المسؤولية المدنية عن الإضرار بالبيانات السيبرانية

إعداد

تامر سليمان عواد معتوق

إشراف

الدكتور علاء الفواعير

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة

الماجستير في القانون

عمادة البحث العلمي والدراسات العليا

جامعة جرش

شباط، 2024

التفويض

أنا الموقع أدناه الطالب تامر سليمان عواد معتوق، أفوض جامعة جرش بتزويد نسخ من رسالتي بعنوان "المسؤولية المدنية عن الإضرار بالبيانات السيبرانية للمكتبات أو المؤسسات أو الهيئات أو الأشخاص عند طلبهم حسب التعليمات النافذة في الجامعة.

التوقيع:.....

التاريخ:.....

قرار لجنة المناقشة

نوقشت هذه الرسالة الموسومة ب"المسؤولية المدنية عن الإضرار ببيانات الأمن السيبراني وفقاً لأحكام القانون الأردني (دراسة مقارنة)"

وأجيزت بتاريخ..... .

أعضاء لجنة المناقشة التوقيع

أعضاء لجنة المناقشة	المسمّى	التوقيع
الدكتور علاء الفواعير	رئيساً ومشرفاً	
أ.د. منصور الصرايرة	مناقشاً داخلياً	
أ.د. أحمد الحياري/الجامعة الاردنية	مناقشاً خارجياً	

الإهداء

أهدي هذا الجهد العلمي المتواضع إلى صاحبيّ الجلالة الملك عبد الله الثاني بن الحسين والملكة رانيا العبد الله المعظمين، الداعمين والمعززين للبحوث العلمية بكافة مناهجها وأنواعها على مستوى الوطن والعالم، حفظهما الله كما وأهدي ثمرة هذا الجهد إلى مصدر إلهامي وقوتي واعتزازي وإلى من علمني الإصرار والكفاح على النجاح والصبر حين تثقل أحمالي والديّ حفظهما الله، وإلى من تحمّل عناء غيابي عنهم طيلة فترة كتابة هذه الرسالة زوجتي العزيزة وأبنائي سليمان وشجاع حفظكم الله، وإلى أخواني وأخوتي، وإلى أهل العلم الذين غمروني بالحب والتقدير وكانوا لي عوناً بعد الله بما قدموه لي من نصح وإرشاد .

الباحث

الشكر والتقدير

قال الله تعالى عز وجل في كتابه الكريم "وإذ تأذن ربكم لإن شكرتم لأزيدنكم" صدق الله العظيم (القرآن الكريم، سورة إبراهيم، آية 7). فالشكر لله عز وجل الذي يسر لي إكمال دراستي في هذه الجامعة العريقة، وأسأل الله أن يكون هذه الرسالة مما ينتفع به وأنه لعلى ذلك لقدير.

كل الشكر والتقدير إلى أستاذي الفاضل: الدكتور علاء الفواعير لما بذله من جهد وعناء في إشرافه على إنجاز هذا العمل وعلى مقدار ما منحني إياه من وقته الثمين وجهده وعلمه ليخرج هذا العمل إلى حيز الوجود فجزاه الله عنا كل خير.

كما أتقدم بعظيم الشكر والامتنان للأساتذة الكرام الممثلين برئيس وأعضاء لجنة المناقشة على تفضلهم بقبول مناقشة هذه الرسالة، وكذلك الشكر الموصول لجامعة جرش الأهلية التي أتاحت لي فرصة الانضمام إلى الدراسة في حرمها.

الباحث

فهرس المحتويات

الملخص

يعدُ انتشار استخدام تكنولوجيا المعلومات في كافة قطاعات الحياة، وبالأخص لما تتمتع به من ميزات، إضافة إلى سهولة الاستخدام، و إن استخدام هذه التقنيات الحوسبية، يحتاج إلى مجموعة من القائمين عليها، لإدارتها من ناحية، وتقديم الوسائل الفنية والتقنية لتسهيل الاستفادة من شبكة الإنترنت من الناحية الأخرى، وهم ما يعرفون بمقدمي الخدمات عبر الإنترنت، إلا أن الميزات المصاحبة لهذه التكنولوجيا، قد يرافقها مخالفات قانونية، سواء أكانت من مقدمي الخدمات أم من مستخدمي هذه التكنولوجيا، لذلك هدفت دراستي لبيان أحكام المسؤولية المدنية للإضرار بالبيانات السيبرانية في التشريع الأردني والقانون المقارن ، من خلال بيان المقصود بها وأساسها القانوني، وأركانها والأثار المترتبة على قيامها.

وقد تمثلث مشكلة الدراسة في مدى وملائمة القواعد العامة للمسؤولية المدنية ، لقيام مسؤولية منفذي الإضرار ببيانات الأمن السيبراني، ومن هنا كانت أهمية دراسة الموضوع للوقوف على أحكام هذه المسؤولية ومدى كفايتها للتطبيق، وتم أعتماد المنهج الوصفي والتحليلي المقارن في أعداد هذه البحث.

وقد توصلت الدراسة إلى مجموعة من النتائج أهمها، إن التشريع الأردني جاء خالياً من قواعد خاصة تنظّم المسؤولية المدنية لمقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية، وكذلك أوصت بعدة توصيات ومن أهمها، ضرورة تنظيم أحكام قانونية خاصة تعالج الطبيعة التقنية والفنيةالإلكترونية لمقدمي الخدمات عبر شبكات الإنترنت للبيانات، لاستكمال القواعد، العامة في المسؤولية المدنية.

الكلمات المفتاحية المسؤولية العقدية، المسؤولية التقصيرية، الالتزامات، الأمن السيبراني.

SUMMARY

The spread of the use of information technology in all sectors of life, especially because of its advantages, in addition to ease of use, the use of these computing technologies requires a group of those in charge of them, to manage them on the one hand, and to provide technical and technological means to facilitate benefiting from the Internet. On the other hand, they are known as online service providers. However, the features associated with this technology may be accompanied by legal violations, whether from service providers or users of this technology. Therefore, my study aimed to clarify the provisions of civil liability for damage to cyber data in Jordanian legislation and comparative law. By explaining its meaning, its legal basis, its elements and the effects resulting from its establishment. The problem of the study may be represented in the extent and suitability of the general rules of civil liability, for the establishment of the responsibility of the perpetrators of damage to cybersecurity data. Hence, the importance of studying the subject was to determine the provisions of this responsibility and the extent of their adequacy for application, and it was Adopting the descriptive and analytical approach was adopted. The research reached a set of results, the most important of which is that Jordanian legislation was devoid of special rules regulating civil liability for service providers over Internet networks for cyber data. It also recommended several recommendations, the most important of which is the necessity of regulating Special legal provisions that address the technical and electronic nature of data service providers over Internet networks, to complement on the provisions of this responsibility and their adequacy for application, the descriptive and analytical approach was adopted Comparative in the technical and electronic nature.

الفصل الأول:

الإطار النظري للدراسة

المقدمة

تطور تكنولوجيا المعلومات واتجاه الأفراد إلى إدخال هذه التكنولوجيا لجميع مجالات الحياة، سواء أكانت اقتصادية ممثلة بالشركات والبنوك والمصارف أم اجتماعية أو سياسية أو شخصية، واتجاههم بشكل عام إلى أرشفة جميع معلوماتهم وبياناتهم أرشفة إلكترونية بموجب حواسيب، أو بواسطة آلات وخوادم، وباستخدام الإنترنت، كوسيلة نقل معلومات بين الأفراد، أو شركاتهم وتوجههم إلى أن تكون هذه المعلومات معلومات سرية أو تتصف بهذه الصفة على أقل تقدير، وكذلك فإن البنوك والقطاع المالي بدأ يستخدم ما يعرف بالتداول المالي الإلكتروني، وهو ما يتضمن معلومات رقمية، وإلكترونية تتعلق بحسابات العملاء، من حيث مقدارها أو التداول فيما بينهم أو استخدامها في عمليات التجارة.

إن الاتجاه إلى استخدام الوسائل الإلكترونية وأجهزة الحاسوب والانترنت بشكل عام يتميز بخاصية السرعة وسهولة العمل اليومي دون الوقوع في الروتين، ومما يتجلى معه في الأفق إن استخدام هذه التكنولوجيا الرقمية، والتي تعتمد على لغة الأرقام والحواسيب والخوادم، تحتاج إلى نظام حماية لها من أي اعتداء أو اختراق وخاصة أن هذه البيانات المحفوظة على هذه أجهزة وحواسيب يمكن إلحاق الضرر بها بواسطة أجهزة وحواسيب مماثلة لها، باستخدام تقنيات فنية معينة، يصعب معها أحيانا تحديد هوية فاعله، كونه بإمكانه أن يقوم بها من أي بلد في العالم سواء أكان بقصد التخريب أو سرقة البيانات، فكان لا بد من ظهور ما يعرف بالأمن السيبراني (أمن المعلومات).

يعد أمن المعلومات السيبراني من الموضوعات القانونية المستحدثة؛ وذلك كون الهجمات الرقمية قد تأخذ أشكال ومستويات عدة، منها انتحال الهوية أو الابتزاز، وصولاً إلى فقدان البيانات أو الاستيلاء عليها، وبناءً عليه كان لابد من دراسة المسؤولية المدنية للأضرار بالبيانات السيبرانية، ومدى التزامات القائمين على أمن البيانات السيبرانية، و بيان مسؤولية مالكي البيانات في حال المساهمة في الحاق الضرر بتلك البيانات، وفق القوانين الناظمة لها وماهي العلاقة القانونية الناشئة بينهم وبيان مسؤوليتهم، إذا كان الضرر ناتج عن تقصير أو خلل منهم، وماهي مسؤولية كل طرف اتجاه الآخر بناءً على ذلك، وما هي القوانين الناظمة لذلك، وبيان حدود المسؤولية المدنية لما ينتج عن هذه الأضرار.

مشكلة الدراسة:

تكمن مشكلة الدراسة، بالبحث عن مدى كفاية القواعد العامة للمسؤولية المدنية لقيام مسؤولية منفذي الإضرار بالبيانات السيبرانية، وبيان حقوق مالكي تلك البيانات في اللجوء للقضاء، للمطالبة بالتعويض عن ما لحقهم من ضرر هذا من جانب، ومن جانب آخر بيان حدود المسؤولية المدنية في حال ثبوت دور مقدمي خدمات البيانات السيبرانية، بالتسبب في حدوث الضرر بالبيانات السيبرانية مناط المسؤولية.

أسئلة الدراسة:

1. ما مفهوم الامن السيبراني؟
2. ما مفهوم البيانات السيبرانية؟
3. ما الاثار المترتبة على الاضرار بالبيانات السيبرانية؟
4. ما المعايير القانونية التي يمكن الاستناد عليها لتأصيل المسؤولية المدنية لإلحاق الضرر بالبيانات السيبرانية؟

5. ما الأثر المترتب على مساهمة كل من مالكي البيانات السيبرانية ومقدمي الخدمات على مسؤولية محدث الضرر؟

أهداف الدراسة:

1. بيان مفهوم البيانات السيبرانية ومفهوم الأمن السيبراني.
2. بيان التأصيل القانوني للمسؤولية المدنية لإلحاق الضرر بالبيانات السيبرانية
3. تحديد مدى المسؤولية المدنية لمحدث الضرر على البيانات السيبرانية.
4. تحديد مسؤولية مقدمي الخدمات عبر شبكات الإنترنت في حال المساهمة في إلحاق الضرر بتلك البيانات.

أهمية الموضوع وأسباب اختياره:

تنبُع أهمية هذه الدراسة من أهمية وجدّة الموضوع الذي تتناولته؛ حيث يعتبر التطور التكنولوجي وأمن المعلومات من الموضوعات المستحدثة في إطار العمل القانوني، ونظراً لما قد يلحق بالبيانات السيبرانية من أضرار، وما يترتب على هذه الأضرار من تكلفة باهظة، قد يصعب تغطيتها في حال حدوثها، الأمر الذي يترتب عليه أهمية تحديد المسؤولية المدنية لمحدث الضرر.

منهج الدراسة:

سيتم إعداد هذه الدراسة وفقاً للمنهج الوصفي والتحليلي من خلال وصف القوانين والتشريعات المعنية بقواعد المسؤولية المدنية العامة والقوانين الناظمة للأمن السيبراني وتحليلها من خلال دراسة قانون المدني الأردني رقم 43 لسنة 1976م والمنشور بتاريخ 1976/8/1م في الجريدة الرسمية رقم 2645 الصفحة 2 وتعديلاته وقانون الأمن السيبراني رقم 16 لسنة 2019 والمنشور في الجريدة الرسمية رقم 5595 بتاريخ 2019/9/16م، ص5143

وقانون المعاملات الإلكترونية رقم 15 لسنة 2015 وتعديلاته ومقارنتها بالتشريعات العربية الأخرى.

الدراسات السابقة:

وهنا كان لابد من الإشارة إلى الجهد العلمي في دراسة هذا الموضوع لكي لا ننقص حق الآخرين مما سبق وقدموا دراسات وأبحاث علمية أثرت في هذا الموضوع وكانت مرجع لهذا البحث ونذكر منها:

1. أبو الهيجاء، محمد ابراهيم، الخصاونة، علاء الدين، المسؤولية التقصيرية لمزودي خدمات الإنترنت عن محتوى غير مشروع، دراسة في التوجيه الأوروبي الخاص بالتجارة الإلكترونية، بحث منشور في مجلة الشريعة والقانون، العدد 42، أبريل 2010م.

تناولت هذه الدراسة تأصيل المسؤولية التقصيرية، لمزودي خدمات الإنترنت، عن المحتوى غير المشروع، في ضوء التوجيه الأوروبي حول التجارة الإلكترونية لسنة 2000، والقانون الفرنسي حول الثقة بالاقتصاد الرقمي 2004، كما وبينت الدراسة الشروط التي تقوم بموجبها المسؤولية التقصيرية لمزودي خدمات الإنترنت وآثار هذه المسؤولية، وتوصلت لعدة نتائج، منها أن صور الضرر التي تلحق بالبيانات والمعلومات على شبكة الإنترنت، متنوعة وتقع على أشكال مختلفة، وإن إخلال مزودي الخدمات عبر شبكات الإنترنت، بالمراقبة على المحتوى غير المشروع الموكول إليهم بموجب التوجيه الأوروبي والقانون الفرنسي ينهض المسؤولية التقصيرية بحقهم، وتوصلت هذه الدراسة لعدة توصيات كان من أهمها العمل على إعادة صياغة القوانين الناظمة للقواعد العامة للمسؤولية التقصيرية في القانون الأردني، ودراستي هنا تميزت عن الدراسة السابقة ببيان كل ما يتعلق بالمسؤولية المدنية سواء العقدية

أو التقصيرية لكل من مقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية، والغير الذي ألحق الضرر بالبيانات السيبرانية التي لم تتطرق لها الدراسة السابقة الذكر.

2. بني حمد، عبد السلام أحمد، تأصيل المسؤولية العقدية لمتعهد الإيواء في شبكة الإنترنت، في القانون الأردني، بحث منشور في مجلة العلوم للشريعة والقانون، مجلد 45، عدد 4 ملحق 4، بتاريخ 2018م

تناولت هذه الدراسة تأصيل المسؤولية العقدية لمتعهد الإيواء في شبكة الإنترنت في القانون الأردني، دراسة مقارنة، وتوصلت لعدة نتائج منها أن المشرع الأردني على الرغم من تنظيمه قانوناً خاصاً للمعاملات الإلكترونية، إسوة بباقي الدول العربية والأجنبية إلا أنه جاء خالياً من أي إشارة يحدد فيها طبيعة المسؤولية العقدية لمتعهد الإيواء، كما هو الحال في التشريعات المقارنة، وتوصلت هذه الدراسة لعدة توصيات كان من أهمها العمل على إعادة صياغة القوانين الناظمة للمعاملات الإلكترونية لتكون أكثر جراءة ومواكبة للتطور التكنولوجي، ودراستي هنا تميزت عن الدراسة السابقة ببيان كل ما يتعلق بالمسؤولية المدنية سواء العقدية أو التقصيرية لكل من مقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانة، والغير الذي ألحق الضرر بالبيانات السيبرانية التي لم تتطرق لها الدراسة السابقة الذكر.

3. أبو حسين، حنين جميل، الإطار القانوني لخدمة الأمن السيبراني (دراسة مقارنة)، رسالة ماجستير، جامعة الشرق الأوسط، الاردن، تاريخ 2021م، المنشورة على محرك البحث جوجل، **https\\www.meu.edu,jo.**

تناولت هذه الدراسة أساس الإطار القانوني لخدمات الأمن السيبراني وبيان مفهومها ومفهوم الفضاء السيبراني تأثيرها على دول العالم من خلال دراسة مقارنة مع القوانين ذات العلاقة، وتوصلت لعدة نتائج منها أن الأمن السيبراني يقوم على حماية المنظمات والموظفين والأفراد،

ويجب على المنظمات والخدمات تنفيذ أدوات الأمن السيبراني والتدريب على أساليب إدارة المخاطر وتحديث الأنظمة باستمرار مع تغير التقنيات وتطورها، وتوصلت هذه الدراسة لعدة توصيات كان من أهمها بضرورة مباردة المشرع الأردني لإيجاد قواعد قانونية خاصة ناظمة لالتزامات وحالات قيام مسؤولية مقدمي خدمات الأمن السيبراني سواء جزائيا أو مدنيا وحالات الإعفاء منها.

ودراستي هنا تميزت عن الدراسة السابقة ببيان الإطار القانوني لما يتعلق بالمسؤولية المدنية لمتسبب الإضرار باليانات السيبرانية ومسؤولية مقدمي خدمات عبر شبكات الإنترنت في حال المساهمة في مثل هذه الأضرار وبيان حدود مسؤولياتهم في ظل الرابطة القانونية الناتجة عن مسؤوليتهم المدنية التي لم تتطرق لها الدراسة السابقة الذكر.

4- عوايشة، آلاء فراس، المسؤولية المدنية لمزودي الخدمة في الأمن السيبراني، رسالة ماجستير، جامعة عمان العربية، الأردن، تاريخ 2021م، المنشورة على محرك البحث جوجل، **https\\www.aau.edu,jo.**

تناولت هذه الدراسة أساس المسؤولية المدنية لمزودي الخدمة في الأمن السيبراني من خلال الرجوع للقوانين ذات العلاقة ،من ثم تطرقت إلى الفضاء السيبراني وإثارة بين الدول؛ وتوصلت لعدة نتائج من أهمها أن المشرع الأردني لم يعالج في قانون الأمن السيبراني المسائل التقنية والفنية لحادث الأمن السيبراني من حيث الطبيعة والآثار والتصنيف الذي من شأنه التأثير على ضمان الحماية المرجوة من الأمن السيبراني، وتوصلت لعدة توصيات كان من أهمها ضرورة ان تسمح قوانين بعض الدول أن يتم اللجوء للدعاوي أو الطلبات لوقف بث مضمون التقني غير المشروع وان يتم التحديد بدقة الاجراءات الواجب اتباعها لسحبه أو منع وصوله لمستخدمي الشبكة، ودراستي هنا تميزت عن الدراسة السابقة ببيان كل ما يتعلق بالمسؤولية

المدنية للإضرار بالبيانات السيبرانية وبيان القانون الواجب التطبيق في حال كان متسبب الضرر من خارج المملكة التي لم تتطرق لها الدراسة السابقة الذكر.

5. الصرايرة، منصور عبد السلام، المسؤولية التقصيرية الناشئة عن الإخلال بالتزامات مقدمي خدمات الأمن السيبراني، دراسة في التشريع الأردني، بحث مقدم الى المؤتمر الدولي الثاني / الجرائم الإلكترونية والأمن السيبراني / 3-4 مايو 2023م.

تناولت هذه الدراسة تأصيل المسؤولية التقصيرية، لمزودي خدمات الإنترنت، عن المحتوى غير المشروع، في ضوء التشريع الاردني ، كما وبينت الدراسة الشروط التي تقوم بموجبها المسؤولية التقصيرية لمزودي خدمات الإنترنت وآثار هذه المسؤولية، وتوصلت لعدة نتائج، منها أن المشرع الأردني قد عزز الدعم القانوني لحماية خدمات الأمن السيبراني من خلال تعزيز خدمات مقدمي الأمن السيبراني بموجب قانون الأمن السيبراني لسنة 2019م، ، وتوصلت هذه الدراسة لعدة توصيات كان من أهمها ضرورة إيجاد المشرع الأردني قواعد قانونية تضبط التزامات مقدمي خدمات الأمن السيبراني، ودراستي هنا تميزت عن الدراسة السابقة ببيان كل ما يتعلق بالمسؤولية المدنية سواء العقدية أو التقصيرية لكل من مقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية، والغير الذي ألحق الضرر بالبيانات السيبرانية التي لم تتطرق لها الدراسة السابقة الذكر.

الفصل الثاني

ماهية الأمن السيبراني

إن التطور الذي يشهده العالم في تكنولوجيا المعلومات، والازدهار المتزايد فيها من خلال لجوء الدول والأفراد إلى إدخال التقنيات الإلكترونية، واستخدام الاتصالات وتكنولوجيا المعلومات في كافة مجالات الحياة، والتي أصبحت تعتمد في إدامة عملها بشكل أساسي على شبكة الإنترنت، ونتيجة هذا التطور السريع في هذه التقنيات، لسهولة استخدامها إضافة الى تخفيف الكلف والجهد والوقت.

إتجهت الدول ومنها الدولة الأردنية إلى إدخال تكنولوجيا المعلومات لكافة قطاعاتها في المؤسسات العامة، حيث جعلت من الشبكة الإلكترونية ركيزة أساسية في عمل هذه القطاعات، وذلك لتسهيل الإجراءات أمام المستفيدين من خدمات هذه القطاعات، ومثالها الحكومات الإلكترونية، والصحة الإلكترونية، والتعليم عن بعد، والتجارة الإلكترونية والتي تشهد ازدهاراً عالمياً وخلافه من القطاعات.

تزامناً مع ذلك أصبح لكل فرد حساب خاص له في الفضاء الإلكتروني على شبكة الإنترنت، سواء من خلال جهاز الحاسوب أو الهاتف النقال، ليتمكن من التعامل مع غيره وينشئ كافة أنواع المعاملات بكافة أشكالها.

إن استخدام تكنولوجيا المعلومات وفق هذا الازدياد جعل منها محط اهتمام الشراع في الدول و القانونيين المتخصصين، حيث لا يقبل أن يكون هناك نمو في هذه الأنشطة والقطاعات بدون تحقيق الأمن سواء الأمن التقني أو الأمن القانوني، وهذا انطلاقاً لكون الأمن هو اللبنة الأساسية في ازدهار الدول والمجتمعات، والمعيار الأساسي للتطور والحضارة، فأصبح أمن هذه القطاعات مرتبطاً ارتباطاً وثيق بالأمن القومي للدول، وبالأخص مع ظهور مشكلات تتعلق بأمن المعلومات سواء كانت ترتبط بالدولة أو بالأفراد، وعليه كان لا بد بيان مفهوم حماية أمن المعلومات وأهمية هذه الحماية وهذا ما سوف نتناوله في هذا الفصل من خلال مبحثين، المبحث الأول: مفهوم الأمن السيبراني وأهميته والمبحث الثاني: وتنظيم المشرع الأردني للأمن السيبراني.

المبحث الأول

مفهوم الأمن السيبراني وأهميته

تزامناً مع التطور الملحوظ لاستخدام تكنولوجيا المعلومات في كافة المجالات ظهر مصطلح الأمن السيبراني بشكل واسع وملحوظ؛ لكونه يشكل جدار الحماية للمعلومات الخاصة التي يتم تداولها عبر شبكات الإنترنت، سواءً من الدولة أو الأفراد، وهذا ما سوف يبينه الباحث في هذا المبحث من خلال بيان مفهوم الأمن السيبراني ووالأسس التي تبنى عليه أهميته.

المطلب الأول

تعريف الأمن السيبراني

مصطلح الأمن السيبراني مصطلح حديث النشأة؛ حيث ظهر جنباً الى جنب مع تطور استخدام تكنولوجيا المعلومات من قبل الدول ولجوء الأفراد إلى مشاركة معلوماتهم وبياناتهم الخاصة عبر استخدام الإنترنت والفضاء الإلكتروني وفيما يلي بيان تعريف الأمن السيبراني.

الفرع الأول: التعريف اللغوي للأمن السيبراني

يتطلب ذلك بيان المعنى اللغوي لمصطلح الأمن ومصطلح السيبراني.

جاء في تعريف الأمن لغةً "الأمن من أَمِنَ يَأْمَنُ أَمْناً، فهو آمِن وأَماناً، وأَمِنَ الرُّجُلُ اِطْمَأَنَّ ولم يَخَفْ، وكذلك فالأمْنُ يعني الاستقرار والاطمئنان نقول أَمِنَ مِنْهُ أي سَلِمَ مِنْهُ، وأَمَنَ على مَالِه عند فُلانٍ أي جَعْلَهُ في ضَمانَتِهِ، فالأمن والأمانة بمعنى واحد، الأَمْنُ ضد الخَوْفِ والأَمَانَةٌ ضد الخَيَانِةٌ

والمَأمَنُ الموضع الآمِنُ " [1] وجاءت كلمة الأمن في مواضع كثيرة في القرآن الكريم ومن ذلك قوله تعالى "أَطْعَمَهُم مِّنْ جُوعٍ وَأَمَنَهُم مِّنْ خَوْفِ" [2].

أما تعريف الأمن السيبراني في اللغة فعند البحث عن التعريف اللغوي للأمن السيبراني نجد أن المعاجم العربية جاءت خالية الوفاق من هذا المصطلح، ولا جذور لغوية له فيها، ويرجع هذا لكون هذا المصطلح غربي وحديث المنشأ، وفي البحث في المعاجم الغربية (القاموس) نجد أن كلمة السيبراني "(syper) لاتينية الأصل وهي تعني التَخْيُلي أو التقني" وجاء ايضاً في تعريف مشتقات هذه الكلمة "حالة الأمان من الجريمة الإلكترونية والإجراءات المتخذة لتنفيذ ذلك " [3].

الفرع الثاني: الأمن السيبراني اصطلاحا

الأمن اصطلاحا "هو الإحساس بالطمأنينة يشعر به الفرد، سواء بسبب غياب الأخطار التي تهدد وجوده، أو نتيجة لامتلاكه الوسائل الكفيلة بمواجهة الأخطار حال ظهورها" [4]

ويجد الباحث أن الأمن هو ما استقر في خلجات النفس من شعور بالراحة، والاستقرار، والمأمن على النفس والمال وما ارتبط بهما، وكرسه العمل المادي بممارسة النشاط الاعتيادي بدون خوف يصطحب هذا النشاط.

وعرف المشرع الأردني الأمن السيبراني بأنه" الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية، والبنى التحتية الحرجة، من حوادث الأمن السيبراني والقدرة على استعادة عملها

---

[1] أبن منظور، توفي سنة (711هـ)، لسان العرب، مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت، 1987م، ص163

[2] القرآن الكريم، صورة قريش، آية 4

[3] قاموس، (2020)،oxford ، أنظر (cybersecurity)، وقاموس، (2020)، word-reference

[4] زهرة عطا محمد، الامن القومي العربي، (1991)، بنغازي، جامعة قاريونس، بحث منشور على http;\\www,nli.org.il تاريخ الدخول 24 / 6 /2023 م وقت الدخول الساعة 16:00

واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الإخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك [1] " .

وجاءت التشريعات الدول العربية لوضع تعريف للأمن السيبراني حيث لم تبتعد كثيراً عما ورد لدى شراح القانون والمنظمات الدولية بل أنها ربطت هذا المصطلح بالأمن القومي ومنها التشريع المصري حيث جاء في الدستور المصري اعتبار أمن الفضاء السيبراني للمعلومات جزء أساسي من منظومة الاقتصاد والأمن القومي، وألزم الدولة وضع قوانين تنظم الإجراءات اللازمة لحماية أمن المعلومات [2]" وعليه يتضح أن المشرع المصري وضع أساس تشريعي للأمن السيبراني، وجاء أيضاً في التشريع المصري اعتبار الأمن السيبراني متصل باستقلال واستقرار أمن الوطن وحدة سلامة أرضه [3].

وعرف التنظيم السعودي الأمن السيبراني أنه " حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع [4]" ويرى الباحث أن المنظم السعودي نهج نفس النهج بجعله مفهوم الأمن السيبراني شامل لأمن المعلومات والأمن الإلكتروني والأمن الرقمي بشكل عام وواسع.

جاء أيضاً من هذه التعريفات أن الأمن السيبراني هو "عبارة عن مجموعة الوسائل التقنية والإدارية التي تستخدم لمنع الوصول غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية

---

[1] المادة (2) قانون الأمن السيبراني رقم 16 لسنة 2019م، والمنشور في الجريدة الرسمية رقم 5595 بتاريخ 2019/9/16م، ص5143

[2] انظر المادة 31، الدستور المصري وتعديلاته لسنة 2014م

[3] أنظر المادة 1، قانون مكافحة جرائم تقنية المعلومات رقم 175 سنة 2018م

[4] تنظيم الهيئة الوطنية للأمن السيبراني الصادر بأمر ملكي رقم 6801 عام 1439هـ والمشار الية في الضوابط الأساسية للأمن السيبراني الملحق (أ) مصطلحات وتعريفات

ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظام المعلومات وتأمين الحماية وسرية وخصوصية البيانات الشخصية لحماية المواطنين والمستهلكين في الفضاء السيبراني " وهو التعريف الذي تطرقت له المنظمة الدولية المتخصصة التابعة للأمم المتحدة في مجموعة السياسات والأدوات للاتحاد الدولي للاتصالات عام 2008م[1].

عرف أيضاً حسب التقرير الصادر عن الاتحاد الدولي للاتصالات في عام 2010م"هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى وتقنيات يمكن استخدامها لحماية البنية السيبرانية، وموجودات المؤسسات والمستخدمين" [2].

وتجدر الإشارة هنا ان التشريعات العربية لم تكن بعيدة عما ورد في التشريعات الغربية، حيث قدمت وزارة الدفاع للولايات المتحدة تعريفاً دقيقاً لمصطلح الأمن السيبراني وعرفته بأنه "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم، الهجمات ، التخريب، التجسس، الحوادث "، وكذلك اعتبر الاعلان الاوروبي حول الأمن السيبراني أن معنى الأمن السيبراني هو " قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات" وهذا ما أكدة أستاذ الاتصالات في جامعة كاليفورنيا "ريتشارد كمرر" حيث عرف الأمن السيبراني هو "عبارة عن وسائل دفاعية من شأنها أن تكشف وتحبط المحاولات التي يقوم بها القراصنة " [3].

---

[1] انظر مقال بعنوان الامن السيبراني وادارة مخاطرة في مجال الأعمال، أعداد غسان الطالب، والمنشور بتاريخ (19 /أكتوبر /2019م) في محرك البحث جوجل على الرابط http://cutt.ly.gbtcv7u، تاريخ الدخول (6 /2023/7م، ساعة الدخول 13:30)

[2] دليل الأمن السيبراني للبلدان النامية، الاتحاد الدولي للاتصالات، لعام (2010م)، ص 421

[3] أنظر، بو غراره يوسف، (2018)، الأمن السيبراني، الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني، مجلة الدراسات الأفريقية وحوض النيل، العدد3، المجلد 1، المركز الديمقراطي العربي، ص207

وعرفه كذلك بعض شراح القانون بأنه " هو جملة المهمات والأدوات والطرق والاستراتيجيات والمبادئ والإجراءات الأمنية والمبادئ التوجيهية والمقاربات الخاصة بإدارة المخاطر، والتدريبات والممارسات المثلى والتكنولوجيا التي يكون في مقدورها أن تواجه وتحمي البيئة السيبرانية" [1].

ويرى الباحث هنا أن هذه التعريفات جاءت فضفاضة وشاملة، لكل من أمن المعلومات والاتصالات وحتى المعاملات الإلكترونية وسائل الحماية لها ولعل الهدف من هذا لكون هذا المصطلح وضع في إطار واسع لحداثته ولمحاولة ان يكون شمولي وفي نطاق العمومية بأكثر قدر ممكن.

يعرف الباحث مفهوم الأمن السيبراني على أنه "مجموعة الإجراءات المتخذة من قبل الهيئات المعنية، والتي تعتمد على خليط مركب من التقنيات الإلكترونية والفنية الهادفة لحماية البيانات والمعلومات للأفراد والشركات والمؤسسات الحكومية ذات الطابع السري والشخصي في المجمل والمستخدمة بوسائل إلكترونية".

يتطلب الأمر منا بعد بيان التعريف بالأمن السيبراني الإشارة الى ركائز الأمن السيبراني والمستمدة من التوصيات الصادرة عن الإتحاد الدولي للاتصالات للإحاطة أكثر بتعريف مفهوم الأمن السيبراني حيث جاء فيها أن صلاحيات الأمن السيبراني الوطنية تعتمد على ركائز منها[2].

1. تشكيل إستراتيجية وطنية للأمن السيبراني وحماية البنى التحتية للمعلومات الهامة والسرية وتطويرها.
2. تحقيق التعاون بين الحكومات والشركات المعنية بالاتصالات وتكنولوجيا المعلومات لترسيخ الأمن السيبراني وردع الجريمة السيبرانية.

---

[1] جاب الله عادل، (2022)، وسائل حماية الامن السيبراني، دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، بحث منشور في مجلة كلية الشريعة والقانون، جامعة الازهر، ص2243

[2] الفتلاوي حمزة صيوان، (2015م)، الأمن السيبراني والحروب السيبرانية، مجلة خيمة العراق، وزارة الدفاع، العدد357، السنة الثالثة، ص 1

3. العمل على بناء ثقافة وطنية للأمن السيبراني، وخلق قدرات وطنية للإدارة حوادث الحاسب الآلي.

استكمالاً لركائز الأمن السيبراني، وللقدرة على بناء مفهوم الأمن السيبراني لابد من الإشارة الى الجهات المناط بها مهمة الأمن السيبراني، على الرغم من أن هذا المهمة تكون لأكثر من جهة في وقت واحد، حيث تتداخل معه الاختصاصات لتحقيق التكاملية في هذه المهمة، إلا أن التشريعات العربية جعلت حماية الأمن السيبراني تقع على عاتق هيئة مستقلة، فقد تكون مثلاً وزارة معينة أو مجلس أو اتحاد، وهذا يختلف من دولة الى أخرى حسب مقتضى الحال، ففي جمهورية مصر العربية، وحسب القرار الصادر عن مجلس وزرائها رقم 2259 لسنة 2014م ، يكون المسؤول عن الأمن السيبراني المجلس الأعلى للأمن السيبراني، وفي المملكة العربية السعودية ، وحسب الأمر الملكي رقم 6801 لعام 1439هـ ، تتولى هذه المهمة الهيئة الوطنية للأمن السيبراني، وفي المملكة الأردنية الهاشمية، ووفقاً للقانون الأمن السيبراني لسنة 2019م يكون المجلس الوطني للأمن السيبراني المناطة به هذه المهمة .

