جامعة النجاح الوطنية

كلية الدراسات العليا

خصوصية الجرائم المعلوماتية

إعداد

نداء نائل فايز المصري

إشراف

د. فادي شديد

قدمت هذه الأطروحة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، بكلية الدراسات العليا في جامعة النجاح الوطنية في نابلس- فلسطين.

2017

خصوصية الجرائم المعلوماتية

إعداد

نداء نائل فايز المصري

نوقشت هذه الأطروحة بتاريخ / / 2017م، وأجيزت.

أعضاء لجنة المناقشة		**التوقيع**
– د. فادي شديد	**/مشرفاً ورئيساً**	.....
– د.	**/ ممتحناً خارجياً**	.....
– د.	**/ ممتحناً داخلياً**	.....

الإهداء

إلى من أحمل اسمه بكل فخر...

إلى روح أبي

إلى من سهرت معي الليالي الطوال وساندتني... إلى من وقفت إلى جانبي في كل صغيرة وكبيرة... إلى كل الحنان

أمي

إلى من شجعني على مواصلة مسيرتي العلمية رفيق دربي

زوجي

إلى رمز المحبة والسلام... إلى وطني الحبيب وشعبه المجاهد

فلسطين

إلى إخوتي وأصدقائي الأعزاء جميعاً

أهدي هذا الجهد المتواضع إلى كل من ساعدني في إتمام هذا العمل

الشكر والتقدير

كم يرفع العلم أشخاصاً إلى رتب ويخفض الجهل أشرافا بلا أدب

بعد رحلة طويلة من الجهد والاجتهاد تكللت بإنجاز هذا البحث المتواضع، فالحمد الله عز وجل على النعمة التي منّ بها علينا، فهو العلي القدير.

وأتقدم بجزيل الشكر للدكتور المشرف "فادي شديد " حيث كان خير معلم وناصح، ولم يدخر جهدا بمساعدتي، وأتوجه بخالص الشكر والعرفان إلى الأستاذ بدر شواهنة (رئيس نيابة نابلس) على مساعدته لي في جمع المراجع التي لم أتمكن من الحصول عليها، وأتقدم بالشكر الجزيل لكل من أسهم في تقديم يد العون لنا ونخص بالذكر أساتذتنا الكرام في القانون الجنائي وإدارة كلية الحقوق بجامعة النجاح الوطنية، والشكر موصول لأختي فداء على مساندتها لي في هذه الرحلة، والشكر الموفور لأهلي وأخص بالذكر والدة زوجي التي كانت ومازالت خير مساند وأشكر صديقاتي اللواتي كنّ عونا لي في بحثي هذا ونورا يضيئ الظلمة التي كانت تقف أحيانا في طريقي.

وشكري الممزوج بنبض القلب لزوجي الذي كان سندا لي وداعما، وآخذاً بيدي وعونا في كل المراحل، وأمي التي علمتني كيف أقف أمامكم في لحظة تتسابق فيها الدموع إلى مقلتي.

أما الشكر من النوع الخاص فنحن نتوجه به إلى كل من لم يقف إلى جانبنا وعرقل مسيرة بحثنا فلولا وجودهم لما أحسسنا بمتعة العمل وحلاوة البحث ولما وصلنا إلى ماوصلنا اليه.

الإقرار

أنا الموقعة أدناه، مقدمة الرسالة التي تحمل العنوان:

خصوصية الجرائم المعلوماتية

أقر بأن ما اشملت عليه هذه الرسالة إنّما هو نتاج جهدي الخاص، باستثناء ما تمّت الإشارة إليه حيثما ورد، وأنّ هذه الرسالة ككل، أو أيّ جزء منها لم يقدّم من قبل لنيل أيّ درجة أو لقب علميّ لدى أيّ مؤسسة تعليمية أو بحثية أخرى.

Declaration

The work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted elsewhere for any other degree or qualification.

Student's Name: **اسم الطالبة:**

Signature: **التوقيع:**

Date **التاريخ:**

فهرس المحتويات

خصوصية الجريمة المعلوماتية

إعداد

نداء نائل فايز المصري

إشراف

د.فادي شديد

الملخص

لقد تناولت الباحثة هذا الموضوع لما له من خصوصية على مستوى التجريم والعقاب، حيث تكمن هذه الخصوصية بعدم قدرة التشريعات التقليدية على إحتواء هذا النوع من الجرائم، بسبب مايميز هذه الجرائم من طبيعة متجددة ومتغيرة فهي مرتبطة بتطور التقنيات، ومن حيث أركانها فهي تختلف عن الجريمة التقليدية في أركانها الأساسية المكونة للجرم وفي طبيعة ونوع العقوبات الرادعة لهذه الجريمة، أما بالشق الإجرائي كان لهذه الخصوصية الأثر الواضح في عدم إتساع قوالب التشريعات الإجرائية التقليدية في مواجهة هذا النوع من الجرائم بحيث يواجه رجل القانون الكثير من الصعوبات في مرحلة التحقيق الإبتدائي سواء من حيث الإجراءات أو بما يتعلق بالدليل الرقمي، ومن الجدير ذكره أن هناك خصوصية على مستوى التحقيق النهائي تبرز في قواعد الإختصاص القضائي المتعلقة بالجريمة المعلوماتية فهي جرائم عابرة للحدود، وفي سلطة القاضي في قبول الأدلة الرقمية حيث أن هناك العديد من المواقف الفقهية والتشريعات المختلفة التي تناولت مسألة الإثبات بالدليل الرقمي وعليه تعتبر هذه الدراسة بمثابة تحليل للنصوص القانونية التقليدية المطبقة على الجرائم المعلوماتية وبيان أوجه القصور في هذه النصوص ومحاولة وضع خطوط رفيعة يجب أن يلتفت إليها المشرع عند إعداد أو صياغة أي تشريع يتعلق بالجرائم المعلوماتية.

المقدمة

تعتبر الجريمة المعلوماتية "الإبن الغير شرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات والعولمة" وإنّ حماية المجتمع من هذا النوع من الجرائم يقتضي وضع تشريعات فاعلة تواجه هذه الظاهرة الإجرامية، وملاحقة مرتكبيها وإنزال العقوبات المناسبة بحقهم[1].

كما أن من أكبر المشاكل التي تواجه عملية مكافحة الجريمة المعلوماتية والتي تشكل قلقا للأفراد والدول هي اكتشاف النشاط الإجرامي، وتحديد الفاعل، والملاحقة الجزائية لمرتكبي هذه الجريمة.

ومن أجل هذه الطبيعة الخاصة للجرائم المعلوماتية وخصوصية أساليبها على مستوى الموضوعي والإجرائي أصبح لا بدّ من وجود نصوص تشريعية خاصة بالتجريم والعقاب لمكافحة هذه الجريمة[2]مما أوجب تطوير البنية التشريعية الجزائية الوطنية بذكاء تشريعي تعكس فيه الدقة الواجبة على المستوى القانوني مع ضرورة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى[3].

ولعل أهم إنجازات العصر الحديث التي ساعدت على ظهور هذه الجريمة هو ظهور ما يسمى الحاسب الآلي والإنترنت وما حققته تكنولوجيا المعلومات والإتصالات من فوائد عديدة في معظم مجالات الحياة سواء الاجتماعية، أو الاقتصادية، أو التعليمية، أو الطبية.

---

[1] الرواشدة، سامي حمدان، **مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجا، المجلة الأردية في القانون والعلوم السياسية**، مجلد1: عدد4، دار المنظومة، ص11.

[2] اليحيى، تركي بن محمد، بن عبدالله، **مكافحة الجرائم المعلوماتية في المملكة العربية السعودية**، مجلد 2، عدد7، دار المنظومة، ص254.

[3] الشوابكة، محمد أمين، **جرائم الحاسوب والانترنت**، دار الثقافة للنشر والتوزيع، ط4، 2011، ص7.

ومن جملة ماذكر يمكن القول إنّ الجريمة المعلوماتية هي"كل فعل أو إمتناع معاقب عليه بموجب القانون والمتعلق باستخدام نظم وشبكات ووسائل المعلومات والبرمجيات والحواسيب والإنترنت والأنشطة المتعلقة بها استخداما مجرما"[1].

ويمكن القول إنّ التطور التاريخي لمجالات الحاسب الآلي قد بدأ بالظهور في السيتينات حيث أصبحت الحاسبات الالية تستخدم للتقليل من العمالة، وكان وجود هذه الحاسبات مقتصرا على الشركات الكبرى، وذلك نظرا لإرتفاع ثمنها من جهة، ولما تتطلبه من أماكن مجهزة تجهيزا خاصا ومتخصصين مدربين لتشغيلها من جهة أخرى، أما في السبعينات فطرأ تطور آخر حيث فُصل بين البرامج المسؤولة عن تشغيل الحاسبات الآلية، وبين المكونات المادية ومن هنا بدأ التطور في صناعة الحاسب الآلي بصورة كبيرة، بالتالي أصبح هناك إنخفاض في أسعار الحاسب الآلي مما كان له الأثر في تمكن الشركات الكبرى والصغرى من استعمال هذه الحاسبات. وبالثمانينات ظهر مايسمى الحاسب الآلي الشخصي الذي أحدث ثورة في تقنية المعلومات، وبناء عليه أصبحت هذه الحاسبات متاحة للجميع، والسبب الرئيسي وراء تطوير الحاسبات الآلية هو ظهور مايعرف بالمعالجة الآلية للمعطيات ومايرتبط بها من بنوك المعلومات، وبلغ هذا التطور ذروته بالتسعينات، حيث أصبحت لهذه الحاسبات الآلية قيمة كبرى لقدرتها على تخزين المعلومات واسترجاعها في ثوان معدودات[2].

وقد واكب هذا التطور بروز خبراء يتمتعون بالخبرة والحرفية لتطويع هذه التقنية للقيام بأعمال إجرامية ذات طابع معاصر يتمثل باستخدام أسلوب تقني في تنفيذ الفعل المجرم بأساليب مبتكرة وطرق جديدة لم تكن معروفة من قبل، وقد لخص بعض الفقهاء هذه الثروة المعلوماتية بما يلي: "إن الكمبيوتر يتمتع بشراهة في جمع المعلومات على نحو لا يمكن وضع حد له، وما يتصف به من دقة، ومن عدم نسيان ما يختزن به قد يقلب حياتنا رأسا على عقب، يخضع فيها الأفراد

[1] طه، ابراهيم قاسم السيد، محمد، **شرح قانون جرائم معلوماتية**، ط2، 2015، ص2.

[2] قورة، نائلة عادل محمد فريد، **جرائم الحاسب الاقتصادية**، دار النهضة العربية، 2003:2004، ص9-10.

لنظام رقابة صارم، ويتحول المجتمع بذلك إلى عالم شفاف، تصبح فيه بيوتنا ومعاملاتنا المالية، وحياتنا العقلانية والجسمية عارية لأي مشهد[1]".

وبناء عليه لابد من مواكبة التشريعات المختلفة هذا التطور الإجرامي الملحوظ المتمثل في استخدام الحاسب الآلي وشبكات الإنترنت فأحيانا قد يؤدي هذا الاستخدام إلى خلق شلل كامل للأنظمة المدنية والعسكرية، وتعطيل المعدات الإلكترونية، اختراق النظم المصرفية، وإرباك حركة الطيران، وشلل محطات الطاقة، وبذلك يصل الجاني إلى أي مكان يرغب به دون أن يترك المجرم المعلوماتي أثرا ملموسا، وعليه تعتبر جرائم الحاسب الآلي من الآثار السلبية التي خلفتها التقنية العالية.

وإزاء التصدي لظاهرة الإجرام المعلوماتي، فإنّ المصطلحات التي تناولت هذه الظاهرة قد اختلفت فيما بينها، فنلاحظ أن الفقه الجنائي لم يتفق على تسمية موحدة للجريمة المعلوماتية فالبعض يطلق عليها جرائم الكمبيوتر، والبعض الآخر يطلق عليها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات، والبعض يسميها جرائم الكمبيوتر والانترنت، وهناك من يطلق عليها الجرائم المستحدثة بالاضافة إلى عدم الاتفاق على تعريف تشريعي شامل لهذا النوع من الجرائم.

فذهب الفقهاء في تعريف الجريمة المعلوماتية مذاهب مختلفة ووضعوا تعريفات متنوعة وبالتالي فلا نجد تعريفا محددا للجريمة المعلوماتية نتيجة للاجتهادات الفقهية المتشعبة[2].

ونتيجة للتطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حال ذلك دون وضع تعريف فقهي جامع وشامل حيث بذل الفقهاء جهودا مختلفة في محاولة وضع تعريف محدد إلا أنّ البعض وسع من مفهوم الجريمة المعلوماتية والبعض الآخر ضيق منه.

---

[1] الرواشدة، سامي حمدان، **مكافحة الجريمة المعلوماتية بالتجريم والعقاب**، مرجع سابق، ص115.

[2] الشكرى، عادل يوسف عبد النبي، **الجريمة المعلوماتية وازمة الشرعية الجزائية**، جامعة الكوفة، العدد السابع،2008، ص111.

أما أنصار اتجاه التضييق فعرفوا الجريمة المعلوماتية على أنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لإرتكابه من ناحية وملاحقته من ناحية أخرى[1]".

كما ويرى الأستاذ(tredman) أن الجريمة المعلوماتية تشمل (أي جريمة ضد المال، مرتبطة باستخدام المعالجة الالية للمعلومات)[2].

أو "هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه"

من خلال التعريفات السابقة نلاحظ أنّ مفهوم الجريمة المعلوماتية ارتبط إمّا بموضوع الجريمة، أو وسيلة ارتكابها، أو على فاعل الجريمة، بينما قد تقع الجريمة المعلوماتية على الحاسب الآلي بشقية المادي والمعنوي، بالإضافة إلى حصر مفهوم الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة الفنية، وهذا يعني أنّ التوجه إلى المفهوم الضيق للجريمة المعلوماتية قد لايسعف في التوصل إلى تعريف شامل جامع.

أما أصحاب اتجاه الموسع فعرفها بأنه "كل سلوك إجرامي يتم بمساعدة الكمبيوتر " أو "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها[3]".

كما اعتبرتها الدكتورة هدى قشقوش "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات "

وقد تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين – حديثا –تعريفا جامعا لجرائم الحاسب الآلي وشبكاته، حيث عرف الجريمة المعلوماتية بأنها "اي جريمة يمكن

---

[1] بكار، الحسن، **الطبيعة القانونية للجرينة المعلوماتية**، دار المنظومة، مجلة الملف، المغرب، عدد17، 2010، ص183.

[2] الشوابكة، محمد امين، **جرائم الحاسوب والانترنت**، مرجع سابق، ص8.

[3] إبراهيم، خالد ممدوح، **الجرائم المعلوماتية**، دار الفكر الجامعي، ط 1، 2009، ص74.

ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية[1]".

وفي ظل حديثنا عن الجريمة المعلوماتية لابد لنا من التعريج على مفهوم المعلومة التي تعتبر محل لهذه الجريمة فقد عرفها قانون الجرائم الإلكترونية الفلسطيني "أية معلومات يمكن تخزينها ومعالجتها وتوريدها ونقلها بوسائل تكنولوجيا المعلومات بوجه خاص بالكتابة، أو الصور، أو الصوت، أو الارقام، أو الحروف، أو الرموز، أو الإشارات، أو غيرها[2].

من خلال ما تقدم من التعاريف الفقهية السابقة يلاحظ أنّ مفهوم الجريمة المعلوماتية اقتصر على مفاهيم عامة ارتبطت بجهاز الحاسوب من جهة، وبالبيانات من جهة أخرى، فالفقهاء الذين تبنوا الاتجاه الموسع لتعريف الجريمة الإلكترونية كانوا أكثر حكمة، لأن هذا العالم الافتراضي سريع التطور، وأيّ تضييق في مفهوم الجريمة المعلوماتية سوف يقنّن مفهوم الجريمة المعلوماتية .

كما أنّ عدم تبني التشريعات أي تعريف للجريمة المعلوماتية يعتبر الصواب بعينه، وذلك يرجع إلى التضييق من نطاق تطبيق النص الجزائي الخاص في الجريمة الإكترونية في حال تبني أي تشريع تعريف محدد لهذه الظاهرة، وذلك نظرا للتطور الهائل الذي يجتاح هذا النوع من الجرائم.

من خلال التعاريف السابقة يلاحظ أنّ الجريمة المعلوماتية تتميز عن غيرها من الجرائم التقليدية، وذلك لسهولة ارتكاب هذ النوع من الجرائم، لإعتماده على أساليب تقنية، وتتوقف على مهارات الجاني الذي عادة مايتصف بذكاء شديد، سهولة إخفاء آثار الجريمة، لأنها لاتترك أثرا ماديا، وإنما معلومات يمكن شطبها فور تنفيذ الجاني لفعله الإجرامي، بالإضافة إلى خطورة هذه الجرائم لأنها ترتكب بواسطة أصحاب الياقات البيضاء من خلال الاحتيال على البنوك، وتطورت حتى أصبحت تسهل عمليات غسل الأموال الناتجة من مصادر غير مشروعة، وذلك من خلال

[1] مؤتمر فينا في الفترة من 17/10 نيسان، 2000.

[2] قانون الجرائم الالكترونية الفلسطيني رقم 16 لسنة2017.

استخدام التحويلات الإلكترونية لإضفاء المشروعية على الأموال الغير مشروعة.[1] كما أنّ الجرائم المعلوماتية هي جرائم عابرة للحدود، إذ غالبا مايكون الجاني في بلد والمجني عليه في بلد آخر، وقد يكون هناك ضرر محتمل في بلد ثالث، وعليه فهي جرائم ذات طابع جديد، فهي عابرة للحدود الإقليمية، والوطنية، والقارية، وتعتبر الجرائم المعلوماتية أقل عنفا من نظيرتها التقليدية فهي لاتحتاج إلى أدنى مجهود عضلي، لاعتمادها على الدراية الذهنية، والتفكير المدروس، بحيث يعتبر مرتكبوها ليسوا من محترفي الإجرام بصورته التقليدية، كما أنّ الباعث في الجرائم المعلوماتية يختلف عن الباعث في الجرائم التقليدية المتمثل في معظم الأحيان بالخروج عن النظام العام، والقواعد القانونية فنجد أنّ الباعث من ارتكاب الجرائم المعلوماتية غالبا مايكون الحصول على الربح المادي والسريع، وغالبا ما تكون الأموال المتحصل عليها طائلة، وقد يكون دافع الجاني عرض قدراته الذهنية.[2]إن أهم مايميز الجريمة المعلوماتية وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات: ويشترط لإتمام الجريمة أن تكون المعلومات أو البيانات بما يتيح للمستخدم إمكانية كتابتها، أو تصحيحها، أو تعديلها، أو محوها، أو تخزينها، أو استرجاعها، وهذه العمليات تعتبر المحور الأساسي للجريمة الإلكترونية فلا بد من فهم الفاعل لهذه العمليات وإتقانه لها[3].

أهمية الدراسة

تنبع الأهمية النظرية للدراسة من الجدل الفقهي القائم حول اعتناق تشريع خاص للحد من الجريمة المعلوماتية فالبعض يرى أن هناك حاجة ملحة لوجود تشريع خاص بالجرائم المعلوماتية يعالج الجانب الموضوعي من جهة والجانب الاجرائي من جهة اخرى والبعض الاخر يرى إن الطريقة الفضلى هي دمج نصوص في قانون العقوبات التقليدي من خلال طرق مختلفة.

---

[1] مصطفى، خالد حامد أحمد، **المعلوماتية والمسؤولية الجزائية**، مجلة الفكر الشرطي مركز بحزث الشرطة، القيادة العامة لشرطة الشارقة الإمارات، مجلد 20، عدد79، دار المنظومة، ص159.

[2] سالم، محمد علي، **الجريمة المعلوماتية**، مجلة جامعة بابل العلوم النسانية، مجلد14 عدد2، دار المنظومة، ص92.

[3] شكري، عادل يوسف عبد النبي، **الجريمة المعلوماتية وازمة الشرعية الجزائية**، مجلة مركز دراسات الكوفة، ع7، دار المنظومة، 2011، ص115.

بالاضافة الى أهمية الموضوع المنوي تناوله وهو الجريمة المعلوماتية، فتبرز أهميته في مدى الخطورة التي باتت تشكلها تلك القضية من خطر كبير على أعمال المؤسسات والشركات والمنظمات حتى على الأشخاص، حيث أن تلك الجريمة باتت تطال جميع شرائح المجتمع، ولا بد من وجود قواعد تشريعية موضوعية واجرائية للحد من هذه الظاهرة.

أهداف الدراسة

تحاول هذه الدراسة تحقيق الأهداف التالية:

1. التركيز على خصوصية الجريمة المعلوماتية ومدى إختلافها عن الجريمة التقليدية .

2. الوصول إلى قوانين مستحدثة تتسع لقوالب الجريمة المعلوماتية.

3. ايجاد حلول قانونية لتحقيق التوازن بين مصلحة المجتمع في الاستفادة من الثورة المعلوماتية من جهة، وحق الفرد في حماية خصوصيته من جهة أخرى.

منهج الدراسة

اتبعت الباحثة منهجا تأصيليا وتحليليا ومقارنا، فهو أولا منهج تأصيلي يرجع بالنقاط التفصيلية إلى أصولها النظرية، فعند معالجة أي صورة من صور الجريمة المعلوماتية نردها إلى الأركان العامة في التجريم، وكذلك الحال عند التطرق إلى أي إجراء موضوعي كالتحقيق مثلا فنرده إلى النظرية العامة للتحقيق.

أما المنهج التحليلي الذي اتبعته الباحثة فهو قائم على التحليل النصوص القانونية ذات الصلة، بالإضافة إلى شرح وجهات النظر الفقهية والقانونية المختلفة.

ولقد استعانت الباحثة بالمنهج المقارن من خلال عرض مواقف عدة دول المتمثلة في التشريعات المختلفة لمعالجة الجرائم المعلوماتية.

مشكلة الدراسة

إنّ الحديث المستمر عن الجرائم المعلوماتية يكاد لاينقطع، ومع انتشار الجريمة المعلوماتية تزداد خطورة هذه الجريمة، وتتسع الآثار السلبية لثورة تقنية المعلومات، ويزداد الجناة إجراما فيما تتعاظم خسائر المجني عليهم، أفرادا ومؤسسات، من هنا جاءت هذه الدراسة لمحاولة التعرف على أكثر الجرائم حداثة في هذا العصر، وقد أثار البحث تساؤلات عديده منها:

ما مفهوم الجريمة المعلوماتية والاركان العامة لهذه الجريمة؟

ما العقوبات اللازمة للحد من هذه الجريمة؟

ما الإجراءات الواجب تتبعها عند وقوع جريمة معلوماتية؟

وعليه تتبلور الإشكاليه الجامعة المانعة لهذه الدراسة والمتمثلة في:

ما هي خصوصية التنظيم القانوني لجريمة تقنية المعلومات؟

ومن اجل الإجابة على هذه الإشكالية، لابد من بيان خصوصية الجرائم المعلوماتية على مستوى التجريم والعقاب وهذا في (الفصل الأول)، ومن ثم على مستوى التتبع والملاحقة وهذا في (الفصل الثاني).

الفصل الأول

خصوصية الجرائم المعلوماتية على المستوى الموضوعي

أدى التقدم العلمي إلى ظهور أنماط مستحدثة من جرائم لم يُنص على تجريمها في التشريعات العقابية القائمة، فأصبحت النصوص الجزائية التقليدية غير قادرة على ملاحقتها، ومما لاشك فيه أنّ التشريع وليد الحاجة، ووجود نص يعالج الجريمة المعلوماتية على مستوى التشريع والعقاب أصبح ضرورة ملحة يجب تناولها في التشريعات العربية كافة، على غرار التشريعات في البلدان الأوروبية، حيث بدأت هذه البلدان في تنظيم تشريعاتها بالثمانيات من القرن الماضي، فأصدرت قانون الحاسب الآلي سنة 1984 لمواجهة النمط الجديد من الجرائم المعلوماتية[1].

وعليه لابد من وجود تغيير تشريعي من شأنه أن يؤسس قاعدة تشريعية تستوعب الجريمة المستحدثة، حتى نستطيع بناء مجتمع متماسك على مختلف الأصعدة، فتكنلوجيا المعلومات أصبحت أداة للربط، والاتصال، والتخزين، والإسترجاع بين الناس في مختلف أرجاء المعمورة، لذلك لا بد من تنظيم هذه المعاملات من خلال قواعد قانونية ترتقي بالمجتمع من جهة، وتحفظ حق الفرد من جهة أخرى، وعليه لا بد من التطرق إلى جرائم تقنية المعلومات في المبحث الأول، والجزاءات المقررة لهذه الجرائم في المبحث الثاني[2].

المبحث الأول: خصوصية على مستوى التجريم

أصبحت تقنية المعلومات من أساسيات الحياة، وسمة بارزة في هذا العصر إلا أن الإنسان استغلها، وأصبحت أداة لارتكاب الجريمة بدلا من كونها نعمة تُسخر لخدمة البشر ومن الجدير ذكره أن الجريمة المعلوماتية تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي

---

[1] حجازي، عبد الفتاح بيومي، **نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي**، ط1، 2009، ص9-13.

[2] الطائي، جعفر حسن جاسم، **جرائم تكنلوجيا المعلومات**، دار البداية، ط1، 2007، ص7-9.

المعلوماتي وحتى يتسنى لنا فهم الجريمة المعلوماتية تطرق الباحث في المطلب الأول إلى أركان الجريمة المعلوماتية، وفي المطلب الثاني إلى صور الجريمة المعلوماتية[1].

المطلب الأول: توسع في الأركان العامة لجرائم تقنية المعلومات.

لقد غيرت الجريمة المعلوماتية الكثير من المبادئ القانونية الخاصة في القانون الجزائي، حيث أصبحت النصوص القانونية التي تعالج الجريمة المعلوماتية اكثر مرونة ،وتحتوي على عبارات عامة فضفاضة قابلة للتفسير الواسع، وذلك على عكس النصوص التقليدية التي تتسم بالوضوح والدقة، ولبيان هذه الخصوصية على مستوى التجريم لابد من التطرق إلى الأركان العامة للجريمة المعلوماتية :

الفرع الأول: الشرط المفترض (نظام المعالجة الآلية للمعطيات).

لقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة ومستحدثة تتسع قوالبها لتشمل الجرائم المعلوماتية، فالجريمة المعلوماتية تحتاج إلى شرط مفترض كغيرها من الجرائم التقليدية، فمثلا في جريمة الإجهاض لا بد من توافر عنصر الحمل حتى نكون في صدد جريمة إجهاض ومن دون توافر هذا العنصر لا مجال لوجود جريمة إجهاض، وهذا هو الحال بالنسبة للجريمة المعلوماتية فمن دون توافر جهاز الحاسب الآلي، والشبكة المعلوماتية، ووجود معلومات معالجة آليا لا مجال لوقوع هذه الجريمة[2].

فالشرط المفترض هو" الشرط الذي يفترض القانون تواجده وقت مباشرة الجاني لفعله وبدونه لايتصف هذا النشاط بأي جريمة"[3]. وعليه يعتبر القاسم المشترك بين الجرائم المعلوماتية هو وجود الشبكة المعلوماتية، وجهاز الحاسب الآلي، ووجود نظام معالجة آلي للبيانات.

---

[1] المقصودي، محمد بن احمد بن علي، **الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونا**، دار المنظومة، 2015، ص25.

[2] قارة، مال، **الجريمة المعلوماتية**، رسالة ماجستير، كلية القانون، جامعة الجزائر، 2002/2001، ص32.

[3] http://www.qanouni-net.com/2010/10/blog-post_9421.html، مدونة القانوني، ماهية الجريمة وتقسيماتها، جامعة الشارقة، الساعة 12:23، 2017/4/3.

وهذا ما أكد عليه قانون الجرائم المعلوماتية السوداني عام 2007 حيث اشترط أن تتم الجريمة بواسطة أجهزة الحاسوب أو شبكة المعلومات حتى نكون بصدد جريمة معلوماتية.

والشبكة المعلوماتية "هي ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية(الإنترنت[1])".

أما الجهاز المعلوماتي (جهاز الحاسب الآلي): " أي جهاز الإكتروني ثابت أو منقول، سلكي أو لاسلكي يحتوي على نظام معالجة البيانات، أو تخزينها، او ارسالها، او استقبالها، او تفحصها، يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له[2]".

ولا بد من التعريج على ماهية بيانات وبرامج الحاسب الآلي حتى يتسنى للقارئ فهم الشرط الافتراضي بشكل سلس، تعد البيانات والبرامج روح الحاسب الآلي، ودون وجودها يعتبر لا قيمة له تذكر، ومن الممكن تعريف البرامج أنها "مجموعة متسلسلة من التعليمات التي ترشد الحاسب الآلي، أو الجهاز العالي التقنية لإتمام العمليات المنطقية بغرض الوصول إلى نتيجة معينة."

وتهدف هذه البرامج إلى المعالجة الآلية للمعطيات أاو البيانات، وتعرف البيانات على أنها "مجموعة من التعليمات المكتوبة بطريقة مرتبة تصلح لأغراض الاتصالات أو أي نوع من المعالجة بواسطة الانسان أو الآلة[3]".

كما وعرف المشرع الفلسطيني في المادة الأولى معالجة البيانات على انها "إجراء أو تنفيذ عملية او مجموعة عمليات على البيانات سواء تعلقت بأفراد أو خلافه ،بما في ذلك جمع تلك البيانات أو استلامها، أو تسجيلها، أوتخزينها، أوتعديلها، أو نقلها، أو استرجاعها، أو محوها، أونشرها، أو حجب الوصول إليها، أو ايقاف عمل الأجهزة، أو الغاؤه، أو تعديل محتوايته[4]".

---

[1] قانون الجرائم الالكترونية الفلسطيني رقم 16 لسنة 2017.

[2] اليحيى تركي بن محمد بن عبد الله، **مكافحة الجرائم المعلوماتية**، دار المنظومة، مجلد2 عدد7، 2013، ص260.

[3] المضحكي حنان، **الجرائم المعلوماتية، منشورات الحلبي الحقوقية**، 2014، ط 1، ص57-69.

[4] قرار بقانون رقم 16 لسنة 2017 بشان الجرائم الالكترونية الفلسطيني.

يمثل نظام المعالجة الآلية للمعطيات الشرط المفترض في الجرائم المعلوماتية كافة حسب التشريع الفرنسي، ودون هذا النظام لايكون هناك مجال للبحث عن أي ركن من أركان الجريمة، وهذا شرط يعتبر لازما لتوافر أي جريمة من الجرائم المعلوماتية.

إنّ نظام المعالجة الآلية هو مفهوم تقني فني لابد من وجود أشخاص فنيين متخصصين حتى يتسنى لرجل القانون فهمه، بالإضافة الى كون هذا المصطلح يخضع لتطورات متكررة نظرا لمرونته، وقد اقترح مجلس الشيوخ الفرنسي تعريفا له "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة، والبرامج، والمعطيات، وأجهزة الإدخال، والإخراج وأجهزة الربط التي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة، وهي معالجة المعطيات، وعليه يكون هذا المركب خاضع لنظام الحماية الفنية[1]"، ويؤدي توافر هذا الشرط إلى إمكانية الانتقال إلى المرحلة التالية، وهي البحث بأركان الجريمة حيث يعتبر هذا الشرط ضروريا لكل منها[2]

وبناء عليه نلاحظ أن للجريمة المعلوماتية طبيعة خاصة حيث أن وسيلة إرتكابها تعتبر جزء لا يتجزأ من الشرط المفترض الذي يعتبر عنصر أساسي لقيام الجريمة المعلوماتية.

الفرع الثاني: الركن الشرعي

يعد التشريع المصدر الأساسي للتجريم والعقاب، كما أن صلاحية القاضي الجنائي محدودة بالنص التشريعي، فهو لايملك صلاحية إكمال تشريع ناقص، أو استبدال العقوبة، أو حتى تفسير القاعدة القانونية، أو خلق نص تشريعي وذلك لضمان إرساء قواعد العدالة[3].

