كلية الحقوق

قسم الدراسات العليا

بحث للنشر

الجرائم الواقعة على البريد الإلكتروني

(جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية

وجريمة اختراق البريد الإلكتروني)

تحت إشراف

أ.د . تامر محمد صالح

أستاذ القانون الجنائي

كلية الحقوق _ جامعة المنصورة

إعداد الباحث

عيسى عبد الله الحبسي

٢٠٢٠

جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية

وجريمة اختراق البريد الإلكتروني

مقدمة البحث

لقد صاحب التطور الذي شهده العالم في الحقبة الأخيرة من القرن الماضي ظهور تقنيات جديدة في شتى المجالات، وخاصةً فيما يتعلق بوسائل الاتصال التي جاءت مترافقة مع ظهور الشبكة الدولية للمعلومات (الإنترنت)، وشمل ذلك التطور كافة وسائل استخدامها وكافة النتائج الإيجابية أو السلبية الناشئة عن استخدام تلك الوسائل التي تعتبر أعجوبة القرن العشرين التي انتشرت بشكل مذهل في جميع أنحاء العالم، والإنترنت شأنه شأن أي اختراع جديد وبظهوره خلق ممارسات جديدة ومفاهيم وقيم سلوكية مستحدثة، بعضها مفيد والآخر ضار ناجم عن استخدام هذه التقنية التي فرضت نفسها بعضها علينا وتحولت إلى واقع نبحث عن الأسلوب الأمثل للتعامل معه، فأصبح أسلوباً للتعامل اليومي بين الأفراد[١].

ويعرف البريد الإلكتروني بأنه: "خط مفتوح في كل أرجاء العالم يتمكن الفرد بواسطته من إرسال واستقبال كل أنواع الرسائل"[٢]

وظهرت جرائم عديدة واقعة على البريد الإلكتروني ومن أبرزها جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية وجريمة اختراق البريد الإلكتروني، ومن منطلق بيان قواعد التجريم والعقاب على هذا النوع من الجرائم تبلورت فكرة البحث.

أولاً: مشكلة البحث.

لا شك في أن الواقع العملي أظهر لنا سلبيات الاختراعات العلمية باعتبار أن لها طبيعة خاصة متميزة ذات صفة فنية وخاصةً البريد الإلكتروني،

---

[١] د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٥، ص ٩.

[٢] Mr. Tariq Banday: Techniques and Tools for Forensic Investigation of E-mail, India, 2011, p. 4, www.semanticscholar.org.

وارتباطها بمفردات مصطلحات جديدة كالبرامج والبيانات والبريد الإلكتروني المرتبط بالإيميل، التي تشكل محلاً للاعتداء، أو تستخدم كوسيلة للاعتداء ، فمحل الجريمة موضوع البحث (جرائم البريد الإلكتروني) في الغالب هو تطبيق البريد الإلكتروني المصمم للعمل بواسطة إحدى وسائل تقنية المعلومات (الإيميل)، أو ضمن نظام معلوماتي معين، وتتميز تلك الوسائل العلمية بالحداثة والتطور المستمر، وذلك على خلاف القواعد القانونية التي تتسم بالثبات النسبي، الأمر الذي يثير إشكالية في مواجهتها والتصدي لها بواسطة التنظيم القانوني، ووضع الضوابط الكفيلة بمجاراة التطورات العلمية السريعة والمستجدة، تبع ذلك مشكلة التكييف القانوني للفعل، فضلاً عن مشكلة التمييز بين الفعل التحضري والبدء في تنفيذ الجريمة وغيرها.

وقد ثار تساؤل مهم حول مدى كفاية نصوص قانون العقوبات الاتحادي والقوانين الجنائية الخاصة (قانون مكافحة جرائم تقنية المعلومات الاتحادي وقانون مكافحة جرائم تقنية المعلومات في جمهورية مصر العربية)، في مواجهة جرائم إغراق البريد الإلكتروني بالرسائل الاقتحامية واختراق البريد الإلكتروني) وتتمحور مشكلة الدراسة حول التساؤل التالي: ما هو موقف المشرع الإماراتي والمشرع المصري في قواعد التجريم والعقاب في جرائم إغراق البريد الإلكتروني بالرسائل الاقتحامية واختراق البريد الإلكتروني؟

ثانياً: أهمية البحث.

١) **الأهمية النظرية:** تكمن أهمية البحث من الناحية النظرية في أنه يسلط الضوء على ماهية إغراق البريد الإلكتروني بالرسائل الاقتحامية، ويبين أيضاً ماهية تلك الرسائل، كما أنه يبين ماهية اختراق البريد الإلكتروني وصوره، ويبين أركان كل جريمة من هذه الجرائم والعقوبات المقررة لها في التشريع الإماراتي والتشريع المصري.
٢) **الأهمية العلمية:** تتمثل أهمية البحث من الناحية العملية في أنه يبين موقف المشرع الإماراتي والمشرع المصري من تجريم إغراق البريد الإلكتروني بالرسائل الإقتحامية.

ثالثاً: أهداف البحث.

يسعى البحث لتحقيق الأهداف التالية:

١) التعريف بماهية اختراق البريد الإلكتروني والتعريف بإفراق البريد الإلكتروني بالرسائل الاقتحامية.
٢) بيان أركان جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية.
٣) بيان أركان جريمة اختراق البريد الإلكتروني.
٤) تحديد عقوبة جريمة اختراق البريد الإلكتروني وعقوبة جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية في القانون الإماراتي والقانون المصري.

رابعاً: منهج البحث.

يعتمد البحث على المنهج الوصفي التحليلي، وذلك من خلال وصف الموضوع من خلال عرض الأدبيات وتحليل الآراء الفقهية والنصوص القانونية المتعلقة بموضوع البحث، كما يعتد أيضاً على المنهج المقارن من خلال المقارنة بين التشريعات الإماراتية والمصرية وبعض التشريعات الأجنبية.

خامساً: تقسيم البحث

الفصل الأول: جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية

- المبحث الأول: ماهية الإغراق البريدي بالرسائل الإقتحامية
- المبحث الثاني: أركان الجريمة وعقوبتها.

الفصل الثاني: جريمة اختراق البريد الإلكتروني.

- **المبحث الأول:** ماهية اختراق البريد الإلكتروني وأنواعه.
- **المبحث الثاني: أركان الجريمة وعقوبتها.**

الخاتمة

الفصل الأول

جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية

تمهيد وتقسيم:

إن شبكة الإنترنت من أكثر التقنيات الإلكترونية أهمية في زمن المعلوماتية، فهي وليدة انتشار نظم الحوسبة الآلية ونظم الاتصالات . وقد أحدثت شبكة الإنترنت قفزة نوعية في مجال نشر المعلومات الإلكترونية بكافة أنواعها بين الأفراد وفي جميع أرجاء العالم بواسطة طرق التواصل والتراسل المختلفة ومنها البريد الإلكترونية، الذي من خلاله يمكن إيصال أي رسالة لأي فرد، وفي أي مكان من العالم خلال ثوان. وعلى الرغم من كل الآثار الإيجابية للشبكة العالمية إلا أنها لم تخلو من السلبيات، وفي مقدمتها ظهور أنماط جديدة من الجرائم ألا وهي الجرائم الإلكترونية التي شكل بعضها انتهاكاً لحق الفرد في الخصوصية الشخصية، نتيجة التقدم الهائل في مجال اتصال المعلوماتية والذي كان له الأثر الكبير في تهديد وانتهاك حق الفرد في الخصوصية المعلوماتية[1].

وجريمة إغراق البريد الإلكترونية بالرسائل الإقتحامية والتي يراد بها إرسال الجاني نسخاً مكررة للرسالة ذاتها وبأعداد ضخمة لنظام البريد الإلكتروني العائد لأحد الأفراد، مما يسبب إيقاف أو تعطيل البريد الإلكتروني أو إتلاف محتوياته، علما أن هذه الرسائل الإقتحامية تمتاز بعدة خصائص منها أنها رسائل ذات طابع تجاري لتضمنها إعلانات في شتى المجالات، فضلاً عن ذلك فإنها ترسل بشكل عشوائي من خلال شبكة الإنترنت عن طريق استعمال برامج معينة تستطيع التعرف على شكل عناوين البريد الإلكتروني الموجودة في مواقع الإنترنت، ليتم بعد ذلك إرسال الرسائل الإقتحامية إلى هذه العناوين[٢]، علما إن النتيجة الجرمية التي يسعى الجاني

---

(1) أسامة الحسيني، الشبكة العنكبوتية العالمية -الإنترنت، مكتبة ابن سينا للنشر، بدون سنة نشر، ص ٨٣.

(٢) إمام حسانين عطا الله، حقوق الإنسان بين العالمية والخصوصية، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٤، ص ٧٥.

لتحقيقها من خلال إرسال هذا الكم الهائل من الرسائل الإقتحامية هي إيقاف البريد الإلكتروني عن أداء مهامه بشكل كلي أو جزئي أو تعطيله عن القيام بوظيفته لفترة مؤقتة من الزمن وأخيراً إتلاف محتوياته، لذا كان لابد من مواجهة هذه الجرائم المستحدثة من خلال إدراج نصوص تجرمها في ثنايا قوانين الجريمة الإلكترونية والتي للأسف لاحظنا في بعضها غياب هكذا نصوص على الرغم من وجود قانون الجريمة الإلكترونية. الكلمات المفتاحية: جريمة البريد الإلكتروني - الإغراق – الرسائل الإقتحامية - شبكة الإنترنت - الخصوصية المعلوماتية - نظم الاتصالات[1]

وسنبين في هذا الفصل ماهية الإغراق البريدي بالرسائل الإقتحامية وأركانها وعقوبتها من خلال مبحثين على النحو التالي:

- **المبحث الأول:** ماهية الإغراق البريدي بالرسائل الإقتحامية
- **المبحث الثاني:** أركان الجريمة وعقوبتها.

[1] بولين انطونيوز ايوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط١، بيروت، ٢٠٠٩، ص ٩٣.

المبحث الأول

ماهية الإغراق البريدي بالرسائل الإقتحامية

تعاني اليوم أغلب صناديق البريد الإلكترونية من مشاكل إغراقه بالرسائل الإقتحامية والتي أضحت من المشاكل المهمة في عالم التكنولوجيا الرقمية، نظراً لما تسببه هذه الرسائل من إزعاج وتهديد كبير لبنية الإنترنت وتطبيقاته ومنها البريد الإلكتروني، إذ يسبب هذا الإغراق البريدي حالة من عدم الاتزان في مجال التعامل التقني للبريد مما يؤدي إلى إيقافه عن تقديم الخدمة المناطة به[1] . واستناداً إلى ما تقدم ذكره سوف أتناول في هذا المبحث مفهوم الإغراق البريدي بالرسائل الإقتحامية في مطلبين، إذ أتناول في المطلب الأول تعريف الإغراق لغة واصطلاحاً، أما المطلب الثاني فأتناول فيه خصائص الرسائل الإقتحامية والأساس القانوني في تجريمها وذلك كالآتي:

- **المطلب الأول: تعريف جريمة الإغراق البريدي**
- **المطلب الثاني: خصائص الرسائل الإقتحامية والأساس القانوني في تجريمها**

(1) جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٥٦.

المطلب الأول

تعريف جريمة الإغراق البريدي

لبيان معنى الإغراق فإن ذلك يقتضي التعريف به من الناحية اللغوية والاصطلاحية وذلك ببيان أصل هذه الكلمة ومعناها في اللغة العربية، كما يستلزم توضيح معناها من الناحية الاصطلاحية وهذا ما سوف أتناوله على النحو التالي:

أولاً: تعريف الإغراق لغة

الإغراق: هو بمعنى أغرق في الشيء وجاوز الحد وبالغ[1]، وكذلك يأتي الرسوب في الماء ويقال رجل غرق وغريق وقد غرق غرقا وهو غارق والغرق كما ذكرنا هو الرسوب في الماء، أما الغريق فهو الميت فيه وقد أغرقه غيره وغرقه فهو مغرق وغريق[2]، والغرق في الأصل دخول الماء في منطقة الأنف حتى تمتلئ المنافذ فيهلك[٣]، وفي تعريف آخر جاء فعل غرق بمعي الغرق في الدين أو البلوي[٤].

ثانياً: تعريف إغراق البريد الإلكتروني اصطلاحاً

---

[1] إبراهيم مصطفى، أحمد حسن الزيات، حامد عبد القادر، محمد علي النجار، المعجم الوسيط ، ج ١، المكتبة الإسلامية، تركيا، بدون سنة طبع، ص ٦٥٠.

[2] جمال الدين محمد بن مكرم بن منظور: معجم لسان العرب، ج ١، دار إحياء التراث العربي، بيروت، ١٩٨٨ م، ص ٥٦.

[٣] محمد مرتضى الحسيني: تاج العروس، دار صادر، بيروت، بدون سنة طبع، ص ٨٢٣

[٤] إبراهيم مصطفى، أحمد حسن الزيات، حامد عبد القادر، محمد علي النجار، المعجم الوسيط، مصدر سابق، ص ٦٥٠.

عـرف جانـب مـن الفقـه البريـد الإلكترونـي بأنـه (طريقـة تسـمح بتبـادل الرسـائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات)[٥].

بينمـا عرفـه الـبعض بأنـه[١]" مكنـة التبـادل الإلكترونـي غيـر المتـزامن للرسـائل بـين أجهـزة الحاسـب الآلـي". كمـا عرفهـا الـبعض الآخربأنـه " تلـك المسـتندات التـي يـتم إرسـالها أو اسـتلامها بواسـطة نظـام اتصـالات بريـدي إلكترونـي وتتضـمن ملحوظـات مختصـرة ذات طـابع شـكلي حقيقـي، ويمكنـه استصـحاب مرفقـات بـه مثـل معالجـة الكلمـات وأيـة مسـتندات أخـرى يـتم إرسـالها برفقـة الرسالة ذاتها.

علـى صـعيد الاصـطلاح الفقهـي عـرف الإغـراق البريـدي بأنـه" :إرسـال نسـخ مكـررة لرسـالة معينـة وبأعـداد كبيـرة لنظـام البريـد الإلكترونـي العائـد إلـى أحـد الأشـخاص ممـا يترتـب عليـه إعاقـة عمـل النظـام التقنـي الإلكترونـي للبريـد وبالتالي إعاقة استعمال تلك الخدمة أو توقفها"[٢].

فـي تعريـف آخـر عـرف بأنـه:" إرسـال المجـرم عشـرات الرسـائل دفعـة واحـدة لنظـام البريـد الإلكترونـي عبـر شـبكة الإنترنـت مـن خـلال اسـتعمال بـرامج تـتمكن مـن التعـرف علـى عنـاوين البريـد الإلكترونـي الموجـودة فـي مختلـف المواقـع ومـن ثم إرسالها للأفراد، هذا وفي الغالب يكون محتوى هذه الرسائل إعلانات"[٣].

