المسؤولية المدنية الناجمة عن هجوم النقرة الصفرية
(دراسة مقارنة)

الدكتور/ أحمد محمد فتحي الخولي *

الملخص:
إن التطور المذهل الذي يشهده العالم في كافة المجالات لاسيما في ميدان التكنولوجيا، والانتشار المتسارع في وسائل الاتصال الحديثة، واستغلالها شبكة الإنترنت في التعاملات بين الأفراد والشركات قد أدي بدوره إلى ظهور جرائم مستحدثة لم تكن معهودة من قبل. فقديما كانت الجرائم تقليدية ونمطية، أما في هذا العصر فقد تطورت الجرائم تبعا لتطور وسائلها، وغدا المجرمون يستغلون شبكة الإنترنت كساحة لإنفاذ جرائمهم وإلحاق الضرر بالآخرين والتعدي عليهم مستخدمين في ذلك وسائل مُبتكرة فرضتها التكنولوجيا الحديثة، مما أدى إلى استحداث أضرار جسيمة لم تكن موجودة من قبل كإفشاء الأسرار التجارية واختراق الحواسب الشخصية وانتهاك خصوصية الأفراد. بل الأسوأ من ذلك أنها تسببت في أضرار كارثية، وهذه الطرق المستخدمة تُعدّ احتيالية وصعبة الاكتشاف وتحدث أضراراً بالغة بضحاياها وتعرف بهجوم النقرة الصفرية أو الهجوم الصفري، وهذه الجريمة معدودة من الجرائم الحديثة جدا والتي تختلف عن الجرائم الإلكترونية في طريقة تنفيذها وفداحة أضرارها التي قد تؤدي إلى خسائر مادية ومعنوية جسيمة، فهل التشريعات الوطنية قادرة فعلا على مواجهة هذه الجرائم الحديثة وتعويض المتضرر منها؟ وهل القواعد الموجودة حاليا صالحة للتطبيق على جريمة هجوم النقرة الصفرية؟ هذا ما سوف نوضحه من خلال بحثنا إن شاء الله.

الكلمات المفتاحية: هجوم النقرة الصفرية – المسؤولية المدنية – الجرائم الإلكترونية – اختراق – انتهاك الخصوصية.

---

* أستاذ القانون الخاص المساعد – كلية إدارة الأعمال – جامعة المجمعة – المملكة العربية السعودية.

Civil Liability Caused by the (Zero-Click Attack) (A Comparative Study)

Dr. Ahmed Mohamed Fathy El-Kholy*

Abstract:
The astonishing development that the world is witnessing in all fields, especially in the field of technology, and the rapid spread of modern means of communication, and the exploitation of the Internet in transactions between individuals and companies, has in turn led to the emergence of new crimes that were not previously known. In the past, crimes were traditional and stereotypical, but in this era, crimes have evolved according to the development of their means, and criminals are exploiting the Internet as an arena for enforcing their crimes and harming others and attacking them using innovative means imposed by modern technology, which led to the creation of serious damages that did not exist before as disclosure Trade secrets, hacking of personal computers and violating the privacy of individuals. Even worse, it caused catastrophic damage, and these methods used are fraudulent and difficult to detect and cause severe damage to their victims and are known as the zero-click attack or the zero-attack, and this crime is a few of the very modern crimes that differ from electronic crimes in the way they are implemented and the severity of the damage that may lead to huge material and moral losses. Is national legislation really capable of confronting these modern crimes and compensating those affected by them? Are the existing rules applicable to the zero-click attack crime? This is what we will clarify through our research, God willing.

Keywords: Zero-Click Attack - Civil Liability - Cybercrime - Hacking - Violation of Privacy.

---

*Assistant Professor of Private Law, College of Business Administration, Majmaah University, Kingdom of Saudi Arabia.

المقدمـــة

لقد أصبحنا الآن في القرن الحادي والعشرين وتزامن ذلك مع تطور فائق السرعة في تقنية المعلومات والاتصالات وانتشار واسع وملحوظ للإنترنت ونتج عن ذلك ظهور العديد من المواقع الإلكترونية، وغدت معظم المعاملات الرسمية الآن تتم عبر العديد من المواقع الإلكترونية المتنوعة من بيع أو شراء أو تسوق ناهيك عن تعدد وسائل التواصل الاجتماعي ومواقعه التي من أبرزها وأوسعها انتشاراً :(الفيس بوك، تويتر، واتس أب).

وقد صاحب هذا التطور التكنولوجي أيضا تطور الأجهزة الإلكترونية ونتج عن ذلك ظهور أجهزة رقمية منها الحواسب المحمولة والهواتف الذكية وظهور علم البرمجيات، كما انتشرت البرامج الإلكترونية التي من الممكن تثبيتها على الحواسيب الشخصية والهواتف المحمولة، ولا ريب أن كل ذلك يعد من الإيجابيات التي أفرزها التطور التكنولوجي الرهيب في مجال الإنترنت.

بيد أنه على الجانب الآخر، ظهرت العديد من السلبيات، منها زيادة معدلات الجرائم الإلكترونية التي لم نسمع بها من قبل كعمليات الاختراقات الممنهجة، والتجسس علي الأشخاص باستخدام برامج يتم تطويرها من مبرمجين مارقين تم تسميتهم بالهاكرز (hackers) وأيضاً ال (crackers) بقصد الإضرار وللأسف فقد تعرض العديد من الأشخاص، بل الدول الي تلك الهجمات التي كبدتهم الخسائر الفادحة في الأموال وانتهاك الخصوصية فضلاً عن إلحاق المخاطر الكبيرة بالاقتصاد والأمن القومي وحياة الأفراد، فتحولت شبكة الإنترنت الي ساحة من الصراعات وتصفية الحسابات وبعدما كانت الجرائم تتم على أرض الواقع انتقلت هذه الجرائم المتمثلة في القرصنة والإرهاب وجرائم غسيل الأموال والتزوير والتزييف ونشر العنصرية والإباحية، والتجسس علي الآخرين، وسرقة الأموال بدون وجه حق إلى الواقع الافتراضي الموجود في

ساحات الإنترنت بشكل يتلاءم مع خصائص الإنترنت مما دفع العديد من الدول إلى سنّ تشريعات صارمة لمواجهة هذه الجرائم السيبرانية[1].

وفي الآونة الأخيرة زادت الهجمات الإلكترونية واتخذت أشكالاً عديدة، وطرقاً ملتوية، لكن تلك الهجمات تتفق في اتخاذ شكل معين طبيعي، وهو أن يقوم المخترق باستغلال نقاط ضعف الجهات الحكومية والمنظمات والأفراد، وعدم تجديد نظام الأمان لديهم، وإتباع نظام الأمان الإلكتروني، واستخدام البرامج التي تحميهم من هذه الهجمات؛ فيقوم المخترق (الهاكرز) بإرسال رسائل ملغمه تحمل في طياتها برنامج تم صناعته خصيصا لفتح ثغرة في جهاز الضحية سواء كان فرداً أو شركه أو جهة حكومية، وبمجرد الضغط على هذا الملف المرسل يصبح جهاز الضحية بالكامل في حوزة المخترق بحيث يستطيع نسخ كل الملفات الموجودة في جهاز الضحية، ومعرفة كل كلمات المرور الموجودة به، بل يمكنه أيضاً تشغيل الكاميرا الخاصة بالضحية، وتسجيل فيديوهات بدون أن يعلم أحد بذلك، وأيضاً فتح الصوت الخاص بالجهاز المخترق، وتسجيل كل ما يدور حوله علي مسافه تقريباً تقدر من عشرة الي عشرين متر علي حسب جوده الجهاز المستخدم طالما أن الجهاز متصل بالإنترنت.

وفي تطور ملحوظ لهذه الهجمات الإلكترونية ظهر نوع جديد من الهجمات أكثر شراسة من الهجمات العادية التي تمت ملاحظتها في الأعوام الماضية؛ حيث إن الهجمات العادية تعتمد دائماً على استخدام وسائل احتيالية لإيقاع الضحية؛ كإرسال

---

[1] المقصود بالجرائم السيبرانية: نوع من أنواع الجرائم ترتكب ضد أفراد أو جماعات بدافع جرمي ونية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواءً كان ذلك بطريقة مباشرة أو غير مباشرة، وأن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت، غرف الدردشة، البريد الإلكتروني أو المجموعات. للمزيد من المعلومات راجع د عبير شفيق رحباني، الجرائم الإلكترونية ومخاطرها، دار الثقافة للنشر والتوزيع، الأردن، ٢٠٢١، ص .٢٩، وراجع أيضا د محمد الدسوقي الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة رسالة دكتوراه، جامعة القاهرة، بدون سنة نشر ص ٥٢.

بريد إلكتروني ملغم يحتوي على رابط أو ملف ملغم مستغلاً جهل الضحية بأمور الحاسب أو الإنترنت أو يعتمد علي خداعة بتزوير رابط إلكتروني أو تطبيق مجهول المصدر يستخدمه الضحية أو إرسال له عروض وهميه في شكل ملفات، ويتم تفعيل البرنامج المدمج بداخلها فور فتح الضحية لتلك الملفات أو الروابط مما يجعل وصول المخترق إلى جهاز الضحية سهلاً ميسوراً.

أما الطريقة الحديثة والتي ظهرت مؤخرا تعرف بهجوم (النقرة الصفرية) أو هجوم (الضغط الصفري) (ZERO CLICK ATTACK) لا يحتاج فيها المخترق إلي إرسال رسالة الي الضحية أو إيميل مزور أو أي رابط علي الإطلاق، وهنا تكمن الخطورة المطلقة؛ حيث يستطيع المخترق الدخول الي أي جهاز بدون أي رد فعل إيجابي من الضحية مستغلاً ثغرات أمنية في أنظمة التشغيل للحاسب الألي أو الهاتف الذكي الذي يستعمله الضحية، فلا يحتاج المخترق سوى معرفة معلومات بسيطة ومتاحه للجميع عن ضحيته؛ كرقم هاتفه الخاص، أو الأماكن التي يتردد عليها أو نظام التشغيل الذي يستخدمه أو الشبكة اللاسلكية (Wi Fi) الذي يستخدمها، ويستغل الثغرات الموجودة في هذا النظام مباشرة لتثبيت برامج التجسس بدون علم الضحية أو بدون أي تصرف إيجابي منها، وفي حقيقة الأمر فإن هجوم النقرة الصفرية يضعنا في مواجهة مباشرة مع نوع جديد من الهجمات الإلكترونية التي نتج عنها جرائم إلكترونية أدانتها التشريعات المختلفة ومنها المشرع المصري والمنظم السعودي والمشرع الفرنسي؛ حيث وضعوا نظاماً خاصاً لمكافحة الجرائم المعلوماتية[٢].

---

[٢] للمزيد من المعلومات يمكنكم الاطلاع على المرسوم الملكي الخاص بمكافحة الجرائم المعلوماتية الصادر برقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨ حيث كان أخر ولوج في ١٤٤٣/٥/٥ هـ:
https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1

مشكلة البحث:

هل تُعدّ قواعد المسؤولية المدنية التي حددتها التشريعات الوطنية- مثل المشرع المصري والمنظم السعودي والمشرع الفرنسي- في قوانينها كافية لتعويض المتضررين من جراء الجرائم الجديدة التي نجمت مؤخراً عن هجوم النقرة الصفرية والتي تختلف في خصائصها عن التي كانت موجودة من قبل؟

إننا نجد الشخص الذي تم الإيقاع به في براثن هذا الهجوم قد تعرض لضرر كبير إلى جانب جهله به، وعدم انتباهه له أصلاً، لذا يلزم سن قانون يحدد بدقة العقوبة الجنائية المقررة لمرتكب جريمة هجوم النقرة الصفرية، وكذا سنّ قانون يعوض الضحية عن الأضرار الجسيمة التي لحقته من جراء ذلك الهجوم سواء كانت أضرارًا مادية أو معنوية.

أهمية البحث:

تكمن أهمية البحث في التعريف بجريمة النقرة الصفرية وبيان المخاطر المترتبة عليها من انتهاك للخصوصية والاعتداء على حقوق ثابته أقرها القانون للمتضرر وتوضيح الحماية القانونية التي أقرها القانون المدني لمثل هذه الجرائم مع إلقاء الضوء على إمكانية الاكتفاء بتطبيق القواعد العامة الموضوعية التي حددها القانون المدني من عدمه، وإذا تم تطبيق تلك، فهل تندرج تحتها جريمة هجوم النقرة الصفرية؟

وأيضاً قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ حيث كان أخر ولوج في ١٤٤٣/٥/٥ هـ:

https://manshurat.org/node/31487

ووضعت فرنسا القانون رقم «١٩-٨٨» الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة له.

منهج البحث:

يرتكز هذا البحث على ثلاثة محاور منهجية هي: الوصفي، والتحليلي، والمقارن، فنقوم أولاً بإماطة اللثام عن ماهية هجوم النقرة الصفرية، محاولين – قدر الطاقة المقارنة بين كل من القانون الذي أصدره المنظم السعودي الصادر بمرسوم ملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨والخاص بمكافحة جرائم المعلوماتية، وبين القانون المصري رقم ١٧٥ لسنة ٢٠١٨ والخاص بمكافحة جرائم تقنية المعلومات وذلك في ضوء القانون الفرنسي رقم «١٩–٨٨» والذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي، ثم تحليل النصوص القانونية لكل منهم بُغية تحديد النظام القانوني لجريمة النقرة الصفرية وكذا تحديد طرق تعويض المتضررين من الخسائر التي ألمّت بهم.

خطة البحث:

المبحث الأول: ماهية الجرائم الإلكترونية.

المبحث الثاني: مفهوم جريمة هجوم النقرة الصفرية.

المبحث الثالث: الأساس القانوني للمسؤولية المدنية الناشئة عن جرائم هجوم النقرة الصفرية.

المبحث الرابع: آثار المسؤولية المدنية عن الأضرار الناشئة من هجوم النقرة الصفرية.

المبحث الأول

ماهية الجرائم الالكترونية

قبل أن نبدأ بالحديث عن جرائم الضغط الصفري أو جرائم هجوم النقرة الصفرية علينا أولاً أن نتحدث عن الجرائم الإلكترونية ثم نوضح خصائصها ونبين بعدها كل ما هو متعلق بجرائم الهجوم الصفري.

المطلب الأول

مفهوم الجريمة الإلكترونية

الجريمة الإلكترونية تعتبر من الظواهر الحديثة؛ لأن ظهورها ارتبط بظهور تقنيات حديثة مثل الكمبيوتر والإنترنت ولذلك لم يتم الاتفاق على تعريف محدد لها، وذهب العديد من فقهاء القانون إلى عدم وضع تعريف محدد لها، وكانت حجتهم في ذلك أنها مجرد جريمة عادية لكن استُخِدمت الوسائل الإلكترونية لتنفيذها.

الفرع الأول

تعريف الجريمة الإلكترونية:

لتعريف الجريمة الإلكترونية ظهر اتجاهان من الفقه، أحدهما ضيّق مفهوم الجريمة الإلكترونية وعرفها بأنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الي معلومات مخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه"[٣].

