pdf.

(2) السحيباني، عبدالله (2011): كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

(3) حمدي، خالد (2017). الحماية القانونية للكيانات المنطقية (برامج المعلومات)، رسالة دكتوراة، جامعة عين شمس.

ولعل الدليل الأوضح، على هذه القيمة، هو استهداف هذه المعلومات، منذ القديم، سواء من خلال عمليات التجسس الصناعي والعسكري التقليدية، أو من خلال الاعتداء على الملكية الفكرية. هذا عدا عن التأثيرات المالية السلبية، التي يتركها، الاعتداء على أنظمة المعلومات، وتعطيلها، كما سرقة نتائج أبحاث، أو غيرها من معلومات، أو كتفشي الفيروسات، على غرار ما حصل، مع فيروس الحب، والذي انطلق من الفيليبين، في العام 2000. [1]

وترى الباحثة ان على الأمن السيبراني دمج المخاطر الإلكترونية في ثقافات المخاطر الحالية يعني النظر فيها جنبًا إلى جنب مع المخاطر التنظيمية الأوسع.

الفرع الخامس: الأبعاد القانونية

يرتب النشاط الفردي والمؤسساتي والحكومي، في الأمن السيبراني، كما أسلفنا، نتائج قانونية، وموجبات، تستدعي اهتماماً، لجهة إيجاد القواعد الخاصة، بحل النزاعات التي يمكن أن تنشأ عنها. لذا، لا بد من مراعاة بعض التحولات، التي رافقت ظهور مجتمع المعلومات، فإلى الحقوق الأساسية، والحريات الإنسانية المعترف بها، في الدساتير والتشريعات الدولية، أضيفت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، كما توسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات على الإنترنت، كما الحق في حماية ملكية البرامج المعلوماتية.[2]

---

(1) *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain,* United States Government Accountability Office, Sept. 2007, GAO-07-1036, www.gao.gov/new.items/d071036.pdf. In 1997 (hackers attacked the Worcester Airport in the U.S., disabling phone services to the airport tower and shutting down the control system managing the runway lights).

(2) الشهري، فايز بن عبد الله (2011): استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي: دراسة وصفية على عينة من المواقع الأمنية العربية على شبكة الإنترنت، مجلة البحوث الأمنية، الرياض: كلية الملك فهد الأمنية ، مركز الدراسات.

كذلك، برزت موجبات جديدة، ذات انعكاسات اقتصادية، ومنها، على سبيل المثال: موجب الاحتفاظ ببيانات الاتصالات، وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى، لما يعنيه هذا الأمر، من كلفة خاصة بحفظ المحتوى وإدارته. ويبقى أن المحور الأساس، في حماية الأشخاص الطبيعيين والمعنويين، على السواء، تبقى ضرورة حماية البيانات، لا سيما الشخصية والحساسة منها، إضافة إلى حماية الحق في الخصوصية.[1] وذلك يضاف إلى ما يتوقع من تحولات على مستوى سياسات القطاعات الصناعية، والتجارية، على ضوء الحاجة إلى إعادة صياغتها، بما ينسجم مع توسع استخدام الشبكات الاجتماعية، والمسائل القانونية التي لا بد وأن تُثار، على مستوى حماية المستهلك، والخصوصية، والبيانات الشخصية، وحقوق العمال والمستخدمين، والملكية الفكرية. فالسنوات القادمة، لا بد وأن تشهد، تصاعداً في أعداد، الأعمال الجرمية، والممارسات غير القانونية، في الأمن السيبراني، ما يعني عملياً، ازدياد عدد القضايا التي سترفع أمام المحاكم، ما يستدعي، إعداد البيئة التنظيمية والتشريعية، وبناء قدرات هيئات المكافحة والحكم.[2]

ومما لا شك فيه، أن النزاعات القانونية ستطاول: الإعلان الذي يرتكز إلى أطياف مستخدمي الإنترنت، انطلاقاً من اهتماماتهم البحثية، أو المواقع التي يزورونها، والاختراقات، والتسريبات

(1) عطية، أيسر محمد الجرائم، المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، المتلقى العامي، ورقة علمية بعنوان: دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الإلكتروني وطرق مواجهته، كلية العلوم الاستراتيجية، عمان، الأردن.

(2) القهوجي، علي عبد القادر (2013). الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والإنترنت والذي عُقد خلال الفترة من 1-3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية.

للبيانات الشخصية، والمالية، سواء منها المقصودة أو غير المقصودة، ومسؤوليات الجهة التي تملكها، أو تديرها، والحق في تصحيح البيانات الشخصية، ومحوها، وتعديلها. [1]

وترى الباحثة أن على المشرّع وضع الاسس التي تحد من مخاطر الخدمات في القطاعات المالية والقطاعات المصرفية أكثر عرضة للهجمات الأمنية، ويتطلب العمل على الخدمات المصرفية عبر الإنترنت مستوى معينًا من المعرفة بتكنولوجيا المعلومات لأن الكثير من تهديدات أمن الإنترنت لا تزال مستمرة، مما يجبر البنوك على اعتماد تدابير جديدة لحماية عملائها من خلال نشر سياسات أمن المعلومات لضمان تجربة مصرفية عبر الإنترنت أكثر أمانًا.

(1) عوض، محمد محي الدين (2009). مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة.

المبحث الثاني
خدمات الأمن السيبراني

في السنوات الاخيرة اعتمدت المؤسسات بشكل كبير في تسيير أعمالها على تقنية المعلومات وشكلت شبكات الاتصال وسطاً تنساب فيه البيانات وتسكن فيه خزائن المعلومات وبذلك تحتاج هذه الشبكات إلى حماية تصون سلامة محتوياتها وتضمن استمرارية عملها، ونظراً لكثرة الأخطار التي تهدد سلامة البيانات التي تنساب في الشبكات أو البيانات المحتضنة في خزائنها وتعدد الأخطار التي تهدد استقرار تلك الشبكات وأمنها كالإصابة بالفيروسات والبرامج الضارة ومحاولات الاختراق لأغراض سرقة المعلومات أو التخريب أو التعديل والعبث، تأتي أهمية الحماية على مدار الساعة لمكوِّنات شبكات المعلومات المادية والبرمجية بتثبيت أجهزة وبرامج الحماية في بوابات الشبكات المحلية وداخل تلك الشبكات، وإدارة تلك الأجهزة والبرمجيات من الزاوية الأمنية وسد الثغرات أولا بأول لتضييق فرص قراصنة المعلومات والمنافسين والأعداء من التمكن من اختراق أو سرقة أية بيانات من شبكات المعلومات [1].

ومن هنا توجهت العديد من الدول لوضع استراتيجية وطنية شاملة من أجل ضمان أمن المعلومات في الأمن 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 إلى 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

---

(1) الشهري، فايز بن عبد الله (2011): استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي: دراسة وصفية على عينة من المواقع الأمنية العربية على شبكة الإنترنت، مجلة البحوث الأمنية، الرياض: كلية الملك فهد الأمنية، مركز الدراسات.

الاستخدام الغير قانوني للشبكة العنكبوتية ومن أجل حماية نظم المعلومات ووسائل الاتصالات لحماية الوطن والمواطن والمؤسسات من أخطار الأمن السيبراني[1].

ولذلك جاء هذا المبحث لدراسة خدمات الأمن السيبراني وتم تقسيمه لمطلبين:

المطلب الأول: التعاون لتعزيز الأمن وحماية وتطوير البنية الإدارية.
المطلب الثاني: يقوم بتوضيح الأمن وسلامة المعلومات في الأمن السيبراني.

المطلب الأول
التعاون لتعزيز الأمن وحماية وتطوير البنية الإدارية

يشكل ارتباط البنى التحتية الخاصة بتقنيات المعلومات والاتصالات، كما الاعتماد المتزايد عليها من قبل الدول والأفراد والمؤسسات، عاملا محفزا لتصاعد نسبة المخاطر، ما يفرض اتخاذ تدابير واجراءات، تضمن ادارة فاعلة للمخاطر التقنية والسيبرانية، تعتمد على منهجية تتناسب والأبعاد الواسعة لهذا الارتباط، ما ينسحب على البلدان أجمع. فالبلدان النامية، مثلا، لا بد وان تحرص على أمنها السيبيري، ليس فقط لحماية نفسها، بل ودفعا لاستبعادها، عن المجال السيبراني، باعتبارها مصدرا للخطر.[2]

الفرع الأول: التعاون لتعزيز الأمن

في هذا المجال، لا بد من ايجاد الإطار التشريعي والتنظيمي الحاضن، الذي يشجع مبادرات التعاون، اذ ان استمرارية عمل تقنيات المعلومات والاتصالات، وفي مقدمها الانترنت، كما استقرار الأمن السيبراني، يستدعيان سياسات لمعالجة الثغرات الأمنية، ولمواجهة الأخطار والحد من آثار

(1) الشوا، سامي (2009). الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، 25-28.

(2) *Understanding Cybercrime: A Guide for Developing Countries*, at 72, International Telecommunication Union, April 2009, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (hereinafter "Understanding")

الأعمال الجرمية. وبالتالي، لا بد من دعم الجهود الآيلة إلى وضع مقاييس ومعايير دولية، كما لا بد من دعم إقرار الأطر القانونية والتنظيمية، والإفادة من أفضل الممارسات والتجارب الناجحة، التي تعزز الثقة في الأمن السيبراني، وتؤمن بيئة داعمة، لنمو النشاط الاقتصادي، والاجتماعي، في الأمن السيبراني. [1]

وفي هذا الإطار، لا بد من الابتعاد عن السياسات، التي تتعارض وطبيعة عمل الانترنت المفتوحة، وامكاناتها التي تشكل أرضية للإبداع، والنمو الاقتصادي والاجتماعي، بحيث لا تتحول هذه السياسات، إلى أدوات تعيق الانسياب الحر للمعلومات، والوصول اليها، تحت ذريعة تحقيق الأمن والحماية على خط مواز، لا بد لسياسات الأمن أن تعزز المبادرات الفردية، والجماعية، العاملة على تحقيق الأمن والحماية. [2]

فنجاح خطط الحماية والأمن السيبراني، يفرض ترابطا وتكاملا، بين استراتيجيات الأمن وسياساته، كما يفترض، إمكانية وصول الجمهور اليها، ليس فقط على المستوى الوطني، وانما على المستويين، الاقليمي والعالمي أيضًا. كذلك، هنالك حاجة لمشاركة الجميع، في وضع الحلول، بحيث تأتي هذه الأخيرة ناجعة ومؤسسة لتفاهم اجتماعي وسياسي، بما يعزز فرص نجاحها وفعاليتها. كما انه، لا بد لمتخذي القرار، أن يأخذوا مقترحات القطاعات المهنية، والاختصاصيين، والمجتمع المدني، وغيرهم، بعين الاعتبار، لدى صياغة التشريعات، ووضع الأطر التنظيمية. [3]

---

(1) سندالي، عبد الرزاق (2017). التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر 19–20 نيسان، المملكة المغربية.

(2) السراج، عبود (2013). مفهوم جرائم المعلوماتية، واقع وآفاق، بحث مقدم إلى المؤتمر الإقليمي الأول لمكافحة جرائم المعلواتية الذي نظمته الجامعة الأردنية واتحاد المحامين العرب خلال الفترة 18–19 كانون الثاني عام 2013.

(3) Trust in the Information Society: *A Report of the Advisory Board RISEPTIS*, http://www.think-trust.eu/; David-Olivier Jaquet-Chiffelle, ed., *Identity Revolution: Multidisciplinary Perspectives*, FIDIS, May 2009, http://www.fidis.net/resources/identity-revolution/

وترى الباحثة ان استقرار الأمن السيبراني، يستدعيان سياسات لمعالجة الثغرات الأمنية، ولمواجهة الأخطار والحد من آثار الأعمال الجرمية.

الفرع الثاني: تطوير البنية الإدارية

ترتبط الثقة في الأمن السيبراني، بقدرة الاجهزة المعنية، على ضبط الامور، كما ترتبط، بوضوح المسؤوليات، والمرجعيات المعنية، بإقرار الحقوق وحمايتها، وبالقدرة على الردع، والملاحقة لكل عمل جرمي، أو تصرف يعرض استقرار المعاملات، والأمن السيبراني. وتتطلب المكافحة الفاعلة، اجهزة متخصصة، وعناصر تتميز بالكفاءة، والقدرة على الاحاطة، بجوانب كيفية ادارة أنظمة المعلومات، وطرق معالجة البيانات، والحقوق المتصلة بها. [1]

وتعرف البنية التحتية على انها: مجموعة الوسائل والقدرات التي يتم تنسيقها عادة بواسطة منظمة مركزيه للمعلومات بحددها القانون الدولي.

يضاف إلى ذلك، ضرورة وجود مرجعية، تشرف على توثيق الحقوق، وارساء قواعد متينة للثقة في العاملين في مجال معالجة المعلومات، والأنظمة المتصلة بها، كما الحقوق الناشئة عنها، في سجلات خاصة، ذات قيود موثوقة. [2]

وترى الباحثة على ضرورة ايجاد أجهزة إدارية متخصصة، تتولى إعطاء شهادات خاصة للأشخاص الذين يتولون مراقبة المعلومات، وحفظها، ومعالجتها، كما تتولى تسجيلهم في سجلات خاصة، وتلزمهم بقواعد لحماية المعلومات والأنظمة فتشجيع الاستثمار، والابداع، والاختراع، في

(1) السعدي، واثبة (2019). الحماية الجنائية لبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب المنعقد في جامعة اليرموك – إربد بتاريخ 12–14 تموز ، ص 6–7.

(2) البشري، محمد أمين (2014): التحقيق في الجرائم المستحدثة، الرياض: جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث.

اسواق العمل المتصلة بوسائل الاتصالات، يرتكز على تحديد واضح للحقوق والموجبات، كما على آليات محددة، لحماية الحقوق الناشئة عن هذا النشاط، كما كان عليه الحال، مع إقرار قوانين الملكية الفكرية، وحقوق المؤلف، والعلامات التجارية، والسجلات التي تثبت الملكية، في عصر ما قبل الانترنت. وفي ذلك أيضًا، حفاظ على حقوق المستخدمين، لاسيما حقهم في تطبيق القوانين المرعية الإجراء.

الفرع الثالث: تعزيز وحماية الانسياب العالمي الحر للمعلومات

يرتكز اقتصاد الانترنت، كما نموها، بشكل أساسي، على الانسياب الحر للمعلومات. وإذا كانت الدول المختلفة، مدعوة إلى وضع سياسات تعزز هذا الانسياب، وتشجعه، وتدعمه، الا انها في المقابل، مدعوة أيضًا، إلى تامين الإطار القانوني الذي يوفر حماية الحق في الخصوصية، والبيانات الشخصية، والحريات الفردية، وبعض الفئات العمرية، كالأطفال والشباب، والملكية الفكرية. ومن هنا، ضرورة التفاتها إلى الأمن السيبراني، والعمل على ارساء قواعد ثابتة له. ويتصل انسياب المعلومات، بالطبيعة المفتوحة للإنترنت، التي تتكل بدورها، على اعتماد مقاييس ومعايير تقنية عالمية. وترد في هذا الإطار أيضًا، سياسات المنافسة، والسوق المفتوح، والتنوع، والخدمات العابرة للحدود، التي تسمح بتأمين خدمات، بكلفة معقولة، تساهم في اتاحة الإنترنت للجميع. [1]

ترى الباحثة بان الأمن السيبراني هو الإطار القانوني الذي يوفر حماية الحق في الخصوصية، والبيانات الشخصية، والحريات الفردية، وبعض الفئات العمرية، كالأطفال والشباب، والملكية الفكرية.

الفرع الرابع: الحفاظ على الخصوصية

يعتبر الحفاظ على الحق في الخصوصية، من أساسيات تعزيز الثقة، في الأمن السيبراني، والافادة من طاقات تقنيات المعلومات والاتصالات، على المستويات: الاجتماعية، والاقتصادية، والثقافية. فالتحديات الحالية، التي تطرحها وسائل معالجة البيانات وجمعها، واستخدامها، واستثمارها، لا بد وان تكون ذات انعكاسات سلبية، على استخدام الانترنت، ومروحة التقنيات المتصلة بها، سواء تجارياً، أو اجتماعياً، أو حكومياً. ولا بد للإطار التشريعية والتنظيمية، من ان تمكن المستخدمين، من فهم حقيقة ما يجري، من ممارسات تطال بياناتهم الشخصية، والمعلومات التي يضعونها على الانترنت. كما لا بد من تمكينهم، من ممارسة حقوقهم، في ادارتها، بالشكل الذي يطمئنهم إلى إمكانية الحفاظ على خصوصيتهم، وعلى حقوقهم الفكرية، والصناعية والادبية. وفي هذا المجال، يمكن للتشريعات، ان تسترشد بالقواعد الدولية، والمبادئ التي سبق إقرارها، على المستوى العالمي، كجزء من أساسيات المحافظة، على نمو واستقرار، الأمن السيبراني. [1]

ترى الباحثة بأن الأمن السيبراني هو يعمل على الحفاظ على خصوصيتهم، وعلى حقوقهم الفكرية، والصناعية والأدبية الإطار القانوني الذي يوفر حماية الحق في الخصوصية، والبيانات الشخصية، والحريات الفردية، وبعض الفئات العمرية، كالأطفال والشباب، والملكية الفكرية.

المطلب الثاني
الأمن وسلامة المعلومات في الأمن السيبراني

في ظل الثورة الرقمية المعاصرة والتي شكلت ثورة حقيقية في كل مناحي الحياة، وفي ظل التطور الهائل في وسائل الاتصال وأجهزة الاتصالات، وهو تطور حوّل العالم إلى نقطة الصفر

---

(1) كيرون أوهارا، Trust: From Socrates to Spin, Icon Books, Cambridge, 2004 at page 10, http://eprints.ecs.soton.ac.uk/9361/.

وتحولت الكرة الأرضية إلى اصغر من كرة صغيرة بيد مستخدم هذه الوسائل، ويكفي أن نعرف أن مستخدمي وسائل التواصل الاجتماعي (الفيسبوك كأنموذج) بلغ في الفترة الأخيرة ما يتجاوز مليار ونصف مستخدم نشط في الشهور الأخيرة، وتشير الاحصائيات لارتفاع عدد العرب المستخدمين للموقع إلى قرابة 100 مليون مستخدم، ونسبة كبيرة من هذا العدد تستخدم أجهزة الهاتف الجوال الحديثة. [1]

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 (الهاكرز) للأمن الشخصي إلى اختراقات الأجهزة الأمنية، [2] وهذا جعل حياة البشر وخصوصياتهم مخترقة بشكل لا يصدق، وكثرت عمليات الابتزاز والجرائم الإلكترونية من خلال ذلك، فلم يعد يسلم فرد من هذه العمليات القذرة، سواء كان مسئولا أو مواطنا.

ويهدف الأمن السيبراني إلى تعزيز حماية جميع ما يتعلّق بالدولة إلكترونياً وأفراداً لحماية هذه الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وجميع مكوناتها المحيطة بالمجتمع من أجهزة وبرمجيات ومعدات وجميع ما يؤثّر على تقدّم هذه الخدمات، وما تحويه من بيانات، فأصبحت هذه أيضًا من أهم الأولويات المهمة والحيوية لجميع دول العالم لأنهم يريدون أن يحافظوا على بيانات مواطنيهم وحفظ ممتلكاتهم وبياناتهم الإلكترونية، وأخذ كثير من الدول على

---

(1) رستم، هشام (2009). جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، ورقة عمل مقدمة إلى اللجنة العلمية لإعداد التقرير الوطني المصري لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيوط، عدد 17، القاهرة.

(2) الاكلبي، مفلح بن دخيل ومحمد، محمد ادم (1430هـ). دور محتوى مناهج التعليم الثانوي بالمملكة العربية السعودية في مواجهة الإرهاب الفكري والتقني (الواقع والمأمول)، بحث مقدم المؤتمر الوطني الأول للأمن الفكري (المفاهيم والتحديات)، الفترة من 22-25 جمادى الأول 1430هـ، كرسي الأمير نايف بن عبدالعزيز لدراسات الأمن الفكري، جامعة الملك سعود، 1430 هـ.

عاتقها وخاصة الدولة المتقدّمة في الكثير من الاهتمامات والاحتياطات والتعمق في هذا التخصص الذي يمس حياة مواطنيهم، فأنشأوا الكليات والمعاهد ومراكز البحوث حتى يتم معرفة كل شيء يقوم بتوفير الحماية لمواطنيهم ولمجتمعاتهم، ومن أهم ما يدور في هذه التخصص والذي يقدّمه هو: [1]

1- حماية شبكة المعلومات والاتصالات والتي تلعب دوراً كبيراً في تدفق خط سير تدفق البيانات بين المواطنين والدولة ومن طرف إلى طرف آخر، والتي إذا تعرضت إلى تخريب أو تدمير أو اختراق حتماً قد يؤثِّر ويقطع هذه الاتصالات ويتوقف سير العمل وتتوقف الخدمات.

2- حماية شبكة المعلومات من أي هجوم وذلك بمعرفة آخر التقنيات والتكنيكات الموجود في هذا المجال ومن أهمها كشف أهداف رسائل هذا العدو والتعرّف على طبيعة هذا المهاجم وذلك وماذا يريد من خلال معرفة تكنيكاته المستخدمة والأساليب المختلفة لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني مُحكم يمنع هذا الهجوم.

3- تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق أو مهاجم أو عابث أن يدخل بسهوله لهذه البيانات والتطبيقات لأن التشفير أحد أساليب الحماية والتي يصعب فك رموزها.[2]

وكون انجاز هذه المهمة يحتاج للحصول على أفضل الوسائل التكنولوجية، من أجل مقاومة الاختراقات والتخريب، وضرورة الاطلاع على افضل الطرق لحماية الأمن الوطني بشموليته، وحماية البنية المعلوماتية لكل المؤسسات، اضافة لعمليات التدريب والتثقيف والتوعية، فهذا يعني تكاليف عالية لا يمكن لمؤسسات فردية أن تتحملها، فمن هنا كانت ضرورة انشاء الهيئات الوطنية للأمن السيبراني، فمن خلالها يمكن التوجه أيضًا لصناعة وطنية تعزز مفهوم الحماية وتوفر

(1) فرح، أحمد قاسم (2007) النظام القانوني لمقدمي خدمات الإنترنت-دراسة تحليليّة مقارنة -قسم الدراسات القانونية، كلية الدراسات الفقهية والقانونية، جامعة آل البيت.

(2) Arthur J. Wylene (2012). PRESENTED AT THE TWENTY THIRD ANNUAL NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE . pp 12-27.

بالتكاليف المتزايدة لحماية أمن الوطن والمواطن، اضافة لتشريع قوانين تحمي المؤسسات والأفراد من الجرائم الإلكترونية. [1]

ومن الملاحظ للجميع أن الدول أصبحت ترتب أمورها لمواجهة حروب المستقبل التي تعتمد على التخريب والتدمير من خلال الأمن السيبراني، وهذا أصبح جزءً من تكتيك واستراتيجيات الدول المتقدمة، لمواجهة هذه الحروب أو القيام بها، وأصبحت عمليات مقاومة هذه الحروب جزءً لا يتجزأ من استراتيجيات الدفاع لدول كثيرة، وبيّن جوزيف يقول: ((هناك أربع فئات رئيسية للتهديدات السيبرانية للأمن الوطني، وكل منها تحتل فترة زمنية مختلفة وتتطلب (من حيث المبدأ) حلولاً مختلفة: الحرب السيبرانية والتجسس الاقتصادي، وهو ما يرتبط إلى حد كبير بالدول، وفئة الجريمة السيبرانية والإرهاب السيبراني، وهو ما يرتبط في الأغلب بجهات فاعلة غير تابعة لدولة. وتتبع أعلى التكاليف حالياً من التجسس والجرائم، ولكن الفئتين الأخريين ربما تصبحان أعظم تهديداً على مدى العقد المقبل مقارنة بحالهما اليوم. وعلاوة على ذلك، ومع تطور التحالفات والتكتيكات، ربما تتداخل الفئات بشكل متزايد)). [2]

الفرع الأول: التنظيم الإداري لمتابعة شؤون الأمن السيبراني

تنشئ كل دولة مجلساً وطنياً مستقلاً، للسلامة والأمن في الفضاء السيبراني، يشكل المرجع الاعلى، لمسائل السلامة والأمن، في المجال السيبراني، وتكون مهامه: [2]

1- وضع استراتيجية سيبرانية، وسياسات تنفيذها.

---

(1) جوشوا بينل، *NetworkSecurityEdge.com*، "Securing the Smart Grid: The Road Ahead," at 2, 5 فبراير 2010. http://www.networksecurityedge.com/content/securing-smart-grid-road-ahead

(2) جوزيف، جون (2015) التهديدات السيرانية في الأمن الوطني، جامعة هارفارد.

(3) المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية (2018). الإتفاقية العربية لحماية الفضاء السيبراني بين الواقع والطموح.

2- الموافقة على الاستراتيجية والسياسة الموضوعة في كل ادارة حكومية، لتنفيذها.

3- تحديد اولويات الأمن، والمبادرات الوطنية

4- تنسيق الجهود والمبادرات، على المستوى الوطني

5- تحديد الجهات المعنية، المسؤولة عن حفظ الأمن والسلامة، وارساء قواعد الثقة، في الاقتصاد الرقمي

6- تنسيق العلاقات مع القطاع الخاص، لمعالجة مسائل الأمن والسلامة السيبرانية

7- التعاون مع الاجهزة الأمنية المختلفة، مثل: المخابرات، والأمن العام، والأمن الداخلي، والشرطة القضائية، والجهات القضائية المعنية، بهدف وضع معايير واصول ردع وملاحقة وتحقيق موحدة، وإقرار توافق مؤسساتي

8- التعاون مع الهيئات المسؤولة، عن تطبيق القانون، على المستويات الوطنية، والاقليمية والدولية.

9- مراقبة أنظمة المعلومات الحكومية، والبنية التحتية للاتصالات

10- الاشراف على تطوير أنظمة المعلومات، الخاصة بالهوية الرقمية، والهوية الرقمية الموحدة، وادارة الممارسات في هذا المجال، واصدار التوصيات

11- تطوير وتنسيق الجهود الخاصة، ببرامج تأهيل، وتدريب، وبناء قدرات، في مجال الأمن والسلامة في الفضاء السيبراني، والتعاون مع الجهات الوطنية، والاقليمية، والعربية، والدولية المعنية.

للدولة أن تنشئ هيئة وطنية عليا مستقلة، للسلامة والأمن في المجال السيبراني، تضطلع بتنفيذ استراتيجيات وسياسات الأمن والسلامة، وبتنسيق الجهود الوطنية، في هذا المجال، وتتولى هذه السلطة:[1]

1- اتخاذ الخطوات التي تضمن تنفيذ التدابير، التي يحددها ويوصي بها، المجلس الوطني.

2- مراقبة التزام الجهات الحكومية، والخاصة، بما يوصي به المجلس الوطني.