وعلى الرغم من التطورات التي طرأت على مبدأ الشرعية حيث أصبح للقاضي سلطة في تقدير العقوبة، فتطور التشريع، وأصبح للعقوبة حد أعلى وآخر أدنى، بالإضافة إلى سلطة القاضي

---

[1] قارة، مال، **الجريمة المعلوماتية**، جامعة الجزائر، كلية الحقوق،2002/2001، ص32-33.

[2] الزراع، ماجد بن كريم، **الركن المادي في الجرائم المعلوماتية في النظام السعودي**، 2014، ص30.

[3] المضحكي، حنان ريحان، **الجرائم المعلوماتية**، مرجع سابق، ص57.

بوقف تنفيذ العقوبة، إذا ماتبين أنّ أخلاق المتهم وماضيه حسنة، وبالتالي وقف تنفيذ العقوبة أجدى في إصلاح الجاني وتأهيله، إلا أن هذه المرونة طرأت على الشق الثاني المتمثل في (تقدير العقوبة) دون الشق الأول الخاص بخلق الجرائم فقد بقي هذا الشق على جموده، ومنع القاضي من ممارسة أي سلطة تقديرية في شأن تقدير الجرائم[1].

ولكن مايميز النص التشريعي الذي يعالج الجريمة المعلوماتية عن غيره من النصوص التقليدية التي تعالج الجريمة التقليدية ،أنه يتسم بإتساع دائرة التجريم لأنه عادة مايحتوي على مصطلحات فضفاضة تتناسب مع خصوصية الجريمة المعلوماتية فنصت المادة 51 من قانون الجرائم الإلكترونية الفلسطيني "إذا وقعت أي جريمة في هذا القانون بغرض الإخلال بالنظام العام ،او تعريض سلامة المجتمع وأمنه للخطر ،أو تعريض حياة المواطنين للخطر ...."كما ونصت المادة 6 من نفس القانون "كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية ،ما من شأنه إيقافها عن العمل ،أو تعطيلها،أوتدمير البرنامج ....." [2] تبين مما سبق أن النصوص التشريعية في القانون الفلسطيني تم صياغتها بعبارات واسعة وعامة تحتوي على أوجه تفسير عديدة ،حيث أصبح للقاضي سلطة أكبر في إسقاط القاعدة القانونية على عدد أكبر من هذه الجرائم التي تتميز بسعتها وتطورها السريع مع مرور الزمن.

لذلك استقر الفقه القانوني على ضرورة وجود نصوص قانونية خاصة تعمل على معالجة الجرائم المعلوماتية، وخاصة بعد انتشار شبكة الإنترنت التي ساهمت بشكل واسع في انتشار هذا النوع من الجرائم، ونلاحظ أن المجلس الأوروبي عام 1989 قام بوضع توصية لتشجيع الدول على اعتناق تشريع خاص للحد من الجريمة المعلوماتية ونرى أن بعض الدول تبنت قانونا خاصا للحد من الجريمة المعلوماتية، والبعض الآخر قام بدمج بعض النصوص قي قانون العقوبات التقليدي.[3]،

---

[1] الشكري، عادل يوسف عبد النبي، **الجريمة المعلوماتية وازمة الشرعية الجزائية**، مجلة مركز دراسات الكوفة، عدد7، 2011 ص120.

[2] قانون الجرائم الالكترونية الفلسطيني رقم 16 لسنة 2017.

[3] قارة، مال، **الجريمة المعلوماتية**، مرجع سابق، ص37.

وقد اختلفت الدول في طريقة تعاملها مع ظاهرة الجريمة المعلوماتية، فهناك أشكال أاو أنماط تشريعية مختلفة قد يلجأ إليها المشرع:

1. الإضافة وذلك من خلال قيام المشرع بإضافة السلوك الإجرامي بواسطة الحاسب الآلي إلى النصوص التقليدية، أو أنا يضيف إلى محل النشاط الإجرامي المعلومات التي يحتويها نظام الحاسب الآلي كما في نصوص جريمة السرقة.

2. وضع نصوص جديدة بالقياس مع النصوص القديمة(التقليدية) بحيث يتحول النص من صورته التقليدية إلى صورة أخرى، لكنه مرتبط بالحاسب الآلي ونظامه، وأغلب الدول تتبع هذه الطريقة.

3. تجميع كل مايتعلق بالجريمة المعلوماتية في قسم مستقل ملحق بالتشريع الجنائي، أو في تشريع مستقل، أو وضع نص رئيسي قادر أن يشمل أوجه الجريمة المعلوماتية المختلفة، وقد تبنت الولايات المتحدة الامريكية هذا الاتجاه.

4. وضع قانون خاص كما هو الحال في فلسطين حيث اقر رئيس السطة الوطنية الفلسطينية قرار بقانون رقم 16 لسنة 2017 ونلاحظ ان هذا القانون اشتمل على كافة الأفعال الجرمية المتعلقة بالجريمة المعلوماتية في قانون خاص[1].

وبناء على ذلك من الممكن اعتناق أكثر من نمط تشريعي بما يتلائم مع طبيعة النظام القانوني في كل دولة، فتعد السويد من طليعة الدول التي تناولت جرائم الإنترنت والحاسب الآلي بتشريعات قانونية جديدة وخاصة حيث صدر أول قانون خاص بها سمي قانون البيانات في عام (1973).

كما صدر في الولايات المتحدة الأمريكية في ولاية فرجينيا أيضا قانون خاص بجرائم الحاسبات الآلية عام(1986) حيث تضمن نص يجرم سرقة الخدمات التي يقدمها الحاسب الآلي وتميز هذا النص بأنه بتطلبه أن يكون الاستعمال قد تم بسوء نية، أما المملكة المتحدة لاتوجد بها

[1] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

تشريعات مكتوبة تعالج الجرائم المعلوماتية، لأنها تعتمد على نظام السوابق القضائية، وفي النمسا صدر تشريع خاص في عام (2000)، ومن الدول التي وضعت قوانين خاصة لبرامج الحاسوب كوريا الجنوبية "قانون حماية برامج الحاسب الآلي" عام (1986) كما اصدرت الدنمارك قانون" جرائم الحاسب الآلي"(1985). ومن الضروري وضع قواعد قانونية خاصة بالجرائم المعلوماتية وليس إدراجها في قانون العقوبات، لما لهذه الجرائم من طبيعة خاصة تتطلب نصوص موضوعية وإجرائية متخصصة.

من خلال ماسبق نلاحظ أن أوائل الدول التي وضعت التشريعات الجنائية الخاصة بالظاهرة المعلوماتية هي الدول ذات التقدم الحضاري والتقني.

أما بالنسبة لدور الدول العربية في مواجهة الجرائم المعلوماتية نلاحظ أن الدول الخليجية برزت في هذا الخصوص حيث يعتبر القانون العماني أول قانون عربي يواجة الجريمة المعلوماتية، حيث تم التعديل على قانون الجزاء العماني، وتعد دولة الإمارات العربية أول دولة عربية تصدر قانونا مختصا في مكافحة الجرائم المعلوماتية، ويعد من القوانين النموذجية التي اشتملت على أغلب الجرائم المعلوماتية عام 2006 وتم تعديله عام 2012 كما صدر نظام مكافحة الجرائم الإلكترونية في المملكة العربية السعودية عام 2007 وتم تعديله سنة 2015 [1] بالإضافة الى قانون الجرائم الإلكترونية الفلسطيني سنة 2017.

الفرع الثالث: الركن المادي

يتحقق الركن المادي لأي جريمة إما بالقيام بعمل يعاقب عليه القانون، أو الامتناع عن عمل يلزم به القانون مع تحقق النتيجة الضارة وبالتالي توافر علاقة السببية بين الفعل والنتيجة.[2]

---

[1] البقمي، ناصر بن محمد، **مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية**، مركز الامارات للدراسات والبحوث الاستراتيجية، سلسلة محاضرات الامارات 116، ص33-40.

[2] الزراع، عادل بن كرم. رسالة ماجستير **بالركن المادي في الجرائم المعلوماتية بالنظام السعودي**، الرياض، 2014، ص33.

وحتى يتسنى لنا فهم الركن المادي للجريمة المعلوماتية سوف نتطرق إلى:

1- السلوك الإجرامي: هو سلوك إيجابي أو سلبي، حيث يصدر من الجاني اعتداء على المصلحة المحمية، ويظهر بمظهر يستدل عليه بالحواس، ويختلف مظهره باختلاف الجريمة، كما أن الأعمال التحضيرية لا تعتبر جزءا من الركن المادي مالم يعاقب عليها القانون بشكل منفصل[1].

إن النشاط أو السلوك المادي في الجرائم المعلوماتية يتطلب وجود بيئة رقمية، واتصال بالإنترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يهيئ له حدوث الجريمة فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، وتحميلها على الجهاز المضيف (Hosting Server)، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها[2].

وعليه فإن الفعل والامتناع هو الذي يبرز الجريمة إلى حيز الوجود، لأن هذا الفعل هو المظهر الخارجي للنشاط المحظور وتوافره شرط لازم في جميع صور الجريمة، فإذا كان السلوك تاما كانت الجريمة كذلك، وإذا وقف عند حد معين كانت الجريمة شروعا[3].

والسلوك الإجرامي في كل جريمة يحدده المشرع، فبالنسبة للجريمة المعلوماتية نلاحظ أن السلوك الإجرامي قد يرتبط بالمعلومات المخزنة على جهاز الحاسوب الآلي، أو المعلومات التي أدخلت به، او سرقة صور من[4] الهاتف النقال.

---

[1] الزراع، عادل بن كرم. رسالة ماجستير **بالركن المادي في الجرائم المعلوماتية بالنظام السعودي**، الرياض،2014، ص33.

[2] الركن المادي في جرائم الإنترنت، س11:42 ص، 2016/7/3http://www.startimes.com/?t=25263137

[3] الحلبي محمد علي السالم، **شرح قانون العقوبات**، مكتبة الثقافة والنشر للتوزيع، ص231.

[4] المضحكي، حنان، **الجرائم المعلوماتية**، مرجع سابق، ص84-90.

وفي الجريمة المعلوماتية قد يبدأ السلوك الإجرامي بضغطة زر، أو لمسة على الشاشة، فمثلا يمكن أن يقوم المجرم المعلوماتي ببرمجة فايروس، وإرساله إلى أحدهم مما أدى إلى إحداث ضرر في الجهاز الآخر، فالسلوك الإجرامي يتمثل في إرسال هذا الفايروس في تلك الحالة، أي بضغطة زر(نشاط ايجابي)، ويمكن أن يتحقق الركن المادي من خلال الامتناع عن عمل، ومثال ذلك جريمة التزوير المعلوماتي كالشخص الذي يقوم بتغيير الحقيقة من خلال الترك، كمن عهد اليه كتابة محرر وتعمد إغفال بيانات مهمة فيه، فيتم تغيير الحقيقة من خلال امتناعه (نشاط سلبي)[1].

2- النتيجة الجرمية: تعني الأثر المترتب عل السلوك الإجرامي ولها مدلولان: الأول مادي يتمثل في تغيير العالم الخارجي، وهذا المدلول هو السائد اليوم بصفة شبه مطلقة، وبمقتضاه تكون النتيجة في استظهارها مستقلة تماما عن نفسية الجاني، وبناء عليه ووفقا لهذا المعيار تعتبر النتيجة فكرة نسبية تتحدد بالنظر إلى جريمة بعينها وتختلف من جريمة إلى أخرى. أما المدلول الثاني فهو قانوني يتمثل في الاعتداء على المصلحة المحمية، فالنتيجة وفقا لهذا المدلول لاتعبر عن الأثر المادي الملموس لنشاط الجاني، وإنما هي حقيقة قانونية محضة تتمثل في الاعتداء على الحق الذي يحميه القانون، وحسب رأي أنصار المدلول القانوني أن جميع الجرائم تتضمن بين عناصرها نتيجة إجرامية لأن كل نص من نصوص التجريم يقوم دائما على حماية مصلحة معينة[2].

وبالنسبة للجريمة المعلوماتية لايختلف مفهوم الضرر بشكل عام بالجرائم المعلوماتية عن مفهوم الضرر التقليدي بشكل جازم فهو "كل إخلال بمصلحة مشروعة للمتضرر في ماله أو شخصه"إلا أنه يختلف بوصفه ذات طبيعة غير محددة، لأنه يمس الطبيعة المعلوماتية وقد يكون الضرر ماديا مثل التلاعب ببيانات ومعلومات قد تؤدي إلى إزهاق أرواح كما في الطائرات والسيارات وغيرها من الأمور الحيوية، وقد يكون معنويا مثل التجسس الإكتروني، أو الحصول على بيانات خاصة، أو صور خاصة.

---

[1] الزراع، ماجد بن كريم، **الركن المادي في الجرائم المعلوماتية**، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، 2014، ص77.

[2] رمضان، عمر السعيد، **فكرة النتيجة في قانون العقوبات**، دار الاسراء للنشر والتوزيع، الاردن، 1998، ص4-8.

ومما لا شك فيه تثير مسألة النتيجة الإجرامية في الجرائم المعلوماتية مشاكل عديدة، فعلى سبيل المثال مكان تحقق النتيجة الإجرامية وزمانها، والقانون الواجب التطبيق، فلو قام أحد المجرمين في بلد ما باختراق جهاز خادم Server أحد البنوك في بلد آخر، وهذا بلد موجود في مكان ثالث فكيف يمكن معرفة وقت حدوث الجريمة؟ هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم؟[1]

من الجدير ذكره أن النتيجة قد لا تدخل عنصرا بالركن المادي في الجرائم كافة، حيث إن هناك جرائم تقوم على النشاط المحض، فيعاقب القانون على النشاط ذاته، وعليه نلاحظ مدى تاثير النتيجة الجرمية على الركن المادي من حيث التمييز بين جرائم الضرر وجرائم الخطر، وكذلك الأمر بالنسبة للجريمة المعلوماتية، فبعض جرائم معلوماتية تصنف على أنها جرائم لاتحتاج إلى نتيجة ضارة مثل جريمة الدخول الالكتروني (جرائم خطر)، والبعض الاخر تصنف على أنها (جرائم ضرر) مثل جريمة التزوير المعلوماتي.

3- علاقة السببية: وتعني وجود علاقة سببيه بين السلوك الإجرامي، والنتيجة الجرمية فحتى يثبت السلوك الإجرامي لابد من توفر علاقة السببية بين السلوك والنتيجة، والقانون غالبا لايضع معيارا لتحديد علاقة السببية وأنا يترك الموضوع للفقه والقضاء.

إن المعيار في ربط علاقة السببية بين الفعل والنتيجة يقوم على عدم تصور النتيجة لولا حدوث ذلك الفعل، وبناء عليه هناك عدة نظريات وضعها الفقهاء لتحديد معيار علاقة السببية بين الفعل والنتيجة:

أولاً: نظرية السبب الأقوى

فهي تقوم على فكرة السبب المباشر في حدوث النتيجة، أما العوامل الأخرى فهي مجرد عوامل مساعدة.

[1] **أركان الجريمة المعلوماتية**، 11:30 م، 2016/1/3 http://www.startimes.com/?t=25263137.

ثانياً: نظرية تعادل الأسباب

تقوم على فكرة أن هناك عدة أسباب متداخلة ساهمت في حدوث الجريمة إلا أن فعل الجاني المسؤول عن النتيجة بحيث أن العلاقة بين الفعل والنتيجة لا ينفيها اجتماع أسباب أخرى سواء جهلها الفاعل أو كانت مستقلة عن فعله.

ثالثاً: نظرية السبب الملائم

تقوم على فكرة ان فعل الجاني يصلح في الظروف التي وقع فيها أن يكون سببا ملائما في حدوث النتيجة وفقا للمجرى العادي للامور[1].

وعليه نلاحظ على الرغم من اختلاف المعايير في الربط بين السلوك والنتيجة الا انه يجب ان يثبت قيام علاقة السببية بين النشاط الاجرامي والنتيجة الاجرامية فمثلا في جريمة انتهاك الحق في الخصوصية عبر الانترنت، يجب أن يكون هناك دخول على الإنترنت باستخدام حاسوب العامل، والقيام باختراق الخوادم المختلفة في مسارها، وبعد ذلك التعدي على خصوصية موقع ما، فالعلاقة السببية تثبت بمجرد ثبوت الضرر على المجني عليه، ونسبته إلى الفاعل الذي قام بالسلوك ومن الجدير ذكره أن القانون عادة لايضع معيارا لقيام علاقة السببية تاركا ذلك لاجنهاد الفقه والقضاء[2].

الفرع الرابع: الركن المعنوي

ماهية الركن المعنوي في الجرائم المعلوماتية: أن الركن المعنوي في الجرائم المعلوماتية هو اتجاه إرادة الجاني إلى إحداث النتيجة الجرمية وارتكاب إحدى الجرائم المعلوماتية المنصوص عليها بالتشريعات المختلفة لأنه بتوافر هذا الركن تتوافر اركان المسؤولية الجنائية كافة، وعند الحديث عن الركن المعنوي لا بد من ذكر عنصريه العلم والإرادة.

---

[1] الحلبي، محمد علي السالم، **شرح قانون العقوبات**، دار الثقافة للنشر والتوزيع، ص239-243.

[2] الزراع، ماجد بن كريم، **الركن المادي في الجرائم المعلوماتية في النظام السعودي**، رسالة ماجستير، 2014، ص34.

فالعلم يعني علم الجاني بالصفة الإسمية والشخصية للبيانات أو أن يعلم بطبيعة الحاسب الآلي بأنه يقوم بعملية المعالجة الآالية للبيانات، أما الإرادة فهي أن تتجه نية الجاني إلى القيام بالمعالجة الآلية للبيانات بأي صورة كانت (مخالفة الإجراءات المعتمدة لإجراء المعالجة الإلكترونية للبيانات) أي أن القصد المتطلب لقيام هذا النوع من الجرائم هو القصد العام بحيث لاعبرة بالبواعث التي دفعت الجاني إلى ارتكاب فعله، فسواء كان الباعث هو الإضرار المادي بالشخص أم استغلال هذه البيانات للإساءة لسمعة الشخص[1].

ونلاحظ أن القوانين والتشريعات التي نظمت الجريمة المعلوماتية حتى عام (1990) ركزت في المقام الأول على السلوك الإجرامي، وهو الامر الذي تطلب ضرورة تطوير القوانين والتشريعات التي تأخذ في اعتبارها الشق الخاص بالقصد الجنائي بالجريمة المعلوماتية.[2]

وبالرجوع إلى نظام مكافحة الجرائم المعلوماتية السعودي نلاحظ أن المشرع لم يتطرق أو لم يعالج موضوع الجرائم المعلوماتية غير العمدية، وبالتالي اعتبر المشرع السعودي أن الجرائم المعلوماتية هي من الجرائم العمدية يتطلب توافر عنصري العلم والإراده فيها.

كما ونلاحظ أن القصد الجرمي في الجريمة المعلوماتية يختلف باختلاف الجريمة وبالنسبة للمشرع الالفلسطيني نلاحظ انه تطلب في بعض الجرائم توافر العلم والارادة كما هو الحال في نص المادة 8 "كل من قام عمدا بفك بيانات مشفرة في غير الاحوالالمصرح بها قانونا...."[3] كما افترض المشرع السعودي وجود العلم والإرادة المسبقين لدى الجاني بمجرد ارتكاب السلوك المجرم ويقع على عاتق مرتكب السلوك نفي علمه وإرادته.

كما أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الإنترنت من حيث مدى تحديد إذا ماكانت تتطلب قصد عام أو خاص.

---

[1] السالم محمد علي، **الجريمة المعلوماتية**، مجلة جامعة بابل، عدد2، المجلد 14، 2007، ص94.

[2] كريري، عبد الله بن حمد، **الركن المعنوي في الجرائم المعلوماتية في النظام السعودي**، رسالة ماجستير،2013، ص103.

[3] قانون الجرائم الالكترونية الفلسطين رقم 16 لسنة 2017.

أما في القضاء الفرنسي نلاحظ أنّ سوء النية يكتسح النصوص التي تطبق بشأن الجرائم المعلوماتية (أي توافر قصد خاص) ومن ذلك ماهو مقرر في المادة 15-226 عقوبات فرنسي التي تشترط سوء النية حين وجود عدوان على البريد الالكتروني[1].

وقد اختار الباحث بعض التطبيقات العملية للجرائم المعلوماتية وذلك حتى يتنسى للقارئ فهم الخصوصية في الجرائم المعلوماتية بشكل أوضح، ففي الآونة الأخيرة الكثير من الدول استشعورا ضرورة وجود تشريعات جديدة تحمي المعلومات داخل نظام الكمبيوتر، وذلك لعجز النصوص التقليدية عن حماية هذا النظام، فمنها من يجرم مجرد التداخل في نظام الحاسوب، ومنها ماجرم إتلاف المعلوماتت المبرمجة، ومنها ماجرم تغيير هذه المعلومات[2].

المطلب الثاني: توسع في صور الجرائم المعلوماتية

يمكن النظر إلى الجريمة المعلوماتية على أنها استخدام لتقنيات المعلومات في عمليات اختراق وتعد، وتزوير للبيانات، حيث يصنف الفقهاء الجرائم المعلوماتية ضمن فئات متعددة تختلف حسب الأساس أو المعيار الذي يستند إليه التقسيم، وقد ارتئينا تسليط الضوء على عينة من صور الجرائم المعلوماتية الأكثر شيوعا والأكثر إثارة للجدل بين أوساط المتخصصين، ولما لها من خصوصية في موضوع البحث، وقد تم تناول هذه الصور على ثلاثة فروع أساسية، الفرع الأول جريمة الدخول والبقاء غير المصرح به، والفرع الثاني جريمة الإتلاف المعلوماتي، والفرع الثالث جريمة التزوير المعلوماتي.

[1] إبراهيم، خالد ممدوح، **الجرائم المعلوماتية**، دار الفكر الجامعي، ط1، 2009، ص105-108.

[2] عطا الله، شيماء عبد الغني، **الحماية الجنائية للتعاملات الإلكترونية**، دار الجامعة الجديدة، ط 2227، ص94.

الفرع الأول: الدخول والبقاء غير المصرح بهما.

تتحقق جرائم اختراق جهاز الحاسب الآلي أاو المواقع في الشبكة المعلوماتية بأن يدخل الجاني لصفحات المواقع الالكترونية والاطلاع على البيانات والمعلومات الموجودة بها دون أن يكون مصرحا له بذلك، ولمعرفة متى تتحقق جريمة الدخول لا بد من تحديد أركان هذه الجريمة[1].

أولا: الركن المادي لجريمة الدخول

بالنسبة لفعل الدخول فلا يقصد به معناه المادي كدخول منزل أو حديقة، إنما يقصد به الدخول المعنوي والمتمثل بالدخول إلى الأفكار الذهنية التي يقوم بها نظام المعالجة الآلية، وغالبا مايكون على البرامج المخصصة لتخطي أنظمة الحماية الفنية، فعادة ماتكون هناك أنظمة فنية تحول دون الاتصال غير المشروع بالبرامج والبيانات المخزنة، ولكن بالمقابل هناك أنظمة أو برامج تستخدم لتتخطى حواجز الحماية هذه قد يلجأ إليها الأاشخاص من أجل تحقيق دخول غير مشروع، وهذه البرامج إذا ما وقعت بأيدي أشخاص غير مصرح لهم فهي شديدة الخطورة، لأنها قد تخترق أمن وسرية البيانات كافة، والتغلغل في منظومات الحاسوب حتى لو كانت محمية بشكل دقيق، وكما ذكرنا سابقا تعتبر الجريمة قد ارتكبت في حال قام الجاني بفعل الدخول سواء أكان يستفيد من هذا الدخول أم لا، وسواء كان الدخول جزئيا أو كليا.

كما أن الدخول المقصود به ليس الدخول المادي أي الدخول إلى المكان الذي يتواجد به الحاسب الآلي بشكل غير مشروع، وإنما يتطلب الموضوع النشاط الذهني الذي يقوم به الجاني، كما أنه لا يشمل الحالات الناشئة عن طريق الصدفة، ومما لا شك فيه يجب أن يكون الدخول غير محق أو غير مصرح به حتى نكون بصدد جريمة تستوجب العقاب[2]. وهذا ما نص عليه قانون الجرائم الالكترونية الفلسطيني في الماد 4 "كل من دخل عمدا دون وجه حق باي وسيلة موقعا إلكترونياً، أو نظاما، أو شبكة إلكترونية، أو وسيلة تكنلوجيا معلومات، أو جزء منها، أو تجاوز

[1] المضحكي، حنان، ريحان مبارك، **الجرائم المعلوماتية**، منشورات الحلبي الحقوقية، ط1، سنة 2014، ص101.

[2] قورة، نائلة عادل محمد، **جرائم الحاسب الاقتصادية**، مرجع سابق، ص344-345.

الدخول المصرح به ..... " نلاحظ من خلال استقراء النص أن القانون الفلسطيني اشترط حتى تتم جريمة الدخول ان تكون قد تمت بشكل عمدي[1].

كما ونصت المادة 4 فقرة 2 "إذا ارتكب الفعل المحدد على البيانات الحكومية[2] ....".

كما أن فعل الدخول ممكن إن يتم بسلوك إيجابي (من خلال أي وسيلة تمكن الجاني من الدخول إلى جهاز الحاسب الآلي سواء من خلال برامج أو فيروسات)، أما السلوك السلبي فيتمثل بالامتناع عن الخروج في حال كان الدخول مسموحا إلا أن الجاني تجاوز المدة المصرح بها).

وعليه تتمثل جريمة الدخول والبقاء بشكلها البسيط في حال الدخول أو البقاء غير المشروع في نظام المعالجة الآلية، وتكون الصورة المشددة لهذا الدخول أو البقاء في حال محو أو تغيير في النظام وهذا ما ورد بالمادة 323 من قانون العقوبات الفرنسي..

اما بالنسبة للقانون الفلسطيني فإن صورته المشددة لجريمة الدخول تتحقق كما ورد في نص المادة 4 فقرة 3 عندما يرافق هذا الدخول إلغاء بينات او معلومات الكترونية مخزنة في النظام المعلوماتي أو حذفها، أو إضافتها، أو إفشاؤها، أو تدميرها، أو إتلافها، أو تغييرها، أو نقلها، أو نسخها، أو نشرها، أو إلحاق الضرر بالمستخدمين، أو تغيير الموقع الإلكتروني، أو إلغاؤه، أو تعديل محتوايته، أو شغل عنوانه وتصميماته، أو انتحال شخصية مالكه أو القائم على إدارته، وتصبح العقوبة في أوجها عندما يتعلق أي عمل من الأعمال المرافقة للدخول في صورته المشددة على البيانات الحكومية[3].

يتبين من خلال ماسبق أن المشرع الفلسطيني أورد صورا مختلفة للدخول تتمثل بصدور فعل من قبل المجرم المعلوماتي من خلال الشبكة المعلوماتية يهدف للحصول على معلومات بطريقة غير مشروعة بغض النظر عن طبيعة هذه المعلومات، فمعيار العقوبة هو مجرد فعل

[1] قانون الجرائم الإكترونية الفلسطيني رقم 16 لسنة 2017.

[2] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

[3] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

الدخول بغض النظر عن دواعيه وأسبابه إلا ان العقوبة تتشدد إذا رافق الدخول حدوث ضرر أو اذا كان فعل الدخول قد استهدف بيانات حكومية[1].

وقد عرف نظام مكافحة الجرائم في المملكة العربية السعودية في فقرته السابعة من المادة الأولى الدخول غير المشروع "دخول شخص بطريقة متعمدة في نظام الحاسب الآلي، أو موقع الكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها "[2].

وهناك بعض التشريعات التي حذت حذو التشريع الفرنسي التي جرمت مجرد الدخول والبقاء، ولكن كان موقف هذه التشريعات متباينا، فالبعض قيد جريمة الدخول بتوافر قصد خاص، وهو قصد التاثير على البيانات، أو التاثير على جهاز الحاسب الآلي نفسه حتى يعاقب على جريمة الدخول من ذلك القانون الألماني، والقانون الكندي، والقانون النمساوي ومنهم من لايعاقب على الدخول إلا إذا اقترنت نية المجرم المعلوماتي بالاستيلاء على أموال الغير بطريق الغش مثل ولاية فرجينيا في الولايات المتحدة الامريكية، ومن هذه التشريعات ما تعاقب على مجرد الدخول بغض النظر عن نية المتهم ومنها التشريع الهولندي، والاسترالي، والفنلندي[3].

حتى أن القانون الإنجليزي اعتبر أن الدخول إلى النظام المعلوماتي من أجل مراقبة الاتصالات المرسلة عبر شبكة الاتصالات يعتبر جريمة يعاقب عليها، وتتلخص وقائع أول قضية نظرها القضاء الانجليزي بقيام شخص كان عضوا في مجلس ادارة احدى الشركات ومساهما فيها بالطلب من موظف يعمل بالشركة بمراقبة البريد الالكتروني الخاص برئيس مجلس الإدارة وذلك بعد أن تم تزويده بالتفاصيل المتعلقة بكلمة المرور، واسم المستخدم من قبل أحد الموظفين المصرح له بالدخول حتى يتمكن ذلك الموظف من الدخول إلى النظام المعلوماتي ومراقبة الرسائل الإلكترونية، ونسخها وفي هذه القضية أدانت المحكمة المتهم بصفته موظفا غير مصرح له بالدخول للنظام

---

[1] المضحكي، حنان ريحان، الجرائم المعلوماتية، منشورات الحلبي الحقوقية ط.1، 2014، ص101-105.

[2] قارة، مال، **الجريمة المعلوماتية**، مرجع سابق، ص42-44.

[3] د.شيماءعطا الله، **الحماية الجنائية للتعاملات الإالكترونية**، دار الجامعة الجديدة، بدون ط، 2007، ص94-97.

المعلوماتي بجريمة[1]. كما أن المشرع السعودي يرى أن الدخول يمثل كل استعمال للحاسب الآلي دون رضا صاحب الحق فيه أيا كان هذا الاستعمال[2]."

وعلى الرغم من ضرورة تجريم الدخول غير المصرح به لنظام الحاسب الآلي إلا أن هناك من يرى أنه لاضرورة لتجريمه، لأن مجرد الدخول العادي غير المقترن بجريمة لاتوجد ضرورة ملحة لتجريمه، حيث أنه لا يتعدى مجرد استعراض للمهارات أو القدرات كما أنه من الناحية العملية حالات الدخول التي لايترتب عليها أي إتلاف للمعلومات غالبا ما يصعب الكشف عنها لما تنطوي عليه من صعوبة فنية بالغة سوف تحول دون تجريم الفعل[3].

على الرغم مما أثاره أنصار عدم تجريم عقوبة الدخول إلا أننا نجدد ضرورة تجريم هذا السلوك، لأن الدخول بحد ذاته يؤدي إلى انتهاك خصوصية المعلومات حتى أن نية ارتكاب الجريمة قد تتولد بعد ارتكاب فعل الدخول، أما فيما يتعلق بصعوبة إثبات الجريمة فإن هذه الصعوبة تنطوي على الجرائم المعلوماتية بشكل عام، ومع ذلك لابد من تجريم هذه السلوكيات دون استثناء.

والسؤال هنا: هل تعد جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي جريمة مادية أم جريمة شكلية؟

بعض التشريعات لم تشترط تحقيق النتيجة الإجرامية بأن ينجح الفاعل في الوصول إلى أي معلومات أو برامج، وعلى الرغم من أن علة التجريم هي حماية المعلومات إلا أن هذا النوع من الجرائم يمثل عدوانا محتملا على الحق حتى إنّ أغلب الدول أخذت بهذا الاتجاه وهذا ما أاخذت به كل من واليونان والبرتغال وفنلندا وهولندا، ففعل الدخول هنا ينطوي على أساس المساس بحق المسئول عن النظام في السيطرة عليه بغض النظر عن المساس بسرية المعلومات.

---

[1] الرواشدة، سامي حمدان، **مكافحة الجريمة المعلوماتية بالتجريم والعقاب**، مجلد 1، العدد3، 2009، ص131.

[2] الزراع ماجد بن كريم، **الركن المادي في الجرائم المعلوماتية بالنظام السعودي**، مرجع سابق، ص118.

[3] قورة، نائل عادل محمد، **جرائم الحاسب الاقتصادية**، دار النهضة العربية، د ط، 2004/2003، ص328.