---

[٣] انظر: د. نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية"، ٢٠٠٥، ص ٢٨، وللمزيد من المعلومات انظر د. خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠١٩، ص ٣٥٧، وراجع أيضا د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول الجرائم المستخدمة عن استخدام الحاسب الآلي، الطبعة الرابعة، ٢٠٠٢ دار النهضة العربية ص ٤٧.

وعرفها الفقيه الفرنسي "باركر" من خلال مؤلفه بأنها فعل متعمد مرتبط بأي وجه بالحاسبات، يتسبب في تكبد المجني عليه خسارة "[٤].

أما بالنسبة إلى الاتجاه الموسع فقد عرّف الجريمة الإلكترونية بأنها: " كل سلوك إجرامي يتم بمساعدة الكمبيوتر"[٥]، وعرفت الجريمة الإلكترونية أيضاً بأنها:" أحد الأنشطة الجنائية التي تمثل اعتداء على برنامج وبيانات الحاسب الآلي"، وعرفها المنظم السعودي بأنها: "أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[٦]، أما بالنسبة إلى المشرع المصري فلم يضع تعريفًا محددا لها، واكتفي بالإشارة الي العقوبات المترتبة على الجريمة الإلكترونية مثل انتهاك حرمة الحياة الخاصة وجرائم الاحتيال على البنوك والبطاقات المصرفية الخ ...

والملاحظ من خلال هذه التعريفات التي سبق ذكرها أن الجريمة الإلكترونية ظهرت نتيجة الثورة الرقمية وأنشطتها العابرة للحدود والتي اخترقت بذلك كل القوانين التي تم وضعها من قبل الحكومات للجرائم التقليدية فهذه الجرائم تتم بطرق مختلفة سواء من ناحية مباشرة أومن ناحية آخري غير مباشر مستهدفه الأفراد والمنظمات والحكومات وتهدف إلى اختراق المعلومات الحساسة والتجسس وبدون وجود الحراسة الإلكترونية يتطور الأمر ليصل في النهاية إلى الإرهاب الإلكتروني.

---

(4) Casey, E, Dijital Evidence Computer Crime 2005 San DI-ego ACADMIC PRESS, P 5. &" David Bainbridge- Introduction to computer law-third edition-Pit Man publishing2004" p.14.

(٥) د. خالد ممدوح إبراهيم، المرجع السابق، ص ٣٥٨. راجع أيضا:

"Chriss Reed, Internet Law- CAMPRIDGE UNIVERCITY PRESS". 2004. p13.

(٦) للمزيد من المعلومات يمكنكم الاطلاع على المرسوم الملكي الخاص بمكافحة الجرائم المعلوماتية الصادر برقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨ حيث كان أخر ولوج في ١٤٤٣/٥/٥ هـ:

"https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/"12

الفرع الثاني

خصائص الجريمة الإلكترونية:

تتميز الجرائم الإلكترونية بالعديد من المزايا غير الموجودة في الجرائم التقليدية، منها على سبيل المثال أنها جرائم عابرة للحدود، ومردّ ذلك إلى اعتمادها على الإنترنت الذي هو أيضاً عابر للحدود، وبالتالي يمكن للمجرم الإلكتروني أن يرتكب الجريمة في دولة، ويكون مقيمًا في دولة أخري تمامًا مثل التعدي على قواعد بيانات شركة أو سرقة بطاقات ائتمان، أو انتهاك حرمة الحياة الخاصة وتهديد الأفراد[٧].

ومن خصائص الجرائم الإلكترونية أيضا صعوبة إثباتها وصعوبة اكتشافها؛ فمعظم هذه الجرائم لا تترك أثرًا بعد ارتكابها[٨] وكذا يصعُب جدًا تحديد مكان وقوعها؛ نظراً لاتساع النطاق المكاني وكمية البيانات الكبيرة التي تتعامل فيها فضلاً عن سرعة ارتكاب الفعل الإجرامي حيث يستطيع المجرم الإلكتروني في لحظات معدودة سرقة كل كلمات المرور الموجودة في الجهاز المخترق ليس ذلك فحسب بل يستطيع أيضًا أن يحذف كل البيانات المهمة الموجودة على الجهاز كل ذلك في غضون ثوانٍ معدودة[٩].

والجدير بالذكر أن الجريمة الإلكترونية من الجرائم المستحدثة التي لم تكن معهودة من قبل، وبالتالي لا يوجد هناك مفهوم مشترك بين الدول سواء في تعريفها أو في العقوبات المترتبة عليها، ووقع الخلاف في تحديد مفهوم موحد لها، ونتج عن ذلك عدم وجود تعاون دولي كافٍ في مجال الجرائم الإلكترونية وإن وجدت مؤخرا العديد من

---

[٧] راجع د عبدالعال الدريبي، الأستاذ محمد صادق إسماعيل، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، الطبعة الأولي، القاهرة، ٢٠١٢، ص ٥٤.

[8] "Johan Eaton& jermy smithers A Managers Guide to information Technology, London, Philip Allan" 1982, p263.

[٩] راجع د. خالد ممدوح إبراهيم، حوكمة الإنترنت، المرجع السابق ص ٣٦٣ وأيضًا راجع د. هشام محمد فريد، بحث مقدم إلى مؤتمر القانون والكومبيوتر والإنترنت والذي عقد بدولة الإمارات، جامعة الإمارات العربية المتحدة خلال الفترة من ١ – ٣ مايو ٢٠٠٠.

المشروعات الناجحة في هذا المضمار منها على سبيل المثال مشروع الاتفاقية الأوروبية لجرائم الحاسب الآلي.

المطلب الثاني

صور للجرائم الإلكترونية في الوقت الحالي

ظهرت العديد من الجرائم التي تتم بشكل إلكتروني منها الجرائم التي تستهدف البيانات الموجودة والمخزنة على الكمبيوتر بشكل غير قانوني وقد تكون هذه البيانات خاصه بالأفراد أو الشركات أو الحكومات ويتم سرقتها أو حذفها أو إفشاؤها أيضا ظهرت جرائم يتم فيها اختراق أجهزة الحاسب الآلي وهدفها الوحيد هو تدمير كل البيانات المخزنة على جهاز الكمبيوتر ويكون الهدف في الغالب تدمير ملفات مهمة لشركات تجارية وتكون هذه الملفات إما ملفات إدارية أو ملفات مالية أو زرع برامج تخفي كل البيانات الموجودة على جهاز الكمبيوتر وتعرف باسم (الفدية) حيث يقوم المخترق بتشفير كل البيانات الموجودة على جهاز الكمبيوتر ويطلب مقابل فك التشفير مبلغ من المال جرائم متعددة منها سرقة البريد الإلكتروني، سرقة أسماء المستخدمين وكلمات المرور، تهديد الأفراد والمستثمرين وإفشاء أسرارهم التجارية.

ما يعرف بجرائم سلاسل التوريد حيث يتم اختراق شركة تبيع للمستخدمين وللشركات الأخرى برامج لأجهزة الكمبيوتر الخاصة بهم فيتم اختراق المصدر ومن ثم كل البرامج التي يتم بيعها للمستخدمين سواء أفراد أو شركات تكون ضحية سهلة للمخترقين ويتم قرصنة ألاف الأجهزة من ويكون المسؤول عن ذلك الشركة صاحبة البرامج.

المبحث الثاني

مفهوم جريمة هجوم النقرة الصفرية

انتشرت الهجمات الإلكترونية انتشاراً مخيفًا في الآونة الأخيرة، وتنتهج جميعها – في الغالب– نهجاً موحداً، وهو الاعتماد على عدم تحديث النظام الأمني لدي الضحية سواء كانت الضحية فردًا أو منظمه أو شركة أو جهة حكومية لا تراعي إجراءات السلامة والأمان الإلكتروني بتوفير أحدث برامج مكافحة الفيروسات وبرامج التجسس.

فيقوم المجرم الإلكتروني بإرسال رابط غير موثوق به أو بريد إلكتروني يحتوي علي ملفات تلفت انتباه الضحية مثل جعل الإيميل يبدو كأنه من أحد المديرين في الشركة أو يبدو كأنه من شركات عملاقة ذات أسماء رنانة أو يرسل له صوراً أو بيانات، فيدفعه الفضول إلى الضغط علي هذا الملف أو الرابط الملغوم، وفور الدخول علي الرابط أو فتح الملف الملغوم يتم فتح ثغرة في جهاز الضحية ويصبح التحكم بالكامل لدي جهاز الشخص المخترق فيستطيع أن يتحكم حرفياً بكل شيء علي سبيل المثال الدخول إلي وحدة التخزين الداخلية ونسخ كل محتوياتها وأيضاً معرفة كل كلمات المرور الموجودة علي الجهاز، معرفة كلمات السر لكل البطاقات المصرفية الموجودة علي الجهاز[١٠].

ليس ذلك فحسب، بل يستطيع المخترق تسجيل كل هذا حتي في حالة عدم وجود المخترق علي جهازه الخاص به؛ فالبرنامج الخبيث المستخدم في فتح الثغرات لدي

---

[١٠] راجع د. أحمد خليفه الملط، الجرائم المعلوماتية، القاهرة، دار الفكر الجامعي، ٢٠٠٥، ص٥٣٩.

وللمزيد من المعلومات راجع أيضاً د. إسراء جبريل رشاد مرعي، "الجرائم الإلكترونية: الأهداف الأسباب، طرق الجريمة ومعالجتها"، نشرت بواسطة المركز الديموقراطي العربي اخر ولوج كان في يوم ١٤٤٣/٨/٢٣

http://democraticac.de/?=35426

جهاز الضحية يقوم بتسجيل كل شيء حتي اذا تصادف عدم وجود المخترق علي جهازه، وتم تسجيل الدخول من الضحية في وقت أخر، يقوم بحفظ كل التحركات والأوامر والصور وكلمات المرور في شكل سجل، يستطيع المخترق أن يدخل إليها مره أخري لو صادف عدم وجوده لحظه فتح الضحية الجهاز الخاص به، بل وتسجيل كل الأصوات التي حدثت، والمكالمات التي أجرتها الضحية في كل الأوقات، طالما كان الجهاز متصل بشبكة الإنترنت.

قد يتساءل البعض ما فائدة برامج مكافحة الفيروسات التي يتم دفع الكثير من الأموال فيها ولماذا لا توقف مثل هذه الهجمات؟

وللإجابة على هذا التساؤل يجب أن نعرف أن المجرم الإلكتروني من مميزاته الذكاء والحرفية؛ وذلك لأنه يستخدم طريقه تسمي تقنية التشفير[١١].

المطلب الأول

آلية عمل تقنية التشفير (Encryption)

يستخدم المجرم الإلكتروني برامج مثل برنامج بايوفرست (Biofrost) أو برنامج بايزون ايفي (Piso Ivy) لإعداد ملف الهاكرز، ويقوم بدمجه مع صورة أو رابط أو ملف ، ثم يرسله للضحية ،وفور فتح الضحية له يتمكن المخترق في الحال من فتح الثغرة الإلكترونية في جهاز الضحية، أما لو كان لدي الضحية برنامج من برامج

---

[١١] المقصود بالتشفير في الأمن الإلكتروني: تحويل البيانات من تنسيق قابل للقراءة إلى تنسيق مشفر لا يمكن قراءة البيانات المشفرة أو معالجتها إلا بعد فك تشفيرها، ويستخدم الهاكرز نفس الطريقة ولكن بطريقة عكسية، عن طريق إخفاء برنامج التجسس بصيغة غير مقروءة، تجعل برامج الفيروسات لا تستطيع اكتشافها. للمزيد من المعلومات يمكنكم الاطلاع على هذا الموقع الإلكتروني حيث كان آخر ولوج في ١٤٤٣/٨/٢٣:

- https://me.kaspersky.com/resource-center/definitions/encryption

مكافحة الفيروسات مثل برنامج كاسبرسكاي (kasperskay) فسوف يكتشف مباشرة أن الملف المرسل له هو من الملفات الخبيثة ويرفض فتحه فما العمل إذن؟

يفهم المخترق جيداً طريقة عمل برامج مكافحة الفيروسات، وكيفية اكتشافها للبرنامج الخبيث أو ما يعرف بالـ (patch) الملف الملغوم فيقوم بعمليه اسمها التشفير، وهي أن يغير في خصائص الملف الملغوم الذي يتم إرساله إلي الضحية فيما يشبه المناورة الاحتيالية علي برنامج مكافحة الفيروسات؛ لإيهامه أنه ملف عادي ولا يحتوي علي أي ملفات خبيثة عن طريق دمجه فعلاً مع ملف عادي ليس به أي مشكلة؛ فبمجرد أن يفحص برنامج مكافحة الفيروسات الملف يراه ملفاً عادياً وليس فيه أي مشكلة؛ فيسمح للضحية بفتحه، وبمجرد فتحه مباشرة يتم تفعيل البرنامج الخبيث الموجود بداخله، ويتم فتح الثغرة في جهاز الضحية، والتي تسمح مباشرة بدخول المخترق إلى جهاز الكمبيوتر الخاص بالضحية أو لهاتفه المحمول.

لكن يبقي السؤال الذي يطرح نفسه كيف يعرف المخترق أن الضحية تستخدم برنامج مكافحة فيروسات أم لا؟ أو كيف يضمن أن مناورة التشفير الاحتيالية التي قام بها ستمر على برنامج مكافحة الفيروسات أثناء الفحص ولا يكتشفها؟ وللإجابة على هذا السؤال يجب أن نعرف جيداً أن برامج مكافحة الفيروسات ليست كلها بنفس القوة التي تمكنها من اكتشاف البرنامج المرسل للضحية، فبعضها يتمكن، وبعضها لا يتمكن، فما الحل إذن؟

الحل وللأسف أن كافة برامج مكافحة الفيروسات دون استثناء تضع على المواقع الخاصة بها روابط للفحص المجاني على الأجهزة؛ لتشجيع الناس على شرائها، وخاصه حين اكتشاف بعض الفيروسات الضارة على أجهزة المستخدمين تظهر لهم ذلك،

وتطلب منهم شراء البرنامج إذا رغبوا في إزالة الفيروسات الضارة والملفات الخبيثة الموجودة على الجهاز الخاص بيهم[١٢].

فماذا يفعل المخترق إذن؟ بعد ما يقوم المخترق بإعداد البرنامج الخبيث الذي يقصد به اختراق الضحية، يشرع في تشفيره لكي يخدع برنامج مكافح الفيروسات والبرامج الخبيثة، فيقوم بعرضه علي كل المواقع الخاصة ببرامج مضاد الفيروسات، فإذا تم اكتشافه من قبل هذه المواقع يعيد الكرة مره أخرى، ويشفره مره أخرى، ولكن بطريقه مختلفة إلى أن يصل في النهاية للنتيجة المرضية، وهي نجاحه في الاختبار بعدما تم فحصه من كل البرامج المضادة للفيروسات، والبرامج الخبيثة، ولم يتم اكتشافه حينها يرسله للضحية، وهو علي يقين تام أنه حتي لو موجود عند الضحية برنامج مكافح للفيروسات لن يتم اكتشافه أو يتم تنبيه الضحية بذلك؛ فيقع الضحية فريسة سهلة للمخترق.

