جريمة اختراق البريد الالكتروني
The E-mail hacking crime

أ. معمر بن علي
دكتوراه في القانون الخاص
جامعة عمار ثليجي الأغواط – الجزائر–

الملخص:

تتمحور دراستنا عن جريمة قرصنة البريد الالكتروني، حيث نقوم بتعريف البريد الالكتروني وعلاقته بهوية الشخص الذي يجب على هذا الأخير ملأ معلوماته ليتسنى له الحصول على بريد الكتروني، كما نسعى في ورقتنا البحثية إلى إعطاء نظرة لصور الاعتداء على البريد الالكتروني من بينها انتهاك الحياة الخاصة للأفراد وجريمة الدخول غير المصرح به ، والإجراءات التي تتخذها الهيئات المختصة للتحري وجمع الأدلة خصوصا عند تحقق جريمة الاختراق.

الكلمات الدالة: البريد الالكتروني، صور الاعتداء، إجراءات التحري، جمع الأدلة.

Abstract:

Our study focus on the e-mail piracy crime, where we define e-mail and its relationship to the identity of the person whose information that the latter ought to fill in, in order to get an e-mail. we also in our rechearch paper seek to give a look at the types of e-mail assault, including the violation of the private individuals life and the crime of the unauthorized entry and the procedures who are taken by competent authority to investigate and collect evidence, especially when The crime of hacking has been achieved.

Keywords : E-mail, the assault types, the investigate procedures, the evidence collect.

المقدمة:

تعرف الجرائم الالكترونية بأنها الأنشطة الالكترونية التي ترتكب عمداً بدافع إجرامي لإلحاق ضرر مادي أو ضرر معنوي بشخص ما أو جهة ما، سواءً بشكل مباشر أو غير مباشر، والهدف من هذه الأنشطة غير المشروعة هي من أجل تحقيق مكاسب مادية أو معنوية أو خدمة أهداف سياسية أو الهدف منها ابتزاز الضحية وتشويه سمعتها، ووسائل هذه الجرائم الالكترونية تعتمد أساساً باستخدام الحاسوب الآلي مع اتصاله بالإنترنت.

لذلك سارعت الكثير من الدول من خلال الجهات القانونية المعنية بالبحث في مواجهة تلك الظواهر المستحدثة من الإجرام، وذلك بالبحث عن كيفية الحماية لنظم المعلومات، فالفقه أخذ بالبحث عن الحماية الملائمة، لكي يمهد للمشرع اختيار وانتقاء الحماية الملائمة لمواجهة تلك الجرائم، ولعل أهم الجرائم التي تخطر ببالنا هي جريمة اختراق البريد الالكتروني دون إذن مصرح به والإطلاع على سرية مراسلات مع انتهاك حرمة الخاصة بالمراسلات، وقد يعتمد مرتكب هذه الجريمة على نفس الوسائل المستعملة في الجرائم الالكترونية إلا أنها تختلف في البرامج المستعملة للاختراق، ومن خلال ما سبق ذكره طرحنا الإشكالية التالية **ما هي الإجراءات المتبعة لإثبات جريمة اختراق البريد الالكتروني؟**

ولمعالجة هذه الإشكالية اتبعنا المنهج الوصفي والتحليلي والمنهج المقارن، وذلك عن طريق تحليل النصوص القانونية الصادرة عن التشريع الجزائري ومقارنتها مع القوانين المقارنة واستخراج أوجه التشابه والاختلاف، وترجيح الأصلح منها، ولحل هذه الإشكالية قسمنا بحثا إلى مبحثين:

المبحث الأول: مفهوم جريمة اختراق البريد الالكتروني

المبحث الثاني: إجراءات التحري والتحقيق وجمع الأدلة لإثبات جريمة الاختراق.

المبحث الأول: مفهوم جريمة اختراق البريد الالكتروني

قبل التطرق إلى مفهوم جريمة قرصنة البريد الالكتروني يجب أن نعرف المقصود بالبريد الالكتروني الذي يقوم باستعماله كافة مستخدمي الانترنت وذلك لتسهيل الاشتراك في مواقع الانترنت وحسن التعامل بالأنشطة التجارية سواء من طرف المستهلك أو التاجر، وعلاقة جريمة الاختراق بمساس الحياة الخاصة للفرد.

المطلب الأول: تعريف البريد الالكتروني:

يُقصد بالبريد الالكتروني استخدام شبكة الانترنت في نقل الرسائل بدلاً من الوسائل التقليدية، بحيث يسمح أي البريد الالكتروني بتبادل المراسلات من وثائق، ومطبوعات وأفلام أياً كان حجمها.

ويتم ذلك بتخصيص صندوق بريد الكتروني، وهو عبارة عن ملف وحدة الأقراص الممغنطة التي تستخدم في استقبال الرسائل لكل شخص خاص به، حيث ترسل الرسالة إلى عنوان الشخص بحيث

يستطيع هو وحده أن يطَّلع عليها باستخدام كلمة سر خاصة به لفتح الصندوق، والإطلاع على الرسائل الالكترونية التي يرسلها إليه الغير[1]، وبذلك يمكن للشخص تصفح بريده الالكتروني في أي وقت يشاء للرد عليه إن أراد ذلك سواء كان الرد مباشرة أو قد يتم تأجيل الإرسال إلى وقت أخر محدد[2].