والمشرع الفرنسي في المادة (323) من قانون العقوبات الفرنسي لم يشترط حدوث نتيجة جرمية، فالجريمة تقع عند دخول المجرم المعلوماتي للنظام من دون موافقة صاحبه، حتى وإن لم يحدث ضرر، أما الفقرة الثانية من المادة ذاتها فاعتبرت أن حدوث ضرر جراء الحذف أو التعديل من الظروف المشددة لهذه الجريمة، وتقع جريمة الدخول تامة حتى لو لم يحصل المتدخل على المعلومات، وحذا المشرّع السعودي حذو المشرع الفرنسي فلم يشترط حدوث أي نتيجة للعقاب على فعل الدخول فهي تعد من الجرائم الشكلية التي لاتحتاج الى حدوث نتيجة[1] علما أن بعض التشريعات اشترطت اقتران الدخول بالحصول على المعلومات مثل استراليا [2].

أما بالنسبة لفرضيات الدخول بأن يكون المجرم موجودا مكان توافر أجهزة الكمبيوتر، ويقوم باختراقها واستعمالها، أو أن يدخل المجرم المعلوماتي إلى النظام عن بعد عن طريق شبكة الإنترنت، ولكن هل يعتبر الدخول عن بعد جريمة دخول أم جريمة تجسس على النظام المحوسب؟

والإجابة عن هذا التساؤل تختلف من مشرّع إلى آخر، ولكن في فرضية التجسس لا يقوم الفاعل باستعمال النظام ولكنه يقوم بالاطلاع عليه من الخارج فنكون بصدد جريمة تجسس، أما إذا قام باقتحامه واستعماله نكون بصدد جريمة دخول، فالتداخل عن بعد لايشكل جريمة دخول بالسياق السابق ذكره وإنما هو أقرب إلى جريمة التجسس.

ويقصد بالنظام في جريمة الدخول غير المصرح به هو نظام الحاسب الآلي، ويستوي أن يكون محميا بأسلوب معين مثل كلمة سر أم غير محمي، وفي هذا قضت معظم التشريعات (الإنكليزية، والفرنسية، والكندية، والسعودية) فلم تشترط وجود كلمة مرور للعقاب على الدخول غير المشروع، كما يشمل الدخول اعتراض الاتصالات بين جهازين أو أكثر من خلال شبكات تربط بين هذه الأجهزة.

---

[1] قارة، مال، **الجريمة المعلوماتية**، مرجع سابق، ص43.

[2] قورة، نائلة عادل محمد، **جرائم الحاسب الاقتصادية**، مرجع سابق، ص352-357.

وبناء على ما ذكر لا يلزم أن يكون هناك نظام محمي حتى تتوافر الحماية الجنائية للنظام إلا أانه من الناحية العملية نلاحظ أنّ غالبية أنظمة المعالجة الآلية للبيانات أو المعطيات تشمل على نظام حماية فني، وذلك حتى يتسنى إثبات أركان الجريمة وخصوصا الركن المعنوي.

ومن الضروري وجود حماية فنية للنظام، واعتباره شرطا أساسيا لتطبيق القاعدة القانونية، وذلك لأن القانون من المفروض أن يقوم بحماية الأشخاص الذين لديهم الحرص على أموالهم، وبالتالي يكون دور القانون الجنائي دورا وقائياً[1].

أما بالنسبة لفعل البقاء، أي التواجد في نظام المعالجة الآلية للمعطيات بمخالفة إرادة من له الحق في السيطرة على هذا النظام، وأحيانا قد تكون جريمة البقاء متلازمة مع الدخول، وأحيانا قد تكون منفردة، ففي بعض الأحيان قد يكون الدخول مشروعا، كأن يتم الدخول على نظام معين بطريق السهو أو الخطأ، ومع ذلك يبقى دون وجه حق، وأحيانا يكون الدخول مسموحا والاطلاع مشروعا، إلا أنه في الحالة التي يتم طباعة أو نسخ المعلومات قد نعتبرها صورة من صور البقاء، ويعتبر من صور البقاء أيضا بالنسبة للخدمات المفتوحة للجمهور مثلا الحصول على خدمة تيلفونية من دون دفع الرسوم المطلوبة، أو الحصول على مدة أطول من المدة التي دفع مقابلها، من خلال وسائل غير مشروعة، وفي حال اجتماع الدخول والبقاء غير الشرعيين نكون بصدد الاجتماع المادي للجرائم، ونلاحظ أن هذا النوع من الجريمة يهدف إلى حماية النظام الآلي للبيانات فهو، أيضا يحمي المعلومات والمعطيات بطريقة غير مباشرة[2].

إلا إن هناك رأيا آخر يستوجب أن يكون الدخول غير مصرح به ابتداء حتى نكون بصدد جريمة بقاء، فإذا كان الدخول قد تم بموافقة المسؤول عن النظام فيعني ذلك رضاه بالاضطلاع على المعلومات الموجودة داخل النظام، ففي حال تجاوزه للفترة الزمنية المحددة فلا يكون بصدد جريمة بقاء، وإنما يشكل هذا الفعل جريمة أخرى وهي الاستعمال غير المصرح به، أو سرقة وقت الحاسب الآلي، فالقانون الفدرالي لجرائم الحاسبات الآلية الصادر عام (1984) في الولايات

---

[1] شيماء، **الحماية الجنائية للتعاملات الإلكترونية**، مرجع سابق، ص99-120.

[2] قورة، **جرائم الحاسب الاقتصادية**، مرجع سابق، 358-365.

المتحدة الامريكية قد حدد بالمادة (1030) (أ) أن جريمة الدخول غير المصرح به لا تقوم إذا كان الشخص الذي قام بالدخول مصرحا له بذلك، إلا أنه قام باستخدام هذا الدخول لأغراض تتجاوز هذا التصريح فالأمر يتعلق باستعمال الحاسب الالي وليس دخوله[1].

وقد كان التشريع التشريع الفرنسي إيجابي، حيث "ذهبت محكمة استئناف باريس في حكم لها صدر في(5) إبريل (1994) إلى أن القانون يجرم البقاء غير المصرح به داخل نظام الحاسب الآلي سواء كان دخوله قد تم عن طريق الخطأ أو بطريقة مشروعة"[2]، الذي جعل من البقاء داخل نظام الحاسب الآلي جريمة، حتى ولو كان الدخول بموافقة المسؤول لأن الحكمة من هذا التجريم هي حماية المعلومات، وذلك نظرا لأن هذه المعلومات قد تتغير أو قد يطرأ عليها تغيرات يجب أن يكون المصرح له بالدخول في منأى عنها.

وقد أعمل النظام الفرنسي جريمة البقاء في قضية تتلخص وقائعها في قيام العاملين في شركة خطوط تلفونية باستعمال الخط من دون دفع مقابل مادي، وقد أعمل هذا القضاء وصف البقاء في النظام بطريق الغش وليس الدخول، لأن العاملين كان من المصرح لهم الدخول إلى النظام والإشراف عليه، وإصلاح أعطاله.[3]

وهنا نسأل متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؟

ذهب رأي من الفقهاء إلى أن جريمة الدخول تبدأ من لحظة دخول البرنامج، ومجرد البقاء فترة من الزمن تنتهي جريمة الدخول وتبدأ جريمة البقاء وتنتهي بانتهاء هذا البقاء.

وهذا الرأي لايحدد بشكل دقيق لحظة بدء جريمة البقاء، ومن الممكن الاستعاضة عنه بحسم الموضوع وذلك وفقا للركن المعنوي، أي أن جريمة البقاء تبدأ منذ اللحظة التي يعلم بها المجرم أن بقاءه غير مشروع، إلا إن هذه النظرية يمكن إن تكون صعبة الإثبات.

---

[1] إلا أن هذا التحديد قد اختفى بعد تعديل القانون عام 1968 على العكس فقد تضمن القانون بعد تعديله الاخير عام 1996 نصا يجرم مثل هذا التجاوز باعتباره دخولا غير مصرح به.

[2] قورة نائلة عادل فريد، **جرائم الحاسب الالي الاقتصادية**، منشورات الحلبي الحقوقية، ط1،2005، ص347.

[3] قارة، مال، **الجريمة المعلوماتية**، مرجع سابق، ص44.

ومن الجدير ذكره أن القضاء االفرنسي اعتبر تجريم البقاء من النصوص الاحتياطية التي لايمكن نسبها إلى فاعل جريمة الدخول، وذلك كما في جريمة القتل فمن قام بارتكاب جريمة القتل لايرتكب جريمة إخفاء جثة القتيل على الرغم من ارتكابه لها، إنما وجد النص لمخاطبة غير المساهم في القتل، وكذلك غير المساهم في التدخل لذلك فجريمة البقاء لا تصدر من الفاعل في جريمة الدخول.

وترجع أهمية ماسبق كون الدخول من الجرائم الوقتية، أما البقاء فهي جريمة مستمرة، وبالتالي فإن التقادم تحتسب مدته من وقت التدخل لمن قام به مادام هذا التدخل يشكل جريمة، وإذا تقادمت جريمة التدخل فإنه يصح تحريك الدعوى جنائية عن جريمة البقاء وتحتسب مدة التقادم من الوقت الذي ينتهي فيه هذا البقاء[1].

ثانياً: الركن المعنوي لجريمتي الدخول والبقاء.

يلزم لقيام المسؤولية الجنائية في هاتين الجريمتين توفر القصد الجنائي بصورتيه: العلم والإرادة، فلا يعاقب على هذه الجرائم إلا إذا تمت عن طريق الغش، وهي جريمة عمدية يجب أن تتجه إرادة الجاني إلى فعل الدخول أو فعل البقاء، فإذا توفر القصد الجنائي فلا يعتد بالباعث من الدخول أو البقاء كما لو كان مثلا الفضول أو إثبات المهارة.[2]

جميع النصوص القانونية تطلبت وجود القصد العام في جريمة الدخول على الرغم من اختلاف في بعض المصطلحات، أو الصياغة المستخدمة فنلاحظ أن الدنمارك، وفنلندا، وسويسرا، والبرتغال، والولايات المتحدة اشترطت أن يتم الدخول إلى النظام دون تصريح، وفي السويد، واليونان، أن يتم الدخول إلى النظام دون وجه حق، والقانون الإنجليزي أن يتم الدخول إلى النظام على نحو غير مصرح به.

---

[1] عطا الله، شيماء عبد الغنى محمد، **الحماية الجنائية للتعاملات الالكترونية**، مرجع سابق، ص121-123.

[2] مقلة، آمال، **الجريمة المعلوماتية**، مرجع سابق، ص59-6.

وعليه يجب أن يكون الجاني عالما بمايتطلبه القانون من وقائع لإستكمال عناصر الجريمة، وأيضا أن يكون متوقعا للنتيجة الجرمية وهي الدخول غير المصرح به، ولكن لايشترط أن يتوقع الضرر الذي سوف يلحق النظام من جراء هذا الدخول[1].

وفي حكم بهذا الشأن أصدرته محكمة التمييز في دبي حول واقعة إختراق شبكة مؤسسة الإتصالات ونسخ بعض الملفات ورسائل البريد الإلكتروني ونقلها إلى حاسب آلي خاص حيث ورد في الحكم"إذا ورد في النص التشريعي لفظ مطلق ولم يقم الدليل على تقييده فقد أفاد ثبوت الحكم على إطلاقه ولما كانت المادة 46 من القانون رقم 1/91 تنص على عقاب كل من يستخدم الأجهزة أو الخدمات أو التسهيلات التي تقدمها المؤسسة في الإزعاج أو إيذاء مشاعر الآخرين أو أي غرض آخر غير مشروع وكانت هذه العبارة الأخيرة قد وردت على سبيل الإطلاق في مجال بيان الأعمال المؤثمة بما مفاده شمول الحظر لكل فعل غير مشروع في نطاق إعمالها أيا كانت طبيعته طالما خرج عن الغرض محدد له في استخدام الشبكة طبقا للشروط المنصوص عليها في المادة 12 من القانون ، حيث أن ماقام به المتهم من إعترافه بإختراق لشبكة الاتصالات التابعة لمؤسسة الإمارات مستخدما برامج للبحث عن الثغرات واستطاع بذلك الحصول على كلمات السر لبعض المواقع المحظورة وهو يعلم بحظر ذلك هذا يوقعه تحت طائلة العقاب[2].

و عليه يتحقق القصد الجنائي بغض النظر عن البواعث فلو كان الهدف من الدخول هو أن يثبت للقائمين على النظام أن هناك ثغرات أمنية فإن ذلك يعتبر من البواعث التي لا تنفي القصد الجرمي، وبناء عليه قُضي بوقوع جريمة من مهندس كمبيوتر أراد أن يثنت لأحد البنوك قدرته على اختراق أنظمة البنك حتى يفوز بعقد تدريب كوادر بنك[3].

أما بالنسبة للقصد الخاص في جريمة الدخول فتتطلب بعض التشريعات توافر قصد خاص في جريمة الدخول غير المصرح به، ففي الدنمارك تشدد العقوبة متى كان الدخول بنية الإحاطة

---

[1] إبراهيم، خالد ممدوح، **الجرائم المعلوماتية**، مرجع سابق، ص234.

[2] المضحكي، حنان ريحان مبارك، **الجرائم المعلوماتية**، مرجع سابق، ص108.

[3] محمد عطا الله، شيماء، **الحماية الجنائية للتعاملات الالكترونية**، مرجع سابق، ص126.

المعلومات التي تتعلق بعمل إحدى الشركات، وفي استراليا تشدد العقوبة إذا كان الهدف من الدخول نية الإضرار بالغير، وفي النرويج تُشدد العقوبة إذا كان هدف الجاني الحصول على ربح غير مشروع، وفي المملكة المتحدة يجرم الدخول غير المصرح به متى توافر للجاني قصد خاص متمثل بنية ارتكاب جريمة أخرى لاحقة على فعل الدخول[1].

وعند الحديث عن القصد الجنائي يجب التفريق بينه وبين الدافع، لأنه يجب توافر القصد الجنائي بجميع عناصر الجريمة، ولا يشترط أن يكون سابقا لارتكاب الجريمة، بل من الممكن ان يكون معاصرا، وقد يكون متولدا عن السلوك الإجرامي، وقد يتطلب المشرع في بعض الجرائم قصد خاص يتمثل في تحقيق نتيجة معينة، أو ضرر خاص فهناك بعض الجرائم المعلوماتية التي يستوجب الركن المعنوي توافر قصد خاص، مثل الدخول غير المشروع لتهديد شخص، أو ابتزازه، فقد اشترط المشروع أن يكون الهدف من الدخول هو التهديد أو الابتزاز[2].

أما المشرع السعودي فعند حديثه عن جريمة الدخول فإنه اشترط لتوفر الركن المعنوي:

1. علم الجاني بأنّ دخوله إلى النظام هو دخول غير مشروع

2. اتجاه إرادة الجاني للدخول لتحقيق الأهداف التالية:

أ.تغيير تصاميم الموقع

ب.إتلاف الموقع

ج.شغل عنوانه.

د.تعديل الموقع[3].

---

[1] ابراهيم، خالد ممدوح، **الجرائم المعلوماتية**، مرجع سابق، ص259-236.

[2] كريري، محمد بن عبد الله، رسالة ماجستير بعنوان **الركن المعنوي في الجرائم المعلوماتية بالنظام السعودي**، الرياض،2013 ص105-108.

[3] كريري، عبد الله بن محمد، **الركن المعنوي للجرائم المعلوماتية**، رسالة ماجستير، الرياض، 2013.

أما المادة رقم 4 من قانون مكافحة الجريمة المعلوماتية السوداني لعام 2007 اشترطت أن يقوم الجاني بدخول موقع أو نظام معلومات، واختراق هذا الموقع، كما أنها اشترط قصدا خاصا متمثلا في دخول الموقع للاطلاع عليه، أو نسخه، أو إلغاء بياناته، أو معلومات موجودة به مملوكة للغير، أو حذها، أو تغييرها، أو إعادة نشرها، أو تغيير تصاميم الموقع، أو إلغائه، أو شغل عنوانه، وهذا الركن يعني أن تكون المعلومات الواردة بالموقع سرية غير متاحة للجميع، وأان يتحقق ضرر، أو أكثر من الأفعال المنصوص عليها بالمادة[1]

من خلال ماتقدم نلاحظ أن معظم النصوص القانونية التي تناولت جريمة الدخول تطلبت وجود قصد خاص لاكتمال الركن المعنوي، وذلك على النحو السابق حيث يلتقي القصد العام مع القصد الخاص في جميع عناصره، ويزيد عنه في تحديد الإرادة الجرمية لدى الجاني.

الفرع الثاني: إتلاف البيانات أو العبث بها

تقع جريمة الإتلاف على المكونات المعنوية لنظام الحاسب الآلي، كالمعلومات، والبيانات، والبرامج على اختلاف أنواعها، ولكن ما مدى صلاحية البرامج والمعلومات المعالجة آليا لأن تكون محلا يرد عليه الاعتداء بجريمة الاتلاف عندما لا يترتب بالمساس بها أي إتلاف لأي من العناصر المادية التي يتكون منها نظام المعالجة الآلية للمعطيات؟

وعليه قد يقع الإتلاف على المكونات المادية لجهاز الحاسب الآلي (الشاشة، ولوحة المفاتيح، والفاره، والأقراص الممغنطة) ويطبق على هذا النوع من الإتلاف النصوص التقليدية الخاصة بجريمة الإتلاف فهذه الصورة لاتثير أي مشكلة ونجدها في التشريعات كافة، مثل قانون العقوبات الأردني سنة 1960 بالمادة(262)، والتشريع المصري بالمادة (361) من قانون عقوبات مصري، والفقره الاولى من المادة (334) من قانون عقوبات فرنسي[2].

[1] طه، ابراهيم قسم السيد، **شرح قانون الجرائم المعلوماتية**، مرجع سابق، ص15.

[2] الرواشدة، سامي حمدان، **مكافحة الجريمة المعلوماتية بالتجريم والعقاب**، مرجع سابق، ص138.

لكن في حديثنا عن الإتلاف في المجال المعلوماتي لا بد من تسليط الضوء على إتلاف المكونات المعنوية للنظام المعلوماتي، ونظرا للطبيعة الخاصة التي تتسم بها المكونات المعنوية في الحاسب الآلي التي تتسم بالطابع الفني المستحدث فقد أطلق عليها بعض الفقهاء "تدمير المعلومات، أي إتلاف تعليمات البرامج ومحوها، أو البيانات ذاتها، ولايهدف التدمير مجرد الحصول على منفعة النظام المعلوماتي أيا كان شكلها، ولكن يهدف إلى إحداث ضرر بالنظام المعلوماتي، وإعاقته عن أداء وظيفته، وغالبا ما يكون هدف الجاني من جريمة الاتلاف المعلوماتي الانتقام، أو محو، أو مجرد العبث، وعليه لا بد من التطرق إلى الركن المادي، والركن المعنوي لجريمة الإتلاف المعلوماتي .

أولاً: الركن المادي لجريمة الإتلاف المعلوماتي

ويتحقق الاعتداء على المعطيات أو البيانات إما عن طريق إدخال معطيات جديدة، أو محو معطيات موجودة أو تعديلها، كما ويؤدي الاعتداء على نظام الحاسب الآلي أيضا إلى إبطاء عمل الحاسوب، بالتالي صعوبة التعامل مع المعطيات، وذلك من خلال جعل ذاكرة الحاسوب ممتلئة، بالتالي عدم القدرة على استخراج هذه المعطيات بشكل مطبوع، أو عدم القدرة على إرسالها عن طريق البريد الالكتروني، فعند إعطاء جهاز الحاسوب أي من الأوامر يعطي إشارة أنّ الأسطوانة مملوءة، وبالتالي تفقد كل المعلومات والمعطيات الموجودة بالحاسوب[1].

ولتحليل الركن المادي لجريمة الإتلاف المعلوماتي سوف نتطرق إلى:

فعل الإتلاف: "تدمير البرامج الإلكترونية سواء أكان كليا أو جزئيا ،أو جعلها على نحو غير قابل للإستعمال"[2] ويكون بعدة صور وعادة ما يغلب على هذا السلوك الطابع الفني والتقني، ومن أهم صور السلوك الجرمي لجريمة الإتلاف:

---

[1] الحلبي، خالد عياد، **اجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة للنشر والتوزيع، ط1، 2011، ص71-73.

[2] قانون الجرائم الالكترونية الفلسطيني رقم 16 لسنة 2017.

1-التخريب: أي بجعل الشيء غير قابل للاستعمال أي أفقده صلاحيته.

2-الإتلاف: يختلف هذا السلوك عن سابقه حيث ينقص من صلاحيته للاستعمال إلا أنه يبقى قابلا للاستعمال.

3-تعطيل الشيء: أي إعاقة الشيء إما بشكل كلي أو جزئي.

محل الضرر: فلو تمعنا بجرائم الإتلاف لنظرنا إليها على أنها جرائم ضرر، وجرائم خطر بالنسبة لكونها جرائم ضرر، فهي التي اشترط المشرّع بها وقوع نتيجة معينة، وفي جريمة الإتلاف قد يكون الضرر الواقع على شكل تعطيل أو إتلاف لكل البيانات، أو المعطيات المعلوماتية، أو أن يكون تعييب للأجزاء المكونة للحاسب الآلي، أما اعتبارها من جرائم الخطر حيث يكون الضرر الناتج على شكل تعديل، وحذف للمعلومات التقنية، فالنتائج المتحققة من الإتلاف معنوية، فالبيانات والمعلومات هي محل لوقوع الإتلاف.[1] وعليه ستعرض أهم الوسائل التي يتم عن طريقها تدمير أو تعطيل أو مسح للبرامج والبيانات المعلوماتية ومنها أولا: الفيروس المعلوماتي، ثانيا: القنبلة المعلوماتية، ثالثا: الدودة المعلوماتية.

أولاً: الفيروس المعلوماتي

وهو "مجموعة من المعلومات التي تتكاثر بشكل سريع لدرجة أنها تصيب النظام المعلوماتي بالشلل، أو قد تكون خلية كهرومغناطيسية نائمة مبرمجة تنشط في وقت محدد لتخريب البرنامج الأصلي، وتنتشر في الأجهزة الأخرى التي تضمنها الشبكة بحيث تفسد ماتحتويه من معلومات ".[2]

[1] الزراع، ماجد بن كريم، **الركن المادي في الجرائم المعلوماتية**، رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، 2014، ص71.

[2] الملط، أحمد خليفة، **الجرائم المعلوماتية**، مرجع سابق، ص647.

وهناك أنواع عديدة من الفيروسات ومنها:

1_ الكرة المرتدة.

2-مايكل أنجلو.

3-المخ.

4-أول إبريل.

5-فايروس حصان طروادة.

6-القنبلة المعلوماتية.

7-الدودة المعلوماتية.

وسوف نعلق على النوعين الأخيرين نظرا لأهميتهما.

ثانياً: القنبلة المعلوماتية.

وهي" فيروسات تهدف إلى تدمير البرامج، ومن ثم إتلافها، وينشط الفيروس، وتبدأ آثاره المدمرة عند حصول واقعة محددة بتاريخ محدد، والقنابل المعلوماتية نوعان قنابل منطقية وقنابل زمنية ".

فالقنبلة المنطقية ترتبط بواقعة معينة، أما القنبلة الزمنية تنشط في تاريخ محدد، ويوجد كثير منها بالولايات المتحدة الأمريكية وإسرائيل[1].

ولعل ماحدث بالولايات المتحدة الأمريكية يعطينا صورة عن أثر القنابل الإلكترونية بعد انفجار قنبلة إلكترونية استهدفت نظام البريد الإلكتروني للجامعة، الذي يرتبط بعمليات تبادل الأبحاث، والتسجيل، ودفع الرسوم وأدى ذلك إلى خسائر تجاوزت عشرات الآلاف من الدولارات،

[1] حجازي، عبد الفتاح بيومي، **الجرائم المستحدثة في نطاق تكنلوجيا الاتصالات الحديثة**، مرجع سابق،508.

فشُكل فريق تحقيق فدرالي، وبعد مواجهة المتهم اعترف وحُبس ثلاث سنوات، وغرامة مالية مقدارها مئة ألف دولار.

ثالثاً: الدودة المعلوماتية

وهي "عبارة عن برنامج له القدرة على تعطيل أو إيقاف نظام الحاسوب الآلي بصورة كاملة، وهو يستنسخ نفسه عدة مرات، وهذا الفايروس يعمل على الجزء المتعلق بنظام التشغيل

أما بالنسبة لبرامج الدودة فهي تستغل الفجوات الموجودة في أانظمة التشغيل، حيث بدأ برنامج الدودة بالإنتشار عندما أنتجه (روبرت موريس) عندما كان في مرحلة الدكتوراه، وأراد أن يثبت ضعف الإجراءات الأمنية القائمة لحماية الشبكات، حيث قام بربط مجموعة من الشبكات الأمريكية المتصلة مع الجامعات، والجهات الحكومية والعسكرية، وبعد أن تم برنامج الدودة اكتشف (موريس) أنه يقوم بالانتشار بسرعة كبيرة، الأمر الذي ترتب عليه تلف الكثير من برامج الكمبيوتر وتوقيفها عن العمل، وتم إلقاء القبض عليه، ومحاكمته، وتمت إدانته، ووضعه تحت المراقبة لمدة ثلاث سنوات وغرامة عشرة آلاف و(50) دولار أمريكي.

مما سبق نجد الإتلاف المعلوماتي يلحق ضررا كبيرا بالفئة المستهدفة، لذلك حاولت بعض الدول سن تشريعات للحد من هذه الظاهرة.

ففي فلسطين وفي ظل صدور قانون الجرائم الإلكترونية نلاحظ ان المادة 6 عالجت موضوع الإتلاف المعلوماتي "كل من أنتج ،أو أدخل عن طريق الشبكة الإلكترونية ،أو إحدى وسائل تكنلوجيا المعلومات ،ما من شأنه إيقافها عن العمل ،أو تعطيلها ،أو تدمير البرامج ،أو حذها ،أو إتلافها،أو تعديلها ...."[1].

[1] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

أما قانون العقوبات الفرنسي نظم هذه المسألة في نص المادة (3/323) "كل من يدخل بطريقة مخادعة لمعطيات داخل نظام المعالجة الآلية... يعاقب بالسجن لمدة ثلاث سنوات وغرامة قيمتها ثلاثمئة ألف فرنك فرنسي[1]".

وعاقب المشرع الإماراتي في المادة (6) على جريمة" إيقاف أو تعطيل أو تدمير.... عن طريق إدخال ما من شأنه القيام بهذه الأفعال من خلال الشبكة المعلوماتية، أو بإحدى وسائل تقنية المعلومات". نلاحظ من خلال نص المادة ان السلوك الاجرامي الذي قصده المشرع يكون من خلال تدمير البيانات وذلك عن طريق برامج معلوماتية بما فيها الفايروس بحيث لا تتحقق النتيجة الا من خلال برنامج معلوماتي وليست وسيلة مادية[2].

من خلال استقراء النصوص السابقة يتبين أن التشريعات المختلفة ومنها المشرع الفلسطيني لجأت إلى استخدام عبارات فضفاضة وصور متعددة للسلوك الإجرامي الواحد حيث أصبحت دائرة التجريم في هذا النوع من الجرائم أكبر و أوسع من نظيرتها التقليدية، وعلى الرغم من أن هذه الصياغة لاتتناسب مع المبادئ العامة التي نادى بها القانون الجزائي المتمثلة بالتفسير الضيق للنص وعدم التوسع في التفسير كما أنه يتعارض مع مبدأ الشرعية لأن ذلك من شأنه أن يخلق قاعدة قانونية جديدة وقد يؤدي إلى الإخلال بالتوازن بين مصلحة الفرد وتعسف القاضي إلا أن خصوصية الجريمة المعلوماتية تتطلب من المشرع أن يترك الباب مواربا أمام السلطة القضائية وذلك لأن هذا النوع من الجرائم كما ذكرنا سابقا يتطور بشكل سريع فالأولى عالمشرع وضع نصوص قانونية مرنة تتسع لهذا النوع من الجرائم .

وعلى الرغم من وجود وسائل مختلفة للإتلاف إلا أنّ تغيير الوسيلة قد يؤدي إلى تغيير التكييف القانوني، ومن التطبيقات القضائية على ذلك تكييف واقعة محو محاسب بيانات معالجة آليا تخضع لنظام الشركة على أنها نصب معلوماتي على الرغم من أن المحو وسيلة من وسائل

---

[1] **ئم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع.2009، 100-107 عبابنة، محمود أحمد، جرا.

[2] حجازي، عبد الفتاح بيومي، **الجرائم المستحدثة في نطاق تكنلوجيا الاتصالات الحديثة**، ط1، 2009، ص505.

الإتلاف، وقد يكيف الاعتداء بالتغيير والتعديل على أن يشكل جريمة تزوير معلوماتي، وهذا ما سنتحدث عنه لاحقا [1]

رابعاً: الركن المعنوي لجريمة الإتلاف المعلوماتي

إنّ جريمة إتلاف البيانات من الجرائم العمدية التي تتطلب توافر العلم والإرادة ويجب ان تتجه ارادة الجاني الى فعل الادخال او المحو او التعديل بالاضافة الى القصد الخاص المتمثل في الغش[2].

وعليه إذا اعتقد الجاني أنّ الأموال المعلوماتية مملوكة له فان القصد الجنائي ينتفي ويجب ان تتجه إرادته أيضا للقيام بهذه النتيجة فمثلا لو قام أحدهم بتحميل القرص المرن دون التأكد من خلوها من الفايروسات ويستخدمه في جهاز حاسب الي فانه يسأل عن الخطأ نتيجة إهماله أو رعونته أو تقصيره.[3]

تعد هذه الجريمة من الجرائم العمدية وفي ذلك تقول محكمة النقض الفرنسية ان نية الغش يمكن استخلاصها من واقعة استعمال القنبلة المنطقية لأنه كان بنية الغش أو بنية إضرار الغير وقد طبق القضاء الفرنسي المبدأ السابق حيث قام متخصصون في علم الكمبيوتر ببيع مجلات ملحق بها (سي دي) محمل بفيروس أدى إلى تدمير بيانات في أنظمة الغير إلا ان محكمة الاستئناف قضت ببراءتهم لأنه لم يثبت علم هؤلاء بوجود فايروس في تلك الأقراص إلا أن قانون العقوبات الفرنسي يعاقب على جريمة إتلاف المعطيات بنية الغش وبذلك لم يشترط فقط قصد عام ينطوي على العلم والإرادة وإنما اشترط وجود قصد جنائي خاص يتبلور بعبارة الغش.

---

[1] الشوابكة، محمد أمين، **جرائم الحاسوب والإنترنت الجريمة المعلوماتية**، دار الثقافة للنشر والتوزيع، ط4، 2011، ص230 -231.

[2] مقلة، آمال، **الجريمة المعلوماتية**، مرجع سابق، ص59-61.

[3] شوابكة، محمد أمين، **جرائم الحاسوب والإنترنت**، دار الثقافة للنشر والتوزيع، ط4، 2011، ص221.

فلا يكفي أن يكون الجاني قد اتجهت أرادته إلى القيام بمحو أو تعديل أو إدخال أو أي تلاعب بالمعطيات بل يجب ان يقترن فعله بنية الغش وتكوت نية الغش مقترنة بالعلم والإرادة وإحداث ضرر للغير[1].

وفي ذلك صدرت عدة احكام من محكمة النقض المصرية بشأن القصد الجنائي لجريمة الإتلاف "إن جريمة الإتلاف جريمة عمدية يتحقق القصد الجنائي فيها متى تعمد الجاني إرتكاب الفعل المنهى عنه بالصورة التي حددها القانون واتجاه إرادته إلى إحداث الإتلاف أو التخريب وعلمه أنه يحدثه بغير حق وهو مايقتضى أن يتحدث الحكم عنه إستقلالا أو أن يكون فيما أورده من وقائع وظروف مايكفي للدلالة على قيامه[2]".

الفرع الثالث: التزوير المعلوماتي

تعتبر هذه الصورة الثالثة من صور الجريمة المعلوماتية، وتتمثل بالمساس بمنتجات الحاسب الآلي، ويتجسد هذا المساس بفعل التزوير المعلوماتي، وعليه يعرف التزوير المعلوماتي "أي تغيير بالحقيقة في محرر بكل الطرق التي يقرها القانون المادية والمعنوية تغيرا من شأنه إحداث ضرر للغير بواسطة استخدام الحاسب الآلي " وعليه سنتناول الركن المادي والركن المعنوي لجريمة التزوير المعلوماتي.

