

مدونة المنبر القانوني
Tribunejuridique.blogspot.com

جامعة نايف العربية للعلوم الأمنية
كلية الدراسات العليا
قسم العدالة الجنائية

إثبات الجريمة الإلكترونية

دراسة تأصيلية تطبيقية

إعداد

ثنيان ناصر آل ثنيان

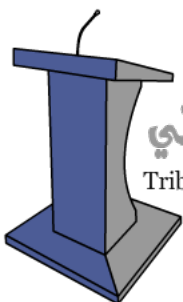
إشراف

د/ جلال الدين محمد صالح

رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية

الرياض

١٤٣٣ هـ / ٢٠١٢ م



مدونة المنبر القانوني
Tribunejuridique.blogspot.com

الفصل الأول مشكلة الدراسة وأبعادها

• المقدمة:

الحمد لله رب العالمين والصلاة والسلام على نبينا محمد وعلى آله وصحبه أجمعين.. أما بعد،،،

فبقدر ما يحققه تطور التقنيات من فوائد كبيرة في مجال الرقي والتقدم الإنساني، فإنها في الوقت ذاته مهدت السبيل إلى بروز أشكال جديدة من الجرائم، لاسيما بعد أن تم ربط الحاسب الآلي بالشبكة العالمية للإنترنت حيث وجد المجرم تقنية عالية وأساليب حديثة تساعده في ارتكاب العديد من الجرائم دون أن يترك أثراً واضحاً لتلك الجريمة، والمجرم يستطيع باستغلال هذه المخترعات العلمية والأجهزة الإلكترونية وما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم من خلال الإمكانيات الهائلة لهذه التقنيات، ويصل إلى أي مكان يرغب فيه، وإلى أعداد بشرية هائلة في نفس الوقت، فلا مكان ولا زمان يستطيع وضع حدود لهذه الشبكة.

وتتميز الجرائم الإلكترونية بصعوبة متابعتها حيث إنها في الغالب لا تترك أثراً، فليست هناك أموال وممتلكات مفقودة، وإنما هي أرقام تتغير في السجلات، ومعظم الجرائم الإلكترونية ربما يتم اكتشافها بالصدفة، وبعد وقت طويل من ارتكابها، كما أن الجرائم الإلكترونية تتميز بالدقة والتعقيد التقني، وغالبا من يرتكب تلك الجرائم يتمتع بالذكاء.

وإذا كانت الجريمة الإلكترونية أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي بحثاً عن إمكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الجرائم مع احترام مبدأ الشرعية، والتفسير الضيق للنصوص الجنائية، فقد أثارت في نفس الوقت العديد من المشكلات في نطاق القانون الجنائي الإجرائي، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بجرائم

تقليدية، لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي في الاقتناع وصولاً إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

غير أن المشكلات الإجرائية في مجال الجرائم الإلكترونية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونيا وكيانات غير ملموسة، وبالتالي يصعب من ناحية كشف هذه الجرائم، ويصعب من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة الإجراءات في هذا المجال، سرعة ودقة تنفيذ الجرائم الإلكترونية وإمكانية محو آثارها، وإخفاء الأدلة المتحصلة عنها عقب التنفيذ مباشرة، ويواجه التفتيش وجمع الأدلة صعوبات كثيرة في هذا المجال، وقد يتعلقان ببيانات مخزنة في أنظمة أو شبكات إلكترونية موجودة بالخارج.

ويثير مسألة الدخول إلى البيانات ومحاولة جمعها وتحويلها إلى الدولة التي يجري فيها التحقيق، مشكلات تتعلق بسيادة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات. وفي هذه الحالة يحتاج الأمر إلى تعاون دولي في مجالات البحث والتفتيش والتحقيق وجمع الأدلة، وتسليم المجرمين، بل وتنفيذ الأحكام الأجنبية الصادرة في هذا المجال.

وقد يلجأ بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة في الخارج، فيصعب إثباتها، ويثور التساؤل حول حرية تدفق المعلومات ومدى صلاحية متابعه تدفق البيانات الموجودة خارج الدولة المتعلقة بالجريمة محل البحث، ويثير التفتيش أو الضبط أو المصادرة في مجال أنظمة الاتصال الإلكترونية ضرورة وضع ضوابط إجرائية لها، تعمل على إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد، وبين تحقيق الفاعلية المطلوبة للأجهزة الأمنية، وسلطات التحقيق في كشف غموض الجريمة وضبط فاعليها والتحقيق مع الجناة وتقديمهم للمحكمة. وهذا ما أحاول تناوله في هذه الدراسة.

• مشكلة الدراسة:

في ظل التقدم التقني في العصر الحالي، ظهرت صور من الإجرام ترتبط بالتقنيات، وقد تزايدت معدلات هذه الجرائم في العقدين الآخرين على وجه الخصوص، بصورة أدت إلى بروز ظاهرة إجرامية جديدة، تعرف بالإجرام المعلوماتي أو الإجرام الإلكتروني.

وإن تفاقم الجرائم الإلكترونية يشكل تهديداً مباشراً لأكثر المرافق العامة والمصالح الخاصة، ويقوض الأمن الاجتماعي، ويمثل عدواناً على حقوق الأفراد فيما يتعلق بحفظ خصوصياتهم الاقتصادية والاجتماعية، وتتسم هذه الجرائم بأنها غير ملموسة، كما أنها تحدث من أي مكان وهناك صعوبة في تتبعها، لأنها قد تخرج عن نطاق الدولة، لذا فإن إثبات مثل هذه الجرائم يواجه صعوبات مختلفة، ولها من الخصوصية ما يتطلب إجراءات معينة للإثبات، وهذه مشكلة الدراسة الحالية والتي يمكن اختزالها في السؤال الرئيس التالي: كيف يمكن إثبات الجريمة الإلكترونية؟

• أسئلة الدراسة:

تجيب الدراسة على التساؤلات التالي:

١. ما مفهوم الجرائم الإلكترونية وما خصائصها وتصنيفها؟
٢. ما تأصيل الجريمة الإلكترونية في الشريعة الإسلامية والنظام السعودي؟
٣. ما أهمية الاستدلالات في إثبات الجريمة الإلكترونية؟
٤. ما ضوابط إثبات الجريمة الإلكترونية؟
٥. ما كيفية إثبات الجريمة الإلكترونية بالشهادة والإقرار؟
٦. ما كيفية إثبات الجريمة الإلكترونية بالخبرة الفنية؟
٧. ما معوقات إثبات الجرائم الإلكترونية؟

• أهداف الدراسة:



مدونة المنبر القانوني
Tribunejuridique.blogspot.com

تهدف الدراسة إلى معرفة إثبات الجرائم الإلكترونية وذلك من خلال ما يلي:

١. معرفة مفهوم الجرائم الإلكترونية وخصائصها وتصنيفها.
٢. التعرف على تأصيل الجريمة الإلكترونية في الفقه الإسلامي والنظام السعودي.
٣. معرفة أهمية الاستدلالات في إثبات الجريمة الإلكترونية.
٤. دراسة ضوابط إثبات الجريمة الإلكترونية.
٥. التعرف على كيفية إثبات الجريمة الإلكترونية بالشهادة والإقرار.
٦. معرفة كيفية إثبات الجريمة الإلكترونية بالخبرة الفنية.
٧. معرفة معوقات إثبات الجرائم الإلكترونية.

• أهمية الدراسة:

الأهمية النظرية:

تكمن الأهمية النظرية لهذه الدراسة في مراجعة النصوص النظامية التي تجرم الاستخدام غير المشروع للحاسب الآلي وملحقاته، وشبكات الإنترنت من خلال تصنيف هذه الجرائم وتحديد العقوبات المترتبة عليها في النظام السعودي، وفي ما تقدمه هذه النصوص من دعم في مجال مكافحة الجرائم الإلكترونية والتصدي لها. ولأن أساس توقيع العقوبة على المتهم إثبات إدانته بإقامة الأدلة عليه و عرضها على القاضي ليحكم على الجاني حسب الأدلة الجازمة التي لديه لذا فان الإثبات موضوع في غاية الأهمية، وعلى مستوى التحقيق الجنائي تكمن الأهمية في تحديد إجراءات التحقيق في الجرائم الإلكترونية بالإضافة إلى التعريف بالبرامج والأنظمة الخاصة التي تساعد في إثبات مثل هذه الجرائم والتي ينبغي على رجال الأمن وأعضاء هيئه التحقيق والادعاء العام والقضاة معرفتها لإثبات وقوع الجريمة.

الأهمية التطبيقية:

تكمن الأهمية التطبيقية لهذه الدراسة في الإسهام في عرض وتحليل آليات إثبات الجريمة الإلكترونية، وفي تبصير رجال القضاء والمحامين على أهمية التأكد من وقوع الجريمة الإلكترونية وإثبات حدوثها ومن ثم إدانة المتهم بارتكابها، كما يتم عرض عدد من القضايا أو الجرائم المتعلقة بالجريمة الإلكترونية، وسيتم ذلك من

خلال تحديد مكان وزمان وقوع الجريمة ونوعها، وذكر المعطيات التي يبني عليها المحقق في إثبات الجريمة وإدانة الجاني بموجب نظام الجرائم المعلوماتية.

• منهج الدراسة:

اعتمدت هذه الدراسة على المنهج الاستقرائي الوثائقي التحليلي مع تأصيل الموضوع في الشريعة الإسلامية؛ لإبراز إثبات الجريمة الإلكترونية.

• حدود الدراسة:

الجانب الموضوعي:

اقتصرت الدراسة على بيان إثبات الجريمة الإلكترونية في النظام السعودي والشريعة الإسلامية وذلك من خلال معرفة مفهوم الجرائم الإلكترونية وخصائصها وتصنيفها، والتعرف على أدوات الجريمة الإلكترونية، والتعرف على الجريمة الإلكترونية في الشريعة والنظام السعودي، ومعرفة المهارات المطلوبة لإثبات الجريمة الإلكترونية، ودراسة الإثبات بالشهادة والإقرار والخبرة الفنية في إثبات الجرائم الإلكترونية، والتعرف على معوقات إثبات الجرائم الإلكترونية، وأيضاً معرفة ظروف التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية.

الجانب التطبيقي: وفي هذا الجانب يتم تطبيق المفاهيم ذات الجانب النظري على نصوص النظام السعودي للجريمة الإلكترونية مع بحث وتحليل عشر قضايا تخص الجرائم الإلكترونية.

• مصطلحات الدراسة

١. الإثبات

الإثبات لغة، هو إثبات الشيء، أي عرفه حق المعرفة وثبت ثباتاً وثبوتاً، فهو ثابت، والثبات والثبوت يعني الدوام والاستقرار، فالإثبات لدى علماء اللغة يعني تأكيد وجود الحق بالدليل^(١).

الإثبات: إقامة الدليل على إدعاء أمام القضاء.

(١) الفيروز آبادي (١٤٠٧ هـ)، القاموس المحيط، مؤسسة الرسالة، بيروت، لبنان، ط٢، ص ١٤٤.

الإثبات بالشهادة: إثبات بأقوال أشخاص يقررون صدور وقائع من غيرهم تثبت حقوقاً لأشخاص آخرين.

الإثبات بالشهرة: الإثبات بالأمر المشتهر.

الإثبات بالكتابة، الدليل الخطي: الإثبات بتقديم دليل مكتوب سواء أكان محرراً رسمياً أم عرفياً^(١).

الإثبات شرعاً، هو الإتيان بالدليل الذي ثبت الحق أو الواقعة المطروحة أمام القضاء وفقاً للطرق المحددة شرعاً^(٢).

الإثبات قانوناً، هو إقامة الدليل لدى القضاء على حقيقة واقعة ذات أهمية قانونية، ونسبتها إلى المتهم بالطرق التي حددها القانون. في حين يعرف الإثبات في المواد الجنائية بأنه: كل ما يؤدي إلى إظهار الحقيقة التي تتجلى في وقوع الجريمة بوجه عام ونسبتها للمتهم بوجه خاص^(٣).

التعريف الإجرائي:

إقامة الدليل لدى القضاء على حقيقة جريمة تتعلق بالجانب الإلكتروني، ونسبتها إلى المتهم بالطرق التي يحددها النظام السعودي استمداداً من الشريعة الإسلامية.

٢. الجريمة:

للجريمة عدة تعاريف تختلف من دستور إلى آخر، ومن علم إلى آخر، مع أن فكرة الجريمة لا تتغير في جوهرها بل تتغير صورها وتتعدد بحسب المصدر الذي وضع الأوامر والأنظمة. وعليه فإن للجريمة مفاهيم متعددة نعرض لها فيما يلي:

(١) مجمع اللغة العربية، جمهورية مصر العربية، معجم القانون، القاهرة، الهيئة العامة لشئون المطابع الأميرية، ١٤٢٠هـ. ص ٤٢

(٢) آل معجون، خلود سامي، إثبات جريمة الزنا بين الشريعة والقانون، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، الرياض، ١٤١٣هـ. ص ٢١.

(٣) العرابي، علي زكي المبادئ الأساسية للتحقيقات والإجراءات الجنائية، الجزء الأول، ١٩٤٠، ص ٥٥٨.

تعريف الجريمة في الشريعة الإسلامية:

الجريمة هي "إتيان فعل محرم معاقب على فعله، أو ترك فعل واجب معاقب على تركه". إلا أن أشهر تعريف للجريمة وأكثرها تداولاً تعريف الماوردي المتوفى سنة ٤٥٠ هـ رحمه الله بأنها: "محظورات شرعية زجر الله تعالى عنها بحد أو تعزير" أو قصاص^(١).

تعريف الجريمة من المنظور القانوني:

الجريمة هي "كل ما نص الشرع أو القانون على تجريمه من الأفعال والأقوال وجعل له عقوبة صريحة"، مثل جرائم الحدود والقصاص أو منح القاضي صلاحية تحديد العقوبة، كما هو الحال في جرائم التعزير، وبالتالي لا يعتبر الفعل جريمة إلا بوجود نص على ذلك وبوجود عقوبة قابلة للتطبيق. فالإنسان يعيش في مجتمع من الناس، وفعاليته التي تتجلى في تأكيد حقوقه الطبيعية واستعمالها لا يمكن ممارستها إلا في حدود القوانين وبالقدر الذي لا يكون فيه نموها ضاراً بنمو فعالية غيره من الناس، فمن يتجاوز هذه الحدود يقلق النظام الاجتماعي، ويقترب ما يسميه رجال القانون جريمة ويتعرض والحالة هذه للعقوبات المنصوص عليها في القوانين الجزائية^(٢).

كما تعرف الجريمة على أنها "فعل غير مشروع صادر عن أداء جنائية يقرر لها القانون عقوبة"^(٣).

التعريف الإجرائي:

فعل غير مشروع صادر عن استخدام التقنيات الحديثة صادر عن أداة جنائية يقرر لها النظام السعودي عقوبة.

(١) الطخيس، إبراهيم عبدالرحمن (١٩٩٤م)، دراسات في علم الاجتماع الجنائي، ط١، دار العلوم للطباعة والنشر، الرياض، ص ٣٨.

(٢) ماركيزية، جان (١٩٨٣م): الجريمة، ترجمة عيسى عصفور، منشورات عويدات، بيروت، ص ٥-٦.

(٣) مصري، عبد الصبور (٢٠١٠م)، الجريمة الإلكترونية، دار العلوم، للنشر والتوزيع، القاهرة، ص ٢٧.

-الجريمة الإلكترونية-

الجريمة الإلكترونية هي كل فعل ضار يأتيه المواطن عبر استعماله الحاسب الآلي وشبكة الإنترنت، وهي أيضاً فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسة، وهي أيضاً الجريمة التي تلعب فيها التقنية الرقمية بيانات الحاسب والبرامج المعلوماتية دوراً مهماً^(١).

التعريف الإجرائي:

كل الجرائم التي تتعلق بالتقنية الرقمية والبرامج المعلوماتية والتي ورد فيها نص عقوبة في النظام السعودي.

٣. الإنترنت (Internet):

الإنترنت هو نظام ووسيلة اتصال من الشبكات الحاسوبية يصل ما بين حواسيب حول العالم ببروتوكول موحد هو بروتوكول إنترنت، تربط الإنترنت ما بين ملايين الشبكات الخاصة والعامة في المؤسسات الأكاديمية والحكومية ومؤسسات الأعمال وتتباين في نطاقها ما بين المحلي والعالمي وتتصل بتقنيات مختلفة، من الأسلاك النحاسية والألياف البصرية والوصلات اللاسلكية، كما تتباين تلك الشبكات في بنيتها الداخلية تقنيا وإداريا، إذ تدار كل منها بمعزل عن الأخرى لا مركزيا ولا تعتمد أيا منها في تشغيلها على الأخريات^(٢).

٤. الضبط

المقصود بالضبط هو مهمة الكشف عن الجرائم بعد وقوعها وتتبع مرتكبيها وجمع الأدلة فيها تمهيداً للتحقيق معهم وإحالتهم إلى القضاء^(٣).

(١) عمار، زكريا أحمد، الحلقة العلمية: الدليل الرقمي والتحقيق في الجرائم الإلكترونية، جامعة نايف العربية للعلوم الأمنية، كلية علوم الأدلة الجنائية، من ٢٢ إلى ٢٦/١٢/١٤٢٩ هـ، ص ١٥.
(٢) موسوعة ويكيبيديا، موقع: <http://ar.wikipedia.org/wiki>، ٢٦/٥/٢٠١٢ م.
(٣) كلزي، ياسر حسن (٢٠٠٧ م) حقوق الإنسان في مواجهة سلطات الضبط الجنائي، دراسة مقارنة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، ص ٦٢

٥. التحقيق

يعني التحقق من أن أمراً ما قد حدث. وهو من الحقيقة بمعنى البحث عن حقيقة واقعة حدثت في الماضي والقائم بهذا التحقيق يسلك مسالك معينة هي ما يطلق عليها إجراءات التحقيق^(١).

٦. التفتيش

التفتيش في اللغة من فتش: الفَتَشُ والتَفْتِيشُ: الطلبُ والبحثُ، وفتَّشْتُ الشيءَ فتَّشاً وفتَّشَه تَفْتِيشاً مثله^(٢).

هو البحث والاستقصاء وهو إجراء يهدف إلى ضبط أدلة الجريمة من أجل إثباتها أو نسبها أو إسنادها للمتهم وكل ما يفيد في كشف الحقيقة^(٣).

• الدراسات السابقة:

أقوم في هذا الجزء بعرض بعض الدراسات السابقة؛ وذلك للمساعدة في تشخيص المشكلة؛ وللوقوف على ما توصل إليه الباحثون في معالجتهم لموضوعاتهم من نتائج يمكن أن تعين على تجنب تكرار ما تم إنجازه، وسيتم استعراض الدراسات العربية والمحلية والتي لها علاقة بالدراسة الحالية وذلك على النحو التالي:

١. دراسة محمد أمين الشوابكة (٢٠٠٢م) بعنوان: الجرائم المرتكبة عبر الإنترنت، وهي رسالة ماجستير غير منشورة، جامعة الدول العربية، المنظمة العربية للتربية والثقافة والعلوم، قسم البحوث والدراسات القانونية، واستهدفت الدراسة معرفة الجرائم المرتكبة عبر الإنترنت، وتوصلت الدراسة إلى عدة نتائج وهي:

• إن توفير حماية جنائية لأطراف التجارة الإلكترونية لا يتأتى إلا باتخاذ نصوص جنائية تكفل الحماية اللازمة للتجارة الإلكترونية.

(١) القحطاني، فيصل بن معيض (١٩٩٩م) هيئة التحقيق والادعاء العام ودورها في نظام العدالة الجنائية في المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، ص ٢٤
 (٢) ابن منظور، أبو الفضل جمال الدين، لسان العرب، (دار صادر، بيروت، لبنان، ط٣).
 (٣) القحطاني، فيصل بن معيض (١٩٩٩م) هيئة التحقيق والادعاء العام ودورها في نظام العدالة الجنائية في المملكة العربية السعودية، مرجع سابق، ص ٢٤

- اهتمام المجتمع الدولي عبر المنظمات الدولية بالتجارة الإلكترونية أسفر عن صدور القانون النموذجي للأمم المتحدة الأونسيترال، والذي وضع قواعد عامة يمكن للدول الاسترشاد بها حين تنظيم قواعد التجارة الإلكترونية في قوانينها الداخلية.
 - اهتمت المنظمات الإقليمية بالتجارة الإلكترونية، وحاولت وضع قواعد لتنظيمها، مثل غرفة التجارة الدولية، ومنظمة العالمية للملكية الفكرية، ومنظمة التعاون والتنمية في المجال الاقتصادي، والاتحاد الأوروبي من خلال توجيهاته المميزة في هذا المجال.
 - اهتمت القوانين المقارنة بتنظيم التجارة الإلكترونية، نظراً للتطور التكنولوجي السريع في هذا المجال والذي يجب أن يواكبه تطور تشريعي، وضرورة الاهتمام بحماية مواقع هذه التجارة الإلكترونية وأنظمتها ووسائلها من أي اعتداء عليها.
 - أن الدول العربية بدأت تشعر بالخطر من ظاهرة الإجرام المعلوماتي، وضرورة تنظيم التجارة الإلكترونية، وإعطاء التوقيع الإلكتروني والمحركات الإلكترونية الحجية في الإثبات، فصدر قوانين بهذا الشأن منها صدور نظام بالمملكة العربية السعودية يواجه الجريمة الإلكترونية.
 - اهتمت أغلب تشريعات الدول المقارنة بالمستهلك الإلكتروني وتوفير أقصى درجات الحماية له، باعتباره الطرف الضعيف في عملية التجارة الإلكترونية.
- أوجه التشابه والاختلاف بين هذه الدراسة والدراسة الحالية:**

تتفق هذه الدراسة مع الدراسة الحالية من ناحية إلقاء الضوء على الجرائم المرتكبة عبر الإنترنت، لكن تختلف هذه الدراسة عن الدراسة الحالية في أنها ركزت على إحدى الجرائم الإلكترونية، كما أنها لم تسلط الضوء على إثبات الجريمة، وذلك من ناحية تدابير وإجراءات كشف الجريمة، وأركانها من جهة الجرائم الإلكترونية التي غطتها الرسالة ولم تنبه عليها الرسالة السابقة.

٢. دراسة سليمان مهجع العنزي (٢٠٠٣م) بعنوان: وسائل التحقيق في جرائم نظم المعلومات، وهي رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية،

قسم العلوم الشرطية، وسعت هذه الدراسة إلى وضع إطار عام للسياسة الأمنية الشاملة لحماية نظم المعلومات، وتحديد أنماط جرائم نظم المعلومات، ومدى حدوثها بالمؤسسات، وأضرارها، ودوافعها وحصر الأساليب المستخدمة في ارتكاب جرائم نظم المعلومات ومنافذها. وحصر الأدوات المستخدمة من قبل مجرمي نظم المعلومات وكيف يمكن لمجرمي نظم المعلومات بالملكة أن يحصلوا عليها. والكشف عن وسائل التحقيق في جرائم نظم المعلومات، وبيان العوائق التي تحول دون استخدام تلك الوسائل. وتحديد أنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات.

واستخدم الباحث المنهج الوصفي من خلال أسلوب المسح الاجتماعي، كما استخدم استبانة لجمع البيانات من أفراد عينة الدراسة والبالغ عددهم (١٤١) فرداً، منهم (٣٦) محققاً من شرطة الرياض والشؤون الفنية بوزارة الداخلية، و(٦٨) عاملاً بمجال نظم المعلومات في القطاع العام والخاص في الرياض، وجدة، والدمام، و(٣٧) متخصصاً في المؤسسات الموفرة لتقنيات أمن المعلومات في مدينة الرياض.

وتوصلت الدراسة إلى عدد من النتائج من أهمها:

- أن هناك برامج حماية تساعد في تحديد نوع الجريمة، وفي تحديد توقيت ارتكابها وتحديد مصدرها.
- أنه بالإمكان الاعتماد على عنوان (IP)، وبرامج الحماية، وبرامج تتبع المخترقين، وبرامج تتبع مصدر الرسائل الإلكترونية، ووسائل أمن البيانات، بتحديد شخصية مرتكب جريمة نظم المعلومات في المؤسسات.
- أن هناك أدوات مهمة تساعد على ضبط الجريمة، وهي سجل الصلاحيات للمستخدمين، والتقارير التي تنتجها نظم أمن البيانات، وبرامج النسخ الاحتياطي والتسجيل، وبرامج كشف الفيروسات، وأدوات المراجعة، وتقارير الجدران النارية، وأدوات مراقبة المستخدمين للشبكة، وبرامج تتبع المخترقين، ومراجعة قاعدة البيانات، وبرامج تتبع مصدر الرسائل.

- هناك أدوات تساعد على التحقيق وهي: أداة فك التشفير، وبرامج كسر كلمة المرور، وأدوات استرجاع المعلومات من الأقراص التالفة، وبرامج مقارنة النسخ، وبرامج تشغيل الحاسب.

أوجه التشابه والاختلاف بين هذه الدراسة والدراسة الحالية:

تتفق هذه الدراسة مع الدراسة الحالية من ناحية إلقاء الضوء على وسائل التحقيق في جرائم نظم المعلومات، لكن تختلف هذه الدراسة عن الدراسة الحالية في أنها ركزت على وسائل التحقيق، كما أنها لم تسلط الضوء على إثبات الجريمة الإلكترونية.

١. دراسة خالد بن عبد الله بن معيوض العبيدي (٢٠٠٨م) بعنوان: الحماية

الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، وهي رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، قسم العدالة الجنائية. واستهدفت الدراسة بيان مفهوم التعاملات الإلكترونية، وبيان مفهوم الحماية الجنائية للتجارة الإلكترونية، بالإضافة إلى بيان مفهوم الحماية الجنائية للتوقيع الإلكتروني، واتباع الباحث في هذه الدراسة المنهج الاستقرائي والمنهج الثاني، المنهج التحليلي المقارن، وتوصلت الدراسة إلى عدة نتائج أهمها:

- الجريمة الإلكترونية مختلفة عن بقية الجرائم في أن لها طبيعة قانونية خاصة تستمدّها من أن الاعتداء فيها ينصب على المعلومات التي لا يخفى على أحد أن هناك اختلافاً في تحديد طبيعتها.
- أن نظام مكافحة الجرائم المعلوماتية ونظام التعاملات الإلكترونية السعودي يمكن من الحد من الجريمة الإلكترونية بفرض الضوابط والعقوبات ومن فوائد ذلك حماية التجارة الإلكترونية.
- يتضمن نظام التعاملات الإلكترونية قواعد خاصة بالضبط والتحقيق والمحاكمة على الجرائم الإلكترونية.

أوجه التشابه والاختلاف بين هذه الدراسة والدراسة الحالية:

تتفق هذه الدراسة مع الدراسة الحالية من ناحية إلقاء الضوء على الحماية الجنائية للتعاملات الإلكترونية في النظام السعودي، والتطرق لنظام التعاملات الإلكترونية، الذي تضمن قواعد خاصة بالضبط والتحقيق والمحاكمة على الجرائم الإلكترونية، لكن تختلف هذه الدراسة عن الدراسة الحالية في أنها ركزت على أحد الجوانب في الجرائم الإلكترونية، كما أنها لم تسلط الضوء على إثبات الجريمة، وذلك من ناحية تدابير وإجراءات كشف الجريمة، وأركانها.

٢. دراسة عبد الله بن سعود بن محمد السراني (٢٠٠٩) بعنوان: فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، وهي رسالة دكتوراه غير منشورة، بجامعة نايف العربية للعلوم الأمنية، قسم العلوم الشرطية، وتتناول مشكلة الدراسة في التعرف على فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، وتشكل مجتمع الدراسة من المحققين في الجهات المعنية بمكافحة التزوير بالأمن العام والجوازات بمناطق المملكة العربية السعودية وعددهم (٢٥٣) محققاً.

واستخدم الباحث المنهج الوصفي التحليلي عن طريق المدخل المسحي حيث قام بحصر شامل لمجتمع الدراسة باستخدام الاستبانة كأداة لجمع البيانات، كما استخدم منهج تحليل المضمون لقرارات صادرة عن الدوائر الجزائية المختلفة بديوان المظالم لبعض القضايا. وتوصلت الدراسة إلى عدة نتائج أهمها:

- إن الوسائل المهمة جداً لارتكاب جريمة التزوير الإلكتروني هي: أدوات كسر كلمات السر، وإفشاء الرقم السري، والمحاولة المتكررة من خلال استخدام لوحة المفاتيح.
- إن الأساليب الفعالة جداً في إثبات جرائم التزوير الإلكتروني من قبل المحقق الجنائي هي: الاستعانة بخبراء الحاسب الآلي في فهم المصطلحات، والاستفادة من علم الحاسب الجنائي في إثبات جريمة التزوير الإلكتروني.
- إن الأساليب الفعالة جداً في إثبات جرائم التزوير الإلكتروني من قبل المحقق الفني هي: الاستعانة بمركز المعلومات لمعرفة المستخدم الذي قام بعملية

التزوير من الموظفين في الإدارات الإلكترونية التابعة لها، وعمل نسخة كاملة من البيانات الموجودة على الحاسب الآلي الذي تعرض للاختراق والتعدي.

- إن المعوقات المهمة التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بدرجة قوية هي: ندرة البرامج التدريبية اللازمة لتأهيل المحققين لإثبات جرائم التزوير الإلكتروني، وقلة إلمام بعض المحققين بالبرامج الخاصة بالتعدي والاختراق والتزوير، وقلة إلمام المحققين بمجال الحاسب الجنائي في إثبات الجريمة.

أوجه التشابه والاختلاف بين هذه الدراسة والدراسة الحالية:

تتفق هذه الدراسة مع الدراسة الحالية من ناحية تناولها لموضوع إثبات جريمة التزوير الإلكتروني، لكن تختلف هذه الدراسة عن الدراسة الحالية في أنها ركزت على إحدى الجرائم الإلكترونية وهي التزوير الإلكتروني.

٣. دراسة عبدالله ذيب عبدالله محمود (٢٠٠٩م) بعنوان: حماية المستهلك في

التعاقد الإلكتروني: دراسة مقارنة، وهي رسالة ماجستير غير منشورة، بجامعة النجاح الوطنية، فلسطين، وتهدف الدراسة إلى بيان حاجة المستهلك للحماية من المنظور التقليدي والتقني، والكشف عن مدى الحاجة لحماية المستهلك قبل إبرام العقد الإلكتروني، كما وتهدف أيضاً إلى توضيح، ووضع التشريعات السارية في فلسطين والمتعلقة بحماية المستهلك، والتعرف على حقوق المستهلك في كافة مراحل العقد الإلكتروني، بالإضافة إلى الكشف عن مدى حاجة المستهلك للإعلام اللاحق لإبرام العقد الإلكتروني. واعتمد الباحث على المنهج الوصفي التحليلي والمنهج المقارن، وتوصلت الدراسة إلى عدة نتائج أهمها:

- أن فكرة اكتساب المزود لوصف المستهلك غير دقيقة، بسبب أن الشخص المبحوث عن حمايته هو الطرف الضعيف في العملية التعاقدية، وبالتالي هو الأولى في تطبيق نصوص قانون الاستهلاك عليه، أما المزود الذي يتمتع بالخبرة والقوة في المعاملات الاقتصادية فإن الحماية التي يمكن أن تتوفر له هي التي نصت عليها قواعد القانون المدني.

- قد يعتبر الإعلان التجاري الإلكتروني الموجه إلى المستهلك إيجاباً، وقد يكون دعوة للتفاوض أو للتعاقد، فإذا تضمن الإعلان الشروط الجوهرية والأساسية للتعاقد، أي تضمن عرض السلع والخدمات عن طريق الإنترنت وضمن المبيع فإن هذا العرض يعتبر إيجاباً، أما في حالة اعتبار الإعلان الإلكتروني الموجه إلى المستهلك دعوة للتفاوض أو للتعاقد، فإن ذلك يتمثل في عدم احتواء الإعلان الإلكتروني على الشروط الأساسية للتعاقد، كبيان أسعار السلع والخدمات عبر الإنترنت، أي عند الشك في وضوح المعلومات الجوهرية عن التعاقد فإن الإعلان الإلكتروني لا يعتبر إيجاباً وإنما دعوة للتفاوض.
- يتمثل حق المستهلك في الإعلام والتبصر من خلال تحديد شخصية المزود، ووصف المنتج أو الخدمة محل التعاقد، وبيان السمات الأساسية للسلعة أو الخدمة، فالحق بالإعلام بخصائص وصفات السلع والخدمات المعروضة، جوهر فكرة الالتزام بالإعلام، لأن خصائص السلعة أو الخدمة قد تكون الباعث الرئيس لدى المستهلك على التعاقد، وفي إطارها يقع المستهلك ضحية الغش والتقليد.
- يعتبر العقد الإلكتروني عقد إذعان إذا لم يكن هناك تفاوض، فالأمر يتوقف على مدى إمكانية التفاوض حول شروط العقد، فإن كان العقد الإلكتروني يجيز التفاوض، ويسمح للمستهلك بمراجعة بنود العقد وتعديله أحياناً، فإنه لا يعتبر عقد إذعان، أما إذا انعدمت سمة التفاوض أو المساومة، وجاءت بنود العقد بطريقة جامدة لا تقبل المراجعة أو التمهيص فهو عقد إذعان، حيث قررت أغلب التشريعات الوطنية وضع حماية للطرف الضعيف - المستهلك - تتمثل في مظهرين أساسيين، الأول وهو الحماية من الشروط التعسفية من خلال تخويل القاضي سلطة تعديل عقد الإذعان، والثاني تفسير الشك في مصلحة الطرف المذعن.
- أن المنظم الفلسطيني قد وفق في عدم التفريق ما بين العيب الجسيم والعيب البسيط في قانون حماية المستهلك رقم ٢١ لسنة ٢٠٠٥م، لأن مجرد وجود

العيب ولو كان بسيطاً يفقد المستهلك الرغبة في المبيع، على الرغم من أنه قد لا تتوفر كافة شروط العيب في العيب البسيط، والتي نصت عليها النظرية التقليدية، ويحق للمستهلك الرجوع على البائع بالضمان.

- إن توسيع مسؤولية المزود عن المنتجات والخدمات المعيبة هو في صالح المستهلك، وأن مجرد وقوع الخطأ حتى ولو كان غير مقصوداً من قبل المزود يجيز للمستهلك أن يطالب بالتعويض حتى وإن لم يكن هناك ضرر، لأن التزام المزود في انتفاع المستهلك بالمبيع هو التزام بتحقيق نتيجة.
- تعاني هيئات حماية المستهلك الفلسطينية من العديد من الصعوبات، وذلك لنتامي وجود ظاهرة فساد السلع والغش والتقليد والتزوير بكافه أشكاله، والذي جعل هيئات حماية المستهلك أمام تحد صعب في توفير الحماية للمستهلك من مخاطر ظاهره التقليد والتزوير والضرر الذي يقع عليه من جراء تناول سلع تضر بسلامته، كما أن هناك دور مهم للقضاء والذي هو مغيب في هذا الجانب، حيث لا توجد محاسبة للمزودين الذي يضبط لديهم مواد فاسدة.

أوجه التشابه والاختلاف بين هذه الدراسة والدراسة الحالية:

تتفق هذه الدراسة مع الدراسة الحالية من ناحية دراسة حماية المستهلك في التعاقد الإلكتروني، لكن تختلف هذه الدراسة عن الدراسة الحالية في أنها ركزت على جانب الحماية للتعاقد الإلكتروني.

٤. دراسة محمد بن محسن بن باعث الرويلي (٢٠١٠م) بعنوان: تجريم الأفعال

الإباحية الإلكترونية والعقاب عليها، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، قسم العدالة الجنائية. واستهدفت الدراسة عدة أهداف منها: إيضاح الأفعال الإباحية الإلكترونية المجرمة في النظام السعودي، وبيان عقوبة الأفعال الإباحية الإلكترونية في الشريعة الإسلامية والنظام السعودي، واعتمد الباحث على المنهج الوصفي الاستقرائي فيما يتعلق بجميع المسائل المتعلقة بموضوع الدراسة، والمنهج التأصيلي فيما يتعلق بالمنظور الشرعي، ومنهج تحليل المضمون بالنسبة للجانب التطبيقي من الدراسة. وتم تحليل مضمون عشر قضايا نظرتها المحاكم الشرعية بالمملكة العربية السعودية تتعلق بالأفعال الإباحية الإلكترونية، وتوصلت الدراسة إلى عدة نتائج منها:

- عظم الشريعة الإسلامية وتكاملها وشمولها، فقد حرصت على الأعراس، وجعلت حمايتها مقصداً من مقاصدها وضرورة من ضرورياتها، وجرمت المساس بها.
- اتضح أن مفهوم الأفعال الإباحية الإلكترونية يختلف من بلد لآخر فما يعتبر من الأفعال الإباحية في بلد قد لا يعتبر في بلد آخر من تلك الأفعال.
- عقوبة الأفعال الإباحية الإلكترونية تعزيرية في الشريعة الإسلامية والنظام السعودي.

أوجه التشابه والاختلاف بين هذه الدراسة والدراسة الحالية:

تتفق هذه الدراسة مع الدراسة الحالية من ناحية إلقاء الضوء على تجريم الأفعال الإباحية الإلكترونية والعقاب عليها، وهي إحدى الجرائم الإلكترونية، لكن تختلف هذه الدراسة عن الدراسة الحالية في أنها ركزت على التجريم والعقاب، كما أنها لم تسلط الضوء على إثبات الجريمة، وذلك من ناحية تدابير وإجراءات كشف الجريمة، وأركانها.

الفصل الثاني

ماهية الجرائم الإلكترونية

المبحث الأول: مفهوم الجرائم الإلكترونية وخصائصها وتصنيفها
المبحث الثاني: الجريمة الإلكترونية في النظام السعودي والفقه الإسلامي

المبحث الأول

مفهوم الجرائم الإلكترونية وخصائصها وتصنيفها

يوصف العصر الحالي بأنه العصر الرقمي أو ما يسمى بالعصر الإلكتروني الرقمي، فهو يتضمن تطورات تكنولوجيا هائلة وكبيرة ومعقدة تخدم جميع المجالات العامة والخاصة داخل الإطار الضيق للدول، مما يؤدي إلى خدمة المجتمع الدولي بأكمله، فهذه التكنولوجيا تخدم جميع مجالات الحياة، حيث بات هذا العصر يتحرك من خلال تكنولوجيا المعلومات والاتصالات، التي واكبتها حركة إجرامية كبيرة، فانتشرت الجرائم الإلكترونية بشكل واضح وكبير في جميع دول العالم، فالجميع يستخدم الحاسب الآلي، والجميع معرض للوقوع تحت تهديد هذه الجرائم، وهي دون أدنى شك جرائم من نوع فريد، تحتاج إلى تشريعات خاصة وقوية، وإلى وسائل إثبات مختلفة ومعقدة^(١).

أولاً: مفهوم الجرائم الإلكترونية:

لا يوجد تعريف موحد للدلالة على الجرائم الإلكترونية، فتعددت التعاريف واختلفت باختلاف وجهات النظر، ويمكن عرض أهم التعاريف التي تناولت مفهوم الجريمة الإلكترونية كما يلي:

تعرف الجريمة الإلكترونية بأنها "أنماط من الجريمة تستخدم فيها التقنية الحديثة من أجل تسهيل عملية الإجرام"^(٢).

كما عرفت هذه الجريمة على أنها "سلوك غير مشروع معاقب عليها قانوناً صادر عن إرادة جرمية محله معطيات الحاسوب"^(٣).

(١) عبد الله، الأزرق. (٢٠١٠). مؤتمر البيئة المعلوماتية الآمنة. الرياض، جمعية المكتبات والمعلومات السعودية، ص ٢.

(٢) اليوسف، عبد الله بن عبد العزيز. (١٩٩٩). الظواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض، جامعة نايف العربية للعلوم الأمنية، ص ١٣.

(٣) المرزوقي، محمود محمد. (٢٠٠٣). جرائم الحاسب الآلي. المجلة العربية للفقه والقضاء، العدد ٢٨، الأمانة العامة لجامعة الدول العربية، ص ٥٣.

وتعرف الجريمة الإلكترونية أيضاً بأنها "النشاط الإجرامي الذي تستخدم فيه التقنية الإلكترونية الرقمية بصورة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف"^(١).

كما تعرف الجريمة الإلكترونية على أنها "الجريمة التي يتم ارتكابها إذا قام شخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة، ومصلحة الأفراد الخاصة"^(٢).

وقد عرفت الجريمة الإلكترونية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"^(٣).

وقد عرفها نظام مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية بأنها "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"^(٤).

كما عرفها السراني بأنها "استخدام الحاسب الآلي وتقنية الاتصال والمعلومات في عمليات الاختراق والتعدي على البيانات والملفات والمعلومات بسرقتها أو تغيير محتواها أو تزويرها، لاستغلالها في عمليات بيع وشراء وهمية، أو تحويل حسابات لصالح الجاني بعد سرقة بيانات بطاقات الائتمان الخاصة بالآخرين"^(٥).

والجريمة الإلكترونية ناشئة أساساً من التقدم التكنولوجي ومدى التطور الذي يطرأ عليه وهو متجدد بصفة دائمة ومستمرة وخاصة في مجال تكنولوجيا المعلومات ويطلقون عليه اصطلاح "جرائم التكنولوجيا الحديثة"، فهي جرائم تكنولوجيا باعتبارها مرتبطة

(١) موسى، مصطفى محمد. (٢٠٠٣). أساليب إجرامية للتقنية الرقمية: ماهيتها، مكافحتها، القاهرة، دار النهضة العربية، ص ٥٦.

(٢) أبكر، سليمان مصطفى. (١٤٢٢هـ). جرائم الحاسب الآلي. مجلة الأمن والحياة. العدد ٢٤٢، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ص ٥٠.

(٣) القحطاني، منصور بن سعيد. (٢٠٠٨). مهددات الأمن المعلوماتي وسبل مواجهتها. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، ص ٢٣.

(٤) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧هـ، المادة ١، الفقرة ٨.

(٥) السراني، عيد الله بن سعود محمد. (٢٠٠٩). فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، قسم العلوم الشرطية، ص ١٧.

ارتباطاً وثيقاً بالتكنولوجيا التي تعتمد أساساً على الحواسيب، وغيرها من أجهزة تقنية قد تظهر في المستقبل، وهي كذلك جرائم حديثة، نظراً لحدوثها النسبية من ناحية وارتباطها الوثيق بما قد يظهر من أجهزة حديثة تكون ذات طاقة تخزينية وسعة فائقة، ومرونة في المستقبل^(١).

وتعرف الجريمة الإلكترونية على أنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه وذلك عن طريق كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"^(٢).

وعند المقارنة بين هذه التعاريف يظهر لي أن أشمل تعريف للجريمة الإلكترونية هو تعريف قطب الذي يرى الجريمة الإلكترونية على أنها "الجريمة التي تتم باستخدام الحاسب الآلي، أو تلك التي تقع على الحاسب الآلي ذاته"^(٣). ويوضح هذا التعريف أن الجريمة الإلكترونية لها ركنان أساسيان يمكن توضيحهما كما يلي^(٤):

(١) الركن المادي في الجريمة الإلكترونية: إن النشاط أو السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة رقمية واتصال بالإنترنت ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسب؛ لكي يحقق 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، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبحثها.

(١) المويشير، تركي بن عبد الرحمن. (٢٠٠٩). بناء أنموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته. الرياض، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، ص ١٥-١٦.
(٢) عبد الله، الأزرق. (٢٠١٠). مؤتمر البيئة المعلوماتية الآمنة. مرجع سابق، ص ٢.
(٣) قطب، محمد علي. (٢٠١٠). الجرائم المعلوماتية وطرق مواجهتها. مملكة البحرين، وزارة الداخلية، الأكاديمية الملكية للشرطة، ص ٢.
(٤) المرجع السابق، ص ٢-٣.

(٢) **الركن المعنوي في جريمة الإنترنت:** ويتضح الركن المعنوي للجريمة من خلال توضيح الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني.

ومن خلال ما سبق، يمكن تعريف الجريمة الإلكترونية على أنها كل انحراف يستخدم الحاسب الآلي أو أي جهاز رقمي آخر بطريقة غير صحيحة لأهداف تخريبية.

ثانياً: خصائص الجرائم الإلكترونية:

تتميز الجرائم الإلكترونية بخصائص تختلف إلى حد ما عن الجريمة العادية، ويمكن توضيح خصائص هذه الجرائم الإلكترونية كما يلي:

(١) جرائم ناعمة ومغرية للمجرمين:

إذا كانت الجريمة بصورتها التقليدية تحتاج في الأغلب إلى مجهود عضلي من نوع ما كجرائم القتل، السرقة، الاغتصاب، فإن الجريمة الإلكترونية على العكس لا تحتاج إلى أدنى مجهود عضلي، بل تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي، ولذا كان الشرط الأساسي في المجرم توافر العلم الكافي بكيفية عمل الحاسب الآلي وآلية تشغيله، بالإضافة إلى الإحاطة ببعض البرامج التشغيلية هذا فيما يخص نعومة هذه الجرائم^(١).

أما الإغراءات التي تجذب المجرمين نحو هذه الجرائم أنها في الحقيقة جرائم سريعة التنفيذ، إذ غالباً ما يتمثل الركن المادي فيه باستعمال جهاز الحاسب الآلي، مع إمكانية تنفيذ ذلك عن بعد، دون اشتراط الوجود في مسرح الجريمة. وأيضاً ضخامة الفوائد والمكاسب التي يستطيع الجاني تحقيقها باقتراف مثل هذه الجرائم، دون جهد يذكر، ودون أن يخاف أن يكتشف أمره. كما أن الجرائم الإلكترونية يمكن اعتبارها بمثابة إغراء كبير للمجرمين، لاستغلال التكنولوجيا الحديثة، بغية اقتراف الجرائم بصورها المتعددة، خصوصاً عندما يكون الجاني موظفاً في شركة تعتمد الحاسب الآلي

(١) أبكر، مصطفى سليمان. (٢٠١٤ هـ). جرائم الحاسوب وأساليب مواجهتها. مجلة الأمن والحياة، العدد (٢١٠)، السنة ١٩، ص ٤٧.

في عملها، إذ يكون لديه كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسب الآلي في الشركة، وتحقيق أرباح طائلة، والواقع يثبت ذلك^(١).

٢) جرائم عابرة للدول:

يطلق تعبير "جرائم عابرة للدول" أو جرائم غير وطنية على تلك الجرائم التي تقع بين أكثر من دولة، بمعنى أنها لا تعترف بالحدود الجغرافية للدول كجرائم تبييض الأموال، والمخدرات وغيرها. وفي عصر الحاسب الآلي، ومع انتشار شبكة الاتصالات العالمية (الإنترنت)، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر التنقل والاتصال فيما بينها أمراً سهلاً، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة، أو غير مشروعة. وفي هذه البيئة يمكن أن توصف الجريمة الإلكترونية بأنها جرائم عابرة للدول، إذ غالباً ما يكون الجاني في بلد، والمجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه. وعليه تعتبر الجرائم الإلكترونية شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية. وإذا تقرر أن الجرائم الإلكترونية جرائم عابرة للدول تظهر الحاجة الملحة للتعاون الدولي في مجال مكافحة هذه الجرائم وضبط فاعليها، وتجدر الإشارة هنا إلى جهود الإنتربول في هذا المجال، من خلال ضباط الارتباط المنتشرين في كافة الدول عبر العالم، والمكلفين بتوفير قاعدة بيانات ضخمة يمكن أن تشكل نقطة انطلاق للمكافحة والتصدي لهذه الجرائم^(٢).

٣) سرعة التنفيذ:

من خصائص الجريمة الإلكترونية سرعة التنفيذ، بحيث يمكن تنفيذها خلال جزء من الثانية وبصورة خفية لا يلحظها المجني عليه، كما أنها تتم في بيئة خاصة هي بيئة

(١) أبكر، مصطفى سليمان. (١٤٢٠هـ). جرائم الحاسوب وأساليب مواجهتها، ص ٤٧.
(٢) محمود، عبد الله حسين. (٢٠٠٢). سرقة المعلومات المخزنة في الحاسب الآلي. القاهرة، دار النهضة العربية، الطبعة الثانية، ص ٣٦١-٣٦٢.

المعالجة الآلية للبيانات، وتتميز بخطورتها المتناهية على الأفراد والحكومات والشركات، وهذا يهدد الأمن السياسي والأمن الاقتصادي للدول. يضاف إلى ذلك صعوبة اكتشافها ومتابعتها وتطبيق الإجراءات الجنائية عليها من حيث جمع الأدلة والمعاينة والتفتيش والتحقيق فيها، وإمكانية تدمير الأدلة الناجمة عنها، كما أنها تحتاج إلى خبرة خاصة، هذا فضلاً عن ضخامة البيانات التي تحويها الشبكة المعلوماتية، واتساع نطاقها المكاني^(١).

٤) صعوبة اكتشاف الجريمة الإلكترونية:

تتميز الجريمة الإلكترونية بصعوبة اكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة الإلكترونية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، وكذلك اختفاء السلوك المكون لها، كما إن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، إذ إن الجريمة الإلكترونية جريمة عابرة للدول (دولية)، وكذلك فإن قدرة الجاني على تدمير الإدانة في أقل من الثانية الواحدة يشكل عاملاً إضافياً في صعوبة اكتشاف هذا النوع من الجرائم^(٢). فالجريمة الإلكترونية في أكثر صورها خفية لا يلحظها المجني عليه أو لا يدري حتى بوقوعها، والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أمر ليس عسيراً في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات لدى مرتكبيها^(٣).