على الرغم من إناطة مهام حماية الأمن السيبراني لهيئات معينة، إلا أنه قد تشترك جهات أخرى في مثل هذه الحماية فمكافحة الجريمة الإلكترونية لو وردت في التعريفات السابقة فهي سياسة جنائية تنظمها الدول في الأغلب أما بإسقاط القواعد العامة الجزائية على الجرائم السيبرانية أو تشريع قوانين مستقلة تكفل مكافحة هذه الجريمة [1].

إن أمن الشبكات بما يخص حماية البنى التحتية، من أجهزة وحواسيب أو حسابات شخصية أو شركات مزودي الخدمات، حتى لو كان يدخل في مفهوم الأمن السيبراني إلا أنه يقع على عاتق

[1]Kriangask kittchaisaree (,2017), public international law of cyberspace,springer international publishing Switzerland, p263

جهات معينه غير سابقة الذكر أعلاه منها وزارة الاتصالات، أما حماية النظام والآداب العامة في الفضاء السيبراني، فهو أيضاً يقع ضمن اختصاص جهات أخرى منها وزارة الداخلية والأجهزة التابعة لها [1].

بقي الإشارة الى مصطلحات لها صلة وثيقة بمفهوم الأمن السيبراني وبشكل موجز ؛ لأنها تعد مفتاح له وهي الفضاء السيبراني والبنية التحتية للأمن السيبراني. [2]

المطلب الثاني

أهمية الأمن السيبراني

إن ثورة تكنولوجيا المعلومات التي يشهدها العالم، وانتشارها المهول، التي لا يكاد مجال من مجالات الحياة يخلو منها، وما رافق هذه التكنولوجيا من إيجابيات، إلا انها حملت معها العديد من التهديدات والمخاطر التي ظهرت بصورة جرائم إلكترونية، لم تفرق بين الأشخاص والمؤسسات والشركات مما دعى الى تعزيز الحماية وضرورة توفير أمن إلكتروني لمواجهة هذه التهديدات وهو ما يعرف بالأمن السيبراني [3].

الأمن السيبراني جاء مرادف للتطور في استخدام تكنولوجيا المعلومات ومن هنا جاءت أهميته في إمكانية مواجهة التهديدات سواء أكانت متعمدة أو غير متعمدة وسرعة حل هذه التهديدات ومعالجتها

([1]James Graham,Richard Howward,Ryan Olson"edit",(2011), cyber security Essentials, Taylor &francis croup,new york , p25

[2] الفضاء السيبراني: وهو "بيئة تتكون من تفاعل الأشخاص والبيانات والمعلومات ونظام المعلومات والبرامج على الشبكات المعلوماتية وأنظمة الاتصالات والبنى التحتية المرتبطة بها"، البنية التحتية "مجموعة من الأنظمة والشبكات الإلكترونية والأصول المادية وغير المادية أو الأصول السيبرانية "، المادة (2) من قانون الأمن السيبراني الأردني رقم 16 لسنة 2019م

[3] بارة سمير، (2017)، الدفاع الوطني والسياسات الوطنية للأمن السيبراني (cyber security) في الجزائر، الدور والتحديات، ط2، الملتقى الدولي حول سياسات الدفاع الوطني بين الالتزامات والتحديات الإقليمية، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، الجزائر، ص426.

والتعافي منها [1]، وسوف يتم بيان أهمية الأمن السيبراني من خلال إستعراض أهم القطاعات التي يشملها، والأهداف التي يتوخاها.

الفرع الأول: القطاعات التي يشملها الأمن السيبراني بخدماته

لا يقتصر الأمن السيبراني على قطاع محدد بذاته أو مجال عمل بعينه، فهو يشمل كل قطاع اعتمد بشكل أساسي على تسيير معاملاته وأعماله بواسطة شبكة الانترنت، أي أن هذه المجالات تنتمي إلى الفضاء الإلكتروني، سواء كان باتصال مباشر أو غير مباشر، ومنها ذو الطابع الاقتصادي والاجتماعي والسياسي وسنوضح أهم هذه القطاعات استناداً إلى طابعها العام

أولاً : القطاع الاجتماعي:

الأمن السيبراني للأفراد والمجتمعات يستمد أهميته وأصوله التاريخية من احترام خصوصية وسرية الأفراد، التي أقرتها الأديان السماوية أولاً والأعراف ثانياً، وتم تجسيدها في الإعلان العالمي لحقوق الإنسان حيث جاء الإعلان مؤكداً على عدم المساس أو التدخل التعسفي في حياة الفرد الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، وعدم المساس بمكانته بين الناس وشرفه، بل وأكد الإعلان على أن كل فرد له الحق في أن يحميه القانون من ذلك [2].

أصبح استخدام شبكة الإنترنت جزء لا يتجزأ من أي مجتمع، كونه بات الرابط بين المجتمعات الحقيقية والمجتمعات الافتراضية على شبكة الإنترنت، فأصبح كل فرد يستطيع التعبير عن تطلعاته وطموحاته الاجتماعية بكافة الأشكال وبكل سهولة، حيث اختلط كل من الواقع الحقيقي والواقع

---

[1] أنظر فاطمة علي ابراهيم، ورحاب يوسف، ووليد محمود السيد، (2022)، الأمن السيبراني والنظافة الرقمية، بحث منشور، المجلة المصرية لعلوم المعلومات، مجلد 9، عدد 2، ص 397 وما بعد.

[2] أنظر المادة الثانية عشر من الاعلان العالمي لحقوق الأنسان الصادر 10 / كانون الأول / 1948.

والافتراضي بشكل يصعب معه الفصل فيما بينهما، مما ينتج عنه انفتاح المجتمعات على بعضها البعض وبالتالي يكون هناك تبادل للخبرات والأفكار التي ينتج عنها احتياجات جديدة[1].

تتضح أهمية الأمن السيبراني للقطاع الاجتماعي من خلال المحافظة على المجتمعات من أي محاولة لتعديل الهندسة الاجتماعية وإدخال سلوكيات وعادات غير متعارف عليها لتغيير ثقافة أو معتقد مجتمع معين من خلال مراقبة هذا الاستخدام ليكون أمن، لذلك دأبت الدول الحديثة على أن تكون تشريعاتها في هذا الإطار لحماية حريات وحقوق الأفراد مع حماية المجتمعات من أي تهديد إلكتروني، إضافة الى تعين جهات فنية مختصة في الحماية السيبرانية لتحقيق هذه الحماية.

نضيف الى ذلك أن حماية الأمن السيبراني ترتبط في حماية الحياة الخاصة للأفراد في ظل استخدام تكنولوجيا المعلومات في سائر شؤون حياتهم، فاستخدام الإنترنت والحاسوب وخلافه قد ينطوي في الغالب على معلومات شخصية تتسم بالسرية ولها مساس مباشر في سمعته ومكانته مستخدمها، وهذا ما دفع أيضاً تشريعات الدول ومنها الأردن لترسيخ هذا المبدأ حيث صدر في عام 2023م قانون حماية البيانات الشخصية للأفراد من خلال القواعد العامة لحماية البيانات[2] هدفه أسباغ الصفة التشريعية على هذه الحماية.

ويرى الباحث أن أهمية الأمن السيبراني بالنسبة للأفراد تتجلى من خلال حماية بياناتهم الشخصية الموجودة على حساباتهم الشخصية وحواسيبهم ومنها كلمة المرور وصور والملفات والفيديوهات ونحوه.

---

[1] العنزي سلمان، (2003)، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، الرياض، جامعة نايف للعلوم الأمنية، والمنشورة على الأنترنت على موقع الإلكتروني http;\\archive.org تاريخ الدخول 3 \ 8\ 2023م ساعة الدخول 12:00.

[2] أنظر قانون حماية البيانات الشخصية رقم 24 لسنة 2023م، المنشور في الجريدة الرسمية بتاريخ 2023/9/17م، عدد 5881، ص4338

ثانياً: القطاع المالي والاقتصادي

يرتبط الأمن السيبراني بعلاقة وطيدة بالقطاع الاقتصادي؛ حيث يتم ممارسة الأنشطة الاقتصادية المختلفة بوسائل إلكترونية ولا سيما التجارة التي أضحت من أهم الركائز الاقتصادية في الأغلبية العظمى لدول العالم التي اتجهت إلى التجارة الإلكترونية وما يرافقها من التعامل المالي الرقمي والمعاملات المصرفية المالية والتي تتم إلكترونياً [1].

وعليه انتهجت البنوك والمصارف والشركات لتسهيل على عملائها إعتماد الدفع الإلكتروني والبطاقات المصرفية الذكية والحسابات المالية التي تعتمد على البيانات الرقمية [2]، لذلك تسعى الشركات والمصارف المالية والبنوك، للحفاظ على سمعتها، من خلال وجود نظام حماية أمن وفعال للمحافظة على أمن معلومات عملائها من أي تهديد قد يلحق بها، فأصبح امتلاك فريق أمن سيبراني من قبل تلك الشركات والبنوك من أهم ركائز تعزيز الثقة بينها وبين عملائها، ومساهم أساسي في جلب العملاء لها، ومساهم أساسي للإبقاء على معيار النزاهة والمصداقية فالاستمرار في مراقبة الأنظمة المستخدمة من قبل الشركات والبنوك والعملاء من أي اختراق أو تهديد ينعكس بصورة إيجابية وفعالة عليها ويجعل منها وجهة أمنة للتعامل معها بكافة أشكال المعاملات من قبل العملاء [3].

---

[1]حسن إشراق، (2020)، الحماية المدنية للاموال الالكترونية دراسة مقارنة، بحث منشور على مجلة التربية، جامعة واسط، كلية القانون، العدد29، ص581).

[2]انظر دراسة بعنوان العملات المشفرة، البنك المركزي الاردني، دائرة الاشراف والرقابة على نظام المدفوعات الوطني، (اذار ،2020)، والمنشور على موقع البنك المركزي الاردني http\\www.cbj.gov.jo ساعة الخول20:55 تاريخ الدخول 2023/8/4م).

[3] مقال بعنوان اهمية الأمن السيبراني، اعداد الصوالحة رشا والمنشور بتاريخ (16/ 11/ 2021م) في محرك البحث جوجل على الرابط http://mawdoo3.com، (تاريخ الدخول2023/7/27م، ساعة الدخول 22:30)

ثالثاً: القطاع السياسي والعسكري

يعد القطاع العسكري من أهم القطاعات التي يقوم الأمن السيبراني بخدماته المختلفة بتغطيتها، لا سيما أن الحروب الإلكترونية أصبحت حقيقة واقعية وهناك العديد من النماذج على ذلك ومنها الحرب الروسية الأوكرانية، حيث قامت روسيا بشل الحكومة الأوكرانية إلكترونياً وإيقافها بشكل كامل قبل اندلاع النزاع المسلح، ومثاله أيضاً ما حدث في جورجيا حيث تطور إلى نزاع مسلح بين روسيا وجورجيا، وكذلك انقطاع الإنترنت في أستونيا بين المواطنين والدولة مما أدى إلى تشويش الإدارات الحكومية هناك، وما حصل من اختراق المنشآت النووية الإيرانية مما يهدد الأمن والسلم الدولي، وكذلك ما حصل في البرازيل والمملكة المتحدة من اختراق البنية التحتية للطاقة حيث انقطع فيها التيار الكهربائي مما الحق الضرر بملايين الأشخاص والمؤسسات العامة والمصالح وكل ما أسبق هو أبلغ مثال على مخاطر الحرب السيبرانية [1].

إن تطور التكنولوجيا المعلومات والاتصالات لم يعد يقتصر على الدول وحروبها فقط في القطاع السياسي والعسكري؛ فبعد أن جعل الإنترنت المجال واسعاً ومفتوحاً خالياً من أي حدود فيمكن لمستخدمه الوصول الى أي بلد في العالم بدون قيود أو معوقات وكل ما يحتاجه المستخدم بعض المعلومات والتقنيات ليستطيع اقتحام الحواجز الإلكترونية، حيث استغلت ذلك بعض الجماعات الإرهابية واستفادة من ذلك من خلال الدعاية والترويج لأفكارها المتطرفة باستغلال المواقع الإلكترونية والفضاء الإلكتروني ونشر الإرهاب بكافة أشكاله [2].

---

[1] أنظر ستيفن إليوت، (2010)، july، 8 ، island، infosec ، cyber and defense on analysis" warfare" والمنشور على موقع https;\\Infosesisland.com\blogvie5160-Analysis-on-Defense-and cyber-warfare.html (ساعة الدخول16:20 تاريخ الدخول 2023/8/5م).

[2] المعموري علي، (2020)، الأمن السيبراني ودورة في انتشار ظاهرة الإرهاب في العراق بعد عام 2003م، بحث مستل من رسالة ماجستير، كلية العلوم السياسية، جامعة بغداد، منشور في مجلة الدراسات الدولية، العدد 80، ص 158 وما بعد.

لا يقل القطاع السياسي أهمية عن القطاع العسكري، فالسياسة هي فن التعامل مع الغير، والدول تتعامل مع غيرها من الدول وفق سياسات تراعي فيها مصالحها وأمنها القومي، ومن هنا للدولة حق حماية نظامها السياسي في ظل التطور باستخدام التكنولوجيا ، حيث أصبح للفرد القدرة عن التعبير عن آرائه السياسية بكل سهولة بعض النظر عن صحة هذه الآراء التي قد تصل لمستوى النقد والاعتراض على سياسة الدولة، حيث أصبح الفضاء الإلكتروني منبر للترويج عن الأفكار السياسية والمبادئ، والمواقف من الحكومات والدول، وهذا قد ينطوي على مخاطر عدة منها تعكير صفو العلاقات بين الدول أو التحريض على الكراهية، والعنصرية من جانب آخر[1]، وغيره من الجرائم المتصلة بذلك، وهو ما يظهر معه جلياً دور الأمن السيبراني في حماية الأمن القومي للدول.

يرى الباحث أن أهمية الأمن السيبراني تستمد من أهمية القطاع الذي يستخدم تكنولوجيا المعلومات في إدارته بغض النظر عن طبيعة هذا القطاع فلا أفضلية لقطاع على أخر، فلا تقوم الدول بلا المحافظة على مجتمعاتها واقتصادها وأمنها الداخلي والخارجي من أي ضرر إلكتروني قد يلحق بتلك القطاعات.

الفرع الثاني: أهمية الأمن السيبراني تبعاً للأهداف التي يسعى لتحقيقها

لنتمكن من بيان أهمية الأمن السيبراني بشكل أدق فلا بد من بيان الأهداف التي يسعى الأمن السيبراني لتحقيقها، من خلال حماية البيانات، والمعلومات المستخدمة في الفضاء الإلكتروني، حيث يستمد الأمن السيبراني أهميته من تحقيق هذه الأهداف بل ويرتبط وجوداً بها وهذا ما سيبينه الباحث من خلال بيان أهم الأهداف وبشكل مقتضب:

---

[1] البشري محمد أمين، (2004م)، بحث بعنوان التحقيق في الجرائم المستحدثة، الرياض، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، السعودية.

أولاً: تأمين وحماية البنية التحتية لأمن المعلومات

نظراً لارتباط البنية التحتية بالأمن السيبراني وأهميتها فقد بينتها معظم التشريعات العربية، حيث عرفها التشريع الأردني على انها "مجموعة من الأنظمة والشبكات الإلكترونية والأصول المادية وغير المادية أو الأصول السيبرانية والأنظمة التي يعد تشغيلها ضرورة لضمان أمن الدولة واقتصادها وسلامة المجتمع "[1] .

كما ورد بالتنظيم السعودي أن البنية التحتية الوطنية تشمل المرافق والنظم والشبكات والعمليات والعمال الأساسيين الذين يقمون بتشغيلها ومعالجتها وجميع الاصول التي يؤدي فقدانها أو تعرضها لانتهاكات أمنية الى أضرار في النواحي الاقتصادية والاجتماعية والأمن القومي ونحوه[2].

إن البنية التحتية للأمن وتكنولوجيا المعلومات ،تعد اللبنة الأساسية التي تقوم عليها تلك المعلومات، كون البنية التحتية تشمل الأدوات ومنها الأجهزة والحواسيب والخوادم (سيرفرات)، وحتى كوابل توصيل الإنترنت والأبنية، وكل ما اتصل باستخدام تكنولوجيا المعلومات ، وكذلك الأنظمة الرقمية الإلكترونية المستخدمة في حماية البيانات والمعلومات، بل وأحياناً تشمل الاشخاص العاملين عليها إذا ارتبطت بهم وجوداً، وعليه فإن نجاح المؤسسات والأفراد في تحقيق الأمن السيبراني للبنية التحتية يحقق استقرار تلك المؤسسات وعملياتها أمنياً، فحفظ البيانات الخاصة بالمؤسسة أو الأفراد يسهم إيجاباً في عمل المؤسسات وينعكس على أداء العاملين فيها ويحقق الإبداع المرجو منهم [3].

---

[1] أنظر المادة (2) من قانون الأمن السيبراني الأردني.

[2] تنظيم الهيئة الوطنية للأمن السيبراني الصادر بأمر ملكي رقم 6801 عام 1439هـ والمشار الية في الضوابط الأساسية للأمن السيبراني الملحق، مرجع سابق.

[3] فاطمة علي، وآخرون، (2022)، الأمن السيبراني والنظافة الرقمية ن مرجع سابق، ص399.

يرى الباحث أن الحفاظ على البنية التحتية من أي ضرر يلحق بها سواء متعمد أم غير متعمد هو من أهم أهداف الأمن السيبراني والذي يحتاج لتطوير التقنيات والتكتيكات الفنية بشكل مستمر لمواجهة أي ضرر قد تتعرض له، كون تلك التقنيات بحاجة لمواكبة التطور بشكل مستمر.

ثانياً: حماية البيانات ومعلومات الأفراد من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

لبيان هذا الهدف لابد من بيان المقصود بقواعد البيانات والتي عرفت على أنها "مجموعة كبيرة من البيانات موضوعة بطريقة منتظمة بحيث يمكن الوصول اليها بسهولة وإجراء العمليات المختلفة عليها إلكترونياً" [1]، أما المعلومات "فهي مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون موضوعاً للتبادل أو الاتصالات أو التغير أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية "[2].

إن أهم أهداف الأمن السيبراني هو اتخاذ التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة أثناء استخدام الانترنت في مختلف المجالات، ومنها حماية الأنظمة التشغيلية و قواعد البيانات والمعلومات من أي محاولة للدخول اليها بشكل غير مسموح به لأهداف غير سليمة، وكذلك ضمان توافر استمرارية عمل نظم المعلومات [3]، وهنا يمكن القول أنه تتعدد أشكال إلحاق الضرر بالمعلومات فقد تكون على شكل أرسال برامج، أو رموز، أو شيفرة، أو أوامر بشكل متعمد ينتج عنه ضرر في حاسوب يتمتع بالحماية وقد يكون إلحاق الضرر من

---

[1] البهلوان علي، (2009) استخدام قاعدة البيانات ومنج التطبيقات، دار الكتب العلمية للنشر والتوزيع، ط2، مصر، القاهرة، ص 21.

[2] مغبغب نعيم، (2006)، حماية برامج الكمبيوتر، منشورات الحلبي، ط 1، بيروت، لبنان، ص 205 وص206.

[3] مقال بعنوان الأمن السيبراني والثورة الصناعية الرابعة، اعداد الربعي علي محمد والمنشور بتاريخ 12 \ فبراير \2020م في محرك البحث جوجل على الرابط http;\\www.okaz.com\articles\outhors2010045، تاريخ الدخول 8\2023/8، ساعة الدخول 22:30).

خلال الدخول عمداً الى حاسوب محمي بدون تفويض ينتج عنه ضرر سواء قصداً أو بسبب الأهمال[1].

يرى الباحث أن أهمية الأمن السيبراني مستمدة من تحقيق الحماية لمعلومات، وقواعد البيانات التي يتم معالجتها باستخدام الحاسوب، سواء نصوص أو صور أو رموز أو ملفات أو برامج أو بيانات شخصية من قبل الأفراد بواسطة الفضاء الإلكتروني، فدخول الأفراد بدون قيود على المواقع المختلفة على شبكة الانترنت والفضاء الإلكتروني ومشاركتهم معلوماتهم وبياناتهم التي تتم معالجتها في الحاسوب تحتاج للأمن السيبراني للمحافظة عليها من أي ضرر يلحق بها.

[1] ميلاد علي ميلاد، (2007م)، رسالة ماجستير، جريمة أتلاف نظم المعلومات (دراسة مقارنة)، كلية الدراسات القانونية العليا، جامعة عمان العربية لدراسات العليا.

المبحث الثاني

التنظيم القانوني للأمن السيبراني وفقاً لتشريع الأردني

الأردن وكسائر دول العالم، ونتيجة لتطور أهمية الأمن السيبراني وتكنولوجيا المعلومات، كان من السباقين لإيجاد إطاراً قانونياً لتنظيم الأمن السيبراني غايته حماية المعلومات والأنظمة الإلكترونية ومكافحة الجرائم السيبرانية، وهذا ما سوف يتم بيانه من خلال بيان التنظيم القانون للأمن السيبراني ، وتحديد الجهات المعنية به وفقاً لتشريع الأردني .

المطلب الأول

الإطار التشريعي للأمن السيبراني في الأردن

سن المشرع الأردني مجموعة من القوانين والأنظمة الهدف منها وضع أحكام تنظم الأمن السيبراني داخل المملكة الأردنية الهاشمية وتنظم الخدمات الخاصة به أيضاً أسوةً بالدول الأخرى ومنها جمهورية مصر، وسوف يبين الباحث ذلك من خلال إستعراض قانون الجرائم الألكترونية الأردني وقانون الأمن السيبراني الأردني وقانون حماية البيانات الشخصية الأردني.

الفرع الأول: قانون الجرائم الإلكترونية.

يعد قانون الجرائم الإلكترونية أحد القوانين الأساسية التي تنظم الجرائم الإلكترونية في الأردن جزائياً ، وهو يسعى إلى حفظ المعلومات والبيانات ويمنع الاعتداء عليها، وهو ما يتفق مع مفهوم الأمن السيبراني، كما جاء قانون الجرائم الإلكترونية رقم 27 لسنة 2015 وبين المقصود بنظام المعلومات وشبكة المعلومات حيث عرفها بأنها "ارتباط بين أكثر من نظام معلومات لإتاحة

البيانات والحصول عليها [1] "، وكذلك بين القانون ما المقصود بالموقع الإلكتروني والتصريح باستخدامه والدخول الى شبكة المعلومات، وكذلك بين عقوبة الدخول العمد بدون تصريح أو تجاوز حدود التصريح وإلحاق الضرر بالشبكات ،أو الاطلاع أو الحصول على البيانات والمعلومات المتعلقة بالأفراد أو تنفيذ المعاملات المالية والمصرفية الإلكترونية بدون حق وبوجه غير مشروع ، وإشتمل على مجموعة من الجرائم المتعلقة بالاختراقات الإلكترونية والتزوير الإلكتروني والاحتيال الإلكتروني والتجسس الإلكتروني والاستغلال الجنسي وغيرها من الجرائم التي تتم بوسائل الإلكترونية وكذلك بين الجرائم المتعلقة بالقدح والذم والتحقير الإلكتروني [2].

لكن التطور السريع في مجال تقنية المعلومات ، وبسبب ظهور بعض الأفعال التي تتم بوسائل الإلكترونية والتي لم يتطرق لها القانون السابق، استوجب ضرورة إصدار قانون جديد للجرائم الإلكترونية لتحقيق الردع العام والخاص، و توفير مزيداً من الحماية للحريات العامة والأشخاص فأقر قانون الجرائم الإلكترونية رقم 17لسنة 2023م من قبل مجلس الأمة الأردني موشحاً بالإرادة الملكية بتاريخ 13\8\2023م [3]، والذي جاء فيه مجموعة مفاهيم لم تكن بالقانون السابق ومنها مفهوم منصة التواصل الاجتماعي والعنوان الإلكتروني و خط سير البيانات ومفهوم مزود الخدمة، وكذلك المقصود بالبنى التحتية الحرجه، كما وبين مجموعة من الجرائم المستحدثة مثل جرائم الابتزاز الإلكتروني وجرائم العنف الإلكتروني، وأضاف جرم اغتيال الشخصية "وهي كل إتهام بدون وجه حق للأشخاص عبر منصات التواصل الاجتماعي " كما فرض عقوبات أشد ووسع من

---

[1] أنظر المادة 2، قانون الجرائم الإلكترونية رقم 27 لسنة 2015، المنشور بتاريخ 1 \ 6 \2015م في الجريدة الرسمية رقم 5343، ص5631.

[2] أنظر المادة 3والمادة 12، قانون الجرائم الإلكترونية رقم 27 لسنة 2015م

[3] مقال بعنوان الجرائم الإلكترونية مشروع قانون يغلظ العقوبات، اعداد الشوابكة لينا والمنشور بتاريخ 30\7\2023م في محرك البحث جوجل على الرابط http://www.bbc.com، تاريخ الدخول11\8\2023م، ساعة الدخول (23:30

صلاحيات المحكمة المختصة في إيقاف أي موقع عن ممارسة نشاطه للمدة التي تراها مناسبة ، شرط أن تكون ارتكبت أي من الجرائم المنصوص عليها في القانون المعدل [1].

يجد الباحث أن قانونا الجرائم الإلكترونية رقم 27 لسنة 2015م ورقم 17 لسنة 2023م اقتصرا على الجرائم العمدية فقط، والتي تسبب إلحاق الضرر بالمعلومات والبيانات سواء للأفراد او المؤسسات والدولة، ولم يتطرقا الى فرضية حدوث مثل ذلك الضرر بدون قصد ونتيجة الخطأ، على رغم من تشديده العقوبة في حال ارتكبت الجرائم الواردة فيه من موظف بحكم عمله لكنه اشترط العمدية على الرغم من إمكانية حدوثها نتيجة الإهمال من قبل الموظف.

بعد استقراء التشريع المصري حول الجرائم الإلكترونية بالرجوع الى قانون جرائم تقنية المعلومات رقم 157 لسنة 2018م، نجد المشرع شمل كل من الجرائم العمدية، وجرائم الخطاء وفرض عليها عقوبة وقسم القانون لفصول ليشمل معظم أنواع الجرائم التقنية والأشخاص العاملين فيها من مستخدمين أو مقدمي الخدمة أو نقالي الخدمة ونحوه [2]، مما جعله أشمل وأوسع نطاقاً من التشريع الأردني الذي لم يتطرق من خلال قانون الجرائم الإلكترونية الأردني.

الفرع الثاني: قانون الأمن السيبراني رقم 16 لسنة 2019م

كانت المملكة الأردنية الهاشمية من الدول السباقة بسن التشريعات التي تنظم مفهوم الأمن السيبراني، ومن هذه التشريعات قانون الأمن السيبراني رقم 16 لسنة 2019م والذي يعد الإطار التشريعي للجهات المعنية بالأمن السيبراني، حيث ورد فيه مجموعة من المصطلحات التي تعنى بمفاهيم الأمن السيبراني، ومنها تعريف الفضاء السيبراني ومفهوم الأمن السيبراني والذي يلاحظ

---

[1] أنظر قانون الجرائم الإلكترونية رقم (17) لسنة 2023م والمنشور بتاريخ 13\8\2023م في الجريدة الرسمية، ص3579.

[2] أنظر قانون جرائم تقنية المعلومات رقم 175 لسنة 2018م، والمنشور في الجريدة الرسمية العدد 33مكرر(ج) في 14\أغسطس\2028م، ص3 وما بعدها.

فيه الشمولية وتحديد أشكال الاعتداءات سواء عمدية أو غير عمدية ".... سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الإخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك" [1]،وجاء فيه بيان التصريح باستخدام نظام المعلومات والشبكة المعلوماتية من قبل أصحاب العلاقة، وبيان أشكال هذا الاستخدام، كما وجاء فيه بيان ما المقصود بالبيانات والمعلومات، والبنية التحتية الحرجة، والبرامج ،كما و جاء فيه بيان مفهوم حادث الأمن السيبراني هو "الفعل والهجوم الذي يشكل خطراً على البيانات أو المعلومات أو نظم المعلومات أو الشبكة المعلوماتية أو البنى التحتية المرتبطة بها ويتطلب استجابة لإيقافه أو التخفيف من العواقب أو الآثار المترتبة" [2]، ويلاحظ هنا شمول حادث الأمن السيبراني الفعل ويقبل هنا الفعل الناشئ عن عدم العمدية (الخطآء) وكذلك الهجوم وهي كلمة تدل على العمدية بإحداث الضرر ووفق المشرع بجعل الحادث يشمل كلا التصرفين.

إن قانون الأمن السيبراني لعام 2019م هو قانون تنظيمي وليس تجريمي ويوفر مراكز استجابة لتنظيم جهود المعنيين كافة وفق سند قانوني وتشريعي [3]، حيث حدد الجهات المعنية بالأمن السيبراني، من حيث التشكيل والواجبات، وهي المجلس الوطني للأمن السيبراني والمركز الوطني للأمن السيبراني [4]، وهذا ما سوف نتطرق له في مبحث مستقل.

بقي أن نشير إلى أن حوادث الأمن السيبراني عابرة للحدود وتقع في بيئة رقمية تتسم بالخطورة ويمتاز مرتكبوها بالتخصصية والمهارة في استخدام تكنولوجيا المعلومات ، لتحقيق أهدافهم سواء

---

[1] المادة 2، قانون الامن السيبراني الأردني، رقم 16 لسنة 2019م

[2] المرجع نفسه

[3] مقال بعنوان قانون الأمن السيبراني تنظيمي وليس تجريمياً، اعداد القضاة يعرب والمنشور بتاريخ 2020/11/28م، في محرك البحث جوجل على الرابط http;\\www.patra.gov.jo، تاريخ الدخول 13\8\2023م، ساعة الدخول 16:05.

[4] أنظر المادة 3 والمادة 5، قانون الأمن ال سيبراني رقم 16 لسنة 2019 م.

للعبث أو التخريب أو التسلية، أو الانتقام، لذا سعت الدول لتوحيد جهودها للحد من مخاطر تلك الحوادث، وكانت الأردن من تلك الدول؛ وقعت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2012م ، ونظمت هذه الاتفاقية الأحكام الموضوعية والإجرائية لحوادث الأمن السيبراني، وبيت أشكال التعاون القانوني والقضائي في تطبيقها [1]،وكذلك صادق الأردن على اتفاقية بودابست الدولية لعام 2001م، والتي تعد الاتفاقية الدولية الوحيدة على مستوى العالم التي تهدف الى توسيع الاختصاص الدولي في متابعة الجرائم الإلكترونية [2].

الفرع الثالث: قانون حماية البيانات الشخصية رقم 24 لسنة 2023 م

يعد قانون حماية البيانات الشخصية أحد القوانين التي عُنيت بأمن البيانات والمحافظة عليها من أي إعتداء، وهذه الحماية ما يتماشى ومفهوم الأمن السيبراني، حيث أرسى القانون حق حماية البيانات الشخصية، وعدم الاعتداء عليها من قبل الغير أو معالجتها بدون موافقة مالكها أو الأحوال المصرح بها قانوناً [3]، وكذلك بين القانون المقصود بالبيانات الشخصية؛ حيث عرّفها بأنها "أي بيانات أو معلومات تتعلق بشخص طبيعي ومن شأنها التعريف به بطريقة مباشرة أو غير مباشرة ...."، وبيّن كذلك المقصود بالبيانات الشخصية الحساسة التي تدل على أصل مالكها أو عرقه أو تدل على آرائه أو انتماءاته السياسية أو معتقداته الدينية أو أية بيانات تتعلق بوضعة المالي أو حالته الصحية أو الجسدية أو العقلية ونحو ذلك أو بيانات يقرر المجلس اعتبارها حساسة إذا كان إفشاؤها أو سوء استخدامها يلحق الضرر بالشخص المعني بها، وكذلك بيّن المقصود بالبيانات و

---

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لسنة (2012م) المنشورة في الجريدة الرسمية بتاريخ، 17\6\2012م، رقم5162

[2] اتفاقية بودابست، لعام (2001م)، الاتفاقية المتعلقة بالجريمة الإلكترونية، المجلس الأوروبي مجموعة المعاهدات الاوروبية رقم 185 والمنشورة على محرك البحث قوقل على الرابط الإلكتروني http;\\rm.coe.int تاريخ الدخول 13/8/ 2023م، ساعة الدخول 23:48.

[3] المادة 4، قانون حماية البيانات الشخصية لسنة 2023م

قواعد البيانات، وإن هذا القانون اهتم بهذه البيانات كونها ترتبط بالأمن الشخصي للأفراد، وإن الفرد جزء من المجتمع، فالحفاظ على أمن بياناته هو حفاظ على أمن المجتمعات بشكل عام وهو ما يتوافق مع الأهمية التي يلعبها الأمن السيبراني في القطاع الاجتماعي، كما بيّن القانون الطرق التي يمكن أن تعالج بها البيانات الشخصية من قبل مالكيها؛ حيث خول لهم الحق في العلم، والاطلاع والوصول إلى البيانات الموجودة لدى أي شخص طبيعي أو اعتباري سواء أكان داخل المملكة أو خارجها وتكون هذه البيانات في عهدته (وهذا ما يعرف بالمسؤول)، ومنحه مالكها الموافقة المسبقة على معالجة هذه البيانات، كما خوله سحب هذه الموافقة أو التصحيح أو التعديل أو الإضافة أو التحديث لتلك البيانات، أو تخصيص المعالجة في نطاق محدود أو الاعتراض على المعالجة، وكذلك يحق له نقل نسخة من بياناته من مسؤول إلى مسؤول آخر، وكذلك يحق لمالك البيانات معرفة أي اختراق أو انتهاك أو إخلال بأمن وسلامة بياناته، [1] وعرف القانون كذلك في المادة الثانية منه المقصود بالإخلال بإمن وسلامة البيانات بأنه " أي وصول غير مشروع أو عملية أو نقل أو إجراء غير مصرح به على البيانات".

