حـمـاية الأشـخـاص مـن الرسـائـل الإلـكـترونـيـة غـيـر الـمـرغـوب فـيـها

" دراســـــة مـقـــارنـــة "

دكـــــتـــور

أحـمـد عـلي حـسن عـثـمان

مـــدرس الـقـانـون الـمـدني

بكـلـية الـحقـوق – جـامـعـة الـزقـازيـق

ملخص البحث

لقد تناولت في هذا البحث مسألة حماية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها. وبدأت هذا التناول بتعريف هذه الرسائل بأنها رسائل تُرسل على نطاق واسع وبصورة متكررة لأغراض تجارية وغير تجارية مع إخفاء هوية مرسلها في أغلب الأحيان. ويتم إرسال هذه الرسائل عن طريق العديد من الوسائل التقنية والتي يعد من أبرزها البريد الإلكتروني للأشخاص. وتتميز هذا الرسائل بالعديد من الخصائص أهما: أنها تتم عبر وسيلة إلكترونية، وطابعها الجبري، وطابعها الجماعي، وعدم مرغوبية الأشخاص لها، وتعدد أهدافها، وانتمائها إلى طائفة البرمجيات الخبيثة.

وتعرضت بعد ذلك لبيان الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها. حيث بدأت هذا التعرض بكيفية تحقق هذه الحماية من خلال ضرورة موافقة الأشخاص على أن تُرسل إليهم هذه الرسائل، وصور تحقق هذه الحماية سواء من خلال اشتراط الموافقة المسبقة أو طريقة الرفض اللاحق، وبيان موقف المشرع المصري من ذلك.

وتعرضت كذلك للحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها باعتبارها مساندة للحماية القانونية. وتتم هذه الحماية من خلال بعض الوسائل الفنية كخاصية تصفية الرسائل، وأنشاء مواقع إلكترونية تحارب هذه الرسائل، والحماية من خلال إعمال خاصية التشفير.

وأخيرًا، تعرضت للحماية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها. حيث تعرضت لهذه الحماية من منظورين، أحدهما تقني والآخر قانوني. فالحماية من المنظور التقني، تتطلب توافر العديد من الأمور الفنية للمحافظة على البريد الإلكتروني، كاختيار كلمة مرور قوية، وتفقد جهة إرسال الرسالة وفحص الرسالة ذاتها قبل فتحها وعدم عرض عنوان البريد الإلكتروني للعامة و الكشف عنه. بينما تتمثل الحماية من المنظور القانوني في ضرورة التزام شركات الدعايا والإعلان بالبنود التعاقدية، ومحاولة سن تشريعات دولية، وضرورة توعية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها.

وأختتمت تعرضي لهذه الدراسة، ببيان نتائج البحث التي توصلت إليها بعد عرض محتواه،

وكذلك توصيات الدراسة، ثم قائمة بالمراجع التي استعنت بها في إتمام الدراسة، وفهرس يضم موضوعات البحث.

Abstract of research

In this paper, I address the issue of protecting people from unwanted email messages. This approach began by defining these messages as messages that are widely and frequently sent for commercial and non-commercial purposes, with the identity of their sender often anonymous. These messages are sent by many technical means, the most prominent of which is people's e-mail. These messages are distinguished by many characteristics, the most important of which are: that they are carried out via an electronic means, their forcible nature, their collective nature, the lack of desirability of people for them, the multiplicity of their goals, and their belonging to the malware class.

And then came up with a statement of legal protection for people from unwanted e-mails. As I began this exposure to how this protection is achieved through the need for people to agree that these messages are sent to them, and pictures that achieve this protection, whether through the requirement of prior approval or the method of subsequent refusal, and the position of the Egyptian legislator on that.

It was also subjected to the technical protection of people from unwanted e-mails, as it was in support of legal protection. This protection is done through some technical means, such as filtering messages, creating websites that fight these messages, and protection by implementing the encryption feature.

Finally, it has been put into general protection for people from unwanted emails. I was exposed to this protection from two perspectives, one technical and the other legal. Protection from a technical perspective requires the availability of many technical matters to preserve the e-mail, such as choosing a strong password, checking the message sender, checking the message itself before opening it, and not displaying the e-mail address to the public or disclosing it. While protection from the legal perspective is represented in the necessity for advertising companies to

adhere to contractual terms, try to enact international legislation, and the need to educate people about unwanted e-mails.

I concluded my exposure to this study, with a statement of the results of the research that I reached after presenting its content, as well as the recommendations of the study, then a list of the references that I used in completing the study, and an index that includes the research topics.

– مقدمة عامة :

لقد أصبح دور الإنترنت باعتباره وسيط تتم من خلاله التعاملات الإلكترونية، متزايدًا بصورة ملحوظة وبشكل لم يكن يتوقعه أحد في شتى مناحي الحياة. فانتشار وترويج وتبادل السلع والخدمات وإتمام صفقاتها، أصبح في كثير من الأحيان يتم عن طريق وسائل الاتصال الإلكتروني وتكنولوجيا تبادل المعلومات الحديثة.

وصاحب هذا الانتشار – رغم المزايا التي يحققها للمستخدمين أو للمتعاملين – بعض الأمور السلبية التي تجعل هؤلاء المتعاملين ينفرون أو ينزعجون من هذه الوسائل الحديثة. ويعد من أبرز هذه الأمور، انتشار ظاهرة إرسال الرسائل الإلكترونية غير المرغوب فيها أو المزعجة، وما تخلّفه من آثار سلبية في نفوس الأشخاص، وخلقت لديهم بعض التخوفات أو الحذر بصدد استخدامهم لتكنولوجيا الاتصالات والمعلومات بوسائلها المتعددة.

وتعد ظاهرة الرسائل الإلكترونية غير المرغوب فيها، من الأمور التي تشغل الرأي العام الإلكتروني وذلك بسبب التزايد المستمر لاستخدام الإنترنت في إبرام التعاملات سواء المدنية أو التجارية. حيث يتوافق ظهور وانتشار هذه الظاهرة مع ظهور وانتشار التعاقد الإلكتروني، الذي

أصبح منتشرًا بصورة كبيرة وخصوصًا في مجال التجارة الإلكترونية؛ لاسيما في ظل تبني العديد من الدول سياسة التحول الرقمي [1].

وتـعـد جمـهورية مصر العربية، من الدول التي بدأت تتجه وبقوة نحو سياسة التحول الرقمي. وهذه خطوة طال انتظارها بحق، لما في ذلك من مسايرة للتطورات الواقعية والتكنولوجية الحديثة، والتي يجب ألا يكون بلدنا بمعزلٍ عنها. وأيضًا لما في انتهاج هذه السياسة من العديد من المزايا في جميع النواحي، سواء السياسية أو الاقتصادية أو غيرهما، وخصوصًا تأثيرها الإيجابي على الاقتصاد الرقمي للدولة.

وترتيبًا على ما تقدم وبسبب انتشار التعاقدات الإلكترونية، ظهرت مشكلة إرسال الرسائل

---

[1] – يهدف التحول الرقمي إلى تقديم خدمات متميزة للمواطنين من خلال معاملات إلكترونية، والتي تُسهم في القضاء على الفساد، من خلال مشروع التحول لمجتمع رقمي يهدف إلى إتاحة الخدمات الرقمية بطرق بسيطة، وتكلفة ملائمة في أي وقت وأي مكان لجميع المؤسسات والمواطنين من خلال تطوير منظومة رقمية متكاملة مؤمنة على المستوى القومي، وكذلك تحفيز الصناعات الرقمية من خلال جذب الاستثمارات الأجنبية، وخلق فرص عمل عن طريق دعم وتنمية الصناعة الرقمية والإبداع التكنولوجي، وإنشاء ممر مصر الرقمي لضمان تحقيق الاستغلال الأمثل لموقع مصر الجغرافي لتصبح مركزًا عالميًا لخدمات الاتصالات وتكنولوجيا المعلومات..... أنظر في ذلك الرابط التالي:

- https://gate.ahram.org.eg/News/1992424.aspx (27-4-2021).

الإلكترونية غير المرغوب فيها؛ وذلك لأن هذه التعاقدات تتم عبر شبكة الإنترنت من خلال أدوات وتقنيات حديثة للغاية بعضها يتسم بالوضوح والبساطة بعض الشيء، والكثير منها يتسم بالتعقيد التقني والفني العالي، والتي يكون من المستعصي على عموم الأشخاص فهمها أو القدرة على التعامل معها بصورة كاملة، الأمر الذي ترتب عليه انتشار إرسال المذكورة للأشخاص عبر وسائل تقنية متعددة أبرزها الإرسال عن طريق عناوين البريد الإلكتروني لهؤلاء الأشخاص دون وجود الضمانات القانونية للازمة لذلك.

- إشكالية البحث:

تتمثل الإشكالية الأساسية لهذه الدراسة، في البحث عن بعض الضمانات التي تكفل عدم إرسال رسائل إلكترونية غير مرغوب فيها للأشخاص وذلك عنما يقومون بإبرام التعاملات الإلكترونية عبر شبكة الإنترنت، على نحو يبعث الثقة والطمأنينة في نفوسهم حال قدومهم على إبرام، وخصوصًا وأن هذه التعاملات تفتقد في كثير من الأحيان إلى الضمانات التي تتوافر في التعاملات المدنية التقليدية.

وترجع صعوبة مشكلة البحث في هذا الصدد، إلى الندرة الكبيرة في المراجع التي تعرضت لهذه المسألة؛ لكونها مسألة لم يتعرض لها الكثير من فقهاء القانون ولاسيما الفقه العربي. وإذا كان كان هناك تعرض لها، فهو تعرض بسيط غير متعمق؛ ذلك سنتناولها – بمشيئة الله تعالى – بصورة تفصيلة في هذا البحث.

وتثير إشكالية هذا البحث العديد من التساؤلات القانونية التي سنجيب عنها – بمشيئة الله – من خلال هذا البحث، والتي تتمثل في الآتي:

1- ما هو المقصود بالرسائل الإلكترونية غير المرغوب فيها؟

2- كيف تُرسل الرسائل الإلكترونية غير المرغوب فيها للأشخاص؟

3- ما هي خصائص الرسائل الإلكترونية غير المرغوب فيها؟

4- كيفية الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها؟

5- ما هي صور تحقق الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها؟

6- ما هي صور تحقق الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها؟

7- ما هي صور تحقق الحماية التقنية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها؟

8- ما هي صور تحقق الحماية القانونية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها؟

- أهمية البحث:

تتبلور أهمية هذا البحث بالدرجة الأولي في الاعتبارات العملية، التي تتأتى من خلال قيام الأشخاص بسلوك التعاقدات الإلكترونية في شتى المجالات، سواء من الناحية المدنية أو من الناحية التجارية في مجال التجارة الإلكترونية. ويرجع ذلك إلى أن هذه التعاملات تتم عبر وسيط إلكتروني من خلال عالم افتراضي وهو عالم الإنترنت؛ فكانت من المسائل الشاغلة لأذهان المتعاملين، هي مسألة الرسائل الإلكترونية غير المرغوب فيها وكيفية حماية الأشخاص منها.

فإذا ما توافر للمتعامل الضمانات اللازمة لحمايته من هذه الرسائل، انعكس ذلك على نطاق استخدام التعاقدات التي تتم عبر وسائط إلكترونية بقدر قليل من القلق أو المخاوف التي تنتاب الكثير من الأشخاص بصدد هذه التعاملات، مما سيكون له بالغ الأثر على كثرة انتشار هذا التعاملات من ناحية، والتأثير الإيجابي من الناحية الاقتصادية للتعاملات الإلكترونية من ناحية أخرى.

- منهج البحث:

في إطار تعرضنا لموضوع حماية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها، سنعتمد على المنهج التأصيلي، والمنهج التحليلي، والمنهج المقارن. فالمنهج التأصيلي يكون من خلال رد الفروع والجزئيات إلى أصولها في القواعد العامة المعروفة في القانون المدني من أجل فهم جوانب هذا الموضوع. وسيأتي اعتمادنا على المنهجين التحليلي والمقارن من خلال تحليل مظاهر حماية الأشخاص من هذه الرسائل في التشريعين الفرنسي والمصري ، ومقارنة هذه المظاهر ببعضها البعض.

- خطة البحث:

سنتناول – بمشيئة الله تعالى – موضوع حماية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها من خلال مبحث تمهيدي وثلاثة فصول، على النحو التالي:

المبحث التمهيدي: ماهية الرسائل الإلكترونية غير المرغوب فيها.

المطلب الأول: تعريف الرسائل الإلكترونية غير المرغوب فيها.

المطلب الثاني: كيفية إرسال الرسائل الإلكترونية غير المرغوب فيها.

المطلب الثالث: خصائص الرسائل الإلكترونية غير المرغوب فيها .

<u>الفصل الأول</u>: الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها.

المبحث الأول: كيفية الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها.

المبحث الثاني: صور تحقق الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها.

المطلب الأول: : الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها من خلال اشتراط الموافقة المسبقة (مبدأ التقيد).

المطلب الثاني: الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها من خلال إعمال مُكنة إلغاء الاشتراك (نظام قائمة الرفض أو الاعتراض) (نظام الرفض اللاحق).

المبحث الثالث: موقف المشرع المصري من مسألة الموافقة على إرسال أو استقبال رسائل إلكترونية غير مرغوب فيها.

<u>الفصل الثاني</u>: الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها.

المبحث الأول: الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها عن طريق خاصية تصفية الرسائل.

المبحث الثاني: الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها عن طريق إنشاء مواقع إلكترونية لمحاربتها.

المبحث الثالث: : الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها عن

طريق إعمال خاصية التشفير.

الفصل الثالث: الحماية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها.

المبحث الأول: الحماية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها من منظور تقني.

المبحث الثاني: الحماية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها من منظور قانوني.

المبحث التمهيدي

ماهية الرسائل الإلكترونية غير المرغوب فيها

- تقسيم:

سأتناول بيان ماهية الرسائل الإلكترونية غير المرغوب فيها، من خلال التعرض لتعريف هذه الرسائل (مطلب أول)، ثم التعرض لكيفية إرسال هذه الرسائل (مطلب ثان)، وأخيرًا التعرض لخصائص هذه الرسائل (مطلب ثالث). وذلك على البيان التالي:

المطلب الأول

تعريف الرسائل الإلكترونية غير المرغوب فيها

لاشك أن شبكات وخدمات الاتصالات الإلكترونية الحديثة – المتقدمة والمتطورة – أصبحت جزءًا من الحياة اليومية سواء في المكاتب أو في المنازل، وهو أمر يتضح أكثر وأكثر كل يوم، وحقيقة واقعية لا يستطيع أحد إنكارها أو جحدها.

غير أن هذا التطور رغم ما يحققه من مزايا للأشخاص على جميع المستويات، إلا أنه لا

يخلو بالتأكيد من بعض المخاطر والمشكلات التي كانت ومازالت سببًا رئيسيًا في تنفير وإزعاج الأشخاص من هذه التقنيات المتطورة. ويعد من أبرز وأهم المشكلات، تلك الخاصة بالرسائل الإلكترونية غير المرغوب فيها.

وقبل أن نتعرض لبيان المقصود بالرسائل الإلكترونية غير المرغوب فيها، فإن المرادفات الإصطلاحية لهذه الرسائل تتعدد، كتسميتها بالبريد الإلكتروني العشوائي، والبريد الإلكتروني غير المرغوب فيه، والبريد الإلكتروني الإحتيالي، والرسائل التطفلية، والرسائل المزعجة.

ولقد تعددت التي التعريفات التي قيلت بشأن تحديد المقصود بالرسائل الإلكترونية غير المرغوب فيها أو البريد الإلكتروني العشوائي. فعرفها جانب فقهي بأنها عبارة عن رسائل يقوم بإرسالها المرسل على نطاق واسع ولأغراض تجارية عن طريق إخفاء هويته أو تزويرها. وتُعرف أيضًا بأنها رسائل إلكترونية غير مرغوب فيها بصرف النظر عن محتواها [1].

ومن جانبها عرفت اللجنة الوطنية للمعلوماتية والحريات (La Commission National de L'informatique et libertés) [2]، بأنها عبارة عن ممارسة لإرسال رسائل البريد الإلكتروني غير المرغوب فيها بأعداد كبيرة وبصورة متكررة لأفراد لا تربطهم رابطة عقدية بالمرسل إليهم، والذي

---

[1] - Schryen ، Guido , Anti-Spam Measures , Analysis and Analysis and Design , provides a detailed over view of the technological , organizational and economic facets of spam- emails , Springer – p.7.

[2] – عن هذه اللجنة، أنظر الموقع التالي:

- https://www.cnil.fr/fr/definition/commission-nationale-de-linformatique-et-des-libertes-cnil(29-3-2021).

يتحصل على عناوين بريدهم الإلكتروني بشكل غير صحيح [1].

كما عرفها البعض أيضًا، بأنها عبارة عن إرسال نسخ مكررة لعدد كبير من نفس الرسالة عبر نظام المراسلات الخاص بالبريد الإلكتروني، بما يترتب عليه عدم انتظام سير النظام التقني المعلوماتي [2].

ومن الناحية التاريخية، فإن أول بريد إلكتروني عشوائي تم إرساله في 3 مايو 1978 بواسطة شخص يعمل مسوق في شركة (Equipment Corporation Digital)، عندما قام بإرسال رسالته إلى حوالي (600) شخص من المستخدمين المهتمين بالتكنولوجيا يعيشون على الساحل الغربي للولايات المتحدة الأمريكية؛ وذلك من أجل دعوتهم إلى عرض توضيحي لمجموعة (Equipment Corporation Digital). وعلى الرغم من قيام هذا الشخص المرسل بالإرسال بحسن نية رغبةً منه في تجنب كتابة الرسالة التوضيحية لكل شخص على حدة، إلا أن الإدارة الأمريكية أدانت الشبكة الممارسة بحكم منصبها على أساس أن هذا الأمر غير متوافق مع شروط استخدام الشبكة[3].

وترجع خطورة الرسائل الإلكترونية غير المرغوب فيها أو البريد الإلكتروني العشوائي، إلى أن

---

[1] - Schryen ، Guido , op. cit , p. 7.

[2] – د/ خالد ممدوح إبراهيم، أمن المستندات الإلكترونية، دار الجامعة الجديدة، سنة 2008، ص 158.

[3] – أنظر في ذلك الرابط التالي:

- https://fr.wikipedia.org/wiki/Spam#Histoire(29-3-2021).

هذا الأمر قد أصبح نشاطًا في حد ذاته؛ حيث يقوم مرسلوا هذا البريد العشوائي بتأجير أو بيع العناوين التي يتحصلون عليها إلى شركات السلع والخدمات المختلفة. بالإضافة إلى أن هذا البريد لم يعد مجرد مصدر إزعاج فحسب، بل أصبح بصورة تدريجية نشاطًا ذا طبيعة احتيالية وإجرامية[1].

وخير مثال على ذلك استخدام رسائل البريد الإلكتروني المخادعة من أجل إقناع المستخدم بالكشف عن بيانات سرية وذلك باستخدام موقع غير رسمي يُزعم أنه يمثل شركات حقيقية، مما يثير المخاوف من حالات سرقة الهوية المحتملة والإضرار بسمعة الشركة. كما أن استمرار توزيع برامج التجسس عن طريق البريد الإلكتروني أو البرامج التي تتبع سلوك المستخدم عبر الإنترنت والإبلاغ عنه؛ حيث يمكن لهذه البرامج أيضًا جمع المعلومات الشخصية عن المستخدم مثل كلمات المرور وأرقام بطاقات الائتمان [2].

ويعد من أهم مظاهر الخطورة الناشئة عن إرسال الرسائل الإلكترونية غير المرغوب فيها، المحتوى الذي يتضمنه هذا البريد؛ حيث إنه كثيرًا ما يكون متضمنًا إعلانات تروج لمنتجات وخدمات غالبًا ما تكون إباحية وكذلك العقاقير – وغالبًا ما تكون عبارة عن منشطات جنسية أو هرمونات تُستخدم في مكافحة الشيخوخة أو فقدان الوزن – وبعضها يكون له علاقة بالائتمان

---

[1] - Document de la Commission COM (2006) 688 final du 15 novembre 2006 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la lutte contre la pourriel, les espiogiciels et les logiciels malveillants ….. .... https://www.dalloz.fr/documentation/Document

[2] – المرجع السابق.

المالي ومنها ما يتعلق بالخرافات كعلم التنجيم [1].

ويعد من صور الإحتيال الذي يحدث عن طريق إرسال الرسائل الإلكترونية غير المرغوب فيها ، أن يرسل المحتالون عروضًا يزعمون أنها بإمكانها إثراء المستخدم بسرعة كالعمل من المنزل ونصيحته بشراء الأسهم الصغيرة مثلًا. ومن ذلك أيضًا، خداع المستلم عن طريق تمرير بريد إلكتروني إليه يتضمن رسالة من بنك أو من أي خدمة تكون محمية بكلمة مرور بهدف استعادة البيانات الشخصية للمستلمين، وعلى وجه الخصوص كلمات المرور ورقم البطاقة المصرفية، وذلك عن طريق جذبهم إلى موقع وهمي يسجل جميع تصرفاتهم [2].

وما يسهل الإحتيال المتقدم، هو سهولة الإرسال المكثف للرسائل الإلكترونية غير المرغوب فيها بشكل كبير من خلال انتشار الشفرات الضارة مثل الفيروسات المتنقلة؛ فالفيروسات بمجرد تثبيتها تسمح للمهاجمين بالسيطرة على نظام الكمبيوتر المصاب وتحويله إلى (بوت نت) (Botnet) [3] عن طريق إخفاء هوية مرسل البريد العشوائي الحقيقي؛ حيث يتم استئجار شبكات

---

[1] – أنظر في ذلك الموقع التالي:

- https://fr.wikipedia.org/wiki/Spam#Histoire(29-3-2021) -

[2] – الموقع السابق.

[3] – البوت نت Botnet هو مجموعةٌ من أجهزة متصلة ببعضها عبر شبكة إنترنت، قد تكون هذه الأجهزة حواسب أو هواتف ذكية أو خوادم أو أجهزة أخرى تعرف بإنترنت الأشياء، وجميع هذه الأجهزة المتصلة تكون مصابة ويتم التحكم بها عبر نوع من البرامج الخبيثة، وفي حالات عديدة قد لا يدرك المستخدم أن حاسبه يتعرض لهجوم أو إصابة بوت نت. والأجهزة المصابة

(البوت نت) من قبل مرسلي البريد العشوائي ومقدمي برامج التجسس؛ تحقيقًا لأغراض إحتيالية وإجرامية [1].

وعلى ذلك فالرسائل الإلكترونية غير المرغوب فيها، قد تتضمن محتوى غير لائق أو محتوى مضلل. فمن أمثلة المحتوى غير اللائق، أن توضع صورة غير أخلاقية من أجل لفت انتباه الكثير من زوار موقعك الخاص بك كمرسل، وبالتالي حصولك على نقرات أكبر للعرض الذي تسوق له. ومن أمثلة المحتوى المضلل، أن تضع في موقعك روابط لتحميل ملف يتوجه له الزوار عادة ليحصلوا على الملف الذي تقدمه لهم، وعند نقرهم على رابط التحميل يتم توجيههم إلى موقع العرض بدًلا من الملف [2].

