جامعة المنوفية
كلية الحقوق

الأحكام الموضوعية والإجرائية
لجريمة الاعتداء على البريد الإلكتروني
(دراسة تحليلية في ضوء التشريع الجنائي المصري)

الباحث الدكتور
كمال الدين مصطفى توفيق شعيب

مدرس القانون

بمعهد الألسن العالي للحاسبات ونظم المعلومات

kamalshoeib@yahoo.com

المقدمة

أولًا – موضوع البحث:

إن للتطور التكنولوجي الهائل في مجال المعلومات الذي أسهم بشكل كبير في رخاء البشرية في جوانب عديدة من الحياة، هو نفسه الذي وفر ملاذًا أكثر أماناً لنوع جديد من المجرمين، وهيأ مجالاً خصباً لنمو جرائم جديدة تتسم بالنعومة في ظاهرها وبالخطورة الشديدة في نتائجها المدمرة، إذ تبين وجود كم هائل من الأفعال الجرمية التي وجدت في فضاء الانترنت، وهي في تطور وتزايد مستمر، إلا أن الاعتداء على البريد الإلكتروني يمثل اعتداءً على جانب مهم في الحياة اليومية، وهو الحق في الخصوصية، وتحديداً الحق في سرية المراسلات والاتصالات، ومن ثم كان من الضروري على الأفراد الذين تعرض بريدهم الإلكتروني للاختراق أو الإغراق التبليغ عن هذه الجرائم للجهات المعنية، كذلك ينبغي على الدولة أن تتدخل لوضع حد لهذه الظواهر الإجرامية، وذلك عن طريق إنشاء هيئات متخصصة في مكافحة الجريمة الإلكترونية، أو باستحداث مصالح على مستوى أجهزة مكافحة الجريمة، تعطي الأولوية في التوظيف فيها للمتخصصين في الإعلام الآلي[١].

ونظـرًا للاتسـاع الكبيـر الـذي يشـهده الفضـاء الإلكترونـي، ومـا ترتـب عليـه مـن كثـرة مستخدمي الإنترنـت، تعـددت المخـاطر الناشـئة عـن إسـاءة اسـتغلال البريـد الإلكترونـي كوسـيلة للتواصـل وتبـادل المراسـلات، لـيس فـي اسـتغلاله فقـط فـي ارتكـاب جـرائم إلكترونيـة، وإنمـا تعـدى الأمر إلى ارتكاب الكثير من الجرائم التقليدية من خلال التخطيط لها وتبادل المعلومات والبيانات بشأنها عن طريق البريد الإلكتروني[٢]، إلى حد أن اصبحت الجرائم الإلكترونية تهدد استقرار وسلامة الأفراد والمجتمعات وأمنها[٣].

وتمتد هذه الجرائم إلى حد الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات ذاتها، مما يمثل اعتداءً مباشرًا على حرمة الحياة الخاصة للأفراد والجماعات على حد سواء، من خلال الاطلاع غير المشروع على المحتوى المعلوماتي الخاص بهم.

وقد لعب المشرع المصري دورًا كبيرًا في مواجهة التحديات الراهنة، وما ينتج عنها من محاطر، وذلك من خلال إصدار القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية

---

(١) عبدالحليم محمد الشريف بن مشري، ضرورة تجريم الاعتداء على البريد الالكترونى، مجلة العلوم القانونية، جامعة الزيتونة – كلية القانون ترهونة، السنة ٤، العدد ٧، ٢٠١٦، ص٣١٣.

(٢) د. رامي القاضي، شبكة الإنترنت المظلمة، مجلة الأمن العام، العدد ٢٠٢٥، أكتوبر ٢٠٢١م.

(٣) الإرهاب الإلكتروني الظاهرة والمواجهة، الإصدار الحادي والستون، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، ٢٠١٦م، ص١١.

المعلومات[1]، وكان الهدف من ذلك خلق نوع من التوازن بين الحماية الجنائية لحرمة الحياة الخاصة وما تتضمنه من أحكام موضوعية وإجرائية للتصدي للأفعال غير المشروعة من جهة، وبين ما قد ينشأ عنها من جرائم من جهة أخرى، وبين تحقيق ضمان سرية المعلومات والبيانات الشخصية من جهة ثالثة.

ثانيًا- أهمية البحث:

تكمن أهمية هذا الموضوع في التزايد المضطرد للاستخدام غير المشروع لأجهزة الحاسب الآلي وشبكة المعلومات الدولية، ومن ثم تسليط الضوء على الدور الذي يلعبه قانون مكافحة جرائم تقنية المعلومات المصري في مواجهة جريمة الاعتداء على البريد الإلكتروني، وذلك إعمالًا للأحكام العامة للمادة (٢٧) من هذا القانون، والتي تصدت لمواجهة إساءة استخدام تقنية المعلومات في ارتكاب جميع الجرائم، وقد تصدى المشرع المصري لمواجهة الجرائم الإلكترونية بصفة عامة، وذلك بمقتضى أحكام هذا القانون وما تضمنه من عقوبات رادعة.

حيث إنّ الاستخدام المتزايد للإنترنت، والانتشار الكبير له في في كافة البلدان، أدى إلى بروز عدد كبير من السلبيات، على كافة المستويات الأمنية والاجتماعية والاقتصادية والثقافية والسياسية، فضلًا عن ذلك ظهور العديد من الإشكاليات القانونية، فضلًا عن تطور الأنشطة الإجرامية واتخاذها صورًا إجرامية مستحدثة[2].

ثالثًا- إشكالية البحث:

تبدو إشكالية هذا البحث في التساؤل الرئيسي التالي: ما هي جريمة الاعتداء على البريد الإلكتروني؟ وما هو دور المشرع الجنائي المصري في مواجهتها؟ حيث أخذت هذه الجريمة في التزايد والانتشار في مجالات متعددة، مما أثار قلق المشرع الجنائي للتصدي لهذه الجريمة.

---

(1) الجريدة الرسمية - العدد ٣٢ مكرر (ج) - السنة الحادية والستون ٣ ذى الحجة سنة ١٤٣٩هـ، الموافق ١٤ أغسطس سنة ٢٠١٨م.

(2) د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة الإنترنت - دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩م، ص٩.

رابعًا – أهداف البحث:

يهدف هذا البحث إلى تحقيق العديد من النتائج، من أهمها: الوقوف على مدى كفاية النصوص الجنائية الحالية في مواجهة جريمة الاعتداء على البريد الإلكتروني.

خامسًا – منهج البحث:

المنهج المتبع في هذا البحث، هو المنهج الوصفي التحليلي، الذي يقوم على التشخيص السليم لواقع المشكلة، والوقوف غلى الأسباب الفعلية لجريمة الاعتداء على البريد الإلكتروني، ومدى كفاية النصوص الجنائية الحالية في التصدي لها.

سادسًا – خطة البحث:

في ضوء ما تقدم، فإننا نقسّم خطة هذا البحث إلى مبحثين، وخاتمة، وذلك على النحو التالي:

المبحث الأول: الأحكام الموضوعية لجريمة الاعتداء على البريد الإلكتروني.

المطلب الأول: الأحكام العامة للجرائم الإلكترونية.

المطلب الثاني: أركان جريمة الاعتداء على البريد الإلكتروني والعقوبات المقررة لها.

المبحث الثاني: الأحكام الإجرائية لجريمة الاعتداء على البريد الإلكتروني.

المطلب الأول: مرحلة جمع الأدلة والمعاينة في جريمة الاعتداء على البريد الإلكتروني.

المطلب الثاني: التفيتش والضبط في جريمة الاعتداء على البريد الإلكتروني.

الخاتمة – وتتضمن:

أهم النتائج والتوصيات.

المبحث الأول
الأحكام الموضوعية
لجريمة الاعتداء على البريد الإلكتروني

تمهيد وتقسيم:

ترتب على وجود الإنترنت والنظم الإلكترونية بيد كل شخص وفي كل بيت، فضلًا عن دخولها كافة الجهات العامة والخاصة، ترتب على كل ذلك مزايا إيجابية تمثلت معظمها في توفير الوقت والجهد المبذول في إنجاز الأعمال المطلوبة، والسرعة العالية في في تنفيذ الخدمات المجتمعية المقدمة بشكل أسهل وأيسر عن غيرها من الوسائل التقليدية القديمة، إلا أنه على الرغم من هذه المزايا والإيجابيات، فإن بعض مستخدمي هذه الوسائل، قد استغل تلك التطورات لتحقيق أهدافه الخاصة، بارتكاب سلوك غير مشروع، مما ترتب عليه استخدام الأنظمة الإلكترونية المستحدثة بغرض الوصول إلى المعلومات والبيانات الإلكترونية بطرق ووسائل غير مشروعة، وذلك من خلال الاستخدام غير المشروع لبرامج وتقنيات محظورة بغية تحقيق الأهداف المحظورة،

ولم يتوقف الأمر عند حد الاعتداء على الحياة الخاصة للأفراد فحسب، بل ازدادت الخطورة المترتبة على هذه الصور من الجرائم، إلى حد أنها ترتكب ضد الأعمال الحكومية الرسمية؛ حيث ترتب عليها المساس بأمن البلاد واستقرارها، مما دفع المشرع الجنائي إلى إصدار القوانين التي تنظم استخدام الوسائل الإلكترونية والتصدي لصور الجرائم المرتكبة من خلالها؛ حيث توسع المشرع في صور الحماية الجنائية لأمن الدولة من الداخل ومن الخارج، لضمان عدم المساس بالمصلحة محل الحماية الجنائية تحقيقًا لأمن المجتمع وسلامته، ولقد تعرض المشرع لهذا النوع من أنواع الحماية الجنائية في قانون العقوبات[1]، وفي القانون رقم (١٧٥) لسنة ٢٠١٨م بشأن مكافحة جرائم تقنية المعلومات.

ترتيبًا على ما سبق، فإننا نعرض للأحكام الموضوعية الخاصة بجريمة الاعتداء على البريد الإلكتروني، من خلال مطلبين، وذلك على النحو التالي:

المطلب الأول: الأحكام العامة لجريمة الاعتداء على البريد الإلكتروني.

المطلب الثاني: أركان جريمة الاعتداء على البريد الإلكتروني والعقوبات المقررة لها.

([1]) اردلان نور الدين محمود، أحكام الجرائم الماسة بأمن الدولة في القانون والشريعة الإسلامية، ط١، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٤م، ص٣١.

المطلب الأول

الأحكام العامة

لجريمة الاعتداء على البريد الإلكتروني

الأحكام العامة لجريمة الاعتداء على البريد الإلكتروني من خلال التعرض لمفهوم الجريمة الإلكترونية بوجه عام (فرع أول)، ثم نبين الأساس القانوني لتجريم الاعتداء على البريد الإلكتروني (فرع ثانٍ)، وذلك على النحو التالي:

الفرع الأول

مفهوم الجريمة الإلكترونية

يُعتبر الإنترنت من أبرز تطورات العصر الحالي، بل وأهمها على الإطلاق في تاريخ البشرية، وهي نتيجة اندماج تكنولوجيا الحاسب الآلي من جهة، وتكنولوجيا الاتصال بين الأفراد والأمم من جهة أخرى، وقد تتضعاف أهميتها بسبب الزيادة المضطردة المستخدمين من سائر الجنسيات على مستوى العالم، إلى جانب تزايد الاعتماد على الإنترنت بشكل يومي وبصورة فاقت تخيلات العقل البشري، بحيث أصبحت شبكة الإنترنت هي الأداة التي لا غني عنها للحصول على المعلومات والبيانات بكافة أشكالها وصورها وأيًّا كان نوعها، كما أصبحت تلك الشبكة أداة مهمة من الأدوات التي تسهل الاطلاع على الأخبار والأحداث العالمية في جميع بلدان العالم بسهولة ويسر وبشكل اسرع من البرق في الحصول على المقصود[1].

ومما تجدر الإشارة إليه في هذا الصدد، أنه بالرغم من هذا التقدم التقني فيما يتعلق بنقل المعلومات والبيانات وتداول الرسائل البريدية، واتجاه العديد من البلدان إلى الاعتماد على ما يعرف بالحكومة الإلكترونية، إلا أنه على الرغم من هذه المزايا والإيجابيات لشبكة الإنترنت، إلا أن كثيرًا من المستحدمين قد أساء استخدام هذه الوسائل مما ترتب عليه خطورة بالغة على الحياة الخاصة للأفراد والمجتمعات، من خلال ارتكاب صورة من صور الاعتداء على البريد الإلكتروني.

وهو ما نبيه في الفقرات الآتية:

أولًا – مفهوم جريمة الاعتداء على البريد الإلكتروني.

تُعد تقنية البريد الإلكتروني من أهم وأبرز التطبيقات الإلكترونية المعاصرة المتاحة غبر شبكة المعلومات الدولية، وتتمثل خدمة البريد الإلكتروني من خلال انتقال وتبادل الرسائل بين الأشخاص عبر خاصية البريد الذي تم ربطه بهذه البشبكة، وتتميز الخدمات المقدمة من قبل

---

(1) د. محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، ط١، جامعة نايف للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، ٢٠٠٩م، ص٤٩٤ وما بعدها.

البريد الإلكتروني بسرعتها الفائقة في الانتقال والأداء، مقارنةً بذات السرعة في البريد العادي، كما تتميز بقلة تكاليفها؛ حيث تقتصر تكاليف البريد الإلكتروني على دفع اشتراكات مقابل خدمة التزود بشبكة الإنترنت[١].

وقد عرف المشرع المصري البريد الإلكتروني في القانون رقم (١٧٥) لسنة ٢٠١٨م بشأن مكافحة جرائم تقنية المعلومات في المادة (١) بأنه: "وسيلة لتبادل رسائل إلكترونية على عنوان محدد بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية، أو غيرها من رسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلي وما في حكمها".

وفي الفقه القانوني، يُعرف البريد الإلكتروني باعتباره: العنوان الشخصي لمستخدم الإنترنت، والذي بموجبه يتم تيعيين اسم هذا المستخدم، ويتم تحديد اسم الشركة المضيفة لهذا العنوان[٢]، كما يمكن تعريف البريد الإلكتروني بأنه: الاستخدام المشروع للإنترنت في نقل الرسائل دون اللجوء إلى الطرق التقليدية[٣]، بحيث يتمكن المُستخدم من إرسال الرسائل الإلكترونية إلى شخص أو أكثر من مستخدمي الإنترنت[٤]، وأخيرًا فإنه يمكن تعريف البريد الإلكتروني بأنه: البيانات والمعلومات التي يمكن إرسالها أو استلامها من خلال نظم الاتصالات البريدية الإلكترونية يتضمن ملاحظات مختصرة ذات طابع شكلي حقيقي، ويمكنه استصحاب مرفقات به مثل معالجة الكلمات وأية وثائق أخرى يتم إرسالها برفقة الرسالة ذاتها[٥].

ومن ثم فإن مضمون تعريفات للبريد الإلكتروني سالفة الذكر، باعتبارها العملية التي من خلالها يتم نقل الرسائل والوثائق من حاسب آلي إلى آخر عبر شبكة المعلومات الدولية بغض النظر عن نوع هذه الشبكة، ويتم نقل الرسائل في معظم الأحوال بشكل مجاني، ولا تستغرق عملية الإرسال غير ثوانٍ معدودة، مع ملاحظة وجود برنامج للبريد الإلكتروني لدى مستخدم الإنترنت.

---

(١) د. عبد المنعم يوسف بلال، البريد الإلكتروني، مجلة كمبيوتر، القاهرة، العدد ٦٣، مايو١٩٩٣م، ص١٤.

(٢) د. علي عدنان الفيل، جريمة الاحتيال عبر البريد الإلكتروني – دراسة مقارنة، مجلة الحقوق، الكويت، العدد الثاني، السنة السادسة والثلاثون، يونيو ٢٠١٢م، ص٥٧٥.

(٣) مصعب عبدالله النقبي، جريمة إتلاف محتويات البريد الإلكتروني في التشريع الإماراتي، مجلة جامعة الشارقة للعلوم القانونية، مجلد ٢٠، العدد ٣، جامعة الشارقة، ٢٠٢٣، ص١٣٩.

(٤) د. عبد الله جفعر الكوفلي، مراقبة الاتصالات في التنظيم الدولي والداخلي، المركز القومي للإصدارات القانونية، القاهره، ٢٠١٧م، ص٦٧ وما بعدها.

(٥) د. عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، ٢٠٠٥م، ص١٣.

ونظرًا لأهمية البريد الإلكتروني، جريمة الاعتداء عليه، تعد من صور الجرائم الأكثر ارتكابًا في الوقت الحالي؛ حيث تتسم بالعديد من بمزايا سهولة ارتكابها من قبل المجرمين، مما يدفعهم إلى ارتكاب هذه الجريمة دون عناء، وعلى ذلك، يمكننا تعريف الجريمة الإلكترونيةبأنها: الجريمة التي لا تحترم الحدود الجغرافية (Trans Border)؛حيث يتم ارتكابها من أي مكان في العالم بواسطة الحاسب الآلي المتصل بشبكة الإنترنت، ويرتكبها شخص يكون على دراية تامة بهذا الحاسب والإنترنت، وتعد الجريمة الإلكترونية، من الجرائم التي تتسم بالعديد من الخصائص التي تميزها عن غيرها من الجرائم التقليدية، من حيث وسائل ارتكابها[١] .

وفي سبيل التصدي لهذه الجريمة، فقد سلكت كافة التشريعات الجنائية مسلك التجريم لصور الاعتداء على البريد الإلكتروني، بإصدار القوانين الخاصة بالجرائم الإلكترونية [٢].

وجريمة الاعتداء على البريد الإلكتروني، هي الجريمة التي تقع بواسطة الحاسب الآلي بمشتملاته المتعلقة بالجانب المادي أو بالجانب المعنوي، بالإضافة إلى الجرائم التقليدية التي تطال الجانب المادي للحاسب الآلي[٣].

وقد عرفت المادة (١) الخاصة بالتعريفات من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات، الموقع بأنه: "مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة".

وعلى ذلك يمكن القول بأن الموقع: هو الحيز المتاح على الإنترنت، والذي يتضمن معلومات متوفرة على ما يسمى بالحاسبات المضيفة Hosts[٤].

والمكان الافتراضي، هو ما يبين حقيقة الموقع، وأنه افتراضيًّا وليس حقيقيًّا أو واقعيًّا، كما يُمكن أن يطلق عليه مكان حكمي، والأصل في الموقع أنه يتضمن معلومات، بيد أن ذلك ليس

---

(١) د. منير محمد الجنبيهي، د. ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص١٣.

(٢) د. عبدالله ذيب محمود، جريمة الاختراق الواقعة على البيانات والمواقع الحكومية – دراسة مقارنة على التشريعات الأردنية والفلسطينية، مجلة المنارة للدراسات القانونية والإدارية، عدد خاص حول الثورة الرقمية وإشكالاتها أبريل ٢٠٢٠م، ص١٧٠.

(٣) عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، ٢٠١٤م، ص١٧.

(٤) يُقصد بها: الحاسبات المضيفة، وهي تلك الحاسبات التي تتصل بالشبكة العالمية للمعلومات، وتتميز بالسعة التخزينية العالية، وتقوم بعرض ما تحتويه من بيانات وملفات على شكل صفحات مواقع الشبكة العالمية للمعلومات. انظر في ذلك: ألن نيبارو، الإنترنت، ترجمة: مركز التعريب والبرمجة طبعة الدار العربية للعلوم، ص١١٨.

شرطًا، فقد يوجد الموقع دون أن يتضمن أية معلومات، أو بيانات، وليس لهذا الموقع مكان محدد؛ لأن هذا الأمر خارج عن حقيقة الموقع الإلكتروني المراد تعريفه.

تعريف الشبكة الإلكترونية:

يُقصد بالشبكة التداخل والاختلاط في أي شيء، فيسمَّى كل تداخل واختلاط في اللغة "تشابك وشبكة واشتباك"، وقد عرّفت المادة (١) الخاصة بالتعريفات من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات الشبكة المعلوماتية بأنها: "مجموعة من الأجهزة أو نظم المعلومات مرتبطة معًا، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليه".

أمّا في الفقه، فقد عرفت الشبكة بالعديد من تعريفات من أهمها: أنها ربط مجموعة من الحاسبات الآلية بعضها ببعض، بحيث تشترك هذه المجموعة من الحاسبات في الموارد[١].

ومن جانبنا: نعرف الشبكة بأنها: تداخل الحاسبات الآلية مع بعضها البعض عن طريق موصلات بهدف مشاركة المعلومات.

(١) جريمة الاعتداء على البريد الإلكتروني في القانون:

عرفت المادة (١) الخاصة بالتعريفات من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات اختراق البريد الإلكتروني بأنه: "الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأى طريقة غير مشروعة، إلى نظام معلوماتى أو حاسب آلى أو شبكة معلوماتية، وما في حكمها".

وعلى ذلك تعتبر جريمة الدخول غير المشروع إلى النظام المعلوماتي جريمة خطر وليست جريمة ضرر، ولا يشترط أن يترتب على الدخول غير المشروع أي نتيجة، مثل حدوث ضرر للشبكة أو البيانات أو حدوث فائدة للجاني، وتُعد جريمةً تامةً بمجرد ارتكاب النشاط الإجرامي، وهو التدخل في النظام المعلوماتي دون موافقة صاحبه، حتى وإن لم يجد الجاني في الملفات ما يبحث عنه من معلومات أو بيانات، إلا أن دخول الجاني للنظام المعلوماتي دون أن يكون لديه تصريح بالدخول يُعد انتهاكًا أو اختراقًا لقواعد خصوصية وسائل تقنية المعلومات[٢].

---

(١) د. طارق بن عبد الله الشدي، آلية البناء الأمني لنظم المعلومات، ط١، دار الوطن للطباعة والنشر والإعلام، ٢٠٠٠م، ص١٣٠.

(٢) إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقًا للمرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، ٢٠١٨م، ص١١٦ وما بعدها.

وجريمة اختراق البريد الإلكتروني أو الدخول غير المشروع أو المصرح به إلى الأجهزة الإلكترونية بهدف الاطلاع أو الحذف أو الإتلاف والنسخ أو النقل للبيانات والمعلومات الإلكترونية، بحيث يكون النظام الإلكتروني محلاً لارتكاب الجريمة أو وسيلة لارتكاب جريمة أخرى[1].

وإذا كان من الصعوبة بمكان وضع تعريف دقيق لأي مصطلح قانوني بصفة عامة، فإن ذلك ينطبق – بصفة خاصة – على تعريف الجريمة الإلكترونية، حتى ردد البعض معبرًا عن هذه الصعوبة، بأن الجريمة المعلوماتية تقاوم التعريف، أو أنها فوق مستوى التعريف، أو أنها صعبة التعريف، الأصل إعمالًا للأحكام العامة بشأن التجريم، أن يعمد المشرع إلى تحديد الأفعال التي تكون على مساس مباشر بالمصلحة المحمية، وهو أمر يقتضيه مبدأ شرعية الجرائم والعقوبات، وقد تعددت الاتجاهات الفقهية في وضع تعريف محدد لجريمة تقنية المعلومات، ونعرض في هذا المقام جانبًا من تلك التعريفات الفقهية، وكذا موقف بعض التشريعات المقارنة والتشريع المصري من هذه الجرائم.

وفيما يلي نشير إلى التعريف التشريعي والفقهي لجريمة تقنية المعلومات، وذلك على النحو الآتي:

أولاً – التعريف التشريعي للجريمة المرتكبة بواسطة الإنترنت:

حرصت بعض التشريعات على وضع تعاريف محددة لبيان المقصود بالجرائم المتعلقة بالاستخدام غير المشروع للحاسبات وشبكات المعلومات وتقنية المعلومات.

ولم يضع المشرع المصري تعريفًا محددًا لبيان المقصود بجريمة تقنية المعلومات في القانون رقم (١٧٥) لسنة ٢٠١٨م، غير أنه عرف تقنية المعلومات ذاتها في المادة (١) من القانون ذاته بأنها: "أي وسيلة أو مجموعة وسائل مترابطة وغير مترابطة تستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًّا أو لا سلكيًّا".

وتتبلور فلسفة المشرع المصري في تحديد مفهوم جرائم تقنية المعلومات في ضوء الجرائم التي حددها حصرًا، بالنظر إلى المعلومات ذاتها، سواء باعتبارها محلاً لتلك الجرائم أو أداة في ارتكابها.

---

(١) د. عبدالله ذيب محمود، جريمة الاختراق الواقعة على البيانات والمواقع الحكومية – دراسة مقارنة على التشريعات الأردنية والفلسطينية، مرجع سابق، ص١٧٤.

ثانيًا – التعريف الفقهي للجريمة المرتكبة بواسطة الإنترنت:

ذهب الفقهاء في تعريف الجريمة المعلوماتية إلى مذاهب واتجاهات مختلفة، بالنظر إلى اعتبار تقنية المعلومات إمّا محلاً لارتكاب الجريمة أو أداة لارتكابها، وذهب جانب من الفقهاء إلى تعريف جريمة تقنية المعلومات بأنها: كل استخدام في صورة فعل أو امتناع مشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على أية مصلحة مشروعة، سواء كانت مادية أو معنوية، فهي تمثل الاعتداء الذي يرتكب بواسطة المعلوماتية بغرض تحقيق ربح[١].

ثالثاً– تعريف الجريمة المرتكبة بواسطة الإنترنت بالنظر إلى وسيلة ارتكابها (الحاسب الآلي):

استنادًا لهذا المعيار يرى جانب من الفقه في تعريفهم للجريمة الإلكترونية على أساس وسيلة ارتكابها المتمثلة بجهاز الحاسوب أو الكمبيوتر أو إحدى وسائل التقنية الحديثة المرتبطة به، فتعد الجريمة الإلكترونية متى كان جهاز الحاسب الآلي أو الكمبيوتر وسيلة لارتكابها.

فعرفها البعض بأنها: "الفعل غير المشروع الذي يتورط بارتكابه الكمبيوتر"[٢]، أو أنها: "كل فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الكمبيوتر أو التي تحول عن طريقه"[٣]، وكما عرفها آخر أنها: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب عن طريق الكمبيوتر، وداخلاً بارتكابها"[٤]،

وعلى ذلك، فإن جريمة الاعتداء على البريد الإلكتروني على الشبكة العالمية للمعلومات هي: دخول شخص ما إلى مكان افتراضي موجود على الشبكة العالمية للمعلومات لا يملكه،

---

(١) د. عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، ط١، المركز القومي للإصدارات القانونية، ٢٠١٢م، ص٤٠ وما بعدها.

(٢) د. محمد أمين الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان – الأردن، ٢٠١٥م، ص٨.

(٣) د. لورنس حوامدة، الجرائم المعلوماتية وأركانها وآلية مكافحتها – دراسة تحليلية مقارنة، بحث منشور في مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية، المجلد الرابع، العدد الأول، كانون الثاني، ٢٠١٧م، ص١٨٨.

(٤) د. هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م، ص٨، بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، ط٣، جامعة الإمارات العربية المتحدة، ٢٠٠٤م، ص٤٠٥.

وليس مأذونًا له بذلك، ويقوم بالتصرف في كافة البيانات التي يحتويها، ويشل يد المالك الأصلي من التصرف فيه [١].

رابعاً- تعريف الجريمة المرتكبة بواسطة الإنترنت بالنظر إلى غايتها:

وفي هذا المعيار يرى جانب من الفقه بتعريفهم للجريمة الإلكترونية أنه يستند إلى الغاية التي يُراد في تحقيقها أو ما ينتج عنها مع عدم حصر الجريمة في جهاز الكمبيوتر وحده، وإنما بالتقنية المستخدمة في جميع الأجهزة المعلوماتية، وعرفت وفق هذا المعيار على أنها: "كل فعل إجرامي متعمد أيًا كانت صلته بالمعلوماتية ينشأ عنه خسارة المجني عليه أو كسبًا يحققه الفاعل[٢]، أو هي كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال والحقوق المعنوية"[٣]، أو أنها كل سلوك غير معاقب عليه قانونًا صادر عن إرادة مذنبة، ومحله معطيات الكمبيوتر[٤].