كما أن من أوجه الحماية للبيانات الشخصية أن المشرع في المادة المادة من هذا القانون حدد حالات التي يجوز بها إجراء معالجة بيانات شخصية دون الحصول على الموافقة المسبقة أو إعلام الشخص ومنها:

1. المعالجة التي تتم مباشرة من قبل جهات عامة مختصة بالقدر الذي يقتضيه تنفيذ القانون.
2. إذا كانت هذه المعالجة ضرورية للأغراض الطبية الوقائية أو التشخيص الطبي أو تقديم الرعاية الصحية من مرخص له من مزاولة المهن الطبية.

---

[1] أنظر المادة 2، والمادة 4، قانون حماية البيانات الشخصية لسنة 2023م

3. إذا كانت ضرورية لحماية ذات الشخص المعني (مالك البيانات) أو لحماية مصالحه الحيوية أو كانت ضرورية لمنع جريمة أو الكشف عنها من قبل الجهات المختصة.

4. إذا كانت هذه المعالجة بموجب أي من التشريعات النافذة أو بقرار من المحكمة المختصة.

5. إذا كانت مطلوبة لأغراض قيام الجهات الخاضعة لرقابة وإشراف البنك المركزي الأردني بأعمالها وفقاً لما يقرره البنك المركزي.

6. إذا كانت بقصد البحث العلمي أو التاريخي شريطة أن لا يكون الغرض منها اتخاذ أي قرار أو إجراء بشأن شخص محدد.

7. إذا كانت هذه البيانات ضرورية لأغراض الإحصاء والأمن القومي أو لتحقيق المصلحة العامة.

8. إذا كان محل المعالجة بيانات متاحة للجمهور من الشخص المعني.[1]

كما بيّن القانون أنه لا يجوز الاحتفاظ بهذه البيانات بعد الانتهاء من الغرض التي عولجت من أجله ما لم تنص التشريعات على خلاف ذلك، و بيّن القانون الشروط التي يجب أن تتوافر في هذه المعالجة وكذلك حدد الواجبات التي تقع على عاتق المسؤول التي تكون هذه البيانات في عهدته، فيقع عليه حمايتها وتوفير الوسائل الآلية والفنية لتأمين هذه الحماية وتوفير الوسائل من أجل تمكين مالكيها من ممارسة حقوقهم المقررة بموجب هذا القانون، كما بيّن الإجراءات المتّبعة من قبل المسؤول ليتمكن من محو أو إخفاء البيانات بناءً على طلب من مالكها أو في تحقق مجموعة من الحالات منها إذا تمت المعالجة لغير الغرض الذي جُمعت من أجله أو بشكل غير الذي تمت الموافقة المسبقة عليه أو سحب الشخص المعني الموافقة المسبقةأو خضعت البيانات للمعالجة خلافاً للقانون إذا كان تنفيذ الالتزام قانوني أو تعاقدي.[2]

---

[1] انظر المادة 6 /أ من قانون حماية البيانات الشخصية لسنة 2023م

[2] انظر المواد 8 و9 و10 من قانون حماية البيانات الشخصية لسنة 2023م

يرى الباحث أن هذا القانون اهتم بالبيانات الشخصية للأفراد الطبيعيين على الرغم من الممكن أن يكون هناك بيانات شخصية للأفراد الاعتباريين ينطبق عليها ما ينطبق على البيانات الشخصية للأفراد.

المطلب الثاني

الهيئات المعنية بتنظيم الأمن السيبراني وفقاً للتشريع الأردني

المشرع الأردني سن قانون الأمن السيبراني رقم 16 لسنة 2019م ليكون قانوناً تنظيمياً لا تجريمياً، حيث ورد فيه الهيئات المعنية بتنظيم الأمن السيبراني في المملكة الأردنية الهاشمية وهما المجلس الوطني للأمن السيبراني، والمركز الوطني للأمن السيبراني.

الفرع الأول: المجلس الوطني للأمن السيبراني

أنشأ المجلس الوطني للأمن السيبراني قانوناً بموجب نص المادة الثالثة من قانون الأمن السيبراني لسنة 2019 [1]، حيث يتشكل المجلس من رئيس يعين بقرار ملكي، ومعه أعضاء ممثلون عن وزارة الاقتصاد الرقمي والريادة والبنك المركزي والقوات المسلحة الأردنية و دائرة المخابرات العامة ومديرية الأمن العام والمركز الوطني للأمن السيبراني وإدارة الأزمات بالإضافة إلى ثلاثة أعضاء يتم تسميتهم من مجلس الوزراء لمدة سنتين يجوز التمديد لهم لمره واحدة فقط، ويلزم هؤلاء الأعضاء أن يكون عضوين منهم من أصحاب الخبرة ويتبعان للقطاع الخاص [2].

نص قانون الأمن السيبراني لعام 2019م على كيفية انعقاد المجلس، والنصاب القانوني في اتخاذ قراراته، حيث يجتمع المجلس لأربع مرات في العام الواحد من خلال دعوة توجه من قبل الرئيس أو نائبه، ويكون هذا في الأحوال الاعتيادية، إلا إذا استدعت حالة طارئة إلى اجتماع المجلس فيتم

---

[1] المادة 3، قانون الأمن السيبراني رقم 16 لسنة 2019.

[2] عبابنة، محمد، (2020)، جرائم الحاسوب وأبعادها الدولية، مرجع سابق، ص239.

دعوته عندها للانعقاد حتى لو استنفذ الاجتماعات الأربعة، أما بما يخص النصاب القانوني فقد بين القانون أن الاجتماع يكون منعقداً قانونياً بحضور ما لا يقل عن ثلثي أعضائه وتتخذ قراراته بأغلبية إصوات الأعضاء الحاضرين [1].

منح قانون الأمن السيبراني المجلس مجموعة من الاختصاصات والصلاحيات نوجزها بالآتي:

- إقرار الخطط والسياسات والاستراتيجيات والمعايير الخاصة بالأمن السيبراني.
- إقرار المخططات والبرامج التي تضمن سير عمل المركز وفق المهام المحددة له ضمن إطار التعاون الاقليمي والدولي في مجال الأمن السيبراني.
- اعتماد التقارير المقدمة له سواء المتعلقة بالأمن السيبراني للمملكة وتكون على شكل ربع سنوية، أو التقرير المتعلق بأعمال المركز الوطني للأمن السيبراني والذي يكون بشكل سنوي.
- إقرار الموازنة السنوية للمركز الوطني للأمن السيبراني
- تشكيل اللجان التنسيقية من أصحاب العلاقة وتحديد كيفية اجتماعهم واتخاذ القرار وواجباتهم ومهامهم ويكون الهدف منها تمكين المركز الوطني من تحقيق أهدافه [2].

الفرع الثاني: المركز الوطني للأمن السيبراني

الهدف الأساسي من إنشاء المركز الوطني هو تأسيس منظمة قانونية فعالة للأمن السيبراني على الصعيد الوطني، تعمل من خلال ممارسة أنشطتها على تطوير وتنظيم الأمن السيبراني في المملكة، من خلال أصباغ الحماية على المملكة من أي تهديدات أو أخطار سيبرانية يمكن التعرض لها، لذلك أقر لهذا المجلس شخصية اعتبارية ليتمكن من تملك الأموال المنقولة وغير المنقولة وإجراء جميع التصرفات القانونية ومن ضمنها إبرام العقود والتقاضي وينوب عن المركز في

---

[1] أنظر مادة 7/3/ج، قانون الامن السيبراني.

[2] مادة 4، قانون الأمن السيبراني الأردني.

إجراءات التقاضي وكيل إدارة قضايا الدولة ، كما ويرتبط المجلس برئيس الوزراء ويكون مقره في العاصمة عمان مع قدرته على إنشاء فروع أخرى في محافظات المملكة [1].

أناط قانون الأمن السيبراني رقم 16 لستة 2019 م بموجب المادة السادسة منه مجموعة من الصلاحيات والاهداف للمركز الوطني للأمن السيبراني يمكن إجمالها بما يلي:

- وضع الخطط والسياسات ومعايير الأمن السيبراني ورفعها للمجلس للموافقة عليها، والإشراف على تنفيذها.
- تطوير عمليات الأمن السيبراني وتنفيذها، وتقديم الدعم والاستشارة اللازمين لتشكيل فرق أمن سيبراني متخصصة في القطاعين العام والخاص.
- وضع المعايير والضوابط الخاصة بالأمن السيبراني، والتي تستخدم في تصنيف حوادث الأمن السيبراني.
- إصدار التراخيص لمقدمي خدمات الأمن السيبراني.
- تفعيل التعاون والشركات الوطنية والإقليمية والدولية من خلال إبرام الاتفاقيات ومذكرات التفاهم في ما يخص الأمن السيبراني.
- تعزيز الوعي الوطني للأمن السيبراني من خلال تطوير برامج بناء القدرات والخبرات الوطنية في قطاع الأمن السيبراني.
- تعزيز أمن الفضاء السيبراني من خلال توحيد الجهود والتنسيق مع الجهات المختصة.
- التعاون مع الجهات المعنية لأعداد مشروعات التشريعات المرتبطة بالأمن السيبراني ورفعها للمجلس.

---

[1] المادة 5 والمادة 6/أ قانون الأمن السيبراني.

- تقييم وضع الأمن السيبراني في المملكة بشكل مستمر بالتنسيق مع الجهات المختصة في القطاعين العام والخاص.
- تحديد البنى التحتية الحرجة، وإنشاء قاعدة بيانات بالتهديدات السيبرانية، وتطوير الفرق للاستجابة لهذه التهديدات.
- إعداد معايير أمن وحماية المعلومات ودعم البحث العلمي في مجال الأمن السيبراني بالتنسيق مع الجامعات.
- إعداد الموازنة السنوية للمركز، وإعداد التقرير السنوي عن أعمال المركز وبياناته المالية.
- إعداد التقارير الربع سنوية عن الوضع السيبراني في المملكة ورفعه للمجلس [1].

ويشير الباحث هنا إن تشكيلات دوائر الحكومة ودرجاتها وأسمائها وهيكلها التنظيمي وكيفية تعين موظفيها وعزلهم والإشراف عليهم، وحدود صلاحياتهم بموجب وظائفهم، والاختصاص المكاني والموضوعي لهم يكون بموجب أنظمة خاصة تصدر من قبل مجلس الوزراء بموافقة جلالة الملك وهذا راسخ ومحدد بموجب الدستور الأردني [2]، وبناءً على ما سبق صدر نظام خاص للمركز الوطني للأمن السيبراني في عام 2020م تحت اسم نظام المركز الوطني للأمن السيبراني والذي يبين صلاحيات ووظائف رئيس المركز وارتباطاته وكيفية إدارة أعماله والتنسيق مع الجهات المعنية للتحقيق أهداف المركز [3].

صدر للمركز الوطني للأمن في عام 2012م نظام تحت اسم نظام التنظيم الإداري للمركز الوطني للأمن السيبراني، حيث بين النظام الهيكل التنظيمي للمركز، من ناحية الرئيس والإدارات التابعة

---

[1] المادة 6/ب، قانون الامن السيبراني الأردني.

[2] أنظر المادة 120 الدستور الأردني وتعديلاته لسنة 1952م.

[3] أنظر نظام المركز الوطني للأمن السيبراني رقم 1لسنة 2020، والمنشور في الجريدة الرسمية رقم 5614 بتاريخ 2020/1/2م، ص1.

له، وهي إدارة العمليات وإدارة الاستخبارات السيبرانية وما يتبع لهما من مديريات، وبين النظام كذلك اللجان المختصة بالتخطيط وتنسيق والتعاون وواجباتهم وكيفية اجتماعها والنصاب القانوني للاجتماعات وكيفية إصدار القرارات، كما ومنح رئيس المركز بموجب هذا النظام الصلاحية بإصدار التعليمات اللازمة لتنفيذ أحكامه [1].

بعد أن تم بيان مفهوم الأمن السيبراني وأهميته والإطار القانوني والتشريعي للأمن السيبراني وفق التشريع الأردني نكون قد أنهينا الفصل الثاني من هذه الرسالة وفي صدد بحث المسؤولية المدنية لمزودي خدمات الإنترنت وعلاقتهم بالأمن السيبراني في الفصل الثالث وبيان التزاماتهم القانونية والفنية وارتباطها بمفهوم الأمن السيبراني وما يقع على عاتقهم نتيجة إلحاق أي ضرر ببيانات الأمن السيبراني سواء متعمد أم غير متعمد.

[1] نظام التنظيم الإداري للمركز الوطني للأمن السيبراني رقم 25لسنة 2021م، والمنشور في الجريدة الرسمية رقم 5721 بتاريخ 2021/6/1م، ص2006.

الفصل الثالث

الالتزامات القانونية لمقدمي خدمات البيانات السيبرانية

يقوم الأمن السيبراني على مجموعة من الأشخاص، سواء أشخاص طبيعيين أم اعتباريين يقع على عاتقهم تقديم خدمات الأمن السيبراني، حيث تتنوع واجباتهم ومهماتهم وتختلف أدوارهم، ومن الممكن لشخص واحد بنفس الوقت أن يقوم بمهمة أو أكثر، وهنا يظهر جلياً أهمية تحديد التزامات هؤلاء الأشخاص وخاصةً أن منهم من تتسم طبيعة عملة بطابع معلوماتي ومنهم من تتسم بطابع فني [1].

فبيان التزامات مقدمي الخدمات، يِسهل من خلاله تحديد إطار المسؤولية المدنية عن أي إضرار يلحق بالبيانات السيبرانية نتيجة الإخلال في الالتزامات الملقاة على عاتق مقدمي الخدمات وهو ما سيتم بيانه في هذا الفصل والفصل الذي يليه.

لم يتطرق المشرع الأردني في قانون الأمن السيبراني لسنة 2019م إلى تحديد الالتزامات التي تقع على كاهل مقدمي خدمات عبر شبكات الإنترنت بشكل واضح ودقيق، واقتصر على التنظيم القانوني لمقدمي خدمات الأمن السيبراني، من خلال عدم السماح لأي شخص أو جهة بتقديم خدمات الأمن السيبراني إلا بعد الحصول على التصاريح والتراخيص القانونية الأزمة لذلك، بدون بيان أي التزامات تفرضها هذه التصاريح أو التراخيص [2]، وكذلك لم يسن المشرع الأردني نظاماً قانونياً مستقلاً لمقدمي خدمات الأمن السيبراني، فكان لابد من بيان الخدمات التي يقدمها مقدمي خدمات الأمن السيبراني، وتحديد التزاماتهم وفقاً لهذه الخدمات بالرجوع إلى التشريع المقارن والتشريع الأردني في القواعد العامة من خلال مبحثين هما: إلتزمات مقدمي الخدمات المعلوماتية كمبحث أول والإلتزمات الفنية لمقدمي خدمات البيانات السيبرانية كمبحث ثاني.

---

[1] ابو الحسن حنين جميل، (2021م)، الإطار القانوني لخدمة الأمن السيبراني (دراسة مقارنة)، رسالة ماجستير، جامعة الشرق الأوسط، كلية الحقوق، قسم القانون الخاص، ص74 وما بعد.

[2] المادة 10/أ، قانون الامن السيبراني رقم 16 لسنة 2019، مرجع سابق.

المبحث الأول

التزامات مقدمي الخدمات المعلوماتية

تزايد الإقبال على استخدام تكنولوجيا المعلومات من قبل الأفراد والشركات والحكومات بشكل مهول في جميع مجالات الحياة جعل من المواقع الإلكترونية على شبكات الإنترنت وجهة للاستثمار وسبباً لكسب المال، وهذا نظراً لقلة التكلفة والجهد والوقت، مقارنة بغيرها من القطاعات، فكان لابد من تنوع عملية تقديم الخدمات المعلوماتية على شبكات الإنترنت، والتي تقع على نوعين؛ النوع الأول يمثل إيواء المعلومات، من خلال ما يسمى متعهد الإيواء، وهو من يقدم خدمة إيواء المعلومات والبيانات ويكون دوره إدارة المعلومات على شبكات الأمن السيبراني وتقديم جميع التسهيلات أمام مستخدمي هذه المواقع، بتوفير الوسائل الفنية، والتقنية لهم، والمساحات اللازمة لتخزين المعلومات والبيانات وحفظها وسهولة الرجوع إليها [1]، وهذا ما سيبينه الباحث بالتفصيل في المطلب الأول من هذا الفصل، والنوع الثاني من مقدمي خدمات المعلومات هم موردي المعلومات وتقع على عاتقهم أما جمع المعلومات والبيانات، أو تأليفها، وإنشائها، ومن ثم توريدها عبر شبكات الأمن السيبراني، وتقع عليهم مجموعة من التزامات وهذا ، ما سوف يتم بيانه بالمطلب الثاني من هذا الفصل.

[1] منصور محمد حسين، (2003م)، المسؤولية الإلكترونية دار الجامعة الجديدة للنشر مصر، طبعة 1، ص239.

المطلب الأول

التزامات متعهد الإيواء لخدمات الأمن السيبراني

تعتمد تكنولوجيا المعلومات في عملها على أدوات تقنية وفنية تدار من قبل أشخاص متخصصين، الهدف منها تسهيل استخدامها من قبل مستخدمي هذه التكنولوجيا، علاوة على أن هذا القطاع أصبح وجهة للاستثمار، فهو يعتمد على أدوات ووسائل فنية وتقنية، منها شبكات الإنترنت، وخوادم تعتمد على أقراص، ومساحات للحفظ المعلومات والبيانات، يمكن الرجوع إليها في أي وقت وهذه التقنيات تحتاج إلى أشخاص يديرونها ويشرفون عليها وهم أصلاً من يتيحون هذه المساحات أمام المستخدمين ، وهو ما يعرف بالإيواء ولتحديد التزامات متعهد الإيواء لابد بيان تعريف متعهد الإيواء اصطلاحا وقانونا.

الفرع الأول: مفهوم متعهد الإيواء

يعرّف اصطلاحاً" هو شخص طبيعي أو معنوي، يعرض إيواء صفحات ل(web) على حساباته الخادمة العملاقة مقابل أجر" [1] وعرفه الفقه الفرنسي "شخص طبيعي أو معنوي يتولى تخزين وحفظ البيانات والمعلومات لعملائه، ويوفر الوسائل الفنية والمعلوماتية التي تسمح لهم بالحصول على هذه البيانات والمعلومات طوال ساعات اليوم وذلك عبر الإنترنت [2] باستقراء النصوص القانونية لتعريف متعهد الإيواء قانوناً نجد المشرع الأردني، لم يورد نصً قانوني مباشر، يبين المعنى القانوني لمتعهد الإيواء، واكتفى بالإشارة في نصوص متفرقة منها المعاملات الإلكتروني لسنة 2015م حيث جاء فيه تعريف المنشئ "هو الشخص الذي بقوم بإنشاء رسالة المعلومات

---

[1] حجازي عبد الفتاح بيومي، (2008م)، الحكومة الإلكترونية بين الواقع والطموح، مصر، دار الفكر الجامعي، ج2، ص344.

[2] المتعهد الإيواء في شبكة الإنترنت في القانون الأردني، مرجع سابق، ص345.

وإرسالها" وعرف الوسيط الإلكتروني فيه أيضاً بـ"البرنامج الإلكتروني الذي يعمل لتنفيذ إجراء، أو الاستجابة، لإجراء بشكل تلقائي، بقصد إنشاء رسالة معلومات أو إنشائها أو تشكيلها "[1]، ويلاحظ أن هذه التعريفات الواردة في قانون المعاملات اقتصرت على بيان تبادل الرسائل الإلكترونية فقط وهذا غير كاف لبيان معنى متعهد الإيواء الذي يتجاوز دورة ذلك .

ورد بقانون الجرائم الإلكترونية الأردني لعام 2023م تعريف مزود الخدمة "أنه أي شخص طبيعي أو معنوي خاص أو عام، يزود المشترك بالخدمات الإلكترونية بواسطة تقنية المعلومات، أو يقوم بمعالجة المعلومات، أو تخزينها نيابة عن خدمة الاتصالات أو مستخدميها [2] " ونجد أن التعريف السابق جاء عاماً يشمل مقدمي الخدمات سواء متعهد إيواء أو مورد المعلومات، ولم يحدد الطبيعة القانونية لمتعهد الايواء بشكل مباشر.

التشريعات العربية في الغالب، حالها حال المشرع الأردني، الذي لم يضع تعريفا مباشرا للمتعهد الايواء، فكان لابد من البحث في التشريعات الغربية وبعض التشريعات العربية لإيجاد التعريف القانوني حيث يورد الباحث بعضاً منها.

حيث جاء التشريع القطري في قانون المعاملات والتجارة الإلكترونية لسنة 2010م وعرف خدمات الاستضافة "خدمات إلكترونية تقدم للمستخدمين إمكانيات لتخزين المعلومات على نظم معلومات مقدم الخدمة، بحيث يمكن الوصول إليها من قبل مستخدمي خدمات تجارة إلكترونية آخرين[3] "

كما وجاء تعريف خدمة الإيواء في البرلمان والتوجيه الأوروبي في المادة 14 لتوجيه رقم 2000/31 (ec) والمتعلق بشأن الجوانب القانونية لخدمات جمع المعلومات ولا سيما في مجال

---

[1] المادة 2، قانون المعاملات الإلكترونية الأردني لسنة2015م.

[2] المادة 2، قانون الجرائم الإلكترونية رقم (17) لسنة 2023م

[3]المادة 1، قانون المعاملات والتجارة الالكتروني القطري رقم 16 لسنة 2010م .

التجارة الإلكتروني هو "عبارة عن نشاط يمارسه شخص طبيعي أو معنوي، يهدف إلى تخزين مواقع إلكترونية وصفحات ويب على حساباته الآلية الخادمة بشكل مباشر ودائم مقابل أجر أو بالمجان، ويضع من خلاله تحت تصرف عملائه الوسائل التقنية، والمعلوماتية، التي تمكنهم في أي وقت بث ما يريدون على شبكة الإنترنت من نصوص وصور وأصوات وتنظيم المؤتمرات والحلقات النقاشية "، وجاء أيضاً في التوجيه أنه من الوسائل التي يقدمها متعهد الإيواء لعملائه تخصيص مساحة قرص، أو شريط مرور، لبث المعلومات، التي يرغبون بنشرها على شبكة الإنترنت ، وتزويد العميل بحساب خاص يتضمن مفتاح دخول للتعريف به ، وتزويده ببرنامج خاص يمكنه من الاتصال بمتعهد الإيواء ،وإضافة، أو حذف، أو تغيير ما يريد من المعلومات [1]. وعرف المشرع الفرنسي متعهد الإيواء بأنه " كل شخص طبيعي ومعنوي يضع ولو بدون مقابل تحت تصرف الجمهور عبر الإنترنت تخزين النصوص والصور والأصوات والرسائل أياً كان طبيعتها التي تزود بواسطة المستفيد من هذه الخدمات [2] ".

يعرف الباحث متعهد الإيواء بأنه هو كل شخص طبيعي أو معنوي يتعهد بوضع إمكانياته التقنية والفنية أمام المستخدمين؛ ليتمكنوا من إيواء صفحات الويب الخاصة بهم على حاسباته الآلية، من خلال تخصيص مساحات لهم بشكل دائم ومستمر، مقابل أجر أو بالمجان، تمكنهم من بث ما يريدون على شبكة الإنترنت سواء صور أو أصوات أو فيديو، وأي خدمات إلكترونية أخرى.

---

(1) Directive No. 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) PDF HTML ،والمنشور على 6393\wipo.int\wipolex\ar\iegistution\details، والمشار الية في بني حمد ،عبد السلام أحمد، (2018م) ، تأصيل المسؤولية المدنية لمتعهد الإيواء في شبكة الإنترنت في القانون الأردني، مرجع سابق، ص340

(2) المادة 6\1\2، قانون الثقة حول الاقتصاد الرقمي الفرنسي رقم 45 لسنة 2004م

الفرع الثاني: التزامات متعهد الإيواء الإلكتروني لخدمات البيانات السيبرانية

ببيان مفهوم متعهد الإيواء نجد أن طبيعة الخدمات التي يقدمها متعهد الإيواء تجعل منه أقرب مقدمي خدمات المعلومات على شبكة الإنترنت بل وهو أقدرهم،على معرفة محتوى أي نشاط معلوماتي يتم تداوله عبر شبكات الأمن السيبراني.

إذا ما تبين أن هذا المحتوى المأوى على حاسباته غير مشروع فإن ذلك يشير إلى عدداً من الإشكاليات القانونية على صعيدين ،الأول مدى التزام متعهد الإيواء بمراقبة محتوى المعلومات المتداولة عبر شبكات الأمن السيبراني، والصعيد الثاني يتمثل في الالتزامات التي تقع على عاتق متعهد الإيواء في حالة علمه بتداول محتوى معلوماتي غير مشروع على شبكة الأمن السيبراني، وأمام هذه الإشكاليات وفي ظل غياب النص التشريعي، لمعالجة هذه الإشكاليات، أوجد المشرع الفرنسي الحد المعقول من الالتزامات على متعهدي الإيواء الإلكتروني على شبكات الأمن السيبراني ومن ثم سن القوانين التي تنظم هذه الالتزامات أسوتً بالمشرع الأوروبي [1].

لابد من الإشارة إلى أن التشريع الأردني لا يزال غائباً من الناحية التشريعية بخصوص بيان الالتزامات التي تقع على عاتق متعهدي الإيواء.

تتمثل الالتزامات التي تقع على عاتق متعهد الإيواء وفقاً للمتعارف عليه والغالب في تشريع وأحكام القضاء المقارن بكل من؛ الإلتزام بالإعلام؛ الإلتزام باليقضة، والإلتزام بوقف بث المحتوى المعلوماتي غير المشروع.

---

[1] حجازي عبد الفتاح بيومي، (2003م)، النظام القانوني لحماية الحكومة الإلكترونية بين الواقع والطموح، الكتاب الثاني، دار الفكر الجامعي، مصر، الإسكندرية، طبعة 1، ص 18.

أولاً: الالتزام بالإعلام

وهو التزام يقع على عاتق متعهد الإيواء، يوجب عليه إعلام مالكي الموقع الإلكترونية، الذي يقدم لهم خدمة الإيواء، بضرورة تجنب أي مخالفة، لم تنص عليها القوانين ذات العلاقة، والامتناع عن أي فعل يحتوي على الاعتداء على حقوق الملكية الفكرية، وأي أفعال يمكن أن تترتب عليها إضرار بالغير، ومن جانب آخر أكدت المحكمة الفرنسية في قراراتها عدم التزام متعهد الإيواء الإفصاح عن هوية مالكي تلك المواقع [1].

واستندت المحكمة الفرنسية في عدم إلزام المتعهد الإفصاح عن هوية مالك المواقع لعدة ركائز، أولها عدم إمكانية المتعهد من التأكد من المعلومات التي يقدمها الأشخاص عندما يطلبون إيواء مواقعهم، حيث يتم إعطاء المعلومات إلكترونياً، عن طريق تعبئة نموذج معروض على شبكة الإنترنت، وثانياً صعوبة معرفة الرمز التعريفي للحاسوب المستخدم في إنشاء الموقع الإلكتروني ذي المضمون غير المشروع [2].

---

(1) TGI of Nanterre, 8 December 1999, précité, Aucune obligation légale n'existe in ce domaine (identification de l'éditeur du site lors de l'ouverture de son compte) à la charge du prestataire d'hébergement». V Guide Permanent Droit and Internet, E 133.3Hébergement du site, précité, n° 28.p، المشار اليه في في بني حمد عبد السلام أحمد،(2018م)، تأصيل المسؤولية المدنية لمتعهد الإيواء في شبكة الإنترنت في القانون الأردني ، مرجع سابق، ص345

(2) TGI of Nanterre, 8 December 1999, précité, Aucune obligation légale n'existe in ce domaine (identification de l'éditeur du site lors de l'ouverture de son compte) à la charge du prestataire d'hébergement». V Guide Permanent Droit and Internet, E 133.3Hébergement du site, précité, n° 28.p، المشار اليه في في بني حمد عبد السلام أحمد،(2018م)، تأصيل المسؤولية المدنية لمتعهد الإيواء في شبكة الإنترنت في القانون الأردني ، مرجع سابق، ص345.

يجب الإشارة أن ذات المحكمة عادت عن موقفها هذا في قضية أخرى عام 2000م؛ حيث قضت في قضية رفعها الاتحاد العام للطلبة اليهود في فرنسا UEJF، ضد متعهد الإيواء Multimania، نتيجة لإيوائه موقعاً إلكترونياً تتضمن عرض وبيع أغراض ورموز نازية؛ حيث قررت، بأنه يجب على متعهد الإيواء

وبالتعاون مع متعهد الوصول الكشف عن هوية صاحب الموقع الإلكتروني ذي الموضوع غير المشروع أو الضار [1].

ثانياً: الالتزام باليقظة

ومضمون هذا الالتزام هو أن يكون متعهد الإيواء على درجة من الانتباه، ليتمكن من اكتشاف أي نشاطات غير مشروعة، تتضمنها أياً من المواقع الإلكترونية التي يقوم بمنحها خدمة الإيواء.

وهنا ووفق هذا الالتزام لا يطلب من متعهد الإيواء أن تكون المراقبة دقيقة وعميقة على المواقع الإلكترونية، التي يقدم لها خدمة الإيواء، ولكن يجب أن يتمتع بالقدر اللازم والمناسب من اليقظة، التي تمكنه من الكشف عن الأنشطة غير المشروعة على هذه المواقع، ويشترط لذلك أن يكون هذا النشاط يحمل بوادر ظاهرة بعدم المشروعية.

---

[1] TGI de Nanterre (Ire Ch.), 24 May 2000, available at the address: www. juriscom.nct., voir également sur l'obligation de collaboration et d'information, E. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in M. ANTOINE, A. CRUQUENAIRE et d'autres, Commerce electronique européen sur Les Rails?, Iredition, 2001, Bruylant, Bruxelles, n° 526 et s., p. 280 et s., selon le tribunal « The absence of rigueu générale in the profession aux niveaux national and international, is palliée par the faculté who dont dispose fournisseur d'hébergement de se faire communiquer par le fournisseur d'accès les éléments certains de l identi de son client, au terme d'une procédure rapide dont il doit assurer la charge lorsque des tiers sont apparemme

استناداً لذلك يقع على عاتق متعهد الإيواء توجيه الموقع لتصحيح ذلك النشاط والمضمون، بما يتناسب والقوانين والأنظمة المعمول بها، وفي حال عدم استجابة الموقع وامتثاله لهذا التوجيه يقع على عاتق المتعهد وقف تزويد الموقع بالخدمة وقطعها عنه [1].

إن أصل هذه الالتزامات أعلاه هو اجتهادات قضائية حيث ورد في دعوى مشهور لعارضة الأزياء Estelle hallyday أمام محكمة بداية باريس ضد "v.lacambere " مؤسس وصاحب الموقع الإلكتروني "fltren.org " تطالبه فيها بالتعويض عن الأضرار التي سببها لها نتيجة إيواء موقعاً إلكترونياً نُشر عليه تسعة عشر صورة تظهرها وهي عاريه بشكل كامل أو جزئي ، وجاء قرار المحكمة في 9\حزيران \1998م، ليضع على عاتق متعهد الإيواء بذل العناية والجهد اللازمين بالبحث عن المواقع الإلكترونية التي تخالف القانون أو تتسبب بإضرار الآخرين[2]، كما أقر هذا القرار في حيثياته لانتفاء المسؤولية عن متعهد الايواء لابد من:

أولاً: إثبات قيام متعهد الإيواء بإعلام أصحاب المواقع الإلكترونية المأوية بضرورة مراعاة القوانين والأنظمة السارية

ثانياً: عدم الاعتداء على حقوق الأخرين وحقوق الملكية الفكرية على الإنترنت.

إن الإخلال بهذه الالتزامات يرتب المسؤولية على متعهد الإيواء عملاً بإحكام المادة 1241 من القانون المدني الفرنسي.

---

[1] عبد السلام أحمد، (2018م)، تأصيل المسؤولية المدنية لمتعهد الإيواء في شبكة الإنترنت في القانون الأردني، مرجع سابق، ص345.

[2] Th. VERBIEST et É. WÉRY, (2001), "La responsabilité des fournisseurs de services internet: Derniers développement (35) −jurisprudentiels", Journal des Tribunaux, , p. 166 et s .

بقي أن نشير إلى أن بعض التشريعات العربية، أشارت في نصوصها إلى التزام مقدم الخدمات باليقظة، ومنها المشرع القطري في قانون المعاملات والتجارة الإلكترونية لسنة 2010م، حيث جاء فيه أن مقدم خدمة الاستضافة، لا يسأل عن تلك الخدمات في حال عدم علمه، أو إدراكه الفعلي عن النشاط والمضمون غير المشروع أو الغير القانوني، أو أن تكون هذه التصرفات والنشاطات ليست بموافقة مسبقة من مقدم الخدمة للمستخدم الموقع [1].

هذا ما أكده المشرع البحريني أيضاً في قانون المعاملات الإلكترونية البحريني لسنة2018، حيث أشترط لانتفاء مسؤولية مقدم الخدمة عدم علمه بالمحتوى والنشاط غير المشروع والذي يرتب المسائلة الجزائية والمدنية [2] .

يرى الباحث أن المشرعين العرب تأثروا بالتشريع الغربي في مسألة الالتزام باليقظة، حيث أوجبت التشريعات على مقدم الخدمة القدر المناسب من الرقابة كشرط لانتفاء مسؤوليته عن المحتوى غير المشروع، وهذا ما أكدت عليه التشريعات العربية أيضاً، باشتراطها عدم العلم بالمحتوى غير المشروع لانتفاء الالتزام عن متعهد الإيواء.

ثالثا: الالتزام بوقف بث المحتوى المعلوماتي غير المشروع

يعد هذا الالتزام مكملاً لما قبله من التزام متعهد الإيواء باليقظة، فيقع على عاتق المتعهد بعد علمه بالمحتوى غير مشروع أو الذي يسبب الضرر للآخرين، بتوجيه أصحاب المواقع الإلكترونية لإزالة هذا المحتوى، ولكن قبل مرحلة التوجيه والتصحيح يقع واجباً على المتعهد التزام بوقف بث هذا

---

[1] أنظر المادة 1/47 والمادة 3/47، قانون المعاملات والتجارة الالكتروني القطري رقم 16 لسنة 2010م.