يتم التحكم بها عبر منفذين للجرائم أو مفتعلي المشاكل، أحيانًا ما يكونوا مجرمي إنترنت، ويتم استغلال الأجهزة المصابة أو الضحية لعملياتٍ معيّنة ومحددة، كي لا يلاحظ المستخدم شيء، وبالتالي تبقى العمليات الخبيثة مخفية عن عينه وإدراكه..... أنظر في ذلك الموقع التالي:

- https://www.arageek.com/l/ (30-3-2021)

[1] - Document de la Commission COM (2006) 688 final du 15 novembre 2006 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la lutte contre la pourriel, les espiogiciels et les logiciels malveillants . ….. https://www.dalloz.fr/documentation/Document

[2] – د/ رياض سامر، دليلك المختصر للعمل كمسوق بالعمولة، Edward R، بدون سنة نشر، ص 38.

وعلى الرغم من المخاطر الكثيرة والمضار المتعددة الناشئة عن إرسال الرسائل الإلكترونية غير المرغوب فيها أو رسائل البريد الإلكتروني العشوائي، إلا أنه توجد بعض المغريات التي تجعل الكثير من الأشخاص والجهات يلجأون إليها وخصوصًا على الجانب الإقتصادي في هذا الشأن. فمن ناحية نجد أن إعلانات رسائل هذا البريد قليلة التكلفة المالية [1]، وسريعة الإنتشار عن رسائل الإعلانات العادية؛ ويرجع ذلك إلى أن هذه الرسائل تتضمن في غالب الأمور وسائل جذب قوية للأشخاص تحثهم على فتح الرسالة وقراءة الإعلانات، كوضع صورة ما في مقدمة الإعلان تلفت نظر الشخص أو مقطع فيديو قصير المدة يجعله ينجذب بشدة لمعرفة محتوى الإعلان الذي تتضمنه رسائل البريد الإلكتروني العشوائي [2].

ومن ناحية ثانية، فإن هذه الإعلانات تمكن الأشخاص من التعرف على المنتجات والخدمات التي يتم الإعلان عنها، ومن خلالها أيضًا يعرفون المواقع الجديدة التي تعرض هذه المنتجات والخدمات، وهذا الأمر يترتب عليه زيادة عدد هؤلاء الأشخاص بما يخدم مصالح المعلنين ويزيد من إقبال الأشخاص على السلع والخدمات محل الإعلان.

وما يؤيد هذا الأمر، أن رسائل البريد الإلكتروني العشوائي لها أثر اقتصادي كبير لا يُستهان بما يجعلها محفزة لمن يرسلونها؛ حيث اعترف ما يقرب من 11% من مستخدمي الإنترنت – في

---

[1] - Document de la Commission COM (2006) 688 final du 15 novembre 2006 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la lutte contre la pourriel, les espiogiciels et les logiciels malveillants . ….. https://www.dalloz.fr/documentation/Document

[2] – د/ شريف محمد غنام، التنظيم القانوني للإعلانات التجارية عبر شبكة الإنترنت، ص 95.

بعض الفترات – بشراء منتجات بعد تلقي رسائل دعائية غير مرغوب فيها، وذلك بناءً على دراسة أجرتها الشركة البريطانية (SDPHOS 16) [1].

وعلى الرغم من مغريات البريد الإلكتروني العشوائي وخصوصًا قلة تكلفته المادية، إلا أن أثر ذلك كبير وخطير من الناحية المعنوية؛ وذلك لأن الرسائل العشوائية لها تكلفة اجتماعية بطبيعتها، حيث إنها لا تراعي مبدأ حسن النية بالقدر الكافي، وعدم مراعاة معنويات المستخدم وإحباطه لكونها تتجاهل مسألة ثقته الإلكترونية. علاوة على تعريض مسؤولية شركات خدمات تكنولوجيا المعلومات للخطر حال فشلها في القضاء على البريد الإلكتروني العشوائي بشكل فعال [2].

المطلب الثاني

كيفية إرسال الرسائل الإلكترونية غير المرغوب فيها

والسؤال الذي يُثار هنا هو: كيف يتحصل مرسلوا الرسائل الإلكترونية غير المرغوب فيها على عناوين البريد الإلكترونية للأشخاص والتي عن طريقها يستطيعون إرسال مثل هذه الرسائل إليهم؟

إن التحصل على البريد الإلكتروني في هذا الشأن، يكون عن طريق ما يعرف بتجميع

---

[1] - John Leyden , "30 years of spam and we ain’t finished yet " , the Register , 1er mai 2008.

[2] - Nathalie Dagorn, « Sensibilisation aux coûts et conséquences du spam», Terminal, OpenEdition Journals, no 105 « Technologies et usages de l'anonymat sur Internet », 1er octobre 2010 (ISSN 0997-5551,DOI 10.4000/terminal.1897, lire en ligne , consulté le9 décembre 2019).

عناوين هذا البريد للأشخاص، وذلك عن طريق قيام المتطفل أو المحتال بالوصول إلى هذه العناوين بالعديد من التقنيات الإلكترونية ذات الطابع غير المشروع [1]؛ وذلك من أجل استخدام هذه العناوين في إرسال الرسائل غير المرغوب فيها لهؤلاء الأشخاص، وغالبًا ما يكون هذا الإرسال من منطلق دوافع تجارية لتحقيق مكاسب مادية.

وبصدد إجابتنا عن التساؤل المذكور، سنفرق بين حالتين لتجميع عناوين البريد الإلكتروني وهما: حالة التجميع الرضائي، وحالة التجميع غير الرضائي:

1- الحالة الأولى: حالة التجميع الرضائي لعناوين البريد الإلكتروني: وفي هذه الحالة يتم التحصل على عناوين البريد الإلكتروني للأشخاص برضاهم التام ودون أي معارضة تذكر منهم. ويتأتى هذا الإدلاء الاختياري من منطلق أن هذا العنوان أصبح ضروريًا من أجل الحصول على العديد من الخدمات التي يشترط مقدموها والسلع التي يشترط منتجوها ضرورة إفصاح المستخدم أو المتعامل عن عنوان بريده الإلكتروني.

وتفسير ذلك أن البريد الإلكتروني يعتبر أقدم وأهم وأبرز وسيلة تعامل آمنة وتخلق قدرًا كبيرًا من الثقة الإلكترونية في نفوس الأشخاص، وغالبًا ما يكون متطلبًا ضروريًا من قبل الجهات والهيئات والمؤسسات التي تعلن عن بعض الأمور التي تخصها وترغب في إعلام الأشخاص بها، كما في حالة الإعلان عن مسابقات للتعيين في وظيفة معينة أو الإعلان عن بيع أو شراء سلع معينة.

---

[1] – في هذا المعنى، أنظر:

-Dimitri Perret, « 10 ans de spam : l'ère du phishing ciblé » [archive], Vade Secure, 21 novembre 2015 (consulté le 9 décembre 2019).

ويعتبر تجميع عناوين البريد الإلكتروني في مثل هذه الحالة أمرًا مشروعًا وصحيحًا من الناحية القانونية، وذلك بشروط أهما:

أ- أن يكون الإدلاء أو الإفصاح عن عنوان البريد الإلكتروني قد تم بإرادة صاحب البريد دون أن يشوب إرادته عيب من عيوب الرضا: فلا يكون الإفصاح مشروعًا إذا تم نتيجة وقوع صاحب العنوان في غلط [1]، أو تم نتيجة تدليس[2]، أو بسبب إكراه وقع عليه[3]، أو كان مرجع الإفصاح وقوع الشخص في مصيدة الإستغلال [4].

ب- الإلتزام بالغرض الذي من أجله تم التحصل على عناوين البريد الإلكتروني الخاصة

---

[1] – والمثال على ذلك، أن يفصح الشخص عن عنوان بريده الإلكتروني بمناسبة شراء سلعة معينة ظنًا منه وجود بند في العقد يلزمه بالقيام بذلك، وفي الحقيقة لا يكون لهذا البند وجود.

[2] – والمثال على ذلك، أن يقنع شخص آخر بأي وسائل احتيالية بضرورة إفصاحه عن عنوان بريده الإلكتروني وإلا لن يستطيع شراء السلعة أو الحصول على الخدمة محل التعاقد.

[3] – والمثال على ذلك، أن يمارس شخص على صاحب عنوان البريد الإلكتروني إكراهًا معنويًا، كأن يهدده بقتل ابنه أو ابنته أو إفشاء أسرار عائلته ذات الطابع الشخصي المحض، وذلك من أجل الإفصاح عن عنوان بريده الإلكتروني.

[4] – والمثال على ذلك، أن تستغل فتاة شديدة الجمال في مقتبل عمرها، ولوع رجل مسن بها على درجة من الثراء، بأن تعلق زواجه منها على حصولها على عنوان بريده الإلكتروني والذي يكون عليه الكثير من الأسرار المهنية والشخصية لهذا الرجل من أجل بيعها إلى خصومه واستغلالها ضد مصلحته.

بالأشخاص: وهذا الشرط ينبع من الالتزام بالسرية بوجه عام، لاسيما وأن عنوان البريد الإلكتروني هو بيانًا شخصيًا ويمس مصالح صاحبه بدون شك. وعلى ذلك يلتزم من يتحصل على أي عنوان بريد إلكتروني بعد استخدام هذا العنوان أو الإفصاح عنه للغير، وإلا كان في ذلك إخلاًلا بالالتزام بالسرية الملقى على عاتقه.

وفي هذه الحالة يثور التساؤل بشأن الفرض الذي يكون فيه الشخص في احتياج لسلعة أو خدمة تتطلب الإفصاح عن عنوان بريده الإلكتروني، ويكون لدى هذا الشخص تحفظ أو رفض في بعض الأحيان بخصوص هذا الإفصاح، فما الحل القانوني لذلك؟

نرى في هذا الفرض أنه من أجل التوفيق بين حصول الشخص على السلعة أو الخدمة التي تتطلب الإفصاح عن عنوان بريده الإلكتروني وبين رغبته في الحفاظ على سرية هذا العنوان، يجب التفاوض مع الطرف المعلن عن السلعة أو الخدمة بشأن مدى امكانية إعفاء هذا الشخص من الإفصاح عن هذا العنوان وذلك إذا كان عدم الإفصاح عنه لا يؤثر على الحصول على هذه الخدمة أو تلك السلعة. وإذا تعذر هذا الأمر وأصر الطرف المعلن على الحصول على هذا العنوان، فيجب التشديد على هذا الطرف بصورة كبيرة بضرورة التزامه بالحفاظ على سرية هذا العنوان، كأن يتم الاتفاق بين الطرفين على اعتبار التزام المعلن أو الذي يتحصل على هذا العنوان بتحقيق نتيجة بدًلا من كونه التزامًا ببذل عناية وفقًا للأصل العام [1].

---

[1] – وإن كان يتعذر إعمال هذا الاتفاق من الناحية الواقعية؛ وذلك بسبب صعوبة ضمان المعلن أو المتحصل على البريد الإلكتروني عدم حدوث اختراق أو حدوث اعتداء على هذا البريد لاسيما في ظل تعقد وتعدد الطرق الإحتيالية. غير أنه يمكن اعتبار هذا الاتفاق بمثابة التزام تشديدي

2- الحالة الثانية: حالة التجميع غير الرضائي لعناوين البريد الإلكتروني: وفي هذه الحالة يتم تجميع عناوين البريد الإلكتروني بدون موافقة الشخص صاحب البريد الإلكتروني. ويتحقق هذا الأمر في الحالات الآتية:

أ- تجميع عناوين البريد الإلكتروني من خلال النظام المعروف باسم (القاموس المهاجم) أو (نظام التخمين): وهذه الطريقة تقوم على أساس فكرة التخمين الذي يقوم به المهاجم، وذلك عن طريق اختيار أسماء ذات معنى وإجراء إضافات لنطاقات البريد الإلكتروني، وبعد ذلك تُرسل الإعلانات التجارية إليها، وبعدها إذا انتهى التخمين إلى مصادفة الحقيقة ووصل الإعلان عبر البريد الإلكتروني الذي تم تخمينه، كان صحيحًا ويتم تسجيله في قائمة يسجل فيها البريد الإلكتروني الذي تم التوصل إليه حتى يتم الإرسال مرة أخرى لهذا البريد ويتم معرفة العناوين النشطة من بين مجموعات العناوين المنتجة من القاموس وذلك من خلال رد المتلقي أو المرسل إليه على الإعلانات المرسلة أو عن طريق تتبع الرابط الخاص بالعنوان المختار من خلال بعض برامج التجسس [1].

ب- تجميع عناوين البريد الإلكتروني عن طريق شراء قواعد البيانات: وهنا يقوم المحتال

يقع على عاتق المتحصل ببذل أقصى وأكبر جهد في سبيل الحفاظ على عناوين البريد الإلكتروني التي يُتحصل عليها.

[1] - د/ خالد بن سليمان العثبر؛ د/ سليمان بن عبد العزيز بن هيشة، الاصطياد الإلكتروني، الأساليب والإجراءات المضادة، مركز التميز لأمن المعلومات، الطبعة الأولى، جامعة الملك سعود، الرياض، سنة 2009، ص 34.

بشراء قواعد بيانات كاملة تتضمن الملايين من عناوين البريد الإلكتروني من الشركات المتخصصة في إنشاء مثل هذه القواعد. وهذه الطريقة قليلة التكلفة من الناحية المادية [1].

والحقيقة أن تجميع عناوين البريد الإلكتروني من خلال هذه الطريقة، هو أمر على درجة كبيرة من الانتشار ويلمسه الكثير منا عند قيامه بشراء سلع أو خدمات، فتشترط عليه الشركة أو من بيده هذه السلعة أو تلك الخدمة، ضرورة إفصاح الأشخاص عن عناوين بريدهم الإلكتروني، وفعل ذات الأمر مرارًا وتكرارًا، ومن ثم يتوفر لديهم رصيد هائل من العناوين، تستطيع هذه الشركات استغلاله أو بيعه لجهات أو شركات أخرى.

وما يزيد الأمور تعقيدًا هو التبادل الذي يحدث بين الشركات وبعضها البعض من خلال فكرة استكمال العناوين بين الشركات المختلفة، بمعنى أن الشركة التي يتوافر لديها عناوين بريد إلكتروني ولا تتوافر لدى شركة أخرى ويكون لدى هذه الأخيرة عناوين لا تتوافر للشركة الأولى، فيتم التبادل بينهما، بحيث يتوافر لدى كل شركة رصيد ضخم من عناوين البريد الإلكتروني لدى الجهات والشركات.

ج- تجميع عناوين البريد الإلكتروني عن طريق نظام الحصاد: وهنا يتم الحصول على عناوين البريد الإلكتروني المسجلة في الخادم وكذلك عناوين الأشخاص الموجودين في غرفة الدردشة وأي وسيط إلكتروني آخر شريطة أن يكون هذا الوسيط متصًلا بالإنترنت. وتوضيح ذلك، أنه عن طريق الاستعانة ببعض البرامج يستطيع الشخص أو الشركة معرفة البريد الإلكتروني لكل مستخدم عند تشغيله البرنامج، ثم يقوم البرنامج بجمع هذه العناوين في قائمة موحدة. كما يمكن

[1] - د/ شريف محمد غنام، مرجع سابق، ص 101.

للبرنامج أن يجمع عناوين البريد الإلكتروني للأشخاص الذين يقومون بالمحادثة الشفهية أو ما يُعرف بالدردشة، وكذلك كل الأشخاص المشتركين في دوائر الحوار والأدلة التي تنشر قوائم المشتركين في بعض الخدمات. ثم يُضاف إلى هذه الأسماء اسم كل مستخدم في كل مرة يستعمل فيها شبكة الإنترنت ويُكتب قرين كل مستخدم المواقع التي تجول فيها [1].

المطلب الثالث

خصائص الرسائل الإلكترونية غير المرغوب فيها

تتميز الرسائل الإلكترونية غير المرغوب فيها، ببعض السمات التي تجعلها تتميز عن غيرها من الرسائل الأخرى أو وسائل التواصل، والتي نستخلصها من الطابع الخاص لهذه الرسائل وما تهدف إليه، وهي:

أولًا: الرسائل غير المرغوب فيها تُرسل عبر وسيلة إلكترونية [2]:

بادئ ذي بدء، يُقصد بالرسائل على وجه العموم كل كتابة يوجهها شخص إلى شخص آخر، ويوصلها له عن طريق البريد أو أية وسيلة أخرى [3]. ومن ذلك نجد أن الرسالة قد يتم إرسالها عن طريق البريد أو حتى تسليمها باليد لمن تُرسل إليه. أما الرسائل غير المرغوب فيها فهى تُرسل عبر وسيلة إلكترونية، غالبًا ما تكون البريد الإلكتروني.

---

[1] – المرجع السابق، ص 102، 103.

[2] - Schryen ، Guido , op. cit , p. 8.

[3] – د/ أسامة أبو الحسن مجاهد، الوجيز في قانون الإثبات، دار النهضة العربية، سنة 2018، ص 66.

والبريد الإلكتروني – باعتباره الوسيط أو الدعامة الإلكترونية [1] الذي تُرسل عليه الرسائل غير المرغوب فيها – هو كل رسالة أيًا كان شكلها، نصية أو صوتية، مصحوبة بصور وأصوات يتم إرسالها عبر شبكة عامة للاتصالات، ويتم تخزينها على أحد خوادم هذه الشبكة أو في المعدات الطرفية للمرسل إليه حتى يتمكن هذا الأخير من استعادتها [2].

مع ملاحظة أن الأمر المتقدم لا يعني اقتصار إرسال أو استقبال الرسائل غير المرغوب فيها عن طريق البريد الإلكتروني فقط ، بل يمكن إرسالها كذلك بواسطة رسائل إلكترونية عبر

---

[1] – الدعامة الإلكترونية عرفتها اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 بتنظيم التوقيع الإلكترونى، في المادة (14/1) منها، بأنها وسيط مادى لحفظ وتداول الكتابة الإلكترونية ، ومنها الأقراص المدمجة أو الأقراص الضوئية أو الأقراص الممغنطة أو الذاكرة الإلكترونية أو أى وسيط آخر مماثل.كما عرفها المشرع المصري أيضًا في المادة (1) من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، بأنها أى وسيط مادى لحفظ وتداول البيانات والمعلومات الإلكترونية ومنها الأقراص المدمجة أو الأقراص الضوئية والذاكرة الإلكترونية أو ما فى حكمها .

[2] – د/ عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، بدون سنة نشر، ص 14؛ وعرفه المشرع المصري في المادة (1) من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، بأنه وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعى أو اعتبارى، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلى وما فى حكمها.

وسيط إلكتروني غير البريد الإلكتروني – كواتس آب أو فيس بوك مثلًا – أو بواسطة الرسالة القصيرة (SMS) – ومن ذلك الرسائل اليومية التي تُرسل ترويجًا لبيع السلع والخدمات والعقارات–، وأيضًا عن طريق الرسائل المتعددة للهاتف المحمول، وخدمات الرسائل الفورية [1].

ثانيًا: الطابع الجبري للرسائل الإلكترونية غير المرغوب فيها:

المعروف وفقًا لقواعد القانون المدني وفقًا للأصل العام، أن إبرام أي تعاقد إنما يلزم أن يكون بتراضي الطرفين على ذلك؛ إعمالًا لقاعدة أن الأصل في العقود الرضائية التي تفترض أن العقود تُبرم بوجود إيجاب وقبول صحيحين وتلاقيهما بصورة قانونية بغية إبرام العقد.

غير أن الرسائل الإلكترونية غير المرغوب فيها، يتعارض إرسالها مع القول السابق؛ وذلك لأن مرسلها إنما يرسلها بغير موافقة أو رضاء من تُرسل إليه هذه الرسائل وحتى دون طلبه ممن أرسلها [2]، لذلك فهي تتسم بالطابع الجبري أو القسري.

والحقيقة أن هذا الطابع الجبري أصبح أمرًا منتشرًا بصورة واسعة ومنفرة على جميع وسائل التواصل والكثير من المواقع الإلكترونية التي يزورها الأشخاص بمختلف ميولهم. حيث يلاحظ الكثير منًا أثناء تصفحه أي موقع، ظهور الكثير من الإعلانات والترويج للسلع والخدمات التي يُظهرها المتحكمين في هذه المواقع وذلك دون أخذ موافقة الأشخاص أو حتى محاولة إخطارهم بها مسبقًا قبل إظهارها لهم.

وخطورة الأمر لا تتمثل فقط في ظهور هذه الأمور دون موافقة الأشخاص، بل الخطر

---

[1] - Schryen ، Guido , op . cit , p.8.

[2] - Schryen ، Guido , op . cit , p.8.

الأكبر هو المحتوى الذي تتضمنه. فكثيرًا ما تتضمن محتوى عنيف يبث روح الضغينة والعداء والقتالية في نفوس الكثير – وخصوصًا فئة الأطفال – أو احتوائها على محتوى منافٍ للآداب العامة كالترويج للإباحية والمشاهد الجنسية بصورة علنية وجبرية، ومن هنا يظهر الأثر المدمر لما يُروج.

لذلك نوصي – ونشدد في ذلك – المتحكمين في المواقع الإلكترونية أو المعلنين، بضرورة الاهتمام بالحصول على موافقة الأشخاص على عرض مثل هذه الأمور قبل عرضها عليهم أو إظهارها لهم؛ وذلك احترامًا لقواعد الشفافية والموضوعية الإلكترونية، ومن أجل محاولة الوصول إلى فضاء إلكتروني مطمئن وثقة إلكترونية آمنة بقدر المستطاع. ويلزم الحصول على موافقة الأشخاص بصورة صريحة وواضحة ولا يكفي في هذا الشأن الموافقة الضمنية.

ثالثًا: الطابع الجماعي للرسائل الإلكترونية غير المرغوب فيها (الطابع العشوائي لها):

يلزم في الإيجاب الإلكتروني الصحيح، أن يكون موجهًا إلى شخص معين أو أشخاص معينون، أي أنه إرادة معلنة للتعاقد مع الشخص الموجه إليه الإيجاب، بحيث إذا صادفه قبول الطرف الآخر، انعقد العقد ولو كان موجهًا إلى الجمهور بشرط أن يكونوا محددين بصفتهم كالمستهلكين أو أرباب مهنة معينة [1].

وعلى خلاف القول المتقدم، نجد أن الرسائل الإلكترونية غير المرغوب فيها، توجه إلى عدد كبير من الأشخاص أو المستهلكين دون تحديد ويتم إرسال هذه الرسائل إلى عناوين بريدهم

[1] – د/ أحمد عبد التواب محمد بهجت، إبرام العقد الإلكتروني، دراسة مقارنة بين القانون المصري والفرنسي، دار النهضة العربية، سنة 2009، ص 139.

الإلكتروني [1]، وهذا ما يُظهر الطابع العشوائي لهذه الرسائل.