خامساً- تعريف الجريمة المرتكبة بواسطة الإنترنت بالنظر إلى شخصية الجاني:

إذا كان من الصعب وضع تعريف دقيق لأي مصطلح قانوني بصفة عامة، فإن ذلك ينطبق – على وجه الخصوص – على تعريف الجريمة المعلوماتية، حتى ردد البعض معبرًا عن هذه الصعوبة بأن الجريمة المعلوماتية تقاوم التعريف،

سادساً- تعريف الجريمة المرتكبة بواسطة الإنترنت بالنظر إلى موضوع الجريمة:

يذهب جانب من الفقه في تعريفهم جريمة اختراق المواقع الإلكترونية إلى النظر إلى معيار موضوعي، أو بالنظر إلى محل الجريمة، فهم يرون أن الجريمة تكون إلكترونية إذا كان محلها هو الكمبيوتر أو نظامه الإلكتروني، ويُعد من أهم المعايير على قدرة إيضاح تعريف الجريمة محل التعريف، وذهب الفقيه Rosenblatt بتعريفها إلى أنها: نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو التي تحول عن

---

(١) عبد الرحمن بن محمد الدخيّل، اختراق المواقع على الشبكة العالمية للمعلومات – دراسة مقارنة، رسالة ماجستير، جامعة الإمام محمد بن سعود الإسلامي، المعهد العالي للقضاء، المملكة العربية السعودية، ١٤٢٣هـ -١٤٢٤هـ، ص٣٦.

(٢) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط٢، دار النهضة العربية، القاهرة، ١٩٩٨م، ص٦.

(٣) د. عبد الله حسين محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات المنعقد في الفترة ٢٦-٢٨ أبريل ٢٠٠٣م، دبي – الإمارات العربية المتحدة، ص٣.

(٤) د. نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الأردني، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م، ص٣.

طريقه[1]، كما عرفت بأنها: كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات[2].

سابعاً- تعريف الجريمة المرتكبة بواسطة الإنترنت بالنظر إلى الدمج بين عدة تعريفات:

رغم محاولات الفقه في سبيل تلافي الانتقادات الموجهة للتعريفات السابقة، فقد ذهبوا للدمج بين أكثر من تعريف. وذلك بالنظر إلى معيارين: وصف السلوك، واتصال السلوك بالمعالجة الآلية للبيانات أو نقلها،

فنجد أن المشرع المصري[3] تناول تعريف الجريمة في القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات في ثلاثة فصول: تناول في الأول منها جريمة الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات وصورها (جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها)، وجريمة الدخول غير المشروع، وجريمة تجاوز حدود الحق في الدخول، وجريمة الاعتراض غير المشروع، وجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، وجريمة الاعتداء على البريد الإلكتروني أو الموقع أو الحسابات الخاصة، وجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، وجريمة الاعتداء على سلامة الشبكة المعلوماتية. وفي الفصل الثاني تناول الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات وصورها، وجرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني، والجرائم المتعلقة باصطناع المواقع والحسابات الخاصة بالبريد الإلكتروني. وفي الفصل الثالث تناول الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع.

وفي ضوء هذه المفاهيم للجريمة الإلكترونية، يمكن القول، إن الجريمة المرتكبة بواسطة الإنترنت، تعتبر جريمة خطر، وليست جريمة ضرر، إذ لا يشترط أن يترتب على الدخول أي

---

(١) د. هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، مرجع سابق، ص٤٠٧.

(٢) د. هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، ط١، دار النهضه العربية، القاهره، ١٩٩٢م، ص٢٤.

(٣) ومما تجدر الإشارة إليه في هذا الصدد، أن المشرع المصري قد تناول هذا الموضوع في عدد من التشريعات الخاصة، ذات الصلة بوسائل الجريمة المعلوماتية، ومن هذه التشريعات، قانون مصلحة الأحوال المدنية رقم (١٤٣) لسنة ١٩٩٤م، وكذلك قانون غسل الأموال رقم (٨٠) لسنة ٢٠٠٢م، وقانون الملكية الفكرية رقم (٨٢) لسنة ٢٠٠٢م، وقانون تنظيم الاتصالات رقم (١٠) لسنة ٢٠٠٣م، وقانون التوقيع الإلكتروني رقم (٣٥) لسنة ٢٠٠٥م، وعرفت الفقرة (أ) من المادة الأولى من القانون الأخير بشأن الكتابة الإلكترونية بأنها: "كل حروف أو أرقام أو رموز أو أية علامات أخرى تثبت على دعامة إلكترونية أو ورقية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك".

نتيجة، بمعنى أن هذه الجريمة تُعد جريمةً تامةً بمجرد ارتكاب النشاط الإجرامي، فهي من الجرائم التي تقوم بمجرد ارتكابها ولا يشترط تحقق نتيجة هذا الفعل[١].

ثامناً- خصائص جريمة الاعتداء على البريد الإلكتروني وصورها:

تتسم جريمة الاعتداء على البريد الإلكتروني بالعديد من الخصائص، كونها من الجرائم الإلكترونية، فإنه يغلب عليها ما يغلب على هذه الأخيرة، وتتميز بذات الخصائص التي تتميز بها الجرائم الإلكترونية بوجه عام، كما أن جريمة الاعتداء على البريد الإلكتروني، لا تأخذ صورة واحدة، إنما تأخذ صورًا مختلفة حال ارتكابها، ولما كانت جريمة الاعتداء على البريد الإلكتروني، صورة من جرائم الحاسب الآلي، وهذه الأخيرة جرائم حديثة النشأة ظهرت بعد ظهور الحواسب الآلية والأنظمة الإلكترونية، وذلك لتعلقها بتكنولوجيا المعلومات، مما أدى إلى جعل هذه الجرائم صعبة الفهم وغامضة، نتيجة ثورة تكنولوجيا المعلومات والتقدم العلمي الذي شهده العالم خلال العقدين الماضيين، من استغلال العالم للتطور التقني لوسائل التكنولوجيا الحديثة والحواسب الآلية، فكانت الاستفادة من التطور التكنولوجي للحواسب الآلية للأفراد في حياتهم الشخصية، وللحكومات أيضًا؛ حيث اتجهت أغلبية الحكومات في العالم الي إنشاء ما يسمَّى بالحكومات الإلكترونية (E – Government)، وأصبحت تقدم العديد من خدماتها الإلكترونية وبأقل تكلفة[٢].

ولقد انفردت الجرائم الإلكترونية بخصائص وميزات ميزتها عن الجرائم التقليدية؛ نظرًا لطبيعتها التي ترتكب في بيئة غير تقليدية تقع خارج إطار الواقع المادي الملموس يُطلق عليها البيئة الإلكترونية من حيث إنها تكتسب خصوصية غير عادية، وهي جرائم جديدة في شكلها ووسائلها ومخاطرها بلون وثوب جديدين، وهذه الخصائص سنتناول أهمها، وذلك على النحو الآتي:

(١) جريمة الاعتداء على البريد الإلكتروني جريمة عالمية عابرة للحدود: أطلق على شبكة الإنترنت الإمبراطورية التي لا تغيب عنها الشمس[٣]، فبعد ظهور هذه التقنية أذيبت كافة الحدود

---

(١) إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقًا للمرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)، مرجع سابق، ص٢٨.

(٢) عبد الله محمد الحضري، جريمة الدخول بغير وجه حق إلى المواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطري – دراسة تحليلية مقارنة، رسالة ماجستير، كليّة القانون – جامعة قطر، ٢٠٢٠م، ص٧.

(٣) د. محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، مايو ٢٠٠٠م، ص٢٢.

الجغرافية الفاصلة بين دول العالم، ولم تعد تخضع لنطاق إقليمي محدود، ولم تعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات، فأسفر نقل وتبادل المعلومات بين أنظمة الكمبيوتر لأماكن متباعدة إلى نتيجة مؤداها أن أماكن متعددة في دول العالم المختلفة قد تتأثر بالجريمة الإلكترونية الواحدة في نفس الوقت، فالجريمة الإلكترونية لا تعترف بحدود، وهي شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين جميع الدول[١].

(٢) سهولة ارتكاب جريمة الاعتداء على البريد الإلكتروني: تمتاز الجريمة الإلكترونية بصورة واضحة في أسلوب ارتكابها، فالجرائم التقليدية يتطلب ارتكابها مجهودًا عضليًّا كالعنف والإيذاء بعكس جريمة الاعتداء على البريد الإلكتروني، التي يتطلب ارتكابها أسلوبًا هادئًا، فهي لا تحتاج لعنف؛ لذا تُعد جرائم ناعمة، وأطلق عليها بعض الفقه مصطلح جرائم ذوي الياقات البيضاء[٢]،

(٣) جريمة الاعتداء على البريد الإلكتروني ترتكب بعيدًا عن الأنظار: تتصف الجرائم الإلكترونية بأنها مستترة، فالمجني عليه لا يلحظها مع أنها تقع أثناء وجوده على الشبكة، فالجاني يرتكبها بخفة شديدة، ودون أن يرى أطرافها (سواء الجاني أو الضحية)، فيقوم الجاني بالتعامل مع نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الكمبيوتر[٣]، كما أن الضحية لا يشاهد مرتكب الجريمة (الجاني) فقد تُعد مربحة للجاني، وفي ذات الوقت مكلفة على الضحية، مما يتسبب بإلحاق أضرار مالية بليغة بحقه، مقارنة بما يمكن أن تتسبب به الجريمة التقليدية، فهي جرائم فنية تقنية في الغالب الأعم، والجاني يكون من ذوي الاختصاص في مجال التقنية والتعامل مع شبكات الكمبيوتر أو بيانات مجمعة ومجهزة للدخول للنظام الإلكتروني بغرض معالجتها إلكترونيًّا بما يُمكِّن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة، وهذه العمليات وثيقة الصلة بارتكاب الجرائم، ولا بد من ذكاء وفهم الجاني عند ارتكابها[٤].

(٤) جريمة الاعتداء على البريد الإلكتروني من الجرائم المستمرة: تتنوع الجرائم المستمرة، بحيث يكون لكل نوع منها مدلول محدد،؛ وذلك نظرًا لطبيعة هذه الجريمة، وتفرق أفرادها في أماكن جغرافية متباعدة، هذا بالإضافة إلى أن جريمة الاعتداء على البريد الإلكتروني، لا تخلف خلفها أية آثار مادية؛ بحيث لا يمكن تتبعها بسهولة للوصول إلى الجاني، فهي مجرد أرقام تتغير في السجلات الرقمية بصفة دائمة ومستمرة، وهذه الصعوبات تؤدي إلى ضعف قوى الرصد والمتابعة

---

(١) د. خالد ممدوح إبراهيم، الجريمة المعلوماتية، ط٢، دار الفكر الجامعي، الإسكندرية، ٢٠١٩م، ص٨٨.

(٢) د. أسامة أحمد المناعسة، وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة، ط٣، دار الثقافة للنشر والتوزيع، عمان – الأردن، ٢٠١٧م، ص٩٧.

(٣) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م، ص٤٢.

(٤) د. أحمد خليفة الملط، الجرائم المعلوماتية، ط٢، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص١٠٥.

لدى الأجهزة الأمنية، وهو ما يؤدي بدوره إلى استمرارية جريمة الاعتداء على البريد الإلكتروني، مع المزيد من المناورات والتحركات[١].

(٥) جريمة الاعتداء على البريد الإلكتروني يصعب اكتشافها وإثباتها: تقع جريمة الاعتداء على البريد الإلكتروني في بيئة افتراضية تقنية لا تترك ولا تخلف أية آثار ملموسة؛ إذ يغلب طابع السرية عليها، فالجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق التلاعب بالبيانات، التي تتحقق بغفلة عن المجني عليه، مما يصعب معه الحصول على دليل مادي لمثل هذه الجرائم، التي يحيط بها كثير من الصعوبات المتمثلة في صعوبة اكتشافها، فهي لا تترك أثرًا خارجيًّا؛ حيث يغلب عليها الطابع التقني[٢].

ومما يزيد من صعوبة اكتشاف جريمة الاعتداء على البريد الإلكتروني، ذلك أن كثيرًا من هذه الجرائم لا يتم الإبلاغ عنها من المجني عليه خاصة شركات ومؤسسات الأعمال، إمّا لعدم اكتشاف الضحية، أو خشية من التشهير[٣]، فيصعب معرفة مرتكبها فهي ترتكب في بيئة افتراضية، فلا يترك مرتكبها آثارًا؛ مما يزيد الأمر صعوبة على المحقق الجنائي التقليدي في فهم حدودها وما تخلفه من آثارها غير المرئية، ذلك أن الدليل الإلكتروني لهذه الجرائم، يُعد وسيلة الإثبات لإمكانية تعقب أثر مرتكبها، فهذه الوسيلة من السهوله طمسها وإخفاؤها أو تدميرها؛ إذ لا تتقيد بالزمان والمكان، فملاحقة مرتكبها يكون بحاجة إلى تعاون دولي حقيقي[٤].

(٦) جريمة الاعتداء على البريد الإلكتروني تعتمد على استخدام التقنية الرقمية لارتكاب الجريمة: لقد دأب مرتكبو الجرائم المعاصرة على مواكبة التطورات العلمية والتكنولوجية، واستخدام وسائل الاتصالات الحديثة؛ حيث تعتمد جريمة الاعتداء على البريد الإلكتروني على هذه الوسائل الإلكترونية، وبمعنى أدق فهم يستعملونها، كحلقة وصل لربط أجهزتهم الرقمية مع الشبكات المعلوماتية؛ بغية استهدافها، من خلال الحاسب الآلي المتصل بشبكة الإنترنت؛ وهو ما كان ملجأً أمنًا لكثير من المنظمات الإجرامية في إنشاء العديد من المواقع.

---

(١) د. عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في محكافحة جرائم الإرهاب المعلوماتي، بحث ضمن دورة تدريبية بعنوان: مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من: ١١-١٤٢٧/٣/١٥هـ، الموافق ٩- ٢٠٠٦/٤/١٣م، المغرب – القنيطرة، ص٩ وما بعدها.

(٢) د. نبيل عبد المنعم جاد، أسس التحقيق والبحث الجنائي العلمي، مطبعة كلية الشرطة، القاهرة، ٢٠٠٥م، ص٣٧٣.

(٣) د. محمود عبد العزيز أبو زيد، الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية، رسالة دكتوراه، كلية الحقوق – جامعة القاهرة، ٢٠١٦م، ص١٦٦.

(٤) د. عبد الإله النوايسة، جرائم تكنولوجيا المعلومات – شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط١، دار وائل للنشر والتوزيع، عمان – الأردن، ٢٠١٧م، ص٨٠.

(٧) جريمة الاعتداء على البريد الإلكتروني من الجرائم الخطرة: هذه الخاصية من أهم خصائص جريمة الاعتداء على البريد الإلكتروني، وهي خاصية ليست مستقلة بذاتها، بل مكملة للخاصية التي سبقتها؛ حيث إن استعمال التقنيات الحديثة، هي التي بها قوام الحياة، بحيث لا يمكن بحال الاستغناء عنها، فإن استخدامها بأساليب سيئة أو ضارة، أدت إلى ظهور نوع من الإجرام المُستحدث، الذي يهدد العالم بأكمله،

(٨) مرتكب جريمة الاعتداء على البريد الإلكتروني في الغالب شخص خبير في مجال الإلكترونيات: مرتكب جريمة الاعتداء على البريد الإلكتروني، هو شخص على دراية تامة، ولديه خبرة كبيرة واطلاع واسع في مجالات استخدام الكمبيوتر؛ لارتكاب جريمته الإلكترونية عبر شبكة الإنترنت، مما يجعله يمتلك قدرات خارقة في التحكم والسيطرة على برامج الكمبيوتر، بقصد تحقيق أهدافه[١] .

(٩) جريمة الاعتداء على البريد الإلكتروني تستهدف النظم المعلوماتية: تكمن الأهداف الأساسية جريمة الاعتداء على البريد الإلكتروني، في الحصول على المعلومات والبيانات الإلكترونية، المحفوظة على أجهزة الكمبيوتر، أو المنقولة عبر شبكة المعلومات الدولية؛ حيث تساعدها هذه المعلومات في كيفية الوصول إلى أهدافها الإجرامية[٢].

(١٠) جريمة الاعتداء على البريد الإلكتروني من الجرائم الناعمة: فإذا كانت الحريمة التقليدية تتطلب استخدام الأدوات أحيانًا، غير أن الجرائم المتصلة بالكمبيوتر تتميز بأنها جرائم ناعمة لا تتطلب عنفًا، فنقل بيانات من كمبيوتر إلى آخر أو السطو الإلكتروني على أرصدة بنك ما، لا يتطلب أي عنف، كما أن هناك العديد من الجرائم التقليدية اتخذت منعطفًا جديدًا مع ظهور الإنترنت، مثل الجرائم ضد الأطفال والجرائم المالية، وأبرزها جريمة الاعتداء على البريد الإلكتروني [٣].

---

(١) المرجع السابق، الموضع نفسه.

(٢) عبد الله علي عبد الله القحطاني، إدارة أمن المعلومات ودورها في الحد من الإرهاب الإلكتروني بكلية الحاسبات وتقنية المعلومات بجامعة الملك عبد العزيز بجدة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض – المملكة العربية السعودية، ١٤٣٨هـ/٢٠١٧م، ص٣٦.

(٣) د. صباح كزيز، سمير قط، أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجًا، مخبر أثر الاجتهاد القضائي على حركة التشريع – كلية الحقوق والعلوم السياسية، جامعة محمد خيضر – بسكرة، الجزائر، مجلة الناقد للدراسات السياسية، العدد الثالث، أكتوبر ٢٠١٨م، ص١٢٣.

ثانيًا – صور جريمة الاعتداء على البريد الإلكتروني:

تقسّم الجرائم الإلكترونية عامة إلى جرائم الاعتداء على الأشخاص، وجرائم الاعتداء على الأموال، وهي الصور الأكثر شيوعًا لجرائم الكمبيوتر[١]، وهو ما نبينه فيما يلي:

(١) الجرائم الإلكترونية المرتكبة الواقعة على الأموال:

أسفر الواقع المعاصر عن أن الجرائم المرتكبة على الأموال والاتصالات من أخطر الجرائم الإلكترونية المستحدثة؛ كون هذه الجرائم تؤدي للكثير من الخسائر المادية الضخمة، فالجرائم التقليدية لا تتم إلا بالسطو على المؤسسات المالية أو الشركات، وهي بذلك تحتاج إلى تخطيط مسبق ومجهود عضلي جماعي بخلاف الجرائم المالية الإلكترونية، التي تتم بسهولة، فكل ما تحتاجه أن يتوافر لدى الجاني الدراية الكافية ببرامج الكمبيوتر، كما أنها لا تحتاج لمجهود جماعي، بل يكفي أن يرتكبها شخص أو اثنان لوقوعها[٢]، ومن الجرائم الواقعة على الأموال كجرائم الاحتيال والاعتداء على بطاقات البنوك[٣]، والخدمات وأدوات الدفع الإلكترونية[٤].

(٢) الجرائم الإلكترونية الواقعة على الأشخاص:

كافة جرائم الكمبيوتر ليست فقط جرائم أموال، بل يمكن تصورها أيضًا كجرائم أشخاص ترتكب باستخدام جهاز الكمبيوتر أو أجهزة الاتصالات، ويكون محلها الأشخاص، ومن ذلك على سبيل المثال: جرائم القذف والسب والاعتداء على الحياة الخاصة[٥] والإخلال بالآداب العامة[١]،

---

(١) د. يونس عرب، جرائم الإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل، مقدمة إلى مؤتمر الأمن العربي، ٢٠٠٢م، المنظم بالمركز العربي للدراسات والبحوث الجنائية، أبوظبي، في ١٠/١٢/٢٠١٢م.

(٢) د. محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية شرطة دبي، يناير ٢٠٠٤م، ص١٢ وما بعدها.

(٣) د. هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق، ص١١٤ وما بعدها؛ د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص١٠٥.

(٤) ومنه ما نصت عليه المادة (٢٣) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات المصري على أن: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه، ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكتروني".

(٥) نصت المادة (٢٥) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات على أن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه، ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من اعتدى على أيٍّ من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل

بالإضافة إلى جريمة التهديد والابتزاز عبر الشبكة المعلوماتية، التي أصبحت أجهزة الكمبيوتر والاتصالات توفر لها أسلوبًا وموضوعًا جديدًا، فكثير من القضايا التي يشهدها العالم، وتمثلت بصورة تهديد وابتزاز عبر الشبكات أو داخل المؤسسات المجني عليها، ويتحقق ذلك من خلال الرسم والكتابة والقول، وهذا ما تناولته المادة ٣٠٦ مكرر من قانون العقوبات المصري على تجريم كل من يتعرض للغير في مكان عام أو خاص أو مطروق بإتيان أمور أو إيحاءات أو تلميحات جنسية أو إباحية، سواء بالإشارة أو القول أو الفعل بأية وسيلة بما في ذلك وسائل الاتصالات السلكية أو اللا سلكية.

الفرع الثاني

الأساس القانوني

لتجريم الاعتداء على البريد الإلكتروني

تُعد جريمة الاعتداء على البريد الإلكتروني من صور الجرائم المعاصرة التي تم النص عليها من قبل المشرع المصري[٢]، والتي تأتي في الإطار العام للدخول غير المشروع إلى الأنظمة الإلكترونية، التي يُراد به مجرد الاطلاع بصورة غير مشروعة، أو حذف البيانات والمعلومات[٣]، أو نسخ أو إضافة أو نشر أو تعديل أي بيانات أو معلومات على النظام الإلكتروني. ولما كانت جريمة الاعتداء على البريد الإلكتروني – على نحو ما سبق بيانه –

الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات أخبارًا أو صورًا، أو ما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أم غير صحيحة".

(١) نصت المادة (٢٦) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات على أن: "يُعاقب بالحبس مدة لا تقل عن سنتين، (=) (=) ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه، ولاتجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامه، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه".

(٢) قد يكون محل الاعتداء الأنظمة الموجودة على جهاز حاسوب، أو يمكن أن يكون الحاسوب كوسيلة للاعتداء على أشخاص آخرين، للمزيد انظر: د. هيثم عبدالرحمن البقلي، الجرائم الإلكترونية الواقعة على العرض، ط١، دار العلوم للنشر والتوزيع، مصر، ٢٠٢٠م، ص١٥؛ د. غادة نصار، الجرائم الإلكترونية، ط١، دراسات في الإعلام، مصر، ٢٠١٧م، ص٥.

(٣) للمزيد حول مفهوم المعلومات والبيانات انظر: د. محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، ط١، كتاب الجمهورية، مصر، ٢٠١٠م، ص١٣.

بحيث يكون النظام الإلكتروني محلاً لارتكاب الجريمة، أو أنه وسيلة لارتكاب جريمة أخرى[1]، وقد أشار المشرع المصري إلى الدخول غير المشروع إلى البيانات والمواقع دون تحديد الطبيعة القانونية لهذه البيانات أو تلك المواقع، وقد حدد المشرع محل جريمة الاعتداء على البريد الإلكتروني، بحيث تشمل هذه المواقع بيانات شخصية أو حكومية، أمّا في الحالة التي يكون فيها الدخول مشروعًا، كأن يكون الموظف المختص، أو المستخدم المسؤول هو من قام بالدخول إلى النظام أو الموقع الإلكتروني، ففي هذه الحالة لا تقوم أي جريمة بل يعتبر الفعل مشروعًا؛ حيث إن الدخول المشروع، كما قد تم بناء على إذن مسبق.

فما هو الأساس القانوني لجريمة الاعتداء على البريد الإلكتروني؟ وهو ما نبينه على النحو الآتي:

أولًا- الأساس القانوني لجريمة الاعتداء على البريد الإلكتروني:

ذهب الفقه إلى القول بإمكانية إخضاع النصوص العقابية التقليدية الخاصة ببعض الجرائم، كجريمة السرقة وجريمة خيانة الأمانة، وجريمة دخول ملك الغير على جريمة الاعتداء على البريد الإلكتروني، إلا أن هذه المحاولة لم يكتب لها النجاح؛ لما فيها من تشويه المبادئ المستقر عليها، والتي تقوم عليها هذه الجرائم؛ حيث إن النصوص التقليدية لا تؤمن الحماية الجنائية الكافية للمال المعلوماتي؛ والذي يختلف بطبيعته عن المال التقليدي، والقول بغير ذلك، يؤدي إلى ثغرة في نظام حماية الأموال المعلوماتية، فقد تتشابه جريمة الدخول بغير وجه حق إلى النظم المعلوماتية مع بعض الجرائم التقليدية، مثل جريمة السرقة وجريمة دخول ملك الغير.

ومع ذلك، فإن لجريمة الاعتداء على البريد الإلكتروني ، أساسها القانوني في التشريع الجنائي المصري؛ حيث أراد المشرع من التشريعات الجنائية الخاصة بالجرائم الإلكترونية، تحقيق الردع العام، والذي يتمثل في إنذار الجاني والناس كافة – عن طريق التهديد بالعقاب – بسوء عاقبة الإجرام كي يجتنبوه، وحماية المجتمع بمنع عودة الجاني إلى ارتكاب سلوكه الإجرامي مرة أخرى، وإنذار الجميع بسوء العاقبة متى فعلوا مل فعل.

ومن جانبنا نرى: أن الجرائم الإلكترونية بوجه عام، وجريمة الاعتداء على البريد الإلكتروني خاصة، هي جريمة الأجيال القادمة، وهو ما يدعونا إلى القول بضرورة تتضافر جهود المشرع الجنائي لمكافحة هذا النوع من الجرائم الخطرة والضرب بيد من حديد على مرتكبيها.

المطلب الثاني

أركان جريمة

الاعتداء على البريد الإلكتروني والعقوبات المقررة لها

تمهيد وتقسيم:

يستلزم النموذج القانوني لجريمة الاعتداء على البريد الإلكتروني، ضرورة توافر ركنيها المادي والمعنوي إعمالًا للأحكام العامة الواردة في قانون العقوبات المصري.

وهنا يشترط للقول بوجود جريمة ما، ضرورة توافر ركنيها المادي والمعنوي، فإذا كانت الجريمة من الجرائم العمدية يشترط توافر القصد الجنائي، القائم على علم الجاني وإرادته ارتكاب الجريمة، تأسيسًا على ما تقدم، فإنه متى اتجهت إرادة الجاني إلى ارتكاب جريمة ما، وهو على علم تام بنتيجة سلوكه الإجرامي بأن قام لديه هذا القصد، وقامت مسئوليته الجنائية عمَّا قام به من أنشطة، ومن ثم تقوم مسئوليته الجنائية متى كان عالمًا بما صدر منه واتجهت إرادته إلى هذا الفعل، ورغمًا عما تقدم، فإنه يتعين علينا معرفة الطبيعة القانونية لهذه الجرائم، والتي تفترض أن هناك من جهة من يقوم بإعداد المواد التي يمكن بثها بولسطة الإنترنت، سواء من قبل أشخاص طبيعية أو أشخاص اعتبارية، كالهيئات والمؤسسات عامة كانت أو خاصة ومن أمثلتها الجامعات العلمية ومراكز البحث العلمي، وأيضًا الوزارات والمؤسسات الحكومية، وهناك من يقوم بتوفير هذه الخدمة للمتعاملينInternet service provider سواء كانوا من الأفراد أو الشركات أو المؤسسات البحثية أو المكتبات، ولذلك يثور التساؤل عن طبيعة المسئولية الجنائية لكلٍّ منها، وهل يمكن القول إن المسئولية عمَّا يبث بطريق الإنترنت يعد جريمة إعمالًا لأحكام التشريعات الجنائية يُسأل عنها كل من قام بإنتاج أو توريد الخدمة، أم أن مسؤولية من قام بتوريد الخدمة تختلف عن مسؤولية من قام بإنتاجها؟[1].

ومن نافلة القول، العلم بأن تكنولوجيا المعلومات أصبحت في الآونة الأخيرة ركيزة أساسية لأهداف التطور في كافة نواحي الحياة، بما تتضمنه من أنشطة متنوعة، سواء اقتصادية أو اجتماعية أو سياسية أو زراعية أو صناعية، ولقد أدى الاستخدام المطرد للإنترنت – سواء في شكل أموال معلوماتية أو أساليب مستحدثة – إلى ظهور ما يُعرف بالإجرام المعلوماتي، وهو نتيجة حتمية لكل تقدم علمي أو تقني مستحدث، ويرتكز الإجرام الإلكتروني بوجه عام على

([1]) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص٥٣.

محورين، أحدهما: ضد المال، والآخر: ضد الأشخاص، مستمدًا نشاطه من الإمكانيات الهائلة للحاسب الآلي[1].

وفي ضوء ذلك سوف نتحدث عن أركان جريمة الاعتداء على البريد الإلكتروني، والعقوبات المقررة لها، في فرعين على النحو الآتي:

الفرع الأول: أركان جريمة الاعتداء على البريد الإلكتروني.