[2] أنظر المادة 24/أ والمادة 24/ب، فانون الخطابات والمعاملات الإلكترونية البحريني رقم 54 لسنة 2018م.

المحتوى غير مشروع أو الذي يلحق الضرر بالأخرين، تمهيد لأمرين أم التصحيح، أو وقف تزويد المتعهد لخدمة الإيواء للمستخدم في حال عدم امتثاله بعد التوجيه بالتصحيح [1].

لابد من الإشارة أن المشرع الأوروبي تبنى ما استقر عليه القضاء الفرنسي، حيث رسخ القضاء أن علم متعهد الإيواء بالمحتوى غير المشروع أو الضار بالآخرين، هو علم غير مفترض ولا يستوجب الرقابة الدقيقة، أو البحث النشط من المتعهد لتحديد المحتويات او النشاطات غير المشروعة أو الضارة ، ولا يمكن مساءلة متعهد الإيواء لعدم اتخاذه موقفاً إيجابياً، طالما أنه لا يعلم بهذا المحتوى، والمستقر علية أنه غالباً ما يتم طلب وقف بث المحتوى غير المشروع ،من السلطات العامة، أو الغير الذي لحقة الضرر[2]، وهذا ما يتوافق مع ما سبق حول التزام متعهد الإيواء بوقف بث المضمون المعلوماتي غير المشروع قبل التزام التوجيه والتصحيح الموجه من المتعهد للموقع الإلكتروني صاحب المحتوى . كما أن التشريعات العربية، ومنها المشرع القطري، أكد أن مسؤولية مقدم الخدمة تنتفي في حال اتخذ دون تأخير إجراء بإزالةأو تعطيل الوصول للمعلومات أو الخدمات، عند العلم بعدم مشروعية النشاط أو المعلومات المرتبطة بخدمات استضافة معينة [3]. أكد المشرع البحريني كذلك في قانون المخاطبات والمعاملات الإلكترونية لسنة 2018م أن الوسيط (متعهد الإيواء)، يجب عليه على الفور في حال علمه بالمحتوى غير المشروع بإزالة المعلومات، من أي نظام تحت سيطرته، ووقف إمكانية النفاذ لتلك المعلومةأو تخزينها أو عرض أي من ذلك لانتفاء مسؤوليته [4].

---

[1] ابو الحسن حنين جميل، (2021م)، الإطار القانوني لخدمة الأمن السيبراني (دراسة مقارنة)، مرجع سابق ص 76 وما بعد.

[2] CA Versailles, 8 juin 2000, précité, << Qu'indépendamment des cas où elle en est requise par l'autorité publique (36) ou sur décision judiciaire, de telles diligences doivent être spontanément envisagées par la société prestataire d'hébergement lorsqu'elle a connaissance ou est informé de l'illégalité, de l'illicité ou du caractère dommageable.» du contenu d'un site

[3] المادة 2/47، قانون المعاملات والتجارة الالكتروني القطري رقم 16 لسنة 2010م.

[4] المادة 24/ج، قانون الخطابات والمعاملات الإلكترونية البحريني رقم 54 لسنة 2018م

المطلب الثاني

التزامات موردي معلومات البيانات السيبرانية

يقسم مقدمي الخدمات المعلوماتية للبيانات السيبرانية عادةً إلى قسمين الأول متعهد الإيواء، وهو ما بينه الباحث في المطلب السابق، والقسم الثاني هو مورد المعلومات للأمن السيبراني، حيث يعد موردي المعلومات، هم المتحكمين الرئيسيين في الرقابة على ما يتم بثه من خلال شبكات الأمن السيبراني من محتوى معلوماتي، وهذا ما سيبنه الباحث في هذا المطلب من خلال بيان مفهوم موردي المعلومات وبيان الالتزامات القانونية التي تقع على عاتقهم، حسب ما استقر بالفقه والتشريع المقارن نتيجة لغياب النص التشريعي الأردني.

الفرع الأول: مفهوم موردي المعلومات

توريد المعلومات كما جاء بالقانون الفرنسي يعني " نشرها، أي إتاحة محتوى من المعلومات أمام الجمهور، حيث يظهر هذا المحتوى والمضمون المعلوماتي على شبكة الإنترنت باستخدام صفحات ويب، على اختلاف طبيعة المحتوى سواء مسموع أو مقروء أو مرئي، وعليه فإن خدمة توريد المعلومات إلكترونياً الهدف منها، هو وضع محتوى معلوماتي (صور، أو فيديو، أو أصوات ...) تحت تصرف مستخدمي شبكة الإنترنت، لذلك تعد هذه الخدمة من وسائل الاتصال العلنية " [1].

وكذلك يقصد بتوريد المعلومات عبر شبكة الأمن السيبراني قيام مورد المعلومات " fournisseeur du contenu" باستعمال مساحة من القرص الصلب أو أجهزة التخزين المركزية الممنوحة له من قبل متعهد الإيواء، سواء كان ذلك مقابل أجر (مساحة مستأجرة) أو بالمجان (مساحة معارة)، حيث

---

[1] أنظر المادة 2، القانون الفرنسي حول حرية الاتصال لسنة 1986 وتعديلاته رقم 719 لسنة 2000م، المنشور بالجريدة الرسمية بتاريخ 200/8/2م، والمشار الية في فرح أحمد قاسم ،2007م، النظام القانوني لمقدمي خدمة الإنترنت (دراسة تحليليه مقارنة)، جامعة آل البيت، المنارة، مجلد 13، عدد 9، ص327.

يقوم بتحميل البيانات والمعلومات التي قام بتأليفها أو جمعها حول موضوع معين على تلك المساحة[1].

مما سبق فإن مورد المعلومة أما أن يكون صاحب المادة المعلوماتية، أي مؤلفها، أو جامع لها، وهنا يكون دوره عبارة عن حلقة وصل بين مؤلف المادة ومستخدمي الشبكة الراغبين بالاطلاع عليها [2].

وعليه فإن مورد المعلومات؛ في حال كان هو مؤلف المعلومة والمحتوى ، فإنه يكون قد اتخذ في آن واحد صفة المؤلف والناشر من خلال خدمة التوريد، أما في حال كان هو جامع البيانات والمعلومات، فإنه يأخذ صفة الناشر فقط ، ويقوم المورد بنشر المعلومة على شبكات الإنترنت بناءً على عقد نشر يربطه بصاحب المادة المعلوماتية، فمورد المعلومات سواء كان شخص طبيعي، أو اعتباري هو صاحب السلطة الحقيقة في مراقبة المضمون المعلوماتي الإلكتروني، وهو الذي يقع عليه عاتق تقديم المادة المعلوماتية الحقيقية والمشروعة، فدوره أشبه بدور مدير النشر أو رئيس التحرير في الصحافة المكتوبة، لأنه هو من يقوم بتأليف أو جمع البيانات والمعلومات، وبالتالي يملك القدرة على توريدها للجمهور من مستخدمي الإنترنت أو الامتناع عن ذلك [3].

بقي أن نبين الاختلاف بين متعهد الإيواء ومورد المعلومات، فالأول لا يقوم بتأليف أو جمع المعلومات والبينات مضمون المحتوى المعلوماتي, وإنما يقتصر دوره على تخزينها وحفظها على أجهزته، استناداً الى اتفاق مع مورد المعلومات، ليتيح للجمهور الاطلاع على هذا المحتوى طيلة

---

(1) منصور، محمد حسين، (2003م)، المسؤولية الالكترونية، مرجع سابق، ص 200.

(2)Guide Permanent Droit et Intermet, E 3.13. Responsabilité de l'éditeur, précité, n° 4 et s., p. 5 et s

(3) أنظر منصور محمد حسين، (2003م)، المسؤولية الالكترونية، مرجع سابق، ص201، وأنظر Guide Permanent Droit et Intemet, E3.13, Responsabilité de l'éditeur, précité, n°5, p. 4،

الوقت وعلى مدار الساعة، كما وتعد خدمة التوريد هي نشر للمحتوى المعلوماتي، أما خدمة الإيواء فتكون أما خدمة تأجير (في حال كان هناك مقابل) أو خدمة إعارة (إذا كانت بالمجان) وعلى الرغم من هذه الاختلافات بين كل من المتعهد و المورد إلا أن كليهما من مقدمي خدمات المعلوماتية للأمن السيبراني ،حيث لا يمكن بث أي محتوى إلكتروني على شبكات الإنترنت بدون اشتراكهم، وتدخلهم، من خلال استخدام الوسائل الفنية والتقنية اللازمة للربط بين شبكات الاتصال عن بعد، مع الحاسبات الآلية للمستخدمين[1].

الفرع الثاني: التزامات موردي المعلومات

مورد الخدمات المعلوماتية (مزود المعلومات) هو صاحب السلطة الحقيقية في مراقبة محتوى ما يبث عبر شبكات الأمن السيبراني، لأنه هو من يقوم بجمع البيانات، والمعلومات، أو يؤلفها، فيقع على عاتقه التأكد من حقيقة هذا المحتوى ومشروعيته، وبناءً على هذا الدور الذي يقوم به موردي المعلومات يترتب عليهم مجموعة من الالتزامات تتمثل بالفافية وكفالة حق الرد .

أولاً: الالتزام بالشفافية

يستمد هذا الالتزام طبيعته من طبيعة عمل موردي المعلومات، فهم القائمون على نشر المعلومات عبر شبكات الإنترنت بالمواقع الإلكترونية، وهم أصحاب القدرة على التحكم بالمضمون المعلوماتي[2]، حيث أن أي معلومة تبث على المواقع هم المسؤولون عنها، من حيث المحتوى

(1) فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت، مرجع سابق، ص328.

(2) Guide Permanent Droit et Intemet, E 3.13, Responsabilité de l'éditeur, clairement, n°1, I P.4

والمضمون ومدى حقيقته ومشروعيته وهذا يتفق مع طبيعة عمل المورد كناشر إلكتروني للمحتوى المعلوماتي[1].

يقع على عاتق مورد المعلومات إبلاغ الجهات المختصة عن أي محتوى غير مشروع، ويقوم بتلك المهمة مدير النشر الذي يعينه المورد [2]، واستكمالاً لتعزيز مبدأ الشفافية يجب على مورد المعلومات عدة أمور لتحقيق هذا الالتزام:

1. يجب على مورد المعلومات اِطلاع كل من متعهدي الإيواء الذين يتعاملون معهم و جمهور المستخدمين أيضاً على كافة ما يتعلق بنشاطه الإلكتروني الذي يمارسه والمعلومات اللازمة لتعريف به، من خلال وضع اسمه، وكنيته، وشهرته إذا كان المورد شخصاً طبيعياً، أم إذا كان شخصاً معنوياً فيجب أن يبين اسمه المعنوي وطبيعة نشاطه ومركز إدارته الرئيسي[3].
2. يجب على المورد، وضع المحتوى الإلكتروني بشكل ظاهر وواضح على الموقع الرئيسي، بحيث يسهل الوصول آليه، من خلال نشره على الصفحة الرئيسية للموقع الإلكتروني أو من خلال الضغط على أيقونة أو إشارة أو علامة معينة أعدت خصيصاً لذلك [4].
3. يقع على عاتق المورد، توفير الوسائل الفنية، والتقنية اللازمة التي تمكنه من الكشف عن هوية مالك المحتوى غير المشروع، وخاصة مع وجود رمز تعريفي (ip) لكل جهاز حاسوب مرتبط

---

(1) أنظر المادة 5، قانون المطبوعات والنشر الأردني رقم 8 لسنة 1998وتعديلاتة رقم 30 لسنة 1999م، حيث جاء فيها "على المطبوعات احترام الحقيقة والامتناع عن نشر ما يتعارض مع مبادئ الحرية والمسؤولية الوطنية وحقوق الأنسان وقيم الأمة العربية والإسلامية".

(2)Guide Permanent Droit et Internet, E 3.13, Responsabilité de l'éditeur, précité, n° 6, p.6

(3) المرجع نفسه، ص 11، الفقرة 19

(4)Guide Permanent Droit et Intemet, E 3.13, Responsabilité de l'éditeur, précité n° 19 p.11

على شبكات الانترنت [1]، على أن يكون تعامله مع الآخرين وأصحاب المحتوى المشروع، مقيداً بإلزامه بالسرية وعدم النشر أو الاعلان عن تلك المعلومات، إلا في حالة الضرورة، وهذا ما أكد عليه القانون الفرنسي حول الثقة قي الاقتصاد الرقمي لسنة 2004من خلال الفقرة الثانية من نص المادة 6\3\2.

4. كما يجب على المورد الكشف عن اسم متعهد الإيواء، ولقبه، أو عنوانه، ومركز إدارته الرئيسي، وهذا ما أكد عليه القانون الفرنسي حول الثقة قي الاقتصاد الرقمي في نص المادة 1/3/6 [2].

يرى الباحث أن التزام مورد المعلومات واحترام جميع القيود السابقة، من رقابة على المحتوى المعلوماتي، وتعين مديراً للنشر، والتعريف عن نفسه حسب الأصول السابقة، يجعل من الشفافية ديدناً لعمله وسمةً تتمتع بها أعماله، الأمر الذي يجعل منه بعيداً عن الملاحقة في حال التزامه فيما سبق، على أنه لا يعفى بأي شكل من الأشكال من إتاحة حق الرد، لأي مستخدم يثبت بطريقة أو بأخرى أن المحتوى المنشور يشكل مساساً بحقوقه.

ثانياً: الالتزام بالكفالة حق الرد

يقصد بهذا الالتزام أن يتيح مورد المعلومات حق الرد لأي شخص سواء شخص طبيعي أم اعتباري، قام بنشر أي محتوى معلوماتي على شبكات الأمن السيبراني، ويكون هذا المحتوى مشتملاً على أي مساس بكرامته أو اعتباره أو أياً من حقوقه الأخرى ،ويلحق الضرر به، وله حق الرد خلال ثلاثة أشهر تبدأ من تاريخ وقف بث المضمون غير المشروع على شبكات الأمن السيبراني وليس

---

(1)M. GUILLARD, "Responsabilité des acteurs techniques de l'intemet", précité, p. 2 et s., Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, précité, n° 49 p. 20

(2) أنظر القانون الفرنسي حول ثقة الاقتصاد الرقمي رقم 575 لسنة 2004م والمؤرخ بتاريخ 21/يونيو /2004م والمشور على محرك البحث قوقل على الرابط http;\\ www.wipo.int تاريخ الدخول 2023/8/31م ساعة الدخول 13:35

من تاريخ بدء البث [1]، فيلتزم مدير النشر المعين من قبل المورد بقبول أي شكوى تتعلق بذلك الشأن، وأن يمنح مقدم تلك الشكوى فرصة الرد على ذلك المحتوى، الماس به على ذات شبكة الأمن السيبراني، التي تم النشر المحتوى غير المشروع أو المتسبب بالضرر له عليها. يقع على عاتق مورد المعلومات وتحت طائلة المسؤولية تمكين الشخص الذي لحقه الضرر من أي محتوى نشر، من أن يطالب بتصحيح هذا المحتوى أو شطبه إذا كان غير مشروع من صفحات الويب[2]. منح حق الرد من قبل مورد المعلومات للمضرور يرتب التزاما عاماً على كاهل المورد، ألا وهو تأمين الوسائل التقنية والمعلوماتية اللازمة لتطبيق حق الرد، من قبل الشخص الذي لحقه الضرر [3].

بقي أن نبين موقف المشرع الأردني من حق الرد للمتضرر جراء نشر محتوى معلوماتي، ونستند هنا أن المورد المعلوماتي يعد ناشراً إلكتروني، ولافتقار النص التشريع نرجع إلى مقارنته بالناشر الصحفي أو ناشر المطبوعات، حيث بين قانون المطبوعات لسنة 1998م وتعديلاته إذا نشر في المطبوعات الصحفية خبراً غير صحيح أو مقال يحتوي معلومات غير صحيحة فيحق لشخص المضرور والذي يتعلق به الخبر أو المقال حق الرد والمطالبة بسحب أو تصحيحه، وهنا يلزم رئيس التحرير المسؤول، نشر الرد أو التصحيح مجاناً في العدد التالي لتاريخ نشر الخبر أو المقال غير المشروع، وفي نفس المكان وبعدد الحروف نفسها التي نشر فيها المقال أو الخبر[4]، إلا إن المسؤولية تنتفي عن الناشر بإتاحة حق الرد بعد مرور شهرين على تاريخ نشر الخبر والمقال غير الصحيح والذي تسبب بالضرر للغير [5]. أخيراً لابد من الإشارة إلى أن مورد المعلومات ليس هو المسؤول الوحيد عن المحتوى غير المشروع، فهناك أكثر من شخص يتدخل في العملية، وبتالي يمكن قيام مسؤوليتهم في حال ثبوت مخالفتهم، لأي من الالتزامات الملقاة على عاتقهم، وهذا ما سوف نبينه في المبحث القادم.

---

(1) أنظر المادة 6-2/3، القانون الفرنسي حول ثقة الاقتصاد الرقمي رقم 575 لسنة 2004م

(2) المادة 6-2/4 و6-3/4، القانون الفرنسي حول ثقة الاقتصاد الرقمي رقم 575 لسنة 2004م

(3)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

(4) أنظر المادة 27/أ، قانون المطبوعات والنشر الأردني رقم 8 لسنة 1998وتعديلاتة رقم 30 لسنة 1999م

(5) المادة 28/د، قانون المطبوعات والنشر الأردني رقم 8 لسنة 1998وتعديلاتة رقم 30 لسنة 1999م.

المبحث الثاني

الالتزامات الفنية لمقدمي خدمات البيانات السيبرانية

عملية عرض المحتوى الإلكتروني والوصول إليه عبر شبكات الأمن السيبراني تعتمد على جانبين لا يمكن لأحدهما العمل بدون الآخر، الأول هو مقدمي الخدمات المعلوماتية وهم متعهد الإيواء، ومورد المعلومات، وهم من تم بيان طبيعتهما والالتزامات التي تقع على عاتقهم في المبحث السابق، أما الجانب الثاني فيتمثل بمقدمي الخدمات الفنية على شبكات الأمن السيبراني ويقعون على نوعين، الأول ناقل المعلومات عبر شبكة الإنترنت للبيانات السيبرانية، والثاني متعهد توصيل المعلومات عبر شبكة الإنترنت للبيانات السيبرانية، وهم من سوف نبين طبيعتهم والالتزامات الملقاة على عاتقهم.

المطلب الأول

التزامات ناقل المعلومات عبر شبكة الإنترنت للبيانات السيبرانية

إن تطور تكنولوجيا المعلومات، والإقبال الهائل عليها، واستخدام الوسائل التقنية، لتسهيل استخدام هذه التكنولوجيا، جعل منها محط أنظار القانونيين والمشرعين والقضاة، لشمولها جميع أنحاء مجالات الحياة، فكان لابد من الوقف على الطبيعة القانونية لمقدمي الخدمات الفنية عبر شبكات الأمن السيبراني، والتزاماتهم، وأول هؤلاء المقدمين هو ناقل المعلومات عبر شبكات الأمن السيبراني.

الفرع الأول: مفهوم ناقل المعلومات

حقيقةً ليتمكن مستخدمي شبكة الإنترنت من الاطلاع على المحتوى الإلكتروني الموجود على المواقع الإلكترونية، سواء أكان معلومات أو بيانات ونحوه، يتطلب أن تكون أجهزة الحاسوب

المستخدمة من قبلهم مرتبطة بالمواقع الإلكترونية، من خلال إجراء ربط فني ومادي، بين شبكات الاتصالات عن بعد، بحيث تشكل قنوات مفتوحة على بعضها البعض عبر الفضاء السيبراني[1]، وعادة تتولى مهمة هذا الربط هيئات عامة للاتصالات، وهي تعتبر ناقل مادي للمعلومات، وتتم هذه الخدمة بموجب عقد يسمى عقد نقل المعلومات، الذي بموجبه يرتبط الناقل مع باقي مقدمي الخدمات عبر شبكات الأمن السيبراني، وذلك من خلال توفير الوسائل، والأجهزة الفنية اللازمة لإجراء النقل المادي للمحتوى المعلوماتي، وهو ما يسمى "رفع المحتوى على الموقع الإلكتروني " والذي يتم من خلال ربط المشترك بين مختلف شبكات الاتصال عن بعد [2].

جاء في تعريف ناقل المعلومات "هو العامل الفني، الذي يقوم بالربط بين الشبكات، فهو يقوم وبموجب عقد النقل بنقل المعلومات، في هيئة حُزم من جهاز المستخدم الى الحاسب الخادم لمتعهد الوصول، ثم نقلها من هذا الحاسب الى الحواسيب المرتبطة بمواقع الإنترنت" [3]

إن خدمة نقل المعلومات تستمد قانونيتها من عقد النقل؛ فالخدمة عبر شبكات الأمن السيبراني، هي نقل المعلومة، ومقدم هذه الخدمة هو الناقل"transmetteur"، وبناءً على هذا الوصف والطبيعة القانونية، يكون ناقل المعلومات عبر شبكات الأمن السيبراني أشبه ما يكون بساعي البريد، فكلاهما مهمته تأمين النقل المادي للمعلومات بين الأطراف سواء، مرسل، أو مستقبل [4]. واستناداً إلى المهمة الملقاة على عاتق ناقل المعلومات، فإنه يختلف عن متعهد الإيواء، الذي يتولى تأمين مساحات على أجهزته لتخزين الدائم والمباشر للمادة المعلوماتية، وكذلك يختلف عن مورد

---

(1) حجازي عبد الفتاح بيومي، (2003م)، النظام القانوني لحماية الحكومة الإلكترونية، مرجع سابق، ص339

(2) منصور محمد حسين، (2003م)، المسؤولية الإلكترونية، مرجع سابق ص197.

(3) منصور محمد حسين، (2006م)، المسؤولية الإلكترونية، بدون طبعة، منشأة المعارف، الإسكندرية، ص 168، والمشار اليه في الحسبان، ياسين محمد، (2010م)، المسؤولية المدنية لمقدمي الخدمات غبر الإنترنت في القانون الأردني "دراسة مقارنة "، رسالة ماجستير، كلية الحقوق، جامعة عمان العربية.

(4) حجازي، عبد الفتاح بيومي، (2003م)، النظام القانوني لحماية الحكومة الإلكترونية، مرجع سابق، ص349

المعلومات، فهو لا يقوم بتأليف أو جمع المعلومة ومن ثم نشرها، فدوره مجرد وسيلة للنقل تلك المعلومات، فهو ليس صاحب سلطة حقيقية في الإشراف على مضمون المعلومات التي يقوم بنقلها، بل مجرد ناقل مادي للمعلومة من وحدة لوحدة أخرى، دون أن يكون مكلفاً بمراقبتها أو معرفة مضمونها.

يعرف الباحث ناقل المعلومات بأنه كل شخص طبيعي أو معنوي يتيح أمام مستخدمين شبكات الأمن السيبراني إمكانياته الفنية لربط حواسيبهم الآلية مع المواقع الإلكترونية، ليتمكنوا من الاطلاع على المعلومات والبيانات أو رفع هذه البيانات على المواقع الإلكترونية.

الفرع الثاني: التزامات ناقل المعلومات

يقع على عاتق مقدمي خدمات نقل المحتوى المعلوماتي عبر شبكات الأمن السيبراني استناداً إلى المهمة المكلفين بها، مجموعة من الالتزامات الرئيسية نستدرجها كما يلي:

- يلتزم مقدم خدمة نقل المعلومات، بتوفير كافة الإمكانيات والوسائل الفنية والتقنية اللازمة لإكمال عملية النقل المادية للمضمون المعلوماتي، فهو يقوم بالربط المادي بين الشبكات عن بعد، ويكون هذا الالتزام بموجب عقد النقل الذي يربطه مع عملائه [1].

وبناءً على هذا الالتزام، لا يكون مقدم خدمة نقل المعلومات ملزماً بالرقابة على المعلومات التي تعبر الوسائل الفنية الخاصة به، وبالتالي لا يسأل عن المحتوى غير المشروع، الذي ينقل الى المواقع الإلكترونية بواسطته كناقل [2].

---

(1) انظر حجازي عبد الفتاح بيومي، (2003م)، النظام القانوني لحماية الحكومة الإلكترونية، مرجع سابق، ص349 ومنصور محمد حسين، (2003م)، المسؤولية الإلكترونية، مرجع سابق، ص197.

(2) حجازي عبد الفتاح بيومي، (2003م)، النظام القانوني لحماية الحكومة الإلكترونية، مرجع سابق، ص349.

- ويلتزم مقدم خدمة النقل بعدم الكشف عن أي محتوى معلوماتي يقوم بنقله، أن يحافظ على السرية التامة له [1].
- كذلك يلتزم ناقل المعلومات باحترام نصوص النظام العام، والحفاظ على عدم المساس بحقوق الآخرين، وأن علمه بعدم مشروعية مضمون المحتوى المعلوماتي الذي يقوم بنقله دون اتخاذ إجراء يشكل إخلالاً في هذا الالتزام [2].
- كما ويقع على عاتق مقدم خدمة نقل المحتوى المعلوماتي عبر شبكات الأمن السيبراني إلتزام باحترام حقوق المؤلف، فإن نقل المحتوى المعلوماتي بالوسائل الفنية التي يتيحها الناقل للمستخدم تحتاج الى إجراء فني يتمثل في نسخ هذا المحتوى المعلوماتي بشكل مؤقت من قبل الناقل تمهيداً لنقله مادياً فيما بعد، وهذا النسخ المؤقت، لا يشكل انتهاكا لحقوق المؤلف ما دام أنه ينحصر في التخزين المؤقت للمحتوى المعلوماتي، بدون إجراء أي تعديل، أو إضافة عليه من قبل الناقل، وكذلك يحترم الناقل حق المؤلف عندما يمنع الوصول إلى المحتوى المعلوماتي بعد أخطاره بقرار قضائي أو إداري يقضي بعدم مشروعية المضمون المعلوماتي المخزن بصورة مؤقتة [3].

---

(1) أنظر 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. ومنصور المرجع نفسه، ص197

(2) منصور محمد حسين، (2003م)، المسؤولية الإلكترونية، مرجع سابق، ص 198.

(3) أنظر المواد1\1 و2\1-2، القانون الفرنسي لحق المؤلف والحقوق المجاورة له في مجال المعلوماتية، 2006م، والصادر في 1\أب \2006م، Loi.

المطلب الثاني

التزامات متعهد الوصول عبر شبكة الإنترنت للبيانات السيبرانية

مقدمي الخدمات الفنية عبر شبكات الإنترنت للبيانات السيبرانية، يكونوا على جانبين؛ الأول مقدمين خدمة نقل المعلومات عبر شبكات، وهذا ما بينه الباحث المطلب الأول والجانب الآخر هم مقدمي خدمة الوصول عبر شبكات الإنترنت، ولعل كلا الجانبين قريبين من آلية العمل والالتزامات، ولكن سوف يقوم الباحث ببيان مفهوم متعهد الوصول والالتزامات التي تقع على عاتقه جراء تقديم خدمات الوصول عبر شبكات الأمن السيبراني.

الفرع الأول: مفهوم متعهد الوصول

بعد نشر المحتوى المعلوماتي عبر المواقع الإلكترونية بحيث يصبح متداولاً، يحتاج إلى إتاحة الوصول آليه من قبل مقدمي خدمة الوصول، ليتمكن مستخدمي الإنترنت من الوصول الى هذا المحتوى، ويتم ذلك عن طريق عقد الاشتراك في خدمة الإنترنت، حيث يتمكن المشترك من خلال هذا العقد الدخول إلى شبكة الإنترنت والتصفح والبحث في المواقع الإلكترونية، عما يرغب بالاطلاع عليه من محتوى معلوماتي هناك، فالنشاط الأساسي لمقدمي خدمة الوصول عبر شبكات الأمن السيبراني هو تقديم خدمة إتاحة الدخول إلى شبكة الإنترنت للمشتركين معه من جمهور المستخدمين، وتتطلب هذه العملية أن يقوم مزود هذه الخدمة بتزويد المشترك بكلمة سر وبريد إلكتروني، ليتمكن من استقبال وإرسال الرسائل الخاصة به، ويطلق على من يقدم هذه الخدمة متعهد الوصول عبر شبكات الأمن السيبراني. [1]

---

(1) أنظر فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت (دراسة تحليليه مقارنة)، مرجع سابق، ص329و Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, mars .2002, Éditions Législatives, n° 2 et s., p. 4 et s

إضافة إلى الخدمة السابقة للمتعهد الوصول، فإنه يقدم خدمات إضافية إلى المشتركين لديه، من خلال بيانها نتمكن من بيان المقصود بمتعهد الوصول، وتتمثل هذه الخدمات في اقتراح مضمون معلوماتي معين يتم بثه عبر الشبكة أو التعهد بإيوائه، وفتح حلقات للنقاش أو نشر بيانات ومعلومات معينة على صفحات الويب التابعة له أو حتى تخزين مؤقت لصفحات الويب التي يطلع عليها المشتركين معه في الخدمة، وذلك من أجل تسريع عملية الوصول إليها عند طلبها مرة أخرى [1]. متعهد الوصول لا يقدم هذه الخدمات بصفته متعهد وصول فقط، بل بوصفه متعهد إيواء وبالتالي يخضع في ما يخص هذه الخدمات الإضافية للأحكام الخاصة بمتعهد الإيواء [2].

واستناداً إلى طبيعة النشاط والعمل الرئيسي الذي يمارسه متعهد الوصول كعامل فني للاتصالات عن بعد، فقد عرفه المشرع الفرنسي في قانون البريد والاتصالات لسنة 2001م بالمادة 15/32 " هو كل شخص طبيعي أو معنوي يستغل شبكة الاتصالات عن بعد والمفتوحة للجمهور، أو يورد لهم خدمة الاتصالات عن بعد"، وكذلك عُرفت شبكة الاتصالات عن بعد، بذات القانون بالمادة 2\32 بـ"كل تجهيز أو مجموعة تجهيزات التي تؤمن نقل وتوجيه إشارات الاتصالات عن بعد للتمكن من تبادل المعلومات ومن إدارتها بين نقاط النهاية لهذه الشبكة" [3]".

إن الخدمات التي يقدمها مزود الخدمات الفنية "متعهد الوصول"، بموجب عقد الاشتراك في خدمة الإنترنت، هي أشبه ما تكون بعقد المقاولة، الذي يلتزم بمقتضاه مزود الخدمة (المقاول) بتقديم

---

(1) الشوك محمد عبد الرزاق، (2016م)، النظام القانوني لعقد الاشتراك في خدمة الإنترنت، رسالة ماجستير، جامعة الكوفة، العراق، ص51.

(2) Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, mars 2002، مرجع سابق، فقرة واحد وما بعدها، ص4.

(3) L. nº 86-1067, 30 septembre 1986, art. 1 al. 1, JO, 1 octobre 1986, donnant une définition de la télécommunication. والمشار اليه في فرح، أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت (دراسة تحليليه مقارنة)، مرجع سابق، ص330.

خدمة الدخول، أو القيام بما يلزم لتحقيق هذه الغاية لقاء مقابل يلتزم طالب الخدمة بدفعه، ويشترط كذلك أن يتعهد متعهد الوصول باحترام شروط الاستفادة من الخدمة [1].

وعليه فإن العقد الذي يربط متعهد الوصول والمشترك هو عقد ملزم لكلا الجانبين، ويرتب التزامات قانونية لكلا الطرفين، فيقع على متعهد الوصول إتاحة كافة الوسائل الفنية والبرمجيات التي تمكن المشترك من الوصول الى شبكة الإنترنت، وبذات الوقت يقع على عاتق المشترك دفع قيمة الاشتراك حسب ما اتفق عليه مسبقاً [2].

كما لابد من الإشارة إلى أن تكيف عقد الاشتراك بعقد مقاولة، يتفق وما نص عليه المشرعين الفرنسي في القانون المدني لسنة1804م وتعديلاته في نص المادة 1710، والقانون المدني الاردني لسنة1976 في نص المادة 780، حيث عرفا عقد المقاولة هو العقد الذي يتعهد بموجبه أحد الأطراف بأن يصنع شيئاً أو يؤدي عملاً لقاء بدل يتعهد به الطرف الآخر.

الفرع الثاني: التزامات متعهد الوصول

كما أوضح الباحث فإن متعهد الوصول، هو كل شخص طبيعي أو معنوي يقوم بإمداد عملائه بالأدوات والوسائل الفنية التي تلزم لتوصيلهم إلى شبكات الأمن السيبراني، ليتمكن المشركين معه في هذه الخدمة من تصفح المواقع الإلكترونية، والاطلاع على المحتوى الذي يرغبون فيه، من خلال ربطهم بشبكات الاتصالات عن بعد، ونظراً لارتباط متعهد الوصول بشبكات الأمن السيبراني "الإنترنت" بشكل دائم، ولطبيعة الخدمة التي يقدمها، يعد من أهم مقدمي الخدمات عبر شبكات الأمن السيبراني، وبالتالي يقع على عاتقه مجموعة التزامات ذات طبيعة أعلامية وأخرى تقنية.

---

(1) بني حمد عبد السلام أحمد، (2018م)، تأصيل المسؤولية المدنية لمتعهد الإيواء في شبكة الإنترنت في القانون الأردني، مرجع سابق، ص340.

(2) Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, précité, n° 13, p 7. والمشار اليه في فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت، مرجع سابق، ص331.

أولاً: التزامات ذات طبيعة إعلامية

تبعاً لما استقر عليه أحكام القانون وعمل به القضاء، يجب على متعهد الوصول إدامة نشاطه بكل نزاهة وحياد، وأن يمتاز بشفافية والوضوح، وأن يكون مراعياً لقواعد احترام حسن النية، ولتحقيق هذه المبادئ يفترض على متعهد الوصول وتحت طائلة المسائلة في حالة عدم التقيد الالتزام بالإعلام الإيجابي [1]من خلال:

أ. التزام متعهد الوصول الذي يعرض خدماته على طائفة المستهلكين والمستخدمين إعلامهم بالبيانات والمعلومات الخاصة به وبالمشتركين معه، فيقع على متعهد الوصول احترام القواعد العامة، في حماية المستهلك والقواعد المتبعة في القانون التجاري، والتي تفرض على كل شخص يجعل من تقديم خدمات الوصول عبر شبكات الأمن السيبراني مهنة له التعريف عن نفسه للجمهور، كما وبالرجوع إلى طبيعة العلاقة القائمة بين متعهد الوصول والمشترك نجد أنها تقوم على عقد، وحسب القواعد العامة في كل العقود يجب تحديد هوية المتعاقدين، وعقد خدمة الدخول لا يخرج عن هذه القاعدة، ولكن يتم إبرام هذا العقد وتنفيذه عن طريق وسائل إلكترونية وعن بعد عبر الإنترنت ،الأمر الذي ينتج عنه صعوبة تحديد هوية أطرافه [2].