ويتعاظم هذا الطابع العشوائي بصورة واضحة وكبيرة، من خلال استخدام برامج مُعدة بصورة خاصة للإرسال العشوائي المتكرر للرسائل الإلكترونية غير المرغوب فيها بشكل آلي، مما يؤدي إلى اكتظاظ البريد الإلكتروني بالعديد من الرسائل غير المرغوبة فيها وتضخيم عمل هذا البريد وفقد القدرة على التحكم فيه سواء بفتحه أو إغلاقه أو ربما إلغاء حساب البريد الإلكتروني في حالة ما إذا كانت هذه الرسائل تتضمن ملفات ذات حجم كبير لا يقدر البريد الإلكتروني على استيعابها؛ الأمر الذي يكون سببًا في وجود خسائر اقتصادية ضخمة لا سيما بالنسبة للشركات والمؤسسات التي تعمل في مجال التجارة الإلكترونية والتي تنتظر يوميًا العديد من الرسائل الإلكترونية من أجل إبرام الصفقات التجارية [2].

رابعًا: عدم مرغوبية الرسائل الإلكترونية العشوائية [3]:

إن عدم مرغوبية الرسائل الإلكترونية العشوائية، إنما يرجع إلى أنها تُرسل إلى الأشخاص بدون موافقتهم ورغمًا عنهم، وذلك كما سبق الذكر. وهذا الأمر هو ما عبر عنه التوجيه الأوربي الصادر في 12 يوليو سنة 2002 والمتعلق بالتعامل في البيانات الشخصية وحرمة الحياة الخاصة، حينما وصف هذه الرسائل بصفة عدم القبول أو عدم الرغبة في تلقي هذه الرسائل [4].

---

[1] - Schryen ، Guido , op . cit , p 8.

[2] – د/ خالد ممدوح إبراهيم، مرجع سابق، ص 158.

[3] - Schryen ، Guido , op. cit , p. 8.

[4] – د/ شريف محمد غنام، مرجع سابق، ص 91.

وترجع عدم مرغوبية الرسائل الإلكترونية العشوائية إلى العديد من العوامل التي تجعل الأشخاص ينفرون ويستائون منها. وهذه العوامل إما أن تكون عوامل تقنية، أو عوامل قانونية، أو عوامل تتعلق بالثقة الإلكترونية:

1- العوامل التقنية: وتتمثل في العديد من الأمور ذات الطابع التقني الفني أو التكنولوجي والتي تكون وثيقة الصلة باستخدام البريد الإلكتروني كوسيلة تواصل فعالة ومثمرة وأكثر أمانًا عن غيرها. ومن هذه العوامل – على سبيل المثال – نجد أن الرسائل الإلكترونية غير المرغوب فيها تحمل مستخدم البريد الإلكتروني مصاريف إضافية تثقل وتضخم البريد وتطيل ساعات الاتصال بشبكة الإنترنت بدون أي فائدة. كما أنه يترتب عليها اختناق الشبكة بسبب إطالة مدد الاتصال عند استلام الرسائل، وهو ما يترتب عليه وجود مصروفات إضافية على مورد المنافذ والذي يقوم بدوره بتحميلها للعميل. وكذلك تؤدي إلى إعاقة عمل البريد الإلكتروني، وذلك بسبب كبر حجم هذه الرسائل وصغر مساحة البريد الإلكتروني، مما يترتب عليه صعوبة استدعاء البريد وعدم إمكانية فتحه أو غلقه وربما يُلغى الحساب بصورة نهائية [1].

2- العوامل القانونية: وتستمد هذه العوامل من مقتضيات النظام العام والآداب العامة، والتي تقتضي أن يكون ما يتم عرضه على مواقع التواصل أو المواقع الإلكترونية متوافقًا مع هذا النظام وتلك الآداب. وتعتبر العديد من الرسائل الإلكترونية غير المرغوب فيها – بالإضافة إلى عدم قانونية إرسالها من الأساس – ذات محتوى جنسي يتعارض مع هذه المقتضيات أو محتوى عنيف يحث على الكراهية والتفرقة العنصرية بين طبقات وفئات المجتمع المختلفه، مما يؤثر

[1] – د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 84، 85.

بالسلب على تماسكه وقوة بنيانه ووحدته.

وقد يتذرع البعض بصعوبة مراعاة القيد المتقدم؛ على أساس أن شبكة الإنترنت هي شبكة عالمية وتتخطى الحدود الجغرافية للدولة الواحدة وجعلت العالم منفتحًا على بعضه وكأنه عائلة واحدة، إلا أننا مع تسليمنا بهذا الأمر لكونه أمر وواقع موجود بصورة فعلية، يمكن مراعاة هذا القيد عن طريق وضع ضوابط قانونية يلتزم بها المعلنين عند عرضهم للسلع والخدمات و حتى عند إرسال المشروعة قانونًا للعملاء تراعي مقتضيات النظام العام والآداب العامة والتي تختلف من بلد لآخر.

3- العوامل المتعلقة بالثقة الإلكترونية: وتعد هذه العوامل من أبرز وأهم العوامل التي تجعل الرسائل محل الحديث غير مرغوبة لدى من تُرسل إليهم؛ لكونها تفقدهم الثقة الإلكترونية فيما تعرضهم عليهم هذه الرسائل؛ لكونها تعرض – في الكثير من الحالات – سلع وخدمات بطرق احتيالية بحيث لا تكون مطابقة للحقيقة، بحيث تخلق جوًا من عدم الثقة بين المتعاملين وبين المعلنين والمتحكمين في المواقع الإلكترونية. وهذا الأمر يترتب عليه فقدان المستهلك للثقة في كل عمليات التسوق الإلكتروني ، مما يعوق نمو وتطور التجارة الإلكترونية على وجه العموم وما يصاحب ذلك من التأثير السلبي على الاقتصاد الرقمي للدولة [1].

خامسًا: الرسائل الإلكترونية غير المرغوب فيها ذات أهداف متعددة:

يعتبر الهدف الأكثر شيوعًا وانتشارًا وراء إرسال الرسائل الإلكترونية غير المرغوب فيها، هو

[1] – د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 85، 86.

أنها تُرسل تحقيقًا لأهداف تجارية [1]؛ وذلك عن طريق الترويج للسلع والخدمات بالعديد من الوسائل التقنية سواء كانت وسائل مشروعة من الناحية القانونية أو كانت غير ذلك، سواء تم ذلك عن طريق مواقع التواصل المختلفة أو المواقع الإلكترونية المتاحة على شبكة الإنترنت والتي يزورها الملايين من الأشخاص يوميًا، أو عن طريق إرسال الرسائل الإلكترونية غير المرغوب فيها.

وفي هذا الشأن، يعتبر إرسال الرسائل الإلكترونية غير المرغوب فيها خيارًا مهمًا وجيدًا لتحقيق المكاسب التجارية؛ وذلك لسهولة إرسالها في وقت سريع جدًا مما يعكس سرعة انتشارها وتكلفة إرسالها بسيطة بالمقارنة مع غيرها من الوسائل الأخرى [2].

وما يؤيد هذا الأمر، أن رسائل البريد الإلكتروني العشوائي لها أثر اقتصادي كبير لا يُستهان بما يجعلها محفزة لمن يرسلونها؛ حيث اعترف ما يقرب من 11% من مستخدمي الإنترنت – في بعض الفترات – بشراء منتجات بعد تلقي رسائل دعائية غير مرغوب فيها، وذلك بناءً على دراسة أجرتها الشركة البريطانية (SDPHOS 16) [3].

---

[1] - Schryen ، Guido , op. cit , p. 8.

[2] – أنظر في ذلك الموقع التالي:

- https://www.cisco.com/c/en/us/products/security/email-security/what-is-spam.html#~how-spam-works (12-4-2021)

– وأنظر كذلك الموقع التالي:

- https://www.techopedia.com/definition/1716/spam (12-4-2021)

[3] - John Leyden , "30 years of spam and we ain’t finished yet " , the

وما يؤيد هذا الأمر أيضًا، هو أن نسب الرسائل الإلكترونية غير المرغوب فيها ذات الطابع التجاري، هي الأكثر بالمقارنة مع غيرها من الرسائل الأخرى. فالرسائل المرتبطة بالإعلانات تمثل حوالي 36٪ من جميع رسائل البريد العشوائي، يليها الرسائل ذات الصلة بالبالغين بنسبة بلغت ما يقرب من 31.7٪ من إجمالي الرسائل غير المرغوب فيها، ثم الرسائل المتعلقة بالمسائل المالية بنسبة بلغت حوالي 26.5٪ [1].

ولعل ما يزيد من هذا الأثر الاقتصادي الذي يترتب على إرسال الرسائل الإلكترونية غير المرغوب فيها، هو أنها تُرسل بصورة متكررة [2]، بما يعني أنها تتضمن طابع الإلحاح في عرض السلع والخدمات على الأشخاص مرارًا وتكرارًا بما يؤدي إلى قناعة الكثيرين منهم بها حتى ولو كانت لا تتوافق مع ميولهم ورغباتهم قبل إرسالها؛ لا سيما وأنها تُرسل من شخص أو جهة مجهولة الهوية [3].

ولا يعد هذا الأمر مستغربًا؛ حيث إنه في التعاقد الإلكتروني المشروع من الأساس يغلب عليه الطابع التجاري والاستهلاكي. وذلك لأنه عقد يُبرم عبر شبكة الإنترنت الافتراضية وهو يرد في الغالب على النشاطات الاقتصادية الخاصة بتداول السلع والخدمات بين تاجر صاحب مشروع

Register , 1er mai 2008.

[1] – أنظر في ذلك الموقع التالي:

- https://www.spamlaws.com/spam-stats.html#google_vignette (12-4-2021)

[2] - Schryen ، Guido , op. cit , p. 8.

[3] - Cour européenne des droits de l'homme , 2e section , 13 novembre 2007, n° 31358/03.

تجاري أو صناعي وبين تاجر آخر، أو بين التاجر السابق وبين مستهلك. لذلك يُطلق على العقود الإلكترونية، تعبير التجارة الإلكترونية؛ لأنها عقود تبرم في أغلب الحالات في النشاط التجاري [1].

وعلى الرغم من أن الرسائل الإلكترونية غير المرغوب فيها ذات طابع تجاري، إلا أن لها أهداف أخرى متعددة: كأن تكون رسائل ذات طبيعة سياسية أو دينية. ومن ذلك الرسائل التي تروج لأفكار طائفية، وكذلك الرسائل الجنسية والإباحية – كما سبق الذكر – [2].

سادسًا: انتماء الرسائل الإلكترونية غير المرغوب فيها إلى طائفة البرمجيات الخبيثة [3]:

البرمجيات الخبيثة هي عبارة عن برامج خاصة يكون الغرض منهاهو تعطيل النظام وتخريب العمليات الخاصة به، بالإضافة إلى تخريب البيانات والمعلومات المتواجدة على جهاز الحاسب أو الهاتف أو الشبكة. ويمكن لتلك البرامج أن تقوم بعمليات حذف وتشفير بحيث لا يمكن للمستخدم الوصول إلى بياناته وملفاته دون دفع مال أو قد لا يتمكَّن من الحصول عليها على الإطلاق [4].

وتتمثل خطورة البرمجيات الخبيثة في كونها، واحدة من أنواع البرامج الصغيرة المتعددة التي أصبحت واسعة الانتشار والعدوى. وهي تعتبر بطريقة مجازية أحد أقارب الفيروسات المباشرة،

---

[1] – د/ أحمد عبد التواب بهجت، مرجع سابق، ص 42.

[2] – د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 82.

[3] – أنظر في ذلك: دليل الأمن السيبراني للبلدان النامية، صادر عن الاتحاد الدولي للاتصالات، سنة 2007، ص 37 وما بعدها.

[4] – أنظر في ذلك الرابط التالي:

- https://e3arabi.com (15-4-2021)

وتقوم بعمل العديد من الأشياء السيئة على جهاز الكمبيوتر الخاص بك مثل مراقبة البريد الإلكتروني الخاص بك أو تكليف البريد الإلكتروني الخاص بك بإرسال الرسائل غير المرغوب فيها نيابة عن الأشخاص الآخرين [1]

وبعد التعرض لبيان المقصود بالرسائل الإلكترونية غير المرغوب فيها، وبيان كيفية إرسالها، وإيضاح خصائصها، **فإننا يمكننا تعريف هذه الرسائل – من وجهة نظرنا الشخصية** – بأنها مراسلات جماعية يقوم بإرسالها شخص أو جهة مجهولة الهوية بصورة متكررة وبدون موافقة الشخص المرسل إليه هذه الرسائل، وذلك لتحقيق أهداف متعددة يكون الغرض الغالب من إرسالها ذو طابع تجاري يهدف للترويج للسلع والخدمات وأحيانًا يكون الغرض منها غير تجاري كتحقيق أهداف سياسية أو نشر أفكار دينية أو الترويج لأي أمر آخر يقصده المرسل.

[1] – أنظر الرابط السابق.

الفصل الأول

الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها

إن مسألة التعرض للحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، تفرض نفسها وبقوة من منطلق أن الكثير من الأشخاص يستخدمون خدمة البريد الإلكتروني على الإنترنت ويواجهون يوميًا حالات من الرسائل غير المرغوب فيها، ويتساءل هؤلاء الأشخاص عمَّن هو المرسل وكيف حصل على عناوين بريدهم الإلكتروني [1]. ومن هنا تثور مسألة حمايتهم من هذه الرسائل.

وسأتعرض لهذه الحماية من خلال بيان كيفية الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها (مبحث أول)، ثم بيان صور تحقق هذه الحماية (مبحث ثان)، وأخيرًا بيان موقف المشرع المصري من هذه الحماية (مبحث ثالث). وذلك على النحو التالي:

المبحث الأول

كيفية الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها

إن أبرز ما يمكن التركيز عليه بشأن الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، هو تطلب موافقة الأشخاص الذين تُرسل إليهم هذه الرسائل على إرسالها لهم.

---

[1] - Schryen ، Guido , op . cit , p 1.

فقد سبق وأن سردنا الخصائص التي تتميز بها الرسائل الإلكترونية غير المرغوب فيها، وذكرنا أنها رسائل تتسم بعدم المرغوبية لدى الأشخاص الذين تُرسل إليهم؛ وذلك لأنها تُرسل بدون أن يوافقوا عليها. وبمفهوم المخالفة فإن صفة عدم المرغوبية أو صفة الإزعاج التي تتميز بها هذه الرسائل تنتفي عنها وتكون مشروعة من الناحية القانونية إذا كان المرسل إليه قد وافق على إرسال هذه الرسائل إليه.

والسؤال الذي يُثار هنا: هل موافقة الأشخاص على أن تُرسل إليهم الرسائل الإلكترونية غير المرغوب فيها، تكون حسبما تقضي به القواعد العامة في القانون المدني أم أنها تتميز بخصوصية مختلفة عن ذلك؟

غني عن البيان أن التعبير عن الإرادة أما أن يكون تعبيرًا صريحًا وإما أن يكون تعبيرًا ضمنيًا[1]. فالتعبير الصريح قد يكون باللفظ أو بالكتابة أو بالإشارة والموقف الذي لا تدع ظروف الحال شكًا في دلالته على المقصود [2]. فاللفظ يُقصد به كل ما يتلفظ به الشخص ويدل معناه لغًة

---

[1] – د/ عبد الرزاق السنهوري، الوجيز في النظرية العامة للالتزام، (المصادر – الإثبات – الآثار – الأوصاف – الانتقال – الانقضاء)، تنقيح المستشار/ أحمد مدحت المراغي، منشأة المعارف، سنة 2004، ص 49 وما بعدها؛ د/ أحمد شوقي محمد عبد الرحمن، البحوث القانونية في مصادر الالتزام الإرادية وغير الإرادية، دراسة فقهية وقضائية، منشأة المعارف، سنة 2002، ص 29.

[2] – د/ سمير عبد السيد تناغو، مصادر الالتزام، العقد – الإرادة المنفردة – العمل غير المشروع – الإثراء بلا سبب – القانون، مصدران جديدان للالتزام (الحكم – القرار الإداري)، بدون ناشر،

أو عرفًا أو بحسب ظروف الحال على إرادة الشخص، سواء تلفظ به بنفسه أو عن طريق رسول كلفه بذلك. أما الكتابة فتشمل أي عبارات مكتوبة يدل معناها لغَة أو عرفًا أو بحسب ظروف الحال على إرادة من صدرت منه هذه الكتابة، سواء تمت بخط اليد أو كانت مطبوعة، يستوي في ذلك أن تكون موقعة أم لا [1].

والإشارة، هي كل ما يومئ به الشخص تعبيرًا عن موقف معين يجري العرف على إعطائه معني خاصًا ومحددًا، كتحريك الرأس عموديًا دلالة على القبول، أو تحريكها أفقيًا دلالة على الرفض، وقد تكون هذه الإشارة هي لغة البُكم الذين لا يستطيعون التحدث [2]. وأخيرًا الموقف الذي لا تدع ظروف الحال شكًا في دلالته على حقيقة المقصود، ومثاله عرض التاجر بضاعته على الجمهور مع بيان أسعارها، وكذلك الشأن وقوف سيارات الأجرة ذات الأسعار المحددة في الأماكن المخصصة لركوب الركاب [3].

سنة 1999 – 2000، ص 33؛ د/سهير سيد احمد منتصر، د/حمدي عبد الرحمن، الوسيط في النظرية العامة للالتزامات، الكتاب الأول، العقد والإرادة المنفردة، بدون ناشر، سنة 2010، ص 137.

[1]– د/جلال على العدوي، أصول الالتزامات، مصادر الالتزام، منشأة دار المعارف، سنة 1997، ص 90.

[2]– د/سهير سيد أحمد منتصر؛ د/حمدي عبد الرحمن، الوسيط في النظرية العامة للالتزامات، مرجع سابق، ص138.

[3]– د/رمضان أبو السعود، مصادر الالتزام، دار الجامعة الجديدة، الطبعة الثالثة، سنة 2003،

أما التعبير الضمني [1] فيُقصد به، ذلك الذي يتم بوسيلة لم توضع من الأساس للكشف عن الإرادة بطريقة صريحة، أي أنها لا تدل في ذاتها على حقيقة المعني المقصود، ولكن يمكن استخلاص ذلك المعني من خلال ظروف الحال التي لا تسمح إلا بتفسيرها على هذا المعني [2]. ومثاله بقاء المستأجر في العين المؤجرة بعد انتهاء مدة الايجار، مما يُعد ذلك تعبيرًا ضمنيًا عن رغبته في تجديد العقد.

وهنا هل يلزم توافر الموافقة الصريحة للقول بقانونية إرسال الرسائل الإلكترونية غير المرغوب فيها أم أنه يجوز بالموافقة الضمنية بالإضافة إلى الموافقة الصريحة؟

الواضح من نصوص التشريعات سواء الأوربية أو الوطنية، أنها تطلبت الموافقة الصريحة على إرسال الرسائل الإلكترونية غير المرغوب فيها. فعلى سبيل المثال، نجد أن التوجيه الأوربي الصادر في 12 يوليو سنة 2002 والمتعلق بالتعامل في البيانات الشخصية وحرمة الحياة الخاصة، قد نص في المادة (1/13) منه على أنه:" يُمتنع إرسال رسائل البريد العشوائي غير المرغوب فيها عن طريق الفاكس أو البريد الإلكتروني أو أي وسيلة إلكترونية مثل رسائل (sms) ورسائل (mms)، ما لم تكن هناك موافقة صريحة مسبقة ممن تُرسل إليهم هذه الرسائل).

ص 41.

[1]– وفي ذلك تنص المادة (2/90) من القانون المدني المصري على أنه :" ويجوز أن يكون التعبير عن الإرادة ضمنيًا، إذا لم ينص القانون أو يتفق الطرفان على أن يكون صريحًا ".

[2]– د/محسن عبد الحميد إبراهيم البيه، النظرية العامة للالتزامات، مصادر الالتزام، الجزء الأول 0المصادر الإرادية)، مكتبة الجلاء الجديدة، المنصورة، بدون سنة نشر، ص 70.

وكذلك أيضًا ما نص عليه المشرع الفرنسي؛ وذلك حينما نقل المبدأ الوارد في النص السابق والذي أرساه ونص عليه التوجيه الأوربي المذكور آنفًا، وذلك في القانون رقم 21 يوليو 2004 الخاص بالثقة في الاقتصاد الرقمي. ثم أصبح هذا النص واردًا في المادة (L.34-5) من قانون الاتصالات البريدية والإلكترونية، والتي نصت على أنه:" "يُحظر التنقيب المباشر عن طريق جهاز اتصال آلي أو جهاز فاكس أو بريد إلكتروني عن طريق أي شكل من أشكال الإرسال أو بيانات الاتصال بشخص طبيعي بدون موافقته قبل أن تُرسل إليه هذه الرسائل " [1].

وفي ذات الإطار أيضًا، نجد أن المشرع الأمريكي قد تعرض لضابط ضرورة موافقة الشخص على أن تُرسل له رسائل إلكترونية غير مرغوب فيها، وذلك في القانون الصادر في 16 ديسمبر لعام 2003 والمتعلق بمحاربة البريد التجاري الإعلاني غير المرغوب فيه [1] [2]. وهذا القانون أجاز

---

[1] - Le principe introduit par la directive européenne a été transposé en France par la loi du 21 juin 2004 pour la confiance dans l'économie numérique et figure désormais à l'article L.34-5 du code des postes et des communications électroniques, repris à l'article L.121-20-5 du code de la consommation :

« Est interdite la prospection directe au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen.. »

[2] – ويُعرف هذا القانون باسم CAN-SPAM) Act, P.L. 108-187، والذي دخل حيز التنفيذ

للمعلن إرسال الإعلانات التجارية من خلال عنوان البريد الإلكتروني للشخص بشرط ألا يعرب المستهلك بصورة صريحة عن رغبته في عدم تلقي هذه الإعلانات [2].

بتاريخ 1 يناير 2004.

[1] - The Senate originally passed S. 877 on October 22, 2003, by a vote of 97-0. As passed at that time, the bill combined elements from several of the Senate bills. The House passed (392-5) an amended version of S. 877 on November 21, 2003, melding provisions from the Senate-passed bill and several House bills. The Senate concurred in the House amendment, with an amendment, on November 25, through unanimous consent. The Senate amendment included several revisions, requiring the House to vote again on the bill. The House agreed with the Senate amendment by unanimous consent on December 8, 2003.

[2] - "Spam": An Overview of Issues Concerning Commercial Electronic Mail , June 18, 2003 – May 14, 2008 , Report Type: CRS Report , Source: EveryCRSReport.com, University of North Texas Libraries Government Documents Department .

– متاح على الموقع التالي:

- https://www.everycrsreport.com/reports/RL31953.html#fn14 (14-4-2021).