الفرع الثاني: العقوبات المقررة لجريمة الاعتداء على البريد الإلكتروني.

الفرع الأول

أركان جريمة الاعتداء على البريد الإلكتروني

جريمة الاعتداء على البريد الإلكتروني كأية جريمة يشترط لقيامها توافر ركني الجريمة المادي والمعنوي، حتى يمكن القول بقيام مسؤولية الجاني، وفي ضوء ذلك نتحدث عن أركان جريمة الاعتداء على البريد الإلكتروني، من خلال حديثنا عن ركنها المادي، والمعنوي، وذلك على النحو الآتي:

أولًا – الركن المادي لجريمة الاعتداء على البريد الإلكتروني:

يتمثل هذا الركن في ماديات الجريمة، أي: الصورة المادية التي تظهر بها الجريمة في الواقع[2].

ولا يوجد اختلاف بين جريمة الاعتداء على البريد الإلكتروني عن نظائرها من الجرائم الأخرى، فهي تتكون من نشاط إجرامي يرتكبه الجاني، ونتيجة إجرامية تترتب على ذلك النشاط الإجرامي، وعلاقة سببية تربط بينهما، ويتحقق السلوك الإجرامي المكوّن للركن المادي للجريمة محل البحث من خلال ثلاث صور، حددها النص على سبيل الحصر، تتمثل في الإنشاء أو الإدارة أو الاستخدام، وأن يكون هذا السلوك على موقع أو حساب خاص على شبكة معلوماتية؛ بهدف تسهيل ارتكاب جريمة معاقب عليها قانونًا، فإن جريمة الاعتداء على البريد الإلكتروني، تقوم بأفعال الإنشاء أو الإدارة أو الاستخدام لأيٍّ من المواقع أو الحسابات الخاصة على الشبكة المعلوماتية، بهدف ارتكاب أو تسهيل ارتكاب أيٍّ من الجرائم المنصوص عليها قانونًا.

وأمام ما تقدم، يواجه نص المادة (٢٧) كافة صور السلوك الإجرامي المتمثلة في إنشاء أو إدارة أو استخدام مواقع إلكترونية أو حسابات خاصة، بهدف ارتكاب أو تسهيل ارتكاب جريمة الاعتداء على البريد الإلكتروني .

---

(1) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص٤٥.

(2) د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، ط٨، دار النهضة العربية، القاهرة، ٢٠١٦م، ص٥٢.

النشاط الإجرامي: هو ذلك النشاط المادي الملموس الذي يظهر إلى الحيز الخارجي ليبين لنا ما كان مكنونًا في نفس الجاني، علمًا بأن قانون العقوبات لا يُعاقب على ما يدور في النفس من رغبات أو شهوات أو أفكار لنوايا إجرامية، طالما أن ذلك لم يظهر إلى الحيز الخارجي بشكل يُستدل عليه، وينقسم السلوك إلى نوعين: سلوك إيجابي وسلوك سلبي، ويُراد بالسلوك الإيجابي كل سلوك ذو مظهر مادي يحدث تغييرًا في العالم الخارجي، أمّا السلوك السلبي فيراد به امتناع الجاني عن القيام بفعل إيجابي محدد، كان المشرع يتطلب منه القيام به في ظروف معينة، إلاّ أنه امتنع عن القيام به بإرادته، وفيما يخص جريمة اختراق الموقع الإلكتروني، تجدر الإشارة إلى أن دخول الجاني إلى الموقع الإلكتروني بشكل غير مصرح به قد يكون عن طريق فك كلمة السر أو المرور الخاصة بالموقع الإلكتروني، والتي لا يعلمها إلا المسؤول عن إدارته، أو قد يكون دخول الجاني عن طريق استعمال برامج خبيثة يتم دمجها مع نظام تشغيل الموقع الإلكتروني، بحيث تعمل كجزء منه أثناء تشغيل النظام، لتقوم بتسجيل كلمة السر أو المرور التي يستخدمها المسئول عن إدارة الموقع الإلكتروني، والذي يعرف بأنه كل شخص طبيعي أو معنوي يكون له الحق في الدخول إلى نظام الموقع الإلكتروني التابع له لتحديد محتواه أو مضمونه وكيفية تنظيم عمله[١].

وقد نص المشرع المصري في القانون رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات، على حظر بعض أفعال الاعتداء على المعلومات الرقمية، والتي تمثل في حقيقتها صورًا للركن المادي في جريمة الاعتداء على البريد الإلكتروني، ومن شأنها أن ترتكب بسلوك إيجابي أو سلبي.

ويتحقق الركن المادي لجريمة الاعتداء على البريد الإلكتروني، بمجرد القيام صورة من صور انتهاك سرية المعلومات وخصوصية الحياة الخاصة، حتى لو لم يترتب على الفعل أي نتيجة، فالجريمة سلوكية يكتفي فيها المشرع بتحقق السلوك الإجرامي بدون اشتراط تحقق نتيجة؛ لأن الغرض من التجريم هو الحفاظ على سرية وخصوصية البيانات، وليس تحقق نتيجة إجرامية، ويُعتبر مدى توافر الأمان للبيانات على الإنترنت أمر بالغ الأهمية؛ حيث إنه كلما زاد معدل الأمان في تداول البيانات زاد معه معدل الأمن الاجتماعي[٢].

ويتحقق الركن المادي في الجرائم المرتكبة بواسطة الإنترنت بعدة صور، منها: استخدام تقنية الأنظمة المعلوماتية في إيقاع الضرر أو الفعل المادي، ولا بد في هذه الحالة لقيام الركن

---

(١) د. دلال لطيف مطشر، جريمة الاعتداء على المواقع الإلكترونية – دراسة مقارنة، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٦، العدد ٩، ٢٠١٨م، ص٣٩٩ وما بعدها.

(٢) د. ياسر نوار، المواجهة التشريعية والأمنية لجرائم التجارة الإلكترونية، ط١، بدون دار نشر، ٢٠١٢م، ص٧١.

المادي من ارتباط السلوك الإجرامي بنطاق، أو خلال مجال إلكتروني، ولا يُشترط في جريمة الاعتداء على البريد الإكتروني الإنترنت تحقيق الضرر؛ حيث إن جريمة الاعتداء على البريد الإلكتروني من الجرائم الشكلية، التي يكفي لقيامها ارتكاب النشاط الإجرامي، وذلك بإتيان السلوك أو الفعل الإيجابي، من جانب فرد أو مجموعة أفراد أو جماعة منظمة، بقصد إحداث تخريب أو

ويكون ذلك بالتأثير على مادة الشيء على نحو يذهب أو يق خلل في المواقع الرسمية للدولة، ومن ثَمَّ فإن الجاني (المجرم الإلكتروني) هو المسؤول عن كافة النتائج المتوقع حدوثها، نتيجة لنشاطه الإجرامي؛ حتى ولو اشتركت عوامل أخرى بشكل مباشر أو غير مباشر في إحداث الضرر، ما دامت هذه العوامل لم تتداخل في قطع الرابطة السببية، بين الجاني والنتيجة المترتبة على سلوكه الإجرامي.

ويمكن لنا أن نتصور صور النشاط الإجرامي الكفيل بقيام جريمة الاعتداء على البريد الإلكتروني وإظهارها إلى الواقع المجتمعي ليظهر أثرها، كجريمة تستوجب المساءلة عليها، ومن الممكن اختراق الحاسبات الآلية أو انتحال هوية مستخدمي تلك الحاسبات، إمّا ماديًّا أو إلكترونيًّا، ويسمح الاختراق المادي للبريد الإلكتروني بدخول الجاني إلى مناطق خاضعة للسيطرة عن طريق بوابات إلكترونية أو آلية، وأسلوب اختراق البريد الإلكتروني الأكثر شيوعًا أن يقف شخص غير مسموح له بالدخول أمام البوابات المغلقة، حاملاً بين ذراعيه متعلقات خاصة بالحاسبات الآلية – كالشرائط الممغنطة على سبيل المثال – أو أن ينتظر حتى يتقدم شخص مسموح له بالدخول، ويفتح له الباب فيدخل معه في نفس الوقت، ولذا يمكن القول بأن التواجد في صالات الحاسب الآلية، هو أمر حتمي لارتكاب هذه الجرائم، وينطوي السلوك غير المشروع فيه على البيانات أو المعلومات المخزنة في نظم المعلومات[1].

ثانيًا – الدعاية لكيفية فك الشفرة للأجهزة الإلكترونية الخاصة بمؤسسات وهيئات الدولة:

من خلال تشفيرها، والتحكم في البيانات والمعلومات الخاصة بالدولة وتعطيلها أو تغيير هيئاتها وما شابه ذلك، مما يلحق بها ضررًا بالغًا.

ومن الممكن تحقق عنصر الاختلاس – كأحد مكونات الركن المادي في السرقة – بفعل مادي يتمثل في توصيل Branchement جهاز فك الشفرة القرصان بجهاز الاستقبال (Recepteur)، فهذا التحليل غير صحيح؛ لأن التوصيل غير المشروع لا يهدف إلى نوع حيازة المالك بالنسبة للبرامج التي يستمر في بثها، ولا يمنع مشاهد التليفزيون المشترك، من استقبال

---

(1) د. محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦م، ص١٤٤.

البرامج بشكل عادي وطبيعي، فجهاز فك الشفرة هو – بحسب المحكمة – أداة لتحسين استقبال البرامج، والتي من حق المشاهد أن يتلقاها بحالتها.

ثانيًا – إتلاف البرامج وتخريب المواقع الرسمية للدولة: لل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له، وبمفهوم آخر: إحداث أفعال مادية بالشيء محل الجريمة يكون من شأنها الإنقاص من مكوناته أو أدائه أو كفاءته[1].

ثالثًا – التحريض الإلكتروني على الاعتداء على البريد الإلكتروني:

هو الدفع بالجاني أو حثه أو خلق فكرة الجريمة لديه أو الوعد والوعيد أو التشجيع أو الترويج أو التحبيذ أو الدعوة عبر وسائل التقنية، سواء أكان – ذلك التحريض – شفويًا أو كتابة أو بأية وسيلة ممكنة، وسواء أكان بشكل صورة مرئية بالفيديو أو رسالة على صفحة الإنترنت، أو بالبريد الإلكتروني، كموقع أو مستقر أو رسالة عبر هذه الوسائل المتعددة الخواص الفنية، وذات التقنية العالية، كالشبكات والمواقع والإنترنت والجوال، والمدونات المتعلقة بصفحات الإنترنت، والصوت والصورة الرقمية، والملفات المخزنة في الحاسب، ومزود الخدمة[2].

رابعًا – التجسس على البريد الإلكتروني: يُقصد بالتجسس في هذا الموضع:

"الاطلاع على المعلومات الخاصة بالدولة، والمؤمنة في جهاز آخر، وليس مسموحًا لغير المخولين بالاطلاع عليها؛ حيث أثر الفضاء الإلكتروني على الأدوات الاستخباراتية، وسهل القدرة على جمع المعلومات والتنصت والتجسس، إضافة إلى تسهيل النشاطات السرية في العلاقات الدولية، كعملية الاغتيالات نتيجة تزايد العلاقة بين التكنولوجيا والأمن؛ إذ تقوم مؤسسات استخباراتية خاصة باجتذاب القراصنة للاستفادة من خدماتهم في التعاقد مع شركات كبرى تسعى للحصول على معلومات مهمة عن منافسيها، وتقوم شركات أخرى بتوظيفهم وتوجيههم لإلحاق الضرر المادي والمعنوي بالمنافسين من خلال تدمير ثقة عملائهم بهم، كما أصبح هؤلاء القراصنة سلاحًا مؤثرًا في أوساط العصابات الإجرامية؛ حيث يتم استغلالهم للتجسس ولنشر رسائلهم الترويجية عبر الإنترنت، كما يمكن توظيفهم من قبل الدول من أجل التخطيط أو القيام بهجمات إلكترونية، أو لجمع المعلومات عن الجهات والدول المعادية، وعلى ضوء هذه الحقائق مجتمعة ينبغي التعامل مع هؤلاء المخترقين على أنهم يشكلون تهديدًا لأمن الدول، وفي الوقت الذي يؤكد الخبراء فيه صعوبة خوض معركة حاسمة مع هذه الفئات؛ لذا يجب على كافة الدول توظيف عدد كبير من الخبراء الذين لهم الخبرة الفنية والتقنية لمواجهة

([1]) د. محمد الشهاوي، شرح قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣، ط١، دار النهضة العربية، القاهرة، ٢٠١٠م، ص١٩٩.

([2]) التحريض الإلكتروني، وزارة الداخلية المصرية، أكاديمية الشرطة، مركز بحوث الشرطة، الإصدار التاسع والأربعون، ٢٠١٤م، ص٣٥.

الجوسسة الإلكترونية، وبذلك يمكن القول بأن شبكة الإنترنت سهّلت الأعمال الجاسوسية بشكل كبير؛ حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عمليات التجسس في عصر المعلومات ثلاثة أهداف رئيسية، وهي التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي[١].

خامسًا – جريمة الاعتداء على البريد الإلكتروني:

وذلك بقصد تعريض المجتمع والأمن للضرر أو الخطر، والذي يترتب عليه الإخلال بالنظام العام للدولة، ومن أمثلته: التلاعب بالأنظمة الإلكترونية للمرور والسكك الحديدية وتعطيل القطارات؛ مما يحدث الفوضى والذعر بين أفراد المجتمع، ويؤدي إلى ارتكاب حوادث تعرض حياة الأفراد للخطر والهلاك[٢].

سادسًا – جريمة الاعتداء على البريد الإلكتروني بقصد إلحاق الضرر بالبيئة:

وهلاك النسل والحرث، ومن أمثلة ذلك: العبث بالأنظمة الإلكترونية لضخ المياه في السدود[٣].

سابعًا – جريمة الاعتداء على البريد الإلكتروني:

بقصد الإضرار بموارد البلاد الاقتصادية والتنموية؛ مما يعرضها للخطر، ومن أمثلة ذلك: التلاعب والعبث بأرصدة البنوك والحسابات النقدية، التي يسفر عنها تحويل الأموال إلى جهات مجهولة، والإضرار بالاقتصاد القومي للبلاد[٤].

ثامنا – جريمة الاعتداء على البريد الإلكتروني:

بقصد تعطيل الأنظمة الإلكترونية الخاصة بوسائل الاتصالات بهدف التغطية على أعمال إجرامية، أو إخفائها وعدم الكشف عنها، أو محو أو شطب بيانات قد تُساعد على كشف مخططات إجرامية[٥].

---

(١) د. صباح كزيز، د. سمير قط، أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجًا، مرجع سابق، ص١٣٠.

(٢) د. موسى مسعود أرحومة، الإرهاب والإنترنت، مجلة دراسات وأبحاث، جامعة الجلفة – الجزائر، العدد الرابع، ٢٠١١م، ص١٧٧.

(٣) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي – دراسة تأصيلية، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٤م، ص١٠٢.

(٤) المرجع السابق، الموضع نفسه.

(٥) المرجع سابق، ص١٠٢.

تاسعًا- ممارسة أي أعمال إلكترونية أخرى، من شأنها تعريض نظام الحكم في البلاد للخطر[١].
عاشرًا- ممارسة أي أعمال إجرامية من شأنها، التأثير أو تغيير الكيان الاقتصادي أو التأثير على التوافق المجتمعي، أو إحداث اضطراب في الأوضاع الاقتصادية للمجتمع[٢].

حادي عشر - ومن أهم مظاهر جريمة الاعتداء على البريد الإلكتروني:

ما يسمَّى بالقذف الإلكتروني؛ ومن خلاله يتم إرسال الآلاف من الرسائل الإلكترونية الموجهة إلى أفراد المجتمع، بحيث لم يعد بمقدور هذه الأفراد تجاهل استقبال هذه الرسائل، وقد سقط العديد من المؤسسات والهيئات الكبرى ضحية لهذا النوع من صور الاعتداء على البريد الإلكتروني، مما أثار الرعب والخوف والذعر والهلع لدى الجماهير المتعاملين مع هذه المؤسسات؛ ويتعمد المخترقون إخفاء مصدر هذه الرسائل؛ وذلك باستعمال عناوين وأسماء وهمية؛ بحيث يصعب كشفهم ويستحيل التعرف عليهم[٣].

ثاني عشر- انضمام المخترقين إلى مواقع التواصل الاجتماعي وغزوها:

وذلك بالنظر إلى فاعلية هذه المواقع، في تحقيق أهدافهم المتنوعة؛ وذلك من خلال النظر إلى فعاليته وتحقيق الأهداف المختلفة، من تقديم البيانات والمعلومات التي تخص كيفية عمل وصناعة القنابل والقيام بالعمليات القتالية، مع تقديم كافة المعلومات للمنتسبين الجدد، والقيام بالدعاية والإعلان، واستخدام هذه المواقع كبنك للمعلومات[٤].

ثالث عشر- محل جريمة الاعتداء على البريد الإلكتروني:

يتمثل الهدف الرئيسي في جريمة الاعتداء على البريد الإلكتروني، في الاعتماد على الآثار التي تخلفها هذه الجريمة؛ حيث ينتج عنها إيقاع الهلع والفزع وإثارة الرعب بين أفراد المجتمع، وهو وحده يكفي لقيام الركن المادي واعتبار هذه الجريمة، جريمة الاعتداء على البريد الإلكتروني؛ فلا بد أن يؤدي سلوك الجاني إلى مثل هذه النتائج، ولا يشترط أن يقع بالفعل، وإنما يكفي وجود درجة احتمال وقوعه، وعلى ذلك تعد جريمة الاعتداء على البريد الإلكتروني من

---

(١) د. عمر حوتية، وآخرون، تجربة دولة الإمارات في التصدي للجرائم المعلوماتية الواقعة على التجارة الإلكترونية - المجلة الأردنية للمكتبات والمعلومات - جمعية المكتبات والمعلومات الأردنية - الأردن، المجلد ٥٠ العدد ٤، كانون الأول ٢٠١٥م، ص١٤١.

(٢) د. محمد قيراط، الإعلام الجديد والإرهاب الإلكتروني، آليات الاستخدام وتحديات المواجهة، مجلة الحكمة للدراسات الإعلامية والاتصالية - مؤسسة كنوز الحكمة للنشر والتوزيع - الجزائر، العدد التاسع، يناير ٢٠١٧م، ص٢٤ وما بعدها.

(٣) د. موسى مسعود أرحومة، الإرهاب والإنترنت، مرجع سابق، ص١٧٨.

(٤) د. محمد قيراط، الإعلام الجديد والإرهاب الإلكتروني: آليات الاستخدام وتحديات المواجهة، موجع سابق، ص٢٥.

جرائم الخطر، والتي يكفي فيها إيقاع العقاب على الجاني دون النظر إلى النتيجة التي تحققت بالفعل، بل إن مجرد ارتكاب النشاط الإجرامي الذي يراد به تحقيق النتيجة – نفسيًّا وماديًّا – فيمكن القول بتوافر الركن المادي، وعلى ذلك فإن تحقق الغرض من هذا السلوك قائم، وتحقق الرعب مرتبط بتحقق الفعل[1].

رابع عشر – الركن المعنوي لجريمة الاعتداء على البريد الإلكتروني:

تعتبر الأفعال التي يتم من خلالها إنشاء أو إدارة أو استخدام موقع أو حساب خاص على الإنترنت بغية ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها إعمالًا لأحكام المادة (٢٧) من قانون مكافحة جرائم تقنية المعلومات المصري، تعتبر هذه الجريمة من الجرائم العمدية، التي يلزم للقول بقيام مسئولية من يرتكبها ضرورة توافر القصد الجنائي العام، المكون من عنصري العلم والإرادة؛ وهما كما يلي:

(١) العلم: حيث يشترط علم الجاني بجميع العناصر الأساسية التي يلزم توافرها حتى تكون الجريمة مكتملة الأركان والشروط، وفقًا للنص الجنائي الذي حدد هذه الأركان[2]، وفي الوقت ذاته يدرك الجاني حقيقة نشاطه الإجرامي، والذي يتمثل في إنشاء أو إدارة أو استخدام موقع إلكتروني أو إدارة حساب من الحسابات الخاصة على الإنترنت، لتحقيق أهداف غير مشروعة نتيجة لسلوكه المجرم قانونًا.

(١) الإرادة: حيث تعتبر الإرادة هي العنصر الثاني من عناصر القصد الجنائي في جريمة الاعتداء على البريد الإلكتروني، وإذا كان علم الجاني ضروريًّا ولازمًا، إلا أنه لا يكفي وحده للقول بوجود القصد الجنائي، ومن ثم فإن توافر القصد الجنائي في جريمة الاعتداء على البريد الإلكتروني، يشترط فيه اتجاه إرادة الجاني إلى ارتكاب نشاطه الإجرامي المتمثل في إنشاء أو إدارة أو استخدام موقع أو حساب خاص بغرض الاعتداء على البريد الإلكتروني، وفي الوقت ذاته اتجاه إرادة الجاني إلى تحقيق أهدافه الإجرامية.

أمام ما سبق، يشترط لوجود الركن المعنوي في جريمة الاعتداء على البريد الإلكتروني ضرورة توافر القصد الجنائي العام لهذه الجريمة، وهو ما يعني انصراف إرادة الجاني إلى تحقيق سلوكه الإجرامي، مع علمه بعنصريه العلم والإرادة، وهو ما يغني أن جريمة الاعتداء على البريد الإلكتروني لا تتطلب قصدًا خاصًا بها؛ حيث يعاقب الجاني عليها باعتبارها جريمة من الجرائم

---

(١) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي دراسة تأصيلية، مرجع سابق، ص١٠٣.

(٢) د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، الكتاب الأول، ط٦، دار النهضة العربية، القاهرة، ٢٠١٦م، ص١٦٩.

التي تقوم بذاتها بمجرد توافر القصد الجنائي العام، سواء توافر لدى الجاني قصد ارتكاب جريمة الاعتداء على البريد الإلكتروني أو لم يتوافر ذلك القصد[١].

ترتيبًا على ذلك، فإن القصد الجنائي في جريمة الاعتداء على البريد الإلكتروني، هو ذاته الركن المعنوي في هذه الجريمة، ويمكن القول بتوافر هذا القصد متى علم الجاني بصفة الجريمة وحقيقتها وعناصرها القانونية، وما يمكن أن يترتب على ارتكابها من نتائج، ومن ثم فإن القصد الجنائي، هو المعيار الذي من خلاله يمكن تُقدير العقوبة المناسبة للجرم المرتكب.

والقصد الجنائي العام في التشريع المصري، هو ما يتوافر فيه العمد، أو اتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل، إذا كان هذا الارتكاب أو الامتناع يجرّمه القانون، ويقصد من وراء ذلك إحداث نتيجة إجرامية مباشرة، أو أي نتيجة أُخرى من النتائج التي يجرّمها القانون، ويكون الجاني قد توقع حدوثها، ولم ينص المشرع المصري في قانون العقوبات صراحةً على تعريف القصد الجنائي، **ويرى الباحث:** أن المشرع المصري – في اعتقادنا – لم يساير التشريعات المقارنة، التى نصت على تعريف القصد الجنائى صراحةً.

ويرى الباحث: أنه لمعرفة مدى توافر القصد الجنائى من عدمه، يجب الرجوع إلى القانون؛ حيث يشير المشرع إلى تطلب القصد للركن المعنوي صراحة، وذلك ببعض الألفاظ، كالعمد على سبيل المثال، وقد استخدم المشرع المصري في قانون العقوبات لفظ القصد بمشتقاته (يقصد، بقصد) للدلالة على القصد الجنائي، وذلك في أكثر من ستين موضعًا[٢].

---

(١) د. إبراهيم عبدالخالق، الشامل في جرائم الإنترنت في ضوء قانون العقوبات، المكتب الفني للإصدارات القانونية، القاهرة، ٢٠٢١م، ص٧٦.

(٢) من ذلك ما نصت عليه المادة (٨٠) فقرة (١)؛ حيث نصت على أن: "يُعاقب بالإعدام كل من سلم لدولة أجنبية أو لأحد ممن يعملون لمصلحتها أو أفشى إليها أو إليه بأية صورة وعلى أي وجه، وبأية وسيلة سرًا من أسرار الدفاع عن البلاد، أو توصل بأية طريقة إلى الحصول على سر من هذه الأسرار بقصد تسليمه أو إفشائه لدولة أجنبية أو لأحد ممن يعملون لمصلحتها، وكذلك كل من أتلف لمصلحة دولة أجنبية شيئًا يعتبر سرًا من أسرار الدفاع، أو جعله غير صالح لأن ينتفع به"، والمادة (٨٠) (أ)، والتي نصت على أن: "يُعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن ١٠٠ جنيه ولا تجاوز ٥٠٠ جنيه. ١. كل من حصل بأية وسيلة غير مشروعة على سر من أسرار الدفاع عن البلاد ولم يقصد تسليمه أو إفشاءه لدولة أجنبية أو لأحد ممن يعملون لمصلحتها. ٢. كل من أذاع بأية طريقة سرًا من أسرار الدفاع عن البلاد.٣ـ كل من نظم أو استعمل أية وسيلة من وسائل التراسل بقصد الحصول على سر من أسرار الدفاع عن البلاد أو تسليمه أو إذاعته. وتكون العقوبة السجن إذا وقعت الجريمة في زمن الحرب"، وما ورد بالمادة (٩٠) وغيرها من مواد قانون العقوبات المصري.

الفرع الثاني

العقوبات المقررة

لجريمة الاعتداء على البريد الإلكتروني

نـص الدسـتور المصـري ٢٠١٤م، علـى المبـدأ العـام الـذي يقضـي بشـرعية الجـرائم والعقوبات، والذى يقضي بشكل واضح على أنه: لا جريمة ولا عقوبة إلا بناء على نص قانوني، وعلى ذلك لا يمكن القول بأن هذا الفعل أو ذاك يؤثمه القانون إلا إذا كان هناك نص سابق على وقوعه يمنع ارتكابه ويفرض له عقوبة[١] ، وكان من الواجب أن يحدد المشرع السلوك الإجرامي وعناصره تحديدًا جيدًا، على نحو لا يدع معه للقاضي سلطة تحكمية تعطيه الحق في التدخل لتحديد هذه العناصر، فيحل – القاضي – بذلك محل المشرع في أحكامه التي يصدرها[٢]، فالقاضي ليس بإمكانه أن يكيف فعلاً ما بأنه جريمة ما لم يوجد نص قانوني يجرمه، ولا يمكن القول بتجريمه ما لم يوجد هذا النص، حتى ولو كانت قناعة القاضي أن هذا الفعل لا يتوافق مع مبادئ للعدالة أو الدين أو الأخلاق، أو أن يكون من شأن هذا الفعل إلحاق أضرارٍ بالغَةٍ بالفرد والجماعة[٣] .

ترتيبًا على ما تقدم، فإن التوسع في تفسير النصوص العقابية الخاصة بجريمة الاعتداء على البريد الإلكتروني، تعد خرقًا واضحًا لمبدأ شرعية الجرائم والعقوبات، ومبدأ التفسير الضيق للنصوص التي تقضي بالعقوبة المقررة[٤].

وأمام ما سبق يرى الباحث، أنه يجب ملاحقة مرتكبي الجرائم المستحدثة بوجه عام، وجريمة الاعتداء على البريد الإلكتروني بوجه خاص بإصدار المزيد من القوانين الجنائية التي تحقق الردع العام؛ لمواكبة التطور المذهل في الجرائم الإلكترونية، وبوجه خاص متى علمنا أن هذه الجرائم في زيادة مستمرة.

وحيث إن استمرار عدم قدرة القواعد العقابية التقليدية وعجزها عن مكافحة جريمة الاعتداء على البريد الإلكتروني، مرده أن الجريمة الإلكترونية ترتبط بمال قانونى معنوى جديد،

---

(١) حيث نصت المادة (٩٥) من الدستور المصري الحالي ٢٠١٤ على أن: "العقوبة شخصية، ولا جريمة ولا عقوبة إلا بناء على قانون، ولا توقع عقوبة إلا بحكم قضائى، ولا عقاب إلا على الأفعال اللاحقة لتاريخ نفاذ القانون".

(٢) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، مرجع سابق ص٩.

(٣) د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، مرجع سابق، ص٨٠.

(٤) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، مرجع سابق، ص٢٥.

على الرغم من تعلقه بالعديد من الأشياء المادية التي تتجسد في وسائل التكنولوجيا التي يتم من خلالها معالجة البيانات، كالحاسب الآلي[1].