أولا: الركن المادي لجريمة التزوير المعلوماتي

فعل تغيير الحقيقة: يتمثل في كل تغيير للحقيقة يرد على مستند أصلي معالج آليا، "فلا تتحقق تلك الجريمة من خلال فعل تغيير الحقيقة باستخدام طريقة تزوير مادية أثناء نشأة المستند على خلاف جريمة التزوير العادية " كما لا تكتمل تلك الجريمة من مجرد تصوير أو نسخ لمستند أصلي، ونلاحظ أنه إذا انتفى عنصر التغيير فلا مجال لجريمة تزوير، ولا يشترط أن يكون التغيير كليا، وإنما يكتفي المشرع بتغيير الحقيقة النسبية.

---

[1] عبابنة، محمود احمد، **جرائم الحاسوب وأبعادها الدولية**، مرجع سابق، ص106.

[2] المضحكي، حنان ريحان مبارك، **الجرائم المعلوماتية**، مرجع سابق، ص133.

فالتزوير المعلوماتي ممكن أن يتم من خلال سلوك إيجابي يتمثل في إدخال البيانات، أو استغلال بعض العيوب والأخطاء، وقد يكون بنشاط سلبي، وذلك إذا ترتب على الترك تغيير جوهري يسبب ضررا للغير لاسيما إذا كان متعمدا، وكان بأحد البيانات الجوهرية، فتغيير الحقيقة كعنصر مادي في جرائم التزوير المعلوماتي تقع على البيانات والمعلومات بأي طريقة سواء بالصور أو الرموز أو العلامات، ولكن يشترط أن يتم التزوير المعلوماتي بواسطة جهاز الحاسب الآلي حتى يتم تمييزها عن جريمة التزوير التقليدية[1].

وحتى يقع الضرر لا يكفي تغيير الحقيقة بالمحرر لابد أن يكون هناك ضرر سواء كان هذا الضرر واقع بالحال أو محتمل الوقوع، ويعتبر الضرر قائما في حال وقع على أي فرد من أفراد المجتمع غير محدد بالذات، أو سواء كان شخصا طبيعيا أو معنويا، و يجب أن يكون لهذا المستند حجة على الغير بحيث يقاس ضابط الضرر بما للمستند من حجة قانونية على الغير، ويعتبر الضرر ركنا أساسيا في جريمة التزوير المعلوماتي، حيث لا يكفي تغيير الحقيقة في المحرر، بل لا بد من أن يترتب على هذا التغيير ضرر سواء كان أدبيا أم ماديا أم اجتماعيا، سواء ينصب على المصلحة العامة أو الخاصة .[2] وهذا ماورد في نص المادة 11 الفقرة 2 من قانون الجرائم الإلكترونية الفلسطيني "اذا وقع التزوير وكان من شأنه احداث ضرر يعاقب....."حيث اشترط المشرع ضرورة وجود ضرر حتى تتوافر جريمة التزوير المعلوماتي فيما عدا تزوير المستندات الإلكترونية الرسمية فاعتبر المشرع الفلسطيني في هذه الحالة أن الضرر حاصلا وهذا مانراه جليا في الفقرة الأولى من نفس المادة "كل من زور مستندا إلكترونيا من مستندات الدولة، أو الهيئات والمؤسسات العامة، يعاقب...." نلاحظ من خلال استقراء النص ان المشرع لم يشترط وقوع ضرر عندما يتعلق التزوير بالمستندات الإلكترونية الرسمية فاعتبر الضرر قائما إلا أنه بالفقرة الثانية إذا كان المحرر الواقع عليه التزوير محرر غير رسمي اشترط وقوع ضرر حتى نكون بصدد جريمة معلوماتية[3].

---

[1] قارة، مال، **الجريمة المعلوماتية**، مرجع سابق، ص 55.

[2] الزراع، ماجد بن كريم، **الركن المادي بالجرائم المعلوماتية**، مرجع سابق، ص79.

[3] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

وبالرجوع للمفهوم التقليدي لجريمة التزوير نلاحظ أن معظم التشريعات اشترطت أن يتم فعل التزوير بطرق محددة بموجب هذه التشريعات فقانون العقوبات الأردني سنة 1960 أورد طرق التزوير على سبيل الحصر فنصت المادة 262 "يعاقب بالأشغال الشاقة المؤبدة ....الذي يرتكب تزويرا ماديا في أثناء قيامه بالوظيفة إما بإساءة استعمال إمضاء أو ختم أو بصمة أصبع أو إجمالا بتوقيعه إمضاء مزور وإما بصنع صك أو مخطوط وإما بما يرتكبه من حذف أو إضافة تغيير في مضمون صك أو مخطوط[1]" يتبين من خلال ماسبق أن فعل التزوير في النص التقليدي أكثر تحديدا ودقة ومحصورا بطرق معينة من فعل التزوير بالجريمة المعلوماتية حيث نصت المادة 11 الفقرة 1من قانون الجرائم الإلكترونية الفلسطيني "كل من زور مستندا إلكترونيا رسميا من مستندات الدولة، أو الهيئات والمؤسسات العامة ،معترفا به قانوناً في نظام معلوماتي، يعاقب ..."[2] فجاء لفظ زور بصورة مطلقة من دون تقييد أو حصر بحالات معينة .

ولكن هل تستطيع النصوص التقليدية احتواء التزوير المعلوماتي في المحررات الإلكترونية؟

فالفقه الفرنسي انقسم إلى اتجاهين الأول: يرفض فكرة تطبيق النصوص التقليدية على التزوير المعلوماتي، وذلك لأنّ النص التقليدي يستلزم وجود كتابة، كما أنّ المحررات الإلكترونية الموجودة داخل الحاسب الآلي لا تعتبر من قبيل المحررات المنسوخة، كما أنّ معظم التشريعات في النصوص التقليدية للتزوير اشترطت أن يقع التزوير على صك أو مخطوط.

أما الاتجاه الثاني فيرى إخضاع جريمة التزوير المعلوماتي لقوالب النصوص التقليدية، لأنّ القضاء الفرنسي لم يفرق بين محرر مكتوب ومحرر مختزل.

وهناك ضرورة لوجود نصوص تشريعية مستحدثة لمعالجة التزوير المعلوماتي نظرا لأنّ الجرائم المعلوماتية هي جرائم ذات طبيعة خاصة تختلف من حيث محلها، ونطاقها عن تلك التقليدية، فلا بد من وجود نصوص خاصة لمعالجتها، وأن تتسم هذه النصوص بالمرونة، وذلك

[1] قانون العقوبات الأردني رقم 16 لسنة 1960.

[2] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

لأن هذا النوع من الجرائم قد يتسع مفهومه بين الفينة والأخرى نظرا للتطور التكنولوجي الهائل الذي تشهده هذه الفترة[1].

وهذا مانراه جليا في قانون الجرائم الإلكترونية الفلسطيني حيث تطرق المشرع في المادة 11 إلى حالات وصور التزوير المعلوماتي.

وبالحديث عن الركن المادي لابد من التطرق إلى طرق التزوير، وذلك لأن كثير من التشريعات اشترطت أن تكون هناك طرق مادية معينة حتى يتحقق الركن المادي لجريمة التزوي.

وفعل التزوير يجب أن يقع على مستند أصلي معالج آلياً، وبالطرق المادية وليس المعنوية ويستوي أن تكون هذه المعطيات داخل نظام المعالجة الآلية أو خارجه، إلا انّ بعض الفقهاء يرى أنه لاضير في استخدام الوسائل المعنوية لتحقيق التزوير.[2]

إن التزوير المادي في المحررات الإلكترونية يكون بتغيير البيانات (الحذف، والاضافة)، كما هو الحال بالجرائم التقليدية، وعليه قضت محكمة استئناف باريس بوقوع جريمة التزوير، عندما قام بتغيير التاريخ المثبت على أحد البرامج، والمخزن على ديسكات بغرض أن يثبت أنّه معد هذه البرامج لحسابه الخاص وليس لحساب صاحب العمل.[3]

ومن الجدير ذكره أّن طرق التزوير التقليدي جاءت بأغلب التشريعات مذكورة على سبيل الحصر، وهو ما أشارت إليه المادتين (211)، و(213) من قانون عقوبات مصري بحيث تنقسم طرق التزوير في الجرائم التقليدية إلى تزوير مادي، وتزوير معنوي.

وبالنظر إلى القانون الفرنسي استحدث بنص المادة (441-1) أمرا هاما جديدا، وهو أن طرق التزوير المعلوماتي لم تعد محددة قانونا على سبيل الحصر، وإنما أطلقها المشرع حيث جاء

---

[1] عبابنة، محمود احمد، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع، ط1،2009، ص106-108.

[2] قارة، مال، **الجريمة المعلوماتية**، مرجع سابق، ص54-57 .

[3] عطا الله، شيماء، **الحماية الجنائية للتعاملات الالكترونية**، مرجع سابق، ص90.

النص يما يلي "يعد تزويرا كل تغيير بطريق الغش في الحقيقة، من شأنه أن يحدث ضررا، وأيا كانت الطريقة التي أجري بها..... "[1].

نلاحظ أن المشرع الفرنسي وسع من نطاق طرق التزوير بحيث شملت كل تغيير للحقيقة، ولا شك أن هذا الاتجاه يتلائم مع طبيعة الجرائم المعلوماتية التي تحتاج إلى نصوص مرنة، وأكثر اتساعا من القوالب التقليدية، نظرا للتطور التكنولوجي والتقني السريع والذي لابد أن تحتويه التشريعات كافة، للحد من ظاهرة الجريمة المعلوماتية.

وبما أن التزوير المعلوماتي أمر مستحدث عملت كثير من الدول جاهدة بلورة قوانين، وسن تشريعات قادرة على ضبط هذه الجريمة، والحد من انتشارها فيما اكتفت دول أخرى بما لديها من نصوص تقليدية وأبقتها سارية المفعول.

أما في المملكة المتحدة فقد صدر قانون التزييف والتزوير الخاص بالمحررات عام (1981)، وفي الولايات المتحدة الأمريكية تناول القانون الفدرالي في مادته (1029) المتعلقة بالاحتيال، وتجريم أفعال التزوير المرتبطة بالحاسب الآلي، وعاقب عليها لمدة لا تزيد عن عشر سنوات، أما ألمانيا فاستحدث المشرّع المادة 269، والتي تنص على أفعال يعاقب كل من باشرها بغرض التحايل على الروابط القانونية (أي أنه استعرض طرق التزوير المعلوماتي) وهي:

1.التخزين الإلكتروني أو المغناطيسي غير المشروع، أو بأي وسيلة أخرى غير مرئية أو غير مقروءة مباشرة لبيانات متخصصة لكي تستعمل كوسائل إثبات.

2.أو تعديل غير المشروع لهذه البيانات المختزنة سواء بوسيلة قانونية أو غير قانونية

أو استعمل هذه البيانات المختزنة أو عدلها يعاقب....."

[1] الملط، أحمد خليفة، **الجرائم المعلوماتية**، مرجع سابق، ص574.

كما خصص المرسوم السلطاني رقم (12) لسنة (2011) بإصدار قانون مكافحة جرائم تقنية المعلومات في سلطنة عمان الفصل الرابع "التزوير والاحتيال المعلوماتي" وجاء به مادتان (12،13).

كذلك المشرّع القطري في القانون رقم (14) لسنة (2014) فخصص الفصل الثالث والذي يضم مادتين فقط للتزوير والاحتيال الإكتروني، حيث أفرد المادة (10) للتزوير. أما المشرّع القطري ففرق بين جريمتي تزوير كل من المحرر الإلكتروني الرسمي، ونظيره غير الرسمي ليس فقط من حيث العقوبة، ولكن من حيث النموذج الإجرامي. ولم يشترط المشرّع القطري أن يكون التزوير قد تم بطريقة إلكترونية، أو باستخدام وسيلة تقنية معلومات، ومن ثم يمكن أن يقع التزوير بإحدى الوسائل التي نص عليها قانون العقوبات القطري[1].

ثانيا: الركن المعنوي لجريمة التزوير المعلوماتي

يجب أن تتجه إرادة الجاني إلى تغيير الحقيقة أي توفر القصد الجنائي العام بعنصريه العلم والإرادة، أما بالنسبة للقصد الخاص في هذه الجريمة يتمثل في نية استخدام هذا المستند ويتوافر هذا القصد حتى يتوافر هذا القصد. فبالتالي جريمة التزوير من الجرائم التي تستلزم وجود قصد جنائي عام (العلم، والإرادة) وقصد خاص المتمثل باقتران العلم بنية الغش.

القصد العام: يتوافر القصد العام في جريمة التزوير عندما يعلم الجاني أنه يغير الحقيقة بالمحرر، وأنه من شان هذ التغيير وجود ضرر فعلي أو احتمالي، أما إذا لم يكن يعلم فإن مجرد إهماله لايحقق وجود القصد الجنائي وفي إطار المعلوماتية يجب أن يكون الجاني عالما بأنه يقوم بتزوير مستندات معلوماتية بأي طريقة، وأن تتجه إرادته إلى إحداث فعل التغيير.

القصد الخاص: فجريمة التزوير المعلوماتية شأنها شأن جريمة التزوير التقليدية التي تشترط إحداث ضرر للغير احتماليا أاو فعليا.

[1] خليل امام حسنين، **السياسة الجنائية لمكافحة الجرائم المعلوماتية**، مرجع سابق، ص59_62.

وملخص القول إن الركن المعنوي في جريمة التزوير المعلوماتية يتوافر متى اتجهت إرادة الجاني لتزوير مستندات معلوماتية بأي طريقة بنية استعمال هذه المحررات الإلكترونية المزورة لإحداث ضرر مفعل أو محتمل[1].

وعليه إذا كان جاهلاً بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق لديه القصد الجرمي، وكذلك الحال إذا انتفى علم الجاني بأي ركن من أركان الجريمة فلا يترتب عليه توافر القصد الجنائي، لأنه يفترض بالفاعل أن يكون عالماً أركان جريمته كافة، كما قد لا يتحقق القصد الجنائي إذا كان الفعل الذي يقوم به الجاني غير واضح بصورة صريحة، كما هو الحال بالنسبة لانتحال صفة الغير، أو الاتصاف بصفة غير صحيحة فقد يقوم مبرمج بيانات بتغيير الحقيقة في المحررات ولكنه غير عالم بماهية التغيير، كما ينتفي القصد الجنائي إذا أهمل المبرمج القائم بتحرير المحرر تغيير بيانات معينة دون قصد فإنّ الإهمال وعدم الاحتياط لا يحقق العلم في القصد الجرمي هذا من ناحية، ومن ناحية أخرى يستوجب قيام القصد الجنائي في التزوير المعلوماتي أن تكون إرادة الجاني متجهة إلى إحداث النتيجة الجرمية التي وقعت أو أية نتيجة جرمية أخرى، وهي الإضرار بالأخرين حتى وإن كان هذا الإضرار محتمل الوقوع، وعليه فإن الركن المعنوي يتحقق في جريمة التزوير المعلوماتي بعلم القائم بفعل التزوير بأن الإدخال أو الإتلاف أو المحو أو التحوير للبيانات والبرامجيات المعالجة آلياً يؤدي إلى التأثير على المجرى الطبيعي لتلك البيانات او المعلومات وأنه قد وقع فعله .[2]

ولكن مايميز التزوير المعلوماتي عن التقليدي أنّ معظم التشريعات التي تناورت التزوير الإلكتروني لم تذكر طرقا معينة لهذا التزوير، كما هو الحال في جرائم التزوير التقليدية التي حصرت طرق التزوير سواء المادية أو المعنوية وجعلتها شرطا لاكتمال جريمة التزوير.

---

[1] الحمامى، عمر ابو الفتوح، **الحماية الجنائية للمعلومات المسجلة الكترونيا**، دار النهضة العربية، 2010، ص940-941.

[2] تزوير معلوماتي، منتدى د.شيماء عطا الله، الساعة 2:39 التاريخ 5 / 9/ 2016 http://www.shaimaaatalla.com/vb/showthread.php?t=3940

وأول حكم صادر من محكمة باريس الابتدائية في 12 أوكتوبر 1988 بالنسبة للتزوير المعلوماتي "حيث ارتكب كل من (هيفارت ودومنيجويز) واقعتي تزوير محررات ونسب لكل من (بلوت وكريستان) واقعة إخفاء محرر مزور، واستعماله وهكذا نسبت المحكمة إلى المتهمين الأربعة جريمة تزوير وثائق مبرمجة واستعمالها، فكل من (هيفارت ودومنيجويز) ارتكبا أفعال تزوير في محرر تجاري عن طريق اصطناع عقود أو تصرفات أو التزامات أو مخالصات، ثم أدرجت بعد ذلك في محرر عن طريق تزوير إقرارات أو وقائع، وهكذا استغلت المعلوماتية التابعة لشركة (Tuffier ravier py) في ارتكاب عمليات تحويل نقود معلوماتية مصطنعة من حساب العملاء المؤسسين إلى حسابات كل من (بوت وكريستان) الصورية كما حدث أيضا استعمال لأفعال التزوير هذه أي إقامة تحويلات معلوماتية مزورة[1] ".

فنجد أن المشرع الفرنسي أسند تهمة تزوير وثائق مبرمجة استنادا إلى المادة (145) من قانون عقوبات فرنسي فعلى الرغم من أنّ النصوص التقليدية لا يمكن أن تتسع لتشمل التزوير المعلوماتي بسبب استلزامها لفكرة المحرر إلا أنّ القضاء الفرنسي جاء بنهج موسع في تفسير المحرر بصورته التقليدية، لكنها رأت ضرورة العقاب على تغيير الحقيقة الذي يمس الغير، والذي ينصب على البيانات المعلوماتية، فلا يوجد محرر مكتوب بالمعنى الوارد في المادة(145) لكنّ القاضي استنبط فعل التزوير من خلال وقائع القضية وتوسع في تفسير المحرر ليشمل البيانات المبرمه.

المبحث الثاني: خصوصية الجريمة المعلوماتية على المستوى العقابي

إن نطاق العقوبة في الجرائم المعلوماتية يعتمد على مدى جسامة الضرر، ومدى خطورة الجرائم المعلوماتية، فالعقوبة لا تطبق عبثا، بل يجب أن تكون ذات جدوى، وحتى يتحقق هذا الشرط يجب تنظيمها بطريقة مرنة حتى يتسنى ردع الجاني، وبذلك ينظر للعقوبة على أنها مؤهلة للمجرم للعودة للمجتمع كشخص صالح، وعليه سوف يقوم الباحث بذكر بعض العقوبات التي

[1]الشوا، محمد سامي السيد، **جرائم الحاسب الآلي امام القضاء الجنائي الفرنسي**، مجلة البحوث القانونية والاقتصادية، دار المنظومة، مجلد 2، عدد 3، 1992.

طرحتها أنظمة مختلفة من أجل الحد من الجريمة المعلوماتية مع تحليل هذه العقوبات ومدى ملاءمتها لمثل هذا النوع من الجرائم، وذلك في المطلب الأول (عقوبات أصليه)، والمطلب الثاني (عقوبات تكميلية) .

المطلب الأول: خصوصية على مستوى حساب العقوبة

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا أن المشّرع وضع تدرجا فيما يتعلق بالعقوبات الأصلية، وهذا التدرج في العقوبات يعكس الخطورة الإجرامية لهذا النوع من الجرائم[1]ولعل مايميز النظام العقابي بالجريمة المعلوماتية عن نظيرتها الجريمة التقليدية هو منح القاضي في الجرائم المعلوماتية سلطة واسعة في تقدير العقوبة حيث يترك للقاضي في بعض الأحيان حرية الحكم [2] وفيما يلي بيان لبعض النصوص:

"كل من قام عمدا بإنشاء أو نشر شهادة غير صحيحة، أو قدم بيانات غير صحيحة عن هويته إلى الجهات المختصة بموجب القوانين الخاصة ....يعاقب بالحبس وبالغرامة التي لاتقل عن مائتي دينار أردني ولاتزيد عن ألف دينار أردني، أو مايعادلها بالعملة المتداولة قانونا[3]".

نلاحظ أن قانون الجرائم الإلكترونية الفلسطيني في المادة العاشرة منح القاضي صلاحية واسعة تتعدى وجود الحدين الأعلى والأدنى فجاء بالنص عبارة يعاقب بالحبس من دون وضع حدين بلتزم بهما القاضيي فالنهج العقابي بالجريمة المعلوماتية يعمل على تطوير مبدأ التفريد العقابي والذي يمنح القاضي صلاحية اسعة في تحديد العقوبة نظرا لظروف المجرم وملابسات الجريمة من الناحية الواقعية.

كما نلاحظ أن خصوصية النهج العقابي في الجريمة المعلوماتية في شدة النظام العقابي فمثلا نصت المادة 29 الفقرة الثانية من قانون الجرائم الإلكترونية الفلسطيني على "إذا كان المجني عليه

---

[1] سفيان، سوير، **الجرائم المعلوماتية**، رسالة ماجستر،جامعة الجزائر،2010_2011، ص98.

[2] الفايز عبد العزيز بن عبد الكريم، **العقوبات التكميلية للجرائم المعلوماتية في النظام السعودي**، الرياض، 2014، ص4.

[3] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

طفلا يعاقب المجرم بالأشغال الشاقة المؤقتة مدة لاتقل عن 5 سنوات وبغرامة لاتقل عن ألفي دينار أردني ولا تزيد عن خمسة الآلف دينار أردني ،أو مايعادلها بالعملة المتداولة قانونا، ولو لم تقع الجريمة " من خلال استقراء النص يتبين أن المشرع الفلسطيني جعل من العقوبة وسيلة ردع وقائية حيث أنه حتى لو لم تتم أركان أي جريمة من الجرائم المنصوص عليها في قانون الجرائم الإلكترونية يعاقب الجاني بالأشغال الشاقة المؤبدة طالما أن المجني عليه طفلا.

أما بخصوص أن القانون منح القاضي حرية الحكم فهذا نراه جليا في نص المادة 30 من قانون الجرائم الإلكترونية الفلسطيني "إذا ارتكب باسم الشخص المعنوي أو لحسابه إحدى الجرائم المنصوص عليها في هذا القرار بقانون ،يعاقب بالغرامة التي لاتقل عن خمسة الآف دينار أردني ... وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة اقصاها خمس سنوات أو أن تقضي بحله وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له ".

من خلال استقراء النصوص السابقة يتبين أن طبيعة الجرائم المعلوماتية تحتم على المشرع صياغة نصوص تتميز بالمرونة سواء بشق التجريم وبشق العقوبة لأن هذا النوع من الجرائم يهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية والتي تتطور بشكل كبير يصعب معه وضع نصوص جامدة لاتحتمل التفسير كما أن كل حالة إجرامية يجب التعامل معها بشكل منفرد وبالتالي لابد من وجود نص مرن يعطي السلطة القضائية مساحة واسعة في تقدير العقوبة بما يتلائم مع كل جريمة على حدى.

المطلب الثاني: خصوصية على مستوى نوعية العقوبة

إن الإنتشار الكبير لجرائم تقنية المعلومات، والتي بدأت آثارها السلبية تظهر في المجتمع جعل هناك حاجة ملحة لدى المشرع لفرض جزاءات تتناسب مع طبيعة هذه الجرائم، بحيث تعزز عمليات الوقاية من الهجمات الإلكترونية، فالعقوبة يجب تنظيمها بطريقة مرنة تتناسب مع هدف المشرع اتجاه الجاني [1]وهذا مانراه جليا في قانون الجرائم الإلكترونية الفلسطيني فنص المادة السابعة

[1] الفايز، بن عبد العزيز بن عبد الكريم، **العقوبات التكميلية للجرائم المعلوماتية في النظام السعودي**، مرجع سابق، ص2.

"كل من التقط ماهو مرسل عن طريق الشبكة، أو إحدى وسائل تكنلوجيا المعلومات، أو سجله أو إعترضه، أو تنصت عمدا دون وجه حق ،يعاقب بالحبس أو الغرامة التي لاتقل عن ألف دينار أردني...." يتبين من النص السابق أن المشرع الفلسطيني جمع بين العقوبة الأصلية المتمثلة بالسجن وبين العقوبة التكميلية المتمثلة بالغرامة حيث خول المحكمة سلطة الحكم بعقوبة السجن أو الغرامة أو العقوبتين معا.

كما ونصت المادة 50 من قانون الجرائم الإلكترونية الفلسطيني "كل من امتنع عن قصد في الإبلاغ، أو أبلغ عن قصد بشكل خاطئ عن جرائم معلوماتية ،يعاقب بالحبس مدة لاتقل عن ستة شهور ،وبغرامة لاتقل عن مائتي دينار ولاتزيد عن ألف دينار أردني أو بإحدى هاتين العقوبتين".

من خلال استقراء نصوص قانون الجرائم الإلكترونية الفلسطيني نلاحظ أنه لايكاد أي نص يخلو من عقوبة الغرامة بالإضافة إلى عقوبة السجن حيث ركز المشرع على الجزاءات المادية التي قد تصل إلى خمسة الآلف دينار أو مايعادلها بالعملة المتداولة قانونا حيث جاءت هذه الجزاءات تتناسب مع طبيعة الجريمة المعلوماتية التي غالبا مايكون الهدف منها مادي فخاطب المشرع الجاني بلغته .

أما بالنسبة لعقوبة المصادرة هي عبارة "عن إجراءات وقائية تقرر لحماية المجتمع من وقوع الجرائم وإيقاع الشر بأفراده وهي تتخذ للوقاية والاحتراز[1]".

والملاحظ أن معظم التشريعات في الجريمة التقليدية توجهت إلى عدم العقاب على المصادرة العامة حتى أن بعض الدساتير نصت على عدم شرعيتها باعتبار أن أثرها يمتد في بعض الأحيان ليشمل أسرة الجاني ومن يعولهم واكتفت بالمصادرة الخاصة أي مصادرة الأشياء أو الأموال الناتجة عن الجريمة وبسببها.

أما بالنسبة للقانون الفلسطين فقد نص بالمادة 45 "دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون ،وحقوق الغير حسن النية، تصدر المحكمة قرارا بمصادرة الأجهزة، أو البرامج، أو

[1] الحلبي، محمد علي السالم، **شرح قانون العقوبات**، دار الثقافة للنشر والتوزيع، ص499.

الوسائل المستخدمة في إرتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون، أو الاموال المتحصلة منها، على أنن تكون إزالة المخالفة على نفقة الفاعل .

أما بالنسبة لعقوبة المصادرة في قانون مكافحة الجرائم التقنية المعلوماتي الإماراتي قد تكون وجوبية، وهذا مانصت عليه المادة (41) حيث جعلت المصادرة، ومحو البيانات، وإعدامها هو عقوبة تكميلية وجوبية على المحكمة الحكم بها، وذلك نظرا لاستخدام الجاني في الجرائم المعلوماتية أجهزة وبرامج تنطوي على جانب من الخطورة، فكان لابد من جعل مصادرة هذه الأجهزة والبرامج وجوبية وذلك لتجنب استعمالها مرة اخرى[1].

كما أن المشرّع الفرنسي نص أيضا على عقوبات تكميلية تتمثل في مصارة الأجهزة المستخدمة بالجريمة، وذلك من أجل فعالية مواجهة هذا النوع من الجرائم المنصوصة في هذا القانون مع الأخذ بعين الاعتبار حقوق غير حسن النية.

كما أنّ المشرّع السعودي نص على عقوبة المصادرة بالمادة (13) بنفس الصياغة الواردة في القانون الإماراتي وذلك بإضافة جواز الحكم بإغلاق الموقع الإلكتروني واشترط لإغلاق مكان الجريمة علم صاحب المكان إلا أن المصادرة في التشريع السعودي جوازية على عكس التشريع الإماراتي والعماني فهي وجوبية[2]. أما بالنسبة للتدابير الاحترازية التي أوردها المشرع الإماراتي:

أ. المصادرة حيث يحكم بجميع الأحوال بمصارة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها.

ب. إغلاق المحل: يحكم بإغلاق المحل أو الموقع التي ارتكبت فيه إحدى الجرائم المنصوص عليها في هذا القانون إذا كانت الجريمة ارتكبت بعلم مالك المحل، ويكون ذلك الإغلاق كليا أو بفترة تحددها المحكمة.

---

[1] خليل، إمام حسنين، **السياسة الجنائية لمكافحة الجرائم المعلوماتية**، مرجع سابق، ص12.

[2] خليل، إمام حسنين، **السياسة الجنائية لمكافحة الجرائم المعلوماتية في التشريعات العربية**، مرجع سابق، ص12.

ج. الابعاد: تقضي المحكمة بإبعاد الأجنبي الذي يحكم بالحبس[1].

وفيما يلي عرض لبعض النصوص القانونية التي توضح صور لعقوبات تكميلية نصت عليها تشريعات مختلفة:

حيث نصت المادة (34) من قانون مكافحة الجرائم المعلوماتية الإماراتي "جواز وضع المحكوم عليه تحت المراقبة أو حرمانه من استخدام وسائل تقنية المعلومات أو إلزامه بأداء عمل لمدة معينة أو وضعه في مأوى علاجي"

كما ونصت المادة (35) من نفس القانون مع عدم الإخلال بالعقوبات المنصوص عليها في هذا النظام" القانون"، يجوز للمحكمة أن تقضي بإبعاد الأجنبي الذي يحكم عليه وفقا لأحكام هذا القانون[2].

كما قرر مجلس الشورى السعودي على إضافة عقوبة التشهير في المادة السادسة من قانون مكافحة الجرائم المعلوماتية السعودي، حيث وافق المجلس على إضافة النص كالآتي: "يجوز إضافة إلى العقوبتين المنصوص عليهما في هذه المادة الحكم بنشر الحكم نهائي على نفقة في صحيفة أو أكثر من الصحف المحلية وذلك حسب نوع الجريمة المرتكبة وحجمها وتأثيرها على المجتمع[3]" وقد نصت المادة 26 من قانون مكافحة الجرائم المعلوماتية السوداني في العام (2007) على إبعاد المدان إذا كان أجنبيا في حال ارتكابه جرائم معينة بحد ذاتها[4].

من خلال استقراء النصوص السابقة نلاحظ أنّ الجريمة المعلوماتية تتميز بخصوصية ليس فقط على مستوى الجريمة، بل أيضا على مستوى العقاب، وذلك حتى تكون العقوبة رادعة ومناسبة للجريمة، فمثلا قد تصل العقوبة في بعض التشريعات إلى حجم الإنترنت عن الشخص المدان،

---

[1] البقمى، ناصر بن محمد،**مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية**،مرجع سابق ص71-73.

[2] **قانون مكافحة الجرائم المعلوماتية الاماراتي لسنة 2012.**

[3] الشرق الأوسط، جريدة العرب الدولية ، 2017/4/22، س12:41، صhttp://aawsat.com/home/article.

[4] طه، إبراهيم قسم السيد محمد، **الجريمة المعلوماتية في القانون السوداني**، مرجع سابق، ص88.

وأحيانا أخرى قد تصل إلى إبعاد الشخص إذا كان أجنبيا بالإضافة إلى العقوبات التقليدية المتمثلة بالحبس والغرامة والتدابير الاحترازية.

وبعد تناول الجرائم المعلوماتية من حيث أركانها، وصورها، وعقوباتها وموقف التشريعات منها، لابد من الانتقال إلى الإجراءات الواجب اتباعها بحق من يرتكب مثل هذه الجرائم على مستوى التتبع والملاحقة، ودور كل من النيابة العامة والمحكمة في مرحلتي التحقيق الابتدائي والنهائي وهذا ما سنعرضه في الفصل الثاني.