---

[٥] ou ils definissent ie courier electroniquecomme une faculte d"echange asynchrone des messages entre ordinatenrs . p commerce electronigue vuibert ,2000 ,p77.

[١]"method pernettant d'echanger des messages ecrits entre differents postes d'un reseau informatique".
-F. colantonio, la protection du secret des couriers electroniques en belgique: Aspect techniques, des criminology, 2002, p.9.
مشار إليه لدى د. عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية ، ٢٠٠٥، ص١٣.

[٢] د. محمـد محمـود المكـاوي: الجوانـب الأخلاقيـة والاجتماعيـة والمهنيـة للحمايـة مـن الجـرائم المعلوماتية، المكتبة العصرية للنشر والتوزيع، مصر، ٢٠١٠، ص ١٣٢

[٣] د. خالـد ممـدوح إبـراهيم: حجيـة البريـد الإلكترونـي فـي الإثبـات، دار الفكـر الجـامعي، الإسكندرية، ٢٠٠٨ م، ص ١٤٠.

من جهة أخرى، فتعد رسائل البريد الإلكتروني[٤] غير المرغوب فيها والبرمجيات الخبيثة التهديدات الأكثر انتشاراً في دولة الإمارات، وتحتوي رسالة واحدة من أصل ١٩٩ رسالة بريد إلكتروني على برمجيات خبيثة، في حين أن أكثر من النصف ٥٥,٢% من عدد رسائل البريد الإلكتروني هي رسائل غير مرغوب فيها، وكان لدولة الإمارات في عام ٢٠١٥ م مقارنة مع عام ٢٠١٤ م حصة كبيرة جداً من المعدل العالمي للرسائل غير المرغوب فيها حيث حلت في المرتبة الـ ٣١ عالمياً بعدما كانت قد حلت في المرتبة ٥١ عام ٢٠١٤، ويرجع ذلك إلى مجموعة من العوامل الاجتماعية والاقتصادية، بما في ذلك معدل اختراق الهواتف الذكية العالمي ونسبة الاتصال السريعة بالإنترنت في البلاد لا سيما وأنه يمكن السيطرة واستغلال وسيلتي التواصل هاتين بسهولة من قبل مجرمي الإنترنت[١].

كما بينت اللجنة الوطنية للمعلوماتية والحريات في فرنسا CNIL مفهوم البريد الدعائي المزعج Spam بقولها: "ممارسة إرسال الرسائل غير المرغوب فيها – وهي في معظم الأحيان ذات طبيعة تجارية – وبأعداد كبيرة، وبشكل متكرر للأفراد الذين ليس لهم اتصال سابق مع المرسل، وتم الحصول على عنوان البريد الإلكتروني من الفضاء العام لشبكة الإنترنت، مثل المجموعات الإخبارية، أو القوائم البريدية، أو قائمة مواقع الويب"[٢].

كما عرف المشرع في ولاية Arizona الأمريكية البريد الإلكتروني التجاري غير المرغوب فيه بأنه: بريد إلكتروني تجاري أرسل دون موافقة

---

[٤] البريد الإلكتروني E-mail هو الخدمة التي يتم استخدامها لإرسال البريد الإلكتروني عبر الإنترنت، وثمة العديد من المواقع التي تتيح إنشاء بريد إلكتروني من خلالها، أشهرها الياهو والهوتميل، انظر: أيمن النسور ومحمد الجنيني وأنس أبو طالب، الحاسوب والبرمجيات الجاهزة، (عمان: دار وائل، ٢٠١٣ م) ط ٣، ص ٥٠٩.

[١] عبد الرحمن إسماعيل، الإمارات الأولى إقليمياً في التعرض للهجمات الإلكترونية، منشور في صحيفة الاتحاد بتاريخ: ٢٠١٦/٤/١٨ م، في موقع الصحيفة:
http://www.alittihad.ae/details.php?id=15417&y=2016&article=full

تاريخ الاستفادة من الموقع: ٢٠٢٠/٨/١ م.

[٢] Report on Electronic Mailing and data protection , commission Nationale Informatique et libertes (CNIL) france, sdopted on October 14.1999 (the CNIL report)

المتلقي (المستلم) من قبل شخص لا تربطه علاقة معينة بالمتلقي (المستلم). ويقصد بالبريد الدعائي المزعج أو (Spam) كذلك إغراق صندوق البريد الإلكتروني بعدة نسخ من رسالة واحدة في محاولة لفرض الرسالة على الناس الذين لا يرغبون في استلامها أو هو: "إرسال الرسائل غير المرغوب فيها لأعداد كبيرة من الناس فمصطلح الـ (Spam) يشير إذاً إلى تقديم رسالة معينة إلى مجموعة كبيرة من الأفراد، في محاولة لإجبارهم على الاطلاع على الرسالة التي سيختارون عدم تلقيها: فالبريد الإلكتروني المزعج أو غير المرغوب فيه هو البريد الذي لا يحقق أي فائدة للمستلم من وجهة نظر هذا الأخير[١].

وتعتبر مشكلة البريد الإلكتروني الدعائي من أخطر المشاكل التي تتعرض لها خدمة البريد الإلكتروني وهي مشكلة متنامية باستمرار، ففي دراسة أجريت ثبت أن البريد الدعائي Spam يشكل ٩٠% من حركة البريد الإلكتروني[٢] بل أنه من أهم المشكلات الرئيسية للإنترنت[٣].

ثالثاً: ماهيّة الرسائل الاقتحامية

هي الرسائل المرسلة بشكل عشوائي إلى كثير من الناس دون أخذ موافقتهم على استقبالها، وأكثر أنزاع الرسائل الإلكترونية الاقتحامية هي دعائيّة، فمعظم المرسلين للسبام يستهدفون سلع وخدمات معينة لترويجها، فبعض السلع اختيرت لأن مستخدمي الكومبيوتر قد يهتمون بها، لكن معظم هذه السلع تكوم من السوق السوداء (مثل أدوية طبية غير مصرح بها)[٤].

---

[١] John Magee: The law Regulating unsolicited commercial E-mail; An international perspective , computer& high technology law journal, vol.19, 2003. p.335

[٢] George H.pike: Anti-spam legislation setbacks. Information today, vol 25, December 2008, 17,no 11.

[٣] Leslie Basse, L'action de la CNIL en matière de lutte contre le Spam, mai 2005, no,53,p.1

[٤] حمد نصير، الوسيط في الجرائم المعلوماتية، (الجيزة: مركز الدراسات العربية، ٢٠١٥)، ط ١، ص ٥٤. محمد خليفة، الحماية الجنائيّة لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، (الإسكندرية: دار الجامعة الجديدة، ٢٠٠٧)، ط ١، ص ٥٧.

إضافة إلى ما سبق، فبعض رسائل السبام تكون احتيالية؛ مثل الرسائل التي يدعي صاحبها بأن المستلم يستطيع الحصول على حصة من أموال لم يتمكن المرسل من الحصول عليها بنفسه لأسباب قضائية مقابل مساعدة المستلم في تشريع هذه الأموال، ويطلب من المستلم تقديم تفاصيل بحسابه المصرفي، وبطبيعة الحال إذا قدم المستلم هذه التفاصيل سوف يتم سرقة حسابه الخاص، وبعضها قد تكون إباحية حيث تتضمن عروضاً لمنتجات لزيادة أو تعزيز القدرة الجنسية، أو وصلات لمواقع إباحية، أو إعلانات لإنتاج المواد الإباحية وما إلى ذلك، وبضعها قد تكون صحية، وتشمل هذه الفئة إعلانات لفقدان الوزن، والعناية بالبشرة، وعلاج الصلع، والمكملات الغذائية والأدوية التي قد تكون غير مصرح بها وما إلى ذلك مما يمكن شراؤه عن طريق الإنترنت، وقد تكون هذه الرسائل تقنية فتتضمن بعض العروض لأجهزة وبرمجيات بأسعار مخفضة، فضلاً عن الخدمات لأصحاب المواقع على شبكة الإنترنت مثل استضافة المواقع، وتسجيل النطاق، وتحسين المواقع، وقد تكون عبارة عن خدمات مالية يشمل هذا النوع عروض التأمين، والخدمات لتخفيض الديون، والقروض مع انخفاض أسعار الفائدة وما إلى ذلك، ويمكن أن تتضمن خدمات التعليم والتدريب وتشمل هذه الفئة عروض لعقد حلقات دراسية، والتدريب، والحصول على شهادات دراسية عن طريق الإنترنت وقد تكون هذه الشهادات مزيفة[١].

ويقصد بالبريد الدعائي المزعج أو (SPAM) إرسال رسائل إلكترونية غير مطلوبة، وبأعداد كبيرة لأهداف تجارية[٢] في محاولة لفرض الرسالة على الناس الذين لا يرغبون في استلامها[٣].

---

[١] عبد الله ناصر العمري، الحماية الجنائيّة للبريد الإلكتروني – دراسة تأصيلية مقارنة، (رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية، ٢٠١٠)، ص ٢٦-٢٧.

[٢] د. بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، ٢٠٠٩ م، ص ١٩١.

Eric Goldman: where's the Beef? Dissecting spam's purported Harms, 11 january 2004, p.3,

[٣] Dider colin:spamfiletering;optimization Appoaches to content – based filtering , thése de doctorat ,université de Versailles-saint-quentinen-yvelines, 2009,p.81 kevinGallot: Anti-spam. Paris, 2004,p,25.

المطلب الثاني

خصائص الرسائل الإقتحامية والأساس القانوني في تجريمها

سأقسم هذا المطلب إلى فرعين أذ أنتناول في الفرع الأول خصائص الرسائل الاقتحامية أما الفرع الثاني فأتناول فيه الأساس القانوني في تجريم الرسائل الاقتحامية وكالاتي:

الفرع الأول

الخصائص

إن الرسائل الإقتحامية المرسلة عبر الإنترنت لخدمة البريد الإلكتروني تمتاز بمجموعة من الخصائص وهي كالآتي:

أولاً: ذات طابع تجاري:- أن الرسائل الاقتحامية في الغالب تتضمن إعلاناً عن منتوج أو خدمة معينة أو إعلاناً لمقابلة شخص مثل شخص يريد مقابلتك والتعرف عليك يمكن الاتصال على الرقم كذا للدردشة معه والتعرف عليه وعلى أصدقاء جدد، بالإضافة إلى إعلانات المواقع الإباحية وكذلك قد تتضمن هذه الرسائل إعلانات لمشاريع وهمية كاذبة[1].

[1]د. خالد ممدوح إبراهيم: حجية البريد الإلكتروني في الإثبات، مصدر سابق، ص ١٣٤.

ثانيـــاً: ترســـل مـــن دون موافقـــة مالـــك البريـــد:- فضـــلاً عـــن أنهـــا ترســـل بأعـــداد كبيـــرة وبشـــكل عشـــوائي مـــن خـــلال الإنترنـــت عـــن طريـــق إســـتخدام بـــرامج معينـــة تـــتمكن مـــن التعـــرف علـــى شـــكل العنـــوان البريـــدي الموجـــود فـــي مواقـــع الإنترنـــت علـــى اخـــتلاف أنواعهـــا ســـواء كانـــت مواقـــع تعليميـــة أو ترفيهيـــة أو تجاريـــة وغيرهـــا وبعـــد ذلـــك يـــتم إرســـال هـــذه الرســـائل الإقتحاميـــة إلـــى العنـــاوين التـــي تـــم التعـــرف عليهـــا، علمـــاً انـــه فـــي الآونـــة الأخيـــرة إزدادت نســـبة هـــذه الرســـائل بشـــكل مرتفـــع جـــدا ممـــا اضـــطر كـــل مـــن مقـــدم خدمـــة الإنترنـــت والمســـتخدم علـــى تحمـــل تكـــاليف ماليـــة جديـــدة لمواجهـــة هـــذه المشـــكلة[٢]. يـــتم الحصـــول علـــى عنـــوان البريـــد الإلكترونـــي للمســـتخدم User بإحـــدى وســـيلتين، الأولـــى المـــنح والثانيـــة الاختيـــار[١] ويكمـــن الفـــارق بينهمـــا فـــي مـــدى الحريـــة التـــي يتمتـــع بهـــا مســـتخدم الإنترنت في تكوين عنوانه البريدي الخاص به.

١) **ثالثـــاً: رســـائل مهـــدرة لوقـــت المســـتخدم ومزعجـــة:** أذ أضـــحى اليـــوم البريـــد الإلكترونـــي لأغلـــب الإفـــراد مملـــوءة بعشـــرات الرســـائل الإقتحاميـــة، والتـــي ترســـل مـــن جهـــات غيـــر معروفـــة، ممـــا يجعـــل الأفـــراد أمـــام مشـــكلة قضـــاء ســـاعات طويلـــة أمـــام البريـــد الإلكترونـــي لأجـــل حـــذف هـــذه الرســـائل مـــن القـــوائم البريديـــة فـــي حـــين لجـــأ الـــبعض الآخـــر إلـــى إنشـــاء بريـــد إلكترونـــي جديـــد للهـــروب مـــن هـــذه المشـــكلة التـــي تشـــكل انتهاكـــاً صـــريحاً وواضـــحاً لحـــق الفـــرد في الخصوصية الشخصية[2].

الفرع الثاني

الأساس القانوني في تجريم الرسائل الإقتحامية

أولاً: **الحكم الفقهي لإغراق البريد الإلكتروني بالرسائل الاقتحامية**

بدايـــة يعـــرّج الباحـــث – باختصـــار – حـــول تكييـــف ملكيـــة البريـــد الإلكترونـــي؛ إذ أن هـــذا التكييـــف يبنـــى عليـــه التكييـــف الفقهـــي للجريمـــة، فبعـــد بحـــث ونظـــر؛ خـــرج

---

[٢] هيئـــة الإتصـــالات وتقنيـــة المعلومـــات الســـعودية: تطـــوير الهيكليـــة التنظيميـــة لمكافحـــة الرســـائل الإقتحامية (SPAM). ينظر موقع: www. citci . gov . sa، 2007، ص ١٠.

[1]Manara (C.), Aspects Juridiques de L'e-mail, Dalloz Affaires, no 140, 1999, p.278.

[2] د. خالد ممدوح إبراهيم: حجية البريد الإلكتروني في الإثبات، مصدر سابق، ص ١٣٤.

الباحث بأن الشركات الإلكترونية التي تمنح البريد الإلكتروني للمستخدمين؛ تمنحه على وجهين؛ الأول: قيام المستخدم بتوقيع عقد اشتراك بينه وبين الشركة أو المزوّد للخدمة؛ بحيث يصبح للمشترك حساب للبريد الإلكتروني حسب المساحة المطلوبة التي يرغب بها المشترك بناءً على اشتراكه. والثاني قيام بعض الشركات مثل: ياهو وهوتميل، بفتح الباب في موقعها بالحصول المجاني على البريد الإلكتروني لم يريد من المستخدمين بعد قيام المستخدم بتعبئة الطلب[٣].