المبحث الثاني

صور تحقق الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها

ومن مجمل ما جاء بالتشريعات سالفة الذكر فيما يتعلق بموافقة الأشخاص على أن تُرسل لهم رسائل إلكترونية غير مرغوب فيها، نجد أن الأمر يتمثل صورتين: تُعرف الصورة الأولى بمُكنة الموافقة المسبقة (مطلب أول)، وتُعرف الصورة الثانية بمُكنة إلغاء الاشتراك أو قائمة الرفض أو الاعتراض (مطلب ثان). وذلك على النحو التالي:

المطلب الأول

الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها من خلال اشتراط الموافقة المسبقة (مبدأ التقيد)

وتتمثل الحماية القانونية للأشخاص في هذه الحالة، في ضرورة تقيد المرسل حال إرساله رسائل إلكترونية غير مرغوب فيها، بضرورة حصوله على موافقة مسبقة قبل أن يقوم بالإرسال إلى المرسل إليه، أو كانت هناك علاقة سابقة بين المرسل والمرسل إليه تجعل رضاء هذا الأخير أمرًا

متصورًا [1].

وفي هذا الصدد، يثور تساؤلان على قدر من الأهمية هما:

1- التساؤل الأول: ويتعلق ببيان الكيفية أو الطرق التي يمكن من خلالها الحصول على الموافقة المسبقة للشخص قبل إرسال الرسائل الإلكترونية غير المرغوب فيها إليه؟ وكذلك بيان أي طريقة من هذه الطرق هي أجدى من غيرها؟

بالنسبة للإجابة عن الشق الأول من التساؤل المذكور، **فيمكن القول أن الكيفية التي يمكن من خلالها الحصول على الموافقة المذكورة لها طرق متعددة وهي:** الموافقة المسبقة عن طريق إرسال رسالة إلكترونية، والموافقة المسبقة عن طريق تخصيص قائمة على صفحة موقع المعلن الإلكتروني، والموافقة المسبقة عن طريق إعمال الموافقة المسبقة المكررة أو المزدوجة [2]:

أ- الموافقة المسبقة عن طريق إرسال رسالة إلكترونية: وفي هذه الطريقة يتقيد المعلن أو المرسل قبل إرسال أي رسالة إلكترونية غير مرغوب فيها إلى أي شخص، بضرورة إرسال رسالة إلكترونية إلى الشخص أو المستهلك، طالبًا فيها – أي المعلن – الحصول على الموافقة المسبقة للمرسل إليه على تلقي العروض والإعلانات التجارية من هذا المعلن، وذلك عبر البريد الإلكتروني

---

[1] – د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 86، 87؛ وكذلك :

- Monique LUBY , Publicité commerciale Eur. – Réglementations generals, Janvier 2005 (actualisation : Juillet 2018).

– متاح على الموقع التالي:

- https://www.dalloz.fr/documentation/Document (27-3-2021).

[2] – أنظر في ذلك تفصيلًا: د/ شريف محمد غنام، مرجع سابق، ص 108، 109.

للشخص. وبعد إرسال هذه الرسالة ينتظر المرسل موقف المرسل إليه والذي إما أن يقبل أو يرفض. وفي حالة إهماله – أي المرسل إليه – الرد على رسالة المعلن أو المرسل، كان ذلك بمثابة رفض ضمني لها.

ب- الموافقة المسبقة عن طريق تخصيص قائمة على صفحة موقع المعلن الإلكتروني:

وفي هذه الطريقة يلتزم المعلن أو المرسل قبل أن يرسل أي رسالة، بضرورة تخصيص قائمة على صفحة الموقع الإلكتروني الخاص به، يعرض من خلالها على من يزورون هذه الصفحة ويرغبون تلقي الإعلانات التجارية، بإدراج عناوينس بريدهم الإلكتروني في هذه القائمة. مع ملاحظة أن هذه الموافقة تكون قاصرة على المعلن الذي الزورار على تلقي الإعلانات التجارية منه دون غيره من المعلنيين الآخرين.

ج- الموافقة المسبقة عن طريق إعمال الموافقة المسبقة المكررة أو المزدوجة: وتقوم الموافقة في هذه الحالة على فكرة وجود موافقة مكررة أو مزدوجة من طرف جانب المرسل إليه أو المستهلك، وذلك عن طريق قيام المعلن بإرسال رسالة تأكيد إلى المستهلك بعد موافقته الأولى أو المبدئية على تلقي الإعلانات التجارية طالبًا منه تأكيد قبوله مرة أخرى في استقبال مثل هذه الإعلانات. فإذا رفض المستهلك حال توجيه التأكيد الثاني إليه، أُعتبر ذلك رفضًا للقبول الأول، ولا يحق بعدها للمعلن إرسال أي إعلانات. كما أن المعلن بعد هذا الرفض لا يحق له توجيه رسالة تأكيد الموافقة الأولى مرة أخرى إلا بعد مضي فترة زمنية قدرها البعض بأسبوعين على الأقل.

وبالنسبة للإجابة عن الشق الثاني من التساؤل المذكور، **والخاص بأيًا من طرق الموافقة السابقة أجدى من غيرها**، نجد أن الطريقة الأخيرة هي الأجدى وأفضل الطرق سالفة الذكر؛ وذلك لأنها تحقق مصلحة كل من المعلن أو المرسل وكذلك تحقق مصلحة المرسل إليه أو المستهلك

وكذلك تخدم هذه الطريقة مسألة الثقة الإلكترونية على وجه العموم:

أ- بالنسبة لفائدة طريقة الموافقة المزدوجة بالنسبة للمرسل أو المعلن: نجد أن أبرز فائدة تتحقق بالنسبة له، هي تجنيب الرجوع القانوني بدعوى المسؤولية عليه من قبل المرسل إليه؛ وذلك لأن إرسال الرسائل كان تم بناءً على صدور موافقة. وكان قد سبق وأن بينًا أن صفة الإزعاج أو عدم المرغوبية التي تجعل من إرسال الرسائل محل الحديث أمرًا غير قانوني؛ مرجعه أنها تُرسل بدون موافقة المرسل إليه.

ب- بالنسبة لفائدة طريقة الموافقة المزدوجة بالنسبة للمرسل إليه: نجد أن هذه الطريقة تحترم إرادة المرسل إليه بصورة واضحة وتحترم رغبته بخصوص مدى قبوله للإعلانات التجارية التي تُعرض عليه؛ حيث تمنحه فرصة ثانية لمراجعة نفسه قبل أن يقبل بصورة نهائية إرسال أي رسائل إليه. حيث يمكن أن يحدث عملًا أن تكون موافقته الأولى أو المبدئية قد صدرت عنه بدون قصد لخطأ ما في تصفح الموقع أو الدخول عليه بدون قصد، على نحو على نحو تكون محصلته في الأخير أنه إذا صدر القبول الثاني من الشخص فلا يحق له بعد ذلك أن يتذرع بأن قبوله الثاني كان خاطئًا، فإن كان من الممكن وقوع خطأ في الموافقة الأولى فإنه يصعب صدور الموافقة الثانية بالخطأ أيضًا.

ج-بالنسبة لفائدة طريقة الموافقة المزدوجة بالنسبة لمسألة الثقة الإلكترونية: تعد هذه الفائدة هي أفضل ما تولده الموافقة المزدوجة؛ وذلك لكونها تخلق قدرًا كبيرًا من الثقة بين المعلن أو المرسل والمستهلك أو المرسل إليه. وكذلك يكون فيها احترام كبير من المرسل لإرادة المرسل إليه وعدم إرسال أي رسائل له رغم معارضته أو رسائل لم يُعرض عليه مسبقًا مبدأ الموافقة عليها من عدمه من الأساس.

ولهذا الأمر أهمية بالغة على وجه خاص بالنسبة للبريد الإلكتروني التجاري الذي يكون الغرض الأساسي منه هو الإعلان التجاري أو الترويج لمنتج أو خدمة تجارية، بما في ذلك المحتوى الموجود على موقع الويب على الإنترنت والذي يتم تشغيله لأغراض تجارية [1].

وهذا الأمر الأخير له نتائج إيجابية كبيرة على الاقتصاد الرقمي؛ حيث إن عرض الإعلانات التجارية على المرسل إليه بعد موافقته، يعكس رغبة هذا الأخير وجديته في شراء السلع والخدمات محل الإعلان المعروض عليه. كما أنه يراعي الرغبات الشرائية والميول الاستهلاكية للمرسل إليه، ويضمن له عدم عرض أي إعلانات تجارية عبر عنوان بريده الإلكتروني إلا ما يتناسب مع ميوله.

كما أن هذه الطريقة تحافظ على البريد الإلكتروني ذاته من التلف، وذلك عن طريق ضمان عدم تضخم البريد برسائل إلكترونية غير مرغوب فيها تعطل عمل هذا البريد أو ربما تؤدي إلى إغلاقه في بعض الأحيان؛ وذلك لأن إجازة إرسال هذه الرسائل بدون اشتراط موافقة من المرسل إليه يؤدي إلى تكالب الشركات والمواقع الإلكترونية على إرسال العديد من الرسائل إلى أصحاب عناوين البريد الإلكتروني.

وتطبيقًا لذلك، قضت محكمة باريس التجارية بغرفتها الثامنة في حكمها الصادر في 5 مايو 2004، بإدانة شخص قام بإرسال رسائل إلكترونية غير مرغوب فيها إلى عناوين البريد الإلكتروني الخاص ببعض الأشخاص بصورة متكررة دون أن يُطلب منه ذلك من قبل الأشخاص ولم يسبق له الاتصال بهم، واعتبرت المحكمة أن ما قام به الشخص يمثل خرقًا واضحًا وغير قانوني وفيه

---

[1] – أنظر في ذلك الموقع التالي:

- https://www.everycrsreport.com (14-4-2021).

مخالفة واضحة لشروط استخدام خدمة الـ (hotmail) [1].

2- التساؤل الثاني: ويتعلق ببيان ما هي الضوابط اللازمة لقانونية الموافقة المسبقة على إرسال رسائل إلكترونية غير مرغوب فيها؟

نص المشرع الفرنسي على ضوابط قانونية الموافقة محل الحديث في المادة (5/34) من قانون الاتصالات والبريد الفرنسي. وتتمثل هذه الضوابط في ضرورة كون هذه الموافقة حرة، ومحددة، ومتبصرة[2] ، وإعلان المعلن عن شخصيته [3]. كل ذلك على التوضيح الآتي:

---

[1] - TRIBUNAL DE COMMERCE DE PARIS , C 8 éme chamber , jugement du 5 mai 2004 , n°: 200 – 30 – 94 . 500

[2] - Article L34-5:" Est interdite la prospection directe au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen…..".

[3] - Article L34-5:" Dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la

أ- يجب أن تكون الموافقة حرة: ويعني ذلك ضرورة أن تصدر الموافقة من المرسل إليه الرسائل غير المرغوب فيها عن إرادة خالية من عيوب التراضي المعروفة في القانون المدني وهي: الغلط ، التدليس، الإكراه، الغبن والاستغلال.

وترتيبًا على ذلك، إذا صدرت هذه الموافقة بناءً على وقوع المرسل إليه في غلط كأن يضغط على خانة القبول وهو لا يدري أن هذا القبول سيترتب عليه إرسال رسائل غير مرغوب فيها، أو صدرت بناءً على تدليس مارسه المرسل أو المعلن على إرادة المرسل إليه جعله يقبل هذا الأمر، أو كانت نتيجة إكراه قام به المعلن ترتب عليه صدور القبول بناءً على هذا الإكراه، ففي كل هذه الفروض لا تكون الإرادة الصادرة بالقبول حرة وتكون معيبة وغير قانونية.

ب- يجب أن تكون الموافقة محددة: ويعني هذا الأمر ضرورة أن تصدر موافقة المرسل إليه على الرسائل الإلكترونية غير المرغوب فيها مع تحديد نطاقها وإلى أي نوع من الرسائل أو الإعلانات التجارية تنصرف هذه الموافقة، وعلى المعلن أو المرسل احترام هذا التحديد. فمثًلا إذا أعلن المرسل إليه أو المستهلك عن رغبته في استقبال رسائل خاصة بالدعايا التجارية عن سلع ومنتجات معينة، وجب على المعلن الالتزام بذلك وألا يرسل له رسائل لم تكن ضمن رغبات المستهلك التحديدية والتي سبق وأن ذكرها للمعلن حين أبدى موافقته على استقبال هذه الرسائل.

ج- يجب أن تكون الموافقة متبصرة: ويعني هذا الأمر التزام المعلن بتبصير المرسل إليه أو المستهلك بمضمون موافقته الحرة والمحددة، وأنه بناءً على هذه الموافقة سترسل له العديد من الرسائل غير المرغوب فيها، وأنه لا يحق له مقاضاة المرسل أو المعلن عن ذلك بحجة أنها رسائل

---

prestation ou le service propose ".

مزعجة بالنسبة؛ وذلك لسبق صدور موافقة منه على ذلك.

د- يجب أن يُعلن المرسل عن شخصيته: وهذا الأمر يعني التزام المعلن بألا يخفي شخصيته؛ وذلك لأن الرسائل الإلكترونية غير المرغوب فيها غير المشروعة تصدر في الغالب عن جهة أو شخص مجهول الهوية [1] وهذا يعد سببًا رئيسيًا في اعتبارها مزعجة لمن تُرسل إليهم. ويلزم كذلك ضرورة أن يحدد المرسل أو المعلن عنوانًا صحيحًا له يستطيع المرسل إليه أن يوجه إليه رغبته بعدم تكرار إرسال مثل هذه الرسائل مرة أخرى، وذلك دون أن يتحمل أي مصروفات [2].

المطلب الثاني

الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها من خلال مُكنة إلغاء الاشتراك (نظام قائمة الرفض أو الاعتراض) (نظام الرفض اللاحق)

وتتمثل حماية الشخص من الرسائل الإلكترونية غير المرغوب فيها في هذه الحالة، من خلال السماح للمعلن أو المرسل بإرسال هذه الرسائل إلى المرسل إليه مع تخويل هذا الأخير الحق في رفض تلقيها إذا هو عبر عن رغبته صراحة عن عدم هذا التلقي [3]. ويقع هذا الأمر – رفض تلقي الرسائل – على عاتق المرسل إليه، وذلك بأي وسيلة يستطيع من خلالها إيصال رفضه الصريح

---

[1] - Schryen ، Guido , op. cit , p. 8.

[2] – د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 90.

[3] – د/ نبيل محمد أحمد صبيح، حماية المستهلك في التعاملات الإلكترونية، دراسة مقارنة، بحث منشور في مجلة الحقوق، العدد الثاني، السنة الثانية والثلاثون، جمادي الآخرة 1429 هـ – يونيو 2008م، ص 200.

للمعلن أو المرسل.

ويتم تفعيل الرفض اللاحق من قبل المرسل إليه إما عن طريق إدراج نص صريح بشأن حقه في الرفض وذلك عند عدم رغبته في استلام رسائل دعائية جديدة، وإما إنشاء قوائم بالمنع أو الاعتراض سواء كانت وطنية أو دولية يتم فيها قيد الشخص سواء قبل استلامه للرسائل غير المرغوب فيها أو استلامه لها الأمر الذي يترتب عليه التزام كل معلن بالاطلاع على هذه القوائم قبل أن يوجه عرضه التجاري، وذلك مع التزام المرسل بذكر عنوان بريده الإلكتروني الذي يمكن مراسلته عليه أو عنوان البريد العادي لكي يتمكن من طلب إدراج اسمه في القائمة [1].

ومن الناحية العملية نجد أن طريقة إلغاء الاشتراك هي الأكثر شيوعًا وانتشارًا؛ حيث إن المعلنين أو المتحكمين في المواقع الإلكترونية غالبًا ما يعتمدون على إرسال الرسائل الإلكترونية غير المرغوب فيها للأشخاص معتمدين على أنهم إذا لم يكن لديهم رغبة بشأنها، وجب عليهم إخطار المعلن بذلك. وإن الأمر في حقيقته يعتمد على محاولة استمالة الأشخاص وجذبهم لما تتضمنه هذه الرسائل من الترويج للسلع والخدمات المختلفة حتى وإن كانت لا تتناسب مع ميولهم ورغباتهم؛ على أمل أن يتحقق هذا التناسب من خلال تكرار إرسال هذه الرسائل للأشخاص.

والحقيقة أن سياسة الإلحاح هذه تؤتي بثمارها في الكثير من الحالات التي تُرسل فيها الرسائل غير المرغوب فيها، والدليل على ذلك الإحصائيات العالمية التي تؤكد الرواج الكبير والملحوظ لحركة الاقتصاد الرقمي من خلال العديد من العوامل والتي يعد من بينهما إرسال الرسائل الإلكترونية غير المرغوب فيها.

---

[1] – المرجع السابق، ص 87.

والجدير بالذكر أن السياسة المذكورة يتبعها الكثير من المعلنين على المواقع الإلكترونية المختلفة وصفحات التواصل المتعددة؛ وخصوصًا موقع اليوتيوب. فالكثير منًا أثناء تصفحهم للمواقع أو زيارتهم لها أو أثناء مشاهدة مقاطع الفيديو، نفاجئ بظهور الكثير من الإعلانات المختلفة منها ما يكون الشخص مجبر على مشاهدته ومنها يمكن للشخص تخطيه بعد مدة زمنية قصيرة تحمل بعض الإجبار في مشاهدتها.

ولذلك نوصي الجهات المعنية المسؤولة عن إدارة المواقع والتطبيقات الإلكترونية المختلفة، بعدم إرسال أي رسائل أو إظهار أي إعلانات للأشخاص على المواقع التي يزورنها أو الفيديوهات التي يشاهدونها إلا بعد موافقتهم على ذلك، وعدم حرمانهم من ذلك بسبب رفضهم استقبال هذه الرسائل أو مشاهدة تلك الإعلانات.

فالواقع العملي الإلكتروني الحالي المتعلق بما نتحدث عنه، أصبح يدور بين أمرين نحاول التوفيق بينهما وهما: حماية مصالح التجارة الإلكترونية وحماية إرادة المستهلك واحترام رغبته وعدم إهمالها. ومن أجل التوفيق بين الأمرين، نوصي الجهات المعنية صاحبة القرار، بأن تخبر المستهلكين أو المتصفحين مسبقًا بأن المواقع التي سيتصفحونها أو المقاطع التي سيشاهدونها تتضمن إرسال رسائل إلكترونية أو تعرض إعلانات دعائية معينة. فلا يجوز أن نترك الأمر لمحض المفاجأة والمباغتة للشخص؛ فلا يجوز أنه بمجرد أن يكون هاتفك أو جهازك الإلكتروني متصلًا بشبكة الإنترنت، تجد ظهور الإعلانات والرسائل مباشرة.

وترجع الحكمة من تطلب الموافقة – سواء الموافقة المسبقة أو اللاحقة – على إرسال أو استقبال رسائل إلكترونية غير مرغوب فيها – بالإضافة إلى احترام إرادة المرسل إليه – ، إلى الأمور الآتية:

أ- أن هذه الرسائل تُرسل عبر البريد الإلكتروني والذي هو بيانًا شخصيًا. ويعتبر تجميع عناوين البريد الإلكتروني، تجميعًا لبيانات شخصية تتعلق بأشخاص طبيعيين، وأن الحصول عليها بطريقة غير قانونية هو أمر غير جائز[1]. وهذا ما قضى به القضاء الفرنسي من حظر التجميع العشوائي لعناوين البريد الإلكتروني للأشخاص دون علمهم [2].

ب- أن إرسال الرسائل الإلكترونية غير المرغوب فيها عبر البريد الإلكتروني يمثل اعتداء على مراسلة خاصة. فالمراسلة الخاصة هي يتوافر بشأنهما عنصران: أحدهما موضوعي ويتمثل في أن تكون الرسالة ذات طابع شخصي، والآخر شخصي ويُقصد به إرادة المرسل في اختيار المرسل إليه أي نيته في أن يسمح للجمهور بالاطلاع على مضمون الرسالة أو أنه يريد أن يحمل الرسالة فقط إلى علم شخص معين أو مجموعة محددة من الأشخاص. وهذين العنصرين ينطبقا على المراسلة التي تتم عبر البريد الإلكتروني [3].

ويجب الأخذ في الاعتبار أن تجميع عناوين البريد الإلكتروني للأشخاص، يكون غير مشروعًا إذا ما انتفت موافقة الشخص المعني على ذلك بصرف النظر عن نية المرسل وسواء تحقق ضرر للمرسل إليه من ذلك أم لا.

وتطبيقًا لذلك قضت المحكمة الجزئية الأمريكية للمنطقة الغربية بولاية واشنطن في سياتل،

---

[1] - Bernard Bouloc , Collecte illicite de données nominatives , RTD com. 2006.925.

[2] - Cass. crim., 14 mars 2006, pourvoi n° 05-83.423, Bull. crim., n° 69 ; AJ pénal 2006, p. 260, obs. G. Roussel.

[3] - د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 106، 107.

بالحكم بالسجن لمدة (47) شهر على شخص يدعي (Soloway)، والمعروف باسم ملك البريد العشوائي؛ وذلك بسبب الحجم الهائل من الرسائل غير المرغوب فيها والتي قام بإرسالها في عام 2007. وعلى الرغم من مطالبة المحامية الخاصة بالسيد (Soloway) بتخفيض مدة سجنه؛ لكونه لم يلحق ضررًا بجهاز الكمبيوتر الخاص بأي شخص ولم يرسل تعليمات برمجية ضارة ولم يوجه الأشخاص إلى المواد الإباحية كما يفعل بعض مرسلي البريد الإلكتروني العشوائي [1].

المبحث الثالث

موقف المشرع المصري من مسألة الموافقة على إرسال أو استقبال رسائل إلكترونية غير مرغوب فيها

ذكرنا آنفًا أن المشرع الأوربي وكذلك المشرع الفرنسي قد أخذا بمبدأ التقيد أو الموافقة، بينما أخذ المشرع الأمريكي بالموافقة اللاحقة أو نظام إلغاء الاشتراك. **والسؤال هنا: أي أمر من هذين الأمرين انتهجه المشرع المصري؟**

لقد تعرض المشرع المصري لهذه المسألة في القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات في المادة (٢٥) [2]، والتي تنص على أنه :" يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين

---

[1] – أنظر في ذلك الموقع التالي:

- https://www.pcworld.com/article/148780/spam.html (30-3-2021).

[2] – منشور في الجريدة الرسمية – العدد ٣٢ مكرر (ج) – السنة الحادية والستون، 3 ذى الحجة سنة ١٤٣٩هـ، الموافق ١٤ أغسطس سنة ٢٠١٨م.

العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى، أو انتهك حرمة الحياة الخاصة **أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لترويج السلع أو الخدمات دون موافقته**, أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة" [1].

ومن هذا النص نجد أن المشرع المصري قد انتهج مبدأ التقيد أو الموافقة المسبقة. وعلى ذلك لا يجوز للمرسل أن يُرسل رسائل إلكترونية غير مرغوب فيها إلا بعد أن يوافق الشخص المعني على ذلك. وإذا كان المشرع المصري قد أرسى مبدأ الموافقة ذاته، إلا أنه يوجد بعض التساؤلات على النص المذكور، أهمها التساؤلين الآتيين:

1- التساؤل الأول: ويتعلق ببيان نوع الموافقة التي تطلبها المشرع المصري لقانونية إرسال الرسائل الإلكترونية غير المرغوب فيها ؟

لم يتعرض المشرع المصري لطبيعة هذه الموافقة، وهل هي موافقة صريحة أم أنها موافقة ضمنية. فالموافقة الصريحة قد سبق تعريفها. أما الموافقة الضمنية فهي التي تكون في حالة ما إذا كانت هناك علاقة عمل موجودة مسبقًا بين المرسل والمرسل إليه [2].