الفصل الثاني

خصوصية الجرائم المعلوماتية على المستوى الإجرائي

تحدثنا سابقا عن المشكلات الموضوعية التي أثارتها التطورات التقنية الجديدة في ارتكاب الجرائم المعلوماتية، وهذا ما جعل القانون الجنائي أمام قصور في مواجهته لهذه الجرائم، وكان لهذا تأثير على قانون الإجراءات الجنائية في قدرته على مواجهة هذا النوع من الجرائم، وخصوصا في ظل عدم وجود نصوص للتجريم والعقاب، هذا من جهة وعلى الصعيد الإجرائي فإنّ النصوص الإجرائية التقليدية تعرقل عمل أجهزة العدالة، وسير الدعوى في المراحل كافة، بما فيها مرحلة التحقيق الابتدائي، ففي هذه المرحلة التي هي محور دراسة الباحث يواجه أفراد القانون الكثير من الصعوبات، ولاسيما في الكشف عن الجريمة، وذلك نظرا لصعوبة الإثبات لكون الدليل سهل المحو والتدمير، كما أنّ مسرح الجريمة في هذا النوع من الجرائم مختلف عنه بالجريمة التقليدية، ولكون هذه الجرائم تمتاز بطبيعة خاصة تستلزم أن يكون مأمور الضبط القضائي مكونا علميا وتكنولوجيا حتى يتسنى له فهم هذه النوع من الجرائم، والكشف عنها فهذا النوع من الجرائم جعل موضوع الإجراءات الجنائية في مأزق حقيقي، وفي هذا الصدد قسم الباحث هذا الفصل إلى مبحثين تناول في المبحث الأول (مرحلة التحقيق الابتدائي)، والمبحث الثاني (الأوراق المتحصلة من مرحلة التحقيق الإبتدائي).

المبحث الأول: خصوصية الجرائم المعلوماتية في مرحلة التحقيق الإبتدائي

إنّ إجراءات التحقيق التي تمر بها الجرائم المعلوماتية تأخذ شكل عناصر التحقيق الجنائي المتكامل، وتمر بذات المراحل الفنية والشكلية، وتعد إجراءات التحقيق الجنائي العام هي الأساس في التحقيق في جرائم الحاسب الآلي إلا أنها تتميز ببعض من الخصوصية في عناصر التحقيق

الفرعية والإجراءات الشكلية المتبعة في تلقي البلاغات، والعناية بمسرح الجريمة وتكوين فرق العمل وأساليب تأمين الأدلة المادية[1].

وغالبا لم يُحدد مفهوم التحقيق الإبتدائي في النصوص التشريعية، وإنما تم الاقتصار على الإشارة إلى إجراءاته إلا أنه يمكن تعريف هذه المرحلة بأنها "مجموعة الإجراءات التي تباشرها السلطة المختصة بتحقيق الدعوى عن جريمة ارتكبت لكشف الحقيقة، وذلك بالبحث والتنقيب عن الأدلة وتجميعها وتقديرها لإثبات حدوث الجريمة ونسبتها إلى المتهم، لتحديد مدى كفايتها لإحالة المتهم للمحاكمة أو لنفي ذلك كأساس للأمر لإقامة الدعوى[2]".

وتكمن أهمية التحقيق الإبتدائي في الجرائم المعلوماتية بأنه يتضمن الإجراءات التي من شأنها أن تمهد للمرحلة التالية، وهي مرحلة المحاكمة فيتمثل بإثبات أقوال المبلغ أو المجني عليه، وشهادة الشهود، والانتقال إلى المعاينة، والتفتيش، واستجواب المتهم، وما يتخذ قبله من إجراءات الإحضار والقبض، والحبس الاحتياطي، بالإضافة إلى أهميته في تمحيص الشبهات والأدلة القائمة من قبل المتهم، فهو يعتبر أساس الدعوى الجزائية، بالإضافة إلى الضمانات التي يوفرها التحقيق للمتهم بالتالي زرع الثقة في نفوس الناس[3].

وحيث أنّ التحقيق الإبتدائي يتمثل في إجراءات عديدة ومتنوعة، وذلك حتى يتسنى لرجل القانون تحقيق غايته منه، وستعرض إجراءات التحقيق الإبتدائي في المطلب الأول، ويسلط الضوء على الإجراءات التي تتناسب مع الطبيعة القانونية الخاصة للجرائم المعلوماتية، التي قد تتميز بخصوصية عنها في الجرائم التقليدية، أما المطلب الثاني فخصه الباحث بالأوراق المتحصلة من إجراءات التحقيق الإبتدائي المتمثلة بفحص الأدلة التي من شأنها أن تنسب الفعل إلى فاعله والتي لم يوردها المشرّع على سبيل الحصر.

---

[1] البشرى، محمد الأمين، **التحقيق في جرائم الحاسب الآلي والإنترنت**، وزارة الداخلية _أبو ظبي _دولة الإمارات العربية المتحدة، ص394.

[2] الغافري، حسين بن سعيد، السياسة **الجنائية في مواجهة جرائم الانترنت**، دار النهضة العربية،2009، ص499.

[3] ستار تايمز، ماهية التحقيق الابتدائي، تاريخ2016/14/10، الساعة، http://www.startimes.com/?t=7417291[3]10:21

المطلب الأول: إجراءات التحقيق الإبتدائي

هناك مشكلات عملية وفنية تواجه الجهود المبذولة لمكافحة الجرائم المعلوماتية على المستوى الإجرائي، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بالجريمة التقليدية، وتتمحور المشكلات الإجرائية في الجرائم المعلوماتية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونيا، وكيانات منطقية معنوية، فمن ناحية يصعب الكشف عن هذه الجرائم، ومن ناحية أخرى قد يستحيل جمع الأدلة بشأنها، بالإضافة إلى مشكلات عديدة سوف تقوم الباحثة بعرضها من خلال تفنيدها لإجراءات التحقيق على النحو التالي الفرع الأول: الانتقال والمعاينة، الفرع الثاني: ندب الخبراء، الفرع الثالث :الشهادة، الفرع الرابع التفتيش والضبط .

الفرع الأول: الانتقال والمعاينة.

الانتقال: "هو انتقال المحقق لمكان الجريمة، وملاحظة أدلتها وجمعها وتكوين فكرة عن الحادث، أو ضبط واقعة، أو إجراء معاينة أو الاطلاع على الأوراق، أو سجلات لا يمكن نقلها أو لسؤال أشخاص يتعذر انتقالهم إلى المدعي العام[1]".

فانتقال المحقق إلى مسرح الجريمة قد يكون بغرض المعاينة أو التفتيش أو سماع شهود أو ضبط الأشياء المتعلقة بالجريمة، وانتقاله يكون واجبا إذا كان الفعل يشكل جناية، فوجود المحقق في مكان الحادث ييسر له مباشرة المعاينة الفورية، ودعوة الشهود يمنع العبث بالأدلة.

أما **المعاينة** فهي: "مشاهدة الآثار المادية التي خلفها ارتكاب الجريمة، وإثباتها، بهدف المحافظة عليها خوفا من إتلافها، أو محوها، أو تعديلها[2]".

[1] الدهلاوي، عبد الرحمن محمد، **الانتقال والمعاينة في نظم دول مجلس التعاون الخليجي**، رسالة ماجستير،2008، ص7.

[2] الفيل، علي عدنان، **إجراء التحقيق الابتدائي في الجريمة المعلوماتية**، عدد53، 2010، ص20.

ومن الجدير ذكره أنّ كل من الانتقال والمعاينة يساهم في إثبات الواقعة الجرمية، ونسبتها إلى مرتكبيها، وذلك من خلال المحافظة على مسرح الجريمة باعتباره مستودع سر الجريمة، ومفتاح كشف غموضها، كما يساهم كل منهما بما يلي:

1. الكشف عن مكان الجريمة، وكيفية تنفيذها من بدايتها حتى نهايتها.

2. كشف الأدلة، وحصر آثار الجريمة.

3. تعطي المحقق فرصة ليلمس بنفسه العناصر المادية للجريمة التي قد تفيد بكشف الحقيقة

4. أما فيما يتعلق بالجاني فقد تعطي المحقق نظرة أولية عن أسلوبه الإجرامي، وباعثه من ارتكاب الجريمة وعدد الجناة[1].

إنّ المعاينة وإن كانت واردة في كافة الجرائم إلا أنها قد تكون دون جدوى، إذا كانت الجريمة بطبيعتها لا تستلزم هذا الإجراء، مثل جرائم التزوير المعنوي، أو جرائم السب، أما بالنسبة للمعاينة بالجريمة المعلوماتية نلاحظ أن أهميتها تتضاءل، وذلك بسبب طبيعتها الخاصة التي لا تخلف آثارا مادية تترتب عليها أدلة جنائية من جهة، ومن جهة أخرى أن المتهم بالجريمة المعلوماتية غالبا ما يكون قد تخلص، أو أتلف الآثار المادية للجريمة، كما أن عددا كبيرا من الأشخاص قد يتردد إلى مسرح الجريمة، وذلك ما بين فترة وقوع الجريمة وفترة اكتشافها[2].

فمثلا في قانون مكافحة جرائم التجارة الإلكترونية التونسي تعتبر المعاينة المرحلة الأولى لقيام كل التتبعات، سواء كانت إدارية أو قضائية، حيث يتم تفريغ المعاينة بمحاضر تتم إحالتها إما إلى الوزير المكلف بالتجارة، أو على وزير تكنلوجيات الاتصال والنقل[3].

---

[1] المعيني، سرحان حسن، **التحقيق في جرائم تقنية المعلومات**، مجلة الفكر الشرطي، مجلد20، عدد79، دار المنظومة،2011، ص40-41.

[2] التاج، ايها محمد، **التحقيق وجمع الادلة في الجرائم المعلوماتية**، مجلة العدل، وزارة العدل، السودان، مجلد 11، عدد26، دار المنظومة، 2009، ص 395.

[3] السعيدي، مجيد، **جرائم التجارة الإلكترونية**، رسالة ماجستير، جامعة تونس المنار، 2004/2003، ص120.

وحتى تصبح للمعاينة أهمية في كشف الحقيقة في الجرائم المعلوماتية لابد من مراعاة عدة قواعد أهمها:

1. وجود خريطة توضح الموقع الذي ستتم معاينته، وعدد الأجهزة والخزائن والملفات، ويحدد ذلك من خلال مصادر سرية لجهات الأمن.

2. تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج صعبة أو لينة.

3. تأمين عدم انقطاع التيار الكهربائي، لأنّ معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي[1].

4. إعداد فرق متخصصة، وهي: وفريق لأخذ الإفادات، وفريق الرسم والتصوير، وفريق التفتيش العملي، وفريق التأمين والقبض، وفريق تحرير الأدلة. على أن يرأس كل فريق مشرف على التحقيق.

5. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحبط الخارجي لموقع الحاسب من أيّ مجالات لقوى مغناطيسية ممكن أن تتسبب في محو البيانات المسجلة.

6. أخذ صور لواجهة وخلفية وجوانب الأداة والكوابل المرتبطة مع الأداة.

7. التحفظ على النظام ونسخ بياناته.

[1] حجازي، عبد الفتاح بيومي، **الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية**، ط1، 2009، ص586-587.

8. فصل النظام عن الشبكة، ووقف كل العمليات، ووضع وسائط التخزين في أوعية مناسبة، كما يجب وضع جميع الصناديق التي تخص نظام حاسوب معين مع بعضها البعض، وذلك من أجل تسهيل تتبع نقلها من مسرح الجريمة إلى مختبر الأدلة وتسليمها[1].

فالمعاينة في الجرائم المعلوماتية تتطلب مجهودا خاصا، وخطة واضحة وعلى الأغلب لابد من الاتفاق مسبقا على هذه الخطة مع أعضاء الفريق السابق ذكره، ومعرفة مسبقة عن حجم القضية التي يتم التحقيق بها، وذلك لأن آثار الجريمة غالبا ما تكون قد أُتلفت، كما أن النصوص التقليدية قد لا تساهم في قيام المحقق بالمعاينة بالطريقة المذكورة أعلاه، لأن قانون إجراءات جزائية لم يقم بحصر طرق المعاينة،أو ذكرها، والأولى أن يضع حدا أدنى من الشروط، أو الضوابط التي يجب على المحقق اتباعها ولاسيما عندما يتعلق الأمر بالجريمة المعلوماتية، وذلك قبل فوات الأوان، وعدم قدرة المحقق على التصدي لهذا النوع من الجرائم .

الفرع الثاني: ندب الخبراء

الخبرة:"هي وسيلة من وسائل الإثبات يتم اللجوء إليها إذا اقتضى الأمر كشف دليل أو تعزيز أدلة قائمة، كما أنها تعتبر استشارة فنية يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية، التي يحتاج تقديرها إلى مسائل عملية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته "[2]

فمنذ بداية ظهور الجرائم المعلوماتية نلاحظ أنّ سلطات التحقيق والشرطة تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الإلكتروني، وذلك بغرض التحقيق بالجريمة، والكشف عن ملابساتها وغموضها، وتكتسب الخبرة في الجريمة المعلوماتية أهمية بالغة، لأن كل من الحاسبات

---

[1] الفيل علي عدنان، **إجراء التحقيق الابتدائي بالجريمة المعلوماتية**، مجلة البحوث والدراسات العربية – مصر، عدد53، دار المنظومة، ص21-23.

[2] بن باردة عبد الحليم، **إجراءات البحث والتحري عن الجريمة المعلوماتية**، مجلة الحقوق والعلوم الانسانية، عدد23، دار المنظومة، 2015، ص82.

والشبكات المعلوماتية تتسم بتعدد أنواعها لذلك ان العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية متنوعة.

متطلبات أعمال الخبرة في مجال الجريمة المعلوماتية:

1. الإلمام بتركيب الحاسوب، وصناعته، وطرازه، وطريقة تشغيله.
2. القدرة على أداء مهامه دون تعطيل لأي من الأدلة أو إتلافها.
3. التمكن من نقل أدلة الإثبات غير المرئية وجعلها أدلة مقروءة.
4. معرفته بطرق التعامل مع برامج الحاسب الآلي مثل برامج الفيروسات، أو برامج كشف، أو استرجاع البيانات وإظهار المخفي منها.[1]

ومن ناحية أخرى يجب على المحقق الجنائي أن يحدد للخبير المعلوماتي دوره في المسألة المنتدب بها على وجه دقيق، لذا يجب تأهيل كل من رجال الضبط وسلطات التحقيق، كما أنه يجب تحديد لقاء بين المحقق الجنائي والخبراء كافة الذين تم الاستعانة بهم بالتحقيق، وذلك من أجل حصر الأدلة وترتيبها[2].

والخبير الذي ينتدبه المحقق يحلف اليمين أمام قاضي التحقيق ويقدم رأيه كتابة، ويرفع الخبير تقريره إلى المحقق وفقا للمدة المتفق عليها، ويرفق مع ملف الشكوى، ويكون تقرير الخبير خاضعا للسلطة التقديرية للمحقق، وغالبا ما يكون تقرير الخبير ولاسيما في مجال تكنولوجيا المعلومات محل شك في نهجه وخاصة إذا اعتمد الدفاع التشكيك في هذا التقرير وهدمه[3].

---

[1] بن بادرة، عبد الحليم، اجراءات **البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الانسانية**، ع23، دار المنظومة،2015، ص83-84.

[2] حجازي، عبد الفتاح بيومي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر**، دار الكتب القانونية،2007، ص329-331.

[3] عمري، محمد محمود، **الإثبات الجزائي الإالكتروني في الجرائم المعلوماتية**، مجلة العلوم القانونية والسياسية – العراق، مجلد12، عدد2، دار المنظومة،2016، 311-313.

كما أن الجرائم المعلوماتية من الجرائم التي تتعلق بمسائل فنية وتقنية متطورة جدا تحتاج إلى خبير على درجة عالية من الذكاء والفطنة وخبرة كبيرة في مجال تخصصه، لأنه قد يتعلق الأمر بتزوير المستندات أو التلاعب بالبيانات، أو بالغش في أثناء نقلها أو بثها، وتظهر أهمية الخبير في مجال الجرائم المعلوماتية في حال غيابه لأنه قد تعجز جهات التحقيق عن كشف الغموض أو قد تقوم بتدمير الأدلة[1].

الأساليب الفنية في عمل الخبير المعلوماتي في اكتشاف الدليل الرقمي:

على الخبير المعلوماتي في سبيل تحري الحقيقة استخدام الأساليب كافة، مالم تكن هذه الأساليب غير مشروعة، وليس للمحكمة أن ترفض هذه الأساليب إلا إذا كان رفضها مسببا ومعللا، وقد نوجز أساليب الخبير في تقصي الحقيقة بثلاث مراحل:

1. المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحاسبات التي دخل منها المجرم لمحاولة تتبع آثاره.

2. المرحلة الثانية: مرحلة المراقبة من خلال برامج مراقبة يمكن من خلالها حصر وتسجيل بيانات كل دخول وخروج من الموقع.

3. المرحلة الثالثة: فحص النظام المعلوماتي بكافة مكوناته المادية والمعنوية لاستخراج الأدلة منه، وتقديمها لجهات التحقيق، ومعرفة مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه[2].

---

[1] الفيل، علي عدنان، **إجراءات التحقيق الابتدائي بالجرائم المعلوماتية**، مرجع سابق، ص15-17.

[2] بن بادرة، عبد الحليم، **إجراءات البحث والتحري عن الجريمة المعلوماتية**، مرجع سابق، ص 82-84.

وهناك قواعد عامة يجب مراعاتها لضمان نجاح التحقيق مع الأشخاص ذوي العلاقة بالحاسب الآلي:

1. ضرورة التعامل بين مأموريّ الضبط أو التحقيق وخبراء الحاسب الآلي العاملين في المؤسسة المتضررة، أو مزودي الخدمة وذلك لأنه قد يكون خبراء هذه المؤسسة إما متهمين أو مساهمين عن قصد أو جهل أو إهمال وهذا ما نصت عليه المادة 32 من قانون الجرائم الإلكترونية الفلسطيني "يلتزم مزودو الخدمة بتزويد الجهات المختصة بجميع البيانات والمعلومات الازمة التي تساعد في كشف الحقيقية ،بناء على طلب النيابة أو المحكمة المختصة " كما ونصت الفقرة الرابعة من نفس المادة "يلتزم مزودو الخدمة بالتعاون ومساعدة الجهات المختصة ،وبناء على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والإحتفاظ المؤقت بها".

2. ضرورة مراعاة القوانين السارية في شأن الحقوق الفردية، وسرية البريد الإلكتروني وغير ذلك من الحقوق الخاصة حتى لا تضار البيانات التي يحصل عليها المحقق.

3. حفظ المعلومات أو الأدلة المتحصلة بالطرق التي تضمن سلامتها، وعلى حالتها التي ضبطت بها حتى يتسنى تقديمها للمحكمة دون وجود أي شك أو تأثير أو تعديل عليها، لأن الشك يفسر لصالح المتهم وهذا مانص عليه قانون الجرائم الإلكترونية الفلسطيني حيث نصت المادة [1]حيث نصت المادة 34 الفقرة الخامسة "تتخذ الإحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه بما في ذلك الوسائل الفنية لحماية محتواها".

4. ضرورة الالتزام بإصدار الأوامر القضائية الخاصة بالتفتيش، وضبط أجهزة الحاسب الآلي[2]. وهذا مانصت علية المادة 34 الفقرة الثانية من قانون الجرائم الإلكترونية الفلسطيني "للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات ،أو جزء منه،أو اي وسيلة من وسائل تكنلوجيا المعلومات التي من شأنها ان تكشف الحقيقة ". كما ونصت المادة 33 "للنيابة العامة أو من تنتدبه

[1] قانون الجرائم الالكترونية الفلسطيني رقم 16 لسنة 2017.

[2] حجازي، عبد الفتاح بيومي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص170-173.

من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنلوجيا المعلومات ذات صلة بالجريمة[1]".

فهذه القواعد يجب مراعاتها وذلك لضمان سير التحقيق، لأن الخطأ اليسير في هذه المرحلة قد يؤدي إلى القضاء على الأدلة والبيانات كافة.

ومن التشريعات الحديثة التي نظمت أعمال الخبرة بالجرائم المعلوماتية القانون البلجيكي الصادر 2000/11/23 فقد نصت المادة (88) من القانون المذكور أعلاه "يجوز لقاضي التحقيق، وللشرطة القضائية، الاستعانة بخبير، ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول اليه، أو الدخول إلى البيانات المخزنة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق الحق في أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المحولة أو الخزنة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق ."

نلاحظ من خلال المادة المذكورة أعلاه أنّ مهمة الخبير وفقا للقانون البلجيكي تتمثل بتشغيل النظام، وبتقديم البيانات المطلوبة، وذلك حسب ماتقرره جهة التحقيق، فالتزام الخبير هو إلتزام ببذل عناية وليس بتحقيق نتيجة، ولكن تثور مسؤوليته إذا رفض القيام بالمهمة المكلف بها[2].

وبالتعريج على الوضع في فلسطين تم إنشاء وحدة الجرائم المعلوماتية سنة 2013 وتم تخصيص دائرة المتابعة الفنية في هذه الوحدة، وذلك حتى يكون عملها متزامنا مع عمل سلطات التحقيق، وذلك من أجل الوصول إلى الحقيقة التي تتطلب جهدا متكاملا مع الخبير الفني أو التقني[3].

---

[1] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

[2] الفيل، علي عدنان، **إجراءات التحقيق الابتدائي بالجرائم المعلوماتية**، مرجع سابق، ص19.

[3] مقابلة مع النقيب رهام سائد احمد /مدير وحدة الجرائم المعلوماتية /رام الله /16 -4-2017 الساعة 10 صباحا.

الفرع الثالث: الشهادة

"هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق، بشأن جريمة وقعت، سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم، أو براءته منها ".

الشاهد بالجريمة المعلوماتية: هو الفني وصاحب الخبرة والتخصص في تقنية الحاسب الإلكتروني الذي يكون لديه معلومات جوهرية، أو مهمة لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن الأدلة بداخله، ويطلق عليه الشاهد المعلوماتي لتمييزه عن الشاهد التقليدي".

أما الشاهد المعلوماتي فيندرج في طوائف عديد ومنها:

1. مشغلو الحاسب الآلي: وهو الشخص المسؤول عن تشغيل جهاز الحاسب الآلي ومعداته، ويكون لديه خبرة كافية، لأنه يقوم بنقل البيانات من الوثائق إلى وسائط التخزين التي تجري معالجتها بواسطة الحاسب الآلي.

2. خبراء البرمجة: وهم ينقسمون إلى فئتين، هم مخططو برامج التطبيقات (إذ يقوموا بالحصول على خصائص النظام المطلوب من محلل النظم وتحويلها إلى برامج دقيقة وموثقة)، والثانية هم مخططو برامج النظم (يقومون باختيار برامج الحاسب الداخلية وتعديلها وتصحيحها)[1].

3. المحللون: إذ يقوم المحلل بدراسة البيانات وتحليل النظام، وتقسيمه إلى وحدات واستنتاج العلاقة الوظيفية بين هذه الوحدات.

4. مهندسو الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة المتعلقة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

[1] حجازي، عبد الفتاح بيومي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص339-340.

5. مديرو النظام: وهم الذين يوكل إليهم أعمال الإدارة في النظم المعلوماتية[1].

ويحصر قانون الدليل الخاص بولاية كاليفورنيا الأمريكية الشهود في الجريمة المعلوماتية بما يلي:

أ. محلل النظم الذي صمم برنامج الحاسب الإلكتروني الذي أنتج الدليل.

ب. المبرمج الذي قام بتحرير البرنامج واختباره.

ج. المشغل الذي يقوم بتشغيل البرنامج.

د. طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو قرص)

هـ. أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة أو الاقراص التي تشتمل على البيانات المصدرية الصحيحة.

و. مهندس الصيانة الإلكترونية الذي يقوم على صيانة الجهاز الأصلي، والتأكد من عمله بصورة صحيحة.

ز. موظفو المدخلات والمخرجات والمسؤولون عن معالجة المدخلات المستخدمة في تنفيذ برامجه.

ح. المستخدم النهائي الذي يمد بالمعلومات، ويصرح بتنفيذ برامج الحاسب الإلكتروني، ويستخدم نواتجها.[2]

ويتعين على الشاهد في الجريمة المعلوماتية أن يدلي بالمعلومات الجوهرية كافة التي تساهم بالدخول لنظام المعالجة الآلية للبيانات حتى يتسنى للمحقق البحث عن الأدلة الموجودة داخله والسؤال هنا: نفسه هل يلتزم الشاهد بالإفصاح عن كلمات المرور والشيفرات وبطبع الملفات؟

---

[1] عبد الإله، هلالي، **تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي**، دراسة مقارنة، 2000، ص43.

[2] عقيدة أبو العلا، **التحقيق وجمع الدلة في مجال الجرائم الإلكترونية**، بحث مقدم الى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنشور على شبكة الإنترنت، موقع الدليل الإلكتروني للقانون العربي التاريخ 2016/10/17 الساعة 10:43.

وللإجابة عن هذا السؤال لا بد من عرض اتجاهات مختلفة في هذا الشأن:

الاتجاه الأول: هو أن الشاهد غير ملزم بالإفصاح عن الشيفرات وطبع الأوراق، وذلك حسب الفقه الجنائي الألماني، وذلك على اعتبار أنه لا يوجد التزام قانوني على الشاهد يتضمن هذا الواجب، حتى في تركيا لا يجوز حمل الشاهد على ذكر كلمة المرور أو كشف شيفرات التشغيل.

الاتجاه الثاني: أما الفقه الفرنسي يرى أنه يقع التزام على الشاهد بالإفصاح بما لديه من معلومات بما في ذلك من الإفصاح عن الشيفرات وكلمات المرور وطبع الملفات، ويعاقب جنائيا متى رفض إعطاء هذه الكلمات في مرحلة التحقيق الابتدائي والمحاكمة وذلك حسب المواد (62-109-138) من قانون إجراءات جنائية فرنسي.[1]

فقانون الجرائم الإلكترونية الفلسطيني أوجب في المادة 32 مزودو الخدمة بتزويد الجهات المختصة بجميع البيانات والمعلومات التي تساعد في كشف الحقيقة بناء على طلب النيابة العامة او المحكمة .[2] كما نصت المادة 35 الفقرة الثانية "للنيابة العامة أن تامر بالجمع والتزويد الفوري لأي بيانات بما فيها حركة الإتصالات ،أو معلومات إلكترونية ،أوبيانات مرور،أومعلومات المحتوى التي تراها لازمة لمصلحة التحقيقات ،بإستعمال الوسائل الفنية المناسبة والإستعانة في ذلك عند الإقتضاء بمزودي الخدمة حسب نوع الخدمة التي يقدمها[3]".

وفي هولندا يتيح قانون الحاسب الآلي بإصدار أمر من قبل سلطات التحري والتحقيق للقائم على تشفير النظام، لتقديم كافة المعلومات اللأزمة لاختراقه، والدخول في هذا النظام للوصول إلى أي معلومات قد تفيد بالكشف عن الحقيقة، وفي حال وجود بيانات مشفرة التي قد تساهم في إظهار الحقيقة يتم تكليف القائم على تشغيل النظام بفك هذه الرموز وتحليل البيانات.

أما في اليونان يمكن الحصول من القائم على تشغيل نظام الحاسب الآلي على الشيفرات وكلمات السر للدخول إلى النظام، كما يمكن الحصول منه على بعض الإيضاحات الخاصة

---

[1] الفيل، علي العدنان، **إجراء التحقيق الابتدائي في الجريمة المعلوماتية دراسة مقارنة**، مرجع سابق، ص51-52.

[2] قانون الجرائم الالكترونية الفلسطيني رقم 16 لسنة 2017.

بنظامه الأمني، ولكن لا يوجد على الشاهد أي التزام بطباعة ملفات مخزنة في ذاكرة الحاسب، لأنه يجب أن يشهد على معلومات قد وقعت بين يديه وليس من شأنه كشف معلومات جديدة، وذلك حسب المادة 1/223 من قانون إجراءات الجنائية اليوناني[1].

بعد الإجابة عن السؤال المطروح أعلاه وتحديد مدى تباين التشريعات الجنائية في هذا الشأن لابد من التعريج على الدور الذي يلعبه التزام الشاهد بالإعلام في الجرائم المعلوماتية:

1) تحقيق مبدأ التوازن في المعلومات الجوهرية ذات العلاقة بالنظم المعلوماتية بين الشهود ومستخدمي الحاسبات الآلية وسلطات التحقيق، وهذا النوع من الجرائم بما يحتاجه من خبرة تقنية يصعب على رجل التحري والمحقق الحصول على المعلومات الكفيلة بإظهار الحقيقة، فلابد من وجود التزام قانوني على الشاهد بضرورة الإعلام بما لديه من خلال نص قانوني، لأن نقص المعلومات المتخصصة في هذه الجريمة لايزال هو التحدي الخطير بالنسبة للتحقيقات الجنائية.

2) تدارك أوجه القصور والعجز التي تتسم به الوسائل التقليدية: لأنّ طباعة الملفات وكشف كلمة المرور أو الكشف عن الشفرات المدون بها الأوامر الخاصة بتنفيذ البرامج جميعها لا تشمل الالتزام بتأدية الشهادة حسب المعنى التقليدي لمفهوم الشهادة الأمر الذي يستدعي البحث عن أسلوب جديد يجعل الشاهد المعلوماتي أكثر فاعلية ولاسيما في ظل خصوصية هذه الجريمة ومن هنا تبدو ضرورة الأخذ بفكرة الالتزام بالإعلام في الجريمة المعلوماتية[2].

الفرع الرابع: التفتيش وضبط الاشياء

إجراء من إجراءات التحقيق، يهدف إلى البحث عن أدلة مادية لجناية أو جنحة تتحقق وقوعها في محل تمتع بحرمة المسكن أو تفتيش الشخص، وذلك من أجل إثبات ارتكابها أو نسبتها وفقا للإجراءات القانونية المقررة ".

---

[1] حجازي، عبد الفتاح بيومي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص350.

[2] عبد الإله، الهلالي، **تفتيش نظام الحاسب الآلي وضمانات المتهم في الجريمة المعلوماتية**، مرجع سابق، ص29.

فالتفتيش إجراء من إجراءات التحقيق يتطلب أمرا قضائيا لمباشرته فهو ليس من أعمال الاستدلال، كما أنّ التفتيش مرحلة سابقة على مرحلة الضبط، ولا بد من أن يكون هناك مذكرة تفتيش صادرة من الجهة المختصة التي يحددها القانون تضمن دليلا معقولا، ووصفا محددا للمكان محل التفتيش وللأشخاص، ونطاق امتداده[1].

ويمكن تقسيم قواعد تفتيش أنظمة الحاسوب إلى:

أولا: القواعد الموضوعية

يقصد بالشروط الموضوعية للتفتيش في الجرائم المعلوماتية الشروط الأزمة لإجراء تفتيش صحيح، وهي ضوابط سابقة له ويمكن حصرها في: السبب، والمحل، والسلطة المختصة بالقيام به وفيما يلي بيان ذلك:

1. سبب التفتيش في العالم الافتراضي

لابد أن نكون بصدد جريمة معلوماتية سواء كانت هذه الجريمة جناية، أو جنحة، وأن تكون هناك قرائن تفيد أنّ هناك شخصا معينا أو أشخاصا محددين قد ارتكبوا هذه الجريمة، وأنّ هناك أجهزة معلوماتية تفيد بكشف الحقيقة سواء كانت هذه الأجهزة موجودة مع الشخص المتهم أو في مسكنه أو مع شخص اخر أو في مسكنه لان الهدف من التفتيش وغايته هو جمع الأدلة التي تثبت وقوع الجريمة وتكشف عن هوية فاعلها[2] وهذا مانصت عليه المادة 33 من قانون الجرائم الإلكترونية الفلسطيني "يجب أن يكون أمر التفتيش مسببا ومحددا،ويجوز تجديده أكثر من مرة .."

2. محل التفتيش في الجريمة المعلوماتية

إنّ المحل الذي يقع عليه التفتيش في الجرائم المعلوماتية هو جهاز الحاسب الآلي بمكوناته المنطقية والمادية، وشبكات الاتصال الخاصة به (الخادم، والمزود الآلي، والملحقات التقنية) وقد

[1] الحلبي، خالد عياد، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة للنشر والتوزيع ،2011، ص149-150.

[2] هروال، نبيلة هبة، **الجوانب الاجرائية لجرائم الانترنت**، دار الفكر الجامعي،2007، ص230.