وفي هذا الشأن كان للمشرع المصري دوره من خلال العقوبات الواردة في القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات؛ حيث أحسن المشرع المصري صنعًا في هذا القانون؛ إذ حدد الأفعال التي تمثل خطورة وضررًا للأنظمة الرقمية وأدواتها المختلفة، والتي تؤدي في نهاية الأمر إلى جريمة الاعتداء على البريد الإلكتروني، مع الإشارة إلى العقوبات المرتبطة بارتكاب أيٍّ من صور الاعتداء على البريد الإلكتروني[2].

ولقد حدد المشرع المصري العقوبات الواجب إقرارها على من يرتكب جريمة من الجرائم الإلكترونية – ومنها جريمة الاعتداء على البريد الإلكتروني – المنصوص عليها في هذا القانون، وتمثلت هذه العقوبات في عقوبة الحبس والغرامة والسجن المؤقت باعتبارها عقوبات أصلية، وعقوبتي المصادرة وإبعاد الأجنبي باعتبارها عقوبات تبعية.

وأمام ما سبق، يرى الباحث أن تنوع العقوبات التي قررها المشرع المصري ما بين العقوبات الأصلية والتبعية، هو مسلك حسن من جانب المشرع الجنائي المصري، لتحقيق مبدأ التناسب بين الجريمة والعقوبة المقررة لها.

تأسيسًا على ذلك، نعرض بإيجاز لكل نوع من هذه العقوبات، وذلك فيما يلي:

أولًا – العقوبات الأصلية المقررة لجريمة الاعتداء على البريد الإلكتروني:

لم يعرف المشرع المصري للعقوبة الأصلية، ولكنه اكتفى فقط بالإشارة إلى أنواعها.

والعقوبات الأصلية لجريمة الاعتداء على البريد الإلكتروني، هي العقوبات التي تم النص عليها؛ بوصفها العقوبات الأساسية المناسبة لجريمة الاعتداء على البريد الإلكتروني، والتي تحقق بذاتها ردعًا مباشرًا، وتفي بفكرة القصد من وضع العقوبات.

وما يعنينا في هذا الشأن، ما ورد في القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات من عقوبات، وهي عقوبة السجن المؤبد والسجن المؤقت

---

(١) د. محمد عيد الغريب، مدى انطباق الأحكام العامة في قانون العقوبات على المشاكل القانونية التى كشف عنها استخدام وسائل التكنولوجيا (الحاسب الإلكتروني)، في الدورة المنعقدة بمركز الأستاذ الدكتور/عبد الرؤوف مهدى للبحوث الجنائية بكلية الحقوق، جامعة المنصورة – مصر، يوم السبت الموافق ٢٠١٢/٣/١٧م، ص٤.

(٢) د. عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، المجلد رقم (٢٤) – العدد رقم (٩٥) أكتوبر، ٢٠١٥م، ص٤٣.

والحبس والغرامة؛ وهو ما يفهم منه أن العقوبات الأصلية قد تكون عقوبة سالبة للحرية، وقد تكون عقوبة مالية، وهو ما نبينه فيما يلي:

العقوبات السالبة للحرية: عاقب المشرع المصري بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد على ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين جزاءً لكل من أنشأ أو أدار أو استخدم موقعًا أو حسابًا خاصًا على شبكة معلوماتية، بهدف ارتكاب جريمة معاقب عليها قانونًا[١] .

وإدراكًا من المشرع لأهمية الدليل الإلكتروني وحجيته في الإثبات، فقد عمد إلى حماية تلك الأدلة من العبث بها أو إتلافها أو إخفائها؛ وقد بدا ذلك فيما قرره المشرع بموجب المادة (٢٨) من القانون ذاته، بأن عاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين، وذلك في مواجهة كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي، إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات، وذلك حال وقوعها على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة، وبشأن مجابهة البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات، فقد قرر المشرع بحسب المادة (٢٢) من القانون بعقوبة الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه، ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو صنع أو أنتج أو استورد أو صدر أو تداول بأية صورة من صور التداول، أية أجهزة أو معدات وأدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أيٍّ منها في ارتكاب أو تسهيل ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء[٢].

وقد نصت المادة (٢٠) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات، على أن: "يُعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخوّل له من

---

(١) مساعد بن عبد العزيز بن إبراهيم، عقوبة الغرامة في الشريعة والقانون وتطبيقاتها في اللجان الجمركية بمدينة الرياض، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، ٢٠٠٢م، ص٦٥.

(٢) المرجع السابق، ص٦٦ وما بعدها.

حيث الزمان أو مستوى الدخول، أو اخترق موقعًا أو بريدًا إلكترونيًّا أو حسابًا خاصًا أو نظامًا معلوماتيًّا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها. فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التى لا تقل عن مائة ألف جنيه، ولا تجاوز خمسمائة ألف جنيه. وفى جميع الأحوال، إذا ترتب على أىٍّ من الأفعال السابقة إتلاف تلك البيانات أو المعلومات، أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى، أو تدميرها أو تشويهها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كليًّا أو جزئيًّا، بأية وسيلة كانت، تكون العقوبة السجن والغرامة التى لا تقل عن مليون جنيه، ولا تجاوز خمسة ملايين جنيه".

يُلاحظ الباحث من نص هذه المادة آنفة الذكر، أن المشرع وضع حدًا أدنى لعقوبة السجن.

وقد حدد المشرع المصري، العقوبات السالبة للحرية في هذه الجريمة؛ حيث يُعاقب بالحبس مدة لا تقل عن سنتين: كل من دخل عمدًا، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخوّل له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا إلكترونيًّا أو حسابًا خاصًا أو نظامًا معلوماتيًّا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها، ويُعاقب بالسجن: إذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، ويُعاقب بالسجن: إذا ترتب على أيٍّ من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى، أو تدميرها أو تشويهها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كليًّا أو جزئيًّا، بأية وسيلة كانت.

ويلاحظ من ذلك، أن المشرع المصري، حدد عقوبة الحبس مدة لا تقل عن سنتين، ويفهم من ذلك أنها لا تزيد على ثلاث سنوات؛ حيث إن الحبس في قانون العقوبات المصري لا تقل مدته عن أربع وعشرين ساعة، ولا تزيد عن ثلاث سنوات[1]، كذلك، وضع المشرع المصري في

([1]) حيث نصت المادة (١٨) من قانون العقوبات المصري على أن: "عقوبة الحبس هى وضع المحكوم عليه في أحد السجون المركزية أو العمومية المدة المحكوم بها عليه ولا يجوز أن تنقص هذه المدة عن أربع وعشرين ساعة، ولا تزيد على ثلاث سنوات إلا في الأحوال الخصوصية المنصوص عليها قانونًا. لكل محكوم عليه بالحبس البسيط لمدة لا تتجاوز الثلاثة شهور أن يطلب بدلًا من تنفيذ عقوبة الحبس عليه تشغيله خارج السجن طبقًا لما تقرر من قيود بقانون تحقيق الجنايات إلا إذا نص الحكم على حرمانه من هذا الخيار".

قوله: "يُعاقب بالسجن"، الحد الأدني ثلاث سنوات، والحد الأقصى خمس عشرة سنة، وهو مفهوم السجن في قانون العقوبات المصري[١].

كما اعتبرت المادة (٢٦) من القانون المذكور أن استخدام شبكة المعلومات الدولية أو الإنترنت أو أي نظام إلكتروني معلوماتي، أو أي موقع إلكتروني أو وسيلة تقنية معلومات، من الظروف المشددة حال ارتكاب أية جريمة غير منصوص عليها في هذا القانون.

ثانيًا – العقوبات المالية:

(١) عقوبة الغرامة: وتطلق هذه العقوبة من خلال إلزام المشرع المحكوم عليه في جناية أو جنحة أو مخالفة، بإيداع مبلغٍ معين من المال – يحدده الحكم الجنائي – لدى الخزانة العامة للدولة[٢].

ويلاحظ الباحث: أن المشرع المصري، قد حدد عقوبة الغرامة المالية في جريمة الاعتداء على البريد الإلكتروني بين حدٍ أدنى وحدٍ أقصى، وهو ما نبينه فيما يلي:

(أ) عقوبة الدخول غير المشروع إلى البريد الإلكتروني: يُعاقب بغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه: كل من دخل عمدًا، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخوّل له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا إلكترونيًّا أو حسابًا خاصًا أو نظامًا معلوماتيًّا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها[٣].

(ب) جريمة الاعتراض غير المشروع: يُعاقب بالغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه: إذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات من البريد الإلكتروني[٤].

---

(١) حيث عرفت المادة (١٦) من قانون العقوبات المصري السجن بقولها: "عقوبة السجن هى وضع المحكوم عليه في أحد السجون العمومية وتشغيله داخل السجن أو خارجه في الأعمال التى تعينها الحكومة المدة المحكوم بها عليه، ولا يجوز أن تنقص تلك المدة عن ثلاث سنين، ولا أن تزيد على خمس عشرة سنة إلا في الأحوال الخصوصية المنصوص عليها قانونًا".

(٢) مساعد بن عبد العزيز بن إبراهيم، عقوبة الغرامة في الشريعة والقانون وتطبيقاتها في اللجان الجمركية بمدينة الرياض، مرجع سابق، ص٦٥.

(٣) انظر: المادة (١٤) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات.

(٤) انظر: المادة (١٦) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات.

(ج) جريمة الاعتداء على سلامة بيانات ومعلومات البريد الإلكتروني: يُعاقب بالغرامة التى لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه: إذا ترتب على أيٍّ من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى، أو تدميرها أو تشويهها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كليًّا أو جزئيًّا، بأية وسيلة كانت[1].

ومن ذلك، يُلاحظ الباحث أن المشرع المصري، حدد عقوبة التخيير بين الحبس والغرامة في الحالة الأولى والثانية، بينما عاقب بعقوبتي السجن والغرامة في الحالة الثالثة.

ويرى الباحث، أن القانون رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات يكفي – من وجهة نظره – لردع كافة صور الاعتداء على البريد الإلكتروني.

ثالثاً – العقوبات الفرعية المقررة لجريمة الاعتداء على البريد الإلكتروني:

أورد المشرع المصري في القانون رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات ثلاثة أنواع من العقوبات التبعية، وهي المصادرة وغلق المحل، وعزل الموظف الذي يرتكب – أثناء وبسبب تأديته لوظيفته – جريمة من الجرائم الإلكترونية، وهو ما نبينه فيما يلي:

(١) مصادرة المضبوطات المتحصلة من الجريمة: تعتبر المصادرة العامة محظورة، وقد عرَّفها بعض شراح القانون بأنها: نزع ملكية المال جبرًا عن مالكه وإضافته إلى ملك الدولة بدون مقابل، أو هى: نزع مال – تم ضبطه – جبرًا عن صاحبه؛ لكى يؤول إلى مال الدولة[2]، فهي عقوبة ناقلة للملكية، جوهرها حلول الدولة محل المحكوم عليه – أو غيره – في ملكية المال.

وهي من الأمور الموضوعية التي تستقل المحكمة بتقديرها.

ولم يعرف قانون العقوبات المصري المصادرة، وإنما نص على الحكم بها، وذلك في المادة (٣٠) منه[3].

---

(١) انظر: المادة (١٧) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات.

(٢) د. غنام محمد غنام، الوجيز في شرح قانون العقوبات، مطبعة جامعة المنصورة والكتاب الجامعي، المنصورة، ٢٠٠٨م، ص٥٠٨.

(٣) حيث نصت هذه المادة على أنه: "يجوز للقاضي إذا حكم بعقوبة جنائية أو جنحة أن يحكم بمصادرة الأشياء المضبوطة التي تحصلت من الجريمة، وكذلك الأسلحة والآلات المضبوطة التي استعلمت أو التي من شأنها أن تستعمل فيها، وهذا كله بدون إخلال بحقوق الغير الحسن النية. وإذا كانت الأشياء المذكورة من التي يُعد صنعها أو استعمالها أو حيازتها أو بيعها أو عرضها للبيع جريمة في ذاته وجب الحكم بالمصادرة في جميع الأحوال، ولو لم تكن تلك الأشياء ملكًا للمتهم".

ويلاحظ الباحث: أن القانون المصري قد خلا من وضع تعريف للمصادرة، واكتفى ببيان بعض صورها وحالاتها وشروط الحكم بها وأنواعها.

وعلى ذلك يعرِّف الباحث المصادرة كعقوبة لجريمة الاعتداء على البريد الإلكتروني بأنها: نزع ملكية الأجهزة الإلكترونية – حال استخدامها بطريق غير مشروع – جبرًا عن الجاني، وإضافته إلى ملكية الدولة دون مقابل.

وقد وردت عقوبة المصادرة كعقوبة تبعية في القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات؛ حيث نصت المادة (٣٨) منه على أنه: "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أية جريمة من الجرائم المنصوص عليها في هذا القانون، أن تقضى بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونًا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو أسهم في ارتكابها".

ويرى الباحث: أنه يُستفاد من المادة السابقة، أنه متى كانت جريمة الاعتداء على البريد الإلكتروني – محل الدراسة – من الجرائم المحظورة بموجب هذا القانون، فإنه يجب مصادرة كافة الأجهزة أو البرامج أو الأدوات والآلات والمعدات، أو الوسائل المستخدمة في ارتكاب هذه الجريمة، وذلك إذا حكمت المحكمة بالإدانة، وهو موقف المشرع المصري في شأن المصادرة كعقوبة تبعية.

(٢) إغلاق الموقع الإلكتروني أو حجبه: نصت الفقرة الثانية من المادة (٣٨) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات، على أنه: "فى الحالات التى يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الاعتبارى المُدان بأية جريمة منصوص عليها في هذا القانون لم يحصل على الترخيص فيحكم فضلاً عن العقوبات المقررة بالغلق".

(٣) عزل الموظف: نصت المادة (٣٩) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن مكافحة جرائم تقنية المعلومات على أن: "للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضى بعزله مؤقتًا من وظيفته، إلا في الحالات المشار إليها في المادة (٣٤) من هذا القانون فيكون العزل وجوبيًّا".

وعلى الرغم من تصدي المشرع الجنائي المصري لجريمة الاعتداء على البريد الإلكتروني على نحو ما تقدم بيانه، إلا أن الباحث يؤكد في هذا الصدد، على أنه كنتيجة حتمية لتزايد استخدامات الإنترنت، وما يترتب على ذلك من الآثار الناشئة عن هذا التزايد المضطرد، وهو ما نرى الحاجة الملحة إلى تشديد أكثر صرامة للعقوبات بشكل أكثر مما هو عليه الان، إمعانًا إلى

تحقيق ردع يناسب جسامة الجريمة المرتكبة بغية القضاء على مثل هذه الجرائم الخطرة، وذلك على الرغم من الدور البارز للمشرع الجنائي في هذا الصدد – على نحو ما تقدم – كما يأمل الباحث من مشرعنا الجنائي اليقظة المستمرة والحس الأمني المستنير، لمواجهة جريمة الاعتداء على البريد الإلكتروني.

المبحث الثاني
الأحكام الإجرائية
لجريمة الاعتداء على البريد الإلكتروني

تمهيد وتقسيم:

أدى تنامى معدلات الجرائم في المجتمع بشكل رهيب، مما يجعلنا أمام حتمية البحث عن السبل الكفيلة للحد من تنامي الظاهرة واستفحالها في المجتمع خصوصًا في ظل الاستخدام المفرط لمختلف التكنولوجيات الحديثة، والدخول المفرط لدى الغالبية من أفراد المجتمع في ذلك، وبالتالي السعي الجاد لحماية البريد الإلكتروني من سائر المخاطر والآفات المحدقة بمصالح الأفراد وبالمجتمع على حد سواء[١].

ويكون ذلك من خلال تطبيق الأحكام الإجرائية، على الأحكام المتعلقة بالإجراءات الخاصة بجمع الأدلة والتحقيق الابتدائي والضبط والتفتيش، كما يمكن القول بأن الأحكام الإجرائية، هي الممارسات أو الخطوات الواجب اتباعها من قبل مأموري الضبط، وليس ثمة اختلاف جوهري بين الإجراءات المتعلقة بجمع الأدلة في الأنظمة التقليدية وذات الإجراءات في النظم المعلوماتية، إلا أن هذه الإجراءات الأخيرة تساهم في مدى الاستفادة من إمكانيات الحاسوب في أداء الغالبية العظمى من الأعمال الخاصة بجمع الأدلة؛ ومن ثم فإن مرحلة جمع الأدلة في ضوء المعالجة الإلكترونية ينبغي أن تشمل كافة مكونات الأنظمة المعلوماتية، كالعاملين في مجال الحاسب الآلي، وأجهزة الحاسب الآلي ذاتها، والبرمجيات وقواعد المعلومات البيانات[٢].

تمر الإجراءات المتعلقة بمسائل التحقيق الجنائي في الدعاوي الجنائية بمرحلتين، منها مرحلة جمع الأدلة السابقة على البدء في رفع الدعوى الجنائية مباشرة، وإن كانت هذه المرحلة (جمع الاستدلالات) ليست من الإجراءات المتعلقة بالدعوى الجنائية، بيد أنها ذات أهمية بالغة، وتبدو أهميتها في كونها ضرورية للبدء في رفع الدعوى الجنائية؛ إذ تُعدُّ بمثابة إجراءات تحضيرية وتمهيدية للدعوى الجنائية؛ حيث تهدف إلى جمع التحريات والمعلومات عن الجريمة

---

(١) العمري عيسات، الجريمة الالكترونية لدى المراهقين: دوافع الإقبال وآليات الضبط الاجتماعي، مجلة علوم الإنسان والمجتمع، جامعة محمد خيضر بسكرة – كلية العلوم الإنسانية والاجتماعية، المجلد ١١ العدد١، ٢٠٢٢، ص١٢٦.

(٢) د. فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٦م ص٣٢٣؛ د. عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي – دراسة متعمقة في التعريف بجرائم التقنية الحديثة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٩م، ص٣١٩.

المُرتكبة محل الدعوى، والوصول إلى الجاني، ومن ثَمَّ فإن لمرحلة جمع الاستدلالات أهمية بالغة في مسائل التحقيق الجنائي بوجه عام، وعلى وجه الخصوص في جريمة العدوان على البريد الإلكتروني، والتي تتميز إجراءاتها بطبيعه فنية وتقنية خاصة بها؛ إذ تختلف عن نظيراتها في الجرائم التقليدية.

وفي ضوء ذلك، فإننا نعرض في هذا المبحث للأحكام الإجرائية لجريمة العدوان على البريد الإلكتروني، وذلك من خلال مطلبين، على النحو الآتي:

المطلب الأول: مرحلة جمع الأدلة والمعاينة في جرائم العدوان على البريد الإلكتروني.

المطلب الثاني: التفتيش والضبط في جريمة الاعتداء على البريد الإلكتروني.

المطلب الأول

مرحلة جمع الأدلة والمعاينة

في جرائم العدوان على البريد الإلكتروني

تُعدُّ مرحلة الإجراءات الخاصة بجمع الأدلة من المراحل ذات الأهمية الكبيرة، في مجال التصدي للجرائم الإلكترونية بوجه عام، ومواجهة جرائم الاعتداء على البريد الإلكتروني على وجه الخصوص، والتي يمارسها مأمور الضبط القضائي، وهي مرحلة سابقة على مرحلة التحقيق الابتدائي، التي تقوم به النيابة العامة، فإن المستقر عليه في الغالبية العظمى من التشريعات أن هذه المرحلة ذات أهمية كبيرة باعتبارها مرحلة مهمة بالنسبة لسلطات التحقيق المختصة بتحريك الدعوى الجنائية ضد المتهم، فهي مرحلة إجراءات أولية، وهي مرحلة سابقة على تحريك الدعوى الجنائية[1]، كما تُعدُّ المعاينة من أهم إجراءات التحقيق؛ حيث إنها تمثل تعبيرًا صادقًا وصورة واضحة جلية وصحيحة لمكان ارتكاب الجريمة، وما يحتوي عليه من ماديات وآثار خاصة بمرتكب الجريمة، ومن خلالها يمكن كشف كيفية تنفيذ الجريمة منذ اللحظة الأولى لوقوعها، وحتى نهايتها، فهي عبارة عن تنظير ووصف كامل وفحص تام لمكان ارتكاب الجريمة، بما يتضمنه من أشخاص وأشياء؛ بغية الوقوف على كل الحقائق أو بعضها.

وفي ضوء ما تقدم، فقد ارتأينا أن نقسم هذا المطلب إلى فرعين، وذلك على النحو الآتي:

الفرع الأول: مرحلة جمع الأدلة في جريمة الاعتداء على البريد الإلكتروني.

الفرع الثاني: المعاينة في جريمة الاعتداء على البريد الإلكتروني.

([1]) نقض جنائي مصري ٣ مارس سنة ١٩٨٠م، مجموعة أحكام النقض، س٢١، ص٣٢٢، رقم ٦١.

الفرع الأول
مرحلة جمع الأدلة
في جرائم العدوان على البريد الإلكتروني

تختلف المرحلة الخاصة بإجراءات جمع الأدلة في جريمة العدوان على البريد الإلكتروني عن غيرها من الجرائم التقليدية، وذلك لما تتميز به جريمة العدوان على البريد الإلكتروني من ذاتية خاصة، فتبدأ مرحلة جمع الأدلة منذ اللحظة الأولى لوصول خبر ارتكاب الجريمة إلى علم مأموري الضبط القضائي؛ حيث يضع الأخير كافة المعلومات والبيانات التي تحيط بالجريمة ومن ارتكبها، تحت بصر وسمع سلطات التحقيق، وذلك من خلال ما يصل إليهم من الشكاوى والبلاغات بخصوص هذه الجريمة، سواء كانت هذه الشكاوى والبلاغات جدية أم غير ذلك، وهنا تبدو الحاجة إلى الدور الذي يلعبه مأمورو الضبط القضائي في التعامل مع هذه النوعية من الجرائم، بواسطة ما يتمتع به من المهارات الفنية للتحقيق الجنائي في جريمة العدوان على البريد الإلكتروني، ومن ثَمَّ ضرورة اتباع القواعد المحددة لذلك في قانون الإجراءات الجنائية المصري، والتي تبين طرق الوصول إلى الحقيقة، سواء أكان ذلك بالإدانة أو البراءة، ومن خلال الطرق المشروعة ودون أي انتهاك لحرمة الأفراد[1]، وذلك من خلال اتباع كافة الإجراءات الجنائية التي يحددها القانون للتعامل مع هذه الجريمة، وتشمل الإجراءات التي حددها قانون الإجراءات الجنائية المصري، ومنها الشكاوى وقبول البلاغات وإجراء التحريات اللازمة.

وفي ضوء ذلك، فإننا نتحدث عن مرحلة جمع الأدلة في جريمة الاعتداء على البريد الإلكتروني وذلم على النحو الآتي:

أولًا – أهمية إجراءات جمع الأدلة في جريمة الاعتداء على البريد الإلكتروني:

تخضع جريمة العدوان على البريد الإلكتروني كغيرها من الجرائم لقواعد الإثبات التي قررها قانون الإجراءات الجنائية، بيد أن تلك القواعد تجد عند التطبيق صعوبة في الجرائم المتصلة بالإنترنت، ويلاحظ أن هناك مجموعة من الإجراءات الجنائية بمعناها الواسع والضيق يجريها مأمور الضبط القضائي، وتسبق ضبط جريمة العدوان على البريد الإلكتروني.

للدليل الجنائي دوره الفعال في تحقيق إثبات الجريمة، وتتمثل أهميته من ناحيتين، **الناحية الأولى:** أن الدليل الجنائي يحتل دورًا في السياسة الجنائية، وهذه السياسة هي التي تركز على

---

(١) ألا تنطوي على إجراءات قهر أو إكراه مثل: تجريم التعذيب لحمل المتهم على الاعتراف من خلال نصوص المواد (١٢٦، ١٢٨، ٢٨٠) من قانون العقوبات المصري.

شخص المتهم، فضلاً عن العناية به[١]، أمّا **الناحية الثانية:** فإن القاضي يلعب دورًا إيجابيًّا في استقصاء الأدلة للوصول إلى الحقيقة[٢].

ويمكن تعريف أدلة الحاسوب بأنها: تلك الأدلة التي من الممكن الحصول عليها من الحاسوب بوسيلة من وسائل الإخراج[٣]، كما يمكن تعريفها بأنها: البيان أو التعبير الذي تم إنتاجه أو نقله بدقة متناهية من قبل الحاسوب، سواء تمثل ذلك في التسجيلات الصوتية أو التخطيطية أو أية مطبوعات أخرى[٤].

ولا تُعتبر الإجراءات الخاصة بجمع الأدلة، من إجراءات الدعوى الجنائية، وعلى الرغم من ذلك، فلا بد أن تكون ضمن نطاق المشروعية، ولا يجوز أن تخرج عن هذا النطاق، فلا يجوز أن تمس حقوق وحريات أفراد المجتمع، وإنما غايتها – فقط – جمع الأدلة والقرائن التي تُسهم في إثبات أو نفي الاتهام عن الجاني، وعلى ذلك فهي إجراءات خاصة لضبط الأدلة وتدقيقها، وفي غالب الأحوال أن تتضمن الجريمة المرتكبة أدلة علمية يجب أن تحرر من صيغتها التقليدية لتتوافق مع التقنية العلمية الحديثة، ولهذا فإن القواعد المقررة بقانون الإجراءات الجنائية لمأموري الضبط القضائي غايتها حفظ الأدلة من الضياع أو التلف، حتى تُسهم في الوصول إلى الحقيقة بشكل صحيح وواضح.

وقد بينت المادة (١١) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات أن: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإلكترونية، أو النظام المعلوماتى أو من برامج الحاسب، أو من أية وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائى متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

وفي ضوء هذه المادة، يمكن القول بأن الاستدلال عبارة عن جمع كافة المعلومات والبيانات عن جريمة العدوان على البريد الإلكتروني والبحث عن الجاني من خلال الوسائل

---

(١) د. سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي – دراسة مقارنة، دار الكتب القانونية، ودار شتات للنشر والبرمجيات، (مصر، الإمارات)، ٢٠١١م، ص١٢.

(٢) د. فاضل زيدان، سلطة القاضي الجنائي في تقدير الأدلة، مكتبة دار الثقافة للنشر والتوزيع، عمان، ١٩٩٩م، ص١٤٤.

(٣) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، ٢٠٠٣م، ص١٤.

(٤) د. سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي – دراسة مقارنة، مرجع سابق، ص٥٥.

القانونية[1]، والاستدلال – كذلك – تمهيد أو تحضير لمرحلة التحقيق في الاتهام الموجه إلى المتهم؛ بغية تبصير سلطة التحقيق بما يلزم من معلومات وبيانات تساعدها أو تمكنها من التعرف بشكل أو بآخر، فهو ليس تحقيقًا بمفهومه الفني، كما أنه لا يعتبر مرحلة من مراحل الدعوى الجنائية، وإنما هو إجراء أولي يسبق تحريك الدعوى، ويتسم بطبيعة شبه إدارية[2].

وقد تناول المشرع المصري إجراءات جمع الأدلة في المادة (٢١) من قانون الإجراءات الجنائية المصري[3] .

فمهمة مأموري الضبط القضائي تدور في البحث عن الجرائم ومرتكبيها وجمع الأدلة التي تلزم للتحقيق والدعوى، وعملها لا يبدأ إلا بعد وقوع الجريمة، وبقصد الوصول إلى فاعلها لمعاقبته، سواء عناصر الجريمة تمت أم كانت في مرحلة شروع، فتتكون عناصر جمع الأدلة من إثبات وقوع الجريمة بأركانها وإثبات الظروف والملابسات التي أحاطت بها، والتعرف على فاعلها من خلال أقوال الشهود، والآثار المادية، وتحديد أدلة الإثبات، فهي تهدف إلى البحث والتحقق عن وقوع الجريمة، وجمع العناصر التي تصلح أن تكون أساسًا للبدء من قبل النيابة.

ويلاحظ الباحث: أنه من نص المادة (٢١) من قانون الإجراءات الجنائية المصري، أن المشرع قد أسند إلى مأموري الضبط القضائي وظيفتين غاية في الأهمية[4]، وهما:

الوظيفة الأولى – وظيفة البحث عن الجريمة ومن ارتكبها:

وهذه الوظيفة تتسم بطابعها الإداري، والتي تبدأ بعد وقوع الجريمة، وتعطي صورة واضحة وجلية لسلطة التحقيق عن وقوع جريمة ما وكيفية حدوثها والظروف المرافقة لها، وكشف غموضها.

---

(١) د. فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٥م، ص٢٤٩.