عرفت المادة الاولى من قانون مكافحة جرائم تقنية المعلومات في جمهورية مصر العربية رقم (١٧٥) لسنة ٢٠١٨ -مقدم الخدمة : أى شخص طبيعى أو اعتبارى يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أومن ينوب عنه فى أى من تلك الخدمات أو تقنية المعلومات.

إذن فالباحث أمام صورتين؛ مزود هذه الخدمة، يقوم بتأمين هذه الخدمة مقابل رسوم معينة، والمزود للخدمة ملتزم بتأمين هذه الخدمة للمشتركين وتأمينها ويضمنها لهم؛ لأن مقدم الخدمة ملتزم للخدمات الإلكترونية للبريد وضامن لها، فهو بذلك أجير مشترك، فضلاً عن كون العقد بين مزود الخدمة والمشتركين معلوم الابتداء ومعلوم الانتهاء[1].

بناءً على ما سبق؛ فالتكييف الفقهي للصورة الأولى عقد إجارة، فالمشترك يستفيد من المنفعة التي تقدمها الشركة بناءً على عقد لمدة معلومة ونفع معلوم وهو المساحة الإلكترونية التي تمنحها الشركة للمشترك ومبلغ معلوم من المال يدفعه المشترك، فهي بهذه الوصف إجارة على منفعة، والإجارة – كما هو معروف فقهاً – تقع على المنافع[2]، والحال ذاته بالنسبة للقانون الإماراتي فالإجارة أو الإيجار تمليك المؤجر للمستأجر منفعة مقصودة من الشيء

---

[٣] د. خالد ممدوح إبراهيم: حجية البريد الإلكتروني في الإثبات، مصدر سابق، ص ١٤٠.

[1] انظر: العمري، الحماية الجنائية للبريد الإلكتروني، ص ١٣٧.

[2] عرّف النووي الإجارة بأنها: العوض عن بدل المنافع، وعرّفها المواق بأنها بيع منفعة. يحيى بن شرف النووي، تحرير ألفاظ التنبيه، تحقيق: عبد الغني الدقر، (دمشق: دار القلم، ١٤٠٨ ه)، ط ١، ص ٩١٢ محمد بن يوسف المواق، التاج والإكليل لمختصر خليل، ط ١، (بيروت: دار الكتب العلمية، ١٩٩٤ م)، ط ١، ج ٧، ص ٤٩٣.

المؤجر لمدة معينة لقاء أجر معلوم[3]، وتجدر الإشارة إلى أن طبيعة هذه المنفعة لا بد أن تكون مشروعة فلا تخالف أحكام الشريعة الإسلامية. ولا يخفى على الدارس أن الإجارة جائزة عند جميع الفقهاء[4]، ويستدل لمشروعية الإجارة بقوله سبحانه وتعالى: ((قَالَتْ إِحْدَاهُمَا يَا أَبَتِ اسْتَأْجِرْهُ ۖ إِنَّ خَيْرَ مَنِ اسْتَأْجَرْتَ الْقَوِيُّ الْأَمِينُ))[5]

ثالثاً: الحكم القانوني لإغراق البريد الإلكتروني بالرسائل الاقتحامية

بدايةً مما تميز به المرسوم الاتحادي الإماراتي رقم: ٥ لسنة ٢٠١٢ م بشأن مكافحة جرائم تقنية المعلومات أنه أفرد مسألة إغراق البريد الإلكتروني بالرسائل الاقتحامية بفقرة خاصة إذ نصت الفقرة الثالثة من المادة العاشرة من المرسوم على أنه: ((تكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته))، فمن خلال النص السابق نجد أن المشرع أكد على تجريم الاعتداء على البريد الإلكتروني الذي يحدث من خلال إغراقه بالرسائل الاقتحامية مما يؤدي إلى إيقافه أو تعطيله أو إتلاف محتوياته، وهذا التجريم يؤكد على حرص المشرع الإماراتي في حماية البريد الإلكتروني من الاعتداء عليه، ولعل علة التجريم تكمن في كون ما للبريد الإلكتروني من العديد من الفوائد للإفراد والمجتمعات؛ لذا يجب الحرص عليه وعلى أداء وظائفه على نحو أفضل وحمايته مما بشأنه الإضرار به[1].

إن للتقدم الهائل في مجال الحاسوب وتكنولوجيا المعلومات والثورة العلمية والعالمية في عالم الإنترنت الأثر الكبير في انتهاك وتهديد حق الأفراد في

---

[3] مادة رقم: ٧٤٢ من قانون المعاملات المدنية الإماراتي.

[4] محمد بن أحمد بن رشد، بداية المجتهد ونهاية المقتصد، (القاهرة: دار الحديث، ٢٠٠٤)، ط ١، ج ٤، ص ٥.

[5] سورة القصص، آية ٢٦.

[1] عبد الرزاق عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة، (دبي: المعهد القضائي، ٢٠١٤)، ط ١، ص ١٠٥.

الخصوصية المعلوماتية، إذ أصبح من السهل اختراق هذه الحياة من حيث الإضافة أو النقل أو التعديل لأي معلومة إلكترونية في أقل من ثانية فلم يعد بعد المسافة أو غلق النوافذ عائقا أمام مراقبة الآخرين والإطلاع على أسرارهم الخاصة[٢].

تنص المادة (٣٥) من القانون رقم (١٧٥) لعام ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات في جمهورية مصر العربية على أنه": يعاقب بالحبس مدة لا تقل عن ٣ أشهر وبغرامة لا تقل عن ٣٠ ألف جنية ولا تزيد عن ١٠٠ ألف جنية أو بإحدى هاتين العقوبتين، كل مسئول عن الإدارة الفعلية لأى شخص اعتبارى، إذا تعرض الموقع أو الحساب الخاص أو البريد الإليكترونى أو النظام المعلوماتى المخصص للكيان الذى يديره، لأى جريمة من الجرائم المنصوص عليها فى هذا القانون، ولم يبلغ بذلك الجهات المختصة وقت علمه بالجريمة".

وبالنسبة إلى القانون الدولي فنجد مثلا أن الإعلان العالمي لحقوق الإنسان قد كفل حق الفرد في الخصوصية الشخصية حيث جاء في المادة (١٢) منه "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"[1] وكذلك قد كفلت الاتفاقية الدولية الخاصة بالحقوق المدنية و السياسية ذات الحق في المادة (١٧)[2].

وبذلك يكون القانون الدستوري والقانون الدولي الأساس القانوني الذي تستند عليه التشريعات ومنها الجنائية لتجريم أي انتهاك لحقوق الأفراد وحرياتهم والمتمثلة هنا تحديداً في محل البحث تجريم إغراق البريد الإلكتروني بالرسائل الإقتحامية لكونه يشكل انتهاكاً لحق الفرد في الخصوصية الشخصية.

---

(٢) د. حسام الدين كامل: الحق في إحترام الحياة الخاصة، دار النهضة العربية، القاهرة، بدون سنة طبع، ص ٥.

(1) د. السيد أبو الخير، نصوص المواثيق والإعلانات والاتفاقيات لحقوق الإنسان ، دار إيتراك للطباعة والنشر، القاهرة ، ٢٠٠٥ م، ص ٦٨

(2) المرجع نفسه، ص ١٠٠.

المبحث الثاني

أركان الجريمة وعقوبتها

لقد كان للتقدم التكنولوجي الذي شهده العالم اليوم وتحديداً في مجال الإتصالات عن طريق إستخدام شبكة الإنترنت الدور الكبير في ظهور أشكال جديدة من الجرائم الإلكترونية ومنها جريمة إغراق البريد الإلكتروني بالرسائل الإقتحامية والتي أثارت العديد من الإشكالات اتجاه القائمين على مكافحتها نظراً للخسائر المالية التي تلحقها هذه الجريمة بشركات خدمة الإنترنت من جهة ومن جهة أخرى بمستخدمي تطبيق البريد الإلكتروني من حيث الإزعاج وانتهاك حق الفرد في الخصوصية المعلوماتية.

في حين جرم فعل الإغراق البريدي كل من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢ والذي نص في المادة (١٠) "تكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي

يقصد به إغراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته "وكذلك قانون المعلومات الفرنسي[1].

واستناداً إلى ما تقدم ذكره سوف أقسم هذا المبحث إلى مطلبين وكالآتي:

- **المطلب الأول:** الركن المادي
- **المطلب الثاني:** الركن المعنوي للجريمة

المطلب الأول

الركن المادي

سوف أتناول في هذا المطلب دراسة الركن المادي لجريمة إغراق البريد الإلكتروني بالرسائل الإقتحامية وذلك في ثلاثة فروع أذ أتناول في الفرع الأول فعل الإغراق أما الفرع الثاني فأتناول فيه النتيجة الجرمية أما فيما يخص الفرع الثالث فسأتناول فيه العلاقة السببية وكالآتي:[1]

الفرع الأول

فعل الإغراق

[1] ينظر قانون المعلومات الفرنسي المادة (٢/٣٢٣) .

[1] د. السيد أبو الخير، نصوص المواثيق والإعلانات والاتفاقيات لحقوق الإنسان ، مرجع سابق، ص ٨٠.

الـــركن المـــادي فـــي الجريمـــة قوامـــه عناصـــر ثلاثـــة؛ هـــي الســـلوك الإجرامـــي ونتيجتـــه والرابطـــة الســـببية بينهمـــا، والســـلوك الإجرامـــي يتكـــون مـــن شـــقين؛ الأول نشـــاط إرادي، والثـــاني: محـــل ينصـــب عليـــه هـــذا النشـــاط، أمـــا الســـلوك الإجرامـــي فهـــو فعـــل معـــين تطلبـــه القـــانون مناطـــاً للعقـــاب علـــى هـــذه الجريمـــة علـــى أن تتحقـــق نتيجـــة ضـــارة لهـــذا الســـلوك الإجرامـــي كشـــرط بذاتـــه يتعـــين قيامـــه العقـــاب علـــى الجريمـــة، إضـــافة إلـــى الارتبـــاط بـــين النشـــاط أو الســـلوك الإجرامـــي ونتيجتـــه الضـــارة بعلاقـــة ســـببية، ولا يمكـــن العقـــاب علـــى ســـلوك معـــين مـــا لـــم يكـــن مجرمـــاً قانونـــاً، فالجريمـــة لا توجـــد إلا بـــنص تشـــريعي يجـــرم الفعـــل الإجرامـــي ويضـــع عقوبـــة عليـــه، ومـــؤدى ذلـــك أن يحـــدد قـــانون العقوبـــات مقـــدماً الأفعـــال التـــي يعـــدها جـــرائم معلوماتيـــة والعقوبـــات المقـــررة علـــى مقترفيهـــا، والجريمـــة المعلوماتيـــة لا تختلـــف عـــن الجـــرائم العاديـــة فـــي اشـــتراط وجـــود ســـلوك إجرامـــي يجرمـــه القـــانون، ويمكـــن تعريـــف الســـلوك الإجرامـــي فـــي الجريمـــة المعلوماتيـــة بأنـــه كـــل فعـــل أو امتنـــاع عـــن فعـــل يـــؤدي إلـــى الإضـــرار بمعلومـــات مخزنـــة علـــى إحـــدى الحواســـيب الآليـــة والتـــي تـــؤدي إلـــى هـــدر أو إنقـــاص قيمـــة المعلومـــات وتســـبب ضـــرراً للآخـــرين، فالســـلوك الإجرامـــي فـــي هـــذه الجـــرائم لا بـــد أن يـــتم مـــن خـــلال أجهـــزة الحاسب الآلي أو شبكة الإنترنت[1].

وهـــو مـــا تجلـــى فـــي بعـــض أحكـــام القضـــاء الفرنســـي خاصـــة فـــي قضـــية Claire L والتـــي قضـــي فيهـــا بـــأن « المضـــيف يختلـــف عـــن الناشـــر أو محـــرر الموقـــع فـــالأول تقتصـــر وظيفتـــه علـــى خدمـــة النقـــل إلـــى الجمهـــور عـــن طريـــق الوســـائل الإلكترونيـــة، أمـــا الثـــاني فتكـــون لـــه ســـلطة الســـيطرة التحريريـــة علـــى مـــا يـــتم نشره[٢].

أمـــا محـــل الجريمـــة فـــلا ينفصـــل عـــن النشـــاط الإجرامـــي فيهـــا الأمـــر الـــذي يجعـــل محـــل الجريمـــة عنصـــراً مـــن عناصـــر الـــركن المـــادي، فالمحـــل القـــانوني للجريمـــة هـــو المصـــلحة التـــي تحميهـــا القاعـــدة القانونيـــة، وهـــذا المحـــل لا يتحقـــق إلا إذا

---

[1] عبـــد اللـــه كريـــري، الـــركن المعنـــوي فـــي الجـــرائم المعلوماتيـــة فـــي النظـــام الســـعودي – دراســـة تأصـــيلية، (رســـالة ماجســـتير، الريـــاض: جامعـــة نـــايف العربيـــة للعلـــوم الأمنيـــة، ٢٠١٣)، ص ٤٠-٤١.

[٢]Feral-Schuhl, CH. (2002). Cyber droit, le droit à l'épreuve de l'internet (3eed) Dunod: paris, p129.

توافرت شروط قد ينص عليها المشرع صراحة أو يشير إليها ضمناً، وهذه الشروط ما هي إلا الشروط المفترضة للجريمة، فإذا كان المحل القانوني في جريمة القتل هو حق الحياة، فإن هذا الحق يفترض وجود إنسان على قيد الحياة قبل مباشرة الفاعل لسلوكه، فيكون بمثابة الشرط المفترض لجريمة القتل[٣].