كما أن المجني عليه يلعب دوراً رئيسياً في صعوبة اكتشاف وقوع الجريمة الإلكترونية، حيث تحرص أكثر الجهات التي تعرضت أنظمتها المعلوماتية للانتهاك أو

(١) البقمي، ناصر محمد (٢٠٠٨). مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، أبو ظبي، مركز الإمارات للدراسات والبحوث الإستراتيجية، ص ١٢.
(٢) الصغير، جميل عبد الباقي. (١٩٩٢). الجرائم الناشئة عن استخدام الحاسب الآلي. القاهرة، دار النهضة العربية، الطبعة الأولى، ص ١٧.
(٣) رستم، هشام محمد فريد. (١٩٩٤). الجوانب الإجرامية للجوانب المعلوماتية. مجلة الأمن والقانون، العدد الثاني، شرطة دبي، ص ١٦.

منيت بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له، وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها^(١).

ويرى البعض أن للمجني عليه دوراً مثيراً للريبة في بعض الأحيان فهو قد يشارك بطريق غير مباشر في ارتكاب الفعل ويرجع ذلك بشكل أساسي إلى القصور الذي يعتري الأنظمة المعلوماتية الذي قد يساعد على ارتكاب الفعل الإجرامي، ويترتب على ذلك نتيجة أخرى تميز الجريمة الإلكترونية هي أن هناك إمكانية للحيلولة دون وقوع الجريمة مقارنة بغيرها من الجرائم إذ يعتمد ذلك بشكل أساسي على تطوير نظم الأمن الخاصة بأنظمة الحاسبات وشبكاتها^(٢).

وفي الواقع فإن إحجام المجني عليه عن الإبلاغ عن وقوع الجريمة الإلكترونية يبدو أكثر وضوحاً في المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة، حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم، أو اتخاذ الإجراءات القضائية حيالها إلى تضاول الثقة فيها من جانب المتعاملين معها، حيث إن الجانب الأكبر من الجريمة الإلكترونية لا يتم الكشف أو التبليغ عنها وذلك يؤثر سلباً في السياسة التي يمكن أن توضع لمكافحتها، وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم ومن ثم إنقاص حجم الجرائم الإلكترونية^(٣).

والى جانب ذلك، فإن المجني عليه يتردد أحياناً في الإبلاغ عن هذه الجرائم، خوفاً من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي إلى تكرار وقوعها بناء على تقليدها من قبل الآخرين، كما أن الإعلان عن هذه الجرائم يؤدي إلى الكشف عن

(١) المرجع السابق، ص ٢٥-٢٦.

(٢) قورة، نانلة. (٢٠٠٤). جرائم الحاسب الاقتصادية. القاهرة، دار النهضة العربية، الطبعة الأولى، ص ٤٦.

(٣) رستم، هشام محمد فريد. (١٩٩٤). الجوانب الإجرامية للجوانب المعلوماتية. مرجع سابق، ص ٢٥.

مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي، مما يسهل عملية اختراقه^(١).

٥) صعوبة إثبات الجريمة الإلكترونية:

يعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية، ويزداد الإثبات صعوبة في الجريمة الإلكترونية، حيث إن اكتشاف الجريمة الإلكترونية أمر ليس بالسهل، ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كثير من الصعاب، فالجريمة الإلكترونية تتم في بيئة غير تقليدية، حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والإنترنت، مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر محو الدليل كلياً من قبل الفاعل أمراً غير مستحيل^(٢).

كما أن وسائل المعاينة وطرقها التقليدية لا تغلح غالباً في إثبات هذه الجريمة نظراً لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف أثراً مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة الإلكترونية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين^(٣):

الأول: أن الجريمة الإلكترونية لا تخلف أثراً مادية.

(١) الهيتي، محمد حماد. (٢٠٠٤). التكنولوجيا الحديثة والقانون الجنائي. عمان، جاز الثقافة للنشر والتوزيع، ص ١٦٦.

(٢) رستم، هشام محمد فريد. (١٩٩٤). الجوانب الإجرامية للجوانب المعلوماتية. مرجع سابق، ص ٢٣.

(٣) حجازي، عبد الفتاح. (٢٠٠٢). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت. القاهرة، دار الكتب القانونية، ص ٥٩.

الثاني: أن كثيراً من الأشخاص يترددون على مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي فترة طويلة نسبياً، الأمر الذي يعطي مجالاً للجاني أو للآخرين أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة الإلكترونية.

وبالإضافة إلى ذلك فإن نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الإدعاء والقضاء يشكل عائقاً أساسياً أمام إثبات الجريمة الإلكترونية، ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والإنترنت، ونتيجة لنقص الخبرة والتدريب كثيراً ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة الإلكترونية، فلا تبذل لكشف غموضها وضبط مرتكبيها جهوداً تتناسب وهذه الأهمية، بل إن المحقق قد يدمر الدليل - الذي له علاقة بالجريمة المرتكبة والتي يرشد إليها - بمحوه محتويات الأسطوانة الصلبة عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة^(١).

٦) أسلوب ارتكاب الجريمة الإلكترونية:

ذاتية الجرائم الإلكترونية تبرز بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعاً من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح، كما هو الحال في جريمة السرقة، فإن الجرائم الإلكترونية هي جرائم هادئة بطبيعتها، لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في الأفعال غير المشروعة، وقد تحتاج كذلك إلى وجود شبكة المعلومات الدولية (الإنترنت) مع وجود

(١) المرجع السابق، ص ٢٩.

مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التعزير بالقاصرين كل ذلك دون حاجة لسفك الدماء^(١).

٧) الجريمة الإلكترونية تتم بتعاون أكثر من شخص:

تتميز الجريمة الإلكترونية بأنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضراراً بالجهة المجني عليها، وغالباً ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب، وتحويل المكاسب إليه.

والاشتراك في إخراج الجريمة الإلكترونية إلى حيز الوجود قد يكون اشتراكاً سلبياً وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكاً إيجابياً وهو غالباً كذلك يتمثل في مساعدة فنية أو مادية^(٢).

٨) خصوصية مجرمي المعلومات:

المجرم الذي يقترب الجريمة الإلكترونية، والذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا أثر فيها للمستويين العلمي والمعرفي للمجرم في عملية ارتكابها باعتبارها قاعدة عامة، فإن الأمر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت، فعلى سبيل المثال، فإن الجرائم الإلكترونية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جداً من قبل مرتكبها، كذلك فإن البواعث على ارتكاب المجرم

(١) المويشير، تركي بن عبد الرحمن. (٢٠٠٩). بناء أنموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته. مرجع سابق، ص ٢٤.

(٢) قورة، نائلة. (٢٠٠٤). جرائم الحاسب الاقتصادية. القاهرة، دار النهضة العربية، الطبعة الأولى، ص ٣٢.

المعلوماتي لهذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي^(١).

ثالثاً: تصنيف الجرائم الإلكترونية:

هناك العديد من التصنيفات المختلفة للجرائم الإلكترونية، ويمكن توضيح هذه التصنيفات للجرائم الإلكترونية كما يلي:

١) تصنيف الجرائم تبعاً لنوع المعطيات ومحل الجريمة:

يتفق هذا التصنيف مع قوانين تقنية المعلومات، كما يعكس هذا التصنيف التطور التاريخي لظاهرة جرائم الكمبيوتر والإنترنت، ويقسم هذا التصنيف الجرائم الإلكترونية إلى الطوائف التالية^(٢):

أولاً: الجرائم الماسة بقيمة معطيات الحاسوب، ويشمل هذا النوع فئتين، أولهما، الجرائم الواقعة على ذات المعطيات، كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات) التقنية.

وثانيهما، الجرائم الواقعة على ما تمثله المعطيات آلياً، من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات، وجرائم التحويل والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها (تزوير المستندات المعالجة آلياً واستخدامها).

ثانياً: الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة، وتشمل جرائم الاعتداء على المعطيات السرية والمحمية، وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة.

ثالثاً: الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات) التي تشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص والاعتداء على العلامة التجارية وبراءة الاختراع.

(١) المويشير، تركي بن عبد الرحمن. (٢٠٠٩). بناء أنموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته. مرجع سابق، ص ٢٥.

(٢) عرب، يونس. (٢٠٠٦). تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية. ورقة عمل مقدمة لمؤتمر هيئة تنظيم الاتصالات في الفترة من ٢-٤ أبريل ٢٠٠٦، سلطنة عمان، مسقط، ص ٩.

وبإمعان النظر في هذه الطوائف، يتضح أن الحدود بينها ليست قاطعة ومانعة، فالتداخل متحقق فيما بينها، إذ إن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر المحرك للاعتداء يتضح من خلال قيمة هذه المعلومات. والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج^(١).

كما أن الحماية الجنائية للمعلومات الرقمية في نطاق القانون المقارن وفي إطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج، وحماية البيانات الشخصية المتصلة بالحياة الخاصة وحماية المعطيات بالنظر لقيمتها أو ما تمثله والذي عرف بحماية (الأموال)، كل في ميدان وموقع مستقل. وهو في الحقيقة تمييز بين حماية قيمة المعطيات، وأمنها، وحقوق الملكية الفكرية. لذلك فإن حماية أمن المعطيات (الطائفة الثانية) انحصرت في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرائم الطائفة الأولى الماسة بقيمة المعطيات بالنظر إلى أن الباعث الرئيسي للاعتداء والغرض من معرفة أو إفشاء هذه المعلومات غالباً ما يكون بسبب الحصول على المال مما يعد من الاعتداءات التي تدرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم^(٢).

٢) تصنيف الجرائم تبعا لدور التقنية الرقمية في الجريمة:

يلعب الحاسب الآلي دوراً مهماً في الجريمة الإلكترونية، فقد يكون هدف الاعتداء، هو استهداف المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر والشبكات، وهذا ما يعبر عنه بالمفهوم الضيق لجرائم الكمبيوتر وقد يكون الكمبيوتر

(١) عوض، محمد محيي الدين. (١٩٩٣). مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات. ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ص ٢٣.

(٢) عرب، يونس. (٢٠٠٦). تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية. مرجع سابق، ص ١٠.

وسيلة ارتكاب جريمة أخرى في إطار مفهوم (الجرائم المرتبطة بالكمبيوتر)، وقد يكون الكمبيوتر بيئة الجريمة أو مخزناً للمادة الجرمية، وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن هذا الدور:

الأول: جرائم التخزين: ويقصد بها تخزين المواد الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها.

الثاني: جرائم المحتوى: أو ما يعبر عنه بالمحتوى غير المشروع أو غير القانوني والاصطلاح الأخير استخدم في ضوء تطور أشكال الجريمة مع استخدام الإنترنت، وأصبح المحتوى غير القانوني يرمز إلى جرائم المقامرة ونشر المواد الإباحية والغسيل الإلكتروني للأموال وغيرها باعتبار أن مواقع الإنترنت تتصل بشكل رئيس بهذه الأنشطة^(١).

والحقيقة أن كلاً من المفهومين يتصل بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفي نفس الوقت كوسيلة لارتكابها. ومن خلال هذا التقسيم فإن جرائم الكمبيوتر تنقسم إلى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات وإتلافها، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر. أما تقسيمها كجرائم هدف ووسيلة ومحتوى فانه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية لجرائم الكمبيوتر والإنترنت، حيث إن هناك اتجاه إلى وضع إطار عام لتصنيف الجرائم الإلكترونية، حيث يمكن تقسيمها تبعاً لدور الكمبيوتر في الجريمة كما يلي^(٢):

الأولى: الجرائم التي تستهدف عناصر السرية والسلامة ووفرة المعطيات والنظم وتضم:

- الدخول غير القانوني (غير المصرح به).

- الاعتراض غير القانوني.

- تدمير المعطيات.

(١) البشري، محمد الأمين. (٢٠٠٠). التحقيق في جرائم الحاسب الآلي. بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١-٢ مايو ٢٠٠٠، الإمارات، كلية الشريعة والقانون، ص ١٩.
(٢) رستم، هشام محمد فريد. (١٩٩٤). الجوانب الإجرامية للجوانب المعلوماتية. مرجع سابق، ص ٣٣-٣٤.

- اعتراض النظم.

- إساءة استخدام الأجهزة.

الثانية: الجرائم المرتبطة بالأجهزة الرقمية وتضم:

- التزوير المرتبط بالأجهزة الرقمية.

- الاحتيال المرتبط بالأجهزة الرقمية.

الثالثة: الجرائم المرتبطة بالمحتوى وتضم: الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.

الرابعة: الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق وقرصنة البرمجيات.

(٣) تصنيف الجرائم تبعاً لمساسها بالأشخاص والأموال:

يتم تقسيم الجرائم الإلكترونية طبقاً لهذا التصنيف إلى الجرائم الواقعة على الأشخاص، والجرائم الواقعة على الأموال، وجرائم السرقة والاحتيال، وجرائم التزوير، وجرائم المقامرة والجرائم ضد الآداب، والجرائم ضد المصالح الحكومية ويلاحظ أن التقسيم يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء، لكنه ليس تقسيماً منضبطاً ولا هو تقسيم محدد الأطر، فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة والاحتيال، أما الجرائم التي تستهدف التزوير فتتمس الثقة والاعتبار، والجرائم الواقعة ضد الآداب قد تتصل بالشخص وقد تتصل بالنظام والأخلاق العامة^(١)، ومن خلال ذلك تقسم جرائم الكمبيوتر طبقاً لهذا التصنيف إلى ما يلي:

أولاً: الجرائم التي تستهدف الأشخاص:

تنقسم الجرائم التي تستهدف الأشخاص إلى ما يلي:

أ - الجرائم غير الجنسية التي تستهدف الأشخاص: وتشمل جرائم الإهمال المرتبط بالكمبيوتر، والتحرّيز على الانتحار، والتحرّيز القسدي للقتل عبر الإنترنت والتحرّش والمضايقة عبر وسائل الاتصال والتهديد عبر وسائل الاتصال

(١) غنام، محمد غنام. (٢٠٠٠). عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر. بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١-٢ مايو ٢٠٠٠، الإمارات، كلية الشريعة والقانون. ص ٢١-٢٢.

والإحداث المتعمد للضرر العاطفي أو التسبب بضرر عاطفي عبر وسائل التقنية والملاحقة عبر الوسائل التقنية وأنشطة اختلاس النظر أو الاطلاع على البيانات الشخصية وقنابل البريد الإلكتروني وأنشطة ضخ البريد الإلكتروني غير المطلوب أو غير المرغوب به وبث المعلومات المضللة أو الزائفة والانتهاك الشخصي لحرمة كمبيوتر (الدخول غير المصرح به) ^(١).

ب - **الجرائم الجنسية التي تستهدف الأشخاص:** وتشمل حض وتحريض القاصرين على أنشطة جنسية غير مشروعة، وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية، وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة، وتلقي أو نشر المعلومات عن القاصرين عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة، والتحرش الجنسي بالقاصرين عبر الكمبيوتر، والوسائل التقنية، ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام، وللقاصرين تحديداً، ونشر الفحش والمساس بالحياء عبر الإنترنت، وتصوير أو إظهار القاصرين ضمن أنشطة جنسية، واستخدام الإنترنت لترويج الدعارة بصورة قسرية، أو لنشر المواد الفاحشة التي تستهدف عوامل الضعف والانحراف لدى المستخدم، والحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية، وإمعان النظر في هذه الأوصاف نجد أنها تجتمع جميعاً تحت صورة واحدة هي استغلال الإنترنت والكمبيوتر لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة ^(٢).

ثانياً: الجرائم التي تستهدف الأموال:

يمكن تقسم الجرائم التي تستهدف الأموال كما يلي:

أ - **جرائم الاحتيال والسرقة:** وتشمل جرائم الاحتيال بالتلاعب بالمعطيات والنظم واستخدام الكمبيوتر أو استخدام البطاقات المالية للغير دون ترخيص أو تدميرها

(١) عرب، يونس. (٢٠٠٦). تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية. مرجع سابق، ص ١٢.
(٢) رستم، هشام محمد فريد. (١٩٩٤). الجوانب الإجرامية للجوانب المعلوماتية. مرجع سابق، ص ٤١.

والاختلاس عبر الكمبيوتر أو بواسطته وسرقة معلومات الكمبيوتر وقرصنة البرامج وسرقة خدمات الكمبيوتر (وقت الكمبيوتر) وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر^(١).

ب - جرائم التزوير والمقاومة والجرائم الأخرى ضد الأخلاق والآداب: وتشمل تزوير البريد الإلكتروني وتزوير الوثائق والسجلات وتزوير الهوية وتشمل أيضاً تملك وإدارة القمار على الإنترنت وتسهيل إدارة مشاريع القمار على الإنترنت وتشجيع مشروع مقاومة عبر استخدام الإنترنت لترويج الكحول ومواد الإدمان للقصر^(٢).

٤) تصنيف الجرائم كجرائم الكمبيوتر وجرائم الإنترنت:

من الطبيعي أن يكون هناك مفهوم لجرائم ترتكب على الكمبيوتر وبواسطته قبل أن يشيع استخدام شبكات المعلومات وتحديدًا الإنترنت، ومن الطبيعي أن يخلق الإنترنت أنماطاً جرمية مستجدة أو تأثر بالآلية التي ترتكب فيها جرائم الكمبيوتر ذاتها بعد أن تحقق تشابك الكمبيوترات معاً في نطاق شبكات محلية وإقليمية وعالمية، أو على الأقل تشكل أنماط فرعية من الصور القائمة تختص بالإنترنت ذاتها، وفي نطاق هذا المعيار يجري التمييز بين الأفعال التي تستهدف المعلومات في نطاق نظام الكمبيوتر ذاته وبين الأنشطة التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها، وأيضاً الأنشطة التي تستهدف مواقع الإنترنت وخوادمها من نظم الكمبيوتر الكبيرة والعلاقة أو تستهدف تطبيقات واستخدامات وحلول الإنترنت وما نشأ في بيئتها من أعمال إلكترونية وخدمات إلكترونية^(٣).

وفي إطار هذه الرؤيا، نجد البعض يحصر أنشطة جرائم الإنترنت بتلك المتعلقة بالاعتداء على المواقع وتعطيلها أو تشويهها أو تعطيل تقديم الخدمة، وكذلك أنشطة المحتوى الضار، كترويج المواد الإباحية والمقاومة، وأنشطة إثارة الأحقاد والتحرش

(١) البقمي، ناصر محمد (٢٠٠٨). مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، مرجع سابق، ص ٢٩.

(٢) المرجع السابق، ص ٣١.

(٣) جهاد، جودة حسين. (٢٠٠٠). المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية. بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١-٢ مايو ٢٠٠٠، الإمارات، كلية الشريعة والقانون، ص ٢٩.

والإزعاج ومختلف صور الأنشطة التي تستخدم البريد الإلكتروني والمراسلات الإلكترونية، وأنشطة الاستيلاء على كلمات سر المستخدمين والهوية ووسائل التعريف، وأنشطة الاعتداء على الخصوصية عبر جمع المعلومات من خلال الإنترنت، وأنشطة احتيال الإنترنت كاحتيال المزادات وعدم التسليم الفعلي للمنتجات والخدمات، وأنشطة نشر الفيروسات والبرامج الخبيثة عبر الإنترنت، وأنشطة الاعتداء على الملكية الفكرية التي تشمل الاستيلاء على المواد والمصنفات المحمية وإساءة استخدام أسماء النطاقات أو الاستيلاء عليها أو استخدامها خلافاً لحماية العلامة التجارية وأنشطة الاعتداء على محتوى المواقع والتصميم، وأنشطة الروابط غير المشروعة وأنشطة الأطر غير المشروعة (وهي أنشطة يقوم من خلالها أحد المواقع بإجراء مدخل لربط مواقع أخرى أو وضعها ضمن نطاق الإطار الخارجي لموقعه هو وغيرها من الجرائم التي يجمعها مفهوم (جرائم الملكية الفكرية عبر الإنترنت)^(١).

أما جرائم الكمبيوتر فإنها تعاد إلى الأنشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر وتحديدًا أنشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الحاسوب واعتراض المعطيات خلال النقل (مع أنه مفهوم يتصل بالشبكات أكثر من نظم الكمبيوتر)، بالإضافة إلى التدخل غير المصرح به والذي يتوزع بين دخول غير مصرح به لنظام الكمبيوتر ودخول غير مصرح به للشبكات فيتبع لمفهوم جرائم الإنترنت^(٢).

(١) عرب، يونس. (٢٠٠٢). جرائم الكمبيوتر والانترنت. ورقة عمل مقدمة إلى مؤتمر الأمن العربي المنعقد في الفترة من ١٠-١٢ / ٢٠٠٢، أبو ظبي، المركز العربي للدراسات والبحوث الجنائية، ص ٣٥-٣٦.
(٢) المزمومي، محمد بن حميد. (٢٠٠٧). جريمة الاعتداء على الأموال عن طريق الحاسب الآلي. رسالة ماجستير غير منشورة، جامعة الملك عبد العزيز بجدة، ص ٤٥.

المبحث الثاني

الجريمة الإلكترونية في النظام السعودي والفقه الإسلامي

يدخل نظام الجرائم الإلكترونية في الوقت الحالي حيز التنفيذ في المملكة العربية السعودية، حيث تبدأ من خلاله الأجهزة الأمنية بملاحقة ومقاضاة كل من يستخدم الشبكة العنكبوتية كوسيلة للنصب والاحتيال، أو يعتمد إلى إتلاف وتشويه البيانات والمعلومات والتلاعب بالمواد المخزنة، بالإضافة إلى الجرائم المرتبطة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه "جرائم قرصنة البرمجيات" كالنسخ والتقليد، بما في ذلك انتحال شخصيات أخرى بطريقة غير شرعية على الإنترنت، أو المضايقة والملاحقة برسائل التهديد والتخويف لإحكام السيطرة على الضحية، أو اعتماده كأداة للتشهير وتشويه السمعة أو التغرير والاستدراج، ومن خلال ذلك يتم مناقشة الجريمة الإلكترونية في النظام السعودي وفي الفقه الإسلامي.

أولاً: الجريمة الإلكترونية في النظام السعودي:

تبذل المملكة العربية السعودية جهوداً جادة في تنظيم تقنية المعلومات وحمايتها من الجرائم التي تقع ضدها، ويوضح النظام السعودي أن الجرائم الإلكترونية هي الجرائم التي تقع عن طريق الكمبيوتر والإنترنت، وتعتبر هذه الجرائم من الموضوعات المهمة التي تثير جوانب جديدة ترجع إلى اتصالها بتطور وسائل التعاملات بسبب انتشار استخدام الكمبيوتر وخاصة استعمال شبكة الإنترنت، فقد أصبحت هذه الشبكة ذات طابع دولي يتاح لجميع الأفراد في العالم التعامل من خلالها وذلك بإبرام الصفقات المختلفة وتبادل المعلومات والمراسلات الخاصة^(١).

فالتعاملات بطريق الوسائل الإلكترونية أصبحت تشكل قمة التطور في التبادلات بين الأفراد والشركات والجهات المختلفة. فقد كان على المشتري أن يتقابل مع البائع فيما يسمى بمجلس العقد الذي يتقابل فيه الإيجاب والقبول، ثم تطورت تلك الفكرة وأصبح مجلس العقد أكثر اتساعاً بتطور وسائل الاتصالات؛ منها الاتصالات

(١) الصغير، جميل عبد الباقي. (٢٠٠٢). الإنترنت والقانون الجنائي. القاهرة، دار النهضة العربية، ص ٦.

الهاتفية، والفاكس. فبعد أن كانت وسيلة إتمام التبادلات هو نظام المقايضة حيث يقوم البائع بتسليم سلعة إلي المشتري في نظير تسلمه لسلعة من هذا الأخير كمقابل لها، وذلك قبل ظهور النقود، ثم تطور الأمر بتداول العملات المعدنية والورقية التي سهلت التبادلات بين الناس. واستمر التطور بظهور فكرة العملة الإلكترونية، والتي لا تشكل نقوداً معدنية ولكن وحدات إلكترونية يتم سحبها من حساب إلى آخر دون استعمال نقود معدنية. لذلك كانت حماية التعاملات الإلكترونية ضرورة من ضرورات التطور التقني في العصر الحديث بسبب تطور تقنيات الاتصالات^(١).

ومن خلال تطور الوسائل والتعاملات الإلكترونية، فقد وافق مجلس الوزراء في ١٤٢٨/٣/٧ هـ الموافق ٢٠٠٧/٣/٢٦ علي نظامي مكافحة جرائم المعلوماتية والتعاملات الإلكترونية، وكان ذلك للحد من وقوع الجرائم الإلكترونية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة، فهدف هذا النظام قد حددته المادة الثانية منه "يهدف هذا النظام إلى ضبط التعاملات والتوقيعات الإلكترونية، وتنظيمها وتوفير إطار نظامي لها بما يؤدي إلى تحقيق ما يلي^(٢):

(١) إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بوساطة سجلات إلكترونية يعول عليها.

(٢) إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإلكترونية وسلامتها.

(٣) تيسير استخدام التعاملات والتوقيعات الإلكترونية على الصعيدين المحلي والدولي للاستفادة منها في جميع المجالات، كالإجراءات الحكومية والتجارة والطب والتعليم والدفع المالي الإلكتروني.

(٤) إزالة العوائق أمام استخدام التعاملات والتوقيعات الإلكترونية.

(٥) منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإلكترونية".

(١) خيال، محمود السيد عبد المعطي. (١٩٩٨). الانترنت وبعض الجوانب القانونية. القاهرة، دار النهضة العربية، ص ٦.

(٢) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧ هـ، المادة ٢.

وقد عرفت المادة الأولى من النظام السعودي المقصود بالنظام المعلوماتي بأنه "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية"، كما عرفت المقصود بالشبكة بأنها ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها"^(١)، وجاءت المواد من الثالثة (٣) إلى العاشرة (١٠)، لتحديد أنواع الجرائم الإلكترونية والعقوبة المقررة عليها فمثلاً تنص المادة الثالثة (٣)، "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو إحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم الإلكترونية الآتية"^(٢):

- (١) التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح أو النقطه أو اعتراضه.
- (٢) الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.
- (٣) الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
- (٤) المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.
- (٥) التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة".

كما تنص المادة الرابعة (٤)، على أنه "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم الإلكترونية الآتية"^(٣):

- (١) الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة.

(١) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧ هـ، المادة الأولى (١).

(٢) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧ هـ، المادة الثالثة (٣).

(٣) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧ هـ، المادة الرابعة (٤).

٢) الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو اتثمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول علي بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

ونصت باقي المواد علي جرائم الدخول غير المشروع لإلغاء البيانات أو حذفها، وإيقاف الشبكة أو تعطيلها أو إعاقة الوصول إلى الخدمة أو تشويشها، وأيضاً إنشاء المواقع للاتجار بالجنس البشري، وإنشاء المواد أو البيانات الإباحية، وأيضاً يعاقب القانون على إنشاء موقع لمنظمات إرهابية أو الاتجار بالمخدرات.

وقد عرف نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية الجريمة الإلكترونية على أنها الدخول غير المشروع في المادة الأولى منه بقوله "الدخول غير المشروع، دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"^(١).

فالدخول إذن هو فعل المخترق الذي يستعمل عادة برامج تمكنهم من الدخول إلى أنظمة الغير الخاصة من على بعد. غير أن الدخول يشمل كل استعمال للحاسب الآلي دون رضا صاحب الحق فيه، أي كانت صورة ذلك الاستعمال، كما لو تمكن الفاعل من تشغيله مباشرة أو عن بعد^(٢).

ويلاحظ أن تجريم الدخول في النظام يشكل تجريماً غير مسبوق حيث إن التشريعات تدرج على تجريم الدخول إلى مسكن الغير بدون رضا صاحبه أو الدخول إلى عقار للاستيلاء على حيازته ضد إرادة صاحبة. أما في حالة النظام فالأمر في تجريم الدخول ليس تجريماً مادياً بل هو تجريم معنوي، فالفاعل لا يقوم بالدخول إلى النظام بالكسر أو باستعمال مفاتيح مصطنعة، بل يمكن أن يتم ذلك من على بعد باستعمال برامج الاختراق^(٣).

(١) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧ هـ، المادة الأولى، الفقرة السابعة.

(٢) الصغير، جميل عبد الباقي. (١٩٩٢). القانون الجنائي والتكنولوجيا الحديثة. القاهرة، دار النهضة العربية، ص ٦٦.

(٣) خيال، محمود السيد عبد المعطي. (١٩٩٨). الانترنت وبعض الجوانب القانونية. مرجع سابق، ص ٦٩.

ولم يشترط النظام السعودي أن يكون النظام الإلكتروني الذي يتم اختراقه محمياً بكلمة السر، بل إن الدخول غير المشروع معاقب عليه حتى ولو لم يهتم صاحبه بوضع كلمة المرور عليه لكي يحميه من تطفل الآخرين، والنظام السعودي في ذلك يتماشى مع الاتجاه العالمي في هذا المجال حيث يحمي القانون الفرنسي، والقانون الإنجليزي والقانون الكندي الحاسب الآلي بدون شرط أن يكون محمياً بكلمة مرور^(١). وعلى الرغم من أن النظام السعودي المشار إليه قد جرم الدخول غير المشروع في نظام حاسب آلي أو موقع إلكتروني أو شبكة، فإنه لم يجرم مجرد الدخول، بل اشترط أن يكون ذلك الدخول بقصد تحقيق غاية معينة، أي استلزم توافر نية معينة وهو ما نسميه بالقصد الخاص.

وتجرم أنظمة الحماية الإلكترونية الدخول غير المصرح به في الأنظمة الإلكترونية، فيستلزم هذا التجريم توافر قصد خاص لدى المتهم كما فعل النظام السعودي وهو قصد التأثير في البيانات أو التأثير في نظام الكمبيوتر نفسه أو قصد الحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني للعقاب على هذا الدخول أو قصد التهديد أو الابتزاز^(٢).

يوضح هذا التجريم ضرورة استحداث نصوص خاصة لحماية المعلومات داخل الكمبيوتر فقد استشعر المنظم في دول عديدة الحاجة إلى إدخال تشريعات جديدة تحمي المعلومات داخل نظام الكمبيوتر نظراً لقصور القواعد التقليدية في قانون العقوبات عن حماية هذا النظام، ومن هذه النصوص ما يجرم مجرد التداخل في نظام الكمبيوتر، ومنها ما يجرم إتلاف المعلومات المبرمجة، ومنها ما يجرم تغيير هذه

(١) الشوا، محمد سامي. (١٩٩٤). ثورة المعلومات وانعكاساتها على قانون العقوبات. القاهرة، دار النهضة العربية. ص ١٩٨.

(٢) رمضان، مدحت. (٢٠٠٤). الحماية الجنائية لموقع الإنترنت ومحتوياته، ورقة عمل مقدمة لندوة التجارة الإلكترونية المنعقدة في المعهد العالي للعلوم القانونية والقضائية بدبي، ١٠-١١ مايو ٢٠٠٤، ص ٩.

المعلومات^(١)، ومن خلال ذلك يتم استعراض سياسة النظام السعودي لمكافحة الصور المختلفة للجرائم الإلكترونية، ويمكن توضيح هذه الصور كما يلي:

١) الصورة الأولى: الدخول غير المشروع بقصد التهديد أو الابتزاز:

تعاقب المادة الثالثة من النظام على هذه الصورة من صور الدخول غير المشروع بقولها: "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً"^(٢).

وبالتالي فإن النظام السعودي لا يعاقب في هذا النص على التهديد أو الابتزاز فقط ولكن الدخول بقصد التهديد أو الابتزاز، بمعنى أنه لا يشترط أن يكون المتهم قد قام بالتهديد أو الابتزاز بالفعل مادامت نيته قد اتجهت إلى تحقيق هذا المقصد. ويترك استخلاص تلك النية إلى المحكمة في ضوء ظروف وملابسات القضية. فإذا قام المتهم بالتهديد أو الابتزاز بالفعل، فإنه يرتكب جريمتين، جريمة الدخول وجريمة التهديد أو الابتزاز. وفي غياب نص في نظام خاص بالتهديد أو الابتزاز، فإن هذا التجريم يكون واجب التطبيق بمفرده. ومن اللازم إيراد نص يعاقب على التهديد أو الابتزاز على استقلال، لأنه يمكن أن يقع بطريق آخر غير طريق الكمبيوتر والمعلوماتية^(٣).

٢) الصورة الثانية: الدخول بقصد العبث بالبيانات المبرمجة:

(١) غنام، محمد غنام. (٢٠٠٤). عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، ص ٢٠.

(٢) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧ هـ، المادة الثالثة، الفقرة الثانية.

(٣) قشقوش، هدى حامد. (٢٠٠٠). الإلتفاف العمدي لبرامج وبيانات الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات، في الفترة ١-٣ مايو سنة ٢٠٠٠، ص ١٠.

قد يكون قصد المتدخل أن يقوم بالعبث بالبيانات داخل الكمبيوتر كأن يقوم بمحوها أو تغييرها أو حذف بعض منها أو إعادة نشرها، فتعاقب المادة الخامسة من نظام مكافحة جرائم المعلوماتية على صور أخرى من الدخول غير المشروع بقولها: "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية:

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها"^(١).

في هذا النص اكتفى النظام السعودي بالعقاب على الدخول غير المشروع إذا كان غرض الجاني هو العبث بالمعلومات داخل الكمبيوتر وذلك بالتغيير أو بالحذف. وبناء عليه لا يلزم أن يكون المتهم قد توصل بالفعل إلى ذلك الحذف أو هذا التعديل. أما إذا كان المتهم من حقه الدخول إلى النظام وقام بالتعديل أو الحذف فإن هذا التجريم لا ينطبق. وهنا نجد أن هناك ثغرة في هذا التجريم، إذ كان من الواجب على المنظم أن يعاقب على التغيير أو الحذف في حد ذاته، بالإضافة إلى الدخول بغرض التغيير أو الحذف، أما ما أورده المادة الخامسة من العقاب على "إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها"، فإن ما ورد بها بخصوص العقاب على البيانات جاء خاصاً بالشبكة المعلوماتية والبرامج أو البيانات الموجودة بها، أما إذا تعلق الأمر ببيانات لا توجد في شبكة معلوماتية، فإن النص يقف قاصراً عن العقاب عليه^(٢).

٣) الصورة الثالثة: الدخول غير المشروع للحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني:

(١) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ٢٨/٣/٧ هـ، المادة الخامسة، الفقرة الأولى.

(٢) صابر، زويب حسين. (٢٠١٠). مؤتمر البيئة المعلوماتية الآمنة. الرياض، جمعية المكتبات والمعلومات السعودية، ص ٣.



في هذا الفرض يكون قصد الجاني من الدخول أن يحصل على بيانات تمس الأمن القومي أو الاقتصاد الوطني؛ فتعاقب المادة السابعة (٧) من النظام السعودي على ذلك بقولها:

"يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية :

- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني"^(١).

وفي حالة الدخول غير المشروع للحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني، فإنه يتوافر التجريم حتى ولو لم يتمكن المتهم من الحصول على تلك المعلومات السرية المتعلقة بأمن الدولة أو باقتصاد الدولة، فيكفي أن يكون غرض الجاني من الدخول هو الحصول على هذا النوع من البيانات، عندئذ تقع الجريمة تامة وليست مجرد شروع فيها.

٤) الصورة الرابعة: الدخول غير المشروع بقصد العبث بالموقع:

حيث يعاقب النظام السعودي من يقوم بالدخول غير المشروع في النظام إذا كان قصد المتدخل أن يعتدي على الموقع بطريق من الطرق التالية: تغيير تصميم هذا الموقع، إتلاف أو تعديل الموقع، شغل عنوان الموقع. فالمعروف أن هناك اسماً للموقع، فمن يقوم بالتدخل في عنوان الموقع حتى يحول دون استخدامه بشكل أو بآخر، يسري عليه هذا التجريم. وقد عرفت المادة الأولى من النظام السعودي المقصود بالموقع بنصها على أنه "مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد"^(٢).

ثانياً: الجريمة الإلكترونية في الفقه الإسلامي:

(١) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧ هـ، المادة السابعة، الفقرة الثانية.

(٢) نظام مكافحة الجرائم المعلوماتية السعودي، أقره مجلس الوزراء في ١٤٢٨/٣/٧ هـ، المادة الأولى.

لقد أدى ظهور الحاسبات الآلية إلى تغيير شكل الحياة في العالم، وأصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يوماً بعد يوم، سواء في المؤسسات المالية، أو المرافق العامة، أو المجال التعليمي، أو الأمني أو غير ذلك، إلا أنه وإن كان للوسائل الإلكترونية الحديثة ما يصعب حصره من فوائد، فإن الوجه الآخر والمتمثل في الاستخدامات السيئة والضارة لهذه التقنيات الحديثة ومنها الجريمة الإلكترونية، فقد أصبحت خطراً يهدد العالم بأسره، إن خطر الجريمة الإلكترونية يكمن في سهولة تنفيذها مع شدة أثرها وضررها، فيقوم مستخدمها بعمله وهو في منزله، أو مكتبه، أو في مقهى، أو حتى من غرفته.

ويتشابه تعريف الجريمة الإلكترونية مع تعريف الجريمة التقليدية حيث تعرف على أنها "إتيان فعل معاقب عليه أو ترك فعل مأمور به ومعاقب على تركه بحد أو تعزيز^(١)، ويشمل المفهوم العام للجريمة كل معصية أو خطيئة مخالفة لأوامر الله أو نواهيه، سواء كانت هذه المعصية نتيجة سلوك، يمكننا أن نلمسه مادياً أم كانت المعصية مستترة في النفس البشرية، وسواء كانت العقوبة المقررة لها دنيوية أم عقوبة أخروية.

ويعرف الماوردي الجريمة بأنها "محظورات شرعية زجر الله تعالى عنها بحد أو تعزيز"^(٢)

وقد عرف الفقهاء الجريمة وفقاً لهذا المفهوم بأنها فعل ما نهى الله عنه وترك ما أمر الله به^(٣).

وهناك تشابه أيضاً بين عناصر الجريمة الإلكترونية وعناصر الجريمة التقليدية، حيث يمكن القول من خلالها بأن المكلف ارتكب محظوراً شرعاً إذا توافرت فيه العناصر الآتية^(٤):

(١) الخراساني، فتحي بن الطيب. (٥١٤٢٥) الفقه الجنائي الإسلامي. دمشق، سوريا، دار قتيبة، ص ٨٠.
(٢) الأحكام السلطانية والولايات الدينية للماوردي، ص ٢١٩.
(٣) أبو زهرة، محمد. الجريمة والعقوبة في الفقه الإسلامي. (١٩٩٨). القاهرة، دار الفكر العربي، ١٩٩٨ م، ص ٢٠.
(٤) فوزي، شريف. (١٩٨٦). مبادئ التشريع الجنائي الإسلامي. القاهرة، مكتبة الخدمات الحديثة، ص ٥١.

(١) لقيام الجريمة لابد من ارتكاب فعل يمثل الجانب المادي لها، ويعني بالفعل في مجال الجريمة السلوك الإجرامي أيّاً كانت صورته سواء كان إيجابياً أو سلبياً، ويتحقق السلوك الإيجابي بإتيان فعل منهي عنه، ويتحقق السلوك السلبي بالامتناع عن فعل أمر الشارع به.

(٢) أن يكون الفعل غير مشروع وفقاً لأحكام الشريعة الإسلامية، ويوصف الفعل بأنه غير مشروع إذا جاء مخالفاً لأوامر الله تعالى أو نواهيه.

(٣) يفترض في الجريمة أن يكون الفعل المحظور صادراً عن إرادة إنسانية. وذلك لأن الجريمة هي نتاج عمل إنساني يسأل عنها، ويتحمل تبعاتها، فالإنسان فقط هو محل المسؤولية.

(٤) يفترض في الجريمة أن يقرر لها الشارع عقوبة، سواء كانت العقوبة مقدرة أو غير مقدرة.

(٥) الأهلية في المجرم وإلا لعدت من المسؤولية التقصيرية لا الجنائية. ومن خلال ما تقدم، فلقد أصبحت الجريمة الإلكترونية هاجساً يخيف العالم الذي أصبح عرضة لهجمات المجرمين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم يوماً بعد يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من عمليات الجرائم الإلكترونية والتي سببت أضراراً جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير لمواجهة الجرائم الإلكترونية، إلا أن هذه الجهود قليلة ولا تزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذه الجرائم الإلكترونية^(١)، ويمكن تناول بعض نماذج الجرائم الإلكترونية من خلال منظور الفقه الإسلامي كما يلي:

جرائم اختراق البريد الإلكتروني من منظور الفقه الإسلامي:

يقوم المجرمون باختراق البريد الإلكتروني وهتك أسرار أصحابه والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في

(١) سفر، حسن بن محمد. (٢٠٠٣). الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي. بحث مقدم لمجمع الفقه الإسلامي الدولي، الدورة الرابعة عشر، الدوحة، قطر، ص ١١.

عملياتهم الإرهابية. فلقد نهى الله - جل جلاله - عن التجسس، فقال سبحانه: {ولا تجسسوا} ^(١)، ونهت الشريعة الإسلامية عن الاطلاع على أسرار الناس وهتك حرمتهم، ففي الحديث أن النبي صلى الله عليه وسلم قال: {إنك إن اتبعت عورات المسلمين أفسدتهم أو كدت أن تفسدهم} ^(٢)، واختراق البريد الإلكتروني هو خرق لخصوصية الآخرين وهتك لحرمتهم وتجسس على معلوماتهم وبياناتهم التي لا يرغبون أن يطلع عليها غيرهم، والنبي النبي صلى الله عليه وسلم يقول: {ولا تحسسوا ولا تجسسوا} ^(٣).

فالشريعة الإسلامية كفلت حفظ الحقوق الشخصية للإنسان وحرمت الاعتداء عليها بغير حق، وهؤلاء الذين يعتقدون على بيانات الآخرين ومعلوماتهم عبر اختراق رسائلهم البريدية الإلكترونية آثمون لمخالفة أمر الشارع الحكيم ومستحقون للعقاب التعزيري الرادع لهم، ولا بد من إشاعة هذا الحكم بين الناس وتوعية المتعاملين بشبكة المعلومات العالمية (الإنترنت) بخطورة انتهاك خصوصية الآخرين وحكم ذلك في الشريعة الإسلامية، وأن هذا الأمر مما استقرت الشريعة على تحريمه والنهي عنه، وقد تضافرت نصوص الكتاب والسنة على حفظ حقوق الآخرين وعدم انتهاكها، بل قد تنادت الدول إلى تجريم مخترقي البريد الإلكتروني لما فيه من ضياع للحقوق واعتداء على خصوصيات الآخرين وأسرارهم، ولاسيما إذا كان ذلك لاستغلالها في الجرائم الإلكترونية والعدوان على الآخرين ^(٤).

واستثناء من ذلك فقد يكون التجسس مشروعاً في أحوال معينة كالتجسس على المجرمين، فقد لا يعرفون إلا بطريق التجسس، وقد أجاز الفقهاء التجسس على اللصوص، وطلبهم بطريق التجسس عليهم وتتبع أخبارهم، وكذلك يجوز التجسس في

(١) سورة الحجرات، الآية: ١٢.

(٢) رواه أبو داود، حديث رقم (٤٨٨٨)، وقال عنه النووي: إسناده صحيح. (رياض الصالحين باب النهي عن التجسس، ص ٥٩٦).

(٣) البخاري الأدب (٥٧١٧)، مسلم البر والصلة والآداب (٢٥٦٣)، أحمد (٥٣٩/٢)، مالك الموطأ (١٦٨٤).

(٤) سفر، حسن بن محمد. (٢٠٠٣). الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي. مرجع سابق، ص ١٣.

حال الحرب بين المسلمين وغيرهم لمعرفة أخبار جيش الكفار وعددهم وعتادهم ومحل إقامتهم وما إلى ذلك^(١).

وكذلك يجوز اختراق البريد الإلكتروني للمجرمين المفسدين في الأرض والصوص وقطاع الطريق، لتتبعهم ومعرفة خططهم وأماكن وجودهم، لقطع شرهم ودفع ضررهم عن المسلمين وهذا موافق لمقاصد الشريعة الإسلامية التي جاءت بحفظ الدين والعرض والمال والنفس والعقل^(٢).

اختراق وتدمير المواقع الإلكترونية من منظور الفقه الإسلامي:

يقصد بتدمير واختراق المواقع الإلكترونية الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي أو مجموعة نظم مترابطة شبكياً بهدف تخريب نقطة الاتصال أو النظام، يستطيع قرصنة الحاسب الآلي التوصل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، ويرجع ذلك إلى أن التطور المذهل في عالم الحاسب الآلي يصحبه تقدم أعظم في الجريمة الإلكترونية وسبل ارتكابها، ولا سيما وأن مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي^(٣).

ولقد جاءت الشريعة الإسلامية بحفظ حقوق الآخرين وصيانتها، قال الله عز وجل في النهي عن الاعتداء: {ولا تعتدوا الله إن الله لا يحب المعتدين}^(٤) فنهى الله عز وجل عن الاعتداء، وإن المواقع على شبكة المعلومات العالمية حق للآخرين لا يجوز الاعتداء عليه بأي وجه من الاعتداء، وتدمير المواقع نوع اعتداء فهو محرم ولا يجوز، وقد صدر من مجمع الفقه الإسلامي في دورته الخامسة سنة ١٤٠٩ هـ بأن حقوق

(١) المالكي، برهان الدين بن فرحون. (١٩٩٥). تبصرة الحكام في أصول الأقضية ومناهج الأحكام. تخريج جمال مرعشلي. بيروت، دار الكتب العلمية، ص ١٧١.

(٢) سفر، حسن بن محمد. (٢٠٠٣). الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي. مرجع سابق، ص ١٤.

(٣) حجازي، سهير. (١٩٩٤). التهديدات الإجرامية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي، دولة الإمارات العربية المتحدة، العدد (٩١)، ص ٥.

(٤) سورة البقرة آية: ١٩٠.

التأليف والاختراع أو الابتكار مصونة شرعاً، ولأصحابها حق التصرف فيها ولا يجوز الاعتداء عليها^(١).

ومن خلال ما تقدم نستخلص أن الاعتداء على مواقع الإنترنت ممنوع شرعاً من باب أولى، فإذا كان حق الاختراع والابتكار مصوناً شرعاً، فكذلك الموقع على شبكة الإنترنت مصون شرعاً ولا يجوز الاعتداء عليه. ويعتبر تدمير الموقع من باب الإتلاف وعقوبته أن يضمن ما أتلّفه، فيحكم عليه بالضمان.

جرائم القذف والتشهير وتشويه السمعة بواسطة الإنترنت من منظور الفقه الإسلامي:

تكثر حوادث التشهير والقذف في شبكة الإنترنت كأحد أنواع الجرائم الإلكترونية، فقد وجد ضعفاء النفوس في شبكة الإنترنت، وفي ظل غياب الضوابط النظامية والجهات المسؤولة عن متابعة السلبات التي تحدث أثناء استخدام الإنترنت، متنفساً لأحقادهم ومرتعاً لشهواتهم المريضة دون رادع أو خوف من المحاسبة وقد قيل قديماً "من أمن العقوبة أساء الأدب". والقذف مجرم شرعاً، ونظراً لشناعة الجرم ومدى تأثيره السلبي على المجني عليه والمجتمع كونه يساعد على إشاعة الفاحشة بين الناس بكثرة الترامي به، فقد جعل عقوبته من الحدود والتي لا يملك أحد حق التنازل عنه ولا يجوز العفو عنها بعد طلب المخاصمة أمام القضاء، كما جعلها عقوبة ذات شقين الأول عقوبة بدنية بجلده ثمانين جلدة لقوله تعالى ﴿وَالَّذِينَ يَزْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْ يَأْتُوا بِأَرْبَعَةِ شُهَدَاءَ فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَةً﴾^(٢)، والشق الثاني عقوبة معنوية بعدم قبول شهادة الجاني بعد ثبوت جلده لقوله تعالى في ذات الآية وذات السورة: ﴿وَلَا تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُولَئِكَ هُمُ الْفَاسِقُونَ إِلَّا الَّذِينَ تَابُوا مِنْ بَعْدِ ذَلِكَ وَأَصْلَحُوا فَإِنَّ اللَّهَ غَفُورٌ رَحِيمٌ﴾^(٣)، وشدد رسول الله صلى الله عليه وسلم في جريمة القذف حيث اعتبرها من الموبقات فقال عليه الصلاة والسلام في الحديث المتفق عليه "اجتنبوا السبع الموبقات، قالوا يا رسول الله، وما هن؟ قال الشرك بالله، والسحر، وقتل النفس التي حرم الله إلا

(١) مجلة مجمع الفقه الإسلامي التابع لمنظمة المؤتمر الإسلامي. (١٤١١هـ). جدة، المجمع الفقه الإسلامي برابطة العالم الإسلامي، العدد الخامس، المجلد الثالث، ص ٢٢٦٧.

(٢) سورة النور، الآية ٤-٥.

(٣) سورة النور، الآية ٤.

بالحق، وأكل الربا، واكل مال اليتيم، والتولي يوم الزحف، وقذف المحصنات المؤمنات الغافلات"^(١). ولا تعاقب الشريعة على القذف إلا إذا كان كذباً واختلاقاً فإن كان حقيقة واقعية فلا جريمة ولا عقوبة^(٢).