وقد يظن البعض أن هذه العملية تستغرق العديد من الوقت، لكن في حقيقة الأمر عملية التشفير والفحص لا تستغرق إلا بضع دقائق، فلا يطول الأمر أبداً حتى تقع الضحية فريسة سهله للمخترق.

ورغم كل هذه الخطوات السابقة والطويلة في اختراق الضحية من تشفير، ومحاولة إرسال البرامج الخبيثة إلى الضحية الذي قد يدخل على الملفات الملغومة أو لا يدخل حتي يقع في النهاية فريسه للمخترق نجد أنها لا داعي لها على الإطلاق، وأن هناك

---

[١٢] للمزيد من التوضيح للفكرة يمكنكم الولوج إلى هذا الموقع الإلكتروني حيث به ما يقارب أكثر من عشرين إصدار تجريبي مجاني لأشهر برامج مكافحة الفيروسات بشكل مجاني وهناك نسخ تجريبية على كل برنامج (٦٠ يوم) يمكن لأي شخص الفحص المجاني للحاسب الخاص به، وكذلك يفعل الهاكرز حينما يعرض البرنامج المشفر الذي يريد به اختراق الضحية ليري هل سوف يتم اكتشافه أم لا ويظل يعيد الأمر إلى أن يتأكد تماما أن جميع برامج مكافحة الفيروسات لن تكتشفه فتتم عملية التشفير بنجاح ويكون برنامج التجسس جاهز للإرسال للضحية:
https://afdal10antivirus.com/best-free-antivirus

وسيلة حديثه تختصر كل هذا الجهد والوقت ولا تغامر أبداً باكتشاف أن هناك محاوله للاختراق أو التجسس، ولا تتطلب تدخلاً إيجابياً من الضحية بأي شكل من الأشكال؛ فلا يتم إرسال له رابط مخادع أو ملف ملغوم تم تشفيره أو أي طريقه من الطرق التي تستخدمها الجرائم الإلكترونية العادية في اختراق الضحية.

تُعرف هذا الطريقة بهجوم النقرة الصفرية أو هجوم الضغط الصفري، فما المقصود بهذه الطريقة الحديثة؟ وما آلية عملها حتى نوضح المسؤولية المدنية عنها؟ ومن المسؤول في النهاية عن التعويض المستحق للضحية الناتج عن الأضرار التي لحقت به جراء هذه الجريمة التي لم تكن معهودة من قبل؟ سوف نوضح كل هذا بالتفصيل في السطور القادمة.

المطلب الثاني

تعريف جريمة هجوم النقرة الصفرية وكيفية عملها

تعرف جريمة هجوم النقرة الصفرية بأنها: "هجوم يتم عن بعد على أحد الأجهزة الإلكترونية ولا يتطلب أي إجراء من مستخدمي هذه الأجهزة الإلكترونية، ويتم تنفيذ هذا الهجوم عن طريق الجو (OTA) ويكفي فقط أن يكون المستخدم من ضمن نطاق قناة الاتصال اللاسلكي"[١٣].

---

[١٣] نجد أن هناك شركات متخصصه في البحث عن الثغرات التي تستخدم لهجوم النقرة الصفرية والتي تبحث عنها وتشتريها بملايين الدولارات وتبيع هذه الثغرات في السوق السوداء، وتحصل مقابلها علي ملايين الدولارات؛ لأن بمجرد أن يحصل أي شخص علي الثغرة يستطيع بكل سهوله استغلالها والدخول علي النظام الخاص بالضحية ولكي أقرب الصورة للقارئ الثغرة تكون في نظام التشغيل ذاته بمعني أن يتم اكتشاف الثغرة في نظام تشغيل ويندوز ١١ (WINDOS 11) وهو نظام تشغيل خاص بأجهزة الكومبيوتر، معني ذلك أن أي شخص يستخدم نظام التشغيل الخاص بشركة مايكروسوفت يمكن اختراقه بسهوله، وبدون أي تصرف منه؛ لأن الثغرة موجوده بالفعل في جهاز التشغيل الذي يستخدمه هو وملايين المستخدمين، وبالتطبيق علي أجهزة الهاتف المحمول الذكية لك أن تتخيل أن

الواضح من التعريف أن كل الإجراءات التي يستخدمها المخترقون حتى يتم الإيقاع بالضحية غير موجودة في هذه الجريمة؛ فالضحية غير مطلوب منها أي إجراء على الإطلاق يكفي فقط أن تكون واقعة ضمن نطاق قناة الاتصال، بمعني أنها تستخدم الشبكة اللاسلكية التي يستخدمها المخترق.

ولتوضيح كيفية عمل جريمة هجوم النقرة الصفرية، يجب علينا أن نعرف أولاً أن كلاً من الهواتف النقالة وأجهزة الكمبيوتر المحمولة تحتوي على قنوات اتصال لاسلكية، مثل "(GSM أو LTE أو Wi-Fi أو Bluetooth أو NFC)"، يكفي فقط أن تكون أي من هذه القنوات مفتوحة، والتي بالفعل يستخدمها ملايين البشر بشكل يومي حتى يستطيع المخترق أن يمرر البيانات من خلال هذه القنوات مستغلاً الثغرة الموجودة في نظام التشغيل، والتي تم اكتشافها من قبل، ويرسل من خلالها برنامج تجسس معد خصيصاً لذلك حتي يتناسب مع طريقه الاختراق هذه حيث يقوم البرنامج بمجرد الدخول عبر الثغرة المكتشفة مسبقاً من خلال أحد قنوات الاتصال بتنصيب نفسه مباشرة، ويصبح الجهاز الخاص بالضحية تحت السيطرة الكاملة للمخترق يمارس كل الوسائل الخبيثة التي تم ذكرها في الجريمة الإلكترونية العادية من الدخول على الملفات الموجودة في الجهاز والصور، وسرقة كلمات المرور، واختراق البريد الإلكتروني، ونقله بالكامل، وحذف محتواه بل تسجيل كل ما يدور في جهاز الضحية من مكالمات صوتيه أو مكالمات عبر تقنية الفيديو بمعني آخر أصبح المخترق متحكم تحكماً كاملاً بجهاز الضحية[١٤].

تكون الثغرة في نظام التشغيل اند رويد الذي يستخدمه ملايين البشر في وقتنا هذا معني ذلك أن كل الهواتف الذكية، التي تستخدم نظام اند وريد موجود بها هذه الثغرة، ويسهل اختراقها بسهولة، ومن هذه الشركات التي تبحث عن هذه الثغرات، وتبيعها في السوق السوداء شركه تدعي Zerodium.

[١٤] للمزيد من المعلومات يمكنكم الاطلاع على هذا المقال بعنوان: "هجوم النقرة الصفرية الهجوم الذي لا يقهر"، المنشور على الموقع الإلكتروني التالي: آخر ولوج كان في يوم ١٤٤٣/٨/٢٣:
https://www.computer-wd.com/2021/10/zero-click- attack.html

المطلب الثالث

هل هناك حالات موثقة لجريمة هجوم النقرة الصفرية؟

قد يظن البعض أن ما سبق ذكره ضرب من خيال الباحث، ولا ألومه في ذلك فهل من المتصور فعلاً أن يمر الشخص بأحد الأسواق التجارية أو يستخدم شبكة من شبكات الاتصال اللاسلكية أو يكفي معرفة الشبكة اللاسلكية التي يستخدمها في منزله أو في عمله، ويجد نفسه مباشرة ضحية من ضحايا الجرائم الإلكترونية سيئة السمعة والمعروفة بهجوم النقرة الصفرية؟

في حقيقة الأمر الجواب نعم، وإن كان المخترقون الذين يستخدمون هذه الطريقة لا يستخدمونها عادةً للأهداف السهلة، ولا مع عامة الناس، بل يستخدمونها لكبار الشخصيات العامة، كالوزراء، رؤساء الشركات العملاقة، المعارضين السياسيين، الصحفيين، لكن هذا لا يمنع أن كل شخص منا عُرضة للهجوم الصفري متى قرر المخترق ذلك.

وبالفعل هناك العديد من الحالات التي تم توثيقها بواسطة خبراء مختصين منها علي سبيل المثال قبل أيام قليله أعلنت شركة أبل (APPLE) أنها قامت بإجراء تحديث أمني لكل الأجهزة التي تتبعها بعدما تم اكتشاف ثغرة تم استخدامها في هجوم الضغط الصفري واتهمت شركة(أن أي أو) (NSO) الإسرائيلية والتي تستخدم أسوء برنامج تجسس علي الإطلاق يدعي بيجاسوس أو أداة المراقبة بيجاسوس (PEGASUS) وهو برنامج طورته شركة (أن أي أو) الإسرائيلية يستخدم في هجوم النقرة الصفرية حيث قامت الشركة الإسرائيلية باستغلال ثغرة في نظام شركة أبل (APPLE) عبر تطبيق يستخدم للدردشة يسمي (I MESSAGE) وهو برنامج موجود ضمن نظام التشغيل لمستخدمي شركة (أبل) فكل شخص يوجد عنده هذا التطبيق فهو في مرمي هجوم النقرة الصفرية بصورة مباشرة.

ووجد الباحثون التقنيون بشركة (أبل) آثاراً دالة على هجوم النقرة الصفرية على أجهزة أبل والمعروفة ب (فورسيدإنتريFORCEDENTRY) موجوده من شهر فبراير الماضي، ولم يتم اكتشافها إلا مؤخراً، وبالتالي كل من يستخدمون أجهزة أبل وقبل التحديث الأمني كانوا عُرضةً للاختراق وفق تقنية هجوم النقرة الصفرية من الشركة الإسرائيلية NSO، ومن الحالات الموثقة أيضاً ما تم اكتشافه في شركة تطوير البرامج المعروفة سيتزن لاب (Citizen Lab)[١٥] في سبتمبر الماضي من حالات تم فيها استخدام أداة المراقبة (بيجاسوس) عبر هجوم النقرة الصفرية على بعض الأهداف التي تم فيها تطوير ملف بي دي أف (PDF) قادر على تنصيب نفسه بنفسه.

أيضاً تم استخدام الطريقة ذاتها في عام ٢٠١٩م عبر تطبيق واتس أب، باستخدام هجوم النقرة الصفرية؛ حيث تم تثبيت برنامج التجسس على الأجهزة، يتم تفعيله فور الاتصال بهم، ودون أي إجراء من الضحية.

المطلب الرابع

طرق الحماية من هجوم النقرة الصفرية

حتى الساعة، ونظراً للطريقة الخبيثة التي ينتهجها المخترقون والقائمة على استغلال الثغرات الموجودة بأنظمة التشغيل بالأجهزة الإلكترونية، فإنه من العسير جداً الجزم بحماية مؤكدة من هذه الهجمات، بيد أن هناك نصائح عدة بالغة الأهمية ومنها:

---

[١٥] Citizen Lab من المعامل الموجودة بجامعة تورنتو في كندا والمختص بضوابط المعلومات ومراقبة مسائل التجسس على الشركات والتي تؤثر على أمن وسلامة الإنترنت وتهدد حقوق الإنسان، وذلك من خلال باحثين تقنيين متخصصين في مجال الحاسب الآلي تحت قيادة البروفسور روبرت ديبرت، وحصل هذا المعهد على عديد من الجوائز العالمية لدوره الأخلاقي في مجال الإنترنت.

– توخي الحذر عند شراء البرامج ومحاولة شراء البرامج الأصلية قدر الإمكان وعدم شراء البرامج المقلدة، وكذا توخي الحذر عند نقل البرامج والملفات من الأشخاص فقد تكون مشتملة على برامج للتجسس.

– استخدام برامج لمكافحة الفيروسات وتحديثها بشكل دائم؛ لأنها تعد حائط صد للمخترقين والمخربين حتى لو ثبت عدم جدواها مع هجوم النقرة الصفرية؛ إلا أنها في ظل التحديثات قد تتمكن من كشف الهجوم قبل أن يتم الدخول إلى جهاز الضحية.

– عدم استخدام الشبكات العامة الغير موثوقة؛ لأنها تعد من أسهل الطرق لاختراق الأجهزة الذكية عن طريق هجوم النقرة الصفرية.

– ثمة شيء آخر أكثر أهمية، وهو المحافظة باستمرار على التحديثات الأمنية التي ترسلها الشركات لمستخدميها، أمثال شركة أبل ومايكروسوفت؛ لأن هذه التحديثات– غالباً– تقوم بسد ثغرات تم اكتشافها قد يستخدمها المخترقون في هجوم النقرة الصفرية، لذلك يلزم عمل التحديثات الأمنية بشكل دوري.

– وأيضاً استخدام البرامج التي تغير من ال أي بي I P ADRESS أو التي تخفي العنوان الخاص بك علي الإنترنت مثل برامج ال VPN والتي تخفي هويتك عبر الإنترنت.

المبحث الثالث

الأساس القانوني للمسؤولية المدنية الناجمة عن جرائم هجوم النقرة الصفرية

تمهيد:

أوجب القانون المسؤولية بشكل عام سواء كانت مسؤولية عقدية أو مسؤولية تقصيرية، وذلك لتعويض المتضرر عن الضرر الذي لحق به، ولكن تختلف كل من المسؤوليتين في سبب نشوء كل منهما، فالمسؤولية العقدية تنشأ عن الإخلال بالتزام

عقدي، أما المسؤولية التقصيرية فتنشأ بسبب الإخلال بواجب قانوني أو واجب عام، ونظراً لخصوصية جريمة هجوم النقرة الصفرية ينبغي علينا أولاً أن نوضح نقاط عدة حتى تتجلى الصورة بوضوح للقارئ[١٦]:

أولاً: ذكرنا سابقاً آلية عمل المخترق في ضوء هجوم النقرة الصفرية، وأوضحنا أنه يقوم بفتح ثغره في نظام التشغيل الخاص بالضحية، ثم يقوم بإرسال برنامج التجسس الخبيث إلى جهاز الحاسب الشخصي أو الهاتف الذكي الخاص بالضحية.

ثانياً: المقصود بنظام التشغيل هنا هو البرنامج الذي تم تنصيبه وتثبيته على الجهاز سواء كان حاسب شخصي مثال لذلك نسخه الويندوز التي يتم شرائها من شركة مايكروسوفت وتضم البرامج المهمة التي تمكن جهاز الكمبيوتر من أداء وظائفه وتعرف بنظام التشغيل ويندوز (windows) ويتم تنصيبها على جهاز الكمبيوتر الشخصي أو المكتبي، أو البرنامج الذي تم وضعه على الأجهزة الذكية لتشغيلها مثال لذلك نظام تشغيل الهواتف الذكية في شركة أبل (APPLE) ويسمي آي أو إس (iOS)[١٧]، وتعمل به أجهزة شركة أبل مثل الآيفون (iPhone) والآيباد (I pad) والأيبود (iPod) أو نظام تشغيل الهواتف التي تعمل بنظام اندرويد (Android)[١٨]، وتفعله شركات

---

[١٦] للمزيد من المعلومات راجع د فاروق علي الحفناوي، موسوعة قانون الكومبيوتر ونظم المعلومات، الكتاب الثاني، الجزء الأول، عقود البرمجيات، دار الكتاب الحديث، ٢٠٠٩، ص ٩٨٠.