بالنسبة للنتيجة الإجرامية: فلها مدلولان؛ الأول المادي: وهو الآثار المادية التي تحدثها الجريمة في العالم الخارجي ويرتب القانون على حصولها عقوبة، والثاني: قانوني: وهي المصلحة المحمية بموجب القانون، وما إذا كانت تضررت أم لا، فإن تحقق المساس بهذه المصلحة؛ فقد وقعت النتيجة الإجرامية في صورتها القانونية، فتخريب المعلومات أو السلطة عليها أو إعاقة الوصول إليها أو غيرها من صور الجرائم الإلكترونية التي لا تستهدف المعلومات بذاتها بل تستهدفها لما لقيمتها لدى بعض الأطراف؛ لذا فالمجرم المعلوماتي يسعى للإضرار بمصلحة معينة عن طريق تلك المعلومات. ولكي يتوافر الركن المادي في الجريمة فلا بد من وجود علاقة سببية ما بين السلوك الإجرامي والنتيجة الإجرامية التي تحققت بناء على هذا السلوك، وعلاقة السببية هي العنصر الثالث في الركن المادي للجريمة، ويراد بها الصلة التي تربط بين السلوك الإجرامي والنتيجة الإجرامية الضارة كرابطة العلة بالمعلول، بحيث تثبت ان السلوك الإجرامي الواقع هو الذي أدى إلى حدوث النتيجة الضارة، وللسببية أهميتها الكبيرة فمن دونها لا يقوم الركن المادي، فلو ثبت انتفاء علاقة السببية بين السلوك والجريمة، فمرتكب السلوك لا يسأل إلا عن شروعه في الجريمة إذا كانت عمدية مقصودة، أما إذا كانت غير عمدية، فلا يسأل لأنه لا شروع في الجرائم غير العمدية.[1]

أما بالنسبة لقانون العقوبات الإماراتي لم يحدد عناصر الركن المادي تحديداً كاملاً، بل اقتصر على ذكر أحد عناصره وهو الفعل، فقد نصت المادة رقم: ٣١ منه على أنه: ((يتكون الركن المادي للجريمة من نشاط إجرامي بارتكاب

---

[٣] مجيد خضر السبعاوي، نظرية الغلط في قانون العقوبات المقارن، (القاهرة: المركز القومي للإصدارات القانونية، ٢٠١٣ م)، ط ١، ص ٢١٧. حمد علي الحلبي، شرح قانون العقوبات – القسم العام، (عمان: دار الثقافة، ٢٠٠٧ م)، ط١، ص ١٣٦.

[1] كريري، الركن المعنوي في الجرائم المعلوماتية، ص ٤٢.

فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرماً قانوناً ووفقاً لهذا النص فإن الركن المادي يتم بتحقيق نشاط إجرامي))[٢].

أما الجريمة التي نحن بصددها فمحل الجريمة التي نص عليها القانون – كما وردت في المادة رقم: ١٠ من المرسوم بالقانون الاتحادي رقم ٥ لسنة ٢٠١٢ م بشأن مكافحة جرائم تقنية المعلومات – والتي يقع عليها السلوك الإجرامي هو هنا البريد الإلكتروني، ويقصد به مراسلات وثائقية مكتوبة أو مصورة أو غير ذلك يتم إرسالها واستقبالها من خلال نظام اتصالات بريدي إلكتروني، ويمكن إضافة مواد فلمية أو وثائق إلكترونية ترفق مع الرسالة، وتظهر أهمية البريد الإلكتروني في مزاياه؛ ومن أبرزها: السرعة العالية، فهذه أهم ميزة للبريد الإلكتروني هي إمكانية إرسال الرسائل لأي شخص بالعالم بسرعة عالية، فضلاً عن كونه قابلاً للفتح في أي مكان في العالم، فمتى تم إنشاء بريد إلكتروني، فبإمكان صاحبه الدخول إلى البريد في أي مكان في العالم يتوافر فيه شبكات إنترنت[١].

أما الركن المادي في السلوك الذي يرتكبه الجاني للتعدي على البريد الإلكتروني؛ بيد أن المشرع لم يحدد سلوكاً معيناً يتحقق به الاعتداء على البريد الإلكتروني، وعليه تتنوع صور السلوك التي تشكل اعتداءً على البريد الإلكتروني، وتتمثل في أي فعل يرتكبه الجاني بصورة عمدية بقصد إغراق البريد الإلكتروني بالرسائل الاقتحامية وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته، ويقصد بالإغراق إرسال عدد كبير من الرسائل إلى البريد الإلكتروني لشخص أو اشخاص، ولا يشترط أن تكون الرسائل ذات مضمون معين إنما محملة بملفات ذات حجم كبير تستغرق المساحة المحددة بالبريد الإلكتروني مما يؤدي إلى تعطيله أو توقفه عن العمل[٢].

---

[٢] محمد شلال العاني، أحكام القسم العام في قانون العقوبات الاتحادي الإماراتي – النظرية العامة للجريمة، (الشارقة – الآفاق المشرقة، ٢٠١٠)، ط ١، ص ١٦٩.

[١] عبد الحميد بسيوني، رخصة الحاسوب – المعلومات والاتصالات، (القاهرة، دار الكتب العلمية، ٢٠٠٩)، ط ١، ص ٥٨-٥٩.

[٢] منير الجنبيهي وممدوح الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، (الإسكندرية: دار الفكر الجامعي، ٢٠٠٦)، ط ١، ص ٦٧.

في ختام الحديث عن الركن المادي تجدر الإشارة إلى مدى إمكانية العقاب على الشروع في هذه الجريمة، لا سيما أنها من نوع الجنح، فجريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية بصورتها التامة لا بد أن تحقق فيها صورة من صور النتائج التي نصت عليها الفقرة الثالثة من المادة العاشر: ((.... إيقافه عن العمل أو تعطيله أو إتلاف محتوياته)) أما الشروع في هذه الجريمة فلم ينص القانون على أي عقوبة له، وما دام أن الجريمة من نوع الجنح، فلا بد من تحديد القانون لمدى العقاب عليها من عدمه عملاً بنص المادة رقم: ٣٦ من قانون العقوبات الإماراتي: ((يحدد القانون الجنح التي يعاقب على الشروع فيها وكذلك عقوبة هذا الشروع)).

الفرع الثاني

النتيجة الجرمية

تعد النتيجة الجرمية العنصر الثاني من عناصر الركن المادي ويراد بها التغير الذي يقع في العالم الخارجي نتيجة السلوك الإجرامي، هذا وإن للنتيجة الجرمية مفهومان، الأول مادي والثاني قانوني وبالنسبة إلى المفهوم المادي فيراد به التغير الذي يقع في المحيط الخارجي بطريقة ما فيترك أثرا ملموسة والذي تختلف صورته من سلوك لأخر[1]، علماً أن القانون الجنائي لا يكتفي بوقوع نتيجة ضارة وإنما لابد أن يعتد القانون الجنائي بهذه النتيجة بحيث يرتب عليها آثاراً جنائية[2].

---

[1] د. محمود نجيب حسني: شرح قانون العقوبات القسم العام، مصدر سابق، ص ٢٨٨ .

[2] د. بكري يوسف بكري: قانون العقوبات القسم العام، مصدر سابق، ص ٣٩٦.

وبالنسبة إلى المفهوم الثاني للنتيجة الجرمية والمتمثل بالمفهوم القانوني فيراد به العدوان الذي يمس مصلحة أو حقا يحميه القانون.

واستنادا لذلك يمكن أن نقول أن مدلول النتيجة الجرمية من الناحية المادية في جريمة إغراق البريد الإلكتروني بالرسائل الإقتحامية يتمثل في ثلاث صور، الأولى إيقاف البريد عن العمل، والثانية تعطيله، والثالثة إتلاف محتوياته ، وذلك استنادا إلى المادة (١٠) من قانون مكافحة جرائم تقنية المعلومات الإماراتي السابق ذكرها.

وبالنسبة إلى معنى الإيقاف فيراد به توقف البريد الإلكتروني عن أداء مهامه بشكل كلي أو جزئي[٣]، أما التعطيل فيراد به توقف البريد الإلكتروني عن القيام بوظيفته لفترة مؤقتة من الزمن[٤] وأخيراً الإتلاف والذي يعني تخريب البريد الإلكتروني بجعله غير صالح للاستعمال من خلال إستخدام برامج مشفرة تسمى (الفيروسات) والتي ترسل مع الرسائل الإقتحامية عبر شبكة الإنترنت[١].

أما المدلول القانوني لنتيجة الإغراق البريدي فيتجسد في انتهاك حق الحماية القانونية الذي نص عليه القانون للبريد الإلكتروني.

إن العلاقة السببية موضوعها في الركن المادي للجريمة فهي الصلة التي تربط ما بين السلوك الإجرامي والنتيجة الجرمية، بحيث تثبت أن ارتكاب الفعل هو الذي أدى إلى وقوع النتيجة الإجرامية[٢] وبذلك فهي تربط بين عنصري الركن المادي فتنشأ له وحدته التي بدونها لا قيام ولا تحقق له[٣].

---

[٣] د. حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩ م، ص ٤٢٠.

[٤] د. حسين بن سعيد ، المصدر نفسه، ص ٤٢٠ .

[١] د. أيمن عبد الحميد عبد الحفيظ: إستراتيجية مكافحة جرائم إستخدام الحاسب الآلي، بدون مكان طبع، بدون سنة طبع، ص ١١، د. حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم الإنترنت، مصدر سابق، ص ٤٢٠.

[٢] د. محمود نجيب حسني: علاقة السببية في قانون العقوبات، بدون مكان طبع، بدون سنة طبع، ص ٣.

[٣] د. عبد الحكيم فودة أمام: رابطة السببية في الجرائم العمدية وغير العمدية، دار الفكر الجامعي، الإسكندرية، بدون سنة طبع، ص ٨.

بالنسبة إلى جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية فإن العلاقة السببية تتحقق فيها متى ما كان السلوك الإجرامي المتمثل بالإغراق البريدي والذي يراد به إرسال الجاني عشرات الرسائل المكررة دفعة واحدة لنظام البريد الإلكتروني من خلال شبكة الإنترنت هو الذي أدى إلى تعطيل أو إيقاف أو إتلاف محتويات البريد الإلكتروني أما إذا ثبت انتفاء العلاقة السببية بين سلوك الإغراق البريدي والنتيجة الجرمية المتمثلة بالإيقاف أو التعطيل أو الإتلاف فإن مرتكب السلوك لا يسأل إلا عن الشروع في الجريمة كما لو كان سبب الإيقاف أو التعطيل أو الإتلاف نتيجة برامج تخريبية[٤].

تعد خدمة البريد الإلكتروني من الخدمات المفيدة التي تقدمها شبكة الإنترنت للأفراد والهيئات من خلال اتصال بعضهم ببعض وفي الوقت ذاته فإنها تعد من أشهر وأقدم الخدمات التي تقدم على الشبكة العالمية حيث يعود تاريخ نشأتها إلى بداية السبعينات من القرن الماضي ومع مرور الوقت أحدث البريد الإلكتروني ثورة في مجال الاتصالات الفردية، إذ يستطيع الفرد أن يرسل لآخر رسالة تتضمن معلومات مكتوبة قد يرفق معها ملفات أو صور أو مستندات[١]، وبذلك يمكن أن نعرف البريد الإلكتروني بأنه: "خط مفتوح في كل أرجاء العالم يتمكن الفرد بواسطته من إرسال واستقبال كل أنواع الرسائل"[٢] وكذلك عرف بأنه: "وسيلة تساعد على تبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة الإنترنت"[٣].

من خلال ما تقدم ذكره يتضح أن البريد الإلكتروني يمتاز بعدة مزايا وهي:

---

[٤] تنص م ٢٩ "١- لا يسأل شخص عن جريمة لم تكن نتيجة لسلوكه الإجرامي لكنه يسأل عن الجريمة ولو كان قد ساهم مع سلوكه الإجرامي في أحداثها سبب آخر سابق أو معاصر أو لاحق ولو كان يجهله.
٢- أما إذا كان ذلك السبب وحده كافياً لإحداث الجريمة فلا يسأل الفاعل في هذه الحالة إلا عن الفعل الذي ارتكبه".

[١] د. عبد الفتاح بيومي حجازي: مكافحة جرائم الكومبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦ م، ص ٦٨١.

[٢] Mr. Tariq Banday: Techniques and Tools for Forensic Investigation of E-mail, India, 2011, p. 4

[٣] د. خالد ممدوح إبراهيم: لوجستيات التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨ م، ص ١٨٩.

١. أنه وسيلة اتصال سهلة وسريعة، إذ تصل الرسالة خلال ثوانٍ إلى صندوق البريد الإلكتروني.
٢. وسيلة اتصال غير مكلفة مادياً.
٣. يمكن التواصل عن طريق البريد الإلكتروني بأي وقت لأنه يعمل من دون التقييد بوقت معين خلال اليوم.
٤. لديه خاصية تسجيل وقت وتاريخ وصول الرسالة فضلاً عن حفظها.
٥. بالإمكان إرسال أكثر من رسالة واحدة في الوقت نفسه ولأكثر من شخص.
٦. البريد الإلكتروني مشفر بكلمة سر، وبالتالي فإنه يساعد على منع الاطلاع على الرسائل المرسلة بخلاف المكالمات الهاتفية.
٧. يستطيع صاحب البريد الإلكتروني قراءة الرسائل المرسلة إليه في أي مكان وفي أي وقت طالما أن المستفيد من هذه الخدمة متصل بالشبكة العالمية[٤].

طالما على الرغم من المزايا أعلاه التي يتمتع بها البريد الإلكتروني إلا أنه لا يخلو من العيوب متى ما أسيء استخدامه ومنها إرسال الرسائل الاقتحامية التي تؤدي إلى إيقاف البريد أو تعطيله أو إتلاف محتوياته مما يلحق أضراراً كبيرة بمستخدميه سواء كانوا أفراداً أم شركات.

[٤] د. خالد ممدوح إبراهيم: لوجستيات التجارة الإلكترونية، مرجع سابق، ص ١٨٦.

المطلب الثاني

الركن المعنوي للجريمة

يقصد بالركن المعنوي للجريمة العمد أو الخطأ وفقاً للمادة رقم: ٣٨ من قانون العقوبات الاتحادي، فالعمد هو اتجاه إرادة الجاني إلى ارتكاب الفعل أو الامتناع متى كانا مجرمين قانونيين وذلك لإحداث نتيجة مباشرة أو نتيجة أخرى مجرمة يتوقعها الجاني[1].

فضلاً عن قيام علاقة سببية بين السلوك والنتيجة، وبوجود هذه العلاقة يكتمل الركن المادي لهذه الجريمة، وفي هذه الجريمة يلزم توافر علاقة سببية بين إرسال الرسائل الاقتحامية، وما يترتب على هذا السلوك من نتائج حددها

[1] انظر: النيابة العامة – حكومة دبي:
https://www.dxbpp.gov.ae/NewsPage.aspx?ID=826&Type=5

نص المرسوم بإيقاف أو تعطيل البريد الإلكتروني أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البيانات أو المعلومات[2].

عرفت المادة الاولى من قانون مكافحة جرائم تقنية المعلومات في جمهورية مصر العربية رقم (١٧٥) لسنة ٢٠١٨ البيانات والمعلومات الإلكترونية :" كل ما يمكن إنشاؤه أو تخزينه، أو معالجته،أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات ؛ كالأرقام والأكواد والشفارات والحروف والرموز والإشارات والصور والأصوات ومافى حكمها".