(٢) د. عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠٠٠م، ص١٦١.

(٣) والتي تنص على أنه: "يقوم مأمور الضبط القضائي بالبحث عن الجرائم ومرتكبيها وجمع الأدلة التي تلزم للتحقيق في الدعوى"

(٤) عندما نذكر مأموري الضبط القضائي نقصد بهم أعضاء الضبطيه القضائية من غير أعضاء النيابة، إلا أنهم وطبق نصوص القانون يعتبرون من أعضاء الضبطية القضائية، فدورهم يكون أكثر فاعلية في مرحلة التحقيق.

الوظيفة الثانية – وظيفة جمع الأدلة اللازمة للتحقيق:

وهي وظيفة تتسم بطابعها القضائي، ومهمتها التجهيز للتحقيق والمحاكمة بعد وقوع الجريمة.

ومن الجدير بالذكر، أن الغالبية العظمى من إجراءات مأمور الضبط القضائي تجمع بين الوظيفتين، أو بين الطابعين القضائي والإداري[١]، فليس ثمة حدود تفصل بين الطابعين.

ثانيًا – دور مأموري الضبط القضائي في جمع أدلة جريمة العدوان على البريد الإلكتروني[٢]:

لا يختلف دور مأموري الضبط القضائي في الاستدلال عن جريمة العدوان على البريد الإلكتروني كثيرًا عن القاعدة العامة في دور مأموري الضبط القضائي في إجراء الاستدلال عن الجرائم التقليدية، سوى أن جريمة العدوان على البريد الإلكتروني كونها شيئًا مميزًا ماديًّا تحتاج إلى خبرات من نوع خاص في رجال الضبط القضائي، إضافة إلى صعوبة الكشف عن مثل هذا النوع من الجرائم[٣]، فحدد المشرع المصري موضوع الضبط القضائي في المادة رقم (٢٣) من قانون الإجراءات الجنائية المصري، وقد حصرت هذه المادة رجال الضبط القضائي في عشر فئات[٤].

---

(١) يوجد اختلاف بين وظيفة الضبط الإداري والضبط القضائي: فالضبط الإداري وظيفة منع وقوع الجرائم باتخاذ التدابير الوقائية بهدف حماية النظام العام من الإخلال بتوقي الجرائم، فهذه الوظيفة تُباشر قبل وقوع الجريمة بهدف الحيلوله دون وقوعها في حين أن الضبط القضائي تبدأ وظيفته بعد وقوع الجريمة بقصد تتبع الجرائم للتوصل إلى مرتكبيها وتقديمهم لسلطات التحقيق؛ لذا فان وظيفة الضبط القضائي تبدأ حينما تنتهي وظيفة الضبط الاداري، حول هذه الفوارق: د. محمد محمد مصباح القاضي، الحماية الجنائية للحرية الشخصية في مرحله ما قبل المحاكمة الجنائية، دراسة مقارنة ، دار النهضه العربية، القاهره، ٢٠١٠م، ص١٨ وما بعدها.

(٢) اختلفت التشريعات الإجرائية في اللفظ المُستخدم لمصطلح الضبط القضائي، فقد استخدم المشرع المصري مصطلح مأمور الضبط القضائي.

(٣) تواجه عملية جمع الأدلة الإلكترونية واستعمالها صعوبات، منها: صعوبة الوصول إلى الملفات المحذوفة أو المستتره أو المحمية بكلمات مرور داخل النظام – من الصعوبة العمل على إعادة البيانات من بعض الوسائل أو الوسائط القديمة– من الصعوبة العثور على الملفات أو السجلات المحورية مثل سجلات البريد الإلكتروني– صعوبة تحليل البيانات والملفات، ومعرفة فيما إذا قد جرى عليها أي تعديل أو عمليات مسح، عبد العال الديربي، د. محمد صادق إسماعيل، الجرائم الإلكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، مرجع سابق، ص٣٣٠.

(٤) حيث نصت المادة (٢٣) من قانون الإجراءات الجنائية المصري على أن:

"أ– يكون من مأموري الضبط القضائي في دوائر اختصاصهم: أعضاء النيابة العامة ومعاونوها. ١– ضباط الشرطة وأمناؤها والكونستبلات والمساعدون. ٢– رؤساء نقط الشرطة. ٣– العمد ومشايخ البلاد ومشايخ الخفر. ٤– نظار ووكلاء محطات السكك الحديدية الحكومية، ولمديري أمن المحافظات ومفتشي مصلحة

يلاحظ الباحث: أنه من خلال نص المادة (٢٣) من قانون الإجراءات الجنائية المصري، وحتى لا يكون النص جامدًا فقد فوّض وزير العدل بالاتفاق مع الوزير المختص في إعطاء تلك الصفة لبعض الموظفين فيما يتعلق بوظائفهم، وفي دوائر الاختصاص التابعة له؛ حرصًا منه؛ وتيسيرًا بسبب زيادة القوانين الخاصة، وينبني على ما مر التساؤل الذي مثاره هل مأمورو الضبط القضائي والمبين تحديدهم في المادة (٢٣) من قانون الإجراءات الجنائية المصري، هم أنفسهم المنوط بهم مكافحة جريمة العدوان على البريد الإلكتروني؟ وللإجابة على هذا التساؤل يُراجع ما نصت عليه المادة (٥) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات[١].

ونلاحظ أن المشرع المصري قد أحسن صنعًا، عندما نص في المادتين السابقتين، على منح صفة الضبطية القضائية لأولئك العاملين بالجهاز، سواء أكانوا فنيين أو خبراء حتى يتمكنوا من ضبط جريمة العدوان على البريد الإلكتروني في نطاق عملهم، لا سيما أن التخصص المهني يُسهم بدور فعَّال في كشف هذا النوع من الجرائم، فحصرهم في إطار القانون يؤدي لتقويض يد العدالة في تطبيق القانون، خصوصًا إذا ما كانوا من ذوي الخبرة؛ الأمر الذي يزيد من فاعلية دورهم من خلال معاينة جريمة العدوان على البريد الإلكتروني والتحفظ على أدلتها من جانب،

التفتيش العام بوزارة الداخلية أن يؤدوا الأعمال التي يقوم بها مأمورو الضبط القضائي في دوائر اختصاصهم، (ب) ويكون من مأموري الضبط القضائي في جميع أنحاء الجمهورية:

١- مديرو وضباط إدارة المباحث العامة في وزارة الداخلية وفروعها بمديريات الأمن.

٢- مديرو الإدارات والأقسام ورؤساء المكاتب والمفتشون والضباط وأمناء الشرطة والكونستابل والمساعدون وباحثات الشرطة والعاملون بمصلحة الأمن العام وفي شعب البحث الجنائي بمديريات الأمن.

٣- ضباط مصلحة السجون.

٤- مديرو الإدارة العامة لشرطة السكة الحديد والنقل والمواصلات وضباط هذه الإدارات.

٥- قاد وضباط أساس هجانة الشرطة.

٦- مفتشو وزارة السياحه...

- ويجوز بقرار من وزير العدل الاتفاق مع الوزير المختص تخويل بعض الموظفين صفة مأموري الضبط القضائي بالنسبة إلى الجرائم التي تقع في دوائر اختصاصهم، وتكون متعلقة بأعمال وظائفهم..

- وتعتبر النصوص الواردة في القوانين والمراسيم والقرارات الأخرى بشأن تخويل بعض الموظفين اختصاص مأموري الضبط القضائي بمثابة قرارات صادرة من وزير العدل بالاتفاق مع الوزير المختص".

(١) حيث تنص هذه المادة على أنه: "يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومي بالنسبة إلى الجرائم التي تقع بالمخالفة لأحكام هذا القانون، والمتعلقة بأعمال وظائفهم". والجهاز وفقًا لما بينته المادة الأولى من هذا القانون هو: الجهاز القومي لتنظيم الاتصالات.

ولديهم المعرفة التي تتناسب مع المتغيرات المتلاحقة لجريمة العدوان على البريد الإلكتروني من جهة أخرى.

وقد أشارت إليه المادة (٥) من **القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات بشأن جرائم مكافحة جرائم تقنية المعلومات**، وهم أصحاب الاختصاص العام.

فنجد أن الوضع في القانون المصري؛ حيث تناولت المادة (٣٣) من قانون الإجراءات الجنائية المصري من يملكون صفة الضبط القضائي على سبيل الحصر، ويمارسون وظائفهم في كافة الجرائم، فحدد الأشخاص الذين يتصفون بصفة مأمور الضبط القضائي طبقًا للمادة المشار إليها سالفًا، فمأمورو الضبط القضائي ينقسمون إلى قسمين: قسم لهم صفه الضبط القضائي في كافة الجرائم، ويسمَّى أعضاؤها مأموري الضبط القضائي ذوي الاختصاص العام، وقد ورد تعدادهم على سبيل الحصر[١]، أمّا القسم الآخر، فقد منح هؤلاء صفة الضبطية القضائية في نوع معين من الجرائم دون غيرها، محددة بوظائفهم، فقد أسبغت المادة (٢٣) في فقرتها (ب) عليهم هذه الصفة، وتنحصر مهمتهم في التثبت في جرائم خاصة، موضوعة تحت منحهم بقرار من وزير العدل بالاتفاق مع الوزير المختص ومرتبطة بأعمال وظائفهم[٢]، ويسمَّى أعضاؤها "مأموري الضبط القضائي ذوي الاختصاص الخاص".

يلاحظ الباحث: أن المشرع المصري اكتفى في المادة (١٨٩) بمكان وقوع الجريمة إذا وقعت بالفعل، ويختلف الأمر في حالة الشروع، وفي الجرائم المستمرة، وفي حالة إذا وقعت الجريمة خارج الدولة.

كما استحدثت إدارات أخرى متخصصة في مثل تلك الجرائم، من أهمها[٣]:

(١) **الإدارة العامة لمباحث الأموال العامة.**

(٢) **الادارة العامه للتوثيق والمعلومات.**

(٣) **الإدارة العامة للمصنفات الفنية.**

---

(١) **د. محمد محمد مصباح القاضي، الحماية الجنائية للحرية الشخصية في مرحلة ما قبل المحاكمة الجنائية، مرجع سابق، ص٤٩ وما بعدها.**

(٢) **د. أمجد الكردي، المشاكل العملية التي تواجه النيابة العامه في التحقيق الأولي، دار اليراع للنشر والتوزيع، عمان، ٢٠٠٧م، ص٤٨.**

(٣) **د. أيمن عبد الحفيظ عبد الحميد سليمان، "استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي– دراسة مقارنة"، مرجع سابق، ص ٣٩٤.**

ثالثًا – الطبيعة الخاصة لإجراءات الاستدلال في جريمة الاعتداء على البريد الإلكتروني:

توصلنا فيما سبق إلى أن القانون عهد إلى مأموري الضبط القضائي بمهمة تقصي الجرائم والبحث عن مرتكبيها، وجمع المعلومات اللازمة لمجريات التحقيق بهدف تهيئة الدعوى لمرحلة التحقيق الابتدائي والتحقيق النهائي، فمن حسن السياسة التشريعية ألا تحدد هذه الإجراءات على سبيل الحصر بنصوص قانونية حتى لا يكون ذلك عقبة أمام القائمين بها في سبيل كشف الجريمة والمحافظة على الآثار المتخلفة عنها، مع ضرورة سماع من يُرى سماعه[١].

وشملت الأعمال التي نص عليها المشرع من قبول التبليغات والشكاوى وإجراء التحريات، وهي بطبيعتها غير ماسّة بحقوق الأفراد، فالهدف منها جمع المعلومات، ولهذا في هذه الفقرة سنتعرف على البلاغ والشكوى في جريمة الاعتداء على البريد الإلكتروني والبحث والتحري في الجريمة ذاتها، وذلك على النحو الآتي:

(١) البلاغ والشكوى في جريمة الاعتداء على البريد الإلكتروني:

يبدأ مأمورو الضبط القضائي في أداء عملهم بعد ارتكاب الجريمة ووصول علمها لهم عن طريق بلاغ أو شكوى، فالدور الأساسي في هذه المهمة هو التحري عن الجريمة، وجمع العناصر والدلائل اللازمة لبدء التحقيق فيها، ويُقصد بالبلاغ[٢] في جريمة الاعتداء على البريد الإلكتروني ما يصل إلى علم رجال الضبط القضائي من معلومات حول واقعة تُعدُّ في نظر القانون جريمة، ويتضمن التشريع الإجرائي التزامًا على عاتق رجال الضبط القضائي[٣] بتلقي البلاغات وتدوينها في محاضر[٤]، والاستيضاح بشأنها، أو هو الإبلاغ أو إخبار السلطات

---

(١) د. محمد أبو العلا عقيدة، "شرح قانون الإجراءات الجنائية"، الجزء الأول، دار النهضة العربية، القاهرة، بلا سنة نشر، ص٣٨٣.

(٢) البلاغ بصورة عامة "هو إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع، أو أنها تمثل اتفاقًا جنائيًا أو أدلة أو قرائن أو عزمًا على حدوثها، أو وجود شك أو خوف من أنها ارتكبت" نقض رقم ٣٠٥١٣، لسنة٦٧، ق– جلسة٤/٥/٢٠٠٠.

(٣) نصت المادة (٢٤) من قانون الإجراءات الجنائية المصري على أنه: "يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم بشأن الجرائم، وأن يبعثوا بها فورًا إلى النيابة العامة، ويجب عليهم وعلى مرءوسيهم أن يحصلوا على جميع الإيضاحات ويجروا المعاينات اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم، أو التي يعلنون بها بأية كيفية كانت، وعليهم أن يتخذوا جميع الوسائل، التحفظية اللازمه للمحافظة على أدلة الجريمة...".

(٤) قضت محكمة النقض المصرية على أنه "يجب أن تثبت جميع الإجراءات التي يقوم بها مأمورو الضبط القضائي في محاضر موقع عليها منهم، يبين فيها وقت اتخاذ الإجراءات ومكان حصولها ... لم يرد إلا

المختصة عن وقوع جريمة، أو أنها على وشك الحدوث، أو أن هناك اتفاقًا جنائيًّا أو أدلة أو قرائن أو عزمًا على ارتكابها، أو وجود شكوك أو خوف من أنها ارتكبت[١]،

كما جاء بنص المادة (٨٤) من قانون العقوبات المصري[٢]، ويكون الإبلاغ واجبًا أخلاقيًّا[٣]، وفي هذا تأكيد على المبادئ الاجتماعية العامة، ومن أهمها: مبدأ التكافل الاجتماعي، الذي يعمل على حماية المجتمع، ومواجهة أي اعتداء يهدف إلى المساس بكيانه، كما رتب المشرع في القوانين الإجرائية واجب الإبلاغ عن الجرائم لكافة العاملين، ذلك بما جاء بنص المادة (٢٦) من قانون الإجراءات الجنائية المصري[٤].

(٢) الشكوى في جريمة الاعتداء على البريد الإلكتروني:

كما يتلقى مأمور الضبط القضائي البلاغات، فإنه يتلقى الشكاوى، وهي الطلبات التي تقدم من المجني عليهم المتضررين من الجريمة للمطالبة بتعويض الضرر الذي أصابهم، فهي تلك الطلبات التي يمثل فيها الدعوى المدنية أمام الضبط القضائي[٥]، فالشكوى هي بلاغ أو إخطار من المجني عليه أو وكيله الخاص إلى رجال الضبط القضائي أو السلطة المختصة أو النيابة العامة أو المحكمة في بعض الحالات بواقعة الجريمة، وطلب تطبيق القانون ضد فاعلها، سواء أكان شخصًا أو أكثر، أمّا إذا خلت الشكوى من الدعوى المدنية، فلا تُعتبر سوى بلاغ[٦].

على سبيل التنظيم والإرشاد، ولم يرتب على مخالفة البطلان"، الطعن رقم ١٠٦٩٦، لسنة ٦٧، ق- جلسة١٩٩٩/٥/٢.

(١) د. أسامة محمد حسن، "مختارات من قانون الإجراءات الجنائية"، ط١، دار النهضه العربية القاهره، ٢٠١٩م، ص٤٠.

(٢) نصت المادة (٨٤) من قانون العقوبات المصري على أنه: "يُعاقب بالحبس مدة لا تزيد على سنة والغرامة لا تجاوز ٥٠٠ جنيه أو بإحدى هاتين العقوبتين كل من علم بارتكاب جريمة من الجرائم المنصوص عليها في هذا الباب ولم يسارع إلى إبلاغه إلى السلطات العامة...".

(٣) نصت المادة (٢٥) من قانون الإجراءات المصري على أنه: "لكل من علم بوقوع جريمة يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ النيابة العامة أو أحد مأموري الضبط القضائي عنها".

(٤) حيث نصت هذه المادة على أنه: "يجب على كل من علم من الموظفين العموميين أو المكلفين بخدمة عامة أثناء تأدية عملهم أو بسبب تأديته بوقوع جريمة من الجرائم يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ عنها فورًا النيابة العامة أو أقرب مأموري الضبط القضائي".

(٥) د. نبيلة هبه هروال، جرائم الإنترنت – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد – الجزائر، ٢٠١٣م/ ٢٠١٤م، ص١٨٨.

(٦) نصت المادة (٢٨) من قانون الإجراءات الجنائية المصري على أنه: "الشكوي التي لا يدعي فيها مقدمها بحقوق مدنية تعد من قبيل التبليغات، ولا يعتبر الشاكي مدعيًّا بحقوق مدنية إلا إذا صرح بذلك في شكواه، أو في ورقة مقدمة منه بعد ذلك، أو إذا طلب في إحداهما تعويضًا ما.

رابعًا – البحث والتحري في جريمة الاعتداء على البريد الإلكتروني:

تعد التحريات من أقدم الإجراءات التي عرفتها الشرطة[١] فهي تعنى بالكشف عن الجريمة، والبحث عن دليلها، فهي إجراءات يقوم بها مأمورو الضبط القضائي أو من يستعين بهم من رجال الشرطة أو المرشدين والمخبرين من أجل كشف حقيقة الجريمة المرتكبة، ومعرفة طريقة حصوله، والظروف والملابسات المحيطة به، فالبحث والتحري يقودان الجهات المختصة بهما إلى وضوح الرؤية بالنسبة لهم، ورسم الطريق بشكل جيد[٢] فالقانون أوجب على مأموري الضبط القضائي القيام بالبحث عن الجرائم ومرتكبيها، وهو ما قضت به محكمة النقض المصرية؛ حيث قضت بأن: الكشف عن الجريمة والتوصل إلى مرتكبيها من مهمة مأمور الضبط القضائي[٣]، وذلك طبقًا لأحكام المادة (٢١) من قانون الإجراءات الجنائية المصري، وبيّن اختصاصاتهم بوظيفتي البحث عن الجرائم ومرتكبيها، ثم مرحلة جمع الأدلة التي تلزم للتحقيق، والقيام بتلك الأعمال التي تستلزم ضرورة التحري اللازم للكشف عن الجرائم ومرتكبيها.

وفي موضوع دراستنا جريمة الاعتداء على البريد الإلكتروني التي تقترن بأنماط وأنواع جديدة ذات حداثة بأساليب ارتكابها وسرعة تنفيذها وسهوله اختفائها، ودقة وسرعة محو آثارها، يقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الكمبيوتر وطريقة تشغيلها وأساليب ارتكاب الجرائم عليها أو بواسطتها، وإلى جانب ذلك فيتطلب فيمن يتولى جمع المعلومات حول ارتكابها أن يكون متخصصًا في التحقيق الجنائي ومعالجة البيانات إلكترونيًّا.

ولما كانت مثل هذه المواصفات لا تتوافر إلا لنسبة ضئيلة من فئات مأموري الضبط القضائي بسبب كم ونوع تقنية المعلومات المُستخدمة، وفي هذا قامت بعض الدول بتخصيص مأموري ضبط معينين بالذات لإجراء التحريات عن جريمة الاعتداء على البريد الإلكتروني، في حين يقترح البعض بأخذ أسلوب التحقيق بحيث يشمل متخصصين في كثير من الأمور التقنية[٤].

---

(١) د. مصطفى محمد الدغيدي، التحريات والإثبات الجنائي، دار النهضة العربية، القاهرة، ٢٠٠٢م، ص١٧٠.

(٢) تطبيقًا لذلك، قضت محكمة النقض المصرية بأنه" يجوز للمحكمه أن تعوّل في تكوين عقيدتها على تحريات الشرطة باعتبارها معززة لما ساقته من أدلة"، نقض ١٠ديسمبر١٩٨٦، س٣٧، رقم ١٩٦، ص١٠٢٠.

(٣) نقض جنائي بتاريخ ١٩٨٢/١٢/٨، مجموعة أحكام النقض، ٣٣٧ق ١٩٩، ص٩٦٢.

(٤) د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مرجع سابق، ص٤٤٣.

ويتم ذلك من خلال المراقبة الإلكترونية والتحري عبر شبكة الإنترنت، وهو ما نشير إليه فيما يلي:

(١) المراقبة الإلكترونية عبر شبكة الإنترنت:

حيث تُعدُّ المراقبة الإلكترونية من أهم مصادر التحري التي يستعين بها المحقق الجنائي في البحث والتقصي عن الجرائم، والمشتبه بهم في **جرائم الاعتداء على البريد الإلكتروني،** وخاصة أنها تعتبر أقصر الطرق لكشف الجرائم؛ لذا تُعدُّ وسيلة من وسائل جمع المعلومات عن المشتبه بهم (المراقبين إلكترونيًّا)،[١].

إلا أن المراقبة الإلكترونية لكونها تنطوي على مساس بحق الإنسان في سريته وخصوصية أحاديثه (كمراقبة البريد الإلكتروني الخاص بالمشتبه بهم)، الذي كفله الدستور والقانون، فهي تتجاوز في جسامتها إجراء تفتيش المنازل أو ضبط المراسلات والاطلاع عليها، وتكمن العلة في أن المراقبة تتم بصورة سرية وخلسة دون علم للشخص المراقب[٢]، فالمراقِب الإلكتروني هو ضابط أو عون الشرطة القضائية المُكلف بالمهمة، ويتابع بواسطة التقنية الإلكترونية المشتبه به على شبكة الإنترنت، وبالعادة تُسند المهمة إلى كل شخص يُحسن الاستخدام الأفضل لجهاز الكمبيوتر وأن يكون الشخص المُكلّف بالمهمة لديه إتقان ومهارة إلكترونية، ومعرفة بتقنية الهاتف النقال، الذي إلى عهد قريب، لم يكن بالإمكان مراقبة الاتصالات الإلكترونية التي كانت تتم من خلاله، حتى تمكنت شركة (Schwarz & rode) الألمانية المتخصصة في مجال أنظمة المعلومات في السنوات الأخيرة من تطوير نظام معلوماتي أطلقت عليه (IMSI Catcher)، ويمكن من خلاله التقاط كافة الإشارات الرقمية الصادرة عن الهواتف النقالة، ومن ثَمَّ تحويلها إلى كلمات مسموعة، ونفس الشيء ينطبق على المكالمات التي تجري على الهاتف العادي (الأرضي).

والجدير بالذكر أن هناك أنواعًا وطرقًا للمراقبة الإلكترونية تكون مشروعة بحسب طبيعتها، ويمكن اللجوء إليها حال توافرت حالة من الوقائع والتعدي لأي أفعال تخريبية أو جرائم ماسَّة بأمن الدولة أو جرائم إرهابية؛ حيث يرتكب الإرهاب السيبراني بواسطة الحاسب الآلي، وعبر شبكة الإنترنت، وهو عابر للحدود، ومن ثم صعوبة إثباته لتعدد وسائل ارتكاب جريمة الإرهاب السيبراني ودوافعها من حلال البريد الالكتروني[٣]، فهي تختص بالكشف عن خطر أو

---

(١) د. نبيه هبه هروال، جرائم الإنترنت – دراسة مقارنة، مرجع سابق ص١٩٦ وما بعدها.

(٢) د. كاظم عبد الله نزال المياحي، حجية المراقبة الإلكترونية للصوت والصورة في الإثبات الجنائي – دراسة مقارنة في القانون العراقي والمقارن، رسالة دكتوراه كلية الحقوق، جامعة عين شمس،٢٠١٦م، ص٨٩.

(٣) بوعزاتي عبدالكريم، جريمة الإرهاب السيبراني بين التشريع المغربي والمقارن، مجلة الأبحاث والدراسات القانونية، المركز المغربي للدراسات والإستشارات القانونية وحل المنازعات، العدد ٢١، ٢٠٢٢، ص٨١.

تهديد لأمن الدولة، أو في حالة أخرى، وهي توفر معلومات عن احتمالية اعتداء على منظومة حاسوبية، أو في حالة أن مقتنيات التحريات والتحقيقات القضائية صعب الوصول إليها[١]، وهو ما نص عليه المشرع المصري في المادة (٢) في البندين ثانيًا وثالثًا[٢]، من **القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات.**

ويفهم من هذا النص: أن مزودي الخدمة الذين يحققون في الاستخدامات غير المشروعة لنظم المعلومات، لديهم سلطة موسعة للمراقبة، ولديهم الحق في الكشف عن الدليل للاستخدام غير المشروع، وأن يكون ذلك مع مراعاة الحياة الخاصة ضمن إطار المشروعية، وحالة طلب جهات الأمن القومي، فلا يوجب بذلك انتهاك للقانون، وتحقيق مثل هذا يقتضي أن ينظم المشرع هذه المسأله من إجراءات المراقبة، التي تُعدُّ من الوسائل التحقيقية للبحث والتحري.

(٢) التحري الإلكتروني:

يُقصد به "الإجراء الذي يقوم به مأمور الضبط القضائي عن طريق استخدام تقنية المعلومات للحصول على معلومات توضيحية عن الأشخاص أو أماكنهم أو الأشياء حسب طبيعتها أو البيانات، وذلك للحد من الجريمة الإلكترونية، أو ضبطها لتحقيق الأمن المعلوماتي"[٣]، والمعنى لذلك أن مأمور الضبط القضائي يختص بالقيام بالتحريات اللازمة للكشف عمَّا ارتكب من جرائم وفاعليها، وهو يقوم بذلك بنفسه أو بواسطة مساعديه، فلا يختلف التحري في الجرائم المادية عنه في جرائم الكمبيوتر، فهدفه تحديد هوية مرتكب الواقعة وطبيعتها، ثم بعد ذلك تحديد كيفية الوصول إلى الأدلة، شرط أن يكون هناك ما يدل على وقوع جريمة ما، كما أن الهدف للتحري في **جرائم الاعتداء على البريد الإلكتروني** الحصول على أكبر قدر من

---

(١) د. محمد علي سويلم، الإثبات الجنائي عبر الوسائل الإلكترونية- دراسة مقارنة، دار المطبوعات الجامعية، ٢٠٢٠م، ص٥٧٣ وما بعدها.

(٢) حيث نصت هذه المادة على أن: ".... ثانيًا -مع عدم الإخلال بأحكام قانون حماية المستهلك، يجب على مقدم الخدمة أن يوفر لمستخدمى خدماته، ولأى جهة حكومية مختصة، بالشكل والطريقة التى يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية: ١ - اسم مقدم الخدمة وعنوانه ٢ - معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكترونى. ٣ - بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التى يخضع لإشرافها. ٤ - أي معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمى الخدمة، ويصدر بتحديدها قرار من الوزير المختص. ثالثًا: مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا، حال طلب جهات الأمن القومى ووفقًا لاحتياجاتها، كافة الإمكانيات الفنية التى تتيح لتلك الجهات ممارسة اختصاصاتها وفقًا للقانون".

(٣) د. مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٥م، ص٢٢.

المعلومات عن الفعل المكوّن للجريمة الإلكترونية وأسلوب وظروف ارتكابها في وقت وزمن قصير من خلال المقابلات الاستطلاعية، التي تجري مع ممثلي الجهة المجني عليها، إذا كانت إحدى المؤسسات أو من الأفراد المجني عليهم، وبناءً على طبيعة السلوك الإجرامي المُرتكب يحدد نطاق وزمن التحري والوقت المستلزم، كون الدليل المستند إلى المعالجات الآلية للبيانات يمكن أن يكون متاحًا لفترة قصيرة من الزمن، بالإضافة إلى إمكانية أن تكون تلك الجرائم من النوع المستمر من حيث نتائجها أو تنفيذها، كمثل جرائم نشر الفيروسات، وعند القيام بأعمال البحث والتحري عن الجريمة الإلكترونية لا بد أن يتبع الإرشادات المتعلقة بتحديد نوع النظام المعلوماتي، وأخذ كشف بأسماء العاملين الفنيين والمسئولين عن أمن المعلومات بالمنشأة، وحصر الطرفيات الموجودة، وتحديد الروابط لمعرفة طريقة نقل المعلومات[١].