[١٧] يعتبر نظام (IOS) نظام تشغيل حيث عرف في البداية باسم (iphone osx) وكان هذا الاسم السابق للنظام وظهر هذا النظام في عام ٢٠٠٧ كنظام تشغيل قامت بصنعه شركة أبل من أجل هاتف الأي يفون الخاص بها . للمزيد من المعلومات يمكنكم الاطلاع على هذا الموقع الإلكتروني حيث كان آخر ولوج في: ١٤٤٣/٨/٢٤:

https://mawdoo3.com/%D9%85%D8%A7_%D9%87%D9%88_%D9%86%D8%B8%D8%A7%D9%85_IOS

[١٨] هو نظام تشغيل للأجهزة المحمولة مبنى على نسخة معدلة من نواة نظام تشغيل لينكس الشهير، وبعض البرامج مفتوحة المصدر؛ وهي برامج يسمح مطورها لأي مطور آخر أو مجتمع تقني على تعديل كتابة ترميزها أو إضافة سطور برمجية جديدة لها، طالما تم الالتزام بعدة شروط محددة مسبقاً،

أخرى على هواتفها المحمولة مثل شركة سامسونج (Samsung) وشركة شاومي (XIAOMI).

ثالثاً: من صور التعدي على أنظمة التشغيل استغلال نقاط الضعف الموجودة فيها، والقيام بفتح ثغرات تسمح للمخترقين بالولوج إليها، وتنصيب برامجهم الخبيثة، والقيام بإدخال بيانات لم تكن موجودة من قبل أو يقومون بإتلاف المعلومات التي تحتويها هذه البرامج والملفات المخزنة عليها، ومع تطور التقنية الحديثة تطورت أيضاً طرق المخترقين في هذا الأمر.

المطلب الأول

المسؤولية العقدية عن أضرار هجوم النقرة الصفرية

تقوم المسؤولية العقدية بناء على إخلال أحد الطرفين بالتزامه الناشئ عن عقد بين كل من الدائن والمدين، وحتى تقوم المسؤولية العقدية لابد من توفر مجموعة من الشروط وهي:

– "أن يكون العقد المبرم بين الطرفين عقداً صحيحاً مستوفياً كافة الأركان والشروط، ويلتزم بها الطرفان كلاهما، ويشترط أيضاً أن يكون العقد بين المسؤول عن الضرر وبين المتضرر نفسه"[١٩].

– "وأن يخل أحد طرفي العقد بالتزامه الموجود في العقد"[٢٠].

مثل عدم استخدام النظام في أغراض إجرامية أو تعريض أي فرد للخطر للمزيد من المعلومات يمكنكم الولوج الي هذا الموقع الإلكتروني حيث كان أخر ولوج في ١٤٤٣/٨/٢٤:
https://www.alrab7on.com

[١٩] راجع د. أنور سلطان، مصادر الالتزام في القانون المدني الأردني، "دراسة مقارنة بالفقه الإسلامي"، دار الثقافة للنشر والتوزيع، ٢٠٠٧م، ص ٢٨٦.

[٢٠] راجع د. صلال حسين علي الجبوري، "تعويض الضرر الأدبي في المسؤولية المدنية"، دراسة مقارنة، دار الفكر الجامعي، ٢٠١٤م، ص ٤٣.

وبناء علي ما سبق ذكره اذا كان المتضرر قد تعاقد مع إحدى الشركات صاحبة البرامج التشغيلية لجهاز الكمبيوتر الشخصي مثل شركة مايكروسوفت، والتي تبيع نظام ويندوز، أو اشتري الشخص هاتف محمول تم تحميل أحد البرامج التشغيلية عليه والتي تبيعها شركة أبل مع هواتفها المحمولة والمعروفة بنظام IOS ، أو شركة (سامسونج) التي تبيع مع أجهزتها النقالة نظام تشغيل أندرويد، وكل من هذه الشركات ملزمه بشكل دوري وفقاً لشروط الخدمة، وشروط العقد بينها وبين المستخدمين بإرسال تحديثات أمنية لسد الثغرات التي يتم اكتشافها، وحماية كل من الحواسيب الشخصية والهواتف المحمولة من الاختراق؛ فإن المسؤولية التعاقدية تقوم إذا أخل أحد الطرفين بالتزامه، فلو وقع ضرر بناء على هذه البرامج للشخص المتضرر عن طريق فتح ثغرات أمنية في هذه الأنظمة تكون الشركة المصنعة لهذه البرامج قد أخلت ببنود العقد بينها وبين المستخدمين، وبالتالي هي المسؤولة عن تعويضهم عن الأضرار التي لحقت بهم.

الفرع الأول

أركان المسؤولية العقدية

الركن الأول- الخطأ العقدي:

الخطأ العقدي مضمونه هو عدم تنفيذ أحد طرفي العقد التزامه المنصوص عليه في العقد أو تنفيذه تنفيذا متأخرا أو معيباً.

وتناوله القانون المصري؛ حيث نص على أنه: إذا استحال على المدين أن ينفذ الالتزام، حكم عليه بالتعويض لعدم الوفاء بالتزامه، ما لم يثبت أن استحالة التنفيذ قد نشأت عن سبب أجنبي لا يد له فيه"[٢١].

---

[٢١] المادة رقم (٢١٥) من "القانون المدني المصري"، وهي مادة جوهرية في كل من المسؤولية العقدية والتقصيرية، ولذلك وضعت في الباب المخصص لآثار الالتزام. للمزيد من المعلومات راجع

لم يُعرّف المنظم السعودي الخطأ العقدي ولكن وفقاً للأحكام الشرعية المعمول بها داخل "المملكة العربية السعودية"؛ فإن القضاء السعودي اعتمد في أحكامه على أحكام الشريعة الإسلامية في مبدأ الالتزام بالعقود، وعدم الإخلال بشروطها من الطرفين معتمداً علي قوله تعالى: "يا أيها الذين آمنوا أوفوا بالعقود"[٢٢]، لذلك أوجب الفقهاء علي أطراف العقد أن يفي كل منهم بالتزاماته الموجودة في العقد، وإلا ففي حالة عدم التنفيذ كان المخل بالتزامه مستوجباً الضمان، وهذا ما ذهبت إليه محكمة الاستئناف السعودية في أحكامها حيث نصت على أن: "العقد شريعة المتعاقدين، والمسلمون على شروطهم[٢٣] وفي حالة إخلال أحد الطرفين بالتزامه يلتزم بتعويض الطرف الأخر".

وهو أيضاً ما ذهب إليه مجلس القضاء الأعلى السعودي في حكمه الصادر في ١٤٢٥هـ في قضية ملخصها أن شخصاً قام باستئجار سيارة، وارتكب حادث، وقدرت التلفيات التي أصابت السيارة المؤجرة بمبلغ ٣٠ ألف ريال سعودي؛ فألزمته بمبلغ التعويض؛ لأن الحادث كان بسبب خطئه[٢٤].

المستشار/ منير رياض حنا، المسؤولية المدنية للأطباء والجراحين، في ضوء القضاء والفقه المصري، دار الفكر الجامعي، ٢٠١٤م، ص ١١٢ ،١١٣.

[٢٢] القرآن الكريم، سورة المائدة، أية رقم ١.

[٢٣] حكم محكمة الاستئناف السعودية الصادر في ١٤٣٤/١١/٤هـ، رقم (٣٤٣٤٩١٠٤)، في الدعوى الصادرة في ٢٢ /١٤٣٤/٨هـ، رقم (٣٣٦٨٣٤٣٠)، وصك رقم (٣٤٣٠٢١١٦)، مجموعة الأحكام القضائية لعام ١٤٣٤هـ، المجلد السابع، ص ١٥٣

[٢٤] حكم مجلس القضاء الأعلى السعودي الصادر في ١٤٢٥/١٠/٢٣هـ، رقم (٣٣/١٥١)، مدونة الأحكام القضائية، الإصدار الأول، إصدار الإدارة العامة لتدوين ونشر الأحكام بوزارة العدل، ١٤٢٨هـ –٢٠٠٧م، ص١٠٦.

وأيضاً تناولته وثيقة الكويت[٢٥] حيث نصت على أن: "الحقوق التي ينشئها العقد، فتثبت فور انعقاده أيضاً، ويجب على كل من الطرفين تنفيذ ما أوجبه العقد عليه منها"، وأيضاً في الوثيقة ذاتها نصت على أنه: " يجب تنفيذ العقد طبقا لما اشتمل عليه وبطريقة تتفق مع ما يوجبه حسن النية"[٢٦].

وأيضاً ما تناوله القانون المدني الكويتي[٢٧] عند تعذر تنفيذ الالتزام عيناً، أو التأخير فيه، جيب على المدين تعويض الضرر الذي لحق الدائن بسبب ذلك، ما لم يثبت المدين ان عدم التنفيذ أو التأخير كان لسبب أجنبي لا يد له فيه.

إذا أمعنا النظر في المواد القانونية السابقة سوف نجد أننا لكي نكون بصدد خطأ عقدي لابد أن يتوفر شروط معينة، أولها أن يتحقق عدم تنفيذ الالتزام بشكل كلي أو بشكل جزئي أو يكون التنفيذ متأخراً عما تم الاتفاق عليه في العقد، والشرط الثاني لابد أن يكون الإخلال في تنفيذ الالتزام ناتج عن خطأ شخصي من المدين، ويختلف المعيار المعتمد في تقدير الخطأ العقدي علي حسب طبيعة الالتزام الناشئ عن العقد إذا كان الالتزام بتحقيق نتيجة أم بذل عناية؛ فإذا كان الالتزام تحقيق نتيجة لا تبرأ ذمة المدين إلا بتحقيق النتيجة محل الالتزام، أما اذا كان الالتزام ببذل عناية يكفي أن يقوم المدين ببذل العناية المطلوبة لتحقيق التزامه.

ومن صور الخطأ العقدي، وبناء على ما سبق ذكره من آلية عمل المخترقين وفق نظام هجوم النقرة الصفرية إن الشركات المنتجة والمصنعة لبرامج التشغيل ينبغي عليها وفقاً لبنود العقد بينها وبين العميل أن تسلمه هذه البرامج خالية من العيوب قادرة علي

---

[٢٥] المادة رقم (٢٣٧) من وثيقة الكويت وللمزيد من المعلومات راجع "وثيقة الكويت للنظام الموحد لدول مجلس التعاون لدول الخليج العربية"، الرياض، الأمانة لعامة، الطبعة الثالثة، ١٤٣٢هـ-٢٠١١م، ص ٤٧.

[٢٦] المادة رقم (٢٣٨) من وثيقة الكويت.

[٢٧] المادة رقم (٢٩٣) من القانون المدني الكويتي.

القيام بعملها علي أكمل وجه وألا يكون بها فيروسات أو برامج خبيثة أو بها ثغرات أمنيه تمنح القدرة للمخترقين على الولوج إلى هذه الأنظمة معرضه خصوصية المستخدمين للانتهاك، سواء بسرقة محتويات الأجهزة المملوكة لهم أو حذف محتوياتها أو استغلالهم وابتزازهم أو سرقه محتويات البريد الإلكتروني أو حذف مكوناته أو سرقة كلمات السر الخاصة بهم أو الخاصة بحسابتهم المصرفية ...الخ

الركن الثاني– الضرر العقدي:

تقوم المسؤولية العقدية على عدة أركان، أولها: الخطأ العقدي، وثانيها: الضرر، والذي يُعدّ حجر الزاوية لقيام المسؤولية العقدية فبدونه لا توجد مسؤولية عقدية مهما كان الخطأ جسيماً[٢٨].

وتعريف الضرر هو: "الأذى الذي يصيب الشخص نتيجة المساس بمصلحة مشروعة له أو حق من حقوقه"[٢٩]، ويشترط في الضرر الموجب للتعويض في الموجب للتعويض في المسؤولية العقدية أن يكون محققاً ومباشراً ومتوقعاً؛ فيجب أن يكون الضرر قد وقع بالفعل أو أن يكون مؤكد الوقوع في المستقبل فلا يكفي احتمالية وقوع الضرر بل يجب أن يكون الضرر مؤكد الوقوع.

ويشترط أيضاً أن يكون الضرر مباشراً أي أن يكون نتيجة لعدم وفاء الشخص بالتزامه أو أن يكون متأخراً في الوفاء به وفي الالتزامات العقدية المدين لا يسأل إلا عن الضرر المباشر المتوقع وقت التعاقد، ومن شروط الضرر أيضاً أن يكون متوقع أي الذي يمكن توقعه في العادة عند إبرام العقد، فإذا كان الضرر غير متوقع ولم تنصرف إليه إرادة المتعاقدين؛ فلا يوجد تعويض عنه.

---

[٢٨] للمزيد من المعلومات راجع د. أمجد محمد منصور، النظرية العامة للالتزامات (مصادر الالتزام، ط ١ دار الثقافة عمان، ٢٠٠٩، ص ٢٢٥.

[٢٩] د. أنور سلطان، مصادر الالتزام في القانون المدني الأردني، دراسة مقارنة بالفقه الإسلامي، دار الثقافة للنشر والتوزيع، ٢٠٠٧م، ص ٦٤.

لكن يجب أن نلاحظ أنه أحياناً لا ينَفذ المدين التزامه، وفي الوقت نفسه لا يصيب الدائن أي ضرر، فالعبرة هنا بوقوع الضرر الفعلي، ويكون عبء الإثبات على من يدعي وقوع الضرر وهو في هذه الحالة الدائن، وقد يكون الضرر ضرراً ماديا أو ضرراً أدبياً، فالضرر المادي هو ما يصيب الإنسان في جسمه أو ماله والضرر المعنوي هو ما يصيب الإنسان في سمعته.

وهذا ما جاء في القانون المدني المصري عن الضرر حيث نص على أنه: " كل خطأ سبب ضرراً للغير يلتزم صاحبه بالتعويض "[٣٠]، كما تتطرق إلى الحديث عمّا يشمله التعويض عن الضرر، "ويشمل التعويض ما لحق الدائن من خسارة وما فاته من كسب"[٣١]، ونص أيضاً على التعويض عن الضرر الأدبي، "ويشمل التعويض الضرر الأدبي ولكن لا يجوز في هذه الحالة أن ينتقل إلى الغير إلا إذا تحدد بمقتضي اتفاق أو طالب الدائن به أمام القضاء"[٣٢]، وتحدث القانون الفرنسي عن الضرر حيث نص على أن: "كل فعل أياً كان يقع من الإنسان ويحدث ضرراً بالغير يلزم من وقع هذا الفعل بخطئه تعويض ذلك الضرر"[٣٣]، وبناء علي ما سبق ذكره عن الآلية التي يعمل بها المخترقون وفق هجوم النقرة الصفرية نجد أن هناك ضرراً كبيراً يلحق بالمستخدم أو العميل الذي تعاقد مع الشركة لشراء البرنامج التشغيلي لجهازه الشخصي أو لهاتفه المحمول فوجد نفسه ضحية نتيجة عدم تنفيذ الشركة التزامها بالمحافظة علي البرنامج خالياً من الثغرات التي يستغلها المخترقون مستخدمي هجوم النقرة الصفرية لتنفيذ مخططهم، وقد يكون الضرر مادياً إذا أصابوا جهازه الشخصي بضرر فترتب على ذلك

---

[٣٠] المادة (١٦٣) من القانون المدني المصري.