عرفت المادة الأولى من قانون مكافحة جرائن تقنية المعلومات في جمهورية مصر العربية رقم (١٧٥) لسنة ٢٠١٨ بيانات شخصية: أى بيانات متعلقة بشخص طبيعى محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربن بينها وبين بيانات أخر

- عرفت المادة الاولى من قانون مكافحة جرائن تقنية المعلومات في جمهورية مصر العربية رقم (١٧٥) لسنة ٢٠١٨ بيانات حكومية : بيانات متعلقة بالدولة أو أحد سلطاتها، وأجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة والأجهزة الرقابية، وغيرها من الأشخاص الاعتبارية العامة وما فى حكمها، والمتاحة على الشبكة المعلوماتية أو على أى نظام معلوماتى أو على حاسب أو ما فى حكمها.

إن الركن المعنوي في جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية يتخذ صورة القصد الجرمي والذي يتكون من عنصري العلم والإرادة واستناداً لذلك سأتناول في الفرع الأول العلم أما الفرع الثاني فسأتناول فيه الإرادة وكالآتي:

أولاً: العلم

يحتل العلم مكانة أساسية ومهمة في القانون الجنائي الموضوعي بشكل عام وفي القصد الجرمي بشكل خاص لأن مدى مساءلة الشخص عن سلوكه الإجرامي يعتمد بشكل أساس على إدراك هذا الشخص وعلمه إن ما ارتكبه

[2] انظر: عبد اللطيف، شرح قانون جرائم تقنية المعلومات، ص ١١١.

يعد جريمة يحاسب عليها القانون الأمر الذي يستدعي عدّه مسؤولاً من الناحية القانونية عن سلوكه الإجرامي[1]، وبخلافه ذلك إذا كان الشخص ليس لديه أي علم بالصفة الجرمية لسلوكه الإجرامي قامت بحقه المسؤولية غير العمدية لأن نيته تجردت من أي فكرة جرمية ما لم يثبت أنه اتخذ كافة إجراءات الحيطة والحذر.

وبذلك عرف العلم "بأنه حالة عقلية ساكنة يتخيل من خلالها الشخص حقيقة الشيء على نحو يطابق الحقيقة"[٢].

وبالنسبة إلى جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية فإن العلم يتحقق لدى الجاني إذا كان يعلم بأن إرسال هذا الكم الهائل من الرسائل دفعة واحدة سيؤدي إلى إعاقة عمل النظام التقني الإلكتروني للبريد وبالتالي توقف تلك الخدمة عن أداء عملها نتيجة التعطيل أو الإيقاف أو الإتلاف علماً أن القصد الجرمي يعد متحققاً حتى في حالة ادعاء الجاني بعدم علمه بالنصوص العقابية التي تجرم إغراق البريد الإلكتروني بالرسائل الاقتحامية لأنه لو جاز ذلك لأصبح الأمر فوضى، لأن كل متهم سيدعي بعدم علمه بتجريم سلوك الإغراق البريدي وبالتالي صعوبة إثبات عكس ذلك مما سيؤدي إلى تعطيل تطبيق أحكام القانون الجزائي[١].

ثانياً: الإرادة

إن الإرادة هي العنصر الثاني من عناصر القصد الجرمي وتعرّف "بأنها نشاط نفسي يهدف إلى بلوغ غرض محدد يتمثل بالنتيجة الجرمية التي يهدف الجاني إلى تحقيقها من خلال نشاطه الإجرامي"[٢]، كذلك عرّفت بأنها:

---

(1) د. عمر شريف: درجات القصد الجرمي، دار النهضة العربية، القاهرة، ٢٠٠٢ م، ص ١٢٣.

[٢] د. عمر شريف: درجات القصد الجرمي، مرجع سابق، ص ١٢٦.

[١] د. عمر غبراهيم الوقاد: الغلط في القانون في ضوء أحكام القانون الجنائي، المكتبة المصرية، القاهرة، ٢٠٠١ م، ص ٣٨.

[٢] د. عباس الحسني: شرح قانون العقوبات الجديد، مطبعة الإرشاد، بغداد، ١٩٧٢ م، ص ٩٠.

"نشاط نفسي يتجه نحو غرض معين من خلال استعمال الجاني وسيلة معينة للتأثير على ما حوله من أشخاص وأشياء"[٣].

وللإرادة دور كبير في تصرفات الإنسان القانونية على الصعيدين الداخلي والخارجي، فبالنسبة إلى الصعيد الداخلي تعد الإرادة صاحبة القرار من حيث القيام أو عدم القيام بالسلوك الإجرامي، أما على الصعيد الخارجي فيتمثل دور الإرادة بالحركات التي تظهر إلى الحيز الخارجي نتيجة القرار الداخلي كما في جريمة إغراق البريد الإلكتروني بالرسائل الاقتحامية، إذ يتحقق القصد الجرمي لدى الجاني عندما تتجه إرادته مع العلم نحو ارتكاب فعل الإغراق البريدي لتحقيق نتيجة الجرمية والمتمثلة بإيقاف، أو تعطيل، أو إتلاف البريد الإلكتروني مما يترتب عليه إعاقة استعمال تلك الخدمة أو توقفها.

هذا وإن الجاني عندما يقوم بفعل الإغراق البريدي يجب أن لا يكون ذلك فقط بصورة إرادية وإنما يجب أيضاً أن يكون الجاني متمتع بالإدراك وحرية الاختيار بحيث يتحمل في ضوئهما النتائج المترتبة لانتهاكه القواعد القانونية[٤].

الفرع الثاني

العقوبات المقررة للجريمة

نص المشرع الإماراتي- الفقرة الثالثة من المادة: ١٠ من المرسوم الاتحادي الإماراتي رقم: ٥ لسنة ٢٠١٢ م بشأن مكافحة جرائم تقنية المعلومات – على عقوبة الحبس أو الغرامة أو إحدى هاتين العقوبتين، وتطبق القواعد العامة بالنسبة للعقوبتين السابقتين، فالحبس لا يقل عن شهر ولا تزيد على ثلاث سنوات، والغرامة لا تقل عن مائة درهم ولا تزيد على ثلاثين ألف

---

[٣] المصدر نفسه، ص ٩٠.

[٤] د. محمود نجيب حسني: شرح قانون العقوبات القسم العام، مصدر سابق، ص ٣٨٢.

درهم؛ حيث إن الجريمة جنحة[1]، وقد أعطى المشرع للقاضي سلطة تقديرية في الجمع بين هاتين العقوبتين أو اختيار إحداهما.

من جهة أخرى؛ فقد أضاف المشرع الإماراتي بعض العقوبات التكميلية، إذ نصت المادة رقم: ٤١ من المرسوم بالقانون الاتحادي رقم ٥ لسنة ٢٠١٢ م بشأن مكافحة جرائم تقنية المعلومات على مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في هذه الجريمة، وإغلاق المحل أو الموقع الذي يرتكب فيه الجريمة؛ إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة.

وثمة مجموعة من التدابير طرحها المشرع الإماراتي – المادة رقم: ٤٣ – يجوز للمحكمة الحكم بها إضافة إلى العقوبة الأصلية، والتدابير هي: وضع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة، ونصت المادة رقم: ٤٢ من القانون ذاته على إبعاد الأجنبي المحكوم عليه بالإدانة. ونصت المادة رقم: ٤٨ من القانون عينه على تطبيق أي عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر[1].

في ختام عرض الموقف الفقهي والقانوني لهذه المسألة، يخلص الباحث إلى هذه المقارنة:

١) من حيث التجريم: نجد أن الفقه الإسلامي حرّم الضرر بصوره كافة، وهذا العموم يدخل ضمنه الرسائل الاقتحامية، فبذلك يتفق الإسلامي والقوانين العربية المذكورة سابقاً على هذا التجريم.

---

[1] من الجدير بالذكر أن المادة (٧١) من المرسوم بقانون اتحادي رقم (٧) لسنة ٢٠١٦ م بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم (٣) لسنة ١٩٨٧ م حددت عقوبة الغرامة في الجنح بأنها: إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن ألف درهم ولا أن يزيد حدها الأقصى على مليون درهم في الجنايات وثلاثمائة ألف درهم في الجنح، وذلك كله ما لم ينص القانون على خلاقه.

[1] من الجدير بالذكر أن المادة ١١٠ من المرسوم بقانون اتحادي رقم (٧) لسنة ٢٠١٦ م بتعديل بعض أحكام قانون العقوبات الصادر بالقانون الاتحادي رقم (٣) لسنة ١٩٨٧ م أضافت بعض التدابير المقيدة للحرية، وهي: ١. حظر ارتباد بعض المحال العامة، ٢. منع الإقامة في مكان معين. ٣. المراقبة. ٤. الخدمة المجتمعية، ٥. الإبعاد عن الدولة.

٢) من حيث العقوبة: في الطرح الفقهي يعاقب بالتعزير على كل الجرائم فيما عدا جرائم الحدود وجرائم القصاص فلها عقوباتها الخاصة، ولا يعاقب عليها باعتبار التعزير عقوبة أصلية وإنما باعتباره عقوبة بديلة تجب عند امتناع العقوبة الأصلية كعدم توفر شروط الحد، أو باعتباره عقوبة تضاف إلى العقوبة الأصلية، والمتأمل في منهج التشريع الإسلامي يلحظ أنه لا يفرض لكل جريمة من جرائم التعزير عقوبة معينة؛ لأن تقييد القاضي بعقوبة معينة يمنع العقوبة أن تؤدي وظيفتها،

ويجعل العقوبة غير عادلة في كثير من الأحوال، نظراً لكون ظروف الجرائم والمجرمين تختلف اختلافاً بيناً، وما قد يصلح مجرماً بعينه قد يفسر مجرماً آخر، ما يردع شخصاً عن جريمة قد لا يردع غيره؛ بناءً على ذلك فقد وضعت الشريعة لجرائم التعازير عقوبات متعددة مختلفة هي مجموعة كاملة من العقوبات تتسلسل من أخف العقوبات إلى أشدها، وتركت للقاضي أن يختار من بينها العقوبة التي يراها كفيلة بتأديب الجاني واستصلاحه وبحماية الجماعة من الإجرام، وللقاضي أن يعاقب بعقوبة واحدة أو بأكثر منها، وله أن يخفف العقوبة او يشددها إن كانت العقوبة ذات حدين، وله أن يوقف تنفيذ العقوبة إن رأى في ذلك ما يكفي لتأديب الجاني وردعه وإصلاحه. وغذا كانت الشريعة قد عرفت عقوبات تعزيرية معينة فليس معنى ذلكأنها لا تقبل غيرها، بل إن الشريعة تتسع لكل عقوبة تصلح الجاني وتؤدبه وتحمي الجماعة من الإجرام، والقاعدة العامة في الشريعة أن كل عقوبة تؤدي إلى تأديب المجرم واستصلاحه وزجر غيره وحماية الجماعة من شر المجرم والجريمة هي عقوبة مشروعة. وقد تحدث الفقهاء عن عدد من صور التعزير كالتعزير بالقتل، والجلد، والحبس والتغريب، وغيره[1].

أما الطرح القانوني للعقوبة فقد قيّد المشرع الإماراتي تحديداً القاضي بعقوبتين هما: الحبس والغرامة، بيد أنه أعطى القاضي سلطة تقديرية – ضمن ضوابط عامة – في مسألة الجبس، فقيده بأن لا يقل عن شهر ولا يزيد على ثلاث سنوات، والعقوبة الثانية الغرامة بحيث لا تقل عن مائة درهم ولا تزيد على ثلاثين ألف درهم، فضلاً عن كون المشرع أعطى القاضي سلطة

---

[1] د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، الناشر دار النهضة العربية، القاهرة ٢٠٠٠، ١٠٢.

تقديرية في الجمع بين العقوبتين أو الاكتفاء بإحداهما؛ لذلك يجد الباحث أن الطرح الفقهي ينسجم مع الطرح القانوني؛ فالمسألة فقهاً تدخل ضمن التعزير، والتعزير متروك للحاكم، ثم إن القانون أعطى القاضي مساحة تقديرية في العقوبات، وهذا ما تؤكده القواعد العامة للتعزير، فهو متروك للقاضي في ضوء الأصلح للفاعل؛ عملاً بالقاعدة الفقهية تصرف الإمام على الرعية منوط بالمصلحة[٢].

وتنص المادة ١٨ من قانون مكافحة جريمة تقنية المعلومات في جمهورية مصر العربية رقم (١٧٥) لسنة ٢٠١٨ على أنه": جريمة الاعتداء على البريد الاليكتروني أو المواقع أو الحسابات الخاصة:" يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن ٥٠ ألف جنيه ولا تجاوز ١٠٠ ألف جنيه أو بإحدى العقوبتين كل من أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بأحد الناس، فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ٦ أشهر وبغرامة لا تقل عن ١٠٠ ألف جنيه ولا تجاوز ٢٠٠ ألف جنيه أو بإحدى هاتين العقوبتين.

الفصل الثاني

جريمة اختراق البريد الالكتروني

اختراق البريد الإلكتروني: وهو أن تعمد جهة ما بمحاولة الدخول إلى أنظمة أو شبكات تواصل أو منشئات بمساعدة بعض البرامج المختصة، في سرقة وفك كلمات السر عن طريق المهارات والفنيات المكتسبة[١].

---

[٢] د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص ١٠٣.

[١] عبد الله بن ناصر بن أحمد العمري، المرجع السابق، ص ٥٩.

كما عرف الاختراق في القانون العربي النموذجي الموحد بأنه: "الدخول غير المصرح به أو غير المشروع النظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية"[٢].

ويرتبط الاختراق بالبريد الإلكتروني التي تعد أداة مباشرة لولوج الأجهزة والشبكات المعلوماتية بهدف التأثير في أداء أجهزة الحاسب الآلي وتعطيلها، وتخريب البيانات والنظم والتعدي على الممتلكات وبث البرمجيات الخبيثة التي تقوم بتدمير معطيات وقواعد البيانات الضرورية، كما يعني اختراق البريد الإلكتروني "الدخول غير المشروع إلى المعلومات والبيانات المرسلة عن طريق البريد الإلكتروني"[٣].

- **المبحث الأول:** ماهية اختراق البريد الإلكتروني وانواعه.
- **المبحث الثاني: أركان الجريمة وعقوبتها.**

المبحث الأول

ماهية اختراق البريد الإلكتروني وانواع الاختراق

تعاني شبكة الانترنت من مشاكل الاختراق التي تزداد يوماً بعد يوم وخاصة اختراق البريد الالكتروني مسببة أضرار جسيمة للشركات والأفراد

---

[٢] القانون لنموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات، لعام ٢٠٠٤.

[٣] عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، ط ٢ الرياض، دار الوراق، ٢٠٠٦، ص ٦٥ .

ويصنف الاختراق إلى ثلاثة أنواع: اختراق الأجهزة، واختراق المواقع والشبكات، واختراق البريد الإلكتروني[1].