عليه فإنه يقع على متعهد الوصل التعريف عن نفسه لعملائه من خلال الكشف عن أسمة وعنوانه البريدي والإلكتروني ومكان ورقم القيد التجاري العائد له، وهذا بدوره يعزز الثقة والحماية للجمهور المتعاملين معه في حال أخل بأي من التزاماته [3].

([1]) الحايك أودين سلوم، (2009م)، مسؤولية مزودي خدمات الإنترنت الفنية، المؤسسة الحديثة للكتاب، لبنان، ط1، ص255.

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

([3]) المادة 2\15، التوجيه الاوروبي، المرجع السابق، والمادة 2\6 والمادة 2\3\6من القانون الفرنسي، المرجع السابق.

كما ويجب على متعهد الوصول ،وقبل مرحلة التعاقد، الطلب من عملائه تقديم جميع البيانات والمعلومات الشخصية اللازمة لتحديد هويتهم وأهليتهم القانونية وعناوين بريدهم الإلكتروني، كما ويجب عليه بيان الوسيلة التي يستطيع من خلالها عملائه تقديم هذه المعلومات والبيانات المطلوبة، بحيث تكون هذه الوسيلة لها القدرة على تحديد هوية العميل قبل إيصاله بالشبكة، وكذلك لها القدرة بعد إيصاله إلى الشبكة تحديد وقت، ومكان والصفحات الويب التي زارها العميل، على أن تكون هذه المعلومات سرية، لا يتم الكشف عنها إلا للسلطات القضائية بعد طلب ذلك [1].

بقي أن نشير في هذا الصدد أن المشرع الفرنسي والأوروبي لم يلزم متعهد الوصول، بضرورة التأكد من صحة ومصداقية البيانات والمعلومات المقدمة من قبل العملاء عبر شبكة الإنترنت، إلا أن متعهد الوصول، في الواقع العملي يلجأ إلى آلية تسجيل دقيقة للعملاء على المواقع الإلكترونية، إضافة إلى أن المتعهد قد يلجأ أحياناً إلى حجب مؤقت لمفتاح الدخول لشبكة الأمن السيبراني، وذلك بغية إرسال رسالة للعميل على بريده الإلكتروني المعلن تحتوي على كلمة سر ومفتاح لا يستطيع معرفته إلا بعد قراءته هذه الرسالة من بريدة الإلكتروني[2].

ب. يلتزم متعهد الوصول بحفظ البيانات والمعلومات المقدمة له، وأن تكون مدة هذا الحفظ لا تتجاوز في حدها الأقصى سنة واحدة من تاريخ الحصول عليها، وهذا الالتزام جاء إعمالاً

---

(1) المادة 2/15، التوجيه الاوروبي، المرجع السابق، والمادة 2/6 والمادة 2/3/6من القانون الفرنسي، المرجع السابق.

(2) Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, précité, n° 49, p. 20، والمشار الية في فرح أحمد قاسم (2007م)، النظام القانوني لمقدمي خدمة الإنترنت، مرجع سابق، ص345.

للقواعد العامة الخاصة، بحفظ البيانات والمعلومات بشكل عام من قبل مقدمي خدمات الاتصالات عن بعد [1].

ج. يلتزم متعهد الوصول بالإيضاح للمشتركين معه، بالمخاطر المصاحبة لاستخدام المواقع الإلكترونية عبر شبكات الإنترنت، وإعلامهم بضرورة وجوب احترام القوانين والأنظمة السارية وعدم استخدام شبكات الأمن السيبراني كوسيلة للاعتداء على حقوق الآخرين أثناء استخدامهم لها [2].

د. يتوجب على متعهد الوصول، وانطلاقاً من مبدأ حسن النية في إدارة شبكات الأمن السيبراني عبر الإنترنت، التعاون مع الجهات الإدارية والقضائية وجميع المعنيين بالخدمات المقدمة عبر الشبكة من جمهور المستخدمين والعاملين في قطاع الخدمات عبر الإنترنت، وهذا الالتزام مكمل للالتزامات الأخرى ذات الطبيعة التقنية [3].

ويرى الباحث أن هذه الالتزامات ذات طبيعة فنية تحتاج إلى تقنيات من قبل متعهد الوصول أكثر من كونها بحاجة إلى تشريعات تنظمها فهي تحتاج لبذل عناية من قبل متعهد الوصول لتلافي المسائلة في حال أي خلل فيها من قبل المتعهد أو المستخدم.

---

(1) أنظر المادة 3\32، قانون البريد والاتصالات الفرنسي، مرجع سابق، Loi n° 2001-1062, 15 novembre 2001 relative à la sécurité quotidienne, JO, 16 novembre2001.

(2) حول هذا الصدد أنظر:

CA Versailles, 12e ch., 8 juin 2000, précité, CA Pau, 14 octobre 1999, n° 97/003191, SA France Télécom C/L, TGI Nanterre, 1re ch., sect. A, 8 décembre 1999, précité

(3) التوجيه الأوروبي حول التجارة الإلكترونية، مرجع سابق، المادة 3\14

ثانياً: التزامات ذات طبيعة تقنية

العمل الذي يقوم فيه متعهد الوصول عمل ذو طبيعة فنية يتمثل في تمكين عملائه من الوصول الى شبكة الإنترنت، وإتاحة الطريق أمامهم، للوصول إلى المواقع التي يرغبون في الاطلاع على مضمونها من المعلومات والبيانات، دون أن يكون لمتعهد الوصول أي علاقة بالمحتوى المعلوماتي المنقول أو الرسائل المتبادلة عبر شبكات الإنترنت، فدوره ينحصر ويمتاز بالحياد التام، ولا يحق له الاطلاع على المضمون المعلوماتي ،الذي مر من خلاله، وبالتالي واستناداً لهذا الدور لا يترتب عليه مسؤولية عن المضمون غير المشروع إلا ضمن شروط معينة [1].

وأكد على ما سبق أحكام القضاء الفرنسي في هذا المجال لتؤكد أن دور متعهد الوصول ينحصر فقط في تأمين النقل الفوري للمعلومات والبيانات دون إلزامه بمراقبة المضمون الذي يعبر من خلال له بشكل عام [2]،حيث جاء حكم في دعوى رفعها اتحاد الطلاب اليهود أمام قاضي الأمور المستعجلة لمحكمة بداية باريس ضد عدد من متعهدي الوصول الذين سمحوا بنشر عدد من الخطابات والإرشادات العنصرية المعادية للسامية على شبكة الإنترنت، حيث طالب الاتحاد القاضي الفرنسي إصدار قرار يلزم فيه متعهدي الوصول بشطب المادة المعلوماتية المذكورة على صفحات الويب أو على الأقل منع الوصول إليها بصرف النظر عن موقعها على الإنترنت، ونظراً لاتصاف طلبهم بالعمومية وعدم الدقة، ونظراً لاستحالة تحقيق هذا المطلب فنياً، بسبب عدم إمكانية مراقبة ملايين الرسائل التي تبث يومياً عبر شبكة الإنترنت، جُوبه طلبهم من قبل قاضي الأمور

---

(1) النقروز علي، (2017م)، جرائم نظم المعلومات، دار السناء للنشر، الاردن، عمان، ص335، وانظر كذلك منصور محمد حسين، (2003م) مرجع سابق، ص 214.

(2) انظر our de Cassation Criminelle الجزائية محكمة النقض) , 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.

المستعجلة الفرنسي، وأعلن القاضي في قراره الصادر في 20/تشرين الثاني/2000م، عدم إلزام متعهد الوصول بالرقابة الفعلية للمضمون المعلوماتي الذي يعبر من خلاله [1]، وهذا ما تبناه كذلك مجلس الدولة الفرنسي بإقرار المبدأ سابقاً في عام 1998 حيث أعفى متعهد الوصول من واجب الرقابة السابقة للشرعية المضمون مع أخذ بعين الاعتبار التوازن بين مبدأين أولهما الحياد التام للمتعهد والثاني أخذ الحيطة والحذر بالقدر الكافي الذي يتعين على كل مهني مراعاته [2]، كما وتبنى المشرع الأوروبي المبدأ ذاته وأضاف عدم إلزام متعهد الوصول بالبحث النشط عن الوقائع والظروف التي تكشف الأنشطة غير المشروعة وهذا ما نص عليه التوجيه الأوروبي حول التجارة الإلكترونية لسنة 2001م بالمادة 1/15 .

وكما بينا أعلاه فإن متعهد الوصول لا يسأل عن المضمون غير المشروع إلا ضمن شروط معينة وهي الإخلال بإحدى التزاماته التقنية وهذه الالتزامات هي:

أ. الالتزام بالحفاظ على سرية الاتصالات، وعدم الكشف عن مضمونها إلا للسلطة القضائية المختصة عند الضرورة [3].

ب. الالتزام بممارسة الرقابة المؤقتة والموجهة، للمضمون الذي يقوم تمريره المستخدم من خلاله، وهذا بناءً على أمر من السلطة القضائية المختصة، ويقع على عاتقه تبليغ السلطات العامة في الدولة عن أي مضمون إلكتروني غير مشروع [4].

---

(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.

(2) أنظر: السحيباني عبد الله، (2011م)، كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم الامنية ص 427وانظر منصور، (2003)، مرجع سابق ، ص214.

(3) المادة3/6-2، القانون الفرنسي حول الثقة في الاقتصاد الرقمي.

(4) المادة 1/6-7، المرجع نفسه، وأنظر التوجه الاوروبي حول التجارة الإلكترونية، مرجع سابق، رقم 47.

وهنا يرى الباحث أن التزامات متعهد الوصول التقنية هنا تعتمد على الإخطار من قبل السلطة المختصة أو العلم بالمحتوى غير المشروع حيث يلزم بإبلاغ السلطات العامة عنه، وهذه الالتزامات لا تتعارض مع طبيعة عمله كناقل فقط والالتزام بها يعفيه من المسؤولية.

ج. يقع الالتزام على متعهد الوصول وجوب الاقتراح على المشتركين معه بخدمة الوصول الوسائل الفنية، التي تمكنهم من عدم الوصول إلى بعض المواقع المشبوهة، بحيث تكون هذه الوسائل بمثابة رقابة ذاتية على أنفسهم ابتداءً ومن ثم على أفراد أسرهم [1].

ومن هذه الوسائل الفنية، نظام يمكنهم من فلترة وتصفية المعلومات إلكترونياً، بحيث لا يتم استقبال إلا المحتوى المعلوماتي الإلكتروني الذي يتوائم مع ثقافاتهم والقيم الراسخة لديهم وفق معايير مجتمعاتهم ودياناتهم وأخلاقهم ... [2].

بقي الإشارة إلى أنه وعلى الرغم من الالتزامات السابقة لا يوجد نص قانوني محدد وصريح يفرض على متعهد الوصول مراقبة المحتوى المعلوماتي الذي يعبر من خلاله، وبالتالي لا يستطيع عمل فلترة لجميع المحتوى الغير مشروع والتخلص منه؛ وهذا يرجع للكم الهائل من المعلومات والبيانات التي تعبر عبر شبكة الإنترنت بشكل يومي، فمراقبتها بشكل دقيق، وشمولي، يعد من ضروب الخيال، فلجأ القضاء وفق اجتهاداته إلى عدة مبادئ منها فرض التزام الرقابة العشوائية من خلال انتقاء محتوى معلوماتي بين الحين والآخر ووضعه تحت الرقابة، ومبدأ أن مستخدم الإنترنت هو الأقدر على معرفة ما يعد مشروع أو غير مشروع من المحتوى المعلوماتي، نظراً لاختلاف الثقافات والديانات والقيم من شخص لآخر، ومبدأ أخر وهو أن القضاء الأقدر على تصنيف المحتوى غير

---

(1) المادة 6\1، القانون الفرنسي، المرجع نفسه.

(2) أنظر منصور محمد حسين، (2003م)، المسؤولية الإلكترونية مرجع سابق، ص209.

المشروع، وهو المسؤول عن اصدار الأوامر بوقف نشره أو شطبه تحت طائلة المسؤولية في حال عدم الامتثال من قبل متعهد الوصول [1].

يرى الباحث أن السبب في فرض هذه المبادئ، يرجع إلى الصعوبات الفنية المرافقة للرقابة، وعدم ترك أمر تحديد شرعية المحتوى إلى متعهد الوصول، لاختلاف الثقافات فما يعد مشروعاً في مجتمع، قد يعد غير مشروعاً في مجتمع آخر، وعليه فإرساء هذه المبادئ هو الأقرب للعدالة، والإنصاف، والابتعاد عن المزاجية والأهواء، وإرساء حق المتضرر باللجوء للقضاء وفق قواعد وأعراف العدالة.

بعد أن تم بيان الالتزامات المعلوماتية، والالتزامات الفنية لمقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية وفقاً للقوانين والفقه المقارن، كان لابد من بيان موقف المشرع الأردني من هذه الالتزامات وهل ورد نصوص قانونية تعالج هذه الالتزامات أم ترك الأمر على الغالب أو لاجتهاد القضاء وهو ما سوف يتم بيانه في مطلب مستقل ليكون الباحث قد أتم بيان هذه الالتزامات وفق التشريع الأردني.

---

[1] أنظر في فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت (دراسة تحليليه مقارنة)، مرجع سابق ص249وص250، وأنظر ابو الحسن حنين جميل، (2021م)، الإطار القانوني لخدمة الأمن السيبراني (دراسة مقارنة)، مرجع سابق ص93 وما بعد.

المطلب الثالث

التزامات مقدمي الخدمات الإلكترونية عبر الإنترنت للبيانات السيبرانية وفق التشريع الأردني

بعد بيان مقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية بكافة أسماؤهم الوظيفية، وبطبيعة نشاطاتهم، والالتزامات المترتبة عليهم؛ حيث بين مقدمي الخدمات المعلوماتية وهم متعهد الإيواء، ومورد المعلومات، ومقدمي الخدمات الفنية، وهم ناقل المعلومات ،ومتعهد الوصول عبر شبكات الإنترنت، وكان ذلك ضمن القانون المقارن، والاجتهادات القضائية، مع الإشارة إلى التشريع الأردني بقدر ما نصوص الواردة في التشريع الأردني أسعفت الباحث، إلا أن تلك النصوص جاءت في سياق العمومية وفق القواعد العامة، ومفرقة وموزعة في عدة قوانين من التشريع الأردني، كما ويلاحظ أنها لم تغطي كافة الموضوعات المتعلقة بمقدمي الخدمات عبر شبكات الأمن السيبراني، من ناحية المفهوم والالتزامات المترتبة عليهم، وعليه رأى الباحث ضرورة جمع هذه النصوص والإشارة لها في مطلب واحد على النحو الاتي .

الفرع الأول: مفهوم مقدمي الخدمات الإلكترونية عبر شبكات الإنترنت للبيانات السيبرانية وفق التشريع الأردني

ورد مفهوم مقدمي الخدمات الإلكترونية عبر شبكات الإنترنت للبيانات السيبرانية في نصوص مجموعة من القوانين الأردنية ومنها ما ورد في قانون الجرائم الإلكترونية لسنة 2023م حيث عرف مزود الخدمة فيه "كل شخص طبيعي أو معنوي، عام أو خاص، يزود المشتركين بالخدمات

الإلكترونية بواسطة تقنية المعلومات أو يقوم بمعالجة المعلومات أو تخزينها نيابة عن خدمة الاتصالات أو مستخدميها[1]".

يرى الباحث أن التعريف السابق جاء عام يشمل جميع مقدمي الخدمات الإلكترونية عبر شبكات الأمن السيبراني، فجاء مشتمل لمتعهد الإيواء وهو الذي يقع على عاتقه تخزين المعلومات بإتاحة مساحات على حاسباته الآلية، وجاء أيضاً مبين لمورد المعلومات، الذي يقوم بمعالجة البيانات أو تأليفها أو جمعها، وشمل التعريف كذلك ناقل المعلومات ،ومتعهد الوصول وهذا من خلال الإشارة الى أعمالهم التقنية في مجال الخدمات التقنية عبر شبكات الأمن السيبراني، من خلال هذا التعريف، ورغم حداثة القانون إلا أن التعريف لا يزال في نطاق العمومية ويحتاج الى القياس مع القوانين المقارنة.

كما جاء في قانون الاتصالات لسنة 1995م وتعديلاته، تعريف خدمة الاتصالات "هي الخدمة التي تتكون كلياً أو جزئياً من إرسال المعلومات، واستقبالها، وتمريرها على شبكات الاتصالات، باستخدام أي من عمليات الاتصالات " وكذلك عرف خدمة الاتصالات العامة بأنها "خدمة الاتصالات المقدمة للمستفيدين عامة أو لفئة معينة مقابل أجر [2]".

التعاريف السابقة الواردة في قانون الاتصالات، تتوافق وعمل متعهد الوصول للمعلومات عبر شبكات الأمن السيبراني، الذي يعتمد في عملة على تقديم خدمة نقل المعلومات عبر وسائل الاتصالات عن بعد، وأيضاً يلاحظ أن أساس قيام العلاقة بين مقدم الخدمة والعميل هي خدمة مقابل أجر، وبالتالي لابد من وجود عقد يبين الالتزامات لكل من العميل "دفع أجر"، ومقدم الخدمة

---

[1] المادة 2، قانون الجرائم الإلكترونية رقم 17 لسنة 2023.

[2] أنظر المادة 2، قانون الاتصالات وتعديلاته رقم 13 لسنة 1995، والمنشور في الجريدة الرسمية بتاريخ 1995/10/1م، عدد4072، ص2939، الفصل الاول منه، التعريفات.

"نقل المعلومات"، وهو ما يتفق مع عمل مقدم الخدمات التقنية عبر شبكات الأمن السيبراني "متعهد الوصول"، إلا أننا لا زلنا أمام القياس والمقارنة للتوصل لتعريف متعهد الوصول.

كما جاء في نفس القانون بنص المادة الثانية تعريف تكنولوجيا المعلومات، وهي "إنشاء المعلومات ومعالجتها وتخزينها باستخدام وسائل إلكترونية" وهو ما يتوافق مع واجبات مقدمي الخدمات المعلوماتية عبر شبكات الأمن السيبراني، سواء متعهد الإيواء أو مورد المعلومات الذي يكون جزء من واجباته إنشاء معلومات ومعالجتها ودورة كناشر للمعلومة، والتخزين على الحاسبات الآلية لمتعهد الإيواء.

ورد في قانون الإعلام المرئي والمسموع لسنة 2015م تعريف الإعلام المرئي والمسموع " كل عملية بث تلفزيوني أو إذاعي توصل للجمهور أو فئات معينة منه إشارات أو صوراً أو أصواتاً أو كتابات من أي نوع كانت، لا تتصف بطابع المراسلات الخاصة، وذلك بواسطة القنوات والموجات وأجهزة البث والشبكات وغيرها من تقنيات ووسائل وأساليب البث والنقل" [1].

على الرغم من أن المقصود بهذا التعريف الإعلام التلفزيوني والإذاعي، إلا أنه يشتمل على طابع أقرب ما يكون إلى مقدم خدمات المعلومات عبر الإنترنت، مورد المعلومات الذي يقوم بدور الناشر للمحتوى المعلوماتي عبر شبكات الإنترنت، وبإسقاط القواعد العامة ومع تطور التكنولوجيا، قد تكون قنوات البث عبر الإنترنت، ويتم البث للمحتوى عبر شبكات الإنترنت، كما هو دارج بالبث المباشر، عبر تطبيقات التواصل الاجتماعي أو البث عبر قنوات تطبيق اليوتيوب وهو ما يتوافق عموماً مع التعريف أعلاه.

---

[1] أنظر المادة 2، قانون الاعلام المرئي والمسموع رقم 27 لسنة 2015م، المنشور بالجريدة الرسمية بتاريخ 2015/6/1م، عدد5343، ص5614.

عرف المنشئ في قانون المعاملات الإلكترونية الأردني لسنة 2015م وتعديلاته، بأنه "الشخص الذي يقوم بإنشاء الرسالة المعلوماتية وإرسالها" وعرف كذلك الوسيط الإلكتروني بأنه "البرنامج الإلكتروني الذي يستعمل لتنفيذ إجراء أو الاستجابة للإجراء بشكل تلقائي، بقصد إنشاء رسالة معلومات أو إرسالها أو تسليمها " [1].

يرى الباحث أن التعريف يقتصر على تبادل الرسائل الإلكترونية ليس إلا، وبالتالي غير كافٍ لبيان مفهوم متعهد الإيواء.

بالرجوع إلى قانون الأمن السيبراني الأردني لسنة 2019م نجد أن المشرع، حظر على شخص أو جهة تقديم الخدمات الإلكترونية عبر شبكات الأمن السيبراني، بدون الحصول على التراخيص اللازمة [2]، وهنا أقر القانون بوجود مقدمي خدمات الإلكترونية بدون بيان هذه الخدمات أو تعريف واضح لها.

بقي أن نشير إلى أن التشريع الداخلي للدول، يأتي متناسق مع الاتفاقيات التي ينظم إليها، بمجرد إقرارها والإمضاء عليها ودخولها حيز التنفيذ، لتصبح جزءاً من التشريع حيث أنظم الأردن إلى الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات لسنة 2012م، حيث جاء فيه تعريف مزود الخدمة كما ورد في قانون الجرائم الإلكترونية لسنة 2023م.

الفرع الثاني: التزامات مقدمي الخدمات الإلكترونية عبر شبكات الإنترنت للبيانات السيرانية وفق التشريع الأردني.

كما بين الباحث في المطلب السابق أن تعريفات مقدمي خدمات عبر شبكات الأمن السيبراني والتي جاءت غير مخصصة، وتتسم بالعمومية، ومفرقة بين طيات نصوص قوانين التشريع الأردني،

---

[1] أنظر المادة 2، قانون المعاملات الإلكترونية رقم 15 لسنة 2015م.

[2] أنظر المادة 10، قانون الامن السيبراني الأردني رقم 16 لسنة 2019.

كذلك هو الحال بالنسبة للالتزامات التي تقع على عاتق مقدمي خدمات الإلكترونية عبر شبكات الأمن السيبراني، فكان لابد من الإشارة لهذه النصوص وبيانها مقارنة مع القواعد العامة لالتزامات مقدم الخدمات، بحسب ما استقر عليه القانون المقارن، والاجتهاد القضائي وإسقاطها على المتاح من نصوص التشريع الأردني لنكون أمام أسس موضوعية، تترتب بموجبها التزامات مقدمي الخدمات وهذا ما سوف نبينه من خلال أستعراض إلتزامات مقدمي الخدمات بموجب قانون الجرائم الإلكترونية وإلتزامات موردي الخدمات في التريع الأردني.

أولاً: التزامات مقدمي الخدمات بموجب قانون الجرائم الإلكترونية الأردني

هذا القانون ذو صفة جزائية إلا أن المواد الجزائية تحدد المسؤوليات القانونية، ويمكن القياس على الإجراءات الجزائية، والالتزامات من أجل أعمال القواعد العامة للمسؤولية المدنية في حال عدم وجود نص في القانون المدني يبينها، والباحث في هذا الصدد يبين أهم الالتزامات التي بينها هذا القانون بين طياته، ويستمد منها أهم التزامات مقدمي الخدمات عبر شبكات الأمن السيبراني وتتلخص بالنقاط التالية:

أ: تقع مسؤولية الشخص المسؤول عن إدارة المواقع الإلكترونية، أو منصات التواصل الاجتماعي، أو أي حساب عام، أو مجموعة عبر الإنترنت، أو قناة أو ما يماثلها، في حال علمه بالمحتوى المعلوماتي غير قانوني الذي يبث عبر ما هو مسؤول عن إدارته، عن طريق طلب من المتضرر من جراء نشر المحتوى الغير قانوني أو إخطار من الجهات ذات الاختصاص، بشرط عدم قيامه بإزالة هذا المحتوى المنشور لديه، وتنتفي هذه المسؤولية في حال إزالة هذا المحتوى غير المشروع [1].

[1] أنظر المواد 25/أ و25/ب، قانون الجرائم الإلكترونية رقم 17 لسنة 2023م.

يرى الباحث أن هذا يتوافق مع التزامات مورد المعلومات، المسؤول عن جمع أو تأليف المعلومات ونشرها عبر مواقع الإلكترونية عبر شبكات الأمن السيبراني، كناشر للمعلومة وكما أشرنا فلا بد من وجود ناشر أو مسؤول عن هذه المواقع الإلكترونية، ويشترط لمنع مسؤوليته إزالة المحتوى غير المشروع قانوناً، أو الذي يلحق الضرر بالغير، بناءً على طلب المضرور أو أخطار الجهة ذات الاختصاص [1].

ب: مع مراعاة الغير حسن النية، وبناءً على قرار قضائي، سواء صدر عن المدعي العام أو المحكمة المختصة، يقع على عاتق أي نظام معلوماتي أو موقع إلكتروني أو مزود خدمة قام بنشرِ أي محتوى معلوماتي غير قانوني، أو ارتكب أي فعل غير قانوني، بموجب أحكام قانون الجرائم الإلكترونية، التزام بحظر أو إيقاف أو تعطيل أو تسجيل أو اعتراض خط سير البيانات أو المحتوى المعلوماتي غير المشروع، وكذلك منع الوصول آليه أو حظر المستخدم أو الناشر مؤقتاً [2].

يرى الباحث أن التزامات مقدمي الخدمات الإلكترونية عبر شبكات الأمن السيبراني، وفق قانون الجرائم الإلكترونية، تتطابق وفق ما استقر عليه القانون المقارن، فتنتفي مسؤولية مزودي الخدمة، بعد علمهم بالمحتوى غير المشروع، بموجب قرار قضائي بشرط تعطيلهم أو حجبهم أو إزالة هذا المحتوى، كما أن اشتراط العلم بموجب قرار قضائي، يبعد مزودي الخدمة عن

---

[1] أنظر: منصور محمد حسين، (2003م)، المسؤولية الالكترونية، مرجع سابق، ص 201 وكذلك ما تناوله الباحث حول التزامات مورد المعلومات في ص41 وما بعد.

[2] أنظر: المادة 33/أ/1، قانون الجرائم الإلكترونية.

العشوائية، والهوائية في اعتبار المحتوى مشروع أم لا، لأن ما يعتبر مشروعاً في مكان قد لا يكون مشروعاً في مكان آخر [1].

ج: يقع التزام على عاتق مقدمي الخدمات، كما ورد في نصوص هذا القانون، الاحتفاظ بالبيانات والمعلومات العائدة للمستخدم، التي تمكن الجهات القضائية من الرجوع إليها، عند الحاجة لها، لتحديد هوية الشخص الذي قام بنشر المحتوى غير المشروع عبر شبكات الأمن السيبراني، لتتمكن من إجراء الملاحقة القانونية، مع مراعات الحفاظ على سرية المعلومات والبيانات المتعلقة بالمستخدم [2].

د: يتوجب على مقدمي الخدمات أن تكون لهم معلومات وبيانات تتعلق بهم أيضاً تتسم بالوضوح أمام الجهات المختصة، كما وأكدت نصوص القانون أن منصات التواصل الاجتماعي التي لديها عدد مشتركين يزيد عن مائة ألف مشترك، يجب أن يكون لها مكتب داخل الأردن، للتعامل مع الطلبات والإشعارات القضائية، الصادرة عن الجهات الرسمية والقضائية وفي حال عدم التقيد تكون معرضة للمسؤولية [3].

هـ: يقع على مقدمي الخدمات التزام بحفظ وتخزين البيانات والمعلومات، اللازمة لإظهار الحقيقة، وكذلك المحافظة على سلامتها، وبالأخص المحتوى غير المشروع، ليكون بمقدور المحكمة الرجوع إليها واعتبارها حجية لإثبات الواقعة [4].

---

[1] أنظر في فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت (دراسة تحليليه مقارنة)، مرجع سابق ص249وص250، وأنظر ابو الحسن حنين جميل، (2021م)، الإطار القانوني لخدمة الأمن السيبراني (دراسة مقارنة)، مرجع سابق ص93 وما بعد.

[2] أنظر المواد 33/أ/2 و33/أ/4، قانون الجرائم الإلكترونية الاردني، 2023م.

[3] أنظر، المادة 33/أ/2 والمادة 37، قانون الجرائم الإلكترونية ،2023م.

[4] أنظر المادة 33/أ/3و المادة 36/أ، قانون الجرائم الالكترونية ،2023م.

يرى الباحث، أن المشرع الاردني وفق في هذه الالتزامات، بين أن يكون لمزود الخدمة أسم وسجل ومكان وقيد عمل، وبين أن يكون للمستخدم معلومات وبيانات تدل عليه، كما ولا بد من إعمال القواعد العامة والفنية، التي يتبعها متعهد الوصول لتحديد هوية المستخدم والتي أشرنا إليها فيما سبق، كما ويتضح أنه يجب على مقدمي الخدمات الاحتفاظ المؤقت بالمحتوى المعلوماتي المنشور.

ثانياً: التزامات موردي الخدمات في نصوص التشريع الأردني

1. قانون المعاملات الإلكترونية لسنة 2015م، نظم هذا القانون المعاملات التي تتم بوسائل إلكترونية، حيث جاء فيه أن أحكامه تسري على كافة المعاملات، التي تتم بواسطة وسائل إلكترونية [1]، وعليه وبإسقاط هذه القاعدة على مقدمي الخدمات عبر شبكات الإنترنت، نجد إن الاتفاقيات التي تعقد بين مقدمي الخدمات الفنية، ومستخدمين الإنترنت، ليستفيدوا من الخدمات، ما هي إلا عقود واتفاقيات مبرمه إلكترونياً عبر شبكات الأمن السيبراني، ومنه العقد بين متعهد الوصول وعملائه، فالأول ملزم بتقديم خدمة والآخر ملزم بدفع مقابل للخدمة لذلك فقانون المعاملات منظم بأحكامه لمثل تلك المعاملات وعليه يمكن استخلاص مجموعة من الالتزامات، التي تقع على عاتق مقدمي الخدمات عبر شبكات الأمن السيبراني ،بموجب نصوص القانون يبينها الباحث على النحو الاتي:

أ- يقع على عاتق مقدمي الخدمات الإلكترونية التزام، بتوفير الحماية للسجلات عملائه ومعاملاتهم وبياناتهم، والمحافظة على سريتها وسلامتها من أي تحريف أو اختراق [2].

---

[1] أنظر المادة 3/أ، قانون المعاملات الالكترونية الأردني، لسنة 2015م وتعديلاتة.

[2] أنظر المادة 4/ب/3 قانون المعاملات الالكترونية الأردني، لسنة 2015م وتعديلاتة.

ب- على الرغم من اقتصار القانون على لفظي المنشئ والمرسل إليه(وهو متعلق فقط بتبادل الرسائل الإلكترونية، ومجرد تعريفهما وحدة لا يكفي، ليشمل مزودي الخدمات) إلا أنه ألزم عليهما التعريف عن نفسيهما، وألزم مقدم الخدمات طياً في نصوصه، حفظ وقت وتاريخ إنشاء الرسالة، أو إرسالها، أو تسلمها، وكذلك حفظ محتواها، ليتم الرجوع لهم في أي وقت دعت الحاجة لذلك [1].

يرى الباحث أن هذا يتفق والالتزامات العامة لمقدمي الخدمات، والمتعلقة بالاحتفاظ المعلومات وبيانات المستخدم والمحتوى المرسل من قبله أو المنشور والذي أشير إليه في المطالب السابقة.

2. قانون الأمن السيبراني لسنة 2019م، على الرغم من أن هذا القانون يعد القانون المتعلق بالأمن السيبراني، إلا أنه لم يرد التزامات مقدمي الخدمات عبر شبكات الأمن السيبراني، بشكل واضح ومفصل، إلا أنه يمكن بيان التزامات مقدمي الخدمات من خلال النصوص العامة على النحو الآتي:

أ. يقع على عاتق مقدمي الخدمات التزام الحصول على الرخص اللازمة لتقديم الخدمات وفق أحكام القانون، وبالتالي لابد من أن يكون لمقدم الخدمة عنوان واسم وقيد وسجل للممارسة عمله، وفقاً للعرف فلا يمكن منح تصريح بدون ذلك [2].

ب. يقع كذلك على مزودي الخدمات عبر شبكات الأمن السيبراني، تصويب المخالفة المتعلقة بالأمن السيبراني، من خلال حجب أو إلغاء أو مصادرة أو تعطيل شبكة الاتصالات ونظام

---

[1] أنظر، المادة 7، قانون المعاملات الالكترونية، لسنة 2015م وتعديلاتة.

[2] أنظر المادة 10، قانون الأمن السيبراني رقم 16 لسنة 2019 م.

المعلومات، والرسائل الإلكترونية الخاصة، في حال ارتكب أو أشترك في أي عمل، يشكل حادث أمن سيبراني، وهذا بعد قرار من المركز الوطني لإدارة الأزمات [1].

وهنا يرى الباحث على الرغم من أن هذه الالتزامات جاءت بشكل عام، ووردت من ضمن صلاحيات الهيئات القائمة على الأمن السيبراني، إلا أنها تقع وما استقر عليه الفقه والقانون المقارن، حول التزامات مقدمي الخدمات عبر شبكات الأمن السيبراني.

3. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012، وبانضمام الأردن لها أصبحت جزء من التشريع، حيث جاء فيها مجموعة من الالتزامات لمقدمي الخدمات عبر شبكات الأمن السيبراني ومنها:

أ. يلزم مقدمي الخدمات عبر شبكات الأمن السيبراني، ضمن اختصاصه الفني، بجمع وتسجيل معلومات مستخدمينه، والاحتفاظ بها، لتكون مرجع لسلطات المختصة في حال طلبها من أجل تتبع المستخدمين أصحاب المحتوى غير المشروع.

ب. يقع إلزاماً على مقدمي الخدمات عبر شبكات الأمن السيبراني الحفاظ على سرية المعلومات لعملائه [2].

بقي أن نشير أن هناك تشريعات أخرى، ورد فيها التزامات لمقدمي خدمات الأمن السيبراني، ومنها قانون الاتصالات وتعديلاته رقم 13 لسنة 1995، والقوانين المتعلقة بالملكية الفكرية وحقوق المؤلف الأردني، وقانون البريد والمراسلات، وجميعها كانت شبيها بما سبق ولعدم الإطالة نكتفي بالإشارة لها.