[٣١] المادة (٢٢١) من القانون المدني المصري.

[٣٢] المادة (٢٢٢) من القانون المدني المصري.

[٣٣] المادة (١٣٨٢) من القانون المدني الفرنسي.

مسح محتوياته أو إتلافه أو تقييد المعلومات الموجودة عليه وطلب الفدية[٣٤] أو سرقة كلمات المرور الموجودة على جهازه، والتي يستخدمها لحساباته المصرفية، أو سرقة حسابه البنكي كل هذه أضرار مادية تصيب الشخص، وقد يكون الضرر معنوياً يصيبه في سمعته بانتهاك خصوصيته، وتسريب أخبار عنه بناء على ما وجدوه في جهازه وهاتفه ونشر أسراره.

الركن الثالث– علاقة السببية بين الخطأ العقدي والضرر:

تعد علاقة السببية الركن الثالث في المسؤولية العقدية بحيث لا تقوم المسؤولية العقدية بدون علاقة السببية؛ فقد يوجد الخطأ العقدي وأيضاً يتحقق الضرر، ولكن لا توجد علاقة سببية بين الخطأ العقدي والضرر بالتالي لا توجد مسؤولية عقدية.

إذاً، لقيام المسؤولية العقدية لابد أن يقوم الدائن بإثبات وجود خطأ عقدي ارتكبه المدين، وأن هناك ضرراً لحق به بسبب هذا الخطأ، وبمجرد إثبات الدائن وجود الخطأ العقدي، وأيضاً إثبات الضرر تكون علاقة السببية هنا مفترضه بمعني أن الأصل أن هناك علاقة بين الخطأ والضرر إلا لو أثبت المدين عكس ذلك، وإذا طبقنا الأمر على هجوم النقرة الصفرية لابد أن يثبت المدين، وهو المستخدم حدوث خطأ عقدي، ويتأتى ذلك أولاً بإثبات أن هناك ثغرة أمنية في نظام التشغيل مكنت المخترق من اختراق جهازه وفق هجوم النقرة الصفرية، ثم يثبت الضرر الذي لحق به بسبب وجود مثل هذه الثغرات في نظام التشغيل التي تعمل بها أجهزته سواء الحاسب الشخصي أو الهاتف الذكي، وتجدر الإشارة إلى أن مسألة إثبات علاقة السببية في هجوم النقرة الصفرية من

---

[٣٤] فيروس الفدية يعد من أحد أسوء البرامج الخبيثة على الإطلاق ويعرف ب Ransomware حيث إذا أُصاب الجهاز الخاص بالمستخدم يعمل على تشفير كافة الملفات الموجودة فيه، ويمنع المستخدم من الوصول إليها إلا بعد دفع فدية مادية، وحينما يصيب الجهاز تظهر رسالة طلب الفدية، وكيفية سدادها حتى يقوم المخترق بفك التشفير على الجهاز وتمكين المستخدم من استعادة ملفاته المهمة مرة أخرى.

المسائل الصعبة والمعقدة، إذ إن عملية الاختراق وتنفيذ كافة المهام الخبيثة للمخترق قد تتم بالكامل دون أن يدري المستخدم أصلاً أنه واقع تحت سطوة هجوم النقرة الصفرية؛ نظراً للآلية الخطيرة التي تعمل بها، وفور انتهاء المخترق من جريمته، فإنه بإمكانه حذف ملف التجسس الذي مكنّه من اختراق العميل دون ترك أي أثر على جريمته.

الفرع الثاني

الأساس القانوني لقيام المسؤولية التعاقدية

من الإضرار الناشئة عن هجوم النقرة الصفرية

بادئ ذي بدأ، يتوجب علينا أن نعرف أن البرامج الإلكترونية التي يستخدمها العملاء، ويضعونها على أجهزتهم سواء الحواسيب الشخصية أو الهواتف النقالة تكون محلاً للتعاقد بين طرفي العلاقة التعاقدية، فالطرف الأول قد يكون المنتج لهذه البرامج أو الموزع لها، أو قد يكون بائعاً لها والطرف الثاني المقابل له في العلاقة التعاقدية هو العميل، ويترتب على ذلك إلزام الطرفين كليهما بالتزامات متقابلة، فالطرف الأول (المنتج، الموزع، البائع) يكون ملتزماً بتسليم منتج سليم ليس معيباً، ويُلزَم الطرف الثاني (العميل) بدفع سعر المنتج في الموعد المتفق عليه في العقد الإلكتروني.

فإذا قام المستخدم بشراء هذه البرامج الإلكترونية من الشركة المنتجة أو الموزعين المعتمدين لدى الشركة أو بائعيها، واكتشف بعد ذلك أن هذا المنتج معيب يحتوي على ثغرات أو تم اختراقه بسبب ثغرات في هذا المنتج الخاص بالشركة، تقوم المسؤولية التعاقدية ويحق له الرجوع على الشركة أو أي شخص تابع لها مثل: (المنتج، الموزع، المورد، البائع) يكون قد باع له هذا البرنامج المعيب بناء على إخلاله بما جاء في العقد من التزامات وبناء على ذلك، فإن المسؤولية تقع على كاهل بائع برنامج التشغيل الإلكتروني من عدة جوانب منها:

الغصن الأول- برامج التشغيل الإلكتروني وضمان العيوب الخفية:

من الالتزامات التي يرتبها عقد البيع علي البائع: أن يكون الشيء المبيع خالياً من العيوب حتي يقوم المشتري باستخدام المبيع الاستخدام الأمثل الذي يمَكنه من الحصول علي كافة مميزاته، أما إذا كان هناك ما يمنع ذلك بوجود عيب في الشيء المبيع يمنع المشتري من استخدامه للشيء المبيع أو ينتقص من قيمته أو يسبب له الأضرار يعتبر هذا عيباً موجباً للضمان، ويعتبر أيضاً من العيوب الخفية التي لو كان المشتري على علم بها قبل الشراء لما أقدم علي شراء هذا المنتج، وقد عالج القانون المدني هذه المشكلة ووضع لها نصوصا قانونية منها:

ما نص عليه القانون الفرنسي على أن: "البائع يكون ملزماً بأن يضع تحت تصرف المشتري منتجاً مطابقاً للمنتج المبيع وذلك وفق الاشتراطات المنصوص عليها في الوقت والمكان المتفق عليه"[٣٥].

وأيضاً ما ذهب إليه القانون المدني المصري حيث نص على أن: "يكون البائع ملزماً بالضمان إذا لم يتوافر في المبيع وقت التسليم الصفات التي كفل المشتري وجودها فيه، أو إذا كان بالمبيع عيب ينقص من قيمته أو من نفعه بحسب الغاية المقصودة مستفادة مما هو مبين في العقد أو مما هو ظاهر من طبيعة الشيء، أو الغرض الذ أعد له، ويضمن البائع هذا العيب لو لم يكن عالما بوجوده"[٣٦].

وهناك شروط عدة شروط يجب توافرها في العيب، منها أن يكون خفياً لا يعلمه المشتري، وأيضاً يكون العيب قديما ومؤثراً.

ومما لا شك فيه، أنه إذا كان برنامج التشغيل الإلكتروني به ثغرات تتيح للمخترقين الدخول عبرها محدثين الأضرار بأجهزة المستخدم تعتبر من العيوب الخفية التي

---

[٣٥] نص المادة (١٦٠٤) من "القانون المدني الفرنسي".

[٣٦] نص المادة (٤٤٧) من "القانون المدني المصري".

يصعب للمستخدم الكشف عنها، وهذا العيب ليس وليد اللحظة بل هو قديم ومؤثر، وذلك لأنه عرّض المستخدم للوقوع كضحية لمخترقي هجوم النقرة الصفرية، وبالتالي تلتزم الشركة بتعويض المستخدم عما لحق به من أضرار، وفي حال تحقق كافة هذه الشروط، فإنه يحق للمشتري أن يرد الشيء المبيع أو أن يطالب بإنقاص الثمن مع تعويضه عما لحق به من ضرر إذا توافرت شروط المسؤولية العقدية .

الغصن الثاني– برامج التشغيل الإلكتروني ومبدأ حسن النية في العقود:

الأصل العام في كل العقود سواء العادي منها أو الإلكتروني أنها تقوم على مبدأ حسن النية، وبالتالي يجب أن ينفذ كل طرف من أطراف العقد التزاماته وفق مبدأ حسن النية، ومن ثم يجب علي مقدم برامج التشغيل الإلكتروني أن يكون أميناً مع المستخدم الذي قام بشراء البرامج لاستخدامها والحصول علي مميزاتها، فيجب أن تكون خالية من الثغرات التي قد يستغلها المخترقون في تنفيذ هجماتهم الصفرية علي المستخدمين مسببين لهم أضرار عدة، فإذا أثبت المتضرر أن الشركة المنتجة للبرامج تعاملت بسوء نية، أصبح من حقه المطالبة بالتعويض وتتوافر المسؤولية العقدية.

الغصن الثالث– برامج التشغيل الإلكتروني وقوانين "حماية المستهلك":

من الممكن قيام المسؤولية التعاقدية على أساس قوانين "حماية المستهلك" التي نظمتها العديد من الدول وعلى سبيل المثال "المشرع الفرنسي والمصري والسعودي"، ولكن قبل أن نتطرق إلى هذه التشريعات وجب علينا أولاً تعريف من هو المستهلك، وهل يعتبر ضحية الضرر مستهلكاً حتى يستفيد من قوانين حماية المستهلك؟

وقد عرف المشرع المصري المستهلك؛ حيث نص على أنه: "كل شخص يقدم إليه أحد المنتجات لإشباع احتياجاته الشخصية أو العائلية أو يجري التعامل أو التعاقد معه

بهذا الخصوص"[٣٧] كما عرفه المشرع الفرنسي بأنه: "من يقوم باستعمال السلع والخدمات لإشباع حاجياته الشخصية وحاجيات من يعولهم، وليس بهدف إعادة بيعها أو تحويلها أو استخدامها في نطاق نشاطه المهني"[٣٨].

نستنتج من التعريفات السابقة أن المستهلك هو ذلك الشخص الطبيعي أو المعنوي الذي يتعاقد مع المحترف خارج مجال مهنته قصد إشباع حاجاته أو حاجات عائلته، والمستهلك قد يكون مستهلك عادي أو مستهلك إلكتروني، والمستهلك الإلكتروني هو الذي يستخدم وسيلة تعتمد بشكل أساسي لإشباع رغباته واحتياجاته على الإنترنت، والوسائل الإلكترونية فقد يتعاقد على شراء برنامج إلكتروني من أحد شركات البرامج مثل: نظام تشغيل من مايكروسوفت أو يقوم بشرائه من على الإنترنت، ويرسل له عبر الإيميل، وقد يكون هذا المنتج معيباً يحتوي على ثغرة يتم استغلالها من قبل الهاكرز، ولذلك نجد أن أغلب التشريعات والقوانين قد قامت بحماية المستهلك حيث نص "قانون حماية المستهلك الفرنسي" على أنه: "يجب على كل مهني بائع لسلع أو مقدم لخدمات، قبل إبرام العقد، أن يمكن المستهلك من العلم بالصفات الأساسية للسلعة أو الخدمة"[٣٩].

---

[٣٧] عرّفه المشرع المصري بموجب القرار رقم ٨٨٦ الصادر عن وزارة التجارة والصناعة المصرية سنة ٢٠٠٦ الخاص بإصدار اللائحة التنفيذية وقانون حماية المستهلك الصادر بموجب القانون رقم ٦٧ سنة ٢٠٠٦ في الباب الأول من الفصل الثاني في المادة (١).

[٣٨] ذكر التعريف في القرار الوزاري الفرنسي الصادر في ١٩٧٢/١/١٤ الخاص بتنظيم الإعلان عن أسعار السلع.

[٣٩] نص المادة (L111-1) من قانون حماية الاستهلاك الفرنسي الصادر بتاريخ ٢٦ يوليو ١٩٩٣.

ونص أيضاً: "قانون حماية المستهلك الفرنسي الصادر في ١٩٩٣ على نصوص تحارب الغش والخداع من قبل المنتِج لإيقاع المستهلك في الغلط أو جعل المستهلك عرضه للتدليس"[٤٠].

وهذا ما ذهب إليه القانون المصري لحماية المستهلك حث نص على أنه: " يكون المنتِج مسؤولاً عن كل ضرر يلحقه المنتَج أو يحدثه إذا أثبت أن الضرر بسبب تقصير المورد في اتخاذ الحيطة الكافية لمنع وقوع الضرر، أو التنبيه إلى احتمال وقوعه"[٤١]، وذهب المنظم السعودي أيضاً إلى حماية المستهلك إذا تعرض للخداع من المنتِج وفق "قرار مجلس الوزراء رقم (١١٩) وتاريخ ٢٢/٤/١٤٢٩هـ"[٤٢].

وإذا أمعنا النظر في النصوص القانونية السابقة سنجد أن أغلب تشريعات دول العالم أصدرت قوانين تحمي بها المستهلك إذا تعرض إلى ضرر من منتج معيب ويجوز له الرجوع بالتعويض علي المنتِج، فلو قام المستهلك باستخدام برنامج إلكتروني تم شرائه من أحد الشركات واكتشف بعد تعرضه لهجوم النقرة الصفرية أنه تم استغلال

---

[٤٠] راجع نص المادة رقم (١٢١) وما بعدها من قانون حماية الاستهلاك الفرنسي الصادر بتاريخ ٢٦ يوليو ١٩٩٣.

[٤١] المادة (٢٧) من قانون حماية المستهلك المصري الجديد رقم ١٨١ لسنة ٢٠١٨.

[٤٢] يعد مخالفًا لأحكام هذا النظام كل من:

١-"خدع – أو شرع في الخداع – بأي طريقة من الطرق في أحد الأمور الآتية:"

أ – ذاتية المنتج، أو طبيعته، أو جنسه، أو نوعه، أو عناصره، أو صفاته الجوهرية.

ب-مصدر المنتج.

ج – قدر المنتج، سواء في الوزن، أو الكيل، أو المقاس، أو العدد، أو الطاقة، أو العيار

٢- غش – أو شرع – في غش المنتج

٣- باع منتجًا مغشوشًا، أو عرضه

٤- حاز منتجًا مغشوشًا بقصد المتاجرة

٥- صنع منتجات مخالفة للمواصفات القياسية المعتمدة، أو أنتجها أو حازها، أو باعها، أو عرضه.

ثغرة أمنية في البرنامج، فإن هذا يعني أن البرنامج معيب، وبالتالي وفق قوانين حماية المستهلك يمكن له الرجوع على الشركة المنتِجة للبرنامج بالتعويض.

المطلب الثاني

المسؤولية التقصيرية عن أضرار هجوم النقرة الصفرية

ذكرنا آنفاً أن المسؤولية العقدية تقوم على إخلال بالتزام عقدي؛ فتقوم المسؤولية العقدية إذا أخل أحد طرفي الالتزام بالتزامه الموجود في العقد، ولكن أحياناً قد لا يكون هناك عقد يربط بين المتضرر ومرتكب الفعل الضار، وحينئذٍ كيف سيتم تعويض المتضرر؟ ولهذا، أوجد القانون نوعاً آخر من المسؤولية تُعرف بالمسؤولية التقصيرية والمقصود بها: "أن يخل الشخص بواجب فرضه القانون أو الواجب العام وبسبب هذا الإخلال يلحق ضرر للغير يستلزم تعويضه عما لحقه من ضرر".