الفرع الثاني

المعاينة في جرائم الاعتداء

على البريد الإلكتروني

المعاينة في جوهرها ملاحظة وفحص حسي مباشر بمكان أو شخص له علاقة بالجريمة، وذلك لإثبات حالته، والتحفظ على ما يفيد من الأشياء في كشف الحقيقة، قبل أن تنالها يد العبث والتخريب، وهي صورة من صور الحصول على الإيضاحات[٢]، والمعاينة من الوجهة القانونية ليست وسيلة إثبات، وإنما هي إجراء استقصائي كاشف لأبعاد الجريمة وأركانها[٣].

ويهدف التفتيش في الجرائم المعلوماتية إلى حفظ الوسائط الإلكترونية، التي سجلت عليها هذه البيانات لجمعها وتخزينها، كالاسطوانات والأقراص الممغنطة، ومخرجات الحاسب، والتي تتعلق بالجريمة الإلكترونية، وتفيد في كشف الحقيقة، أي أن محل التفتيش البيانات المعالجة آليًا[٤]، أمَّا الضبط فهو وضع اليد على الدعائم المادية المخزّنة فيها البيانات الإلكترونية أو المعلومات التي تتصل بالجريمة المعلوماتية التي وقعت، وتفيد في كشف الحقيقة عنها، وعن مرتكبها، واستخدام البرامج المهمة من أجل الولوج للبيانات المراد ضبطها، إلى جانب وضع اليد على تلك الدعائم المادية[٥]. وعلى ذلك، فإن الضبط في جرائم الاعتداء على البريد الإلكتروني:

---

(١) د. مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، مرجع سابق، ص٢٧٨.

(٢) د. هشام محمد فريد رستم، الجوانب الإجرامية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ١٩٩٤م، ص٥٧.

(٣) د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠١٠م، ص١٤٦.

(٤) د. فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، مرجع سابق، ص٢٤٩.

(٥) د. نبيلة هبة هروال، جرائم الإنترنت – دراسة مقارنة، مرجع سابق، ص٢٦٦.

هو استخدام نوع من البرامج المهمة عالية الدقة بغرض الدخول للبيئة المعلوماتية، التي تروج لجرائم الاعتداء على البريد الإلكتروني المراد مكافحتها، فضلاً عن وضع اليد على الدعائم المادية لهذه البيانات.

ويُعدُّ المكان الذي ترتكب فيه الجريمة الوعاء الأساسي، الذي يحتوى على أخطر الأدلة الجنائية، التي يخلفها الجاني وراءه في أعقاب ارتكابه الجريمة مما يدل على شخصيته الإجرامية، ومدى دوره في ارتكابها، ويبقي هذا الدليل بمكان الواقعة، وهو الشاهد الصامت على ارتكابها، ويكون معرضًا للهلاك إذا لم تسرع جهات التحقيق بحمايته[١]، فالمعاينة يمكن أن تكون إجراءً تحقيقيًّا[٢] أو استدلاليًّا، وذلك بحسب طبيعة ما يقتضيه إجراؤها من مساس بحقوق الأفراد وحرياتهم، بالرغم أن جانبًا من الفقهاء يرى أنها يمكن أن تكون إجراء استدلال، إن تمت في مكان عام، وإذا تمت بالدخول إلى أحد المنازل كانت إجراء تحقيق[٣]، ونظرًا لما توفره من أدلة إثبات، وتزداد أهميتها إذا ما تعلق الأمر بجرائم الاعتداء على البريد الإلكتروني باعتبارها من الجرائم المستحدثة وغير المألوفة؛ مما يستوجب ابتكار تقنيات جديدة مناسبة بالمعاينة، سيما أنها ركيزة أساسية لكافة الإجراءات اللاحقة عليها، وهو ما نبينه بإيجاز على النحو الآتي:

أولًا – مفهوم المعاينة في جريمة الاعتداء على البريد الإلكتروني: يشير الفقه الجنائي إلى أهمية التمييز في مسألة معاينة مسرح الجريمة في الجرائم المعلوماتية – حسب محل الجريمة – بين أمرين، أولهما: حالة ارتكاب الجريمة على المكونات المادية للحاسب، والثاني: حالة ارتكاب الجريمة على المكونات غير المادية أو بواسطتها، وهو ما سوف نشير إليه على النحو الآتي[٤]:

الحالة الأولى – حالة ارتكاب الجريمة على المكونات المادية للحاسب الآلي: مثل جرائم الاعتداء على أشرطة الحاسب وكابلات وشاشة العرض الخاصة به، ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب ذات الطابع المادي الملموس، ففي هذه الحالة، فإن الأمر لا يثير أدنى صعوبة للتقرير بصلاحية الجريمة، الذي يحوي هذه المكونات لمعاينتها من قبل مأموري

---

(١) د. محمد زكي أبو عامر، الإجراءات الجنائية، ط٢، منشأة المعارف، الإسكندرية، ١٩٩٠م، ص٥٨٠.

(٢) الأصل في المعاينة أنها إجراء من إجراءات التحقيق، ففي غير حالات التلبس التي نص عليها القانون يلزم أن تقوم بها سلطة التحقيق بنفسها، أو تنتدب مأمور الضبط القضائي، ويقتضي ذلك تحرير محضر بها عن طريق كاتب؛ لأنها من الإجراءات التي تستلزم من المحقق تفرغًا ذهنيًّا. د. محمد زكي أبو عامر، الإجراءات الجنائية، كرجع سابق، ص٦٠٤.

(٣) د. عوض محمد عوض، المبادئ العامه في قانون الإجراءات الجنائية، دار المطبوعات الجنائية، الاسكندرية، ١٩٩٩م، ص٣٧٢.

(٤) د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، وفي ضوء الاتفاقيات والمواثيق الدولية، ط١، دار النهضة العربية، القاهرة، ٢٠١١م، ص١٠٧ وما بعدها.

الضبط، والتحفظ على الأشياء، التي تعد أدلة مادية تدل على ارتكاب الجريمة ونسبتها لشخص معين، وكذا وضع الأختام في الأماكن التي تمت فيها المعاينة، وضبط كل ما استعمل في ارتكاب الجريمة، والتحفظ عليه مع إخطار النيابة بذلك.

الحالة الثانية – حالة ارتكاب الجريمة على المكونات غير المادية أو بواسطتها: في هذه الحالة يأتي في مقدمة هذه الجرائم تلك الواقعة على برامج الحاسب والبيانات أو بواسطتها، وهنا يقرر الفقه الجنائي وجود صعوبات عدة، تحول دون فاعلية المعاينة أو فائدتها.

ويمكن تلخيص هذه الصعوبات في عاملين رئيسيين[١]:

العامل الأول: قلة الآثار المادية التي قد تتخلف عن الجرائم التي تقع على برامج الحاسب وبياناته أو بواسطتها.

العامل الثاني: الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة الزمنية، التي غالبًا ما تكون طويلة نسبيًّا – وذلك ما بين اقتراف الجريمة والكشف عنها – الأمر الذي يمنح فرصة لحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها، وهو ما يلقي ظلالاً من الشك على الدليل المنتقى من المعاينة، وهو ما يتطلب ضرورة توخي الحذر حال إجراء المعاينة في مسرح الجريمة المعلوماتية[٢].

معاينة الجرائم التقليدية والاطلاع على مسرح الجريمة فيها له أهمية كبيرة متمثلة في تصوير كيفية وقوع الجريمة وظروف ملابساتها وتوفير الأدلة المادية التي يمكن جمعها، لكن هذه المعاينة لا تؤدي لذات الدور في كشف غموض جرائم الاعتداء على البريد الإلكتروني، وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى فاعلها، ولم يحدد المشرع المقصود بالمعاينة، الأمر الذي دعا الفقه إلى التصدي لتعريفها؛ حيث عرفها بعض الفقهاء: "بأنها إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة، يشاهد بنفسه، ويجمع الآثار المتعلقة بها، وكيفية حصولها، وكذلك جمع الأشياء الأخرى، التي تفيد بكشف الحقيقة"، وعرفها جانب آخر من الفقه بأنها: "رؤية مجال وقوع الوقائع الجنائية وإثبات حالتها بالشكل التي تركها به الجاني عقب الانتهاء من جريمته، كما تنصرف إلى فحص جسم المجني عليه والمتهم وإثبات ما يوجد بهم من آثار[٣]، أمّا المعاينة الإلكترونية فعرفت بأنها "المشاهدة والرؤية بالعين لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والآثار المادية التي خلفها ارتكاب الجريمة الإلكترونية، وضبط كل ما يلزم من الأشياء لكشف الحقيقة عن الجريمة وفاعلها بهدف المحافظة على الأدلة التقنية

---

(١) د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، مرجع سابق، ص١٠٨.

(٢) المرجع السابق، ص١٠٨.

(٣) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة، مرجع سابق، ص٥٥.

من التلف أو المحو أو التعديل[١]. ومن المؤكد أيًّا ما كان الرأي في التعريفات المتقدمة فإن المعاينة في جوهرها ملاحظة وفحص حسي مباشر لمكان أو شخص أو أي شيء له علاقة بالجريمة؛ لإثبات حالته، والكشف والتحفظ على كل ما يفيد لكشف الحقيقة[٢].

وهو ما نصت عليه المادة (٣١) من قانون الإجراءات الجنائية المصري[٣].

وهو ما قضت به محكمة النقض المصرية؛ حيث قضت بأن المعاينة التي تجريها النيابة لمحل الحادث لا يلحقها بطلان بسبب غياب المتهم؛ إذ إن تلك المعاينة ليست إلا إجراءً من إجراءات التحقيق، يجوز للنيابة أن تقوم به في غيبة المتهم؛ إذ هي رأت ذلك موجبًا، وكل ما يكون للمتهم هو أن يتمسك لدى محكمة الموضوع بما قد يكون بالمعاينة من نقص أو عيب، حتى تقدرها المحكمة"[٤].

ويعتمد المحقق الجنائي عند إجرائه المعاينة الإلكترونية بحثًا عن الأدلة الإلكترونية على فحص مجموعة محاور الدليل في البيئة الإلكترونية، التي ارتكبت فيها الجريمة الإلكترونية، والمتمثلة عادةً في:

المعلومات: وتشمل هذه الجرائم في سرقة وحذف معلومات وتغيير كاستهداف البريد الإلكتروني.

الأشخاص والجهات: وهي الجرائم التي تقع على الأشخاص أو المؤسسات باستخدام شبكة الإنترنت والكمبيوتر كجرائم التهديد والاحتيال والسرقة.

الأجهزة: وهي الجرائم التي ترتكب على أجهزة الكمبيوتر بهدف تعطيلها وتخريبها بإرسال الفيروسات أو البرامج، التي تؤدي إلى تلف هذه الأجهزة[٥].

---

(١) د. توفيق عبد الله أحمد الخشاشنة، معاينة مسرح الجريمة من خلال شبكة المعلومات الدولية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٦م، ص٧٧.

(٢) د. عمر السعيد رمضان، قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، القاهره، ١٩٨٥م، ص ٢٨٢.

(٣) حيث نصت هذه المادة على أنه: "يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فورًا إلى محل الواقعة، ويعاين الآثار المادية للجريمة، ويحافظ عليها، ويثبت حالة الأشخاص، وكل ما يفيد لكشف الحقيقة، ويسمع أقوال من كان حاضرًا أو من يمكن الحصول منه على إيضاحات في شأن الواقعه ومرتكبها".

(٤) نقض جنائي الطعن رقم ١٢٧٥١ لسنة ٦٢ ق جلسة ١٩٩٤/٢/٧.

(٥) د. عبد الله عبد الكريم، جرائم المعلومات والإنترنت، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧م، ص١٨.

ثانيًا – القواعد الأساسية الواجب اتباعها في معاينة جرائم الاعتداء على البريد الإلكتروني:

نظرًا للطبيعة الخاصة التي تتميز بها **جرائم الاعتداء على البريد الإلكتروني** عن الجرائم التقليدية، فإنه تتخذ المعاينة في **جرائم الاعتداء على البريد الإلكتروني** بصفة خاصة أشكالاً مختلفه بحسب نوعية الجريمة المرتكبة على أنه توجد خطوات وإرشادات فنية قبل البدء في معاينة أية جريمة إلكترونية، كما أنه يستلزم وجود ضوابط عند المعاينة، والتزام بشروط واجب اتباعها لصحة المعاينة في هذا النوع من الجرائم؛ حيث تعتبر معاينة مسرح الجريمة الإلكترونية لها فائدة في كشف الحقيقة، ومعرفة مرتكبها؛ لذا ينبغي اتباع عدة خطوات وإرشادات فنية قبل الانتقال لمعاينة **جريمة الاعتداء على البريد الإلكتروني، أبرزها**[1]:

(١) ضرورة توفير معلومات مسبقة عن مكان وقوع الجريمة، وعن أعداد الأجهزة المطلوب مداهمتها وأنواعها، وكذلك مداهمة شبكاتها، وتحديد كيفية التعامل معها فنيًّا قبل المداهمه من حيث الضبط أو التأمين أو حفظ الأوراق والمستندات المتداولة.

(٢) وجود خريطة تبين الموقع المطلوب معاينته، وتفاصيل المبنى أو الطابق من المبنى موضوع البلاغ، ووضع خطة أمنية محكمة لعملية المعاينة والضبط.

(٣) تجهيز المعدات والأجهزة والبرامج التي سيتم الاستعانة بها في إجراء عملية المعاينة.

(٤) إعداد فريق من المتخصصين، الذين سيُستعان بهم في إجراء المعاينة من الخبراء ومأموري الضبط القضائي، الذين تتوافر فيهم الكفاءة العلمية والخبرة الفنية.

(٥) تحديد الأدوار وتوزيع الاختصاصات على المختصين وفق قائمة تحدد الأسماء للمختصين؛ لضمان عدم التداخل في الاختصاصات بين فريق المعاينة والمهام على كل شخص بدقة في فريق المعاينة.

(٦) مراعاة أن تتم إجراءات المعاينة في إطار المشروعية، إعمالًا لأحكام القوانين.

(٧) ضرورة تأمين عدم انقطاع التيار الكهربي؛ لكي لا يحدث تلاعب في أنظمة التشغيل.

---

(١) د. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، ورقة بحث مقدمة في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، المنعقد في الفترة من ١٢-١٤/١١/٢٠٠٧م، ص١٧ وما بعدها؛ د. عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط٢، دار النهضة العربية، القاهرة، ٢٠٠٥م، ص٣٦٤؛ د. نديم محمد حسن الترزي، سلطة النيابة العامة في الجرائم المعلوماتية، مجلة الأندلس للعلوم الإنسانية والاجتماعية العدد ١١٣، المجلد ١٥، إبريل ٢٠١٧م، ص٣١٨؛ د. هشام محمد فريد رستم، "الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٦٠ وما بعدها.

٣-التحفظ على مسرح الجريمة الإلكترونية بعد المعاينة:

من الأشياء التي يجب على مأمور الضبط القضائي والمحقق اتباعها هي التحفظ على مسرح الجريمة بعد انتهاء إجراءات المعاينة، وأن العلة لذلك إمكانية العودة كلما أراد المحققون كشف أشياء جديدة، والتأكد من أن الجاني لم يقم بإخفاء أي دليل.

ثالثًا – مسرح جريمة الاعتداء على البريد الإلكتروني ووسائل معاينتها:

من الطبيعي أن كل جريمة حدثت لا بد من مكان تقع فيه، وهذا المكان يمثل التصرفات والأعمال التي تطرأ بداخله أثناء ارتكاب العمل والسلوك المكوّن للجريمة، وهو ما يعرف بمسرح الجريمة؛ مما يؤدي إلى انتقال المحقق إليه والقيام بكافة التحريات الضرورية للمحافظة على الآثار والأدلة الإلكترونية للجريمة الإلكترونية المرتكبة قبل ضياع الأدلة وطمسها، ومن ثَمَّ فإن معاينة مسرح الجريمة الإلكترونية، هو معاينة الآثار التي يتركها مستخدم جهاز الكمبيوتر، وشبكة المعلومات التي تشمل الرسائل المرسلة منه، أو التي يستقبلها، وكافة الاتصالات التي تمت من خلال الكمبيوتر، وشبكة المعلومات، كما يعرف بأنه مناظرة وفحص ووصف المكان أو الشيء أو الشخص الذي له علاقه بالجريمة، وإثبات حالته[١].

ومسرح الجريمة له أهمية بارزة في التحقيق الجنائي، من حيث إثبات حدوث الجريمة وكشف غموضها ونسبتها إلى فاعلها ومعرفة الحقيقة[٢]؛ ذلك أن مسرح الجريمة وعاء السر المنبثق عنه أدلة الإدانة أو أدلة البراءة. فلا جدال أنه مهما كانت درجة حرص الجاني وحذره لا بد أن يترك أثرًا ما، يُستدل منه على شخصيته وتواجده في مكان ارتكاب جريمته، فالمشكلة تكمن في مدى إمكانية العثور على هذه الآثار ورفعها والتعامل معها بالمعمل الجنائي، واستغلال النتائج الدالة على ظروف ارتكاب النشاط الإجرامي.

ويمكن حصر مسرح الجريمة في جرائم الاعتداء على البريد الإلكتروني ه في الآتي:

(١) أجهزة الحاسوب بأنواعها المختلفة والمكونات المادية[٣].

(٢) أجهزة الهواتف المحمولة والهواتف الذكية وملحقاتها، فالهاتف المحمول أصبح بكل أشكاله وصوره يشكل مكانة مهمة ضمن وسائل التقنية الحديثة التي يقبل الأفراد على اقتنائها.

(٣) أجهزة الهواتف الأرضية.

---

(١) د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص١٧١.

(٢) مصعب عبدالله النقبي، جريمة إتلاف محتويات البريد الإلكتروني في التشريع الإماراتي، مجلة جامعة الشارقة للعلوم القانونية، مجلد ٢٠، العدد ٣، جامعة الشارقة، ٢٠٢٣، ص١٣٩.

(٣) المكونات المادية للكمبيوتر: وحدات الإدخال، وحدة الذاكرة الرئيسية، وحدة الحساب والمنطق، وحدة التحكم، وحدة التخزين الخارجية، وحدة الإخراج.

فمستخدم جهاز الكمبيوتر وخاصة مستخدمي شبكة المعلومات الدولية يترك آثار استخدامه في كل مكان يزوره، فالموقع الذي يمر به يفتح سجلاً خاصًا يتضمن عنوان الموقع الذي جاء منه نوع الكمبيوتر والمتصفح المستخدم له، وعنوان رقم ip الدائم أو المتغير للكمبيوتر، الذي يتصل منه، وتحت كل الظروف يمكن للموقع الحصول على عنوان البريد الإلكتروني والاسم الحقيقي.

فلمسرح الجريمة الإلكترونية مسرحان: الأول، مسرح تقليدي يقع خارج بيئة الكمبيوتر، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للكمبيوتر، ويمكن أن يحتوي على آثار مادية مثل بصمات الجاني أو وسائل تخزين رقمية. وهو أقرب ما يكون لأي مسرح جريمة تقليدية[1]. أمَّا الثاني فهو مسرح افتراضي يقع داخل بيئة جهاز الكمبيوتر وشبكاته في ذاكرته وفي الأقراص الصلبة الموجودة بداخله، فالتعامل مع الأدلة الموجوده في العالم الافتراضي في هذا الفرض من خلال جهاز كمبيوتر أو خادم، وينتقل المحقق إمّا من مكتبه من خلال جهاز الكمبيوتر خاصته، أو من خلال اللجوء إلى المقهى الخاص بشبكة الإنترنت، وأيضًا اللجوء إلى مقر عمل مزود الخدمة، الذي يعد أفضل مكان يمكن من خلاله متابعة المعاينة وإجراؤها من خلال الكمبيوتر الخاص بالخبير التقني.

لذا من الضروري العمل على تطوير سبل التحقيق الجنائي الإلكتروني بسرعة؛ ليتحقق معها اكتشاف المزيد من وسائل كشف الجريمة وغموضها، ويجب أن تتم على يد خبير متخصص في التعامل مع الأدلة الإلكترونية من هذا النوع، فالانتقال المادي لا يشكل أي عائق أمام المحقق، وإنما تكون المشكلة من خلال الانتقال إلى العالم الافتراضي، فأثناء المعاينة يجب أن تتوافر صفات خاصة فيمن يطلع على المعلومات من خلال المعاينة في إطار من المشروعية الإجرائية، التي يجب أن يقوم بها مختص، وهو ما يؤكد على أهمية التعاون الدولي في نقل الإجراءات من أجل إجراء المعاينة، وباقي إجراءات التحقيق في إطار من المشروعية الإجرائية.

([1]) د. منير محمد الجنبيهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات"، دار الفكر الجامعي، الإسكندرية، ٢٠١٩م، ص٦٣.

المطلب الثاني

التفتيش والضبط

في جريمة العدوان على البريد الإلكتروني

تمهيد وتقسيم:

يُعدُّ التفتيش من إجراءات التحقيق التي تختص بها أصلاً سلطة التحقيق، واستثناءً مأموري الضبط القضائي من جهاز الشرطة[١]، ولم يضع المشرع الجنائي تعريفًا محددًا للتفتيش كأحد الإجراءات الجنائية، إلا أن محكمة النقض المصرية قد عرّفته بأنه: "البحث عن عناصر الحقيقة في مستودع السر"[٢].

بينما عرّفه جانب من الفقه الجنائي بأنه: إجراء من إجراءات التحقيق بمقتضاه يقوم المحقق أو من يأذن له من رجال الضبطية القضائية بالبحث في منزل شخص معين على أشياء متعلقة بجناية أو جنحة قامت قرائن قوية على حيازته لها، فتفتيش الشخص عبارة عن التنقيب عن الجريمة في جسمه أو ملابسه أو ما يحمله، وهو إجراء استثنائي من الأصل[٣].

والتفتيش إجراء تختص به أصلاً سلطة التحقيق، إلا أن القانون استثنى لهذه السلطة إصدار أمر التفتيش لأحد مأموري الضبط القضائي في الجرائم المعلوماتية؛ لكي يقوم بعمل لا يتسنى لتلك السلطة القيام به، كما لو كان ينبغي القيام بالإجراء خارج نطاق الاختصاص المكاني للتحقيق، ونظرًا لما تتسم به الجريمة المعلوماتية من سرعة محو أو إخفاء أو تغيير الدليل الإلكتروني، ففي هذه الحالة يجوز للمحقق تفويض بعض سلطاته عن طريق الندب، وإن كان هذا الندب يُعدُّ عملاً استثنائيًّا[٤].

ويُعتبر التفتيش إجراءً من إجراءات التحقيق تملكه سلطة التحقيق واستثناءً من الأصل فإنه يُندب مأمورو الضبط القضائي لإجرائه تحت رقابة سلطة التحقيق، ومحكمة الموضوع، فهو ليس بغاية في حد ذاته، وإنما يُعدُّ وسيلة لغاية تتمثل فيما يمكن الوصول إليه من أدلة الجريمة، سواء المادية أو المعنوية، فيترتب على التفتيش أثر مباشر وهو ضبط هذه الأدلة، التي يتم عنها إذا ما نجم عن التفتيش إيجاد هذه الأدلة، فيعد ضبط هذه الأدلة النتيجة الطبيعية للتفتيش،

---

(١) د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، وفي ضوء الاتفاقيات والمواثيق الدولية، مرجع سابق، ص١١٣.

(٢) مجموعة أحكام محكمة النقض: ١٩٩٤/١٢/١٧م، س١٣، رقم ٢٠٠، ص٨٠٣.

(٣) انظر في ذلك: د. غنام محمد غنام، الوجيز في شرح قانون الإجراءات الجنائية، مطبعة جامعة المنصورة، ٢٠٠٩م، ص٢٠٩؛ د. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، ط٢، مطبعة نهضة مصر بالفجالة، القاهرة، ١٩٥٦م، ص٢٣٩.

(٤) د. فهد عبدالله العبيد العازمي، الإجراءات الجنائية المعلوماتية، مرجع سابق، ص٢٤٩ وما بعدها.

فالارتباط يمكن بين ضبط هذه الأدلة والتفتيش، فضبط وتفتيش ماديات الجريمة الإلكترونية يثير الكثير من الصعوبات المتعلقه بمفهوم المحل، الذي يرد عليه الضبط، ومدى إمكانية ضبط الأدلة داخل جهاز الكمبيوتر، وسنقسم هذا المطلب إلى الفرعين التاليين على النحو الآتي:

الفرع الأول: التفتيش في جرائم الاعتداء على البريد الإلكتروني.

الفرع الثاني: الضبط في جرائم الاعتداء على البريد الإلكتروني.

الفرع الاول

التفتيش في جرائم الاعتداء

على البريد الإلكتروني

التفتيش إجراء من إجراءات التحقيق تختص به بحسب الأصل سلطة التحقيق بهدف البحث عن أدلة الجريمة، ويُعدُّ من أهم إجراءات جمع الأدلة لكشف الجريمة التي وقعت، وأجيز لمأمور الضبط القضائي اتخاذه على سبيل الاستثناء في حالات معينة، وبشروط خاصة تختلف باختلاف التشريعات وباختلاف المحل الذي يرد عليه، فالتفتيش يعتبر من أهم المسائل الإجرائية الدقيقة بوجه عام التي تتصل بالمشروعية الإجرائية، وتتعلق بحقوق الأفراد كونه يمس حريتهم وحرمة مساكنهم[1]، وضمانة الدفاع لما تسببه في إباحة لانتهاك حق الخصوصية، طالما هناك مبرر لهذا الانتهاك؛ لذا فهو يُعد من أقصى الصلاحيات التي تمارسها الدولة ضد الأفراد، ويعد أحد مظاهر تقييد الحريات الإنسانية، التي أسهمت التشريعات في دعم المحافظة عليها، فالتفتيش في **جرائم الاعتداء على البريد الإلكتروني** يختلف عن التفتيش بالجرائم التقليدية لما له من طبيعة خاصة ومتميزة عن التفتيش التقليدي، فهو يحتاج إلى قواعد قانونية خاصة بسبب طبيعة الأدلة التي يمكن استخلاصها من نظم الكمبيوتر، كما أنه يتطلب لإجراء التفتيش تقنيات خاصة مختلفة عن حالات التفتيش التقليدية، فهو يهدف إلى الحصول على الأدلة التي تساعد في كشف الحقيقة الجاري التحقيق فيها، سواء كانت هذه الأدلة مادية أم أدلة إلكترونية، بما يعني أنه ليس بدليل بحد ذاته، وإنما هو وسيلة للحصول على الدليل، ولأهمية التفتيش سوف نتناول هذا الفرع من خلال الفقرات الثلاث التالية:

أولًا – مفهوم التفتيش في جرائم الاعتداء على البريد الإلكتروني:

الأصل أن التفتيش إجراء من إجراءات التحقيق، تختص به سلطة التحقيق بصفة أصلية، واستثناءً مأموري الضبط القضائي وغيره من أفراد الشرطة متى كان له هذه الصفة، ولم يحدد المشرع المقصود بالتفتيش، إلا أنه يمكن تعريفه بأنه: أحد إجراءات التحقيق التي يقوم بها

([1]) د. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسه تحليلية، دار الكتب القانونية، القاهره، ٢٠١١م، ص٤٩.

موظف مختص طبقًا للإجراءات المقررة قانونًا في محل يتمتع بالحرمة، بقصد الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها للمتهم[١].

وتفتيش الحاسوب يمكن أن يتم بطرق متنوعة، وهناك أربعة طرق أساسية ممكنة، **أولها:** تفتيش الحاسوب وطبع نسخة ورقية من ملفات معينة في ذات الوقت، **وثانيها:** تفتيش الحاسوب وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت، **وثالثها:** عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، **وأخيرًا:** إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة[٢].

والتفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية، فيُقصد به: إجراء من إجراءات التحقيق، تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات، بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها، ويثير موضوع التفتيش الذي يقع على نظم الوسائل الإلكترونية مسائل عديدة، كمدى صلاحية الكيانات المعنوية في هذه الوسائل كمحل يرد عليه التفتيش، وحكم تفتيش الوسائل التي تتصل مع بعضها البعض وتقع في أماكن عامة أو خاصة، وضوابط هذا التفتيش والضبط[٣].