وتُعد خدمة البريد الالكتروني من أهم الخدمات التي توفرها شبكة الانترنت، وأكثر أدواتها استعمالاً، وهي تُتيح للمشترك تبادل الرسائل الالكترونية بسرعة فائقة وبتكاليف أقل، وفي أي وقت وعلى مدار الساعة، إذ يكون لكل مشترك في البريد الالكتروني عنوان فريد ومتميز، وكذلك صندوق بريد الكتروني خاص به على مستوى الشبكة ككل. ويمكن للمتصل بالشبكة الذي يمتلك عنوان بريد الكتروني خاص به أن يرسل رسائل الكترونية باستخدام هذه الخدمة إلى مشترك آخر بالبريد الالكتروني، ويستطيع المشترك أن يرسل الرسالة نفسها إلى عدد غير محدد من المشتركين قد يبلغ عشرات الآلاف من العناوين البريدية[3].

المطلب الثاني: علاقة البريد الالكتروني بهوية الشخص:

يُعد البريد الالكتروني وسيلة لتحديد هوية أي شخص والذي يتم من خلاله التعرف عليه في حالة التسوق في الانترنت، وتتحدد هويته من اسم ولقب وعنوان، وكذا أهليته من خلال بيانات بريده الالكتروني، الذي يشمل على العناصر الأساسية لتحديد الهوية. وبهذا الصدد قد تكون الهوية الالكترونية مطابقة للهوية الحقيقية أو تكون مخالفة لها في أنها تشمل على بيانات مختارة من صاحبها، والمقدمة آلياً من قِبل نظام المعلومات الآلي، وجرت العادة في هذه الحالة من المعاملات الالكترونية على اعتبار الهوية الالكترونية ملزمة لصاحبها[4].

وبذلك يكون للشخص عنوان بريده الالكتروني وملء الاستمارة المخصصة لذلك، فالبيانات التي ملئها الشخص قصد الحصول على بريده تعتبر جد مهمة في حالة ما إذا كان يريد التعاقد بها[5]، وتقوم

1. حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، مصر، 2000، ص 08.
2. محمود عبد الرحيم الشريفات، التراضي في تكوين العقد عبر الانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص 31.
3. محمد عبد الرزاق محمد عباس، النظام القانوني لعقد الاشتراك في خدمة الانترنت، ب. ط، دار الفكر والقانون للنشر والتوزيع، مصر، 2016، ص 26.
4. يمينة حوحو، عقد البيع الالكتروني في القانون الجزائري، الطبعة الأولى، دار بلقيس دار البيضاء، الجزائر، 2016، ص ص 44-45.
5. عمر خالد زريقات، عقد التجارة الالكترونية: عقد البيع عبر الانترنت، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2007، ص 48.

بعض الشركات بإرسال رسائل دعائية لنوع معين من السلع أو الخدمات في البريد الالكتروني الخاص بالشخص وذلك من أجل غرض التعاقد لأجل اطلاع الشخص على هذه المنتوجات[1]، وعليه؛ فإن التراسل بواسطة البريد الالكتروني يصلح للتعاقد، وقد تلجأ الشركات المتعاقدة مع هذا الشخص أن ترسل إلى سلطة المصادقة الالكترونية للتعرف على الشخص الموقع على المعاملة، حيث يسند لهذه السلطة مهمة تحديد مصدر المعاملة، حيث تتمكن بوسائلها التقنية المتطورة في هذا المجال من تحديد هوية الموقع والتأكد منها بإصدار شهادة المصادقة الالكترونية[2].

يُلاحظ أن التحكم في الهوية الالكترونية من قِبل صاحبها هو أمر صعب على عكس بطاقة الهوية التقليدية، لهذا فإن معظم المواقع تقوم بإدارة الهوية الالكترونية من خلال أنظمة تقنية، وبهذه المناسبة أصبحت الهوية الالكترونية تشغل اهتمام المتخصصين والحكومات، لهذا أصبح من الضروري الاهتمام بأنظمة إدارة الهوية الالكترونية بشكل أكثر تدقيقاً، وهو ما قام به المؤتمر العالمي للاتصالات الذي أُقيم في مدينة جنيف بسويسرا في أكتوبر 2009، حيث تمت مناقشة إدارة الهوية الالكترونية وكيفية التحكم فيها وتطبيقاتها ونظم إدارتها[3].

فرغم إيجابيات المعاملة الالكترونية التي تتم بين الشخص المتعاقد والشركات وأخذ كل المعلومات المتعلقة بهوية الشخص المتعاقد من أجل إبرام ذلك العقد الالكتروني وتعلق هوية الشخص المتعاقد بعنوان بريده الالكتروني، إلا أن خدمات هذا الأخير لا ينفي القول بأن لها بعض السلبيات ولاشك أن أهمها يمكن القول أن السرية التي تضمنها هذه الخدمة هي سرية نسبية وليست سرية كاملة، لأنه باستطاعة الغير القيام بالإطلاع على البريد الالكتروني من دون معرفة أو ترخيص من صاحبه، وهذا ما يُعد أحد أوجه القرصنة التي تمارس عبر الانترنت[4].