يكون الشخص بوصفه محلا للتفتيش من مستخدمي أو مستغلي الحاسب الآلي، أو من خبراء البرامج سواء كانت برامج تطبيقات أو نظام أو من مهندسي الصيانة والاتصالات أو من مديري النظم المعلوماتية، أو أي شخص يكون بحوزته أجهزة أو معدات معلوماتية أو أجهزو محمولة أو تلفونات متصلة بجهاز المودم[1].

أما المنازل وما في حكمها كمحل للتفتيش في الجريمة المعلوماتية: كافة محال الإقامة أو المأوى والملحقات المخصصة لمنافعها، والتي يشغلها الشخص سواء بصفة دائمة أو مؤقتة سواء كانت ثابتة أو متنقلة متى وجد فيها أي من مكونات الحاسب الآلي سواء المادية أو المنطقية أو شبكات الاتصال الخاصة.[2] حيث نصت المادة 33 من قانون الجرائم الإلكترونية الفلسطيني "للنيابة العامة او من تنتدبه من مأموري الضبط القضائي الفلسطيني تفتيش الأشخاص والأماكن ووسائل تكنلوجيا المعلومات ذات الصلة بالجريمة ".

3. السلطة المختصة بالقيام بالتفتيش

الأصل أنّ التفتيش عمل من أعمال التحقيق الابتدائي الذي تختص به النيابة العامة وحدها ولكن رجال الضابطة العدلية يساعدون النيابة العامة في إجراءات التفتيش بهدف الحصول إلى الأدلة الجرمية، ونظرا للمهارات الفنية التي تطلبها هذه الجريمة فلا بد من الاستعانة بخبراء أثناء التفتيش وعلى النيابة أن تعطيهم الإذن بهذا التفتيش وهذ مانصت علية المادة 33 من قانون الجرائم الإلكترونية الفلسطيني "للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ...".

ثانيا: قواعد الشكلية

وهي الإجراءات والسلوكيات الواجب حدوثها خلال عملية تفتيش أداة الجريمة أو مكانها، ويتمثل ذلك في حضور المتهم، محضر التفتيش، وأسلوب تنفيذ التفتيش.

---

[1] العبيدي، أسامة بن غانم، التفتيش **عن الدليل في الجرائم المعلوماتية**، مرجع سابق، ص 99.

[2] الغافري، حسين بن سعيد، السياسة **الجنائية في مواجهة جرائم الانترنت**، مرجع سابق، ص491.

1. الحضور أثناء إجراء التفتيش

الأصل ان الشخص الذي يستوجب القانون حضوره هو المتهم وذلك الشرط يكون قائما عند تفتيش الشخص نفسه أو تفتيش مسكن المتهم إلا انه قد يتصور تفتيش المسكن من دون حضور المتهم وذلك كأن يكون هذا الإجراء قد تم بحضور من ينوب عن المتهم أو بحضور القاطنين معه بالمنزل اوالجيران وذلك لضمان عدم تعسف القائمين على التفتيش[1].

2. محضر التفتيش في الجريمة المعلوماتية

يجب تحرير محضر في التفتيش يثبت فيه كل ما تم من إجراءات بحيث تتم مراعاة القواعد العامة في المحاضر بشكل عام كأن يكون مكتوب باللغة العربية وأن يحمل تاريخ تحريره وتوقيع الشخص الذي قام بالتحرير وغيرها من الشكليات حسب القواعد العامة وحسب تشريع كل دولة.[2] وهذا مانصت علية المادة 33 من قانون الجرائم الإلكترونية الفلسطيني الفقرة 3""إذا أسفر التفتيش عن ضبط أجهزة ،أو أدوات،أو وسائل ذات صلة بالجريمة يتعين على مأنور الضبط القضائي تنظيم محضر بالمضبوطات،وعرضها على النيابة العالمة "[3].

3. أسلوب تنفيذ التفتيش

لإجراءات تنفيذ التفتيش في الجرائم المعلوماتية خصوصية تميزها عن الجرائم التقليدية، فيجب على المحقق القيام بتحريات شاملة ودقيقة قبل القيام بإجراء التفتيش منها:

تحديد نوع النظام المعلوماتي، وتجميع فريق عمل يتكون من (محقق، وخبراء فنيين، ورجال ضبط جنائي)، ووضع خطة لتنفيذ التفتيش على أن تتضمن مسودة التفتيش بيانا مفصلا للاستراتيجية التي سيتم اتباعها عند إجراء التفتيش، أما بالنسبة للميقات الزمني للتفتيش فيجب أن يكون غير محدد نظرا للطبيعة الخاصة للجرائم المعلوماتية التي تتميز بسهولة محو الأدلة أو إتلافها، وعليه

---

[1] هروال، نبيلة هبة، **الجوانب الاجرائية لجرائم الانترنت**، مرجع سابق، ص255.

[2] العبيدي، أسامة بن غانم، **التفتيش عن الدليل في الجرائم المعلوماتية**، مرجع سابق، ص102.

[3] قانون الجرائم الإلكترونية الفسطيني رقم 16 لسنة 2017.

نجد بعض التشريعات التي لم تحدد زمن معين للتفتيش سواء كان ليلا أو نهارا، مثل قانون الإجراءات الجنائية المصري، ومنها من يحدد زمن معين للتفتيش مثل القانون الفرنسي الذي حدده من الساعة السادسة صباحا إلى الساعة التاسعة ليلا بناء على نص المادة (59) من قانون الإجراءات الجنائية[1].

ومما لا شك فيه أن محل التفتيش في الجرائم المعلوماتية يختلف عن محل التفتيش في الجريمة التقليدية، كما ذُكر سابقا، فمحل التفتيش في الجرائم المعلوماتية يشمل جهاز الكمبيوتر، والأجهزة المتصلة به، والشبكة العنكبوتية التي تشمل مقدم الخدمة، والمزود الآلي، والمضيف، والملحقات التقنية، وهذا يعني أنّ التفتيش في الجرائم المعلوماتية سوف ينصب على:

1. المكونات المادية للحاسب الآلي

لا شك أنّ التفتيش عن المكونات المادية للحاسوب من شأنه أن يفيد في كشف الحقيقة عن الجريمة، وعن مرتكبيها، كما أنه يخضع للقواعد الإجرائية الخاصة بالتفتيش، أي أن حجم التفتيش للمكونات المادية يتوقف على طبيعة المكان سواء كان عاما أو خاصا، مع مراعاة التمييز فيما إذا كانت مكونات الحاسب الآلي منعزلة عن غيرها، أو متصلة بجهاز آخر أو بنهاية طرفيه، كأن يكون بمسكن غير مسكن المتهم، فيجب على المحقق أن يراعي القيود والالتزامات التي يفرضها المشرع وذلك تبعا لقواعد التفتيش الإجرائية.

كما أن هناك الكثير من الأجهزة التي توجد بها معلومات كالتي موجودة بالحاسب الآلي مثل الآيفون، والآيباد، وتكون محمولة مع الشخص المتهم، لذلك فإن قواعد التفتيش المتعلقة بالمسكن لا تكفي في الجرائم المعلوماتية، ولابد أيضا من تطبيق قواعد التفتيش المتعلقة بالأشخاص[2].

---

[1] خلف، جاسم خريبط، **التفتيش في الجرائم المعلوماتية**، الخليج العربي، دار المنظومة، مجلد 41، عدد 34، 2014، ص249.

[2] المعمري، عادل عبد الله خميس، **التفتيش في الجرائم المعلوماتية**، مجلة الفكر الشرطي، مجلد22، عدد86، 2013، ص260.

ومن التطبيقات القضائية على التفتيش في المكونات المادية:

القسم 94 من قانون الإجراءات الجنائية الألمانية حيث ينص على أن الأدلة المضبوطة يجب أن تكون ملموسة، ويترتب على هذا أن البيانات المنفردة عن الدعامات لا تعد أشياء لكي يمكن تفتيشها وضبطها، ولكن إذا تم طباعة هذه البيانات تصبح أشياء ملموسة يمكن ضبطها.

أما قانون العقوبات في رومانيا فإنه حدد أنّ الضبط يقع على الأشياء المادية، والتي منها البيانات المحملة على الدعامات كالأشرطة المغناطيسية أو الأقراص، أما البيانات ككيان معنوي فإنها لا تصلح للضبط[1].

2. المكونات المعنوية للحاسب الآلي.

لقد أثار موضوع التفتيش على المكونات المعنوية للحاسب الآلي جدلا فقهيا، فالبعض اعتبر أن هذه المكونات لا تصلح لأن تكون محلا للتفتيش، وذلك لأن هذه المكونات لا تعتبر من قبيل الأشياء المادية والملموسة بالتالي لا تخضع للنصوص التقليدية المتعلقة بالتفتيش.

والبعض الآخر ذهب إلا أن هذه المكونات تصلح لأن تكون محلا للتفتيش، لأنها تتناسب مع الغاية من التفتيش، وهو الحصول على الأدلة الجرمية وضبطها، وكشف الغموض الذي أحاط بها، وتقديم البرامج غير المشروعة المخزنة على الحاسوب الخاص بالمتهم كدليل اتهام ضده أمام المحكمة المختصة. [2]

ولا يجوز التوسع في تفسير النص الجزائي، ويجب أن يكون هناك نص خاص يتيح للمحقق القيام بتفتيش البيانات المعنوية المتحصلة من الجرائم المعلوماتية وضبطها، وهناك تطبيقات تشريعية تجيز تفتيش مكونات الحاسب الآلي المعنوي ومنها:

---

[1] الغافري، حسين بن سعيد، السياسة **الجنائية في مواجهة جرائم الغنترنت**، مرجع سابق ص،476.

[2] عبد الاله، الهلالي، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي**، مرجع سابق، ص 73.

المادة (251) من قانون الإجراءات اليوناني منحت سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع الدليل وحمايته، وكذلك المادة (487) من القانون الجنائي الكندي التي منحت سلطة إصدار إذن لضبط أي شيء، طالما تتوافر أسس معقولة للاعتقاد بأنّ الجريمة ارتكبت أو يشتبه بارتكابها، أو أنّ هناك نية في أن يستخدم في ارتكاب الجريمة، أو انه سوف ينتج دليلا على وقوع الجريمة.

وينص القانون الإنجليزي صراحة على تفتيش نظم الحاسب المادية والمعنوية، ونص على إجراءات تفتيش نظم الحاسوب في جرائم الولوج غير المصرح به على أنظمة الحاسوب، والتعديل غير المصرح به في نظم الحاسوب، دون إذن لارتكاب أفعال غير مشروعة.[1]

3. شبكات الحاسب الآلي

شبكات الحاسب الآلي "هي عبارة عن مجموعة مكونة من جهازين أو أكثر من أجهزة الحاسب الآلي والمتصلة ببعضها اتصالا سلكيا أو لاسلكيا، وتوجد شبكات واسعة في أماكن متفرقة مرتبطة ببعضها البعض بواسطة الهاتف "

فالبيانات التي تحتوي على أدله قد تتوزع عبر شبكات الحاسب الآلي في أماكن قد تكون على مسافات بعيدة من الموقع المادي الذي قد يتم به التفتيش، وفي حال كان الموقع الفعلي للبيانات قد يدخل في اختصاص، مما قد يعقد الصعوبات التي تواجه التفتيش في هذه الجريمة، وفيما يلي عرض للاحتمالات المترتبة على تفتيش شبكات الحاسب الآلي:

الاحتمال الأول: اتصال الحاسب الآلي للمتهم بحاسب آلي آخر، أو نهاية طرفيه موجود داخل الدولة، مما يثير تساؤلا عن مدى إمكانيه امتداد التفتيش في حال كان الحاسب الآلي للمتهم متصلا بحاسب آخر بمكان غير مسكن المتهم؟

[1] الحلبي، خالد عياد، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، دار الثقافة للنشر والتوزيع، ص162.

والفقه الألماني يرى إمكانيه امتداد التفتيش إلى سجلات البيانات التي تكون في مكان آخر، وذلك استنادا إلى ما جاء في القسم (103) من قانون إجراءات الجزائية الذي سمح بامتداد التفتيش إذا كان مكان التخزين الفعلي خارج المكان الذي يتم فيه التفتيش.

أما قانون الإجراءات الجنائية البلجيكي أورد في نص (88) "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو جزء منه فإن هذا التفتيش يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان غير مكان البحث الأصلي ولكن يتم ذلك وفقا للضوابط الآتية:

1) إذا كان هذا الامتداد في التفتيش ضروري لإظهار الحقيقة.

2) إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظرا لسهولة محو البيانات أو إتلافها أو نقلها محل البحث.

ونهج المشرّع الأسترالي والهولندي نفس النهج بحيث لم يعد التفتيش في الجرائم المعلوماتية يقتصر على مواقع معينة[1].

الاحتمال الثاني: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفيه موجودة في مكان آخر خارج الدولة

إنّ من أخطر المشاكل التي تواجه المحقق في الجريمة المعلوماتية قيام مرتكبي الجرائم بتخزين البيانات في أنظمة تقنية خارج الدولة حتى لا يتمكن الادعاء من جمع الأدلة. لذلك يرى كثير من الفقهاء أن التفتيش الإلكتروني العابر للحدود يجب أن يُتفق عليه في ظل معاهدات ثنائية أو دولية، لأن التفتيش دون وجود مثل هذا النوع من الاتفاقيات أو على الأقل الحصول على إذن الدولة الأخرى، لأنّ هذا النوع من التصرفات يعتبر بمثابة تدخل في سيادة الدولة[2].

---

[1] العبيدي، أسامة بن غانم، التفتيش **عن الدليل في الجرائم المعلوماتية**، المجلة العربية للدراسات الأمنية والتدريب، مجلد 29عدد58، ص91.

2 الخثعمي، عبد الله بن عبد العزيز، التفتيش **في الجرائم المعلوماتية في النظام السعودي**، رسالة ماجستير، دراسة تطبيقية، امعة نايف العربية للعلوم الأمنية، 2011، ص93.

وكتطبيق لهذا الإجراء فقد حدث بألمانيا أثناء التحقيق في جريمة غش وقعت ببيانات الحاسب الآلي فقد تبين وجود اتصال بين حاسب آلي موجود بألمانيا، وشبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها، وعندما أرادت السلطات الألمانية ضبط هذه البيانات فلم تتمكن من ذلك إلا من خلال المساعدة بين الدولتين[1].

الاحتمال الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي:

نلاحظ أن القانون البريطاني من التشريعات التي تتيح الرقابة والملاحقة والقبض والتفتيش دون الخضوع للمبادئ والأحكام القانونية التي استقرت بموجب الاتفاقية الأوروبية لحقوق الإنسان، ومبادئ وتوجيهات الاتحاد الأوروبي.

كما أن قانون الجرائم الإلكترونية الفلسطيني جعل صلاحية مراقبة الإتصلات والمحادثات الإلكترونية وتسجيلها والتعامل معها لقاضي الصلح وذلك لمدة 15 يوما قابلة للتجديد مرة واحدة متى توافرت أدلة جديدة[2].

ولكن لو تمعنا بخصوصية التفتيش في الجرائم المعلوماتية بالقانون الفلسطيني نرى أنها تتضمن الكثير من الأحكام التي من شأنها أن تمس حرمة الحياة الخاصة للمواطن فنحن على يقين أن جهاز الحاسوب أو الأجزة الذكية تكاد تشتمل على كافة تفاصيل وحياة الأفراد ولا شك أن ماجاء به القانون الفلسطيني الذي منح النيابة العامة صلاحيات واسعة في التفتيش ومراقبة التصالات والاحتفاظ بالمعلومات الشخصية يتعارض مع مبادئ دستورية تتعلق بإختراق حرمة الحياة الخاصة للمواطن حتى من دون أن يكون هناك ضوابط قضائية في بعض الأحيان ،فكان الأولى على المشرع أن يوازن بين خصوصية الجريمة المعلوماتية التي تحتاج إلى تدخل فوري وسريع وبين حق الفرد والمواطن في إحترام خصوصيتة وحرمة حياته بطريقة أو بأخرى .

[1] الغافري، حسين بن سعيد، **السياسة الجنائية في مواجهة جرائم الإنترنت**، مرجع سابق، ص484-485.

كما أصدر الكونجرس الأمريكي تشريعا يرفع الكثير من القيود على عمليات التنصت والرقابة الهاتفية، ومراقبة الإنترنت والبريد الإلكتروني، خاصة بعد ما أثاره المحققون من أن الإنترنت والبريد الإلكتروني كانا الواسطة التي أتاحت للجهة التي نفذت الهجوم على مركز التجارة العالمي والبنتاغون، ويمثل السبب الرئيس الأول لقبول هذا التشريع رغم تعارضه مع حقوق وحريات الأفراد أنه تشريع موجه لغير المواطنين الأمريكيين، مع أن الواقع العلمي لن يكون كذلك[1].

كما نلاحظ أن التنصت والأشكال الأخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ضوابط محددة في كل الدول تقريبا، مثل هولندا، وفرنسا، واليابان، حيث أقرت المحكمة عام (1991) شرعية التنصت على شبكات الحاسب للبحث عن الدليل[2].

ويعد الضبط في مجال الجريمة المعلوماتية أثرا للتفتيش، وهو وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية أو المعلومات، التي تتصل بالجريمة المعلوماتية التي وقعت، وتفيد في كشف الحقيقة عنها وعن مرتكبيها[3].

والسؤال هنا: ما مدى صلاحية ضبط الأدلة في الجرائم المعلوماتية؟

إن ضبط الأدلة الإلكترونية التي تتعلق بجرائم الحاسوب والإنترنت، وضبط المكونات المعنوية والتي يجري تبادلها في نطاق شبكة المعلومات والإنترنت من الأمور التي أجازها القانون، وذلك حسب ما ورد في القانون الكندي في نص المادة (487) التي أجازت إصدار أمر قضائي لتفتيش وضبط أي شيء تتوافر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأن جريمة قد وقعت، أو يشتبه في وقوعها، وأن تفسير الفقه الكندي لهذه المادة يوسع من نطاقها بحيث يشمل بيانات الحاسوب غير المحسوسة[4].

---

[1] الحلبي، خالد عياد، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، مرجع سابق، 166-167.

[2] الخثعمي، عبد الله بن عبد العزيز، **التفتيش في الجرائم المعلوماتية**، مرجع سابق، ص95.

[3] خلف، جاسم خريبط، **التفتيش في الجرائم المعلوماتية**، مرجع سايق، ص252.

[4] هروال، نبيلة هبة، الجوانب **الإجرائية لجرائم الإنترنت**، مرجع سابق، ص265.

وعلى الرغم مما ورد في القانون الكندي إلا أن هناك اختلافا فقهيا وتشريعيا بهذا الخصوص، فالبعض يرى أن الضبط لا يقع على المكونات المعنوية والمنطقية للحاسب الآلي، وأنّ هذا الأجراء لا يمكن أن يتم إلا إذا جسدته البيانات في دعامة مادية، أما الاتجاه الآخر فيرى أنه لا يوجد مانع من أن يشمل الضبط المكونات المنطقية للحاسب الآلي[1].

ولا بد من أن يكون هناك موقف وسطيّ، وذلك بضرورة تدخل تشريعي لتوسيع دائرة الضبط لتشتمل جميع مكونات الحاسب الآلي.

وثمة صعوبة تتمثل بالضبط ولاسيما إذا كان الضبط متعلقا في الأنظمة المعلوماتية الكبيرة، أو الشبكات الكبيرة حيث يصادف الضبط صعوبتين:

1. عزل النظام المعلوماتي بالكامل عن دائرته لمدة زمنية قد تطول أو تقصر، مما قد يسبب إضرار بالجهة المستخدمة للنظام.

2. عدم إبداء مستخدمي الأنظمة المعلوماتية الاستعداد للتعاون الكامل والفعال مع سلطات التحقيق مما يعني أن الضبط قد يشكل مساسا بحقوق الغير.[2]

نظرا للطبيعة الخاصة بالجرائم المعلوماتية يجب أن يكون هناك قواعد معينة لحفظ المضبوطات، كما ويجب أن يكون المحقق مدربا ومؤهلا على التعامل مع الأدلة المعلوماتية، لمنع إتلافها أو تدميرها، مما يفرض اتخاذ إجراءات خاصة للحفاظ عليها وصيانتها من العبث فعلى المحقق:

1. ضبط الدعائم الأصلية للبيانات، وعدم الاقتصارعلى ضبط نسخها.

2. عدم ثني القرص، لأن ذلك يؤدي إلى تلفه وفقدان البيانات المسجلة عليه.

---

[1] الفيل، علي عدنان، **إجراءات التحقيق الابتدائي بالجرائم المعلوماتية**، مرجع سابق، ص44.

[2] الحلبي، خالد، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، مرجع سابق، 173-174.

3. عدم تعريض الأقراص والأشرطة الممغنطة لدرجات حرارة عالية، فيجب أن تكون درجة الحرارة تتراوح ما بين (4-32)، ولا إلى الرطوبة، مع العلم أن الرطوبة المسموح بها تتراوح ما بين (20-80%)

4. عدم تعريض القرص للغبار والأتربة.

5. عدم كتابة البيانات اللاصقة الورقية المخصصة للمستخدم بعد لصقها على القرص، لأن الضغط بالقلم قد يفسد سطح القرص[1].

وعند الحديث عن الواقع الفلسطيني فيما يتعلق بإجراءات التحقيق نلاحظ وجود وحدة متخصصة لمتابعة الجرائم المعلوماتية بعد انتشار الجريمة المعلوماتية، وتتكون هذه الوحدة من عدة أقسام:

1.المدير، ونائب المدير حيث يقوم كل منهما بالإشراف ومتابعة جميع أقسام الوحدة.

2.المختبر الجنائي يقوم على تحليل واستخراج الدليل الرقمي والتعامل به.

3. المتابعة الفنية يعمل على ملاحقة المشتبه به بارتكاب الجريمة المعلوماتية على مواقع وشبكات الإنترنت وشبكاتها كافة.

4.التوعية والارشاد: حيث تعمل هذه الوحدة على تثقيف المجتمع بكيفية التعامل مع وحدة الجريمة المعلوماتية من جهة، ومع الجريمة المعلوماتية من جهة أخرى، لاسيما مع وجود عادات وتقاليد مجتمعية قد يصعب معها التبليغ عن بعض الجرائم الإلكترونية، كالابتزاز مثلا وبالأخص إذا كان واقعا على فتاة، بالتالي يجب التعامل مع هذه المواضيع بخصوصية معينة فيقع على هذا القسم إرشاد المجتمع حول التعامل مع هذا النوع من الجرائم.

5.الدائرة القانونية: متابعة القضية من لحظة ورود الشكوى حتى إحالة الملف.

---

[1] خلف، جاسم خريبط، **التفتيش في الجرائم المعلوماتية**، مرجع سابق، ص 256.

6. دائرة الاتصالات: متابعة قضايا الاتصالات الواردة من جهاز الشرطة من خلال مكتب النائب العام[1].

لا شك أن وجود مثل هذه الوحدة بات ضروريا، وساهم بشكل كبير في مكافحة الجريمة المعلوماتية بالتزامن مع دخول قانون الجرائم الإلكترونية الفلسطيني حيز التنفي، حيث أن الجهات المختصة كانت صائبة في تحقيق هذا التدرج، فجعلت الخطوة الأولى هي تدريب الكوادر لتأهيلها للتحقيق في الجريمة المعلوماتية والتعامل مع الأدلة الرقمية، ومن ثم خلق وحدة جرائم معلوماتية، بعد ذلك تخصيص نيابة للجرائم المعلوماتية، وأخيرا دخول قانون الجرائم الإلكترونية رقم 16 لسنة 2017 حيز التنفيذ.

ويلاحظ من خلال ما تقدم أنه لا بد من تشريع قانون إجراءات جنائية خاص بالجريمة المعلوماتية، أو التعديل على النصوص الإجرائية التقليدية لتحتوي طبيعة الجرائم المعلوماتية، وذلك لأن النصوص التقليدية لا تتسع لتشمل الإجراءات الضرورية كافة، التي تظهر الحقيقة من جهة وتحمي الأدلة من التلف والضياع من جهة أخرى، كما أن النصوص الجنائية لا يجوز القياس عليها ولا يجوز التوسع في تفسيرها، وهذا يعني أنّ سلطة القاضي تكون محدودة من جعل النص التشريعي مرنا، ليتسع هذا النوع من الجرائم وليشمل هذه الخصوصية الواردة في الإجراءات التي يجب اتباعها في الجرائم المعلوماتية .

المطلب الثاني: الدليل الإلكتروني (الدليل الرقمي) المتحصل عليه في مرحلة التحقيق الابتدائي.

نظرا للطبيعة الخاصة للجريمة المعلوماتية، وللوسائل الخاصة المستعملة في ارتكابها، فمما لا شك فيه أن هناك صعوبة في الحصول على أدلة المعلوماتية، وذلك نظرا لسهولة محو الأدلة وإتلافها في زمن قصير، ويعتبر الدليل المعلوماتي بأنه "ذلك الدليل المستمد من وسائط ترتبط بتقنية المعلومات، وكلها تدور حول استخدامات الحاسب الآلي وتطبيقاته، وشبكة الإنترنت وغيرها

[1] مقابلة مع النقيب رهام سائد احمد /مدير وحدة الجرائم المعلوماتية /رام الله /16 -4-2017 الساعة 10 صباحا.

من التقنيات الحديثة، ويتعلق بالطبع بالجريمة معلوماتية، إذن فالدليل المعلوماتي يتعلق بجريمة معلوماتية[1]".

حيث جاء في قانون الجرائم الإلكترونية الفلسطيني في نص المادة 38"لا يجوز استبعاد اي دليل ناتج عن وسيلة من وسائل تكنلوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو المعلومات، أو البيانات الإلكترونية ،بسبب طبيعة ذلك الدليل" أي أن القانون الفلسطيني أكد على أن الدليل المعلوماتي يتمتع بنفس حجية الدليل التفليدي طالما توافرت فيه الشروط والخصائص القانونية[2].

فالجرائم التي ترتكب على العمليات الإلكترونية تعتمد في موضوعها على التشفير، والأكواد السرية، والنبضات، والأرقام، والتخزين الإلكتروني، وبالتالي يصعب أن تخلف آثارا مادية يستدل من خلالها على الجريمة، ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة تجعل من الصعب على المحقق تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية[3]. وحتى يتسنى لنا فهم الدليل المعلوماتي لابد من التطرق لعدة مواضيع، ومنها:

أولاً: خصائص قبول الدليل المعلوماتي

يمتاز الدليل الإلكتروني الرقمي في الجريمة المعلوماتية عن الدليل المادي المأخوذ من مسرح الجريمة المعتاد بما يلي:

1. يتكون الدليل الرقمي من بيانات ومعلومات ذات صفة إلكرتونية غير ملموسة، ولاتدرك بالحواس العادية، بل تتطلب الاستعانة بالحاسوب أو الأجهزة الإلكترونية باستخدام برامج خاصة.

2. يعتبر الدليل الرقمي دليلا غير ملموس فهو ليس دليلا ماديا، وإنما هو موجات مغناطيسية أو كهربائية.

---

[1] حجازي، عبد الفتاح بيومي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص709.

[2] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017.

[3] طه، إبراهيم قسم السيد أحمد، الجريمة **المعلوماتية في القانون السوداني**، ط1 ،2016، ص60-61.

3. من خلال الدليل الإلكتروني يمكن رصد المعلومات عن الجاني، وتحليلها لذلك فإن البحث الجنائي قد يجد غايته بسهولة أيسر من التقليدي[1].

4. من خلال البرامج الصحيحة والتطبيقات الضرورية يكون من السهل تحديد ما إذا كان قد تم العبث بالدليل الإلكتروني، أو تعديله وذلك لإمكانيه مقارنته بالأصل.

5. الاتساع العالمي لمسرح الجريمة المعلوماتية، والدليل الرقمي يمكّن مستغلي الدليل من تبادل المعرفة الرقمية بسرعة عالية وبمناطق مختلفة من العالم.

6. امتيازه بالسعة التخزينية العالية، فآلة الفيديو الرقمية يمكنها تخزين مئات الصور، ودسك صغير يمكن تخزين مكتبة صغيرة.[2]

7. الدليل الإلكتروني دليل متنوع بمعنى أنه يشمل كافة أنواع المعطيات التي يمكن تداولها من بيانات أو صور، أو أصوات سمعية، أو نصوص مكنوب، فالعالم الرقمي عالم متطور متجدد لا حدود له.[3]

ثانياً: شروط قبول الدليل المعلوماتي.

وبما أنها أدلة يعتمد عليها القاضي في إصدار أحكامه لا بد من توافر شروط فيها، تجعلها ذات قيمة، ومحل ثقة، وأساسا يعتمد عليه بإصدار تلك الأحكام ومن تلك الشروط:

1. أن تكون هذه الأدلة قد تم الحصول عليها بطريقة شرعية.

أي أن يتم الحصول عليها وفقا للقواعد والضوابط العامة، التي يفرضها القانون وفي إطار مشروعية الأدلة الإلكترونية، نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي

---

[1] الحلبي، خالد عياد، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، مرجع سابق، ص231-233.

[2] موسى، مصطفى محمد، **قواعد وإجراءات البحث الجنائي لكشف غموض الجرائم المعلوماتية والتخطيط لها، الرياض** 2012، ص62.

[3] العبيدي، أسامة بن غانم، **الإثبات بالدليل الالكتروني في الجرائم المعلوماتية**، مرجع سابق، ص58.

نصوص تتعلق بمبدأ الأمانة والنزاهة في البحث عن الحقيقة إلا أن الفقه والقضاء أقرا بهذا المبدأ في مجال التنقيب في جرائم الحاسوب والإنترنت، وكان يستخدم أعضاء الضابطة العدلية طرقا معلوماتية في أعمال التنصت على المحادثات الهاتفية، ويشير رأي الفقه الفرنسي إلى استخدام الوسائل العلمية الحديثة للكشف عن الحقيقة، ولا سيما الأدلة المتحصلة من الحاسوب والإنترنت تحت التحفظ، وهو الحصول على هذه الأدلة بطريقة نزيهة وشرعية، بالإضافة إلى ما نجده في لسويسرا وبلجيكا.[1]

أما في بريطانيا فقامت الشرطة بتركيب جهاز تنصت على خط هاتف إحدى الشاكيات بناء على موافقتها، وقد أجرت الشاكية عدة مكالمات هاتفية مع الشخص معرض الشك، وقد تم تسجيل هذه المكالمات التي تضمنت معلومات تدين المتهم، إلا أن القاضي رفض استخدام هذه التسجيلات كدليل لإدانة المتهم، لأنها تمت من خلال شرك خداعي.

أما في هولندا فإذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية فإنّ ذلك يؤدي إلى استبعاد تلك الأدلة. والعمل على ضرورة محو هذه البيانات، ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في (1981) على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، حيث تناولت محورا يتحدث عن ضرورة أن تكون البيانات مضبوطة بشكل صحيح، وكاملة، ودقيقة، ومستمدة بطرق مشروعة، وعدم افشائها أو استعمالها في غير الأغراض المخصصة لها[2].

---

[1] هلالي، عبد الإله احمد، **حجية المخرجات الكمبيوترية في الإثبات الجنائي**، ط1، دار النهضة العربية، القاهرة، 1977، ص121-122.

[2] الطوالبة، علي الحسن، **مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي**، جامعة العلوم التطبيقية – البحرين- 2009.

3. يجب أن تكون هذه الأدلة يقينية غير قابلة للشك.

يشترط ألا تكون الأدلة المتحصلة من الحاسب الآلي أدلة ظنية، وأن تقترب من الحقيقة قدر الإمكان، ويترتب على ذلك أن تخضع كافة المخرجات الإلكترونية إلى تقدير المحكمة، وأن تقوم المحكمة باستنتاج الحقيقة[1].

ويمكن القول إن النظم القانونية تختلف في موقفها من الأدلة بحسب الاتجاه الذي تتبناه، فهناك اتجاه نظام الأدلة القانونية، الذي يحدد حصرا الأدلة التي يجوز للقاضي الاعتماد عليها بالإثبات، كما يحدد القيمة الإقناعية لكل دليل، ويقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون، فهذا النظام مقيد يحدد من صلاحية القاضي، وهذا النظام ينتمي للدول الانجلوسكسونية، مثل بريطانيا، الولايات المتحدة الأمريكية.