3- الاشراف على أعمال تقييم مستوى السلامة والأمن، وأعمال الخبرة Audit والتدقيق.

4- مساعدة المجلس الوطني، في عملياته التنفيذية.

5- المشاركة في وضع القواعد، واعتماد المعايير والمقاييس الدولية، التي تضمن أمن الأنظمة المعلوماتية والمعلومات، وسلامة الاقتصاد الرقمي، والمصادقة على التوقيع الإلكتروني.

6- مراقبة العقود، التي تبرمها الدولة، مع متعهدي الخدمات، وجميع المستثمرين، في مجال تقنيات المعلومات والاتصالات، الذين يقدمون خدمات، تتعلق باستخدام تقنيات المعلومات والاتصالات.

ترى الباحثة بان السلامة والأمن في الفضاء السيبراني، يشكل المرجع الاعلى، لمسائل السلامة والأمن، في المجال السيبراني، وتكون مهامه في المراقبة والمحافظة على سرية المعاملات. [2]

الفرع الثاني: مراكز الاستجابة لطوارئ الانترنت

للدول العربية الأعضاء، إنشاء مراكز الاستجابة لطوارئ الانترنت، تكون مسؤولة عن مراقبة وحماية البنية التحتية للمعلومات والاتصالات، من الاعتداءات عليها، وتشكيل نقطة اتصال

(1) يونس، عمر محمد (2015). الجرائم الناشئة عن استخدام الانترنت، ط1، دار النهضة العربية، القاهرة.

(2) اليوسف، عبد العزيز (2015). التقنية في الجرائم المستحدثة، بحث ضمن كتاب الظواهر الإجرامية المستحدثة وسبل مواجهتها، منشورات أكاديمية نايف للعلوم الأمنية، لرياض.

وتنسيق وطنية، يمكنها ان تتجاوب ومتطلبات الرد السريع، على الأخطار السيبرانية، على المستويات الوطنية والاقليمية والعربية والدولية وتضمن الدولة:[1]

1- أهلية مراكز الاستجابة لطوارئ الانترنت، على العمل بطريقة احترازية وردعية، وتأمين توزيع المعلومات، حول الطوارئ على الانترنت، في الوقت المناسب، للحماية منها، أو للحد من أضرارها، والقدرة على المساعدة في مواجهة الأخطار، ومعالجة نتائج الاعتداءات بطريقة سريعة وفاعلة.

2- تولي المراكز، انذار المؤسسات والادارات والأفراد، وتحصين أنظمة المعلومات، ومعالجة الحوادث، وتنظيم وتنسيق جهود الرد، على الهجمات والاعتداءات، ومعالجة نقاط الضعف، ومشاكل الابواب الخلفية، ودراستها وتحليلها، واستنباط الحلول الملائمة.[1]

3- تولي المراكز، مهمة الإعلام والاعلان، عن الطوارئ، والمخاطر، والحوادث، وتقديم خدمات الخبرة، والتدقيق في مدى جهوزية الأنظمة، وقدرتها على مواجهة الأخطار، ورد الهجمات والاعتداءات، وتطوير برامج حماية، وتوفير خدمات رصد الهجمات والاعتداءات، ومنع وقوعها.

4- رصد، وتحليل، وتنسيق الجهود، في مواجهة الفيروسات، والبرامج التجسسية والخبيثة، ودراسة المخاطر، وتحليلها، ومتابعة، ومواكبة إعادة الأنظمة المعلوماتية، إلى ما كانت عليه، وتقديم استشارات في مجال الحماية، وأمن الأنظمة، والشبكات والمعلومات.

5- تنظيم حملات توعية، والمصادقة على أعمال الخبرة، والتدقيق، وشهادات الكفاءة، في مجال أمن الاتصالات.

---

(1) يوسف، أمير فرج (2011). الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، ط1، مكتبة الوفاء.

(2) جبور، منى الاشقر، مرجع سابق، ص 334.

ترى الباحثة بان مسؤولية مراكز الاستجابة لطوارئ تعمل على مراقبة وحماية البنية التحتية للمعلومات والاتصالات، من الاعتداءات عليها، وتشكيل نقطة اتصال وتنسيق وطنية، يمكنها أن تتجاوب ومتطلبات الرد السريع، على الأخطار السيبرانية.

الفرع الثالث: الإطار التشريعي لحماية الأمن السيبراني

تتعهد كل دولة متعاقدة، إقرار اطر تشريعية وتنظيمية، استنادا إلى النصوص الدولية، والاتفاقيات، وبروتوكولات التعاون، الصادرة حول حماية الفضاء السيبراني، المتعلّقة بمكافحة الجريمة السيبرانية، والتعاون في الجرائم العابرة للحدود، والمقاييس والمعايير الدولية، المفروض اعتمادها، في حماية البنية التحتية للاتصالات، وأنظمة المعلومات.[1]

تلتزم الدول الأعضاء، إقرار التشريعات الملائمة لتشجيع الانخراط السليم والأمن، في مجتمع المعلومات، والاستفادة من آفاق مجتمع المعرفة، بما يخدم النمو والتنمية، لاسيما فيما يتعلق ب:[2]

1- تنظيم التجارة الإلكترونية.

2- حماية الخصوصية والحق في التعبير.

3- ضمان الحق في النفاذ إلى الشبكة العالمية للمعلومات.

4- حماية البيانات الشخصية، والبيانات الحساسة.

5- تنظيم المحتوى.

6- حماية حقوق الملكية الفكرية.

7- حماية الاطفال على الانترنت

---

(1) المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية (2018). الثالثة والعشرون من الإتفاقية العربية لحماية الفضاء السيبراني بين الواقع والطموح.

(2) المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية (2018). المادة الثانية والعشرون من الإتفاقية العربية لحماية الفضاء السيبراني.

8- تنظيم المعاملات الإلكترونية.

9- تنظيم المسؤوليات، وخدمات الحوسبة السحابية.

10- إقرار قواعد تجريم موضوعية.

11- وضع اصول ملاحقة، ومتابعة، وتنفيذ، خاصة بالجرائم السيبرانية.

12- إقرار آليات تعاون وطنية، واقليمية، ودولية.

13- إقرار الإطار التشريعي الملائم، للتعاون بين القطاعين العام والخاص، في مواجهة الجرائم السيبرانية.

تتعهد كل دولة متعاقدة، ضمان انسجام الاجراءات والقواعد القانونية التي تتخذها، في مجال مكافحة الجريمة السيبرانية، مع أفضل الممارسات الدولية، المعمول بها في هذا المجال، مع الاخذ بعين الاعتبار، الحد الادنى المعتمد في الدول، التي لديها أدوات تشريعية وتنظيمية، بحيث يكون المجال متاحا، أمام إمكانية تحقيق الانسجام، بين تشريعات الدول الأعضاء. [1]

تعتمد الدول الأعضاء، فيما يتعلق بالجرائم العابرة للحدود، على مبدأ توحيد القواعد القانونية، الخاصة بتجريم الأعمال الخاصة بالجرائم السيبرانية، واصول الملاحقة والتنفيذ الخاصة بها بحيث تعتمد كل دولة القواعد القانونية التي تسمح لها باعتماد مبدأ التجريم المزدوج، وذلك بهدف انجاح التعاون، وتفعيله.[2]

(1) المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية (2018). المادة الثامنة والعشرون من الإتفاقية العربية لحماية الفضاء السيبراني.

(2) المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية (2018). المادة التاسعة والعشرون من الإتفاقية العربية لحماية الفضاء السيبراني.

ترى الباحثة على الدول الأعضاء اتباع القواعد القانونية والتنظيمية، التي تراها ضرورية، وتنسجم مع تشريعاتها الوطنية، لتسهيل عملية تبادل المعلومات، وتشارك البيانات، بشكل سريع وفوري ومتبادل بين الهيئات المتخصصة، وذات الصلاحية في تطبيق القوانين، في الدول الأعضاء.

الفصل الثالث

الهيكل التنظيمي لخدمات الأمن السيبراني

يتطلب لكل خدمات وجود له هيكل وذلك أن خدمات الأمن السيبراني ومعرفة العلاقة بين الأمن السيبراني، والبنية التحتية الحيوية وحماية البنية التحتية الحيوية للمعلومات، والبنية التحتية غير الحيوية.

فإن البنية التحتية الحيوية (CI) ينظر إليها عموماً باعتبارها الأنظمة والخدمات والوظائف الرئيسية التي يؤدي تعطيلها أو تدميرها إلى آثار موهنة على الصحة العامة والسلامة أو التجارة أو الأمن القومي أو على أي مجموعة من هذه الأمور في آن واحد. وتتألف البنية التحتية الحيوية من عناصر مادية (مثل المرافق والمباني) وعناصر افتراضية، (مثل الأنظمة والبيانات) وقد تتباين الطبيعة "الحيوية" من بلد لآخر، لكنها عادة ما تشمل عناصر تكنولوجيا المعلومات والاتصالات، والطاقة، والأعمال المصرفية، والنقل، والصحة العامة، والزراعة، والأغذية، والمياه، والمواد الكيميائية، والملاحة البحرية، وقطاعات الخدمات الحكومية الأساسية.[1]

ولذلك جاء هذا الفصل لتوضيح الهيكل التنظيمي لخدمات الأمن السيبراني، حيث تم تقسميه إلى مبحثين:

المبحث الأول: البنية التحتية للأمن السيبراني في المملكة الأردنية الهاشمية.
المبحث الثاني: البنية التحتية للأمن السيبراني في الدول والاتفاقيات.

(1) النقروز، علي، المرجع سابق، ص 222.

المبحث الأول
البنية التحتية في الأمن السيبراني في المملكة الأردنية الهاشمية

تعتبر حماية البنية التحتية الحيوية للمعلومات (CIIP) مجموعة فرعية من البنية التحتية الحيوية للمعلومات والأمن السيبراني على السواء. ويوفر الأمن السيبراني الحماية من جميع أشكال الحوادث السيبرانية من خلال تعزيز سلامة البنية التحتية الحيوية للمعلومات التي تعتمد عليها القطاعات الحساسة، وتأمين الشبكات والخدمات التي توفر الاحتياجات اليومية للمستعملين. ويمكن للحوادث السيبرانية أن تؤثر على البنية التحتية للمعلومات الحيوية وغير الحيوية، وربما تأخذ أشكالاً كثيرة من أشكال الأنشطة الضارة، مثل استخدام روبوتات النت (botnets) في الهجمات المتعلقة برفض الخدمة ونشر الرسائل الاقتحامية والبرمجيات الضارة (مثل الفيروسات وبرمجيات وورم التخريبية) التي تؤثر في قدرة الشبكات على العمل. وبالإضافة إلى ذلك، قد تشمل الحوادث السيبرانية أنشطة غير مشروعة مثل التصيد الاحتيالي (phishing) والتحايل لسرقة المعلومات الشخصية (pharming)، علاوة على سرقة الهوية. والخطر السيبراني آخذ في الازدياد مع تزايد الأدوات والمنهجيات وتوفرها على نطاق واسع، ومع اتساع نطاق وتطور القدرات التقنية للمجرمين السيبرانيين. وقد تعرضت البلدان على مختلف مراحل تنميتها لهذه المخاطر السيبرانية. [1]

(1) السحيباني، عبدالله (2011): كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية. ص 314.

المطلب الأول

الإطار القانوني والتشريعي لأمن وسلامة الفضاء السيبراني في الأردن

يعد الأمن السيبراني في الأردن حديث العهد نوعاً ما، حيث نظم المشرّع الأردني قانون الأمن السيبراني في الأردن في عام 2019 م. وأتت الإرادة الملكية السامية بالموافقة على قانون الأمن السيبراني في شهر أيلول من نفس العام. فيما صدرت الإرادة الملكية السامية بالموافقة على نظام المركز الوطني للأمن السيبراني في شهر كانون الثاني من عام 2020م. [1]

الأمن السيبراني هو حماية أجهزة الحاسوب وأنظمتها والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة ومن سرقة أو تلف برامجها أو بيانتها الإلكترونية. يُعرف أيضًا باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية أو أمن الحاسوب. ينطبق المصطلح كذلك على مجموعة متنوعة من السياقات من الأعمال إلى الحوسبة المتنقلة. ويمكن تقسيمه إلى عدة فئات مشتركة. [2]

تهتم الأردن كثيراً بالأمن السيبراني؛ بسبب المخاطر المحيطة بهذا القطاع، وقد وضعت أطر قانونية في هذا الشأن؛ فوافق مجلس النواب على إنشاء مجلس ومركز للأمن السيبراني ضمن مشروع قانون الأمن السيبراني لسنة 2019م.

يهدف قانون الأمن السيبراني في الأردن لحماية المملكة من تهديدات حوادث الأمن السيبراني وبناء قدرات وطنية تضمن مواجهة التهديدات التي تعترض أنظمة المعلومات والبنى التحتية.

القانون الأردني

(1) عبابنة، محمد أحمد (2020). جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ط3، ص 231.

(2) المناعسة، أسامة وجلال الزعبي (2020)، و صايل الهواوشة جرائم الحاسب الآلي الانترنت، دراسة تحليلية مقارنة، دار وائل للنشر، عمان، ص 231.

قانون الأمن السيبراني رقم (16) لسنة 2019 والمعني بحماية الأمن السيبراني للمملكة في ... هذا في الأسباب الموجبة التي دعت إلى تقنيين الأمن السيبراني في الأردن، منها: بناء قدرات أمن سيبراني وطني يضمن مواجهة التهديدات التي تعترض أنظمة المعلومات والبنى التحتية الخاصة بها، حماية المملكة من تهديدات حوادث الأمن السيبراني، خلق بيئة أمنة وجاذبة للاستثمار ومحفزة للاقتصاد الوطني خاصة في ظل تسارع التطور في أنظمة المعلومات والبنى التحتية وتنامي حجم الخدمات الحكومية الإلكترونية.[1]

ومراقبة الفضاء السيبراني الوطني وتوثيق حوادث الأمن السيبراني في الأردن، إيجاد جهة مرجعية تتولى تطبيق وتنفيذ السياسات العامة التي تنبثق عن الاستراتيجية الوطنية للأمن السيبراني. وتعمل على تنسيق الجهود الوطنية، رفع مستوى الأمن الوطني العام والشامل للمؤسسات والأفراد وتطوير قدرات ردع ومراقبة وإنذار والاستجابة لحوادث الأمن السيبراني والتخفيف من الأضرار الناجمة عنها[2].

نص قانون الأمن السيبراني في الأردن لسنة 2019م على " تشكيل المجلس الوطني للأمن السيبراني من رئيس يُعين بإرادة ملكية سامية وعدد من الأعضاء يمثلون وزارة الاقتصاد الرقمي والريادة، البنك المركزي الأردني، القوات المسلحة الأردنية – الجيش العربي، دائرة المخابرات العامة، مديرية الأمن العام، المركز الوطني للأمن وإدارة الأزمات، وثلاثة أعضاء يُسميهم مجلس الوزراء، على أن يكون اثنان منهم من ذوي الخبرة من القطاع الخاص[3]."

---

(1) قانون الأمن السيبراني الأردني رقم (16) لسنة 2019.

(2) الشوبكة، محمد أمين (2019) جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ص 231.

(3) عبابنة، محمد أحمد (2020) مرجع سابق، ص 239.

كما نص القانون على إنشاء المركز الوطني للأمن السيبراني والذي يتمتع بشخصية اعتبارية ذات استقلال مالي وإداري.

الفرع الأول: مهام المجلس

بحسب القانون يتولى المجلس مهام: "إقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني، إقرار الخطط والبرامج اللازمة لقيام المركز بمهامه وواجباته بما فيها برامج التعاون الدولي والإقليمي، اعتماد التقارير ربع السنوية عن الوضع الأمني السيبراني للمملكة والتقرير السنوي عن أعمال المركز، تشكيل اللجان التنسيقية من ذوي العلاقة لتمكين المركز من تحقيق اهدافه على ان تحدد في قرار تشكيلها مهامها وواجباتها وكيفية انعقاد اجتماعاتها واتخاذ قراراتها، إقرار الموازنة السنوية للمركز[1].

الفرع الثاني: أهداف المركز ومهامه وصلاحياته

نصت المادة السادسة من القانون على أهداف المركز ومهامه وصلاحياته وجاء في الفقرة أ منها: "يهدف المركز إلى بناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاء وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات[2]."

وجاء في الفقرة ب من نفس المادة أيضًا: "يتولى المركز في سبيل تحقيق اهدافه المهام والصلاحيات التالية: اعداد استراتيجيات وسياسات ومعايير الأمن السيبراني ومراقبة تطبيقها ووضع الخطط والبرامج اللازمة لتنفيذها ورفعها للمجلس لإقرارها، تطوير عمليات الأمن السيبراني وتنفيذها

(1) عبابنة، محمد أحمد (2020). جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ط3، ص 302.

(2) المرجع السابق، ص 304.

وتقديم الدعم والاستشارة اللازمين لبناء فرق عمليات الأمن السيبراني في القطاعين العام والخاص وتنسيق جهود الاستجابة لها والتدخل عند الحاجة، تحديد معايير الأمن السيبراني وضوابطه وتصنيف حوادث الأمن السيبراني بموجب تعليمات يصدرها لهذه الغاية [1]."

ونصت كذلك على: "منح الترخيص لمقدمي خدمات الأمن السيبراني وفقا للمتطلبات والشروط والرسوم المحددة بموجب نظام يصدر لهذه الغاية، تبادل المعلومات وتفعيل التعاون والشراكات وابرام الاتفاقيات ومذكرات التفاهم مع الجهات الوطنية والاقليمية والدولية ذات العلاقة بالأمن السيبراني، تطوير البرامج اللازمة لبناء القدرات والخبرات الوطنية في مجال الأمن السيبراني وتعزيز الوعي به على المستوى الوطني، التعاون والتنسيق مع الجهات ذات العلاقة لتعزيز أمن الفضاء السيبراني، اعداد مشروعات التشريعات ذات العلاقة بالأمن السيبراني بالتعاون مع الجهات المعنية ورفعها للمجلس."

كما جاء في نفس الفقرة: "التقييم المستمر لوضع الأمن السيبراني في المملكة بالتعاون مع الجهات المعنية في القطاعين العام والخاص، تحديد شبكات البنى التحتية الحرجة ومتطلبات استدامتها، إنشاء قاعدة بيانات بالتهديدات السيبرانية، تقييم النواحي الأمنية لخدمات الحكومة الإلكترونية، تقييم وتطوير فرق الاستجابة لحوادث الأمن السيبراني، إعداد سياسة تتضمن معايير أمن وحماية المعلومات، دعم البحث العلمي في مجالات الأمن السيبراني بالتعاون مع الجامعات، إجراء تمارين ومسابقات للأمن السيبراني."

الفرع الثالث: مؤشر الأمن السيبراني

يحتل الأردن المرتبة الثامنة عربيًا والستين عالميًا في مؤشر الأمن السيبراني، وفقًا للتقرير الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة لعام 2019م، حيث يتعرض لحوالي

(1) الشوبكة، محمد أمين (2019) جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ص 321.

مليون هجمة إلكترونية سنوياً، والرقم قابل للزيادة مع التطور التكنولوجي؛ مما يجعل الأمن السيبراني في الأردن حاجة ملحة خصوصاً مع التحول الإلكتروني في الأردن والعالم على حد سواء[1].

المطلب الثاني

التنظيم القانوني لتصنيف حوادث الأمن السيبراني في الأردن

حدد مجلس الوزراء الموقر الأسباب الموجبة لقانون الأمن السيبراني في كتابه المرسل لمجلس الأمن الموقر بتاريخ 17-6-2019، والذي تناول فيه الإطار العام لأسباب التي دعت إلى ضرورة توفري حماية قانونية للأمن السيبراني (والفضاء السيبراني) على الصعيد الوطني. وما يعنينا ويتصل بموضوع الأسباب التالية [2]:

1. حماية المملكة من تهديدات حوادث الأمن السيبراني.

2. رفع مستوى الأمن الوطني العام والشامل للمؤسسات والأفراد وتطوير قدرات ردع ومراقبة وانذار واستجابة حوادث الأمن السيبراني والتخفيف من الاضرار الناجمة عنها.

3. خلق بيئة أمنة وجاذبة لاستثمار ومحفزة الاقتصاد الوطني خاصة في ظل تسارع التطور في أنظمة المعلومات والبنى التحتية وتنامي حجم الخدمات الحكومية.

4. لمراقبة الفضاء السيبراني الوطني ورصده وتوثيق حوادث الأمن السيبراني.

إلا ان المشرّع لم يعالج في قانون الأمن السيبراني الأردني المسائل التقنية والفنية لحادث الأمن السيبراني من حيث الطبيعة والأثر والتصنيف. الأمر الذي من شأنه التأثير على ضمان الحماية

---

(1) المرجع السابق، ص 324.

(2) القطاونة، مصعب (2019). الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدّم لشبكة قانوني الأردن. ص 312.

المقررة أو المرجوة للأمن السيبراني وسلامة الفضاء السيبراني الأردني.[1]

ترى الباحثة هنا للتعرف على طبيعة تصنيف حوادث الأمن السيبراني واتصالها بقطاعات الخدمات العامة والخاصة، واليات التعامل مع التهديد السيبراني وحوادث الأمن السيبراني ومعالجة اثارها وتأثيرها في هذه القطاعات. ليتم ذلك من خلال فرعين الأول: الإطار الفني والتقني والفرع الثاني الإطار القانوني.

الفرع الأول: الإطار الفني والتقني

تصنيف حوادث الأمن السيبراني: [2]

- طبيعة حادث الأمن السيبراني :يستخدم الجزء الأول من التصنيف: لتصنيف طبيعة الحادث (تحديد نوع التهديد الذي أثار الحادث، وشدة هذا التهديد).
- تأثير/ أثر حادث الأمن السيبراني يستخدم الجزء الثاني من التصنيف لتصنيف تأثير الحادث (تأثيره على الخدمات، في قطاع من قطاعات الاقتصاد والمجتمع): القطاعات المتأثرة يتصل دراسة أثر حوادث الأمن السيبراني بتأثيرها على الخدمات التي تقدمها القطاعات العامة – أو إخلاصه –في الفضاء السيبراني. ومن القطاعات الهامة – على سبيل المثال – التي يجب ان تكون محلا للاعتبار لدى النظر في أثر حوادث الأمن السيبراني القطاعات التالية:[3]
- الخدمات المتصلة بالقطاعات السيادية.
- الخدمات العامة.
- الخدمات الحكومية.

---

(1) المرجع السابق، ص 317.

(2) السعدي، واثبة (2019). الحماية الجنائية لبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب المنعقد في جامعة اليرموك – إربد بتاريخ 12–14 تموز 2019، ص 7.

(3) المرجع نفسه.

- الخدمات ذات الطابع الحساس.
- خدمات الثقة وتحديد الهوية.
- الخدمات الرقمية.
- خدمات الاتصالات.

شدة التأثير/الاثر يتم قياس شدة التأثير للتعرف على وتقييم الأثر الناجم عن الحادث في المجتمع والاقتصاد... إلخ. الأمر الذي يتطلب الأخذ في العوامل التي يجب مراعاتها عند تقييم شدة التأثير:

المخاطر على صحة وسلامة السكان، ومثال ذلك:

- التأثير على خدمات الطوارئ.
- التأثير على الاقتصاد والمجتمع، ومثال ذلك: التسبب في خسائر كبيرة.
- الاضرار والتكاليف للمواطنين و/أو المنظمات/المؤسسات /الشركات المتضررة.
- اضطراب الحياة اليومية.[1]
- الآثار المتتالية في القطاعات الحرجة.
- تأثير وسائل الإعلام والتغطية.
- التأثير السياسي والأهمية.

الفرع الثاني: الإطار القانوني أو التشريعي

تكمن الغاية من بيان الإطار الفني والتقني – الفرع الأول– في الاستناد اليها في صياغة ووضع الاحكام والضوابط والمعايير القانونية، والتي تمثل الركيزة والمرجع الاساس للجهات المعنية

(1) السعدي، واثبة (2019). الحماية الجنائية لبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب المنعقد في جامعة اليرموك – إربد بتاريخ 12–14 تموز 2019، ص 7.

في المملكة (المجلس الوطني والمركز الوطني للأمن السيبراني) لضمان حماية الأمن السيبراني الوطني. وبالرجوع إلى ما سبق بيانه، وباستقراء قانو الأمن السيبراني الأردني، نجد ان القانون لم ينظم المسائل التقنية والفنية حادث الأمن السيبراني من حيث الطبيعة والاثر والتصنيف.

إذ ان المشرّع لم يتناول هذه المسائل في القانون، انما اكتفى في المادة (9) بتنظيم إطار عام (غير واضح) بين الاختصاص الهيكلي (الإداري) للمجلس الوطني للأمن السيبراني في تحديد حوادث الأمن السيبراني وصلاحيات المركز الوطني للأمن السيبراني في الاستجابة لها.

وترى الباحثة على ضرورة تحديد معايير قياس مناسبة لتكون المرجع الأساس للجهات المعنية (المجلس والمركز الوطني للأمن السيبراني) لتصنيف حوادث الأمن السيبراني على الصعيد الوطني وفق أسس واضحة لا تدع مجالاً للاجتهاد أو للتجاوز أو التغول أو التشدد، ولتكون مرجعاً واضحاً للأفراد والشركات والمؤسسات وكل معنى في تقديم خدمات أو استخدام الفضاء السيبراني الوطني (بوضوح وشفافية درء لاي غموض أو ضبابية أو المساس بحقوق المستخدمين أو الحد من تلك الحقوق).[1]

(1) السعدي، واثبة (2019). الحماية الجنائية لبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب المنعقد في جامعة اليرموك – إربد بتاريخ 12–14 تموز 2019، ص 22.

المبحث الثاني
البنية التحتية للأمن السيبراني في الدول والاتفاقيات

للأمن السيبراني وجود استراتيجية شاملة تشمل استعراضاً عاماً أولياً لمدى كفاية الممارسات الوطنية الحالية والنظر في دور جميع أصحاب المصلحة (الهيئات الحكومية، والقطاع الخاص، والمواطنين) في هذه العملية. [1]

ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي، تحتاج الحكومات إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية، وتعزيز هذه الحماية وضمانها. فالبنية التحتية للمعلومات في عصرنا الحالي تشمل جميع قطاعات الصناعة في أي بلد كما أنها تتجاوز حدود البلدان. ومن شأن الطابع الشامل للبنية التحتية الحيوية للمعلومات الذي يجعلها موجودة في كل مكان أن يهيئ فرصاً ومزايا اقتصادية هائلة.[2]

على أن هذه المزايا تقترن أيضًا بالكثير من حالات الاعتماد المتبادل والمخاطر المكلفة. ولخَّصت دراسة جرت بتفويض من مكتب تنمية الاتصالات بالاتحاد هذه التكاليف على النحو التالي:[3]

تقتضي التغييرات التي أحدثتها تكنولوجيات المعلومات والاتصالات مزيداً من التركيز على التعاون من جانب الحكومات والأعمال التجارية وغيرهما من المنظمات وفرادى المستعملين الذين يضعون ويملكون ويوردون ويديرون الخدمة، ويستخدمون أنظمة وشبكات المعلومات. وفي حين تواصل الحكومات في كثير من الأحيان الاضطلاع بدور قيادي في أمن الشبكات، فإن مما له

(1) إبراهيم، خالد ممدوح (2019). الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1. ص33.