وتم تعريفها أيضاً على أنها: "التزام المدين بتعويض الضرر الذي ترتب على إخلال بالتزام يقع عليه ومصدر هذا الالتزام هو القانون حيث يستقل بتحديده وكيفية التعويض عنه"[٤٣].

الأصل العام أن كل شخص يمارس حياته بحريه كفلها له القانون دون إضرار بالغير، فإذا ارتكب هذا الشخص خطأ وترتب على هذا الخطأ إضرار الغير، فإنه مُلزم بتعويضه عن الخطأ الذي ارتكبه في حقه، وهذا هو أساس المسؤولية التقصيرية، والأصل في المسؤولية التقصيرية أنها تقوم على خطأ واجب الإثبات يكمن في أن كل شخص ألحق بخطئه ضرر للغير كان واجب عليه جبر هذا الضرر؛ لأن القاعدة

---

[٤٣] د. عصام احمد البهيجي، ضمان الحق في حرمة الحياة الخاصة في ضوء المسؤولية المدنية وحقوق الإنسان، دار الجامعة الجديدة، مصر، ٢٠٠٥، ص٤٣.

العامة تقضي بعدم الإضرار بالغير وأي إخلال بهذا الالتزام القانوني يعتبر خطأ يلزم صاحبة بتعويض المضرور عما لحق به من ضرر.

الفرع الأول

المسؤولية التقصيرية من منظور تشريعي

سوف نجد أن هناك عدة تشريعات تحدثت عن المسؤولية التقصيرية ومنها على سبيل المثال:

ما نص عليه القانون المدني الفرنسي أن: "كل فعل يحدث ضررا للغير يلزم من وقع الضرر بخطئه بتعويضه"[٤٤]، وهذا ما تناوله أيضاً القانون المدني المصري؛ حيث نص على أنه: "كل خطأ سبب ضرراً للغير يلزم من ارتكبه بالتعويض"[٤٥]، وهذا ما قررته وثيقة الكويت، حيث جاء فيها أن: "كل إضرار بالغير يلزم فاعله ولو غير مميز بضمان الضرر"[٤٦]، ونصت الوثيقة ذاتها على أن: "يكون الإضرار بالمباشرة أو التسبيب فإذا كان بالمباشرة لزم لضمان ولا شرط له وإذا وقع بالتسبيب فيشترط التعدي أو التعمد أو أن يكون الفعل مفضياً إلى الضرر"[٤٧]، وبناء على ما سبق، فإن الشخص إذا ارتكب خطأ وترتب على هذا الخطأ الإضرار بالغير، فإن مرتكب الخطأ مُلزَم بالتعويض، ولكن في ظل التطور الذي نشاهده الآن والتقدم التكنولوجي وظهور الإنترنت ظهرت أنواع جديده من الأخطاء التي يمكن أن تُرتَكب ليس في الواقع وإنما عبر الإنترنت وقد تشكل هذه الأفعال غير مشروعه أضراراً للغير، فهل القواعد العامة

---

[٤٤] المادة (١٣٨٢) من "القانون المدني الفرنسي".

[٤٥] المادة (١٦٣) من "القانون المدني المصري".

[٤٦] المادة (٢٦١) من وثيقة الكويت

[٤٧] المادة (٢٦٢).

في المسؤولية قادرة على مواجهة هذا النوع الجديد من الإخلال بالالتزامات القانونية التي تحدث ضرراً بالغير عبر الإنترنت؟

ومع هذا التطور الذي نشهده، فقد ظهر ما يعرف بالمسؤولية التقصيرية الإلكترونية والتي تعتمد بشكل أساسي على القواعد العامة في المسؤولية التقصيرية وتقوم أيضا على عناصرها من خطأ وضرر وعلاقة سببية، ولكن يوجد اختلاف بينها وبين المسؤولية التقصيرية التقليدية حيث إن المسؤولية التقصيرية الإلكترونية الخطأ فيها خطأ مفترض[٤٨]، حيث أن الخطأ المفترض هو قرينة بسيطة قابلة لإثبات العكس عن طريق نفي الخطأ من جانب المسؤول أو المدعي عليه أو عن طريق نفي علاقة السببية بين الخطأ المفترض من جانبه والفعل الضار بأن يثبت أن الضرر قد وقع نتيجة قوة قاهره أو حادث فجائي أو خطأ الغير.

الفرع الثاني

أركان المسؤولية التقصيرية

إذا تأملنا واقع الأمر سوف نجد أن المسؤولية التقصيرية تستند في أساس قيامها إلى فعل شخصي[٤٩] يسبب ضرراً بالغير رغم أن الواجب العام والقانون كل منهما ينادي بعدم التسبب بالضرر للغير، وأي إخلال بهذا الحق يُلزم مرتكب الفعل الضار بتعويض من وقع الضرر عليه بسبب هذا الفعل الضار أو الخطأ وبذلك يلزم لقيام المسؤولية التقصيرية ثلاثة أركان أولها: الخطأ، والثاني: الضرر، والثالث: علاقة السببية بين الخطأ والضرر وسوف نتناول كلاً منهم بالتفصيل.

---

[٤٨] راجع د. خالد مصطفي فهمي المسؤولية المدنية للصحفي، دار وائل: عمان، ٢٠٠٧، ص١٢٧.

[٤٩] سوف نكتفي بدراسة الفعل الشخصي في المسؤولية التقصيرية لأنه أعم وأشمل ويعتبر الأصل العام في المسؤولية حيث أن المسؤولية التقصيرية تقوم بشكل كامل حول فعل خطأ صدر وسبب ضرر للغير.

الركن الأول- الخطأ:

يعتبر الخطأ بشكل عام من أهم أركان المسؤولية التقصيرية، ورغم أن معظم التشريعات لم تتطرق إلى تعريفه، فقد قام العديد من الفقهاء بتعريفه، وكانت تعريفات الفقهاء جميعها تدور حول كونه: "إخلال بواجب قانوني محمي بالقانون أو بالنصوص التشريعية"[٥٠].

وإذا نظرنا على مستوي مجلس التعاون الخليجي سوف نجد أن وثيقة الكويت في مادتها (٢٦١) نصت على الآتي: "كل إضرار بالغير يلزم فاعلة ولو غير مميز بضمان الضرر"[٥١]، وما تناوله القانون المدني الكويتي: "عند تعذر تنفيذ الالتزام عيناً، أو التأخير فيه، جيب على المدين تعويض الضرر الذي لحق الدائن بسبب ذلك، ما لم يثبت المدين أن عدم التنفيذ أو التأخير كان لسبب أجنبي لا يد له فيه"[٥٢].

والخطأ وفق ما سبق ذكره لابد أن يتوافر فيه ركن مادي وركن آخر معنوي، أما بالنسبة إلى الركن المادي فهو عبارة عن إخلال بالتزام قانوني قد يكون هذا الالتزام منصوصاً عليه في القانون أو في أي نصوص تشريعية أو من الواجبات العامة التي تجبر الفرد على أن يحترم حقوق الغير، وألا يمس بسلامة أفراد المجتمع، وإذا نظرنا للخطأ في هذا السياق سوف نجده يتمثل في فعل إيجابي أو سلبي.

الفعل الإيجابي هو إتيان عمل يحدث ضرراً أو قد يكون سلبياً مثل امتناع شخص عن انقاذ شخص آخر يغرق عن طريق عدم مده بأداة انقاذ لكي يمسك بها، أما الركن المعنوي في الخطأ هو الإدراك أو التمييز بالتالي لا يكفي الركن المادي فقط فلا يكفي أن يخل الشخص بالتزام قانوني أو واجب عام، وإنما يجب أن يصدر هذا الإخلال من

---

[٥٠] د. عبد القادر العرعاري، "النظرية العامة للالتزامات في القانون المدني المغربي"، مصادر الالتزام الكتاب الثاني المسؤولية عن الفعل الضار، ١٩٨٨، ص ١١.

[٥١] المادة (٢٦١) من "وثيقة الكويت للنظام الموحد لدول مجلس التعاون الخليجي".

[٥٢] المادة (٢٩٣) من القانون المدني الكويتي.

شخص مميزاً ومدركاً لنتائج أفعاله، ولا يلتفت هنا عما إذا كان الشخص قاصد إحداث الضرر أو ناتج عن إهمال وتقصير منه[٥٣].

لكن يبقي السؤال الذي يطرح نفسه هل الخطأ وتعريفه وفق القواعد التقليدية يُعدّ كافياً لتحديد المسؤولية وفق المعاملات الإلكترونية، والتي تحتوي على العديد من المخاطر؟ في حقيقة الأمر، قد قام العديد من الفقهاء بوضع تعريف مستقل للخطأ الإلكتروني أو للخطأ الذي يحدث ضرراً بسبب استخدام الإنترنت حيث تم تعريفه على أنه: "الفعل الضار المرتكب عبر الإنترنت"[٥٤]، وتم تعريفه أيضاً بأنه: "كل استخدام لأجهزة الإنترنت بشكل يلحق ضررا بالغير مع إدراك مرتكب الفعل لذلك"[٥٥]، وبناء على التعريفات السابقة، سوف نجد أن الخطأ التقصيري الإلكتروني ورغم محاولة بعض الفقهاء تعريفه بشكل مستقل عن الخطأ التقصيري التقليدي؛ إلا أنه في حقيقة الأمر لا يختلف عن الخطأ التقصيري التقليدي إلا من حيث الوسيلة المستخدمة فالخطأ التقصيري التقليدي مع توفر عناصره هو نفس الخطأ التقصيري الإلكتروني المختلف بينهما فقط الوسيلة المستخدمة في ارتكابه، ومن صور الخطأ التقصيري على سبيل المثال: انتهاك الخصوصية الخاصة بالضحية والدخول غير المصرح به لدي أجهزة الغير سواء كان الحاسب شخصي أو هاتف نقال.

وأيضاً التلاعب بالمعلومات الموجودة على جهاز الشخص الذي تم اختراقه وفق هجوم النقرة الصفرية، وكل هذا يتم عن طريق استغلال المخترق ثغرة في النظام

---

[٥٣] د. عبد الرزاق احمد السنهوري – الوسيط في شرح القانون المدني الجديد – المجلد الثاني – نظرية الالتزام بوجه عام – مصادر الالتزام – ص ٩٠١.

[٥٤] د. سمير حسني المصري، "المسؤولية التقصيرية الناشئة عن استخدام الإنترنت"، دراسة مقارنة بالقانون الأنجلو أمريكي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠١٦، ص ٣٢.

[٥٥] د. قارس بو بكر، المسؤولية المدنية في مجال المعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة ١، الجزائر، ٢٠٢١، ص ١٩.

التشغيلي لجهاز الضحية دون علمه، فيقوم باستغلال هذه الثغرة في تثبيت البرامج الخبيثة المشفرة في جهاز الضحية فيصبح جهاز الضحية كالكتاب المفتوح بين يديه يستطيع أن يقوم بنسخ كل البيانات المتاحة على الجهاز، ومعرفة كل كلمات المرور التي يستخدمها الضحية سواء لحسابات التواصل الاجتماعي مثل الفيس بوك، وتويتر، تليجرام، والإيميل الشخصي[٥٦].

ليس هذا فحسب، بل يستطيع أيضاً معرفة كافة البيانات الخاصة بالمصرف والحسابات البنكية، وأيضاً تسجيل صوت وصورة للضحية واستغلال هذه التسجيلات في ابتزازه فيما بعد، وأخطر ما في الأمر، أنه يستطيع اختراق كل المستخدمين الموجودين والذين يتعاملون مع الضحية واستغلال الضحية كحصان طروادة، ويستغل ثقتهم في تلقي الرسائل من الضحية؛ فبإمكان المخترق انتحال صفة الضحية، وإرسال البرنامج المشفر الخبيث لهم، ويتمكن بواسطته من فتح ثغره في أجهزتهم، فيقع الكل ضحية سهله للمخترق غضون لحظات.

الركن الثاني- الضرر:

يعتبر الضرر من الأركان المهمة لقيام المسؤولية التقصيرية، فلا تقوم المسؤولية بدونه لكن يبقي السؤال المهم هل يختلف الضرر وفق المسؤولية التقصيرية التقليدية عن الضرر في المسؤولية التقصيرية الإلكترونية؟ لا ريب أن الضرر يعتبر عنصراً بالغ الأهمية في المسؤولية التقصيرية التقليدية فلا تعويض بدون وجوده، وهذا ما أقرّته

---

[٥٦] د. محمد رشاد القطعاني، الحماية الجنائية للحق في حرمة الاتصالات الشخصية، الطبعة الثانية، الفتح للطباعة والنشر، الإسكندرية، ٢٠١٥، ص ١٠٣، وحسب إحدى الأحكام الصادرة عن محكمة في الولايات المتحدة الأمريكية فأنه لكي تتسم المراسلات عبر البريد الإلكتروني بالخصوصية يلزم وجود عنصرين أساسيين هما: ١- عنصر موضوعي يتعلق بمحتوي الرسالة، وعدم رغبته بكشفه من قبل شخص غيره.

أشار للحكم د. عمر محمد يونس في كتابة أشهر المبادئ المتعلقة بالإنترنت في القضاء الأمريكي، دار النهضة العربية، القاهرة، ٢٠١٤، ص ٥٨٠.

وثيقة الكويت أن: "كل إضرار بالغير يلتزم فاعلة ولو غير مميز بضمان الضرر"[٥٧]، حيث نصت على أنه: "ليس للمالك أن يستعمل ملكه بما يسبب للغير ضرراً"[٥٨]، وبالتالي تتبدى لنا أهميته القصوى أيضاً في المعاملات التي تتم بشكل إلكتروني، وذلك بسبب الخسائر المادية والمعنوية الفادحة التي من الممكن أن تصيب الشخص من استعماله الإنترنت.

وقبل أن نتعمق في الضرر الإلكتروني يجب علينا أولاً أن نتطرق بشكل موجز إلى تعريف الضرر وفق المسؤولية التقصيرية التقليدية؛ حيث عرفه البعض بأنه: "الأذى الذي يصيب الشخص من جراء المساس بحق من حقوقه أو مصلحة مشروعة له سواء تعلق الحق أو تلك المصلحة بسلامة جسمه أو عاطفته أو بمالة أو حريته أو شرفه أو غير ذلك"[٥٩]، وعرفه البعض أيضاً بأنه: "الأذى الذي يصيب الشخص في حق من حقوقه أو في مصلحة مشروعة سواء كان ذلك الحق أو تلك المصلحة ذات قيمة مالية أو لم تكن"[٦٠].

وفقاً للتعريفات السابقة نجد أن الضرر الذي يصيب الشخص في ذمته المالية يكون معروف بالضرر المادي ويصيب الشخص بسبب الفعل الغير مشروع المرتكب في حقة سواء كان على شكل اعتداء جسماني يهدد صحة الإنسان وسلامته، وأيضاً كل مساس بحق من الحقوق المتصلة بشخص الإنسان مثل حريته الشخصية، وحرية العمل وحرية الرأي إذا ترتب عليها خسارة مثل حبسه أو منعه من السفر، أما بالنسبة إلى الضرر

---

[٥٧] المادة رقم (٢٥٦) من وثيقة الكويت للنظام الموحد لمجلس التعاون الخليجي.