---

[1] – جاءت هذه المادة ضمن نصوص الفصل الثالث، الخاص بالجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع.

[2] – أنظر في ذلك الموقع التالي:

وإزاء عدم التعرض لهذه المسألة، يمكن القول بتوافر الموافقة على إرسال الرسائل الإلكترونية غير المرغوب فيها سواء تمت بصورة صريحة أو بصورة ضمنية؛ لأن ظاهر صياغة النص تفيد ذلك. وذلك على عكس المشرع الأوربي والمشرع الأمريكي اللذين اشترطا الموافقة الصريحة على إرسال هذه الرسائل.

فعلى سبيل المثال، يمكن افتراض وجود الموافقة الضمنية على استقبال الرسائل المذكورة، في الحالة التي يكون فيها المرسل إليه قد سبق وأن وافق على استقبال رسائل إلكترونية غير مرغوب فيها تروج لبيع أحذية من ماركة معينة بمواصفات محددة، فيجوز للمعلن أو المرسل إرسال رسائل إلى نفس الشخص لترويج بيع أحذية بنفس المواصفات ولكن من ماركة غير تلك التي سبق وأن قد وافق على استقبال الرسائل الخاص بها صراحة.

وعلى الرغم من ذلك، **فإنني أرى من وجهة نظري الشخصية**، أن الموافقة على استقبال رسائل إلكترونية غير مرغوب فيها لا يجوز إلا صراحة، ولا يجوز أن يقوم مقامها الموافقة الضمنية، وذلك مهما كانت العلاقة السابقة بين المرسل والمرسل إليه. حيث لا يجب تغليب مصالح التجارة الإلكترونية على مصالح المرسل إليه أو المستهلك والذي يجب أخذ إرادته الصريحة بعين الاعتبار، أو على الأقل إعمال التوازن بينهما وهو الذي لا يكون إلا مع اشتراط الموافقة الصريحة؛ لاسيما وأننا نتعامل في ظل فضاء إلكتروني عالمي يصعب التحكم فيه.

2- التساؤل الثاني: ويتعلق ببيان عدد المرات التي يكون فيها إرسال الرسائل الإلكترونية أمرًا غير مرغوب فيه أو مزعج !!!

- https://www.everycrsreport.com (14-4-2021).

الواضح من صياغة نص المادة (25) من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، والتي جاء بها عبارة " أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين"، أن الإرسال غير المرغوب فيه هو الذي يكون أكثر مرة.

وبمفهوم المخالفة لظاهر عبارة النص أنه إذا كان إرسال الرسائل لمرة واحدة فلا يعتبر إرسالًا مزعجًا. والحقيقة أن هذا الأمر يتفق مع الخصائص التي تتسم بها الرسائل الإلكترونية غير المرغوب فيها، والتي منها أنها رسائل تُرسل بصورة متكررة.

وعلى الرغم من ذلك، **فإنني أرى من وجهة نظري الشخصية**، إن إرسال الرسائل للمرسل إليه يكون غير مرغوبًا فيه حتى ولو كان لمرة واحدة. وذلك لأن المهم في هذا الشأن هو أن هذه الرسالة تكون غير مرغوب فيها ومزعجة بالنسبة للشخص، يستوي أن تُرسل لمرة واحدة أو لأكثر من مرة. فأحيانًا يكون الإرسال لمرة واحدة – أي غير مكثفًا وفقًا لنص المشرع المصري – ويكون مضمونه مخالف للنظام العام والآداب العامة، كإرسال الرسائل الجنسية والإباحية أو تلك التي تحرض على العنف أو تحس على الكراهية والعنصرية.

ولقد أحسن المشرع المصري صنعًا في صياغة النص المتقدم؛ لأنه لم يفرق بشأن عدم قانونية إرسال الرسائل الإلكترونية المزعجة بين ما إذا كان ما تتضمنه هذه الرسائل يتوافق مع ميول ورغبات المرسل إليه أو المستهلك أم لا. أي أن المعول عليه فقط – وفقًا للنص – هو مدى وجود موافقة على الإرسال من المرسل إليه أم لا. وهذا الأمر هو ما يُستفاد من عبارة النص التي جاء بها " أو أرسل بكثافة العديد من الرسائل الإلكترونية" دون الأخذ في الاعتبار ما إذا كانت مرغوب فيها لدى الشخص أم لا.

ورغم تعرض المشرع المصري لمسألة الموافقة على إرسال أو استقبال الرسائل الإلكترونية

غير المرغوب فيها؛ إلا أننا نأمل منه أن يتعرض لهذا الأمر بصورة تفصيلية وبنصوص تشريعية واضحة وصريحة؛ وذلك لانتشار ظاهرة الرسائل غير المرغوب فيها وما تمثله من مخاطر لأصحاب عناوين البريد الإلكتروني، وذلك على غرار ما قام به المشرع الأوربي والمشرع الفرنسي والمشرع الأمريكي.

الفصل الثاني

الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها

- تقسيم:

نظرًا لخطورة الرسائل الإلكترونية غير المرغوب فيها، فلا يكفي لحماية الأشخاص منها مجرد سن قوانين تشترط ضوابط تشريعية؛ بل إنها تحتاج بوضوح إلى نهج متعدد الجوانب ويستلزم تطبيق أنواع مختلفة من تدابير مكافحة هذه الرسائل بصورة متكاملة[1] . لذلك وجب وضع ضوابط تقنية أو فنية بالإضافة إلى الحماية القانونية سالفة الذكر.

وترجع عدم كفاية القوانين وحدها في مكافحة ظاهرة الرسائل الإلكترونية غير المرغوب فيها؛ لأن القانون يكون في كثير من الحالات وسيلة أقل فعالية لتنظيم الأنشطة الاقتصادية الجديدة وخصوصًا عند مواجهة مجتمع معلوماتي. ويرجع هذا الأمر للعديد من الأسباب منها: انتشار العولمة الاقتصادية في ظل اقتصار عمل القوانين على الحدود القضائية الوطنية، وكذلك تطور الإنترنت إلى وسيط مفتوح لا مركزي يقوم على التدفق الحر للمعلومات والأفكار بين المستخدمين والذي يختلف عن العالم المادي بحدوده الجغرافية وسلطاته القضائية الوطنية، وأيضًا التطور

[1] - Schryen ، Guido , op. cit , p. 4.

التكنولوجي السريع بشكل متزايد في ظل بطئ عملية صنع القرار وسن التشريعات [1]. لا سيما وأن إرسال هذه الرسائل يعد بمثابة ارتكاب جريمة إعاقة عمل نظام معالجة البيانات الآلي ويشَكل أيضًا دخول احتيالي إلى هذه النظم يقوم بها مجموعة من مجرمي الكمبيوتر [2].

ويُقصد بالحماية التقنية في هذا الشأن، مجموعة الإجراءات والتدابير ذات الطابع الفني والتكنولوجي، والتي يتم وضعها من قبل متخصصين في هذا الشأن، ويكون الغرض منها محاولة الحفاظ على البريد الإلكتروني للفرد بقدر المستطاع من الاختراقات والتهديدات التي يمكن أن تحيط بهذا البريد على وجه العموم وتجنب إرسال رسائل إلكترونية غير مرغوب فيها على وجه الخصوص.

وتتعدد الطرق التقنية والفنية لحماية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها، ومن أهمها: الحماية عن طريق خاصية تصفية الرسائل (مبحث أول)، والحماية عن طريق إنشاء مواقع إلكترونية (مبحث ثان)، وأخيرًا الحماية عن طريق إعمال خاصية التشفير (مبحث ثالث). وذلك على البيان التالي:

---

[1] - Timothy R. Fenoulhet , La co-régulation : une piste pour la régulation de la société de l'information ? , RMCUE 2001. 598.

[2] – أنظر في ذلك الموقع التالي:

- https://www.dalloz.fr/documentation/Document?id=(27- 3- 2021)

المبحث الأول

الحماية التقنية من الرسائل الإلكترونية غير المرغوب فيها عن طريق خاصية تصفية الرسائل

تتم تصفية الرسائل محل الحديث عن طريق برامج توجد على الخوادم لمنع وصول الرسائل غير المرغوب فيها إلى صندوق البريد الإلكتروني الخاص بالمرسل إليه أو المستهلك، وذلك باعتراض هذه الرسائل ومسحها [1]. وتتم عملية التصفية بطرق ووسائل معينة، وذلك على النحو التالي:

1- طرق تصفية الرسائل الإلكترونية غير المرغوب فيها: تتم تصفية هذه الرسائل بطريقتين هما، طريقة الفحص وطريقة الترخيص [2]:

أ- طريقة الفحص: ويُقصد بها فحص الرسالة الواردة إلى صاحب البريد الإلكتروني من خلال السماح بالتأكد من صحة العنوان المستخدم لإرسال الرسالة. وهذه الطريقة يترتب عليها أنه إذا كان العنوان البريدي عبارة عن (fast – money – make)؛ فسيوف يتم رفضه لأنه لا يحيل إلى خادم في أسماء النطاق.

---

[1] – د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 96.

[2] – أنظر في ذلك: المرجع السابق، ص 96.

ب- طريقة الترخيص: وفي هذه الطريقة يتم السماح لمدير الشبكة بأن يختار ما إذا كان يرغب أم لا في وصول رسائل معينة إلى المستخدمين من أشخاص معينين أو من مواقع محددة. ويترب على هذه الطريقة أن قد يرى مدير الشبكة أن من مصلحة صاحب البريد الإلكتروني رفض وصول رسائل معينة إلى المستخدم رغم أن جهة الإرسال تستخدم عنوانًا صحيحًا.

2- وسائل تصفية الرسائل الإلكترونية غير المرغوب فيها: تتم عملية التصفية بواسطة مجموعة من الوسائل التقنية المختلفة، والتي نذكر منها الوسائل الآتية [1]:

أ- التصفية باستخدام مرشحات العناوين: وهنا يتم فحص عناوين الرسائل وتحليلها لمعرفة مصدر هذه الرسائل، وكذلك الخوادم التي ساهمت في توصيل الرسائل إلى بريدك الإلكتروني؛ حيث إن معظم مرسلي هذه الرسائل التطفلية أو المزعجة يستخدمون معلومات غير حقيقية حتى لا يمكن لأي شخص الوصول إليهم. وهنا تكون وظيفة المرشحات هي الكشف عن صحة المعلومات التي يحتويها عنوان الرسالة وتحديد مدى صحتها، بحيث يتم تصفية الرسائل ذات العناوين المشبوهة.

ب- التصفية باستخدام مرشحات اللغة: وهنا يتم تحديد لغة معينة فقط للرسائل التي يرغب أو ينتوي صاحب البريد الإلكتروني استقبالها. وهنا تكون وظيفة المرشحات هي رفض الرسائل التي تُرسل للشخص بلغات أخرى غير اللغة المحددة.

ج- التصفية باستخدام مرشحات المحتوى: وهنا يتم فحص محتوى الرسالة ورفض

---

[1] - أنظر في ذلك: د/ رائد محمد عبد ربه، التسويق الإلكتروني، Al manhal، 2013، ص 228، 229.

المحتويات التي تعتبر مزعجة من وجهة نظر الفلاتر.

د- التصفية باستخدام مرشحات يحددها المستخدم (صاحب البريد الإلكتروني): وهنا يقوم مستخدم البريد الإلكتروني بتحديد هذه المرشحات؛ وذلك عن طريق قيامه بانشاء مجلدات لاستقبال الرسائل طبقًا لعناوينها أو محتوياتها ثم يقوم بحذف محتويات المجلدات غير المرغوب فيها وقراءة محتويات المجلدات التي يعتبرها غير مزعجة.

وبتقييم الوسائل السابقة، نجد أن التصفية باستخدام مرشحات العناوين، على الرغم من فعاليتها وأهميتها إلا أنه يُعاب عليها أن العناوين التي يحددها المستخدم قد لا تكون كافية لتلبية رغباته وتحقيق مراده من عدم وصول الرسائل غير المرغوب فيها إليه؛ وذلك بسبب ما قد يحدث في بعض الأحيان من كون عنوان الرسالة مرغوب فيه بينما يكون مضمونها غير مرغوب فيه.

أما التصفية باستخدام مرشحات اللغة، فهي وسيلة غير مجدية من الناحية العملية؛ وذلك لأن تعدد اللغات في التعامل بين الأشخاص من مختلف الدول أصبح أمرًا طبيعيًا وطريق يُعتمد عليه بشدة في إدارة الأشخاص لأموالهم وأعمالهم وتصرفاتهم القانونية وغيرها، وهو ما يتعارض معه تحديد لغة واحدة كمرشح لاستقبال رسائل البريد الإلكتروني.

وإن كان يمكن التخفيف من حدة هذا الانتقاد، عن طريق قيام صاحب البريد الإلكتروني بتحديد أكثر من لغة أو اختيار اللغات التي يتعامل بها هذا الشخص مع غيره في مراسلاته ومخاطباته، أو اختياره للغات الرسمية المعترف بها دوليًا وذات الانتشار الكبير في التعامل بين أفراد المجتمع الدولي واستثناء اللغات ذات الاستخدام أو الانتشار القليل ما لم يشملها تحديد المستخدم.

وبالنسبة للتصفية باستخدام مرشحات المحتوى، فنرى أنها أكثر فعالية من الناحية العملية من

الوسيلتين السابقتين؛ وذلك لأنها تخول صاحب البريد الإلكتروني الحق في تحديد المضمون أو المحتوى الذي يرغب في تلقي رسائل إلكترونية عنه، وذلك على حسب ميوله ورغباته. فبواسطة هذه الطريقة مثلًا، يستطيع المستخدم السماح باستقبال رسائل ذات طبيعة سياسية أو دينية أو ثقافية أو رياضية. وبواسطتها أيضًا، يستطيع منع وصول رسائل ذات محتوى معين من الوصول إليه إذا كان لا يرغب فيها، كالرسائل الإباحية أو تلك التي تحس على الضغينة والكراهية والتفرقة العنصرية بين الأشخاص.

وعلى الرغم من ذلك، إلا أنه يُعاب عليها أن بعض المحتويات مثل النشرات الدورية التي ترسلها بعض المواقع بناءً على رغبة صاحب البريد الإلكتروني، ستصنف على أنها مزعجة أو غير مرغوب فيها، ولذلك يجب عليه سرد المواقع التي يرغب في استقبال رسائلها بطريقة واضحة [1].

وبخصوص التصفية باستخدام مرشحات يتولى تحديدها صاحب البريد الإلكتروني، فنرى أنها أفضل وسيلة من وسائل تصفية رسائل البريد الإلكتروني؛ لأنها تتماشي مع المبدأ القاضي بضرورة موافقة صاحب البريد على ما يُرسل إليه من رسائل وتحترم إرادته. فبواسطتها يستطيع تحديد المحتوى الذي يريد استقبال رسائل عنه كيفما يشاء وبالطريقة التي يرغب فيها. ويستطيع عن طريقها أيضًا الاشتراط على المواقع التي يرغب في استقبال رسائل منها بعد إرسال نشرات دورية لا يرغب المستخدم في استقبالها.

وهناك بعض المواقع الكبيرة والمشهورة، تحافظ على سرية وأمان عناوين البريد الإلكترونية

---

[1] – المرجع السابق.

الخاصة بالأشخاص، على أساس تحديد الخصاص الشائعة للبريد الإلكتروني العشوائي، ومن ذلك (Microsoft Outlook)[1]. وتعتمد هذه الطريقة على أساس فرز وتحديد عناوين البريد التي غالبًا أو دائمًا ما تقوم بإرسال رسائل دعائية غير مرغوب فيها في مجال أو مجالات معينة، والقيام بحظرها من قبل المسؤولين بسبب سوء سمعتها الإلكترونية واشتهارها بإرسال رسائل غير مرغوب فيها.

وتطبيقًا لذلك، فإن خاصية التصفية قد تمكنت من التصدي بالفعل للعديد من الرسائل الإعلانية المزعجة أو غير المرغوب فيها؛ وذلك إما بحذف هذه الرسائل أو بنقلها إلى مجلد البريد الإلكتروني غير المرغوب فيه. ويستطيع صاحب البريد الإلكتروني التحقق من ذلك عن طريق معاينة هذا المجلد من وقت لآخر من أجل التأكد من عدم وجود رسائل مهمة تم تصفيتها بطريق الخطأ. وإذا حدث وأن تمت عملية تصفية لرسائل مهمة لدى المستخدم أو كانت مرغوب فيها بالنسبة له، فيمكن له أن يسحبها إلى علبة البريد الوارد [2].

---

[1] – أنظر في ذلك الموقع التالي:

- https://support.microsoft.com/ar-sa/topic/ (17-4-2021)

[2] – د/ بسام فنوش الجنيد، المسؤولية المدنية عن الإعلانات التجارية عبر الإنترنت، رسالة دكتوراة بكلية الحقوق جامعة عين شمس، سنة 1437 هـ – 2016 م، ص 261.

المبحث الثاني

الحماية التقنية من الرسائل الإلكترونية غير المرغوب فيها عن طريق إنشاء مواقع إلكترونية لمحاربتها

وتتمثل الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها هنا من خلال إيجاد وإنشاء البرامج والمواقع الإلكترونية التي تمثل وسيلة دفاع فعالة لعناوين البريد الإلكتروني الخاصة بالأشخاص ومنع وقوع أي اعتداءات أو اختراقات بقدر المستطاع، ومن ذلك ما يلي:

1- قيام المواقع الإلكترونية بإنشاء ما يُعرف بالقوائم السوداء: وفي هذه القوائم يتم تسجيل أسماء الأشخاص والشركات التي تمارس إرسال الرسائل غير المرغوب فيها. وتظهر أهمية هذه القوائم في أنه عند مرور البريد الإلكتروني لهذه الشركات يتم حجزه وتعطيله مدة معينة. والبعض الآخر يقدم قوائم بعناوين غير صحيحة تظهر بطريقة آلية عند فتح الصفحة، الأمر الذي يترتب عليه أنه عند قيام شخص بمحاولة جمع عناوين إلكترونية يتم تحويله إلى هذه العناوين، وبالتالي عند قيامه بإرسال رسائل مزعجة سيكون الرد على ذلك بوجود خطأ في العنوان البريدي، مما يصعب من عمله [1].

[1] – د/ عبد الهادي فوزبي العوضي، مرجع سابق، ص 97.

ويعد من أشهر هذه المواقع الإلكترونية، موقع (spam.@cnil.fr)، الخاص باللجنة الوطنية الفرنسية للمعلومات والحريات، وذلك بشأن مكافحة الرسائل الإعلانية غير المرغوب فيها. ومن خلال هذا الموقع يتم دعوة الجمهور إلى إرسال الرسائل المزعجة أو غير المرغوب فيها إلى هذا الموقع وإملاء طلب شكوى عبر الإنترنت ضد المرسل لكي تتمكن اللجنة من دراسة الظاهرة واتخاذ الإجراءات القانونية ضد الشركة أو الجهة المرسلة للبريد الإلكتروني غير المرغوب فيه [1] [2].

2- الحماية عن طريق برامج (Spam blockers):هي برامج تقوم بالتصفية [3] وترشيح الموقع الذي لا يرسل رسائل مزعجة [4]. وهذه البرامج كثيرة ومتوافرة على شبكة الإنترنت، والبعض منها يكون مجاني وبعضها الآخر يكون بمقابل مادي. ويمكن لصاحب البريد الإلكتروني تحميل بعض هذه البرامج وتجربتها من أجل معرفة البرنامج الذي سيعمل بطريقة جيدة بالنسبة له. ومن أجل تسهيل مهمة اختيار أفضل هذه البرامج، يمكن للشخص قراءة تعليقات الأشخاص الذي سبق

---

[1] – د/ محمد سعد عيسى الزبون، وسائل حماية المستهلك من إعلانات البريد الإلكتروني المزعجة، بحث منشور في المجلة القانونية، ص 189.

[2] – أنظر في ذلك أيضًا: الموقع التالي:

- https://www.cnil.fr/fr/spam-phishing-arnaques-signaler-pour-agir (18-4-2021).

[3] - M.Myard , Répons ministérielle à question écrite n° 787 C J O A N Q , 16 décembre 2002 , p. 5004.

[4] – د/ محمد مصطفى الشقيري، السرية المعلوماتية، ضوابطها وأحكامها الشرعية، دار البشائر الإسلامية للطباعة والنشر والتوزيع، سنة 2008، ص 304.

لهم استعمال هذه البرامج ومقارنتها ببعضها البعض من أجل الانتهاء إلى أفضلها، ويُلاحظ على هذه البرامج الأمور الآتية [1]:

أ- تتميز هذه البرامج بقدرتها على حجب نسبة كبيرة من البريد الإلكتروني المزعج أو العشوائي وصلت إلى 90% من حجم الرسائل غير المرغوبة فيها. والحقيقة أن هذه النسبة كبيرة ومرضية للأشخاص في ظل الزخم التقني المتعلق بمكافحة هذه الظاهرة.

ب- تعد هذه البرامج أفضل من مرشحات التصفية آنفة الذكر؛ وذلك لأن هذه البرامج لا تسمح بدخول الرسائل المزعجة إلى البريد الإلكتروني الخاص بالشخص من الأساس، على عكس مرشحات التصفية والتي تعمل على نقل البريد المزعج إلى مجلد آخر يستطيع صاحب البريد حذفه – أي البريد المزعج – فيما بعد.

ج- لهذه البرامج القدرة على تسجيل الإجراءات التي يقوم بها مستخدم البريد الإلكتروني. فعلى سبيل المثال، إذا قام هذا المستخدم بحذف رسالة دون فتحها أو قراءتها ، فالبرنامج يعتبر هذه الرسالة مزعجة ويقوم بحجب جميع الرسائل القادمة إلى هذا البريد الإلكتروني من نفس العنوان في المستقبل.

د- يلزم لتحقيق أكبر قدر ممكن من الاستفادة من المزايا التي تحققها هذه البرامج، ضرورة تحديثها وتحميل الإصدارات الحديثة لها؛ وذلك لأن الرسائل الإلكترونية غير المرغوب فيها تنتمي إلى طائفة البرمجيات الخبيثة والتي تتميز بالتطور المستمر – كما ذكرنا سلفًا – ، لذلك وجب تحديث هذه البرامج لمسايرة التطور الذي يلحق بهذه البرمجيات الخبيثة.

---

[1] – د/ رائد محمد عبد ربه، مرجع سابق، ص 227.