المطلب الأول

تعريف اختراق البريد الالكتروني

يتم الاختراق للبريد الالكتروني بواسطة هاكرز محترفين أو هواة، أو بعض مواقع الإنترنت نفسها، واحياناً بواسطة مؤسسات وجهات دولية، ويمكننا القول بأن الاختراق هو: القدرة على الوصول لجهاز او شبكة أو موقع معين أو بريد الكتروني بطريقة غير مشروعة عن طريف ثغرات في نظم التشغيل أو برامج الحماية الخاصة بالضحية المستهدفة[2].

والمقصود من الاختراق بشكل عام هو قدرة المخترق على الدخول إلى جهاز شخص ما أو بريده الالكتروني بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول إلى جهاز آخر فهو مخترق (Hacker). أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرب (Cracker). وإن كان هناك من يرى أن الهاكرز هم المخربون، وأن الكراكرز هم مجرد قراصنة برامج، ونحن أقرب لهذا الرأي[٣].

عرفت المادة الاولى من قانون مكافحة جرائم تقنية المعلومات في جمهورية مصر العربية رقم (١٧٥) لسنة ٢٠١٨ -الاختراق : الدخول غير المرخص به، أو المخال لأحكام الترخيص، أو الدخول بأى طريقة غير مشروعة، إلى نظام معلوماتى أو حاسب إلى أو شبكة معلوماتية، وما فى حكمها."

كما عرفت المادة الاولى من قانون مكافحة جرائم تقنية المعلومات في جمهورية مصر العربية رقم (١٧٥) لسنة ٢٠١٨ -المحتوى : أى بيانات

---

(1) علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة، مرجع سابق، ص ١٤٠.

(2) المرجع سابق، ص ١٤١.

(٣) علي عدنان الفيل، الإجرام الإلكتروني، ط ١، مكتبة زين الحقوقية والأدبية، بيروت، ٢٠١١، ص ١٢٩.

تـؤدى بـذاتها، أو مجتمعـه مـع بيانـات أو معلومـات أخـرى إلـى تكـوين معلومـة أو تحديد توجه أو اتجاه أو تصور أو معنى أو الإشارة إلى بيانات أخرى"[1]

ولاختـراق الأجهـزة – أو الشـبكات أو المواقـع أو البريـد الالكترونـي – طـرق وأسـس يسـتطيع مـن خلالهـا المختـرق التطفـل علـى أجهـزة الآخـرين عـن طريـق معرفـة الثغـرات الموجـودة فـي أنظمـتهم. وغالبـاً مـا تكـون تلـك الثغـرات فيمـا يسـمى بالمنافـذ الخاصـة بالحاسـب وهـذه المنافـذ يمكـن وصـفها بأبسـط شـكل علـى أنهـا بوابـات للجهـاز علـى الانترنـت. ويصـل عـددها إلـى نحـو (٦٥٥٣٥ منفـذ). وهـذه المنافـذ ليسـت منافـذ ماديـة يمكـن رؤيتهـا كمنافـذ الطابعـة أو المـاوس أو لوحـة مفـاتيح جهـاز الحاسـب. ولكنهـا فـي واقـع الأمـر جـزء مـن الـذاكرة لـه عنـوان معـين يتعـرف عليـه الجهـاز بأنـه منطقـة اتصـال يـتم عبـره إرسـال واسـتقبال البيانـات. وعلـى سـبيل المثـال: فـإن المنفـذ ٨٠ غالبـاً مـا يكـون مخصصـاً لمـوفر الخدمـة كـي يـتم دخـول المسـتخدم الانترنـت وفـي بعـض الأوقـات يكـون المنفـذ رقمـه (٨٠٨٠). وهنـاك طـرق عديـدة للاختـراق أبسطهـا عبـر البـرامـج التـي تعتمـد نظـام (الزبون/الخـادم) حيـث تحتـوي علـى ملفـين احـدهما Server يرسـل إلـى الجهـاز المصـاب بطريقـة مـا. والآخـر Client يـتم تشـغيله مـن قبـل المختـرق للـتحكم فـي الجهـاز المصـاب وعنـد تشـغيل ملـف الخـادم –مـن قبـل المُختَـرَق يصـبح الكمبيـوتر عرضـة للاختـراق حيـث يتـم فـتح أحـد المنافـذ (Ports) وغالبـاً مـا يكـون المنفـذ ١٢٣٤٥ أو ١٢٣٤٦ وبـذلك يسـتطيع الاختـراق ببرنـامج مخصـص لـذلك كبرنـامج NetBus أو NetSphere أو Back Orifice ويفعـل مـا يحلـو لـه. كمـا يسـتطيع أشـخاص آخـرون (إضـافة إلـى مـن وضـع الملـف فـي جهـاز الضـحية) فعـل نفـس الشـيء بـه حينمـا يقومـون بعمـل مسـح للمنافـذ المفتوحـة علـى الشـبكة (Port Scanning). وهنـاك طـرق عديـدة تمكـن المتطفلـين مـن اختـراق الأجهـزة مباشـرة بـدون إرسـال ملفـات لدرجـة أن إحـدى جمعيـات الهـاكرز فـي الولايـات المتحـدة ابتكـرت طريقـة للاختـراق متطـورة للغايـة عـن طريـق اعتـراض حـزم البيانـات التـي تتـدفق مـع الاتصـالات

---

[1] المـادة الأولـى مـن قـانون مكافحـة جـرائم تقنيـة المعلومـات فـي جمهوريـة مصـر العربيـة رقـم (١٧٥) لسنة ٢٠١٨- المحتوى.

الهاتفية عبر الانترنت، ويتم عبر اعتراض تلك البيانات، إدخال بيانات مرافقة لها من المخترقين، والتحكم في الحاسبات المتلقية لتلك البيانات!![1].

وكشفت معلومات أمنية أن ٥٥% من مستخدمي الإنترنت على الشبكة يتعرضون لتجسس المواقع الإلكترونية التي زاروها والتي يتم التوجه إليها مشيرة إلى أنه من بين اكثر من 1,678 مليون مستخدم قاموا بعملية مسح أجهزتهم للتعرف على المخاطر الأمنية التي يمكن أن يتعرضوا لها أثناء تصفح الإنترنت فإن ٥٥% منهم يتعرضون لعملية جمع معلومات عنهم من خلال الشبكات والمواقع التي يقومون بزيارتها مما يشكل انتهاكها لخصوصياتهم على الشبكة. وأنه من بين المستخدمين الذين قاموا بعملية فحص أجهزتهم فإن ٤٥% منهم في مأمن بسبب قيامهم برفع مستوى الأمان في مستعرضات ومتصفحات الإنترنت التي يستخدمونها ووضع برامج حماية من نوع الجدران النارية (Fire Wall) لمنع مزودات الإنترنت من جمع معلومات عنهم بطريقة غير مشروعية[٢].

ووفقاً لمعلومات أمنية: إن ٢٤% من المستخدمين يتصلون عبر شبكات غير آمنة وتوجد بها ثغرات أمنية (Vulnerability)، يمكن للهاكرز الاستفادة منها لشن حرب معلوماتية خطيرة. وأن ٧% من اجهزة المستخدمين مصابة ببرامج تجسس خطيرة (Trojan) وحذرت معلومات أمنية من تدني مستوى درجات الأمن على الشبكة، حيث وجدت من خلال عمليات الفحص المجانية التي تقدمها عبر موقعها أن ٣٠% من مجموع برامج الحماية الخاصة بالمستخدمين المشاركين في عملية جمع المعلومات تتهدها المخاطر بسبب ضعف تحديث قواعد البيانات الخاصة بها مما يجعلها عديمة الفائدة.[٣]

المطلب الثاني

---

(1) عماد قادوري، البريد الإلكتروني، خصائصه وبرامجه، دار علاء الدين للنشر، دمشق، ط ١، ٢٠٠٢ م، ص ١٦٢.

(٢) عماد قادوري، البريد الإلكتروني، خصائصه وبرامجه، مرجع سابق، ص ١٦٤.

(٣) http://www.norton.com or www.symantec.com

انواع الاختـــــراق التي يتعرض لها البريد الالكتروني

طبقـــاً لأهـــداف المختـــرقين، فـــإن الاختـــراق ينقســـم – مـــن حيـــث الطريقـــة المستخدمة – إلى ثلاثة أقسام:[1]

١- اختـــــراق المـــــزودات أو الملقمـــــات او الأجهـــــزة الرئيســـــية للشـــــركات والمؤسســـات أو الجهـــات الحكوميـــة، وذلـــك بـــاختراق أنظمـــة التشـــغيل غيـــر المحميـــة، أو حتـــى المحميـــة ببـــرامج الجـــدران الناريـــة، وغالبـــاً مـــا يـــتم ذلـــك باســـتخدام طريقـــة المحاكـــاه (Spoofing)، وهـــو مصـــطلح يطلـــق علـــى عمليـــة انتحـــال شخصـــية للـــدخول إلـــى النظـــام حيـــث أن حـــزم ال IP تحتـــوي علـــى عنـــاوين للمرســـل والمرســـل إليـــه وهـــذه العنـــاوين ينظـــر إليهـــا علـــى أنهـــا هنـــاوين مقبولـــة وســـارية المفعـــول مـــن قبـــل البـــرامج وأجهـــزة الشـــبكة. ومـــن خـــلال طريقـــة تعـــرف بمســـارات المصـــدر (Source Routing)، فـــإن حـــزم ال IP قـــد تـــم إعطاؤهـــا شـــكلاً تبـــدو معـــه وكأنهـــا قادمـــة مـــن كمبيـــوتر معـــين، بينمـــا هـــي فـــي حقيقـــة الأمـــر ليســـت قادمـــة منـــه وعلـــى ذلـــك فـــإن النظـــام إذا وثـــق بهويـــة عنـــوان مصـــدر الحزمـــة فإنـــه يكـــون بـــذلك قـــد تـــم خداعـــه بطريقـــة محاكـــاة حـــزم البيانـــات الأصـــلية، وهـــذه الطريقـــة هـــي ذاتهـــا التـــي نجـــح بهـــا مخترقـــو بريـــد الهوتميـــل (Hotmail) فـــي الولـــوج إلـــى معلومـــات النظـــام منـــذ فتـــرة. ويوجـــد فـــي مواقـــع الهـــاكرز علـــى الإنترنـــت بـــرامج لاختـــراق المواقـــع، أو الطفـــو فوقهـــا عبـــر إغراقهـــا بـــآلاف الطلبـــات مـــن البيانـــات، ولا توجـــد جهـــة (حكوميـــة أو اهليـــة) تســـعى بجديـــة للإيقـــاف مثـــل هـــذه المواقـــع عـــن العمـــل، ومعظمهـــا يقـــدم دروســـاً فـــي الاختـــراق بكافـــة أنواعـــه، ولا نـــود هنـــا ان نقـــدم عنـــاوين مثـــل هـــذه المواقـــع، ولـــو فـــي الهـــوامش كمصـــادر، لعـــدة أســـباب: أهمهـــا خطـــورة هـــذه المواقـــع علـــى زوارهـــا – حتـــى وإن كانـــت خبـــراتهم جيـــدة -، وأيضـــاً حتـــى لا يقـــوم أبناؤهـــا بالانـــدفاع –عبـــر

[1] http://shkoon.coolfreepage.com/amn/pages/hack-mop.html

هذه المواقع– وراء غريزة حب الاستطلاع فيتحولون إلى قراصنة إنترنت، أو هاكرز[1].

٢- اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات، وهي طريقة شائعة وسهلة، ويمكن لأي شخص له دراسة متوسطة بالانترنت أن يقوم بها، لعدم إدراك أصحاب الأجهزة الشخصية بمخاطر التواجد على الشبكة دون حماية – من جهة، ولسهولة تعلم برامج الاختراقات وتعددها وتوافرها أيضاً، من جهة أخرى.

٣- التعرض للبيانات في أثناء انتقالها والتعرف على شفرتها، إن كانت مشفرة، وهذه الطريقة تستخدمها أجهزة الاستخبارات، كما يستخدمها الهاكرز المحترفون – غالباً – في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية (ATM) وسرقتها[2]. وهذا ما أقرته محكمة استئناف باريس في حكمها الصادر في ١٧ ديسمبر ٢٠٠١ وأكدته أيضاً محكمة النقض الفرنسية في ٢ أكتوبر ٢٠٠١ في قضية Nikon Feance حيث قضت أن الرسائل الإلكترونية الشخصية التي يرسلها العامل أو يستقبلها على الحاسب الخاص برب العمل تدخل في نطاق حياة العامل الخاصة وعليه يحظر الاطلاع عليها أو المساس بسريتها[٣].

وفي هذا الشأن ينبغي التنبه إلى أمر يغفله الكثير من الناس، وهو: كشف أرقام بطاقات الائتمان الخاصة بهم لمواقع التجارة الإلكترونية، وينبغي ألا يتم ذلك إلا بعد التأكد من التزام تلك المواقع بمبادئ الامان والموثوقية. وهناك أمر آخر لا يلتفت إليه الكثيرون رغم خطورته[٤]: فالبعض عندما يستخدم بطاقة السحب الآلي من آلات البنوك النقدية (ATM) لا ينتظر خروج السند

---

(1) عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل للنشر، ط ١، ٢٠٠٥، ص ٩٤.

(2) عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دراسة مقارنة، ط ١، دار النهضة العربية، القاهرة، ٢٠٠١ م، ص ٨٣.

(٣) Cour d Cassation, Paris, 17 Dec, 2000, Cassation 02 Oct, 2001 .

(٤)Charles Trapper, Electronic Commerce Strategic, Printed in the USA Edition 2000.p188

الصغير المرفق بعملية السحب أو يأخذه، ثم يلقي به جانباً، دون أن يكلف نفسه عنا، تمزيقه جيداً. ولو نظرنا إلى ذلك المستند سنجد أرقاماً تتكون من عدة خانات طويلة هي بالنسبة لنا ليست بذات أهمية ولكن تلك الأرقام هي انعكاس للشريط الممغنط الظاهر بالجهة الخلفية لبطاقة (ATM)، وهذا الشريط هو حلقة الوصل بين صاحب البطاقة ورصيده بالبنك الذي من خلاله تتم عملية السحب النقدي، ولو وقع هذا المستند في يد أحد الهاكرز المحترفين، لأمكنه استخراج رقم الحساب البنكي بل والتعرف على الأرقام السرية للبطاقة البنكية (ATM)، ومن ثم، استخدامها!![1]

المطلب الثالث

دوافع ووسائل اختراق البريد الالكتروني

أما عن دوافع الاختراق، فقد أجمل الخبراء المتخصصون في هذا المجال الدوافع الرئيسية في عدة نقاط، هي: الدافع السياسي والعسكري والأمني أو الاستخباري، والدافع التجاري والتنافسي، والدافع الشخصي الفردي[3].