المطلب الثالث: جريمة اختراق البريد الالكتروني:

من خلال عرضنا السابق، تبين لنا أن البريد الالكتروني له من المزايا ما تجعلنا نتعامل به يومياً، إلا أن سلبياته تكمن في اختراق وقرصنة المعلومات الخاص بنا في البريد الالكتروني، فهي تعتبر انتهاك سرية رسائل البريد الالكتروني، وقد أشارت دراسة على أن هذا الأخير هو المسؤول عن نشر 80% من الفيروسات عبر الانترنت، وذلك لأن معظم الفيروسات مبرمجة لتستفيد من إمكانية الوصول إلى

1. لزهر بن سعيد، النظام القانوني لعقود التجارة الالكترونية، ب. ط، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012، ص 64.
2. انظر المادة 06 وما يليها من قانون رقم: 15-04 المؤرخ في الأول من فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج. ج. د. ش، ج. ر عدد، 06، ص 08.
3. يمينة حوحو، المرجع السابق، ص: 45.
4. محمد عبد الرزاق محمد عباس، المرجع السابق، ص 28.

المستخدمين المسجلين لدى المستخدم الذي تلقى جهازه نسخة من الفيروس، إن اختراق البريد الالكتروني: هو يعني الدخول غير المشروع إلى المعلومات والبيانات المرسلة عن طريق البريد الالكتروني[1].

فجريمة قرصنة البريد الالكتروني من الجرائم المضرة بالمصلحة العامة، كونها تستهدف مصلحة خصوصية الأفراد (حق الأفراد في الخصوصية الشخصية)، لذلك تحتم المعاقبة على كل فعل يمس حق الفرد في الخصوصية وهذا الحق مثلما يجب توفره في الحق بحرية المسكن وعدم جواز دخوله دون إذن، كذلك يترتب وجود هذا الحق في خصوصية المراسلات بأي وسيلة تقليدية أو الالكترونية وله الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت ويُعاقب القانون على كل انتهاك لهذه الحقوق[2]. وعليه تجرم كل أفعال القرصنة والاختراق لنظام البريد الالكتروني لضمان عدم نفاذ المجرمين من العقاب[3].

فاختراق البريد الالكتروني وهو أن تعمد جهة ما بمحاولة الدخول إلى أنظمة أو شبكات تواصل أو منشآت بمساعدة بعض البرامج المختصة، في سرقة وفك كلمات السر عن طريق المهارات والفنيات المكتسبة، كما عُرف الاختراق في القانون العربي النموذجي الموحد بأنه "الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية"[4].

أما المشرع الفرنسي فإنه عدّها من جرائم المعلوماتية، وقد تناول جرائم الاعتداءات على نظام المعالجة الآلية، وكان تجريمه واضحا، وبذلك شمل جريمة قرصنة البريد الالكتروني، وبالنسبة للمشرع المصري فإنه لم يعرف جريمة قرصنة البريد الالكتروني، لكنه جعل البريد الالكتروني من وسائل الاتصال المحمية دستورياً وذلك عندما نص في المادة 57 من دستور مصر 2014 على " للحياة الخاصة حرمة، وهي مصونة لا تُمس. وللمراسلات البريدية، والبرقية، والالكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الإطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين

1. عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية، الطبعة الأولى، دار الوراق، بيروت، لبنان، 2004، ص ص 199 – 200.
2. انظر المادة 47 من الدستور لسنة 2020 المؤرخ في 30 ديسمبر 2020، ج. ج. د. ش، ج. ر عدد 82.
3. حسون عبيد هجيج، صفاء كاظم غازي، آثار جريمة قرصنة البريد الالكتروني، مجلة القادسية للقانون والعلوم السياسية، جامعة القادسية، العراق، المجلد 07، العدد 02، ديسمبر 2016، ص: 171.
4. براهيم بن داود، أشرف شعت، الإطلاع على البريد الالكتروني، مجلة دفاتر السياسة والقانون، جامعة ورقلة، الجزائر، المجلد 09، العدد 16، ص 28.

في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، ويُنظم القانون ذلك"[1].

ومن خلال التعريفات التي أشرنا إليها سابقاً، نجد أن جريمة البريد الالكتروني ليست واحدة فهناك جريمة الدخول غير المشروع وجريمة انتهاك سرية رسائل البريد الالكتروني وفعل الاختراق قد يحتاج هو الأخر إلى ارتكاب جريمة أخرى وهي جريمة سرقة كلمات المرور أو اصطيادها[2]، أو استعمال إحدى برامج الاختراق التي تصنف على أنها برامج محظورة وغير شرعية[3].

المطلب الرابع: صور الاعتداء على البريد الالكتروني:

تُعد جريمة قرصنة البريد الالكتروني من الجرائم ذات المفهوم الواسع التي يمكن حصر مضمونها في جريمة واحدة، لذا ارتأينا أن نضع مجموعة من صور الاعتداء على البريد الالكتروني.