*** موقف المشرع المصري من الحماية التقنية من الرسائل الإلكترونية غير المرغوب فيها عن طريق إنشاء مواقع إلكترونية لمحاربتها:**

لقد تعرض المشرع المصري في العديد من النصوص القانونية للمسألة محل الحديث، وذلك في اللائحة التنفيذية للقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات [1]. حيث أكد المشرع المصري على ضرورة إنشاء نظم وبرامج وتطبيقات حمائية وذلك في المواد الآتية:

1- المادة رقم (2) من اللائحة المذكورة، تنص على أنه:"يلتزم مقدمو خدمات تقنيات المعلومات باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (2،3) من الفقرة أولًا من المادة رقم (2) من القانون:"2- تنصيب واستخدام نظم وبرامج ومعدات مكافحة البرمجيات والهجمات الخبيثة والتأكد من صلاحيتها وتحديثها".

2- المادة رقم (3) من اللائحة المذكورة، تنص على أنه:" يلتزم مقدمو خدمات تقنية المعلومات والاتصالات التي تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة المخاطبين بأحكام هذا القانون، باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (2،3) من الفقرة أولًا من المادة رقم (2) من القانون:" 9- تنصيب واستخدام نظم وبرامج ومعدات المكافحة والحماية من

[1] – صدرت هذه اللائحة بقرار رئيس مجلس الوزراء بالقرار رقم 1699 لسنة 2020. منشور بالجريدة الرسمية، العدد 35 تابع (ج)، في 27 أغسطس سنة 2020.

البرمجيات والهجمات الخبيثة والكشف عنها والتأكد من صلاحيتها وتحديثها".

وبالنسبة لضرورة إجراء التحديثات التقنية للبرامج المستخدمة في الحماية، جاء نص المشرع المصري على ذلك في المواد الآتية:

1- المادة رقم (2) من اللائحة المذكورة، والتي تنص على أنه:" 9- إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري وإتمام الاختبارات اللازمة قبل إجراء التحديثات".

2- المادة رقم (3) من اللائحة المذكورة، والتي تنص على أنه:" 9- إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري. مع الأخذ في الاعتبار ضوابط التعامل مع إجراء التحديثات على أنظمة التحكم الصناعي مع عدم اتصالها المباشر بشبكة الإنترنت، وإتمام الاختبارات اللازمة قبل إجراء التحديثات".

وحرصًا من المشرع المصري على التأكيد على الأمور السابقة وضمان فاعليتها بصورة عملية، ألزم مقدمو خدمات تقنية المعلومات والاتصالات بضرورة إجراء اختبار سنوي للكشف عن الاختراقات أو المخاطر الأمنية وتثبيت أجهزة المنع والكشف عن الاختراقات [1].

ويجب الأخذ في الاعتبار أن الحماية التي نص عليها المشرع المصري في نصوص اللائحة التنفيذية سابقة الذكر، هي حماية لا تنطبق فقط على البريد الإلكتروني، بل تنطبق كذلك على جميع تقنيات المعلومات والاتصالات بجميع أشكالها وأنواعها وتطبيقاتها التقنية المختلفة، والتي يعد من أبرزها بلاشك البريد الإلكتروني.

---

[1] – المادة رقم (12/3) من اللائحة التنفيذية للقانون رقم 175 لسنة 2018 بشأن مكافحة تقنية المعلومات.

المبحث الثالث

الحماية التقنية من الرسائل الإلكترونية غير المرغوب فيها عن طريق إعمال خاصية التشفير

يعتبر التشفير كخاصية تقنية، من أهم وأبرز الوسائل الحمائية التقنية التي تُستخدم في مجال التأمين المعلوماتي لكافة البيانات والمعلومات على وجه العموم وحماية عناوين البريد الإلكتروني للأشخاص على وجه الخصوص. فهو يشَّكل جزء من منظومة دفاعية تقنية كبيرة تتعدد حلقاتها والتي يعد من بينها خاصية التشفير.

ومن منطلق أهمية خاصية التشفير من الناحية التقنية، فلقد تم التعرض لتعريفها من الناحيتين التشريعية والفقهية. فمن الناحية التشريعية، نجد أن المشرع المصري قد تعرض لتعريف التشفير وذلك في المادة (14/1) من اللائحة التنفيذية للقانون رقم 15 لسنة لسنة 2004 بشأن تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات [1]، وكذلك في المادة (1) من

[1] – المادة (14/1) من اللائحة التنفيذية للقانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة التكنولوجيا، وذلك بموجب قرار وزارة الاتصالات وتكنولوجيا المعلومات رقم 361 لسنة 2020، بتاريخ 2020/4/19، والخاص بتعديل اللائحة التنفيذية

اللائحة التنفيذية للقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، واللتا نصتا على أن:" التشفير منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة".

ومن الناحية الفقهية، فتم تعريف التشفير بأنه عبارة عن عملية تقنية يتم فيها تحويل نص واضح أو مقروء إلى نص غير مقروء واضح، أو نص معمي بطريقة تستطيع بواسطتها الأطراف المتعارف عليها فقط أن تحل التعمية وتحول النص غير الواضح أو المعمي إلى نص مقروء [1].

وتتمثل أهمية نظام التشفير في أنه بالإضافة إلى الفائدة الواضحة من حماية المعلومات الخاصة من السرقة أو الاختراق [2]، فهو يعد وسيلة لإثبات أن المعلومات أصلية وتأتي من المصدر الأصلي لها. يمكن استخدام التشفير للتحقق من أصل رسالة والتأكد أنه لم يتم تعديلها أثناء عملية

للقانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني وبإنشاء هيئة صناعة تكنولوجيا المعلومات..... منشور في الوقائع المصرية، العدد 95 (تابع)، في 23 أبريل سنة 2020.

[1] – د/نادية حجازي، الوسائط المتعددة، دار أخبار اليوم، القاهرة، سنة 2017، ص 35.

[2] – مع ملاحظة أن هذا الأمر لا يعني بأن يكون نظام التشفير في مأمن كامل من التهديدات والاختراقات الخارجية، فأحيانًا قد تحدث مثل هذه التهديدات، ومن ذلك محاولة كسر التشفير عن طريق مجموعة تقنيات تستخدم لفك تشفير الرسالة بطريقة غير شرعية، أي كسر تشفيرها عن طريق طرف غير مصرح له ذلك ولا يعرف المفاتيح اللازمة لذلك.....أنظر في ذلك: د/ محمد بن إبراهيم السويل، المدخل إلى علم التشفير، دار الخريجي، بدون سنة نشر، ص 2.

الإرسال [1].

ومنذ وقت ليس ببعيد، كان استخدام خاصية التشفير قاصرًا على بعض القطاعات دون غيرها، كقطاع الخدمات المالية وقطاع الدفاع؛ حيث كان يتم استخدام هذه الخاصية لتأمين المعلومات الأكثر حساسيةً فقط . لكن هذا الأمر تغير، حيث يلجأ إليه الأشخاص لتأمين بياناتهم ومعلوماتهم من الفقد، وخصوصًا البيانات الموجودة على الوسائط القابلة للإزالة مثل الأشرطة والأجهزة المحمولة كأجهزة الكمبيوتر المحمول [2].

وبالنسبة للطريقة التي يتم أو يُستخدم بها التشفير، فهي تختلف بحسب نوع التشفير المستخدم في تأمين وحماية عنوان البريد الإلكتروني. فالتشفير إما أن يكون تشفيرًا متماثلًا، وإما أن يكون تشفيرًا غير متماثلًا [3]:

---

[1] – أنظر في ذلك الموقع التالي:

- https://me.kaspersky.com/resource-center/definitions/encryption (19-4-2021).

[2] – أنظر في ذلك الموقع التالي:

*https://web.archive.org/web/20180325232131/http://www.computerweekly.com:80/feature/Encryption-key-management-is-vital-to-securing-enterprise-data-storage (20-4-2021).

[3] - Dr. Bill Young , Foundation of Computer Security , Lrcture 44: Symmetric vs Asymmetric Encryption , p. 1.

– متاح على الموقع التالي:

- https://web.archive.org/web (20-4-2021)

1- التشفير المتماثل: يعرف أيضًا باسم خوارزمية المفتاح السري [1]، وهو أسلوب فردي لفك ترميز الرسالة ويجب إعطاؤه للمستلم قبل فك ترميز الرسالة. والمفتاح المستخدم للترميز هو نفسه المستخدم لفك الترميز، وهو ما يجعل هذا الأسلوب الأفضل للمستخدمين الفرديين والأنظمة المغلقة. بالإضافة إلى ميزتي البساطة والسرعة اللتا يتسم بهما هذا النوع من أنواع التشفير [2].

وعلى الرغم من من مزايا التشفير المتماثل، إلا أنه يُؤخذ عليه بعض الأمور السلبية، أهمها إيجاد الوسيلة الآمنة لتبادل هذا المفتاح السري؛ لذلك فالتشفير بهذه الطريقة لا يتصور استخدامه إلا في الشبكات المغلقة بسبب المخاطر المرتبطة بعملية نقل المفتاح السري ولا يمكن أن يكون موثوقًا به في الشبكات المفتوحة كالإنترنت؛ حيث لا يعرف الأشخاص بعضهم البعض، هذا من ناحية. ومن ناحية ثانية، يُؤخذ على التشفير المتماثل تكلفته المادية المرتفعة [3]، مما يجعله خيارًا تقنيًا قد لا يناسب بعض الجهات والأشخاص. ومن ناحية ثالثة، يُعاب على هذا التشفير، تعدد

---

[1] – المفتاح السري هو عبارة عن قيمة غير معتمدة على الرسالة، يختارها نظام التشفير أو مستخدم البريد الإلكتروني.

[2] – أنظر في ذلك الموقع التالي:

- https://me.kaspersky.com/resource-center/definitions/encryption (19-4-2021).

– وأنظر في ذلك أيضًا:

- JEFF TYSON , HOW ENCRYPTION WORKS …… https://computer.howstuffworks.com/encryption2.htm (20-4-2021).

[3] - Dr. Bill Young , op . cit , p. 6.

المفاتيح السرية؛ حيث يجب على كل شخص أن يحتفظ بعدد من المفاتيح بعدد كل من يريد التراسل معهم[1].

2- التشفير غير المتماثل: وفي هذا النوع من أنواع التشفير، يتم استخدام مفتاحين مختلفين، أحدهما عامًا والآخر خاصًا، يكونا على ارتباط مع بعضهما البعض من الناحية الحسابية. والمفتاحان هما في الأساس مجرد أرقام كبيرة تم ربطهما معًا لكنهما ليسا متماثلين، ومن هنا جاءت التسمية "غير متماثل". وهنا يمكن مشاركة المفتاح العام مع أي شخص، مع ملاحظة ضرورة إبقاء المفتاح الخاص سرًا. ويمكن استخدام المفتاحين لتشفير رسالة، ثم يُستخدم المفتاح المختلف عن المفتاح الذي استُخدم أصلاً في تشفير تلك الرسالة لفك ترميزها [2].

ويُعاب على نظام التشفير غير المتماثل أنه بطئيًا بالمقارنة مع التشفير المتماثل. ورغم ذلك، إلا أنه يُحسب له درجة الأمان العالية التي يتمتع بها هذا النظام، وذلك على عكس نظام التشفير المتماثل؛ ويرجع ذلك لوجود المفتاحين العام والخاص [3].

وبالنسبة لطريقة استخدام أو عمل هذا النظام، فهي تختلف باختلاف الغرض منه والوظيفة

---

[1] – د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 171، 172.

[2] – أنظر في ذلك الموقع التالي:

- https://me.kaspersky.com/resource-center/definitions/encryption (19-4-2021).

[3] – أنظر في ذلك الموقع التالي:

- http://www.hackingwithphp.com/17/3/3/asymmetric-vs-symmetric (20-4-2021).

التي يتم اللجوء إليه لتحقيقها، وهل هي وظيفة التشفير أم التوقيع الإلكتروني. فإذا كان الغرض من استخدامه هو التشفير، فهنا يقوم المرسل بتشفير الرسالة بالمفتاح العام للمرسل إليه، ثم يقوم هذا الأخير بفك رموز الرسالة عن طريق المفتاح الخاص والذي يكّمل المفتاح العام. أما في حالة استخدام التشفير غير المتماثل في التوقيع الإلكتروني، فهنا يقوم المرسل بتشفير الرسالة عن طريق المفتاح الخاص، ويقوم المستقبل بفك تشفيرها عن طريق المفتاح العام الموافق للمفتاح الخاص [1].

وهذين النوعين من التشفير، تعرض لهما المشرع المصري في المادة رقم (1) من اللائحة التنفيذية للقانون رقم 175 لسنة 2018، بشأن مكافحة جرائم تقنية المعلومات، والتي تنص على أن :" مفتاح التشفير .... أرقام أو رموز ذات طول محدد، تُستخدم في عمليات التشفير وفك التشفير. ويُستخدم نفس المفتاح في التشفير وفك التشفير ويسمى التشفير المتماثل، ويجب الحفاظ على سرية المفتاح. ويُستخدم زوج من المفاتيح مترابطين بعلاقة رياضية، بحيث يُستخدم أحدهما في التشفير والآخر في فك التشفير ويسمى بالتشفير غير المتماثل، ويجب الحفاظ على سرية أحد المفاتيح، بينما يُعلن عن الآخر بشروط ومعايير محددة ".

والملاحظ أن فكرة التشفير غير المتماثل تقوم على أساس وجود مفتاحين، أحدهما عام والآخر خاص، فما المقصود بكل منهما من أجل تسهيل إيضاح فكرة هذا النوع من أنواع التشفير؟

عبَّر المشرع المصري عن تقنية التشفير غير المتماثل بتقنية شفرة المفتاحين العام والخاص أو تقنية شفرة المفتاح العام. وعرفها بأنها منظومة حسابية تسمح لكل شخص طبيعي أو معنوي بأن يكون لديه مفتاحين متفردين، أحدهما عام متاح إلكترونيًا، والثاني خاص يحتفظ به الشخص

[1] – د/ عبد الهادي فوزي العوضي، مرجع سابق، ص 172، 173.

ويحفظه مع درجة عالية من السرية [1].

وتعرض كذلك المشرع المصري لتعريف المفتاح الشفري العام والخاص. حيث عرف المفتاح الشفري العام بأنه أداة إلكترونية متاحة تنشأ بواسطة عملية حسابية خاصة وتُستخدم في التحقق من شخصية الموَّقع على المحرر الإلكتروني والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي [2].

بينما عرف المفتاح الشفري الخاص، بأنه أداة إلكترونية خاصة بصاحبها، يُنشأ بواسطة عملية حسابية خاصة، ويتم الاحتفاظ بها على أداة إنشاء التوقيع الإلكتروني، وتُستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية [3].

ويُلاحظ على التعريفات التشريعية السابقة والخاصة بتقنية التشفير، أمرين هما:

1- الأمر الأول: ويتمثل في أنه على الرغم من أن التعريفات السابقة، قد وردت أو جاء النص عليها بمعرض تناول المشرع المصري لأحكام التوقيع الإلكتروني، إلا أن الأحكام الخاصة بالتشفير يمكن استخدامها وتفعيلها من أجل حماية البريد الإلكتروني للأشخاص. فالتوقيع الإلكتروني يكون مُتضمَنًا في محرر إلكتروني، وهذا الأخير لكي يحتج بقوته القانونية في مجال الإثبات القانوني، فلابد من تداوله عبر وسيط إلكتروني يصلح لهذا التداول، وهذا الوسيط قد يتمثل

---

[1] – المادة رقم (15/1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم 15 لسنة 2004.

[2] – المادة رقم (16/1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم 15 لسنة 2004.

[3] – المادة رقم (17/1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم 15 لسنة 2004.

في صورة بريد إلكتروني أو غيره من الوسائط الإلكترونية[1] . لذلك فإن القواعد الخاصة بالتشفير والتي تم النص عليها في قانون التوقيع الإلكتروني يمكن تطبيقها وتفعيلها من أجل حماية البريد الإلكتروني؛ وخصوصًا في ظل عدم وجود حماية قانونية أو تقنية خاصة لحماية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها.

2- الأمر الثاني: ويتمثل في تعرف المشرع لوضع تعريفات قانونية لبعض المصطلحات الخاصة بالمسائل التي يتناولها في بعض القوانين. فمن المعلوم أنه المشرع لا يلتزم بوضع تعريفات للمصطلحات التي ترد بالتشريعات، فبرغم تسليمنا بهذا الأمر، إلا أنه في بعض الحالات والمسائل ذات التطور التقني والتي تتسم بحداثة الظهور على الساحة القانونية، فإنها تفرض نفسها على المشرع من أجل وضع تعريفًا لها ولا يستطيع المشرع إغفال تعريفها، إما لأهميتها بالنسبة للتشريع الذي يتناول تنظيمه، وإما للمبررات العملية والواقعية التي تفرض على المشرع ذلك. وخصوصًا بالنسبة للتعريفات التقنية التي يمكن أن نطلق عليها مصطلح "التعريفات المرنة"، والتي يتغير تعريفها بتغير التطور التكنولوجي الذي يلحق بها، والتي يلتزم المشرع بأن يسايرها وألا يقف عاجزًا أمامها أو متخذًا موقفًا سلبيًا حيالها. ومن هنا يمكننا القول بأن المشرع المصري قد أحسن صنعًا حينما تعرض للتعريفات السابقة.

ونظرًا لأهمية نظام التشفير في الحفاظ على سرية البيانات والمعلومات وكذلك سرية مراسلات البريد الإلكتروني ومحاربة ظاهرة إرسال الرسائل الإلكترونية غير المرغوب فيها، فقد جعله – أي

---

[1] – أنظر في ذلك: د/ سامح عبد الواحد التهامي، المحرر الإلكتروني، بدون ناشر، سنة 2020، ص 42 وما بعدها.

نظام التشفير – المشرع المصري التزامًا يقع على عاتق مقدمو خدمات التقنيات والمعلومات. وجاء ذلك في اللائحة التنفيذية للقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات في المواد الآتية:

1- المادة رقم (1/2) من اللائحة المذكورة، تنص على أنه:"يلتزم مقدمو خدمات تقنيات المعلومات باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (2،3) من الفقرة أولًا من المادة رقم (2) من القانون .....1- تشفير البيانات والمعلومات بما يحافظ على سريتها وعدم اختراقها باستخدام نظام تشفير قياسي متماثل أو غير متماثل لا يقل في تأمينه عن Encryption standard (ASE-128) Advanced، بمفتاح شفرة لا يقل عن (128 بت)، مع مسئوليته بالحفاظ على سرية وأمان مفتاح التشفير".

2- المادة رقم (3/3) من اللائحة المذكورة، تنص على أنه:" يلتزم مقدمو خدمات تقنية المعلومات والاتصالات التي تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة [1]

[1] – يُقصد بالبنية التحتية المعلوماتية الحرجة، مجموعة أنظمة أو شبكات أو أصول معلوماتية أساسية يؤدي الكشف عن تفصيلاتها تعطيلها أو تغيير طريقة عملها بطريقة غير مشروعة، أو الدخول غير المصرح به، أو الدخول أو الوصول بشكل غير قانوني للبيانات والمعلومات التي تحفظها أو تعالجها، أو يؤدي القيام بأي فعل غير مشروع آخر بها إلى التأثير على توافر خدمات الدولة ومرافقها الأساسية أو خسائر اقتصادية أو اجتماعية كبيرة على المستوى الوطني. ويعد من البنية التحتية المعلوماتية الحرجة على الأخص ما يستخدم في الطاقة الكهربائية، الغاز الطبيعي والبترول والاتصالات، والجهات المالية والبنوك، والصناعات

المخاطبين بأحكام هذا القانون، باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (2،3) من الفقرة أولًا من المادة رقم (2) من القانون :" تشفير البيانات والمعلومات بما يحافظ على سريتها وعدم اختراقها باستخدام نظام تشفير قياسي متماثل أو غير متماثل لا يقل تأمينه عن Encryption standard (ASE-128) Advanced، بمفتاح شفرة لا يقل عن (256 بت) يتم توليده باستخدام نظام عشوائي آمن، واستخدام نظام إدارة مفاتيح تشفير قياسي للحفاظ على سريتها ودورة حياتها ومستويات استخدامها في التطبيقات المختلفة ".

وترتيبًا على ما تقدم، فإن أهمية اللجوء إلى خاصية التشفير في هذا الصدد، هي الرغبة في الحفاظ على سرية المراسلات التي تحدث عن طريق البريد الإلكتروني؛ لأن التساهل في هذا الأمر يجعل هذه المراسلات عرضة للاختراق ومن ثم معرفة المخترقون لرغبات الشخص بالنسبة للسلع والخدمات والمنتجات على وجه العموم، مما يترتب عليه فتح باب إرسال الرسائل الإلكتروني غير المرغوب فيها لهؤلاء الأشخاص بما يتناسب مع ميولهم. لذلك نوصي المستخدمين بضرورة تفعيل نظام التشفير لتحقيق أقصى حماية وسرية ممكنين لحماية البريد الإلكتروني، فأساليب التشفير

المختلفة، والنقل والمواصلات والطيران المدني، والتعليم والبحث العلمي، والبث الإذاعي والتلفزيون، ومحطات مياه الشرب والصرف الصحي والموارد المائية والصحة، الخدمات الحكومية وخدمات الإغاثة وخدمات الطوارئ، وغيرها من مرافق المعلومات والاتصالات التي قد تؤثر على الأمن القومي أو الاقتصاد القومي والمصلحة العامة وما في حكمها" ..... المادة رقم (1) من اللائحة التنفيذية للقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

القياسية هي من وسائل الحماية من رسائل البريد العشوائي [1].

الفصل الثالث

الحماية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها

- تقسيم:

تتمثل الحماية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، في مجموعة من التوجيهات ذات الطابع العام، سواء على المستوى التقني أم على المستوى القانوني، الغرض منها مساندة وتأييد الحماية القانونية والتقنية الخاصة والتي ذكرناها في الفصول السابقة.

وهنا سنبدأ الحديث بالتعرض للحماية العامة من منظور تقني (مبحث أول)، ثم الحماية العامة من منظور قانوني (مبحث ثان)؛ وذلك باعتبار أن الحماية العامة التقنية سيكون لها نصيب الأسد في هذا الصدد. وذلك على البيان التالي:

المبحث الأول

الحماية العامة للأشخاص من الرسائل غير المرغوب فيها من منظور تقني

[1] – د/ رياض سلطان علي، نظم المعلومات الإدارية وتطبيقاتها في الصناعة، التنظيم والتكنولوجيا بين النظرية والتطبيق، Almanhal, 2006، ص 209.

تدور هذه الحماية في إطار مجموعة من العوامل الحمائية التقنية العامة التي يمكن تطبيقها من أجل مساعدة الأشخاص على محاربة ظاهرة الرسائل الإلكترونية غير المرغوب فيها وغير هذه الظاهرة. ولما كانت معظم هذه الرسائل ترد إلى الأشخاص عبر البريد الإلكتروني، فوجب البحث عن الضوابط التي تجنب الأشخاص إرسال أو استقبال رسائل غير مرغوب فيها إليهم، والتي يعد منها الأمور الآتية:

أولًا: بالنسبة لكلمة المرور الخاصة بالبريد الإلكتروني [1]:

حيث يجب اختيار كلمة مرور قوية يصعب اختراقها؛ لأنه كلما كانت هذه الكلمة ضعيفة وسهل توقعها كلما كانت فرص اختراق البريد الإلكتروني من السهولة بما كان. فمن يحاول اختراق هذا البريد من أجل إرسال رسائل غير مرغوب فيها، سيعتمد في ذلك على ضعف كلمة المرور.