والتفتيش في البيئة الإلكترونية، هو إجراء من إجراءات التحقيق، يستهدف البحث عن الحقيقة في مستودع السر، لذلك يُعتبر من أهم إجراءات التحقيق في كشف الحقيقة؛ لأنه غالبًا ما يُسفر عن أدلة مادية تزيد نسبة الجريمة إلى المتهم، والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية، تُسهم في بيان وظهور الحقيقة[٤].

والولوج إلى أنظمة المعلومات للبحث والتنقيب في البرامج المُستخدمة أو ملفات البيانات المخزنة عمّا قد يتصل بجريمة وقعت، مما يفيد بكشف الحقيقة وغموضها عن الجريمة وعن

---

(١) د. عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي – دراسة متعمقة في التعريف بجرائم التقنية الحديثة والمجرم المعلوماتي، مرجع سابق، ص٢٤٤.

(٢) د. عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي (المرشد الفيدرالي الأمريكي، لتفتيش وضبط الحواسيب وصولاً إلى الدلي الإلكتروني في التحقيقات الجنائية)، دار النهضة العربية، القاهرة، ٢٠٠٦م، ص١٧٠.

(٣) د. أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥م، ص٤٥.

(٤) المرجع السابق، ص١٤٠.

مرتكبها، وبما تقتضيه ظروف ومصلحة التحقيق في **جرائم الاعتداء على البريد الإلكتروني**، فهو ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول إلى أدلة مادية تُساعد في ظهور الحقيقة عن جريمة وقعت باستخدام الأنظمة الإلكترونية، وللتفتيش أهمية كبيرة بالنسبة للتحقيق الجنائي.

ثانيًا – تفتيش مكونات الكمبيوتر:

يعرف جهاز الكمبيوتر على أنه جهاز إلكتروني يستطيع ترجمة عمليات إدخال البيانات وإخراج المعلومات وإجراء عمليات حسابية ومنطقية، ويقوم بالكتابة على أجهزة الإخراج، فالجهاز الإلكتروني له مكونات مادية[١]، ومكونات معنوية[٢]، تشتمل برامج النظام والكيانات المعنوية التطبيقية أو برامج التطبيقات، كما أن له شبكات محلية وعالمية، مما يثير التساؤل بمدى قابلية مكونات وشبكات الأجهزه الإلكترونية للتفتيش؟ وما هي الضوابط التي يجب اتباعها في تلك الحالات؟ وهذا ما سنتناوله فيما يلي:

(١) المكونات المادية للكمبيوتر ومدى خضوعها للتفتيش:

لا يختلف اثنان في أن الولوج إلى المكونات المادية للكمبيوتر بحثًا عن شيء ما يتصل بجريمة إلكترونية وقعت يفيد في كشف الحقيقة عنها، وعن فاعلها، يخضع للإجراءات القانونية الخاصة بالتفتيش[٣]، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه تلك المكونات، وهل هو من الأماكن العامة أم من الأماكن الخاصة؟ ذلك أن لصفة المكان وطبيعته أهمية ضرورية في مجال التفتيش، فإذا كانت موجودة داخل مكان خاص كمنزل المتهم أو أحد ملحقات المنزل فلها ما في حكمه، فلا يجوز تفتيشها[٤]، إلا في الحالات التي يجوز فيها تفتيش منزله، وبذات الضمانات والإجراءات المقررة قانونًا في التشريعات المختلفة، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات، وهل يُعدُّ من الأماكن العامة أم من الأماكن الخاصة، فلوصف المكان أهمية خاصة في مجال

---

(١) تنقسم المكونات المادية للكمبيوتر إلى ست وحدات (وحدات الإدخال، وحدة الذاكرة الرئيسية، وحدة الحساب والمنطق، وحدة التحكم، وحدة المخرجات، وحدة التجزئة الثانوية).

(٢) المكونات المعنوية هي عبارة عن تعليمات مكتوبة بلغة الكمبيوتر، موجهة إلى الكمبيوتر بوصفه جهازًا تقنيًا معقدًا بغرض الوصول إلى نتيجة معينة، وتنقسم برامج الكمبيوتر إلى نوعين: برامج نظام، وبرامج التطبيقات، وهو البرنامج الخاص لمستخدم الكمبيوتر.

(٣) د. علي عواد شحاته، نحو بناء نظرية عامة لمكافحة جرائم الحاسب الآلي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠١٧م، ص٢٣٨.

(٤) د. حسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون المقارن، منشأة المعارف، الإسكندرية، ١٩٨٢م، ص٣٨٥.

التفتيش. ويجب هنا مراعاة التمييز بين ما إذا كانت مكونات الكمبيوتر المراد تفتيشها منعزلة عن غيرها من الكمبيوترات الأخرى، أم أنها متصلة بكمبيوتر آخر أو بنهاية طرفية في مكان آخر كمنزل غير المتهم، فإذا كانت كذلك، وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير، ومن شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن[١].

أمّا لو وجد شخص يحمل مكونات الكمبيوتر المادية، أو كان مسيطرًا عليها أو حائزًا لها في مكان ما من الأماكن العامة، سواء أكانت بطبيعتها كالطرق العامة والميادين والشوارع، أو كانت في الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فتفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبذات الضمانات والقيود المنصوص عليها في هذا النطاق[٢].

وأمام ما سبق، فإن حكم التفتيش بمكونات الكمبيوتر المادية لا تثير أي مشكلة؛ لكون هذه الأشياء تدخل بحكم طبيعتها في مفهوم الأشياء المادية ومن ثَمَّ يمكن لسلطات التحقيق تفتيش جهاز الحاسب أو الطابعة أو الماسح الضوئي، وغيرها من المكونات؛ سعيًا للوصول إلى الأدلة التي تُساعد بالكشف عن الحقيقة، إعمالًا للأحكام العامة في قانون الإجراءات الجنائية.

(٢) المكونات المعنوية ومدى خضوعها للتفتيش:

هناك اتجاهات فقهية ثارت بشأن جواز تفتيش المكونات المعنوية للكمبيوتر؛ تمهيدًا لضبط الأدلة الإلكترونية، وقد انقسمت الاتجاهات الفقهية إلى ثلاثة اتجاهات نستعرضها على النحو الآتي:

الاتجاه الأول: يرى جانب من الفقه أن محل تفتيش نظام للكمبيوتر بحثًا عن شيء، أي أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي إلى توسيع تفسير عبارة "ضبط أي شيء"، لتشمل كافة مكونات الحواسب المادية والمعنوية، ويقترح أنصار هذا

---

(١) د. نبيله هبه هروال، جرائم الإنترنت – دراسة مقارنة، مرجع سابق، ص٢٣٨.

(٢) منح المشرع المصري مأمور الضبط القضائي سلطة التفتيش، بتفتيش الأشخاص بشكل استثنائي في الأحوال التي يجوز فيها القبض، وقد نصت المادة ٤٠٦ من قانون الإجراءات الجنائية على أنه "في الأحوال التي يجوز فيها القبض قانونًا على المتهم يجوز لمأمور الضبط القضائي أن يفتشه، وإذا كان المتهم انثى وجب أن يكون التفتيش بمعرفة أنثى يندبها لذلك مأمور الضبط القضائي".

الرأي إضافة عبارة المواد المعالجة عن طريق الحاسب الآلي إلى النص القانوني، الذي ينص على التفتيش ليواكب التطور الحاصل في مجال تكنولوجيا المعلومات والاتصالات،[١].

الاتجاه الثاني: يرى جانب آخر من الفقه في هذا الاتجاه عدم انطباق المفهوم المادي على بيانات الكمبيوتر غير المرئية أو غير الملموسة، وهذا على النقيض من الرأي السابق؛ لذلك فإنه يقترح لمواجهة هذا القصور بالنص الصريح عن أن تفتيش الكمبيوتر يجب أن يشمل المواد المعالجة أو بياناته، بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بُعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحكم بواسطة الكمبيوتر؛ لذا فمن أعمال قواعد التفسير المنطقي أن تجعل من الكيانات المعنوية، مما يمكن تفتيشها وضبط ما بها من محتويات.

الاتجاه الثالث: وفي مقابل الرأيين أعلاه، فإن هذا الرأي ابتعد عن البحث عمّا إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الكمبيوتر أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي،الذي يتطلب أن يقع الضبط على بيانات الكمبيوتر إذا اتخذت شكلاً ماديًّا. ومن هذا المنطلق نجد أن تشريعات معظم دول العالم مدت نطاق الحماية الجنائية لحقوق المؤلِّف لتشمل برامج الكمبيوتر كقوانين حماية تقنية المعلومات، أو قوانين حماية حق المؤلِّف[٢].

وعلى ضوء الآراء الفقهية نرى أن تفتيش نظم الكمبيوتر بحثًا عن الدليل الإلكتروني في **جرائم الاعتداء على البريد الإلكتروني** يتسع ليشمل المكونات المادية والمعنوية للكمبيوتر على السواء؛ لأن ذلك هو الهدف والمطلب من الحصول على الدليل الإلكتروني، والبحث في مستودع السر للكشف عن الحقيقة وهو الهدف من إجراء التفتيش كإجراء من إجراءات التحقيق بمعناه القانوني.

ويترتب على ذلك، أنه يمكن تفتيش نظام معلومات الكمبيوتر ووسائط أو أوعية حفظ وتخزين البيانات المُعالجة إلكترونيًّا كالاسطوانات والأقراص والأشرطة الممغنطة ومخرجات الكمبيوتر، ويدخل في هذا التفتيش – أيضًا – المحتويات المخزّنة في الوحدة المركزية للنظام، والتي يمكن عزلها ككيان قائم بذاته[٣].

---

(١) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٦م، ص٢٠١.

(٢) د. علي حسن محمد الطوالبه، التفتيش الجنائي على نظم الحاسوب والإنترنت – دراسة مقارنة، ط١، كلية الحقوق، البحرين، ٢٠١٠م، ص١٣٥.

(٣) د. مصطفى علي خلف، الضوابط الإجرائية لجرائم التقنية الحديثة، رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠١٦م، ص٦٢.

هذا وقد ساير المشرع المصري التقدم التقني الذي جاوز المفهوم التقليدي للتفتيش، وذلك بما يتناسب مع هذا الغرض، فقد نص في المادة (٦) بالبند ثانيًا من الباب الثاني الخاص بالأحكام والقواعد الإجرائية من **القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات** على أنه: "لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمرًا مسببًا لمأموري الضبط القضائي المختص، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد مرة واحدة متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة مُعاقب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يأتي:.... ٢- البحث والتفتيش والدخول والنفاذ إلى قواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية؛ تحقيقًا لغرض الضبط".

وأمام ما سبق، يكون المشرع المصري قد اعترف صراحةً وبحق بإمكانية تفتيش البرامج والكيانات المعنوية، ومن ثَمَّ فإن إجراءات التفتيش للمكونات المعنوية للحاسب الآلي تجاوزت المفهوم التقليدي للإجراءات الجنائية.

(٣) مدى خضوع شبكات المعلومات للتفتيش:

تتميز أنظمة الكمبيوتر أنها تتصل مع بعضها البعض داخل حدود الدولة عن طريقة الشبكة المحلية، أو أنها تتصل بأجهزة إلكترونية أخرى تقع خارج حدود الدولة عن طريق الربط الشبكي بين أجزاء الدول المختلفة، ونظرًا للتحدي أمام أعمال التفتيش بسبب امتداد الأدلة الإلكترونية عبر الشبكات في أماكن بعيدة عن الموقع المادي للتفتيش؛ مما ثار إشكاليات حول إجراءات التفتيش للأنظمه المتصلة بالنظام المأذون بتفتيشه إذا كان في دوائر اختصاص مختلفة، مما أظهر تحديات كبيرة، بمدى قانونية هذه الإجراءات، ومدى المساس بحق الخصوصية، وفي هذا الصدد نفرّق بين عدة فروض[١]:

الفرض الأول: اتصال جهاز كمبيوتر المتهم بجهاز كمبيوتر آخر، أو نهاية طرفية موجودة في مكان آخر داخل الدولة:

في هذا الفرض فإن وقوع الجريمة في نظام الكمبيوتر يقع داخل الدولة يجوز بالنسبة لها إصدار الإذن بالتفتيش، فإن حدود هذا الإذن إعمالًا للأحكام القانونية ينفذ بالنسبة لجهاز الكمبيوتر الصادر له إذن التفتيش فقط، أمّا إذا كان جهاز الكمبيوتر المُراد تفتيشه يتصل بجهاز آخر لم يصدر له الإذن بالتفتيش، فما مدى إمكانية امتداد الحق في تفتيش جهاز الكمبيوتر أو النهاية الطرفية في منزل المتهم أو النهاية الطرفية في مكان آخر مملوك لشخص غير المتهم؟

---

(١)د. محمد محمد مصباح القاضي، الحماية الجنائية للحرية الشخصية في مرحله ماقبل المحاكمة الجنائية، دراسة مقارنة، دار النهضه العربية، القاهره، ٢٠١٠م، ص٢١١.

وجدت بعض الدول حلاً لمعالجة هذا الفرض[1]، أمّا المشرع المصري، فنجد أن البند (١) من المادة (١) من **القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات نص** على أنه: "لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمرًا مسببًا لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد مرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يأتي: ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو كمبيوتر تكون موجودة فيه. ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، على ألا يؤثر ذلك على استمرارية النظم، وتقديم الخدمة إن كان لذلك مقتضى"، وبالتفحص للنص نجد أنه استخدم في فقرة منه في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو كمبيوتر تكون موجودة فيه دون تحديد صريح، على أن هذا المكان أو البرنامج أو النظام أو الدعامة أو الكمبيوتر يقع في الخارج"، مما يدعو لتدارك المشرع لذلك باللائحة التنفيذية لهذا القانون، ويحدد موقفه المقصود بالعبارات المذكورة، وتحديد آليات وضوابط ذلك، ونرى أن النص على توسيع التفتيش في أنظمة الكمبيوتر ليشمل التفتيش عن بُعد يمثل ضرورة يجب التنبه لها من قبل المشرع؛ تلافيًا لأية صعوبات تعترض تطبيق القواعد التقليدية؛ لما لهذه الأدلة في هذه الجرائم من خصوصية تتطلب السرعه في إجراءاتها للحصول عليها، وهذا لن يتأتى إلا بالتنسيق بين الدول التي يمتد إليها نطاق التفتيش، إذا ما كان يستلزم أن يمتد إلى النطاق الإقليمي لدولة أخرى؛ مما يُعزز ضرورة التعاون الدولي في مجال الجرائم الإلكترونية.

كما أن المشرع المصري عالج هذا الفرض من خلال النص التقليدي المنظّم لإجراء التفتيش إعمالًا لأحكام الفقرة (٢) من المادة (٧١) من قانون الإجراءات الجنائية المصري[2].

وأمام ما سبق، نلاحظ أنه متى كان جهاز الكمبيوتر محل الإذن مرتبطًا بجهاز آخر، وكان الدخول للمعلومات الموجودة بهذا الجهاز تتم عن طريق الجهاز محل الإذن، فإن إذن التفتيش يمتد ليشمل ذلك الجهاز، ولو لم ينص المشرع على ذلك صراحةً في القانون المتعلق بالجرائم الإلكترونية طالما أن المشرع لم يجرّم أو يرتب بطلانًا على الدخول والتفتيش لداخل

---

(١) مما تجدر الإشارة إليه في هذا الصدد، أن بعض الدول ما زالت تعتمد القواعد الإجرائية التقليدية للتفتيش عن بُعد، ومن هذه الدول سويسرا وبلجيكا وإيطاليا والبرتغال؛ حيث تقصران التفتيش على الأجهزة الموجودة في مكان محدد، دون امتدادها إلى الأجهزة المرتبطة.

(٢) حيث نصت هذه الفقرة على أن: "للمندوب أن يجري أي عمل آخر من أعمال التحقيق أو أن يستجوب المتهم في الأحوال التي يخشى عليها من فوات الوقت متى كان متصلًا بالعمل المندوب له، ولازمًا في كشف الحقيقة.

النظام المعلوماتي المتصل بالنظام محل التفتيش بغير إذن، فيمكن للسلطة المختصة القيام بذلك وصولاً لضبط الجناة.

الفرض الثاني: اتصال جهاز كمبيوتر المتهم بجهاز آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة:

من المشاكل التي تواجه سلطة التحقيق قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج النطاق الجغرافي للدولة، وتجاوزه للحدود الجغرافية المرسومة، وهو ما يسمَّى بالتفتيش عن بُعد، وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة، التي صدر من أجهزتها المختصة بالإذن، ودخوله إلى المجال الجغرافي لدولة أخرى، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها[١].

لذا يرى جانب من الفقه أن التفتيش الإلكتروني العابر للحدود لا بد وأن يتم في إطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد، وأن تعقد هذه الاتفاقيات ما بين الدول، فلا يجوز القيام بذلك التفتيش العابر للحدود في ظل غياب الاتفاقيات، وهذا ما يؤكد على دور التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني.

ثالثًا – ضوابط التفتيش في جرائم الاعتداء على البريد الإلكتروني:

(١) وجود سبب من أسباب التفتيش:

لا يمكن اللجوء لتفتيش مكونات الكمبيوتر أو شبكاته، إلا إذا وقعت جريمة إلكترونية، وحتى يكون التفتيش مشروعًا لا بد من توافر الشروط الآتية:

(أ) أن تكون الجريمة الإلكترونية جناية أو جنحة وقعت بالفعل[٢]:

وتطبيقًا لمبدأ شرعية الجرائم والعقوبات، فلا محل لإصدار الإذن بالتفتيش، إلا إذا نص المشرع صراحةً على الأفعال التي تُشكل جرائم من هذا النوع، وهذا ما بينه المشرع المصري في المواد (١٢–٢٦) من القانون رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات[٣].

---

(١) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٧١.

(٢) الجريمة الإلكترونية: هي كل فعل غير مشروع مرتبط باستخدام الحاسب الإلكتروني لتحقيق أغراض غير مشروعة. مشار إليه لدى: د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص٣٠.

(٣) ومن أمثلة هذه الجرائم: جريمة الاعتداء على البريد الإلكتروني، وجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، والجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة، وجريمة الاعتداء على سلامة الشبكات، وجريمة الاختراق الإلكتروني، والإضرار بأنظمة المعلومات، والاعتداء على البيانات والمعلومات الشخصية، والحكومية، وغيرها من الجرائم.

(ب) توافر أمارات قوية[1]، أو قرائن قوية[2] توحي إلى وجود أدلة مادية في كشف الحقيقة بارتكاب الجريمة الإلكترونية: فلا يكفي بطبيعة الحال قيام دلائل على ارتكاب شخص أو أشخاص معينين لجريمة إلكترونية كسبب لتفتيش الكمبيوتر وشبكاته، بل لا بد أن تكون هناك أمارات قوية ودلائل وقرائن على وجود أشياء أو أدوات استخدمت في الجريمة الإلكترونية أو أشياء متحصلة منها، أومستندات إلكترونية يحتمل أن يكون لها فائدة في كشف الحقيقة لدى المتهم أو غيره؛ إذ من المقرر أن كل ما يشترط لصحة التفتيش الذي تجريه النيابة أو مأمورو الضبط القضائي قد علم من تحرياته واستدلالاته أن جريمة معينة، جناية أو جنحة، قد وقعت من شخص معين، أو أن تكون هناك من الدلائل والأمارات الكافية والشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التفتيش لحريته أو لحرمة مسكنه في سبيل كشف اتصاله بالجريمة الإلكترونية، يحتمل أن يكون لها فائدة في استجلاء الحقيقة لديه أو لدى غيره[3].

(٢) محل التفتيش في جريمة

يُقصد بمحل التفتيش هنا "كل المكونات المادية والمعنوية وشبكات الاتصال المتعلقة بالوسائل الإلكترونية، بالإضافة إلى الأشخاص[4]، الذين يستخدمون أجهزة الكمبيوتر، ومحل التفتيش في جرائم الاعتداء على البريد الإلكتروني، هو جهاز الكمبيوتر الذي يعتبر النافذة التي تطل بها الإنترنت على العالم، والشبكة التي تشمل في مكوناتها الخادم والمزود الآلي والمضيف والملحقات التقنية، وبالتالي فقد يكون محل التفتيش الشخص نفسه، أو ينصب على منزل ما [5].

وأمام ما سبق، وإعمالاً لأحكام القواعد العامة في قانون الإجراءات الجنائية المصري، وفي ضوء ما سبق بيانه، فإنه يمكن تفتيش أجهزة الكمبيوتر المملوكة للشخص، وكل ما يتعلق

---

(١) استخدم المشرع الإجرائي المصري مصطلح "أمارات قوية" في المواد (٤٧، ٩٥) من قانون الإجراءات الجنائية.

(٢) استخدم المشرع الإجرائي المصري مصطلح "قرائن قوية" في المواد (٤٩، ٩١) من قانون الإجراءات الجنائية.

(٣) د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة الإنترنت – دراسة مقارنة، مرجع سابق، ص٣٨١.

(٤) يمنح القانون محل الجريمة حصانة معينة، فيمنع إجراء تفتيشه على الرغم من توافر الشروط اللازمة للتفتيش، ويرجع سبب منح القانون لمحل معين هذه الحصانة بسبب تعلقها بمصلحة معينة عامة كانت أم فردية، يدعي المشرع أنها أولى بالرعاية من مصلحة التحقيق ومن الحصانات التي منحها القانون لأماكن وأشخاص معينين- الحصانة الدبلوماسية التي تشمل مقرات البعثات الدبلوماسية والمبعوثين الدبلوماسيين، والحصانات البرلمانية، والحصانة القضائية، للمزيد من التفاصيل: د. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، مرجع سابق، ص١٣١ وما بعدها.

(٥) نقض ١٩٩٩/١١/٤ مجموعة أحكام محكمة النقض، سنة ٥٠ ق، رقم ١١٠، ص٧٥.

بكيانه المادي وما يتصل به، كما أن المعلومات الموجودة في جهازه، باعتبارها تحمل أفكاره وقصده الجرمي وأفعاله الجرمية المتمثلة على شكل أنظمة وبرامج (مثل: المخططات الإجرامية، أو الإرهابية)، وتستمد مشروعية تفتيشها القانونية من مشروعية تفتيش المتهم نفسه.

الفرع الثاني

الضبط في جرائم الاعتداء على البريد الإلكتروني

لا يمكن أن يقع الضبط على شيء إلا بوصفه دليلاً من أدلة الجريمة، التي يجري التفتيش بشأنها، ولذلك فإنه يباشر من أجل الحقيقة، أي بمعنى: ما دام التفتيش يستهدف الحقيقة ذاتها، فيتعين أن يباشر ضبط ما يتعلق بها من أدلة، سواء كانت تفيد للادانة أم للبراءة؛ لان ما يضبط في الحالتين يحقق العدالة المنشودة، ويفيد معنى الارتباط بالتفتيش[1]، ولأهمية الضبط في **جرائم الاعتداء على البريد الإلكتروني**، التي تزداد بسبب طبيعة هذه الجرائم، سنقسم هذا الفرع إلى ثلاث فقرات، على النحو الآتي:

أولًا – مفهوم الضبط في جرائم الاعتداء على البريد الإلكتروني.

يُعدُّ الضبط النتيجة الطبيعية للتفتيش، وهو الهدف من عمل هذا الإجراء، فالارتباط مكين بين ضبط الأشياء والتفتيش، فاذا كان ضبط ماديات الجريمة في الجرائم التقليدية لا يثير أية صعوبات، إلا أن الصعوبات تبدأ بالظهور عند امتداده إلى ضبط المكونات المعنوية لتحديد مدى إمكانية ذلك، لكون طبيعة الضبط "تختلف في نطاق **جرائم الاعتداء على البريد الإلكتروني** عنه في الجرائم التقليدية؛ ذلك أن تقنية المعلومات تنطوي على حالات مختلفة من حيث ظروفها وأحوالها؛ مما يتطلب لإجراء الضبط بها تقنيات خاصة تختلف عن حالات الضبط على الموجودات التقليدية، والضبط بمعناه التقليدي الوسيلة القانونية التي تضع الجهات المختصة يدها من خلاله على كافة الأشياء من إجراءات جمع الأدلة للجريمة، التي وقعت، والناتجة عنها، أو استعملت لارتكابها، فهو الأثر المباشر لعملية التفتيش، فالارتباط مكين بين ضبط الأشياء والتفتيش، ويعرف ـ أيضًا ـ على أنه وضع اليد على الأوراق أو الأسلحة المتعلقة بالجريمة التي تفيد في كشف الحقيقة[2]، فالحكمه من هذا الإجراء تحقيق الغاية المبتغاة من التفتيش، وهي التوصل إلى الأشياء المادية ذات العلاقه بالجريمة، وتساعد المحقق في التوصل إلى الحقيقة سواء في صالح المتهم أم ضده، فإنه ينبغي إلا يقتصر الضبط على الأشياء التي تؤدي إلى

([1]) د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص٢٠٨.

([2]) د. محمد أبو العلا عقيدة، المجني عليه ودوره في الظاهرة الإجرامية، مرجع سابق، ص٣٧٣.

إدانة المتهم دون غيرها، بل إنه يتعين أن ينصب على الأشياء التي تفيد الحقيقة، أيًّا كانت، وإن أدت إلى تبرئة المتهم[١].

وقد عرف بعض الفقهاء الضبط في مجال جريمة الاعتداء على البريد الإلكتروني بأنه: "وضع اليد على الكيان المادي المخزن فيه، فهناك من يرى أن المعلومات التي تتصل بالجريمة الإلكترونية التي وقعت وتفيد في كشف الحقيقة عنها، وعن الجاني[٢].

وتطرق المشرع المصري إلى قواعد الضبط في **جرائم الاعتداء على البريد الإلكتروني** في البند (١) من المادة (٦) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات؛ إذ نصت على أن: "ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة به". كما نص البند (٢) من ذات المادة على أن: "البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزه والنظم المعلوماتية تحقيقًا لغرض الضبط".

ثانيًا – المكونات المادية والمعنوية في الجرائم الإلكترونية:

الضبط لا يرد إلا على الأشياء التي لها صلة بالجريمة، فالأشخاص لا يصلحون محلاً للضبط، فإذا تحدث المشرع الإجرائي في بعض نصوص المواد عن ضبط الأشخاص وإحضارهم، فإنه يعني بذلك القبض عليهم وإحضارهم، فالقبض نظام قانوني مختلف عن ضبط الأشياء، فالضبط لا يرد إلا على الأشياء التي لها صلة بالجريمة، فهو يرد على الأدلة المادية في الجرائم التقليدية وعلى الأدلة المعنوية في **جرائم الاعتداء على البريد الإلكتروني،**

وأمام ما سبق، لا صعوبة في تطبيق القاعدة التقليدية المتبعة في ضبط الأدلة المادية للكمبيوتر فيمكن ضبطها ولها القيمة في الإثبات لتلك الجرائم ونسبتها إلى المتهم[٣].

---

(١) د. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص٢٠٩.

(٢) د. نبيلة هبة هروال، جرائم الإنترنت – دراسة مقارنة، مرجع سابق، ص٢٦٦.

(٣) وتشمل الأشياء والمتحصلات المادية ما يلي:

(١) جهاز الكمبيوتر وملحقاته: وجود جهاز الكمبيوتر مهم جدًا حتى يمكننا القول بأن الجريمة الواقعة هي جريمة إلكترونية، وأنها مرتبطة بالمكان أو الشخص الحائز لهذا الجهاز، ولأجهزة الكمبيوتر أشكال وأحجام وألوان مختلفة، وخبير الكمبيوتر وحده الذي يستطيع التعرف على الكمبيوتر ومواصفاته بسرعة فائقة.

(٢) الورق: كثير من الجرائم الواقعة على المال أو جسم الإنسان تترك خلفها قدرًا كبيرًا من الأوراق والمستندات الرسمية منها العامة والخاصة، فوجود أجهزة الكمبيوتر تجعل من المعلومات التي يتم حفظها في الجهاز كثيرة، مما قلل من حجم الأوراق والملفات، ومع ذلك فالكثيرون يقومون بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع

وعلى الخبير الإلكتروني أن يباشر الضبط لهذه المكونات من نقل وتفريغ بذاته لضمان عدم تلف جهاز الكمبيوتر[1] وتدعيمًا لذلك، ما ورد في المادة (٥٦) من قانون الإجراءات الجنائية المصري[2].

الجريمة، فالورق أربعة أنواع: أوراق تالفة تتم طباعتها للتأكد، ومن ثَمَّ تركها في سلة المهملات، وأوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة، وأوراق تحضيرية كالمسودات، وأوراق أساسية وقانونية محفوظة في الملفات.