(2) أحمد، هلالي عبد اللاه (2013). الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة. ص231.

(3) *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain,* United States Government Accountability Office, Sept. 2007 . Pp55-59.

أهميته الحاسمة ضمان إدماج أصحاب المصلحة الآخرين المعنيين، بمن فيهم مشغلو البنية التحتية وموزِّدوها، في عملية التخطيط ورسم السياسة بوجه عام. ومن خلال العمل معاً، يمكن لكل من الحكومة والقطاع الخاص أن يعززا من خبراتهما ومن إدارة المخاطر المتصلة بالبنية التحتية الحيوية للمعلومات. ومن شأن هذا الإدماج أن يضاعف من الثقة وأن يكفل تطوير وتطبيق السياسات والتكنولوجيات بالشكل الملائم والأكثر فعالية. وعلى الصعيد الدولي، تقتضي حماية البنية التحتية الحيوية للمعلومات وتعزيز الأمن السيبراني التعاون والتنسيق بين الدول والشركاء على الساحة الدولية.[1]

المطلب الأول

المهام التي تقوم عليها إدارة الحوادث والمراقبة في الأمن السيبراني

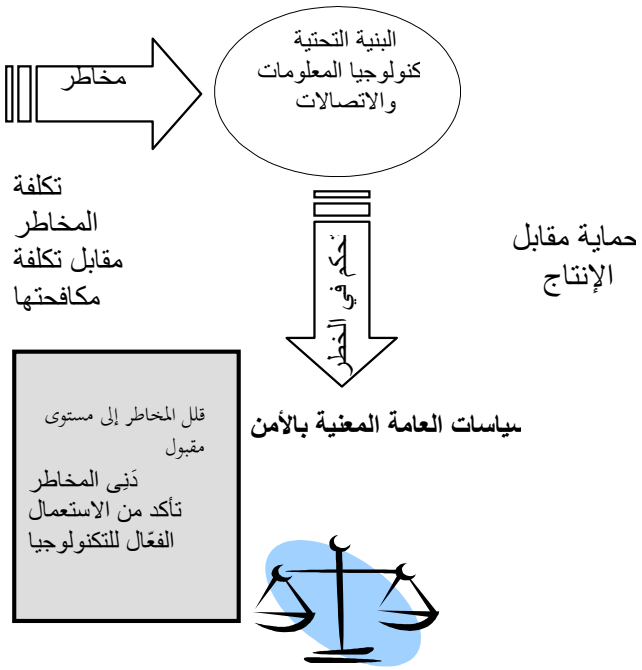
تقوم الحكومة بإنشاء أو تحديد منظمة وطنية تعمل كجهة اتصال لضمان الفضاء السيبراني وحماية البنية التحتية الحيوية للمعلومات تتضمن المهام الموكل إليها المراقبة والإنذار والاستجابة وجهود الانتعاش وتيسير التعاون بين الكيانات الحكومية والقطاع الخاص؛ والدوائر الأكاديمية؛ والمجتمع الدولي.

ويتعلق أحد الأدوار الرئيسية للحكومات في معالجة الأمن السيبراني على المستوى الوطني في الإعداد لرصد وإدارة الحوادث السيبرانية والاستجابة لها. وتتطلب الإدارة الفعالة للحوادث النظر في اعتبارات التمويل والموارد البشرية والتدريب والقدرات التكنولوجية والعلاقات بين الحكومات والقطاع الخاص والمتطلبات القانونية. ويعتبر التعاون على جميع المستويات الحكومية ومع القطاع الخاص والدوائر الأكاديمية والمنظمات الدولية عنصراً ضرورياً لإدارة الحوادث ولاستثارة الوعي بالحوادث

---

(1) انظر أبراهام د. سوفاير وسيمور ي. جودمان، *The Transnational Dimension of Cyber Crime and Terrorism,* 2001 at 16, http://media.hoover.org/documents/0817999825_1.pdf.

المحتملة والخطوات اللازمة صوب العلاج. وللحكومات دور رئيسي لضمان التنسيق بين هذه الكيانات.[1]



نموذج يوضح التصنيفات والمعايير الاوربية لتصنيف حوادث الأمن السيبراني

وذلك يتطلب إنشاء قدرات وطنية في مجال إدارة الحوادث ويمكن توضيح ذلك ما يلي: [2]

1- إقامة نظام وطني منسق للاستجابة لأمن الفضاء السيبراني لتلافي الحوادث السيبرانية وتتبعها وردعها والاستجابة لها والتعافي منها.

2- إنشاء جهة تنسيق لإدارة الحوادث السيبرانية بحيث تضم هذه الجهة العناصر المهمة في الحكومة (بما في ذلك عنصر إنفاذ القانون) والعناصر الأساسية من مشغلي البنية التحتية والموردين بغية الحد من المخاطر والتخفيف من حدة الحوادث. [3]

---

(1) جبور، منى الاشقر، مرجع سابق، ص 401.

(2) أحمد، هلالي عبداللاه (2013). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ط1، دار النهضة العربية، القاهرة، ص332.

(3) جبور، منى الاشقر، مرجع سابق، ص 402.

3- المشاركة في آليات مراقبة الحوادث والإنذار بها والاستجابة لها وتقاسم المعلومات بشأنها.

4- وضع الخطط والإجراءات والبروتوكولات بشأن الاستجابة لحالات الطوارئ، واختبارها، والتمرين عليها بما يكفل بناء الثقة بين المتعاونين من الجهات الحكومية وغير الحكومية وتعاونهم الفعال وقت الأزمات.

الفرع الأول: خطوات تحديد اهداف الأمن السيبراني

يعد إنشاء قدرة وطنية لإدارة الحوادث مهمة طويلة الأجل تبدأ بإنشاء قدرة وطنية أو فرقة وطنية للاستجابة لحوادث الحاسوب.[1] وتتفرع منها: [2]

اولا: تحديد أو إنشاء قدرات وطنية لفرقة (CIRT) Cyber Incident Response Team.

1) قد تؤدي الاستجابة الفعالة للحوادث السيبرانية الكبيرة إلى الحد من الأضرار التي تلحق بأنظمة المعلومات وضمان توافر وسائل فعالة للاستجابة والحد من طول أمد الوقت اللازم للانتعاش وتكاليفه. ويتعين بالاقتران مع القطاعين العام والخاص وجود فرقة استجابة لحوادث الأمن الحاسوبي المعينة وطنياً (CIRT) للعمل كجهة اتصال مع الحكومة وخاصة فيما يتعلق بالحوادث ذات الأهمية الوطنية لتنسيق الدفاع ضد الحوادث السيبرانية والتصدي لها. ويتعين في هذه الحالات، أن تعمل فرقة الاستجابة لحوادث الأمن الحاسوبي مع سلطات إنفاذ القوانين والمعلومات دون أن تقوم بتوجيه أنشطتها أو مراقبتها.

2) يتوقع أن تقوم فرقة الاستجابة لحوادث الأمن الحاسوبي (CIRT) بتوفير الخدمات والدعم لتلافي القضايا ذات الصلة بالأمن السيبراني والاستجابة لها والعمل كجهة اتصال وحيدة للإبلاغ

(1) دليل الأمن السيبراني للبلدان النامية الاتحد الدولي للاتصالات، لعام 2010، ص 406.

(2) بهلوان، علي (د.ت). استخدام قاعدة البيانات ومنتج التطبيقات، دار الكتب العلمية للنشر والتوزيع، ط2، القاهرة.

عن حوادث الأمن السيبراني والتنسيق والاتصالات ذات الصلة. ويتعين أن تتضمن مهام هذه الفرقة الوطنية التحليل والإنذار وتقاسم المعلومات والحد من مواطن الضعف والتخفيف ومعاونة جهود الانتعاش الوطنية للبنية التحتية للمعلومات الحرجة. وينبغي، على وجه الخصوص، أن تقوم الفرقة الوطنية للاستجابة لحوادث الأمن الحاسوبي بالعديد من الوظائف على المستوى الوطني بما في ذلك ما يلي دون أن تقتصر عليه: [1]

- رصد وتحديد النشاط الخارج على القياس.
- تحليل المخاطر السيبرانية ومواطن الضعف ونشر المعلومات المتعلقة بالإنذار بالأخطار السيبرانية.
- تحليل وتجميع المعلومات المتعلقة بالحوادث ومواطن الضعف التي توزعها الجهات الأخرى، بما في ذلك الموردون وخبراء التكنولوجيا لتوفير تقييم يقدم لأصحاب المصلحة المهتمين؛
- إقامة آليات اتصالات موثوق بها وتيسير الاتصالات فيما بين أصحاب المصلحة لتقاسم المعلومات ومعالجة القضايا ذات الصلة بالأمن السيبراني.
- توفير معلومات الإنذار المبكر، بما في ذلك المعلومات المتعلقة بالتخفيف من مواطن الضعف والمشاكل المحتملة.
- وضع استراتيجيات للتخفيف والاستجابة وتفعيل الاستجابة المنسقة للحوادث؛
- تقاسم البيانات والمعلومات عن الحوادث والاستجابة المقابلة؛
- تتبع ورصد المعلومات لغرض تحديد الاتجاهات واستراتيجيات العلاج طويلة الأجل؛

---

(1) الجنيهي، منير محمد والجنيهي، ممدوح محمد (2016). جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ط1، ص 406.

- نشر أفضل الممارسات العامة المتعلقة بالأمن السيبراني والتوجيهات المتعلقة بالاستجابة للحوادث وتلافيها.[1]

ثانيا: آليات داخل الحكومة للتنسيق بين الوكالات المدنية والحكومية.

1) يتمثل أحد الأدوار الرئيسية للفرقة الوطنية للاستجابة لحوادث الأمن الحاسوبي في نشر المعلومات، بما في ذلك المعلومات عن مواطن الضعف والأخطار الحالية على أصحاب المصلحة المعنيين. وتمثل الوكالات الحكومية المعنية أحد أصحاب المصلحة المجتمعية ويتعين إشراكها في أنشطة الاستجابة.

2) ويمكن أن يتخذ التنسيق الفعال مع هذه الكيانات عدة أشكال منها، على سبيل المثال، ما يلي: [2]

1- إقامة موقع على شبكة الويب لتبادل المعلومات؛ توفير المعلومات عن طريق قوائم المراسلات بما في ذلك النشرات الإخبارية وتقارير الاتجاهات والتحليل؛ إعداد المطبوعات التي تتضمن التنبيهات والأفكار المفيدة والمعلومات عن مختلف جوانب الأمن السيبراني بما في ذلك التكنولوجيات الجديدة ومواطن الضعف والأخطار والنتائج.

ثالثا: وضع أدوات وإجراءات لحماية الموارد السيبرانية للكيانات الحكومية.[3]

1) تتطلب عملية الإدارة الفعالة للحوادث أيضًا وضع وتنفيذ سياسات وإجراءات ومنهجيات وأدوات أمنية لحماية الأصول السيبرانية للحكومات وأنظمتها وشبكاتها ووظائفها. ويمكن أن يتضمن ذلك، بالنسبة لفرقة الاستجابة لحوادث الأمن الحاسوبي، إجراءات التشغيل المعيارية ومبادئ

(1) حجازي، عبد الفتاح بيومي (2020). مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية.

(2) الرومي، محمد أمين، (2013). جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، الإسكندرية، ص 19.

(3) حسن، سعيد عبد اللطيف. (2017) . إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، ط.4، ص 316.

توجيهية للعملية الداخلية والخارجية وسياسات أمنية للتنسيق مع أصحاب المصلحة وتنفيذ شبكات المعلومات الأمنة لعمليات فرقة الاستجابة لحوادث الأمن الحاسوبي وتأمين الاتصالات. ويتعين على فرق الاستجابة لحوادث الأمن الحاسوبي، بوصفها جهة اتصال بشأن الاستجابة للحوادث، التنسيق مع بعضها الآخر والمساعدة في التمكين من التعاون مع كيانات الاستجابة للحوادث الأخرى. ويتعين على الحكومات أن توفر التدريب المستمر لجميع الموظفين الجدد والحاليين بشأن الاستجابة للحوادث. [1]

رابعا: تنسيق العمليات الحكومية للاستجابة للهجمات السيبرانية واسعة النطاق والتعافي منها. [2]

في حالة وقوع حادثة ترقى إلى مستوى الأهمية الوطنية، سيلزم وجود جهة اتصال مركزية للتنسيق مع الكيانات الحكومية الأخرى ومع أصحاب المصلحة الآخرين، مثل القطاع الخاص. ومن المهم وضع الخطط والإجراءات التي تكفل استعداد الفرقة الوطنية للاستجابة للحوادث للتصدي لأي حادث محتمل.

المطلب الثاني
الثقافة الوطنية للأمن السيبراني

نظراً لما أصبحت عليه التكنولوجيات تتقارب في سماتها، وأن استخدام تكنولوجيا المعلومات والاتصالات يتزايد انتشاره باطراد، وأن التواصل عبر الحدود الوطنية آخذه في التزايد، يتعين على جميع المشاركين الذين يقومون بوضع وملكية وتوريد وإدارة الخدمات ويستخدمون شبكات

(1) حجازي، عبد الفتاح (2012). الدليل الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة.

(2) حجازي، عبد الفتاح بيومي، (2003). النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى. ص 116.

المعلومات فهم قضايا الأمن السيبراني، وأن يتخذوا من الإجراءات ما يتناسب وأدوارها في حماية الشبكات. وينبغي للحكومات أن تمسك بزمام القيادة في نشر ثقافة الأمن السيبراني ودعم جهود المشاركين الآخرين.[1]

الفرع الأول: لترويج لخدمات الأمن السيبراني

الترويج لثقافة وطنية للأمن بما يتسق مع قرار الجمعية العامة للأمم المتحدة 57/239، إرساء ثقافة عالمية للأمن السيبراني، والقرار 58/199، إرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية البنى التحتية الحيوية للمعلومات.[2]

1) تتطرق مسألة الترويج لثقافة وطنية للأمن ليس فقط لدور الحكومة في تأمين تشغيل واستخدام البنية التحتية للمعلومات، بما في ذلك الأنظمة التي تديرها الحكومة، ولكن أيضًا لتوعية القطاع الخاص، والمجتمع المدني، والأفراد. وبالمثل، فإن هذا العنصر يشمل تدريب مستعملي الأنظمة الحكومية والخاصة، وإدخال تحسينات في المستقبل على الجوانب الأمنية، ومسائل أخرى هامة تشمل الخصوصية، والرسائل الاقتحامية، والبرمجيات الضارة. [3]

2) ووفقاً لما أوردته تقارير منظمة التعاون والتنمية في الميدان الاقتصادي، فإن القوى الدافعة الرئيسية لأي ثقافة للأمن على المستوى الوطني تتمثل في تطبيقات الحكومة الإلكترونية وخدماتها، وحماية البنية التحتية الحيوية للمعلومات. ونتيجة لذلك، ينبغي للإدارات الوطنية تنفيذ تطبيقات وخدمات الحكومة الإلكترونية من أجل تحسين عملياتها الداخلية وتوفير الخدمات الأفضل للقطاع الخاص والمواطنين. ولا ينبغي تناول مسألة أمن أنظمة وشبكات المعلومات من منظور تكنولوجي

(1) رستم، هشام (2017). قانون العقوبات ومخاطر تقنية المعلومات، ط1، مكتبة الآلات الحديثة، أسيوط.

(2) EVELYNE, JACQUES (2020). REGULATING CYBERSECURITY What civil liability in case of cyber-attacks p . 301

(3) رستم، هشام (2012). الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، أسيوط.

فحسب، ولكن ينبغي أن يشمل هذا المنظور عناصر من قبيل تلافي المخاطر، وإدارة المخاطر، وتوعية المستخدمين. ورأت منظمة التعاون والتنمية في الميدان الاقتصادي أن التأثير المفيد لأنشطة الحكومة الإلكترونية يتمثل في الانتقال إلى ما يتجاوز الإدارة العامة صوب القطاع الخاص والأفراد. ويبدو أن مبادرات الحكومة الإلكترونية قد عملت كعنصر مضاعف نحو تعزيز نشر ثقافة الأمن.[1]

3) ينبغي للبلدان من خلال أنشطتها التعاونية، والأفضل من خلال نوع من الاتفاقات أن تعتمد نهج متعدد التخصصات ومتعدد أصحاب المصلحة إزاء تنفيذ الأمن السيبراني، ويقوم بعضها بإنشاء هيكل إدارة رفيع المستوى لتنفيذ السياسات الوطنية. وتعتبر مبادرات استثارة الوعي والتوعية على جانب كبير من الأهمية، بجانب تقاسم أفضل الممارسات وإقامة الشراكات فيما بين المشاركين واستخدام المعايير الدولية.[2]

4) ويكتسي التعاون الدولي أهمية بالغة في تعزيز ثقافة للأمن، جنباً إلى جنب مع دور المنظمات الإقليمية في تيسير التفاعلات والتبادلات.[3]

الفرع الثاني: تنفيذ الخطة الأمنية للأنظمة التي تديرها الحكومات.

1) تتضمن الخطوة الأولية للإجراء الحكومي الرامي إلى تأمين الأنظمة التي تديرها وضع وتنفيذ خطة أمنية وطنية. وينبغي أن يتطرق إعداد هذه الخطة إلى إدارة المخاطر، فضلاً عن تصميم مخطط للأمن وتنفيذه. وينبغي من آن لآخر إعادة تقييم كل من الخطة وتنفيذها لقياس

(1) رستم، هشام محمد(2015). جرائم الحاسب المستحدثة، دار الكتب القانونية، مصر، ط1.

(2) الزعبي، محمد علي(2013). الحماية القانونية لقواعد البيانات وفقا لقانون حماية حق المؤلف، ط1، منشأة المعارف، الاسكندرية.

(3) الزيدي، وليد (2019). القرصنة على الإنترنت والحاسوب، دار أسامة للنشر، عمان، ط3.

ما تحقق من تقدم وتحديد المجالات التي تحتاج إلى تحسينات في الخطة أو في تنفيذها. كما ينبغي أن تتضمن الخطة أحكاماً تتعلق بإدارة الحوادث، بما في ذلك الاستجابة والمراقبة والإنذار والانتعاش والصلات المتعلقة بتقاسم المعلومات. كما ينبغي أن تعالج الخطة الأمنية الإجراءات التي طلبت في الفقرة.

2. لتدريب مستخدمي هذه الأنظمة الحكومية والتعاون فيما بين الحكومة والقطاع الخاص والمجتمع المدني بشأن التدريبات والمبادرات الأمنية. وتعتبر توعية المستخدمين ومسؤوليتهم القضايا الرئيسية التي يتعين على التدريب أن يعالجها.[1]

الفرع الثاني: تنفيذ برامج ومبادرات التوعية الأمنية لمستخدمي الأنظمة والشبكات الحكومية.

ينبغي لأي برنامج وطني فعال للتوعية بالأمن السيبراني أن يعزز من التوعية بالأمن السيبراني فيما بين عامة الجمهور والمجتمعات الرئيسية وداخل هذه المجتمعات، وإقامة روابط مع المتخصصين الحكوميين في مجال الأمن السيبراني من أجل تقاسم المعلومات بشأن مبادرات الأمن السيبراني، وتنمية التعاون وتعزيزه في مجال المسائل المتصلة بالأمن السيبراني. [2]

وهناك ثلاثة عناصر وظيفية يتعين النظر فيها لدى وضع برنامج للتوعية في هذا المجال: [3]

(1) توعية وإشراك أصحاب المصلحة مما يؤدي إلى بناء وتعزيز روابط تسودها الثقة فيما بين القطاع الخاص والحكومة والأوساط الأكاديمية من أجل زيادة الوعي بالأمن السيبراني وتحقيق الأمن الفعلي للفضاء السيبراني.

---

(1) طوال، علي حسن (2019). مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، دراسة مقارنة، مركز الإعلام الأمني.

(2) عبد الله، عبد الله عبد الكريم (2011). جرائم المعلوماتية والإنترنت – الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ط1.

(3) العريان، محمد علي(2019). الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ط2.

(2) التنسيق الذي من شأنه أن يكفل التعاون بشأن الحوادث والأنشطة المتصلة بالأمن السيبراني بين مختلف القطاعات الحكومية.

(3) تبادل الاتصالات والرسائل، مع التركيز على تنمية الاتصالات الداخلية (داخل الوكالة الحكومية المسؤولة عن هذا البرنامج)، والاتصالات الخارجية (الوكالات الحكومية الأخرى، ودوائر الصناعة، والمؤسسات التعليمية، ومستعملي الحواسيب المنزلية، وعامة الجمهور).

الفرع الثالث: إيجاد ثقافة للأمن داخل مؤسسات الأعمال التجارية.

يمكن إيجاد ثقافة للأمن داخل مؤسسات الأعمال التجارية عن طريق عدد من السبل المبتكرة. فقد وُجِّه الكثير من المبادرات الحكومية نحو استثارة الوعي لدى المنشآت التجارية الصغيرة والمتوسطة الحجم. ويمكن أن يساعد الحوار الحكومي، مع روابط دوائر الأعمال أو الشراكات بين القطاعين العام والخاص والناس، الإدارات على تصميم وتنفيذ مبادرات للتوعية والتدريب. ومن بين الأمثلة على هذه المبادرات: [1] إتاحة المعلومات (على الخط مباشرةً وبطريقة غير مباشرة)، مثل الكتيبات والأدلة والكتيبات الإرشادية والسياسات النموذجية والمفاهيم؛ وإنشاء مواقع على شبكة الويب موجهة بصورة خاصة إلى المنشآت التجارية الصغيرة والمتوسطة الحجم وأصحاب المصلحة الآخرين؛ وتوفير التدريب (على الخط مباشرة)؛ وتوفير أدوات للتقييم الذاتي على الخط مباشرة؛ وعرض المساعدة المالية والدعم الضرائبي أو أي حوافز أخرى بغرض تعزيز إنتاج أنظمة مأمونة أو القيام بخطوات استباقية لتحسين الأمن السيبراني. [2]

(1) عمار، ماجد (2016). المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، ط1، دار النهضة العربية، القاهر.

(2) By Wayne M. Alder (2018). Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend A Claim. P. 201.

الترويج لبرنامج وطني شامل للتوعية حتى يتمكن جميع المشاركين– دوائر الأعمال واليد العاملة العامة والجمهور العام– من تأمين أدوارهم في الفضاء السيبراني. [1]

1) يوجد الكثير من مواطن الضعف في أنظمة المعلومات نتيجة لنقص الوعي بالأمن السيبراني من جانب المستعملين ومديري الأنظمة وواضعي التكنولوجيات وموظفي التوريدات والمدققين وكبار موظفي المعلومات ومجالس المؤسسات. ويمكن أن تشكل مواطن الضعف هذه مخاطر جسيمة على الهياكل الأساسية حتى إذا لم تكن هذه جزءاً فعلياً من هذه الهياكل ذاتها. وعلى سبيل المثال، فإن نقص الوعي الأمني لدى مديري الأنظمة كثيراً ما يشكل نقطة ضعف للخطة الأمنية للمؤسسة.

ولذا فإن تعزيز جهود القطاع الخاص في تدريب الموظفين واعتماد شهادات أمنية مقبولة على نطاق واسع للموظفين سوف تساعد في الحد من مواطن الضعف هذه. ومن ناحية أخرى، فإن التنسيق الحكومي للأنشطة الوطنية للإرشاد والتوعية للتمكين من ثقافة الأمن سوف يبني أيضًا الثقة مع القطاع الخاص. [2]

فالأمن السيبراني عبارة عن مسؤولية مشتركة. ويمكن لإنشاء منافذ ومواقع على الويب أن يشكل آلية مفيدة لوضع برنامج وطني للتوعية لتمكين الوكالات الحكومية ودوائر الأعمال وفرادى المستهلكين من الحصول على المعلومات ذات الصلة والقيام بالتدابير التي تحمي الأجزاء الخاصة بهم في الفضاء السيبراني.[3]

---

(1) الفيل، علي عدنان (2011). الإجرام الإلكتروني: دراسة مقارنة، الطبعة الأولى، لبنان.

(2) قايد، أسامة عبد الله، (2016) الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة.

(3) العنزي، سليمان (2013): وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

الفرع الرابع: تعزيز الأنشطة المعنية بالعلم والتكنولوجيا والبحث والتطوير.

على الدول والحكومات ان تدعم العلم والتكنولوجيا والبحث والتطوير، يتعين توجيه بعض جهودها صوب أمن البنية التحتية للمعلومات. فبوسع البلدان أن تساعد، من خلال تحديدها أولويات البحوث والتطوير في المجال السيبراني، في تطوير المنتجات ذات الخواص الأمنية الذاتية، فضلاً عن معالجة التحديات التقنية الصعبة. وبالقدر الذي يتم به الاضطلاع بأنشطة البحث والتطوير في المؤسسات الأكاديمية، قد تتاح الفرص لإشراك الطلاب في مبادرات الأمن السيبراني.[1]

ويُعتبر الذكاء الاصطناعي أحد فروع علوم الكمبيوتر وأحد الركائز الرئيسية التي تستند إليها صناعة التكنولوجيا في العصر الحالي، ويمكن تعريف مصطلح الذكاء الاصطناعي – الذي يشار إليه باختصار – (AI) بأنه قدرة الآلات الرقمية وأجهزة الكمبيوتر على أداء مهام معينة تحاكيها وتماثلها تلك التي تقوم بها كائنات ذكية، مثل القدرة على التفكير أو التعلم من التجارب السابقة أو غيرها من العمليات التي تتطلب عمليات عقلية، والذكاء الاصطناعي يهدف إلى الوصول إلى الأنظمة التي استمتع بالذكاء وتتصرف بالطريقة التي يتصرف بها البشر فيما يتعلق بالتعلم وعدم الفهم، بحيث توفر هذه الأنظمة لمستخدميها خدمات مختلفة مثل التعليم والإرشاد والتفاعل، إلخ ولقد انطلق البحث الفلسفي في مجال الذكاء الاصطناعي تزامنا مع انبثاق الثورة العلمية الكبيرة في هذا المجال، إذ استند هذا المشروع العلمي الخلاق على تلاحم علمي فلسفي يندر مثيله، وعلى الرغم من التلاحم بين الفلسفة والعلم في إنجاز ثورات علمية قد حصل في تاريخ الفكر الإنساني بشكل استثنائي ولعل الثورة العلمية في اكتشاف قوانين التفاضل والتكامل خير مثال على ذلك، إلا

(1) قشقوش، هدى حامد (2017). جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة.