ومن أجل تجنب ذلك، يجب التأني عند اختيار كلمة المرور وجعلها قوية، وذلك عن طريق بعض الأمور التقنية وهي: أن تكون كلمة المرور طويلة، فكلما كانت طويلة كلما كانت أفضل من الناحية الحمائية. ويلزم كذلك استخدام الأحرف الكبيرة والصغيرة. ويجب أن تتضمن كلمة المرور على حروف مثل "1،2،3"، وكذلك يلزم أن تتضمن عناصر مميزة كعلامة الاستفهام وعلامة

---

[1] – أنظر في ذلك:

- Essential Cyber Security Handbook In Arabic , Nam H Nguyen , 2018.

– متاح على الموقع التالي:

- https://books.google.com.eg/books (21-4-2021).

النسبة المئوية [1].

وبالنسبة للرسائل الجماعية، فيجب تعقيد إرسالها عن طريق بعض الضوابط التقنية كتطلب إدخال رمز التأكيد بالإضافة إلى كلمة المرور، وفرز الرسائل المستلمة لفصل الرسائل غير المرغوب فيها عن الرسائل الشرعية من خلال الإبلاغ عن الرسائل المستلمة إلى المنظمات التي يمكنها محاربتها عن طريق تحديد وإدانة مرسلي هذه الرسائل.

ثانيًا: بالنسبة لجهة الإرسال ذاتها:

وهنا تتم حماية عنوان البريد الإلكتروني من الرسائل الإلكترونية غير المرغوب فيها، من منظور الجهة التي ترسل هذه الرسائل، وذلك بفحص جهة الإرسال وهذا من ناحية، وتجنب الضغط على أي رابط يرسل رسائل ويكون مصدره مجهول وهذا من ناحية ثانية [2]:

1- فحص جهة إرسال البريد الإلكتروني: وهنا نجد أن أغلب الرسائل الإلكترونية غير المرغوب فيها تُرسل من مصادر مجهولة أو يصعب التعرف عليها، وتُرسل عادة من عناوين بريد إلكتروني غريبة. غير أن ذلك لا يعني بالضرورة أن كل رسالة مجهولة المصدر هي رسائل غير مرغوب فيها أو مزعجة؛ فالنشرات البريدية الشرعية والرسائل الواردة من إدارة المواقع الإلكترونية كتلك المتعلقة باستعادة كلمات المرور ومنح إذن الولوج وغير ذلك. وعندما تكون الرسالة مهمة

---

[1] – أنظر في ذلك الموقع التالي:

- https://www.itpillars.com/ar/blog/ (15-4-2021).

[2] – أنظر في ذلك الموقع التالي:

- https://ar.wikihow.com (16-4-2021).

بالنسبة لصاحب البريد الإلكتروني، فيُحتمل أن تأتي من بريد إلكتروني غريب في غالب الأمور. ولكي تسهل مهمة تمييز الرسائل غير المرغوب فيها، فيجب أن يتوقع المستخدم أن البريد الإلكتروني الذي يرسلها يحتوي على عدة أرقام وتركيبات غريبة للحروف والكلمات.

2- تجنب الضغط على أي رابط يرسل رسائل ويكون مصدره مجهول: إن إرسال رسالة من بريد إلكتروني مجهول المصدر، يتضمن قرينة على أن هذه الرسالة عشوائية أو غير مرغوب فيها[1]؛ حيث إن الهدف الرئيسي المعتاد لأي رسالة بريد إلكتروني غير مرغوب فيها هي دفع الشخص لأن يضغط على رابط إلكتروني يمنحهم الإذن من صاحب البريد الإلكتروني بسرقة بياناته أو تثبيت البرمجيات الخبيثة على جهاز الشخص. لذلك لا تضغط نهائيًا على أي رابط إلكتروني لا تثق به في رسائل البريد الإلكتروني طالما أنها كانت مرسلة من مصدر مجهول لا يمكن الوثوق به.

ولكن ما الذي يجب فعله في حالة ما إذا كانت الرسالة واردة من بريد إلكتروني من شخص يعرفه المرسل كصديق أو قريب مثلًا، وانتابه الشك بشأن مصدر هذه الرسالة؟

في هذه الحالة قد يستشعر المرسل إليه الحرج من عدم فتح الرسالة لكونها واردة إليه من شخص تربطه به إما رابطة قرابة أو صداقة؛ لذلك ومن أجل التوفيق بين حرص الشخص على عدم استقبال رسائل غير مرغوب فيها وبين رفع الحرج عنه؛ فلا ضير أن يسأل أو يستفسر المرسل إليه من المرسل عن مصدر هذه الرسالة وهل هو مصدر موثوق منه أم أنه غير ذلك؛

---

[1] – مع ملاحظة أن هذه القرينة غير قاطعة؛ فأحيانًا ترد الرسالة من مصدر مجهول ولا تكون غير مرغوب فيها، كما سبق الذكر بالبند رقم 1.

وذلك لأن كون الرسالة من عنوان بريد إلكتروني معروف ومحل ثقة لدى المرسل إليه لا يعني بالضرورة أن مصدر الرسالة ذاته محل ثقة. فأحيانًا يتم اختراق البريد المرسل – والذي يكون معروفًا لدى المرسل إليه – وتتم السيطرة على جهات الاتصال الموجودة في بريد المرسل ويحاول المخترق السيطرة على العناوين البريدية المتاحة بالبريد الإلكتروني المخترق.

ثالثًا: بالنسبة للرسالة ذاتها:

وهنا ترتكز وسيلة الحماية التقنية العامة من الرسائل الإلكترونية غير المرغوب فيها، على الرسالة المرسلة ذاتها. ويتمثل هذا الارتكاز على أمرين هما [1]:

1- الأمر الأول: ويتمثل في ضرورة التزام المرسل إليه بالتدقيق في الكتابة الإملائية واللغوية لنص الرسالة. فغالبًا ما تتضمن الرسائل الإلكترونية غير المرغوب فيها على أخطاء إملائية ونحوية وتركيبات لغوية غريبة وغير صحيحة [2]. وأحيانًا يتمثل ذلك في صورة تنسيق غريب لنص الرسالة كتضخيم الخط أو إمالته أو التلوين العشوائي للنص أو تكبير غريب للأطرف في نصف الكلمات في حالة ما إذا كانت الرسالة باللغة الإنجليزية أو تضمنت علامات ترقيم في موضع غير صحيح.

2- الأمر الثاني: ويتمثل في ضرورة التزام المرسل إليه بالقراءة المتأنية الحريصة للرسالة

---

[1] – أنظر في ذلك الموقع التالي:

- https://ar.wikihow.com (16-4-2021).

[2] – أنظر في ذلك الموقع التالي:

- https://support.microsoft.com/ar-sa/windows (21-4-2021).

المرسلة. ويعني ذلك أن وجه عدم المرغوبية بالنسبة للرسالة المرسلة يتضح من المحتوى غير المصدق للرسالة ذاتها، كالرسالة التي تخبر الشخص بفوزه بجائزة مالية كبيرة في مسابقة لم يشارك فيها المرسل إليه من الأساس [1]، أو الرسائل التي تتضمن عرضًا على الشخص بالحصول على ثروة كبيرة أو أجهزة إلكترونية أو مجوهرات أو منتجات باهظة الثمن أو سيارات فاهرة إذا ما اشترك الشخص في مسابقة ما وذلك من أجل إجبار الشخص على الإفصاح عن عنوان بريده الإلكتروني أو كلمة المرور الخاصة بهذا العنوان.

والسؤال الذي يُثار هنا: كيف يتسنى للمرسل إليه معرفة مضمون الرسالة لكي يفحصها إملائيًا أو يتفقد مضمونها دون أن يفتح هذه الرسالة؟

يستطيع المرسل إليه أن يتجنب فتح الرسالة غير المرغوب فيها ومعرفة مضمونها من خلال نافذة العرض المقدمة من قبل مزودي خدمات البريد الإلكتروني والتي تعرض للمستخدم الجزء الأول من الرسالة، الأمر الذي يمكّن المرسل إليه عادة من فهم طبيعة محتوى الرسالة ليحدد موقفه وما إذا كان سيتجاوب معها أم أنه سيتجنبها بصورة كلية لأنها غير مرغوب فيها أو مزعجة.

رابعًا: بالنسبة لعرض عنوان البريد الإلكتروني ذاته:

وهنا تتمثل الحماية التقنية العامة من الرسائل الإلكترونية غير المرغوب فيها، من منظور مدى عرض عنوان البريد الإلكتروني ذاته للعامة من عدمه وهذا من ناحية، ومدى قابلية هذا العنوان للاكتشاف حال عرضه من عدمه وهذا من ناحية ثانية، ومدى تشابه هذا العنوان مع غيره

---

[1] – أنظر في ذلك الموقع التالي:

- https://blog.hotmart.com (22-4-2021).

من العناوين الأخرى من عدمه وهذا من ناحية ثالثة [1]:

1- ضرورة التزام صاحب البريد الإلكتروني بعدم عرض عنوان هذا البريد للعامة: وهذا الأمر يعني ضرورة أن يحطاط صاحب البريد الإلكتروني وألا يجعل عنوان بريده متاحًا للعامة على الصفحات والمواقع الإلكترونية المختلفة عبر شبكة الإنترنت؛ وذلك لأن الجهات والأشخاص الذين يرسلون الرسائل الإلكترونية غير المرغوب فيها يعتمدون في جمع عناوين البريد الإلكتروني التي يرسلون إليها هذه الرسائل على جمع آلاف هذه العناوين من المواقع التي تعرضها بشكل عام، وذلك من خلال الاعتماد على "الروبوتات البرمجية الآلية"[2]. وكذلك يلتزم المستخدم بعدم إدخال عنوان بريده الإلكتروني الشخصي في عمليات التسجيل للأشياء مثل أقسام الشراء. وأيضًا يلتزم بألا يكتب هذا العنوان في تعليق أو منشور إلكتروني؛ لأن ذلك يسّهل من أمر معرفة العامة لهذا العنوان.

2- ضرورة العمل على جعل عنوان البريد الإلكتروني غير قابل للاكتشاف: وهذا يعني أنه إذا كان المستخدم مضطرًا لتقديم هذا العنوان، فمن الممكن أن يقدمه بطريقه تجعله غير قابل للاكتشاف من قبل الغير، أي يجب كتابته بطريقة ذكية، كاستبدال العلامة المختصرة (@) بـ (at)

---

[1] – أنظر في ذلك الموقع التالي:

- https://ar.wikihow.com (16-4-2021).

[2] – الروبوتات البرمجية الآلية، هي عبارة عن برامج نصية يتم إنشائها لاستخراج عناوين البريد الإلكتروني من المواقع الإلكترونية ..... أنظر في ذلك الموقع التالي:

- https://www.automationanywhere.com/ae/rpa/robotic-process-automation (22-4-2021).

واستبدال العلامة المختصرة (com)، بـ (dot com)؛ وذلك بغرض منع مرسلي الرسائل الإلكترونية غير المرغوب فيها من التوصل إلى عنوان البريد الإلكتروني عن طريق الروبوتات البرمجية الآلية.

وفي بعض الأحيان يكون الفرد مجبرًا على تقديم عنوان بريد إلكتروني صحيح لتتم مراسلته عليه كما في حالة التقديم لوظيفة ما أو شراء سلعة ضرورية استلزمت ضرورة إفصاح الشخص عن هذا العنون، فمن الممكن أن يستخدم الشخص حساب بريد إلكتروني عشوائي يؤدي الغرض المطلوب؛ حفاظًا على سرية وأمان الحساب الحقيقي [1]. أي يفضل أن يكون للشخص أكثر من عنوان بريد إلكتروني، يكون من بينها عنوان خاص يُستخدم للمراسلات الخاصة، وعنوان آخر أو أكثر لغير المراسلات الخاصة يمكن للشخص تقديمه لأي شخص أو جهة ما إذا تطلب الأمر ذلك[2].

3- ضرورة الالتزام بعدم استخدام اسم مستخدم مشابه لعنوان البريد الإلكتروني: حيث إنه عادة ما تكون أسماء المستخدمين في مختلف المنتديات والمواقع متاحة للاطلاع العام، وهو ما يجعل توقع بريدك الإلكتروني المطابق له مسألة وقت وبعض التخمينات لا أكثر. فعلى سبيل المثال، نجد أن بعض الخدمات مثل (yahoo chat)، يعيبها أنها تسَهل من هذا الأمر؛ فغالبًا ما

---

[1] – أنظر في ذلك الموقع التالي:

- https://www.youm7.com/story (16-4-2021).

[2] – أنظر في ذلك الموقع التالي:

- https://me.kaspersky.com/resource-center/threats/spam-phishing (22-4-2021).

يكون عنوان البريد الإلكتروني مطابقًا لنفس اسم المستخدم عليها مضافًا إليه (@ yahoo.com) فقط لا غير.

ويجب بالإضافة إلى ما تقدم، ضرورة ألا يتجاوب المرسل إليه مع أي رسالة يظن أنها غير مرغوب فيها، وله في سبيل تسهيل معرفة ذلك أن يستعين بمرشحات فلترة البريد الإلكتروني لاكتشاف مثل هذه الرسائل [1]. كما أنه إذا حدث وأن فتح المستخدم رسالة كانت غير مرغوب فيها، فعليه حظر جهة الإرسال على الفور؛ لأن هذا الحظر يساعد على منع الوصول إلى صندوق البريد الخاص بالمستخدم. كما أنه يمكن استعمال تقنيات الذكاء الاصطناعي للتعرف على البريد العشوائي الذي يرسل الرسائل الإلكترونية غير المرغوب فيها [2].

المبحث الثاني

الحماية العامة للأشخاص من الرسائل غير المرغوب فيها من منظور قانوني

تتمثل الحماية القانونية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، في مجموعة من الضوابط والإرشادات ذات الطابع القانوني، والتي تلتزم بها الجهات المعنية حماية للأشخاص من مثل هذه الرسالة. ويعد من أهم هذه الضوابط ما يلي:

أولًا: التزام الشركات بالبنود التعاقدية:

---

[1] – أنظر في ذلك الموقع التالي:

- https://support.microsoft.com/ar-sa/office (17-4-2021).

[2]- Emmanuel Ghesquier, « Gmail utilise l'IA pour lutter contre le spam » [archive], sur *Presse-Citron*, 8 février 2019 (consulté le 12 mars 2019).

وهنا نؤكد على ضرورة التزام شركات الدعايا والإعلان عن السلع والمنتجات والخدمات التي تُباع أو تُعرض عبر شبكة الإنترنت عن طريق المواقع الإلكترونية وصفحات التواصل المختلفة بالبنود التعاقدية التي يتم الاتفاق عليها بين الطرفين، والتي يكون من بينها التزام هذه الشركات بعدم إرسال رسائل إلكترونية غير مرغوب فيها إلى الأشخاص، ما لم يوافقوا على ذلك على النحو الذي بينّاه في موضعه.

حيث إنه في كثير من الأحيان، لا تكون الشركات على دراية بكيفية تقديم إعلانات منتجاتها وخدماتها للجمهور؛ فمعظم هذه الشركات توفر حزم من البرامج القانونية مع برامج التجسس بهدف الوصول إلى البيانات الحساسة للأشخاص مثل أرقام بطاقات الائتمان والمستندات السرية. فهنا تلتزم هذه الشركات بالامتناع عن هذه الأمور وهذا من ناحية، ومن ناحية ثانية تلتزم هذه الشركات من التأكد من أن أنشطة شركائها التجاريين قانونية ومشروعة وتلتزم بهذا الأمر. فيجب على هذه الشركات تفهم كيفية عمل سلسلة العلاقات التعاقدية والتحقق من الامتثال للقانون والتحكم في كيفية وصول الإعلانات إلى المستهلكين ومتابعة المخالفات [1].

فالتزام شركات الدعايا والإعلان بالبنود التعاقدية، يحتم أن تكون الرسائل المرسلة للمستخدم أو الإعلانات التجارية التي توجه إليه نزيهة سواء بالنسبة للمعلن أو بالنسبة للمرسل إليه أو المستهلك. وتعني نزاهة هذه الدعايا والإعلانات، ضرورة ألا تتضمن كذبًا أو خداعًا أو حتى رسائل إلكترونية

[1] - Document de la Commission COM (2006) 688 final du 15 novembre 2006 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la lutte contre la pourriel, les espiogiciels et les logiciels malveillants.

غير مرغوب فيها، واحترام خصوصياتهم وبياناتهم ومراعاة الضوابط القانونية عند المساس بأي من هذه الأمور [1].

وذلك لأن الواقع العملي يبرز لنا أمثلة وواقعات غير مرضية للأشخاص في هذا الشأن؛ حيث لا تحترم العديد من شركات الدعايا والإعلان الشروط التعاقدية التي تحظر عليهم إرسال رسائل إلكترونية غير مرغوب فيها. بل أكثر من ذلك، نجد أن العديد من هذه الشركات تعتمد في ترويج منتجاتها وخدماتها على العرض الجبري لها على الأشخاص عن طريق تعمد إرسال الرسائل المذكورة دون موافقة المرسل إليه، وتعتبر أن هذه الطريقة هي وسيلة عرض وفعالة؛ نظرًا لقلة تكلفتها المادية والعائد الاقتصادي الكبير منها.

وترجع أهمية التزام شركات الدعايا والإعلان بالنزاهة عند عرضهم للسلع والخدمات والمنتجات وعدم إرسال رسائل غير مرغوب فيها، إلى أن البريد الإلكتروني لا يزال هو قناة الاتصال المفضلة للعملاء؛ لذلك فمن المهم بالنسبة لهذه الشركات إعادة التفكير في استراتيجية التسويق عبر هذا البريد كل يوم، وذلك من أجل بناء اتصال حقيقي مع العملاء. ويكون ذلك عن طريق الالتزام بضرورة أن تكون رسائل البريد الإلكتروني توفر معلومات ذات صلة وقيمة في الوقت المناسب وأن تكون مرغوب فيها لدى الأشخاص الذين تُرسل إليهم هذه الرسائل، وإلا كانت رسائل غير مرغوب فيها[2].

---

[1] – أنظر في الإعلانات الإلكترونية النزيهة: د/ أحمد عبد التواب محمد بهجت، الحماية القانونية للمستهلك الإلكتروني، دار النهضة العربية، سنة 2020، ص 31 وما بعدها.

[2] – أنظر في ذلك الموقع التالي:

ثانيًا: سن التشريعات الدولية:

من المعلوم أنه إذا كانت القوانين الداخلية أو الوطنية تساعد في محاربة ظاهرة الرسائل الإلكترونية غير المرغوب فيها، إلا أن ذلك لا يعتبر كافيًا لمواجهة ظاهرة تتم عبر شبكة عالمية لا تُعرف حدوها الجغرافية أو معالمها المادية، الأمر الذي يترتب عليه ضرورة وجود تكاتف تشريعي على المستوى الدولي؛ لاسيما وأنه ليس للإنترنت إدارة مركزية تدير عملية استخدامه بشكل مركزي مباشر يتحكم بقواعد استخدامه أو بالنواحي التقنية للشبكة [1].

وهذا السن التشريعي الدولي يتمثل في صورة إبرام اتفاقيات دولية تتضمن إقرار تشريعات دولية تضع حلولًا لمكافحة ظاهرة الرسائل الإلكترونية غير المرغوب فيها. وذلك لأن التزايد في إبرام المعاملات الإلكترونية أصبح يعرض المستخدم أو المستهلك للتلاعب في العمليات التعاقدية. فنظرًا لأن التعامل يتم من خلال وسيلة إلكترونية أصبح المستهلك من خلالها غير مقيد بأية حواجز زمانية أو مكانية تمكنه من الحصول على المنتج أو الخدمة من أي مكان في العالم [2]، وكذلك الأمر بالنسبة للمعلن عن هذه السلع والخدمات.

- https://www.vtiger.com/ar/blog/a-quick-guide-to-email-marketing/ (23-4-2021).

[1] – التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات، بحث صادر عن مركز هرود لدعم التعبير الرقمي، القاهرة، سنة 2018، ص 5..... متاح على الرابط التالي:

- https://hrdoegypt.org/wp-content/uploads (23-4-2021).

[2] – د/ أحمد أسامة بدر، الوسائط المتعددة بين الواقع والقانون، دار النهضة العربية، بدون سنة نشر، ص 95.

وما يبرر هذا التعاون التشريعي الدولي، هو أن إرسال الرسائل الإلكترونية غير المرغوب فيها يمكن أن يندرج تحت مضمون الجريمة الإلكترونية. فهذه الأخيرة هي عبارة عن الممارسات التي توقع ضد فرد أو مجموعة مع توفر باعث إجرامي بهدف التسبب بالأذى لسمعة الضحية عمدًا أو إلحاق الضرر النفسي والبدني به، سواء كان ذلك بأسلوب مباشر أو غير مباشر كالاستعانة بشبكات الاتصال الحديثة كالإنترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المحادثة والهواتف المحمولة [1] [2].

وهذا التعاون الدولي يستتبع ضرورة القيام بإجراءات إنفاذ القانون. فكلما كانت هذه الإجراءات الخاصة بظاهرة الرسائل الإلكترونية غير المرغوب فيها مطبقة، كلما انعكس ذلك على عدد الاختراقات لعناوين البريد الإلكتروني ومن ثم الرسائل التي تُرسل للأشخاص من خلاله [3].

---

[1] – يُقصد بغرف المحادثة أو غرف الدردشة، ساحات افتراضية للقاء بين مستخدمي شبكة الإنترنت والتحدث وتبادل الأفكار والمعلومات، وذلك من خلال الرسائل المكتوبة مباشرة عبر لوحة المفاتيح لجهاز الكمبيوتر أو من خلال التليفون المحمول المتصل بالإنترنت أو من خلال إرسال رسائل عبر البريد الإلكتروني. وهذا التخاطب عبر الإنترنت يمكن للآخرين رؤيته سواء المشتركين في الغرف أو من ينضم لاحقًا ..... م/ بهاء المري، شرح جرائم تقنية المعلومات، القانون رقم 175 لسنة 2018، منشأة المعارف، سنة 2019، ص 28.

[2] – التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات، مرجع سابق، ص 7.

[3] - Document de la Commission COM (2006) 688 final du 15 novembre

ثالثًا: ضرورة إعمال توعية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها:

وتتم هذه التوعية من خلال زيادة وعي المستخدمين وأصحاب عناوين البريد الإلكتروني من خطورة وأضرار الرسائل الإلكترونية غير المرغوب فيها وكيف تُرسل إليهم. وهنا تقع مسؤولية كبيرة على عاتق مزودي خدمات الإنترنت، تتمثل في إمداد عملائهم بالمشورة والمساعدة حول كيفية حماية أنفسهم من برامج التجسس والفيروسات [1].