---

[1] أنظر المادة 16، قانون الأمن السيبراني رقم 16 لسنة 2019 م.

[2] أنظر المادة 28/ب، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2012م.

بعد بيان الالتزامات لمقدمي الخدمات عبر شبكات الأمن السيبراني، سواء وفق القانون المقارن، أو الفقه أو الاجتهادات القضائية أو التشريع الأردني، نجد أن أهم التزام هو حفظ البيانات والمعلومات، والمحافظة على سريتها وسلامتها، وهذا يقودنا إلى تسأل حول فيما إذا أخل بهذه الالتزامات، ونتج عنها إضرار ببيانات الأمن السيبراني، فما هي حدود المسؤولية المدنية لمقدمي خدمات الأمن السيبراني، إذا ما كانون هم السبب في هذا الضرر، أو كان ناتجاً عن الغير وهذا ما سوف يبينه الباحث في الفصل القادم من هذا البحث.

الفصل الرابع

الإطار القانوني للمسؤولية المدنية عن الإضرار بالبيانات السيبرانية

تحديد المسؤولية المدنية لمقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية، يعتبر من أكثر الموضوعات صعوبة، وذلك يرجع لعدة محاور؛ أولها اعتماد شبكات الأمن السيبراني على طرق فنية معقدة لإدارة أعمالها، وثانيها أن النشاط الإلكتروني ذو طابع عالمي، فقد أصبحت جميع دول العالم على الإنترنت كقرية صغيرة، وبالتالي لا يخضع هذا النشاط لسيطرة دولة معينة، أو يتبع لإدارة مركزية بعينها، ونظراً لاجتماع الطابع الفني والعالمي للنشاط الإلكتروني نتج عنهما، المحور الثالث وهو كثرة الجهات التي تعرض خدماتها في هذا المجال، أما المحور الرابع فهو وجود كم هائل من المتدخلين في تسير هذه الشبكة، وهنا أيضاً يثار تساؤل عن مدى مسؤولية كل متدخل في المعلومات عبر شبكات الأمن السيبراني، وخاصةً أن النشاط الإلكتروني يظهر بشكل سلاسل متصلة ومرتبطة ببعضها البعض.

تتحقق المسؤولية المدنية بحق صاحب المعلومة أو منتجها أو مؤلف الرسالة التي تبث عبر شبكات الأمن السيبراني، والتي يتضمن محتواها مخالفة للقانون أو الأنظمة السارية، أو تحتوي بذاتها على أمور غير مشروعة، أو تلحق ضرر بالآخرين، أو ببيانات الأمن السيبراني، إلا أنه هناك تباين وجدل حول المسؤولية المدنية للقائمين على إدارة هذه المحتويات عبر شبكات الأمن السيبراني من مقدمي الخدمات عبر الإنترنت [1].

إن التباين والجدل في أساس المسؤولية لا يعني، بأي صورة من الصور، استبعاد المسؤولية المدنية عن مقدمي الخدمات، بحيث يصبح الممنوع مشروعاً، لأن هذا الاختلاف في الأسس القانونية

---

[1] منصور محمد حسين، (2003م)، المسؤولية الالكترونية، مرجع سابق، ص 185 و196.

يقودنا إلى الأسباب التي تستند عليها المسؤولية المدنية لمقدمي الخدمات عبر شبكات الأمن السيبراني، كالإخلال بالتزام تعاقدي أو انتهاك حقوق الملكية الفكرية أو إفشاء أسرار مهنية أو المساس بحرمة الحياة الخاصة، فمجرد هذا الاختلاف في نوعية المخالفات المتعددة، يثير الجدل حول الأساس الأنسب للمسؤولية القانونية، حيث يظهر نظريتان، أولهما الأخذ بطبيعة المخالفة نفسها فقط، بحيث يخصص نصوص قانونية لمعالجة كل مخالفة على حدى، ثانيهما وضع قواعد عامة للمسؤولية جراء الإضرار ببيانات الأمن السيبراني، بغض النظر عن طبيعة المخالفة [1] .

تطبيقاً للنظريتين السابقتين، اتجه المشرع الأمريكي للحد من الإعتداءات على حقوق الملكية الفكرية، من خلال إصدار قانون في 28\ تشرين الأول \1998م تحت اسم " Digital Milleniam Copyright Act "(DMCA) والذي خصص فيه الباب الثاني منه، لتحديد مسؤولية مقدمي خدمات الإنترنت، جراء التعدي على حقوق الملكية الفكرية، حيث أفرد هذه المخالفة لوحدها بهذا القانون، و بين شروط معينة لتحقيق مسؤوليتهم أو انتفائها، وهذا يعني تطبيق النظرية الأولى لتحديد أسس المسؤولية المدنية لمقدمي الخدمات، وعلى خلاف ذلك اتجه الإتحاد الأوروبي، من خلال التوجه الأوروبي حول "التجارة الإلكترونية " لعام 2000م، حيث ترك الخيار للدول في هذا السياق، فاتجهت أغلب الدول الأوروبية الى تبني توجه عام، مضمونه وضع قواعد عامة للمسؤولية المدنية جراء الإضرار ببيانات الأمن السيبراني دون أي تخصيص[2].

---

[1] منصور محمد حسين، (2003م)، المسؤولية الالكترونية، مرجع سابق، 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] André LUCAS, "La responsabilité des différents intermédiaires de l´internet", in L´internet et le droit– Droit européen et comparé de l´internet, Colloque organisé par L´Université de Paris I, Paris, 25 et 26 septembre 2000, p. 2, disponible à l´adresse: www.droit-internet-2000.univ-paris1.fr/di2000_20.htm., p. 2.. وقت الدخول "20:30" تاريخ الدخول 5\11\2023م.

تطبيقاً لهذا التوجه، جاء القانون الفرنسي الصادر في 21/ حزيران/2004 م حول الثقة في الاقتصاد الرقمي، والقانون البلجيكي الصادر في 1/أذار/2003م حول التجارة الإلكترونية، والقانون الألماني الصادر في 22/ تموز /1997م وتعديلاته حول الاتصالات عن بعد، وغيرها من القوانين الأوروبية، لتثبيت قواعد عامة لحدود المسؤولية دون إجراء أي تفرقة بين نوعية المخالفة المرتكبة عبر شبكات الأمن السيبراني، حيث تم تحديد نطاق المسؤولية، وشروط تحققها وأساسها القانوني. تكون المسؤولية المدنية واضحة الأساس، عندما نكون أمام نصوص تشريعية تبين حدود المسؤولية المدنية لمقدمي الخدمات عبر شبكات الأمن السيبراني، وفقاً لنوع المخالفة كما بالتشريع الأمريكي، ولكن في حال إعمال القواعد العامة للمسؤولية المدنية، وبالأخص أن المشرع الأردني لم يفرد نصوصاً تشريعية خاصة بالمسؤولية المدنية لمقدمي الخدمات عبر شبكات الأمن السيبراني اتجاه الإضرار بالبيانات السيبرانية، وعندها لا بد من البحث في القواعد العامة للمسؤولية المدنية والتي تقع على قاعدتان عامتان، هما المسؤولية العقدية والمسؤولية التقصيرية، وإسقاطهما على مقدمي الخدمات عبر شبكات الأمن السيبراني، في حال كان لهم دور في الإضرار بالبيانات السيبرانية، وفقاً للتشريع المقارن والتشريع الأردني، إن إثارة هذا الكم من التساؤلات، هو ما سوف يتم الإجابة عنه في هذا الفصل على صعيدين الأول أحكام المسؤولية العقدية ،والثاني أحكام الفعل الضار (المسؤولية التقصيرية).

المبحث الأول

تأصيل المسؤولية المدنية نتيجة الإضرار بالبيانات السيبرانية تبعاً للمسؤولية العقدية

حتى تتحقق المسؤولية العقدية لا بد ابتداءً من أن ينعقد العقد صحيحاً، مستوفياً أركانه وشروطه، منتجاً لآثاره، فلا تقوم المسؤولية من عقد باطل، افتقد أحد أركانه " الرضا والسبب والمحل " فالعقد الباطل من العدم، والعدم لا ينتج آثار وبالتالي لا تقوم المسؤولية.

إن العقود المبرمة بوسائل إلكترونية، ولو كانت ذات طبيعة مختلفة عن العقود العادية، إلا أنها ترتب آثارها حال انعقادها صحيحة، بعد توفر أركان العقد وشروطه، والإخلال من أطراف العقد يترتب عليه المسؤولية التعاقدية، وهذا ما سوف يتم بيانه من خلال ما يلي.

المطلب الأول

ماهية المسؤولية العقدية الإلكترونية وفقاً للقواعد العامة

يعرف شرّاح القانون المسؤولية العقدية بأنها هي الجزاء الذي يترتب على الإخلال بالتزامات التعاقدية، فالعقد شريعة المتعاقدين، فإن من الواجب احترام مضمون هذا العقد، وعدم الإخلال به، ويتحمل المسؤولية الطرف الذي أقدم على الإخلال بشروط العقد، وبالتالي يتحمل التعويض عن عدم الوفاء بالتزاماته، أو التأخير بالوفاء [1].

تقع العقود المبرمة بين مقدمي خدمات الأمن السيبراني عبر الإنترنت ومستخدمين الإنترنت، على أشكال عدة ومتنوعة حسب طبيعة الالتزام لمقدمي الخدمات في العقود، لكن المتفق عليه أنها عقود

---

[1] الحسبان نهاد عبد الكريم، (2019م)، الخبرة الفنية وإجراءاتها وأسس تقديرها، بحث علمي، المعهد القضائي الأردني، عمان، ص3.

تعقد عن بعد، بوسائل إلكترونية، وتندرج تحت اسم عقود الخدمات الإلكترونية، وتعنى في المجمل تقديم الإمكانيات للمشتركين، للاستفادة من الخدمات عبر شبكات الأمن السيبراني، ولعل أهمها، عقود الإيواء، وعقود الدخول إلى شبكة الإنترنت، وعقود توريد المعلومات، وعقود تقديم المساعدة الفنية ونحوه من العقود.

إن العقود الناشئة بين مقدمي الخدمات والمستفيدين من هذه الخدمات، على اختلاف أهدافها، هي في الأغلب عقود ملزمة للجانبين، بحيث ترتب على عاتق كلا طرفي العقد التزامات، فيقع على مقدم الخدمة عبر شبكات الأمن السيبراني كالتزام عام، تخزين المادة المعلوماتية، وإيصالها إلى مستخدمي شبكة الإنترنت عن طريق تزويدهم بالوسائل الفنية اللازمة لتسهيل ذلك، وبالمقابل يقع على عاتق المستخدم مجموعة التزامات، أهمها تسديد ما يترتب في ذمته من مستحقات مالية جراء تلك الخدمة المقدمة، ويقع عليه احترام القواعد العامة من قوانين وأنظمة سارية وفق العادة والعرف وقواعد السلوك الثابتة في هذا المجال [1] .

بموجب هذه العقود فإن المسؤولية العقدية تنشأ في حال إخلال أي من طرفي العقد بالتزاماته، حيث يحق لكل مشترك الحصول على خدمات الإنترنت المتعاقد عليها، وفي حال استحال ذلك، بسبب صعوبة اتصاله بالشبكة، أو عدم قدرته على الوصول للمحتوى المعلوماتي الذي يرغب فيه تحت أي سبب، فإنه تقوم مباشرة المسؤولية العقدية [2].

اعترف المشرع الفرنسي بالمسؤولية العقدية لمقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية قانوناً من خلال تنظيمه لأحكام المسؤولية في التجارة الإلكترونية، حيث أصدر القانون

---

[1] أنظر فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت، مرجع سابق، ص355.

[2] أنظر محمد حسين منصور، (2003م) المسؤولية الإلكترونية، المرجع السابق، ص 186. حول القواعد العامة لهذه المسؤولية، راجع نصوص المواد: 360 و363 من القانون المدني الأردني، و1147 من القانون المدني الفرنسي.

الفرنسي حول الثقة في الاقتصاد الرقمي لعام 2000؛ حيث نصت المادة 14 منه "كل نشاط اقتصادي، مُوجه من قبل شخص معنوي أو طبيعي، يتولى عملية اقتراح، وتقديم بضائع أو خدمات، باستخدام وسائل الاتصال عن بعد، أو الوسائل الإلكترونية" [1].

نهج المشرع الأردني النهج الغربي واعترف بالمسؤولية العقدية الإلكترونية على الرغم أنه لم يستخدم مصطلح التجارة الإلكترونية، ووسع من مفهومها باستخدامه مصطلح المعاملات الإلكترونية، في قانون المعاملات الإلكترونية لعام 2015 وتعديلاته؛ حيث جعلها تتحمل جميع المعاملات التي تعقد بوسائل إلكترونية، وعرَّف المشرع الأردني المعاملات في ذات القانون بأنها "إجراء أو مجموعة الإجراءات، تتم بين طرفين أو أكثر لإنشاء التزامات على طرف واحد أو التزامات تبادلية بين أكثر من طرف، ويتعلق بعمل تجاري، أو التزام مدني، أو بعلاقة مع أي دائرة حكومية" [2] .

إن كلا المشرعين الأردني والفرنسي، قد وسعا من مفهوم العقود المبرمة عن بعد عبر وسائل إلكترونية في مفهوم التجارة الإلكترونية، وذلك لكي تشمل الغالبية العظمى من العقود الإلكترونية، ومنها عقود توريد المعلومات، وعقود الدخول إلى الشبكة، وعقود الإيواء وعقود توريد البحث الآلي، واستناداً عليه فإن مقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية، مسؤولين بقوة القانون اتجاه المشترك معهم بتنفيذ كامل التزاماتهم بموجب العقود المبرمة إلكترونيا، وأنه لا يمكن أن يعفَو من أحكام المسؤولية العقدية إلا إذا أثبتوا أن سبب عدم التنفيذ لا يرجع إليهم، وإنما يرجع إلى قوة

---

[1] أنظر 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

[2] أنظر المادة 2، قانون المعاملات الإلكترونية الأردني.

قاهرة، أو فعل الآخرين أو فعل المشترك نفسه [1]، وعليه فإن هذه الحماية للمستهلكين ليست فقط للمشتركين ولكن تمتد لكل من يستفيد من هذه الخدمات بغض النظر عن صفاتهم [2].

يثار التساؤل بين القانونيين والقضاة أصحاب الاختصاص، بما أن عقود الخدمات الإلكترونية وليدة الإرادة فهل يجوز الاتفاق على إعفاء مقدمي الخدمات من المسؤولية العقدية بموجب العقد المبرم، وتطبيقاً للقواعد العامة المتعلقة بالعقود بشكل عام.

حقيقةً إن الاتجاه العام في فرنسا ذهب مع جواز ذلك، مع مراعاة سبب الإخلال الذي ينتج عنه المسؤولية العقدية، وعليه يتصور صحة الاتفاق على استبعاد أو تحديد مسؤولية مقدمي الخدمات في عقود الخدمات إذا أهمل أو قصر في تنفيذ التزاماته، بشرط عدم العمدية، أو أن يرتكب ذلك نتيجة خطأ جسيم، مما يترتب عليه وحسب القواعد العامة أن عبئ الإثبات يقع على المشترك أو المتضرر لإثبات الغش، حتى يرفع عن مقدمي الخدمة عبر شبكات الأمن السيبراني شرط الإعفاء من المسؤولية، وبهذا فإن البطلان في العقود لا يلحق من الأساس إلا الشروط التعسفية[3].

---

[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.

[3] أنظر Guide Permanent Droit et Internet, E 1.2., Fourniture d'accès, précité, n° 36, p. 15، أنظر: فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت، مرجع سابق، ص357.

اتبع المشرع الأردني نفس الهدي الذي سار عليه المشرع الفرنسي؛ حيث نجد من خلال استقراء نصوص القانون المدني أن المشرع ولو بصورة ضمنية أجاز الإعفاء من المسؤولية العقدية أو تحديدها؛ حيث نص القانون المدني الأردني "إذا كان المطلوب من المدين هو المحافظة على الشيء، أو القيام بإدارته، أو توخي الحيطة في تنفيذ التزاماته، فإنه يكون قد وفى بالالتزام إذا ما بذل في تنفيذه من العناية كل ما يبذل الشخص العادي ولم يحقق الغرض المقصود، هذا ما لم ينص القانون أو الاتفاق على غير ذلك [1]"، وكذلك جاء في الفقرة الثانية من نفس المادة " وفي كل حال يبقى المدين مسؤول عما يأتيه من غش أو خطأ جسيم [2] ".

بإسقاط القواعد العامة للمسؤولية العقدية، على المسؤولية العقدية الإلكترونية لمقدمي الخدمات عبر شبكات الإنترنت للبيانات السيبرانية، فإنه بالنتيجة يمكن الإعفاء من المسؤولية العقدية إذا لم يرجع السبب الإخلال بالالتزام إلى خطأ جسيم أو غش من جانب مقدم الخدمات [3]، وعليه فإن مثل هذا الشرط ينعقد صحيحاً إلا أنه لا يعتد به طبقاً للقواعد العامة وإعمالاً لنسبية آثار العقد، إلا في مواجهة المتعاقد معه، ولا يمتد إلى الغير الذي يضار من المخالفة المرتكبة من قبل مقدمي الخدمات لأنه لا تربطه به علاقة عقدية بالأصل [4].

---

[1] أنظر المادة 1/358، القانون المدني الأردني.

[2] أنظر الفقرة الثانية، المادة 385، القانون المدني الأردني.

[3] أنظر في مفهوم الخطأ الجسيم، نوري حمد خاطر، (2003م)، "الخطأ ألجسيم في ظل تطبيقاته التشريعية والقضائية: دراسة مقارنة"، المنارة للبحوث والدراسات، المجلد التاسع، العدد الثالث، جامعة آل البيت، ص43 وبعدها.

[4] أنظر فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت، مرجع سابق، ص358.

المطلب الثاني

أركان المسؤولية العقدية الإلكترونية

بعد بيان القواعد العامة في المسؤولية العقدية، المترتبة بحق مقدمي الخدمات عبر شبكات الأمن السيبراني فإنه لا تكتمل هذه القواعد إلا بعد بيان أركان المسؤولية العقدية الناتجة عن عقود الخدمات الإلكترونية، إن أركان المسؤولية التعاقدية في العقود الإلكترونية هي نفسها الأركان المقررة في المسؤولية العقدية العادية حسب القواعد العامة وهي ثلاثة أركان أساسية، الخطأ، والضرر والعلاقة السببية بين الخطأ والضرر وهذا ما سوف يتم بيانه على النحو التالي.

الفرع الأول: الخطأ

جاء تعريف الخطأ في اللغة" الخطأ والخطّاء ضد الصواب، وخطّأه تخطِئة وتخطيئا: نسبة إلى الخطأ وقال له أخطأت، والخطأ ما لم يتعمد، والخِطء ما تعمّد، وقال الأموي المخطئ من أراد الصواب فصار إلى غيره، والخاطئ من تعمّد لما لا ينبغي" [1].

وعرفه شرّاح القانون بأنه "هو عدم قيام المدين بتنفيذ التزاماته المترتبة في المسؤولية العقدية نتيجة عن عمد أو إهمال" [2].

الخطأ هو أحد الأركان التي ترتكز عليها المسؤولية العقدية، وفي عقود الخدمات الإلكترونية نجد أن محور الالتزام الأساسي في هذه العقود تحقيق النتيجة التي اتجهت إليها إرادة المتعاقدين، وبذل العناية المعتادة من أجل جعل تحقيق النتيجة مؤكدة، وعليه يعتبر المدين مرتكباً خطأً عقدياً في حال لم ينفذ التزاماته كلياً أو جزئياً أو تأخر في تنفيذه أو نفذه بشكل معيب وهذا ينطبق على كلا

---

[1] ابن منظور، (توفي سنة 711هـ)، تهذيب الخواص من درة الغواص، تحقيق رضوان أحمد طه، دار النشر للجامعات، القاهره، 2011م، ص65.

[2] عبد الرحمن حمدي، (2010م)، الوسيط في النظرية العامة في الالتزامات، الكتاب الأول، المصادر الإرادية للالتزام العقد والإرادة المنفردة، ط2، دار النهضة العربية، القاهرة، ص102.

المتعاقدين حيث كل منهما دائن ومدين في نفس الوقت، وإن هذا التقصير في تنفيذ الالتزامات يعتبر خطأ في سلوك المدين يوجب المسائلة، ومعيار هذا الخطأ هو معيار الرجل المعتاد، وعلى هذا المعيار سار المشرع الأردني في القواعد العامة للمسؤولية العقدية، وحيث جاء في نص المادة 1/358 من القانون المدني الأردني "إذا كان المطلوب من المدين هو المحافظة على الشيء، أو القيام بإدارته، أو توخي الحيطة في تنفيذ التزاماته، فإنه يكون قد وفى بالالتزام إذا ما بذل في تنفيذه من العناية كل ما يبذل الشخص العادي ولم يحقق الغرض المقصود، هذا ما لم ينص القانون أو الاتفاق على غير ذلك"، واستناداً لهذا النص فإن المسؤولية العقدية تثار إذا لم يقم المدين بتنفيذ التزاماته أو أهمل فيها أو نفذها بشكل معيب عن عمداً أو إهمال وتقصير وجب عليه تعويض الدائن عما لحقه من ضرر جراء ذلك [1].

إن عدم التنفيذ الكلي أو التنفيذ المتأخر للعقد الإلكتروني لا يثير أي إشكالية، وذلك لوضوح الإخلال الواقع بالتزامات المدين وتحقق المسؤولية العقدية ما لم يتمسك المدين بوجود سبب أجنبي أو أن الخطأ نتج عن خطأ الدائن، لكن الإشكالية التي تظهر عند تنفيذ الالتزام بشكل معيب وهذا يرجع إلى طبيعة العقود الإلكترونية التي تبرم عن بعد وتنفيذها يكون عن بعد، ويغلب على تنفيذها مبدأ حسن النية، خاصة في مواجهة المستهلك غير المحترف، ويختلف تحديد المسؤولية تبعاً لاختلاف طبيعة الالتزام فيما إذا كان بذل عناية أم تحقيق نتيجة [2].

لتحديد طبيعة الالتزام من حيث النتيجة، هل هو بذل عناية أم تحقيق نتيجة فإنه لا بد من الرجوع إلى النية التي اتجهت إليها إرادة كل من المتعاقدين أثناء انعقاد العقد، وذلك بالنظر إلى الغاية

---

[1] علي صالح براء، (2020م)، المسؤولية العقدية لمزودي خدمات عبر الإنترنت (دراسة مقارنة)، رسالة ماجستير، جامعة الشرق الأوسط، كلية الحقوق، ص54.

[2] سعد نبيل ابراهيم، (2007م)، النظرية العامة في الالتزام مصادر الالتزام، القاهرة، دار الجامعة الجديدة للنشر، ص107.

المرجوة من العقد (محل الالتزام)، هل هي نتيجة مؤكدة أم نتيجة احتمالية وعليه إذا كانت تحتاج إلى بذل عناية الرجل المعتاد لتؤدي إلى تحقيق محل الالتزام بشكل مؤكد نكون أمام التزام بتحقيق نتيجة، أما إذا كان المطلوب لتحقيق النتيجة عناية اليقظة وهي لا تكفل بالضرورة الوصول إلى النتيجة المرجوة وغالباً ما تعتمد على عوامل مستقلة عن المدين فنكون أمام بذل عناية، ومثاله العقود الإلكترونية التي ترد على تقديم خدمات فنية أو ذهنية فالالتزام فيها هو بذل عناية [1] .

إن الإخلال بالالتزام التعاقدي يتصور أن يقع من أشخاص آخرين غير المدين، في العقود الإلكترونية؛ حيث قد يعين المتعاقد شخص آخر لمساعدته في الالتزامات التعاقدية، وتثور المسؤولية العقدية عن فعل الغير في المعاملات الإلكترونية؛ حيث تتولى الشركات المتعاقدة لتنفيذ التزاماتها من خلال العاملين لديها وممثليها ومندوبيها والمقاولين من الباطن، وهنا تقع المسؤولية التعاقدية بحق هذه الشركات [2].

لا بد من الإشارة إلى أن الخطأ المنتج للمسؤولية العقدية لا يقتصر فقط على عدم تنفيذ ما ورد في العقد بين المتعاقدين، فهو أيضاً يشمل ما سكت عنه المتعاقدين، وبما يكمله القانون بما نص عليه من القواعد المكملة لإرادة المتعاقدين لتنفيذ الالتزام بما يتوافق مع العرف والعدالة وحسب طبيعة الالتزام، ليصبح جزءاً من العقد حاله حال الالتزامات المتفق عليها وهذا ما أكده المشرع الأردني في القانون المدني؛ حيث جاء فيه "لا يقتصر العقد على التزام إلزام المتعاقد بما ورد فيه فحسب، بل يتناول أيضاً ما هو من مستلزماته وفقاً للقانون والعرف والعدالة بحسب طبيعة الالتزام.

---

[1] عبد الرحمن حمدي، (2010م)، الوسيط في النظرية العامة للالتزام، مرجع سابق، ص102.

[2] المرجع نفسه، ص 102، والمشار الية في علي صالح براء، (2020م)، المسؤولية العقدية لمزودي خدمات عبر الإنترنت مرجع سابق، ص55وص56.

الفرع الثاني: الضرر

بعد بيان الركن الأول من أركان المسؤولية العقدية الإلكترونية وقياسه على القواعد العامة للمسؤولية العقدية، فإن ركن الخطأ لا يكفي وحده لقيام المسؤولية العقدية، سواء في العقود الاعتيادية أو في العقود الإلكترونية، فلا بد من أن ينتج الخطأ ضرراً يلحق بالمدين، والضرر يعد من النتائج الخطيرة لقيام المدين بفعل خاطئ مباشرةً، وعليه فالضرر هو مقدار الأذى الذي يصيب الشخص بحق من حقوقه أو بمصلحة مشروعة له سواء ذلك الحق أو مصلحة متعلقة بسلامة ماله أو جسمه أو حريته أو شرفه أو اعتباره [1].

وعليه فإن الضرر يقع على ثلاثة أنواع ضرر مادي يصيب الدائن في ذمته المالية، وضرر جسدي وهو الذي يصيب الإنسان في جسمه وضرر أدبي يصيب الدائن في شرفه أو سمعته أو كرامته[2].

يرى الباحث أن الضرر الإلكتروني هو كل ضرر يلحق بالمكونات المادية للحاسب أو أي من برامجه والبيانات الإلكترونية أو أي موقع إلكتروني على شبكة الإنترنت، فمن الممكن أن يكون الضرر مادياً وجسدياً يقع على أجهزة الحاسوب المادية والبرامج المتصلة فيها أو ببيانات الأمن السيبراني، مما يسبب عبء بالذمة المالية للدائن، ويتصور الضرر الأدبي من خلال نشر المحتوى المعلوماتي غير المشروع أو المخالف للقانون والأنظمة والذي يمس بسمعة وشرف ومكانة المتضرر.

أشار المشرع الأردني للضرر من خلال بيان التعويض عن الضرر عموماً، ومنها الضرر الناشئ عن الإخلال بالالتزام التعاقدي من خلال نصوص متفرقة في القانون المدني الأردني؛ حيث نصت

---

[1] أحمد هيثم السيد، (2013 م)، المسؤولية المدنية في إطار المعاملات عبر شبكة الإنترنت، طروح الدكتوراة، كلية الحقوق، جامعة المنوفية، ص305.

[2] سرحان عدنان، ونوري خاطر، (2021م)، شرح القانون المدني، مصادر الحقوق الشخصية الالتزامات، دراسة مقارنة، دار الثقافة للنشر والتوزيع، بدون رقم طبعة، عمان، ص309 وص310.

المادة 360 "إذا تم التنفيذ العيني أو أصر المدين على رفض التنفيذ حددت المحكمة مقدار الضمان الذي تلزمه المدين مراعية في ذلك الضرر الذي أصاب الدائن والعنت الذي بدا من المدين"، وكذلك نصت المادة 363 من ذات القانون "إذا لم يكن الضمان مقدرا في القانون أو في العقد فالمحكمة تقدره بما يساوي الضرر الواقع فعلاً حين وقوعه"، ويرى شرّاح القانون أن المشرع الأردني لم يتطرق لتعريف واضح للضرر، ولكنه قصد به الضرر الناشئ عن التزام عقد يصيب الدائن نتيجة إخلال المدين بالتزاماته العقدية، وهو يمثل الضرر المباشر المتوقع الذي يلحق بالدائن [1].

ليتحقق الضرر الناشئ عن إخلال التزام تعاقدي يجب توافر ثلاثة شروط وهي:

1. أن يكون الضرر حالاً أو محقَّق الوقوع.

فالضرر المادي يجب أن يكون حالاً، أي وقع فعلاً أو محقّق الوقوع في المستقبل القريب، أما الضرر الاحتمالي لا يلزم التعويض إلا إذا تحقق فعلاً [2].

2. أن يكون الضرر مباشراً.

ويقصد به أن الضرر واجب التعويض مباشرة، والمباشرة تعني أن الضرر هو النتيجة إخلال المدين بالتزاماته التعاقدية، وهنا تشترك المباشرة في كل من المسؤولية العقدية والمسؤولية التقصيرية [3].

3. أن يكون الضرر متوقعاً.

ويقصد به أن يكون الضرر متوقع الحصول أثناء التعاقد وإبرام العقد، وإذا كان غير متوقع لا يسأل عنه المدين، إلا إذا ارتكب غشَ أو خطأً جسيماً، ويعتمد على مدى التوقع معيار الشخص العادي، ويرجع قصر التعويض في المسؤولية العقدية على الضرر المتوقع ذلك إعمالاً لقاعدة العقد شريعة

---

[1] سرحان عدنان، ونوري خاطر، (2021م)، شرح القانون المدني، مصادر الحقوق الشخصية الالتزامات، دراسة مقارنة، دار الثقافة للنشر والتوزيع، بدون رقم طبعة، عمان، ص309.

[2] انظر لطفا قرار تمييز حقوق 95/82 الصادر بتاريخ 1982، مجلة المحامين، 1982 عدد 1-،4 ص242 والمشار إليه في، سرحان عدنان، وخاطر نوري، (2021م) شرح القانون المدني مصادر الحقوق الشخصية، مرجع سابق، ص311.

[3] أنظر المادة 220، القانون المدني المصري، والمادة 207، القانون المني العراقي.

المتعاقدين، وإن الإرادة هي مَن تحدد التزامات كلا طرفي العقد لذلك فهي تحدد الالتزامات والتعويض عن الضرر المتوقع، ولا يمكن إلزام أي من الأطراف بأكثر مما توقع عند التعاقد [1] .

لا بد من الإشارة إلى أن عبء إثبات الضرر يقع على عاتق الدائن المتضرر، لأنه من المتصور أن يخل المدين بالتزاماته دون إلحاق أي ضرر بالدائن فلا تقوم المسؤولية العقدية.

الفرع الثالث: العلاقة السببية

بعد بيان ركني المسؤولية العقدية وقياسهما على المسؤولية العقدية الإلكترونية، فإنه لا يتصور هذان الركنان، (الخطأ والضرر) إلا بوجود رابطة فيما بينهما، فلولا وجود الخطأ لما وجد الضرر ولا تتحقق المسؤولية العقدية إلا إذا كان الضرر ناشئ عن الخطأ الصادر من المدين وهو ما يسمى بالعلاقة السببية [2].

وعليه فإن عدم تنفيذ الالتزام العقدي (الخطأ) لا يكفي لقيام المسؤولية العقدية، وكذلك لا يكفي الضرر وحده لقيام المسؤولية بل يجب أن يكون الضرر مباشراً ناجماً عن خطأ المدين بإخلاله بتنفيذ التزامه العقدي، وأن يثبت الدائن أن الخطأ هو السبب في الضرر [3].

سار المشرع الأردني على هذا الهدي؛ حيث جاء في المادة 261 من القانون المدني الأردني على أنه تنتفي المسؤولية العقدية إذا تبين أن الضرر ناشئ عن سبب أجنبي وليس للمدين دخل فيه وهنا تقطع العلاقة السببية بين الخطأ والضرر، وبالتالي تنتفي معها المسؤولية العقدية، وجاءت

---

[1] انظر سرحان عدنان، خاطر نوري، (2021م)، شرح القانون المدني مصادر الحقوق الشخصية، مرجع سابق، ص312.

[2] أنظر نصار أيناس مكي عبد، (2013 م)، التفاوض الإلكتروني "دراسة مقارنة في ضل التشريعات العربية المعاصرة "، بحث علمي، منشور في مجلة بابل للعلوم الإنسانية، جامعة بابل، مجلد 21، عدد3، ص959.

[3] انظر سرحان عدنان، وخاطر نوري، (2021م) شرح القانون المدني مصادر الحقوق الشخصية، مرجع سابق، ص313.

المادة وبينت كذلك ما المقصود بالسبب الأجنبي وردته إلى ثلاثة صور وهي القوة القاهرة وفعل الغير وفعل المضرور [1].

تنتفي المسؤولية العقدية الإلكترونية نتيجة انتفاء العلاقة السببية بين الخطأ والضرر، ومرد ذلك إلى القواعد العامة، وعليه فإن إخلال المدين بالتزاماته (الخطأ) وحدوث الضرر وانتفاء العلاقة السببية بسبب تدخل عامل أجنبي تنتفي معه المسؤولية ولكن يجب توفر عدة شروط مجتمعة لتأكيد هذا النفي وهي:

1. أن يكون عدم تنفيذ الالتزام من المدين لسبب خارجي وغير منسوب له مثل الظواهر الطبيعية.
2. يجب أن يكون السبب الأجنبي غير متوقع؛ أي يجب أن يكون كلا المتعاقدين لا يتوقعان السبب الأجنبي أثناء التعاقد، وإذا حدث هذا التوقع وجب أخذه بعين الاعتبار، وعليه يُسأل المدين عن الضرر، لأن شرط المفاجأة قد سقط بالتوقع المسبق، ومثاله أن يكون هناك حرب قريبة النشوب أو أزمة اقتصادية متوقعة الحدوث.
3. أن لا يكون بمقدور دفع السبب الأجنبي ببذل جهد الرجل المعتاد إذا وجد بنفس ظرف المدين.
4. أن يمنع السبب الأجنبي المدين من تنفيذ التزاماته فعلاً ويرتبط هذا بالشرط السابق، ويفترض حسن نية المدين [2].