أولا: جريمة الدخول غير المشروع أو البقاء غير المصرح به: وهي قدرة الوصول لهدف محدد بطريق غير مشروع بواسطة الثغرات الموجودة في نظام الحماية الخاص بالهدف[4].

وجاء هذا التعريف على أنه حصر الدخول إلى نظام الحاسب الآلي عن طريق الثغرات الموجودة في النظام الخاص بالحماية، وهذا الأمر هو غير دقيق إذ قد يكون الدخول إلى نظام الحاسب الآلي نتيجة خلل في الأمن المعلوماتي أو أنه غير محمي بنظام تشفير، أو قد يكون الجاني هو موظف له الحق باستخدام البريد الالكتروني خلال أوقات الدوام الرسمي فقط، أما غير ذلك فيعتبر من قبيل الدخول غير المشروع[5].

وقد عرفها جانب من الفقه على أنه الدخول والاستيلاء على المعلومات والبيانات بصورة غير مشروعة بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر بواسطة التقاط الموجات الكهرومغناطيسية الصادرة عن الحاسب الآلي أثناء تشغيله وباستخدام هوائيات موصلة بحاسب آخر[6].

ثانيا: جريمة انتهاك سرية المعلومات: يعتبر الحق في الحياة الخاصة هي حق الفرد في حماية اسمه ومراسلاته واتصالاته وشرفه واعتباره وحياته المهنية والعائلية، وكل ماله تأثير على حياته الشخصية،

1. أنسام سمير طاهر، جريمة السرقة الالكترونية، مجلة بابل للعلوم الإنسانية، الجامعة الإسلامية بابل، العراق، المجلد 27، العدد 05، ديسمبر 2019، ص 137.
2. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية الإسكندرية، مصر، 2008، ص 91.
3. خالد محمد خالد، أمن المعلومات والمواقع وأجهزة الكمبيوتر والدفع الالكتروني، ب. ط، المركز العلمي لتبسيط العلوم، مصر، 2006، ص 52.
4. رامي عبد العزيز، الفيروسات وبرامج التجسس، دار البراءة الإسكندرية، مصر، 2005، ص 82.
5. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، المرجع السابق، ص 84.
6. رامي متولي القاضي، مكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2011، ص 40.

وبذلك نجد أن المعلومات[1]، المخزنة في البريد الالكتروني لها خصوصية خاصة بالنسبة لشخص البريد الالكتروني، فمثلا لو تُرك البريد الالكتروني مفتوحاً، وهذا أمر وارد من الممكن حدوثه، فإن مجرد الإطلاع على الرسالة وقراءتها، دون علم ورضا صاحبها، ودون إحداث أي تغيير على محتواه أو إتلافها أو حذفها؛ يُعتبر ذلك اعتداءً على خصوصية المراسلات الخاصة الموجودة في البريد الصادر أو الوارد أو في الملفات المحفوظة في البريد الالكتروني التي تتضمن أسراراً ومعلومات شخصية خاصة، يتم تبادلها بين الأفراد خفية، ويخشى عليها من تطفل الآخرين واطلاعهم، وهذا يعتبر قصوراً تشريعيا يمس الإنسان في حقه في حرمة حياته الخاصة لعدم وجود نص صريح في قانون العقوبات والقوانين المكملة له يُعالج هذه المسألة[2].

ثالثا: جريمة إغراق البريد الالكتروني: وهي جريمة تقوم على مبدأ إرسال شخص أو مجموعة من الأشخاص مجموعة من الرسائل إلى البريد الالكتروني بصفة متكررة وفي آن واحد، وذلك بالاستعانة ببرامج متخصصة، وهذا قصد الإضرار بصاحب البريد الالكتروني المستهدف، بحيث يؤدي هذا العمل بطبيعة الحال إلى ملء المساحة المخصصة للبريد الالكتروني للشخص المستهدف وتعطل البريد الالكتروني عن الخدمة وتبعثر وتشتت الرسائل الالكترونية في الفضاء المفتوح مما يُسهل من عملية الإطلاع الرسائل السرية وتكبد الضحية خسائر مادية ومعنوية[3].

فهذه أهم صور الاعتداء على البريد الالكتروني إضافة إلى جرائم أخرى كالتجسس والتنصت والسب والقذف وإرسال رسائل دعائية التي قد تزعج صاحب البريد الالكتروني. لكن في حالة تحقق وقوع الجريمة فما هي الإجراءات الواجب اتخاذها لردع هذه الجرائم.

المبحث الثاني: إجراءات التحري والتحقيق وجمع الأدلة لإثبات جريمة الاختراق:

تعتبر الإجراءات المتخذة قبل تحريك الدعوى العمومية عن جريمة قرصنة البريد الالكتروني من إجراءات التحري وجمع الأدلة والتحقيق الابتدائي من أهم الإجراءات لسير هذه العملية ومحاكمة الجاني على أفعاله غير المشروعة.