أن ابتكار الذكاء الاصطناعي جاء على خلفية فلسفية متطورة ومدروسة بشكل جيد خطط لها أن تستثمر علميا، ففلسفة المنطق ثنائي القيمة المعاصرة وصلت إلى أوجها في بداية القرن العشرين بعد الجهود التي بذلت إلى شحن المنطق المعاصر بقدرة هائلة من المرونة المنبثقة من الجبر المنطقي المبتكر واللغات الرمزية المتعددة، بحيث يستطيع أن يتعامل مع المجالات العلمية الأكثر دقة وصورية متمثلا ذلك بعلم الرياضيات،[1] إذ استطاع المنطق المعاصر أن يفسر الأسس الفلسفية المبني عليها هذا العلم، كونه تسلح بلغة لا تستطيع أي لغة غيرها أن تبوح بما تعني به قوانين الرياضيات وعلى أي بنية فكرية تستند، ذلك أن المنطق المعاصر بالإضافة إلى خاصيته الصورية الرمزية التي يشترك بها مع الرياضيات لكنه يتميز عنها بخاصية قدرته على شرح المضمون الفلسفي التي تنطوي عليه الجمل الرمزية على شكل إجرائية متسلسلة من الاستنتاجات ما تمتلكها الرياضيات الصرفة، فهذه الخاصية الإجرائية التي تستطيع أن تشيد فرضيات أدق العلوم انطلاقا من أساسها الفكري بالإضافة إلى اللغة الفائقة البساطة التي يصوغ بها مضمونه الفكري والتي تتكون فقط من حرفين كونه منطق ثنائي القيمة، ما جعل المنطق الرياضي المعاصر جاهزا بأن يداعب خيال العلماء لاستنساخ منه هاتين الخاصيتين وتنفيذها تقنيا على شكل لغة اصطناعية نتفاهم بها مع الآلة اما المعنى الشائع للذكاء الاصطناعي يتعلق كليا بمقارنة وتمييز ذكاء ماكينة الحاسوب نسبة إلى ذكاء الكائن البشري، أو بوصف آخر للذكاء الاصطناعي بأنه الكيفية التي تصنف بها ماكينة الحاسوب ضمن حقل الذكاء ولكن كلا الوصفين لم يلق قبولا عاما ليكون تعريفا للذكاء إذ جاء الاعتراض منصبا على أن " الذكاء " نشاط يستمد فهمه من تلاصقه بمالكه الشرعي وهو الإنسان.

(1) . *A2J Author*. www.kentlaw.iit.edu/institutes-centers/center-for-access-to-justice-andtechnology/a2j-author (accessed January 30, 2015).

الفرع الخامس: نظام الخصوصية السائد وتحديثه ليلائم بيئة الخط المباشر.

ينبغي أن ينظر هذا الاستعراض في آليات الخصوصية التي اعتمدتها مختلف البلدان والمنظمات الدولية، مثل منظمة التعاون والتنمية في الميدان الاقتصادي. وما زالت الخطوط التوجيهية التي وضعتها هذه المنظمة بشأن حماية الخصوصية وتدفق البيانات الشخصية عبر الحدود، وهي الخطوط التي اعتمدت في 23 سبتمبر 1980، تمثل توافقاً دولياً في الآراء بشأن التوجيه العام المتعلق بجمع وإدارة المعلومات الشخصية.[1] وتضطلع هذه الخطوط التوجيهية، بما وضعته من مبادئ أساسية، بدور رئيسي في مساعدة الحكومات ودوائر الأعمال وممثلي المستهلكين في جهودهم لحماية الخصوصية والبيانات الشخصية وفي إلغاء القيود غير الضرورية على تدفق البيانات عبر الحدود سواء على الخط مباشرة أو بصورة غير مباشرة.[2]

الفرع السادس: الوعي بالمخاطر السيبرانية والحلول المتاحة.

- يقتضي تناول القضايا التقنية تكاتف الحكومات والأعمال التجارية والمجتمع المدني وفرادى المستعملين في العمل معاً لوضع وتنفيذ التدابير التي تدمج بين عنصر العملية (التكنولوجية) (أي المعايير) (مثل المبادئ التوجيهية الاختيارية أو اللوائح الإلزامية)، وعنصر الأفراد (أي أفضل الممارسات). [3]
- وأحد الأمثلة على المخاطر السيبرانية الرسائل الاقتحامية وما يرتبط بها من مخاطر مثل البرمجيات الضارة. [4]
- وإدارة الهوية هي أحد الأمثلة على وجود أداة تكنولوجية لمعالجة مختلف احتياجات الأمن السيبراني. [5]

---

(1) القهوجي، علي عبد القادر (2016). الحماية الجنائية لبرامج الحاسب، ط1، دار الجامعة الجديدة للنشر، الإسكندرية.

(2) العنزي، سليمان (2013): وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

(3) قورة، نائلة عادل (2012). جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، ط1.

(4) لطفي، محمد حسام (2016). الحماية القانونية لبرامج الحاسب الإلكتروني، ط1، دار الثقافة للطباعة والنشر، القاهرة.

(5) لطفي، محمد حسام (2012). عقود خدمات المعلومات، ط1، بدون ناشر، القاهرة.

الفصل الرابع
التزامات أطراف مقدمي خدمات الأمن السيبراني

بدايات التقدم العلمي والتكنولوجي، وفي ظلِّ غزوِ شبكة الأمن السيبراني لكافة مناحي الحياة، بزغت بوادر الخير لفتحِ آفاقٍ جديدة لتقدم البشريَّة ولجني ثمار التواصل والمعرفة، إلاَّ أنه، وللأسف، ظهرت في نفس الوقت نوازع الشر لاستغلال هذا التقدم لتحقيق أغراضٍ شخصية رخيصة على حساب قيم المجتمع، وحقوق الأفراد والجماعة وأمنهم. فما كان من أصحاب النفوس الضعيفة إلاَّ أن تجرَّؤوا على تحويل شبكة الأمن السيبراني إلى مسرحٍ يرتكبون فيه العديد من الجرائم والمخالفات: فقاموا بنشر الأخبار المزيَّفة، وبثوا الأفكار والممارسات المناهضة للأديان السماوية وللإنسانية، ونشروا الصور الفاضحة للصغار قبل الكبار، وانتهكوا حرمة الحياة الخاصة لأفراد المجتمع، وسبُّوا الأشخاص وقذفهوهم، وتعدُّوا على حقوق الملكية الفكرية... وما هذه إلاَّ نماذج من سلسلة مخالفات تُرتكب عبر الأمن السيبراني يصعب حصرها. [1]

والواقع العملي يُثبت أن تداول المعلومات عبر شبكة الأمن السيبراني بحاجة إلى تضافر جهود الأشخاص القائمين على إدارتها، والذين تتنوَّع أدوارهم وأنشطتهم في تشغيلها. فحتى يتمكن مستخدمو الأمن السيبراني من الدخول إلى الشبكة، والإبحار فيها بحرِّية، والوصول إلى ما يصبون إليه من معلومات أو بثِّها، لا بُدَّ من وجود عدَّة أشخاص، يُطلق عليهم عادةً مصطلح "مقدمي خدمات الأمن السيبراني"، أو "الوسطاء في خدمات الأمن السيبراني"، يتولُّون عملية إيواء

(1) المسؤولية الإلكترونية بشكلٍ عام عن المخالفات المرتكبة عبر الإنترنت، راجع، محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، الطبعة الأولى، 2003.

المعلومات، وبثِّها، وعرضها [1] وهذا التنوُّع في أدوارهم والتعدُّد في أنشطتهم يجعل من اليسير عليهم تتبُّع النشاط المعلوماتي غير المشروع وكشفه، إلاَّ أن تحقيق ذلك يبقى رهن وجود ضوابط قانونية تُحدِّد حقوق أطراف النشاط الإلكتروني والتزاماته في مواجهة بعضهم البعض من جهة، وفي مواجهة المجتمع الذي يعيشون فيه من جهةٍ أُخرى. لذا بدت الحاجة ماسة لإيجاد تنظيم تشريعي متكامل يُحدد المركز القانوني لمقدمي خدمات الأمن السيبراني، ويُبين في نفس الوقت مسؤولية كلٍّ منهم عمّا يُرتكب من مخالفات عبر الشبكة، الأمر الذي لا يُمكن تحقيقه إلا بتضافر جهود المشرّعين على الصعيدين: الوطني والدولي.

المبحث الأول
التزامات مقدمي خدمات الأمن السيبراني

يتَّضح لنا جليَّاً مما تقدم، تنوُّع مهام أشخاص القائمين على خدمات الأمن السيبراني، وتعدُّد أدوارهم المتبادلة، إذ من الممكن للشخص الواحد أن يقوم في نفس الوقت بمهمة أو أكثر. ويثور التساؤل حول كيفية تحديد التزامات كل شخص من أشخاص القائمين على خدمات الأمن السيبراني. فمن هؤلاء الأشخاص من يتَّسم عمله على الشبكة بالطابع المعلوماتي، ومنهم من يغلب على عمله الطابع الفني، الأمر الذي يستدعي تحديد التزامات كل من مقدمي الخدمة المعلوماتية (المطلب الأول)، ومقدمي الخدمة الفنية (المطلب الثاني). ولا بدَّ أن ننوه هنا أن المشرّع الأردني لم يضع، كما أسلفنا، نظاماً قانونياً خاصاً بمقدمي خدمات الأمن السيبراني. لذلك، فإن طرحنا سيعتمد في حدٍّ كبيرٍ منه على موقف التشريعين: الأُوروبي والفرنسي اللذين تناولا هذه المسألة بشيءٍ من

(1) في تعدُّد أشخاص القائمين على خدمات الإنترنت، انظر: عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2003م، ص 339 وما بعدها، محمد حسين منصور، ص 196 وما بعدها،

Lionel THOUMYRE, "Hyper dossier sur les acteurs de l'Internet en France", juriscom.net, 22 juin 2004, disponible à l'adresse www.juriscom .net /pro/ visu. php? ID= 485.

التفصيل، فألقيا على عاتق مقدمي الخدمات أنواعاً خاصة من الالتزامات تختلف في طبيعتها عن طبيعة الالتزامات الملقاة على عاتق غيرهم من المهنيين.

المطلب الأول
التزامات مقدمي الخدمة المعلوماتية

إن من يُقدِّم خدمة الإيواء على الأمن السيبراني، ويأوي على الموقع الذي أنشأه، ويتوَّلى إدارته المعلومات والرسائل الخاصة، ويُتيح لها فرصة الدخول إلى الشبكة لتكون متاحة لكل الراغبين في الاطلاع عليها يتجاوز حتماً دوره الفني كناقل للمعلومات[1]، فهو يتولَّى، من جانب، إدارة النشاط المعلوماتي على شبكة الأمن السيبراني، ومن جانب أخر فإنه يمد العملاء بالوسائل التقنية التي تُمكِّنهم من الوصول إلى الموقع الذي خُزِّنت فيه المعلومات. فآلية عمل متعهد الإيواء والإمكانيات التقنية والمعلوماتية التي يتمتَّع بها تُساهم، وبشكلٍ فعّال، في تداول المضمون المعلوماتي عبر الشبكة، وبالتالي، في تيسير عملية إيصال الخدمة المعلوماتية لطالبيها من عملاء ومستخدمين (الفرع الأول). كذلك الحال بالنسبة لمورِّد المعلومات والذي يتمتع بالسيطرة الكاملة على المضمون المعلوماتي الذي يقوم بجمعه أو تأليفه، ومن ثم توريده إلى الجمهور عبر شبكة الأمن السيبراني (الفرع الثاني).

الفرع الأول: التزامات متعهد الإيواء

إن طبيعة الخدمة التي يقدمها متعهد الإيواء تجعله، حتماً، الأقرب والأقدر على معرفة مضمون أيِّ نشاطٍ معلوماتي متداول عبر شبكة الأمن السيبراني، وإذا ما ثبتت عدم مشروعية المضمون المأوي فإن ذلك سيثير عدداً من الإشكاليات القانونية على صعيدين مختلفين: الأول،

(1) Paris (Cour d'Appel de Paris), 9 février 1999, JCP G, 2000, p. 580, note F. OLIVIER CA. كما ورد في محمد حسين منصور، المرجع السابق، ص 206.

يتعلَّق بمدى التزام متعهد الإيواء برقابة المضمون المعلوماتي المتداول عبر شبكة الأمن السيبراني، والثاني، يتمثل في الالتزامات التي تقع على عاتق متعهد الإيواء في حال علمه بتداول مضمون معلوماتي غير مشروع عبر هذه الشبكة. وأمام هذه الإشكاليات، وفي ظل غياب نص تشريعي خاص يُعالجها، فرض القضاء الفرنسي حدَّاً معقولاً من الالتزامات على متعهدي الإيواء (أولاً)، فما كان من المشرّع الفرنسي إلا أن استجاب لهذا القضاء وأن قنَّن هذه الالتزامات أُسوةً بالمشرّع الأُوروبي (ثانياً). ونتمنَّى كذلك على كل من قضائنا ومشرِّعنا الأردنيين أن يحذوا حذو نظيريهما الفرنسيين، فلا يترددا في التصدِّي لهذه المسائل.

أولاً: موقف القضاء

لم يكن من السهل في البداية على القضاء الفرنسي، وأثناء نظره الدعاوي المرفوعة ضد متعهدي الإيواء، تحديد نطاق الالتزامات ومضمونها التي تقع على عاتقهم، فحاول جاهداً التغلب على الصعوبات التي واجهته كي لا يكون الأمن السيبراني منطقة بلا قانون. ونظراً لطبيعة الخدمة الي يقدمها متعهدو الإيواء، وفي ظل غياب نصوص قانونية خاصة، أبدى القضاء الفرنسي قدراً من التساهل في نوعية الالتزامات الملقاة على عاتقهم، فلم يفرض عليهم التزاماً عاماً بممارسة الرقابة الدقيقة على محتويات المواقع الإلكترونية التي يأوونها، ولم يكلفهم بالبحث النشط عن المضمون المعلوماتي الإلكتروني غير المشروع [1]. بالمقابل، ألزمهم القضاء بأخذ الحيطة والحذر، وأقام مسؤولياتهم حيال التقصير، وقد استند القضاء في ذلك على القواعد العامة في المسؤولية، وبالأخص نص المادتين: 1382 و1383 من القانون المدني الفرنسي اللتين تُلزمان صاحب الفعل الضار الذي أدَّى بخطئه، أو بإهماله، أو بتقصيره إلى الإضرار بالغير بضمان هذا الضرر.

(1)) Luc GRYNBAUM, "LCEN. Une immunité relative des prestataires de services Internet", précité, nº 9, p. 37.

وتطبيقاً لذلك، وبمناسبة الاعتداء على الحق في الصورة من قِبل متعهد الإيواء Altern.org، أقامت عارضة الأزياء الفرنسية Estelle Hallyday دعوى قضائية أمام محكمة بداية باريس ضد V. Lacambre مُؤسس وصاحب الموقع Altern.org تُطالبه فيها بالتعويض عن الأضرار التي سببها لها نتيجة لإيوائه موقعاً إلكترونياً نُشر عليه تسع عشرة صورة تظهرها عارية بشكل كلِّي أو جزئي. جاء قرار المحكمة في 9 حزيران 1998م ليضع على عاتق متعهد الإيواء التزاماً ببذل العناية والجهد اللازمين لمراقبة احترام المواقع الإلكترونية المأوية لحقوق الآخرين وللآداب العامة، ويُرتب مسؤوليته في حال إخلاله بهذا الالتزام استناداً إلى المادة 1383 من القانون المدني الفرنسي. وقد ورد في حيثيات قرار المحكمة شروط إعفاء متعهد الإيواء من المسؤولية والتي تمثلت بوجوب إثبات قيامه بإعلام أصحاب المواقع الإلكترونية المأوية بضرورة مراعاة القوانين والأنظمة السارية، وبعدم الاعتداء على حقوق الآخرين وحقوق الملكية الفكرية على الأمن السيبراني. كما يجب عليه أن يُثبت، أيضًا، أنه قام بالإجراءات اللازمة من أجل التقاط المواقع الإلكترونية المأوية التي تحتوي على مضمون معلوماتي غير مشروع. فعلى حد تعبير المحكمة من يأوي البيانات والمعلومات، ويقوم ببثها إلى الجمهور يتجاوز، حتماً، دوره كناقل فني بسيط للمادة المعلوماتية، ويتوجب عليه بالتالي تحمل المسؤولية الناجمة عن ممارسة هذا النشاط في حال انتهاك حقوق الغير[1].

(1) TGI de Paris (Tribunal de Grande Instance de Paris محكمة بداية باريس), ord., réf., 9 juin 1998, JCP éd. E, 1998, n° 21, p. 953, obs. M. VIVANT et Ch. LE STANC, « Le fournisseur d'hébergement ne peut s'exonérer de sa responsabilité qu'à la condition de justifier du respect des obligations mises à sa charge, spécialement quant à l'information de l'hébergé sur l'obligation de respecter les droits de la personnalité, le droit des auteurs, de la réalité des vérifications qu'il aura opérées, au besoin par des sondages », « En hébergeant (…) des signaux, d'écrits, d'images, V. Lacambre excède manifestement le rôle d'un simple transmetteur d'informations et doit, d'évidence, assurer à l'égard des tiers aux droits desquels il serait porté atteinte (...) les conséquences d'une activité qu'il a, de propos délibéré, entrepris d'exercer dans les conditions susvisées et qui contrairement à ce qu'il prétend, est rémunératrice et revêt une ampleur que lui même revendique»

وقد تمَّ التأكيد على هذا القرار في مرحلة الاستئناف من قِبل محكمة استئناف باريس[1].

وفي 8 كانون الأول 1999م، وأمام محكمة بداية (نانتير)، كان الدور هذه المرَّة لعارضة الأزياء الفرنسية Lynda Lacoste، والتي توجهت للمحكمة للمطالبة بإدانة أربعة متعهدي إيواء لإيوائهم المباشر والدائم لعدد من الصور التي تُظهرها بشكلٍ فاضحٍ، وعرضها على شبكة الأمن السيبراني دون الحصول على موافقتها. جاء قرار المحكمة في هذه القضية ليُحدِّد، بشكلٍ واضح وصريح، نوعية الالتزامات الملقاة على عاتق متعهدي الإيواء وليطالبهم بوجوب إثبات تقيدهم بالالتزامات الواقعة على عاتقهم، خاصةً تلك المتعلقة بإعلام اصحاب المواقع الإلكترونية المأوية بضرورة احترام حقوق الآخرين، وبذلهم العناية والجهد اللازمين للكشف عن أي مضمون معلوماتي غير مشروع، والتوقف عن بثه حال التقاطه [2]. وبقرارها هذا، حدَّدت المحكمة مضمون الالتزامات التي تقع على عاتق متعهدي الإيواء، وحصرتها بثلاثة: أولها الالتزام بالإعلام، وثانيها الالتزام باليقظة، وثالثها الالتزام بوقف بث المضمون المعلوماتي غير المشروع، أو على حد تعبير المحكمة، وجوب اتخاذ موقف إيجابي.

---

(1) CA Paris, 10 février 1999, JCP G, II, 10101, note OLIVIER et BARBRY, D. 1999, p. 389, note M. POUJOL, Comm. Com. Électr., 1999, comm. p. 34, note R. DESGORCES, disponible également à l´adresse: www. droit-technologie.org.

(2) TGI de Nanterre, 1re ch., sect. A, 8 décembre 1999, Comm. Com. Électr., mars 2000, p. 29, note A. LEPAGE, disponible également à l´adresse: www.droit-technologie.org, rubrique jurisprudence, Th. VERBIEST et É. WÉRY, Le droit de l´internet et de la société d´information, précité, n° 411, p. 225, « L'hébergeur devrait démontrer le respect des obligations mises à sa charge, spécialement quant à l'information de l'hébergé sur l'obligation de respecter les droits de la personnalité, le droit des auteurs, des propriétaires de marques, de la réalité des vérifications qu'il aura opérées, au besoin par des sondages, et les diligences qu'il aura accomplies dès la révélation d'une atteinte au droit des tiers pour faire cesser cette atteinte », « Il appartient au prestataire d'hébergement de prendre les précautions nécessaires pour éviter de léser les droits des tiers et de mettre en oeuvre à cette fin des moyens raisonnables d'information, de vigilance et d'action ». Vº Guide Permanent Droit et Internet, E 3.3 Hébergement du site, précité, nº 50, p, 17.

أكَّدت محكمة بداية (نانتير) موقفها هذا بقرار آخر أصدرته في 31 كانون الثاني 2000م، انظر:

TGI de Nanterre (réf.), 31 janvier 2000, Comm. Com. Électr., Juin 2000, nº 6, p. 19, disponible également à l´adresse: www. Legalis.net/jnet/index.htm.

إن التزام متعهد الإيواء بالإعلام يفرض عليه أن يُعلم أصحاب المواقع الإلكترونية المأوية بضرورة احترام القوانين والأنظمة، وعدم الاعتداء على حقوق الملكية الفكرية، ووجوب عدم إلحاق الضرر بالآخرين. بالمقابل، فقد أكَّدت المحكمة عدم التزام متعهدي الإيواء بالكشف عن هويَّة أصحاب المواقع الإلكترونية [1]، وذلك، أولاً، لعدم إمكانيتهم من التأكد من المعلومات التي يُدلي بها الأشخاص عندما يطلبون إيواء مواقعهم، حيث يتم الإدلاء بهذه المعلومات إلكترونياً عن طريق تعبئة نموذج معروض على شبكة الأمن السيبراني، وثانياً، لصعوبة معرفة الرمز التعريفي– IP Internet Protocol للكمبيوتر المُستخدم في إنشاء الموقع الإلكتروني ذي المضمون غير المشروع. إلاَّ أن ذات المحكمة عادت عن موقفها هذا، وقضت في 24 أيار 2000م، بمناسبة دعوى رفعها الاتحاد العام للطلبة اليهود في فرنسا UEJF ضد متعهد الإيواء Multimania نتيجة لإيوائه موقعاً إلكترونياً تضمَّن عرض وبيع أغراض ورموز نازية، بأنه يتوجب على متعهد الإيواء، وبالتعاون مع متعهد الوصول، الكشف عن هويَّة صاحب الموقع الإلكتروني ذي المضمون المعلوماتي غير المشروع أو الضار [2].

ثانياً: استجابة المشرّع

يبدو، من الاتجاه العام لأحكام القضاء السابقة، أنها تميل إلى إلزام متعهدي الإيواء ببذل العناية اللازمة لمنع تداول المضمون أو المعلومات غير المشروعة، وذلك من خلال الجهود اليقظة

---

(1) TGI de Nanterre, 8 décembre 1999, précité, « Aucune obligation légale n’existe en ce domaine (identification de l’éditeur du site lors de l’ouverture de son compte) à la charge du prestataire d’hébergement ». Vº Guide Permanent Droit et Internet, E 3.3 Hébergement du site, précité, nº 28, p, 13.

(1)) TGI de Nanterre (1re Ch.), 24 mai 2000, disponible à l´adresse: www. juriscom.net., voir également sur l´obligation de collaboration et d´information, É. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in M. ANTOINE, A. CRUQUENAIRE et d´autres, Commerce électronique européen sur les rails?, 1re édition, 2001, Bruylant, Bruxelles, n° 526 et s., p. 280 et s., selon le tribunal « L’absence de rigueur générale dans la profession aux niveaux national et international, est palliée par la faculté dont dispose le fournisseur d’hébergement de se faire communiquer par le fournisseur d’accès les éléments certains de l’identité de son client, au terme d’une procédure rapide dont il doit assurer la charge lorsque des tiers sont apparemment lésés ».

التي تتناسب وإمكانياتهم. إلاَّ إن مضمون هذه الجهود ومداها يبقى غامضاً [1]. فنص المادة 6-7/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" والذي جاء متفقاً مع نص المادة 15-1 من التوجيه الأوروبي حول "التجارة الإلكترونية" يمنع فرض التزام عامٍ على متعهد الإيواء "بمراقبة المعلومات التي يتولى نقلها أو تخزينها، أو البحث النشط عن الوقائع والظروف التي تكشف عن الأنشطة غير المشروعة". فبموجب هذا النص يجد متعهدو الإيواء أنفسهم أنهم يُعفون، على السواء، من ممارسة الرقابة السابقة على المضمون المعلوماتي غير المشروع، ومن الصعوبات التقنية والاقتصادية التي تصاحب هذه الرقابة، والتي شكك البعض بفاعليتها. [2]

غير أنه، وبحسب نص الفقرة الثانية من المادة 6-7/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" والتي جاءت متفقةً مع أحكام التوضيح رقم 47 من التوجيه الأوروبي حول "التجارة الإلكترونية": إن عدم فرض التزام عامٍ على متعهد الإيواء بمراقبة المضمون المتداول عبر شبكة الأمن السيبراني، لا يُعفيه من الالتزام بممارسة هذه الرقابة في حالاتٍ خاصة، بمعنى أنه لا يُعفيه من القيام "بنشاط رقابي موجَّه ومؤقت بناءً على طلب السلطة القضائية" [3]. وقد أثار هذا الأمر حفيظة القائمين على هذه الخدمة، ووصل ببعضهم حد القول: بأن هذا الموقف يتَّسم بالتشدد

---

(1) محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، الطبعة الأولى، 2003.

(2) É. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", précité, n° 526 et s., p. 280

(3) المادة 6-7/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، ويقابلها في بلجيكا الفقرة الثانية من المادة 21-1 من القانون الصادر في 2003/3/11م حول "شركات المعلومات" والمادة 3 من بروتوكول التعاون الفرنسي الذي تم توقيعه بين مقدمي خدمات الإيواء ومقدمي خدمات الوصول في 2004/10/14م، وقد جاء توقيع هذا البروتوكول من أجل التأكيد على وجوب تقيُّد مقدمي هذه الخدمات بأحكام القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" ووجوب تعاونهم في منع تداول أيٍّ مضمون غير مشروع عبر شبكة الإنترنت. شبيه من هذا البروتوكول، بروتوكول التعاون الذي تم توقيعه في بلجيكا بتاريخ 1999/5/28م بين مقدمي خدمات الإنترنت ووزارة العدل البلجيكية. لمزيد من التفاصيل حول هذين البروتوكولين، انظر:

Charte des prestataires de services d'hébergement en ligne et d'accès à Internet en matière de lutte contre certains contenus spécifiques, 14/10/2004, disponible en ligne à l´adresse: www.foruminternet.org/texte/documents/chartes-codes-labels /lire. et www.ispa.bi/fr/c040202.html., sur le protocole belge, voir É. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", précité, n° 527 et s., p. 281 et s.

في مواجهتهم، لا سيَّما وأن الفقرة الرابعة من نص المادة 6-1/7، من نفس القانون، تزيد من قسوة هذا الالتزام بوضعها على عاتقهم التزاما من نوع أخر يتمثَّل، من ناحية، في وجوب تأمين الوسائل التقنية اللازمة لمنع نشر مضمون معلوماتي غير مشروع وتداوله عبر شبكة الأمن السيبراني، ومن ناحيةٍ أُخرى، في ضرورة إعداد وسيلة اتصال مفتوحة من شأنها أن تربطهم مباشرةً بمستخدمي الأمن السيبراني، وتُمكِّنهم، في نفس الوقت، من تبليغ السلطات العامة في الدولة عن أيِّ مضمون إلكتروني مخالف للقانون [1].