أولاً: الدافع السياسي والأمني:

في حقبة الحرب الباردة كان الصراع المعلوماتي والتجسسي بين الأمريكان والسوفييت على أشده. ولا ننسى ما أشرنا إليه في الفصل الأول بشأن النشأة العسكرية للإنترنت، فقيام الإنترنت أصلاً كان على خلفية سباقات التسلح وأبحاث الدفاع والتجسس. ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول، أصبح الاعتماد كبيراً على الحاسبات وشبكات الكمبيوتر، ومن البديهي أن يؤدي التطور العلمي والتقني إلى الاعتماد بشكل شبه كامل على أنظمة الكمبيوتر في أغلب الاحتياجات المعاصرة على مستوى الدول والأفراد والمؤسسات. وبالتالي: أصبح

---

(١) عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ١٢٥.

(٣) عمرو أحمد حسبو، المرجع السابق، ص ١٢٦.

الاختـــراق مـــن أجـــل الحصـــول علـــى معلومـــات سياســـية وعســـكرية واقتصـــادية مسألة بالغة الأهمية[١].

ثانياً: الدافـــع التجـــــاري:

عـــالم المـــال والتجـــارة والأعمـــال يغـــص بـــالكثير مـــن الأســـرار والخفايـــا، وقـــد تســـتعين بعـــض الشـــركات بمختـــرقين محتـــرفين، للتجســـس والتلصـــص علـــى شـــبكات الشـــركات المنافســـة، أو حتـــى شـــبكات الجهـــات الحكوميـــة والأهليـــة ذات الصـــلة بنشـــاطها، بـــل إن شـــركات الاتصـــالات والمعلومـــات نفســـها تســـعى دومـــاً لمعرفة أسرار بعضها، بهدف تحقيق المزيد من المكاسب[٢].

ثالثاً: الدافع الشخصي أو الفردي:

النســـبة الكبـــرى فـــي عمليـــات الاختـــراق تـــتم بواســـطة أفـــراد، لأهـــداف شخصـــية فـــي معظمهـــا، فقـــد بـــدأت أولـــى محـــاولات الاختـــراق بـــين طـــلاب الجامعـــات بالولايـــات المتحـــدة، كنـــوع مـــن التبـــاهي بالنجـــاح فـــي اختـــراق أجهـــزة شخصـــية لأصـــدقائهم ومعـــارفهم، ومـــا لبثـــت أن تحولـــت تلـــك الظـــاهرة إلـــى تحـــدٍ فيمـــا بيـــنهم لاختـــراق الأنظمـــة بالشـــركات ثـــم بمواقـــع الانترنـــت، ولا يقتصـــر الـــدافع علـــى الأفـــراد فقـــط بـــل توجـــد جماعـــات أشـــبه مـــا تكـــون بالأنديـــة وليســـت لأهـــداف تجاريـــة بالأســـاس. وهنـــاك بعـــض الأفـــراد بشـــركات كبـــرى فـــي الولايـــات المتحـــدة، ممـــن كـــانوا يعملـــون مبـــرمجين ومحللـــي نظـــم، تـــم تســـريحهم مـــن أعمـــالهم للفـــائض الزائـــد بالعمالـــة: فصـــبوا جـــام غضـــبهم علـــى أنظمـــة شـــركاتهم الســـابقة، مقحمـــين لأنظمتهـــا، ومخربين لكل ما تقع أيديهم عليه من معلومات حساسة بقصد الانتقام[٣].

رابعاً: وسائل اختراق البريد الالكتروني (الهاكـــــرز)

نـــود مبـــدئياً أن نشـــير إلـــى أن كلمـــة ((هـــاكر)) لـــم تكـــن تعنـــي شـــيئاً ســـيئاً عنـــد نشـــأتها، ونشـــأة أصـــحابها، فـــي أواخـــر حقبـــة الســـتينات، وفـــي الواقـــع فإنهـــا كانـــت

---

[١] عمـــرو أحمـــد حســـنو، حمايـــة الحريـــات فـــي مواجهـــة نظـــم المعلومـــات، دراســـة مقارنـــة، ط١، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ١٤٣.

[٢] عمرو أحمد حسبو، المرجع السابق، ص ١٤٤.

[٣] محمـــد الشـــهاوي، الاعتـــداء علـــى الحيـــاة الخاصـــة بواســـطة القنـــوات الفضـــائية ووســـائل الإعلام والاتصال، دار النهضة العربية، القاهرة، ط ١، ٢٠١٥، ص ١١١.

تعني في بادئ الأمر: المبرمج العبقري، حيث كان عالم الكمبيوتر لا يزال في مهده، وكانت أجهزته ضخمة، ولم يكن الحاسب الشخصي قد ظهر بعد. فالهاكرز في تلك الفترة كانوا هم المبرمجون الذين يقومون بتصميم أسرع برنامج من نوعه، ويعتبر العبقريان: ((دينيس ريتشي)) و((كين تومسون)) أشهر هؤلاء الهاكرز على الإطلاق – بالمعنى الجيد – لأنهم صمموا برنامج ((يونكس)) وكان يعتبر الأسرع والأقوى وذلك في عام ١٩٦٩.

حتى وقت قريب كان تصنيف برامج التخريب والاختراق الضارة بأنظمة الحاسب ينقسم إلى ثلاثة فروع فقط وهي:

١) الفيروسات
٢) ديدان الإنترنت
٣) أحصنة طروادة

ولكن مع تطور هذه البرامج والتكونولوجيا المستخدمة فيها تم تحديث طريقة التصنيف لبرامج الأشرار والتي تمكن هؤلاء الهاكرز من الوصول إلى أهدافهم. والتصنيف الحديث لبرامج الهاكرز هو كما يلي: [1]

١- برامج سريعة التكاثر والانتشار

وهي الفيروسات وديدان الإنترنت حيث أنها قادرة على التكاثر والانتشار بسعة كبيرة لتصيب أجهزة وبرامج أخرى، والفرق بين الفيروسات والديدان هو أن الفيروس بحاجة إلى أحد البرامج المنتشرة بين المستخدمين لكي يحتضنه وبالتالي يستطيع التكاثر والانتشار عن طريقة، وأشهر مثال على ذلك هو فيروس مليسا وفيروس الحب حيث ان الأخير كان بحاجة إلى برنامج مايكروسوفت أوت لوك كحاضن له، أما الديدان فهي ليست بحاجة إلى أي برنامج لكي يحتضنها. وأشهر مثال على هذا النوع هو دودة ((موري وارم))[٢].

---

[1] محمد الشهاوي، الاعتداء على الحياة الخاصة بواسطة القنوات الفضائية ووسائل الإعلام والاتصال، مرجع سابق، ص ١١٢.

[٢] سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، مرجع سابق، ص ١٦٣.

٢- برامج للتجسس وإرسال المعلومات

تقوم هذه البرامج بجمع كل المعلومات التي يريدها الهاكر وتقوم بإرسال تلك المعلومات إلى مصدر ذلك البرنامج حتى لو كان هناك جدران اللهب التي تحمي الجهاز،و ذلك لقدرة هذا النوع على استغلال نقطة ضعف في معظم أنواع جدران اللهب التي تسمح بخروج وتصدير المعلومات من الجهاز أو الشبكة المحلية بواسطة HTTP AND FTP[١].

٣- برامج التحكم عن بعد والهجوم المنسق

تسمح هذه البرامج للهاكرز – في حال وصولها إلى أي جهاز من الأجهزة – بالتحكم الكامل في الجهاز.أما أشهر الأمثلة على البرامج القادرة على التحكم عن بعد والتي تستطيع تسخير الأجهزة لتنفيذ الهجوم المنسق وتعطيل عمل المواقع المشهورة [٢].

٤- برامج جديدة من أحصنة طروادة تجمع من كل بحر قطرة

هذه البرامج من أخطر أنواع أحصنة طروادة حيث أنها تستفيد من ميزة كل نوع من أنواع البرامج السابقة وذلك بالدمج بين عدة خصائص فمثلاً يكون لها خاصية التكاثر مثل الفيروسات وعدم حاجتها لبرنامج محتضن تماماً مثل الديدان ولديها القدرة على التعامل مع الملفات الصادرة أو الواردة من نوع: ((FTP and HTTP)) تماماً مثل برامج التجسس والنتيجة هي برنامج جديد قادر على تخطي وخداع جدران اللهب وبالتالي جمع ما لذّ وطاب من المعلومات من كلمات عبر وأسماء مستخدمين وأرقام بطاقات الائتمان وكذلك تدمير بعض الملفات وتعديل مهامها التي تملك أسماء نطاقات تجارية (com وnet. وorg)[٣]. ونطاقات محلية في جميع دول العالم تقريباً. وتشير الدراسات إلى أن حوالي ٢٠ في المائة من عمليات التشويه، تتم يوم الأحد.

---

[١] شريف درويش اللبان، تكنولوجيا الاتصال، المخاطر والتحديدات والتأثيرات الاجتماعية، مرجع سابق، ص ١٠٢.

[٢] شريف درويش اللبان ، المرجع السابق، ص ١٠٣.

[٣] جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص ١٨٢.

ويرجع السبب في ذلك إلى أن تغيير الصفحة الرئيسية في موقع معين يوم العطلة الأسبوعية (في معظم دول العالم).[١]

((الوصول إلى هذا البريد، غير ممكن!)) قد تعني الرسالة السابقة أن البريد الذي تحاول أن تزوره، تعرض لهجامت حجب خدمة، خاصة إذا كان واحداً من الموقاع الكبرى، التي يعني ظهور مثل هذه الرسالة في موقعها، خسارة عشرات الآلاف من الدولارات! وقد حدث هذا للعديد من كبريات المواقع في العالم ومن بينها بوابات انترنت شهيرة مثل بوابة ((ياهو))[٢]

توجد عدة أهداف، قد تدفع جهة معينة، أو شخصاً معيناً، إلى القيام بمثل هذه الهجمات، وأهمها:

١- التسلل إلى النظام: يمكن أن يتمكن بعض المخترقين من التسلل إلى النظام وقت انهيارة وحجبه عن الخدمة، أو وقت إعادة إقلاعه، وتوجد عدة طرق لذلك، على مختلف الأنظمة، وهي أحد الأسباب الأكثر منطقية لمثل هذه الهجمات.
٢- أسباب سياسية: قد توجه جهة معينة، مثل هذه الهجمات، إلى موقع حكومي يتبع دولة تعاديها، او موقع شركة تنتمي إلى هذه الدولة، ومن هذا ما حدث من هجمات متبادلة بين المخترقين العرب والصهاينة، وأيضاً الهجمات التي حدثت بين مخترقين صينيين ومواقع أمريكية مؤخراً ويتوقع أن تزداد في المستقبل، الهجمات ذات الأهداف السياسية، مع ازدياد انتشار إنترنت![٣]
٣- أسباب اقتصادية: قد توجه شركة صغيرة مثل هذه الهجمات، إلى شركة كبيرة تسيطر على السوق، في نوع من المنافسة التجارية غير الشريفة!

---

[١] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص ١٤٥.

[٢] أحمد حسام طه تمام ،المرجع السابق، ص ١٤٦.

[٣] جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، النهضة العربية، دون طبعة، ٢٠٠١، ص ١٥٥.

٤- الانتقام: يحدث كثيراً، أن تسرّح شركة أحد الموظفين المسئولين عن إدارة الشبكة. وقد يلجأ بعض هؤلاء، إذا ما شعروا بالظلم، إلى الانتقام من الشركة!

٥- الطبيعة التخريبية: يلجأ بعض الأشخاص إلى مثل هذه الهجمات، لإشباع رغبات تخريبية تتملكهم![١]

وتعتبر هجمات حجب الخدمة الموزعة نوعاً جديداً من هجمات حجب الخدمة العادية التي تعتمد على استخدام برامج معينة في الهجوم، وهذا النوع من الهجمات، هو الذي استخدم في الهجوم على كبرى مواقع إنترنت، مثل ZDNet و Yahoo!، وeBay، وAmazon، وCNN، وغيرها. وتعتمد هذه الهجمات على تجنيد أجهزة كمبيوتر متصلة بإنترنت بدون علم مالكيها وتوجيهها إلى بث الرزم الشبكية إلى مزود معين، بهدف إيقافه عن العمل، نتيجة ضغط البيانات المستقبلية. ويعتمد هذا النوع من الهجمات على وضع برنامج خبيث خاص، من نوع ((حصان طروادة)) (Trojan horse)، في كل كمبيوتر متصل بإنترنت يمكن الوصول إليه، عن طريق إرسال البرنامج بواسطة البريد الإلكتروني، مثلا، وتفعيله على هذه الأجهزة، لتعمل كأجهزة بث للرزم الشبكية، عند تلقيها الأمر بذلك من برنامج محدد يقبع على جهاز أحد المخترقين، ويعتبر هذا النوع من هجمات حجب الخدمة، أكثر الأنواع خطورة، حيث يمكن أن يشكل خطراً على شبكة إنترنت كلها، وليس على بعض المواقع فقط، حيث أن كل موقع من المواقع التي أصيبت في شهر فبراير ٢٠٠١ بهذا النوع من هجمات حجب الخدمة، هي مواقع تحجز جزءاً كبيراً من حزمة البيانات في إنترنت، ما قد يهدد الشبكة بالكامل، وإن حدث ذلك يوماً، فنتوقع أن يشهد العالم أزمة اقتصادية شاملة! وهناك حلول تقنية لمثل هذه الهجمات لكنها شديدة التخصص، ومن غير المستحب عرضها في هذه الدراسة، غير أننا نضع بعض الروابط الخاصة بمعالجة هذا الأمر لمديري المواقع والمعنيين تخصصياً بمثل تلك المشكلات[٢]

---

[١] جميل عبد الباقي الصغير ،المرجع السابق، ص ١٥٦.

[٢] جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص ١٥٨.

المبحث الثاني

أركان الجريمة وعقوبتها

سنبين في هذا المطلب أركان الجريمة وعقوبتها من خلال مطلبين على النحو التالي

المطلب الأول

أركان الجريمة

يتألف بنيان هذه الجريمة من ركنين أحدهما مادي والآخر معنوي.

الركن المادي: يقوم الركن على نشاط إيجابي، ومحل لهذا النشاط.

أولا العنصر الأول السلوك: يتمثل السلوك أو النشاط الإجرامي في دخول الجاني عمدا أو عن طريق الخطأ والبقاء بدون وجه حق أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اختراقه موقع أو بريد الكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة أو لحساب الدولة أو احد الأشخاص الاعتبارية العامة أو مملوكة لها أو يخصها. وقد سبق بيان أفعال الدخول سواء عن طريق العمد أم عن طريق الخطأ، و البقاء بدون وجه حق أو تجاوز حدود الحق المخول للشخص من حيث الزمان أو مستوى الدخول، وكذلك اختراق الموقع أو البريد الإلكتروني. ومؤدى ذلك أن يتجسد النشاط الإجرامي في العناصر التالية:

١- فعل الدخول أو البقاء أو الاختراق على النحو المار بيانه.