جرائم الاعتداء الإلكتروني على الأموال من منظور الفقه الإسلامي:

من الكليات الكبرى التي جاءت الشريعة الإسلامية بالمحافظة عليها حفظ المال، ونهت عن الاعتداء عليه، فقد خطب النبي صلى الله عليه وسلم في حجة الوداع فكان مما قال: (إِنَّ اللَّهَ حَرَّمَ عَلَيْكُمْ دِمَاءَكُمْ وَأَمْوَالَكُمْ كَحُرْمَةِ بِلَدِكُمْ هَذَا، وَكَحُرْمَةِ شَهْرِكُمْ هَذَا، وَكَحُرْمَةِ يَوْمِكُمْ هَذَا) . ثم قال صلى الله عليه وسلم: (أَلَا هَلْ بَلَّغْتُ؟) قالوا: نعم فقال صلى الله عليه وسلم: اللَّهُمَّ اشْهَدْ"^(٣)، ولذلك حرمت الشريعة الإسلامية السرقة، وأوجبت على السارق العقوبة، قال الله تعالى:  وأوجب على الله عليه وسلم فيما روته عائشة رضي الله عنها: (تقطع اليد في ربع دينار فصاعدا)^(٤).

ولكن هل الاعتداء على الأموال عن طريق الجريمة الإلكترونية يوجب الحد، هناك شروط لإقامة حد السرقة وهي:

أولاً: أن يكون السارق مكلفاً، وأن يقصد فعل السرقة، وأن لا يكون مضطراً إلى الأخذ، وأن لا تكون شبهة في استحقاقه ما أخذ^(٥).

(١) أخرجه الإمام البخاري، من حديث أبي هريرة رضي الله عنه ٣٩٣/٥ من الفتوح، وأخرجه الإمام مسلم ٩٢/١.
(٢) عودة، عبد القادر. (١٤٠١هـ). التشريع الجنائي الإسلامي. بيروت، مؤسسة الرسالة، المجلد الأول، ص ٦٤٦-٦٤٥.
(٣) أخرجه الإمام البخاري من حديث عبدالله بن عمر رضي الله عنها ٨٢/٨، وأخرجه الإمام مسلم ٢٢٤٧/٤ .
(٤) سورة المائدة، الآية: ٣٨ .
(٥) أخرجه البخاري في باب: قوله تعالى: (والسارق والسارقة فاقطعوا أيديهما) من كتاب الحدود ١٩٩/٨ ، رقم 15787 .
(٦) الماوردي، علي بن محمد. (١٤٢٥هـ). الأحكام السلطانية. بيروت، دار الكتب العلمية، ص ٢٢٨ .

ثانياً: أن يكون المسروق منه معلوماً، وأن تكون يده صحيحة على المال وأن يكون معصوم المال، فقد ذهب الجمهور إلى درء الحد عن السارق إذا كان المسروق منه مجهولاً، بأن ثبتت السرقة ولم يعرف من هو صاحب المال لأن إقامة الحد تتوقف على دعوى المالك أو من في حكمه، ولا تتحقق الدعوى مع الجهالة^(١)، وذهب المالكية إلى إقامة الحد على السارق متى ثبتت السرقة دون تفريق بين ما إذا كان المسروق منه معلوماً أو مجهولاً لأن إقامة الحد عندهم لا تتوقف على خصومة المسروق منه^(٢).

ثالثاً: أن يكون المال المسروق متقوماً، وأن يبلغ نصاباً، وأن يكون محرراً فلو سرق ما لا قيمة له في نظر الشرع فلا قطع عليه، كسرقة الخنزير والخمر، والميتة، وآلات اللهو، والكتب المحرمة. وإن كان المسروق أقل من النصاب فلا قطع، على اختلاف بين الفقهاء في مقدار النصاب^(٣)، ولا بد أن يكون المسروق محرراً، والحرز: الموضع الحصين الذي يحفظ فيه المال عادة، بحيث لا يعد صاحبه مضيقاً له بوضعه فيه، فقد ذهب جمهور الفقهاء إلى أن حد السرقة لا يقام إلا إذا أخذ السارق النصاب من حرزه لأن المال غير المحرز ضائع بتقصير صاحبه في حفظه^(٤).

وبعد هذا الاستعراض لما ذكره الفقهاء من شروط وضوابط لجريمة السرقة التي باكتمالها يجب قطع يد السارق، وتطبيقها على الاعتداء على الأموال بطريق الحاسب الآلي نجد أنه وإن اتفقت جريمة السرقة التي تتم عن طريق الحاسب الآلي مع جريمة السرقة بالطرق العادية في نتائجها إلا أن هناك أموراً تختلف عنها ولا بد من توافرها في السرقة بطريق الحاسب الآلي، فإن من الأمور الجديدة بالبحث ولها أثر في الحكم مدى الضمانات الفنية والحماية النظامية للتعاملات التي تتم بطريق الحاسب الآلي،

(١) زين العابدين، ابن إبراهيم. (١٨٩٣). البحر الرائق شرح كنز الحقائق. القاهرة، المطبعة العلمية، ٦٨/٥.
(٢) الزرقاني، محمد بن عبد الباقي بن يوسف. (١٤١١هـ). شرح الزرقاني على موطأ الإمام مالك، بيروت، دار الكتب العلمية، ١٠٦/٨.
(٣) الكاساني، علاء الدين أبو بكر. (١٩٨٢). بدائع الصنائع في ترتيب الشرائع. بيروت، دار الكتاب العربي، ٦٧/٧.
(٤) الكاساني، علاء الدين أبو بكر. (١٩٨٢). بدائع الصنائع في ترتيب الشرائع. بيروت، دار الكتاب العربي، ٦٦/٧.

فإن هذه الضمانات والحماية النظامية كلما قويت دلت على وجود الحرز الذي هو شرط من شروط اكتمال جريمة السرقة، وكذلك ربما تمت السرقة بسبب إهمال مالك المال المسروق في حفظه بالطرق الفنية المعروفة في مجال الحاسب الآلي والأخذ بالسبل الواقية من الاعتداءات الإلكترونية على ماله، وأيضاً ربما صاحب السرقة تخريب أو إتلاف أو تزوير، ومما يؤثر في الحكم أيضاً عدم مطالبة مالك المال المسروق بماله وذلك بسبب ما يترتب عليها من إساءة لسمعته وفقد الثقة به، وهذا هو الذي يدعو بعض البنوك والمؤسسات المالية إلى الإحجام عن الإبلاغ عن السرقات التي يتعرضون لها، فضلاً عما يصاحب هذه الاعتداءات من مجاهرة ومغالبة فإن معظم هذه الاعتداءات المالية الإلكترونية تتم عن طريق كيانات منظمة تهدد أمن واستقرار واقتصاد المجتمع، وهذا ما دعا بعض الكتاب إلى اعتبار هذه الجرائم من الحراية والإفساد في الأرض، فإن هذه الجرائم أصبحت جرائم دولية بعد انتشار شبكة الإنترنت، فإذا كان الجاني ذا قوة وتبدير وتنظيم مما يتعذر معه الاستغاثة من المجني عليه، وقام بالتخريب أو إزالة للمواقع وسرقة للأموال، وهو الغالب في الجريمة الإلكترونية، فإن هذه الجرائم تدخل في جرائم الحراية ويطبق عليها ما يطبق على جرائم الحراية^(١)، وهذا الموضوع يتطلب بحثاً مستقلاً بذاته.

ومن خلال ما تقدم نستخلص عظمة الشريعة الإسلامية وكمالها وشمولها وصلاحياتها لكل زمان ومكان وسعة الفقه الإسلامي ورحابته وقدرته على مواكبة مستجدات العصر، ولذلك لا بد من نشر الوعي بأهمية حماية المعلومات الخاصة بالفرد، سواء على الإنترنت أو على غيرها من الشبكات الأخرى، وتشجيع ما يسمى بالأمان الإلكتروني.

(١) موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت، د/ عطا عبدالعاطي محمد السنباطي دار النهضة العربية، الطبعة الأولى، ١٤٢٢هـ، ص ٨١.

الفصل الثالث

ضبط الجريمة الإلكترونية

المبحث الأول: الاستدلالات الأولية والتحقيق لإثبات الجريمة الإلكترونية
المبحث الثاني: ضوابط إثبات الجريمة الإلكترونية

المبحث الأول

الاستدلالات الأولية والتحقيق لإثبات الجريمة الإلكترونية

يمكن توضيح طرق الاستدلالات الأولية لإثبات الجريمة الإلكترونية من خلال

ما يلي:

أولاً: تلقي وضبط البلاغ:

يعرف ضبط البلاغ على أنه "وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها"^(١)، والضبط بهذا المعنى ينصرف إلى الأشياء دون الأشخاص، وبناء على ذلك، يجب توضيح مدى صلاحية الجرائم المرتكبة في البيئة الإلكترونية لضبط البلاغ. ويعد البلاغ هو المشكلة الحقيقية التي تواجه الجريمة الإلكترونية، فغالبية المنظمات تخشى من الإبلاغ لكي لا تفقد ثقة عملائها، ومن ثم يفلت مرتكب الجريمة الإلكترونية بفعلته نتيجة إجماع المنظمات والشركات والمؤسسات المالية عن الإبلاغ خوفاً على سمعتها، حيث تفضل هذه المرافق عدم إبلاغ السلطات المختصة للمحافظة على ثقة عملائها أكثر من اهتمامها بكشف الجريمة ويفضلون الترضية المالية لعملائهم ومنحهم الأموال التي سلبت منهم نتيجة الاختراق والتعدي^(٢). ومن خلال ما تقدم، يمكن تلقي وضبط البلاغ كما يلي:

■ بالنسبة للجرائم الواقعة على المكونات المادية للبيئة الإلكترونية:

بالنسبة للجرائم الواقعة على المكونات المادية للبيئة الإلكترونية فإن الأمر لا يثير أي صعوبة تذكر، ذلك أن الضبط يرد بالأساس على الأشياء المادية محل الجريمة المرتكبة^(٣).

(١) الصيفي، عبد الفتاح مصطفى. (٢٠٠٢). تأصيل الإجراءات الجنائية. الإسكندرية، دار المعرفة الجامعية، ص ٢٢٥.

(٢) الهيتي، محمد حماد. (٢٠٠٥). جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها. عمان، دار المناهج للنشر والتوزيع، ص ٢١٨.

(٣) الصيفي، عبد الفتاح مصطفى. (٢٠٠٢). تأصيل الإجراءات الجنائية. مرجع سابق، ص ١١٩.

■ بالنسبة للجرائم الواقعة على المكونات غير المادية للبيئة الإلكترونية:

فيما يتعلق بالجرائم الواقعة على المكونات غير المادية للبيئة الإلكترونية، فإن الأمر يثير العديد من الإجراءات، يمكن توضيحها كما يلي:

أ - بالنسبة للبرامج التطبيقية ونظم التشغيل:

وفي هذه الحالة يمكن ضبط أدلة الجريمة إذا كان محلها سرقة الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخه بصورة غير مشروعة أو إتلافه بوسائل تقليدية، ولكن الأمر يزداد صعوبة في حال استخدام وسائل فنية في إتلاف البرنامج كالفيروسات مثلاً، ويتمثل مكن الصعوبة في هذه الحالة في قلة خبرة الجهات الأمنية باعتبارها الجهة الأصلية المختصة بالضبط، وهناك صعوبة ثانية تتصل باتساع الشبكة الإلكترونية، فقد يؤدي الضبط إلى عزل النظام الإلكتروني بالكامل عن دائرته لمدة زمنية طويلة وهو ما يسبب حتماً أضراراً بالجهة مستخدمة النظام، هذه النتيجة المتوقعة من عملية الضبط ستؤدي حتماً إلى امتناع مستخدمي الأنظمة الإلكترونية من التعاون الكامل والفعال مع سلطة التحقيق، الأمر الذي يخلق إشكالية كبيرة تواجه إجراءات الضبطية القضائية^(١).

ب - بالنسبة للبيانات الرقمية:

في هذه الحالة يصطدم المحقق الجنائي بعوامل عدة تحول دون ضبطه للبيانات التي تعد دليلاً على ارتكاب الجريمة، وتكمن هذه العوامل في عدم وجود دليل مرئي يمكن فهمه بالقراءة، بالإضافة إلى عدم وجود آثار مادية يمكن على أساسها الاستدلال على وجود دليل على ارتكاب الجريمة، ويتجلى ذلك في جرائم الاختلاس والتزوير التي تستعمل فيها التقنية الإلكترونية، وحتى البيانات التي يمكن الوصول إليها يستطيع الجاني أن يدمرها في فترة زمنية قصيرة تعد بالثواني، بالإضافة إلى الخبرة

(١) حسن، سعيد عبد اللطيف. (١٩٩٩). إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت: الجرائم الواقعة في جرائم تكنولوجيا المعلومات. مرجع سابق، ص ٤٢.

الفنية المتطلبة لفحص هذه الأدلة لتحديد البيانات التي تصلح كأدلة إدانة للجاني من عدمه^(١).

ومن خلال ما سبق فالبلاغ إجراء يصدر عن الغير أو عن المجني عليه في غير الجرائم التي يتوقف تحريك الدعوى الجنائية فيها على شكوى، بهدف إحاطة المختص علماً بوقوع جريمة أو واقعة مخالفة للقانون. والأصل أن يقبل رجل الضبط الجنائي جميع البلاغات والشكاوى التي ترد إليه بشأن الجرائم بغض النظر عن شخصية الشاكي أو صفته، فقد يكون المتقدم بالبلاغ أو الشكوى الجاني أو المجني عليه، أو أي فرد من عامة الناس^(٢). ومن خلال ما تقدم يجب على رجال الضبط كل على حسب اختصاصه أن يقبلوا البلاغات والشكاوى التي ترد إليهم في جميع الجرائم وان يقوموا بفحصها وجمع المعلومات المتعلقة في محضر رسمي، ومن ثم إرسالها إلى الجهة المختصة.

ثانياً: معاينة مسرح الجريمة:

يقصد بالمعاينة "مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفاً من إتلافها، أو محوها أو تعديلها"^(٣). والمعاينة من إجراءات التحقيق الابتدائي، ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، والأصل أن يحضر أطراف الدعوى المعاينة، وقد يقرر المحقق أن يجربها في غيبتهم، ولا يلتزم المحقق بدعوة محامي المتهم للحضور، ومجرد غياب المتهم عند إجراء المعاينة ليس من شأنه أن يبطلها. وتظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجد مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيداً لفحصها لبيان مدى صحتها في الإثبات، وليس الحال كذلك بالنسبة للجرائم الإلكترونية، حيث يتخلف عن ارتكابها آثار مادية،

(١) الهيتي، محمد حماد. (٢٠٠٥). جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها. مرجع سابق، ص ٢٣٩.

(٢) سلامة، مأمون محمد. (١٩٩١). الإجراءات الجنائية في التشريع المصري. القاهرة، دار الكفر العربي، ص ٤٧٤.

(٣) أبو العينين، عبد الفتاح محمد. (١٩٩٢). القضاء والإثبات في الفقه الإسلامي مع المقارنة بقانون الإثبات اليمني. القاهرة، جامعة الأزهر، ص ١١٥.

وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها. وإذا تمت المعاينة بعد وقوع الجريمة في المجال الإلكتروني، فيجب مراعاة ما يلي^(١):

١. تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

٢. العناية بملاحظة الطريقة التي تم بها إعداد النظام.

٣. ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.

٤. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

٥. التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة، وفحصها، ويرفع من عليها البصمات ذات الصلة بالجريمة.

٦. التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

٧. قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات.

وعلى الرغم من أهمية المعاينة في إثبات حالة مسرح الجريمة، فهذا لا يعني أنها تكون فعالة لضبط كافة أدلة الجرائم، نظراً لوجود طائفة من الجرائم لا تصلح بحسب طبيعتها لأن تكون محلاً للمعاينة، لذلك يجب توضيح مدى صلاحية مسرح جرائم البيئة الإلكترونية للمعاينة، وذلك من خلال توضيح الفرق بين ما يلي:

(١) عبد المطلب، ممدوح عبد الحميد. (٢٠٠٧). أدلة الصور الرقمية. ورقة عمل مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة: الجرائم الإلكترونية الملامح والأبعاد، المنعقدة بكلية الملك فهد الأمنية بالرياض في الفترة من ٢٢ إلى ٢٤ أبريل، ٢٠٠٧. الرياض، كلية الملك فهد الأمنية، ص ٥٣٣،

■ بالنسبة للجرائم الواقعة على المكونات المادية للبيئة الإلكترونية:

تتمثل المكونات المادية للبيئة الإلكترونية في كل ما هو مادي محسوس، مثل وحدات الإدخال والإخراج والتحكم والذاكرة وشاشة العرض وغيرها، وفي هذه الحالة يمكن التقرير بصلاحيات مسرح الجريمة للمعاينة من قبل سلطة التحقيق، للضبط والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبتها لفاعل معين، كما يمكن في هذه الحالة وضع الأختام في الأماكن التي ارتكبت فيها مسرح الجريمة وضبط كل ما استعمل في ارتكاب الجريمة^(١).

■ بالنسبة للجرائم الواقعة على المكونات غير المادية للبيئة الإلكترونية:

تتمثل المكونات غير المادية للبيئة الإلكترونية في كل ما هو غير مادي محسوس، مثل البرامج والمعطيات، وفي هذه الحالة تظهر الصعوبة في مواجهة فاعلية المعاينة، حيث تكمن هذه الصعوبات في أمرين أساسيين^(٢):

- (١) تتمثل الصعوبة الأولى في قلة الآثار المادية التي قد تتخلف عن هذه الجرائم.
- (٢) تتمثل الصعوبة الثانية في كثرة الأشخاص الذين يترددون على مسرح الجريمة خلال المدة بين اقتراف الجريمة والكشف عنها، وهو ما يتسبب عادة في إتلاف الآثار المادية للجريمة، الأمر الذي يصعب الدليل المستقى من الجريمة بالشك والريبة.

لهذا يوصي المتخصصون بضرورة التقيد ببعض الإرشادات الفنية عند إجراء المعاينة لمسرح الجريمة المرتكبة في البيئة الإلكترونية، وتنقسم هذه الجهود إلى جهود ما قبل الوصول إلى مسرح الجريمة، وجهود ما بعد الوصول إلى مسرح الجريمة، ويمكن توضيحهما كما يلي:

أ - جهود ما قبل الوصول إلى مسرح الجريمة:

هناك مجموعة من الجهود المختلفة التي يجب أن تتوفر في معاينة مسرح الجريمة قبل الوصول إلى مسرح الجريمة ويمكن توضيح هذه الجهود فيما يلي^(١):

(١) المرجع السابق، ص ٥٣٩،
(٢) الشوابكة، محمد أمين. (٢٠٠٦). جرائم الحاسوب والانترنت: الجريمة المعلوماتية. عمان، دار الثقافة للنشر والتوزيع، ص ١٢٣.

- (١) توفير معلومات مسبقة عن مكان الجريمة، ونوعية وعدد الأجهزة المتوقع مداومتها وشبكاتها.
- (٢) إعداد خريطة للموقع وتفاصيل المبنى أو الطابق من المبنى موضع البلاغ، وتحديد مواقع الأجهزة والخزائن والملفات عن طريق المصادر السرية.
- (٣) تحديد عدد وأنواع الأجهزة المحتمل تورطها في ارتكاب الجريمة لتحديد إمكانات التعامل معها فنياً من حيث الضبط والتأمين وحفظ المعلومات.
- (٤) الحصول على الاحتياجات الضرورية من أجهزة وبرامج صلبة ومرنة للاستعانة بها في الفحص والتشغيل.
- (٥) إعداد فريق التفتيش من المتخصصين وفق قائمة تحدد الأسماء والاختصاصات والمهام الموكولة بدقة.
- (٦) إخطار أعضاء الفريق قبل التحرك لمسرح الجريمة بوقت كافٍ لتمكينهم من إعداد خططهم الخاصة.
- (٧) كتابة بيانات بالمهام المطلوبة من كل عضو في الفريق وتوزيعها على الجميع لضمان الإنجاز مع عدم التداخل.
- (٨) إعداد خطة واضحة ومفهومة للجميع، مع تفصيلها بالرسومات ومراجعتها مع أعضاء الفريق قبل التحرك لمسرح الجريمة مع مراعاة الحالة، والرسالة، والتنفيذ، والمداخل والمخارج، والاتصالات.
- (٩) تأمين التيار الكهربائي لكي لا يتم التلاعب أو التخريب عن طريق قطع التيار الكهربائي.

ب - جهود ما بعد الوصول إلى مسرح الجريمة:

وهناك مجموعة من الجهود الأخرى المختلفة التي يجب تحديدها في معاينة الجريمة، بعد الوصول إلى مسرح معاينة الجريمة، ويمكن توضيحها كما يلي^(٢):

(١) البشري، محمد الأمين. (٢٠٠٠). التحقيق في جرائم الحاسب الآلي والانترنت. المجلة العربية للدراسات الأمنية والتدريب. المجلد (١٥)، العدد (٣٠)، الرياض، جامعة نايف العربية للعلوم الأمنية، ص ٣٥٦.

(٢) حجازي، عبد الفتاح بيومي. (٢٠٠٥). الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت. القاهرة، دار الكتب القانونية، ص ٦٣-٦٤.

(١) تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة، وتحديد مواقعها بأسرع وقت ممكن، وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملفات، بهدف تعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها، مع تصوير الأجهزة الموجودة، وبصفة خاصة أجزائها الخلفية. وضرورة ملاحظة طريقة إعداد أنظمة الحاسب الآلي أو الإلكتروني بعناية فائقة، مع إثبات الحالة التي تكون عليها توصيلات الحاسب، وهذا لتسهيل عملية تحليل النظام عند عرض الموضوع أمام المحكمة المختصة.

(٢) وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة، ورصد الاتصالات الهاتفية من وإلى مسرح الجريمة مع إبطال مفعول أجهزة الهاتف المتحرك التي قد تساعد عن طريق تقنية معينة على تدمير أدلة الجريمة الإلكترونية متى ما تم توصيلها بالأجهزة محل المعاينة. ويجب التأكد من عدم وجود أي مجالات كهرومغناطيسية في المحيط الخارجي لمسرح الجريمة حتى لا يتم أي إتلاف للبيانات المخزنة، وهذا يتطلب إجراء اختبارات وفحوصات تقنية قبل نقل أي مادة معلوماتية من مسرح الجريمة.

(٣) ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها، ومعرفة السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار، وبروتوكولات الاتصال عبر الإنترنت وإن تعلق الجريمة بهذه الشبكة والتي تعرف اختصاراً بـ (IP) ويتعين أيضاً ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام لكي يمكن تحليل البيانات ومقارنتها والوصول منها إلى دليل عند عرض الأمر على القضاء.

(٤) عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات القوى المغناطيسية (الممرات المغناطيسية) التي قد تتسبب في محو البيانات، ولن يتأتى ذلك إلا عن طريق خبراء الحاسب الآلي، ولذلك يجب أن يتضمن الفريق الذي يتولى ضبط وتحريز الأدلة على

اثنين أو أكثر من خبراء الحاسب الآلي لضبط وإدخال المعلومات المضبوطة في الحاسب، وتصنيف الأدلة وتحريزها في صناديق، ووضع العلامات الدالة عليها، ويقوم الفريق بنقل أجهزة الحاسب الآلي المضبوطة بعد استكمال إجراءات الرسم والتصوير، مع مراعاة تنوع خبراء الحاسب الآلي ما بين محققين وآخرين مدربين على التعامل مع الأدلة الرقمية وتقييمها.

٥) التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وشرائط وأقراص ممغنطة وغير سليمة أو محطة ورفع البصمات التي قد توجد عليها، والتحفظ على مستندات الإدخال والمخرجات الورقية لجهاز الحاسب الآلي، والتي قد تكون ذات صلة بالجريمة.

٦) قصر المعاينة على المحققين الجنائيين والفنيين أصحاب الخبرة والدراسة والكفاءة العلمية والفنية في مجال الحاسبات والشبكات واسترجاع المعلومات من الذين تلقوا تدريبات متخصصة

ثالثاً: التحري وكشف غموض الجرائم الإلكترونية:

تتسم الجرائم ذات الصلة بالحاسب الآلي، بحداثة أساليب ارتكابها، وسرعة تنفيذها، وسهولة إخفائها، ودقة وسرعة محو آثارها. هذه الخصائص العامة تقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها، وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكابها أو تلك التي تكون محلاً للجريمة^(١).

وقد وجدت أجهزة الشرطة والتحقيق صعوبات جمة منذ ظهور هذا النوع المستحدث من الجرائم، سواء في كشف غموضها أو إجراء التفتيش والضبط اللازمين، أو التحقيق فيها على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنية على نحو

(١) عقيدة، محمد أبو العلا. (٢٠٠٣). التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية. المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في الفترة من ٢٦-٢٨ أبريل ٢٠٠٣، دبي، أكاديمية شرطة دبي، مركز البحوث والدراسات. ص ٦.

يمكنها من تحقيق المهمة المطلوبة منها وبالكفاءة المطلوبة، ففي الفترة الأولى لظهور هذا النوع من الجرائم، وقعت الشرطة في أخطاء جسيمة أدت إلى الإضرار بالأجهزة أو الملفات، أو الأدلة الخاصة بإثبات الجريمة، ونعطي مثلاً لهذا الخطأ من عمل الشرطة بالولايات المتحدة الأمريكية. فقد حدث أن طلبت، إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، وقد حدث نتيجة لذلك أن تسببت دائرة الشرطة بدون قصد في إتلاف ما كان قد سلم من الملفات والبرامج^(١).

وأساليب التحري أو التحقيق التقليدية، قد لا تصلح لكشف الجريمة، وضبط مرتكبيها، والتحفظ على أدلتها، ويمكن إجراء بعض التحريات المبدئية قبل عملية التفتيش أو الضبط والتحقيق، توصلاً لكشف غموض الجريمة تمهيداً لضبط مرتكبيها، وجميع الأدلة المتعلقة بها. ويمكن للمجني عليه في هذه الجرائم أن يقدم خدمات كبيرة لرجال الشرطة أو لسلطة التحقيق، فما يقدمه لرجل الشرطة من معلومات، تحقق فائدة كبيرة في معرفة طبيعة الجريمة التي وقعت وأساليب ارتكابها، والأدوات المستخدمة في ارتكابها والأشخاص المشتبه فيهم، وبواعث الجريمة، وما إذا كان هناك شهود أم لا. ولكي تنتج التحريات آثارها الإجرائية، يجب أن تتسم بما يلي^(٢):

(١) أن تتعلق بجريمة ارتكبت فعلاً؛ لأن إذن جهة التحقيق الذي يصدر استناداً عليها هو إجراء من إجراءات التحقيق، ولا يصدر عن جريمة لم تقع أو محتملة، فلصودر إذن التفتيش يجب إجراء تحريات جدية تشير بوضوح إلى ارتكاب شخص معين جريمة معلوماتية وفق دلائل وإمارات قوية تحدده وتتسبب الجريمة إليه دون غيره تجنباً للمساس بحريته وحرمة مسكنه.

(٢) استخدام الوسائل المشروعة في إجراء التحريات، وعلى ذلك فلا يجوز استراق السمع أو التجسس من ثقب الأبواب.

(١) طنطاوي، إبراهيم حامد. مرسى. (١٩٩٧). سلطات مأمور الضبط الجنائي. القاهرة، دار النهضة العربية، الطبعة الثانية، ص ٢٤٩.

(٢) الصيفي، عبد الفتاح مصطفى. (٢٠٠٢). تأصيل الإجراءات الجنائية. مرجع سابق، ص ٢٢٨.

٣) عدم التدخل في جلب الجريمة بالتحريض عليها وذلك لكي يسهل على رجل الضبط الجنائي اكتشافها وتحديد مرتكبها، لكونه على علم مسبق بها.

٤) التقيد بقواعد الاختصاص النوعي والمكاني، لكي تكون إجراءاته منسجمة مع ما تنص عليه التعليمات، فلا تبطل التحريات.

٥) كفاية التحريات وجديتها بحيث تتضمن معلومات وافية وصحيحة وكاملة وغير مغلوطة، بحيث يتخذها المحقق أساساً لتحقيقه فيما بعد.

وترجع أهمية التحريات إلى دورها في التحقق من صحة ما ورد في البلاغات والشكاوي، ففي الجريمة الإلكترونية لا يمكن إجراء التحريات إلا بعد تقديم الجهة المتضررة لبلاغ يفيد بتعرضها لذلك، أو تقديم شخص بلاغ يفيد بالسحب من رصيده وشراء أغراض لم يشتريها، أو قيام فرد أو شركة باكتشاف وجود عمالة مخالفة على كفالتها دون علمها نتيجة استخدام توقيعه الإلكتروني في تزوير طلبات الاستقدام، ويفضل التحقق من ذلك على سبيل التخفي لكي لا يتخذ الجناة حذرهم، وقد يكتشف رجل الضبط الجنائي كذب البلاغ أو أن الشكوى كيدية وبالتالي يوفر الجهود في عدم إشغال جهات التحقيق فيما لا جدوى منه، كما أن بعض إجراءات التحقيق لا يمكن مباشرتها إلا إذا توافرت تحريات جدية أمام سلطة التحقيق لكي تأذن بها، فلا يمكن إصدار إذن بتفتيش المتهم أو مسكنه في الجريمة الإلكترونية إلا بعد توافر تحريات جدية على ارتكابه الجريمة أو الواقعة الإجرامية، وذلك باستخدام تقنيات التتبع والتأكد من وقوع الاختراق والتعدي على جهاز المجني عليه أو موقعه الإلكتروني سواء كان فرداً أو هيئة تصديقات أو نحوهما، أو من خلال مخاطبة الجهات المشرفة كمركز المعلومات في المنظمات الأمنية بالجوازات والأمن العام والأحوال المدنية باعتبار العاملين يحملون أرقاماً كودية تحدد هوياتهم وهذه غالباً في المنظمات التي لديها عدد كبير من المستخدمين وفي مناطق مختلفة^(١).

رابعاً: الاستعانة بالخبرة الفنية:

منذ بدء ظهور الجرائم ذات الصلة بالحاسب الآلي، تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، وذلك

(١) طنطاوي، إبراهيم حامد. مرسى. (١٩٩٧). سلطات مأمور الضبط الجنائي. مرجع سابق، ص ٢٦٦-٢٦٧.

بغرض كشف غموض الجريمة، أو تجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق. وإذا كانت الاستعانة بخبير فني أمر جوازي للمحقق أو لجهة التحقيق والحكم، إلا أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأي دون استطلاع رأي أهل الخبرة، ففي هذه الحالة يجب عليه أن يستعين بالخبير، فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير كان حكمه معيباً مستوجباً نقضه^(١).

وتظهر أهمية الاستعانة بالخبرة في مجال الجرائم الإلكترونية، عند غيابه، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هي أو جهة التحقيق عن جميع الأدلة حول الجريمة وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه. ولا يشترط في الخبير كفاءة علمية عالية فقط في مجال التخصص بل يجب أن يضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه، وعلى وجه الخصوص الجرائم ذات الصلة بالحاسب الآلي، فقد يتعلق الأمر بتزوير المستندات، أو بالتلاعب في البيانات أو الغش أثناء نقل أو بث البيانات أو جريمة من جرائم الأموال أو الاعتداء على حرمة الحياة الخاصة، أو عرض صور أو أفلام مخلة بالآداب العامة^(٢).

(١) تاج الدين، مدني عبد الرحمن. (٢٠٠٤). أصول التحقيق الجنائي وتطبيقاتها في المملكة العربية السعودية. الرياض، معهد الإدارة العامة، ص ٢١.

(٢) عقيدة، محمد أبو العلا. (٢٠٠٣). التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية. المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في الفترة من ٢٦-٢٨ أبريل ٢٠٠٣، مرجع سابق. ص ١٣.

خامساً: التفتيش:

لم تحدد القوانين المقارنة المقصود بالتفتيش إلا أنه يمكن أن نعتبره أحد الإجراءات يقوم بها موظف مختص طبقاً للإجراءات المقررة قانوناً في محل يتمتع بالحرمة والخصوصية، بهدف الوصول إلى أدلة مادية لجريمة تحقق وقوعها لإثبات نسبتها إلى شخص معين، والتفتيش كأصل عام تختص به سلطة التحقيق، وفي هذا الصدد يجب توضيح مدى صلاحية جرائم البيئة الإلكترونية للتفتيش، وذلك حتى يتسنى لنا إثبات الجريمة الإلكترونية^(١)، ولذلك يجب أن نفرق بين الحالتين التاليتين:

■ بالنسبة للجرائم الواقعة على المكونات المادية للبيئة الإلكترونية:

في هذه الحالة لا تثار أية إشكالية أو صعوبة إذا كان محل الجريمة أشياء مادية محسوسة، حيث ينطبق عليها ذات القواعد التقليدية للتفتيش دون أدنى عائق يحول دون هذا الإجراء^(٢).

■ بالنسبة للجرائم الواقعة على المكونات غير المادية للبيئة الإلكترونية:

فيما يتعلق بالبرامج الإلكترونية لا يحتاج الأمر إلى قواعد جديدة للتفتيش عن أدلة الجريمة التي يكون محلها سرقة أو إتلاف أو استعمال هذه البرامج للتزوير أو التلاعب بالبيانات المخزنة، وذلك لكفاية القواعد التقليدية الموضوعية والإجرائية لإثبات وقوع الجريمة عن طريق الالتجاء إلى المتخصصين في مجال المعلوماتية. أما فيما يتعلق بالبيانات الإلكترونية، فإن الأمر تكتنفه بعضاً من الصعوبات العملية والإجرائية نظراً لتجرد هذه الأخيرة من الكيان المادي المحسوس في المحيط الخارجي، وهو ما يعيق عملية إخضاعها لقواعد التفتيش التقليدية، ففي هذا النمط من الجرائم التي تتم عادة على شبكات المعلومات، وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة به، وهذا هو الوضع الغالب في ظل شيوع الشبكات الداخلية على مستوى الشركات أو المؤسسات، والشبكات المحلية والإقليمية والدولية على مستوى الدول. لذلك فإن امتداد نطاق التفتيش إلى نظم غير النظام محل الاشتباه موضع تحديات كبيرة، أولها مدى قانونية هذا الإجراء نظراً لمساسه بحقوق

(١) تاج الدين، مدني عبد الرحمن. (٢٠٠٤). أصول التحقيق الجنائي وتطبيقاتها في المملكة العربية السعودية. مرجع سابق، ص ٧١.

(٢) طنطاوي، إبراهيم حامد. مرسى. (١٩٩٧). سلطات مأمور الضبط الجنائي. مرجع سابق، ص ١٧٧.

الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش. وللتغلب على هذه الصعوبات لجأت بعض القوانين الحديثة إلى التوسع في تفسير نصوص التفتيش بغية مدحها إلى البيانات المخزنة آلياً في الأنظمة الإلكترونية ويتجلى ذلك فيما يلي^(١):

- بالنسبة للصعوبة الخاصة بوجود النهاية الطرفية للنظام المعلوماتي في مسكن آخر غير مسكن المتهم، فيمكن امتداد تفتيش المسكن إلى تفتيش نظام آلي موجود في مكان آخر بغرض التوصل إلى بيانات تفيد في كشف الحقيقة، وبالتالي يجوز للقائم بالتفتيش بأن يسجل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق من قاضي التحقيق.

- أما بالنسبة للصعوبة الخاصة بالدخول في أنظمة المعلومات لضبط ما يعد صالحاً كدليل لارتكاب الجريمة فإنه يجب العمل على إيجاد إدارة أمنية متخصصة في مكافحة الجرائم الإلكترونية، تتمكن من التفتيش على الحاسب الآلي، وبالتالي يتم التعرف على الجريمة.

ومن خلال ما سبق، فالتفتيش أو البحث في الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدلة المطلوبة، ومحل التفتيش وما يتبعه من ضبط يشمل^(٢):

- (١) البرامج أو الكيانات الرقمية.
- (٢) البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته.
- (٣) السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات.
- (٤) دفتر يومية التشغيل وسجل المعاملات، والسجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات، وما يتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة.

(١) الحميد، محمد دباس، ونيو، ماركو إبراهيم. (٢٠٠٧). حماية أنظمة المعلومات. عمان، دار الحامد للنشر والتوزيع، ص ١٠٥ - ١٠٦.

(٢) عقيدة، محمد أبو العلا. (٢٠٠٣). التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية. المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في الفترة من ٢٦-٢٨ أبريل ٢٠٠٣، مرجع سابق، ص ١٣.

ونظراً لكون التفتيش يتضمن تقييداً للحرية الفردية ويمثل اعتداء على حرمة الحياة الخاصة فيجب أن تتوافر فيه الضمانات القانونية اللازمة لصحته ومنها أن يتم صدور أمر قضائي مسبب بشأنه وأن يباشره الشخص أو الجهة المختصة.

وبحسب الأصل يجب أن يصدر إذن التفتيش مكتوباً إلا أن هذا الشرط يحمل بعض المخاطر أحياناً وذلك في حالة ما إذا كان البحث عن أدلة الجريمة يستدعي أن يتم التفتيش في مكان آخر، في نظام معلوماتي آخر غير الذي صدر بشأنه الإذن المكتوب. كما تتمثل المخاطر في إمكانية قيام الجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها، خلال الفترة التي يراد الحصول على إذن مكتوب بشأنها. ولمواجهة هذه المخاطر، يرى البعض أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث. ويشير امتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الآخر مباشرة التفتيش لديه، ويرى البعض في هذه الحالة عدم استمرار أو امتداد البحث لديه إلا في حالتي التلبس، أو رضائه بالتفتيش^(١).

سادساً: الضبط:

الغاية من التفتيش ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأن الجريمة الإلكترونية، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئاً نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة، ونظراً لكون الضبط في مجال الجرائم الإلكترونية هو ضبط البيانات المعالجة إلكترونياً، فقد ثار التساؤل: هل يصلح هذا النوع من البيانات لأن يكون محلاً للضبط؟ فقد انقسم الفقه القانوني إلى اتجاهين عند الإجابة عن هذا التساؤل^(٢):

- **الاتجاه الأول:** يرى البعض أن بيانات الحاسب لا تصلح لأن تكون محلاً للضبط، لانتهاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي

(١) السبهان، فهد إبراهيم. (١٩٩٥). استجواب المتهم بمعرفة سلطة التحقيق. الإمارات العربية المتحدة، مطبعة بن دسمال، ص ٣٤.

(٢) الشاذلي، فتوح، وعفيفي، عفيفي كامل. (٢٠٠٣). جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون. بيروت، منشورات الحلبي الحقوقية، ص ٩٢-٩٣.

لملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية. ويستند هذا الرأي إلى أن النصوص القانونية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملموسة.

■ الاتجاه الثاني: ويرى الاتجاه الثاني أن البيانات المعالجة إلكترونياً ما هي إلا

ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره، ويستند هذا الاتجاه إلى أن بعض النصوص القانونية، تنص على أن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة، حتى ولو كانت السجلات مكتوبة في شكل إلكتروني، وهذا الخلاف دعا المنظم في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط ليشمل فضلاً عن الأشياء المادية المحسوسة، البيانات المعالجة إلكترونياً، أو إصدار تشريعات تتعلق بالجريمة الإلكترونية، تتضمن القواعد الإجرائية المناسبة لهذه الصورة من البيانات، وذلك من خلال الحجز على الأشياء المادية وعلى البيانات المعالجة إلكترونياً.

وخوفاً من محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها بطريق التفتيش، فالمحقق التحفظ على هذه الأدلة، ويتم التحفظ على البيانات محل الجريمة، وكذلك الأدوات التي استخدمت في ارتكابها، أو الآثار المتخلفة عنها وتفيد في كشف الحقيقة. ويتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، وتبقى تحت تصرفها إلى حين انتهاء المحاكمة، ويرى البعض ضرورة حفظ نسخة أخرى، خوفاً من تلف أو ضياع النسخة الوحيدة المرجوة تحت تصرف جهة التحقيق أو المحكمة.

سابعاً: أهمية التحقيق في إثبات الجريمة الإلكترونية:

إن إثبات أي قضية جنائية أو مالية أو أي من القضايا تعتمد على الإجراءات الأولية وطرق التحقيقات المتخذة من جهات الضبط، وعلى ضوء هذه الإجراءات واتباع الأساليب المناسبة يمكن التوصل إلى اكتشاف ملبسات أي جريمة مما يسهل على الجهات القضائية إثبات الجريمة ومن ثم إدانة المتهم.

وتتطلب طبيعة الجريمة الإلكترونية أساليب غير تقليدية في التحقيق لاكتشاف الدليل الرقمي ودعمه من قبل الفنيين المختصين، وذلك يستدعي اتخاذ إجراءات سريعة؛ لأن الدليل الرقمي غير مادي، ويمكن التخلص من أية أدلة أو آثار من قبل مرتكبي الجرائم الإلكترونية، كما تختلف أساليب تلقي البلاغ وإجراء المعاينة والقيام بالتحريات والتفتيش والاستجواب عنها في الجرائم التقليدية نظراً لطبيعة الجرائم الإلكترونية وخصائصها^(١)، ولا شك أن الأجهزة الأمنية تلعب دوراً محورياً في عملية إنفاذ القانون والسيطرة على احترامه على الوجه الصحيح، باعتبارها المنوط بها أساساً واجب منع الجريمة ووقاية المجتمع منها، وهي بذلك تحافظ على القيم الاجتماعية والاقتصادية والأخلاقية للمجتمع. والجرائم الإلكترونية باعتبارها من الجرائم المرتبطة بالتطور التكنولوجي فهي تلقي مزيداً من الأعباء على أجهزة الأمن وهذا يرجع بالأساس إلى قلة الخبرة الفنية، ومن جهة أخرى إلى قصور المنظومة التشريعية في هذا المجال، وهذا ما خلق عدة صعوبات حالت دون أداء هذه الأجهزة لدورها في مواجهة هذه الجرائم.

ويتطلب التحقيق في الجرائم الإلكترونية في مجال الضبط والتفتيش انتقال المحقق إلى مسرح الجريمة الإلكترونية، واسترجاع ومعالجة الدليل المادي، أما اكتشاف المعلومات فيشمل وصول المحقق إلى مصادر المعلومات من غير المواد المضبوطة مثل سجلات الملفات وقواعد البيانات، بهدف تحديد ومعالجة المعلومات التي قد تثبت أو تنفي التهمة. وقد تتطلب القضية تفتيشاً وضبطاً بالإضافة إلى اكتشاف المعلومات.

(١) السراي، عبد الله بن سعود. (٢٠٠٩). فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني. رسالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية، ص ٦٥.

وتواجه طرق التحقيق في إثبات الجريمة الإلكترونية صعوبات متعددة شأنها شأن طرق اكتشاف الجرائم الإلكترونية، حيث تستدعي هذه الطرق في المقام الأول اكتشاف الجريمة الإلكترونية، ومحلها، وبيئتها، ومن ثم البلاغ عنها، وأخذ إذن الجهات المختصة قبل القيام بالمعاينة والتفتيش للموقع أو الجهاز المشتبه به، وذلك للبحث عن الدليل الرقمي الإلكتروني بالطرق الفنية، ومن ثم إجراء التحريات، وبعد تحديد المشتبه به الذي تقوم دلائل قوية على ارتكابه أو ارتكاب الجريمة الإلكترونية من جهازه أو موقعه الإلكتروني في مرحلة جمع الاستدلالات، حيث يتم تحديد الموقع المشتبه به، وصاحب الجهاز، ويتم سؤاله، وإجراء المعاينة والتفتيش الدقيق بمساعدة المحقق الفني الذي يتولى البحث عن الدليل الإلكتروني وتقييمه، وإعداد التقرير الفني الجنائي، وتقديمه لجهة التحقيق تمهيداً للمحاكمة في مرحلة جمع الاستدلالات، وفي الوقت ذاته النقاط القرائن والأدلة المساندة التي تثبت إدانته بارتكاب جريمة من الجرائم الإلكترونية^(١).

وفي ضوء ما سبق، يمكن القول أن إثبات الجريمة الإلكترونية تشوبه بعض المصاعب مقارنة بالجرائم الأخرى، مما يتطلب إجراءات معينة لإثبات الجريمة.

(١) أحمد، هلالى عبد الله. (٢٠٠٣). الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر، ٢٠٠١. القاهرة، دار النهضة العربية، ص ٣٢.

المبحث الثاني

ضوابط إثبات الجريمة الإلكترونية

التحقيق علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فهو له قواعد ثابتة راسخة وبدونها ما كان ليتمتع التحقيق بتلك الصفة، وهذه القواعد قانونية وفنية، الأولى وإن كانت لها صفة الثبات القانوني لا يملك المحقق إزائها شيئاً سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته. ولقد تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تتطوراً ملموساً يواكب حركة الجريمة وتطور أساليب ارتكابها، فبعد أن كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الاستعانة بالأساليب العلمية واستخدام شبكة الإنترنت هي الصفة المميزة والغالبة. ويرجع ذلك إلى حدوث طفرة علمية في مجال تكنولوجيا المعلومات والاتصالات واستخدام الوسائط الإلكترونية في شتي مجالات الحياة، فكلما اكتشف العلم شيئاً حديثاً وجد هذا الاكتشاف طريقه إلى مجال الإثبات الجنائي والتدليل^(١).

وتبعاً لذلك فإنه من البدهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس قاصراً على أسباب التقدم التقني فقط بل يحدث دوماً وبصفة مستمرة، فالمجرم والجريمة في تقدم وتجدد مستمر، فمجرم الأمس ليس كمجرم اليوم وبالتالي فجريمة الأمس ليست كجريمة اليوم. ولا شك أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة من السابق ونحن لا نزال في بداية عصر الانفجار المعلوماتي، يعنى توقع ظهور المزيد من هذه الأنماط الجديدة، والذي يتوجب معها تحديث الأنظمة

(١) مصطفى، محمود محمود. (١٩٧٧). الإثبات في المواد الجنائية في القانون المقارن. القاهرة، مطبعة جامعة القاهرة، ص ١٣٩.

والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة، وهو ما يستتبع تطوير أسلوب التحقيق فيها وكيفية إثباتها^(١).

أولاً: القواعد التي تحكم إثبات الجريمة الإلكترونية:

الإثبات في معناه العام هو "كل ما يؤدي إلى كشف الحقيقة، أما الإثبات في معناه القانوني فهو إقامة الدليل على وجود واقعة قانونية تترتب آثارها أمام القضاء بالطرق التي حددها القانون، وهو الوسيلة التي يتم من خلالها إقرار وقوع الجريمة، وهو كل ما يؤدي إلى ثبوت إجرام المجرم أو براءته من التهمة المنسوبة إليه"^(٢).

والإثبات هو "إقامة الدليل على وقوع الجريمة أو عدم حصولها، وعلى إسنادها إلى المتهم، أو براءته منها"^(٣).

والدليل هو "أداة الإثبات، وهو إما دليل إثبات أو دليل نفي، فالدليل هو الأداة التي يستخدمها القاضي للبرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه، فالإثبات أعم وأشمل من الدليل، فكل منهما مدلوله الخاص"^(٤). وتفترض الواقعة الجنائية وقوع الحدث المجرّم بموجب نص جنائي يجرمه ويحدد مقدار العقوبة، وإسناد الحدث إلى شخص معين بحيث يوجه إليه الاتهام من خلال الدعوى العمومية أو الدعوى الجزائية^(٥).

ومن أهم القواعد التي تحكم الإثبات قاعدة «لا حاجة لإقامة الدليل على ما تنهض الشواهد على تقرير ثبوته، وإنما يلجأ إلى الإثبات من يدعي عكس ما تؤيده

(١) العريان، محمد علي. (٢٠٠٤). الجرائم المعلوماتية. الإسكندرية: الدار الجامعية الجديدة للنشر، ص ٣١.

(٢) الهيتي، محمد حماد. (٢٠٠٥). جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها. مرجع سابق، ص ٢٢٢.

(٣) مصطفى، محمود محمود. (١٩٧٧). الإثبات في المواد الجنائية في القانون المقارن. مرجع سابق، ص ١٥٠.

(٤) النمر، أبو العلا. (١٩٩١). الأدلة الجنائية في ضوء الفقه وأحكام النقض الجنائي، دراسة تحليلية للدليل الجنائي فقهاً وعملاً. القاهرة، دار الصداقة، ص ٣-٤.

(٥) العكيلي، عبد الأمير، وحرية، سليم إبراهيم. (١٩٨١). أصول المحاكمات الجزائية. المجلد الأول، الموصل، دار الكتب للطباعة والنشر، ص ٢١.

الشواهد^(١)، ولذلك لا يتم اللجوء إلى الإثبات إلا في حالة وجود إدعاء بارتكاب جريمة « لأن الأصل في الإنسان هو البراءة، وما تقوم عليه الشواهد هو براءة الإنسان، والإدعاء بارتكاب جريمة إدعاء يخالف الأصل ويناقضه، فلا بد من توافر الدليل، ولذلك أوكل المنظم للجهات التي خولها حق الاتهام تقديم الدليل، فالأصل يمكن نقضه بما خالفه، فقريئة البراءة التي يفترضها المنظم بالإنسان قريئة بسيطة قابلة لإثبات العكس، فقريئة البراءة من القرائن القانونية البسيطة لكونها قابلة لإثبات العكس^(٢).

أي أن سلطة الاتهام هي التي يقع عليها عبء الإثبات من خلال تجميع أدلة الاتهام، بمعنى إثبات عناصر الجريمة بجميع أركانها ما لم يشترط القانون عكس ذلك، فإثبات الجريمة لا يعني التحقق من وقوعها فحسب، بل يمتد ليشمل نسبتها إلى شخص معين من خلال أدلة تثبت ارتكابه الجريمة، أو تحدد صلته بها في نطاق الجريمة، والأدلة إما مادية أو معنوية، أو قولية كالإقرار والشهادة، أما الأدلة المادية فهي المخلفات والآثار المحسوسة التي تتخلف في مسرح الجريمة نتيجة احتكاك الجاني بالمجني عليه أو الأدوات التي يستعملها في ارتكاب الجريمة، أو العلاقات المكانية في مسرح الجريمة نتيجة الاضطراب أو الصراع الذي يدور بين الجاني والمجني عليه، فمقتضى إثبات الجريمة هو وجود أدلة كالاقرار أو الشهادة، أو وجود آثار مادية كالبقع الدموية، وبصمات الأصابع، وغير ذلك من الأدلة المادية^(٣).