واتخاذ مثل هذا الموقف من قِبل المشرّع الفرنسي لم يأتِ إلاَّ تطبيقاً لمبدأ أرسته المادة 15-2 من التوجيه الأوروبي حول "التجارة الإلكترونية"، والذي بدوره لم يُغفل التزام متعهد الإيواء بممارسة الرقابة اللاحقة على المضمون المعلوماتي غير المشروع، فسمح للدول الأعضاء بأن تفرض على متعهد الإيواء التزاما بإعلام السلطات العامة في الدولة، وذلك بصورةٍ عاجلةٍ، عن أيَّة نشاطات أو معلومات غير مشروعة، كما طالبهم بالكشف عن البيانات والمعلومات التي تسمح بتحديد شخصية صاحب المضمون[2]. وتطبيقاً لذلك جاءت المادة 6-2 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" لتُؤكِّد على التزام متعهد الإيواء بطلب البيانات والمعلومات الخاصة بعملائه، والاحتفاظ بها من أجل اطلاع السلطة القضائية عليها عند الطلب، وهذا الالتزام هو التزام تبادلي، بمعنى أن صاحب المضمون يلتزم من جهته بتزويد متعهد الإيواء بالبيانات والمعلومات المطلوبة، والتي تسمح بتحديد هويته، وبالمقابل على متعهد الإيواء، وفقاً لنص المادة 6-1/3 و2 من القانون

(1) Luc GRYNBAUM, "LCEN. Une immunité relative des prestataires de services Internet", précité, nº 15, p 39.

(2) É. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", précité, n 527 et s., p. 280 et s.

الفرنسي الاحتفاظ بها سرية وعدم إساءة استخدامها وعدم الكشف عنها إلا للضرورة [1]. وقد أناطت الفقرة الخامسة من نص المادة 6–2، من نفس القانون، بمجلس الدولة تبنِّي نظام قانوني غايته تحديد البيانات والمعلومات الواجب على متعهد الإيواء حفظها وتحديد مدة هذا الحفظ وطريقته. وفي انتظار اتخاذ المجلس لهذه الخطوة، ومن أجل سدِّ الفراغ القانوني الحاصل في هذا المجال، لم يكن أمام المحاكم الفرنسية وأمام القائمين على هذه الخدمة من سبيلٍ سوى اللجوء إلى القواعد العامة في قانون الإجراءات المدنية. فاستناداً لنص المادتين: 809 و872 من قانون أصول المحاكمات المدنية الفرنسي الجديد لرئيس محكمة البداية، بصفته قاضي الأمور المستعجلة اتخاذ الإجراءات الملائمة لحفظ أدلة الإثبات.[2]

وتطبيقاً لذلك، أوضحت محكمة بداية باريس في قرارها الصادر في 2 شباط 2004م أن متعهد الإيواء، الذي يُزوِّد قاضي الأمور المستعجلة باسم صاحب المضمون غير المشروع، وعنوانه البريدي والإلكتروني ورمزه التعريفي، يُعدُّ مستجيباً لقرارها القاضي بطلب الكشف عن البيانات والمعلومات الشخصية لصاحب المضمون[3].

ولا شك أن كشف البيانات والمعلومات الشخصية يتعارض مع رغبة مستخدمي الأمن السيبراني في التخفي، ومع اتجاههم العام بضرورة ترك شبكة الأمن السيبراني مجالاً مفتوحاً لحرية التعبير. إلا إننا نؤكد هنا أن الرغبة في التهرب من عالم الواقع إلى عالم الافتراض والحريَّة الشخصية لا يُمكن أن يكوِّنا وسيلةً لارتكاب المخالفات والجرائم عبر الأمن السيبراني؛ فحرية تعني مسؤولية، والمطلوب إذن هو إقامة التوازن بين وجوب طلب البيانات التي تسمح بتحديد شخصية العملاء

(1) E. CAPRIOLI, "Responsabilité des prestataires du commerce électronique et conservation de données aux fins de traçabilité", 2003, p. 2 et s, disponible à l´adresse: www.caprioli-avocats.com.

(2) Luc GRYNBAUM, "LCEN. Une immunité relative des prestataires de services Internet", précité, n° 12, p. 39.

(3) TGI Paris, (Réf.,), 2 février 2004, Comm. Com. Électr., mars 2004, Comm., p. 29.

والاحتفاظ بها بسريَّة، وعدم الكشف عنها إلا للضرورة [1]. فلا نستطيع، والحال كذلك، إلا أن نقبل بهذا الحد الأدنى من الالتزامات الملقاة على عاتق متعهدي الإيواء. إذا كان هذا هو حال متعهدي الإيواء، فما هو الوضع بالنسبة لمورِّد المعلومات؟

الفرع الثاني: التزامات مورد المعلومات

مورِّد المعلومات هو صاحب السلطة الحقيقية في مراقبة المادة المعلوماتية التي تُبث عبر الأمن السيبراني؛ لأنه هو من يقوم بجمعها أو تأليفها، وبالتالي يقع على عاتقه توريد مادة معلوماتية مشروعة وحقيقية [2]. وعليه، يتعين على مورِّد المعلومات، الحريص على أداء دوره في إدارة شبكة الأمن السيبراني بمسؤولية وشفافية، إبلاغ السلطات المختصة في الدولة عن أيِّ نشاطٍ معلوماتي غير مشروع، كما يتوجَّب عليه الكشف عن هويَّة جميع القائمين على المضمون المعلوماتي المورَّد عبر الأمن السيبراني، وهو ما يدخل تحت باب التزامه بممارسة عمله بشفافية (أولاً). وكذلك يتوجب على مورِّد المعلومات السماح للجمهور بممارسة حق الرد (ثانياً).

أولاً: الالتزام بالشفافية

لكونه ناشراً للمعلومات على الموقع الإلكتروني، وبالتالي صاحب القدرة الفعلية في السيطرة عليها والتحكُّم في نشرها، يتحمَّل مورِّد المعلومات المسؤولية بالدرجة الأولى عن مضمون الرسائل، والمعلومات، والصور التي يبثها [3]. فهو ملتزم مثل مورِّد المضمون المعلوماتي التقليدي بمراقبة المضمون المعلوماتي الذي يصل إليه، وسلطة المراقبة هذه تتفق مع طبيعة عمله كناشر إلكتروني للمادة المعلوماتية. وبالنظر إلى طبيعة عمله، فإنه مُلزم بإخطار السلطات المختصة في الدولة عن

---

(1) في نفس هذا الاتجاه، انظر: محمد حسين منصور، المرجع السابق، ص 208.

(2)) Guide Permanent Droit et Internet, E 3.13, Responsabilité de l´éditeur, précité, nº 1, p.4.
وأيضاً عبد الحي بيومي حجازي، المرجع السابق، ص 353، محمد حسين منصور، المرجع السابق، ص 199 و218.

(3) Guide Permanent Droit et Internet, E 3.13, Responsabilité de l´éditeur, précité, nº 6, p.6

أيِّ نشاط إلكتروني غير مشروع، وذلك من خلال مدير النشر المسؤول، فيتعيَّن عليه إذن تعيين شخص طبيعي مديرٍ للنشر. فضلاً عن ذلك وتطبيقاً لمبدأ الشفافية، يتوجَّب على مورِّد المعلومات اطلاع مستخدمي الأمن السيبراني ومتعهدي الوصول والإيواء على البيانات والمعلومات التي تُعرِّف به وبالنشاط الإلكتروني الذي يُديره. ومن عناصر التعريف التي يلتزم مورِّد المعلومات تقديمها:

– إذا كان مورِّد المعلومات شخصاً طبيعياً، يجب عليه التعريف باسمه، وكنيته، وعنوانه، أمَّا إذا كان شخصاً معنوياً فيلتزم بالتعريف باسم الشخص المعنوي، وطبيعة نشاطه، ومركز إدارته الرئيسي.

– على مورد المعلومات، أيضًا، تعيين مدير للنشر، وعند الضرورة رئيساً للتحرير، وعليه كذلك، طبقاً لنص المادة 6–1/3 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، الكشف عن اسم متعهد الإيواء ولقبه، أو عنوانه ومركز إدارته الرئيسي.

إن هذه العناصر يجب أن تكون ظاهرة للعيان ومنشورة على الصفحة الرئيسية للموقع الإلكتروني، أو على الأقل من الممكن الوصول إليها، من خلال الضغط على أيقونة، أو إشارة، أو علاقة معينة أُعدَّت خصيصاً لهذا الغرض[1]. كذلك يتوجب على مورد المعلومات تأمين الوسائل التقنية اللازمة للتعريف بصاحب المضمون غير المشروع. ومن المؤكد أن ذلك لا يُثير لمورِّد المعلومات أيَّة إشكاليات نظراً لوجود رمز تعريفي (IP) واسم موقع إلكتروني لكل حاسب آلي مرتبط بشبكة الأمن السيبراني[2]. ونُنوِّه هنا إلى أن التعامل مع هذه البيانات والمعلومات، بحسب نص

(1) Guide Permanent Droit et Internet, E 3.13, Responsabilité de l´éditeur, précité,nº 19, p.11.

(2) M. GUILLARD, "Responsabilité des acteurs techniques de l´internet", précité, p. 26 et s., Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, précité, nº 49, p. 20

الفقرة الثانية من المادة 6-2/3 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، لا بد أن يتم بسريَّة بالغة، ويجب عدم الكشف عن هذه المعلومات إلا للضرورة.

ثانياً: الالتزام بإتاحة حق الرد

وفقاً لنص الفقرة الثانية من المادة 6-2/3 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، يتمتع كل شخص طبيعي أو معنوي بحق الرد على أيَّة مادة معلوماتية منشورة على شبكة الأمن السيبراني، تمس بشرفه، أو بسمعته، أو تنتهك حقوقه. ويجب عليه أن يُقدم هذا الرد إلى مدير النشر المسؤول خلال مدة أقصاها ثلاثة شهور تبدأ من تاريخ وقف بث المضمون غير المشروع على شبكة الأمن السيبراني، وليس من تاريخ بدء البث. كذلك يقع على عاتق مورِّد المعلومات التزام عامٍ بتأمين الوسائل التقنية والمعلوماتية اللازمة لتمكين الشخص المضرور من ممارسة هذا الحق، وبالتالي من نشر رده مباشرةً على شبكة الأمن السيبراني[1]. كما يجب عليه، وفقاً لنص المادة 6-2/4 و3 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، وتحت طائلة المسؤولية، تمكين الشخص المضرور من المطالبة بتصحيح أو حتى بشطب المادة المعلوماتية غير المشروعة من على صفحات الويب.

غير أنه ليس من العدل إلقاء كامل المسؤولية على مورد المادة المعلوماتية غير المشروعة وحده، فهناك أكثر من شخص يتدخَّل في العملية، ومن الممكن بالتالي قيام مسؤوليتهم في حال ثبوت خرقهم لأيٍّ من الالتزامات الملقاة على عاتقهم، ومن هؤلاء الأشخاص الذين يقدِّمون الخدمة الفنية.

(1) Th. VERBIEST et P. REYNAUD, "Comment exercer un droit de réponse sur l´internet?", disponible à l´adresse: www.droit-technologie.org, 22 mai 2006, p. 2.

المطلب الثاني
التزامات مقدمي الخدمة الفنية

مقدمو الخدمة الفنية هم أشخاص طبيعيون، أو معنويون، يقومون بدور فني بحت لربط شبكات الاتصال من ناحية، ولتوصيل الجمهور إلى شبكة الأمن السيبراني من ناحيةٍ أُخرى، ويتم ذلك بموجب عقدين مختلفين: الأول: يتمثَّل في عقد نقل المعلومات، ويتولَّى الناقل بمقتضاه عملية الربط الفني بين شبكات الاتصال (أولاً)، في حين يهدف الثاني، من خلال متعهد الوصول، إلى تأمين توصيل العميل إلى الموقع الإلكتروني المنشود (ثانياً).

الفرع الأول: التزامات ناقل المعلومات

إن عملية نقل المعلومات عبر الأمن السيبراني تقتضي، كما رأينا سابقاً، ربط حاسبات مستخدمي الشبكة بالمواقع الإلكترونية، وذلك من خلال الربط المادي لشبكات الاتصال عن بُعد. ويلتزم ناقل المعلومات، بموجب عقد النقل الذي يربطه بعملائه، بتقديم الوسائل التقنية والفنية اللازمة لعملية النقل المادي للمضمون المعلوماتي. فناقل المعلومات هو كل شخص طبيعي، أو معنوي، يستغل شبكة الاتصالات عن بُعد لإيصال المادة المعلوماتية إلى الجمهور[1]. وهذا ما مكننا من تشبيهه بساعي البريد، فدورهما ينحصر في النقل المادي للمعلومات بين الوحدات المختلفة، ولا يُفترض به مراقبة المعلومات التي تمر عبر شبكته، ولا يكون بالتالي مسؤولاً عن عدم مشروعية المادة المعلوماتية المتداولة. لا بل أكثر من ذلك، إن ناقل المعلومات مُطالب بالحفاظ

(1) انظر: عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2003م، ص 339 وما بعدها، محمد حسين منصور، ص 196 وما بعدها.

على سرية المعلومات التي تمر من خلال شبكته، ومُطالب، أيضًا، بالحياد التام تجاه المضمون المعلوماتي المنقول[1].

ولكن، هل يبقى الحال كذلك فيما لو علم ناقل المعلومات بعدم مشروعية الرسائل والمعلومات المقدمة؟ إن علم الناقل بأوجه عدم المشروعية للمضمون المعلوماتي وبالرغم من ذلك نقله له عبر شبكته، يُشكِّل إخلالاً بالتزامه بضمان احترام نصوص النظام العام، وبواجب الحرص على عدم المساس بحقوق الآخرين[2].

ويثور التساؤل هنا حول مدى شرعية النسخ المؤقت للمضمون المعلوماتي المنقول والذي يقوم به ناقل المعلومات كجزءٍ من عمله، وكخطوة تمهيدية وضرورية لنقل الرسائل والمعلومات عبر شبكة الأمن السيبراني، وفقاً لنص المواد 1-3/1 و 2-2/1 من القانون الفرنسي الصادر في 1 آب 2006م[3]، و5-1/أ وتوضيحها رقم 33 من التوجيه الأُوروبي الصادر بتاريخ 22 أيار 2001م[4] والمتعلِّقين ب "حق المُؤلِّف والحقوق المجاورة له في مجال المعلوماتية"، إن عملية النسخ المؤقَّت لا تُشكِّل انتهاكاً لحق المؤلِّف والحقوق المجاورة له، بشرط انحصار العملية في نطاق وحدود وضرورة إيصال المعلومات كما هي دون إجراء أيِّ تعديلٍ أو تحديثٍ عليها من قِبل ناقل المعلومات؛ أي دون التأثير على حق مؤلِّف المضمون، خاصةً إذا ما التزم الناقل بسحب النسخة التي تم تخزينها

---

(2) محمد حسين منصور، المرجع السابق، ص 197، انظر أيضاً:

Pierre TRUDEL, La responsabilité civile sur Internet selon la loi concernant le cadre juridique des technologies de l'information, 2001, p. 18, disponible à l'adresse www.crdp.umontreal.ca/cours/drt6929f/Resp.

(3) T. Com., Paris, 14 septembre 1992, Les Petites Affiches, 20 novembre 1992, note C. HAISY

كما ورد في محمد حسين منصور، المرجع السابق، ص 198.

(3) Loi 2006-961 du 1er août 2006 relative au droit d´auteur et aux droits voisin dans la société de l´information, JO, n° 178 du 3 août 2006, p. 11529.

(4) Directive du 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur "l´harmonisation de certains aspects du droit d´auteur et des droits voisins dans la société de l´information", Journal Officiel des Communautés européennes, 22/6/2001, L. 167/10.

بشكل مؤقَّت، وبمنع الوصول إليها في حال أن علم بصدور قرار قضائي أو إداري يقضي بعدم مشروعية المضمون المُخزَّن[1]. ويُمكننا أن نلاحظ، بهذا الصدد، أن آلية عمل ناقل المعلومات قريبة جداً من آلية عمل والتزامات متعهد الوصول والتزاماته.

الفرع الثاني: التزامات متعهد الوصول

نظراً لارتباطه الدائم بشبكة الأمن السيبراني ولطبيعة الخدمة التي يقدمها، يُعدُّ متعهد الوصول واحداً من أهم مقدمي الخدمات في العالم الافتراضي. فنشاطه الرئيسي يتمحور في تزويد مشتركيه بالوسائل الفنية اللازمة لربطهم بشبكة الأمن السيبراني، ولإبحارهم فيها بحريَّة ولوصولهم إلى المواقع الإلكترونية التي يريدون الاطلاع على مضمونها. ومتعهد الوصول هو كل شخص طبيعي، أو معنوي، يستغل شبكات الاتصال عن بُعد في سبيل إيصال عملائه بشبكة الأمن السيبراني، وذلك بموجب "عقد تقديم خدمات الدخول". لذا يُفترض بمتعهد الوصول المسؤول احترام التزاماته الجوهرية، الإعلامية منها (أولاً)، والتقنية (ثانياً).

أولاً: التزامات ذات طبيعة إعلامية

وفقاً لأحكام القانون والقضاء، يتوجب على متعهدي الوصول ممارسة عملهم بكل شفافية ووضوح، وبما يتلاءم مع مقتضيات حسن النية، ومن أجل تحقيق ذلك، ألزمت هذه الأحكام متعهدي الوصول بلعب دور إعلامي إيجابي في ادارة شبكة الأمن السيبراني ، وأقامت مسؤوليتهم على عدم أدائه، وعليه فقد أصبح لزاماً على متعهدي الوصول، من ناحية، إعلام مستخدمي الشبكة بالبيانات والمعلومات الخاصة بهم وبالمشتركين معهم، ومن ناحيةٍ أخرى، تبصرة المشتركين

(1) انظر في هذا الصدد، محمد حسين منصور، المرجع السابق، ص 199، وكذلك نص المادة 13، الخاصَّة بـ (forme de stockage dite "caching")، من التوجيه الأوروبي حول "التجارة الإلكترونية".

Pierre TRUDEL, "La responsabilité civile sur Internet selon la loi concernant le cadre juridique des technologies de l’information", précité, p. 20.

بمخاطر الإبحار عبر الأمن السيبراني، وإعلامهم بوجوب احترام القوانين والأنظمة السارية، وبعدم الاعتداء على حقوق الغير أثناء هذا الإبحار[1].

وفيما يخص التزام متعهدي الوصول بالإعلام، أو الكشف عن البيانات والمعلومات الخاصة بهم وبالمشتركين معهم، فمن المعلوم أن القواعد العامة في التعاقد تُوجب تحديد هويَّة المتعاقدين، ولم يخرج عقد تقديم خدمات الدخول عن هذه القاعدة. إلا إن عملية إبرام هذا النوع من العقود وطرق تنفيذه عادةً ما تتم عن طريق الأمن السيبراني، الأمر الذي ينتج عنه بعض الصعوبات في تحديد هوية أطرافه. لذا، يتعيَّن على متعهد الوصول، الذي يعرض خدماته على طائفة المستهلكين أو المهنيين، احترام القواعد العامة في حماية المستهلك وقواعد القانون التجاري التي تفرض على كل شخص، يتَّخذ من تقديم خدمات الأمن السيبراني مهنةً له التعريف بنفسه لجمهور المتعاملين. فوفقاً لنص المادتين:[2] 5 من التوجيه الأُوروبي حول "التجارة الإلكترونية"، و6-3/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي": على متعهد الوصول الكشف لعملائه، على الأقل، عن اسمه وعنوانه البريدي والإلكتروني، ومكان ورقم قيده التجاري. فالاطِّلاع على هذه المعلومات يُضفي حمايةً فعَّالة على جمهور المتعاملين عند إخلال متعهد الوصول بأيٍّ من التزاماته.

وفي المقابل، يقع على عاتق متعهد الوصول، وفقاً لنص المادتين: 15-2 من التوجيه الأُوروبي حول "التجارة الإلكترونية"، و6-2 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي":

---

(1) محمد حسين منصور، المرجع السابق، ص209.

(2) Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, précité, nº 17, p. 8.

انظر في هذا الصدد:

TGI Paris, ord.réf., 17 janvier 2003 et CA Paris, 4ème ch., 7 juin 2006, disponibles à l'adresse www.legalis.net, rubrique responsabilité, « Les fournisseurs qui détiennent, pour mise à disposition du public, les messages de toute nature sont tenus de détenir et conserver les données d'identification de toute personne ayant contribué à la création du site litigieux, afin de répondre à toute réquisition judiciaire ».

وبمقتضى أحكام القضاء الفرنسي[1]الطلب من عملائه، وذلك في المرحلة ما قبل التعاقدية، تقديم جميع البيانات والمعلومات الشخصية التي تُمكِّنه من تحديد هويَّة العميل، وأهليته، وعنوانه البريدي والإلكتروني. كما يتوجب عليه، وفقاً لنص الفقرة الثانية من المادة 6-2 من القانون الفرنسي أعلاه، تحديد آلية جمع هذه المعلومات، أي؛ الوسيلة التي يُمكن للعميل من خلالها تزويد متعهد الوصول بالبيانات والمعلومات المطلوبة. ويثور السؤال هنا حول كيفية تأكد متعهد الوصول من صدق البيانات والمعلومات المقدمة من قِبل العميل، في حال أن أخلَّ هذا الأخير بالتزامه بعدم خرق القوانين والأنظمة السارية، وباحترام حقوق الآخرين على شبكة الأمن السيبراني، خاصةً أن تقديمها يتم عن طريق الأمن السيبراني.

أما فيما يتعلَّق بمدَّة حفظ البيانات والمعلومات وآلياتها، فمن المتوقَّع، طبقاً لنص الفقرة الخامسة من المادة 6-2 من نفس القانون، أن يصدر قريباً نظامٌ لتحديد ذلك. ولحين صدور هذا النظام، فإنه لا مناص أمام القضاء الفرنسي من الاستمرار في أعمال القواعد العامة الخاصة بحفظ البيانات والمعلومات بشكلٍ عام من قِبل مقدمي خدمات الاتصال. وتطبيقاً لذلك، فإن المادة 32-3 بفقرتيها الأولى والثانية من قانون البريد والاتصالات عن بُعد، والذي تمَّ تعديله في 15 تشرين الثاني 2001م [2] تنص على أن مدَّة حفظ البيانات والمعلومات المقدمة لمتعهدي خدمات الاتصال يجب ألا تتجاوز، في حدِّها الأقصى، السنة الواحدة.

---

(1) انظر في هذا الصدد:

TGI Paris, ord.réf., 17 janvier 2003 et CA Paris, 4ème ch., 7 juin 2006, disponibles à l'adresse www.legalis.net, rubrique responsabilité, « Les fournisseurs qui détiennent, pour mise à disposition du public, les messages de toute nature sont tenus de détenir et conserver les données d'identification de toute personne ayant contribué à la création du site litigieux, afin de répondre à toute réquisition judiciaire ».

(2) Loi n° 2001-1062, 15 novembre 2001 relative à la sécurité quotidienne, JO, 16 novembre 2001.

ومن ناحيةٍ أُخرى، يُوجب القضاء الفرنسي على متعهدي الوصول، وذلك تنفيذاً لعقد تقديم خدمات الدخول، تبصرة العملاء بالمخاطر التي من الممكن أن يتعرضوا لها خلال عملية إبحارهم في عالم الأمن السيبراني ودخولهم إلى مواقع إلكترونية معينة أو التعامل معها. كما يضع على عاتقهم الالتزام بإعلام عملائهم بضرورة احترام القوانين والأنظمة السارية، ووجوب عدم استخدام شبكة الأمن السيبراني كوسيلة للاعتداء على حقوق الغير[2]. كذلك يتوجب على متعهدي الوصول، وفقاً لنص المادة 3/14 من التوجيه الأوروبي حول "التجارة الإلكترونية"، وانطلاقاً من مبدأ حُسن النية في إدارة شبكة الأمن السيبراني، التعاون مع جميع المعنيين بالخدمات المقدمة على الشبكة من جهات إدارية وقضائية، ومن جمهور المستخدِمين، ومن العاملين في قطاع خدمات الأمن السيبراني. ويأتي هذا الالتزام مكمِّلاً لالتزاماته الأخرى ذات الطبيعة التقنية.

ثانياً: التزامات ذات طبيعة تقنية

سبق أن أوضحنا بأن متعهد خدمات الوصول يقوم بدور فني بحت، يكمن في توصيل عملائه بشبكة الأمن السيبراني، وفي فتح الطريق أمامهم للوصول إلى المعلومات المطلوبة دون أن يكون له أيَّة علاقة بالمادة المعلوماتية المنقولة، أو بمضمونها، أو بموضوع الرسائل المتبادلة عبر الأمن السيبراني. فدوره يتميَّز بالحياد التام وليس له حق الاطِّلاع على مضمون المعلومات التي تمر من خلاله ولا يُمكن بالتالي تحميله المسؤولية عن مضمون الرسائل المتبادلة، أو عن طبيعة المادة المعلوماتية المقدمة، إلا ضمن شروط مُعيَّنة. [1]

(1) النقروز، علي (2017) جرائم نظم المعلومات، دار السناء للنشر، الأردن، عمان، ص 335.

(2) Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, précité, nº 41 et 44, p. 17 et 18.

وأيضاً محمد حسين منصور، المرجع السابق، ص 210.

جاءت أحكام القضاء الفرنسي في هذا المجال لتؤكِّد هذا الدور ولتُقرِّر انحصار دور متعهد الوصول في تأمين نقل البيانات والمعلومات بطريقة فورية. وبالتالي، لا يقع على عاتقه التزام عام بمراقبة مضمون المادة المعلوماتية التي تمر من خلاله [1]. وتمَّ تبنِّي نفس الموقف من قِبل مجلس الدولة الفرنسي والذي أعلن صراحةً في تقريرٍ له صدر عام 1998م إعفاء متعهد الوصول من واجب الرقابة السابقة للمضمون المعلوماتي الذي يمر من خلاله. وقد حاول بعضهم إقامة التوازن ما بين مبدأين أساسيين: أولهما الحياد التام لمتعهدي الوصول، وثانيهما واجب أخذ الحيطة والحذر الذي يتعيَّن على كل مهني مراعاته.[2]

المشرّع الأوروبي بدوره لم يشذ عن هذا الموقف، فقد أعلن في المادة 15-1 من التوجيه الأوروبي حول "التجارة الإلكترونية" أنه يحظر على الدول الأعضاء فرض التزام عامٍ على مقدمي خدمات الأمن السيبراني برقابة المعلومات التي يتولُّون نقلها أو تخزينها، أو التزام بالبحث النشط عن الوقائع والظروف التي تكشف عن الأنشطة غير المشروعة. وباعتبار فرنسا إحدى الدول الأعضاء في الاتحاد الأُوروبي كان لزاماً على المشرّع الفرنسي تبنِّي موقف مطابق لموقف المشرّع الأُوروبي، وتم ذلك بالفعل، فجاء نص المادة 6-7/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" ليضع على عاتق متعهدي الوصول التزاما بالحياد التام فقط، وبالتالي عدم التدخُّل في مضمون المادة المعلوماتية المنقولة، مع ما يتطلَّبه ذلك، بحسب نص المادة 6-2/3 من نفس القانون، من وجوب المحافظة على سرِّية الاتصالات، وعدم الكشف عن مضمونها إلاَّ للسلطة القضائية المختصة عند الضرورة.