أما الاتجاه الآخر فهو نظام الإثبات الحر: الذي يتمتع القاضي بحرية مطلقة في شأن الوقائع المعروضة عليه، ومدى فعاليتها للإثبات، ففي مثل هذا النظام لا تثار مشكلة الأدلة اليقينية، والظنية، لأن الموضوع يخضع للسلطة التقديرية للقاضي، وهذا ما أخذت به الأنظمة اللاتينية.[2]

ويشترط قانون البوليس والإثبات في بريطانيا لسنة (1984) حتى تتحقق يقينية الأدلة الإلكترونية، أن تكون البيانات دقيقة وناتجة عن الحاسوب بطريقة سليمة، أما في كندا فإن الرأي السائد اعتبار مخرجات الحاسوب من أفضل الأدلة، لأنها تحقق اليقين المنشود في الأحكام الجنائية.

ونصت بعض القوانين في أمريكا على أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد من أفضل الأدلة المتاحة لإثبات هذه البيانات، وتنص القواعد الفيدرالية على أن (الشرط الأساسي للتوثيق أو التحقق من صحة أو صدق الدليل كشرط مسبق لقبوله، هو أن يفي

---

[1] العبيدي، أسامة بن غانم، **الإثبات بالدليل الإلكتروني بالجرائم المعلوماتية**، مرجع سابق، ص 61.

[2] الحلبي، خالد، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، مرجع سابق، ص237-238.

بإمارة أو بينة كافية، لأن تدعم اكتشاف الأمور التي تتسم بالموضوع بما يؤيد الادعاءات أو المطالبة المدعى بها)[1].

4. أن تكون هذه الأدلة قد تمت مناقشتها في المحاكمة الجنائية:

وهذا من المبادئ الأساسية في قانون الإجراءات الجنائية، فلا يجوز للقاضي أن يأخذ بأي دليل يقدمه أي خصم دون عرضه على الخصوم بشكل علني، أو شفهي لمناقشة الشهود هذا الدليل، وبناء عليه يصل القاضي إلى تكوين قناعة بخصوص قيمة الدليل في الإثبات، وقد نص قانون إجراءات جنائية فرنسي في الفقرة (2) من المادة (427) "لا يجوز للقاضي أن يؤسس حكما إلا على أدلة طرحت عليه أثناء المحاكمة، ونوقشت أمامه في مواجهة الأطراف[2]".

ثالثاً: أنواع الأدلة المعلوماتية

يمكن تقسيم الأدلة المادية التي يتم ضبطها والتحفظ عليها، والتي لها قيمة في الإثبات إلى عدة أنواع:

1. الأدلة الورقية: كثير من الجرائم الإلكترونية تترك وراءها قدرا من الأوراق على الرغم من وجود الحاسب الآلي نجد الكثير يقومون بطباعة المعلومات لأغراض المراجعة، والتأكد من الشكل العام للمستند، أو الرسالة، أو الرسومات موضوع الجريمة، وعليه يعتبر الورق من الأدلة التي ينبغي الاهتمام بها في تفتيش مسرح الجريمة، والورق أربعة أنواع:

أوراق تحضيرية: يتم إعدادها بخط اليد كتصور لعملية البرمجة.

أوراق تالفة تتم طباعتها للتأكد، ومن ثم إلقاؤها في سلة القمامة.

أوراق أصلية: تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.

---

[1] الطوالبة، علي حسن، **مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي**، مرجع سابق، ص11.

[2] العبيدي، أسامة بن غانم، **الإثبات في الدليل الإلكتروني في الجرائم المعلوماتية**، مرجع سابق، ص61.

2. جهاز الحاسوب الآلي وملحقاته: يعد وجود حاسب آلي مهم جدا حتى نكون بصدد جريمة معلوماتية، ويمكن للمتخصصين بالجوانب التقنية تحديد نوع الجهاز المرتكب به الجريمة، وتحديد سرعته، وأسلوب التعامل معه حيث أن أجهزة الحاسوب تتفاوت في سرعتها وفي قدرتها على تخزين البيانات والمعلومات واستعادتها وقت الحاجة، فكلما كان جهاز الحاسوب أكثر تطورا استطاع الجاني إتمام جريمته، وقد يكون الجاني شخصا طبيعيا أو معنويا كمؤسسة أو شركة أو هيئة[1].

أما الأجزاء التي تستخدم في تخزين البيانات والمعلومات:

الأقراص المغناطيسية: وتعتبر من أفضل أنواع الوسائط التي تتميز بإمكانياتها وقدراتها التخزينية العالية وسرعة تداول المعلومات التي تخزن عليها.

الأقراص المرنة: وتستخدم لتخزين الملفات التي لا تحتاج إلى سعة كبيرة، وهي قابلة للتلف بشكل أسهل، ويمكن مسح البيانات وإعادة تخزينها مرة أخرى من دون أن يفقد القرص كفاءته.

الأقراص الصلبة: وهي عبارة عن أقراص معدنية مغطاة بمادة ممغنطة، وهي أكثر الأقراص استخداما لكفاءتها وسرعتها العالية.

أقراص الليزر: تبدو أهمية هذه الأقراص في الجرائم المعلوماتية في وجود عدد كبير من هذه الأقراص عامة مع الجهاز الآلي للمتهم، ويفترض بالمحقق الاستعانة بخبير مختص بالحاسب الآلي ليقوم بتفريغ هذه الأقراص، والحصول على الأدلة المتمثلة بالبيانات والمعلومات المفرغة لتقديمها إلى جهات التحقيق.

أقراص الكارتريج: وهي تجمع ما بين إمكانية القرص الصلب بالتخزين وبين إمكانية تغيير القرص المرن من مكانه بقرص آخر[2].

---

[1] البشرى، محمد الأمين، **التحقيق في جرائم الحاسب الآلي والإنترنت**، وزارة الداخلية –أبو ظبي–دولة الإمارات العربية المتحدة، ص362.

[2] البشرى، محمد أمين، **التحقيق في جرائم الحاسب الالي والانترنت**، مرجع سابق، ص362

المودم: الوسيلة التي تمكّن أجهزة الحاسب الآلي من الاتصال ببعضها البعض، وللمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الحاسب الآلي.

الطابعات: وهي أنواع الطابعة الليزرية والملونة، وغير الملونة.

البطاقات: وتستعمل في أجهزة الحاسب الآلي الصغيرة النوت بوك، واللابتوب، وهي في شكل البطاقات الائتمانية.

البرامج اللينة والمراشد: المراشد المصاحبة للحاسب الآلي مفيدة في التعرف على الجهاز والبرامج المستعملة فيه.[1]

كل ذلك يعد أثرا أو جزءا من جسم الجريمة ينبغي البحث عنها، وفحصها، والاستفادة منها بالتحقيق، علما أنّ التعامل مع هذه الآثار يحتاج إلى خبرة فنية في مجال الحاسب الآلي ومعرفة بالقواعد القانونية.

رابعاً: صعوبات تتعلق بالحصول على الدليل المعلوماتي

1. انعدام الآثار التقليدية للجريمة: في معظم الأحيان لا يترك المجرم المعلوماتي آثارا خارجية أو مادية تدل على الجريمة أو مرتكبيها لأنه بكل بساطة هناك عالم افتراضي يعبر عن هذه الجريمة[2].

2. عدم الإبلاغ عن هذه الجرائم للسلطات المختصة بالوقت المناسب: وذلك من تخوف المجني عليه من أن يصبح محفزا لمجرمين آخرين ولاسيما إذا كان هناك ثغرات أمنية في النظام المعلوماتي محل الجريمة[3].

---

[1] هلال، محمد رضوان، **كيفية التعامل التقني والأامن مع أوعية الجريمة الرقمية في مسرح الجريمة لضمان حيادة الدليل المستخلص**، ص46.

[2] العلماء، محمد عبد الرحيم، **جرائم الإنترنت والاحتساب عليها**، مرجع سابق، ص29-30.

[3] وسيلة، بوحية، **صعوبات التحقيق وإثبات الجرائم المعلوماتية**، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، جامعة الإمام محمد بن سعود، ص117.

3. صعوبات تتعلق بالجانب الفني: نقص الخبرة والكفاءة سواء في أجهزة الشرطة أو الادعاء، ولاسيما في الدول التي لاتزال تتعامل مع هذا النوع من الجرائم بالنصوص التقليدية، وتفتقر سلطاتها الضبطية والقضائية للأجهزة التقنية المتطورة في متابعة الجرائم الإلكترونية وضبط أدلتها وبالتالي تكون النتائج سلبية لامحالة[1].

4. سهولة التلاعب في مجريات وبيانات هذه البيئة، وذلك بضغطة زر على الجهاز المعلوماتي، مما يجعل من الصعب على الأجهزة الأمنية ضبط هذه الجريمة واكتشافها.

5. كما أن ارتكاب الجريمة ومسح آثارها لا يتطلب تواجد الجاني في مكان وقوع الجريمة، أو نشوء الضرر.[2]

6. صعوبات تتعلق بإجراءات الحصول على الدليل الرقمي: مما لا شك فيه أن هناك صعوبات تتمثل في إجراءات الحصول على الدليل الرقمي، لأنّ المجرمين الذين يرتكبون هذه الجرائم يتميزون بالذكاء، فهم يضربون سياجا أمنيا على أفعالهم غير المشروعة حتى لا يطالهم العقاب، ويزيدون من صعوبة التفتيش باستخدامهم الكلمات السرية، وشيفرات الدخول بحيث لا تتمكن الجهات المختصة من الوصول إلى البيانات المخزنة، أو المنقولة عبر شبكات الإنترنت، كما قد يلجأ إلى إدخال تعليمات خفية بحيث يستحيل على غيرهم الاضطلاع عليها[3].

---

[1] المطردي، مفتاح بو بكر، **الجريمة الإلكترونية والتغلب على تحدياتها**، المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 2012، ص53-54.

[2] المضحكي، حنان ريحان مبارك، **الجرائم المعلوماتية**، منشورات الحلبي الحقوقية، ص355-357.

[3] القحطاني، عبد الله بن حسين، **تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية**، رسالة ماجستير في قسم العلوم الشرطية، الرياض، ص72.

المبحث الثاني: خصوصية الجرائم المعلوماتية على مستوى التحقيق النهائي

تمثل المحاكمة المرحلة الأخيرة للدعوى العمومية، لذا فهي تعرف باسم التحقيق النهائي، وهي "مجموعة الإجراءات المتخذة بهدف تمحيص جميع أدلة الدعوى سواء كانت لمصلحة المتهم أو ضده، وذلك بهدف استقصاء الحقيقة الواقعية والقانونية المتعلقة بالدعوى ومن ثم الفصل فيها[1]".

وعليه تخضع عملية التحقيق النهائي لمجموعة من القواعد العامة، وهي تختلف عن مرحلة التحقيق الابتدائي، فالهدف من المحاكمة تحري الحقيقة عن طريق الأدلة الحاسمة والقاطعة حتى يمكن الوصول إلى حق الدولة بالعقاب، لذلك تتمتع هذه المرحلة بخصائص أو ضمانات وضعها المشرع، وذلك حتى يثق المشتكي والناس جميعا بعدالة القضاء ومن هذه الخصائص:

علانية جلسات المحاكمة، وشفوية إجراءات المحاكمة، وحضور الخصوم لإجراءات المحاكمة، وتقييد المحكمة بحدود الدعوى، وتدوين إجراءات المحاكمة[2].

وبما أن دراستنا تتمحور حول خصوصية الجرائم المعلوماتية فإن دراسة هذه المرحلة ستركز على قواعد الاختصاص القضائي من جهة، وسلطة القاضي في قبول الدليل الرقمي من جهة أخرى، ولأّن إجراءات المحاكمة في درجات التقاضي المختلفة بالجرائم الإلكترونية هي ذات الإجراءات في الجرائم التقليدية، أي لا تبرز أي خصوصية في هذا الموضوع على مختلف الأصعدة، كان تسليط الضوء في هذه المرحلة على قواعد الاختصاص القضائي المتعلقة بالجرائم المعلوماتية في المطلب الأول، وسلطة القاضي في قبول الأدلة الرقمية في المطلب الثاني.

المطلب الأول: قواعد الاختصاص القضائي المتعلقة بالجرائم المعلوماتية.

يُعرّيف الاختصاص القضائي على أنه "السلطة التي يقررها القانون للقضاء في أن ينظر في دعاوى من نوع معين، حددها المشرّع وفق قواعد وإجراءات معينة"." فالقاضي بداية يلتزم بالفصل في الاختصاص الدولي، أي بمعنى الكشف بداية إذا كان القضاء الوطني هو المختص،

---

[1] الغافري، حسين بن سعيد، **السياسة الجنائية في مواجهة جرائم الإنترنت**، مرجع سابق، ص575.

[2] نمور، محمد سعيد، **أصول الإجراءات الجزائية**، دار الثقافة للنشر والتوزيع،2005، ص459-470.

ثم يبحث في الاختصاص الداخلي. ومن المهم تحديد المحكمة المختصة بالفصل بالنزاع، لأنه يترتب على ذلك تحديد القانون الواجب التطبيق، لذلك لابد من تحديد معيار يتلاءم مع الطبيعة الخاصة للجرائم المعلوماتية.

الفرع الاول: مبدأ الاختصاص الإقليمي

نلاحظ أن اغلب التشريعات تأخذ بمبدأ الإقليمية وتعطيه الأولوية في تطبيق قواعد الاختصاص، وهذا ما أخذ به المشرّع الفرنسي ففي المادة (113) ف (2) (يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية، وتعتبر قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد ارتكب في أو وقع على هذا الإقليم)[1].

وهذا مانصت عليه المادة الثانية من قانون الجرائم الإلكترونية الفلسطيني "تطبق احكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه،إذا ارتكبت كليا، أو جزئيا داخل فلسطين، أو خارجها، أو اذا امتد أثرها داخل فلسطين، سواء كان الفاعل اصليا، أو شريكا، أو متدخلا[2] .

وهذا ما نصت عليه المادة (2) من قانون الجرائم المعلوماتية السوداني لعام (2007) "تطبق أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه إذا ارتكبت كليا أو جزئيا داخل أو خارج السودان، سواء أكان الفاعل أصيلا أو شريكا أو محرضا ..."

ومن خلال هذا النص نلاحظ أن مبدأ الإقليمية ينطبق في حال ارتكاب الجريمة كليا أو جزئيا داخل السودان، وبهذه الحالة ينطبق قانون جرائم المعلوماتية لسنة (2007) دون النظر إلى جنسية الجاني[3]. ونصت المادة (7) من القانون الأردني "تسري أحكام هذا القانون على كل من يرتكب في المملكة جريمة من الجرائم المنصوص عليها فيه"، وهذا يعبر عن اعتناق القانون الأردني لمبدأ الإقليمية، وعليه لا سلطان لقانون العقوبات على الجرائم التي ترتكب خارج إقليم

---

[1] محمد، لموسخ، **تنازع الاختصاص بالجرائم المعلوماتية**، دفتر السياسة والقانون الجزائر، دار المنظومة، عدد2، 2009، ص149.

[2] قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017 .

[3] طه، إبراهيم قسم السيد أحمد، **الجريمة المعلوماتية في القانون السوداني**، مرجع سابق، ص20.

الدولة، كما أنه لا يسمح بتطبيق قانون أجنبي داخل إقليم الدولة، فالقاضي مقيد بتطبيق قوانين وتشريعات بلاده الجزائية، وتحديد مكان الجريمة ليس أمرا سهلا، فهو يختلف اذا ما كانت الجريمة وقتية، أو مستمرة، أو من الجرائم المتتابعة، وكما ذكرنا سابقا يكفي أن يقع أحد العناصر التي تؤلف الجريمة على أرض المملكة حتى تصبح للمملكة الولاية الأصلية[1].

وفي الولايات المتحدة الأمريكية قرر القضاء الأمريكي عام (1999) في جرائم المراهنات والقمار عبر شبكة الإنترنت الاعتماد على مكان ارتكاب الجريمة، وليس مكان وجود الخادم أو المضيف أو المزود. وفي بريطانيا نجد أن القضاء الإنجليزي يكون مختصا وفقا للمادتين (3-4) من قانون إساءة استخدام الحاسب الآلي بنظر الدعوى طالما أن هناك ارتباطا بين الواقعة وبين بريطانيا.

والاتجاه ذاته في القضاء الفرنسي منذ قضية اتحاد الطلبة اليهود ضد (ياهو) فرنسا، حيث اتجه القضاء الفرنسي إلى الإقرار باختصاصه بهذه الدعوى رغم أن (ياهو) فرنسا فرع لمركز رئيسي في الولايات المتحدة الأمريكية[2].

وشهد مفهوم الإقليمية في الآونة الأخيرة تطورا ملحوظا في تفسيره فيما يتعلق بمكان وقوع الجريمة، فلم يعد لازما وقوع فعل مادي أو أحد العناصر المكونة لهذا الفعل، وهكذا اعتبر مجرد قيام مكالمة هاتفية مع شخص في دولة أخرى مبررا لاعتبار الجريمة قد وقعت في إقليم الدولة، وعليه يجب على أية محاولة لصياغة معيار الاختصاص الإقليمي لملاحقة جريمة الكرتونية أن تعكس هذا التوجه[3].

وعليه نقول إن مبدأ الإقليمية يقوم على أساس مكان وقوع الجريمة أو أحد عناصرها مادية وذلك بالمفهوم الضيق لهذا المعيار

---

[1] الحلبي، محمد علي السالم، **شرح قانون العقوبات**، مكتبة دار الثقافة للنشر والتوزيع، ص57-58.

[2] الغافري، حسين بن سعيد، **السياسة الجنائية في مواجهة جرائم الإنترنت**، مرجع سابق، ص579-581.

[3] المقصودي، محمد بن أحمد بن علي، **الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيا**، مرجع سابق، ص28-29.

وهذا المبدأ أو المعيار لا يتناسب مع الطبيعة الخاصة للجريمة المعلوماتية، وذلك لطبيعتها غير المحسوسة من جهة، ولصعوبة تحديد مكان الجريمة وزمانها من جهة أخرى، فالتقدم العلمي، وتطور وسائل الاتصالات أصبح من الضروري معها الخروج عن مبدأ الإقليمية، لأنه لم يعد هو المعيار الوحيد، بل على العكس تراجعت أهميته، وزادت أهمية معايير أخرى كانت تعتبر احتياطية مثل معيار العينية، ومعيار العالمية.

الفرع الثاني: الاختصاص الشخصي

يعني هذا المبدأ "ملاحقة الجاني حامل الجنسية للدولة المعنية حال ارتكابه فعلا في الخارج يشكل جريمة حال عودته للوطن "وهذا ما نصتت عليه المادة (7) من القانون الجنائي السوداني لسنة (1991) وينطبق مبدأ شخصية القانون الجنائي على الجرائم المنصوص عليها في قانون الجرائم المعلوماتية (2007) [1].

وقد تم الإقرار بهذا المبدأ وذلك تخوفا من وجود ثغرات في مبدأ الإقليمية، فمن الممكن أن يهرب المواطن من البلد التي ارتكب فعله الإجرامي بها، وهذا ما ورد في المادة(3) من القانون المصري (كل مصري ارتكب وهو خارج القطر فعلا يعتبر جناية أو جنحة في هذا القانون يعاقب بمقتضى أحكامه إذا عاد إلى القطر وكان الفعل معاقبا عليه بمقتضى قانون البلد الذي ارتكب فيه)، وبالتالي حتى نكون بصدد تطبيق مبدأ الشخصية يجب أن يكون المواطن مصريا وقد هرب من بلده، وأن يكون الفعل معاقبا عليه وفقا لقانون البلد الذي ارتكبت به الجريمة[2] .

ويعلل هذا المبدأ بأن الدولة يجب عليها أن تضمن حسن سلوك رعاياها بالخارج، وقد أخذت التشريعات بهذا المبدأ، وذلك لأن الدولة عادة لا تقوم بتسليم رعاياها للدول الأخرى، إنما تقوم بمعاقبتهم بدلا من تسليمهم، وقد أخذ القانون الأردني بهذا المبدأ بحيث تطال أحكام قانون العقوبات

[1] طه، إبراهيم قسم السيد محمد، **الجريمة المعلوماتية في القانون السوداني**، مرجع سابق، ص25.

[2] - http://www.f-law.net/law/threads/19941

كل أردني ارتكب جريمته، سواء كانت جناية أو جنحة بالخارج، ويستوي في ذلك أن يكون فاعلا أومتدخلا أو محرضا أو شريكا، بشرط أن يكون هذا الفعل مُجرّما في القانون الأردني[1].

كما ونلاحظ أن المشرع الفرنسي أخذ بهذا المبدأ في شقيه الإيجابي والسلبي، ونفس الاتجاه أخذته الولايات المتحدة الأمريكية، ففي إحدى القضايا قضت المحكمة العليا لولاية نيويورك بتطبيق مبدأ الاختصاص الشخصي في جريمة انتهاك قانون المستهلك والدعاية الكاذبة، حول بيع مجلات عبر البريد الإلكتروني[2].

إنّ هذا المبدأ قد تشوبه عدة إشكاليات بحيث أن تطبيق القانون الوطني على الجرائم الواقعة بالخارج من شأنه أن يمس بمبدأ أساسي وهو عدم جواز معاقبة الشخص عن الفعل الواحد مرتين، هذا من جهة، ومن جهة أخرى قد يضطر المتضرر التنقل إلى الدولة حيث ارتكب الفعل لرفع دعوى مدنية، فلذلك لابد من وجود قانون جنائي دولي لحل الإشكالية[3].

وهذا المبدأ يعتمد بصفة أساسية على الجاني من حيث جنسيته وهويته، كما أن محاكمة المجرم في بلد أجنبي تحتاج إلى إجراءات طويلة ومعقدة، وتكاليف مرتفعة، ومعرفة هوية الفاعل في الجرائم الإلكترونية غالبا ما يكون عسيرا، فهو غالبا ما يستعمل التشفير والألغاز المعقدة وأسماء مستعارة،

الفرع الثالث: الاختصاص العيني

ويقصد بهذا المبدأ تطبيق القانون الجنائي للدولة بغض النظر عن جنسية مرتكبيها إذا كانت تمس بسيادة الدولة، لأن كل دولة تحرص على حماية مصالحها، وحماية نظامها القضائي والتشريعي من خلال خضوع الجرائم التي تمسها لقضائها الوطني، حيث أنها لا تثق بأي دولة

[1] الحلبي، محمد علي السالم، **شرح قانون العقوبات**، مرجع سابق، ص73-75.

[2] الغافري، حسين بن سعيد، **السياسة الجنائية في مواجهة جرائم الإنترنت**، مرجع سابق، ص582.

[3] محمد لموسخ، **تنازع الاختصاص بالجرائم المعلوماتية**، مرجع سابق، ص149.

للعقاب عليها، ومن الجدير ذكره أن معيار العينية عادة لا تعطيه التشريعات الجنائية الأولوية، وإنما تلجأ إليه لتكملة مبدأ الشخصية والإقليمية.

هناك بعض الجرائم الخطيرة التي تمس أمن الدولة، وتهدف إلى الإضرار بمؤسساتها العسكرية، والاقتصادية، والسياسية، لأن الجريمة إذا ما ارتكبت بالخارج فقد لا يجرّمها قانون الدولة التي وقع الجرم على إقليمها، وأنّ الاستثناء الوارد على مثل هذه الجرائم نظرا لخطورتها، لأنها تهدد كيان الدولة ومصالحها الجوهرية ومكانتها، وهذا ما نصت عليه المادة (9) من القانون الأردني بحيث أن القانون الأردني ذكر الجرائم على سبيل الحصر:

1. الجرائم التي تقع على أمن الدولة الداخلي والخارجي كجرائم الخيانة وحمل السلاح.

2. جريمة تقليد ختم الدولة، تقليد إمضاء جلالة الملك، أو استعمل دون حق ختم دولة، أو قلد دمغة ختمها أو قلد ختما أو ميسما أو علامة أو مطرقة خاصة بإدارة عامة أردنية.

3. جريمة تزوير أوراق النقد الأردنية.[1]

وهذا المبدأ قد يتناسب مع طبيعة الجريمة المعلوماتية ولاسيما إذا كانت الجريمة المرتكبة تؤثر على سيادة الدولة وكيانها، إلا انه نلاحظ أن عددا لا بأس به من التشريعات ذكرت الجرائم التي يشمها مبدأ العينية، إلا أنه بمفهومه الواسع نلاحظ أنه يتناسب مع الجرائم المعلوماتية ومع طبيعتها باعتبارها جرائم عابرة للحدود.

[1] الحلبي، محمد علي السالم، **شرح قانون العقوبات**، مرجع سابق، ص69-71.

الفرع الرابع: الاختصاص العالمي

وهذا المبدأ يعطي قانون العقوبات مجالا واسعا ليشمل العالم كله، فلا يتقيد بمكان ارتكاب الجريمة، أو أحد سلوكياتها، ولا جنسية الفاعل أو الجاني، ولا بطبيعة الجريمة ولا مساسها بسيادة الدولة[1].

نلاحظ أن معظم التشريعات أخذت بهذا المبدأ بصفة تبعية، وأن هذا المبدأ يتعارض مع طبيعة قانون العقوبات، لأنه بالأصل هو قانون إقليمي، وهو ليس بعالمي فهو مبدأ احتياطي ثانوي لا يمارس إلا إذا تعذر معاقبة المجرم بدون اللجوء إليه[2].

ولا شك أن مبدأ العالمية الملائم لمعظم الجرائم المعلوماتية التي يتوزع بها نشاط المجرم لأكثر من دولة، لأن الشبكة المعلوماتية لا تستأثر بها دولة معينة، بحيث يستطيع مستخدموها ولوجها من أي موقع بالعالم من خلال حاسوب يكون متصلا بها.

ومن خلال عرض معايير الاختصاص القضائي المتبعة في معظم دول العالم والتي تتناسب بشكل عام مع الجرائم التقليدية[3] ولاسيما أن معظم التشريعات أعطت الأولوية لمبدأ الإقليمية، وذلك نظرا لطبيعة قانون العقوبات، والسؤال هنا: هل هذه الأولوية تتناسب مع الطبيعة الخاصة للجرائم المعلوماتية؟

إنّ من أهم ما يثيره موضوع الجرائم المعلوماتية أن شبكة الإنترنت ليس لها مقر في دولة معينة، ولاتخص شخصا محددا فهي بالتالي لا تخضع لرقابة أو سيطرة دولة معينة، لأنها تجمع لعدد كبير من الشبكات مختلفة المصدر والوظيفة، ولا يوجد قانون جنائي موحد يربطها، أي أن قواعد الإباحة والتجريم تتعدد بتعدد الدول التي ترتبط بهذه الجريمة وهنا تكمن المشكلة[4].

---

[1] محمد، لموسخ، **تنازع الاختصاص بالجرائم المعلوماتية**، مرجع سابق، ص150.

[2] الحلبي، محمد علي السالم، **شرح قانون العقوبات**، مرجع سابق، ص 79.

[3] بن باردة، عبد الحليم، **إجراءات البحث والتحري عن الجريمة المعلوماتية**، مرجع سابق، ص92.

[4] الغافري، حسين بن سعيد، **السياسة الجنائية في مواجهة جرائم الإنترنت**، مرجع سابق، ص576.

وهنا نسأل: كيف يمكن تحديد إقليم الدولة التي وقعت عليه هذه الجرائم بتنوعها وتحددها وتعقيدها؟ إن الإجابة على هذا السؤال يترتب عليها ابتداء الخروج عن مبدأ الإقليمية، وذلك نظرا للتطور الهائل في وسائل الاتصال الحديثة وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية، أو على الأقل إعادة النظر في ترتيب تلك المعايير بحيث يصبح لمعيار العينية أو الدولية الأولوية على مبدأ الإقليمية.

وعليه فإن الدولة التي تقع في إقليمها الجريمة أو الجزء الأكبر من النشاط المادي أو الدولة التي توجد في إقليمها متحصلات الجريمة تبدو أكثر الدول اختصاصا بملاحقة الجريمة ومحاكمة فاعلها[1].

ومما يجدر الإشارة إليه أنه إذا توافر بالقضية الواحدة عنصر دولي (الاتجاه الموسع) فإن القاعدة تقتضي باختصاص أكثر من دولة بنظر الدعوى، وبناء عليه قضت محكمة العدل الأوروبية في قضية زراعي العنب الهولنديين الذين أضروا في مزارعهم بسبب تلوث مياه نهر الراين الذي سببه أحد مشروعات المناجم في فرنسا باختصاص محكمة وقوع الضرر في هولندا، وباختصاص المحكمة الفرنسية وهي محكمة الفعل الضار.

وتطبيقا لذلك أيضا حكمت المحكمة الابتدائية بباريس باختصاص المحاكم الفرنسية، وبالتالي تطبيق القانون الفرنسي إذا كان مركز البث موجودا في خارج الإقليم الفرنسي، وبناء عليه إذا كان الجهاز الخادم موجودا في أمريكا بينما تظهر الرسائل التي يقوم ببثها هذا الجهاز بفرنسا، فإن المحكمة الفرنسية ينعقد لها اختصاص، وتعتبر الجريمة مرتكبة في كل مكان تظهر فيها الرسائل المؤثمة محل البث[2].

أما قانون العقوبات بدولة الإمارات العربية المتحدة فيأخذ بمبدأ العالمية في بعض الجرائم، وقد جاء في المادة (21) منه "يطبق مبدأ العالمية على الجرائم التالية:

---

[1] المطردي، مفتاح بو بكر، **الجريمة الإلكترونية والتغلب على تحدياتها**، مرجع سابق، ص 24-25.

[2] محمد عطا الله، شيماء عبد الغنى، **الحماية الجنائية للتعاملات الإلكترونية**، مرجع سابق، ص370-371.

-جريمة تخريب أو تعطيل وسائل الاتصال الدولية، ويقصد بذلك جرائم خطف الطائرات.

-جرائم الإرهاب الدولي.

- جرائم القرصنة.

- جريمة الإتجار بالرقيق الأبيض في حالة الدعارة.

- جرائم الإتجار بالصغار أو الرقيق.

وبناء عليه فإن تطبيق قواعد الاختصاص التقليدية لا تتناسب مع الجريمة الإلكترونية، لأن هذا الصنف من الجرائم يتطلب تجاوز المعايير التقليدية، سواء كان على مستوى التجريم والعقاب، أو على مستوى التتبع والملاحقة، فهذه الجرائم لا تعترف بالحدود الجغرافية والسياسية للدول، ولا بسيادتها، حيث أصبح الفضاء الإلكتروني هو الذي يحكم هذه الجرائم، فقواعد الاختصاص التقليدية وجدت لتنظم الجرائم القابلة للتحديد المكاني، وبالتالي لاينيغي إعمالها بالجريمة الإلكترونية فحتى المعايير التي تضمنتها اتفاقية بودابست والمتعلقة بالجريمة الإلكترونية باعتبارها الإطار القانوني أو المرجع الدولي عندما يتعلق الأمر بالجريمة المعلوماتية لم تستطع إيجاد حل لمشكلة الاختصاص القضائي باعتبارها نصت على معايير تقليدية بالمقارنة بطبيعة الجريمة الإلكترونية[1].

المطلب الثاني: سلطة القاضي في قبول الأدلة الرقمية

وبما أن القاضي من له الحق في وزن البينة، وإصدار الأحكام لابد من تتمتع الدليل المعلوماتي بحجية أمام القاضي، وفيما يلي بيان ذلك:

أولا: حجية الدليل الإلكتروني أمام القضاء الجنائي

يعد مبدأ حرية الإثبات من المسائل المتفق عليها في عملية الإثبات الجزائي، ويعني ذلك أن يلجأ الأطراف إلى كافة طرق الإثبات، للتدليل على صحة ما يدعونه وهذا ما نصت عليه المادة

[1] قجاج، يوسف، **اشكالية الاختصاص في الجريمة الالكترونية**، http://www.hespress.com/opinions/256777.html

(237) من قانون الإجراءات الجزائية الفلسطيني "تحكم المحكمة بالدعوى حسب قناعتها التي تكونت لديها بكامل حريتها[1] ....."

إن حجية المخرجات المتحصلة من الحاسوب هي قيمة ما يتمتع به المخرج المتحصل من الكمبيوتر بأنواعه المختلفة الورقية، والالكترونية، والمصغرات الفيلمية، من قوة استدلالية في كشف الحقيقة[2].