المطلب الأول: إجراءات التحري وجمع الأدلة:

ويقصد بالبحث والتحري هو مجموعة الإجراءات التي يباشرها أعضاء الضبط القضائي (الشرطة القضائية) بمجرد علمهم بارتكاب الجريمة التي تهدف البحث عن الآثار والأدلة والقرائن التي تثبت ارتكاب

1. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 166.
2. سمية بلغيث، ضرورة حماية خصوصية مراسلات البريد الالكتروني في التشريع الجزائري، مجلة الواحات للبحوث والدراسات، جامعة غرداية، الجزائر، المجلد 12، العدد 02، ديسمبر 2019، ص 185.
3. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، المرجع السابق، ص 93 وما يليها.

تلك الجريمة والبحث عن الفاعل والقبض عليه وإثبات ذلك في محاضر تمهيدية للدعوى العمومية من طرف النيابة.

وعليه؛ فإن العناصر الأساسية للتحريات الأولية هي كالتالي:

-أنها مجموعة من الإجراءات الجزائية؛

-ينفذها أعضاء الضبط القضائي؛

-تبدأ بعد ارتكاب الجريمة وتنتهي بتحريك الدعوى العمومية؛-مضمونها معاينة الجرائم وجمع الأدلة عنها والبحث عن مرتكبيها؛

-تهدف التمهيد لتحريك الدعوى العمومية ومباشرتها والسير في التحقيق القضائي[1].

وعليه؛ فإن إجراءات التحري وجمع الأدلة، هي المرحلة الأولى من إجراءات إثبات الجريمة، وقد نظم المشرع الجزائري عملية التحري وجمع الأدلة في المواد من 11 إلى 28 من قانون الإجراءات الجزائية. وعلى من يقوم بإجراءات التحقيق والتحري أن يلتزم بسرية هذه العملية ما لم ينص القانون على خلاف ذلك[2].

المطلب الثاني: أعضاء الضبط القضائي وأدواته

ولكي تقوم الجهة المختصة بالتحري والتحقيق لابد من أعضاء تقوم بهذه المهمة، فقانون الإجراءات الجزائية ذكر هؤلاء الأشخاص، ودورهم في التحري وجمع الأدلة وذلك عن طريق أدوات تساعدهم في ذلك.

أولا: أعضاء الضبط القضائي: يقوم بمهمة الضبط القضائي فهم رجال القضاء والضباط والأعوان والموظفون[3].

ونصت المادة 17 من قانون الإجراءات الجزائية الجزائري على أن أعضاء الضبط القضائي مكلفون في جهات اختصاصهم مع مراعاة أحكام المادة 28 من ذات القانون بالتحري عن الجرائم وقبول البلاغات والشكاوى التي ترد إليهم بشأنها. ويقومون بجمع الاستدلالات وإجراءات التحقيقات الابتدائية، وعليهم أن يثبتوا جميع الإجراءات التي يقومون بها في محاضر موقعة منهم ومن الحاضرين يُبين فيها الوقت الذي اتخذت فيه الإجراءات ومكانها ويرسلوا البلاغات والشكاوى والمحاضر والأوراق الأخرى

1. عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة، الجزائر، 2004، ص 183 وما يليها.
2. انظر المادة 11 من الأمر رقم: 66-155 المؤرخ في 08 يونيو سنة 1966، المعدل والمتمم بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المتعلق بقانون الإجراءات الجزائية، ج. ج. د. ش، ج. ر عدد 84.
3. انظر المادة 12 من الأمر رقم: 66-155، قانون سبق ذكره.

والمواد المضبوطة إلى وكيل الجمهورية المختص إقليمياً ويجب أن ينوه في تلك المحاضر عن صفة الضبط القضائي الخاص بمحرريها[1].

من ملاحظة النصوص القانونية نجد أن المشرع الجزائري قد اعتمد بالدرجة الأولى على أعضاء الضبط القضائي في التحري عن الجريمة، ويطلق على أعضاء الضبط القضائي بأنه الجهاز الإجرائي الذي يتخذ الإجراءات الفنية والتقنية للبحث عن مرتكبي الجريمة[2]. فمتى ما وقعت جريمة الاختراق في البريد الالكتروني، وتلقى رجال الشرطة القضائية البلاغات أو الشكاوى الكتابية أو الشفوية، يقوم هؤلاء بتقييد هذه الشكاوى في الدفتر الخاص، وبعد إبلاغ المسؤول الرئيسي وإخطار الجهات المختصة[3].

ثانيا: أدوات أعضاء الضبط القضائي: يبدأ الجهاز المختص بالتحري وجمع الأدلة، ويقصد بالأدلة مجموعة حقائق تثبت الجريمة،[4] أو كل ما يؤدي إلى إثبات إدانة المتهم أو براءته، فالدليل هو أداة الإثبات عموماً، ويقصد بهذا الإثبات القواعد المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء وتقديرها من جانبه للوصول إلى حكم بشأن الواقعة محل الإثبات[5].

أما تعريف الدليل غير التقليدي أو ما يُعرف بالدليل الالكتروني " هو الدليل المشتق من أو بواسطة النظم البرامجية والمعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال وأصوات لإثبات وقوع الجريمة أو لتقرير البراءة والإدانة فيها[6].