---

(1) Cour de Cassation Criminelle (محكمة النقض الجزائية), 15 novembre 1990, Bulletin criminelle, n° 388, 1990, CA Pau, 1re Ch., 14 octobre 1999, précité, Tribunal du Commerce de Paris, ord. Réf., 14 mars 2001, Revue fiduciaire, 2001, p. 16.

(2) السحيباني، عبدالله (2011): كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية. ص 427.

غير أنه، وفقاً لنص الفقرة الثانية من المادة 6-7/1 من القانون الفرنسي، والتي جاءت متفقةً مع أحكام التوضيح رقم 47 من التوجيه الأُوروبي حول "التجارة الإلكترونية"، إن التزام متعهدي الوصول بالحياد التام لا يُعفيهم، لا من الالتزام بممارسة الرقابة الموجَّهة والمؤقَّتة للمعلومات التي تمر من خلالهم، بناءً على أمرٍ صادرٍ من السلطة القضائية المختصة، ولا، بحسب نص الفقرة الرابعة من نفس المادة، من واجب تبليغ السلطات العامة في الدولة عن أيٍّ مضمون إلكتروني غير مشروع.

نوعٌ آخرٌ من الالتزامات يقع على عاتق متعهدي الوصول، يتمثَّل في وجوب اقتراحهم على عملائهم الوسائل الفنية اللازمة لمنع الوصول إلى بعض المواقع الإلكترونية المشبوهة. فالمادة 6-1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" تُلزم هؤلاء المتعهدين بتزويد المشتركين بالوسيلة الفنية التي تسمح لهم، إن أرادوا ذلك، بفرض نوع من الرقابة الذاتية على أنفسهم أو على أفراد أُسرهم في هذا المجال. ومن الوسائل التي يقترحها متعهدو الوصول على عملائهم، في سبيل تحقيق هذا الغرض، تلك المتعلِّقة بتقنية تصفية أو تنقية (Filtrage) المعلومات الإلكترونية. فمن خلال هذه التقنية يُمكن للعملاء إجراء عملية فلترة للمعلومات الواردة عبر متعهد الوصول الخاص بهم، بحيث لا يتم استقبال إلاَّ تلك التي تتفق مع قيمهم ومعاييرهم الدينية والأخلاقية، والثقافية...[1]

وتطبيقاً لذلك، حكمت المحكمة العليا في أمريكا في 22 حزيران 1998م في دعوى أقامها المواطن Kenneth ZERAN، والذي وقع ضحية مزاح صدر من شخص مجهول الهويَّة، قام بالنشر على صفحات إحدى المواقع الإلكترونية عن رغبته ببيع قمصان يمتلكها مطبوعٌ عليها شعارات متصلة بالحادث المأساوي لمدينة Oklahoma الأمريكية، والتي انفجرت في أحد أحيائها

(1) محمد حسين منصور، المرجع السابق، ص 209.

قنبلة أودت بحياة المئات من الأشخاص. وحيث إنه لم يكن بالإمكان تحديد هويَّة ناشر الخبر، توجَّه ZERAN إلى القضاء، وأقام دعوى تعويض ضد متعهد الوصول AOL مستنداً إلى أنه كان يعلم بمضمون الرسالة المتداولة عبر الأمن السيبراني، ولكنه لم يتَّخذ الإجراءات اللازمة للحيلولة دون وصولها إلى العملاء، مما ألحق ضرراً معنوياً فادحاً بهم. وقضت المحكمة في هذا الصدد بعدم إمكانية مساءلة شركة AOL بصفتها متعهداً للوصول عن المعلومات التي قام الآخرون ببثِّها من خلالها. كذلك رفضت المحكمة في قرارها الصادر، وللمرَّة الأولى، إقامة أي تشابه بين متعهد الوصول ومحرري الصحافة المرئية والمكتوبة، وذلك لأن سرعة انتقال المعلومات عبر شبكة الأمن السيبراني تجعل من المستحيل إخضاعها للرقابة الفعلية [1].

أما في فرنسا، فقد ثار الموضوع بمناسبة الدعوى التي رفعها اتِّحاد الطلاب اليهود أمام قاضي الأمور المستعجلة لمحكمة بداية باريس ضد عدد من متعهدي الوصول، الذين سمحوا بنشر عدد من الخطابات والإشارات العنصرية المُعادية للساميَّة على شبكة الأمن السيبراني. وطالب اتِّحاد الطلاب القاضي الفرنسي بإصدار قرارٍ يُلزم فيه متعهدي الوصول بشطب المادة المعلوماتية المذكورة من على صفحات الويب، أو على الأقل منع وصول العملاء إليها، بصرف النظر عن موقعها على الأمن السيبراني. ونظراً لاتصاف طلبهم هذا بالعمومية وعدم الدِّقة، ونظراً لاستحالة تحقيقه من الناحية الفنية، لعدم إمكانية مراقبة ملايين الرسائل التي تُبث يومياً عبر الشبكة، جُوبه طلبهم بالرفض من قبل القاضي الفرنسي، وقد أعلن القاضي الفرنسي في هذا الصدد، في قراره

(1) Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain, United States Government Accountability Office, Sept. 2007. pp100-112.

الصادر في 20 تشرين الثاني 2000م، عدم التزام متعهد الوصول بالمراقبة الفعلية للمضمون المعلوماتي الذي يعبر من خلاله. [1]

ولو تتبَّعنا قرار المحكمة الفرنسية السابق لوجدنا أنها قد أعلنت صراحةً أن تدخُّل متعهد الوصول في تنقية المعلومات التي تمر من خلاله لا يُمكن أن يتم إلاَّ بأمرٍ من السلطة القضائية المختصة. والحكمة من ذلك، باعتقادنا، هي تفادي أن تدخل مزاجية متعهد الوصول في شطب أو منع وصول مستخدمي الأمن السيبراني إلى معلومةٍ أو أُخرى، دون وجود أدنى رقابة. ومن هنا، جاء نص المادة 6-1/8 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي " ليُقرِّر بأن السلطة القضائية هي الوحيدة المخوَّلة بتحديد عدم مشروعية المضمون الإلكتروني المتداول عبر شبكة الأمن السيبراني، وبالتالي شطبه أو منع وصوله للمشتركين. ومُؤدى هذا الموقف أن قيام متعهدي الوصول بشطب المادة المعلوماتية المتداولة عبر الأمن السيبراني، أو بمنع الوصول إليها دون وجود قرارٍ قضائي يسمح بذلك، يُشكِّل مخالفة قانونية تستوجب المساءلة. فمخالفة الالتزام يُقابله قيام المسؤولية. وعليه، فإن دراسة النظام القانوني لمقدمي خدمات الأمن السيبراني لا يُمكن أن تكتمل إلاَّ بتحديد مسؤوليتهم عن المخالفات المرتكبة عبر الشبكة.

(1) TGI Paris, ord.réf., 22 mai 2000 et 11 août et 20 novembre 2000, (UEJF) c/Yahoo, Communication et commerce électronique, décembre, 2000, p. 25, note J.-C. GALLOUX.

المبحث الثاني

مسؤولية مقدمي خدمات الأمن السيبراني عمّا يحدث من مخالفات عبر الشبكة

إن تحديد مسؤولية مقدمي خدمات الأمن السيبراني يُعدُّ من أصعب المواضيع الممكن مواجهتها. ومرد ذلك عدَّة أسباب: أولها: الطابع الفني المعقَّد للشبكة، وثانيها: عالمية النشاط الإلكتروني غير الخاضع لسيطرة دولة معينة أو لإدارة مركزية، وثالثها: تعدُّد الهيئات التي تعرض خدماتها في هذا المجال، ورابعها: وجود كم هائل من المتدخِّلين في تسيير هذه الشبكة... والتساؤل الذي يثور هنا هو مدى مسؤولية كل متدخِّل عن السلسلة المعلوماتية المتواصلة عبر الأمن السيبراني. فإذا كان هناك إجماع على تحقُّق مسؤولية صاحب المعلومة، أو منتجها، أو مؤلِّف الرسالة التي تُبث عبر الأمن السيبراني عن كل ما تتضمنه من مخالفة للقوانين، أو أُمور غير مشروعة، أو ما قد تُسببه من أضرار للآخرين، إلاَّ إن الأمر يُثير الجدل حول مسؤولية القائمين على إدارتها من مقدمي خدمات الأمن السيبراني[1].

إن الحقيقة الواضحة أمامنا تقودنا إلى القول بأن هذا الجدل لا يُمكن أن يُؤدِّي بأيِّ شكلٍ من الأشكال إلى استبعاد مسؤولية مقدمي الخدمات، بحيث يُصبح الممنوع مشروعاً. والواقع أن مسؤوليتهم يُمكن أن تجد أُسساً مختلفة، كالإخلال بالتزام تعاقدي، أو انتهاك حقوق الملكية الفكرية، أو إفشاء أسرار مهنية، أو المساس بحرمة الحياة الخاصة، أو عبارات السب والقذف. فإزاء هذه المخالفات المتعددة يثور السؤال حول الطريقة الأنسب لمعالجتها. فهل من الأمثل الأخذ بعين الاعتبار خصوصية بعض المخالفات، كتلك المتعلقة بحقوق الملكية الفكرية مثلاً، وبالتالي

(1) محمد حسين منصور، المرجع السابق، ص 185 و196.

تخصيص النصوص القانونية لمعالجة كل مخالفة وحدها؟ أم من الأفضل وضع قواعد عامة للمسؤولية عن المخالفات المرتكبة على الأمن السيبراني بصرف النظر عن مضمونها [1]؟

على خلاف القانون الأمريكي الصادر في 28 تشرين الأول 1998م للحد من الاعتداءات على حقوق الملكية الفكرية في نطاق الأمن السيبراني والمسمَّى بـ Digital Millenium Copyright Act (DMCA)، والذي خصص الباب الثاني منه لتحديد مسؤولية مقدمي خدمات الأمن السيبراني عن التعدي على هذه الحقوق، فحماهم من بعض دعاوى التقليد والتزييف، واشترط لقيام مسؤوليتهم في هذا المجال تحقق شروط معينة، ترك التوجيه الأُوروبي حول "التجارة الإلكترونية" الخيار للدول في هذا المجال. فعملت أغلب الدول الأُوروبية على تبني اتجاه عامٍ، مُؤدَّاه وضع قواعد عامة للمسؤولية على الأمن السيبراني دون أيِّ تخصيص[2]. فجاء القانون الفرنسي الصادر في 21 حزيران 2004م حول "الثقة في الاقتصاد الرقمي"، والقانون البلجيكي الصادر في 11 آذار 2003م حول "التجارة الإلكترونية"، والقانون الألماني الصادر في 22 تموز 1997م وتعديلاته حول "الاتصالات عن بُعد" وغيرها من قوانين الدول الأُوروبية، لتُنظِّم مسؤولية مقدمي خدمات الأمن السيبراني من خلال تبنِّي قواعد عامة، دون إجراء أيَّة تفرقة بين نوعيَّة المخالفات المرتكبة باستخدام الشبكة. فتمَّ بذلك، للمرَّة الأولى وبشكلٍ كُلِّي، تحديد نطاق هذه المسؤولية (المطلب الأول)، وشروط تحقُّقها (المطلب الثاني)، وأساسها القانوني (المطلب الثالث).

---

(1) المرجع السابق نفسه، ص 188 و

A. LUCAS, J DEVÈZE et J. FRAYSSINET, Droit de l´informatique et de l´internet, 1 éd., 2001, PUF, Paris, n° 699, p. 451.

(2) Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain, United States Government Accountability Office, Sept. 2007 . P312

المطلب الأول
نطاق مسؤولية مقدمي خدمات الأمن السيبراني

لا تختلف طبيعة مسؤولية مقدمي خدمات الأمن السيبراني باختلاف نوعيَّة المخالفات المرتكبة على الأمن السيبراني، ولكن باختلاف مضمونها. فقد تكون هذه المسؤولية جزائية إذا تضمَّن المضمون الإلكتروني على ما يُدخله في نطاق التجريم كانطوائه على عبارات السب والقذف، وقد تكون المسؤولية مدنية إذا احتوى هذا المضمون على تعدٍّ على حقوق الآخرين، أو أمرٍ أضرَّ بهم، كانتهاك حرمة الحياة الخاصة، أو التعدّي على حقوق الملكية الفكرية. وفيما يتعلَّق بالمسؤولية المدنية بوجهٍ خاص، يُمكن أن تثور لنوعين من الأسباب: فإمَّا أن يكون سببها إخلال مقدم خدمات الأمن السيبراني بالتزاماته التعاقديَّة، وإمَّا أن ترجع إلى نشر مضمون معلوماتي غير مشروع على صفحات الويب.

يلزمنا إذن لتحديد نطاق مسؤولية مقدمي خدمات الأمن السيبراني أن نُحدِّد، بدايةً، بُعديها: الجزائي والمدني (الفرع الأول)، ومن ثمَّ ننتقل إلى التمييز في داخل المسؤولية المدنية نفسها بين المسؤولية العقدية والمسؤولية التقصيرية لهؤلاء المقدمين (الفرع الثاني).

الفرع الأول: المسؤولية الجزائية والمسؤولية المدنية

كان لتناول الصحافة المتكرِّر لمسألة انتهاك حرمة الحياة الخاصة، وقداسة الأديان على شبكة الأمن السيبراني الأثر الأكبر في انتشار الحديث عن المسؤولية الجزائية لمقدمي خدمات الأمن السيبراني. غير أن اختلاف المضمون الإلكتروني غير المشروع، وانتفاء القصد الجرمي، في بعض الأحيان، للمتدخِّلين في خضم الشبكة، كان وراء ظهور الحديث عن نوعٍ آخر من المسؤولية، وهي المسؤولية المدنية عن الأضرار المسبَّبة للآخرين عبر الأمن السيبراني. وثار السؤال حول إمكانية

المطالبة بالتعويض عنها. ومن هنا، كان لزاماً قانوناً، وقضاءً، وفقهاً، الفصل الدقيق بين كل من المسؤولية الجزائية والمسؤولية المدنية لمقدمي خدمات الأمن السيبراني، على الرغم من الصلة الوثيقة بينهما في هذا المجال.

وفيما يتعلَّق بالمسؤولية الجزائية، جاء القضاء الفرنسي ليُقرر بأن مسؤولية مقدمي خدمات الأمن السيبراني الجزائية يُمكن أن تقوم على أساس التدخُّل في الجريمة أو الاشتراك الجرمي. ففي قرارها الصادر في 10 تموز 1997م، أعلنت محكمة بداية باريس أن مساهمة مقدم خدمات الأمن السيبراني في بث مضمون معلوماتي غير مشروع، من الممكن أن يُشكِّل تدخُّلاً منه في ارتكاب الجريمة، الأمر الذي يستوجب معه إدانته إلى جانب الفاعل الأصلي على هذا الفعل [1]. وفي قرارٍ لها صدر بتاريخ 28 أيار 1998م، أدانت محكمة صلح ميونخ الألمانية أحد مقدمي خدمات الأمن السيبراني كشريك في جريمة نشر صور جنسية للأطفال على صفحات الويب [2].

جاء المشرّع الفرنسي متفقاً بهذا الخصوص مع الاتجاه العام للتوجيه الأُوروبي حول "التجارة الإلكترونية"، حيث نصَّت المادة 6-3/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي: "أن أفعال مقدمي خدمات الأمن السيبراني الخاطئة لا يُمكن أن تدخُل في نطاق التجريم إلاَّ إذا ثبت علمهم الفعلي بالمضمون الإلكتروني غير المشروع، وعلى الرغم من علمهم هذا لم يتخذوا الإجراءات اللازمة لشطبه، أو على الأقل لمنع وصول الجمهور إليه. فكل دولة في هذا الشأن تنتظر، بالتأكيد، من مقدمي خدمات الأمن السيبراني الذين يُمارسون أنشطتهم من على أراضيها، وفيما لا يُجاوز في حدِّه الأعلى الشروط السابقة، مساعدة السلطات العامة فيها على مُحاربة

---

(1) انظر أبراهام د. سوفاير وسيمور ي. جودمان، The Transnational Dimension of Cyber Crime and Terrorism, 2001 at 16, http://media.hoover.org/documents/0817999825_1.pdf

(2) منصور، محمد حسين، (2003) المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، الطبعة الأولى. ص 401.

الجريمة الإلكترونية. وبخلاف ذلك، سيجدون أنفسهم تحت طائلة المسؤولية الجزائية كمتدخِّلين في الجريمة، أو كمشتركين فيها. غير أنه وبالرجوع إلى نصوص قانون العقوبات الأردني والفرنسي، نجد بأنه لا يُمكن أن يُدان شخص بجريمة التدخُّل أو بالاشتراك الجرمي ما لم يثبت علمه بالأفعال المرتكبة. وتطبيقاً لذلك، فإن القصد الجرمي لمقدمي خدمات الأمن السيبراني ينتفي في حال ثبت عدم علمهم الفعلي بالمضمون الإلكتروني غير المشروع، أو إذا ما قاموا بمجرد علمهم بعدم مشروعية هذا المضمون، بشطبه، أو بمنع وصوله للجمهور.

من جهته حصر القانون الأمريكي (DMCA) مساءلة مقدمي خدمات الأمن السيبراني جزائياً في حدود الاعتداء على حقوق الملكية الفكرية في نطاق الأمن السيبراني، فأقام مسؤوليتهم فقط في حال علمهم بعدم مشروعية المضمون المعلوماتي الإلكتروني الذي يقومون بنقله أو تخزينه. ويثبت علمهم هذا في حالتين: الأولى: أن تكون عدم المشروعية ظاهرة إلى حدٍّ لا يُمكن تجاهلها، والثانية: قيام السلطات الأمريكية المختصة أو الشخص المتضرر من نشر المضمون المعلوماتي بإبلاغ مقدم الخدمة بوجه عدم المشروعية. فإذا ما تحقق علمه بعدم المشروعية، وعلى وجه الخصوص بالعمل المقلَّد أو المنسوخ بصورة غير شرعية، توجب عليه المبادرة إلى اتخاذ موقف إيجابي بشطب المضمون الإلكتروني غير المشروع، أو على الأقل منع وصوله لجمهور مستخدمي الشبكة. وبخلاف ذلك، يُعدُّ مقدم الخدمة مُخلاًّ بالتزاماته، مما يستوجب قيام مسؤوليته[1]. ونلاحظ في هذا الصدد تطابق حالات قيام المسؤولية وانتفائها في التشريعات الثلاث: الأوروبي، والفرنسي، والأمريكي.

---

(1) حول القانون الأمريكي (DMCA)، راجع:

M. GUILLARD, "Responsabilité des acteurs techniques de l´internet", précité, p. 29, A. STROWEL, "Responsabilité des intermédiaires: actualité législatives et jurisprudentielles", 10/10/2000, p. 17, article disponible à l'adresse www.droit- technologie. org, V. SÉDALLIAN, "La responsabilité des prestataires techniques sur Internet dans le Digital Millenium Copyright Act américain et le projet de directive européen sur le commerce électronique", Cahiers Lamy, Droit de l'informatique et des réseaux, n° 110, janvier 1999, p.

ولكي تنتفي مسؤولية مقدمي خدمات الأمن السيبراني الجزائية، بشكلٍ كُلِّي، وفي إطار مساعدتهم للسلطات العامة في الدولة في مُحاربة جرائم انتهاك حقوق الملكية الفكرية، وحرمات الحياة الخاصة وقداسة الأديان وجرائم الحث على المشاعر العنصرية، والاعتداء الجنسي على الأطفال، فإنهم مُطالبون، أيضًا، وفقاً لنص الفقرة الثالثة من المادة 6-7/2 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، والتي جاءت متفقةً مع الاتجاه العام للمواد 13 و14 من التوجيه الأُوروبي حول "التجارة الإلكترونية"، ومع المادة 512/g/3 من القانون الأمريكي (DMCA)، والخاصة بالتعدي على حقوق الملكية الفكرية في نطاق الأمن السيبراني، بأن يضعوا تحت تصرُّف عملائهم الوسائل اللازمة لتسهيل عملية التبليغ عن أيِّ مخالفات قد تتم عبر الشبكة. وبعد تحقق مقدم الخدمات من صحة موضوع التبليغ ومن عدم مشروعية المضمون الإلكتروني عليه أن يُبادر فوراً إلى إبلاغ السلطات العامة في الدولة عن هذه الواقعة، وذلك من أجل استصدار أمرٍ إداري أو قضائيٍّ بشطب هذا المضمون، أو منع وصوله لمستخدمي الشبكة.

ولكن كيف بالإمكان ضمان جدِّية التبليغ وبالتالي تجنُّب التبليغات التعسُّفية أو الكيدية؟ أجابت على هذا التساؤل المادة 6-4/1 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي"، والتي نصَّت على أن كل من بلَّغ مقدمي خدمات الأمن السيبراني بوجود مضمون إلكتروني غير مشروع، من أجل شطبه أو منع الجمهور من الوصول إليه، مع علمه المسبق بعدم صحَّة تبليغه، يُعاقب بالسجن لمدة عام وبغرامة مقدارها خمس عشرة ألف يورو.

مسؤوليةٌ من نوعٍ آخر تثور عند الحديث عن نشر مضمون إلكتروني غير مشروع، أو بصفةٍ عامة عند الحديث عن إخلال مقدمي الخدمات على شبكة الأمن السيبراني بأيٍّ من التزاماتهم، وتتمحور هذه المرَّة حول إمكانية مطالبة الشخص الذي لحقه ضرر جرَّاء هذا الإخلال بالتعويض،

استناداً لقواعد المسؤولية المدنية. فممَّا لا شكَّ فيه أن مبدأ قيام هذه المسؤولية متفقٌ عليه، إلا إن الخلاف ثار حول طبيعة هذه المسؤولية وأساسها، ونطاق تطبيقها. بل أكثر من ذلك، إن مقدمي خدمات الأمن السيبراني أنفسهم لم يُراودهم أيِّ طموحٍ في إعفائهم تماماً من التعويض عن الأضرار التي من الممكن أن يُلحقوها بالآخرين خلال قيامهم بعملهم، إلاَّ إنهم، في المقابل، بذلوا أقصى ما في وسعهم من أجل تحديد نطاق مسؤوليتهم بشقيها: العقدي، والتقصيري، ونادوا بالتخفيف من آثارها، وعملوا على تفادي مخاطرها [1]. ولإعطاء المسألة أهميتها وأبعادها القانونية، فقد ارتأينا أن نُفرِدَ فرعاً خاصاً لتحليلِ الشقِّ العقدي والشقِّ التقصيري لمسؤولية مقدمي خدمات الأمن السيبراني المدنية.

الفرع الثاني: المسؤولية العقدية والمسؤولية التقصيرية

تتنوَّع العقود التي تعنى بتجهيز وتقديم والاستفادة من خدمات الأمن السيبراني، ويتم إبرام هذه العقود المتفق على تسميتها "بعقود الخدمات الإلكترونية"، بين القائمين على تقديم خدمات تلك الشبكة والمستفيدين منها. ومن الأمثلة على هذه العقود: عقد الدخول إلى الشبكة، وعقد توريد المعلومات، وعقد الإيواء، وعقد تقديم المساعدة الفنية. وبموجب هذه العقود، والتي يتم إبرامها وتنفيذ بنودها من كلا الطرفين عبر شبكة الأمن السيبراني نفسها، يلتزم مقدمو خدمات الأمن السيبراني، كقاعدة عامة وكما سبق وأن أوضحنا، بتخزين المادة المعلوماتية وإيصالها إلى مستخدمي الشبكة عن طريق تزويدهم بالوسائل الفنية التي تسمح بذلك. وبالمقابل يلتزم مستخدمو الشبكة والمستفيدون من هذه الخدمات بتأدية ما ترتَّب في ذمَّتهم من استحقاقات مالية، وكذلك باحترام القوانين والأنظمة السارية والأعراف، وقواعد السلوك الثابتة في هذا المجال.

---

(1) محمد حسين منصور، المرجع السابق، ص 191 و

André LUCAS, "La responsabilité des différents intermédiaires de l´internet", précité, p. 2.

وفيما يخص مقدم خدمات الأمن السيبراني، محور دراستنا، فإن مسؤوليته العقدية تثور في حال إخلاله بالتزامه بتقديم الخدمة. حيث يحق لكل مشترك الحصول على خدمة الأمن السيبراني المتعاقد عليه، وفي حال أن استحال ذلك، كتعذُّر اتصاله بالشبكة، أو عدم وصوله إلى المادة المعلوماتية المطلوبة لأيِّ سببٍ كان، تُطبَّق مباشرةً قواعد المسؤولية العقدية. (1)

وعلى غرار المشرّع الأُوروبي فإن المشرّع الفرنسي لم يتناول المسؤولية العقدية لمقدمي خدمات الأمن السيبراني إلاَّ من خلال تنظيمه لأحكام المسؤولية في التجارة الإلكترونية، ولكنَّه على خلاف المشرّع الأُوروبي الذي لم يُوفَّق في تعريفها، فقد أعطاها المشرّع الفرنسي تعريفاً قانونياً واسعاً. إذ جاءت المادة 14 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" لتُعرفها على أنها كل نشاط اقتصادي مُوجَّه من قِبل شخص معنوي أو طبيعي يتوَّلى عملية اقتراح وتقديم بضائع، أو خدمات، باستخدام وسائل الاتصال عن بُعد أو الوسائل الإلكترونية. (2)

والمشرّع الأردني بدوره لم يستخدم مصطلح "التجارة الإلكترونية"، وإنما ارتأى أن يُوسِّع هذا المفهوم، وأن يستخدم بدلاً منه مصطلح "المعاملات الإلكترونية"، والذي يمتد ليشمل، وفقاً لنص المادة الثانية من قانون المعاملات الإلكترونية المؤقت، جميع "المعاملات التي تُنفَّذ بوسائل إلكترونية". وقد عرَّف المشرّع الأردني مصطلح "المعاملات"، في ذات المادة السابقة، على أنها "إجراء أو مجموعة من الإجراءات، يتم بين طرفين أو أكثر لإنشاء التزامات على طرف واحد، أو

---

(1) فرح، أحمد قاسم (2007) النظام القانوني لمقدمي خدمات الإنترنت–دراسة تحليليَّة مقارنة –قسم الدراسات القانونية، كلية الدراسات الفقهية والقانونية، جامعة آل البيت، ص 145.

(2) راجع في تفاصيل هذا الموضوع:

N. MATHEY, "Le commerce électronique dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l´économie numérique", Contrats, Concurrence, Consommation, étude n° 13, O. CACHARD, "Définition du commerce électronique et loi applicable", Comm. Com. Électr., 2004, étude n° 31.