وتتنوع قواعد إثبات الجريمة الإلكترونية، حيث يمكن أن تصنف على النحو التالي^(٤):

(١) من زاوية قوتها الإثباتية: هناك أدلة مباشرة تثبت الجريمة بصورة مباشرة، وأدلة غير مباشرة تنصب على وقائع لا تشير إلى الجريمة مباشرة وإنما يحتاج الأمر إلى إعمال العقل والمنطق لاستخلاص الأدلة منها.

(١) عوض، محمد محيي الدين. (١٩٦٣). القانون الجنائي: مبادئه الأساسية ونظرياته العامة في التشريعين المصري والسوداني. القاهرة، المطبعة العالمية، ص ٤٤١.
(٢) الهيتي، محمد حماد. (٢٠٠٥). جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها. مرجع سابق، ص ٢٢٣.
(٣) الشاذلي، فتوح عبد الله. (١٩٩٨). قانون العقوبات: القسم العام. الإسكندرية، دار المطبوعات الجامعية، ص ١٢٧.
(٤) عبد الحميد، أحمد فاروق. (١٤٢٠هـ). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. مرجع سابق، ص ١٨٦-١٨٧.

(٢) من زاوية النتيجة القضائية المستخلصة منها: هناك دليل يدل على وقوع الجريمة، ودليل على تحديد شخص مرتكبها، ودليل يثبت ارتكابها على المتهم.

(٣) من زاوية وظيفة الدليل الإثباتية: فهناك أدلة تنصب على إثبات توافر أحد ركني الجريمة المادي أو المعنوي، وهناك أدلة تنصب على تحديد شخصية المتهم. فأما التحديد القاطع فيشير إلى تحديد شخصية الجاني دون أدنى شك، كالبصمات، وآثار الأقدام العارية، والشهادة بالرؤية، والاعتراف، وضبط محصلات الجريمة في حوزة المتهم، وآثار المقاومة على جسده أو بأظافر المجني عليه، أو التحديد غير القاطع يشير إلى مجرد احتمال لتحديد شخصية الجاني وهي مجرد قرائن.

(٤) من زاوية مضمون الدليل: هناك أدلة مادية محسوسة بإحدى الحواس، وهناك أدلة معنوية مثل الشهادة وأدلة قوليه مثل أقوال المتهم.

ولذلك فقواعد الإثبات النظامية يقصد بها الأدلة التي حددها المنظم وعين حالات استخدامه ومدى حجيتها، وبالرغم أن هناك من يعد تلك الأدلة الإلكترونية مرحلة متقدمة من الأدلة المادية، أو أدلة فنية لأنها تتبع من رأي الخبير الفني، إلا أنها تعد نوعاً متميزاً من وسائل الإثبات. وذلك بسبب كونها نبضات غير محسوسة، وأن حجمها وشكلها تخيلي وأنها سريعة الانتقال. ويمكن استخراج نسخ من الأصل والحصول على نفس الدليل الموجود بمسرح الجريمة التقليدي بالمسرح الإلكتروني أو بمسرح إلكتروني آخر، وقد يكون بمقدور المحققين استرجاع الدليل بعد حذفه^(١).

(١) البشري، محمد الأمين. (٢٠٠١). التحقيق في جرائم الحاسب والانترنت. المجلة العربية للدراسات العربية والتدريب، العدد (٣٠)، مرجع سابق، ص ١١٥.

ثانياً: ضوابط وعناصر إثبات الجريمة الإلكترونية:

عند التحدث عن ضوابط وعناصر إثبات الجريمة الإلكترونية، فإن ذلك يقتضي التعرض إلى المبادئ الأساسية للتحقيق في الجرائم الإلكترونية وهو ما يتطلب معرفة العناصر الأساسية للتحقيق، حيث يجب على المحقق أن يستظهر الركن المادي، والركن المعنوي للجريمة محل التحقيق، وتحديد وقت ومكان ارتكاب الجريمة الإلكترونية بالإضافة إلى علانية التحقيق، ويتطلب أيضاً التحدث عن ضوابط إثبات الجريمة الإلكترونية وهو ما يتم توضيحه على النحو التالي:

■ ضوابط إثبات الجريمة الإلكترونية:

تنقسم ضوابط إثبات الجريمة الإلكترونية إلى ضوابط إثبات الجريمة بالأدلة العلمية، وضوابط إثبات الجريمة بالأدلة الإجرائية، ويمكن توضيحهما كما يلي:

أ) ضوابط إثبات الجرائم الإلكترونية بالأدلة الرقمية:

يحتاج إثبات الجرائم الإلكترونية إلى الدليل الرقمي كوسيلة لإثبات ارتكاب جريمة الاختراق والتعدي على البيانات والمعلومات سواء بسرقتها أو إتلافها أو تزويرها، أو سرقة المنظومة الإلكترونية الخاصة بفرد معين أو منظمة معينة لصالح الفرد أو الغير، والدليل العلمي يتطلب استخدام طرق غير تقليدية في الإثبات، والدليل العلمي يقتصر على إجراء تجارب علمية ومعملية على جهاز الحاسب الآلي الذي استخدم في الاختراق أو التعدي لتعزيز دليل سبق تقديمه سواء بالنفي أو الإثبات للواقعة التي ثار الشك بشأنها^(١)، ويحتاج إجراء هذه التجارب إلى محقق جنائي وفني متخصص لديه مهارات فنية وتقنية لاستخلاص الأدلة الرقمية؛ لأن الفصل في الدعوى الجزائية في هذه الحالة يتوقف على الرأي الفني الذي يثبت أو ينفي ارتكاب الجريمة من قبل المشتبه به^(٢).

(١) حجازي، عبد الفتاح بيومي. (٢٠٠٥). الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت. مرجع سابق، ص ٤٩-٥٠.

(٢) حسني، محمود نجيب. (١٩٨٨). شرح قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية، الطبعة الثانية، ص ٤٧٤.

والدليل العلمي هو النتيجة التي تسفر عنها التجارب العملية والمعملية لتعزيز دليل سبق تقديمه، سواء للإثبات أو نفي واقعة ثارت شكوك حولها، وهو لا يعدو كونه رأياً فنياً يعتمد على خبرة ومهارة فني متخصص يحدد إذا كان الاختراق والتعدي قد تم من الحاسب المشتبه به أم لا^(١).

وبالرغم من الاختلاف بين شراح القانون في اعتبار الخبرة الفنية دليلاً أو قرينة، إلا أن واقع التقدم التقني المعاصر استدعى الاستعانة بالمختصين والخبراء وأصحاب الرأي الفني في دراسة الوقائع المتصلة بالجريمة ونسبتها إلى المتهم، في ضوء تحري الدقة في تحديد المتهم، وهي في النظام تعد بمثابة قرائن لا ترقى إلى أدلة الإثبات المادية، ولكنها تعد بمثابة إحدى طرق الإثبات كقرائن^(٢)، والرأي السابق قد جانبه الدقة؛ لأن الخبرة العلمية والفنية تستخدم في حالات كثيرة لإثبات الوقائع المختلفة، كتحديد الحالة العقلية للمتهم لتحديد مسؤوليته، وكذلك في حالة استخدام البصمة الوراثية لتحديد الجاني أو إثبات النسب والبنوة والقربة للفصل في قضايا النسب والميراث وغيرها^(٣).

إن عدم الاعتداد بالخبرة الفنية كوسيلة لإثبات الجريمة الإلكترونية، واعتبارها بمثابة قرائن فقط، يضيف صعوبة أخرى إلى صعوبات اكتشاف المجرم وتحديد هويته في ضوء عدم التسليم بالأمور التي تحكم الدليل الرقمي في الفكر الجنائي خارج نطاق تلك الجرائم^(٤).

وهناك ضرورة لاعتبار الخبرة الفنية في الجرائم الإلكترونية دليلاً مادياً فهي وسيلة علمية في مواجهة الجرائم الإلكترونية في ضوء طبيعة هذه الجريمة التي تعتمد على نبضات إلكترونية تتم من خلال التلاعب بقواعد البيانات في المنظمات، وذلك

(١) الهيتي، محمد حماد. (٢٠٠٥). جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها. مرجع سابق، ص ٢٣٢.

(٢) حجازي، عبد الفتاح بيومي. (٢٠٠٥). الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت. مرجع سابق، ص ٥١.

(٣) حسني، محمود نجيب. (١٩٨٨). شرح قانون الإجراءات الجنائية. مرجع سابق، ص ٤٧٥.

(٤) الهيتي، محمد حماد. (٢٠٠٥). جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها. مرجع سابق، ص ٢٣٣-٢٣٤.

بالإضافة أو الحذف أو التعديل وإخراج مخرج أو وثيقة إلكترونية مزورة بصورة صحيحة مستغلاً مهاراته في الدخول على النظام والقيام بالجرائم الإلكترونية والتلاعب التي يصعب كشفها بالطرق التقليدية، مما يحتم الاستعانة بأساليب علمية وخبرات فنية ذات فاعلية في إثبات الجريمة الإلكترونية والعمل على تطويرها والاستفادة من فاعليتها في إثبات هذه الجرائم. ومن خلال ذلك يمكن توضيح الأدوات العلمية لضبط إثبات الجريمة على أنها "أدوات تقوم بضبط الجريمة كغالبية برامج الحماية، وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وأدوات التصنت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، وأدوات الضبط الأخرى، ويمكن استخدام الأدوات المستخدمة في الجريمة كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين للمواقع"^(١). وتوضح هذه البرامج والتقنيات التي تستخدم في إثبات الجريمة بالأدلة العلمية وتكون نتائجها محكومة بقواعد معينة حسب طبيعتها ومنها:

(١) برامج حاسب آلي:

من خلال عمليات التحري الإلكتروني يمكن استخدام برامج استرجاع المعلومات من الأقراص التالفة، وبرامج كسر كلمة المرور، وبرامج الضغط، وفك الضغط ، وبرامج البحث عن الملفات العادية والمخفية، وبرامج تشغيل الحاسب، وبرامج نسخ البيانات، بالإضافة إلى برامج منع الكتابة على القرص الصلب التي تستخدم بعد ارتكاب الجريمة لحماية مسرحها، وكذلك برامج استرجاع الملفات المحذوفة التي يلجأ المجرم إلى حذفها للتخلص من الدليل الإلكتروني، وذلك بهدف جمع الاستدلالات إلكترونياً. وتظهر فاعليتها عند إتباع الإجراءات العلمية والفنية للتحري، حيث تمنع من تغيير المواد والبرامج المستخدمة في الاختراق والتعدي وارتكاب الجرائم^(٢).

(٢) برامج فحص ومراقبة الشبكات:

(١) العريان، محمد علي. (٢٠٠٤). الجرائم المعلوماتية. مرجع سابق، ص ٤٤ - ٤٥.
(٢) العنزي، سلمان. (٢٠٠٢). وسائل التحقيق في جرائم نظم المعلومات. رسالة ماجستير غير منشور، الرياض، جامعة نايف العربية للعلوم الأمنية، ص ٩٩.

وهي البرامج التي تستخدم في فحص البروتوكول TCP/IP لمعرفة المشكلات المتعلقة بالشبكات والعمليات التي تعرضت لها، وترجع فاعليتها إلى قدرتها الفائقة في الدخول على الشبكات، وتلمس برامج السرقة والتلصص، وكذلك الفيروسات التي تستخدم في عمليات الاختراق والتعدي والتزوير، وتحديد مصدرها بدقة^(١).

٣) برامج فحص الشبكة المحلية وبرامج التشارك في الموارد:

وهي برامج تستطيع فحص الشبكة المحلية، وكذلك التعرف على البرامج المشاركة في الموارد، ومن ثم تتبع حالات الاختراق والتعدي، حتى اكتشاف الـ (IP) الخاص بالمخترق الذي قام بارتكاب جريمة التزوير والتعرف على موقع الجهاز وترجع فاعليتها إلى قدرتها الفائقة على اكتشاف العنوان الرقمي (IP) الخاص بالجاني داخل الشبكة المحلية، وتحديد موقع الجهاز بدقة^(٢).

٤) برامج تتبع الاختراق الموجودة على شبكة الإنترنت:

يتم ذلك باستخدام بروتوكول تخاطب خاص بهذه البرامج، لتتبع نشاطاتها خلال فترة زمنية محددة، والتعرف على البرنامج الذي استخدم في الاختراق والتعدي من خلال خادمت الملفات التي يمكن من خلالها تحديد موقع الاختراق والتعدي^(٣). وترجع فاعليتها إلى قدرتها الفائقة على اكتشاف الـ (IP) الخاص بالجاني داخل الشبكة الدولية، وتحديد موقع الجهاز بدقة، وتختلف عن سابقتها باختلاف الشبكة، فهي ذات قدرة أعلى على التوغل في الشبكات الخارجية^(٤).

٥) برامج اكتشاف الثغرات التي تتخلل البرامج الموجودة على النت:

توجد بعض البرامج على شبكة الإنترنت، وهذه البرامج تساعد المستخدم على القيام بأعمال مهمة كالاتصال، وزيادة سرعة الإنترنت، ولكن المشكلة في إمكانية ترك المخترقين لثغوب بهذه البرامج يستطيعون من خلالها النفاذ إلى النظام واختراقه من

(١) المرجع السابق، ١٠٢.

(٢) العريان، محمد علي. (٢٠٠٤). الجرائم المعلوماتية. مرجع سابق، ص ٦١.

(٣) عبد المطلب، ممدوح عبد الحميد. (٢٠٠١). جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية: الجريمة عبر الإنترنت. الشارقة، مكتبة دار الحقوق، ص ٢٢٠.

(٤) عبد المطلب، ممدوح عبد الحميد. (٢٠٠١). جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية: الجريمة عبر الإنترنت. الشارقة، مكتبة دار الحقوق، ص ٢٢٠.

خلال البحث عن هذه البرامج والدخول من خلالها إلى نظم المعلومات والسيطرة عليه وارتكاب الجرائم الإلكترونية. ويمكن اكتشاف الثغوب الموجودة على البرامج باستخدام جدران الحماية، والبرمجيات التي تساعد في معرفة مصدر الاختراق^(١).

٦) برامج فك الشفرات:

من أهم فوائد التشفير أنه يقي من كشف التصنت على حزم المعلومات الخاصة بالمنظمات، والتصنت يعني نسخ حزم المعلومات عند انتقالها عبر الشبكة، حيث يمكن من الناحية التقنية مراقبة أداء الشبكة من خلال حزم البيانات المتدفقة عبر الشبكة؛ مما ييسر وصول المخترقين لهذه الحزم، ولكن يمكن منع التصنت باستخدام وسائل التشفير المناسبة؛ لأن عدم معرفة الشفرة معناه الحصول على بيانات ومعلومات مبهمه وغير مفهومة^(٢)، إلا أن هناك برامج يمكنها فك الشفرات، وبصفة خاصة للبرامج والمواقع التي تقوم بعمليات الاختراق والتعدي والتزوير، وهذه البرامج تحتوي على مليارات من الشفرات، وتقوم باستغلال الحاسب الآلي في تجربة هذه الشفرات في ثوانٍ معدودة حتى تقوم بفتح الموقع المشفر، ومن ثم متابعتها، ومعرفة ما إذا كان قد استخدم في عملية الاختراق والتعدي وارتكاب الجرائم الإلكترونية. وتتميز هذه البرامج بفاعلية عالية في فك أية شفرة، ومن ثم إمكانية الدخول على البرامج المشفرة التي استخدمت في الاختراق والتزوير والتعدي، ومعرفة مصدرها^(٣).

ب) ضوابط إثبات الجريمة الإلكترونية بالأدلة الإجرائية:

الضوابط الإجرائية هي الأساليب التي تستخدم لإثبات وقوع الجريمة وتحديد شخصية مرتكبها، وهذه الأساليب ذات فاعلية في التحقيق الفني، حيث تسهم في إثبات الجريمة وبيان الغموض وإيجاد العلاقة بين الجاني والمجني عليه من قبل المحقق الفني باستخدام تقنيات وبرامج التتبع الإلكتروني والتفتيش الإلكتروني والضبط الإلكتروني التي تتميز بقدرات فائقة على القيام بمهام التتبع والاسترجاع للبرامج

(١) الحمدان، عبد الرحمن بن عبد العزيز. والقاسم، محمد بن عبد الله. (٢٠٠٤). أساسيات أمن المعلومات. الرياض، مطابع الحميض، ص ٥٣.

(٢) الحميد، محمد دباس، ونيو، ماركو إبراهيم. (٢٠٠٧). حماية أنظمة المعلومات. مرجع سابق، ص ٥٤.

(٣) عبد المطلب، ممدوح عبد الحميد. (٢٠٠١). جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية: الجريمة عبر الانترنت. مرجع سابق، ص ٢٢٠.

والأدوات التي استخدمت في الاختراق والتعدي وارتكاب الجريمة، ويمكن توضيح هذه الضوابط حسب الطريقة المتبعة للوصول وحسب البرنامج المتبع، ومن تلك الطرق:

(١) الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته:

يجب على المحقق الفني الاطلاع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات، وكذلك قاعدة البيانات وإدارتها، وخطة تأمينها، وموارد النظام، والمستفيدين، والملفات، والإجراءات، وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، والوقت المخصص لكل مستفيد في حالة تعدد المستخدمين، وإجراءات أمن العاملين، وأسلوب النسخ الاحتياطي، وبرامج الحماية المتوفرة^(١). وتتم عملية الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته من خلال ما يلي:

أ - الاستعانة بالبرامج التحليلية الحديثة:

يمكن الاستعانة بهذه البرامج في حصر الحقائق والاحتمالات والأسباب والفرضيات، واستنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي وفق برامج لتغطية كافة الاحتمالات وتقديم الاحتمال الأقوى^(٢).

ب - التوقيف خلال فترة التحقيق:

هو سلب المتهم الذي تنور دلائل وشبهات قوية نحو ارتكابه جريمة إلكترونية حريته خلال فترة التحقيق حسب مقتضيات التحقيق ومصلحته، وهو إجراء من إجراءات التحقيق، ويطلق عليه مسمى الحبس الاحتياطي، وينتهي ببراءة المتهم والإفراج عنه، أو إصدار الحكم بتوقيع العقوبة عليه، والغرض من تقييد حرية المتهم في الجرائم الإلكترونية الخوف من استغلال مهارته في طمس وتدمير الأدلة المادية والإلكترونية^(٣).

(٢) إظهار الحقائق:

(١) العريان، محمد علي. (٢٠٠٤). الجرائم المعلوماتية. مرجع سابق، ص ٨١.
(٢) البشري، محمد الأمين. (٢٠٠١). التحقيق في جرائم الحاسب والانترنت. المجلة العربية للدراسات العربية والتدريب، العدد (٣٠)، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ص ١٨٦.
(٣) العززي، سلمان. (٢٠٠٢). وسائل التحقيق في جرائم نظم المعلومات. مرجع سابق، ص ١٠٦.

يجب على المحقق إظهار الحقائق خلال مرحلة جمع الاستدلالات الإلكترونية، وإثباتها في محضره نظراً لأهميتها في تحديد الجريمة، ورسم خطوات البحث من خلال التثبت من توافر أركان الجريمة، وتحديد مكان الجريمة ووصفه، وتحديد وقت وقوع الجريمة، وتحديد أسلوب ارتكاب الجريمة، وأداة ارتكاب الجريمة، والظروف المحيطة بالجريمة، ودوافع الجريمة^(١).

٣) التحقق من توافر أركان الجريمة

يحدد وقوع جريمة ما توفر ركنين أساسيين وهما الركن المادي ويقصد به الواقعة أو الضرر المادي للجريمة ويتمثل في نشاط الفاعل والنتيجة التي يحققها وعلاقة السبب بينهما، والركن الآخر هو الركن المعنوي ويقصد به الإرادة التي اقترن بها الفعل المرتكب ويأخذ صورة القصد الجنائي في الجريمة المتعمدة والصورة الخطاء غير المقصودة إن قانون العقوبات حدد لكل جريمة أركاناً معينة يجب توافرها حتى يتم الجزم بوقوعها، ومن البدهي أن أول حقيقة يجب أن يستظهرها محقق جمع الاستدلالات هي التثبت من وجود هذه الأركان ثم الجزم بوجود أو عدم وجود الجريمة، ففي جريمة السرقة مثلاً يجب على الباحث أن يتأكد من أن هناك مالاً منقولاً استولى عليه من شخص غير ماله ب قصد تملكه وهي أركان جريمة السرقة التي أوضحها قانون العقوبات وهكذا بالنسبة لجرائم نظم المعلومات^(٢). وتتم عمليات التحقق من توافر أركان الجريمة من خلال ما يلي:

أ - تحديد مكان الجريمة ووصفه:

يتوقف التوصل إلى الجاني على قدر كبير من نجاح عملية البحث في مكان الجريمة الذي سيوجد فيه الآثار والأدلة الجنائية المتصلة بها، ونتيجة لذلك يعتمد كثير

(١) كامل، محمد فاروق عبد الحميد. (١٩٩٩). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. الرياض، جامعة نايف العربية للعلوم الأمنية، ص ٦٦-٦٧.

(٢) بحر، عبد الرحمن. (١٩٩٩). معوقات التحقيق في جرائم الانترنت: دراسة مسحية على ضباط الشرطة في دولة البحرين. رسالة ماجستير منشورة، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ص ٣٨.

من الجناة إدراكاً منهم لهذه الحقائق إلى نقل هدف الجريمة من مكان إتمام الجريمة وإلقائه في مكان آخر لتضليل المحقق وتعقيد عمله البحث^(١).

ب- تحديد وقت وقوع الجريمة:

يتضمن تحديد وقت الجريمة تحديد تاريخ وساعة وقوعها، ويتم ذلك التحديد من أقوال المجني عليه أو المبلغ أو الشهود وقد يتم عن طريق الخبراء والمتخصصين، وهو عنصر هام لتحديد مسؤولية المتهم في ارتكاب الجرائم وذلك عند مناقشته عن خط سيره والأماكن والأشخاص الذين كان بصحبته في الفترة المعاصرة لارتكاب الجريمة واكتشاف مدى صدق البلاغ وصحة شهادة الشهود، بالإضافة إلى أن الوقت في بعض الجرائم تعد ظرفاً مشدداً، ولذلك يجب على المحقق الاطلاع على التوقيعات التي تظهرها برامج الحماية والتطبيقات^(٢).

ج- تحديد أسلوب ارتكاب الجريمة:

الأسلوب هو الكيفية المتغيرة في طريقة الوصول إلى الهدف التي اتبعتها الجاني في ارتكاب جريمته. ويدخل تحديد الأسلوب في الحقائق الجوهرية التي يجب أن يستوضحها المحقق نظراً لأهميته القصوى في تحديد خطة البحث عن الجاني في الجرائم، فكما أن لكل مجرم أسلوبه الإجرامي الذي لا يغيره إلا نادراً، فمن الأسلوب يستطيع المحقق حصر قطاعاً محدداً من المجرمين يركز البحث عن الجاني بينهم، ويكون التسجيل الجنائي مفيداً في تحديد أسلوب ارتكاب الجريمة ومعرفة مجرمين اعتادوا ارتكاب الجرائم المشابهة للجريمة المرتكبة. ومثالها زراعة برامج اختراق وتجسس أو الحصول على المعلومات فهذا الأسلوب يقوم به من أراد الحصول على معلومات ولا يستطيع الاقتراب من مصدرها ويكون التركيز على من يقوم بصيانة لتلك

(١) عبد الحميد، أحمد فاروق. (١٤٢٠هـ). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. الرياض، جامعة نايف العربية للعلوم الأمنية، ص ٦٥..

(٢) بحر، عبد الرحمن. (١٩٩٩). معوقات التحقيق في جرائم الانترنت: دراسة مسحية على ضباط الشرطة في دولة البحرين. مرجع سابق، ص ٤٢ .

الأجهزة، وينحصر البحث على موظفي الصيانة والتشغيل بالمؤسسة، أو أسلوب تغيير الإعدادات فغالباً يقوم به المبرمون الذين يعملون بالمؤسسة^(١).

د - تحديد أداة ارتكاب الجريمة:

تحديد الأدوات المستخدمة أمر جوهري لتحديد شخص الجاني، وتحديد الأشياء التي يقع على المحقق عبء التفتيش بحثاً عنها وضبطها، ومن أمثلة الأدوات برامج التصنت على الشبكات، وأقراص بدء التشغيل، وغيرها^(٢).

هـ - إيضاح الظروف المحيطة بالجريمة:

يستوجب على المحقق إيضاح الظروف التي تحيط بالجريمة، ومعرفتها. وتعد خطوة المحقق الأولى في تحديد ومعرفة سبب ودوافع الجريمة، وبعض هذه الظروف يكون سابقاً على وقوع الجريمة. ومثالها سوء سمعة المتهم وسلوكه والشكاوى والمشكلات السابقة التي حدثت بالمؤسسة وبعض الظروف المعاصرة وارتكاب الجريمة ومن أمثلته مكان وجود المتهم حال الجريمة، وتحديد درجة الإضاءة، وساعة ارتكاب الجريمة، وبعض هذه الظروف لاحق على ارتكاب الجريمة ومن أمثلته تصرفات وسلوك من تحوم حولهم الشبهات بعد ارتكاب الجريمة^(٣).

و - تحديد دوافع الجريمة:

من الأمور المهمة التي يسعى المحقق لكشفها معرفته دوافع الجريمة، ويعني سبب الجريمة الوقائع المادية التي حدثت فأثرت في نفسية الجاني مما أدى إلى بروز الدافع على ارتكابه للجريمة وهو أمر نفسي داخلي يرتبط أساساً بمجموعة من الغرائز الإنسانية وهو يتبلور عادة في بروز حاجة ما تدفع الشخص إلى توجيه سلوكه لإشباعها، فتحدد السبب في بعض الجرائم يشكل في حد ذاته دليلاً على ارتكاب المتهم للجريمة، ويكفل تحديد السبب حصر دائرة البحث في عدد محدد من الأشخاص، وبالعكس فإن عدم تحديد أسباب الجريمة يربك المحقق لتعدد الطرق التي

(١) عبد الحميد، أحمد فاروق. (٢٠١٤هـ). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. مرجع سابق، ص ٦٢.

(٢) العريان، محمد علي. (٢٠٠٤). الجرائم المعلوماتية. مرجع سابق، ص ١٥١.

(٣) شتا، محمد محمد (٢٠٠٠). فكرة الحماية الجنائية لبرامج الحاسب الآلي. القاهرة، دار الجامعة الجديدة للنشر، ص ١٦٣.

يجب عليه أن يسلكها في بحثه لكشف الجريمة ويطيل من فترة البحث مما قد يوقعه في دائرة اليأس من كشف الجريمة، ويؤخذ عدم وضوح سبب ودوافع الجريمة كدليل نفي قد يشير إلى براءة من تحوم حوله الشبهات مما قد يؤدي إلى استبعاده من قائمة الاتهام أو الحكم ببراءته إذا كان الاتهام قد وجه إليه^(١)، وفي جرائم نظم المعلومات غالباً ما يصبح من الصعب جداً معرفة سبب الحادث وذلك لأن دوافع الجناة غير واضحة، أو قد تحدث الجريمة بالخطأ، أو أن الجاني لا يحدد هدفاً للجريمة وهذا راجع لأسلوب ارتكاب الجريمة.

٤) إتباع القواعد الفنية لكشف الجريمة

أن عمل المحقق يبدأ منذ الوقت الذي يصله فيه خبر وقوع جريمة، ويقوم بالإجراءات التي يتخذها عقب ذلك من معاينة وتفتيش وانتداب للخبراء وسماع للشهود واستجواب لأطراف الجريمة، وجمع التحريات، وهو في كل هذه الإجراءات يستخلص العديد من الأدلة ويحاط علماً بكثير من الوقائع المتصلة بالجريمة والتي تختلف في قوة ثبوتها، وتأتي في أعقاب ذلك مرحلة يجد المحقق فيها نفسه وأمامه مجموعة ضخمة من الأدلة والوقائع التي أمكنه جمعها^(٢)، ولمحاولة كشف الجريمة على المحقق التقيد بالتالي:

أ- مراعاة الاحتمالات الشائعة في الجرائم:

لا يمكن حصر الاحتمالات نتيجة لتعدد واختلاف هذه الاحتمالات حسب ظروف وأسباب كل جريمة، إلا أن هناك مجموعة من الاحتمالات التي يضعها المحقق عادة في ذهنه عند فحصه لبعض أنواع الجرائم كاحتمال عدم وجود جريمة أصلاً أو احتمال كذب البلاغ أو تصويره على غير حقيقته، كذلك احتمالات الظروف المحيطة بالجريمة مثل مدى وقوع الجريمة فجأة ونتيجة لظروف عارضة، أو كونها

(١) عبد الحميد، أحمد فاروق. (٢٠١٤هـ). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. مرجع سابق، ص ٦٩.

(٢) الشوا، محمد سامي. (٢٠٠٠). ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة، دار النهضة العربية، ص ٧٤.

متصلة بحوادث أخرى وسبقها تهديد من الجاني، وهل الجاني فرد واحد أم عدة أفراد، هل كان على صلة بالضحية أم لا، وهل هو أحد الموظفين أو المتواجدين أساساً بالمؤسسة أم هو شخص من الخارج، وتتضمن الاحتمالات الأساليب المختلفة التي يمكن أن يرتكب بها الحادث^(١).

ب- حصر احتمالات وقوع الجريمة:

يقصد باحتمالات وقوع الجريمة الخطوات التي يتصور المحقق أن الجريمة قد سارت فيها منذ مرحلة نشوء أسبابها والتفكير فيها والتحضير لها ثم تنفيذها وهي الأدوار التي تمر بها الجرائم عادة، والمحقق في تصوره لهذه المراحل يعتمد أساساً على الأدلة والوقائع التي تمكن من جمعها خلال مراحل بحثه في الجريمة وذلك بإتباع طرق متعددة عند فحصه لهذه الأدلة، كما أن التصورات التي يمكن أن يستخلصها من هذه الأدلة تختلف حسب نوع الجريمة التي يبحثها، ومن طرق تحديد الاحتمالات تحليل الأدلة التي لا بد وأن تشير إلى مدلول محدد أو عدة مدلولات تتصل بالجريمة التي يجري بحثها، كما أنه يفضي إلى مجموعة من الاستنتاجات التي يمكن تصور حدوثها نتيجة لوجوده، كما يترتب عليه استبعاد عديد من الوقائع التي يتنافى وجودها مع وجوده فضلاً عن مساهمته في إعطاء صورة تقريبية لمكان وقوع الحادث، والمحقق عندما يحلل ما حصل عليه من أدلة ووقائع بالصورة السابقة يبني في نفس الوقت الاحتمالات الممكنة لوقوع الجريمة التي يبحثها^(٢).

ج- فحص الاحتمالات:

بعد أن يحصر المحقق الاحتمالات التي يمكن أن تقع على أساسها الجريمة وذلك في ضوء مدلولات الأدلة والحقائق التي استنتجها منها وما استبعده من احتمالات نتيجة لها وما استخلصه من تصورات لكيفية ارتكاب الجريمة يبدأ بعد ذلك في فحص كل احتمال من هذه الاحتمالات متبعاً في ذلك القواعد الفنية: رسم خطة البحث، والبدء

(١) شتا، محمد محمد (٢٠٠٠). فكرة الحماية الجنائية لإبرام الحاسب الآلي. مرجع سابق، ص ١٧١.
(٢) بحر، عبد الرحمن. (١٩٩٩). معوقات التحقيق في جرائم الانترنت: دراسة مسحية على ضباط الشرطة في دولة البحرين. مرجع سابق، ص ٦٩.

بالاحتمال الأقوى، وعدم التشبث باحتمال واحد، وعدم التعجل للوصول إلى نتيجة إيجابية من فحص الاحتمال^(١).

■ عناصر إثبات الجريمة الإلكترونية:

هناك العديد من العناصر المختلفة لإثبات الجريمة الإلكترونية، ويمكن توضيح هذه العناصر ما يلي:

العنصر الأول: إظهار الركن المادي للجرائم الإلكترونية:

إن النشاط أو السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة رقمية واتصال بالإنترنت، ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل الكمبيوتر 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، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها. لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإلكترونية حتى ولو كان القانون لا يعاقب علي الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، ف شراء برامج اختراق، وبرامج فيروسات، ومعدات لفك الشفرات وكلمات المرور، وحياسة صور مخلة بالآداب للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها^(٢).

(١) عبد الحميد، أحمد فاروق. (١٤٢٠هـ). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. مرجع سابق، ص ٣١٤.

(٢) عبد المطلب، ممدوح عبد الحميد. (٢٠٠١). جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية: الجريمة عبر الانترنت. مرجع سابق، ص ٢٢٦.

العنصر الثاني: إظهار الركن المعنوي للجرائم الإلكترونية:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويتحدد الركن المعنوي للجريمة المعلوماتية من خلال مبدأ الإرادة ومبدأ العلم، فالمجرم المعلوماتي تارة يستخدم الإرادة للتخطيط للجريمة، وتارة أخرى يستخدم العلم من أجل تنفيذ الجريمة الإلكترونية^(١).

العنصر الثالث: تحديد وقت ومكان ارتكاب الجريمة الإلكترونية

تشير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم احد البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين، وهذا بالتالي يثير مشكلة أخرى وهي مكان ارتكاب الجريمة الإلكترونية، ويثار أيضاً إشكاليات القانون الواجب التطبيق في هذا الشأن، حيث إن هناك بعد دولي في هذا المجال ذلك أن الجريمة الإلكترونية جريمة عابرة للحدود^(٢).

العنصر الرابع: علانية التحقيق:

إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولهذا قيل إن العلانية في مرحلة المحاكمة لا يقصر فيها الأمر علي وضع الاطمئنان في قلب المتهم، بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلاً للشك أو الخضوع تحت التأثير، كما أن فيها اطمئناناً للجمهور علي أن الإجراءات تسير في طرق طبيعية. والعلانية المقررة للتحقيق في الإجراءات الجنائية هي من بين الضمانات الخاصة به، وهي تختلف في التحقيق الابتدائي عنها في مرحلة المحاكمة. ففي الابتدائي تعتبر العلانية نسبية أي قاصرة علي الخصوم في الدعوى الجنائية، والعلانية في التحقيق النهائي أو

(١) العريان، محمد علي. (٢٠٠٤). الجرائم المعلوماتية. مرجع سابق، ص ١٥٧.

(٢) شتا، محمد محمد (٢٠٠٠). فكرة الحماية الجنائية لبرامج الحاسب الآلي. مرجع سابق، ص ١٩٢

مرحلة المحاكمة هي علانية مطلقة، بمعنى أنه يجوز لأي فرد من أفراد الجمهور الدخول إلى قاعة الجلسة وحضور المحاكمة^(١).

على أن المنظم يجيز في المرحلتين التحقيق الابتدائي والتحقيق النهائي مباشرة الإجراءات في غير علانية، فيصدر القرار بجعله سرياً، ولما كان هذا استثناء يأتي على قاعدة عامة أصلية كان من المنطقي أن نرى المنظم يحدد الأحوال التي يجوز فيها جعل التحقيق سرياً، وهذه علي كل حال رخصة لا يحسن الالتجاء إليها إلا عند الضرورة، ولهذا كان القرار بجعل التحقيق سرياً موجهاً للجمهور عامة وللشهود خاصة بأهمية وخطورة الواقعة التي يجري التحقيق فيها، وينعكس هذا الأثر في صورة اضطراب وتردد، بل قد يصل الأمر إلى إنكار المعلومات من جانب الشاهد. ولذلك فان ظروف مثل هذا التحقيق ينبغي أن تكون محل تقدير دقيق حين الاستهداء بأقوال الشاهد، فرغم أن العلانية النسبية في التحقيق الابتدائي تجعل حضور إجراءاته قاصراً على من له علاقة بالدعوى الجنائية، إلا أن هؤلاء بذاتهم قد يكون لهم أعمق الأثر في نفسية الشاهد. وهناك بعض المسائل التي تتصل بعلانية التحقيق لها أهمية عملية خاصة، هي اختيار مكان التحقيق، وحضور الخصوم أثناء التحقيق، والقواعد التي ينبغي مراعاتها في معاملة الحضور^(٢).

(١) السبهان، فهد إبراهيم. (١٩٩٥). استجواب المتهم بمعرفة سلطة التحقيق. مرجع سابق، ص ٥٢.
(٢) الشاذلي، فتوح عبد الله. (١٩٩٨). قانون العقوبات: القسم العام. مرجع سابق، ص ١٤٦.

الفصل الرابع

طرق إثبات الجريمة الإلكترونية

المبحث الأول: إثبات الجريمة الإلكترونية بالشهادة والإقرار

المبحث الثاني: إثبات الجريمة الإلكترونية بالخبرة الفنية (الأدلة الرقمية والقرائن)

المبحث الثالث: معوقات إثبات الجريمة الإلكترونية

المبحث الأول

إثبات الجريمة الإلكترونية بالشهادة والإقرار

تمثل قواعد الإثبات أهمية خاصة إذ إن الحق موضوع التقاضي يتجرد من كل قيمة إذا لم يقيم الدليل على الواقعة التي يستند إليها، فالدليل هو عصب الواقعة أو هو النتيجة التي تحققت باستعمال وسائل الإثبات المختلفة أي إنتاج الدليل. ويقصد بهذا الإثبات: القواعد المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء وتقديرها من جانبه، فالإثبات هو مجموع الأسباب المنتجة لليقين، وبالتالي فإن الإثبات في المواد الجنائية ما هو إلا كافة الأدلة التي تؤكد وقوع الجريمة، وتحقق حالة اليقين لدى القاضي لإدانة المتهم، أو ترجح حالة الشك لديه فيقضي بالبراءة. أو هو كل ما يؤدي إلى إظهار الحقيقة، ولأجل الحكم على المتهم في المسائل الجنائية يجب ثبوت وقوع الجريمة في ذاتها وأن المتهم هو المرتكب لها. أو بعبارة أخرى وقوع الجريمة بوجه عام ونسبتها للمتهم بوجه خاص، وحتى يتحقق الدليل اللازم للإثبات فإنه لا بد من جمع عناصر التحقيق والدعوى، وتقديم هذه العناصر إلى سلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو أدلة ترجح معها إدانة المتهم قدمته إلى المحكمة، ومرحلة المحاكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي بإدانة المتهم وإلا قضى ببراءته^(١).

أولاً: إثبات الجريمة الإلكترونية بالشهادة (شهادة الخبير):

- مفهوم الشهادة:

الشهادة هي إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه من هذه الواقعة بطريقة مباشرة. وتعرف أيضاً على أنها: (تقرير يصدر من شخص في شأن واقعة عاينها بحواسه عن طريق السمع أو البصر، وهي دليل شفوي يدلي به شفويّاً أمام السلطة المختصة)، ومن خلال ما جاء في التعريفين يمكن

(١) فرغلي، عبد الناصر محمد، والمسماري محمد عبيد. (٢٠٠٧). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة. المؤتمر العربية الأول لعلوم الأدلة الجنائي والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، ص ١٦.

القول أن المقصود بالشهادة (شهادة الشهود) هي تلك المعلومات التي يقدمها شخص أو أشخاص إلى السلطة المعنية سواء سلطة التحقيق أو أمام المحكمة^(١).

- أنواع الشهادة المستخدمة في إثبات الجريمة الإلكترونية:

تنقسم الشهادة حسب الفقه الجنائي إلى ثلاثة أنواع هي الشهادة المباشرة والشهادة السماعية والشهادة بالتسامع، ويتم توضيح كل منها كما يلي:

(١) **الشهادة المباشرة:** وهذه الشهادة هي الأصل لأن الأصل في الشهادة أن تكون مباشرة، سواء كان أمام قاضي التحقيق أو حتى في مرحلة جمع الاستدلالات وأيضاً أمام التحقيق النهائي أي أمام المحكمة فيدلي بما وقع تحت سمعه وبصره مباشرة، فهو إذا شهد على واقعة وقعت من الغير أمامه يترتب عليها حق لغيره وهنا يكون متيقناً من حواسه وفي العادة يدلي الشاهد بأقواله مما رآه أو سمعه من الوقائع المتعلقة بالدعوى أمام القضاء كما قد يكتفي بتلاوة شهادته المكتوبة أو يضم هذه الشهادة إلى ملف القضية في الظروف الاستثنائية، وتطبق هذه الحالة على الجريمة الإلكترونية حيث يقوم الشاهد بالإدلاء بما شاهده من قيام مرتكب الجريمة بأية ترتيبات برمجية تتعلق بارتكاب الجريمة، أو من خلال ما شاهده من قيام مرتكب الجريمة، بعملية الاختراق لأي ملفات إلكترونية أو القيام بأي من أنواع التزوير الإلكتروني، وفي هذه الحالة تعتبر الشهادة على مرتكب الجريمة شهادة مباشرة^(٢).

(٢) **الشهادة السماعية (الشهادة غير المباشرة):** الشهادة السماعية هي بخلاف الشهادة المباشرة فهي تكون غير مباشرة، لأنها شهادة من علم بالأمر من الغير فيشهد مثلاً أنه سمع من شخص آخر واقعة ارتكاب جريمة معلوماتية مثل ارتكاب أي من أنواع الجرائم الإلكترونية المستحدثة أو جرائم الإنترنت، وهذه الشهادة من حيث قيمتها في الإثبات هي أقل درجة من الشهادة المباشرة ولكنه عند وفاة الشاهد الأصلي يأخذ القاضي بهذه الشهادة والقانون لم ينص على عدم الأخذ

(١) الخماسي، فتحي بن الطيب. (١٤٢٥ هـ) الفقه الجنائي الإسلامي. دمشق، سوريا، دار فتيية، ص ٩٧.
(٢) عبد الحميد، أحمد فاروق. (١٤٢٠ هـ). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. مرجع سابق، ص ٧٧.

بهذه الشهادة، وربما تكون هذه الشهادة في حد ذاتها موضع ثقة إلا إذا كانت نتيجة معلومات أدركها الشاهد بحواسه لأن خلاف ذلك يجعل الشهادة معرضة للتحريف ويشوبها الشك وعليه إذا اعتمدت المحكمة على الشهادة السماعية وحدها كان حكمها مشوباً في الاستدلال، وتطبق هذه الشهادة أيضاً على الجريمة الإلكترونية، فربما يسمع الشاهد من شخص آخر عن ارتكاب أحد الأفراد جريمة معلوماتية أو أي من جرائم الإنترنت، ولكنه لم ير بنفسه، وفي هذه الحالة يجوز للمحكمة أن تأخذ بالشهادة أو لا، حسب ما يراه قاضي التحقيق^(١).

٣) الشهادة بالتسامع: تختلف الشهادة بالتسامع عن الشهادة السماعية المتعلقة بأمر معين نقلاً عن شخص معين شاهد هذا الأمر بنفسه وهذه الشهادة بالتسامع تتعلق أيضاً بأمر معين لكنها ليست نقلاً عن شخص معين شاهد الأمر بنفسه فيقول الشاهد سمعت كذا أو أن الناس قالوا كذا دون أن يستطيع إسنادها لأشخاص معينين أما من حيث قيمتها في الإثبات فهي ضئيلة ولا تلقى قبولاً في المسائل الجنائية المتعلقة بارتكاب أي من أنواع الجرائم سواء الجرائم التقليدية أو الجرائم الإلكترونية، وإن كان القضاء يقبلها في بعض المسائل المتعلقة بالجوانب التجارية^(٢).

ويتضح من خلال ذلك أن من أكثر المسائل جدلاً في حقل الأبعاد الإجرائية لدعوى المعلوماتية في نطاقها الحقوقي والجزائي، مسألة نطاق الإفشاء بالمعلومات المطلوب أو الجائز للشاهد المعلوماتي، فالشاهد يشهد فيما شهد بذاته أو قال أو علم، لكن الأمر في دعوى المعلوماتية مختلف، إذ ثمة نظام معين للمنشأة وثمة أعمال لا تتصل بالشاهد بذاته بل ربما لا تتصل بشخص طبيعي وقد تكون متصلة بنظام إلكتروني أو نحوه، كما أن الشاهد يعلم الكثير وجزء مما يعلم واقع ضمن إطار الخصوصية والسرية. ولذلك فإن التنظيم القانوني لإثبات الجريمة الإلكترونية في الدعوى المعتمدة على أدلة معلوماتية أو تتصل بعوالم التقنية والإلكترونيات يجب إعادة توصيفها قانوناً بل

(١) كامل، محمد فاروق عبد الحميد. (١٩٩٩). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. الرياض، جامعة نايف العربية للعلوم الأمنية، ص ١٠٩.
(٢) الخماسي، فتحي بن الطيب. (١٤٢٥هـ) الفقه الجنائي الإسلامي. دمشق، سوريا، دار قتيبة، ص ١٠٢-١٠٣.

وتنظيمها بشكل لا يضع الشاهد موضع المساءلة ولا يحرم القضاء فرصة الإفادة من شهادة الشاهد في توضيح الحقيقة التي تتوقف في أحيان كثيرة على ما يعلمه الشاهد بالخبرة النظرية لا ما يعلمه بالواقع من حقائق قد رآها أو سمعها أو نقلت له^(١).

والشهادة في الجريمة الإلكترونية قد لا تتطلب الرؤية أو السماع ولكن يتم الأخذ بها من خلال الاستعانة بالخبراء الفنيين المختصين في مجال الحاسب الآلي، ففي حالة عدم إمام المحقق الجنائي بمجال الحاسب الجنائي، فعليه أن يستعين بخبراء الحاسب الآلي بهدف تأمين الحاسب الآلي والحفاظ على الأدلة الموجودة به من التلف أو تعطيلها من قبل مرتكب الجرائم الإلكترونية، وفي هذه الحالة يمكن الأخذ بشهادة الفنيين فيما تم ارتكابه من جرائم إلكترونية معتمدة على الحاسب الآلي.

- إثبات الجريمة الإلكترونية بالشهادة:

أ) دور الشهادة في إثبات الجريمة الإلكترونية:

تدل الشهادة على واقعة ذات أهمية قانونية فهي تدل على وقوع الجريمة ونسبتها إلى المتهم في الإطار الجزائي والشهادة يقدمها (أي يدلي بها الشاهد) وهو شخص خارج عن أطراف الخصومة ولديه معلومات تفيد في الكشف عن الحقيقة المتصلة من حيث تحديد الأفعال المرتكبة وجسامة الجريمة وبالتالي نسبتها إلى فاعلها ومنه فترديد الشائعات ليس من قبيل الشهادة، والشاهد حين يدلي بشهادته غير مطالب بتقييم الواقعة كأن يدلي الشاهد بأن الجاني كان في حالة سكر فهنا ليس من اختصاصه تحليل عامل السكر كمانع للمسؤولية الجزائية^(٢). والشهادة في مجال الجريمة الإلكترونية لا تختلف من حيث ماهيتها عنها في الجريمة التقليدية، وأمر سماع الشهود متروك لفطنة المحقق ومرتبطة بظروف التحقيق، والأصل أن يطلب الخصوم سماع من يرون من الشهود، وللمحقق أن يدعو للشهادة من يقدر أن لشهادته أهمية، وله أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه. والشاهد في الجريمة الإلكترونية هو ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية أو هامة لأزمة للدخول

(١) السرحاني، محمد نصير. (٢٠٠٤). مهارات التحقيق الجنائي الفني في جرام الحاسب الآلي والإنترنت. رسالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية، ص ٣٣.
(٢) الخماسي، فتحي بن الطيب. (١٤٢٥ هـ) الفقه الجنائي الإسلامي. مرجع سابق، ص ١١٢.

في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التتقيب عن أدلة الجريمة داخله، ويطلق على هذا الشاهد اسم الشاهد المعلوماتي (وذلك تمييزاً له عن الشاهد التقليدي). والشاهد المعلوماتي بهذا المفهوم قد يكون واحداً من عدة طوائف أهمها^(١):

(١) **مشغلو الحاسب الآلي** : وهم الخبراء الذين تكون لهم الدراية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به واستخدام لوحة المفاتيح في إدخال البيانات وتكون لديهم معلومات عن قواعد كتابة البرامج.

(٢) **المحللون** : والمحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة واستنتاج العلاقات الوظيفية منها، كما يقوم كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

(٣) **المبرمجون**: وهم الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين:

- **الفئة الأولى**: هم مخططو برامج التطبيقات، ويقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقومون بتحويلها إلى برامج دقيقة وموثوقة لتحقيق هذه المواصفات.

- **الفئة الثانية**: هم مخططو برامج النظم، ويقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية وإدخال أية تعديلات أو إضافات لها.

(٤) **مهندسو الصيانة والاتصالات**: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

(٥) **مديرو النظم**: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية. ويتضح من خلال ما سبق أن الشهادة تمثل أهمية كبيرة في إثبات الجريمة الإلكترونية في المواد الجزائية فهي ترد على وقائع مادية وترشد القاضي إلى تحري قيمتها ولذا يقال أن الشهادة عماد الإثبات والشهود عيون المحكمة وأذانها، في إثبات الجريمة،

(١) عبد اللاه، هلاي. (٢٠٠٠). التزام الشاهد بالإعلام في الجرائم المعلوماتية. القاهرة، دار النهضة العربية، ص ٢٣-٢٤.