في نهاية مطلب المسؤولية العقدية لا بد من الإشارة إلى أنه ليس من القانون المدني الأردني

---

[1] انظر المادة 261، قانون المدني الأردني، أنظر منصور محمد حسين، (2003م)، المسؤولية الالكترونية، مرجع سابق، ص 293- ص296.

[2] انظر السرحان عدنان، خاطر نوري، (2021م)، شرح القانون المدني مصادر الحقوق الشخصية، مرجع سابق، ص313 و314.

وحده الذي يبين أن الإخلال بالتزام المتعاقدين يرتب المسؤولية العقدية؛ حيث أشار قانون حماية المستهلك الأردني لسنة 2017م في المادة 6/ب "يعتبر إخلال من الالتزامات التعاقدية أي من الحالات التالية:

1. عدم تسليم السلعة أو تقديم الخدمة إلى المستهلك خلال المدة المتعاقد عليها.
2. عدم صحة المعلومات التي تم تزويد المستهلك بها عن السلعة أو الخدمة أو إخفاء المزود المستهلك أي معلومة جوهرية" [1].

إن المسؤولية العقدية الأصل فيها عدم التضامن بين المشتركين في الضرر، ولكن للقاضي أن يقرر التضامن إن وجد مبرر محدد له، وهذا متصور بين مقدمي خدمات الأمن السيبراني، وذلك في حال عدم معرفة في أن الشخص محدث الضرر، وحصل الضرر من خلال المواقع التي يديرونها [2].

نص القانون المدني الأردني إلى أن إذا تعدد المسؤولون عن الضرر، كان كل منهم مسؤولاً بنسبة نصيبه فيه وللمحكمة أن تقضي بالتساوي أو بالتضامن أو بالتكافل فيما بينهم [3].

المطلب الثالث

التعويض عن الإضرار بالبيانات السيبرانية وفقاً للمسؤولية العقدية

الجزاء المترتب للمسؤولية العقدية الناتج عن إخلال التزام تعاقدي نشأ عنه ضرر هو التعويض، بعد اكتمال أركان المسؤولية العقدية وتبين للقضاء أن المتضرر لحقه ضرر جراء الخطأ فتحكم المحكمة بالتعويض الذي يتناسب مع الضرر، وهو عادة يقع على صورتين الأولى التعويض العيني أو التعويض بمقابل، وإن التعويض كما ينطبق كجزاء للمسؤولية العقدية في القواعد العامة

---

[1] أنظر المادة 6اب، قانون حماية المستهلك الأردني رقم 7 لسنة 2017م.

[2] أنظر علي صالح براء، (2020م)، المسؤولية العقدية لمزودي خدمات عبر الإنترنت، مرجع سابق، ص60.

[3] انظر المادة 265، القانون المدني الأردني.

فإنه ينطبق أيضاً بنفس الصور على المسؤولية العقدية للإضرار ببيانات الأمن السيبراني وهو ما سيتم بيانه بهذا المطلب.

الفرع الأول: التعويض العيني.

التعويض العيني، يعني إعادة الحالة إلى ما كانت عليه، قبل الخطأ قدر الإمكان، وما كان ذلك ممكناً، وأن الهدف من التعويض هو التخفيف من وطأة الضرر الذي لحق بالمضرور[1].

ويعرف كذلك التعويض العيني "الوفاء بالتزام عيناً، ويقع كثيرا في الالتزامات العقدية" [2]، ويعرف أيضا هو "إعادة الحالة إلى ما كانت عليه قبل أن يرتكب المسؤول الخطأ الذي أدى إلى وقوع الضرر [3]".

ولعل التعويض بهذا المعنى هو النتيجة المثالية لجبر الضرر، كونه يزيل الضرر ويعيد الحال إلى ما كان عليه، وهو أفضل من دفع مبلغ من المال مع إبقاء الضرر كما هو [4].

أخذ المشرع الأردني بالتعويض العيني؛ حيث نصت المادة 275 من القانون المدني على التعويض العيني؛ حيث جاء فيها " من أتلف مال غيره، أو أفسده، ضمن مثله إذا كان مثلياً، وقيمته إذا كان قيمياً وذلك مع مراعاة الأحكام العامة للتضمين". كما ونصت المادة 2/269 من ذات القانون على أن " يقرر الضمان بالنقد، على أنه يجوز للمحكمة وتبعاً للظروف وبناءً على طلب المضرور، أن تأمر بإعادة الحالة إلى ما كانت عليه، وأن تحكم بأداء أمر معين متصل بالضرر، وذلك على سبيل التضمين".

---

[1] دندون حسن علي، (1998م)، المبسوط في المسؤولية المدنية، الضرر، الجزء الأول، بدون مكان وسنة نشر، ص278.

[2] السنهوري عبد الرزاق أحمد، (1949م) الوسيط في القانون المدني، الجزء الثاني، ص816.

[3] الجبوري نصير صبار، (2019م)، التعويض العيني، دراسة مقارنة، ط1، دار القنديل للنشر والتوزيع، عمان، ص21.

[4] دندون حسن علي، (1998م)، المبسوط في المسؤولية المدنية، المرجع سابق، ص278.

وعليه فإن المشرع أقر التعويض العيني كجزاء لجبر الضرر ولكنه تركه كسلطة تقديرية للمحكمة بعد التعويض النقدي وهذا ما دفع البعض للقول بأن التعويض العيني نطاقه في المسؤولية العقدية.

الفرع الثاني: التعويض بمقابل.

في حال لم يُستطع جبر الضرر بالتعويض العيني، لاستحالة إعادة الحالة إلى ما كانت عليه فإن يُلجأ للتعويض بمقابل وهو يقع على صورتين الأولى التعويض غير النقدي والثانية التعويض النقدي.

أولاً: التعويض غير النقدي.

ويقصد بالتعويض غير النقدي هو الحكم بأمر معين على سبيل التعويض وذلك لترضية المضرور من خلال إنصافه، ويوصف أحياناً بأنه التعويض المعنوي والأدبي، والتعويض الأدبي هو تعويض دعت إليه الظروف المتصلة بالضرر ونوعه، فهو ليس عيني لأنه لا يمكن إعادة الحالة إلى ما كانت عليه قبل فعل المضرور، أو تعويض نقدي لأنه لا يتضمن إلزام المدين المخل بتنفيذ التزاماته بأداء مبلغ معين للدائن [1].

هذا التعويض يعد الفريق الأوسط بين التعويض العيني والنقدي، وهو الأنسب في بعض الصور في الضرر، كما لو تعلق الأمر بنشر الحكم الصادر بإدانة المسؤول عن الضرر في الصحف، ولذلك يعد هذا التعويض هو الأبرز في مجال المسؤولية لمقدمي الخدمات عبر شبكات الأمن السيبراني، فعندما يتم نشر معلومات مغلوطة، أو تشهير بشركة معينة تطلب هذه الشركة من

[1] انظر دندونحسن علي، (1998م)، المبسوط في المسؤولية المدنية، المرجع السابق، ص283.

المحكمة بأن تعلن للكافة بطريق الصحافة ووسائل الإعلام وعلى نفقة المسؤول قرار إدانة أن تلك المعلومة مغلوطة [1].

ثانياً: التعويض النقدي.

هو إلزام المسؤول عن الضرر بدفع مبلغ نقدي للمضرور، يتناسب مع حجم الضرر الذي لحق به، وقد ذهب غالبية الفقهاء إلى أن هذا التعويض النقدي هو الأصل في التعويض عن الضرر في المسؤولية العقدية، سواء كان الضرر ماديا أو أدبيا، خاصة في الأحوال التي يتعذر فيها إرجاع الوضع إلى ما كان عليه (التعويض العيني) [2].

ويرى الباحث مما تقدم أن المسؤولية العقدية لمقدمي الخدمات عبر شبكات الأمن السيبراني ذات طابع خاص، ويتطلب التعامل معها من حيث الأثر التعامل بصورة تتوافق مع طبيعة الخطأ العقدي في حال وقوعه، فإن التعويض النقدي هو الأنسب للضمان وجبر الضرر، لاستحالة التعويض العيني، ففي حال أخل مقدم خدمات الأمن السيبراني بالتزامه بتقديم سرعة معينة يتمكن من خلالها المستخدم الدخول إلى أحد المواقع التي يقوم بإيوائها ونتج عن ذلك ضرر لحق بالمستخدم فلا يمكن إعادة الوقت للوراء والأنسب هو التعويض عما لحق المستخدم من ضرر.

---

[1] انظر المادة 2/209، من القانون المدني العراقي، حيث اعتمد على هذه الطريقة في التعويض، حيث نصت المادة "... للمحكمة تبعاً للظروف وبناءً على طلب المضرور...أن تحكم بأداء أمر معين أو على سبيل التعويض"، وكذلك تقابلها المادة 2/171 من القانون المدني المصري.

[2] انظر حول آراء الفقهاء، ابو الليل ابراهيم الدسوقي، (1995م)، تعويض الضرر في المسؤولية المدنية، مطبوعات جامعة الكويت، ص14.

المبحث الثاني

تأصيل المسؤولية المدنية نتيجة الإضرار بالبيانات السيبرانية تبعاً للمسؤولية التقصيرية

القاعدة العامة الثانية من المسؤولية المدنية، والتي تستند عليها في صدور المسؤولية المدنية هو الفعل الضار أو ما يعرف قانوناً بالمسؤولية التقصيرية، وهي بشكل عام تعني محاسبة الشخص عن فعله، الذي سبب به ضرر للغير، نتيجة مخالفة قاعدة قانونية، أو قاعدة خلقية، وإن المسؤولية التقصيرية تقوم حالها حال المسؤولية العقدية، ومن المتصور أن يكون الفعل الضار إلكترونياً، وهو يعني أن تقوم المسؤولية التقصيرية الإلكترونية، اتجاه مقدمي الخدمات عبر شبكات الأمن السيبراني إذا كان الفعل الضار ناتج عنهم، أو عن الغير، وهذا ما سوف يتم بيانه من خلال إسقاط القواعد العامة في التشريع المقارن والتشريع الأردني على المسؤولية التقصيرية للإضرار بالبيانات السيبرانية.

المطلب الأول

ماهية المسؤولية التقصيرية الإلكترونية وفقاً للقواعد العامة

تتصور المسؤولية التقصيرية لدى مقدمي خدمات البيانات السيبرانية عبر شبكات الإنترنت، كما هي للأشخاص العاديين؛ حيث دأب الاتجاه العام لدى المشرع الفرنسي والأوروبي، من خلال نصوص القانون الفرنسي حول الثقة في الاقتصاد الرقمي، والتوجه الأوروبي حول التجارة الإلكترونية، إلى إعفاء مقدمي الخدمات الإلكترونية عبر شبكات الأمن السيبراني من المسؤولية التقصيرية، إلا إذا ثبت علمهم الفعلي بالمضمون الإلكتروني غير المشروع، ولم ينفذوا التزاماتهم

المتمثلة بشطب هذا المحتوى غير المشروع أو منع وصول جمهور المستخدمين إليه، ويكون ذلك بعد الطلب من السلطات المختصة القضائية وعدم تنفيذهم ذلك [1].

نهج المشرع الأمريكي ذات النهج الأوروبي من خلال القانون الصادر بتاريخ 1998 تحت اسم " Digital Milleniam Copyright Act (DMCA)"؛ حيث اشترط لعدم مسؤولية مقدمي الخدمات عبر شبكات الأمن السيبراني عن المحتوى غير المشروع، عدم علمهم بسبب عدم المشروعية، وعدم تلقيهم أي مكاسب مادية من وراء هذه المخالفة، كما ويشترط لانتفاء المسؤولية التقصيرية سحبهم المضمون غير المشروع حال إخطارهم من المتضرر بذلك، وعليه فإن مقدم الخدمات وفق هذا التشريع لا يُسأل عن أفعال الآخرين، ويتحمل فقط نتيجة خطأه الشخصي [2].

استناداً لما تقدم فإن هذا يتفق مع القواعد العامة للمسؤولية التقصيرية؛ حيث نص القانون المدني الفرنسي في المادتين 1240 و1241 على إلزام صاحب الفعل الضار، الذي نتج الضرر عن خطائه أو إهماله أو تقصيره إلى إلحاق الإضرار بالآخرين بضمان الضرر؛ حيث يقع على عاتق المتضرر من جراء نشر مضمون إلكتروني غير مشروع على شبكات الأمن السيبراني، الاعتماد على الخطأ الثابت لمقدم الخدمات، ليتمكن من المطالبة بالتعويض عما لحق به من ضرر [3].

جاء المشرع الأردني، وبيّن من خلال نصوص قانون المدني الأردني، أن الشخص يكون ضامناً للضرر الذي يسببه للغير نتيجة اتصاف فعله بعدم المشروعية؛ حيث نصت المادة 256 من

---

[1] انظر المادة 6، قانون الفرنسي حول الثقة في الاقتصاد الرقمي، انظر المادة 12-14 من التوجه الأوروبي حول التجارة الإلكترونية.

[2] انظر القانون الأمريكي الصادر بتاريخ 28/تشرين الأول/ 1998م، Digital Milleniam Copyright Act.

[3] أنظر محمد حسين منصور، (2003م) المسؤولية الإلكترونية، المرجع السابق، ص 203 و

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

القانون "كل إضرار بالغير يلزم فاعله، ولو غير مميز بضمان الضرر". وهنا نجد أن المشرع أشار إلى الإضرار وليس الخطأ، وهو مناط المسؤولية التقصيرية في القانون المدني الأردني، وبالرجوع إلى المذكرات الإيضاحية لقانون المدني الأردني نجد أنه يقصد بالإضرار "مجاوزة الحد الواجب الوقوف عنده أو التقصير عند الحد الواجب الوصول إليه في الفعلأو الامتناع مما يرتب عليه الضرر [1] "، وعليه فالإضرار بهذا المعنى يختلف عن الضرر ويعني إحداث الضرر بفعل غير مشروع ومخالف للقانون [2].

وفي ظل غياب النصوص الخاصة في القانون المدني الأردني تبين المسؤولية التقصيرية لمقدمي خدمات البيانات السيبرانية عبر شبكات الإنترنت، وتبين حدودها وشروطها وأساسها، فلا بد من إعمال القواعد العامة للمسؤولية التقصيرية، وعليه فإن مقدم الخدمات الإلكترونية وحسب ما تقدم بيانه يكون مسؤولاً كضامن لما لحق بالغير من ضرر نتيجة نشر المحتوى غير المشروع حتى لو انتفى خطأه.

وبإعمال هذه النصوص فإن مقدم الخدمات عبر شبكات الإنترنت للبيانات السيبرانية لن يكون قادراً على إثبات أنه لن يأتي بفعل غير مشروع عند نشره محتوى إلكتروني مخالف للقانون، ولم يكن عالماً بعدم مشروعية هذا المضمون، لأن مناط هذه المسؤولية حسب القانون المدني الأردني هو الإضرار وليس العلم والإدراك، لذلك تتسم تطبيق قواعد المسؤولية التقصيرية في القانون المدني الأردني بالتشدد في مواجهتهم.

---

[1] المذكرات الإيضاحية للقانون المدني الأردني، (1992م)، إعداد المكتب الفني في نقابة المحامين الأردنيين، الجزء الأول، الطبعة الثالثة، عمان، ص 277.

[2] حول مفهوم الإضرار في القانون المدني الأردني، انظر: عدنان السرحان، ونوري خاطر، (2021م) مصادر الحقوق الشخصية، المرجع السابق، ص 364 وبعدها.

يرى الباحث أن هذا انتقاد يوجه حول إعمال هذه النصوص على المسؤولية التقصيرية لمقدمي الخدمات الإلكترونية كونها لا تتلاءم والطبيعة الخاصة لآلية عمل مقدمي الخدمات عبر شبكات الإنترنت، التي جاءت تشريعات الدول في القانون المقارن بأحكام خاصة تنظمها، إضافة أن مثل هذا التشدد يعيق حركة النشاط الإلكتروني، بالإضافة إلى الكم الهائل من التعويضات التي سوف تثقل كاهل مقدمي خدمات الأمن السيبراني، جراء التعويضات التي سوف يتكبدوها عن تلك الأضرار.

المطلب الثاني

أركان المسؤولية عن الفعل الضار الإلكتروني وفقاً للقواعد العامة

إن قيام المسؤولية التقصيرية في القواعد العامة، يفترض ثلاث أركان أساسية للنهوض بها، في مواجه المتسبب بالضرر أو الإضرار، باختلاف المشرّعون سواء أخذو بنظرية العلم والإدراك، أم بدونهما كما هو معمول به لدى المشرع الأردني؛ حيث يجب أن يتوفر ركن الخطأ " الفعل الضار"، وركن الضرر أو الإضرار، وركن العلاقة السببية بين الخطأ والضرر[1].

تنهض المسؤولية التقصيرية الإلكترونية، بنفس الأركان المفترضة بالقواعد العامة، ولكن إلحاق الضرر بالغير بوسائل إلكترونية، أو إلحاق الضرر ببيانات الأمن السيبراني، يثير بعض الخصوصية، بسبب إضافة بعض الشروط الخاصة لتحقُّق المسؤولية التقصيرية، وهذا حسب ما أقرّته بعض التشريعات في القانون المقارن.

استناداً على الذي تقدم، فإن المسؤولية التقصيرية الإلكترونية تتطلب، أن يكون الفعل الضار إلكترونيا، والضرر الناتج إلكترونياً أيضاً، فالمسؤولية تعني إلزام مرتكب الفعل الضار الإلكتروني،

[1] عدنان السرحان ونوري خاطر، (2021م)، مصادر الحقوق الشخصية، المرجع السابق، ص 355 وما بعد.

بجبر الضرر الإلكتروني اللاحق بالبرامج المستخدمة، أو البيانات، أو المعطيات الإلكترونية المخزنة على شبكات الأمن السيبراني، أو ذاكرة الحاسب الآلي المستخدم [1].

سوف يتم بيان الأركان الخاصة بالمسؤولية العقدية، والشروط الخاصة الملحقة بها وفقاً للتشريع المقارن والتشريع الأردني على النحو الاتي.

الفرع الأول: الإضرار

الإضرار في المسؤولية التقصيرية، هو خرق للقواعد القانونية، أو ارتكاب فعل ضار دون وجه حق، فمحوره هو عدم مشروعية الفعل الذي قام به الخاطئ، يجب إثبات هذا الإضرار وفق معيار شخص المعتاد الحذر، لو كان في نفس الظروف [2].

وبإسقاط القواعد العامة للمسؤولية التقصيرية، نجد أن الإضرار الذي يلحق الضرر بالبيانات السيبرانية، التي توجب المسؤولية التقصيرية، تكون نتيجة إحدى خطأين، الأول الإضرار الناتج عن فعل ضار صدر من قبل مقدمي الخدمات الإلكترونية، والثاني الإضرار الناتج عن الفعل الضار الموجه إلى البيانات السيبرانية من قبل الغير "مستخدم الإنترنت".

تتنوع صور الإضرار، الصادر من قبل الغير اتجاه البيانات السيبرانية، حيث يأخذ الإضرار، أشكالاً مختلفة، نتيجة التطور والازدهار في مجال تكنولوجيا المعلومات، والازدياد المهول في عدد مستخدمي شبكات الأمن السيبراني من أصحاب القدرات الخاصة في استخدام التقنيات[3]، ولعل أهمها:

---

[1] مساعدة نائل علي، (2005م)، أركان الفعل الضار الإلكتروني في القانون الأردني، بحث علمي منشور في مجلة الدراسات، الجامعة الأردنية، مجلد 32، العدد1، ص56.

[2] سرحان عدنان، (1997م)، الفعل عير المشروع الإضرار كأساس للمسؤولية التقصيرية، الالتزام بالضمان في الفقه الإسلامي والقانون المدني، بحث منشور في مجلة المنارة، مجلد 2، عدد 2، ص 106.

[3] أنظر مساعدة نائل علي، (2005م)، أركان الفعل الضار الإلكتروني في القانون الأردني، مرجع سابق، ص 59

1- القرصنة الإلكترونية

يقصد بها أن يتمكن الفاعل من البرامج والبيانات الإلكترونية للبيانات السيبرانية، والحصول عليها دون إرادة مالكها، باستخدام وسائل وتقنيات إلكترونية، ويعرف الفاعل باسم "الهكر"[1].

2- التجسس على البرامج والبيانات الإلكترونية

يقتصر الفعل الضار، على مجرد اختراق البرامج، والبيانات ذات الطبيعة السيبرانية، بقصد الاطلاع عليها، دون إعادة نسخها، أو إنتاجها، أو تخريبها، ولعل الهدف الحصول على معلومة أو المنافسة غير المشروعة في مجال التجارة [2].

3- الإتلاف الإلكتروني

يقصد بهذا الفعل الضار، استخدام برامج خاصة هدفها، تدمير البرامج والبيانات الإلكترونية كلياً، يجعلها غير صالحة للاستعمال، أو جزئياً من خلال التقليل من أدائها، ويكون ذلك، بإرسال الفايروسات الإلكترونية " برامج ضاره " على اختلاف أنواعها وأشكالها، أو إرسال القنابل المنطقية أو المؤقتة أو الزمنية " هي برامج أو أجزاء من برامج، تنفذ في وقت محدد، أو أوقات زمنية محددة وبشكل منتظم، وهدفه تحديد ظروف او حالة النظام الإلكتروني بغرض تسهيل تنفيذ عمل غير مشروع " [3].

كما تتنوع أشكال، الفعل الضار من قبل الغير، فهي كذلك الحال في الفعل الضار "الخطأ" الصادر عن مقدمي الخدمات الإلكترونية عبر شبكات الإنترنت للبيانات السيبرانية، إلا أنه لا تقوم مسؤوليتهم

---

[1] رستم هشام علي، (1994م)، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ص 73.

[2] أنظر القويماني بدر علي، (2011م)، المسؤولية المدنية عن الفعل الضار الناجم عن التصرفات الواردة عبر النظام الرقمي، رسالة ماجستير، كلية الحقوق، جامعة آل البيت، ص 54.

[3] لمعرفة المزيد عن الفايروسات وأشكالها، والبرامج المعروفة باسم القنابل، أنظر القويماني بدر علي، (2011م)، المسؤولية المدنية عن الفعل الضار، مرجع سابق، ص 55 وما بعد، وكذلك أنظر مساعدة نائل علي، (2005م)، أركان الفعل الضار الإلكتروني في القانون الأردني، مرجع سابق، ص61.

إلا في شروط معينة وخاصة بينتها التشريعات المقارنة، ولعل أشكال الفعل الضار الصادر عن مقدمي الخدمات يختلف باختلاف نشاطهم الإلكتروني ومنها:

1. نشر صور عارية أو فاضحة، بعد إيوائها بدون رضا أصحبها، ومثاله ما حصل في القضية المشهورة لعارضة الأزياء الفرنسية "إيستل هاليداي".
2. من صور الفعل الضار لمقدمي خدمات البيانات السيبرانية عبر الإنترنت، المساس بالحقوق الفكرية وانتهاكها ومثاله قضية الشركة joyeuxnoel بث مقاطع فيلم بدون إذن ما الكيها.
3. كذلك من صور الفعل الضار، بث أفكار متطرفة، او مناهضة للتطرف، أو العنصرية ومثالة الدعوى التي رفعها اتحاد الطلاب اليهود في فرنسا UEJF ضد متعهد الإيواء Multimania نتيجة لإيوائه موقعاً إلكترونياً تتضمن عرض وبيع أغراض ورموز نازية.
4. قد تستخدم الشبكة للمساس بالحياة الخاصة للمشتركين، من خلال الاعتداء على خصوصية حساباتهم بنشر بياناتهم أو حساباتهم، بما تحتويه من بيانات، إضافة الى القدح والذم والتحقير والتشهير ومثاله قرار محكمة بداية باريس بتاريخ 31 / تموز/ 2000م بقرار ألزمت بموجبه مورد المعلومات بالمسؤولية التقصيرية، كونه استخدم اسم شخص ما بطريقة غير مشروعة، حيث وضع الاسم تحت أيقونة، تدخل المستخدم الى موقع إلكتروني إباحي، وهو ما تسبب بضرر لصاحب الاسم [1].

لا تكتفي هذه الصور من الأفعال، لقيام المسؤولية التقصيرية لمقدمي خدمات البيانات السيبرانية، إلا بتوفر شروط خاصه أقرها التوجه الأوروبي حول اتجاه الإلكترونية لعام 2000م وهي:

---

[1] أنظر أبو الهيجاء محمد ابراهيم، والخصاونة علاء الدين عبد الله، (2009م)، المسؤولية التقصيرية لمزودي خدمات الأنترنت عن المحتوى غير المشروع، دراسة التوجه الأوروبي الخاص بالتجارة الإلكترونية لسنة 2000م والقانون الفرنسي، بحث منشور في مجلة الشريعة والقانون، بتاريخ إبريل 2010م، العدد 43، ص 60وص61

- لا تنهض المسؤولية التقصيرية لمقدمي الخدمات عبر شبكات الإنترنت، إذا كان يمارس التزاماته بالمراقبة على المحتوى المعلوماتي.
- حتى يعتبر مقدم الخدمات عبر شبكات الإنترنت للبيانات السيبرانية مخطئ، يجب ألا يتخذ أية وسيلة لمنع المستخدمين من الدخول الى المحتوى المعلوماتي غير المشروع، بعد إخطاره من قبل الجهات المختصة، أو المتضرر[1].

حاول المشرعين والقانونيين وضع الأساس للمسؤولية التقصيرية لمقدمي خدمات البيانات السيبرانية عبر شبكات الإنترنت، بما يتوافق مع التوجه الأوروبي، وذلك من خلال تحديد شروط يمكن من خلالها تحقق المسؤولية التقصيرية، وهي:

1- العلم الفعلي بالطابع غير المشروع للمحتوى [2].

الأصل المفترض في هذا الشرط عدم مسؤولية مقدمي الخدمات عبر شبكات الإنترنت، على اختلاف وظائفهم ومهامهم، سواء ناقل للمعلومة أو موردها أو مأوي الموقع الذي نشرها، عن المحتوى المعلوماتي غير المشروع، أو الضرر الذي لحق بالغير، أو بالبيانات السيبرانية، إلا أذا كان يعلم أن المحتوى غير المشروع، أو كان يعلم الظروف التي تجعل عدم المشروعية واضحاً وظاهراً[3].

---

[1] أنظر التوجه الأوروبي حول التجارة الإلكترونية لسنة 2000م.

[2] فرح أحمد قاسم، (2007م)، النظام القانوني لمقدمي خدمة الإنترنت، مرجع سابق، 365.

[3] P. TRUDEL, La responsabilité civile sur Internet selon la loi concernant le cadre juridique des technologies de l'information, 2001, disponible sur le site,, p 14 http//www.papyrus.bib.umontreal.ca

قرر أغلب الفقه [1]، إن العلم المطلوب لقيام المسؤولية التقصيرية، هو العلم الأكيد وليس العلم المفترض، والعلم الأكيد ينتج عن الإخطار من الجهات المختصة أو الشكوى المقدمة من المتضرر، وبالنتيجة فإن التزام المراقبة للمحتوى المعلوماتي الذي يقع على مقدمي الخدمات، هي المراقبة بالحد الأدنى وليس المراقبة الفعلية [2].

تطبيقاً لهذا ما أقره المشرع الفرنسي، في القانون الفرنسي حول الثقة بالاقتصاد الرقمي وتحديداً في المادة السادسة منه، حيث اعتبرت الإخطار من السلطات المختصة أو الغير الموجه لمقدمي الخدمات عبر شبكات الإنترنت عن المحتوى غير المشروع أو المتسبب بالضرر، هي قرينة على العلم الفعلي[3].

3-عدم قيام مقدمي الخدمات بالتصرف بسرعة لسحب أو حذف المحتوى غير المشروع

تنهض المسؤولية التقصيرية، ويعتبر مقدم الخدمة مخطئاً، ويتحمل المسؤولية إذا لم يقم بشطب المحتوى المعلوماتي غير المشروع أو حضر المعلومة وناشرها بسرعة بعد قيام المتضرر بكشف هويته، وتوجيه رسالة يطالب فيها تعديل أو شطب أو سحب المحتوى المعلوماتي، مع بيان سبب عدم المشروعية، أو كيف لحق به الضرر، وتبرير عدم إمكانيته الاتصال بالمؤلف أو الناشر للمحتوى المعلوماتي الإلكتروني، أو بناءً على الإخطار من السلطات القضائية [4].

03عدم تقيد موردي الخدمات عبر شبكات الإنترنت بالتزاماتهم الواجب احترامها وفقاً للقانون.

---

[1]Morgan. LAVANCHY, La responsabilité délictuelle sur Internet en droit Suisse, 2002, p 72-75 disponible sur le site www.droit-technolgies.org

[2] إلياس ناصيف، (2009م)، العقود الدولية، العقد الإلكترونية في القانون المقارن، منشورات الحلبي الحقوقية، ص 267

[3] أنظر المادة 6 من القانون الفرنسي حول الثقة بالاقتصاد الرقمي

[4]Trudel, op. cite, p 14 , Morgan Lavanchy, La responsabilité délictuelle sur Internet, op cite, p19

يعد من الشروط التي توجب المسؤولية التقصيرية بحق مقدمي الخدمات بالواجبات، عدم احترامهم الالتزامات الملقاة على عاتقهم ومنها، تحصيل أسماء وهوية الشخص، مستخدم الموقع الإلكتروني، ومن ثم الاحتفاظ بهذه البيانات، لتحديد هوية المستخدم عند الحاجة إليها، لأن الدخول بصفة المجهول، تعيق المضرور من تحصيل ما لحق به من ضرر [1].

يقع واجباً تحديد هوية مؤلف المعلومة، وعلى مقدمي الخدمات الإلكترونية للبيانات السيبرانية عبر شبكات الإنترنت، أن يحتفظ بملفات "logs" التي تحتوي على عنوان الـ ip للآلات المتصلة بالخادم، العائد للمقدمي الخدمات التي تسمح بالوصول للمستخدمين [2]، وهذا ما أكد عليه المشرع الفرنسي من خلال، القانون الفرنسي حول الثقة بالاقتصاد الرقمي؛ حيث فرض على مقدمي الخدمة الاحتفاظ بالبيانات التي تسمح بتحديد هوية كل شخص ساهم في إيجاد المحتوى الإلكتروني على شبكات الأمن السيبراني، كما يفرض على ناشرين المحتوى الإلكتروني والذين يعملون بشكل محترف، وضع المعلومات الخاصة بهم الهادفة للتعريف بهم، أما ناشرين المحتوى الإلكتروني الهواه أو الذين يرغبون أن يبقوا مجهولين بباقي المستخدمين، فإنهم يضعون بياناتهم بالتعريف لدى موردي الخدمات والرجوع إليها من قبل الجهات المختصة عند الحاجة [3].

تطبيقاً لذلك صدر قرار من محكمة استئناف باريس بتاريخ 12/كانون الأول/2007؛ حيث أدانت شركة جوجل لعدم قيامها بالاحتفاظ بالبيانات؛ حيث رفعت دعوى من المدعوة أنجيلا بروزي ادعت فيها أنه يتم التقاط صور خاصة بالملابس الداخلية لصالح مجموعة "bentton" ونشر المعلومات

---

(1) ier. HANCE , Business et droit de l'Internet, 1996, p 190, Morgan Lavanchy, La responsabilité délictuelle sur Internet, op cite, p 44-49

(2) n Lavanchy, La responsabilité délictuelle sur Internet en droit Suisse, op. cite, p 50

(3) Morgan Lavanchyg, La responsabilité délictuelle sur Internet en droit Suisse, op. cite, p. 77

عن طريق موقعين جوجل ومايكروسفت، وقد طلب هذا الشخص إرسال صور بالملابس الداخلية، فقامت الشركة bentton بإنذار الموقعين لحذف المحتوى غير المشروع، فاستجابت شركة مايكروسفت وحجبت الدخول إلى هذه المدونة، بالمقابل رفضت جوجل القيام بذلك فقامت الشركة بالادعاء ضد جوجل أمام قاضي الأمور المستعجلة في باريس بتاريخ 4 أيار 2007 ، وبتاريخ 29 أيار 2007 حكمت محكمة بداية باريس بإلزام شركة جوجل بمنع الدخول إلى المدونة خلال ستة أيام، إلا أن شركة جوجل لم ترتضي بهذا الحكم واستأنفت الحكم على اعتبار أن الطابع غير المشروع لم يكن ظاهراً بشكل جلي، وواضحاً بالنسبة لهم، حتى لو رُفع إخطار من المتضرر، وبتاريخ 12 كانون الأول 2007 أيدت محكمة استئناف باريس الحكم الصادر من محكمة بداية باريس وأقامت المسؤولية التقصيرية اتجاه شركة جوجل لعدم قيامها بحجب المحتوى غير المشروع وعدم الاحتفاظ بالبيانات الخاصة بتحديد هوية الناشر واعتبارها قائمة من تاريخ الإخطار الموجه إليه.

لا بد من الإشارة إلى أن الالتزامات التي تقع على عاتق مقدمي الخدمات عبر شبكات الأمن السيبراني والتي تم بيانها في المباحث السابقة أي إخلال فيها يوجب المسؤولية التقصيرية.

الفرع الثاني: الضرر والعلاقة السببية في المسؤولية التقصيرية حسب القواعد العامة.

يشترط لقيام المسؤولية التقصيرية إضافة إلى الفعل الضار وحسب القواعد العامة، أن يكون الفعل الضار نشأ عنه ضرر أصاب الغير، ولا بد لهذا الضرر أن يكون حصل نتيجة للفعل الضار (العلاقة السببية)، ويعرَّف الضرر بشكل عام هو المساس بمصالح مشروعة للشخص المتضرر سواء أكانت في المال أو الجسد [1].

---

[1] عدنان سرحان، ونوري خاطر، (2021م)، مصادر الحق الشخصي، مرجع سابق، ص209، وانظر كذلك يوسف عبيدات، (2009م)، مصادر التزام في القانون المدني، دار الميسرة، عمان ص319.

كما يعرف بعض شراح القانون الضرر " الأذى الذي يصيب الشخص من جراء المساس بحق من حقوقه أو بمصلحة مشروعة له" [1].