المطلب الثالث: صعوبة جمع الأدلة الالكترونية:

إن الحصول على أدلة الالكترونية قد جعل أكثر هذه الأدلة تتميز بطبيعة غير مرئية بحيث يصعب الوصول إليها، لأنها تكون نِتاج تلاعب في رموز ونبضات والكترونيات. كما أنه قد زاد من صعوبة إجراءات الحصول عليها، لأنه قد أمَّد الجناة بوسائل متطورة تمكنهم من إخفاء أفعالهم غير

1. انظر المادتين 17 و18 من القانون نفسه.
2. عبد الله أوهابية، المرجع السابق، ص 208.
3. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ب.ط، دار الكتب القانونية، مصر، 2008، ص ص 170-171.
4. سلطان الشاوي، أصول التحقيق الإجرامي، مطبعة إياد بغداد، العراق، 1982، ص 37.
5. عبد الفتاح بيومي حجازي، مبادئ الإجراءات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007، ص 58.
6. هدى طالب علي، الإثبات الجنائي في جرائم الانترنت والاختصاص القضائي بها، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2012، ص 116.

المشروعة كاستخدام كلمات السر والتشفير واستطاعة التلاعب في البيانات المخزونة، بل وإتلافها في الوقت الذي يرونه مناسباً وفي ثوانٍ معدودة[1].

ونظراً لحساسية هذه الأدلة فمن واجب أعضاء الضبط القضائي إتباع قاعدتين الأولى ترك البريد الالكتروني على حاله وعدم إدخال أي تعديل عليه، لأنه في بعض الأحيان قد يكون عضو الضبط القضائي قليل الخبرة، مما يؤدي التلاعب بهذا البريد إلى إتلاف الأدلة بغير قصد، وكذلك عدم السماح للمتهم باستخدام بريده الالكتروني ومنعه من الاتصال بالشبكة لأنه بمجرد إتاحة الفرصة أمامه يقوم بإتلاف وإخفاء ما يدل على جريمته.

المطلب الرابع: تدخل الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

تبعاً لما سبق ذكره، من صعوبة جمع الأدلة الالكترونية على أعضاء الضبط القضائي، فإنه أسندت بعض مهام إجراءات التحقيق الابتدائي في حالة وقوع جريمة اختراق البريد الالكتروني إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[2].

تمارس الهيئة العديد من المهام تتمثل أساسا في:

-الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: وتكون بتوعية مستعملي شبكة الانترنت بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه الشبكة، ومن أهم هذه الجرائم التجسس والتنصت على الاتصالات والرسائل الالكترونية، التلاعب بحساب العملاء أو بطاقات إئتمانهم، الابتزاز، السب والقذف، الاعتداء على خصوصية الأفراد، الدخول غير المصرح به...إلخ.

-مكافحة الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال: فعلى حسب المادة 14 من قانون رقم: 09-04 نوعان من المكافحة التي تقوم بها هذه الهيئة، بمساعدة السلطات القضائية ومصالح الشرطة في التحريات التي تجريها بشأن الجرائم المتصلة بهذه التكنولوجيات بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعلومات والمعطيات المفيدة في التعرف على مرتكبي الجريمة وتحديد مكان تواجدهم[3].

1. خالد ممدوح إبراهيم، التقاضي الالكتروني، دار الفكر الجامعي الإسكندرية، مصر، 2007، ص 323 وما بعدها.
2. المرسوم الرئاسي رقم: 19-172 المؤرخ في 06 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج. ج. د. ش، ج. ر عدد 37.
3. انظر المادة 14 من القانون رقم: 09-04 المؤرخ في 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ج. د. ش، ج. ر عدد 47، 16 غشت 2009.

ويمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني، كما يمكن في حالة الاستعجال ومع مراعاة لاتفاقية الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية بخصوص التحريات في الجرائم المعلوماتية، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني، غير أن المشرع الجزائري وضع قيداً على هذه المساعدات القضائية، إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام[1].

ولا يجوز إجراء مراقبة الاتصالات الالكترونية إلا بإذن مكتوب من السلطة القضائية المختصة، وتكون هذه المراقبة في حالة مقتضيات التحريات والتحقيقات القضائية[2]، وعلى وكيل الجمهورية أو قاضي التحقيق أو لضابط الشرطة القضائية أن يسخر عوناً مؤهلاً لدى الهيئة المكلفة بالاتصالات سواء كانت عامة، أو خاصة للقيام بهذا الإجراء، كما يمكنه طلب المساعدة من قِبل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، وعلى العون المسخر أن يقوم بهذه العملية في سرية تامة، وأن يحرر هذا العون المسخر محضراً يحوي العناصر الأساسية للعملية التاريخ، الساعة لبداية ونهاية الإجراء.....نسخ المراسلات أو الصور وتحميل البيانات المفيدة للتحقيق...إلخ، ويُودع المحضر لدى الجهة القضائية المكلفة. كما على الهيئة الوطنية المكلفة بمراقبة الاتصالات الالكترونية أن تحمي المعطيات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في القانون رقم: 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3].

المطلب الخامس: أسلوب التفتيش في أمريكا:

قد نظم المشرع الأمريكي أحكام التفتيش عند تعديل القواعد الخاصة بالإجراءات الجنائية عام 1970 لتسمح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الالكترونية بما في ذلك البريد الالكتروني[4].