(٣) البرمجيات: إذا كان الدليل الإلكتروني ينشأ باستخدام برنامج خاص واسع الانتشار، فإن أخذ الأقراص الخاصة تثبت وتنصب هذا البرنامج أو في غاية الأهمية عند فحص الدليل.

(٤) وسائل التخزين المتحركة: كالأقراص المدمجة، وأقراص الليزر، والأقراص المرنة، والأشرطة المغناطيسية، والفلاش ميموري وغيرها، وتعد هذه الوسائط جزءًا من الجريمة الإلكترونية متى كانت محتوياتها تشكل عنصرًا للجريمة.

(٥) المودم: عبارة عن وسيلة تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر وسائل الاتصال المتعددة، وتطورت المودم لتكون أجهزة إرسال واستقبال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.

(٦) المراشد: الخاصة بالمكونات المادية والمنطقية للكمبيوتر، والتي تفيد بالكشف عن التفاصيل الدقيقة لكيفية عملها.

(٧) الشرائط الممغنطة: تستعمل هذه الشرائط عادة للحفظ الاحتياطي، وقد يكون في مكان بعيد آمن، كما يقوم البعض بإيداعها في خزائن البنوك التجارية ومراكز التوثيق الحكومية الآمنة.

(٨) البطاقات الممغنطة وبطاقات الائتمان والمواد البلاستيكية المستعملة في إعداد تلك البطاقات، وتعتبر قرائن للإثبات في جرائم الاعتداء على البريد الإلكتروني.

وبخصوص مكونات الكمبيوتر المادية يحتاج من القائم بضبطها عناية خاصة؛ حيث تبرز ضرورة وجود خبير إلكتروني مدرب على التعامل مع الأدلة وطرق تقييمها للتعاون مع فريق التفتيش، كونه الشخص الذي يستطيع تحديد الطريقة المناسبة، والمواد اللازمة لضبطها وحفظها وتغليفها والمقاومة للكهرباء الساكنة والحرارة، مثل: الأغطية البلاستيكية، ورغوة التغليف، والصناديق الكرتونية .. وغيرها من الموادد. راجع في ذلك: خالد ممدوح إبراهيم، "فن التحقيق الجنائي في الجرائم الإلكترونية"، مرجع سابق، ص٢٧٥؛ د. كمال أحمد الكركي، التحقيق في جرائم الحاسوب، بحث مقدم، المؤتمر العلمي الأول، للجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات، ٢٠٠٣م، ص٢٢.

(١) د. عبدالفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، مرجع سابق، ص٢٢٧.

(٢) والتي نصت على أن: "توضع الأشياء والأوراق التي تضبط في حرز مغلق، وتربط كلما أمكن، ويختم عليها، ويكتب على شريط داخل الختم تاريخ المحضر المحرر بضبط تلك الأشياء، ويُشار إلى الموضوع الذي حصل الضبط من أجله".

ونأمل من المشرع المصري، ضرورة تحديد الجهة التي تتولى مساعدة جهات التحقيق في ضبط الأدلة، وتقديم المساعدة خلال التحقيق في أمور الضبط للبحث عن الأدلة في هذا النوع من الجرائم.

ولا يختلف الحديث عن مدى صلاحية ضبط المكونات المعنوية للجرائم الإلكترونية عما تم ذكره سابقًا في الحديث عن مدى صلاحية ضبط المكونات المعنوية للتفتيش، إلا أن ضبط المكونات المعنوية لجهاز الكمبيوتر أكثر صعوبة وتعقيدًا[١]، ولهذا ثار الجدل الفقهي بين فقهاء القانون الجنائي.

ثالثًا – ضبط المراسلات الإلكترونية:

الضبط لا يقف عند المكونات المادية أو المعنوية في الوسائل الإلكترونية ويمكن – أيضًا – أن يشمل المراسلات الإلكترونية التي تتم من خلال هذه الوسائل، فالمراسلات تعرف بصفة عامة "أنها جميع الرسائل لدى مكاتب البرق والمحادثات السلكية واللا سلكية[٢]، وأحاط المشرع ضبط المراسلات الإلكترونية بضمانات عدة؛ حماية لحرمة الحياة الخاصة[٣].

ولقد تطلب المشرع المصري لضبط المراسلات بأنواعها المختلفة أن يكون إجراء الضبط مفيدًا في ظهور الحقيقة، أو أن يكون ذلك بصدد جريمة أو جنحة، فمثلاً ما نصت عليه المادة (٩٥) من قانون الإجراءات الجنائية المصري[٤].

---

(١) المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في ريودي جانيرو بالبرازيل في الفترة من ٤-٩ سبتمبر ١٩٩٤.

(٢) تنص المادة (٥٧) من الدستور المصري الحالي ٢٠١٤م على أن: "للحياة الخاصة حرمة، وهى مصونة لا تمس.

وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون.

كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها ، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك".

(٣) د. هلالي عبد اللاه أحمد، "تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي"، مرجع سابق، ص٢٨١.

(٤) حيث تنص هذه المادة على أن: "لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق، وأن يأمر بمراقبة المحادثات السلكية واللا سلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص، متى كانت هناك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر، وفي جميع الأحوال يجب

وأمام ما سبق، يُعدُّ الضبط في العالم الافتراضي هو النتيجة المترتبة على إجراءات التحقيق الابتدائي والتفتيش الصحيح لنظام الكمبيوتر.

وقد حرصت الدساتير وإعلانات حقوق الإنسان[١] والمواثيق والاتفاقيات الدولية والإقليمية على حرمة المراسلة للإنسان، وعدم التدخل التعسفي وغير المبرر قانونًا أو رقابيًّا أو مصادرتها أو الاطلاع عليها إلا في أضيق الحدود وطبقًا للقواعد الإجرائية التي حددها المشرع بأنه يجب حمايتها فلا يجوز التنصت عليها أو الاطلاع على الأسرار التي تحويها[٢]، فتتسم المراسلات بالبريد الإلكتروني بخصوصية تتوافر فيها عنصران، هما: العنصر الموضوعي والذي يتعلق بمضمون الرسالة، أن تكون ذات طابع شخصي أو خاص فيما يخبر به، وعنصر شخصي، كإرادة المرسل بتحديد رغبته عدم السماح للغير للاطلاع على مضمون الرسالة، فأكدت المحكمه العُليا في كندا على هذا العنصر بالقول: "إن الحالة الذهنية للمرسل هي الحاسمة .

أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناء على أمر مسبب ولمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمدة أو مدد أخرى".

(١) وهو ما تضمنته المادة (١٢٥) من الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في ١٩٨٤٥/١٢/١٠ والتي نصت على أنه: "لا يجوز تعرض أحد لتدخل تعسفي في حياته الخاصة، أو مراسلاته، ولكل شخص الحق في الحماية القانونية ضد هذا التدخل".

(٢) راجع في ذلك، نص المادة (٢٠٦) من قانون الإجراءات الجنائية المصري؛ حيث تنصت على أنه: "لا يجوز للنيابة العامة تفتيش غير المتهم أو منزل غير منزله إذا اتضح من أمارات قوية أنه حائز لأشياء تتعلق بالجريمة، ويجوز لها أن تضبط لدى مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب البرق وجميع البرقيات وأن تراقب المحادثات السلكية واللا سلكية، وأن تقوم بتسجيلات لمحادثات جرت في مكان خاص، متى كان لذلك فائدة في ظهور الحقيقة من جناية أو في جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر، ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول مقدمًا على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق، وفي جميع الأحوال يجب أن يكون الأمر بالضبط أو الاطلاع أو المراقبة لمدة لا تزيد على ثلاثين يومًا ويجوز للقاضي أن يجدد هذا الأمر مدة أو مددًا أخرى مماثلة، وللنيابة العامة أن تطلع على الخطابات والرسائل والأوراق الأخرى والتسجيلات المضبوطة، على أن يتم كلما أمكن ذلك بحضور المتهم والحائز لها أو المرسلة إليه، وتدون ملاحظاتهم عليها، ولها حسب ما يظهر من الفحص أن تأمر بضم تلك الأوراق إلى ملف الدعوى أو بردها إلى من كان حائزًا لها أو من كانت مرسلة إليه".

الخاتمة

جاء هذا البحث في مقدمة ومبحثين، أولهما عن: الأحكام الموضوعية لجريمة الاعتداء على البريد الإلكتروني، والثاني: الأحكام الإجرائية لذات الجريمة، وخاتمة بينا فيها أهم النتائج والتوصيات، وهو ما نبينه فيما يلي:

أولاً – نتائج البحث:

(١) أن الجرائم الإلكترونية بشكل عام، وجريمة الاعتداء على البريد الإلكتروني بشكل خاص، أصبحت مصدر قلق لكافة المجتمعات؛ لما تمثله هذه الجرائم صعوبة ضبطها والقبض على من يرتكبها وإثباتها؛ حيث تُعد من نوع الجرائم العابرة لحدود الدول.

(٢) تبين من الدراسة عدم كفاية القواعد العامة في قانون العقوبات المصري، لمكافحة هذه الجريمة، وهو ما جعل المشرع المصري، يصدر القوانين التي تناسب مكافحة هذه الجريمة ومواجهتها.

(٣) يحمد للمشرع المصري سياسته الجنائية في الحماية الجنائية التي اتبعها لحماية البريد الإلكتروني من صور الاعتداء عليه، مما يدل على مواكبته للتطورات المستجدة في الجرائم الإلكترونية مما يجعله على قائمة التشريعات، التي تنبهت إلى خطورة جريمة الاعتداء على البريد الإلكتروني ومن ثم تحقيق الضمانات الكافية لحماية المجتمع من آثار هذه الجرائم الخطرة.

(٤) تبين لنا أن جريمة الاعتداء على البريد الإلكتروني التي يمكن لمن تتوافر لديه دراية فنية، ارتكابها في أي مكان وضد أس شخص على مستوى العالم دون أدنى عناء متى شاء وكيف شاء، دون الأخذ في الاعتبار بحدود المكان والزمان.

(٥) تقوم جريمة الاعتداء على البريد الإلكتروني على ركنيها المادي والمعنوي، ويستحيل قيام المسئولية الجنائية عن ارتكابها دون وجود هذين الركنين.

(٦) يتكون النشاط الجنائي لجريمة الاعتداء على البريد الإلكتروني من صور عديدة، من أبرزها وأكثرها انتشارًا الدخول غير المصرح به.

(٧) اشتمل القانون المصري رقم (١٧٥) لسنة ٢٠١٨م بشأن جرائم مكافحة جرائم تقنية المعلومات، على عقوبات أصلية تمثلت في الحبس والغرامة، وعقوبات أخرى التبعية، كالمصادرة وإغلاق الموقع، وإبعاد الأجنبي وعزل الموظف.

ثانيًا – توصيات الدراسة:

ترتيبًا على النتائج المتقدمة، نوصي بالآتي:

(١) السعي على وجود تنسيق دولي – أكثر فعالية – بين التشريعات الجنائية بعية وضع قانون دولي موحد لمكافحة الجرائم الإلكترونية واللتصدي لمرتكبيها، مع مراعاة إجراءات التفتيش والضبط على نحو لا ي يؤثر على حقوق الإنسان وحرياته.

(٢) نناشد مشرعنا المصري العمل على إجراء التعديلات المناسبة على بعض مواد قانون الإجراءات الجنائية المصري، ليشتمل بالإضافة إلى القواعد العامة، قواعد خاصة تتناسب والتطور التكنولوجي الذي يشهده العصر الحالي.

(٣) نناشد المجتمع الدولي ضرورة السعي إلى إنشاء لجان مشتركة لمكافحة الجرائم الإلكترونية ووأدها في مهدها قبل استفحال خطرها.

(٤) نناشد السلطات المختصة، العمل الجاد على نشر الوعي الأمنى المعلوماتي ونشر الثقافة التكنولوجية لدى كل موظف عام في الدولة، خاصة من تكون وظيفته إدخال البيانات إلى الحاسب الآلي، بحيث لا أن يكتفى بكونه موظفًا تقتصر وظيفته على إدخال البيانات فقط، وإنما يلزم أن يتعلم كيفية تأمين البيانات المدخلة من قبله.

قائمة المصادر والمراجع[1]

(١) إبراهيم عبدالخالق، الشامل في جرائم الإنترنت في ضوء قانون العقوبات، المكتب الفني للإصدارات القانونية، القاهرة، ٢٠٢١م.

(٢) إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقًا للمرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، ٢٠١٨م.

(٣) أحمد خليفة الملط، الجرائم المعلوماتية، ط٢، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.

(٤) أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، الكتاب الأول، ط٦، دار النهضة العربية، القاهرة، ٢٠١٦م.

(٥) اردلان نور الدين محمود، أحكام الجرائم الماسة بأمن الدولة في القانون والشريعة الإسلامية، ط١، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٤م.

(٦) الإرهاب الإلكتروني الظاهرة والمواجهة، الإصدار الحادي والستون، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، ٢٠١٦م.

(٧) أسامة أحمد المناعسة، وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة، ط٣، دار الثقافة للنشر والتوزيع، عمان – الأردن، ٢٠١٧م.

(٨) أسامة محمد حسن، مختارات من قانون الإجراءات الجنائية، ط١، دار النهضه العربية القاهره، ٢٠١٩م.

(٩) أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥م.

(١٠) ألن نيبارو، الإنترنت، ترجمة: مركز التعريب والبرمجة طبعة الدار العربية للعلوم.

(١١) أمجد الكردي، المشاكل العملية التي تواجه النيابة العامه في التحقيق الأولي، دار اليراع للنشر والتوزيع، عمان، ٢٠٠٧م.

(١٢) بوعزاتي عبدالكريم، جريمة الإرهاب السيبراني بين التشريع المغربي والمقارن، مجلة الأبحاث والدراسات القانونية، المركز المغربي للدراسات والإستشارات القانونية وحل المنازعات، العدد ٢١، ٢٠٢٢م.

(١٣) التحريض الإلكتروني، وزارة الداخلية المصرية، أكاديمية الشرطة، مركز بحوث الشرطة، الإصدار التاسع والأربعون، ٢٠١٤م.

---

[1] **تم ترتيب قائمة المصادر والمراجع ترتيبًا أبجديًا، مع الاحتفاظ للجميع بألقابهم ودرجاتهم العلمية.**

(١٤) توفيق عبد الله أحمد الخشاشنة، معاينة مسرح الجريمة من خلال شبكة المعلومات الدولية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٦م.
(١٥) حسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون المقارن، منشأة المعارف، الإسكندرية، ١٩٨٢م.
(١٦) حسين بن سعيد الغافري، السياسة الجنائية في مواجهة الإنترنت – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٩م.
(١٧) خالد ممدوح إبراهيم، الجريمة المعلوماتية، ط٢، دار الفكر الجامعي، الإسكندرية، ٢٠١٩م.
(١٨) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠١٠م.
(١٩) دلال لطيف مطشر، جريمة الاعتداء على المواقع الإلكترونية – دراسة مقارنة، مجلة جامعة بابل للعلوم الإنسانية، المجلد ٢٦، العدد ٩، ٢٠١٨م.
(٢٠) رامي متولي القاضي، شبكة الإنترنت المظلمة، مجلة الأمن العام، العدد ٢٠٢٥، أكتوبر ٢٠٢١م.
(٢١) رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، وفي ضوء الاتفاقيات والمواثيق الدولية، ط١، دار النهضة العربية، القاهرة، ٢٠١١م.
(٢٢) رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، ط٢، مطبعة نهضة مصر بالفجالة، القاهرة، ١٩٥٦م.
(٢٣) سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي – دراسة مقارنة، دار الكتب القانونية، ودار شتات للنشر والبرمجيات، (مصر، الإمارات)، ٢٠١١م.
(٢٤) سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسه تحليلية، دار الكتب القانونية، القاهره، ٢٠١١م.
(٢٥) صباح كزيز، سمير قط، أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجًا، مخبر أثر الاجتهاد القضائي على حركة التشريع – كلية الحقوق والعلوم السياسية، جامعة محمد خيضر – بسكرة، الجزائر، مجلة الناقد للدراسات السياسية، العدد الثالث، أكتوبر ٢٠١٨م.
(٢٦) طارق بن عبد الله الشدي، آلية البناء الأمني لنظم المعلومات، ط١، دار الوطن للطباعة والنشر والإعلام، ٢٠٠٠م.

(٢٧) عبد الإله النوايسة، جرائم تكنولوجيا المعلومات – شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط١، دار وائل للنشر والتوزيع، عمان – الأردن، ٢٠١٧م.
(٢٨) عبد الرحمن بن محمد الدخيّل، اختراق المواقع على الشبكة العالمية للمعلومات – دراسة مقارنة، رسالة ماجستير، جامعة الإمام محمد بن سعود الإسلامي، المعهد العالي للقضاء، المملكة العربية السعودية، ١٤٢٣هـ –١٤٢٤هـ.
(٢٩) عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ٢٠٠٠م.
(٣٠) عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، ط١، المركز القومي للإصدارات القانونية، ٢٠١٢م.
(٣١) عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي – دراسة متعمقة في التعريف بجرائم التقنية الحديثة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٩م.
(٣٢) عبد الله جفعر الكوفلي، مراقبة الاتصالات في التنظيم الدولي والداخلي، المركز القومي للإصدارات القانونية، القاهره، ٢٠١٧م.
(٣٣) عبد الله حسين محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات المنعقد في الفترة ٢٦–٢٨ أبريل ٢٠٠٣م، دبي – الإمارات العربية المتحدة.
(٣٤) عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، ٢٠١٤م.
(٣٥) عبد الله عبد الكريم، جرائم المعلومات والإنترنت، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧م.
(٣٦) عبد الله علي عبد الله القحطاني، إدارة أمن المعلومات ودورها في الحد من الإرهاب الإلكتروني بكلية الحاسبات وتقنية المعلومات بجامعة الملك عبد العزيز بجدة، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض – المملكة العربية السعودية، ١٤٣٨هـ/٢٠١٧م.
(٣٧) عبد الله محمد الحضري، جريمة الدخول بغير وجه حق إلى المواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطري– دراسة تحليلية مقارنة، رسالة ماجستير، كليّة القانون – جامعة قطر، ٢٠٢٠م.

(٣٨) عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في محكافحة جرائم الإرهاب المعلوماتي، بحث ضمن دورة تدريبية بعنوان: مكافحة الجرائم الإرهابية المعلوماتية، خلال الفترة من: ١١-١٤٢٧/٣/١٥هـ، الموافق ٩- ٢٠٠٦/٤/١٣م، المغرب – القنيطرة.

(٣٩) عبد المنعم يوسف بلال، البريد الإلكتروني، مجلة كمبيوتر، القاهرة، العدد ٦٣، مايو١٩٩٣م.

(٤٠) عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، ورقة بحث مقدمة في المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، المنعقد في الفترة من ١٢-٢٠٠٧/١١/١٤م.

(٤١) عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، ٢٠٠٥م.

(٤٢) عبدالحليم محمد الشريف بن مشري، ضرورة تجريم الاعتداء على البريد الالكترونى، مجلة العلوم القانونية، جامعة الزيتونة – كلية القانون ترهونة، السنة ٤، العدد ٧، ٢٠١٦م.

(٤٣) عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط٢، دار النهضة العربية، القاهرة، ٢٠٠٥م

(٤٤) عبدالله ذيب محمود، جريمة الاختراق الواقعة على البيانات والمواقع الحكومية – دراسة مقارنة على التشريعات الأردنية والفلسطينية، مجلة المنارة للدراسات القانونية والإدارية، عدد خاص حول الثورة الرقمية وإشكالاتها أبريل ٢٠٢٠م.

(٤٥) عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، المجلد رقم (٢٤) – العدد رقم (٩٥) أكتوبر، ٢٠١٥م.

(٤٦) علي حسن محمد الطوالبه، التفتيش الجنائي على نظم الحاسوب والإنترنت – دراسة مقارنة، ط١، كلية الحقوق، البحرين، ٢٠١٠م.

(٤٧) علي عدنان الفيل، جريمة الاحتيال عبر البريد الإلكتروني – دراسة مقارنة، مجلة الحقوق، الكويت، العدد الثاني، السنة السادسة والثلاثون، يونيو ٢٠١٢م.

(٤٨) علي عواد شحاته، نحو بناء نظرية عامة لمكافحة جرائم الحاسب الآلي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠١٧م.

(٤٩) عمر السعيد رمضان، قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، القاهره، ١٩٨٥م.

(٥٠) عمر حوتية، وآخرون، تجربة دولة الإمارات في التصدي للجرائم المعلوماتية الواقعة على التجارة الإلكترونية – المجلة الأردنية للمكتبات والمعلومات – جمعية المكتبات والمعلومات الأردنية – الأردن، المجلد ٥٠ العدد ٤، كانون الأول ٢٠١٥م.

(٥١) عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي (المرشد الفيدرالي الأمريكي، لتفتيش وضبط الحواسيب وصولاً إلى الدلي الإلكتروني في التحقيقات الجنائية)، دار النهضة العربية، القاهرة، ٢٠٠٦م.

(٥٢) العمري عيسات، الجريمة الالكترونية لدى المراهقين: دوافع الإقبال وآليات الضبط الاجتماعي، مجلة علوم الإنسان والمجتمع، جامعة محمد خيضر بسكرة – كلية العلوم الإنسانية والاجتماعية، المجلد ١١ العدد١، ٢٠٢٢م.

(٥٣) عوض محمد عوض، المبادئ العامه في قانون الإجراءات الجنائية، دار المطبوعات الجنائية، الاسكندرية، ١٩٩٩م.

(٥٤) غادة نصار، الجرائم الإلكترونية، ط١، دراسات في الإعلام، مصر، ٢٠١٧م.

(٥٥) غنام محمد غنام، الوجيز في شرح قانون الإجراءات الجنائية، مطبعة جامعة المنصورة، ٢٠٠٩م

(٥٦) غنام محمد غنام، الوجيز في شرح قانون العقوبات، مطبعة جامعة المنصورة والكتاب الجامعي، المنصورة، ٢٠٠٨م.

(٥٧) فاضل زيدان، سلطة القاضي الجنائي في تقدير الأدلة، مكتبة دار الثقافة للنشر والتوزيع، عمان، ١٩٩٩م.

(٥٨) فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٦م.

(٥٩) فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٥م.

(٦٠) كاظم عبد الله نزال المياحي، حجية المراقبة الإلكترونية للصوت والصورة في الإثبات الجنائي – دراسة مقارنة في القانون العراقي والمقارن، رسالة دكتوراه كلية الحقوق، جامعة عين شمس،٢٠١٦م.

(٦١) كمال أحمد الكركي، التحقيق في جرائم الحاسوب، بحث مقدم، المؤتمر العلمي الأول، للجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات، ٢٠٠٣م.

(٦٢) لورنس حوامدة، الجرائم المعلوماتية وأركانها وآلية مكافحتها – دراسة تحليلية مقارنة، بحث منشور في مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية، المجلد الرابع، العدد الأول، كانون الثاني، ٢٠١٧م.

(٦٣) ماجد بن كريم الزارع، الركن المادي في الجرائم الإلكترونية في النظام السعودي – دراسة تأصيلية، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٤م.
(٦٤) محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية شرطة دبي، يناير ٢٠٠٤م.
(٦٥) محمد أبو العلا عقيدة، "شرح قانون الإجراءات الجنائية"، الجزء الأول، دار النهضة العربية، القاهرة، بلا سنة نشر.
(٦٦) محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، ط١، جامعة نايف للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، ٢٠٠٩م.
(٦٧) محمد الشهاوي، شرح قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣، ط١، دار النهضة العربية، القاهرة، ٢٠١٠م.
(٦٨) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان – الأردن، ٢٠١٥م.
(٦٩) محمد زكي أبو عامر، الإجراءات الجنائية، ط٢، منشأة المعارف، الإسكندرية، ١٩٩٠م.
(٧٠) محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط٢، دار النهضة العربية، القاهرة، ١٩٩٨م.
(٧١) محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، مايو ٢٠٠٠م.
(٧٢) محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦م.
(٧٣) محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، ط١، كتاب الجمهورية، مصر، ٢٠١٠م.
(٧٤) محمد علي سويلم، الإثبات الجنائي عبر الوسائل الإلكترونية– دراسة مقارنة، دار المطبوعات الجامعية، ٢٠٢٠م.
(٧٥) محمد عيد الغريب، مدى انطباق الأحكام العامة في قانون العقوبات على المشاكل القانونية التى كشف عنها استخدام وسائل التكنولوجيا (الحاسب الإلكتروني)، في الدورة المنعقدة بمركز الأستاذ الدكتور/عبد الرؤوف مهدى للبحوث الجنائية بكلية الحقوق، جامعة المنصورة – مصر، يوم السبت الموافق ٢٠١٢/٣/١٧م،
(٧٦) محمد قيراط، الإعلام الجديد والإرهاب الإلكتروني، آليات الاستخدام وتحديات المواجهة، مجلة الحكمة للدراسات الإعلامية والاتصالية – مؤسسة كنوز الحكمة للنشر والتوزيع – الجزائر، العدد التاسع، يناير ٢٠١٧م.

(٧٧) محمد محمد مصباح القاضي، الحماية الجنائية للحرية الشخصية في مرحله ما قبل المحاكمة الجنائية، دراسة مقارنة، دار النهضه العربية، القاهره،٢٠١٠م.
(٧٨) محمود عبد العزيز أبو زيد، الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية، رسالة دكتوراه، كلية الحقوق – جامعة القاهرة، ٢٠١٦م.
(٧٩) محمود نجيب حسني، شرح قانون العقوبات – القسم العام، ط٨، دار النهضة العربية، القاهرة، ٢٠١٦م.
(٨٠) مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م.
(٨١) مساعد بن عبد العزيز بن إبراهيم، عقوبة الغرامة في الشريعة والقانون وتطبيقاتها في اللجان الجمركية بمدينة الرياض، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، ٢٠٠٢م.
(٨٢) مصطفى علي خلف، الضوابط الإجرائية لجرائم التقنية الحديثة، رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠١٦م.
(٨٣) مصطفى محمد الدغيدي، التحريات والإثبات الجنائي، دار النهضة العربية، القاهرة، ٢٠٠٢م.
(٨٤) مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، ٢٠٠٥م.
(٨٥) مصعب عبدالله النقبي، جريمة إتلاف محتويات البريد الإلكتروني في التشريع الإماراتي، مجلة جامعة الشارقة للعلوم القانونية، مجلد ٢٠، العدد ٣، جامعة الشارقة، ٢٠٢٣م.
(٨٦) منير محمد الجنبيهي، د. ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.
(٨٧) منير محمد الجنبيهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات"، دار الفكر الجامعي، الإسكندرية، ٢٠١٩م.
(٨٨) موسى مسعود أرحومة، الإرهاب والإنترنت، مجلة دراسات وأبحاث، جامعة الجلفة – الجزائر، العدد الرابع، ٢٠١١م.
(٨٩) نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الأردني، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م.
(٩٠) نبيل عبد المنعم جاد، أسس التحقيق والبحث الجنائي العلمي، مطبعة كلية الشرطة، القاهرة، ٢٠٠٥م.

(٩١) نبيلة هبه هروال، جرائم الإنترنت – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد – الجزائر، ٢٠١٣م/ ٢٠١٤م.
(٩٢) نديم محمد حسن الترزي، سلطة النيابة العامة في الجرائم المعلوماتية، مجلة الأندلس للعلوم الإنسانية والاجتماعية العدد ١١٣، المجلد ١٥، إبريل ٢٠١٧م
(٩٣) هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، ط١، دار النهضه العربية، القاهره، ١٩٩٢م.
(٩٤) هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠م.
(٩٥) هشام محمد فريد رستم، الجوانب الإجرامية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ١٩٩٤م.
(٩٦) هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م.
(٩٧) هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٦م.
(٩٨) هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، ٢٠٠٣م.
(٩٩) هيثم عبدالرحمن البقلي، الجرائم الإلكترونية الواقعة على العرض، ط١، دار العلوم للنشر والتوزيع، مصر، ٢٠٢٠م
(١٠٠)ياسر نوار، المواجهة التشريعية والأمنية لجرائم التجارة الإلكترونية، ط١، بدون دار نشر، ٢٠١٢م.
(١٠١)يونس عرب، جرائم الإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل، مقدمة إلى مؤتمر الأمن العربي، ٢٠٠٢م، المنظم بالمركز العربي للدراسات والبحوث الجنائية، أبوظبي، في ٢٠١٢/١٢/١٠م.