٢- أن يكون هذا الدخول إلى موقع أو بريد الكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكة لها أو يخصها.

٣- أن يكون الدخول أو البقاء بغير وجه حق.

٤- أن يحدث السلوك الإجرامي عن طريق شبكة المعلومات أو إحدى وسائل تقنية المعلومات[١].

الركن المنوي: تعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي.

ويتألف القصد الجنائي من عنصرين، هما: العلم والإرادة.

فالعلم يقتضي إدراك الجاني لحقيقة النشاط الإجرامي، وهو دخوله عمدة أو عن طريق الخطأ والبقاء بدون وجه حق أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى

الدخول أو اختراقه موقع أو بريد الكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكة لها أو يخصها.

ويتعين أن يعلم الجاني بخطورة فعله على محل الجريمة الذي ينالله الاعتداء بارتكاب الجريمة، ومن ثم إذا أتي فعله وهو يعتقد أنه لم يدخل أو يتجاوز بغير وجه حق، والتزم حدوده، انتفى عنصر العلم ومعه القصد الجنائي[٢]

كما ينبغي أن تتجه إرادة الجاني إلى أحد الأفعال التبادلية الواردة بالنص، فإذا انتفت هذه الإرادة انتفى القصد الجنائي، كما لو حدث الفعل نتيجة خطأ أو رعونة أو إهمال وخرج على الفور ولم يتحقق البقاء بدون وجه حق أو التجاوز[٣] ولا أهمية للباعث على السلوك الإجرامي؛ إذ لا يعتد القانون باي منها[٤].

---

[١] د. حسني الجندي: المرجع السابق، ص ٢٤٤.

[٢] د. حسني الجندي: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة ص ١٢٣؛ الدكتورة نائلة عادل قورة: جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى ٢٠٠٠، ص ٢٢٢.

[٣] د. احمد محمد خليفة الملط: الجرائم المعلوماتية دار الفكر الجامعي، الطبعة الثانية ٢٠٠٦ ص ٥٤٩

[٤] د. حسني الجندي: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة ص ١٣٨.

المطلب الثاني

عقوبة الجريمة

تنص المادة (١٠) من قانون مكافحة جرائم تقنية المعلومات الاتحادي على أنه:" يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات. وتكون العقوبة السجن والغرامة التي لا تجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين إذا لم تتحقق النتيجة. وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته".

المادة (٢٩) : يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ٢٠ ألف ولا تجاوز ٢٠٠ ألف جنية، أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإليكتروني أو النظام المعلوماتي عرض أي منهم لإحدى الجرائم المنصوص عليها في هذا القانون.ويعاقب بالحبس مدة لا تقل عن ٦ أشهر وبغرامة لا تقل عن ١٠ الاف جنية ولا تجاوز ١٠٠ ألف جنية أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإليكتروني أو النظام المعلوماتي، تسبب بإهماله في تعرض أي منهم لإحدى الجرائم المنصوص عليها في هذا القانون، وكان ذلك بعدم اتخاذه التدابير والاحتياطات التأمينية الواردة في اللائحة التنفيذية.

الخاتمة

تعتبر جرائم إغراق البريد الإلكتروني بالرسائل الاقتحامية، واختراق البريد الإلكتروني من أكثر الجرائم التي تقع على البريد الإلكتروني، ونظراً لخطورة هذا النوع من الجرائم فقد وضع كلاً من المشرعين الإماراتي والمصري قواعد خاصة بالتجريم والعقاب على هذا النوع من الجرائم، وفي نهاية البحث توصلنا لبعض النتائج والتوصيات وهي التالي:

أولاً: النتائج.

١) ويتيح البريد الإلكتروني إمكانية نقل الرسائل بطريقة سريعة للغاية وكلفة المكالمة الهاتفية المحلية وتتوافر في البريد الإلكتروني عوامل الأمان والسرية، فلا يمكن اختراق البريد الإلكتروني شخص إلا بمعرفة كلمة السر الخاصة به أو من خلال طرق فنية معقدة لا يجيدها إلا محترفي عمليات اختراق شبكات الحاسوب

٢) أن من المخاطر التي تتعلق بالبريد الإلكتروني العمل على إغراقه بالرسائل الإلكترونية، وجعل البريد الإلكتروني غرضة للشركات والمؤسسات الدعائية، أو للمحتالين الذي يستخدمون البريد الإلكتروني في اختلاس أموال الآخرين عن طريق مشاريع كاذبة أو حكايات ملفقة.

أ- جرم المشرع الإماراتي إغراق البريد الإلكتروني بالرسائل الاقتحامية في قانون مكافحة جرائم تقنية المعلومات الاتحادي رقم (٥) لسنة ٢٠١٢، والعقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته، كما جرم المشرع المصري في القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن جرائن تقنية المعلومات أيضاً إغراق البريد الإلكتروني بالرسائل الاقتحامية بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من التلف أو عطل أو أبطأ أو اخترق بريدة إلكترونية أو موقعة أو حسابا خاصة بأحاد الناس. الظرف المشدد: إذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة،

تكـــون العقوبـــة الحـــبس مـــدة لا تقـــل عـــن ســـتة أشـــهر، وبغرامـــة لا تقـــل عـــن مائـــة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

ثانياً: التوصيات.

١) لمنـــع اختـــراق البريـــد الإلكترونـــي المداومـــة علـــى تغييـــر كلمـــة الســـر الخاصـــة بالبريـــد الإلكترونـــي دوريـــة، فتغييـــر كلمـــة الســـر الخاصـــة بالمســـتخدم بشـــكل دوري يجعـــل مـــن الصـــعوبة بمكـــان اختـــراق البريـــد الإلكترونـــي، فضـــلا عـــن السماح لأي أحد بالاطلاع على كلمة السر.

٢) يجـــب تعـــديل بعـــض نصـــوص قـــانون مكافحـــة جـــرائم تقنيـــة المعلومـــات المصـــري بحيـــث يتضـــمن مـــواد تـــنص صـــراحة علـــى تجـــريم إغـــراق البريـــد الإلكترونـــي بالرســـائل الاقتحاميـــة أســـوة بالمشـــرع الإمـــاراتي بحيـــث تكـــون هذه الجريمة مستقلة عن غيرها من الجرائم الأخرى.

قائمة المراجع

أولاً: المراجع العربية.

١) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٥

٢) أسامة الحسيني، الشبكة العنكبوتية العالمية -الإنترنت، مكتبة ابن سينا للنشر، بدون سنة نشر

٣) إمام حسانين عطا الله، حقوق الإنسان بين العالمية والخصوصية، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٤

٤) بولين انطونيوز ايوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط١، بيروت، ٢٠٠٩

٥) جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ٢٠٠١

٦) إبراهيم مصطفى، أحمد حسن الزيات، حامد عبد القادر، محمد علي النجار، المعجم الوسيط ، ج ١، المكتبة الإسلامية، تركيا، بدون سنة طبع

٧) جمال الدين محمد بن مكرم بن منظور: معجم لسان العرب، ج ١، دار إحياء التراث العربي، بيروت، ١٩٨٨ م

٨) محمد مرتضى الحسيني: تاج العروس، دار صادر، بيروت، بدون سنة طبع،

٩) إبراهيم مصطفى، أحمد حسن الزيات، حامد عبد القادر، محمد علي النجار، المعجم الوسيط

١٠) محمد محمود المكاوي: الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، المكتبة العصرية للنشر والتوزيع، مصر، ٢٠١٠

١١) د. خالد ممدوح إبراهيم: حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨ م

١٢) أيمن النسور ومحمد الجنيني وأنس أبو طالب، الحاسوب والبرمجيات الجاهزة، (عمان: دار وائل، ٢٠١٣ م)

١٣) ط ٣محمد نصير، الوسيط في الجرائم المعلوماتية، (الجيزة: مركز الدراسات العربية، ٢٠١٥)، ط ١

١٤) حمد خليفة، الحماية الجنائيّة لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، (الإسكندرية: دار الجامعة الجديدة، ٢٠٠٧)، ط ١

١٥) عبد الله ناصر العمري، الحماية الجنائيّة للبريد الإلكتروني – دراسة تأصيلية مقارنة، (رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية، ٢٠١٠)

١٦) يحيى بن شرف النووي، تحرير ألفاظ التنبيه، تحقيق: عبد الغني الدقر، (دمشق: دار القلم، ١٤٠٨ ه)، ط ١
١٧) محمد بن يوسف المواق، التاج والإكليل لمختصر خليل، ط ١، (بيروت: دار الكتب العلمية، ١٩٩٤ م)، ط ١، ج ٧
١٨) محمد بن أحمد بن رشد، بداية المجتهد ونهاية المقتصد، (القاهرة: دار الحديث، ٢٠٠٤)، ط ١، ج ٤
١٩) عبد الرزاق عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة، (دبي: المعهد القضائي، ٢٠١٤)، ط ١
٢٠) حسام الدين كامل: الحق في إحترام الحياة الخاصة، دار النهضة العربية، القاهرة، بدون سنة طبع
٢١) السيد أبو الخير، نصوص المواثيق والإعلانات والاتفاقيات لحقوق الإنسان ، دار إيتراك للطباعة والنشر، القاهرة ، ٢٠٠٥ م
٢٢) عبد الله كريري، الركن المعنوي في الجرائم المعلوماتية في النظام السعودي – دراسة تأصيلية، (رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية، ٢٠١٣)
٢٣) مجيد خضر السبعاوي، نظرية الغلط في قانون العقوبات المقارن، (القاهرة: المركز القومي للإصدارات القانونية، ٢٠١٣ م)، ط ١
٢٤) محمد علي الحلبي، شرح قانون العقوبات – القسم العام، (عمان: دار الثقافة، ٢٠٠٧ م)، ط١
٢٥) محمد شلال العاني، أحكام القسم العام في قانون العقوبات الاتحادي الإماراتي – النظرية العامة للجريمة، (الشارقة – الآفاق المشرقة، ٢٠١٠)، ط ١
٢٦) عبد الحميد بسيوني، رخصة الحاسوب – المعلومات والاتصالات، (القاهرة، دار الكتب العلمية، ٢٠٠٩)، ط ١
٢٧) فهمي الصيرفي، الرخصة الدولية لقيادة الحاسب، (دمشق: دار رسلان، ٢٠٠٩)، ط ١
٢٨) منير الجنبيهي وممدوح الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، (الإسكندرية: دار الفكر الجامعي، ٢٠٠٦)، ط ١
٢٩) حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩ م
٣٠) أيمن عبد الحميد عبد الحفيظ: إستراتيجية مكافحة جرائم إستخدام الحاسب الآلي، بدون مكان طبع، بدون سنة طبع
٣١) محمود نجيب حسني: علاقة السببية في قانون العقوبات، بدون مكان طبع، بدون سنة طبع
٣٢) عبد الحكيم فودة أمام: رابطة السببية في الجرائم العمدية وغير العمدية، دار الفكر الجامعي، الإسكندرية، بدون سنة طبع

٣٣) عبد الفتاح بيومي حجازي: مكافحة جرائم الكومبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦ م
٣٤) د. خالد ممدوح إبراهيم: لوجستيات التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨
٣٥) عمر شريف: درجات القصد الجرمي، دار النهضة العربية، القاهرة، ٢٠٠٢
٣٦) عمر غبراهيم الوقاد: الغلط في القانون في ضوء أحكام القانون الجنائي، المكتبة المصرية، القاهرة، ٢٠٠١ م
٣٧) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، الناشر دار النهضة العربية، القاهرة ٢٠٠٠
٣٨) علي عدنان الفيل، الإجرام الإلكتروني، ط ١، مكتبة زين الحقوقية والأدبية، بيروت، ٢٠١١
٣٩) عماد قادوري، البريد الإلكتروني، خصائصه وبرامجه، دار علاء الدين للنشر، دمشق، ط ١، ٢٠٠٢ م
٤٠) عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل للنشر، ط ١، ٢٠٠٥
٤١) عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دراسة مقارنة، ط ١، دار النهضة العربية، القاهرة، ٢٠٠١ م
٤٢) عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٠
٤٣) محمد الشهاوي، الاعتداء على الحياة الخاصة بواسطة القنوات الفضائية ووسائل الإعلام والاتصال، دار النهضة العربية، القاهرة، ط ١، ٢٠١٥
٤٤) جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، النهضة العربية، دون طبعة، ٢٠٠١

ثانياً: المراجع الأجنبية.

1) Mr. Tariq Banday: Techniques and Tools for Forensic Investigation of E-mail, India, 2011, p. 4,
2) ou ils definissent ie courier electroniquecomme une faculte d"echange asynchrone des messages entre ordinatenrs . p commerce electronigue vuibert ,2000 ,p77.
3) "method pernettant d'echanger des messages ecrits entre differents postes d'un reseau informatique".
4) -F. colantonio, la protection du secret des couriers electroniques en belgique: Aspect techniques, des criminology, 2002, p.9.

5) Report on Electronic Mailing and data protection , commission Nationale Informatique et libertes (CNIL) france, sdopted on October 14.1999 (the CNIL report)
6) John Magee: The law Regulating unsolicited commercial E-mail; An international perspective , computer& high technology law journal, vol.19, 2003. p.335
7) George H.pike: Anti-spam legislation setbacks. Information today, vol 25, December 2008, 17,no 11.
8) Leslie Basse, L'action de la CNIL en matière de lutte contre le Spam, mai 2005, no,53,p.1
9) .Eric Goldman: where's the Beef? Dissecting spam's purported Harms, 11 january 2004, p.3,
10) Dider colin:spamfiletering;optimization Appoaches to content – based filtering , thése de doctorat ,université de Versailles-saint-quentinen-yvelines, 2009,p.81
11) kevinGallot: Anti-spam. Paris, 2004,p,25.
12) Manara (C.), Aspects Juridiques de L'e-mail, Dalloz Affaires, no 140, 1999, p.278.
13) Feral-Schuhl, CH. (2002). Cyber droit, le droit à l'épreuve de l'internet (3eed) Dunod: paris, p129.
14) Mr. Tariq Banday: Techniques and Tools for Forensic Investigation of E-mail, India, 2011, p. 4.
15) Cour d Cassation, Paris, 17 Dec, 2000, Cassation 02 Oct, 2001 .
16) Charles Trapper, Electronic Commerce Strategic, Printed in the USA Edition 2000.p188

ثالثاً: المواقع الإلكترونية.

1) http://www.alittihad.ae/details.php?id=15417&y=2016&article=ful
2) https://www.dxbpp.gov.ae/NewsPage.aspx?ID=826&Type=5
3) (http://www.norton.com or www.symantec.com
4) http://shkoon.coolfreepage.com/amn/pages/hack-mop.html