[٥٨] المادة رقم (٩٥٣) من وثيقة الكويت للنظام الموحد لمجلس التعاون الخليجي.

[٥٩] انظر: د. يوسف محمد عبيدات، "مصادر الالتزام في القانون المدني"، الطبعة الأولى، دار المسيرة للنشر والتوزيع والطباعة، الأردن، ٢٠٠٩، ص ٢١٩.

[٦٠] رمضان أبو السعود، أحكام الالتزام، دار المطبوعات الجامعية، مصر، ١٩٩٨، ص ٢٤٠.

الأدبي هو ما يصيب الإنسان في الشعور والشرف وسواء ارتكب الشخص ضرراً مادياً أو أدبياً يلتزم مرتكب الفعل الضار بتعويضهم عما لحقهم من أضرار.

أما بالنسبة إلى الضرر الناتج عن الوسائل الإلكترونية فيمكن تعريفه بأنه: "الضرر الذي يتسبب به التعامل مع أجهزة الحاسب الآلي الحديثة عن طريق استخدام شبكة الإنترنت"[٦١]، ومن خلال هذا التعريف نجد أن الضرر الإلكتروني قد يسبب أضراراً سواء بشكل مادي أو بشكل معنوي، ويجب أن تتوفر فيه شروط عدة، منها أن يكون الضرر مؤكد الحدوث، ويجب أيضاً أن يكون الضرر الإلكتروني: "ضرر مباشر يصيب الشخص في حق أو مصلحة مشروعة"[٦٢]، وللضرر الإلكتروني الناجم عن هجوم النقرة الصفرية عدة صور منها: انتهاك خصوصية الشخص أو الشركة، وتسريب بياناتهم وحسابتهم الشخصية، التلاعب بمحتوي الإيميل الشخصي، تسجيل صوت وصورة لكل ما يدور حول الحاسب الشخصي للضحية واستغلال كل ما يتم تسجيله ضده لابتزازه فيما بعد.

وإذا قمنا بتحليل الضرر الناتج عن هجوم النقرة الصفرية فسوف نجد أن الضرر أصاب الضحية في حق يحميه القانون، ومن ثم يحق له الاحتماء بالقضاء واللجوء إليه للمطالبة بالتعويض؛ لأن الحفاظ على خصوصية الفرد حقة كفله القانون، وكذا عدم التعرض للابتزاز، وكافة الأضرار سواء كانت أضراراً مادية أو أضراراً معنوية، وتجدر الإشارة إلى أن المصلحة التي يحميها القانون لابد أن تكون مصلحة مشروعة، فإذا كانت غير مشروعة بأن كان صاحب الجهاز يستخدمه للأفعال المنافية للآداب، أو يستغله في أعمال تخريبية، سواء جهازه الشخصي أو الموقع الإلكتروني كأن يكون

---

[٦١] راجع د. نائل علي المساعدة، أركان الفعل الضار الإلكتروني في القانون الأردني، مجلة دراسات علوم الشريعة والقانون، الجامعة الأردنية، المجلد ٣٢، العدد ١ ، سنة ٢٠٠٥، ص ٥٥.

[٦٢] د. أحمد كمال صبري، المسؤولية المدنية للمرور على شبكات المعلومات، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠١٠، ص ٢٠٥.

موقعاً إباحياً، أو كان هذا الشخص يستغل جهازه وموقعه لصالح المنظمات الإرهابية، فإنه في كل تلك الحالات لا تشمله الحماية القانونية البتّة.

الركن الثالث– "علاقة السببية بين الخطأ والضرر":

من العناصر المهمة جداً، والتي تمثل الركن الثالث في المسؤولية التقصيرية: علاقة السببية بين الخطأ والضرر، إذ إنه لو انعدم الارتباط السببي بين الخطأ والضرر يصبح كلاهما عديم الفائدة، فلو كان الخطأ ليس هو المتسبب في الضرر فلا تقوم المسؤولية التقصيرية، ونجد أن معظم التشريعات قد نادت بعلاقة السببية من خلال نصوصها القانونية، على سبيل المثال ما ذهب إليه المشرع المصري حيث نص على أنه: "كل خطأ سبب ضرراً للغير يلتزم من ارتكبه بالتعويض"[٦٣]، وكذا ما ذهبت إليه وثيقة الكويت حيث نصت على أنه: "كل إضرار بالغير يلزم فاعله ولو غير مميز بضمان الضرر"[٦٤].

أما بالنسبة إلى القانون الفرنسي نجد أن علاقة السببية موجودة في نصوصه؛ حيث نص في أكثر من موضع على هذا الأمر حيث ذكر أن: "كل عمل أياً كان يوقع ضرراً بالغير يلزم من وقع بخطئه هذا الضرر أن يقوم بتعويضه"[٦٥]، وفي موضع آخر ذكر "كل شخص يكون مسؤولاً عن الضرر الذي يحدثه لا بفعله فحسب بل أيضاً بإهماله وعدم تبصره"[٦٦].

فمن الملاحظ أن أغلبية التشريعات اعتمدت في قيام المسؤولية على قيام علاقة السببية بين الخطأ أو الفعل الضار وبين الضرر الذي لحق بالشخص، فإذا انعدمت

---

[٦٣] انظر: المادة (١٦٣) من القانون المدني المصري.

[٦٤] نص المادة (٢٦١٩) من وثيقة الكويت.

[٦٥] المادة (١٣٨٢) من القانون المدني الفرنسي.

[٦٦] نص المادة (١٣٨٣) من القانون المدني الفرنسي.

علاقة السببية لن يقوم للمسؤولية التقصيرية قائمة، لكن التساؤل الذي يطرح نفسه في حالة تعدد الأسباب ما هو المعيار المتبع لتحديد علاقة السببية.

في هذه الحالة نجد أن أغلب التشريعات أخذت بنظرية السبب الفعال أو السبب المنتج، ومعني هذه النظرية أنه إذا كان هناك تدخل بأكثر من سبب في إحداث الضرر؛ فإنه يتوجب علينا التفرقة بين الأسباب الأقل قوة العارضة وبين الأسباب المنتجة، والتي تكون سبباً مباشراً لوقوع الضرر.

وإذا طبقنا الأمر على هجوم النقرة الصفرية فسوف نجد أن عناصر المسؤولية التقصيرية كلها متوفرة، فهناك خطأ تم ارتكابه تمثل في الدخول غير المشروع إلى الجهاز الخاص بالضحية دون إذنه، وتم فتح ثغرة في جهازه منتهكا بذلك خصوصية الضحية بتثبيت برامج خبيثة على الجهاز الخاص به مستغلا إياها لأغراض سيئة السمعة، منها استغلاله وسرقة محتوي البيانات الموجودة، ونجد أن هذا الدخول كان السبب المباشر في إلحاق الضرر المادي والمعنوي للضحية وبذلك نجد أن السبب المنتج أو الفعال لحدوث الضرر تحقق بشكل مباشر بسبب الهجوم الصفري.

ورغم أن قواعد المسؤولية التقصيرية من خطأ وضرر وعلاقة سببية من السهل تكييفها قانوناً علي الجرائم التقليدية، بيد أنه لو ألقينا نظرة فاحصة علي جريمة هجوم النقرة الصفرية متأملين طبيعتها؛ فسوف نجد أن مرتكب الخطأ أو الفعل غير المشروع المتمثل في الهاكر أو المخرب أو الكراكرز المستغل للثغرات في أجهزة المستخدمين يشبه الشبح حرفياً فبإمكانه الدخول إلى جهاز الضحية دون أن تشعر، ويرتكب كل الأفعال الغير مشروعة، ويخرج بدون أن يدري أحد وتفاجئ الضحية بعد مرور الوقت أنه يتم تهديده بتسجيلاتٍ صوتيةٍ له، أو مقاطع فيديو غير لائقة تم تسجيلها دون علمه، أو أنه تم تسريب محتوي جهازه بدون أن يعلم تحديداً من قام بذلك أو متي فعل ذلك، لذلك يعد هجوم النقرة الصفرية من أخطر الجرائم نظراً لتأثيرها البالغ الخطورة، وعدم سهولة اكتشاف مرتكبها حيث إن الأمر غاية في الصعوبة من جانبين، أولهما:

أن مرتكبه قد يكون خارج البلاد التي يقيم فيها الضحية، ثانيهما: صعوبة اكتشاف هذا الهجوم إلا بعد فوات الأوان؛ نظراً لدقته واستخدام تقنيات عالية في التخفي والاختراق، لكن لو تم اكتشاف المسؤول عن ذلك فهو ملتزم بالتعويض عما لحق الضحية من ضرر مادي وأدبي.

المبحث الرابع

آثار المسؤولية المدنية الناجمة من هجوم النقرة الصفرية

إذا توفرت عناصر المسؤولية من خطأ وضرر وعلاقة سببية يترتب عليها أن المسؤول يكون ملتزماً بالتعويض عما لحق بالمتضرر من ضرر ليتم جبر هذا الضرر، وبإذن الله تعالي سوف نتحدث في هذا المطلب عن التعويض الناشئ بسبب هجوم النقرة الصفرية، لكن قبل الحديث عنه، سوف نتحدث أولاً عن كيفية الحصول على هذا التعويض عن طريق القضاء؛ حيث إن القانون المدني قد كفل للمتضرر الحماية من الاعتداء سواء من انتهاك خصوصيته عبر اختراق أجهزته الشخصية أو الاعتداء على بياناته وحساباته باستخدام هجوم النقرة الصفرية.

المطلب الأول

دعوي المطالبة بالتعويض عن أضرار هجوم النقرة الصفرية

مما ينبغي التأكيد عليه أن القانون المدني قد وفر للمتضرر الحماية من الاعتداء سواء من انتهاك خصوصيته عبر اختراق أجهزته الشخصية أو الاعتداء على بياناته وحساباته مستخدماً هجوم النقرة الصفرية، وذلك برفع دعوى قضائية أمام القضاء المختص للحصول على تعويض عما لحق به من ضرر مترتب على هذا الهجوم،

وسنقوم – بادئ ذي بدء– بتحديد أطراف الدعوى، ثم نوضح بعد ذلك المحكمة المختصة بنظر الدعوي[٦٧].

الفرع الأول

أطراف الدعوى

تقوم المسؤولية بشكل عام على تعويض الضرر الذي لحق بالمتضرر لكن وعلى خلاف المعهود، فالمتضرر هنا هو المدعي وليس المدعي عليه، فالشخص الذي أصابه ضرر ناتج عن هجوم النقرة الصفرية يسمي المدعي، والشخص بعينه هو الذي يقوم بالتوجه إلى القضاء للمطالبة بالتعويض عن الضرر الذي لحق به، وكذا يتحمّل عبء إثبات الضرر الذي لحق به، ومن الطبيعي أن تتوافر فيه الشروط العامة لقبول دعواه بحيث يكون له مصلحة معلومة مشروعة من رفع الدعوي وأن يرفعها في المواعيد المحددة لذلك وليس بعد مرور الوقت ومرجع ذلك إلى القواعد العامة حيث تكون مدة التقادم ٣ سنوات من وقت معرفته بمن قام باختراق أجهزته وفق للهجوم الصفري أو ١٥ عاماً اذا لم يعلم من قام بهذا الهجوم أو الضرر الذي لحق به الطرف الأخر وهو المدعي عليه، وهو من قام بهذا الهجوم على المدعي، ويكون ملزماً بالتعويض عما ارتكبه من أضرار لحقت بالمدعي، ولو كان المدعى عليهم أكثر من شخص يكونوا متضامنين بالتعويض تجاه المتضرر.

لكن في حقيقة الأمر ونظراً لما سبق وأوضحناه من الطبيعة الخطيرة لجريمة هجوم النقرة الصفرية، ومدي احترافية مرتكبها، والآلية التي يتم استخدامها، والتي تخفي تماماً هوية المخترق؛ بحث لا يشعر الضحية إطلاقاً بوجوده أو بهجومه نجد أنه من الصعب

---

[٦٧] راجع د. عايد رضا الخلايلة، "المسؤولية التقصيرية الإلكترونية (المسؤولية الناشئة عن استخدام أجهزة الحاسوب والأنترنت دراسة مقارنة)"، دار الثقافة للنشر، عمان، ٢٠٠٩ م، ص ٢١٢.

جداً تحديد هوية المدعي عليه (المخترق)، وبذلك من الصعب إثبات الواقعة، ومن ثم يتعسر على الضحية اللجوء للقضاء للمطالبة بالتعويض.

الفرع الثاني

المحكمة المختصة بنظر الدعوى

لتعيين المحكمة المختصة في الدعاوى التي يرفعها المدعي للمطالبة بتعويضه عما لحق به من ضرر ناتج عن الهجوم الصفري أو هجوم النقرة الصفرية يجب أولاً تحديد الطريق الذي يسلكه المدعي للمطالبة بتعويضه، فإذا كان هناك علاقة عقدية بين المتضرر وبين المتسبب بالضرر فنكون حينئذٍ بصدد مسؤولية عقدية، فإذا استخدم المتضرر أحد البرامج التي قام بشرائها من شركة عالمية مثل شركة مايكروسوفت وكانت هذه البرامج تحتوي على ثغرات أمنية سهلت استغلال المخترق استخدام مثل هذه الثغرات للقيام بعملية الاختراق، حينها يتوجب علي الشركة الالتزام بالضمان، وذلك من نواحٍ متعددة؛ لأن المنتج تم شراؤه بموجب عقد بين المتضرر وبين الشركة أو من خلال حماية المستهلك من المنتجات المعيبة؛ لأن البرنامج في هذه الحالة يعد معيباً، وحينئذٍ تكون المحكمة المختصة هي محكمة موطن أو محل إقامة المدعي عليهم[٦٨].

أما في حال انعدام العلاقة العقدية؛ فإن المحكمة المختصة بالمسؤولية التقصيرية – وفقاً لأحكام القانون – حينئذٍ هي محكمة موطن المدعي عليه أو المخترق، ولكن كما ذكرنا آنفاً فمحل جريمة هجوم النقرة الصفرية هو الإنترنت، ومن الممكن أن يكون المدعي المتضرر (الضحية) في بلد ومرتكب هذا الهجوم في بلد آخر، وكما بيّنا فمن العسير جداً تحديد من ارتكب هذه الجريمة أو الفعل الضار، وبسبب مثل هذه الجرائم

---

[٦٨] راجع د. عباس العبودي، شرح أحكام قانون المرافعات المدنية – دراسة مقارنة، دار الكتب للطباعة والنشر جامعة الموصل، ٢٠٠٠، ص ٢٠٣.

فقد نادي العديد من فقهاء القانون بسَنّ مبادئ قانونية موحدة تفصل في مثل هذه المنازعات خاصة أن الإنترنت يعد عالم افتراضي ليس له مكان محدد.