حيث يكون غالباً للشهادة أثناء التحقيق أثر كبير فيما يتعلق بالبراءة والإدانة ولها أهميتها في الكشف عن الأدلة إذا أدلى بها قبل ضياع معالم الجريمة المتمثلة في الأجهزة والوسائل الإلكترونية الأخرى التي تساعد في ارتكاب الجريمة الإلكترونية، وذلك لأن هناك وقائع مادية لا يمكن إثباتها بالكتابة غير أنه ورغم أن هذه الأهمية للشهادة إلا أن هناك من ينتقدها على أساس أن قدرة الشاهد على استجماع الوقائع في ذاكرته قد تضعف مع مرور الوقت كما قد تعتمد في أحيان أخرى على ضمير الشاهد ومدى حرصه على قول الحقيقة^(١).

ومن خلال ما تقدم يمكن القول أن الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها، وللشهادة في مجال الإجراءات أهمية بالغة، لأن الجريمة ليست تصرفاً قانونياً ولكنها عمل غير مشروع يجتهد الجاني في التكتّم عند ارتكابه وبحرص على إخفائه عن الناس. ولهذا فإن العثور على شاهد يعتبر مكسباً كبيراً للعدالة ومن هنا جاءت قاعدة عدم رد الشهود.

ب) تقدير الشهادة على الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي:

تتنوع نظم الأدلة الجنائية في الإثبات الجنائي للجرائم الإلكترونية، بين التي تأخذ بنظام الأدلة القانونية في الإثبات، وأخرى تعتق نظام الإثبات الحر القائم على حرية المحقق في الاقتناع، وتلك التي تجمع بين النظامين بما يسمى بالنظام المختلط. ووجه الفرق بين هذه النظم أنه في نظام الأدلة يقيّد القاضي في الإثبات الجنائي للجريمة الإلكترونية بأدلة يحددها له المنظم مقدماً ويقدر له قيمتها في الإثبات، فيقيّد القاضي بأن يستمد اقتناعه من هذه الأدلة دون غيرها. أما في نظام الأدلة الإقناعية للجريمة الإلكترونية مثل الشهادة والإقرار فإن القاضي لا يقيده المنظم بأدلة إثبات معينة وإنما يترك له حرية الإثبات وفقاً لسلطته التقديرية في تقدير الدليل، ويترتب على ذلك أن

(١) الحمدان، عبد الرحمن بن عبد العزيز. والقاسم، محمد بن عبد الله. (٢٠٠٤). أساسيات أمن المعلومات. مرجع سابق، ص ١٢٢.

للقاضي الجنائي قبول أي دليل يمكن أن يتولد منه اقتناعه، وأنه هو الذي يقدر قدرته في الإثبات على قدر اقتناعه به^(١).

ويسيطر على الإثبات الجنائي للجريمة الإلكترونية مبدأ حرية القاضي في الاقتناع بالشهادة أو الإقرار، فالقاضي يستطيع أن يستمد قناعته من أي دليل يرتاح إليه وجدانه. وهذه الحرية التي يتمتع بها القاضي ليست مقررّة لكي تتسع سلطته من حيث الإدانة أو البراءة، وإنما هي مقررّة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجنائية. فاستنباط الحقيقة من هذا الدليل إنما يتم بمعرفة القاضي ومدى قدرته على الوصول إلى الحقيقة ومدى توافر حاسة القضاء لديه. ولذلك نجد أن القاضي يتمتع دائماً بدور إيجابي في الدعوى الجنائية. وينطبق ذلك أيضاً على الجريمة الإلكترونية، فيلاحظ أنه على الرغم من تمتع القاضي بالحرية في تكوين عقيدته عن الجريمة الإلكترونية، إلا أنه يلتزم ببيان الأدلة الإلكترونية التي استمد منها اقتناعه، فليست الحرية أن يطلق له العنان لكي يقتنع بما يحلو له، وإنما تتضح حريته في استخلاص الحقيقة من أي مصدر مشروع. فهناك طرق للإثبات نص عليها قانون الإجراءات الجنائية وهي التي تعتبر مشروعة وهي التي يجوز له استخلاص الحقيقة منها، وذلك مثل الشهادة والإقرار والمراقبة والتفتيش^(٢).

- تعيين الشهود واستدعائهم في الجريمة الإلكترونية:

يعتبر سماع الشهود كسائر إجراءات التحقيق من الأمور التقليدية للمحقق فله أن يسمع الشهود أو يستغني عنهم فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه، والأمر متروك إلى فطنة المحقق ومرتبطة بظروف التحقيق والأصل أن يطلب الخصوم سماع من يرون من الشهود غير أن للمحقق أن يجيبهم إلى طلبهم أو يرفضه وله أن يدعو للشهادة من يقدر أن لشهادته أهمية بل له أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه، ومن المبادئ المستقرة أن الشاهد لا يرد ولو غلب على الظن أنه لن يتحرى الصدق في شهادته سواء كان ذلك راجعاً لانحطاط في خلقه أو

(١) السرحاني، محمد نصير. (٢٠٠٤). مهارات التحقيق الجنائي الفني في جرام الحاسب الآلي والإنترنت. مرجع سابق، ص ٤٥.

(٢) البداينة ذياب. (١٩٩٩). جرائم الحاسب والإنترنت: الظواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض، أكاديمية نايف العربية للعلوم الأمنية، ص ٤٥.

لوجود صلة مودة أو لعداوة بينه وبين المتهم تجعله يميل له أو ضده^(١). ومن خلال ما سبق يمكن توضيح طريقة تعيين الشهود واستدعائهم في الجريمة الإلكترونية كما يلي:

١) التزامات الشاهد المعلوماتي:

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للدخول في نظام المعالجة الآلية للبيانات سعياً عن أدلة الجريمة بداخله، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟ فهناك اتجاهان في هذا الصدد:

▪ **الاتجاه الأول:** ويرى أنه ليس من واجب الشاهد وفقاً للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل أصحاب هذا الاتجاه إلى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب وكذلك لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة^(٢).

▪ **الاتجاه الثاني:** وينقسم أنصار هذا الاتجاه إلى فئتين، فترى الفئة الأولى من أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة حيث يرى أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم، ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائياً إلا في مرحلة التحقيق والمحاكمة. بينما ترى الفئة الثانية من أنصار هذا الاتجاه أن مشروع قانون الحاسب الآلي يتيح لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام

(١) حسن، سعيد عبد اللطيف. (١٩٩٩). إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت. القاهرة، دار النهضة العربية، ص ٧٦.

(٢) جاد، نبيل عبد المنعم. (٢٠٠٥). جرائم الحاسب الآلي. ندوة المواجهة الأمنية للجرائم المعلوماتية، مركز دعم اتخاذ القرار بالقيادة العامة لشرطة دبي، مطبعة بن دسمال، ص ١٢٨.

لتقديم المعلومات اللازمة لاختراقه والدخول إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة وإذا وجدت بيانات مشفرة داخل ذاكرة الحاسب وكانت مصلحة التحقيق تستلزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات، وترى الفئة الثالثة من أنصار هذا الاتجاه أنه يمكن الحصول من القائم على تشغيل نظام الحاسب على كلمة المرور السرية للدخول في نظام المعلومات كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني لكن ليس على الشاهد أي التزام بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسب وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل وليس الكشف عن معلومات جديدة^(١).

٢) الشهادة على الكيانات المادية والمعنوية التي ترتكب من خلالها الجريمة الإلكترونية:

تخضع الكيانات المعنوية في الوسائل الإلكترونية لإجراء عملية الشهادة عليها، فقد يقوم مستخدم هذه الكيانات باستخدامها في ارتكاب الجرائم، وفي هذه الحالة يجب الشهادة عليه من قبل قام بملاحظته في هذا الاستخدام، كما أن هناك تشريعات قد نصت صراحة على صلاحية هذه الكيانات لتكون محلاً للشهادة، وأن هناك جانباً من الفقه قد ذهب إلى صلاحية هذه المكونات كمحل يقع عليه الشهادة والإقرار.

ويجب أن يتم خضوع الكيانات المعنوية التي يتم بها ارتكاب الجريمة الإلكترونية لعملية الشهادة، وذلك لأن الكيانات المادية وفقاً للتفسير المنطقي الذي يفسر النص على ضوء المصلحة التي يحققها المنظم من ورائه. ويترتب على ذلك أن الشيء طالما يحقق منفعة أو مصلحة اقتصادية فإنه يكون محلاً للحماية سواء أكان هذا الشيء من الكيانات المادية أو المعنوية، ولذلك فالشيء إذا كان يمثل قيمة اقتصادية أو ذهنية فإنه يستحق الحماية الجنائية سواء أكان ذو طبيعة مادية أو معنوية ويجوز أن تتم الشهادة على هذا الشيء أيضاً حيث تستخدم هذه الشهادة كإثبات للجريمة، فإذا كان التفتيش ينتهي بتحديد موضع ومكان البيانات التي يستهدف الوصول إليها، فإن المعالجة التي تجري عليها

(١) عبد الله، هلال. (٢٠٠٠). التزام الشاهد بالإعلام في الجرائم المعلوماتية. مرجع سابق، ص ٣٤-٣٥.

لجعلها مرئية للإطلاع عليها وإثباتها، أو بإخراجها من الحاسب في صورة مستندات مطبوعة لا تعد تفتيشاً عن أدلة الجريمة، ولكنها تمثل وصولاً إلى هذه الأدلة ومن ثم تعد ضبطاً لها، ولذا يمكن الشهادة على هذه الأدلة الإلكترونية التي تم الحصول عليها، وعلى من قام باستخدامها لارتكاب الجريمة^(١).

ويلاحظ كذلك أنه يمكن الشهادة على كافة الأدوات والمستندات التي تكون قد استعملت أو تحصلت من الجرائم التي تقع على العمليات الإلكترونية، فيمكن الشهادة على من قام باستعمال الأوراق المالية المزورة، وقد تضبط هذه الأوراق بداخل الحاسبات الآلية، أو تضبط أدواتها بداخل نظم الحاسب كالأوراق المعدلة لذلك والأشرطة المغناطيسية وغير ذلك من وسائل التزوير، ويمكن أيضاً الشهادة على المحررات الإلكترونية المزورة كمخرجات أو بيانات داخل ذاكرة الحاسب الآلي، ويمكن كذلك الشهادة على عمليات الغش والنصب التي تتم بالنسبة لأنظمة الصرف الآلي للنقود طبقاً لما هو مسجل من بيانات حقيقية داخل هذه الأنظمة. وأيضاً فإن الشهادة قد تشمل الأشياء التي تكون قد تعرضت للتخزين أو للإتلاف على النحو الذي تكشف عنه الكيانات المادية والمنطقية للحاسبات الآلية، كذلك تتم الشهادة على من قام بتخزين هذه المعلومات التي تم استخدامها في ارتكاب الجرائم الإلكترونية^(٢).

٣) الشهادة على المراسلات الإلكترونية التي تساعد في ارتكاب الجريمة الإلكترونية:

يقصد بالمراسلات الإلكترونية استخدام شبكات الإنترنت في نقل الرسائل بدل من الوسائل التقليدية. وبالنظر إلى سهولة استخدام هذه الوسائل، فقد أصبحت من أكثر وسائل الإنترنت شيوعاً واستخداماً في الوقت الحالي. ولعل من المسائل الهامة التي تتعلق بالمراسلات الإلكترونية وجوب المحافظة على سريتها، وهو ما جعل المبتكرين لهذه

(١) الخليفة، هند سليمان. (٢٠٠٧). الحاسب الجنائي في الدول الغربية: دراسة استطلاعية. دراسة مقدمة لمؤتمر تقنية المعلومات والأمن الوطني المنعقد بالرياض خلال الفترة من ١ - ٤ ديسمبر ٢٠٠٧، ص ٤٤.
(٢) جاد، نبيل عبد المنعم. (٢٠٠٥). جرائم الحاسب الآلي. ندوة المواجهة الأمنية للجرائم المعلوماتية، مرجع سابق، ص ١٤٣.

البرامج يقومون ببرامج تشفير خاصة به بحيث لا يمكن الإطلاع على أي رسالة إلا لمن يعرف هذه الشفرة، ويمكن حفظ البريد الإلكتروني في صناديق بريد خاصة أو في ملف، أو نسخ الرسالة والاحتفاظ بها. ولقد ساعد ظهور التوقيع الإلكتروني في تسهيل عملية التراسل عبر البريد الإلكتروني، فالبرنامج يقوم بتخزين توقيع المستخدم كرمز أو شفرة ويضعه تلقائياً على كل رسالة، ويعتبر هذا التوقيع بمثابة شهادة من قبل مرسل الرسالة بمسؤوليته عن كل ما تتضمنه الرسالة^(١).

ولذلك فإذا كان مفهوم المستندات قد تغير اليوم فقد حلت المستندات الرقمية محل الكثير من الوثائق المطبوعة على الورق، فإن الرسائل الإلكترونية تعد مستندات، أو إقرار لصاحبها بما فيها، فالمستند أصبح مفهومه الذي يتفق مع ثورة الاتصالات عن بعد كل أسلوب به تحدد فكرة معينة أو تعبير محدد من خلال كتابة ورقية أو كتابة إلكترونية، ولذلك يمكن اعتباره بمثابة إقرار إلكتروني، فالعالم يعيش اليوم عصر الثورة الرقمية، حيث صارت الكلمة والصوت والأشعة والصورة والمعلومات رقمية، حتى ليكن القول أنه قد صار للأرقام هيمنة كونية. ومن خلال ذلك فقد تم الاعتراف في الكثير من التشريعات بالإقرار للمستندات الإلكترونية بحجيتها في الإثبات وأنها تصلح لأن تكون محلاً يقع عليه التزوير. فإذا كان محتوى المحرر قد أصبح يعبر عنه بلغة رقمية، فإن هذه اللغة هي التي حلت محل الكتابة، ومن ثم يصلح هذا المحرر الرقمي لتقوم به جريمة التزوير. فالمستند الإلكتروني طالما عبر عن فكرة وكان في الإمكان قراءته وإدراك معناه وفهم مضمونه فإنه يعد محرراً وإقراراً بما فيه. ومن ثم فإنه يحوز الحجية وفقاً لطبيعة الشخص المنسوب إليه إصداره ولمن وضع عليه توقيعه الإلكتروني^(٢).

- شروط قبول الشهادة كأدلة إثبات في الجريمة الإلكترونية:

إذا كانت الشهادة على الجريمة الإلكترونية قد توجس منها القضاء خيفة من عدم تعبيرها عن الحقيقة نظراً لما يمكن أن تخضع له من معلومات مزيفة أو محرفة، فإن ذلك

(١) درويش، عبد الكريم أبو الفتوح. (٢٠٠٣). الإدارة الإستراتيجية لمكافحة الجرائم المستحدثة. الإمارات العربية المتحدة، شرطة دبي، ص ٣٤.

(٢) السعيد، كامل. (١٩٩٣). جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة من ٢٥-٢٨ أكتوبر، ١٩٩٣، القاهرة، ص ٤٣.

قد تطلب وجوب توافر مجموعة من الشروط التي قد تضيف عليها المصادقية ومن ثم اقترابها نحو الحقيقة وقبولها كأدلة إثبات في المواد الجنائية. ولذلك فإنه لقبول الشهادة كأساس تشيد عليه الحقيقة في الدعوى الجنائية المتعلقة بالجريمة الإلكترونية سواء أكان الحكم الصادر فيها بالإدانة أم بالبراءة فإنه يلزم أن تتوافر فيها الشروط الآتية:

(١) يجب أن تكون الشهادة بمثابة دليل يقيني:

وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات، فلا محل لدحض مبدأ أن الأصل في الإنسان البراءة بالنسبة لهذه الأدلة إلا بتعيين مثله أو أقوى منه، وهذا يقين، ويترتب على ذلك أن كافة مخرجات الوسائل الإلكترونية من مخرجات ورقية أو إلكترونية أو أقراص مغناطيسية أو مصغرات فيلمية تخضع لتقدير القاضي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال، ولا يعتمد على أن هذه العوامل المتحصلة يمكن اعتبارها بمثابة شهادة بل يجب أن يتم التعامل معها بمثابة أدلة يقينية تساعد في توضيح الحقيقة. والقاضي يمكنه أن يصل إلى يقينية الشهادة عن طريق: المعرفة الحسية التي تدركها الحواس من خلال معاينته لهذه المخرجات وفحصها، وعن طريق المعرفة العقلية عن طريق ما يقوم به من استقراء واستنتاج ليصل إلى الحقيقة التي يهدف إليها ويحبب أن يصدر حكمه استناداً إليها^(١).

(٢) يتعين مناقشة الشاهد كدليل على الجريمة الإلكترونية تطبيقاً لمبدأ شفوية المرافعة:

فإذا كانت الشهادة تعد أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم، وقد تكون أدلة الشاهد المتعلقة بالجريمة الإلكترونية أدلة مطبوعة أو بيانات معروضة على شاشة الحاسب، أو بيانات مدرجة في حاملات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، تكون محلاً للمناقشة عند الاعتماد عليها كأدلة أمام المحكمة. فإذا كان القاضي يحكم باقتناعه

(١) الخليفة، هند سليمان. (٢٠٠٧). الحاسب الجنائي في الدول الغربية: دراسة استطلاعية. مرجع سابق، ص ٦٢.

هو وليس باقتناع غيره، فإنه يجب عليه أن يعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يتمكن من تكوين اقتناع بقرينه نحو الحقيقة الواقعية التي يصبو إليها كل قاض عادل ومجتهد. ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الإلكترونية استناداً إلى علم شخصي له، أو استناداً إلى رأي للغير، إلا إذا كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث إن الاقتناع الذي يكون قد أصدر حكمه بناء عليه يكون متولداً من عقيدته هو وليس من تقرير الخبير. ولقد ذهب جمهور الفقه الإسلامي إلى أن القاضي لا يجوز له أن يقضي بعلمه الشخصي، لأنه لا يجوز له أن يكون شاهداً في القضية التي يحكم فيها^(١).

٣) مشروعية الدليل الجنائي بالنسبة للشهادة:

من المقرر أن الإدانة في أي جريمة تبنى على دليل أخلاقي، وهذا يتطلب أن تكون الأدلة مشروعة أي أن الحصول عليها يكون قد تم وفق قواعد الأخلاق والنزاهة واحترام القانون، فمبدأ مشروعية الدليل الجنائي بالنسبة للشهادة والإقرار على الجريمة الإلكترونية يتطلب ضرورة اتفاق إجراءات الحصول على الشهادة كأدلة إثبات للجريمة، بما يتفق والقواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر. فمشروعية الشهادة تتطلب الصدق في مضمونها، وأن يكون هذا المضمون قد تم توضيحه بطرق مشروعة وتدل على الأمانة والنزاهة من حيث طرق الحصول عليه.

ويجب التحوط بالنسبة لشرط شرعية أدلة الشهادة لأن هذه الأدلة قد تحتوي على حقيقة علمية تخالف الحقيقة القضائية التي تتطلب لقبول هذه الحقيقة العلمية أن يكون الوصول إليها قد تم بطرق مشروعة. ومن أمثلة الطرق غير المشروعة التي قد يتم من خلالها الحصول على أدلة تتعلق بالشهادة على أية جريمة إلكترونية، استخدام التعذيب أو الإكراه المادي أو المعنوي في مواجهة الجاني الذي يرتكب جريمة إلكترونية لكي يفك شفرة أو يبوح بكلمة السر، أو يقر بارتكاب جريمة إلكترونية. ويعد من قبيل هذه الطرق

(١) السعيد، كامل. (١٩٩٣). جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. مرجع سابق، ص ٥٩.

غير المشروعة أيضاً، استخدام التدليس أو الغش أو الخديعة في الحصول على أدلة الشهادة المتحصلة من الوسائل الإلكترونية^(١).

ثانياً: إثبات الجريمة الإلكترونية بالإقرار:

- مفهوم الإقرار:

لم يستقر الفقه القانوني على رأي واحد في تحديد معنى الإقرار في المفهوم الاصطلاحي، فقد عرفه البعض بأنه "إقرار المتهم على نفسه بارتكاب الوقائع المكونة للجريمة كلها أو بعضها من خلال إقرار المتهم بكل أو بعض الوقائع المنسوبة إليه^(٢).

وهناك من وضع تعريفاً يشمل شروط صحة الإقرار قائلاً بأن الإقرار القانوني يعني الإقرار على النفس بحرية وإدراك بارتكاب الأفعال المكونة للجريمة أو بعضها دون تأثير وإكراه وإن إقرار المدعى بارتكابه وقائع الجريمة كلها أو بعضها وأنه هو الذي قام بهذا الفعل بنفسه وهذا ما أقره الفقه والقضاء. ويتضح بذلك أن الاعتراف في جوهره تقرير أو إعلان وأن موضوعه هو الواقعة سبب الدعوى ونسبة هذه الواقعة إلى المتهم وأنه يتعين أن يكون من صدر الإقرار عنه هو نفسه من تتسبب إليه الواقعة بما يترتب عليه من قيام المسؤولية الجنائية عنها ويعني ذلك أن المتهم هو المقر وهو نفسه الذي تتسبب إليه الواقعة موضوع الإقرار^(٣).

ومن خلال ما سبق، يمكن القول أن الإقرار يقصد به إقرار المرء على نفسه فيما نسب إليه وقد عرف بسيد الأدلة في المواد الجزائية. ولا يؤثر في الإقرار أن يرد مجملاً إذا لا يشترط أن يكون مفصلاً شاملاً كافة ظروف الجريمة ودوافعها والعوامل التي أثرت في تكوينها فإذا جاء الاعتراف مجملاً فإنه يكون صحيحاً طالماً كان دالاً على ارتكاب الجريمة.

- أشكال الإقرار وأنواعه:

-
- (١) درويش، عبد الكريم أبو الفتوح. (٢٠٠٣). الإدارة الإستراتيجية لمكافحة الجرائم المستحدثة. مرجع سابق، ص ٥٢-٥٣.
- (٢) الصغير، جميل عبد الباقي. (١٩٩٢). القانون الجنائي والتكنولوجيا الحديثة. القاهرة، دار النهضة العربية، ص ٩١.
- (٣) شمس الدين، أشرف توفيق. (٢٠٠٦). الحماية الجنائية للمستند الإلكتروني "دراسة مقارنة". القاهرة، دار النهضة العربية، الطبعة الأولى، ص ٦٦.

(١) أشكال الإقرار:

إقرار المتهم إما أن يكون شفهياً وإما أن يكون مكتوباً وأي منهما كاف في الإثبات، ومن خلال ذلك يمكن توضيح أشكال الإقرار كما يلي^(١):

- **الإقرار الشفوي:** يمكن أن يثبت بواسطة كاتب التحقيق أو كاتب الجلسة ولا يلزم أن يكون الإقرار المثبت بمحضر التحقيق موقعاً عليه من المتهم طالما أن المحضر قد وقع عليه المحقق أو الكاتب. ولكن الإقرار الشفهي يعتبر أقل قيمة من الإقرار المكتوب فكثير من المعترفين ينكرون اعترافاتهم الشفهية ويدعون أنهم أجبروا عليها باستعمال العنف معهم أو التهديدات والوعود.

- **الإقرار المكتوب:** لا يتطلب أن يكون له شكل معين فقد يكون مكتوباً على الآلة الكاتبة أو باليد أو في صورة حديث مسترسل أو في شكل أسئلة وأجوبة. وقد نصت بعض التشريعات على أنه يجب لكي يقبل الإقرار في الإثبات أن يكون مكتوباً وموقعاً عليه من المتهم. وعلى أية حال فإن الإقرار سواء كان شفوياً أو مكتوباً فأمره متروك لتقدير القاضي وإقناعه به.

(٢) أنواع الإقرار:

يمكن تقسيم الإقرار إلى عدة أنواع، وهي كما يلي:

■ الإقرار القضائي:

وهو الإقرار الذي يصدر أمام المحكمة التي تنظر الدعوى الجزائية بالفعل ويجيز هذا الإقرار للمحكمة الاكتفاء به والحكم على المتهم بغير سماع الشهود فيبدأ التحقيق في الجلسة بالمناداة على الخصوم والشهود ويسأل المتهم عن اسمه ولقبه وسنه ثم يسأل المتهم عما إذا كان معترفاً بارتكاب الفعل المسند إليه فإن أقر جاز للمحكمة الاكتفاء باعترافه والحكم بغير سماع الشهود وإلا فتسمع شهادة شهود الإثبات^(٢).

■ الإقرار غير القضائي:

(١) السرحاني، محمد نصير. (٢٠٠٤). مهارات التحقيق الجنائي الفني في جرام الحاسب الآلي والإنترنت. مرجع سابق، ص ٧٥.

(٢) عرب، يونس. (٢٠٠٢). جرائم الحاسب الآلي والإنترنت. منشورات اتحاد المصارف العربية، مرجع سابق، ص ٣٠٤.

وهو الإقرار الذي يصدر خارج المحكمة التي تنتظر الدعوى الجزائية فإذا صدر الإقرار الجزائي في تحقيق النيابة أو أمام إحدى جهات التحقيق أو قضاء الإحالة أو في محضر جمع الاستدلالات يعتبر اعترافاً غير قضائي. كما يعتبر إقراراً غير قضائي الإقرار الذي يرد ذكره في التحقيقات نقلاً عن أقوال منسوبة إلى المتهم خارج مجلس القضاء. ويعتبر الإقرار غير قضائي مثل ما يقر به في تحقيق إداري أو كمن يقر بارتكاب الجريمة أمام أحد الأشخاص ويشهد ذلك الشخص بالتحقيق بالإقرار الذي سمعه. على أنه طبقاً لمبدأ حرية القاضي في تكوين اعتقاده فإن القاضي الجزائي حر في تقدير قيمة الاعتراف قضائياً كان أو غير قضائي وليس هناك ما يمنع من أن يكون الإقرار الغير قضائي سبباً في الإدانة لأنه لا يخرج عن كونه دليلاً في الدعوى، ويخضع لتقدير القاضي كباقي الأدلة وكل ما في الأمر أن الإقرار الغير قضائي لا يصلح أن يكون سبباً في اكتفاء المحكمة به والحكم على المتهم بغير سماع شهود^(١).

المبحث الثاني

إثبات الجريمة الإلكترونية بالخبرة الفنية (الأدلة الرقمية والقرائن)

أولاً: ماهية الخبرة:

الخبرة هي إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكان استخلاص الدليل الرقمي منه، أو هي الاستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدة فنية أو إدارية لا تتوفر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته^(٢). والخبرة كدليل في الإثبات تنصرف إلى رأي الخبير الذي يثبتته في تقريره، وبما أن تقرير الخبير، يعتبر من

(١) الصغير، جميل عبد الباقي. (١٩٩٢). القانون الجنائي والتكنولوجيا الحديثة. مرجع سابق، ص ٩٧.
(٢) سلامة، مأمون محمد. (٢٠٠١). الإجراءات الجنائية في التشريع المصري. القاهرة، دار النهضة العربية، ص ٦٤٥.

الأدلة الفنية فإن إجراء ندب الخبير هو من إجراءات جمع الأدلة، فللمحقق الاستعانة بالخبراء ليستطلع رأيهم في بعض الأمور التي تعرض له أثناء تأدية مهمته في التحقيق الذي ينتهي بإصدار قرار بأن لا وجه لإقامة الدعوى أو بإحالتها إلى محكمة الموضوع، وأما الخبرة في مرحلة المحاكمة فإنها تساعد القاضي في تكوين عقيدته للفصل في القضية^(١).

تعريف الخبير:

الخبير هو كل شخص له دراية خاصة بمسألة من المسائل، وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه فيمكنه أن يستشير فيها خبيراً كما هو الحال في تقرير الصفة التشريحية في جرائم القتل أو فحص لخطوط الكتابة المدعى بتزويرها، وتقوم الخبرة في العصر الراهن بدور بارز في عملية الإثبات القضائي نظراً لما شهدته هذا العصر من تطور علمي وتكنولوجي، لحد وصفه بعصر المعلومات^(٢).

(١) فرغلي، عبد الناصر محمد، والمسماري محمد عبيد. (٢٠٠٧). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مرجع سابق، ص ٢٤.
(٢) المرجع السابق، ص ٢٤.

ثانياً: الخبرة الفنية في الشريعة الإسلامية:

تقتضي طبيعة الحياة وتطورها الاستعانة بأشخاص ليسوا من فقهاء الشريعة والقانون، من أجل الوقوف على حقيقة الأمر المطروح، كي يتم الفصل فيه، فالأشخاص الذي يتم الاستعانة بهم في معرض حسم النزاعات والخصومات هم أشخاص متخصصون في معارف وعلوم متعددة، يطلق عليهم الخبراء، فالمحقق منذ القدم، يستعين بأهل الخبرة والاختصاص لأداء مهمته في الفصل في الجرائم المعروضة عليه، لما لهذه الوسيلة من أهمية كبرى في إنارة وتوضيح موضوع الجريمة من النواحي المتصلة بفن من الفنون أو علم من العلوم، مما لا يتاح للمحقق معرفته والوقوف على دقائقه دون الاستعانة بأهل الخبرة والاختصاص، وتزداد أهمية الاستعانة بالخبرة الفنية مع التطور العلمي والتقني، وعند الاستعانة بالخبرة الفنية يجب تطبيق جميع الشروط والأحكام المتعلقة بالخبرة، ولا تحد أهمية الخبرة من سلطة المحقق التقديرية في الأخذ بها في حكمه أو رفضها، وذلك وفق ضوابط وشروط محددة^(١).

ومن خلال ذلك فقد وضعت الشريعة الإسلامية قواعد كلية في مجال المعاملات وأنظمة التحقيق والإدارة، وتتسم تلك القواعد بالمرونة بحيث تصبح صالحة لكل مكان وزمان، فقد أكدت الشريعة الإسلامية فكرة الاستعانة بالخبرة باعتبارها نوعاً من أنواع الشهادة أو الاستشارة، وذلك بقوله تعالى [ولا ينبئك مثل خبير]^(٢)، وقوله تعالى [فاسألوا أهل الذكر إن كنتم لا تعلمون]^(٣)، أي أن الشريعة الإسلامية أباحت الاستعانة بأهل الخبرة، وذلك لتحديد كيفية الوصول إلى الحقيقة^(٤).

وقد عرف في التاريخ الإسلامي من أهل الخبرة ما يسمى (بالخارص)، والخارص هو من يقوم بتقدير وتقويم الثمار والغلال التي لا تزال على الشجر أو في الأرض لمعرفة مقدار الزكاة التي تفرض عليها، وكان النبي صلى الله عليه وسلم، يرسل عبد الله بن رواحه إلى

(١) واصل محمد، والهاللي حسين بن علي. الخبرة الفنية أمام القضاء "دراسة مقارنة". عمان، المكتب الفني بالمحكمة العليا بوزارة العدل، ٢٠٠٤، ص ٩-١٠.

(٢) سورة فاطر، الآية ١٤.

(٣) سورة النحل، الآية ٤٣.

(٤) واصل محمد، والهاللي حسين بن علي. الخبرة الفنية أمام القضاء "دراسة مقارنة"، مرجع سابق، ص ١٤.

يهود خبير كي يحرص عليهم النخل لتقدير الجزية، كما عرف في الإسلام ما كان سائداً عند العرب في الجاهلية من الخبرة بما يسمى بالقيافة، والقيافة تعني إلحاق الولد بأصوله لوجود الشبه، وقد اعتبرت الشريعة الإسلامية الخبرة نوعاً من أنواع الشهادة، حيث إن المسائل التي كانت تعرض على المحقق المسلم، من خلال المنازعات القائمة بين الأفراد، لم تكن تتطوي على تقنية عالية مركبة ومعقدة، بل كانت في معظمها مسائل بسيطة يستطيع المحقق بفطنته وجزارة علمه الإحاطة بها، ومن ثم تطبيق الأحكام العادلة بشأنها^(١).

وهكذا نخلص القول أن التشريع الإسلامي والفقهاء الإسلامي لم يبحثوا في الخبرة الفنية كمسألة تفصيلية، بل تركوا أمر اللجوء إليها إلى فطنة وحكم المحقق المسلم في ظل ظروف كل قضية على حدة.

ثالثاً: أهمية الاستعانة بالخبراء:

تكمن أهمية الخبرة في أنها تثير الطريق للقاضي الذي يهتدي به لتحقيق العدالة لا سيما في المجال الجنائي، لذا فقد اهتمت القوانين المختلفة بأهمية الاستعانة بالخبراء، ولم يحظر أحد من القانونيين على المحاكم أن تستعين بالخبراء وبالتالي فإنه يجوز دائماً للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم، ولكن إذا كان الطلب مقدماً من أحد الخصوم لا يجوز رفضه إلا إذا كان عديم الفائدة، وذلك لتعلق الأمر بحق المتهم في الدفاع، وكون تعيين الخبير هو طريق من طرق الإثبات المباحة للخصوم، ولا يجوز حرمانهم من الانتفاع به لتأييد طلباتهم. وإذا كان للخبرة تلك الأهمية في الجرائم التقليدية فإن أهميتها تزداد وتصبح ضرورية بل وحتمية في إثبات الجرائم الإلكترونية فالخبرة وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية، وهي بحث لمسائل مادية أو فنية يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات، ومنذ ظهور الجريمة الإلكترونية تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، وذلك بغرض كشف غموض الجريمة، أو تجميع أدلتها

(١) الخطيب، الشرييني. مغني المحتاج إلى معرفة معاني ألفاظ المنهاج. بيروت، دار العلم للملايين، ١٤٢٥هـ، المجلد الرابع، ص ٤٨٨

والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق^(١).

وبلاحظ أن نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرهوناً بكفاءة وتخصص هؤلاء الخبراء، ويجوز للمحقق الاستعانة بالخبراء وتحليفهم اليمين إذا خيف ألا يستطيع فيما بعد سماع شهادتهم بيمين. وأهمية الاستعانة بالخبير في مجال الجرائم الإلكترونية تظهر عند غيابه، فقد تعجز الشرطة عن كشف غموض الجريمة، وقد تعجز هي أو جهة التحقيق عن جمع الأدلة حول الجريمة، وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه^(٢).

رابعاً: دور الخبرة الفنية في عملية استخلاص أدلة إثبات الجريمة الإلكترونية:

تعد عملية الحصول على الأدلة الرقمية أمر صعب الوصول إليه لما تتطلبه من خبرة ومهارة كبيرة في مجال الحاسب الآلي؛ ويرجع ذلك لتعدد صور وأشكال الجرائم الإلكترونية، ما بين مهاجمة المعلومات بغرض تدميرها أو الاستيلاء عليها أو قد يكون المقصود بالهجوم هو الأجهزة كنشر فيروس يعمل على إتلاف وحداته الرئيسية مثلاً، أو قد يكون الأمر مجرد اختراق لكلمة مرور خاصة ببنك أو مؤسسة كبرى بغرض الاحتيال والحصول على الأموال، وقد تكون لمجرد إثبات الذات وإظهار المقدرة العالية في مجال الحاسب الآلي^(٣)، ولما كانت عملية تجميع الأدلة الرقمية الجنائية في الجرائم الإلكترونية أو الرقمية، تعد من أهم وأصعب الأمور التي تواجه عملية الإثبات الجنائي، لذا كان لزاماً أن يتم اللجوء إلى خبير قضائي معلوماتي، متخصص، لاشتقاق الدليل العلمي الفني الجنائي. ويرى بعض

(١) حمودة، علي محمود. (٢٠٠٣). الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي. بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية - مركز البحوث والدراسات أكاديمية شرطة دبي - محور القانون الجنائي في الفترة من ٢٦ - ٢٨ أبريل ٢٠٠٣، ص ٢٨٥.

(٢) فرغلي، عبد الناصر محمد، والمسماري محمد عبيد. (٢٠٠٧). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مرجع سابق، ص ٢٥.

(٣) فرغلي، عبد الناصر محمد، والمسماري محمد عبيد. (٢٠٠٧). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مرجع سابق، ص ٣٤.

المتخصصين أن عملية تجميع الأدلة الرقمية في الجرائم الرقمية التي تتم عبر الشبكة العالمية (الإنترنت) تتم عبر ثلاثة مراحل^(١):

المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة حيث تتبع الحاسبات الخوادم التي دخل المجرم منها ومحاولة إيجاد أي أثر له.

المرحلة الثانية: مرحلة المراقبة: فهناك فرضية بأن المجرم لابد أن يعود أو يحوم حول مسرح جريمته. وتتعدد طرق مراقبة هذه الحواسيب، ويمكن توضيح هذه الطرق كما يلي:

- استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع.

- استخدام أجزاء توضع في الحاسب الآلي لمراقبته.

- استخدام كاميرات مراقبة لشاشة الحاسب الآلي المعدة للاستخدام التجاري، وأبسط الطرق لمراقبة الحاسب هي الدخول لمكان وجوده.

- وهناك وسيلة أخرى وهي أصعب قليلاً وهي زرع فيروس كمبيوتر أو دودة من نوع حصان طروادة وهذه الوسيلة لها ميزة أنها تستطيع مراقبة كأثر من جهاز واحد ولكن يجب عدم السماح للفيروس بالانتشار وإلا سوف يصبح هدفاً لبرامج الدفاع ضد الفيروسات.

المرحلة الثالثة: ضبط الأجهزة المشتبه فيها وفحصها فحصاً فنياً وشرعياً. حيث يبدأ في هذه المرحلة عمل الخبير المعلوماتي في فحص النظام الحاسوبي المشتبه فيه بمكوناته المادية ومكوناته البرمجية، سعياً لاشتقاق الدليل الرقمي لتقديمه لجهة التحقيق أو الحكم، لتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه، ولتقرير إدانة المتهم، أو تأكيد براءته، ويتم ذلك وفق القواعد الفنية المتعارف عليها والمتبعة في مجال الخبرة المعلوماتية، مع مراعاة القواعد القانونية لمبدأ المشروعية.

ومن خلال ما سبق، يمكن إيجاز خطوات اشتقاق الدليل بمعرفة الخبير المعلوماتي، من أجل إثبات الجريمة الإلكترونية كما يلي^(١):

(١) البشري، محمد أمين. (٢٠٠٠). التحقيق في جرائم الحاسب الآلي. مؤتمر القانون والحاسب الآلي والإنترنت المنعقد في الفترة من ١ - ٣ مايو ٢٠٠٠، الإمارات العربية المتحدة، العين، كلية الشريعة والقانون، ص ٢٤٣.

(١) التأكد من مطابقة محتويات إحرار المضبوطات لما هو مدون عليها، مع التأكد من صلاحية وحدات النظام للتشغيل وتسجيل بيانات وحدات المكونات المضبوطة، كالنوع والطراز أو الموديل، والرقم المسلسل.

(٢) استكمال تسجيل باقي بيانات الوحدات من خلال قراءات الجهاز.

(٣) عمل نسخة أو نسخ مطابقة للأصل من كل وسائط التخزين المضبوطة، وعلى رأسها القرص الصلب، ويفضل البدء بذلك، لإجراء عملية الفحص المبدئي عل هذه النسخ لحماية الأصل من أي فقد، أو تلف أو تدمير، سواء من سوء الاستخدام، أو لوجود فيروسات، أو أفخاخ وشارك، قنابل برمجية.

(٤) تحديد أنواع وأسماء المجموعات البرمجية، برامج النظام (برامج التشغيل)، وبرامج التطبيقات، وبرامج الاتصالات، وما إذا كان هناك برامج معينة ذات دلالة بموضوع الجريمة، برامج إنشاء ومعالجة الصور في جرائم التزييف والتزوير، والمونتاج.

(٥) تحديد ما إذا كان هناك برامج أو ملفات، أو بيانات، أو معلومات، ذات دلالة ترابطية بموضوع الجريمة، كصور للعلامات، وصور للعلامات المائية وشريط الضمان، والأرقام المسلسلة في جرائم تزييف العملة، أو للمستندات والتوقيعات، وبصمات الأختام وبصمات الأصابع بجرائم التزوير، ووجود رسائل التهديد في صندوق الصادر في البريد الإلكتروني، في جريمة القتل أو التهديد بالقتل، وغير ذلك.

(٦) إظهار الملفات المخبأة، والنصوص المخفية داخل الصور.

(٧) تحويل الدليل الرقمي إلى هيئة مادية وذلك عن طريق طباعة الملفات، أو تصوير محتواها إذا كانت صور أو نصوص، أو وضعها في أي وعاء آخر حسب نوع البيانات والمعلومات المكونة للدليل.

ونذب الخبير من سلطات المحقق فليس في القانون ما يلزمه بالاستجابة للمتهم ولا لغيره من الخصوم إذا طلبوا ندب الخبير، ويحدد المحقق للخبير مهمته والميعاد الذي يقدم

(١) عبد المطلب، ممدوح عبد الحميد. (٢٠٠٦). البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت. مصر، دار الكتب القانونية، ص ٩٢-٩٣.

فيه تقريره، والأصل أن يباشر الخبير عمله في حضور المحقق وتحت إشرافه والاستثناء أن يتم ذلك في غيابه، وللخصوم حق الحضور أثناء عمل الخبير ويجوز مع ذلك أن يباشر الخبير عمله في غياب الخصوم وأن يمنعهم كذلك من الحضور إذا كان للمنع سبب، ويعد الحصول على المستندات خلال عملية التفتيش أمراً سهلاً حيث يمكن التعرف عليها بالرؤية ولن يحتاج المحقق لأي مساعدة من قبل الخبراء وهذه المستندات مثل أدلة عمل النظام، سجلات إدارة الكمبيوتر، وثائق البرامج^(١).

ومن خلال توضيح دور الخبرة الفنية في إثبات الجريمة الإلكترونية، فإن البحث عن المعلومات داخل جهاز الكمبيوتر ذاته يعد أمراً بالغ التعقيد ويحتاج إلى وجود خبير. وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم الإلكترونية هي:

أ - وصف الحاسبات وأثرها: ويتضمن وصف الحاسبات وأثرها على ما يلي^(٢):

(١) تركيب الحاسبات وصناعاتها وطرارها ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها بالإضافة إلى الأجهزة الطرفية الملحقة بها وكلمات المرور أو السر ونظام التشفير.

(٢) طبيعة بيئة الحاسب أو الشبكة من حيث التنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختزانها.

(٣) الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

(٤) أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام.

ب - بعض المعلومات والتقنيات المتعلقة بالحاسبات: ويتضمن ذلك ما يلي^(٣):

(١) بيان كيف يمكن عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.

(٢) بيان كيف يمكن عند الاقتضاء نقل أدلة الإثباتات إلى أوعية ملائمة بغير أن يلحقها تلف.

(١) بصلة رياض فتح الله. (٢٠٠١). حدود الإثبات العلمي في قضايا التزييف والتزوير. القاهرة، دار نوبار للطباعة، ص ٢٨.

(٢) فرغلي، عبد الناصر محمد، والمسماري محمد عبيد. (٢٠٠٧). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مرجع سابق، ص ٢٧.

(٣) حسين، محمود عبد الله (٢٠٠٢). سرقة المعلومات المخزنة في الحاسب الآلي. مرجع سابق، ص ٣٩.

٣) كيفية تجسيد الأدلة في صورة مادية بنقلها إذا أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للمسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة.

خامساً: متطلبات أعمال الخبرة الفنية لإثبات الجرائم الإلكترونية:

تتنوع الوسائل الإلكترونية والأجهزة التي تستخدم نظم الحاسبات الآلية (الكمبيوترية) كما تتنوع شبكات الاتصال بينها، وتتميز خصائصها الفنية فتدرج تحت تخصصات فنية وعلمية دقيقة، مما يستوجب والحال كذلك أن تدقق جهات التحقيق والمحاكمة عند اختيارها للخبير، فيجب أن تتيقن أنه تتوافر لديه الإمكانيات والقدرات العلمية والفنية في مجال التخصص الدقيق للحقل الذي يطلب منه بحثه، ولا يكفي في ذلك حصول الخبير على درجة علمية معينة وإنما يجب أن تتوافر لديه أيضاً الخبرة العلمية التي تمكنه من اكتساب كفاءة فنية عالية. وبالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجرائم الإلكترونية فإنه يمكن تحديد هذه الخبرة التي تساعد في إثبات الجريمة الإلكترونية في الموضوعات الآتية^(١):

١) حصول الخبير على شهادات مهنية معتمدة ومعترف بها في مجال الخبرة المطلوبة منه.

٢) الإلمام بتركيب الحاسب وصناعته وطراره ونظم تشغيله الرئيسية والفرعية، والأجهزة الطرفية الملحقة به، وكلمات المرور وأكواد التشفير، بالإضافة إلى إتقان العمل المطلوب منه.

٣) طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

٤) قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك أي مشاكل أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.

(١) رستم، هشام فريد. (١٩٩٤). الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مصر، مكتبة الآلات الحديثة، ص ١٤٠-١٤١.

٥) التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة.

سادساً: القواعد الفنية التي تحكم صحة الأدلة الرقمية:

للدليل الجنائي الرقمي أهمية كبرى ودور أساسي في معرفة كيفية حدوث الجريمة. ولتأكيد ذلك لا بد وأن يحتوي التحقيق الجنائي الرقمي على هذا الدليل ويجب أن تكون المنشأة على استعداد وتأهب لمثل هذه الأمور غير الاعتيادية. ويجب أن يكون الأشخاص المسؤولون عن التعامل مع هذه الأمور على فهم كبير واضطلاع بالأمور التقنية وكيفية التعامل معها، وتتسم الجرائم الإلكترونية بصعوبة اكتشافها وإثباتها، فالجريمة الإلكترونية تتم في بيئة أو إطار لا علاقة له بالأوراق أو المستندات بل تتم بواسطة الحاسب الآلي أو الشبكة العالمية ويمكن للجاني عن طريق نبضات اليكترونية لا تري العبث في بيانات الحاسب الآلي أو برامجه وذلك في وقت قياسي قد يكون جزء من الثانية، وهذه البيانات التي يتم العبث بها يمكن محوها كذلك في زمن قياسي قبل أن تصل يد العدالة إليه، حيث إن عملية الضبط لا تتم سوى بمعرفة خبير فني أو متخصص^(١). ومن خلال ما تقدم يمكن توضيح القواعد الفنية التي تحكم عمل الخبير في مجال الجرائم الإلكترونية كما يلي:

١) الطرق الحديثة للوصول إلى الدليل الرقمي وتأثيرها على قوته في الإثبات الجنائي:

من المعروف أن لكل عصر سماته وخصائصه، وسمات العصر الحالي الدخول في عالم ثورة الاتصالات عن بعد وما ترتب عليه من تغيير في نمط الحياة سواء كان ذلك على مستوى الأفراد أو الحكومات، فلقد أصبح التعامل اليوم يتم عن طريق الإلكترونيات التي لا تعتمد على الأشياء المادية المحسوسة وإنما تعتمد على النبضات والذبذبات والتشفير، فحلت النقود الإلكترونية محل النقود الورقية، وحلت الشيكات ووسائل الدفع الأخرى الإلكترونية محل الشيكات ووسائل الدفع الورقية، وحلت بطاقات الائتمان الإلكترونية مكان الدفع اليدوي وحلت البنوك الإلكترونية محل البنوك التقليدية، وقل استخدام الأوراق التقليدية وأرشيدها

(١) حجازي، عبد الفتاح بيومي. (٢٠٠٥). القانون الجنائي والتزوير في جرائم الكمبيوتر والانترنت. مصر، دار الكتب القانونية، ص ٢٤.

ومستنداتها وبزغ بدلاً منها الحاسبات الآلية وما تتمتع به من مدخلات ومخرجات تتمتع بقدرات هائلة، وظهرت كذلك الحكومة الإلكترونية لكي تتعامل عن طريقها أجهزة الحكومة مع بعضها البعض، أو تتعامل الحكومة عن طريقها مع الأفراد. ولذلك فقد تطورت الطرق التي تؤدي إلى الجريمة، فلم تعد الجرائم التي ترتكب بالوسائل الإلكترونية والتي تقع على الصور المختلفة للعمليات الإلكترونية من نوع الجرائم التقليدية، وإنما قد أطلق الفقه عليها الجرائم الإلكترونية. ولا شك في أن كشف ستر هذا النوع من الجرائم الذي يرتكب بالوسائل الإلكترونية يحتاج أيضاً إلى طرق إلكترونية تتناسب مع طبيعته بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة. فتطوير الإثبات الجنائي بتطوير طرقه أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، لكي نمنع ما يمكن أن يقال من أن صعوبة هذا الإثبات قد يؤدي إلى عدم التجريم^(١).

فإذا كانت الوسائل التقليدية قد تكفي لإثبات الجرائم التقليدية، إلا أنها قد تعجز عن إثبات الجرائم التي ترتكب بالوسائل الإلكترونية، فالدليل أثر يولد أو حقيقة تتبع من الجريمة المرتكبة، ويجب لمنطقية هذا الدليل ومصادقته أن تكون طبيعية بحيث إن الحقيقة التي يعبر عنها تصل إلى القاضي من تلقاء ذاتها ولا يتعجل هذا الأخير الوصول إليها، لأنه إن فعل ذلك قبل أن تصل هذه الحقيقة إليه فإن وضوح هذا الدليل يصبح نتيجة لذلك عملية غير طبيعية زائفة وغير معبرة عن واقع الدعوى. ولذلك فإن طبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها، فدليل التزوير مثلاً يأتي من إثبات تغيير الحقيقة في المحررات التي يقع عليها، ودليل جريمة القتل العمد قد يولد من فحص الأداة التي استخدمت في القتل وطلقات الذخيرة التي استعملت فيها، ويمكن تطبيق ذلك أيضاً على أدلة إثبات الجرائم الإلكترونية، فإثبات جريمة الغش الإلكتروني أو التزوير في المحررات الإلكترونية أو

(١) البداية ذياب. (١٩٩٩). جرائم الحاسب والانترنت: الظواهر الإجرامية المستحدثة وسبل مواجهتها. مرجع سابق، ص ٧٧-٧٨.