التزامات تبادلية بين أكثر من طرف، ويتعلَّق بعمل تجاري، أو التزام مدني، أو بعلاقة مع أي دائرة حكومية".

ومن الملاحظ أن كلا المشرّعيْن: الفرنسي والأردني قد وسَّعا من مفهوم التجارة الإلكترونية ليشمل الغالبية العُظمى من العقود التي تُبرم عن بُعد، لا سيَّما عقود تزويد المعلومات عن طريق الأمن السيبراني، وعقود الدخول إلى الشبكة، وعقود الإيواء، وعقود تزويد خدمات البحث الآلي. وإذا ما ربطنا بين هذا التعريف ونص المادة 121-3/20 من قانون الاستهلاك الفرنسي لوجدنا أن مقدمي خدمات الأمن السيبراني مسؤولون بقوُّة القانون تجاه المشتركين عن تنفيذ كامل التزاماتهم التعاقدية، وأنه ليس بإمكانهم أن يتنصَّلوا من أحكام هذه المسؤولية إلاَّ إذا أثبتوا أن سبب عدم التنفيذ لا يرجع إليهم، وإنما إلى قوة قاهرة، أو فعل الآخرين، أو فعل المشترك نفسه [1]. إذن الهدف هو إصباغ حماية فعَّالة للمشترك وبسطها لتمتد، ليس فقط لطائفة المستهلكين، وإنما لكل من يستفيد من هذه الخدمات، بغض النظر عن صفته. [2]

وبما أن عقد تقديم الخدمات الإلكترونية وليد الإرادة، يثور التساؤل حول إمكانية اتفاق المتعاقدين على عدم مسؤولية مقدم الخدمات، أو على الأقل التخفيف منها عند إخلاله بالتزامه بتقديم الخدمة المتفق عليها. وفي الواقع، إن الاتجاه العام في فرنسا يذهب إلى أن ذلك يعتمد على سبب هذا الإخلال، فمن الممكن بالتالي تصوُّر صحة شروط استبعاد أو تحديد مسؤولية مقدم الخدمة في عقد الخدمات الإلكترونية إذا أهمل أو قصَّر في تنفيذ التزامه، وذلك دون أن يتعمَّد أو

---

(1) ونفس الموقف تمَّ تبنيه من قبل القضاء الفرنسي بصدد المسؤولية التعاقدية لأحد مقدمي خدمات الإنترنت (France Télécome)، انظر:

Juridiction de proximité de RAMBOUILLET, 8 février 2005, disponible à l'adresse www.legalis.net, rubrique responsabilité, « L'impossibilité de se connecter ne peut être imputable au fournisseur d'accès à Internet que si elle est due à un cqs de force majeure, ou à une faute émanant de l'abonné ou d'un tiers, en l'espèce aucune faute ne peut être reprochée aux demandeurs ni à un tiers ».

(2) Ch. HUGON, "La responsabilité des acteurs de l´internet dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l´économie numérique", précité, n° 4 et s., p. 7 et s.

يرتكب خطأ جسيماً. ويعني هذا أنه يقع على المشترك عبء إثبات غش مقدم الخدمة حتى يرفع عنه شرط الإعفاء. وبهذا، فإن البطلان في هذا النوع من العقود لا يلحق من الأساس إلاَّ الشروط التعسُفيَّة. [1]

ولم يخرج المشرّع الأردني عن هذه القواعد، فمن خلال استقرائنا لبعض النصوص في القانون المدني الأردني يُظهر لنا، ولو بصورة ضمنية، جواز الإعفاء من المسؤولية أو تحديدها. فالمادة 358-1 من هذا القانون تنص على أنه: "إذا كان المطلوب من المدين هو المحافظة على الشيء، أو القيام بإدارته، أو توخِّي الحيطة في تنفيذ التزامه، فإنه يكون قد وفَّى بالالتزام إذا بذل في تنفيذه من العناية كل ما يبذل الشخص العادي، ولو لم يتحقق الغرض المقصود. هذا ما لم ينص القانون أو الاتفاق على غير ذلك"، كما تنص الفقرة الثانية من هذه المادة على أنه: "وفي كل حال يبقى المدين مسؤولاً عمَّا يأتيه من غش أو خطأ جسيم". وبتطبيق ما تقدَّم من قواعد عامة على مسؤولية مقدمي خدمات الأمن السيبراني فإنه يُمكننا القول بجواز إعفائه من المسؤولية إذا لم يرجع سبب الإخلال إلى خطأ جسيم أو غش من جانبه [2]. فلا شكَّ إذن في صحَّة هذا الشرط، إلاَّ إنه لا يُعتد به، طبقاً للقواعد العامة وأعمالاً لمبدأ نسبية آثار العقد، إلاَّ في مواجهة المتعاقد معه، ولا يسري في مواجهة الغير الذي يُضار من المخالفة المرتكبة.

---

(1) Guide Permanent Droit et Internet, E 1.2., Fourniture d′accès, précité, nº 36, p. 15.

في 31 كانون الأول 2003م، أصدرت لجنة الشروط التعسُفيَّة المُكلَّفة من قِبل وزير الاقتصاد الفرنسي بشؤون الاستهلاك، توصيةً حدَّدت فيها 28 نوعاً من الشروط التعسُفيَّة التي من الممكن أن تتضمَّنها عقود الخدمات الإلكترونية، وعدَّتها جميعها باطلة. انظر في أنواع هذه الشروط وحيثيَّات التوصية

Recommandation n 03-01 relative aux contrats de fourniture d´accès à l´internet, BOCCRF du 31/1/2003, disponible à l´adresse: www.finances.gouv. fr/clauses_abusives/recom/03r01.htm.

(2) راجع في مفهوم الخطأ الجسيم، نوري حمد خاطر، "الخطأ ألجسيم في ظل تطبيقاته التشريعية والقضائية: دراسة مقارنة"، المنارة للبحوث والدراسات، المجلد التاسع، العدد الثالث، آب 2003م، جامعة آل البيت، ص 43 وبعدها.، وفي شروط الإعفاء من المسؤولية، أو تحديدها في القانون الأردني، عدنان السرحان ونوري خاطر، شرح القانون المدني. مصادر الحق الشخصي (الالتزامات)، دراسة مقارنة، الطبعة الأولى، الإصدار الثاني، دار الثقافة، 2005م، فقرة 372 وبعدها، ص 319 وبعدها.

وعلى صعيد المسؤولية التقصيرية، يبدو من الاتجاه العام لنصوص المواد 6 من القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" و12-14 من التوجيه الأُوروبي حول "التجارة الإلكترونية" أنها تميل إلى إعفاء مقدم خدمات الأمن السيبراني من المسؤولية، إلاَّ في حال أن ثبت علمه الفعلي بالمضمون الإلكتروني غير المشروع، ومع ذلك لم يتَّخذ الإجراءات اللازمة لشطبه أو لمنع وصوله للجمهور، أو في حالةٍ أُخرى، إذا طُلب منه شطب هذا المضمون أو منع وصول الجمهور إليه من قِبل السلطة القضائية، ولم يستجب لهذا الطلب.

ويتَّضح، أيضًا، من القانون الأمريكي (DMCA) أن مقدمي خدمات الأمن السيبراني غير مسؤولين عن المضمون الإلكتروني غير المشروع، طالما أنهم يجهلون سبب عدم المشروعية، ولم يتلقُّوا مكسباً ماديًّاً من وراء المخالفة، وقاموا بسحب هذا المضمون بمجرَّد تلقِّيهم تحذيراً من الشخص المتضرِّر. وينتج عن مجموع هذه الشروط أن مقدم الخدمات لا يُسأل عن فعل الآخرين ويتحمَّل، فقط، نتيجة خطئه الشخصي، وهذا يتَّفق بدوره مع القواعد العامة في المسؤولية في القانون الفرنسي، وبوجهٍ خاص، مع نص المادتين: 1382 و1383 من القانون المدني واللتين تُلزمان صاحب الفعل الضار الذي أدَّى بخطئه، أو إهماله، أو تقصيره إلى الإضرار بالآخرين بضمان هذا الضرر. وترتيباً على ذلك، يجب على من تضرَّر من نشر مضمون إلكتروني غير مشروع على شبكة الأمن السيبراني التأسيسِ على الخطأ الثابت لمقدم الخدمات لكي يتمكَّن من تضمينه الضرر الذي لحقه[1].

(1) راجع في ذلك، محمد حسين منصور، المرجع السابق، ص 203 و

Ph. LE TOURNEAU, "La responsabilité civile des acteurs de l´internet", expertises, janvier 1999, p. 419, TGI Paris, 3e Ch., 1re Sect., 23 mai 2001, Comm. Com. Électr., novembre 2001, Chronique, n 112, observation Ch. LE STANC.

المطلب الثاني
شروط تحقق مسؤولية مقدمي خدمات الأمن السيبراني

البحث عن مساءلة مقدمي خدمات الأمن السيبراني يعكس رغبة المشرّع الحقيقية في إيجاد مسؤول مُحدَّد الهويَّة، وموسر لضمان الأضرار التي يُسبِّبها نشر مضمون إلكتروني غير مشروع. غير أن العدالة تقتضي عدم مساءلة مقدمي الخدمات وحدهم، بل البحث عن مُؤلِّف هذا المضمون، أو صاحبه والذي هو بالأساس مصدره. من هنا فإن المسؤول الأول: قانوناً وقضاءً عن المضمون الإلكتروني غير المشروع هو الشخص الذي أوجده [1]، وذلك بالطبع في حدود عدم علم مقدم الخدمات بوجوده، وعدم قيام الشخص المضرور بتبليغه بأسباب عدم مشروعيته، خاصةً أن مقدمي الخدمات غير ملزمين بممارسة الرقابة العامة على المحتوى المعلوماتي لشبكة الأمن السيبراني. ولهذا، يلزم لتحقُّق مسؤولية مقدمي الخدمات عمَّا يحدث من مخالفات عبر الشبكة توافر عدد من الشروط، منها ما هو موضوعي (الفرع الأول)، ومنها ما هو إجرائي (الفرع الثاني).

الفرع الأول: الشروط الموضوعية

أمام تنامي ظاهرة مُخالفة القانون، والاعتداء على حقوق الغير باستخدام شبكة الأمن السيبراني، وفي ظلِّ غياب قواعد قانونية مُحدَّدة لحكم مسؤولية مقدمي الخدمات، لم يجد القضاء له من بُدٍّ سوى اللجوء إلى القواعد العامة لتقرير حالات قيام مسؤوليتهم، وليردع، في نفس الوقت، من اعتقدوا أن الأمن السيبراني منطقة بلا قانون يستطيعون أن يصنعوا فيها ما شاءوا دون رقابة أو مساءلة. فانطلق القضاء، في بداية أحكامه، من افتراض الخطأ لقيام المسؤولية، وانتهى، لاحقاً، بتكريس الخطأ الثابت لتحقُّقها.

---

(1) P. WILHEM, "La hiérarchie des responsabilité sur Internet", Cahiers Lamy, Droit de l’informatique et des réseaux, n° 114, mai 1999, p. 2.

الفرع الثاني: الشروط الإجرائية

تتحقَّق مسؤولية مقدمي خدمات الأمن السيبراني، إمَّا لارتكابهم المخالفة، وإمَّا لامتناعهم عن وقف بثِّها. وارتكاب المخالفة أو عدم وقفها مفاده علم مقدم الخدمات بمضمونها غير المشروع. وبحسب أغلب التشريعات التي نظَّمت هذه المسألة، فإن العلم مقترن بالتبليغ [1]، لاسيَّما إذا لم تكن عدم المشروعية ظاهرة بما يكفي. لذا، لكي تثور مسؤولية مقدم الخدمات عن المضمون الإلكتروني غير المشروع يلزم إثبات تبلُّغه بعدم مشروعيته، وبالتالي، إثبات سلبيَّته بوضع حدٍّ للمخالفة أو تجنُّب وقوعها. فما هي الإجراءات الواجبة الاتِّباع في هذا الإطار، ومَن صاحب الحق في طلب وقف بثِّ المضمون؟

بالنظر لأهميَّة المسألة، حاولت أغلب التشريعات المعاصرة التصدِّي لها، فنصَّ التوجيه الأوروبي حول "التجارة الإلكترونية" من خلال مواده: 3/12، و2/13، و3/14 والتوضيح رقم 45 على حق السلطات الإدارية أو القضائية في الدول الأعضاء بإصدار قرارات تُلزم مقدمي خدمات الأمن السيبراني، بغض النظر عن صفتهم أو طبيعة الخدمة التي يقدمونها، بوقف بثِّ المضمون الإلكتروني المخالف للقانون. ووفقاً لنص المادة 8-3/1 وتوضيحها رقم 59 من التوجيه الأُوروبي حول "حق المُؤلِّف والحقوق المجاورة له في مجال المعلوماتية" فإن التطوُّر الحاصل في شبكة الأمن السيبراني من الممكن أن يزيد من الاعتداء على حقوق الآخرين، مما يستدعي تدخُّل مقدمي الخدمات لوضع حدٍّ لتلك الاعتداءات. وعليه، مع عدم الإخلال بأيِّ جزاء أو إجراء يتمتَّع به صاحب الحق، يجوز لهذا الأخير التوجُّه للقضاء، وتقديم طلب على عريضة من أجل استصدار

(1) précité, p, 6. D. MELISON, "Responsabilité des hébergeurs: une unité de régime en trompe l'œil",

قرار يأمر مقدم الخدمات بسحب العمل المُقلَّد أو المنسوخ الذي يأويه أو ينقله على أجهزته. ويتم تنظيم شروط هذا الطلب وإجراءاته حسب قانون كل دولة من الدول الأعضاء[1].

تبنَّت بعض التشريعات الأُوروبية، بالفعل، هذه النصوص. ففي فرنسا، يُعطي القانون الفرنسي حول "الثقة في الاقتصاد الرقمي" الحق في تبليغ مقدم الخدمات بوقف المضمون الإلكتروني غير المشروع للسلطة القضائية وللشخص المتضرِّر من بثِّه. فطبقاً لنص المادة 6-1/8 من هذا القانون، فإن السلطة القضائية تملك إصدار قرار مستعجل، أو أمر على عريضة تطلب فيه من مقدم الخدمات وقف بث المضمون الإلكتروني غير المشروع. وتبليغه بهذا الطلب يُثبت علمه بعدم مشروعية المضمون الذي يأويه أو ينقله، وهو ما يُفترض من أجل قيام مسؤوليته في حال أبدى موقفاً سلبياً من طلب المحكمة [2]. أمّا إذا قرَّر الشخص المتضرِّر عدم اللجوء لدعاوى الوقف، والتوجُّه بطلبه مباشرةً إلى مقدم الخدمات المعني فيلزمه، لكي يُثبت علم هذا الأخير بعدم مشروعية المضمون الإلكتروني بحسب نص المادة 6-1/5 من نفس القانون، بأن يكشف له عن هويَّته، وأن يُحدِّد له المضمون المشتكى منه، وأسباب عدم مشروعيته، وأن يُزوِّده بما يُثبت قيامه بإرسال نسخة من طلب وقف المضمون غير المشروع إلى صاحبه أو مُؤلِّفه، ولاشكَّ، أن سلبيَّة مقدم الخدمات، في هذه الحالة، تُثير مسؤوليته عن خطئه الثابت[3]. وبمفهوم المخالفة، إعفاء مقدم الخدمات من المسؤولية إذا امتثل لقرار القضاء، أو استجاب لإخطار الشخص المتضرِّر، في حال أن كانت عدم المشروعية ظاهرة، وقام بسحب المضمون الإلكتروني غير المشروع، أو منع الوصول إليه [4]. لا

(1) Arthur J. Wylene (2012) PRESENTED AT THE TWENTY THIRD ANNUAL NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE . pp 56-78

(2) Arthur J. Wylene (2012) PRESENTED AT THE TWENTY THIRD ANNUAL NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE . pp 123-145

(3) دليل الأمن السيبراني للبلدان النامية الاتحد الدولي للاتصالات، لعام 2010، ص 345.

(4) CA Paris, 7 juin 2006, précité, « Le prestataire d'hébergement a rempli ses obligations ayant, sans attendre notre décision, pris les dispositions qui ont conduit l'éditeur à empêcher l'accès au jeu litigieux ».

بل أكثر من ذلك، فإن مسؤولية مقدم الخدمات عن المضمون الإلكتروني غير المشروع يُمكن أن تثور دون تبليغه به، أي أن علمه بوجوده يكون مفترضاً، وذلك عندما تكون عدم مشروعية المضمون ظاهرة بما يكفي، والمعيار هنا موضوعي[1].

وفيما يتعلَّق ببعض الدول الأُوروبية الأُخرى، كألمانيا، وسويسرا، وإيطاليا، فإنها تُعطي حق طلب وقف المضمون الإلكتروني غير المشروع لسلطات الضبط الإداري. فيُمكن لهذه السلطات أن تُلزم مقدم الخدمات بشطب المضمون، أو بمنع وصوله لجمهور المستخدمين. وفي حال عدم استجابته، بالإمكان اللجوء إلى القوَّة الجبريَّة القانونية للقيام بذلك.

وفي الولايات المتحدة الأمريكية يُمكن الطلب من مقدمي الخدمات وقف بثِّ المضمون الإلكتروني غير المشروع من خلال ما يُسمَّى بإجراءات الأخطار والسحب، أو الرفع (procedure de notice et take down). فطبقاً لهذه الإجراءات، يجب على مقدم الخدمات التصرُّف بعناية من أجل سحب العمل المُقلَّد أو المنسوخ بصورةٍ غير شرعيَّةٍ، أو منع الوصول إليه بمجرَّد تبليغه بذلك من قِبل صاحبه أو مُؤلِّفه الحقيقي. ومن أجل استلام التبليغات وتنظيمها حسب الأُصول والتأكُّد من جدِّيتها، على مقدم الخدمات أن يُعيِّن وكيلاً له، مهمته القيام بذلك، وبمجرَّد أن يُرسل الشخص المتضرِّر إلى الوكيل إخطاراً مكتوباً وموقَّعاً منه، ومبيَّناً فيه العمل المُقلَّد أو المنسوخ ومكان تواجده، ويتأكد الوكيل من ذلك، على مقدم الخدمات المباشرة فوراً بسحب العمل موضوع التبليغ، أو منع الوصول إليه. وفي المقابل، لحفظ حقوق مورِّد العمل، على مقدم الخدمات إخطاره بالواقعة، فإن أرسل ردَّاً مضادَّاً قام مقدم الخدمات بإرساله إلى مدَّعي الحق، وأخطره بأن العمل

(1) انظر محمد حسين منصور، المرجع السابق، ص 203.

موضوع النزاع سيُبث من جديد، خلال مدَّة أقصاها أربعة عشر يوماً من تاريخ الأخطار، إذا لم يرفع خلالها دعوى يعرض فيها الأمر بمجمله على القضاء، وذلك لحسم النزاع[1].

احتج بعض القائمين على خدمات الأمن السيبراني على هذه الإجراءات، وعلى تحميلهم المسؤولية بناءً عليها، وتذرَّعوا بأنه يصعب عليهم، في أغلب الحالات، تقدير مدى جدِّية أو حقيقة طلبات الوقف أو الغلق، وأن وضعهم القانوني لا يسمح لهم بممارسة أيَّة رقابة على المضمون الإلكتروني احتراماً لحرِّية التعبير عن الرَّأي. ولاشكَّ، أن الأمر دقيقٌ بالنسبة لمقدمي الخدمات، حيث يجدون أنفسهم، باستمرار، محل لوم، سواء بسبب تدخُّلهم، أو بسبب سلبيَّتهم، إلاَّ إن هذا لا يُبرِّر المجاملة أو السلبيَّة تجاه المضمون غير المشروع [2]، خاصةً إذا ما باشروا بإجراءات الوقف هذه، استناداً لقرار صادر من السلطة القضائية المختصة، وهو ما سيُعفيهم من أيَّة مسؤولية محتملة، وذلك بسبب انتفاء خطئهم.

المطلب الثالث
أساس مسؤولية مقدمي خدمات الأمن السيبراني

يتَّضح، من تفحُّصنا للنصوص القانونية التي وضعتها أغلب التشريعات التي نظَّمت مسؤولية مقدمي خدمات الأمن السيبراني، أن قيام هذه المسؤولية يتوقَّف على علم مقدمي الخدمات بالمضمون الإلكتروني غير المشروع، والمُتحصِّل من تبلُّغهم بوجوده. فأساس المسؤولية إذن هو الخطأ الثابت المتمثِّل في تدخُّل مقدمي الخدمات في المخالفة، أو في سلبيَّتهم باتخاذ الإجراءات اللازمة لسحب المضمون الإلكتروني غير المشروع، أو لمنع الوصول إليه. وتأسيس مسؤولية

(1) حول تجارب هذه الدول في هذا المجال، راجع: P. SIRINELLI, "La responsabilité des intermédiaires de l´internet", précité, p. 7

(2) محمد حسين منصور، المرجع السابق، ص 225.

مقدمي خدمات الأمن السيبراني على الخطأ الثابت يجد مُبرِّراً له، في أنه في عالم الأمن السيبراني الذي يتَّصف باللامركزيَّة، والذي يعمل فيه كل مُتدخِّل لحسابه الخاص دون الخضوع لتنظيم إداري تدرُّجي مُعد مُسبقاً لتوزيع الأدوار والمهام[1]، لا يُمكن أن يكون الشخص مسؤولاً إلاَّ عمَّا يُمكنه مراقبته والسيطرة عليه. ومن ثُمَّ فلا مجال للبحث، وقت تحقُّق الضرر، عن مسؤولية المتبوع أو عن المسؤولية عن حراسة الأشياء طبقاً لنص المادتين: 1384 من القانون المدني الفرنسي و289، 291 من القانون المدني الأردني، أو فيما عدا مسؤولية مورد المعلومات، عن المسؤولية بالتتابع المعمول بها في نطاق الصحافة والإعلام المرئي والمسموع، والتي تستند لتحمُّل المخاطر والتبعيَّة[1]، بل يجب تحديد المسئول شخصيًّا، وإثبات ارتكابه للخطأ بالمعنى الذي أوردته نصوص المواد: 1382 و1383 من القانون المدني الفرنسي واللتان تشترطان لقيام المسؤولية عن الفعل الشخصي خطأ ثابت، وضرر، وعلاقة سببيَّة تجمعهما.

وتطبيقاً لذلك، قرَّر القضاء الفرنسي في قضيَّة عارضة الأزياء Estelle Hallyday، سابقة الذكر، عدم إعفاء مقدم الخدمات من المسؤولية إلا إذا أثبت قيامه بجميع الالتزامات الملقاة على عاتقه. كما أعلن هذا القضاء أن نشاط مقدم الخدمات لا يقتصر على الدور الفنِّي لنقل المعلومات، ويُمكن في حال إخلاله بالتزاماته قيام مسئوليته على أساس الخطأ الثابت، طبقاً لنص المادة 1383 من القانون المدني الفرنسي. ذلك أن إعفاءه من ممارسة الرقابة العامة والدقيقة على مُحتوى الشبكة المعلوماتي لا يمنع من اتخاذه للإجراءات اللازمة والمعقولة، التي يُفترض بكل مهني يقظ اتخاذها

---

(3) Guide Permanent Droit et Internet, E 3.3 Hébergement du site, précité, nº 12, p. 8.

انظر حول المسألة:

Conseil d´état - Section du rapport et des études. Internet et les réseaux numériques, précité, p. 175, Guide Permanent Droit et Internet, E 3.3 Hébergement du site, précité, nº 12, p. 8., André LUCAS, "La responsabilité des différents intermédiaires de l´internet", précité, p. 4, A. LUCAS, J DEVÈZE et J. FRAYSSINET, op. cit., n° 705, p. 459.

ومحمد حسين منصور، المرجع السابق، ص 193.

من أجل التقاط المعلومات الإلكترونية التي تتَّسم بعدم المشروعية الظاهرة. ويتَّفق هذا الحل المتوازن مع النظام القانوني لمسؤولية مقدمي خدمات الأمن السيبراني الذي أرساه التوجيه الأُوروبي حول "التجارة الإلكترونية"، والقانون الفرنسي حول "الثقة في الاقتصاد الرقمي" واللذان يميلان إلى وضع معيارٍ عامٍّ للخطأ الثابت، يتمثَّل في ارتكاب مقدم الخدمات للمخالفة، أو سلبيَّته في وقفها.

فطبقاً لنصوص المواد 12–14 من التوجيه الأُوروبي، لا يجوز، كما سبق وبينَّا، مساءلة مقدمي الخدمات إلاَّ على أساس خطئهم الثابت. بل لم يكتفِ هذا التوجيه بذلك، وإنما حظر على الدول الأعضاء بأن تفرض عليهم التزام عامٍ بمراقبة المعلومات الإلكترونية التي يتولُّون تخزينها، أو نقلها، أو حتَّى التحرِّي النشط عن الوقائع والظروف التي تكشف الأنشطة غير المشروعة. ونفس الوضع أصبح في فرنسا، فجاء نص المادة السادسة من قانون "الثقة في الاقتصاد الرقمي" لِيُقرِّر عدم إمكانية مساءلة مقدمي الخدمات في حال أن وضعوا حدَّاً للمخالفة، أو عملوا على تجنُّب وقوعها، بما في ذلك سحب المضمون الإلكتروني غير المشروع، أو منع وصوله لمستخدمي الشبكة. وبتبنِّيهما لهذا الموقف، كرَّس المشرّعيْن: الأُوروبي والفرنسي مبدأ المسؤولية عن الفعل الشخصي القائم على أساس الخطأ الثابت.

الفرع الأول: مكافحة الجريمة السيبرانية

ومع هذا الانفتاح ودخول العصر الرقمي وانتقال المجتمعات من الواقع الفعلي المادي إلى الواقع السيبراني أصبحنا نشاهد ظهور الجرائم السيبرانية وتعديها على الفرد والمجتمع، بشكل ملحوظ ومتزايد، ولهذا فقد نص القانون على حماية الأمن السيبراني ومكافحة الجرائم السيبرانية حيث نصت المادة (16) من قانون الجرائم الإلكترونية:

1- كل من أرسل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن هم فوق الثامنة عشر سنة ميلادية دون رضاه، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنتين، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

2- كل من أرسل أو نشر عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن لم يكمل الثامنة عشر سنة ميلادية أو تتعلق بالاستغلال الجنسي لهم، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 3. كل من قام قصداً باستخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشر سنة ميلادية أو من هو من ذوي الإعاقة، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة، أو بكلتا العقوبتين.

الفصل الخامس
الخاتمة، النتائج والتوصيات

أولا: الخاتمة

رافق ثورة تكنولوجيا المعلومات زيادة ملحوظة في حجم الاعتداء على حقوق الآخرين ومخالفة القانون، وبهدف الوصول إلى الاستخدام الأمثل لشبكة الأمن السيبراني، وضبط قواعد السلوك على السواء، لكل من مستخدمي الشبكة والمهنيين، كان التدخُّل التشريعي في عدد من الدول. فجاءت النصوص القانونية المتبناة في هذا الصدد، خاصةً من قِبل المشرّع الأردني ومن بعده الفرنسي، عبر صياغة تشريعية إلكترونية، لتُرسي نظاماً قانونياً متوازناً وملائماً لطبيعة العمل على الأمن السيبراني، ولتُحدِّد بالنتيجة التزامات كل من مستخدمي الشبكة والقائمين على إدارتها من مقدمي خدمات، والأحكام الخاصة بمسؤولية كلٍّ منهم.