وتجدر الإشارة إلى أن الأسلوب الأمريكي لتنفيذ التفتيش نظم الحاسب الآلي، يُلخص في أن قوات الشرطة تقتحم المكان بصورة سريعة ومن كافة منافذه في وقت واحد، وذلك باستخدام القدر الأعظم من القوة بافتراض أن هذا التكتيك يقلل من احتمالية وقوع إصابات بين صفوف رجال الشرطة[5].

1. انظر المادة 16 وما يليها من القانون رقم: 09-04، القانون نفسه.
2. انظر المادة 04 من القانون رقم: 09-04، القانون نفسه.
3. مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة القانون، جامعة غليزان، الجزائر، المجلد 09، العدد 01، جوان 2020، ص 129.
4. حسين محمود إبراهيم، التحقيق الجنائي في مواجهات التقنيات والمتغيرات، عالم الكتب القاهرة، مصر، 1975، ص 11.
5. أحمد عبد الإله هلالي، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، دار النهضة العربية القاهرة، مصر، 2006، ص 171.

وأهمية هذه الخطوة في نظر الشرطة الأمريكية هو إبعاد المشتبه به عن كافة أنظمة ومعدات الكمبيوتر المتواجدة في المكان على الفور، حتى لا يتمكن المشتبه به من تعديل أو محو أي دليل الكتروني، كما يتم إدخال المشتبه به في غرفة لا توجد بها أية أجهزة كمبيوتر وغالباً ما تكون غرفة المعيشة، وذلك في ظل ظروف حراسة مشددة، وفي هذه الحالة يتم تقديم إذن التفتيش الصادر من النيابة إلى المشتبه به، ويتم تحذيره بأن كافة أقواله سوف تُحسب عليه في هذه اللحظة، وقد تُؤخذ بمثابة دليل إدانة ضده[1].

وفي الأخير يجب أن ننوه أن هناك مجموعة من الضوابط على أعضاء الضبط القضائي مراعاتها عند إجراء التفتيش هناك ضوابط موضوعية وأخرى شكلية:

-الضوابط الموضوعية: تتمثل بضرورة وقوع جريم اختراق البريد الالكتروني والتي تعني الدخول غير المشروع لنظام البريد الالكتروني، وتوافر أدلة كافية تدل على ارتكاب الشخص لجريمة قرصنة البريد الالكتروني، وأيضا توافر أسباب مقنعة لدى المحقق بأن الشخص المراد تفتيشه لديه أدوات استخدمت في اختراق البريد[2].

-أما الضوابط الشكلية لتفتيش نظام البريد الالكتروني فهو الحصول على إذن من الجهة المختصة للتفتيش[3]، ولتفتيش نظام البريد الالكتروني لضبط الاختراق، يكون على المكلف بالتحقيق أي عضو الضبط القضائي المسخر من طرف وكيل الجمهورية أو قاضي التحقيق أو من طرف الشرطة القضائية، فعليه تحديد صندوق البريد للمتهم والمبين في قائمة البرامج الرئيسية في الموقع، بعد معرفة اسم المستخدم والرقم السري للدخول وفتح البريد الالكتروني في جهاز المتهم ومراجعة قائمة الرسائل[4].

الخاتمة:

نخلص إلى القول أن البريد الالكتروني هو هوية الفرد، ولا يمكن التعدي عليها لما تحتويه من ملفات وصور شخصية إضافة إلى مراسلات الالكترونية، فحق خصوصية الفرد حق مكفول من قِبل

1. فاطمة مرنيز، التفتيش الافتراضي كإجراء استدلالي في ضوء قانون رقم: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تامنغست، الجزائر، المجلد 10، العدد 02، سنة 2021، ص 248.
2. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الرابعة، دار النهضة العربية، مصر، 2006، ص 369.
3. مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية للنشر والتوزيع، مصر، 2011، ص 528.
4. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي الإسكندرية، مصر، 2010، ص ص 65-66.

دستور 2020، والتعدي على البريد، كأنه التعدي على مسكنه ويُعاقب عليه القانون، إضافة إلى الحرمة الخاصة بالفرد هناك جريمة الدخول غير المصرح به التي ينتهجها الجناة في كسر كلمة سر البريد الالكتروني والإطلاع على محتواه، فرغم كثرة صور التعدي على البريد الالكتروني إلا أن المشرع الجزائري لم ينص صراحة على جريمة اختراق البريد الالكتروني، وكما نعلم أن القاعدة العامة تقول "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون"، فهل يجوز للقاضي الجزائي التوسع في تفسير قانون العقوبات لاسيما المادة 303 مكرر لتطبيقها على كل من يتطفل على رسائل البريد الالكتروني الخاصة بالأفراد وحماية حرمة حياتهم الخاصة، لذا نقترح على المشرع الجزائري

– أن تُسن نصوص صريحة المتعلقة بجريمة التعدي على البريد الالكتروني والتي صورها كثيرة.