التلاعب في الجانب المعنوي للحاسبات الآلية، يمكن أن يثبت بأدلة إلكترونية تكون ناتجة أيضاً عن الوسائل الإلكترونية^(١).

وإذا كان هناك بعض الأدلة التقليدية التي قد تصلح لإثبات الجرائم التي تقع باستخدام الوسائل الإلكترونية، إلا أنها تكون في حاجة إلى تطوير مستمر لكي يمكنها أن تتناسب مع الطبيعة الخاصة بهذه الجرائم. فالخبرة وعلى الرغم من أنها وسيلة إثبات من الوسائل التقليدية إلا أنها تصلح أيضاً لإثبات الجرائم التي ترتكب بالوسائل الإلكترونية، ولكنها تتطلب لكي تقوى على ذلك أن يكون الخبير متمتعاً بمستوى عال من العلم والمهارة الفنية التي تمكنه من أن يشق طريقه بنجاح في مجال الجرائم التي ترتكب بالوسائل الإلكترونية والتي تقع على العمليات الإلكترونية المختلفة. كذلك فإن الخبرة الفنية يمكن أن تتطور طرقها بحيث لا تقف فقط عند ضبط الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يحقق نموذجها القانوني، وإنما يمكن لهذه الطرق كذلك أن تتعامل مع الجرائم التي ترتكب بالوسائل الإلكترونية، أو التي تقع على هذه الوسائل، فيمكن تبعاً لذلك تسجيل البيانات المعالجة إلكترونياً بعد تحويلها من النبضات أو الذبذبات أو الإشارات أو الموجات الكهرومغناطيسية إلى أشياء محسوسة تسجل وتخزن على وسائل معينة، وعلى هذه الوسائل يرد دور الخبرة الفنية في إثبات الجريمة الإلكترونية^(٢).

كما أن الطبيعة الفنية للكثير من الأدلة التي تتحصل من الوسائل الإلكترونية قد يجعلها محلاً لفحص معلمي يقوم به خبراء، وهؤلاء الخبراء قد يتأثرون في عملهم بآراء شخصية لهم أو نتائج علمية قد تكون غير صحيحة، وهذا قد يترتب عليه تشويشاً في الحقيقة التي يجب أن تتمتع بها هذه الأدلة، مما قد يضلل الاقتناع الذاتي للقضاة عندما ينظرون تقارير الخبرة. فالحقيقة العلمية أو التكنولوجيا الزائفة يمكن أن تزيف الحقيقة التي تثبت من الأدلة الأخرى القائمة في الدعوى التي ينظرها القاضي وذلك إذا أثرت في اقتناعه ولم يفتن إلى زيفها، فتكون النتيجة المترتبة عليك فساد الحكم الذي سينتهي إليه. ومما قد

(١) الخليفة، هند سليمان. (٢٠٠٧). الحاسب الجنائي في الدول الغربية: دراسة استطلاعية. مرجع سابق، ص ٨٣.

(٢) درويش، عبد الكريم أبو الفتوح. (٢٠٠٣). الإدارة الإستراتيجية لمكافحة الجرائم المستحدثة. مرجع سابق، ص ٦٤.

يؤثر في صحة الدليل المتحصل من الوسائل الإلكترونية أيضا الإجراءات التي تتبع لأجل الوصول إليه، فإذا كانت هذه الإجراءات وليدة طرق غير مشروعة فإنه سيترتب عليها عدم شرعيتها ومن ثم بطلان الدليل المتحصل منها. فالإذن بتفتيش الحاسب الآلي لضبط جرائم تكون محلها الدعامات الإلكترونية للمعلومات المحفوظة به لا بد أن يصدر وفق إجراءات معينة، فإن لم تراعى هذه الإجراءات فإن الأدلة المتحصلة منها ستكون تبعا لذلك غير مشروعة^(١).

٢) تحديد مدى الترابط بين الدليل المادي والدليل الرقمي:

في هذه المرحلة يتم فحص كل من الدليل المادي المضبوط، والدليل الرقمي المستخرج من جهاز الحاسب الآلي الموجود بملفات النظام المضبوط من صور ونصوص وأصوات. وبذلك يكون تم الربط بين الدليل الرقمي والدليل المادي، مما يكسب الدليل الموثوقية، واليقينية، اللتان تؤديان إلى قبوله لدى جهة التحقيق وجهة الحكم، ويقوم بعد ذلك بإعداد تقرير بجميع خطوات وإجراءات البحث، ويرفق به في الغالب الملاحق الإيضاحية المصورة أو المسجلة، وغيرها، لاعتمادها، ثم تصديرها إلى جهة التحقيق أو جهة الحكم^(٢).

(١) السعيد، كامل. (١٩٩٣). جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. مرجع سابق، ص ٧٢-٧٣.

(٢) صالح، نائل عبد الرحمن. (٢٠٠٠). واقع جرائم الحاسوب في التشريع الأردني. بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في العين بدولة الإمارات العربية المتحدة في الفترة من ١-٣ مايو ٢٠٠٠، ص ٧١.

المبحث الثالث

معوقات إثبات الجريمة الإلكترونية

يتحدث هذا المبحث عن معوقات إثبات الجريمة الإلكترونية، فالجريمة الإلكترونية جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكاء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات، فالاستدلال عن الجرائم يشمل التحري كما يشمل كل ما يمكن جمعه من المعلومات عن الجرائم الإلكترونية، متى وصل أمرها إلى علم المحقق سواء عن طريق مشاهدتها بنفسه أو نتيجة لتلقيه بلاغ بذلك، وعلى الرغم من الجهود المبذولة في مكافحة الجريمة الإلكترونية، إلا أن هناك بعض المعوقات في إثبات الجريمة الإلكترونية، ويمكن توضيح هذه المعوقات على النحو التالي.

أولاً: معوقات متعلقة بالدليل ذاته:

في الجريمة التقليدية، فإن دليل الإثبات فيها يكون مرئياً من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب، وكذلك المادة السامة التي استعملت في القتل، أو المحرر ذاته الذي تم تزويره، أو النقود التي زيفت وأدوات تزيفها، وفي كل هذه الأمثلة يستطيع رجل الضبط أو التحقيق الجنائي رؤية الدليل المادي وملامسته بإحدى حواسه. ولكن في الجريمة الإلكترونية عن طريق الحاسب الآلي، فإن الوسيلة المستخدمة عبارة عن نبضات إلكترونية غير مرئية تتم عبر أجزاء الحاسب الآلي والشبكة، كما تتساب الكهرباء عبر الأسلاك، فهي غير مرئية، ولا يقف الأمر عند حد عدم الرؤية، لكنها غالباً مشفرة بحيث لا يمكن للإنسان قراءتها، بل تقرأها الآلة وتظهر على شاشة الحاسب الآلي، ولذلك يمكن للمجرم أن يطمس دليل جريمته طمساً كاملاً ولا يترك وراءه أي أثر، ومن ثم يتعذر إن لم يسكن مستحيلاً ملاحقته أو كشف شخصيته^(١).

(١) رستم، هشام محمد فريد. (١٩٩٢). قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص ٢٨.

وقد يكون مصدر صعوبة الدليل في أن أجهزة الحاسب الآلي، وحسب نظمها، لا يمكن فيها أن تتبع الطريق العكسي لما يخرج منها، بمعنى لو طبعت ورقة تحتوي على بيانات مخزنة من جهاز الحاسب الآلي، فلا يمكن معرفة من قام بطباعتها وغرض الطباعة إلى خلفه، وحتى لو جددت هذه الخاصية فإنه يتعين على من يقوم بالتحليل أن يكون متخصصاً وعلى مستوى عال من التدريب والتقنية في علوم الحاسب الآلي وهو ما لم يتوافر لدى رجل الأمن العادي أو المحقق العادي. ولذلك يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم، وهذا يقتضى توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم الإلكترونية، وبمعنى آخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال، للاستعانة بها في التحقيق في هذه الجرائم ويتعين عدم التدرع بالميزانيات المالية كسبب يحول دون قيام الدول بواجباتها نحو تحقيق العدالة الجنائية، وحتى يتم ذلك يرى هذا الجانب ضرورة الاستعانة بالنخبة المتخصصة في الحاسب الآلي حال تحقيق الجريمة الإلكترونية عن طريق الحاسب الآلي وذلك لضبط هذه الجرائم واكتشافها، وتقديم أدلة الإدانة فيها، وشرح هذه الأدلة وأبعادها أمام المحاكم. ونرى ذلك شرط أن يتم في إطار القانون الجنائي وخصوصاً قواعد الخبرة أمام المحاكم والتي ينظمها قانون الإجراءات الجنائية^(١).

وبعد انتحال الشخصية، وكذلك التسلل الإلكتروني من أبرز أمثلة السلوك الإجرامي في الجرائم الإلكترونية، وذلك كدليل على عدم رؤية دليل الجريمة، فكلاهما يستخدم أساليب عالية التقنية في الدخول إلى المناطق المؤمنة والمحمية إلكترونياً أو الوصول إلى مراكز الحاسب الآلي والدخول إلى قواعد المعلومات، ويكون الدخول شخصياً أو إلكترونياً، فالدخول أو التسلل الإلكتروني، يتم عن طريق قيام الجاني بتوصيل جهازه إلى جهاز آخر له حق الدخول وذلك عن طريق خط هاتفي، وعندما يفتح الجهاز المتصل بمركز المعلومات والمسموح له بذلك، نجد أن جهاز الجاني

(١) البشري، محمد الأمين. (٢٠٠٠). التحقيق في جرائم الحاسب الآلي. مرجع سابق، ص ٥٢.

يمارس نشاطه ويحصل على ذات المعلومات دون أن يراه أحد إلى أن يغلق الجهاز الأصلي صاحب الحق في الدخول، وهذه الجريمة وإن أمكن السيطرة عليها بوسائل متطورة وحراسة شخصية ومراقبة إلكترونية، فإن محاولات القراصنة والمحتالين في الجرائم الإلكترونية تتجاوز هذه الحراسات، ويتضح من خلال ما سبق، أنه عند كشف وتجميع الأدلة في الجرائم الإلكترونية عن طريق الحاسب الآلي تواجهه صعوبة بالغة سببها عدم رؤية الدليل أو عدم القدرة على استظهاره^(١).

ثانياً: معوقات ترتبط بفقدان الآثار المتعلقة بالجريمة:

تظل الجريمة الإلكترونية عن طريق الحاسب الآلي مجهولة ما لم يبلغ عنها للجهات الخاصة بالاستدلالات أو التحقيق الجنائي، والمشكلة التي تواجه أجهزة العدالة الجنائية أن هذه الجرائم لا تصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، لا تخلف آثاراً مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة، وجثة المجني عليه في القتل، واختلاس المال من المجني عليه في السرقة إلى آخره، ويرجع ذلك إلى صعوبة اكتشاف الجريمة الإلكترونية عن طريق الحاسب الآلي، ذلك أن الجهات التي تتعامل بالحاسب الآلي في معاملاتها اليومية كالشركات التجارية أو المؤسسات لا تراجع أعمالها يومياً، وحتى تلك التي تقوم بالمراجعة اليومية أو الأسبوعية أو الشهرية، قد لا تكتشف الجريمة وتبدو لها وكأنها خسائر عادية على أثر ممارسة نشاطها، وحتى في حال اكتشافها فإن بعض الجهات المجني عليها لا تقدم على الإبلاغ خوفاً من الأثر السلبي الذي ينعكس عليها من جراء هذا البلاغ^(٢).

وقد يرجع السبب في افتقاد الآثار التقليدية للجريمة الإلكترونية عن طريق الحاسب الآلي ما يلاحظ من أن هناك بعض العمليات التي يجرى إدخال بياناتها مباشرة في جهاز الحاسب الآلي دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معداً ومخزناً على جهاز الحاسب، ويتوافر أمام

(١) فرغلي، عبد الناصر محمد، والمسماري محمد عبيد. (٢٠٠٧). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مرجع سابق، ص ٢٦.

(٢) (البشري، محمد الأمين. (٢٠٠٠). التحقيق في جرائم الحاسب الآلي. مرجع سابق، ص ٢٠

المتعامل عدة اختيارات، وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد فتكتمل حلقة الأمر المطلوب تنفيذه، كما في المعاملات المالية في البنوك، أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى حيث يتم ترصيد الأشياء المخزنة أو حسابات العملاء، أو نقلها من مكان لآخر بطريقة آلية وحسب الأوامر المعطاة لجهاز الحاسب الآلي، ويمكن ارتكاب بعض أنواع الجرائم الإلكترونية كالاختلاس أو التزوير، وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب أو تعديل البرنامج المخزن في جهاز الكمبيوتر، وتكون النتيجة مخرجات على حسب متطلبات مستخدم الجهاز الذي أدخل البيانات أو عدل البرنامج دون استخدام وثائق أو مستندات ورقية، وبالتالي تفقد الجريمة آثارها التقليدية^(١).

ولذلك يتعين عند البحث عن آثار الجريمة الإلكترونية عن طريق الحاسب الآلي وأدلتها بمعرفة سلطات الاستدلال والتحقيق، أن توجه تحرياتها إلى دائرة المتعاملين في نطاق المؤسسة أو الجهة التي وقعت بها الجريمة سواء كانوا موظفين بتلك الجهة أو من المتعاملين معها، وذلك برصد حركة المعاملات الإلكترونية ومراقبة المشبوهين داخل المؤسسات وحولها^(٢).

ويتضح من خلال ذلك ضرورة حصر البحث الجنائي عن آثار الجريمة الإلكترونية عن طريق الحاسب الآلي في دائرة المهتمين والمتعاملين بجهاز الحاسب الآلي، حيث إنه يتعين تطوير ثقافة الحاسب الآلي وسط رجال الأمن، وربط تلك الثقافة بالثقافة الأمنية التقليدية بحيث يكفل للأجهزة الأمنية نجاحاً في مواكبة الظاهرة للتعامل مع الجريمة الإلكترونية وذلك من حيث القدرة على الملاحظة، ومراعاة تصرفات الأشخاص العاملين في مجال الحاسب بدقة أو المهتمين ببرامجه أو هواة صناعة

(١) حمودة، علي محمود. (٢٠٠٣). الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي. بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية - مركز البحوث والدراسات أكاديمية شرطة دبي - محور القانون الجنائي في الفترة من ٢٦ - ٢٨ أبريل ٢٠٠٣، ص ٢٨١.

(٢) جهاد، جودة حسين محمد. (٢٠٠٠). المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، دراسة مقارنة، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١ - ٢ مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون، ص ٤.

الأنظمة المعلوماتية وتقليدها، فدراسة تصرفات هؤلاء ومراقبتها، تعد مدخلاً جيداً للسيطرة الأمنية على نشاط مرتكبي الجريمة الإلكترونية عن طريق الحاسب الآلي ووسيلة لضبطها، ذلك أن الفئات التي يجب وضعها تحت المراقبة والملاحظة الدائمة هم في الغالب من المتعلمين والذين تدل مظاهرهم على الوقار والمكانة الاجتماعية المرموقة، وللتعامل مع هؤلاء يتعين الانتقال بالحس الأمني لرجل البحث الجنائي من اهتمامه بالعاطلين والمتشردين والطبقات الفقيرة إلى مراقبة طبقات اجتماعية حديثة تتسلح بالعلم والخبرة والذكاء والثقافات المتنوعة، ولن يأتي ذلك إلا إذا كان قادراً على فهم عبارات ومفردات لغة الحاسب الآلي، التي تمكنه من جمع المعلومات المناسبة ومتابعتها^(١).

وفضلاً عن رفع المستوى الثقافي لرجال الضبط في الجريمة الإلكترونية عن طريق الحاسب الآلي وأجهزة التحقيق، وربطهم بثقافة الحاسب الآلي، وذلك كوسيلة للسيطرة على آثار الجريمة الإلكترونية عن طريق الحاسب الآلي وضبط أدلتها، لأنها في النهاية ستؤول إلى الجناة بوصفها ثمرة الجريمة، وحينئذ يمكن ضبط مرتكبي الجريمة. ومن الأسباب التي تساعد في تعذر الحصول على آثار تقليدية تخلف الجريمة الإلكترونية عن طريق الحاسب الآلي أن الجاني نفسه يملك محو الأدلة التي تدينه أو تدميرها في زمن قصير جداً وحتى لو تم ضبطه فقد يرجع هذه الجريمة إلى خطأ في نظام الحاسب أو الشبكة أو الأجهزة^(٢).

ثالثاً: معوقات ترتبط بتعذر الحصول على الأدلة بالحماية الفنية:

إن الجريمة الإلكترونية عبارة عن حرب ما بين المجني عليه وهو ربما يكون فرد أو مؤسسة أو شركة وتكون هدفاً للاعتداء على نظامها المعلوماتي ومن ثم الإضرار بها، وما بين المجرم المعلوماتي أو الجناة في حال تعددهم، لذلك فإن الهيئات والجهات التي تتبنى في نشاطها نظاماً معلوماتياً لتسيير حركتها سواء كانت جهات خدمية أو أمنية أو مؤسسات اقتصادية تحاول دائماً الحفاظ على معلوماتها وبياناتها

(١) البشري، محمد الأمين. (٢٠٠٠). التحقيق في جرائم الحاسب الآلي. مرجع سابق، ص ٢١.
(٢) رستم، هشام محمد فريد. (١٩٩٢). قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص ٣٥.

عن طريق تخزين هذه البيانات والمعلومات بعيداً عن أيدي محترفي الجريمة الإلكترونية عن طريق الحاسب الآلي، ويظهر ذلك واضحاً في مجال التجارة الإلكترونية، ومنها التعاقد بطريقة الإنترنت. ولذلك تحاول الجهات المعنية بالتجارة الإلكترونية المحافظة على عمليات الدفع الإلكتروني - أي السداد بطريقة آلية - فضلاً عن تواصل المعلومات والبيانات بينها وبين الأطراف الأخرى، وكذلك حماية عملية التحويلات المالية، ويتبع في ذلك طريقتين هما استخدام أسلوب التشفير والتحقيق عن شخصية المتعاقدين. وفيما يتعلق بالشفرة فهي متفق عليها بين الطرفين، ويعرف كلاهما مفتاح هذه الشفرة لضمان عدم قراءة الرسالة إلا لمن هو مصرح له بذلك^(١).

أما التحقيق من شخصية المتعاقدين فيتم عن طريق استخدام "شفرة المفتاح العام" حيث يمكن للطرفين المتعاقدين أن يوقعا على المستندات بطريقة رقمية، ويتأكد كل طرف من توقيع الطرف الآخر باستخدام المفتاح العام للشفرة^(٢).

وعلى الرغم من قيام الجهات ذات الأنظمة المعلوماتية بحماية نظمها عن طريق الترميز والتشفير وغيرها من طرق الحماية الإلكترونية، فإن قرصنة الحاسب الآلي والعاملين في ذات المؤسسات يستطيعون اختراق هذه الأنظمة ومن ثم يجعلون حمايتها عديمة الجدوى، لا سيما لو كانوا من العاملين داخل المؤسسة، وذلك بالدخول إلى المعلومات السرية أو الأسرار التجارية بغرض بيعها أو استخدامها في مؤسسات جديدة يسعون إلى إنشائها أو يكون هدفهم فقط تغيير الأرقام والبيانات أي تخريب المعلومات، كما أن الأمور لا تقف عند هذا الحد، بل إن هؤلاء يقومون بفرض تدابير أمنية لمنع التفتيش المتوقع بحثاً عن أدلة إدانة ضدهم، وذلك كاستخدام كلمات سر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة الإطلاع على أي دليل يخلفه نشاطهم الإجرامي، الأمر الذي يعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة، حيث إنه بعد تقدم شبكة الإنترنت الدولية، لم تعد الحدود الجغرافية

(١) حجازي، سمير. (١٩٩٩). التهديدات الإجرامية للتجارة الإلكترونية. دبي، مركز البحوث والدراسات بإدارة شرطة دبي، ص ٣.
(٢) المرجع السابق، ص ٤.

عائقاً في الاختراق، بل أكثر من هذا يلجأ الجاني إلى أسلوب حماية لمنع ضبطه أو الإيقاع به، الأمر الذي يشكل تهديداً لحرمة البيانات الشخصية المخزنة، وكذلك أسرار التجارة الإلكترونية وكذلك تدابير الدفاع والأمن^(١).

والحقيقة فإن مسألة استخلاص الدليل في الجريمة الإلكترونية، وبغير الطرق التقليدية، يثير ما يسمى "بالدليل العلمي" في مسألة الإثبات الجنائي، والدليل العلمي يقصد به النتيجة التي تسفر عنها التجارب العلمية والمعملية لتعزيز دليل سبق تقديمه سواء لإثبات أو لنفي الواقعة التي يثار الشك بشأنها، وبطبيعة الحال فإن إجراء هذه التجارب والوسائل لا تكون سوى من مختص فنياً وهو بهذه المثابة لا يعدو إلا أن يكون رأياً فنياً. وهذا الدليل العلمي، يعد شكلاً استثنائياً للأدلة المقدمة في الدعوى الجنائية، ويكون طلبه بناءً على طلب القاضي أو أحد الخصوم في الدعوى. وطلب القاضي للدليل العلمي، هو من المسائل الفنية التي لا يجوز للمحكمة أن تحل نفسها فيها محل الخبير، لأنها مسألة فنية في حاجة إلى خبير فني. ومع ذلك لو كان طلب ندب الخبير من جانب الخصوم فإن المحكمة غير ملزمة بإجابة طلبهم طالما أن الواقعة قد وضحت لديها، وفي مقدورها أن تشق طريقها في المسألة المطروحة عليها^(٢).

والقاعدة العامة أن الدليل العلمي والمستفاد من الخبرة الفنية لا بد وأن يكون مشروعاً. ومع ذلك ورغم مشروعية الدليل العلمي والحاجة إليه، فإن ذلك لا يعنى سلب المحكمة حقها في أن تأخذ أو لا تأخذ بتقرير الخبير الذي ندبته، إن هي رأت لأي سبب من الأسباب ألا تأخذ بتقرير الخبير فلا يصح رميها بالتناقض، وتفسير ذلك أن الدليل العلمي يخضع لوزن وتقدير القاضي في ضوء الأدلة التي قدمت في الدعوى من خلال بحث مشروعية الأساليب التي يمكن من خلالها الحصول على هذا الدليل وإن كان هذا الدليل هو الوحيد في الدعوى فلا يمكن عده قاطعاً في الإثبات أو النفي، ومن

(١) جهاد، جودة حسين محمد. (٢٠٠٠). المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، مرجع سابق، ص ٦.

(٢) حمودة، علي محمود. (٢٠٠٣). الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي. مرجع سابق، ص ٢٨٢.

ثم يفسر الشك لمصلحة المتهم. وهناك جانباً من الفقه القانوني يرى أن الوسائل العلمية في أغلب حالاتها ليست دليلاً مستقلاً في ذاته وإنما هي قرائن يتم دراستها واستخلاص دلالتها، وهي غير مستقلة عن القرائن، ويرجع ذلك إلى أنها لا تصلح في ذاتها كدليل وحيد في الإثبات الجنائي^(١).

ولو تم التسليم بالقواعد التقليدية في الإثبات في شأن وزن الدليل العلمي في الجريمة الإلكترونية عن طريق الحاسب الآلي وعدم اعتماده وحده كدليل في الإثبات بوصفه قرينة ما لم تؤازره أدلة أخرى فسوف يؤدي ذلك إلى إفلات الجناة في هذه القضايا، كما أن عدم وجود كوادرات فنية مدربة من رجال أجهزة العدالة في شأن ضبط هذه الجرائم، فيؤدي ذلك إلى أن تقوم هذه الأجهزة بنبذ الفنيين والخبراء في مجال الحاسب الآلي لضبط هذه الجرائم، وهؤلاء الفنيين والخبراء يقومون بالمعاينة، والمشاركة في الضبط وفحص الأدوات وتحليل الأجهزة والتوصل للمعلومات ووضعها تحت يد أجهزة العدالة وتحت إشرافهم، والقول بأن عمل هؤلاء الخبراء ليس سوى قرينة يتعين أن تؤازر بأدلة أخرى^(٢).

ومن المسائل التي أثرت كذلك بمناسبة تعذر الحصول على الدليل في الجريمة الإلكترونية عن طريق الحاسب الآلي بطرق تقليدية نظراً لخصوصية هذا النوع من الجرائم، وذلك من خلال مدى سريان الحماية المعمول بها بمنع الإطلاع غير المصرح به على الأوراق المختومة أو المغلفة، لتمتد إلى نظام المعالجة الآلية للبيانات، والمحمي فنياً ضد الاختراق. ويتضح من خلال ذلك أنه يحظر على المحقق الإطلاع على الأوراق المختومة أو المغلفة في الجرائم التقليدية، وبالتالي فإنه يحظر على المحقق من الإطلاع على نظام الحماية الآلية للبيانات المخزنة والمحمي كلياً أو جزئياً ضد الإطلاع كما قدمنا، إما عن طريق التشفير أو الترميز أو بأي وسيلة فنية أخرى

(١) عبد المطلب، ممدوح عبد الحميد. (٢٠٠٦). البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت. مصر، دار الكتب القانونية، ص ٨٩.

(٢) حسين، محمود عبد الله (٢٠٠٢). سرقة المعلومات المخزنة في الحاسب الآلي. القاهرة، دار النهضة العربية، ص ٣١.

ضد الاختراق، ويرى الجانب الذي أثار هذه المسألة الرد بالإيجاب وأنه يمنع المحقق من الإطلاع وذلك لسببين^(١):

(١) أن السبب في حظر الإطلاع على الأوراق المغلفة والمغلقة، هو رغبة صاحبها في عدم إطلاع الغير المصرح بها، بدليل أنه اتخذ سبل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها، بدليل إغلاقه هذه الأوراق أو تغليفها بأي طريقة، وذات العلة تتوافر في البيانات المعالجة آلياً، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو الكود أو كلمة المرور الدخول إلى نظام هذه البيانات، وبذلك يكون صاحب ذلك النظام قد رفض مسبقاً عمليات الاطلاع غير المصرح به ما لم يكن الراغب في الاطلاع مصرحاً له عن طريق إعطائه مفتاح المرور إلى هذه البيانات وذلك لا يتوافر في حالة المحقق القائم بالتفتيش موضوع الحديث.

(٢) هناك قاعدة عامة بالنسبة للاطلاع على الأسرار التي حصنها صاحبها ضد الاطلاع غير المصرح به أيّاً كان وعاء هذه الأسرار أو البيانات والمعلومات، يستوي في ذلك أن يكون وعاءها تقليدياً كالأوراق أو الصور الضوئية أو الفوتوغرافية أو غير تقليدي عن طريق استعمال الشرائط المغنطة والأقراص المرنة، وحتى الذاكرات الداخلية للحاسبات، وشبكات المعلومات المحلية والدولية، وعليه يحظر على المحقق الإطلاع على هذه البيانات والمعلومات المخزنة سواء من تلقاء نفسه متى توافرت لديه المقدرة الفنية على ذلك، أو عن طريق آخرين من أهل الخبرة الفنية في مجال الحاسب الآلي لمساعدته في إزالة واختراق الحماية الفنية المقامة حول النظام المعلوماتي المذكور.

ويتضح من خلال ما تقدم، صحة ما يراه هذا الرأي الفقهي والذي يهدف أولاً وأخيراً إلى إيجاد مظلة حماية قانونية لنظام البيانات المعالجة آلياً والتي لا يُصرح

(١) رستم، هشام محمد فريد. (١٩٩٢). قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص ٣٦-٣٧.

للغير بالإطلاع عليها، مع محاولة إيجاد هذه الحماية في ضوء المتوافر من نصوص نظامية، ولكن قبل التسليم بصحة هذا الرأي يجب مراعاة الآتي^(١):

(١) أن المستوى الثقافي المتواضع في الوقت الحالي لأجهزة العدالة سواء تمثلت في رجال الشرطة والأمن أو جهات التحقيق أو المحاكم، يجعل مسألة الإطلاع غير المسموح به، والمثارة في هذا الفرض مجرد تصور نظري، لأن المحقق ليست لديه المقدرة الفنية أو التفتيش على عملية الدخول إلى شبكة البيانات المعالجة آلياً والإطلاع عليها، وخاصة لو كان الأمر يتصف بالسرية ومن ثم سيكون هناك احتياطات أمنية متمثلة في الأكواد السرية وعمليات التشفير والترميز.

(٢) أن عمليات الاختراق أو القرصنة الإلكترونية ليست قاصرة داخل المؤسسة أو داخل الدولة بل قد يكون المتدخل من خارج حدود الدولة، ذلك أن التكنولوجيا وثورة الاتصال قد ألغت ما يسمى بالحدود الجغرافية وأصبحت عملية الاختراق الإلكتروني تتجه لخدمة المصالح لاقتصادية بين الدول. وذلك يتطلب ضرورة تفعيل التعاون الدولي في مجال مكافحة جريمة الاعتداء على الأموال عن طريق الحاسب الآلي.

(٣) أن الآراء القانونية المعروضة في موضوع الجريمة الإلكترونية هي مجرد آراء اجتهادية، وذلك لعدم وجود قواعد عقابية تراعى الطبيعة الخاصة للجريمة الإلكترونية عن طريق الحاسب الآلي، ولذلك يتعين أن يؤخذ بعين الاعتبار وضع تشريع عقابي موضوعي وإجرائي متكامل لمواجهة هذه الجريمة يراعى مبادئ المشروعية، وفي الوقت ذاته يتحلل من القواعد التقليدية في قانون العقوبات وقانون الإجراءات الجنائية التقليدية، والتي قد تكون غالباً قاصرة عن مواجهة هذه الجريمة.

(١) فليبسون، ستيفن. (٢٠٠٠). الجريمة الإلكترونية في القرن الحادي والعشرين. ترجمة آمنة علي يوسف، دبي، مركز البحوث والدراسات بإدارة شرطة دبي، ص ٣-٤.

رابعاً: معوقات متعلقة بصعوبة الإبلاغ ونقص خبرة سلطات الاستدلال والتحقيق في الجريمة الإلكترونية:

١. عدم الرغبة في الإبلاغ عن الجريمة الإلكترونية عن طريق الحاسب الآلي:

تظل الجريمة الإلكترونية مستترة ما لم يتم الإبلاغ عنها، ومن ثم عمل الاستدلالات أو تحريك الدعوى الجنائية حسب النظام السائد، والصعوبة التي تواجهه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة العادية - كما هو الحال في الجريمة التقليدية - وذلك لصعوبة اكتشافها من قبل الأشخاص العاديين أو حتى الشركات والمؤسسات التي وقعت مجنياً عليها في هذه الجرائم، أو لأن هذه الجهات تحاول إخفاء الأثر السلبي للإبلاغ عما وقع لها وحرصاً على ثقة العملاء فلا تبلغ عن تلك الجرائم التي ارتكبت ضدها^(١).

وتدخل هذه المؤسسات في اعتباراتها أن الإبلاغ عن الجريمة الإلكترونية عن طريق الحاسب الآلي التي وقعت ضدها ربما يؤدي إلى إحاطة المجرمين علماً بنقاط الضعف في أنظمة الجهات المجني عليها، والجريمة في صورتها التقليدية تصل إلى علم سلطات الضبط عن طريق الشكوى أو الإبلاغ والتي يجب على المحقق قبولها متى وردت في شأن جريمة ويحرر بها محضراً يرسله فوراً إلى الجهة المختصة، حتى يتسنى لها مراقبة مشروعية أعمال الاستدلال، والشكوى كالبلاغ، إلا أنها توجه ضد شخص معين، وتقدم من المجني عليه أو المضرور من الجريمة، بينما البلاغ يقدم من غيرهما أو يخلو من تعيين اسم من تنسب إليه الجريمة^(٢).

ومن أجل تفعيل عملية الإبلاغ عن الجريمة الإلكترونية عن طريق الحاسب الآلي، ومن ثم المساهمة بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، طالب البعض في الولايات المتحدة الأمريكية بأن تتضمن القوانين المتعلقة بالجريمة الإلكترونية، نصوصاً تلزم موظفي الجهة المجني عليها -أياً كانت- بضرورة الإبلاغ عما يصل إلى علمهم من جرائم تتعلق بهذا المجال، وتقرير خبراء

(١) رستم، هشام محمد فريد. (١٩٩٢). قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص ٤٢.
(٢) رمضان، عمر السعيد. (١٩٩٠). مبادئ قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية، المجلد الأول، ص ٢٨٠.

على الإخلال بذلك الالتزام. إلا أنه ولدى عرض هذا الاقتراح على "لجنة خبراء مجلس أوروبا" قوبل بالرفض لسبب قانوني وهو أن المجني عليه وهو الشركة التي ارتكب في حقها جريمة الاعتداء الإلكتروني، سوف تصبح متهمة أو جانية بعد أن كانت مجنياً عليها ولذلك وردت اقتراحات بديلة قد تكون مقبولة منها الالتزام بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات، وكذلك إصدار شهادة "أمن خاصة" تمنع بعد عمل مراجعة وتدقيق من قبل هيئة خاصة من المراجعين، ويتعين على هذه الهيئة إبلاغ الشرطة بما تكتشفه من جرائم^(١).

ولذلك فإن من صعوبات الإبلاغ عن هذه الجرائم على نطاق دولي، عدم وجود شبكة دولية لتبادل المعلومات الأمنية. ولذلك فإن الشرطة الدولية (الانتربول) بدأت تهتم بمكافحة جرائم الكمبيوتر وأنشأت لديها فرقة خاصة لهذا الغرض. وتثير مسألة الإبلاغ عن الجريمة الإلكترونية عن طريق الحاسب الآلي مسائل تتعلق بمدى ما هو متاح من نصوص في الأنظمة الجزائية التي توجب الإبلاغ وترتب عقوبة على ذلك^(٢).

٢. نقص خبرة سلطات الاستدلال والتحقيق في الجريمة الإلكترونية:

ومن الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة الإلكترونية كذلك نقص الخبرة لدى المحقق، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة الإلكترونية عن طريق الحاسب الآلي وكيفية التعامل معها، وذلك على الأقل في البلدان العربية، نظراً لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخراً عن أوروبا وكندا والولايات المتحدة، وأن أجهزة العدالة المقاومة للجرائم المرتبطة بهذه التقنية تبدأ في التكوين والتشكيل عقب ظهور هذه الجرائم، وهو أمر يستغرق وقتاً أطول من وقت انتشار الجريمة لأن هذه الجريمة تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن فإن الحركة التشريعية، أو الثقافية الأمنية أو

(١) الحسيني، عمر الفاروق. (١٩٩١). تأملات في بعض صور الحماية الجنائية لنظام الحاسب الآلي. تقرير مقدم إلى الدورة التدريبية التي ينظمها اتحاد المصارف العربية في الفترة من ٧ - ٩ مايو، في الجوانب القانونية النجمة عن استخدام الحاسب الآلي في أعمال البنوك، ص ٣٢.

(٢) رمضان، عمر السعيد. (١٩٩٠). مبادئ قانون الإجراءات الجنائية. مرجع سابق، ص ٢٨٢.

القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلباً على فنية إجراء الاستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة الإلكترونية عن طريق الحاسب الآلي، ومن هنا تأتي الدعوة إلى وجوب تأهيل المختصين في جهات التحقيق والإدعاء تأهيلاً مناسباً في شأن هذه الجرائم^(١).

وهذا ما لاحظته جانب كبير من الفقه الجنائي، ذلك أن البحث والتحقيق في الجريمة الإلكترونية هي مسألة في غاية الأهمية والصعوبة، ولا سيما بالنظر لاعتبارات التكوين العلمي والتدريبي، والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي، ذلك أن حادثة هذه الجرائم وتقنياتها العالية تتطلب من القائمين على البحث الجنائي والتحقيق إلمام كاف بها، فلا يكفي أن يكون لديهم الخلفية القانونية أو أركان العمل الشرطي فقط، ولكن لا بد من الإلمام بخبرة فنية في مجال الجريمة الإلكترونية عن طريق الحاسب الآلي^(٢).

خامساً: معوقات متعلقة بصعوبة التعاون الدولي وضخامة البيانات المتعلقة بمكافحة الجريمة الإلكترونية عن طريق الحاسب الآلي:

١. صعوبات التعاون الدولي في مكافحة الجريمة الإلكترونية:

لقد كان لتقدم شبكة المعلومات الدولية (الإنترنت) مجموعة متنوعة من الاستخدامات في مجال السياحة والإعلام والثقافة والشئون العسكرية والاقتصادية والأمنية. ولذلك نادى البعض بضرورة إنشاء وحدات خاصة بمكافحة الجريمة الإلكترونية بواسطة الحاسب الآلي والإنترنت أسوة بجهات البحث الجنائي الوطنية والدولية - الإنترنتول - لإثبات الجريمة عند وقوعها وتحديد أدلتها وفاعلها، وهو ما يعنى كذلك إيجاد صيغة ملائمة للتعاون الدولي لمكافحة الجرائم الإلكترونية عن طريق الإنترنت، وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومركبيها وسبل مكافحتها. ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة الإلكترونية عن

(١) عبد المطلب، ممدوح عبد الحميد. (٢٠٠١). جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية. الشارقة، دار الحقوق، ص ١٧.

(٢) عبد المطلب، ممدوح عبد الحميد. (٢٠٠١). جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية. مرجع سابق، ص ٢٠.

طريق الحاسب الآلي، إلا أن هناك عوائق تحول دون ذلك، وتجعل هذا التعاون صعباً لما يلي^(١):

أ - عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي: ذلك أن الأنظمة القانونية في بلدان العالم لم تتفق على صور محددة يندرج في إطارها ما يسمى "بإساءة استخدام نظم المعلومات الواجب إتباعها"، كذلك ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه، وذلك نتاج طبيعي لقصور التشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي.

ب - عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة الإلكترونية بين الدول المختلفة: خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق، خاصة وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة، عن طريق الضبط أو التفتيش في نظام معلوماتي معين هو أمر غاية في الصعوبة، فضلاً عن الصعوبة الفنية في الحصول على الدليل ذاته.

ج - عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم: وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم برامج الحاسب وشبكة الإنترنت، ومن ثم تطور الجريمة الإلكترونية عن طريق الحاسب الآلي بذات السرعة على نحو يؤدي إلى إرباك المشروع في الدول، ومن ثم يظهر الأثر السلبي في التعاون الدولي، وهو ما حاولت الأمم المتحدة الاهتمام به، وكذلك بلدان أوروبا.

د - مشكلة الاختصاص في الجريمة الإلكترونية: وهي من المشكلات التي تعرقل الحصول على الدليل في الجريمة الإلكترونية عن طريق الحاسب الآلي، ذلك

(١) شاهين، إسماعيل عبد النبي. (٢٠٠٠). أمن المعلومات في الانترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١ - ٢ مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون، ص ٢٢٨-٢٢٩.

أن هذه الجرائم من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع جريمة الحاسب الآلي في مكان معين، ومن هنا تنشأ مشكلة البحث عن الأدلة الجنائية على شبكة الإنترنت، وهذا ما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدول.

٢. الصعوبات المتعلقة بضخامة البيانات المتعلقة بالجريمة:

لعل من الصعوبات الكبيرة التي تواجه رجال الضبط وسلطات التحقيق الجنائي في الجرائم الإلكترونية عن طريق الحاسب الآلي كمية المعلومات والبيانات الضخمة والتي هي في حاجة إلى فحص ودراسة كي يستخلص منها دليل هذه الجريمة، ففضلاً عن ضرورة توافر الخبرة الفنية في مجال الحاسب الآلي والمعلوماتية لدى رجل الضبط أو المحقق، يتعين كذلك أن يتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة على الحاسب الآلي أو على ديسكات أو اسطوانات منفصلة^(١).

ولذلك يمكن القول أن ضخامة هذه البيانات والمعلومات، تعد عائقاً في تحقيق الجرائم الإلكترونية عن طريق الحاسب الآلي، ذلك أن طباعة كل ما هو موجود على الدعامات الممغنطة لحاسب متوسط العمر، يتطلب مئات الآلاف من الصفحات، في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئاً مفيداً للتحقيق. وهذا عكس ضخامة أو وفرة المعلومات في الجرائم التقليدية كالقتل أو السرقة، ذلك أن وفرة المعلومات في مثل هذه الجرائم هو أمر يساعد العدالة ويساعد رجل الضبط أو المحقق -على السواء - في استخلاص الدليل الجنائي في هذه الجريمة^(٢).

ومن خلال ما سبق، وفي ظل تواضع المستوى الفني لرجل الضبط والمحقق الجنائي فيما يتعلق بفنون الحاسب الآلي واستخداماته، فإنه يكون الملائم وجوب ندب خبراء فنيين في مثل هذه الجرائم حتى يمكن فرز المعلومات التي يحتاجها التحقيق عن

(١) علي، نبيل علي. (١٩٩٤). العرب وعصر المعلومات. الكويت، عالم المعرفة، ص ٩١.
(٢) رستم، هشام محمد فريد. (١٩٩٢). قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص ٣٦.

تلك التي لا حاجة لها، وإلا دخل رجل الضبط والمحقق في دائرة مغلقة من المعلومات لن يخرج منها، وهذا يتطلب أن يكون ندب هؤلاء الخبراء وجوبياً، ومن ثم تعديل التشريعات الجنائية القائمة التي تجعل ندب خبير في الدعوى أمر جوازي للمحقق إن شاء أمر به أو رفضه؛ وذلك لأن طبيعة الجريمة تستلزم التعامل معها بطريقة حرفية أو فنية تفوق قدرات رجل الضبط أو المحقق؛ إلا إذا كان مؤهلاً لذلك، فيمكنه الاعتماد على قدراته الشخصية في ضبط وتحقيق هذه الجرائم، بشرط ألا يخرج عمله عن الأصول الفنية المتعارف عليها^(١). ولذلك يحاول الخبراء في مجال الجريمة الإلكترونية طرح حلول عملية وقانونية لمكافحة هذه الجرائم في ظل شيوع الدليل الإجرامي فيها، ويكون هدف هذه الحلول إما مساعدة الجهات المجني عليها في الحصول على حقوقها التي سلبت منها نتيجة لهذه الجريمة الإلكترونية. أو تقرير عقوبة جنائية على تلك الجهات التي تتعرض للجريمة دون أن يكون لديها وسائل حماية فنية تؤمنها^(٢).

سادساً: المعوقات التي تواجه الخبراء الفنيين في عملية الإثبات الجنائي للجريمة الإلكترونية:

يواجه الخبير الجنائي معوقات متعددة في سبيل جمع الأدلة الرقمية من أجهزة الحاسب الآلي أو الشبكات الرقمية، وعليه يجب أخذ الحذر في كل إجراء أو ملاحظة النقاط الآتية خلال أداء عمله: (٣)

(١) فقد جزء كبير من المعلومات والأوامر، التي تشكل الأدلة الرقمية حال إغلاق جهاز الحاسب الآلي بطريقة غير صحيحة، أو في حالة القطع المفاجئ للتيار الكهربائي عن الجهاز. فعند غلق أو قطع التيار الكهربائي عن جهاز الكمبيوتر فإن مثل هذا الفعل قد يؤدي إلي محو المعلومات من ذاكرة الجهاز أو العمل علي تحريف بيانات هامه و حدوث ضرر في أجهزة الكمبيوتر، أو منع نظام التشغيل من إعادة التحميل وبالتالي فقدان للأدلة الجوهرية.

(١) رستم، هشام محمد فريد. (١٩٩٢). قانون العقوبات ومخاطر تقنية المعلومات. مرجع سابق، ص ٣٧.
(٢) فليسون، ستيفن. (٢٠٠٠). الجريمة الإلكترونية في القرن الحادي والعشرين. مرجع سابق، ص ٢٢.
(٣) فرغلي، عبد الناصر محمد، والمسماري محمد عبيد. (٢٠٠٧). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مرجع سابق، ص ٣٢.

(٢) قيام الجاني بتهيئة جهاز الكمبيوتر للتفجير أو التدمير بمجرد تشغيله بالضغط على زر توصيل الطاقة.

(٣) طبيعة مسرح الجريمة، فالشبكات المنتشرة على مستوى العالم، لذا فقد لا يكون ممكناً الحصول على دليل في حالة توزيع مسرح الجريمة بين أكثر من دولة بسبب تعقيد الإجراءات أو وجود مشاكل عملية وتشريعية في بعض الدول مما يحول دون الحصول على دليل رقمي، كما أن سرعة مرور البيانات الرقمية عبر الشبكات لأقل من جزء من الثانية مع مهارة المجرمون في تدمير الأدلة أو تحريف أو تعديل البيانات لحماية أنفسهم، وكذلك حجم البيانات الضخمة التي تمر بالشبكات مما يكون لها التأثير العكسي عند البحث عن دليل إدانة أو البراءة.

(٤) إخفاء الهوية، فعند تعمد المستخدم إخفاء هويته حال استخدام الإنترنت سواء القيام ببعض الإجراءات أو استخدام بعض البرامج والتطبيقات التي تؤدي لطمس الهوية مما يشكل عائقاً أمام المحقق الجنائي أو الخبير الفني.

(٥) وجود بعض البرامج خاصة بإخفاء المعلومات أو البيانات المخفية وذلك لخلق ما يعرف بنظام غير آمن عبر استخدام الشبكة العالمية الإنترنت مما تجعل عملية استعادة الأدلة أو إعادة تركيبها في غاية الصعوبة أمام المحقق الجنائي أو الخبير، ويتضح مما تقدم فإن الحصول على الأدلة الجنائية الرقمية أمر صعب الوصول إليه لما تتطلبه من خبرة ومهارة كبيرة في مجال الكمبيوتر.

الفصل الخامس
الدراسة التطبيقية

الفصل الخامس

الدراسة التطبيقية

تمهيد:

يعتبر الجانب التطبيقي ثمرة للدراسة النظرية، حيث يوضح مدى الاهتمام بتنفيذ الأنظمة المتبعة في تحقيق العدل الذي ينشده النظام في المملكة العربية السعودية، وقد تم انتقاء عدد من القضايا، تشمل الجوانب المختلفة للدراسة، من خلال عرض نوع القضية ورقمها، وعرض وجيز للوقائع والإجراءات التي اتبعت في هذه القضايا، ثم كيفية تصرف جهة التحقيق في هذه القضايا، وتوضيح مبررات هذه العقوبة، وتحليل مضمون القضية وردها إلى الجانب النظري للدراسة، وحرص الباحث عند اختياره لهذه القضايا أن تشمل قضايا من المحاكم وهيئة التحقيق وحرص أيضاً على تنوعها من حيث نوعية الجريمة وجسامتها، وآثارها السلبية وكيفية إدانة المتهم ومبررات القاضي في الحكم وتعامل كل جهة سواء كانت تحقيقية أو قضائية لإثبات الجريمة وعقوباتها وتوافقها مع نظام الجرائم المعلوماتية، وبعد اختيار هذه القضايا، تم تحليلها كما يلي:

القضية الأولى

قضية المال رقم (٣١/٤/٤٩٥)

المسجلة جنائياً برقم (٣١/٢٠٦٠/٢٤٥٤)

الحمد لله والصلاة والسلام على رسول الله.. وبعد:

فبصفتي عضو هيئة التحقيق والادعاء العام بمحافظة جدة، أدعي على:

(أ) "البالغ من العمر (٣٥) عاماً (سعودي الجنسية) بموجب السجل المدني رقم

(×××) يقيم بمدينة جدة، مطلق السراح بالكفالة الحضورية لفة رقم (٢٢).

(بمخالفة الفقرة الثالثة من المادة الثالثة من نظام مكافحة جرائم المعلوماتية).

بالإطلاع على خطاب مدير مركز شرطة البلد رقم (١٠/١/٢٠/٧٠٦٢) وتاريخ

١٤٣١/١٢/٢١ هـ المبني على خطاب سعادة أمين محافظة جدة رقم

(٣١٠٠٢٠٢٠٨٤) وتاريخ ١٤٣١/١٠/١٦ هـ ومشفوعاته التقرير الفني ومحضر

التحفظ والتي تتضمن التحفظ على عدد أربعة أجهزة حاسب آلي تم سحبها من إدارة المتابعة بالإدارة العامة للبلديات الفرعية بسبب الاشتباه في استخدام هذه الأجهزة في أغراض اختراق أجهزة الحاسب الآلي لبعض الموظفين بالأمانة وفقدان ملفات منها بالإضافة إلى وجود حساب الموظف (أ) على هذه الأجهزة كمسئول (Administrator) ووجود سجلات تشير دخوله على بعض الأجهزة المتصلة بشبكة الأمانة وكذلك برامج غير مصرح باستخدامها بسبب تطبيقاتها كأدوات اختراق وتجسس وهذه السجلات والأدوات موجودة في عدد ثلاثة أجهزة فقط استخدمت عن طريق اسم المستخدم (××××) الموظف (أ).

- وباستجواب المدعى عليه ومواجهته بالتهمة المنسوبة إليه / أنكر التهمة الموجهة إليه وأفاد بأنه يوجد لديه جهاز حاسب آلي واحد على مكتبه يستخدمه وجهازين تحت مكتبه بطيئة لا تصلح للاستخدام وأنه لا يستخدمها ولا تعود له وليس لديه علم ببرامج التجسس الموجودة في الأجهزة ولم يقم بتثبيتها ولم يضيف اسمه كمسئول على الأجهزة وأن اسمه على الجهاز الذي يستخدمه مستخدم وليس مسئول وأنه باستطاعة أي موظف الدخول على أجهزة الحاسب الآلي بالأمان باستخدام حسابه الخاص وأن سبب وجود برنامج شؤون الموظفين على جهازه لأن لديه صلاحية من شؤون الموظفين باستخدام هذا البرنامج لتنظيم عملية الخروج من العمل.