فرض هذا النظام القانوني على مقدمي خدمات الأمن السيبراني وجوب اتِّباع قواعد السلوك الصحيح، سواء في تقديمهم للخدمة المتعاقد عليها مع المشترك، أو في إيوائهم ونقلهم للمعلومات الإلكترونية عبر أجهزتهم. وبالرغم من رفض التشريعات والقرارات القضائية المعاصرة فرض التزام عامٍ برقابة المحتوى المعلوماتي للشبكة على مقدمي الخدمات، إلاَّ إن هذا لم يُعفهم لا من الالتزام بممارسة هذه الرقابة في حالات معيَّنة، ولا من بذل العناية والجهود المعقولة لالتقاط أيِّ موقعٍ إلكتروني ذي مضمون معلوماتي غير مشروع، وهنا يقع عليهم واجب الكشف للسلطات العامة في الدولة عن وجود هذا المضمون، وعن هويَّة صاحبه أو مُؤلِّفه.

ووفقاً لهذا النظام، فإن قيام مسؤولية مقدمي الخدمات يتوقَّف على مدى علمهم بعدم مشروعية المضمون الإلكتروني المأوي أو المنقول. وباستثناء حالة عدم المشروعية الظاهرة، فإن علم مقدمي

الخدمات بالمضمون الإلكتروني غير المشروع يتحصَّل بتبليغهم به سواء من قِبل السلطة القضائية، أو الإدارية المختصة في الدولة، أو من قِبل المتضرِّر نفسه. فإذا ما استجاب مقدمو الخدمات للأمر القضائي، أو الإداري، أو لطلب المتضرِّر، وقاموا بسحب المضمون المخالف، أو منعوا الوصول إليه، انتفت مسؤوليتهم الجزائية والمدنية، وإذا ما رفضوا القيام بذلك تحققت، لا على أساس تحمُّل التبعة أو المخاطر أو حراسة الأشياء، وإنما على ثبوت الخطأ الراجع لارتكابهم المخالفة، أو لسلبيَّتهم في وقفها.

ثانيا: النتائج

بعد الاطلاع على الدراسة التي قمنا بها فقد تطرقت إلى بعض النتائج:

1- الأمن السيبراني هو حماية الأنظمة المتصلة بالإنترنت مثل الأجهزة والبرامج والبيانات من التهديدات السيبرانية، يتم استخدام هذه الممارسة من قبل الأفراد والمؤسسات للحماية من الوصول غير المصرح به إلى مراكز البيانات والأنظمة المحوسبة الأخرى.

2- لأمن السيبراني هو مجال متغير باستمرار، مع تطوير التقنيات التي تفتح آفاقاً جديدة للهجمات الإلكترونية، وعلى الرغم من أن الانتهاكات الأمنية الكبيرة هي التي يتم الإعلان عنها فقط، إلا أنه لا يزال يتعين على المؤسسات الصغيرة أن تهتم بالانتهاكات الأمنية، حيث قد تكون غالباً هدفاً للفيروسات والتصيد الاحتيالي.

3- ان الأمن السيبراني يقوم على حماية المنظمات والموظفين والأفراد، يجب على المنظمات والخدمات تنفيذ أدوات الأمن السيبراني والتدريب وأساليب إدارة المخاطر وتحديث الأنظمة باستمرار مع تغير التقنيات وتطورها.

4- تبين من الدراسة ان المشرّع الأردني لم يعالج في قانون الأمن السيبراني الأردني المسائل التقنية والفنية لحادث الأمن السيبراني من حيث الطبيعة والاثر والتصنيف. الأمر الذي من شأنه التأثير على ضمان الحماية المقررة أو المرجوة للأمن السيبراني وسلامة الفضاء السيبراني الأردني.

5- اعتبر الحفاظ على الحق في الخصوصية، من أساسيات تعزيز الثقة، في الأمن السيبراني، والافادة من طاقات تقنيات المعلومات والاتصالات، على المستويات: الاجتماعية، والاقتصادية، والثقافية.

6- الأمن السيبراني يعمل تعزيز حماية جميع ما يتعلّق بالدولة إلكترونياً وأفراداً لحماية هذه الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وجميع مكوناتها المحيطة بالمجتمع من أجهزة وبرمجيات ومعدات وجميع ما يؤثّر على تقدّم هذه الخدمات، وما تحويه من بيانات، فأصبحت هذه أيضًا من أهم الأولويات المهمة والحيوية لجميع دول العالم لأنهم يريدون أن يحافظوا على بيانات مواطنيهم وحفظ ممتلكاتهم وبياناتهم الإلكترونية.

7- يعمل الأمن السيبراني على مراجعة وتدقيق تطبيق الضوابط من قبل أطراف مستقلة عن الادارة المعنية بالأمن السيبراني) مثل الادارة المعنية بالمراجعة في الجهة ويعمل الأمن السيبراني على توثيق نتائج مراجعة وتدقيق البيانات السيبرانية، وعرضها على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية. كما تقوم على المراجعة والتدقيق، الملاحظات المكتشفة، والتوصيات والاجراءات التصحيحية، وخطة معالجة الملاحظات.

8- لقد نظم المشرّع الأردني قانون الأمن السيبراني رقم 16 لسنة 2019 ولكن لم ينظم القواعد الاجرائية التي تقوم على حماية الفضاء السيبراني.

9- لم يعمل المشرّع الأردني بضع إجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان

الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الاخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك، وذلك بما يحدد التشريعات الدولية.

10- لم يحدد المشرّع الأردني في حصر فئات التأثير المحتملة لتكون المرجع والاداة التي تسمح للمركز الوطني للأمن السيبراني من تقييم شدة المخاطر وأولوية الحوادث وحجمها وأثرها -من منظور وطني.

11- لم يتناول المشرّع الأردني في القانون الأمن السيبراني رقم 16 لسنة 2019 التقنيات الفنية لخدمات الأمن السيبراني وانما اكتفى، بتنظيم الإطار العام غير واضح يبين الاختصاص الهيكلي (الإداري) للمجلس الوطني للأمن السيبراني في تحديد حوادث الأمن السيبراني وصلاحيات المركز الوطني للأمن السيبراني.

ثالثا: التوصيات

وبعد معرفة المشرّع الأردني، بدوره، كان، بالنسبة لنا، الغائب الأكبر عن مُجاراة هذا التطوُّر، فجاء قانون المعاملات الإلكترونية المؤقَّت خالياً من أيَّةِ إشارةٍ للمركز القانوني لمقدمي خدمات الأمن السيبراني. ونرى، من الأهمية هنا، إبداء التوصيات الآتية:

1- ضرورة مُبادرة المشرّع الأردني لإيجاد قواعد قانونية خاصة ناظمة لالتزامات وحالات قيام مسؤولية مقدمي خدمات الأمن السيبراني: الجزائية، والمدنية، وحالات الإعفاء منها. وهو ما سيترك آثاراً إيجابيَّةً ستؤدي إلى زيادة حجم التبادل المعلوماتي الإلكتروني، وستُشجِّع الإقدام على الاستثمار في هذا القطاع الشرياني، فتعم المنفعة على اقتصادنا الوطني.

2- على المشرّع الدولي وضع الأنظمة والتشريعات الصارمة في حماية الأمن السيبراني من الاختراق ومحاكمة الدول الغير اعضاء في حالة الاختراق اول غير ذلك وذلك يرجع بالمحاكمة الدولية مما يجعل المحافظة على الخصوصية.

3- أغفلت الكثير من التشريعات المعاصرة في هذا المجال، دون أن نعلم الحكمة من ذلك، تنظيم المركز القانوني لبعض مقدمي خدمات الأمن السيبراني، كمقدم خدمة البحث الآلي وخدمة العلاقات النشطة، مما يستوجب على هذه التشريعات تلافي هذا النقص، والمبادرة لتحديد مركزهم القانوني. فالدور المناط بهم القيام به في إدارة الشبكة لا يقل أهميَّةً عن دور باقي المقدمين الذين تمَّ تنظيم مركزهم القانوني.

4- ضرورة أن تسمح التشريعات، في هذا المجال، باللجوء لدعاوى أو لطلبات وقف بثِّ المضمون الإلكتروني غير المشروع، وأن يتمَّ، بدقَّة، تحديد الإجراءات الواجب إتِّباعها لسحبه، أو لمنع وصوله لمستخدمي الشبكة.

5- إلى جانب دعوى المسؤولية عن المحتوى الإلكتروني غير المشروع، يجب تبنِّي فكرة التصحيح الذاتي الفردي والجماعي للأوضاع على الأمن السيبراني، والتعاون من أجل الوصول إلى أمثل استخدام للشبكة، وهذا بدوره يحتاج إلى:

أ. تثقيف مستخدمي الشبكة، وخلق روح المسؤولية لديهم في عمليَّة اختيار المعلومات على الأمن السيبراني، وفي وجوب اتِّباع قواعد السلوك الصحيح أثناء إبحارهم في العالم الافتراضي، بما في ذلك احترام حقوق الآخرين، وعدم الاعتداء على حقوق الملكية الفكرية، وتزويد مقدمي الخدمات بمعلومات حقيقية.

ب. قيام مقدمو الخدمات ببيان القواعد الأخلاقية، وقواعد السلوك الحسن للمشتركين، والتي تكفل احترام القوانين والأنظمة السارية، وعدم المساس بحقوق الآخرين.

6- وأخيراً، إلى جانب أُسلوب التصحيح الذاتي، العمل على إيجاد أُسلوب دولي مُشترك لتصحيح الأوضاع على الأمن السيبراني، من ناحية، ولبيان الأخلاقيات وقواعد السلوك الحسن الواجب على الجميع التحلِّي والتقيُّد بها، من ناحيةٍ أُخرى. ومن الممكن أن يتمثَّل هذا الأُسلوب في إنشاء منظَّمة دولية للإنترنت، تضم حكومات الدول والقائمين على إدارة الشبكة، وتأخذ على عاتقها هذه المهمَّة، أو في وضع ميثاق شرفٍ للتعاون الدولي في هذا المجال.

7- نوصي على المشرّع الأردني العمل على توضيح تدابير واضحة تعنى حماية الأمن السيبراني الوطني، تراعي فيها الطبيعة الفنية والتقنية لحوادث الأمن السيبراني واثارها على القطاعات العامة والخاصة وتصنيفها.

8- على المشرّع الأردني أن يراعي أسس التصنيف الطبيعة التقنية والفنية للحادث وربطه بالقطاع المتأثر به. ومثال ذلك: يعمل المركز الوطني على تصنيف الحوادث وفق طبيعة القطاعات المتأثرة على الصعيد الوطني. لتكون بذلك قد راعت طبيعة عمل هذه القطاعات ومدى أثر التهديد أو لحادث في التأثير على تقديم خدماتها اقتصادياً واجتماعياً.

قائمة المراجع

المراجع العربية

أولاً: الكتب

إبراهيم، خالد ممدوح (2019). **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط1.

أحمد، هلالي عبد اللاه (2013). **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية**، ط1، دار النهضة العربية، القاهرة.

أحمد، هلالي عبداللاه (2013). **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي**، ط1، دار النهضة العربية، القاهرة

بهلوان، علي(د.ت). **استخدام قاعدة البيانات ومنتج التطبيقات**، دار الكتب العلمية للنشر والتوزيع، ط2، القاهرة.

الجنيهي، منير محمد والجنيهي، ممدوح محمد (2016). **جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية، ط1.

حجازي، عبد الفتاح بيومي (2020). **مكافحة جرائم الكمبيوتر والإنترنت**، دار الفكر الجامعي، الإسكندرية.

حجازي، عبد الفتاح بيومي، (2003). **النظام القانوني لحماية الحكومة الإلكترونية**، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى.

حجازي، عبدالفتاح (2012). **الدليل الجنائي في جرائم الكمبيوتر والإنترنت**، دار الكتب القانونية، القاهرة.

حسن، سعيد عبد اللطيف. (2017) . **إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت**، دار النهضة العربية، القاهرة، ط.4

حسن، سعيد عبد اللطيف. (2017) . **إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت**، دار النهضة العربية، القاهرة، ط.4

رستم، هشام (2012). **الجوانب الإجرائية للجرائم المعلوماتية**، ط1، مكتبة الآلات الحديثة، أسيوط

رستم، هشام (2017). **قانون العقوبات ومخاطر تقنية المعلومات**، ط1، مكتبة الآلات الحديثة، أسيوط.

رستم، هشام محمد(2015). **جرائم الحاسب المستحدثة**، دار الكتب القانونية، مصر، ط1.

الرومي، محمد أمين، (2013). **جرائم الكمبيوتر والأنترنت**، دار المطبوعات الجامعية، الإسكندرية

الزعبي، محمد علي (2013). **الحماية القانونية لقواعد البيانات وفقا لقانون حماية حق المؤلف**، ط1، منشأة المعارف، الاسكندرية.

الزيدي، وليد (2019). **القرصنة على الإنترنت والحاسوب**، دار أسامة للنشر، عمان، ط3.

السند، عبدالرحمن (2016). **الأحكام الفقهية للتعاملات الإلكترونية**، الطبعة الثالثة، الرياض: دار الوراق.

شمدين، عفاف (2013): **الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات**، دمشق.

الشوبكة، محمد أمين (2019). **جرائم الحاسوب والانترنت، الجريمة المعلوماتية**، دار الثقافة للنشر والتوزيع، عمان.

طوال، علي حسن (2019). **مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي**، دراسة مقارنة، مركز الإعلام الأمني.

عبابنة، محمد أحمد (2020). **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة، عمان، ط3.

عبدالله، عبدالله عبدالكريم (2011). **جرائم المعلوماتية والإنترنت – الجرائم الإلكترونية**، منشورات الحلبي الحقوقية، بيروت، ط1.

عدنان السرحان ونوري خاطر، (2005) **شرح القانون المدني. مصادر الحق الشخصي** (الالتزامات)، دراسة مقارنة، الطبعة الأولى، الإصدار الثاني، دار الثقافة.

العريان، محمد علي(2019). **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، ط2.

عمار، ماجد(2016). **المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها**، ط1، دار النهضة العربية، القاهر.

فورة، نائلة عادل، (2014). **جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية)** دار النهضة العربية، القاهرة.

فورة، نائلة عادل، (2014). **جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية)** دار النهضة العربية، القاهرة.

الفيل، علي عدنان (2011). **الإجرام الإلكتروني: دراسة مقارنة**، الطبعة الأولى، لبنان

قايد، أسامة عبدالله (2016). **الحماية الجنائية للحياة الخاصة وبنوك المعلومات**، دار النهضة العربية، القاهرة.

قشقوش، هدى حامد (2017). جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة

القطاونة، مصعب (2019). **الإجراءات الجنائية الخاصة في الجرائم المعلوماتية**، بحث مقدّم لشبكة قانوني الأردن.

القهوجي، علي عبد القادر (2016). **الحماية الجنائية لبرامج الحاسب**، ط1، دار الجامعة الجديدة للنشر، الإسكندرية.

قورة، نائلة عادل (2012). **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي الحقوقية، بيروت، ط1.

لطفي، محمد حسام (2012). **عقود خدمات المعلومات**، ط1، بدون ناشر، القاهرة. د.

لطفي، محمد حسام(2016). **الحماية القانونية لبرامج الحاسب الإلكتروني**، ط1، دار الثقافة للطباعة والنشر، القاهرة.

المناعسة، أسامة وجلال الزعبي (2020). وصايل الهواوشة **جرائم الحاسب الآلي الانترنت**، دراسة تحليلية مقارنة، دار وائل للنشر، عمان

منصور، محمد حسين، (2003) **المسؤولية الإلكترونية**، دار الجامعة الجديدة للنشر، الإسكندرية، الطبعة الأولى.

النقروز، علي (2017) **جرائم نظم المعلومات**، دار السناء للنشر، الأردن، عمان.

النقروز، علي (2017) **جرائم نظم المعلومات**، دار السناء للنشر، الأردن، عمان.

يوسف، أمير فرج (2011). **الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت**، ط1، مكتبة الوفاء

اليوسف، عبد العزيز (2015). **التقنية في الجرائم المستحدثة**، بحث ضمن كتاب الظواهر الإجرامية المستحدثة وسبل مواجهتها، منشورات أكاديمية نايف للعلوم الأمنية، لرياض.

يونس، عمر محمد بن(2015). **الجرائم الناشئة عن استخدام الانترنت**، ط1، دار النهضة العربية، القاهرة.

ثانياً: أوراق عمل ومؤتمرات

الاكلبي، مفلح بن دخيل ومحمد، محمد ادم (1430هـ). **دور محتوى مناهج التعليم الثانوي بالمملكة العربية السعودية في مواجهة الإرهاب الفكري والتقني (الواقع والمأمول)**، بحث مقدم المؤتمر الوطني الأول للأمن الفكري (المفاهيم والتحديات)، الفترة من 22–25 جمادى الأول 1430هـ، كرسي الأمير نايف بن عبدالعزيز لدراسات الأمن الفكري، جامعة الملك سعود، 1430 هـ.

جبور، منى الاشقر، (2018). **السيبرانية، هاجس العصر**، جامعة الدول العربية.

جوزيف، جون (2015) **التهديدات السيبرانية في الأمن الوطني**، جامعة هارفارد.

دليل الأمن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات، لعام 2010

رستم، هشام (2009). **جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة**، ورقة عمل مقدمة إلى اللجنة العلمية لإعداد التقرير الوطني المصري لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيوط، عدد 17، القاهرة.

السراج، عبود (2013). **مفهوم جرائم المعلوماتية، واقع وآفاق**، بحث مقدم إلى المؤتمر الإقليمي الأول لمكافحة جرائم المعلوماتية الذي نظمته الجامعة الأردنية واتحاد المحامين العرب خلال الفترة 18–19 كانون الثاني عام 2013.

السعدي، واثبة(2019). **الحماية الجنائية لبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب** المنعقد في جامعة اليرموك – إربد بتاريخ 12–14 تموز، ص 6–7.

سندالي، عبد الرزاق (2017). **التشريع المغربي في مجال الجرائم المعلوماتية**، ضمن أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر 19–20 نيسان، المملكة المغربية.

الشوا، سامي (2009). **الغش المعلوماتي كظاهرة إجرامية مستحدثة**، بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، 25–28.

عطية، أيسر محمد الجرائم، **المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية**، المتلقى العامي، ورقة علمية بعنوان: دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الإلكتروني وطرق مواجهته، كلية العلوم الاستراتيجية، عمان، الأردن.

عوض، محمد محي الدين (2009). **مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات**، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة.

القهوجي، علي عبد القادر(2013). **الحماية الجنائية للبيانات المعالجة إلكترونياً**، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والإنترنت والذي عُقد خلال الفترة من 1–3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية.

المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية (2018). الاتفاقية العربية لحماية الفضاء السيبراني بين الواقع والطموح.

ثالثاً: الرسائل الجامعية

حمدي، خالد(2017). **الحماية القانونية للكيانات المنطقية (برامج المعلومات)**، رسالة دكتوراه، جامعة عين شمس.

السحيباني، عبدالله (2011): **كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات**، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية

طوالبة، علي(2015). **التفتيش الجنائي على نظم الحاسوب والإنترنت**، رسالة دكتوراه، جامعة عمان العربية، منشورة، ط1، عالم الكتب الحديث، إربد.

عرب، يونس خالد (2012). **جرائم الحاسوب**، رسالة ماجستير، الجامعة الأردنية.

العنزي، سليمان (2013): **وسائل التحقيق في جرائم نظم المعلومات**، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية

فلاح، فادي (2015)، **المعلومات الإلكترونية في القانون الأردني**، رسالة ماجستير، الجامعة الأردنية.

قورة، نائلة عادل(2015). جرائم الحاسب الاقتصادية، رسالة دكتوراه منشورة، ط1، دار النهضة العربية، القاهرة.

محمود، عبد الله حسين(2020). **سرقة المعلومات المخزنة بالحاسوب** _ رسالة دكتوراه، جامعة عين شمس.

رابعاً: المجلات والدوريات:

ابو الهيجاء، محمد، الخصاونة، علاء (2009) **المسؤولية التقصيرية لمزودي خدمات الانترنت عن المحتة الغير مشروع**. جامعة اليرموك.

البشري، محمد أمين (2014): **التحقيق في الجرائم المستحدثة**، الرياض: جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث.

جبور، منى الأشقر (2012). **الإطار القانوني للأمن السيبراني والتحديات**، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت 27 – 28 أغسطس (آب) 2012

خاطر، نوري حمد(2012). **حماية المصنفات والمعلومات ذات العلاقة بالحاسوب بقانون حماية حقوق المؤلف**، بحث منشور في مجلة المنارة العدد (2) كانون ثاني جامعة آل البيت، المفرق، ص 35.

رستم، هشام محمد خليل (2012). **الجوانب الإجرامية للجوانب المعلوماتية**، مجلة الأمن والقانون، عدد 2، شرطة دبي.

الشهري، علي زايد محمد الجبيري، (2019). **الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية**، رسالة (دكتوراه)–جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية، تخصص دراسات استراتيجية.

فرح، أحمد قاسم (2007) **النظام القانوني لمقدمي خدمات الإنترنت–دراسة تحليليَّة مقارنة** –قسم الدراسات القانونية، كلية الدراسات الفقهية والقانونية، جامعة آل البيت.

معاشي، سميرة (2011). **ماهية الجريمة المعلوماتية**، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة، الجزائر.

نوري حمد خاطر، (2003) "**الخطأ ألجسيم في ظل تطبيقاته التشريعية والقضائية:** دراسة مقارنة"، المنارة للبحوث والدراسات، المجلد التاسع، العدد الثالث، جامعة آل البيت.

خامساً: المواقع الإلكترونية

البربري، صالح أحمد، دور الشركة في مكافحة جرائم الإنترنت في إطار الاتفاقية الدولية الموقعة في بودابست في 2020/11/23، http:www.arablawinfo.com, p.2

الحربي، عبدالرحمن حراب (2008) الوقاية من الاحتيال المنظم وتجريمه، ص 9، www.almoslim.net/node/163210، تم الحصول على المعلومات بتاريخ 2014/11/24

ستيفن إليوت، "Analysis on Defense and Cyberwarfare," *Infosec Island*, 8 July 2010) https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html (hereinafter "Elliot").

د. سوفاير وسيمور ي. جودمان، *The Transnational Dimension of Cyber Crime and Terrorism*, 2001 at 14, http://media.hoover.org/documents/0817999825_1.pdf

هيئة تقنية المعلومات بسلطنة عُمان، تاريخ الدخول إلى الانترنت 2016/5/9، ص1. http://www.ita.gov.om/

المراجع الأجنبية

A. LUCAS, J DEVÈZE et J. FRAYSSINET, Droit de l´informatique et de l´internet, 1 éd., 2001, PUF, Paris, n° 699, p. 451.

Arthur J. Wylene (2012) PRESENTED AT THE TWENTY THIRD ANNUAL NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE

Avinash Bharti, Terrorism: Perspectives **from Behavioral anciences**, Cyber Tech Publictions, New Delhi, 2010.

By Wayne M. Alder(2018) Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend A Claim.

CA Paris, 10 février 1999, JCP G, II, 10101, note OLIVIER et BARBRY, D. 1999, p. 389, note M. POUJOL, Comm. Com. Électr., 1999, comm. p. 34, note R. DESGORCES, disponible également à l´adresse: www. droit-technologie.org.

CA Paris, 7 juin 2006, précité, « Le prestataire d'hébergement a rempli ses obligations ayant, sans attendre notre décision, pris les dispositions qui ont conduit l'éditeur à empêcher l'accès au jeu litigieux ».

Clasessens, J., Dem,V., De Cock and Van de walle, J. (2002) on the Security of Today's Online Electronic Banking System, Computer and Security. 253-265.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain, United States Government Accountability Office, Sept. 2007, GAO-07-1036, www.gao.gov/new.items/d071036.pdf. In 1997 (hackers attacked the Worcester Airport in the U.S., disabling phone services to the airport tower and shutting down the control system managing the runway lights).

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain, United States Government Accountability Office, Sept. 2007 . pp100-112

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain, United States Government Accountability Office, Sept. 2007 . P312

EVELYNE, JACQUES(2020) REGULATING CYBERSECURITY What civil liability in case of cyber-attacks p . 231

Gion Green, (2016). **Introduction to Security , Fourth Edition**, Revised by Robert J. Fischer , Butterworth's.

Lionel THOUMYRE, "Hyper dossier sur les acteurs de l'Internet en France", juriscom.net, 22 juin 2004, disponible à l'adresse www.juriscom .net /pro/ visu. php? ID= 485.

Luc GRYNBAUM, "LCEN. Une immunité relative des prestataires de services Internet", précité, nº 9, p. 37.

Oqab, R, (2012) The Role of the Audit Committee in Raising the Efficiency of the Internal Control System to Combat Money Laundering in Jordanian Banks. "Journal of Accounting and Public Policy", Volume 26, Issue 3, p: 300 – 327

Oxford Universal Dictionary, **Compiled by Joyce M. Hawkins**, Oxford University Press, Oxford, 1981, p. 736 faculty.ksu.edu.sa/kabbash/paper.visited on 13/12/2011.

Paris (Cour d′Appel de Paris), 9 février 1999, JCP G, 2000, p. 580, note F. OLIVIER CA.

TGI Paris, ord.réf., 22 mai 2000 et 11 août et 20 novembre 2000, (UEJF) c/Yahoo, Communication et commerce électronique, décembre, 2000, p. 25, note J.-C. GALLOUX

TGI Paris, ord.réf., 30 octobre 2001, J´accuse, voir également E. WÉRY, "Affaire J´accuse: les fournisseurs d´accès libérés de l´obligation de filtrage", 2 novembre 2001, article disponible à l´adresse: www.droit-technologies.org, « Qu'en l'état de notre droit positif, les fournisseurs d'accès n'ont aucune obligation que celle de fournir à leurs clients les outils de filtrage ».

Trust in the Information Society: A Report of the Advisory Board RISEPTIS, http://www.think-trust.eu/; David-Olivier Jaquet-Chiffelle, ed., Identity Revolution: Multidisciplinary Perspectives, FIDIS, May 2009, http://www.fidis.net/resources/identity-revolution/

Understanding Cybercrime: A Guide for Developing Countries, at 72, International Telecommunication Union, April 2009, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (hereinafter "Understanding")

Zhang Y. (2013) "Audit Committee Quality, Auditor Independence, and Internal Control Weakness, "Journal of Accounting and Public Policy", Volume 26, Issue 3, p: 300 – 327.