– إسناد مهام التحقيق الابتدائي المتعلق باختراق البريد الالكتروني لأعضاء الهيئة الوطنية المتعلقة بالوقاية بتكنولوجيات الإعلام والاتصال ومكافحته ويكون بالتنسيق مع وكيل الجمهورية أو قاضي التحقيق.

– تكوين كوادر بشرية للمحافظة على الأدلة الالكترونية دون تلفها من قِبل الجناة.

– إتباع أساليب الدول المتقدمة في جمع الأدلة الالكترونية ومراقبة أثرها.

قائمة المراجع:

أولا: الكتب:

1. أحمد عبد الإله هلالي، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، دار النهضة العربية القاهرة، مصر، 2006.
2. حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، مصر، 2000.
3. حسين محمود إبراهيم، التحقيق الجنائي في مواجهات التقنيات والمتغيرات، عالم الكتب القاهرة، مصر، 1975.
4. خالد محمد خالد، أمن المعلومات والمواقع وأجهزة الكمبيوتر والدفع الالكتروني، ب.ط، المركز العلمي لتبسيط العلوم، مصر، 2006.
5. خالد ممدوح إبراهيم، التقاضي الالكتروني، دار الفكر الجامعي الإسكندرية، مصر، 2007.
6. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية الإسكندرية، مصر، 2008.
7. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي الإسكندرية، مصر، 2010.
8. رامي عبد العزيز، الفيروسات وبرامج التجسس، دار البراءة الإسكندرية، مصر، 2005.
9. رامي متولي القاضي، مكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2011.

10. سلطان الشاوي، أصول التحقيق الإجرامي، مطبعة إياد بغداد، العراق، 1982.
11. عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية، الطبعة الأولى، دار الوراق، بيروت، لبنان، 2004.
12. عبد الفتاح بيومي حجازي، مبادئ الإجراءات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007.
13. عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة، الجزائر، 2004.
14. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الرابعة، دار النهضة العربية، مصر، 2006.
15. عمر خالد زريقات، عقد التجارة الالكترونية: عقد البيع عبر الانترنت، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2007.
16. لزهر بن سعيد، النظام القانوني لعقود التجارة الالكترونية، ب.ط، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012.
17. محمد عبد الرزاق محمد عباس، النظام القانوني لعقد الاشتراك في خدمة الانترنت، ب.ط، دار الفكر والقانون للنشر والتوزيع، مصر، 2016.
18. محمود عبد الرحيم الشريفات، التراضي في تكوين العقد عبر الانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.
19. مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية للنشر والتوزيع، مصر، 2011.
20. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ب. ط، دار الكتب القانونية، مصر، 2008.
21. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن، 2010.
22. يمينة حوحو، عقد البيع الالكتروني في القانون الجزائري، الطبعة الأولى، دار بلقيس دار البيضاء، الجزائر، 2016.

ثانيا: المقالات:

1. أنسام سمير طاهر، جريمة السرقة الالكترونية، مجلة بابل للعلوم الإنسانية، الجامعة الإسلامية بابل، العراق، المجلد 27، العدد 05، ديسمبر 2019.
2. براهيم بن داود، أشرف شعت، الإطلاع على البريد الالكتروني، مجلة دفاتر السياسة والقانون، جامعة ورقلة، الجزائر، المجلد 09، العدد 16، جانفي 2017.

3. حسون عبيد هجيج، صفاء كاظم غازي، آثار جريمة قرصنة البريد الالكتروني، مجلة القادسية للقانون والعلوم السياسية، جامعة القادسية، العراق، المجلد 07، العدد 02، ديسمبر 2016.
4. سمية بلغيث، ضرورة حماية خصوصية مراسلات البريد الالكتروني في التشريع الجزائري، مجلة الواحات للبحوث والدراسات، جامعة غرداية، الجزائر، المجلد 12، العدد 02، ديسمبر 2019.
5. فاطمة مرنيز، التفتيش الافتراضي كإجراء استدلالي في ضوء قانون رقم: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تامنغست، الجزائر، المجلد 10، العدد 02، سنة 2021.
6. مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة القانون، جامعة غليزان، الجزائر، المجلد 09، العدد 01، جوان 2020.

ثالثا: الرسائل والمذكرات:

1. هدى طالب علي، الإثبات الجنائي في جرائم الانترنت والاختصاص القضائي بها، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2012.

رابعا: القوانين والمراسيم التنظيمية:

1-الدستور:

1. دستور 2020 المؤرخ في 30 ديسمبر 2020، ج. ج. د. ش، ج. ر عدد 82.

2-القوانين:

1. الأمر رقم: 66-155 المؤرخ في 08 يونيو سنة 1966، المعدل والمتمم بالقانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006، المتعلق بقانون الإجراءات الجزائية، ج. ج. د. ش، ج. ر عدد: 84.
2. قانون رقم: 09-04 المؤرخ في 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج. ج. د. ش، ج. ر عدد: 47، 16 غشت 2009.
3. قانون رقم: 15-04 المؤرخ في الأول من فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج. ج. د. ش، ج. ر عدد: 06.

3-المراسيم التنظيمية:

1. مرسوم الرئاسي رقم: 19-172 المؤرخ في 06 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج. ج. د. ش، ج. ر عدد: 37.