* وبسماع أقوال كلاً من:

١- مدير قسم المتابعة بأمانة محافظة جدة أفاد بأنه لم يكن يعلم بوجود برامج الاختراق والتجسس على الأجهزة التي لدى المدعى عليه إلا من قبل تقنية المعلومات بالأمانة وأنه قد استفسر سابقاً من المدعى عليه عن ملفات من المفترض أن يرسلها عن طريق البريد الإلكتروني فذكر له بأنها موجودة على سطح مكتبه بالرغم من أن جهازه مؤمن بكلمة سر، وأنه قد شاهد المدعى عليه أثناء الواقعة يخرج الهارد ديسك من جهازه حيث ذكر له بأنه يخصه كون يوجد به ملفات مهمة لا يرغب لأحد العبث بها.

- ٢- والموظف بإدارة المتابعة / أفاد بأنه لا يعلم من قام بتثبيت برامج الاختراق والتجسس وأنه لا يعلم عنها إلا بعد الواقعة.
- ٣- مدير إدارة اللوحات الإعلانية بالأمانة أفاد بأنه لم يلاحظ أي اختراقات على جهازه أو تثبيت برامج تجسس سوى الملف المفقود والذي قام بالتبليغ عنه وأن ××××× طلب منه بأن يشاهد المدعى عليه وهو يخرج الهارد ديسك من جهازه لكنه لم يلتفت للمدعى عليه ولم يشاهده.
- ٤ - مشرف أنظمة الحاسب الآلي بأمانة محافظة جدة أفاد بأنه قام بالكشف على أجهزة الحاسب الآلي التي لدى الموظف (أ) حيث عثر بها على برامج التجسس والاختراق واستخراج كلمات المرور وبعض عناوين أجهزة شبكة الأمانة.
- ٥ - مدير الدعم الفني بتقنية المعلومات بأمانة محافظة جدة أفاد بأن المدعى عليه قام بكسر كلمة المرور الخاصة بحساب مدير النظام المحلي لجهازه ومن ثم قام بإضافة اسمه ضمن قائمة مجموعة المشرفين وأنه تم معرفة ذلك عن طريق وجود اسمه بالملف التاريخي لقائمة المشغلين بالسيرفر الخاص بالأمانة لدى تقنية المعلومات وأنه وجدت برامج اختراق وتجسس وكذلك عناوين أجهزة الحاسب الآلي بالأمانة في قائمة الملف التاريخ في برنامج التحكم عن بعد في جهاز المدعى عليه والذي يستخدمه في عمله ونوعه دليل واسمه على الجهاز مسئول وليس مستخدم أما الجهازان الآخران فهما لا يصلحان للاستخدام كونها بطيئة وكثيرة التوقف عن العمل.
- (وبالبحث عن الحالة الجنائية للمدعى عليه اتضح عدم وجود سوابق جنائية مسجلة عليه).
- وقد انتهى التحقيق إلى توجيه الاتهام لـ (أ) بمخالفة الفقرة الثالثة من المادة الثالثة من نظام مكافحة الجرائم الإلكترونية لقيامه بالدخول غير المشروع لموقع إلكتروني. وذلك للأدلة والقرائن التالية:
- ١ - ما ورد بالتقرير الفني حول التجاوزات الفنية للمدعى عليه لفة رقم (٦).

- ٢ - ما ورد بمحضر التحفظ على الأجهزة لفة رقم (٤، ٥).
 - ٣ - وجود اسم المدعى عليه ضمن قائمة مجموعة المشغلين بالرسيفر الخاص بالأمانة.
 - ٤ - ورود اسمه كمسئول على جهازه وعلى الأجهزة التي بإدارته وهذا الإجراء لا يمكن أن يتم إلا عن طريق تقنية المعلومات بالأمانة.
 - ٥ - ما ورد بأقوال مشرف أنظمة الحاسب الآلي ×××× بدفتر التحقيق لفة رقم (٢٩) صفحة (٦).
 - ٦ - ما ورد بأقوال مدير الدعم الفني بدفتر التحقيق لفة رقم (٣٧) صفحة (١، ٢، ٣، ٧).
- وحيث إن ما أقدم عليه المدعى عليه / (أ) وهو بكامل أهليته المعتبرة شرعاً فعل مجرم ومعاقب عليه نظاماً وفقاً للمادة الثالثة من نظام مكافحة جرائم المعلوماتية، لذا أطلب إثبات إدانته بما أسند إليه والحكم عليه بالعقوبة المقررة وفق المادة الثالثة من النظام ذاته.
- والله الموفق،،،

عضو هيئة التحقيق والإدعاء العام

محقق ثان/

التحليل:

بالنظر إلى هذه القضية يلاحظ أنها ترتبط بالجريمة الإلكترونية، وذلك من خلال تناولها وعرضها لتهمة الدخول غير المشروع على موقع إلكتروني، حيث أوضحت هذه القضية النشاط الإجرامي الذي تستخدم فيه التقنية الإلكترونية الرقمية بصورة مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف، ونجد من خلال النظر إلى التقرير الفني ومحضر التحفظ الخاص بهذه القضية والتي تتضمن التحفظ على عدد أربعة أجهزة حاسب آلي تم سحبها من إدارة المتابعة بالإدارة العامة للبلديات الفرعية بسبب الاشتباه في استخدام هذه الأجهزة في أغراض اختراق أجهزة الحاسب الآلي لبعض الموظفين بالأمانة وفقدان ملفات منها بالإضافة إلى وجود حساب الموظف (أ)

على هذه الأجهزة كمسئول ووجود سجلات تشير دخوله على بعض الأجهزة المتصلة بشبكة الأمانة وكذلك برامج غير مصرح باستخدامها بسبب تطبيقها كأدوات اختراق وتجسس وهذه السجلات والأدوات موجودة في عدد ثلاثة أجهزة فقط استخدمت عن طريق الموظف (أ).

ويتضح من خلال النظر إلى هذه القضية توفر الركن المادي والمعنوي للجريمة، حيث يتمثل الركن المادي لهذه الجريمة في وجود حساب الموظف (أ) على هذه الأجهزة كمسئول ووجود سجلات تشير دخوله على بعض الأجهزة المتصلة بشبكة الأمانة وكذلك برامج غير مصرح باستخدامها بسبب تطبيقها كأدوات اختراق وتجسس وهذه السجلات والأدوات موجودة في عدد ثلاثة أجهزة فقط استخدمت عن طريق الموظف (أ). وهذا ما ينطبق مع الركن المادي للجريمة الإلكترونية الذي يتطلب معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق 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، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها. وهذا ما ينطبق على هذه القضية، حيث أفاد مدير الدعم الفني أن المدعى عليه قام بكسر كلمة المرور الخاصة بحساب مدير النظام المحلي لجهازه ومن ثم قام بإضافة اسمه ضمن قائمة مجموعة المشرفين وأنه تم معرفة ذلك عن طريق وجود اسمه بالملف التاريخي لقائمة المشغلين بالسيرفر الخاص بالأمانة لدى تقنية المعلومات وأنه وجدت برامج اختراق وتجسس وكذلك عناوين أجهزة الحاسب الآلي بالأمانة في قائمة الملف التاريخي في برنامج التحكم عن بعد في جهاز المدعى عليه والذي يستخدمه في عمله ونوعه دليل واسمه على الجهاز مسئول وليس مستخدم أما الجهازان الآخران فهما لا يصلحان للاستخدام كونها بطيئة وكثيرة التوقف عن العمل ويتوافر الركن المعنوي أيضاً في هذه الجريمة، وذلك من خلال توضيح مشرف أنظمة الحاسب الآلي بأنه قام بالكشف على أجهزة الحاسب الآلي التي لدى الموظف (أ) حيث عثر بها على برامج التجسس والاختراق واستخراج كلمات المرور

وبعض عناوين أجهزة شبكة الأمانة، أي أن هناك علاقة تربط بين ماديّات الجريمة وشخصية الجاني.

وتتوفر في هذه القضية الأدلة والقرائن المختلفة التي تدل على إثبات الجريمة على المدعي عليه (أ)، وذلك من خلال ما يلي:

(١) ما ورد بالتقرير الفني حول التجاوزات الفنية للمدعي عليه، وذلك من خلال وجود اسمه بالملف التاريخي لقائمة المشغلين بالسيرفر الخاص بالأمانة لدى تقنية المعلومات وأنه وجدت برامج اختراق وتجسس وكذلك عناوين أجهزة الحاسب الآلي بالأمانة في قائمة الملف التاريخ في برنامج التحكم عن بعد في جهاز المدعى عليه.

(٢) ما ورد بمحضر التحفظ على الأجهزة، وذلك من خلال التحفظ على عدد أربعة أجهزة حاسب آلي تم سحبها من إدارة المتابعة بالإدارة العامة للبلديات الفرعية بسبب الاشتباه في استخدام هذه الأجهزة في أغراض اختراق أجهزة الحاسب الآلي لبعض الموظفين بالأمانة وفقدان ملفات منها بالإضافة إلى وجود حساب الموظف (أ) على هذه الأجهزة.

(٣) ما ورد بأقوال مشرف أنظمة الحاسب الآلي الذي أفاد بأنه قام بالكشف على أجهزة الحاسب الآلي التي لدى الموظف (أ) حيث عثر بها على برامج التجسس والاختراق واستخراج كلمات المرور وبعض عناوين أجهزة شبكة الأمانة.

(٤) ما ورد بأقوال مدير الدعم الفني الذي أفاد بأن المدعى عليه قام بكسر كلمة المرور الخاصة بحساب مدير النظام المحلي لجهازه ومن ثم قام بإضافة اسمه ضمن قائمة مجموعة المشرفين وأنه تم معرفة ذلك عن طريق وجود اسمه بالملف التاريخي لقائمة المشغلين بالسيرفر الخاص بالأمانة لدى تقنية المعلومات وأنه وجدت برامج اختراق وتجسس وكذلك عناوين أجهزة الحاسب الآلي بالأمانة في قائمة الملف التاريخ في برنامج التحكم عن بعد في جهاز المدعى عليه والذي يستخدمه في عمله ونوعه دليل واسمه على الجهاز مسئول

وليس مستخدم أما الجهازان الآخران فهما لا يصلحان للاستخدام كونها بطيئة وكثيرة التوقف عن العمل.

ونتيجة لما سبق، فقد انتهى التحقيق إلى توجيه الاتهام لـ / (أ) بمخالفة الفقرة الثالثة من المادة الثالثة من نظام مكافحة الجرائم الإلكترونية لقيامه بالدخول غير المشروع لموقع إلكتروني. ولذلك ينطبق على المتهم العقوبة التي تحددها المادة الثالثة من نظام مكافحة الجرائم الإلكترونية، حيث أوضحت أن المتهم "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو احدي هاتين العقوبتين، كل شخص يقوم بالدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه ، أو تعديله، أو شغل عنوانه.

ويتضح من خلال هذه القضية أنه لم يتم الإشارة إلى كيفية إتمام عملية تحرير الأجهزة واستخراج الأدلة والتأكد من التقيد بالضوابط الفنية الصحيحة في استخراجها وتحليلها، والحكم يبدو أنه اعتمد على أقوال المختصين من الأمانة وليس من سلطة مستقلة.

القضية الثانية

قضية المال رقم (٣٠/٤/١٨٠)

المسجلة جنائياً برقم (٣٠/١٩٠/٢٢٦٤)

الحمد لله والصلاة والسلام على من لا نبي بعده:

بصفتي عضو هيئة التحقيق والادعاء العام بدائرة محافظة جدة فإنني أدعي على / (أ)، سعودي الجنسية، مضاف بالسجل المدني لوالده رقم (×××××××) مطلق السراح بالكفالة الحضورية لفة رقم (٢).

(الوقائع)

بالإطلاع على خطاب مركز شرطة الشمالية رقم (١٤/٧٩٨٤) وتاريخ ١٤٣٠/٧/٥ هـ ومشفوعاته البلاغ المقدم من المواطن / ××× المتضمن أن المذكور قام باختراق البريد الإلكتروني العائد له عن طريق استخدام الشبكة المعلوماتية وبسماع أقوال المتهم

المذكور اعترف بقيامه باختراق البريد الإلكتروني العائد للمدعي وتغيير معلوماته وقام بإعادة البريد للمدعي وفق محضر دون بالأوراق.
جرى الإطلاع على التحقيقات الأولية المجراه مع المتهم المذكور والمدعي وتم الاكتفاء بها بموجب المحضر المعد لذلك، لفة (١٥).

(الاثهام)

وانتهى التحقيق إلى توجيه الاتهام للمتهم (أ) بارتكابه جريمة معلوماتية بأن اخترق البريد الإلكتروني للمواطن ×× عن طريق الشبكة المعلوماتية (الإنترنت) وتغيير معلوماته للأدلة والقرائن التالية:

- ١ - اعترافه بما أسند إليه المدون بدفتر التحقيق لفة (١١).
- ٢ - ما جاء بمحضر إعادة البريد الإلكتروني المخترق، لفة رقم (٧).

(الطلبات)

وحيث إن ما قام به المتهم المذكور فعل مجرم وفقاً للفقرة (١) من المادة الخامسة من نظام مكافحة جرائم المعلوماتية لذا أطلب إثبات ما نسب إليه وتعزيزه شرعاً لقاء اختراقه لبريد إلكتروني عن طريق الشبكة المعلوماتية (الإنترنت) وتغيير معلوماته استناداً للمادة (١٢٦) من نظام الإجراءات الجزائية ومجازاته شرعاً وفق ما يراه فضيلة ناظر القضية. (علماً بأن الحق الخاص لازال قائماً).
والله ولي التوفيق،،،

عضو هيئة التحقيق والادعاء العام

محقق أول

التحليل:

بالنظر إلى هذه القضية يلاحظ أنها ترتبط بالجريمة الإلكترونية، وذلك من خلال تناولها وعرضها لجريمة اختراق البريد الإلكتروني عن طريق استخدام الشبكة المعلوماتية، ولكي يحقق التحقيق غايته في جمع الأدلة عن الجريمة الإلكترونية التي ارتكبت فلا بد من إيجاد وسيلة بموجبها يتم وضع اليد على شيء يتصل بها ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهذه الوسيلة تتمثل في التفتيش والضبط والشهادة



والإقرار والتي عن طريقها يتم الوصول إلى الأدلة التي تهدف إليها إجراءات الإثبات الجنائي. ومن خلال ذلك فالإقرار بارتكاب الجريمة يعتبر من أهم أدلة الإثبات على ارتكاب الجريمة.

ومن خلال النظر إلى هذه القضية وبسماع أقوال المتهم المذكور اعترف بقيامه باختراق البريد الإلكتروني العائد للمدعي وتغيير معلوماته وقام بإعادة البريد للمدعي وفق محضر دون بالأوراق. ويعتبر اعتراف المدعي عليه بارتكابه للجريمة هو أقوى أدلة الإثبات، وذلك لأنه لا توجد أي شبهة في الغالب اتجاه أقوال المقر بارتكاب الجريمة، لان المقر على نفسه لا يتهم بضغينة عليها، كما أن الإقرار صادر من الشخص الذي عليه الحق وفي هذا دليل على استعداده لقبول الحكم وأداء الحق. وقد توفر في هذا الاعتراف الشروط العامة لصحة الإقرار، فلصحة الإقرار شروط منها ما يتعلق بالمقر، ومنها ما يتعلق بالمقر له، فأما الشروط المتعلقة بالمقر، فيشترط فيه أن تتوفر فيه الأهلية الكاملة للإقرار، وهي أن يكون عاقلاً بالغاً مختاراً، فلا يصح إقرار المجنون ولا الصبي، إلا إذا كان مميزاً ومأذوناً له بالتجارة فيصح إقراره بكل ما يكون سبيله التجارة، ولا يصح إقرار المكره، كما يشترط في المقر له أن يكون معلوماً، فإن كان مجهولاً فلا يصح ذلك، كما أن إقرار المتهم على نفسه يجب أن يكون الاعتراف صادراً من المتهم على نفسه بواقعه تتعلق بشخصه لا شخص غيره فإذا تطرق الاعتراف إلى جرائم صدرت عن الغير ففي هذه الحالة لا يسمى اعترافاً بل شهادة على الغير، وقد توافرت هذه الشروط المختلفة في المدعي عليه الذي اعترف بارتكابه لجريمة اختراق البريد الإلكتروني.

ونتيجة لما سبق، فقد انتهى التحقيق إلى توجيه الاتهام للمتهم (أ) بارتكابه جريمة معلوماتية متمثلة في اختراق البريد الإلكتروني لشخص آخر عن طريق الشبكة المعلوماتية (الإنترنت) وتغيير معلوماته، وقد استندت هيئة التحقيق والإدعاء بتوجيه الاتهام إلى المدعي عليه من خلال اعترافه بما وجه إليه من ارتكاب جريمة معلوماتية، ومن خلال إقراره لذلك وقيامه بعمل محضر وإعادة البريد المخترق إلى المدعي، وحيث إن ما قام به المتهم المذكور فعل مجرم وفقاً للفقرة (١) من المادة الخامسة من

نظام مكافحة جرائم المعلوماتية والتي نصت على الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها، لذلك فقد طلب المحقق إثبات ما نسب إلى المدعي عليه وتعزيزه شرعاً لقاء اختراقه لبريد إلكتروني عن طريق الشبكة المعلوماتية (الإنترنت) وتغيير معلوماته استناداً للمادة (١٢٦) من نظام الإجراءات الجزائية ومجازاته شرعاً وفق ما يراه فضيلة ناظر القضية. ومن خلال ما تقدم، ومناقشة جريمة اختراق البريد الإلكتروني، فقد أوضحت المادة الخامسة من نظام مكافحة الجرائم الإلكترونية، أنه يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يقوم بالدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو إعادة نشرها، وهذا ما ينطبق على هذه القضية، لأن المدعي عليه قام بالاعتراف باختراقه للبريد الإلكتروني للمدعي، ثم قام بعمل محضر وإعادة البريد المخترق إلى المدعي، وفي هذه الحالة يجوز التعزير طبقاً لرؤية القاضي.

القضية الثالثة

قضية المال رقم (٣١/٤/١٨٤)

الصادر بحق /

(أ)، (٢٧) عاماً، سعودي الجنسية، بموجب سجل مدني رقم (X)، مهنته جندي في القوات البرية في حفر الباطن، مفرج عنه بالكفالة الحضورية لمرفقة بالأوراق لفة رقم (٥٥)، يقيم في مدينة الملك خالد العسكرية في حفر الباطن.

(الوقائع)

حيث إنه بتاريخ ١١/٠٣/١٤٣٠ هـ تقدم المدعي المواطن XX ببلاغ لقسم شرطة البلد عن تلقيه بتاريخ ١٠/٠٣/١٤٣٠ هـ مكالمة هاتفية من جوال رقم (XX) أخبره خلالها المتصل بأنه موظف في البنك الأهلي يدعي XX وطلب منه تحديث بيانات المؤسسة التابعة له كما طلب منه رقم الحساب البنكي للمؤسسة وكذلك الرقم السري بعدها طلب منه عدم استخدام الهاتف المصرفي وبعد ذلك قام المدعي بالاستفسار عن رصيده فأتضح له وجود عمليات

تحويل مبالغ قدرها خمسة وتسعون ألف ريال من حساب مؤسسته إلى حسابين أحدهما فردي والآخر لمؤسسة.

وبالبحث عن الأشخاص المستفيدين من المبلغ المالي المحول من حساب مؤسسة المدعي تبين أن حساب المواطن ×× - شقيق المتهم المذكور - تلقى حوالة بمبلغ ثلاثين ألف ريال من حساب المدعي وقام في إثرها بسحب خمسة آلاف ريال منها وتحويل خمسة آلاف ريال إلى ×××× (جری فرز أوراق له)، وتحويل عشرون ألف ريال إلى ×××× (جری فرز أوراق لها) كما تبين أن مؤسسة ×××× تلقت حوالة من حساب المدعي بمبلغ خمسة وستون ألف ريال تم بعد ذلك تحويلها إلى عدد من الأشخاص من ضمنهم تحويل خمسة آلاف ريال إلى حساب شقيق المدعي عليه وتسديد وشحن فواتير اتصالات (جری فرز أوراق لذلك).

وبالاستفسار عن كيفية تنفيذ عمليات التحويل تبين أنها تمت بواسطة الهاتف المصرفي من خلال رقم الجوال (××).

وبالبحث عن معلومات رقم الجوال المشار إليه اتضح أنه يعود للوافد: ×× (جری فرز أوراق له) وتبين وجود مكالمات بين الرقم والمدعي بتاريخ الواقعة ووقتها وعقب تلك المكالمات وجود اتصال من الرقم المشار إليه إلى البنك الأهلي، وأحيلت الأوراق لدائرة المال بمحافظة جدة بخطاب قسم شرطة البلد رقم ١٠/١/٢٠/٢٧٧٤ وتاريخ ١٤٣١/٠٥/٠٧ وقيدت بالوارد العام رقم (١٧٠١٠) وتاريخ ١٤٣١/٠٥/٠٧ هـ.

(التحقيقات)

باستجواب المواطن ××× أفاد بأن الحساب البنكي - الوارد إليه المبلغ المالي من حساب المدعي - يعود له، غير أنه منذ تقريباً عام ١٤٢٨ هـ ظل شقيقه المتهم المذكور أعلاه يتعامل في الحساب البنكي: إيداعاً وسحباً واكتتاباً في الأسهم وبيعاً ونحو ذلك ؛ ولذلك بقيت معه بطاقة الصراف الآلي وعرف رقمها السري والرقم السري الخاص بالهاتف المصرفي، ونفى علمه بالحوالة الواردة من حساب المدعي إلى حسابه.

باستجواب المتهم (أ) أفاد بمثل ما أفاد شقيقه ×××، وأكد بأنه تلقى حوالة مالية في حساب شقيقه المذكور ؛ إثر طلب صديق له يدعى: ×××× - المسجون في سجن حفر الباطن -

(جرى فرز أوراق له) رقم حساب ليتمكن من تلقي حوالة مالية واردة له من شخص، وأضاف بأنه عندما تم تحويل المبلغ إلى الحساب أخبره صديقه المذكور بأنه تم تحويل مبلغ ثلاثين ألف ريال، وطلب منه سحب المبلغ، فقام بسحب خمسة آلاف ريال من الصراف الآلي، وتحويل مثلها إلى المواطن ××××× إلى قام بسحبها وتسليمها لصديقه ××××× الذي سلمه إياها، بعد ذلك التقى بشخص ×××× - لا يعرف اسمه وأعطاه صديقه ×××× رقم جواله وأخبره بأنه يعمل عسكرياً في سجن حفر الباطن - وسلمه مبلغ العشرة آلاف ريال ؛ ليقوم بإيصالها إلى ××××، وبمواجهته بالحوالتين الصادرة عن حساب شقيقه إلى حساب المرأة ××× بمبلغ عشرون ألف ريال = نفى علمه بها وعلاقته بالمرأة المحول إليها وأفاد بأنه أعطى صديقه ××× رقم الحساب والرقم السري ورقم بطاقة الصراف ورقم المستخدم ورقم السجل المدني ؛ ليقوم بعمليات التحويل بسبب انشغاله في العمل، وبمواجهته بالتناقض في أقواله من حيث المبلغ المحول إلى حساب شقيقه إذ أفاد أن قدرة ثلاثون ألف ريال بينما تبين من خلال كشف الحساب أنه خمسة وثلاثون ألف ريال = أفاد بأنه أخبر بما أخبره صديقه ××، وأكد بأنه لا توجد له علاقة بمؤسسة ××× ومؤسسة ××× المحول منهما المبالغ المالية إلى حساب شقيقه.

(الإجراءات)

- ١ - جرى الإفراج عن المتهم المذكور وشقيقه بموجب أمر الإفراج رقم هـ م ٢٧٣٧٠/٤/٢ ورقم هـ م ٢٧٣٦٨/٤/٢ في ١٤٣١/٥/٧ هـ.
- ٢ - جرى مخاطبة البحث الجنائي بخطاب الدائرة رقم هـ م ٢٨٢٤٧/٤/٢ في ١٤٣١/٥/١٢ هـ لتزويدنا بمعلومات عن الجوال رقم (×××).
- ٣ - جرى فرز أوراق من القضية وإعادتها لقسم البلد بالخطاب رقم هـ م ٣١٠٠٩/٤/٢ في ١٤٣١/٥/٢٦ هـ للبحث والتحري عن بقية الأشخاص المستفيدين من المبالغ المالية المحولة من حساب المدعي.
- ٤ - جرى حفظ الدعوى تجاه المواطن ×××× لعدم كفاية الأدلة استناداً للمادة (١٢٤) من نظام الإجراءات الجزائية.

(الإتهام)

لذلك كله أقرر توجيه الاتهام إلى (أ) بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية لقيامه بالاستيلاء على مال عن طريق الاحتيال، وذلك للأدلة والقرائن التالية:

- ١ - اعتراف المتهم المذكور تحقيقاً المدون على ص (٤-٥) من دفتر التحقيق الأول المرفق لفة رقم (٤٨) و ص (١٤-١٥) من ملف إجراءات الاستدلال لفة رقم (٤٥) المتضمن: تلقيه المبلغ المالي في حساب شقيقه بعلمه وتصرفه فيه بالسحب، والتحويل لشخص آخر.
- ٢ - عجز المتهم المذكور عن إثبات سبب شرعي، أو مسوغ نظامي لوجود المبلغ المالي في الحساب ؛ وتصرفه فيه بالسحب والتحويل.
- ٣ - ما جاء في كشف حساب شقيق المتهم المذكور المرفق لفة رقم (٤٦) المتضمن: تلقيه لمبلغ ثلاثون ألف ريال من حساب المدعي وخمسة آلاف ريال من حساب مؤسسة بكر أبو بكر وسحبه منها خمسة آلاف ريال وتحويل خمسة وعشرين ألف ريال لآخرين.
- ٤ - سرعة تصرف المتهم المذكور بالمبلغ المالي عقب تحويل المبلغ: بالسحب والتحويل.

(الطلبات)

وحيث إن ما قام به المتهم (أ) وهو بكامل أهليته المعتبرة شرعاً يعد فعلاً محرماً ومجرماً نظاماً وفقاً للمادة الرابعة من نظام مكافحة جرائم المعلوماتية ؛ لذا أطلب إحالته إلى المحكمة الجزئية لإثبات ما أسند إليه والحكم عليه بالعقوبة المقررة وفق المادة الرابعة من النظام ذاته. (علماً بأن الحق الخاص لازال قائماً). والله موفق،،،

عضو هيئة التحقيق والإدعاء العام

محقق ثان/

التحليل:

بالنظر إلى هذه القضية يلاحظ أنها ترتبط بالجريمة الإلكترونية، وذلك من خلال تناولها وعرضها لجريمة الاعتداء على الأموال عن طريق الأنظمة الإلكترونية الحديثة، حيث يتضح من خلال تفاصيل هذه القضية أنها تمت من خلال اتصال المتهم (أ) بالمدعي، وأخبره بأنه موظف في البنك الأهلي يدعي (أ) وطلب منه تحديث بيانات المؤسسة التابعة له كما طلب منه رقم الحساب البنكي للمؤسسة وكذلك الرقم السري بعدها طلب منه عدم استخدام الهاتف المصرفي وبعد ذلك قام المدعي بالاستفسار عن رصيده فاتضح له وجود عمليات تحويل مبالغ قدرها خمسة وتسعون ألف ريال من حساب مؤسسته إلى حسابين أحدهما فردي والآخر لمؤسسة.

ومن خلال النظر إلى هذه القضية وسماع أقوال المتهم ×× أفاد بأن الحساب البنكي - الوارد إليه المبلغ المالي من حساب المدعي - يعود له، غير أنه منذ تقريباً عام ١٤٢٨ هـ ظل شقيقه المتهم المذكور أعلاه يتعامل في الحساب البنكي إيداعاً وسحباً واكتتاباً في الأسهم وبيعاً ونحو ذلك؛ ولذلك بقيت معه بطاقة الصراف الآلي وعرف رقمها السري والرقم السري الخاص بالهاتف المصرفي، ونفى علمه بالحوالة الواردة من حساب المدعي إلى حسابه. وأيضاً من خلال التحريات التي قامت بها جهات التحقيق وبالبحث عن معلومات رقم الجوال المشار إليه اتضح أنه يعود للوافد: ××× (جرى فرز أوراق له) وتبين وجود مكالمات بين الرقم والمدعي بتاريخ الواقعة ووقتها وعقب تلك المكالمات وجود اتصال من الرقم المشار إليه إلى البنك الأهلي، لذلك كله أقرر توجيه الاتهام إلى (أ) بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية لقيامه بالاستيلاء على مال عن طريق الاحتيال، وذلك للأدلة والقرائن التالية التي ساعدت على إثبات الجريمة، ويمكن توضيح هذه الأدلة كما يلي:

١ - اعتراف المتهم المذكور بتلقيه المبلغ المالي في حساب شقيقه بعلمه وتصرفه فيه بالسحب، والتحويل لشخص آخر. وقد توفر في هذا الاعتراف الشروط العامة لصحة الإقرار، فلصحة الإقرار شروط منها ما يتعلق بالمقر، ومنها ما يتعلق بالمقر له، فأما الشروط المتعلقة بالمقر، فيشترط فيه أن تتوفر فيه

الأهلية الكاملة للإقرار، وهي أن يكون عاقلًا بالغًا مختارًا، فلا يصح إقرار المجنون ولا الصبي، إلا إذا كان مميزاً ومأذوناً له بالتجارة فيصح إقراره بكل ما يكون سبيله التجارة، ولا يصح إقرار المكره، كما يشترط في المقر له أن يكون معلوماً، فإن كان مجهولاً فلا يصح ذلك، كما أن إقرار المتهم على نفسه، يؤكد إثبات الاتهام الموجه إليه، ويؤكد ذلك أيضاً أن الاعتراف صادراً من المتهم على نفسه بواقعه تتعلق بشخصه لا شخص غيره فإذا تطرق الاعتراف إلى جرائم صدرت عن الغير ففي هذه الحالة لا يسمى اعترافاً بل شهادة على الغير، وقد توافرت هذه الشروط المختلفة في المدعي عليه الذي اعترف بتلقيه المبلغ المالي في حساب شقيقه بعلمه وتصرفه فيه بالسحب، والتحويل لشخص آخر.

٢ - عجز المتهم المذكور عن إثبات سبب شرعي، أو مسوغ نظامي لوجود المبلغ المالي في الحساب؛ وتصرفه فيه بالسحب والتحويل.

٣ - ما جاء في كشف حساب شقيق المتهم المذكور بتلقيه لمبلغ ثلاثون ألف ريال من حساب المدعي وخمسة آلاف ريال من حساب مؤسسة ××× وسحبه منها خمسة آلاف ريال وتحويل خمسة وعشرين ألف ريال لآخرين. في هذه المرحلة تم فحص كل من الدليل المادي المضبوط، والدليل المادي المستخرج من جهاز الهاتف (والذي أصله هو الدليل الرقمي) الموجود بملفات النظام المضبوط من نصوص. وبذلك يكون تم الربط بين الدليل الرقمي والدليل المادي، مما يكسب الدليل الموثوقية، واليقينية، اللتان تؤديان إلى قبوله لدى جهة التحقيق وجهة الحكم، ويقوم بعد ذلك بإعداد تقرير بجميع خطوات وإجراءات البحث، وبعد ذلك يتم تصدير هذه التقرير إلى جهة الحكم.

٤ - سرعة تصرف المتهم المذكور بالمبلغ المالي عقب تحويل المبلغ بالسحب والتحويل، حيث ثبت من خلال البحث والتحري لإثبات الجريمة أن المتهم (أ)، قام بالعديد من التحويلات إلى عدة أشخاص بمجرد قيامه بعملية الاعتداء على الأموال.

ونتيجة لما سبق، وقيام المتهم بالاعتداء على الأموال من خلال القيام بعملية التحويل عن طريق الجوال، وحيث إن ما قام به المتهم (أ) وهو بكامل أهليته المعتبرة شرعاً يعد فعلاً محرماً ومجرماً نظاماً وفقاً للمادة الرابعة من نظام مكافحة جرائم المعلوماتية ؛ لذا تتم إحالة المتهم إلى المحكمة الجزئية لإثبات ما أسند إليه والحكم عليه بالعقوبة المقررة وفق المادة الرابعة من النظام ذاته والتي تنص على أنه "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يقوم بالاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، وأيضاً الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات.

القضية الرابعة

الحمد لله وحده والصلاة والسلام على من لا نبي بعده وبعد ففي يوم الأحد ١٤٣١/١١/٩ هـ في تمام الساعة العاشرة صباحاً لدي أنا ××× القاضي بالمحكمة الجزئية بمحافظة جدة فبناءً على المعاملة الواردة لنا من هيئة التحقيق والادعاء العام برقم ٥٧٦٨٤ في ١٤٣١/٣١١ هـ المقيدة لدينا برقم ٣١/٤١٠٤٢ وتاريخ ١٤٣١/١١/٤ هـ والمحالة لنا برقم ١٩٣٩٧ وتاريخ ١٤٣١/١١/٤ هـ افتتحت الجلسة وفيها حضر المدعى العام / ××× لاثته ضد / (أ) (٣٧) عاماً يمني الجنسية بموجب الإقامة رقم (×××) سجن قبض عليه بتاريخ ١٤٣١/١١/١٧ هـ قبض على المتهم أعلاه بعد أن تقدم أحد الأحداث بشكوى يفيد فيها عن قيام المذكور بابتزازه وفي عرضه وزعمه أن لديه صوراً عارية له وأنه إن لم يمكنه من فعل الفاحشة به فسوف يفضحه أمام زملائه في المدرسة كما أنه يقوم بإرسال رسائل تهديد وابتزازه له وأنه مستمر في ذله منذ أكثر من نصف سنة وبمعاينة جوال المدعي عثر به على أربعة رسائل واردة من جوال المتهم وقد ورد اتصال على الحدث وبوجود الفرق القابضة وطلب من الحدث مجاراة المتهم وكان ذلك على مسمع من الفرقة القابضة حيث ذكر

المتهم للحدث بأنه (يريد أن يفعل الفاحشة الليلة وإن لم يمكنه من نفسه فلا يلوم إلا نفسه) فقام الحدث بمجاراته وتم عمل كمين للمتهم وتم القبض عليه وقد أسفر التحقيق عن توجيه الاتهام إليه بابتزاز حدث وتهديده بفضحه إن لم يمكنه من نفسه وتخزين وحيازة مقاطع جنسية على ذاكرة إلكترونية وذلك للأدلة والقرائن التالية: ١ - ما جاء في أقوال المتهم المدونة بدفتر التحقيق لفة (٩) صفحة (١-٢). ٢ - ما جاء بمحضر القبض المعد من قبل الفرقة القابضة المرفق رقم (٤). ٣ - محضر المشاهدة المرفق على لفة رقم (١-٢).

وحيث إن ما قدم عليه المذكور يعد فعلاً محرم ومعاقب عليه شرعاً لذا أطلب إثبات ما أسند إليه والحكم عله بعقوبة تعزيرية لقاء ذلك. كما أطلب الحكم عليه وفق المادة (١/٦) المنصوص عليها في نظام مكافحة الجرائم المعلوماتية الصادر بمرسوم ملكي. كما أطلب مصادرة الجهاز الجوال نوع (S-Colorx6) لاستخدامه في الجريمة وكذلك مصادرة وحدة التخزين الإلكترونية (فلاش ميموري) لاحتوائه على مقاطع جنسية هذه دعواي وأسأله الجواب وبسؤال المدعى عليه أجاب قائلاً بقوله ما ذكره المدعي العام كله صحيح فقد كنت أرسل رسائل للحدث المذكور وأرسلت له رسائل تهديد ولكن كان بحسن نية ولم أكن أريد إيقاع أي ضرر به هكذا أجاب فسألت ما تعني بحسن النية فقال هي مجرد كلام فقط دون فعل فليس لدي صور للحدث وأضاف وما ذكره المدعي من أنني أحوز المقاطع الجنسية التي ذكر فغير صحيح هكذا أجاب على هذا سألت المدعي بينته طبق دعواه حيث أنكر حيازته للذاكرة الإلكترونية ومن ثم قام السجين المدعى عليه وقال أرجع عن نفي الذاكرة الإلكترونية وأقرر أن ما ذكره المدعي العام كله صحيح هكذا قال عليه جرى الرجوع إلى الأوراق واطلعت على محضر القبض ومحضر المشاهدة فلم أجد فيما ذكر زيادة تستوجب تحريرها فبناء على ما تقدم من الدعوى والإجابة ولمصادقة المدعى عليه على دعوى المدعي العام، ولأنه لا عذر لمن أقر ولأن فعله محرم شرعاً ونظاماً وهو وسيلة لجرم عظيم ولأن الجرم كان على حدث وهو صغير السن ولأن فعله هما بالأمر ولا سوابق عليه لذا كله فقد ثبت لدي إدانته بما نسب إليه وحكمت عليه بالسجن ثمانية أشهر من تاريخ إيقافه وجلده ثلاثمائة جلدة

مفرقة على دفعات بين كل دفعة وأخرى خمسة عشر يوماً مقدار كل دفعة خمسون جلدة كما حكمت عليه بالسجن ثلاثة أشهر والغرامة ألفي ريالاً ويكون السجن متصلاً معاً ما سبق وفق المادة المنصوص عليها في نظام مكافحة الجرائم المعلوماتية كما حكمت عليه بمصادرة جهاز الجوال ووحدة التخزين الإلكترونية المنصوص عليها معه وبإعلان الحكم في تمام الساعة العاشرة والنصف قنع المدعى عليه ولم يبد المدعى العام اعتراضاً وصلى الله على نبينا محمد حرر في ١٤٣١/١١/٩ هـ.

القاضي بالمحكمة الجزئية بمحافظة جدة

التحليل:

من خلال النظر إلى هذه القضية، يلاحظ أنها ترتبط بأحد أنواع الجرائم الإلكترونية، وذلك من خلال حيازة بعض المقاطع الجنسية على ذاكرة إلكترونية موجودة في الهاتف الجوال، واستخدام هذه الصور في التهديد، واستخدام الجوال أيضاً في إرسال رسائل التهديد للمدعي، ومن خلال قيام جهات التحقيق بمواجهة المدعي عليه لإثبات الجريمة الموجهة إليه، فقد أجاب قائلاً بقوله ما ذكره المدعي العام كله صحيح فقد كنت أرسل رسائل للحدث المذكور وأرسلت له رسائل تهديد ولكن كان بحسن نية ولم أكن أريد إيقاع أي ضرر به هكذا أجاب فسألت ما تعني بحسن النية فقال هي مجرد كلام فقط دون فعل، فليس لدي صور للحدث وأضاف وما ذكره المدعي من أنني أحوز المقاطع الجنسية التي ذكر فغير صحيح. كما أن المدعي عليه، أنكر عند التحقيق معه حيازته للذاكرة الإلكترونية ومن ثم قام المدعى عليه عند تشديد التحقيق معه وعند فحص جهاز الهاتف الجوال وفحص الذاكرة الموجودة به ومواجهة المدعي عليه، فقد تراجع عن نفيه لعدم امتلاك الذاكرة الإلكترونية وأقر أن ما ذكره المدعي العام كله صحيح.

ومن خلال الرجوع إلى الأوراق والإطلاع على محضر القبض ومحضر المشاهدة فلم نجد فيما ذكر زيادة تستوجب تحريرها فبناء على ما تقدم من الدعوى والإجابة ولمصادقة المدعى عليه على دعوى المدعي العام ولأنه لا عذر لمن أقر ولأن فعله محرم شرعاً ونظماً وهو وسيلة لجرم عظيم ولأن الجرم كان على حدث وهو

صغير السن ولأن فعله هماً بالأمر ولا سوابق عليه لذا كله فقد ثبت لدي إدانته بما نسب إليه وتم الحكم عليه بالسجن ثمانية أشهر من تاريخ إيقافه وجلده ثلاثمائة جلدة مفرقة على دفعات بين كل دفعة وأخرى خمسة عشر يوماً مقدار كل دفعة خمسون جلدة كما حكمت عليه بالسجن ثلاثة أشهر والغرامة ألفي ريالاً ويكون السجن متصلاً معاً ما سبق وفق المادة المنصوص عليها في نظام مكافحة الجرائم المعلوماتية كما حكمت عليه بمصادرة جهاز الجوال ووحدة التخزين الإلكترونية المنصوص عليها معه.

ووفقاً لنظام مكافحة الجرائم المعلوماتية، فنجد أنه تم الحكم على المدعي عليه بهذا الحكم ومعاقبته بمصادرة جهاز الجوال ووحدة التخزين الإلكترونية، وذلك من أجل الحد من وقوع جرائم المعلوماتية، والمساعدة في تحقيق الأمن المعلوماتي، وحماية المصلحة العامة والخلق والآداب العامة. ولذا يعاقب هذا المتهم بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين كل شخص يقوم بالدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً، وأيضاً المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها، وأيضاً التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنية المعلومات المختلفة، وهذا ما ينطبق على هذه القضية، حيث استخدم المتهم الهاتف الجوال في ارتكاب جريمة إلكترونية، من خلال استخدام لبعض الصور الجنسية الموجودة على ذاكرة الهاتف واستخدامها في عملية التهديد، مما يستحق العقوبة التي يقررها نظام مكافحة الجريمة.

القضية الخامسة

الحمد لله وحده وبعد لدى أنا ×× مساعد رئيس المحكمة الجزئية بجدة بناءً على المعاملة الواردة من الإدعاء العام برقم [٤٣٩٦٥] في ١٤٣١/٨/٢ هـ والمحالة لنا من فضيلة الرئيس برقم [١٤٥٨٣] في ١٤٣١/٨/٥ هـ عليه حضر المدعي العام /××××، وادعى على كلاً من: ١/ ×××× [٥٤] عاماً، بنجلاديشي الجنسية بموجب الإقامة رقم [××××]، موقوف، ٢/ المرأة: ××× [٢٨] عاماً، مغربية الجنسية بموجب بطاقة بديلة رقم [×××]، موقوفة، قائلاً: إنهما مدانان بالاشتراك في شبكة لأعمال القوادة والدعارة وتستترهما على بقية أطراف الشبكة وإيصال الأول للثانية وشركائهما إلى مواقع ممارستهم أنشطتهم المحرمة تلك وإلى الثانية بممارسة أعمال الدعارة وعرض نفسها على الغير وإحياء السهرات المحرمة وتصوير نفسها في أوضاع مخلة بالآداب العامة وتخزينها لتلك المقاطع وذلك للأدلة والقرائن المسرودة بملف القضية لذا أطلب إثبات ما اسند إليهما والحكم عليهما بعقوبة تعزيرية رادعة لقاء ذلك كما أطلب الحكم على الثانية وفقاً للمادة [١/٦] من نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم [م/١٨] لعام ١٤٢٨ هـ ومصادرة جوالها وفقاً للمادة [١٣] من ذات النظام لاستعماله في الجريمة علماً بأن المرأة ذكرت عند القبض عليها أن اسمها /××× وقد فصلت لها أوراق مستقلة حيال التزوير هذه دعواي واسألها الجواب ويسأل المدعى عليهما عما جاء بدعوى المدعي العام أجاب كل واحد منهما بمفرده بقوله: ما جاء بدعوى المدعي العام صحيح جملة وتفصيلاً وقد أغوانا الشيطان ومن أجل الكسب المادي ونادمين على ما حصل وتائبين إلى الله عز وجل وبالرجوع إلى أوراق المعاملة وجد أقوالهما تحقيقاً ومحضر القبض المتضمن طبق دعوى المدعي العام، كما لم يعثر لهما على سوابق، فبناءً على ما تقدم من الدعوى والإجابة ونظراً لمصادقة المدعى عليهما لما جاء بدعوى المدعي العام ونظراً لما في عملهما من إشاعة الفاحشة ونشر للفساد والرديلة في المجتمع ونظراً لما في عمل المدعى عليه الأول مع كبر سنه من إعانته للمدعى عليها الثانية على فعل الحرام ونظراً لما في عملهما من نشر للأمراض بين الناس ونظراً لكون الأحكام الشرعية تدور على وجوب حفظ الضروريات الخمس سواءً

كانت في المجتمع أو في نفس الفاعل ويوقع منها ما تدعو الحاجة إليه كماً وكيفاً ونظراً لتقشي هذه الظاهرة في البلاد وعدم الرادع ونظراً لعظم ما نسب إليهما لذا فقد ثبت لدى إدانة المدعى عليهما بالاشتراك في شبكة لأعمال القوادة والدعارة وتستترهما على بقية أطراف الشبكة وإيصال الأول للثانية وشركائهما إلى مواقع ممارستهم أنشطتهم المحرمة تلك وإلى الثانية بممارسة أعمال الدعارة وعرضه نفسها على الغير وإحياء السهرات المحرمة وتصوير نفسها في أوضاع مخلة بالآداب العامة وتخزينها لتلك المقاطع وهما يستحقان تشديد العقوبة عليهما والمدعى عليها الثانية تستحق تطبيق المادة [١/٦] من نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم [م/١٨] لعام ١٤٢٨هـ ونظراً لظهور بؤادر الندم عليهما وعدم وجود سوابق عليهما ونظراً لكونهما أجنب ولا فائدة مرجوة من إطالة سجنهما لذا فقد حكمت على المدعى عليهما بعد أن تم نصحبهما وتوجيههما أولاً: سجن المدعى عليه الأول ××× لمدة سنتين ونصف وجلده ثلاثمائة جلدة، ثانياً: سجن لمدعى عليها الثانية / المرأة: ××× لمدة خمس سنوات وجلدها خمسمائة جلدة وجميع السجن من تاريخ إيقافهما المصادف ١٤٣١/٣/٢٩هـ وجميع الجلد على دفعات كل دفعة خمسين سوط بين الفترة والأخرى خمسة عشر يوماً، ثالثاً: حكمت بمصادرة جهاز جوال المدعى عليها الثانية لاستخدامه في الجريمة وفقاً للمادة [١٣] من ذات النظام، رابعاً: أوصي بإبعادهما عن البلاد بعد تنفيذ محكوميتهما وعدم السماح لهما بالعودة إليها وبعرضه عليهما قررا القناعة به والمدعى العام لم يبدي اعتراضاً حرر يوم الثلاثاء ١٤٣١/٨/٨هـ وصلى الله وسلم على نبينا محمد.

مساعد رئيس المحكمة الجزئية بجدة

التحليل:

من خلال دراسة هذه القضية وتحليلها، يتضح أنها ترتبط بارتكاب جريمة إلكترونية من خلال تصوير بعض المشاهد الجنسية من خلال الجوال، فيلاحظ أن المتهمان في هذه القضية مدانان بالاشتراك في شبكة لأعمال القوادة والدعارة وتستترهما على بقية أطراف الشبكة وإيصال الأول للثانية وشركائهما إلى مواقع ممارستهم أنشطتهم المحرمة تلك وإلى الثانية بممارسة أعمال

الدعارة وعرض نفسها على الغير وإحياء السهرات المحرمة وتصوير نفسها في أوضاع مخلة بالآداب العامة وتخزينها لتلك المقاطع وذلك للأدلة والقرائن المسرودة، فقد استغلت المتهمة انتشار وسائل الاتصال الحديثة التي ساعدت في ظهور بعض الجرائم الإلكترونية وارتفاع مستواها في بعض الدول نتيجة كثرة مستخدمي تلك الوسائل وتعدد مواهبهم.

ومن خلال التحقيق في هذه القضية وقيام جهات التحقيق بمحاولة إثبات الجريمة من خلال أدوات الإثبات والقرائن، التي تؤكد ارتكاب الجريمة، فقد اعترف المتهمان بأن ما جاء بدعوى المدعي العام صحيح جملة وتفصيلاً وقد أغوانا الشيطان ومن أجل الكسب المادي ونادمين على ما حصل وتائبين إلى الله عز وجل وبالرجوع إلى أوراق المعاملة وجد أقوالهما تحقيقاً، أي أن المتهمان قد اعترفا بالقيام بالجريمة، وقد توفر في هذا الاعتراف الشروط العامة لصحة الإقرار، فلصحة الإقرار شروط منها ما يتعلق بالمقر، ومنها ما يتعلق بالمقر له، فأما الشروط المتعلقة بالمقر، فيشترط فيه أن تتوفر فيه الأهلية الكاملة للإقرار، وهي أن يكون عاقلاً بالغاً مختاراً، فلا يصح إقرار المجنون ولا الصبي، إلا إذا كان مميزاً ومأذوناً له بالتجارة فيصح إقراره بكل ما يكون سبيله التجارة، ولا يصح إقرار المكره، كما يشترط في المقر له أن يكون معلوماً، فإن كان مجهولاً فلا يصح ذلك، كما أن إقرار المتهم على نفسه يجب أن يكون الاعتراف صادراً من المتهم على نفسه بواقعه تتعلق بشخصه لا شخص غيره فإذا تطرق الاعتراف إلى جرائم صدرت عن الغير ففي هذه الحالة لا يسمى اعترافاً بل شهادة على الغير، وقد توافرت هذه الشروط المختلفة في المدعي عليه حيث اعترف المتهمان بقيامهم بارتكاب الجريمة، وهذا الاعتراف لا يجوز التشكيك فيه، وهو ما يؤكد إثبات القضية.