إن الضرر في المسؤولية التقصيرية الإلكترونية يختلف عن الضرر في المسؤولية التقصيرية العادية؛ فهو ذو طبيعة مختلفة ويمتاز بأنه معنوي من ناحية ومادي من ناحية أخرى، ولا نعني بالضرر المعنوي الضرر الأدبي وفقاً للمفهوم التقليدي، وإنما المقصود بالضرر المعنوي أنه ليس له مظهراً مادياً؛ فالإضرار ببيانات الأمن السيبراني يلحق الضرر بالأموال المعنوية أي القيمة الاقتصادية لتلك البيانات التي لا تتكون من عناصر مادية ولا يمكن حيازتها، ولكنها مختصة بمخاطبة الفكر[2]، وعليه فإن الضرر المادي الجسدي غير متصور بالنسبة لمقدمي الخدمات نتيجة للطبيعة الإلكترونية للأعمال التي يقوم بها مقدمي الخدمات عبر شبكات الأمن السيبراني.

أما الضرر المادي الذي يصيب الذمة المالية للمتضرر، فهو متصور؛ حيث يمكن المطالبة بالتعويض عما لحق بالمضرور من خسارة مالية أو كسب فائت، وقد يقع الضرر على شكل إضرار بالملكية الفكرية للمتضرر، وتطبيقاً لذلك ما جاء في قضية joyeux noel؛ حيث رفع المدعي دعوى ضد مقدمي الخدمات بسبب نشر مقاطع من فيلم دون ترخيص مما مس بالحقوق الخاصة لمالكي الملكية الفكرية[3].

يقع الضرر على صورة الضرر الأدبي وهو إخلال بمصلحة غير مالية أو ما يتصل بشرف الشخص أو سمعته أو كرامته أو القيم التي يحافظ عليها، أو التشهير أو القدح أو الذم أو المساس

---

[1] انظر أمجد منصور، (2022م) النظرية العامة للالتزامات، مصادر الالتزام، دار الثقافة للطباعة والنشر، عمان، ص283.

[2] أنظر القويماني بدر علي، (2011م)، المسؤولية المدنية عن الفعل الضار الناجم عن التصرفات الواردة عبر النظام الرقمي، مرجع سابق، ص 48.

[3] أنظر أبو الهيجاء محمد ابراهيم، والخصاونة علاء الدين عبد الله، (2009م)، المسؤولية التقصيرية لمزودي خدمات الأنترنت عن المحتوى غير المشروع، مرجع سابق، ص 69.

بحياة المضرور الخاصة بها ونشرها بدون موافقة المتضرر والتي يسعى الشخص للاحتفاظ بسريتها[1].

وتطبيقا لذلك حكمت المحكمة الفرنسية في القضية المشهورة لعارضة الأزياء إيستل هاليداي والمشار إليها سابقا في المباحث السابقة، بمسؤولية متعهد الإيواء عبر شبكات الأمن السيبراني، باستضافة صور لها وهي عارية أو شبه عارية، دون موافقتها.

يقع الضرر أيضاً بالاعتداء على الحق بالاسم، وتطبيقاً لذلك قررت محكمة بداية باريس بتاريخ 31/تموز /2000م بقرار ألزمت بموجبه مورد المعلومات بالمسؤولية التقصيرية، كونه استخدم اسم شخص ما بطريقة غير مشروعة، حيث وضع الاسم تحت أيقونة، تدخل المستخدم الى موقع إلكتروني إباحي، وهو ما تسبب بضرر لصاحب الاسم [2].

يشترط لقيام المسؤولية التقصيرية، وجود رابط بين الفعل الضار والضرر، فالقيام بالفعل الضار وحدة لا يكفي، ويجب وحسب القواعد العامة للمسؤولية التقصيرية، أن يكون الخطأ أو الفعل الضار هو من تسبب بالضرر [3]، وعليه تنتفي المسؤولية التقصيرية، في حال انقطعت العلاقة السببية. تنقطع العلاقة السببية بين الخطأ" الفعل الضار" والضرر، إذا تبين أن الضرر الذي لحق ببيانات الأمن السيبراني، ناتج عن سبب غير متوقع، وخارج عن إرادة مقدمي الخدمات عبر شبكات الأمن السيبراني[4]، ومثاله لو أصاب أحد أنواع الفايروسات، النظام الإلكتروني لموقع ما، مما تسبب

---

(1) انظر يوسف عبيدات، (2009م) مصادر الالتزام في القانون المدني، مرجع سابق ص323، وانظر ماجد الحيارى، (2008م)، المسؤولية الصحفي المدنية، دار يافا العلمية للنسر والتوزيع، ص343.

(2) TGI Paris 31 juin 2000, disponible sur le site http/ www.legalis.net ، والمشار اليه في أبو الهيجاء محمد ابراهيم، والخصاونة علاء الدين عبد الله، (2009م)، المسؤولية التقصيرية لمزودي خدمات الأنترنت عن المحتوى غير المشروع، مرجع سابق، ص 70.

(3) السرحان عدنان، ونوري خاطر، (2021م) مصادر الحقوق الشخصية، مرجع سابق، ص 362وص363.

(4) أمجد منصور، (2022م) النظرية العامة للالتزامات، مرجع سابق، ص203.

بنشر معلومات ومحتوى غير مشروع، رغم عن إرادة مقدمي الخدمات الأمن السيبراني؛ حيث لا يمكن وقفه مما تنتفي معه المسؤولية التقصيرية إذا كان هذا السبب هو السبب الوحيد الناتج عن الضرر.

تنتفي المسؤولية التقصيرية أيضاً عن مقدمي الخدمات عبر شبكات الأمن السيبراني إذا تبين أن فعل المتضرر يشترك مع فعل مقدمي الخدمات في إحداث الضرر، وبالرجوع إلى القواعد العامة ينظر إلى جسامة الفعلين، ويعتد بالفعل الأجسم لتحقيق المسؤولية، أما إذا كان كل فعل مستقل في ذاته، ويشكل لوحدة سبباً لأحداث الضرر، فتوزع المسؤولية فيما بينهم، كل بمقدار فعله [1].

بقي الإشارة أن القواعد العامة المتعلقة بالمباشرة أو التسبب" العمد والتعدي " تنطبق على المسؤولية التقصيرية الإلكترونية.

المطلب الثالث

التعويض عن الإضرار ببيانات الأمن السيبراني وفقاً للفعل الضار

بعد ثبوت المسؤولية التقصيرية بحق من تسبب في الضرر، فلا بد من جزاء عادل لجبر هذا الضرر الذي لحق بالمضرور، فإن تعرض بيانات الأمن السيبراني للضرر تستوجب التعويض عن هذا الضرر، سواء أكان المسبب مقدمي الخدمات عبر شبكات الأمن السيبراني أو الغير، وإن التعويض يقع على نوعين النوع الأول التعويض العيني، والنوع الثاني التعويض بمقابل.

[1] السرحان عدنان، ونوري خاطر، المرجع نفسه، ص370.

الفرع الأول: التعويض العيني.

هو إعادة الحال إلى ما كانت عليه قبل وقوع الفعل الضار وبذات الوقت إزالة الضرر. [1]

يطبق التعويض العيني في الدعاوى للمسؤولية التقصيرية الإلكترونية، يوقف الاعتداء على الحياة الخاصة أو الملكية الفكرية أو أي اعتداء إلكتروني يعتمد على نشر محتوى غير مشروع عبر شبكات الأمن السيبراني ويتخذ التعويض العيني هنا عدة أشكال منها:

1. نشر المورد على المواقع التي يؤويها إعلاناً للحكم بالتعويض لإيوائه موقع يبث محتوى يمس حقوق الغير ومثاله بإعمال القواعد العامة بنشر الحكم في الجرائد والصحف على نفقة المحكوم عليه.
2. قد يقع التعويض على شكل حذف أو سحب أو حجب الوصول إلى المحتوى غير المشروع أو من يبث وينشر المعلومات غير المشروعة [2].
3. قد يأخذ التعويض صورة حق الرد والتصحيح؛ حيث يحق للمتضرر الرد على ما تم نشره، أو يطلب تصحيحه، ويقع التزاما على الموقع الرد أو التصحيح، وهذا الحق مستمد من المسؤولية في مجال الصحافة والنشر [3].

وعليه فالرد والتصحيح يجب أن يكون في نفس مكان الخبر المراد تصحيحه، وبنفس الحجم وبنفس المواصفات التي ينشر فيها وبالمجان وفي العدد اللاحق لتاريخ وصول طلب الرد أو التصحيح[4].

---

[1] أمجد منصور، (2022م) النظريات العامة للالتزام، مرجع سابق، ص352.

[2] وانظر ماجد الحيارى، (2008م)، المسؤولية الصحفي المدنية، مرجع سابق، ص291.

[3] وانظر ماجد الحيارى، (2008م)، المسؤولية الصحفي المدنية، مرجع سابق، ص283.

[4] سامان عمر، (2007م)، المسؤولية المدنية للصحفي، دراسة مقارنة دار وائل للنشر، ص199.

الفرع الثاني: التعويض بمقابل.

تقرر القواعد العامة أنه في حال استحالة التعويض العيني، يتم اللجوء إلى التعويض بمقابل، والذي يكون على شكل مبلغ مالي كتعويض عن الضرر الذي لحق بالمضرور بناء على قرار المحكمة التي نظرت في الدعوى، والهدف منه جبر الضرر الذي وقع على المضرور[1].

أو التعويض غير النقدي، أي الحكم بأمر معين على سبيل التعويض وهنا لا تختلف أنواع التعويض عما ورد في مطلب التعويض عن المسؤولية العقدية في هذا البحث. فمردها جميعاً إلى القواعد العامة للمسؤولية المدنية ولكن يظهر الفرق أنه في المسؤولية التقصيرية يمكن التعويض عن الضرر المتوقع وغير المتوقع والكسب الفائت.

[1] انظر أمجد منصور، (2022م) النظرية العامة للالتزامات، مصادر الالتزام، مرجع سابق، ص353.

الفصل الخامس

الخاتمة

إن تطور تكنولوجيا المعلومات، وازدهارها وتزايد الإقبال عليها واستخدامها في كافة مجالات الحياة، وتنامي وتنوع مقدمي الخدمات عبر شبكات الأمن السيبراني، وتطور الاتصال عن بعد، أصبحت حماية هذه التكنولوجيا مما تحتويه من بيانات ومعلومات ضرورة من ضروريات الأمن المعلوماتي، وأصبحت مرتبطة ارتباطا كبيرا بالأمن القومي للدول، إضافة إلى ظهور أفراد من أصحاب المهارات العالية في استخدام الحواسيب والبرامج، وازدياد المخالفات القانونية بواسطة هذه التكنولوجيا وعبر شبكات الإنترنت سواء أكانت هذه المخالفات من مقدمي الخدمات عبر شبكات الإنترنت أو المستخدمين على حد سواء، فاتجهت التشريعات والقوانين المقارنة ومنها التوجه الأوروبي والقانون الفرنسي لإرساء قواعد عامة لمحاسبة المختص على مثل هذه المخالفات وإرساء قواعد عامة لبيان التزامات مقدمي الخدمات، والجزاء المترتب على مخالفتهم، بوضع شروط عامة وأحكام خاصة للمسؤولية المدنية لكل من المستخدمين أو من مقدمي الخدمات عبر شبكات الأمن السيبراني بما يتعلق عن الإضرار ببيانات الأمن السيبراني.

وبعد هذه المعالجة لموضوع المسؤولية المدنية للإضرار ببيانات الأمن السيبراني وفقاً للقانون الأردني والقانون المقارن والاجتهادات الفقهية توصل الباحث إلى مجموعة من النتائج والتوصيات:

أولاً: النتائج.

1. إن المشرع الأردني كان الغائب الأكبر من مجاراة هذا التطور، وبالرجوع إلى قانون الأمن السيبراني الأردني وقانون المعاملات الإلكترونية الأردني نجده جاء خالياً من إرساء قواعد عامة للمسؤولية المدنية لمقدمي خدمات عبر شبكات الأمن السيبراني على الرغم من الطبيعة الخاصة لأعمالهم.
2. إن التشريع في القانون المقارن سواء أكان في القانون الفرنسي أو التوجه الأوروبي حاول عدم فرض قيود على حرية التعبير وإفساح مجال أمام التطور التكنولوجي في مجال الأمن السيبراني لذلك أرسى قواعد بعدم إلزام مقدمي خدمات عبر شبكات الأمن السيبراني بأي رقابة فعلية على مستخدمي الشبكة واقتصرها على الرقابة بأقل الحدود.
3. إن تنوع صور الخطأ، والإضرار ببيانات الأمن السيبراني؛ حيث منها ما يقع على الملكية الفكرية ومنها ما يقع على الحياة الخاصة للأفراد ومنها ما يمس أمن الدول؛ حيث يرافق ذلك أحيانا صعوبة تحديد هوية الفاعل، فأقر التشريع المقارن أنه يقوم مقدمي خدمات الأمن السيبراني بالاحتفاظ بالبيانات اللازمة، لتحديد هوية مستخدمين المواقع الإلكترونية، للرجوع إليها حال الحاجة إليها بناءً على طلب من الجهات المختصة، وفي حال الإخلال بهذا الالتزام تنهض المسؤولية المدنية، بحق مقدمي الخدمات.
4. إن المسؤولية العقدية الإلكترونية، تنهض بحق مقدمي الخدمات عبر شبكات الأمن السيبراني، والمشتركين بالخدمات عبر شبكات الأمن السيبراني، في حال أخل أي منهم بالتزاماته العقدية.

5. على الرغم من أن القواعد العامة التي تنظم حدود المسؤولية العقدية، يمكن أن تنطبق على التعاقد الإلكتروني، بين مقدمي الخدمات عبر شبكات الأمن السيبراني، و المستخدمين، إلا أنها لم تنظم الطبيعة الفنية، والتقنية، للالتزامات التي تقع على كل من طرفي العق .

6. إن تداول المعلومات، والبيانات عبر شبكات الأمن السيبراني، تحتاج الى مجموعة من الأشخاص لإتمامها، كونها تنقل بشكل حلقات متصلة ببعضها البعض، حيث تتنوع النشاطات والأدوار، لهؤلاء الأشخاص، ومنهم متعهد الوصول، والدخول، والإيواء، وخلافهم من مقدمي الخدمات عبر شبكات الأمن السيبراني، كونهم يقومون ببث المعلومات التي يحتاجها المستخدمين، ولديهم كذلك الوسائل الفنية والتقنية التي تمكنهم من الكشف عن أوجه النشاطات غير المشروعة طبعاً وفق ضوابط قانونية محددة، تنظم علاقاتهم ببعضهم البعض، وعلاقتهم بغيرهم من المستخدمين .

7. لم يورد المشرع الأردني الإجراءات المتخذة لحماية الأنظمة، والشبكات المعلوماتية، والبنى التحتية الحرجة، من حوادث الأمن السيبراني، ولم يفرض حدود المسؤولية المدنية على هذا الأساس بنصوص منفردة.

ثانياً: التوصيات

1. يوصي الباحث بتنظيم أحكام قانونية خاصة تعالج الطبيعة التقنية والفنية الإلكترونية، لاستكمال القواعد العامة في المسؤولية المدنية بشقيها، سواء المسؤولية العقدية، أو المسؤولية التقصيرية.
2. يرى الباحث ضرورة التوسع في تنظيم العقود الإلكترونية لتشمل كل ما يدخل تحت هذا الباب من عقود ويضع تنظيماً موحداً لها ولا سيما أن قانون المعاملات الإلكترونية لم يأتي على تفصيلات تلك العقود.

3. يرى الباحث ضرورة عدم ترك العلاقة القائمة بين مستخدمي المواقع الإلكترونية والموقع الإلكتروني للقواعد العامة وبالأخص فيما يتعلق بالخدمات التي تقدم عبر شبكات الإنترنت للبيانات السيبرانية وتنظيمها بما يخص طرق الإثبات والتراخيص وطرق الدفع الإلكترونية.
4. يوصي الباحث، بضرورة تلافي النقص الموجود في النصوص التشريعية، للقوانين الأردنية، والمتعلقة بتحديد المراكز القانونية، لمقدمي الخدمات عبر شبكات الأمن السيبراني، بحيث يتم تحديد جميع الأدوار التي يجب على هؤلاء القيام بها، فيما يتعلق بالأمن السيبراني.
5. يوصي الباحث بإضافة نصوص تشريعية تلزم مقدمي خدمات البيانات السيبرانية عبر شبكات الإنترنت، بتوفير أجهزة وبرامج فنية، للمواجهة التهديدات السيبرانية والهجمات الإلكترونية التي أصبحت ذات طابع دولي، من خلال متابعة المضمون المعلوماتي، وعمل فلترة تتناسب وقيم وعادات المجتمع الأردني.
6. يرى الباحث ضرورة أن ترد نصوص قانونية في قانون الأمن السيبراني الاردني، تمكن المتضرر من المطالبة بوقف بث المضمون الإلكتروني غير المشروع، وتحدد هذه النصوص الآلية والإجراءات التي يجب إتباعها، لسحب المحتوى غير المشروع أو منع الوصول أليه.
7. يوصي الباحث بإقرار نظام خاص، يبين شروط منح التراخيص لمقدمي خدمات البيانات السيبرانية عبر شبكات الإنترنت، وتحديد إلتزاماتهم وحدود مسؤوليتهم، وشروط سحب التراخيص الممنوحة لهم في حال الإخلال بإلتزاماتهم، وكذلك يبين حالات الإعفاء من المسؤولية.

قائمة المصادر والمراجع

أولاً: المراجع العربية

القرآن الكريم.

ثانياً: المعاجم:

1. إبن منظور، (تاريخ الوفاه 711هـ)، **لسان العرب**، مؤسسة الرسالة للطباعة والنشر والتوزيع، لبنان، بيروت، 1987م.
2. ابن منظو، (تاريخ الوفاه 711هـ)، **تهذيب الخواص من درة الغواص**، المحقق(وهبة أحمد رضوان) ، دار النشر للجامعات، القاهرة، 2011م.

ثالثاً: الكتب:

1. ابو الليل ابراهيم الدسوقي، (1995م)، **تعويض الضرر في المسؤولية المدنية**، الكويت: مطبوعات جامعة الكويت
2. إلياس ناصيف، (2009م)، **العقود الدولية، العقد الإلكترونية في القانون المقارن**، لبنان : منشورات الحلبي الحقوقية.
3. أمجد منصور، (2022م)، **النظرية العامة للالتزامات، مصادر الالتزام**، عمان: دار الثقافة للطباعة والنشر.
4. البهلوان على، (2009م)، **استخدام قاعدة البيانات ومنهج التطبيقات**، (ط2)، مصر: دار الكتب العلمية للنشر والتوزيع، القاهرة.
5. الجبوري نصير صبا، (2019م)، **التعويض العيني، دراسة مقارنة**، (ط1)، عمان: دار القنديل للنشر والتوزيع.

6. الحايك أودين سلوم، (2009م)، **مسؤولية مزودي خدمات الإنترنت الفنية**، (ط1)، لبنان: المؤسسة الحديثة للكتاب.

7. حجازي عبد الفتاح بيومي، (2003م)، **النظام القانوني لحماية الحكومة الإلكترونية بين الواقع والطموح**، (ط1)، الكتاب الثاني، مصر: دار الفكر الجامعي الإسكندرية.

8. حجازي عبد الفتاح بيومي، (2008م)، **الحكومة الإلكترونية بين الواقع والطموح**، (ط2) مصر: دار الفكر الجامعي.

9. الحياري ماجد أحمد، (2008م)، **مسؤولية الصحفي المدنية، دراسة مقارنة بين القانونين المدني والمصري**، عمان: دار يافا العلمية للنشر والتوزيع.

10. دندون حسن علي، (1998م)، **المبسوط في المسؤولية المدنية، الضرر**، الجزء الأول، بدون مكان نشر

11. رستم هشام علي، (1994م)، **قانون العقوبات ومخاطر تقنية المعلومات**، مصر: مكتبة الآلات الحديثة.

12. سامان عمر، (2007م)، **المسؤولية المدنية للصحفي، دراسة مقارنة**، عمان: دار وائل للنشر.

13. سرحان عدنان، ونوري خاطر، 2021، **شرح القانون المدني، مصادر الحقوق الشخصية الالتزامات، دراسة مقارنة**، عمان: دار الثقافة للنشر والتوزيع.

14. سعد نبيل ابراهيم، (2007م)، **النظرية العامة في الالتزام مصادر الالتزام**، القاهرة: دار الجامعة الجديدة للنشر.

15. السنهوري عبد الرزاق أحمد، (1949م)، **الوسيط في القانون المدني، الجزء الثاني**، مصر.

16. عبد الرحمن حمدي، (2010م)، **الوسيط في النظرية العامة في الالتزامات، الكتاب الأول، المصادر الإيرادية للالتزام العقد والإرادة المنفردة**، (ط2)، القاهرة: دار النهضة العربية.

17. الفتلاوي حمزة صيوان، (2015م)، **الأمن السيبراني والحروب السيبرانية**، مجلة خيمة العراق، وزارة الدفاع، العدد357، السنة الثالثة.

18. مغبغب نعيم، (2006م)، **حماية برامج الكمبيوتر**، (ط1) لبنان: منشورات الحلبي بيروت،

19. منصور محمد حسين، (2003م)، **المسؤولية الإلكترونية**، (ط1)، مصر: دار الجامعة الجديدة للنشر.

20. النقروز على، (2017م)، **جرائم نظم المعلومات**، عمان: دار السناء للنشر.

21. يوسف عبيدات، (2009م)، **مصادر التزام في القانون المدني**، عمان: دار الميسرة.

رابعاً: الرسائل العلمية:

1. أبوالحسن حنين جميل، (2021م)، **الإطار القانوني لخدمة الأمن السيبراني (دراسة مقارنة)**، رسالة ماجستير منشورة، جامعة الشرق الأوسط، عمان، الأردن.

2. أحمد هيثم السيد، (2013م)، **المسؤولية المدنية في إطار المعاملات عبر شبكة الإنترنت**، أطروح الدكتوراة منشورة، كلية الحقوق، جامعة المنوفية، مصر.

3. الحسبان ياسين محمد، (2010م)، **المسؤولية المدنية لمقدمي الخدمات غبر الإنترنت في القانون الأردني "دراسة مقارنة "**، رسالة ماجستير منشورة، جامعة عمان العربية، البلقاء، الأردن.

4. السحيباني عبد الله، (2011م)، **كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات**، رسالة ماجستير منشورة، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.

5. الشوك محمد عبد الرزاق محمد عباس (2016م)، **النظام القانوني لعقد الاشتراك في خدمة الإنترنت**، رسالة ماجستير منشورة، جامعة الكوفة، العراق.
6. علي صالح براء، (2020م)، **المسؤولية العقدية لمزودي خدمات عبر الإنترنت (دراسة مقارنة)**، رسالة ماجستير منشورة، جامعة الشرق الأوسط، عمان، الأردن.
7. العنزي سلمان، (2003م)، **وسائل التحقيق في جرائم نظم المعلومات**، رسالة ماجستير منشورة، جامعة نايف للعلوم الأمنية، الرياض، السعودية.
8. القويماني بدر علي، (2011م)، **المسؤولية المدنية عن الفعل الضار الناجم عن التصرفات الواردة عبر النظام الرقمي**، رسالة ماجستير منشورة، جامعة آل البيت، المفرق الأردن.
9. المعموري علي، **الأمن السيبراني ودورة في انتشار ظاهرة الإرهاب في العراق بعد عام 2003م**، رسالة ماجستير منشورة، كلية العلوم السياسية، جامعة بغداد، بغداد، العراق.
10. ميلاد علي ميلاد، (2007م)، **جريمة إتلاف نظم المعلومات (دراسة مقارنة)**، رسالة ماجستير منشورة، جامعة عمان العربية للدراسات العليا، البلقاء، الأردن.

رابعاً: الأبحاث العلمية:

1. أبو الهيجاء محمد ابراهيم، والخصاونة علاء الدين عبد الله، (2009)، **المسؤولية التقصيرية لمزودي خدمات الإنترنت عن المحتوى غير المشروع، دراسة التوجه الأوروبي الخاص بالتجارة الإلكترونية لسنة 2000م والقانون الفرنسي**، بحث منشور في مجلة الشريعة والقانون، بتاريخ إبريل 2010م، العدد 43.
2. بارة سمير(2017م)، **الدفاع الوطني والسياسات الوطنية للأمن السيبراني (cyber security) في الجزائر، الدور والتحديات**، (ط2)، الملتقى الدولي حول سياسات الدفاع

الوطني بين الالتزامات والتحديات الإقليمية، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، الجزائر.

3. البشري محمد أمين، (2004م)، بحث بعنوان **التحقيق في الجرائم المستحدثة**، الرياض، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، السعودية.

4. بني حمد عبد السلام أحمد، (2018م)، **تأصيل المسؤولية المدنية لمتعهد الإيواء في شبكة الإنترنت في القانون الأردني**، أكاديمية الشرطة الملكية، منشور، علوم الشريعة والقانون، مجلد 4، ملحق1.

5. جاب الله عادل، (2022م)، **وسائل حماية الامن السيبراني، دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة**، بحث منشور في مجلة كلية الشريعة والقانون، جامعة الازهر.

6. الحسبان نهاد عبد الكريم، (2019م)، **الخبرة الفنية وإجراءاتها وأسس تقديرها**، بحث علمي، المعهد القضائي الأردني، عمان.

7. حسن إشراق، (2020م)، **الحماية المدنية للأموال الالكترونية دراسة مقارنة**، بحث منشور على مجلة التربية، جامعة واسط، كلية القانون، العدد29.

8. زهرة عطا محمد، (1991م)، **الامن القومي العربي**، بنغازي، جامعة قاريونس، بحث منشور على http;\\www,nli.org.il

9. سرحان عدنان، (1997م)، الفعل عير المشروع الإضرار كأساس للمسؤولية التقصيرية، الالتزام بالضمان في الفقه الإسلامي والقانون المدني، بحث منشور في مجلة المنارة، مجلد 2، عدد 2، ص 106، عمان، 1992م.

10. الصرايرة، منصور عبد السلام، (2023م)، المسؤولية التقصيرية الناشئة عن الإخلال بالتزامات مقدمي خدمات الأمن السيبراني، دراسة في التشريع الأردني، بحث مقدم الى المؤتمر الدولي الثاني / الجرائم الإلكترونية والأمن السيبراني / 3-4 مايو 2023م.
11. فاطمة علي ابراهيم، ورحاب يوسف، ووليد محمود السيد، (2022م)، **الأمن السيبراني والنظافة الرقمية**، بحث منشور، المجلة المصرية لعلوم المعلومات، مجلد 9، عدد 2.
12. المساعدة نائل علي، (2005م)، **أركان الفعل الضار الإلكتروني في القانون الأردني**، بحث علمي منشور في مجلة الدراسات، الجامعة الأردنية، مجلد 32، العدد1.
13. نصار إيناس مكي عبد، (2013م)، **التفاوض الإلكتروني "دراسة مقارنة في ضل التشريعات العربية المعاصرة** "، بحث علمي، منشور في مجلة بابل للعلوم الإنسانية، جامعة بابل، مجلد 21، عدد3.
14. نوري حمد خاطر، (2003م)، "**الخطأ الجسيم في ظل تطبيقاته التشريعية والقضائية: دراسة مقارنة**"، المنارة للبحوث والدراسات، المجلد التاسع، العدد الثالث، جامعة آل البيت.

خامساً: الأحكام القضائية والدوريات:

- المذكرات الإيضاحية للقانون المدني الأردني، إعداد المكتب الفني في نقابة المحامين الأردنيين، الجزء الأول، الطبعة الأولى.

سادساً: التشريعات:

1. الدستور الأردني وتعديلاته لسنة 1952م
2. مدني الأردني رقم 43 لسنة 1976 وتعديلاته

3. قانون الاتصالات الاردني وتعديلاته رقم 13 لسنة 1995م

4. قانون المطبوعات والنشر الأردني رقم 8 لسنة 1998وتعديلاتة رقم 30 لسنة 1999م

5. قانون المعاملات الإلكترونية لسنة 2015 م وتعديلاته

6. قانون الجرائم الإلكترونية رقم 27 لسنة 2015 م

7. قانون الاعلام المرئي والمسموع رقم 27 لسنة 2015م

8. قانون حماية المستهلك الأردني رقم 7 لسنة 2017م

9. قانون الامن السيبراني رقم 16 لسنة 2019م

10. قانون الجرائم الإلكترونية رقم (17) لسنة 2023م

11. قانون حماية البيانات الشخصية رقم 24 لسنة 2023م

12. الدستور المصري وتعديلاته لسنة 2014 م

13. قانون المعاملات والتجارة الالكتروني القطري رقم 16 لسنة 2010م

14. قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 سنة 2018م

15. فانون الخطابات والمعاملات الإلكترونية البحريني رقم 54 لسنة 2018م

16. القانون الأمريكي الصادر بتاريخ 28/تشرين الأول/ 1998م، Digital Milleniam Copyright Act.

17. القانون الفرنسي حول حرية الاتصال لسنة 1986 وتعديلاته رقم 719 لسنة 2000م

18. قانون الثقة حول الاقتصاد الرقمي الفرنسي رقم 45 لسنة 2004م

19. القانون الفرنسي لحق المؤلف والحقوق المجاورة له في مجال المعلوماتية،2006م

20. القانون الفرنسي حول ثقة الاقتصاد الرقمي رقم 575 لسنة 2004م

21. تنظيم الهيئة الوطنية للأمن السيبراني الصادر بأمر ملكي رقم 6801 عام 1439هـ

22. نظام المركز الوطني للأمن السيبراني رقم 1لسنة 2020 م

23. نظام التنظيم الإداري للمركز الوطني للأمن السيبراني رقم 25لسنة 2021م

سابعاً: الاتفاقيات والمعاهدات:

1. الإعلان العالمي لحقوق الأنسان الصادر 10 / كانون الأول / 1948
2. التوجيه الأوروبي حول التجارة الإلكترونية لسنة 2000م
3. اتفاقية بودابست لعام 2001م، الاتفاقية المتعلقة بالجريمة الإلكترونية، المجلس الأوروبي، مجموعة المعاهدات الاوروبية رقم 185 والمنشورة على محرك البحث قوقل على الرابط الإلكتروني http;\\rm.coe.int
4. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012م المنشور في الجريدة الرسمية ،2012/6/17م، رقم5162

ثامناً: المواقع الإلكترونية:

1. مقال بعنوان الامن السيبراني وادارة مخاطرة في مجال الأعمال، إعداد غسان، والمنشور بتاريخ 19 \أكتوبر /2019م في محرك البحث جوجل على الرابط ،http://cutt.ly.gbtcv7u
2. دراسة بعنوان العملات المشفرة، البنك المركزي الاردني، دائرة الاشراف والرقابة على نظام المدفوعات الوطني، اذار ،2020، والمنشور على موقع البنك المركزي الاردني http\\www.cbj.gov.jo
3. مقال بعنوان الأمن السيبراني والثورة الصناعية الرابعة، اعداد الربعي علي محمد والمنشور بتاريخ 12 \ فبراير \ 2020م في محرك البحث جوجل على الرابط ،http;\\www.okaz.com\articles\outhors2010045

4. مقال بعنوان قانون الأمن السيبراني تنظيمي وليس تجريمياً، اعداد القضاة يعرب والمنشور بتاريخ 28 \ 11 \2020م في محرك البحث جوجل على الرابط http;\\www.patra.gov.jo،

5. مقال بعنوان اهمية الأمن السيبراني، اعداد الصوالحة رشا والمنشور بتاريخ 16/ 11/ 2021م في محرك البحث جوجل على الرابط http://mawdoo3.com،

6. مقال بعنوان الجرائم الإلكترونية مشروع قانون يغلظ العقوبات ،اعداد الشوابكة لينا والمنشور بتاريخ 2023/7/30م في محرك البحث جوجل على الرابط http://www.bbc.com،

تاسعاً: المراجع الأجنبية:

1. dictionnaire ،oxford ،2020
2. dictionnaire ،word-reference، 2020
3. André LUCAS, "La responsabilité des différents intermédiaires de l´internet", *in* L´internet et le droit- Droit européen et comparé de l´internet, Colloque organisé par L´Université de Paris I, Paris, 25 et 26 septembre 2000, p. 2, disponible à l´adresse: www.droit-internet-2000.univ-paris1.fr/di2000_20.htm.
4. CA Versailles, 12e ch., 8 juin 2000, CA Pau, 14 octobre 1999, nº 97/003191, SA France Télécom C/L, TGI Nanterre, 1re ch., sect. A, 8 décembre 1999.
5. Cour de Cassation Criminelle الجزائية محكمة النقض, 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
6. 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.
7. Directive No. 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ،(Directive on electronic commerce) PDF HTML والمنشور على wipo.int\wipolex\ar\iegistution\details\6393
8. Guide Permanent Droit et Internet, E 1.2., Fourniture d′accès, précité, nº 36.
9. Guide Permanent Droit et Intemet, E 3.13, Responsabilité de l'éditeur, clairement, n°1

10. M. GUILLARD, "Responsabilité des acteurs techniques de l'intemet", Guide
11. James Graham,Richard Howward,Ryan Olson"edit",2011, cyber security Essentials, Taylor &francis croup,new york
12. Kriangask kittchaisaree ,2017,public international law of cyberspace ,springer international publishing Switzerland
13. Ph. LE TOURNEAU, "La responsabilité civile des acteurs de l´internet", expertises, janvier 1999, , TGI Paris, 3e Ch., 1re Sect., 23 mai 2001, Comm. Com. Électr., novembre 2001, Chronique, n 112,.
14. 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 ،
15. 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
16. Morgan. LAVANCHY, La responsabilité délictuelle sur Internet en droit Suisse, 2002, disponible sur le site www.droit-technolgies.org
17. Olivier. HANCE , Business et droit de l'Internet, 1996.
18. Stephen Elliott ،2010،july،8،""، infosec،islan analysis on defense and cyber warfare" والمنشور على موقع https;\\Infosesisland.com\blogvie5160-Analysis-on-Defense-and cyber-warfare.html م2023/8/5 تاريخ الدخول 16:20ساعة الخول).
19. TGI de Nanterre,24 May 2000, available at the address: www. juriscom.nct., voir également sur l'obligation de collaboration et d'information, E. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in M. ANTOINE, A.

CRUQUENAIRE et d'autres, Commerce electronique européen sur Les Rails?, Iredition, 2001, Bruylant, Bruxelles, n° 526 et s.,

20. P. TRUDEL, La responsabilité civile sur Internet selon la loi concernant le cadre juridique des technologies de l'information, 2001, disponible sur le site ,http//www.papyrus.bib.umontreal.ca
21. Th. VERBIEST et É. WÉRY, "La responsabilité des fournisseurs de services internet: Derniers développement (35) -jurisprudentiels", Journal des Tribunaux, 2001
22. 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,