المطلب الثاني

التعويض عن هجوم النقرة الصفرية

بعد أن تتوفر عناصر المسؤولية من خطأ ارتكب في حق الضحية من المخترق، وكان سبباً مباشراً في وقوع الضرر على الضحية أو المدعي فيذهب للقضاء مطالباً بجبر الضرر من خلال دعوي المسؤولية مطالباً بالتعويض عن الضرر الذي لحق به، وكنا قد أسلفنا القول عن الدعوي وأطرافها وسوف نتحدث الآن عن التعويض.

والتعويض يعرف بأنه: "تصحيح ما اختل من توازن بحالة المتضرر نتيجة وقوع الضرر بإعادة التوازن إلى ما كان عليه قبل وقوع الضرر"[٦٩]، ومن تعريفات التعويض أيضاً جبر الضرر الذي أصاب الشخص المتضرر"[٧٠]، فإذا طبقنا هذه التعريفات على الموضوع الذي نتحدث فيه، وهو هجوم النقرة الصفرية؛ فسنجد أن التعويض هنا يكون جبراً للضرر الناتج عن التعدي غير المشروع للمخترق على الأجهزة الخاصة بالضحية، والتعويض في هذه الحالة قد يكون تعويضاً نقدياً أو قد يكون تعويضاً عينياً أو عن طريق أداء أمر معين، بيد أن الطريقة المثلي للتعويض هي إعادة الوضع إلى ما كان عليه، وهذا ما يعرف بالتعويض العيني لكن مسألة إعادة الأمر إلى ما كان عليه في مسألة الأضرار الناشئة عن هجوم النقرة الصفرية أو عن طريق الإنترنت

---

[٦٩] راجع د. إبراهيم الدسوقي أبو الليل، المسؤولية المدنية والإثراء بلا سبب، دار الكتاب والنشر، الكويت، بدون سنة نشر، ص ٢١٢.

[٧٠] د. نبيل إبراهيم سعد، النظرية العامة للالتزامات، مصادر الالتزام منشأة المعارف، الإسكندرية، ٢٠١١، ص ٤٣٦.

بشكل عام تُعدّ أمراً بالغ الصعوبة، ونجد أنه لا مفر من التعويض النقدي حتى تتم إزالة الضرر أو على الأقل التخفيف منه.

ومن المميزات التي يتميز بها التعويض النقدي مرونته وصلاحيته سواء بالنسبة للضرر المادي أو الضرر الأدبي رغم أن التعويض عن الضرر الأدبي قد يكون أحياناً أكثر قيمة، لاسيما إذا كان الشخص الذي تعرض لهجوم النقرة الصفرية ذا مكانة اجتماعية مرموقة، ويتمتع بسمعة طيبة، ويزداد الأمر سوءاً إذا قام المخترق بنشر أشياء تمسه أو تمس سمعته، وانتشرت هذه الأشياء على نطاق واسع عبر الإنترنت ومواقع التواصل الاجتماعي.

ونجد أن العديد من التشريعات، ومنها المشرع الفرنسي والمصري والكويتي والمنظم السعودي قد تحدثت بشكل واسع عن التعويض عن الضرر.

والتعويض الناشئ عن هجوم النقرة الصفرية يثير العديد من الإشكاليات القانونية خاصة في مسألة الوقت الذي يتم فيه تقدير الضرر؛ حيث إن الضرر الذي لحق بالضحية في وقت رفع الدعوى يمكن أن يكون متغيراً ويظهر غيره فيما بعد، وبالتالي يصعب تحديده بشكل كامل وقت النطق بالحكم "لذلك إذا لم يتسن للقاضي أن يعين التعويض وقت إصدار الحكم فمن جق المتضرر خلال مدة معينة أن يطالب بإعادة النظر في تقدير التعويض"[٧١].

وأيضاً نظراً للطبيعة الخاصة لهجوم النقرة الصفرية، ومدى حداثتها من ناحية التنفيذ والأسلوب المتبع واستخدام أحدث التقنيات والبرمجيات الحديثة للاختراق قد يصعب على القاضي الإلمام بتفاصيلها بشكل كبير، وهذا لا يمنع استعانة القاضي بخبراء

---

[٧١] راجع د. محمد حسين منصور، "المسئولية الإلكترونية، دار الجامعة الجديدة للنشر"، مصر، ٢٠٠٣، ص٣٤٥.

ومهندسين للاستفادة من خبرتهم حتى يقوم بتقدير التعويض بشكل دقيق لكن آرائهم بالتأكيد غير ملزمة للقاضي.

الخاتمـــة

من خلال دراستنا للموضوع فقد أوضحنا إلى أي مدى تم بلوغ العلم التقدم في المجال التكنولوجي الحديث، وأن الإنسان بإمكانه الاستفادة من هذه التكنولوجيا لما فيه مصلحة له لكن رغم هذا التطور الذي حقق خيراً مادياً ومعنوياً ورفاهيةً للإنسان لم يكن يتصور وجودها في يوم من الأيام، لكنها في الوقت نفسه أتت بالكثير من الأضرار التي لم تكن موجوده من قبل، وتركت أضرار تستلزم التعويض فتكلمنا عن جريمة هجوم النقرة الصفرية، والتي تعد من أخطر الجرائم وأحدثها في هذا العصر الحديث لما تسببه من أضرار بالغة للشخص، ووضحنا آلية هذه الجريمة، وكيفية عملها، ومقدار الضرر المادي والمعنوي الذي يصيب الشخص من جراء هذا الهجوم .

وتناولنا من خلال صفحات هذا البحث أيضا مدي ملائمة القواعد العامة في المسؤولية وكفايتها، سواء المسؤولية العقدية والمسؤولية التقصيرية للتصدي للإشكاليات القانونية التي تثيرها جريمة هجوم النقرة الصفرية خاصة في ظل غياب نصوص تنظمها، وهل القواعد العامة ستكون كافية– لو تم اللجوء إليها – لمواكبة هذا النوع من الجرائم الحديثة.

قد تبلور موضوع الدراسة في توضيح ماهية هذه الجريمة، وشرح لكيفية حدوثها مع توضيح خصوصيتها عن باقي الجرائم الإلكترونية، والتي تتمثل في أنها يصعب اكتشافها من جهة، ومن جهة أخرى الطريقة الفريدة والخطيرة التي يستخدمها المخترق في الولوج لجهاز الضحية دون أي دور للضحية في هذا الأمر، وما يترتب على ذلك من أضرار كارثية، ثم بيّنا بعد ذلك المسؤولية العقدية الناجمة عن هجوم النقرة الصفرية، ثم تطرقنا إلى توضيح المسؤولية التقصيرية أيضاً، وأخيراً، أوضحنا كيفية

حصول المتضرر علي تعويض عما أصابه من أضرارٍ جراء هذا الهجوم غير المشروع على حق من حقوقه التي كفلها له القانون.

أهم النتائج:

١- جرائم الهجوم الصفري أو هجوم النقرة الصفرية من الجرائم الحديثة جداً، والتي لم تكن معروفة من قبل، ونشأت بسبب التطور المذهل في استخدام التكنولوجيا والبرامج الحديثة، وتتميز بطريقتها الفريدة في الولوج إلى أجهزة الضحية دون أدني مشاركة منه أو أدني مقاومة.

٢- إن الطبيعة القانونية للانتهاكات التي تحدثها جريمة هجوم النقرة الصفرية تمثل انتهاكاً صارخاً لحق من الحقوق الشخصية التي يحميها القانون.

٣- الخطأ في المسؤولية العقدية الناجمة عن هجوم النقرة الصفرية يكون أساسه إخلال أحد الأطراف بالتزاماته العقدية، أما الخطأ في المسؤولية التقصيرية الناجمة عن هجوم النقرة الصفرية يكون ناتجاً عن إخلال بواجب قانوني يحميه القانون.

٤- إن فكرة الضرر الناجم عن هجوم الضغط الصفري قد يكون ضررا ماديا يصيب الأجهزة الشخصية أو أنظمة التشغيل بخلل عن طريق فتح ثغرات فيها، ومن ثم فمن الممكن أن يكون ضرراً مادياً، ومن الممكن أن يكون ضرر أدبياً إذا سبّب انتهاك خصوصية الشخص، وإيذائه في سمعته.

٥- الأصل العام بخصوص المحكمة المختصة في تقييم الأضرار الناجمة عن هجوم الضغط الصفري هي محكمة المدعي، وليس محكمة المدعى عليه.

٦- الجزاء المترتب على المسؤولية التقصيرية الناجمة عن هجوم الضغط الصفري يتخذ شكل تعويض نقدي، وليس تعويض بشكل عيني، وذلك للصعوبة الكبيرة في إعادة الحال إلى ما كان عليه في مثل هذا النوع من الضرر.

التوصيات:

١- حث جميع التشريعات على إصدار قوانين خاصة لمواجهة جرائم النقرة الصفرية، وألا يعتمدوا فقط على القواعد العامة في أحكام المسؤولية سواء العقدية أو التقصيرية

٢- توخي الحذر عند شراء البرامج ومحاولة شراء البرامج الأصلية قدر الإمكان وعدم شراء البرامج المقلدة، وكذا توخي الحذر عند نقل البرامج والملفات من الأشخاص فقد تكون محتوية على برامج للتجسس.

٣- استخدام برامج لمكافحة الفيروسات وتحديثها بشكل دائم؛ لأنها تعد الدرع الواقي من هجمات المخترقين والمخربين حتى لو ثبت عدم جدواها مع هجوم النقرة الصفرية؛ إلا أنه مع التحديثات قد تتمكن من اكتشاف الهجوم قبل أن يتم الدخول إلى جهاز الضحية.

٤- عدم استخدام الشبكات العامة الغير موثوقة؛ لأنها تعد من أسهل الطرق لاختراق الأجهزة الذكية عن طريق هجوم النقرة الصفرية.

٥- شيء أخر مهم جدا وهو دائماً المحافظة على التحديثات الأمنية التي ترسلها الشركات لمستخدميها أمثال شركة أبل ومايكروسوفت؛ لأن هذه التحديثات - غالباً - تقوم بسد ثغرات تم اكتشافها قد يستخدمها المخترقون في هجوم النقرة الصفرية، لذلك من اللازم عمل التحديثات الأمنية بشكل دوري.

٦- وأيضاً استخدام البرامج التي تغير من ال أي بي I P ADRESS أو التي تخفي العنوان الخاص بك علي الإنترنت مثل برامج ال VPN والتي تخفي هويتك عبر الإنترنت.

٧- عقد دورات تدريبية لتوعية الأشخاص عن طريق حماية معلوماتهم وبياناتهم الشخصية حين استخدام الإنترنت.

المراجـــع

أولاً- الكتب القانونية:

- د. أبراهيم الدسوقي أبو الليل، المسؤولية المدنية والإثراء بلا سبب، دار الكتاب والنشر، الكويت، بدون سنة نشر.
- د. أحمد خليفه الملط، الجرائم المعلوماتية، القاهرة، دار الفكر الجامعي، ٢٠٠٥.
- د. أمجد محمد منصور، النظرية العامة للالتزامات (مصادر الالتزام)، ط ١ دار الثقافة عمان، ٢٠٠٩.
- د. أنور سلطان، مصادر الالتزام في القانون المدني الأردني، دراسة مقارنة بالفقه الإسلامي، دار الثقافة للنشر والتوزيع، ٢٠٠٧م.
- د. جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول الجرائم المستخدمة عن استخدام الحاسب الآلي، الطبعة الرابعة دار النهضة العربية، ٢٠٠٢.
- د. خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠١٩.
- د. خالد مصطفي فهمي المسؤولية المدنية للصحفي، دار وائل للنشر: عمان، ٢٠٠٧.
- د. رمضان أبو السعود، أحكام الالتزام، دار المطبوعات الجامعية، مصر، ١٩٩٨.
- د. صلال حسين علي الجبوري، تعويض الضرر الأدبي في المسؤولية المدنية، دراسة مقارنة، دار الفكر الجامعي، ٢٠١٤م.
- د. عايد رضا الخلايلة، المسؤولية التقصيرية الإلكترونية (المسؤولية الناشئة عن استخدام أجهزة الحاسوب والأنترنت دراسة مقارنة، دار الثقافة للنشر، عمان، ٢٠٠٩ م.

- د. عبد القادر العرعاري، النظرية العامة للالتزامات في القانون المدني المغربي، مصادر الالتزام الكتاب الثاني المسؤولية عن الفعل الضار، ١٩٨٨.
- د. عباس العبودي، شرح أحكام قانون المرافعات المدنية – دراسة مقارنة، دار الكتب للطباعة والنشر جامعة الموصل، ٢٠٠٠.
- د. عبير شفيق رحباني، الجرائم الإلكترونية ومخاطرها، دار الثقافة للنشر والتوزيع، الأردن، ٢٠٢١.
- د. عصام احمد البهيجي، ضمان الحق في حرمة الحياة الخاصة في ضوء المسؤولية المدنية وحقوق الإنسان، دار الجامعة الجديدة، مصر،.٢٠٠٥.
- د. فاروق علي الحفناوي، موسوعة قانون الكومبيوتر ونظم المعلومات، الكتاب الثاني، الجزء الأول، عقود البرمجيات، دار الكتاب الحديث، ٢٠٠٩.
- د. قارس بو بكر، المسؤولية المدنية في مجال المعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة ١، الجزائر، ٢٠٢١.
- د. محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، مصر، ٢٠٠٣.
- المستشار/ منير رياض حنا، المسؤولية المدنية للأطباء والجراحين، في ضوء القضاء والفقه المصري، دار الفكر الجامعي، ٢٠١٤م.
- د. نبيل إبراهيم سعد، النظرية العامة للالتزامات، مصادر الالتزام منشأة المعارف، الإسكندرية، ٢٠١١.
- د. نائل علي المساعدة، أركان الفعل الضار الإلكتروني في القانون الأردني، مجلة دراسات علوم الشريعة والقانون، الجامعة الأردنية، المجلد ٣٢، العدد ١ سنة ٢٠٠٥.

- د. يوسف محمد عبيدات، مصادر الالتزام في القانون المدني، الطبعة الأولي، دار المسيرة للنشر والتوزيع والطباعة، الأردن ،٢٠٠٩.

ثانياً–رسائل الدكتوراه:

- د. أحمد كمال صبري، المسؤولية المدنية للمرور على شبكات المعلومات، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠١٠، ص ٢٠٥.
- د. محمد محمد الدسوقي الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة رسالة دكتوراه، جامعة القاهرة، بدون سنة نشر.
- د. سمير حسني المصري، المسؤولية التقصيرية الناشئة عن استخدام الإنترنت، دراسة مقارنة بالقانون الأنجلو أمريكي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠١٦.

ثالثاً– مراجع باللغة الإنجليزية:

- David (W) e.commerce strategy technolocies and application . Engalnd 2001
- David Bainbridge- Introduction to computer law-third edition-Pit Man publishing1996
- Casey, E ,Dijital Evidence Computer Crime 2005 San DI-ego ACADMIC PRESS,
- Chriss Reed, Internet Law- CAMPRIDGE UNIVERCITY PRESS. 2004
- Johan Eaton& jermy smithers A Managers Guide to information Technology ,London ,Philip Allan 1982.

رابعاً– المواقع الإلكترونية:

- https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1
- https://www.computer-wd.com/2021/10/zero-click-attack.html
- https://alkhabaralyemeni.net/2021/07/22/137272/