إن الطبيعة الفنية الخاصة بالدليل الإلكتروني تجعل من العبث بمحتوياته موضوعا في غاية السهولة دون أن يكون في مقدور الشخص غير المتخصص أن يكتشف الحقيقة، وفضلا عن ذلك إن نسبة الخطأ في الحصول على دليل ذي مصداقية تبدو عالية في هذا النوع من الأدلة.

كما أإن السلطة التقديرية للقاضي في تقدير الدليل الجنائي فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الإلكتروني، حيث يشكك في سلامة الدليل الإلكتروني من ناحيتين:

الأولى: الدليل الإلكتروني من الممكن خضوعه للعبث للخروج به على نحو يخالف الحقيقة.

الثانية: وجود خطأ فني في الحصول على الدليل الإلكتروني، كالخطأ في استخدام الأداة المناسبة في الحصول على الدليل، ويرجع ذلك للخلل في الشيفرة المستخدمة، أو الخطأ في استخلاص الدليل بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية[3].

---

[1] عريقات سهى إبراهيم، **الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي**، جامعة القدس، ص32.

[2] محمد معمر علي إبراهيم، **الدليل الإلكتروني وحجيته في الإثبات الجنائي**، شركة مطابع السودان للحملة المحدودة، 2015، ص95.

[3] الحلبي، خالد عياد، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، مرجع سابق، ص 247-248.

كما أكد المشرع السعودي على حجية الأدلة الإلكترونية، والمستخلصات الإلكترونية بنصه على أن تكون للتعاملات والسجلات والتوقيعات الإلكترونية حجتها الملزمة، ولايجوز نفي حجتها أو قابليتها للتنفيذ ولأمنع تنفيذها بحجة أنها تمت بشكل الكرتوني[1].

السؤال هنا ما القوة الإثباتية لكل من التسجيلات الصوتية والتوقيع الإلكتروني؟

التسجيلات الصوتية: إن الصوت عند تسجيله إلكترونيا لا يحتمل الخطأ ويصعب التلاعب به، ويمكن كشف هذا الخداع بوسائل تقنية عالية الكفاءة، وبالنسبة للتسجيل الصوتي الممغنط تكون له حجة دامغة في الإثبات، ويشترط الفقه لمشروعية الدليل المستمد من المراقبة والتسجيل ما يلي:

1. إذا لم يكن الدليل ينطوي على حق يحميه القانون فيكون مشروعا ويمكن للمحكمة أن تستند إليه

2. تحديد دقيق لشخصية الشخص المراد تسجيل أحاديثه.

3. تحديد نوع الحديث المراد التقاطه والجريمة المتعلق بها، والجهة المصرح لها بذلك والمدة الجائز خلالها التقاط الحديث[2].

أما بالنسبة للبريد الإلكتروني عند إرسال أي شخص رسالة، فإنه يكون لدى الشخص المستقبل توقيعا رقميا، ويكون المستقبل وحده القادر على استعماله، ويمكن لهذه الرسالة أن يكون أي نوع فيديو تحويلات بنكية، وصوت، ويستخدم التوقيع الإلكتروني في تأمين المعلومات من خلال إدخال أختام توقيت الإرسال في الرسائل المشفرة، فإذا ما حاول شخص ما أن يزور أو يلفق فسيكون هذا التلفيق قابلا للكشف[3].

والحقيقة دائما ما تحتاج إلى دليل، وبتطور هذه الحقيقة يتطور الدليل، ويجب أن يشمل هذا التطور جميع عناصر التحقيق من محققين إلى خبراء إلى وسائل تقنية وفنية وغيرها، والدليل

---

[1] العبيدي، أسامة بن غانم، **الإثبات بالدليل الإلكتروني بالجرائم المعلوماتية**، مرجع سابق، ص76.

[2] الهلالي عبد الله أحمد، **حجية المخرجات الكمبيوترية**، مرجع سابق، ص 64-66.

[3] الطوالبة، علي حسن، مشروعية **الدليل الإلكتروني المستمد من التفتيش الجنائي**، مرجع سابق.

الإلكتروني يصلح لأن يكون دليل إثبات لا يستهان به، وذلك نظرا للثورة المعلوماتية التي تجتاح العالم، فأصبحت مخرجات الحاسب الآلي تتمتع بالثقة والكفاءة ولاسيما بالآونة الأخيرة.

وكما ذكرنات سابقا إن موضوع تقدير حجية المخرجات يرجع إلى اختلاف أنظمة الإثبات في تقديرها، ففي النظام اللاتيني (الأردني ،الفرنسي ،المصري ،السوري ،اللبناني) لا تثير حجية الدليل الإلكتروني صعوبات، وذلك بسبب السلطة الممنوحة للقاضي بتقدير هذه الأدلة، وكذلك الحال في فرنسا، وقد قضت محكمة النقض الفرنسية (أن أشرطة التسجيل الممغنطة التي تكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي)، وكذلك الحال بالنسبة لألمانيا، وتركيا، ولوكسمبورغ، واليونان، والبرازيل، بحيث تخضع المخرجات الإلكترونية لحرية القاضي بالاقتناع.

كما أخذ المشرّع السعودي بحجية الدليل الإلكتروني في الإثبات، فقد نص نظام التعاملات الإلكترونية السعودي في المادة (2) على أن أهداف هذا النظام "إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص، بواسطة سجلات إلكترونية يعول عليها " واستخدام المشرّع السعودي كلمة يعول عليها يعني أن لها مطلق الحجية.

أما النظم الإنجلوسكسونية فالمشرّع هو الذي يحدد القيمة الاقناعية للأدلة، وعلى رأسها بريطانيا، وفي كندا يمكن قبول السجلات الناجمة عن الحاسوب إذا توافرت شروط معينة، فقد قضت محكمة استئناف أونتاريو الكندية بأنه يشترط لكي تكون سجلات الحاسوب مقبولة أن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية، كما يتضمن وصفا للإجراءات والعمليات المتعلقة بإدخال البيانات واسترجاعها حتى يتبينا أن المخرج الصادر من الحاسوب موثوق به.

ونلاحظ أن القانون الإنجليزي يتوسع في العمل بقاعدة استبعاد الدليل الجزائي التي تم الحصول عليه بطريق غير مشروع، ومن السوابق القضائية في هذا الخصوص استبعاد أو رفض

المحاكم الإنجليزية قبول اعتراف تم الحصول عليه مع عدم احترام قاعدة إعادة تلاوة الأقوال للتغلب على أي خطأ يكون قد وقع من جانب الشرطة، وكذلك عدم احترام حق الاستعانة بمدافع لكي يقنع متهما صامتا في الحديث أو عدم احترام القواعد المقررة عند ارتكاب مخالفة مرورية، أيضا الغاء الاعتراف الذي تم الحصول عليه بموجب إجراء غير نزيه[1].

أما القوانين ذات النظام المختلط التي تجمع بين النظام اللاتيني والنظام الانجلوسكسوني فيحدد القانون فيها أدلة معينة لبعض الوقائع، أو توضع للدليل شروط في بعض الأحوال، ويترك للقاضي حرية التقدير في أحوال أخرى مثل القانون الياباني حيث حصر المشرّع الياباني طرق الإثبات بما يأتي "أقوال المتهم، وأقوال الشهود، والقرائن، والخبرة)، واستبعد أن تكون السجلات الإلكترومغناطيسية دليلا يستخدم بالمحكمة إلا إذا تم تحويلها لصورة مرئية[2].

أما بالنسبة للمشرّع الفلسطيني فقد حرض على ضرورة الأخذ بحجية الدليل الإلكتروني أمام القضاء الجنائي من خلال قانون مكافحة الجرائم الإلكترونية، وقد أكد المشرّع بأنه سيتيح استخدام الوسائل والسندات والسجلات الإلكترونية كحجية مقبولة أمام القضاء وهو ما سيسهل إثبات حق الطرف الذي يرغب بالاحتجاج بها وهذا ماجاء بنص المادة 38"لايجوز استبعاد اي دليل ناتج عن وسيلة من وسائل تكنلوجيا المعلومات ،أو أنظمة المعلومات ،أو شبكات المعلومات ،أو المواقع الإلكترونية ،أو البيانات والمعلومات الإلكترونية ،بسبب طبيعة ذلك الدليل[3].

وعلى الرغم من اختلاف مدارس نظام الإثبات إلا أنه هناك ضوابط معينة تحكم الأدلة الناتجة عن الحاسب الآلي، وبشكل عام يلتزم بها القضاء لدعم وحماية حقوق الأطراف، ومن هذه الضوابط أصل البراءة، وما يتفرع من هذا المبدأ من آثار ونتائج ، حيث يجب توافر شروط معينة بالمخرجات الإلكترونية حتى يتم دحض قرينة البراءة، وافتراض عكسها فيجب أن يصل القاضي إلى حد اليقين والجزم، وإذا كانت هذه المخرجات الإلكترونية السابق ذكرها تصل الجرم بالمتهم كان

---

[1] البلوشي، راشد بن حمد، **الدليل في الجريمة المعلوماتية**، مرجع سابق، ص38.

[2] محمد، معمر علي إبراهيم، **الدليل الإالكتروني وحجيته في الإثبات الجنائي**، مرجع سابق، ص98-99.

[3] قانون الجرائم الإلكترونية الفلسطيني ررقم 16 لسنة 2017.

على القاضي أن يحكم بالبراءة، كما أنه يجب أن تكون هذه المخرجات الإلكترونية قد طرحت بالجلسة بناء على تحقيقات قد تمت بالطرق القانونية، فلا يستطيع القاضي أن يحكم بناء على علمه الشخصي، وعليه فإن مجمل شروط قبول المخرجات الإلكترونية تتحقق باليقينية والشفوية والمشروعية[1]. ومن أمثلة الطرق غير المشروعة التي قد تستخدم ضد المتهم استخدام وسائل الإكراه مثل حمله على فك الشفرة للنظام المعلوماتي المحمي، أو إنهاك قواه، وذلك من أجل أن يعطي معلومات حول قاعدة بيانات معينة فالمادة (78) من قانون الإثبات الجنائي الإنجليزي تخول المحكمة استبعاد الدليل الإلكتروني إذا ثبت أنه يتعارض مع عدالة إجراءات الدعوى[2].

وبناء عليه نلاحظ نظرا لطبيعة الجريمة المعلوماتية فإن وسائل الإثبات فيها تكون من خلال القرائن والخبرة، وهو ما يزيد من أهمية الدليل العلمي في الإثبات الجنائي كما ويزيد من أهمية دور القاضي من خلال السلطة التقديرية التي يتمتع بها القاضي لتقدير الأدلة حيث أنه لا يمكن تفسير الحقيقة العلمية للدليل الرقمي إلا من خلال الاستعانة بخبراء بالنظام المعلوماتي، وذلك حتى يمكن تقديم دليل علمي تقبل به المحكمة[3].

ثانياً: حجية الدليل الإلكتروني في بعض الدول

لم تتفق التشريعات على مسألة الإثبات بالجرائم المعلوماتية فمنها من أوجد قوانين خاصة لقبول الأدلة الرقمية، ومنها من اكتفى بالقوانين التقليدية، ونلاحظ أن المشرع التونسي أصدر في تونس قانون التجارة والمعاملات الإلكترونية الذي اعترف للمستندات الإلكترونية بحجتها في الإثبات ،كما أصدرت إمارة دبي قانون التجارة الإلكترونية سنة (2002) وتبعها المشرع المصري (2004) الذي أصدر قانون نظم التوقيع الإلكتروني، كما أن القانون العربي النموذجي وكل هذه القوانين أعطت للمستند الإلكتروني ذات الحجية التي يتمتع بها المحرر الورقي، كما أن قانون المعاملات الإلكترونية السوداني لسنة (2007) نص في الفصل الثالث على حجية المستندات الإلكترونية في

---

[1] البلوشي، راشد بن حمد، **الدليل في الجريمة المعلوماتية**، مجلة الحقوق للبحوث القانونية، مجلد1،2008، ص27 26.

[2] العبيدي، أسامة بن غانم، **الإثبات بالدليل االكتروني في الجرائم المعلوماتية**، مرجع سابق، ص 74-76.

[3] البقمي ناصر بن محمد، **أهمية الأدلة الرقمية في الإثبات الجنائي، مجلة الفكر الشرطي**، مجلد21 عدد80، 2012، ص43-44.

المادة(7) تكون لرسالة البيانات .....الحجة القانونية المقررة للمستند الرسمي متى صدرت بتوقيع رقمي معتمد[1] ".

أما بالنسبة للمشرع الفلسطيني في قانون المبادلات والتجارة الإلكتروني أجاز استخدام السند الإلكتروني، ومنحه نفس الأثر القانوني للسند الكتابي، وإن لم يكن نصا خاصا بذلك إلا أنه تم الإشارة بالمادة (5) حيث نصت على "ينطبق على العقود الإلكترونية ما ينطبق على العقود الكتابية من حيث التعبير عن الإرادة وأثرها القانوني وصحتها وقابليتها للتنفيذ[2] ...."

وفي الولايات المتحدة الأمريكية أقر المشرّع الأمريكي بالحجية للدليل الإلكتروني، ونصت التشريعات للعديد من الولايات على ذلك، حيث نص قانون الإثبات الصادر عن ولاية نيويورك على إن النسخ المستخرجة من البيانات والمعلومات التي يحتويها الحاسب الآلي تكون مقبولة في الإثبات[3].

أما قانون الإجراءات الفيدرالي في القاعدة (1001) بند (3) أقرت بقبول الدليل الإلكتروني باعتباره سندا أصليا ما دام أن البيانات الصادرة من الكمبيوتر، أو جهاز مماثل وسواء كانت هذه البيانات مطبوعة أو مسجلة على دعامات أخرى ومقروءة للعين المجردة وتعبر عن البيانات الأصلية بشكل دقيق[4].

والمشرع السعودي أخذ بحجية الدليل الإلكتروني بالإثبات فقد نص نظام التعاملات الإلكترونية على أنه يكون للتعاملات والسجلات والتوقيعات الإلكترونية حجيتها الملزمة، ولا يجوز نفي صحتها أو قابليتها للتنفيذ، ولا منع تنفيذها بسبب أنها تمت كليا أو جزئيا بشكل إلكتروني، كما

---

[1] طه، إبراهيم قسم السيد، **الجريمة المعلوماتية في القانون السوداني**، ط1، 2016، ص59.

[2] سده، إياد محمد عارف، **مدى حجية المحررات الالكترونية في الاثبات**، رسالة ماجستير، جامعة النجاح الوطنية،2009، ص136.

[3] العبيدي، أسامة بن غانم، **الاثبات بالدليل الالكتروني في الجرائم المعلوماتية**، مرجع سابق، ص75.

[4] عطا الله، شيماء عبد الغني، **الحماية الجنائية للتعاملات الإلكترونية**، مرجع سابق، ص388.

ونص المشرع السعودي على أن التعامل والتوقيع الإلكتروني والسجل الإلكتروني حجة يعتد بها بالتعاملات[1].

ويلاحظ أن الدليل الرقمي أصبح ظاهرة جديدة في الإثبات الجنائي لابد من أخذها بعين الاعتبار، لأن القواعد الإجرائية التقليدية لم تعد تكفي لحل المشكلات المتعلقة بالدليل الرقمي وغيره من المشكلات الإجرائية التي تحدثنا عنها سابقا، ومن خلال عرض موقف بعض التشريعات من الدليل الرقمي فقد عمدت كثير من الدول تشجيع البحث العلمي، وابتكار وسائل علمية جديدة تساعد في كشف الغموض عن هذه الجرائم، وفي الحصول على أدلة تساعد الجهاز القضائي على وضع ثقته في هذه الأدلة، بالإضافة طبعا إلى الاستعانة بخبراء مختصين من شأنهم تحديد مدى صحة الدليل من عدمه .

[1] العبيدي أسامة بن غانم، **الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية**، مرجع سابق، ص78.

الخاتمة

نالت الجريمة المعلوماتية أهمية كبيرة لدى المشّرعين، فهي موضوع العصر في القانون الدولي والإقليمي، حيث كان لهذا البحث أهمية كبيرة في تسليط الضوء على بعض الجرائم المعلوماتية، وكذلك إجراءات التحقيق بشقيه الابتدائي والنهائي، لذلك تعتبر هذه الدراسة بمثابة تقييم للنصوص القانونية التقليدية المطبقة على الجرائم المعلوماتية ذات الطبيعة الخاصة، وفيما يلي عرض لأهم النتائج والتوصيات التي توصل إليها الباحث:

أولاً: النتائج

1. إن الجرائم المعلوماتية أصبحت تمثل أهمية كبرى بالمجتمع وخصوصا بعد ظهور أنماط جديدة منها، بالإضافة إلى أن هناك أنماطا شائعة إلا أنها تتمتع بخصوصية ومن أبرزها جريمة الدخول الإلكتروني، وجريمة إتلاف البيانات الإلكترونية، وجريمة التزوير.

2. تثير الجرائم المعلوماتية الكثير من الصعوبات في مجال الحصول على الأدلة الجنائية، فالمحقق اعتاد على كون محل الجريمة شيء مادي وملموس، على عكس البيئة المعلوماتية ذات الطبيعة المعنوية التي يصعب معها تطبيق إجراءات ووسائل الإثبات التقليدية.

3. يتسم التحقيق بالجرائم المعلوماتية بصعوبة وتعقيد بالغين، وذلك لعدم إلمام رجال الشرطة والمحققين بمجالات الحاسب الآلي والإنترنت، وعدم تدريبهم على آليات الوصول إلى الأدلة المعلوماتية والحفاظ عليها من التلف والضياع.

4. يوجد قصور في القواعد والتشريعات الإجرائية الواجب اتباعها في مرحلة التحقيق الابتدائي ومرحلة المحاكمة.

5. ضعف قدرة القاضي على التقدير أو ما يسمى القناعة الوجدانية للقاضي لأن ثقافته القانونية لا تسعفه على إدراك أو استنتاج الحقائق المتعلقة بأصالة الدليل الإلكتروني.

ثانياً: التوصيات

1. ضرورة قيام المشرعين في الدول المختلفة بإصدار تشريعات خاصة بالجرائم المتعلقة بالحاسب الآلي، وتطوير قواعد الإجراءات الجنائية وقواعد الإثبات وذلك لأنها ذات طبيعة خاصة.

2. ضرورة تشديد العقوبات والغرامات في حال ارتكاب أي من الجرائم المعلوماتية، وكذلك المساواة بين الجريمة العمدية وغير العمدية.

3. عقد اتفاقات دولية ثنائية وذلك من أجل تسليم المجرمين المعلوماتيين.

4. ضرورة تأهيل رجال الشرطة والمحققين تأهيلا يستطيع معه كل منهم التعامل مع هذا النوع من الجرائم.

5. ضرورة تأهيل القضاة وتدريبهم حتى يستطيعوا التعامل مع الأدلة الرقمية الناتجة عن الجريمة المعلوماتية وبالتالي يصبح حكمهم أكثر عدالة.

قائمة المصادر والمراجع

أولا: المصادر

1. قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001

2. قانون العقوبات الأردني لسنة 16 سنة 1960

3. قانون المعاملات الإلكترونية السوداني لسنة 2007

4. قانون المبادلات والتجارة الإلكترونية الفلسطيني لسنة 2016

5. نظام التعاملات الإلكترونية السعودي 1428هـ

6. القانون الجنائي السوداني 1991

7. قانون العقوبات لدولة الإمارات العربية 1978

8. قانون مكافحة الجرائم المعلوماتية الإماراتي 2012

9. قانون مكافحة الجرائم المعلوماتية القطري رقم 14 لسنة 2014

10. قانون مكافحة الجرائم المعلوماتية العماني 2011

ثانيا: المراجع

1. ابراهيم، خالد ممدوح، **الجرائم لمعلوماتية**، دار الفكر الجامعي، ط1، 2009.

2. البشرى، محمد الامين، **التحقيق في جرائم الحاسب الآلي والانترنت**، وزارة الداخلية، أبو ظبي، دولة الإمارات العربية المتحدة.

3. البقمي ناصر بن محمد، ***اهمية الأدلة الرقمية في الإثبات الجنائي***، **مجلة الفكر الشرطي**، مجلد21 عدد80، 2012.

4. البقمي، ناصر بن محمد، **مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية**، مركز الإمارات للدراسات والبحوث الاستراتيجية، سلسلة محاضرات الإمارات 116.

5. بكار، الحسن، ***الطبيعة القانونية للجريمة المعلوماتية***، دار المنظومة، **مجلة الملف**، المغرب، عدد17، 2010.

6. البلوشي، راشد بن حمد، ***الدليل في الجريمة المعلوماتية***، **مجلة الحقوق للبحوث القانونية** مجلد1، 2008.

7. بن باردة عبد الحليم، ***اجراءات البحث والتحري عن الجريمة المعلوماتية***، **مجلة الحقوق والعلوم الانسانية**، عدد23، دار المنظومة،2015.

8. التاج، ايها محمد، ***التحقيق وجمع الأدلة في الجرائم المعلوماتية***، **مجلة العدل**، وزارة العدل السودان، مجلد 11، عدد26، دار المنظومة، 2009.

9. حجازي، عبد الفتاح بيومي، **الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية**، ط1، 2009.

10. حجازي، عبد الفتاح بيومي، **نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي**، ط1، 2009.

11. الحلبي، خالد عياد، **اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، دار الثقافة للنشر والتوزيع،2011.

12. الحلبي، محمد علي السالم، **شرح قانون العقوبات القسم العام**، مكتبة الثقافة للنشر والتوزيع، 1997.

13. الحمامى، عمر أبو الفتوح، **الحماية الجنائية للمعلومات المسجلة الكترونيا**، دار النهضة العربية،2010.

14. خلف، جاسم خريبط، ***التفتيش في الجرائم المعلوماتية***، الخليج العربي، مجلد 41 عدد 34، دار المنظومة،2013.

15. خليل، امام حسنين، **السياسة الجنائية لمكافحة الجرائم المعلوماتية في التشريعات العربية.**

16. رمضان، عمر السعيد، **فكرة النتيجة في قانون العقوبات**، دار الإسراء للنشر والتوزيع الاردن،1998.

17. الرواشدة، سامي حمدان، ***مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجا***، **المجلة الأردية في القانون والعلوم السياسية**، مجلد1: عدد4، دار المنظومة.

18. الزراع، عادل بن كرم. **رسالة ماجستير بالركن المادي في الجرائم المعلوماتية بالنظام السعودي**، الرياض،2014.

19. سالم، محمد علي، ***الجريمة المعلوماتية***، **مجلة جامعة بابل العلوم النسانية**، مجلد14 عدد2، دار المنظومة.

20. الشكرى، عادل يوسف عبد النبي، **الجريمة المعلوماتية وأزمة الشرعية الجزائية**، جامعة الكوفة، العدد السابع،2008.

21. شكري، عادل يوسف عبد النبي، ***الجريمة المعلوماتية وأزمة الشرعية الجزائية***، **مجلة مركز دراسات الكوفة**، ع7، دار المنظومة،2011.

22. الشوابكة، محمد امين، **جرائم الحاسوب والإنترنت الجريمة المعلوماتية**، دار الثقافة للنشر والتوزيع، ط4، 2011.

23. الشوابكة، محمد أمين، **جرائم الحاسوب والإنترنت**، دار الثقافة للنشر والتوزيع، ط4، 2011.

24. الشوابكة، محمد سامي السيد، ***جرائم الحاسب الآلي أمام القضاء الجنائي الفرنسي*، مجلة البحوث القانونية والاقتصادية**، دار المنظومة، مجلد 2، عدد 3، 1992.

25. شيماء عطا الله، **الحماية الجنائية للتعاملات الالكترونية**، دار الجامعة الجديدة، بدون ط 2007.

26. الطائي، جعفر حسن جاسم، **جرائم تكنلوجيا المعلومات**، دار البداية، ط1، 2007.

27. طه، ابراهيم قسم السيد احمد، **الجريمة المعلوماتية في القانون السوداني**، ط1، 2016.

28. الطوالبة، علي الحسن، **مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي**، جامعة العلوم التطبيقية _البحرين-،2009.

29. عبابنة، محمود احمد، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع، ط1 2009.

30. عبد الاله، هلالي، **تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي**، دراسة مقارنة،2000.

31. العبيدي، اسامة بن غانم، ***التفتيش عن الدليل في الجرائم المعلوماتية*، المجلة العربية للدراسات الأمنية والتدريب**، مجلد 29عدد58.

32. عريقات سهى ابراهيم، **الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي**، جامعة القدس، ب ن ، ب ط، ب س.

33. عقيدة أبو العلا، **التحقيق وجمع الأدلة في مجال الجرائم الالكترونية**، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، المنشور على شبكة الإنترنت، موقع الدليل الإلكتروني للقانون العربي التاريخ 2016/10/17 الساعة 10:43.

34. عمري، محمد محمود، ***الاثبات الجزائي الإلكتروني في الجرائم المعلوماتية***، **مجلة العلوم القانونية والسياسية – العراق**، مجلد12، عدد2، دار المنظومة،2016.

35. الغافري، حسين بن سعيد، **السياسة الجنائية في مواجهة جرائم الانترنت**، دار النهضة العربية 2009.

36. فالي، علال، ***خصوصيات الجريمة المعلوماتية على ضوء التشريع والقضاء المغربي***، **مجلة القضاء التجاري/المغرب**، م1/ عدد2، 2013.

37. الفيل، علي عدنان، ***اجراء التحقيق الابتدائي في الجريمة المعلوماتية***، عدد53، 2010.

38. قورة نائلة عادل فريد، **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي الحقوقية، ط1 2005.

39. قورة، نائلة عادل محمد فريد، **جرائم الحاسب الاقتصادية**، دار النهضة العربية، 2004/2003.

40. محمد معمر علي إبراهيم، **الدليل الإلكتروني وحجيته في الإثبات الجنائي**، شركة مطابع السودان للحملة المحدودة ،2015.

41. محمد، لموسخ، **تنازع الاختصاص بالجرائم المعلوماتية**، دفتر السياسة والقانون الجزائر، دار المنظومة، عدد2، 2009.

42. مدغمش، جمال، **شرح قانون العقوبات الاردني**، شرح مواد قانون العقوبات نصا نصا بما صدر من أحكام قضائية بمناسبة كل نص قانوني، دار الإسراء للنشر والتوزيع، ب ن، ب س.

43. مصطفى، خالد حامد احمد ***المعلوماتية والمسؤولية الجزائية***، **مجلة الفكر الشرطي**، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة الامارات، مجلد 20، عدد79، دار المنظومة.

44. المضحكي حنان، **الجرائم المعلوماتية**، منشورات الحلبي الحقوقية، ط1، 2014.

45. المطردي، مفتاح بو بكر، **الجريمة الإلكترونية والتغلب على تحدياتها**، المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان 2012.

46. المعمري، عادل عبد الله خميس، ***التفتيش في الجرائم المعلوماتية***، **مجلة الفكر الشرطي** مجلد22، عدد86، 2013.

47. المعيني، سرحان حسن، **التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي**، مجلد20، عدد79، دار المنظومة،2011.

48. مقابلة مع رئيس نيابة الجرائم الالكترونية الاستاذة نسرين رمشاوي بتاريخ 2017/4/19 الساعة 12:00 م

49. مؤتمر فينا في الفترة من 17/10 نيسان،2000.

50. موسى، مصطفى محمد، **قواعد وإجراءات البحث الجنائي لكشف غموض الجرائم المعلوماتية والتخطيط لها**، الرياض،2012.

51. نمور، محمد سعيد، **اصول الإجراءات الجزائية**، دار الثقافة للنشر والتوزيع،2005.

52. هروال، نبيلة هبة، **الجوانب الإجرائية لجرائم الانترنت**، دار الفكر الجامعي،2007.

53. وسيلة، بوحية، **صعوبات التحقيق وإثبات الجرائم المعلوماتية**، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، جامعة الإمام محمد بن سعود.

54. اليحيى، تركي بن محمد، بن عبدالله، **مكافحة الجرائم المعلوماتية في المملكة العربية السعودية**، مجلد 2، عدد7، دار المنظومة.

ثالثاً: الرسائل العلمية

55. الخثعمي، عبد الله بن عبد العزيز، **التفتيش في الجرائم المعلوماتية في النظام السعودي**، رسالة ماجستير، دراسة تطبيقية، جامعة نايف العربية للعلوم الامنية،2011.

56. الدهلاوي، عبد الرحمن محمد، **الانتقال والمعاينة في نظم دول مجلس التعاون الخليجي**، رسالة ماجستير،2008.

57. الروقي، مروان بن مرزوق، **القصد الجنائي بالجرائم المعلوماتية**، رسالة ماجستير،2011.

58. سده، اياد محمد عارف، **مدى حجية المحررات الإلكترونية في الاثبات**، رسالة ماجستير، جامعة النجاح الوطنية، 2009.

59. السعيدي، مجيد، **جرائم التجارة الالكترونية**، رسالة ماجستير، جامعة تونس المنار، 2004/2003.

60. قارة، مال، **الجريمة المعلوماتية**، رسالة ماجستير، كلية القانون، جامعة الجزائر 2002/2001.

61. القحطاني، عبد الله بن حسين، **تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية**، رسالة ماجستير في قسم العلوم الشرطية، الرياض.

62. كريري، عبد الله بن حمد، **الركن المعنوي في الجرائم المعلوماتية في النظام السعودي**، رسالة ماجستير،2013.

63. كريري، محمد بن عبد الله، رسالة ماجستير بعنوان **الركن المعنوي في الجرائم المعلوماتية بالنظام السعودي**، الرياض، 2013.

رابعاً: المواقع الإلكترونية.

64. قجـــاج، يوســـف، **اشـــكالية الاختصـــاص فـــي الجريمـــة الإلكترونيـــة،**

http://www.hespress.com/opinions/256777.html

65. ، ســـتار تـــايمز، **ماهيـــة التحقيـــق الابتـــدائي**، تـــاريخ2016/14/10، الســـاعة،

http://www.startimes.com/?t=741729110:21

66. **تزويـــــر معلومـــــاتي**، منتـــدى د.شـــيماء عطـــا الله، الســـاعة2:39 التـــاريخ

http://www.shaimaaatalla.com/vb/showthread.php?t=39402016/9/5

67. **أركـــــــــــان الجريمـــــــــــة المعلوماتيـــــــــــة**، 11:30، 2016/1/3م

http://www.startimes.com/?t=25263137.

68. **الـــــــركن المـــــــادي فـــــــي جـــــــرائم الانترنـــــــت**، س11:42، ص،

http://www.startimes.com/?t=252631372016/7/3.

69. مدونة القانوني، **ماهية الجريمة وتقسيماتها**، جامعة الشارقة، الساعة 12:23، 2017/4/3

http://www.qanouni-net.com/2010/10/blog-post_9421.html.

\

AN-Najah National University

Faculty of Graduate Studies

Informational Crime Specialty

By
Neda' Nael Fayez Al-Masry

Supervisor
Dr. Fadi Shadeed

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Public law, Faculty of Graduate Studies, An-Najah National University, Nablus- Palestine.

2017

Informational Crime Specialty

By
Neda' Nael Fayez Al-Masry
Supervised
Dr. Fadi Shadeed

Abstract

The researcher discussed the informational crime specialty in two chapters. The former is about the informational crime specialty on the crime and punishment level. Also, it includes the general pillars of the informational technology crime. According to this chapter, the informational crime is characterized by several features which distinguish it from the other crimes in addition to some particular conditions should be available in order to be crime . Chapter one concludes that it is necessary to bridge the legislative gap which cause difficulty in facing the IC in the Arab World.

Retribution against ITC with exception to some punishment procedures such as death sentence and some custody punishment has been discussed. Concentration with some punishments suitable to this kinds of crime such as financial punishments has been also included in this chapter.

Chapter two clarified the pursuit and tracking of the IC specialty. The chapter showed that it is necessary to legislate punishment procedures law related to the IC as a result of losing evidence. The concentration in this chapter was on informational evidence and the best ways to deal with. .The researcher clarified the final stage of investigation with its suitability to informational crimes as a cross- border ones. Moreover, this chapter clarified the judge authority in accepting the digital evidence and

presenting the attitudes of the various legislations in proving the digital evidence .

The research has been ended by a conclusion of what the it resulted and recommended.