ويتعاظم هذا الدور التوعوي لمزودي خدمات الإنترنت؛ لأن الكثير من المهنيين يسعوا إلى اتخاذ وسائل غير مشروعة من أجل الترويج لمنتجاتهم وتسويقها بأي وسائل والتي يكون من بينها إرسال رسائل إلكترونية غير مرغوب فيها، بالإضافة إلى تضليل المستهلك وخداعه في بعض الأحيان عن طريق إيجاد مميزات غير حقيقية على السلع والخدمات، وأصبح المستهلك هدفًا لغش منتشر وفساد مستفحل وإعلام متطور وخادع، سلاحه عدم وعي المستهلك [2].

وفي ختام تعرضنا للحماية القانونية والتقنية سواء العامة أو الخاصة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، يجب أن ننوه إلى أن صور الحماية مهما تعددت فهي لن كافية

2006 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la lutte contre la pourriel, les espiogiciels et les logiciels malveillants.

[1] – الوثيقة السابقة.

[2] – د/ مأمون علي عبده قائد الشرعبي، الحماية القانونية للمستهلك عبر الإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، سنة 2019، ص 78.

بنسبة مائة بالمائة لمحاربة هذه الظاهرة ذات الانتشار الواسع، وإن كانت تمثل محاولات أو اجتهادات – في أغلبها – من أجل ضمان الحفاظ على سرية عنوان البريد الإلكتروني للشخص ومنع إرسال رسائل غير مرغوب فيها إليه.

وفي سبيل تحقيق هذه الهدف الأخير، يجب ألا نغفل بأي حال من الأحوال أن العبء الحمائي الأكبر في هذا الشأن إنما يكون بالتعويل على الحماية التقنية المتطورة والمحدِّثة لكي تجاري التطور الذي يلحق بهذه الظاهرة على وجه الخصوص والجريمة الإلكترونية على وجع العموم. فمهما أُقرت قواعد قانونية في هذا الشأن، فلن تكون فعالة ومجدية بنفس فعالية وكفاءة الحماية التقنية المرنة، كل ذلك على النحو الذي بينَّاه في هذه الدراسة المتواضعة.

الـــخـــاتـمـــة

سنختتم تعرضنا لمسألة حماية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها، بإبراز نتائج هذه الدراسة (أولًا)، وتوصياتها (ثانيًا)، على النحو التالي:

أولًا: نتائج الدراسة:

1- الرسائل الإلكترونية غير المرغوب فيها, هي عبارة عن مراسلات جماعية يقوم بإرسالها شخص أو جهة مجهولة الهوية بصورة متكررة وبدون موافقة الشخص المرسل إليه هذه الرسائل، وذلك لتحقيق أهداف متعددة يكون الغرض الغالب من إرسالها ذو طابع تجاري يهدف للترويج للسلع والخدمات وأحيانًا يكون الغرض منها غير تجاري كتحقيق أهداف سياسية أو نشر أفكار دينية أو الترويج لأي أمر آخر يقصده المرسل.

2- يتم إرسال الرسائل الإلكترونية غير المرغوب فيها وفقًا للوضع الغالب، عبر عناوين البريد الإلكتروني للأشخاص، والتي يتحصل عليها المتطفل أو المحتال عن طريق العديد من التقنيات الإلكترونية ذات الطابع غير المشروع، ومنها: التجميع عن طريق النظام المعروف باسم (القانوس المهاجم)، والتجميع عن طريق شراء قواعد البيانات، والتجميع عن طريق نظام الحصاد.

3- تتسم الرسائل الإلكترونية غير المرغوب فيها، بالعديد من الخصائص القانونية والتقنية التي تبرز ماهيتها ومضمونها وهي: أنها رسائل تُرسل عبر وسيلة إلكترونية، ورسائل لها طابع جبري لكونها تُرسل بدون موافقة الأشخاص، وهي رسائل لها طابع جماعي أو عشوائي لكونها تُرسل إلى المستخدمين أو المستهلكين بدون تحديد، كما أنها رسائل تتسم بطابع عدم مرغوبية المرسل إليهم هذه الرسالة فيها ويرجع ذلك لعوامل قانونية وعوامل تقنية وعوامل تتعلق بالثقة الإلكترونية، وأيضًا هي رسائل ذات أهداف متعددة تُرسل لأغراض تجارية أو سياسية أو دينية، وكذلك هي رسائل تنتمي إلى طائفة البرمجيات الخبيثة التي يكون الغرض منها تعطيل النظام وتخريب العمليات الخاصة به وتخريب البيانات والمعلومات المتواجدة على جهاز الحاسب أو الهاتف أو الشبكة.

4- تتحقق الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها عن طريق تطلب موافقة الأشخاص على إرسال أو استقبال هذه الرسائل. ونص على هذا الأمر كل من المشرع الأوربي والمشرع الفرنسي والمشرع الأمريكي والمشرع المصري، مع اختلاف نوع الموافقة في بعض التشريعات عن غيرها.

5- تتعدد صور تحقق الحماية القانونية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها: فهناك الحماية عن طريق تطلب الموافقة أو ما يُعرف بمبدأ التقيد والتي تحدث إما من خلال إرسال رسالة إلكترونية أو من خلال تخصيص قائمة على صفحة موقع المعلن أو من خلال الموافقة المسبقة المكررة أو المزدوجة. وتحقق هذه الحماية أيضًا من طريق مُكنة إلغاء الإشتراك أو نظام قائمة الرفض أو الاعتراض أو ما يُعرف بنظام الرفض اللاحق لهذه الرسائل.

6- بشأن موقف التشريعات المختلفة من مسألة الموافقة على إرسال أو استقبال رسائل

إلكترونية غير مرغوب فيها، نجد أن المشرع الأوربي قد أخذ في التوجيه الأوربي الصادر في 12 يوليو سنة 2002 الخاص بالتعامل في البيانات الشخصية وحرمة الحياة الخاصة بالموافقة المسبقة وذلك في المادة (13/1) من هذا التوجيه. وأخذ المشرع الفرنسي بذات الموافقة في المادة (L. 5-34)، من قانون الاتصالات البريدية والإلكترونية، وكذلك المشرع المصري في المادة (25) من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات. وعلى عكس هذه التشريعات، أخذ المشرع الأمريكي بنظام الرفض اللاحق وذلك في القانون الصادر في 16 ديسمبر لعام 2003 والمتعلق بمحاربة البريد التجاري الإعلاني غير المرغوب فيه.

7- يُقصد بالحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، مجموعة الإجراءات والتدابير ذات الطابع الفني والتكنولوجي، والتي يتم وضعها من قبل متخصصين في هذا الشأن، ويكون الغرض منها محاولة الحفاظ على البريد الإلكتروني للفرد بقدر المستطاع من الاختراقات والتهديدات التي يمكن أن تحيط بهذا البريد على وجه العموم وتجنب إرسال رسائل إلكترونية غير مرغوب فيها على وجه الخصوص.

8- تتعدد الطرق الفنية والتقنية لحماية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها. فهناك الحماية عن طريق خاصية تصفية الرسائل، والحماية عن طريق إنشاء مواقع إلكترونية تُنشأ خصيصًا لذلط، وأيضًا الحماية عن طريق إعمال خاصية التشفير.

9- تتم الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها عن طريق خاصية التصفية، من خلال طريقتي الفحص والترخيص، وعن طريق مجموعة من الوسائل كاستخدام مرشحات العناوين ومرشحات اللغة ورشحات المحتوى والمرشحات التي يحددها المستخدم.

10- تتم الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، عن طريق إنشاء المواقع الإلكترونية من خلال ما يُعرف بالقوائم السوداء والحماية من خلال برامج Spam Blockers.

11- تتم الحماية التقنية للأشخاص من الرسائل الإلكترونية غير المرغوب فيها من خلال خاصية التشفير عن طريق نوعين من التشفير هما: التشفير المتماثل والتشفير غير المتماثل. فالنوع الأول يُعرف باسم خوارزمية المفتاح السري، وهو أسلوب فردي لفك ترميز الرسالة ويجب إعطاؤه للمستلم قبل فك ترميز الرسالة، والمفتاح المستخدم للترميز هو نفسه المستخدم لفك الترميز. أما التشفير غير المتماثل فهو يتم باستخدام مفتاحين مختلفين، أحدهما عامًا والآخر خاصًا، يكونا على ارتباط مع بعضهما البعض من الناحية الحسابية. والمفتاحان هما في الأساس مجرد أرقام كبيرة تم ربطهما معًا لكنهما ليسا متماثلين، ومن هنا جاءت التسمية "غير متماثل". وهنا يمكن مشاركة المفتاح العام مع أي شخص، مع ملاحظة ضرورة إبقاء المفتاح الخاص سرًا. ويمكن استخدام المفتاحين لتشفير رسالة، ثم يُستخدم المفتاح المختلف عن المفتاح الذي استُخدم أصلاً في تشفير تلك الرسالة لفك ترميزها.

12- تتمثل الحماية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، في مجموعة من التوجيهات ذات الطابع العام، سواء على المستوى التقني أم على المستوى القانوني، الغرض منها مساندة وتأييد الحماية القانونية والتقنية الخاصة والتي ذكرناها في النتائج السابقة.

13- تتمثل الحماية التقنية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، من منظور العديد من الضوابط الفنية المتعلقة بعضها يتعلق بكلمة المرور الخاصة بالبريد الإلكتروني، وبعضها الآخر يتعلق بجهة الإرسال ذاتها، ومنها ما يتعلق بالرسالة ذاتها، ومنها ما يتعلق بعرض

عنوان البريد الإلكتروني ذاته.

14- تتمثل الحماية القانونية العامة للأشخاص من الرسائل الإلكترونية غير المرغوب فيها، في العديد من الضوابط القانونية العامة والتي يعد منها: التزام الشركات بالبنود التعاقدية، وسن التشريعات الدولية وإتباع إجراءات إنفاذ القانون، وضرورة إعمال توعية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها.

ثانيًا: توصيات الدراسة:

1- نوصي المشرع المصري بضرورة سن تشريع خاص لمواجهة ظاهرة الرسائل الإلكترونية غير المرغوب فيها، موضحًا ماهيتها وكيفية إرسالها، واضعًا الحلول المناسبة لها والجزاءات التي يلزم توقيعها على مرسل هذه الرسائل، وذلك على غرار ما فعله المشرع الأمريكي في القانون رقم 16 ديسمبر لعام 2003 والخاص بمحاربة البريد التجاري الإعلاني غير المرغوب فيه. وذلك من منطلق انتشار هذه الرسائل وما تمثله من تهديد لخصوصية الأشخاص الذين تُرسل إليهم هذه الرسائل.

2- نوصي بضرورة التزام شركات الدعايا والإعلان عن السلع والمنتجات والخدمات التي تُباع أو تُعرض عبر شبكة الإنترنت عن طريق المواقع الإلكترونية وصفحات التواصل المختلفة بالبنود التعاقدية التي يتم الاتفاق عليها بين الطرفين، والتي يكون من بينها التزام هذه الشركات بعدم إرسال رسائل إلكترونية غير مرغوب فيها إلى الأشخاص، ما لم يوافقوا على ذلك على النحو الذي بينّاه في موضعه.

3- نوصي بضرورة سن تشريعات دولية تضع حلوًا لمكافحة ظاهرة الرسائل الإلكترونية غير

المرغوب فيها؛ وذلك لأن التعاملالإلكتروني يتم من خلال وسيلة إلكترونية أصبح المستهلك من خلالها غير مقيد بأية حواجز زمانية أو مكانية تمكنه من الحصول على المنتج أو الخدمة من أي مكان في العالم وكذلك الأمر بالنسبة للمعلن عن هذه السلع والخدمات، لاسيما وأن إرسال هذه الرسائل يمكن أن يندرج تحت مضمون الجريمة الإلكترونية.

4- نوصي بضرورة إتباع إجراءات إنفاذ القانون على المستويين الداخلي والدولي؛ لأنه كلما كانت هذه الإجراءات الخاصة بظاهرة الرسائل الإلكترونية غير المرغوب فيها مطبقة، كلما انعكس ذلك على عدد الاختراقات لعناوين البريد الإلكتروني ومن ثم الرسائل التي تُرسل للأشخاص من خلاله.

5- نوصي الأشخاص بضرورة الالتزام بالحماية التقنية من الرسائل الإلكترونية غير المرغوب فيها عن طريق العديد من الوسائل الفنية، كاستخدام مرشحات تصفية الرسائل بمعاييرها المختلفة، واستخدام المواقع الإلكترونية التي تقاوم إرسال هذه الرسائل للأشخاص، وكذلك استخدام خاصية التشفير سواء المتماثل أو غير المتماثل.

6- نوصي الأشخاص بضرورة المحافظة على عناوين بريدهم الإلكتروني باعتباره الوسيط الإلكتروني الأكثر استقبالًا للرسائل الإلكترونية غير المرغوب فيها، وذلك عن طريق مجموعة من الأمور الفنية: كاختيار كلمة مرور قوية يصعب اختراقها، وضرورة تفقد جهة إرسال الرسالة، وفحص الرسالة ذاتها على النو الذي بينَّاه في موضعه، وعدم عرض عنوان البريد الإلكتروني للعامة بقدر الإمكان وجعله غير قابل للاكتشاف.

7- نوصي بضرورة توعية الأشخاص من الرسائل الإلكترونية غير المرغوب فيها وتبصيرهم بماهية هذه الرسائل وخطورتها وطرق الوقاية منها سواء من الناحية القانونية أو من الناحية التقنية.

يستوي في ذلك أن يتم هذا الدور التوعوي من خلال عقد ندوات تثقيفية تتم وجهًا لوجه أو عن بعد أو في صورة كتيبات توزع على الأشخاص.

8- نوصي الجهات المعنية المسؤولة عن إدارة المواقع والتطبيقات الإلكترونية المختلفة، بعدم إرسال أي رسائل أو إظهار أي إعلانات للأشخاص على المواقع التي يزورنها أو الفيديوهات التي يشاهدونها إلا بعد موافقتهم على ذلك، وعدم حرمانهم من ذلك بسبب رفضهم استقبال هذه الرسائل أو مشاعدة تلك الإعلانات.

قـائـمـــة الـــمـراجـــع

أولًا: المراجع العربية العامة:

- **د/ أحمد شوقي محمد عبد الرحمن:** البحوث القانونية في مصادر الالتزام الإرادية وغير الإرادية، دراسة فقهية وقضائية، منشأة المعارف، سنة 2002.

- **د/ أحمد عبد التواب محمد بهجت:** إبرام العقد الإلكتروني، دراسة مقارنة بين القانون المصري والفرنسي، دار النهضة العربية، سنة 2009.

- **د/ أسامة أبو الحسن مجاهد:** الوجيز في قانون الإثبات، دار النهضة العربية، سنة 2018.

- **د/ جلال على العدوي:** أصول الالتزامات، مصادر الالتزام، منشأة دار المعارف، سنة 1997.

- **د/ رمضان أبو السعود:** مصادر الالتزام، دار الجامعة الجديدة، الطبعة الثالثة، سنة 2003.

- **د/ رياض سامر:** دليلك المختصر للعمل كمسوق بالعمولة، Edward R، بدون سنة نشر.

- **د/ سمير عبد السيد تناغو:** مصادر الالتزام، العقد – الإرادة المنفردة – العمل غير المشروع – الإثراء بلا سبب – القانون، مصدران جديدان للالتزام (الحكم – القرار الإداري)، بدون ناشر، سنة

.2000 – 1999

– **د/ سهير سيد احمد منتصر، د/حمدي عبد الرحمن:** الوسيط في النظرية العامة للالتزامات، الكتاب الأول، العقد والإرادة المنفردة، بدون ناشر، سنة 2010.

– **د/ عبد الرزاق السنهوري:** الوجيز في النظرية العامة للالتزام، (المصادر – الإثبات – الآثار – الأوصاف – الانتقال – الانقضاء)، تنقيح المستشار/ أحمد مدحت المراغي، منشأة المعارف، سنة 2004.

– **د/ محسن عبد الحميد إبراهيم البيه:** النظرية العامة للالتزامات، مصادر الالتزام، الجزء الأول (المصادر الإرادية)، مكتبة الجلاء الجديدة، المنصورة، بدون سنة نشر.

ثانيًا: المراجع العربية المتخصصة:

– **د/ أحمد أسامة بدر:** الوسائط المتعددة بين الواقع والقانون، دار النهضة العربية، بدون سنة نشر.

– **د/ أحمد عبد التواب محمد بهجت:** الحماية القانونية للمستهلك الإلكتروني، دار النهضة العربية، سنة 2020.

– **د/ بسام فنوش الجنيد:** المسؤولية المدنية عن الإعلانات التجارية عبر الإنترنت، رسالة دكتوراة بكلية الحقوق جامعة عين شمس، سنة 1437 هـ – 2016 م.

– **د/ خالد بن سليمان العثبر؛ د/ سليمان بن عبد العزيز بن هيشة:** الاصطياد الإلكتروني، الأساليب والإجراءات المضادة، مركز التميز لأمن المعلومات، الطبعة الأولى، جامعة الملك سعود، الرياض، سنة 2009.

- **د/ خالد ممدوح إبراهيم:** أمن المستندات الإلكترونية، دار الجامعة الجديدة، سنة 2008.

- **د/ رائد محمد عبد ربه:** التسويق الإلكتروني، Al manhal، 2013.

- **د/ رياض سلطان علي:** نظم المعلومات الإدارية وتطبيقاتها في الصناعة، التنظيم والتكنولوجيا بين النظرية والتطبيق، Almanhal, 2006.

- **د/ سامح عبد الواحد التهامي:** المحرر الإلكتروني، بدون ناشر، سنة 2020.

- **د/ شريف محمد غنام:** التنظيم القانوني للإعلانات التجارية عبر شبكة الإنترنت.

- **د/ عبد الهادي فوزي العوضي:** الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، بدون سنة نشر.

- **د/ مأمون علي عبده قائد الشرعبي:** الحماية القانونية للمستهلك عبر الإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، سنة 2019.

- **د/ محمد بن إبراهيم السويل:** المدخل إلى علم التشفير، دار الخريجي، بدون سنة نشر.

- **د/ محمد سعد عيسى الزبون:** وسائل حماية المستهلك من إعلانات البريد الإلكتروني المزعجة، بحث منشور في المجلة القانونية.

- **د/ محمد مصطفى الشقيري:** السرية المعلوماتية، ضوابطها وأحكامها الشرعية، دار البشائر الإسلامية للطباعة والنشر والتوزيع، سنة 2008.

- **د/ نادية حجازي:** الوسائط المتعددة، دار أخبار اليوم، القاهرة، سنة 2017.

- **د/ نبيل محمد أحمد صبيح:** حماية المستهلك في التعاملات الإلكترونية، دراسة مقارنة، بحث منشور في مجلة الحقوق، العدد الثاني، السنة الثانية والثلاثون، جمادي الآخرة 1429 هـ – يونيو

2008م.

– **م/ بهاء المري:** شرح جرائم تقنية المعلومات، القانون رقم 175 لسنة 2018، منشأة المعارف، سنة 2019.

ثالثًا: المراجع الأجنبية:

- "Spam": An Overview of Issues Concerning Commercial Electronic Mail , June 18, 2003 – May 14, 2008 , Report Type: CRS Report , Source: EveryCRSReport.com, University of North Texas Libraries Government Documents Department .

- **Bernard Bouloc** : Collecte illicite de données nominatives , RTD com. 2006.925.

- **Dimitri Perret:** « 10 ans de spam : l'ère du phishing ciblé » [archive], Vade Secure, 21 novembre 2015 (consulté le 9 décembre 2019).

- **Dr. Bill Young** : Foundation of Computer Security , Lrcture 44: Symmetric vs Asymmetric Encryption.

- **Emmanuel Ghesquier:** « Gmail utilise l'IA pour lutter contre le spam » [archive], sur *Presse-Citron*, 8 février 2019 (consulté le 12 mars

– Essential Cyber Security Handbook In Arabic , Nam H Nguyen , 2018.

- **John Leyden** : "30 years of spam and we ain't finished yet " , the Register, 1er mai 2008.

- **M.Myard** : Répons ministérielle à question écrite n° 787 C J O A N Q ,

16 décembre 2002.

– **Monique LUBY** : Publicité commerciale Eur. – Réglementations generals, Janvier 2005 (actualisation : Juillet 2018).

- **Nathalie Dagorn**: « Sensibilisation aux coûts et conséquences du spam», Terminal, OpenEdition Journals, no 105 « Technologies et usages de l'anonymat sur Internet », 1er octobre 2010 (ISSN 0997-5551,DOI 10.4000/terminal.1897, lire en ligne , consulté le9 décembre 2019).

- **Schryen ، Guido** : Anti-Spam Measures , Analysis and Analysis and Design , provides a detailed over view of the technological , organizational and economic facets of spam- emails , Springer.

- **Timothy R. Fenoulhet** : La co-régulation : une piste pour la régulation de la société de l'information ? , RMCUE 2001. 598.

2019).

-JEFF TYSON : HOW ENCRYPTION WORKS.

رابعًا: المواقع والروابط الإلكترونية:

- https://gate.ahram.org.eg/News/1992424.aspx

- https://www.cnil.fr/fr/definition/commission-nationale-de-linformatique-et-des-libertes-cnil

- https://fr.wikipedia.org/wiki/Spam#Histoire

https://www.dalloz.fr/documentation/Document

- https://fr.wikipedia.org/wiki/Spam#Histoire

https://www.arageek.com/l/

- https://www.cisco.com/c/en/us/products/security/email-security/what-is-spam.html#~how-spam-works

- https://www.techopedia.com/definition/1716/spam

- https://www.spamlaws.com/spam-stats.html#google_vignette
- https://e3arabi.com
- https://www.everycrsreport.com/reports/RL31953.html#fn14
- https://www.dalloz.fr/documentation/Document
- https://www.everycrsreport.com
- https://www.pcworld.com/article/148780/spam.html
https://www.everycrsreport.com
- https://www.dalloz.fr/documentation/Document?id=(27-
- https://support.microsoft.com/ar-sa/topic/
- https://www.cnil.fr/fr/spam-phishing-arnaques-signaler-pour-agir
- https://me.kaspersky.com/resource-center/definitions/encryption
https://web.archive.org/web/20180325232131/http://www.computerweekly.com:80/feature/Encryption-key-management-is-vital-to-securing-enterprise-data-storage
- https://web.archive.org/web
- https://me.kaspersky.com/resource-center/definitions/encryption
https://computer.howstuffworks.com/encryption2.htm
https://me.kaspersky.com/resource-center/definitions/encryption
- http://www.hackingwithphp.com/17/3/3/asymmetric-vs-symmetric
- https://books.google.com.eg/books
- https://www.itpillars.com/ar/blog/
- https://ar.wikihow.com
- https://ar.wikihow.com
- https://support.microsoft.com/ar-sa/windows
- https://blog.hotmart.com
- https://ar.wikihow.com

- https://www.automationanywhere.com/ae/rpa/robotic-process-automation
- https://www.youm7.com/story
- https://me.kaspersky.com/resource-center/threats/spam-phishing
- https://support.microsoft.com/ar-sa/office
- https://www.vtiger.com/ar/blog/a-quick-guide-to-email-marketing/
- https://hrdoegypt.org/wp-content/uploads

الـــفـــهـــرس

الموضوع الصفحة