وهناك دليل آخر قامت لجنة التحقيق بمواجهة المتهمان به وهو جهاز الهاتف الجوال التي استخدمته المتهمة في القضية في تصوير نفسها به وعثر على هذه الصور موجودة على الهاتف الجوال، وتعتبر هذه الصور من ضمن الأدلة والقرائن التي تثبت قيام المتهمة بارتكاب أحد أنواع الجرائم الإلكترونية، وقد تم تأكيد ذلك من خلال فحص كل من الدليل المادي المضبوط، والدليل المادي المستخرج من جهاز الهاتف (والذي أصله هو الدليل الرقمي) الموجود بملفات النظام المضبوط من نصوص. وبذلك يكون تم الربط بين الدليل الرقمي والدليل المادي، مما يكسب الدليل الموثوقة، واليقينية، اللتان تؤديان إلى قبوله لدى جهة التحقيق وجهة الحكم، ويقوم بعد

ذلك بإعداد تقرير بجميع خطوات وإجراءات البحث، وبعد ذلك يتم تصدير هذه التقرير إلى جهة الحكم.

ومن خلال قيام جهة التحقيق بإثبات الجريمة على المتهمين، فيتمثل الاتهام الموجه إليهم في الاشتراك في شبكة لأعمال القوادة والدعارة وتستترهما على بقية أطراف الشبكة وإيصال الأول للثانية وشركائهما إلى مواقع ممارستهم أنشطتهم المحرمة تلك وإلى الثانية بممارسة أعمال الدعارة وعرضه نفسها على الغير وإحياء السهرات المحرمة وتصوير نفسها في أوضاع مخلة بالآداب العامة وتخزينها لتلك المقاطع وهما يستحقان تشديد العقوبة عليهما والمدعى عليها الثانية تستحق تطبيق المادة [١/٦] من نظام مكافحة الجرائم المعلوماتية، والتي تنص على أنه "يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يقوم ما شأنه بإنتاج المساس بالنظام العام أو القيم الدينية أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي"، كما تم تطبيق المادة الثالثة عشر من نظام مكافحة الجريمة الإلكترونية، والتي تنص على "مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام أو الأموال المحصلة منها، كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكة، ولذا يمكن القول من خلال دراسة هذه القضية أن هذه العقوبة تتناسب مع حجم الجريمة التي تم ارتكابها.

القضية السادسة

الحمد لله وحده وبعد لدي أنا ×××× القاضي بالمحكمة الجزئية بجدة بناءً على المعاملة المحالة لنا من فضيلة رئيس المحكمة برقم ٤٧٨٤ في ١٤/٣/١٤٣١ هـ تقدم المدعي العام / ×××× وادعى على / ١ - (أ) يماني الجنسية بالبطاقة البديلة رقم (٣١/١٩٠/٧٠) ٢ - ×××× يماني الجنسية بالبطاقة البديلة رقم (٣١/١٩٠/٦٩) ٣ - ××× يماني الجنسية بالبطاقة البديلة رقم (٣١/١٩٠/٦٨) قائلاً أنه أسفر التحقيق مع المدعى عليهم إلى توجيه الاتهام إليهم بنسخ وترويج أقراص مدمجة تحتوي على أفلام

خليعة عن طريق الحاسب الآلي وحيث أن ما أقدم عليه المدعى عليهم فعل محرم ومعاقب عليه شرعاً أطلب إثبات ما أسند إليهم والحكم عليهم وفق المادة (١/٦) في نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (٧٩) لعام ١٤٢٨هـ كما أطلب مصادرة جهاز الكمبيوتر الهاردسك والماسح الضوئي والطابعة وأقراص الدي في دي وجهاز نسخ ورق المادة ١٣ من ذات النظام لقاء ذلك وبسؤال المدعى عليهم عن الدعوى أجاب على ×××× و ×××× بأنهما مستأجرين شقة ويقومان بنسخ أفلام وهي أفلام عادية وليست خليعة ولا جنسية وقالوا أن عمر المذكور قبض عليه في الشارع ومعه السيديوهات فسئل المدعي العام عن نوعية هذه الأفلام وبالرجوع إلى أوراق المعاملة وجد أن هذه الأفلام أفلام خليعة وقال ×××× أن الأجهزة المذكورة تعود له فعليه وحيث الحال ما ذكر فإن المدعى عليهم جميعاً مدانون فيما نسب إليهم من الدعوى ويستحقون التعزير البليغ لما ذكر ولما في ذلك من فساد كبير لترويج هذا الكم الكبير من السيديوهات وحكمت بتعزيرهم أولاً بالسجن ثلاث سنوات استناداً للمادة ٦ من نظام الجرائم المعلوماتية ومصادرة الأجهزة المذكورة وهي جهاز الكمبيوتر والماسح الضوئي والطابعة وأقراص الدي في دي وجهاز النسخ استناداً للمادة ١٣ من ذات النظام وبعرضه عليه قرروا عدم القناعة ويرغبون تقديم لائحة اعتراضية وقرر المدعي العام معارضته للحكم بدون لائحة وصلى الله وسلم على عبده ورسوله محمد حرر في ١٤٣١/٣/٢١هـ.

القاضي بالمحكمة الجزئية بجدة

ثم عادت المعاملة من محكمة التمييز بالرقم ١٧٨٥٣/٦ في ١٤٣١/٦/٥هـ الصادر فيها قرار التمييز ذو الرقم ١٦٣/٣/٢/ج وتاريخ ١٤٣١/٦/٤هـ لمتضمن أنه بدراسة القرار وصورة ضبطه ولائحته الاعتراضية تقرر إعادتها لفضيلة حاكمها لملاحظة ما يلي: أولاً - إن المدعى عليهم ثلاثة ومنهم ×××× لم نجد أنه أخذ له جواب على الدعوى والمدعى عليهما ××× لم يعترفا بشيء عن الأفلام الخليعة والمدعي العام لم يجب بشيء عن الأفلام الخليعة حينما سئل عن ذلك ثانياً كيف ثبت لدى فضيلته إن الأفلام خليعة والمدعى عليه ××× لم يؤخذ جوابه على الدعوى ×××× نفياً ذلك ؟ فكيف تمت الإدانة ولا اعتراف ولا بيئة موصلة كما إن عرض الحكم على المدعى عليهم جاء بصيغة المفرد (عليه) لملاحظة

ذلك وللإجابة على أصحاب الفضيلة فإن المدعى عليه ××× كان حاضراً في الجلسة المقررة وسئل عن الدعوى ولكن الموظف أسقط إجابته أثناء الكتابة بدليل بصمته على الإجابة وجابته أنه يبيع ويروج الأفلام ولكنها ليست خليعة كما ذكر وإما كون الأفلام خليعة فإن المدعى العام ذكر ذلك إنها خليعة استناداً إلى محضر المشاهدة المرفق ضمن الأوراق والذي أشير فيه أنه بالإطلاع على عينة منتقاة من الأفلام البالغ عددها ما يقارب الثلاثين ألف ظهر إنها أفلام خليعة ومثيرة للغرائز وأن الإدانة وجود هذه الأفلام معهم أكبر إدانة وأما كون العرض عليه فهذا خطأ من الكاتب وصحته عليهم وإحضار المدعى عليهم الآخرين مع المدعى عليه الحاضر هذه الجلسة للنظر في إمكانية تخفيف الحكم من عدمه وفي يوم السبت الموافق ١٤٣١/٦/٢٩ هـ حضر المدعى عليهم، ورأيت تخفيف العقوبة عنهم لما ظهر من توبة وندم عليهم بعد حضورهم هذه الجلسة جميعاً وعليه رجعت عما حكمت عليهم من سجن وحكمت بتعزيزهم بالسجن سنة وأربعة أشهر استناداً للمادة (٦) من نظام الجرائم المعلوماتية وبعرضه عليهم قرروا جميعاً القناعة بالحكم وصلى الله على نبينا محمد حرر في ١٤٣١/٦/٢٩ هـ

القاضي بالمحكمة الجزئية بجدة

إشارة إلى عودة المعاملة من محكمة التمييز بقرارها رقم ٢٤٦/٢/٣/ج في ١٤٣١/٨/١٥ هـ المتضمن بدراسة القرار وصورة ضبطه ولائحته الاعتراضية تقرر إعادتها لفضيلة حاكمها لملاحظة أن ما حكم به فضيلته على الدعوى عليهم ورد مجملاً وغير مفصل على كل واحد منهم وفي هذا إيهام ينبغي توضيحه لجهات التنفيذ في الضبط والقرار والله الموفق وصلى الله على نبينا محمد وعلى آله وصحبه وسلم. وعليه وشارة إلى ما تضمنه قرار أصحاب الفضيلة أعلاه فقد جرى إيضاح الحكم الصادر بحق المذكورين أعلاه وهو سجن كل واحد منهم سنة وأربعة أشهر ألحق بضبطه وقراره وصورة ضبطه لاتخاذ ما يراه أصحاب الفضيلة لازماً بعد الإجراء الأخير وصلى الله وسلم على سيدنا ونبينا محمد وآله وصحبه وسلم حرر في ١٤٣١/١٠/١٩ هـ.

القاضي بالمحكمة الجزئية بجدة

بسم الله الرحمن الرحيم

الحمد لله وحده والصلاة والسلام على من لا نبي بعده وبعد: فقد جر منا نحن قاضي الاستئناف بالدائرة الجزائية الثالثة بمحكمة الاستئناف بمكة المكرمة الاطلاع على القرار رقم ١٨٨/٢/ج وتاريخ ١٤٣١/٣/٢٣ هـ الصادر من فضيلة الشيخ / ××××× بالمحكمة الجزئية بجدة المتضمن دعوى المدعى العام ضد / ××××× يماني الجنسية ورفيقه المتهمين بنسخ وترويج أقراص مدمجة تحتوي على أفلام خليعة عن طريق الحاسب الآلي المحكوم فيه بما دون باطنه وبدراسة الحكم وصورة ضبطه واللائحة الاعتراضية تقررت الموافقة على الحكم بعد الإيضاح الأخير. والله الموفق وصلى الله على نبينا محمد وعلى آله وصحبه وسلم،

الدائرة الجزائية الثالثة

قاضي استئناف قاضي استئناف رئيس محكمة استئناف

ورئيس الدائرة

التحليل:

من خلال ملاحظة هذه القضية ودراسة المحاور المختلفة لها، يتبين أنها تتعلق بارتكاب جريمة إلكترونية، وذلك من خلال ارتكاب المدعي عليهم جريمة إلكترونية تتعلق بنسخ وترويج أقراص مدمجة تحتوي على أفلام خليعة عن طريق الحاسب الآلي، وهذا ما يحاسب عليه نظام مكافحة الجرائم الإلكترونية، ومن خلال قيام جهات التحقيق من مباشرة التحقيق والتحري في هذه القضية يتبين أن المدعي عليهم لم يعترفوا بحيازتهم للأفلام الخليعة، أو قيامهم بنسخ هذه الأفلام، كما أن المدعي العام لم يجب بشيء عن الأفلام الخليعة. ولذلك فقد قام المحقق بتقديم أدلة الإثبات لهذه القضية قائلاً أن التحقيق مع المدعى عليهم قد أسفر إلى توجيه الاتهام إليهم بنسخ وترويج أقراص مدمجة تحتوي على أفلام خليعة عن طريق الحاسب الآلي وحيث إن ما أقدم عليه المدعى عليهم فعل محرم ومعاقب عليه شرعاً فقد طلب إثبات ما أسند إليهم والحكم عليهم وفق المادة (١/٦) في نظام مكافحة الجرائم المعلوماتية، والتي تنص على أنه "يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يقوم ما شأنه بإنتاج المساس

بالنظام العام أو القيم الدينية أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي".

كما طلب المحقق أيضاً مصادرة جهاز الكمبيوتر الهاردسك والماسح الضوئي والطابعة وأقراص الدي في دي طبقاً للمادة الثالثة عشر من هذا النظام والتي تنص على أنه "مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام أو الأموال المحصلة منها، كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكة". كما اعتمد المحقق في إثبات هذه الجريمة على سؤال المدعي عليهم عن الدعوى فأجابوا بأنهم مستأجرين شقة ويقومان بنسخ أفلام وهي أفلام عادية وليست خليعة ولا جنسية، وبالرجوع إلى أوراق المعاملة وجد أن هذه الأفلام أفلام خليعة، كما اعترف المدعي عليهم بأن الأجهزة المذكورة تعود له فعليه وحيث الحال ما ذكر فإن المدعى عليهم جميعاً مدانون فيما نسب إليهم من الدعوى ويستحقون التعزير البليغ لما ذكر ولما في ذلك من فساد كبير لترويج هذا الكم الكبير من السيديات، ويتضح من خلال ذلك أن المتهمون لم يقوموا بالاعتراف بحيازتهم لسيديات ممنوعة، أو أي أفلام خليعة، ولذلك فقد عادت المعاملة من محكمة التمييز، حيث أنه بدراسة القرار وصورة ضبطه ولأثنته الاعتراضية تقرر إعادتها لفضيلة حاكمها لملاحظة ما يلي:

(١) إن المدعى عليهم ثلاثة، وهناك أحد الأطراف منهم لم نجد أنه أخذ له جواب على الدعوى.

(٢) كما أن المدعى عليهم لم يعترفوا عن امتلاكهم لأفلام خليعة والمدعي العام لم يجب بشيء عن الأفلام الخليعة، أي أنه لا يوجد اعتراف ولا بينة موصلة كما إن عرض الحكم على المدعى عليهم جاء بصيغة المفرد (عليه) لملاحظة ذلك وللإجابة على أصحاب الفضيلة فإن المدعى عليه كان حاضراً في الجلسة المقررة وسئل عن الدعوى ولكن الموظف اسقط إجابته أثناء الكتابة بدليل

بصمته على الإجابة وإجابته أنه يبيع ويروج الأفلام ولكنها ليست خليعة كما ذكر وإما كون الأفلام خليعة فإن المدعي العام ذكر ذلك إنها خليعة استناداً إلى محضر المشاهدة المرفق ضمن الأوراق

ونتيجة لما سبق فقد تم الحكم عليهم بالسجن سنة وأربعة أشهر استناداً للمادة (٦) من نظام الجرائم المعلوماتية والتي توضح أنه يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يقوم ما شأنه بإنتاج المساس بالنظام العام أو القيم الدينية أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي، ويتضح من خلال ذلك أن هذه العقوبة تتناسب مع قام به المتهمين من ارتكاب جريمة معلوماتية يعاقب عليها قانون مكافحة الجرائم الإلكترونية، وقد استند القاضي في إصدار الحكم إلى اعتراف المتهمين بارتكابهم الجريمة.

القضية السابعة

قضية المال رقم (٣١/٤/٢٩٠)

الحمد لله والصلاة والسلام على من لا نبي بعده:

بصفتي عضو هيئة التحقيق والادعاء العام بدائرة محافظة جدة فإنني أدعي على (أ)، ٢٧ عاماً، سعودي الجنسية، بموجب سجل مدني رقم (×××) مطلق السراح بالكفالة الحضورية لفة رقم (٣٠).

بالإطلاع على خطاب مركز شرطة الشمالية رقم (١٤/٩٠٧٢) وتاريخ ١٤٣١/٨/١٦ هـ ومشفوعاته الشكوى المقدمة من المواطن / ×× المتضمنة أن المدعي عليه قام باختراق موقع مؤسسة الخدمات العربية المتكاملة العائد للمدعي عن طريق استخدام الشبكة المعلوماتية من خلال هواتف ثابتة تعود له تحت اسم مستعار يطلق عليه (عرب فيروس) ومن ثم قام بنقل استضافة موقع المؤسسة إلى صفحات مخترقة وقام بنشر ذلك الفعل في المنتديات الحوارية كموقع (سوالف سوفت) معلناً ذلك صراحة والتشهير بمؤسسته وإلحاق الضرر به، حتى تم استرجاع نطاق المؤسسة بواسطة مكتب (×××) مما سبب له ضرر مادي يقدر بمبلغ مليون ريال سعودي وضرر معنوي

بتشويه سمعة المؤسسة لدى عملائها بأنها لا تستطيع حماية نطاقها الإلكتروني فكيف لها أن تقدم خدمات الحماية لهم وأفاد أن المذكور أرسل له رسائل إلى جواله من عدة جوالات تحتوي على تهديد واعتراقات باختراقه موقع المؤسسة وإنه لا يعرف المذكور من السابق ولا تربطهما أي علاقة وسبب إقدامه على ذلك الفعل لتحقيق الشهرة في المنتديات.

وباستجواب المدعى عليه بداية أنكر ذلك وأفاد أنه يعمل في برامج رسم الخرائط بقاعدة الملك عبدا لله الجوية وأنه لا يعرف المدعي ولم يتعامل مع مؤسسته وليس له علاقة بالاسم المستعار (عرب فيروس) ولا يعرف صاحبه واعترف بأن أرقام الجوازات التي ذكرها المدعي تعود له من السابق ولا يذكر أن كان قد أرسل منها أي رسائل للمدعي، ثم عاد عن ذلك واعترف أن الاسم المستعار (عرب فيروس) كان معروفاً له لفترة من الزمن ثم انتقل إلى شخص آخر وإن من قام بالعبث في موقع مؤسس المدعي ونشر الخبر وتشويه سمعته هو من يستخدم الاسم المستعار (××××××××) مقيم في دولة الإمارات ويملك مؤسسة هناك منافسة لمؤسسة المدعي وقد تعرف عليه من خلال زيارته للمواقع التقنية وأعجب في إمكانياته والمواضيع التي يطرحها وعندما قام باختراق موقع المدعي اقترح اسم معرفه (عرب فيروس) ومعرفات أخرى وأطلق عليهم اسم (فريق الشارة الحمراء).

وانتهى التحقيق إلى توجيه الاتهام للمدعى عليه / (أ) بمخالفة الفقرة الثالثة والخامسة من المادة الثالثة من نظام مكافحة جرائم المعلوماتية بأنه اخترق الموقع الإلكتروني لمؤسسة / الخدمات العربية المتكاملة عن طريق الشبكة المعلوماتية (الإنترنت) ونقل استضافة الموقع إلى صفحات مخترقة والتشهير بها والحق الضرر بمالكها وذلك للأدلة والقرائن التالية:

- ١ - ما جاء في اعترافه باستخدام أرقام الهواتف والجوال التي تم الاختراق عن طريقها وأنها تعود له المدون بدفاتر التحقيق لفة رقم (٧٦,٢٦).
- ٢ - إنكاره معرفته بالمدعى أو بالاسم المستعار الذي يستخدمه هو (عرب فيروس) وإنكاره معرفة موقع مؤسسة المدعي المخترق ثم تراجع عن إنكاره.

٣ - ما جاء في النسخ المسحوبة من الموقع المخترق التي قدمها المدعي، لفة رقم (٦١، ٦٥، ٦٦، ٦٧).

وحيث إن ما قام به المدعي عليه فعل مجرم وفقاً للفقرة (٣، ٥) من الماد الثالثة من نظام مكافحة جرائم المعلوماتية لذا أطلب إثبات ما نسب إليه ومجازاته بالعقوبة المقررة بالمادة الثالثة من ذات النظام (علماً بأن الحق الخاص لازال قائماً).

والله ولي التوفيق،،، عضو هيئة التحقيق والادعاء العام

محقق أول /

التحليل:

يلاحظ من خلال دراسة هذه القضية وتحليلها أنها تتناول ارتكاب جريمة إلكترونية، وذلك من خلال توجيه الاتهام إلى المتهم (أ) حيث تم توجيه الاتهام للمذكور بمخالفة الفقرة الثالثة والخامسة من المادة الثالثة من نظام جرائم المعلوماتية، وذلك من خلال قيام المتهم باختراق موقع مؤسسة ×× عن طريق استخدام الشبكة المعلوماتية من خلال هواتف ثابتة تعود له تحت اسم مستعار يطلق عليه (عرب فيروس) ومن ثم قام بنقل استضافة موقع المؤسسة إلى صفحات مخترقة وقام بنشر ذلك الفعل في المنتديات الحوارية كموقع (سوالف سوفت) معلناً ذلك صراحة والتشهير بمؤسسته وإلحاق الضرر بها، حتى تم استرجاع نطاق المؤسسة بواسطة مكتب محاماة تولى القضية، مما سبب له ضرر مادي يقدر بمبلغ مليون ريال سعودي وضرر معنوي بتشويه سمعة المؤسسة لدى عملائها بأنها لا تستطيع حماية نطاقها الإلكتروني فكيف لها أن تقدم خدمات الحماية لهم.

ومن خلال قيام جهات التحقيق بالبحث والتحري لإثبات قيام المتهم (أ) بارتكاب الجريمة، ومحاولتها لاكتشاف الأدلة التي تثبت قيام وارتكاب المتهم بهذه الجريمة، فقد تباينت الأدلة التالية:

١ - أفاد المدعي أن المدعي عليه (أ) أرسل له رسائل إلى جواله من عدة جوالات تحتوي على تهديد واعترافات باختراقه موقع المؤسسة وإنه لا يعرف المذكور من السابق ولا تربطهما أي علاقة وسبب إقدامه على ذلك الفعل لتحقيق الشهرة في المنتديات.

٢ - من خلال استجواب المدعى عليه بداية أنكر ذلك وأفاد أنه يعمل في برامج رسم الخرائط بقاعدة الملك عبدا لله الجوية وأنه لا يعرف المدعي ولم يتعامل مع مؤسسته وليس له علاقة بالاسم المستعار (عرب فيروس) ولا يعرف صاحبه واعترف بأن أرقام الجوازات التي ذكرها المدعي تعود له من السابق ولا يذكر أن كان قد أرسل منها أي رسائل للمدعي، ثم عاد عن ذلك واعترف أن الاسم المستعار (عرب فيروس) كان معرف له لفترة من الزمن ثم انتقل إلى شخص آخر وإن من قام بالعبث في موقع مؤسس المدعي ونشر الخبر وتشويه سمعته هو من يستخدم الاسم المستعار (xxx) مقيم في دولة الإمارات ويملك مؤسسة هناك منافسة لمؤسسة المدعي وقد تعرف عليه من خلال زيارته للمواقع التقنية وأعجب في إمكانياته والمواضيع التي يطرحها وهو الذي قام باختراق الموقع، واقتحم اسم المعرفة (عرب فيروس)، وأطلق عليهم اسم (فريق الشارة الحمراء). ويتضح من خلال تذبذب أقوال المدعي عليه أنه هو مرتكب الجريمة، وهذا ما أدى إلى الشك فيه، على أنه مرتكب الجريمة.

ونتيجة لذلك فقد، انتهى التحقيق إلى توجيه الاتهام للمدعى عليه (أ) بمخالفة الفقرة الثالثة والخامسة من المادة الثالثة من نظام مكافحة جرائم المعلوماتية، وذلك من خلال اختراقه الموقع الإلكتروني لمؤسسة /xxx عن طريق الشبكة المعلوماتية (الإنترنت) ونقل استضافة الموقع إلى صفحات مخترقة والتشهير بها والحق الضرر بمالكها، وقد تم إثبات ذلك من خلال الأدلة التالية:

١ - ما جاء في اعتراف المدعي عليه باستخدام أرقام الهواتف والجوالات التي تم الاختراق عن طريقها وأنها تعود له، فقد تبين للمحقق من خلال معرفة صاحب ملكية هذه الجوالات من هو مرتكب الجريمة.

٢ - إنكاره معرفته بالمدعى أو بالاسم المستعار الذي يستخدمه هو (عرب فيروس) وإنكاره معرفة موقع مؤسسة المدعي المخترق ثم تراجع عن إنكاره، فمن خلال إنكاره ثم تراجع عن هذا الإنكار، وأدلى بعد ذلك بمعرفته بموقع مؤسسة المدعي، فيدل ذلك على أنه لديه معلومات عن مرتكب الجريمة.

ومن خلال ما تقدم، فإن المدعي عليه، قد قام بارتكاب فعل مجرم وفقاً للفقرة (٣)،
 (٥) من المادة الثالثة من نظام مكافحة جرائم المعلوماتية لذا فإنه يعاقب بالسجن مدة لا تزيد
 عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين نظراً لما يلي:
 ١ - دخوله غير المشروع إلى موقع إلكتروني، لتغيير تصاميم الموقع أو إتلافه أو تعديله
 أو شغل عنوانه.

٢ - التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.
 ويتضح من خلال ذلك أن هذه العقوبة تتناسب مع ما قام به المتهم من ارتكاب
 جريمة معلوماتية من خلال قيام المتهم باختراق موقع مؤسسة عن طريق استخدام الشبكة
 المعلوماتية من خلال هواتف ثابتة تعود له.

القضية الثامنة

قضية المال رقم (٣١/٤/٢٧٦)

الصادر بحق /

(أ)، ٣٠ عاماً، سعودي الجنسية، بموجب بطاقة الأحوال رقم (××××)، بتاريخ
 ١٤/٤/١٤١٧هـ، مصدرها جدة، المقبوض عليه بتاريخ ٢٣/٧/١٤٣١هـ، موقوف
 بسجن محافظة جدة بموجب أمر التوقيف رقم ٤٢٦٥٣ وتاريخ ٢٥/٧/١٤٣١هـ وأمر
 تمديد التوقيف رقم هـ م ٢/٤/٢٦٥٢ في ٢٥/٧/١٤٣١هـ وأمر تمديد التوقيف رقم هـ
 م ٢/٤/٤٤٠٠ وتاريخ ٦/٨/١٤٣١هـ.

(الوقائع)

بالإطلاع على خطاب مدير مركز شرطة البلد رقم (١٠/١/٢٠/٤٣٩٠) وتاريخ
 ٢٥/٧/١٤٣١هـ ومشفوعاته الشكوى المقدمة من مندوب مجموعة سامبا المصرفية
 التجارية المتضمنة قيام المذكور أعلاه باستغلال وظيفته كصراف بفرع البنك بحي البلد
 وتحويل مبلغ مليون ومائة وخمس وعشرون ألف ريال إلى حساب زوجته / ×××× من
 حساب عميل البنك وذلك عن طريق استخدام الرقم الوظيفي السري الخاص به والذي
 بموجبه يقوم بكافة الأعمال المصرفية لوظيفته، وكان تحويل المبلغ المالي على دفعات
 من عام ٢٠٠٨م وأن المذكور قام بعمليات الإيداع والسحب بصور وهمية ولم يجد

البنك أي مستندات لتلك العمليات، فتم القبض على المذكور أعلاه وبقيادته سيارة لكزس ذات الموديل ٢٠٠٩م لوحة رقم (××) عائدة له وذلك من قبل دوريات أمن الطرق بالمدينة المنورة بتاريخ ١٤٣١/٧/٢٣هـ بناء على تعميم مركز شرطة البلد. وقد تم سماع أقوال المتهم من قبل جهة الضبط فأنكر قيامه بذلك وذكر أن التحويلات المالية تمت باستخدام رقمه السري بدون علمه من قبل أشخاص آخرين بالبنك.

(التحقيقات)

باستجواب المتهم / (أ) أفاد أنه كان موظفاً بوظيفة صراف بينك سامبا فرع البلد لمدة خمس سنوات وقدم استقالته قبل شهرين تقريباً من تاريخ القبض عليه لحصوله على وظيفة أفضل ولعدم ترقيته في البنك وأن لديه زوجته المرأة / ×× حساب بالبنك ذاته وبسؤاله عن حساب زوجته أفاد أنه هو من فتح الحساب عن طريق أحد موظفي خدمات العملاء بالبنك وهو من استلم بطاقة الصراف وأدخل رقمها السري وهو من يستخدمها وبسؤاله عن ××× أفاد أنه يعرفه وهو عميل تميز في الفرع الذي يعمل فيه وبمواجهته بالبلاغ الذي تقدم به هذا الشخص لبنك سامبا والذي بناء عليه تقدم البنك بالبلاغ عنه ومفاده أنه تم سحب مبلغ مليون ومائة وسبعين ألف وأربعمائة وثمان وتسعون ريال من حسابه بدون علمه، وبعد أن قام البنك بفحص البلاغ والعمليات التي تمت من قبلك اتضح أنه تم سحب مبلغ مليون ومائة وخمس وعشرون ألف وثلاثمائة وسبعة عشر ريال وأودعت بحساب زوجته وتم أيضاً سحب مبلغ ستة وعشرون ألف ومائتين ريال أودعت بحساب المرأة / ×××، أنكر قيامه بذلك ونفى علاقته بالمرأة ××× وعلمه بها.

وبمواجهته بأن العمليات تمت على مدار عامين وجميعها باستخدام الرقم السري الخاص به كموظف أفاد أنه بسبب ثقته بزملائه أصبح يترك جهازه مفتوح ويغفل عنه وأنه من الممكن أن يكون مدير العمليات استخدمه بدون علمه، وبسؤاله عن حساب زوجته ومن يقوم باستخدامه وكيف لم يلاحظ وجود مبالغ لا تخصها فيه أفاد أنه من يقوم بالسحب منه وأنه لم يلاحظ في الحساب ما يثير شكوكه، وبسؤاله عن من قام بتحويل الأموال من حساب زوجته إلى حساب المرأة / ××× أفاد أنه ليس هو وممكن

يكون مدير العمليات في البنك وبسؤاله عن سبب تحويل مدير العمليات لهذه المبالغ لحساب زوجتك أفاد أنه قام بذلك لكي يتم تثبيت الاتهام عليه، وبسؤاله عن عدم إبلاغه عن الأموال المودعة بحساب زوجه وإنما تم صرفها من قبله أفاد أنه لم يصرف إلا من الأموال التي تخصه أما الأموال الأخرى فلم يصرف منها رغم أنها بحساب واحد! وبسؤاله عن سبب قبولهم لاستقالته رغم وجود خطة مدبره للإيقاع به كما يزعم أفاد أن ذلك من ضمن الخطة التي تدبر ضده، وبسؤاله عن الأسماء الوهمية التي تم إتمام عمليات التحويل الوهمية بأسمائهم أفاد أنهم موظفين في البنك استقال أحدهم وبمواجهته بإيداع والده مبلغ خمسمائة ألف ريال في حساب زوجته على دفعتين وذلك رغبة منه في التسوية أفاد أنه لا يعلم لماذا فعل والده ذلك. وبالبحث عن حالته الجنائية لم يعثر له على سوابق.

(الاتهام)

وانتهى التحقيق إلى توجيه الاتهام للمتهم/ (أ) بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية وذلك بالاستيلاء على مبلغ مليون ومائة وسبعين ألف وأربعمائة وثمانية وتسعين ريال من الحسابات البنكية العائدة لأحد عملاء بنك سامبا وذلك أبان عمل المتهم بوظيفة صراف في البنك مستخدماً رقمه الوظيفي السري وتحويله لحساب زوجته وحسابات أخرى وذلك للأدلة والقرائن التالية:

١ - ما جاء في البلاغ المقدم من بنك سامبا لدى مدير شرطة محافظة جدة لفة (١٣).

٢ - ما جاء في الشكوى المقدمة من قبل العميل ×× لإدارة البنك لفة (١٢).

٣ - كون المبالغ المستولى عليها تم إيداعها بحساب زوجته قرينه على قيامه بذلك وخصوصاً أن بطاقة الصراف لديه وهو المستفيد من الحساب.

٤ - قيام المتهم باستعمال بطاقة الصراف الخاصة بحساب زوجته والسحب منه دون اعتراضه على مبالغ ضخمة به لا تخصه.

٥ - ضخامة المبالغ المصروفة من الحساب ومعظمها لسلع استهلاكية ومطاعم راقية لا تتناسب مع دخله وزوجته.

٦ - إيداع والده لمبلغ خمسمائة ألف ريال في حساب زوجة المتهم قرينه على ارتكاب المتهم ذلك الجرم والرغبة في تسوية الموضوع ودياً لفه (٦)

(الطلبات)

وحيث أن ما قام به المتهم المذكور فعل مجرم وفقاً للمادة الرابعة من نظام مكافحة جرائم المعلوماتية مما يتعين معه إحالته للمحكمة الجزئية بمحافظة جدة استناداً للمادة (١٢٦) من نظام الإجراءات الجزائية لإثبات ما نسب إليه ومعاقبته بالعقوبة المقررة في المادة الرابعة من نظام مكافحة الجرائم المعلوماتية، (علماً بأن الحق الخاص لا زال قائماً). والله ولي التوفيق،،،

عضو هيئة التحقيق والادعاء العام

محقق أول /

التحليل:

يتبين من خلال دراسة هذه القضية، أنها مرتبطة بارتكاب جريمة معلوماتية، وذلك من خلال توجيه الاتهام للمذكور (أ) بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية، وذلك من خلال فحص الشكوى المقدمة من مندوب مجموعة سامبا المصرفية التجارية المتضمنة قيام المذكور أعلاه باستغلال وظيفته كصراف بفرع البنك بحي البلد وتحويل مبلغ مليون ومائة وخمس وعشرون ألف ريال إلى حساب زوجته من حساب أحد عملاء التميز وذلك عن طريق استخدام الرقم الوظيفي السري الخاص به والذي بموجبه يقوم بكافة الأعمال المصرفية لوظيفته، وكان تحويل المبلغ المالي على دفعات من عام ٢٠٠٨م وأن المذكور قام بعمليات الإيداع والسحب بصور وهمية ولم يجد البنك أي مستندات لتلك العمليات، فتم القبض على المتهم (أ) وبقيادته سيارة لكزس ذات الموديل ٢٠٠٩م عائدة له وذلك من قبل دوريات أمن الطرق بالمدينة المنورة بناء على تعميم مركز شرطة البلد.

ومن خلال محاولة جهة التحقيق إثبات الجريمة على المتهم من خلال التحري على أدلة الجريمة، فقد تم سماع أقوال المتهم من قبل جهة الضبط فأنكر قيامه بذلك وذكر أن التحويلات المالية تمت باستخدام رقمه السري بدون علمه من قبل أشخاص

آخرين بالبنك، حيث أفاد أنه كان موظفاً بوظيفة صراف ببنك سامبا فرع البلد لمدة خمس سنوات وقدم استقالته قبل شهرين تقريباً من تاريخ القبض عليه لحصوله على وظيفة أفضل ولعدم ترقيته في البنك وأن لديه وزوجته حساب بالبنك ذاته وبسؤاله عن حساب زوجته أفاد أنه هو من فتح الحساب عن طريق أحد موظفي خدمات العملاء بالبنك وهو من استلم بطاقة الصراف وأدخل رقمها السري وهو من يستخدمها.

وعند سؤاله أيضاً عن العميل الذي سحب المبلغ من حسابه أفاد أنه يعرفه وهو عميل تميز في الفرع الذي يعمل فيه وبمواجهته بالبلاغ الذي تقدم به هذا الشخص لبنك سامبا والذي بناء عليه تقدم البنك بالبلاغ عنه ومفاده أنه تم سحب مبلغ مليون ومائة وسبعين ألف وأربعمائة وثمان وتسعون ريال من حسابه بدن علمه، وبعد أن قام البنك بفحص البلاغ والعمليات التي تمت من قبلك اتضح أنه تم سحب مبلغ مليون ومائة وخمس وعشرون ألف وثلاثمائة وبسبعة عشر ريال وأودعت بحساب زوجة المتهم، أنكر قيامه بذلك ونفى علاقته بأي شيء من قبيل ذلك.

كما قامت جهة التحقيق أيضاً بمواجهته بأن العمليات تمت على مدار عامين وجميعها باستخدام الرقم السري الخاص به كموظف أفاد أنه بسبب ثقته بزملائه أصبح يترك جهازه مفتوح ويغفل عنه وأنه من الممكن أن يكون مدير العمليات استخدمه بدون علمه، وبسؤاله عن حساب زوجته ومن يقوم باستخدامه وكيف لم يلاحظ وجود مبالغ لا تخصها فيه أفاد أنه من يقوم بالسحب منه وأنه لم يلاحظ في الحساب ما يثير شكوكه، وبسؤاله عن من قام بتحويل الأموال من حساب زوجته إلى حساب المرأة أفاد أنه ليس هو ويمكن يكون مدير العمليات في البنك وبسؤاله عن سبب تحويل مدير العمليات لهذه المبالغ لحساب زوجتك أفاد أنه قام بذلك لكي يتم تثبيت الاتهام عليه، وبسؤاله عن عدم إبلاغه عن الأموال المودعة بحساب زوجه وإنما تم صرفها من قبله أفاد أنه لم يصرف إلا من الأموال التي تخصه أما الأموال الأخر فلم يصرف منها رغم أنها بحساب واحد، وعند سؤال المتهم عن سبب قبول البنك لاستقالته رغم وجود خطة مدبره للإيقاع به كما يزعم أفاد أن ذلك من ضمن الخطة التي تدبر ضده، وبمواجهته بإيداع

والده مبلغ خمسمائة ألف ريال في حساب زوجته على دفعتين وذلك رغبة منه في التسوية أفاد أنه لا يعلم لماذا فعل والده ذلك.

ومن خلال ما تقدم، فقد انتهى التحقيق إلى توجيه الاتهام للمتهم (أ) بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية وذلك بالاستيلاء على مبلغ مليون ومائة وسبعين ألف وأربعمائة وثمانية وتسعين ريال من الحسابات البنكية العائدة لأحد عملاء بنك سامبا وذلك أثناء وقت عمل المتهم بوظيفة صراف في البنك مستخدماً رقمه الوظيفي السري وتحويله لحساب زوجته وحسابات أخرى وذلك نظراً لوجود الأدلة التالية التي استند عليها المحقق، وهي كما يلي:

١ - ما جاء في البلاغ المقدم من بنك سامبا لدى مدير شرطة محافظة جدة، وما جاء في الشكوى المقدمة من قبل العميل لإدارة البنك بتحويل مبلغ مليون ومائة وسبعين ألف وأربعمائة وثمانية وتسعين ريال من الحسابات البنكية العائدة للعميل مقدم الشكوى.

٢ - كون المبالغ المستولى عليها تم إيداعها بحساب زوجة المتهم، وتم توجيه الاتهام له خصوصاً بعد أن اعترف أن بطاقة الصراف التي تخص زوجته لديه وهو المستفيد من الحساب.

٣ - قيام المتهم باستعمال بطاقة الصراف الخاصة بحساب زوجته والسحب منه دون اعتراضه على مبالغ ضخمة به لا تخصه، مع العلم أنه يجب أن يلاحظ أن هذا الحساب به مبالغ مالية عالية لا تخصه، فكان يجب عليه أن يقوم بالإبلاغ عن ذلك.

٤ - ضخامة المبالغ المصروفة من الحساب ومعظمها لسلع استهلاكية ومطاعم راقية لا تتناسب مع دخل المتهم وزوجته، حيث تبين لجهة التحقيق من خلال فحص حساب زوجة المتهم، أن هناك مبالغ ضخمة يتم صرفها على سلع استهلاكية ومطاعم راقية لا تتناسب مع دخل المتهم وزوجته.

ومن خلال ما تقدم، يطبق على هذا المتهم أحكام المادة الرابعة من نظام مكافحة الجريمة الإلكترونية، حيث أوضحت هذه المادة أنه يعاقب بالسجن مدة لا تزيد

على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين كل شخص يقوم بالاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، وأيضاً الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات.

القضية التاسعة

قضية المال رقم (٣١/٤/١٢٨) المسجلة جنائياً برقم (٣١/٢٠٦/٠٥٤٣)

الحمد لله والصلاة والسلام على رسول الله.. وبعد:

فبصفتي عضو هيئة التحقيق والادعاء العام بمحافظة جدة، أدعي على:

(أ)، ٣١ عاماً، سعودي الجنسية بموجب سجل مدني رقم (×××)، المقبوض عليه بتاريخ ١٤٣١/٠٣/٢١ هـ، والموقوف في سجون محافظة جدة بموجب أمر تمديد توقيف رقم هـ م ١٨٣٤/٤/٢ وتاريخ ١٤٣١/٠٣/٢٤ هـ لمدة خمس وثلاثين يوماً اعتباراً من تاريخ ١٤٣١/٠٣/٢٦ هـ.

(بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية)

حيث إنه بتاريخ ١٤٣١/٠٣/٢١ هـ قبض على المدعي عليه المذكور إثر بلاغ المدعي ××××× عن تلقيه مكالمات هاتفية من الرقم (×××) أخبره خلالها المتصل بأنه موظف في البنك الأهلي وطلب منه تحديث بياناته الشخصية وذلك بالتوجه لأقرب جهاز صراف آلي وأكد له بأنه سيرشده للقيام بذلك وأضاف المدعي بأنه توجه على إثر ذلك لجهاز الصراف وحينها طلب المتصل منه الدخول إلى موقع الخدمات الإلكترونية وإجراء بعض العمليات ثم زوده برقم من أربع خانات وبعدها طلب منه عدم استخدام الحساب مدة ثلاثة أيام وأنهى الاتصال بينهما عقب ذلك شعر المدعي بتعرضه لعملية احتيال ونصب فقام بالتأكد من حسابه فوجد عمليتي تحويل إحداهما إلى حساب المدعي عليه المذكور بمبلغ ثمانون ألف ريال والأخرى إلى حساب آخر بمبلغ عشرون ألف ريال.

وباستجواب المدعى عليه المذكور أفاد بأنه تلقى حوالة بمبلغ ثمانون ألف ريال؛ ذلك إثر طلب صديق له يدعى ××× (جـرى فرز أوراق مستقلة له) - السجن في سجن الدمام - رقم حسابه ليتمكن من تلقي مبلغ مالي له من شخص، وأضاف بأنه عندما تم تحويل المبلغ إلى حسابه طلب منه صديقه المذكور سحب خمس وستين ألف ريال وتسليمها لأخيه ×××× (جـرى فرز أوراق مستقلة له)، كما طلب منه تحويل خمس عشرة ألف ريال إلى حساب لا يذكر رقمه ولا اسم صاحبه، وأنه فعلاً قام بجميع ذلك، وليس لديه ما يثبت أقواله، وبأنه لا توجد بينه وبين المدعى أي علاقة، وبرر سبب سرعة تصرفه بالمبلغ: بالسحب والتحويل عقب تحويل المبلغ من حساب المدعى إلى حسابه؛ لقرب البنك من منزله وعدم وجود ازدحام وقت إجراءاته للعمليات في البنك.

وبالبحث عن معلومات رقم الجوال المشار إليه تبين أنه يعود للمدعو: ××× (جـرى فرز أوراق مستقلة) واتضح وجود مكالمات بين الرقم والمدعى بتاريخ الواقعة ووقتها وعقب تلك المكالمات وورد اتصال من الرقم المشار إليه إلى البنك الأهلي التجاري.

وبالبحث عن معلومات الأشخاص المستفيدين من المبلغ المالي المحول من حساب المدعى تبين أن المدعى عليه المذكور تلقى حوالة من حساب المدعى بمبلغ ثمانون ألف ريال وقام بسحب خمس وستين ألف ريال منها، وتحويل خمس عشرة ألف ريال إلى حساب المواطن ×××× (جـرى فرز أوراق مستقلة له) كما تبين تلقي المواطن ×××××× (جـرى فرز أوراق مستقلة له) لمبلغ عشرون ألف ريال من حساب المدعى، وقام بتسديد فواتير موبايلي وشحن جوالات بمبلغ ثمانية آلاف وخمسون ريالاً، كما قام بتحويل اثني عشر ألف ريال إلى المواطن ××× (جـرى فرز أوراق مستقلة له) الذي بدوره قام بسحبها نقداً.

وبالبحث عن الحالة الجنائية للمدعى عليه اتضح عدم وجود سوابق جنائية عليه. وقد انتهى التحقيق إلى توجيه الاتهام للمدعى عليه / ×××× بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية لقيامه بالاستيلاء لنفسه على مال عن طريق الاحتيال، وذلك للأدلة والقرائن التالية:

- ١ - ما جاء في اعتراف المدعى عليه تحقيقاً المدون على ص (٣-٤، ١٠-١٢) من دفتر التحقيق الأول المرفق لفة رقم (٣٤) المتضمن تلقيه المبلغ المالي في حسابه بعلمه وتصرفه فيه بعد ذلك بالسحب لنفسه والتحويل لشخص آخر.
 - ٢ - عجز المدعى عليه عن إثبات سبب شرعي أو مسوغ نظامي لوجود المبلغ المالي في حسابه؛ وتصرفه بعد ذلك فيه.
 - ٣ - ما جاء في خطاب مؤسسة النقد العربي السعودي المرفق لفة رقم (٢٣) المتضمن تلقي المدعى عليه بمبلغ ثمانون ألف ريال من حساب المدعي وسحبه خمسة وستين ألف ريال وتحويله خمس عشرة ألف ريال لشخص آخر.
 - ٤ - سرعة تصرف المدعى عليه بالمبلغ المالي عقب تحويله من حساب المدعي بالسحب والتحويل.
- وحيث إن ما أقدم عليه المدعى عليه / (أ) وهو بكامل أهليته المعتبرة شرعاً يعد فعلاً محرماً شرعاً ومجرماً نظاماً وفقاً للمادة الرابعة من نظام مكافحة جرائم المعلوماتية؛ لذا أطلب إثبات ما أسند إليه والحكم عليه بالعقوبة المقررة وفق المادة الرابعة من النظام ذاته، (علماً بأن الحق الخاص لا زال قائماً).
- والله الموفق،،،

عضو هيئة التحقيق والإدعاء العام

التحليل:

يلاحظ من خلال الإطلاع على هذه القضية أنها تتعلق بتهمة مخالفة نظام مكافحة جرائم المعلوماتية بالاستيلاء للمتهم على مال بطريق الاحتيال)، وذلك بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية، ومن خلال محاولة جهات التحقيق التأكد من قيام المتهم بارتكاب الجريمة، ومحاولة إثبات أن المدعي عليه هو من قام بارتكاب الجريمة فقد قبض على المدعى عليه المذكور إثر بلاغ المدعي عن تلقيه مكالمة هاتفية من المدعي عليه أخبره خلالها المتصل بأنه موظف في البنك الأهلي

وطلب منه تحديث بياناته الشخصية وذلك بالتوجه لأقرب جهاز صراف آلي وأكد له بأنه سيرشده للقيام بذلك وأضاف المدعي بأنه توجه على إثر ذلك لجهاز الصراف وحينها طلب المتصل منه الدخول إلى موقع الخدمات الإلكترونية وإجراء بعض العمليات ثم زوده برقم من أربع خانات وبعدها طلب منه عدم استخدام الحساب مدة ثلاثة أيام وعقب الاتصال بين المدعي والمدعي عليه شعر المدعي بتعرضه لعملية احتيال ونصب فقام بالتأكد من حسابه فوجد عمليتي تحويل إحداهما إلى حساب المدعي عليه المذكور بمبلغ ثمانون ألف ريال والأخرى إلى حساب آخر بمبلغ عشرون ألف ريال.

ومن خلال قيام جهات التحقيق باستجواب المدعي عليه (أ)، أفاد بأنه تلقى حوالة بمبلغ ثمانون ألف ريال؛ ذلك إثر طلب صديق له مسجون في سجن الدمام رقم حسابه ليتمكن من تلقي مبلغ مالي له من شخص، وأضاف بأنه عندما تم تحويل المبلغ إلى حسابه طلب منه صديقه المذكور سحب خمس وستين ألف ريال وتسليمها لأخيه، كما طلب منه تحويل خمس عشرة ألف ريال إلى حساب لا يذكر رقمه ولا اسم صاحبه، وأنه فعلاً قام بجميع ذلك، وليس لديه ما يثبت أقواله، وبأنه لا توجد بينه وبين المدعي أي علاقة، وبرر سبب سرعة تصرفه بالمبلغ بالسحب والتحويل عقب تحويل المبلغ من حساب المدعي إلى حسابه؛ لقرب البنك من منزله وعدم وجود ازدحام وقت إجرائه للعمليات في البنك.

وقد قامت جهات التحقيق بالبحث عن معلومات رقم الجوال المشار إليه فقد اتضح وجود مكالمات بين الرقم والمدعي بتاريخ الواقعة ووقتها وعقب تلك المكالمات وورود اتصال من الرقم المشار إليه إلى البنك الأهلي التجاري. وبالبحث عن معلومات الأشخاص المستفيدين من المبلغ المالي المحول من حساب المدعي تبين أن المدعي عليه المذكور تلقى حوالة من حساب المدعي بمبلغ ثمانون ألف ريال وقام بسحب خمس وستين ألف ريال منها، وتحويل خمس عشرة ألف ريال إلى أحد الحسابات الأخرى. ونتيجة لما قام به المدعي عليه من عمليات تحويل فقد انتهى التحقيق إلى توجيه الاتهام للمدعي عليه بمخالفة المادة الرابعة من نظام مكافحة جرائم المعلوماتية لقيامه

بالاستيلاء لنفسه على مال عن طريق الاحتيال ويرجع ذلك إلى الأدلة التالية والتي وضحتها عضو هيئة التحقيق وهي كما يلي:

١ - ما جاء في اعتراف المدعى عليه المتضمن تلقية المبلغ المالي في حسابه بعلمه وتصرفه فيه بعد ذلك بالسحب لنفسه والتحويل لشخص آخر، حيث أقر بأن عملية التحويل تمت بعلمه عن طريق تلبيته لرغبة أحد أصدقائه عندما طلب رقم حسابه، وعلى أثر ذلك قام بإعطائه الرقم، وتمت عليه عملية التحويلات.

٢ - عجز المدعى عليه عن إثبات سبب شرعي أو مسوغ نظامي لوجود المبلغ المالي في حسابه؛ وتصرفه بعد ذلك فيه، حيث أقر بأن ذلك يرجع إلى طلب صديقه منه رقم الحساب ليستخدمه في عملية تحويل متلي تأتي إليه من رقم آخر.

٣ - ما جاء في خطاب مؤسسة النقد العربي السعودي وبفيد بتلقي المدعى عليه بمبلغ ثمانون ألف ريال من حساب المدعي وسحبه خمس وستين ألف ريال وتحويله خمس عشرة ألف ريال لشخص آخر، كما جاء في الخطاب أيضاً سرعة تصرف المدعى عليه بالمبلغ المالي عقب تحويله من حساب المدعي بالسحب والتحويل، وقد برر المدعي بأن ذلك يرجع إلى قرب البنك منه، وهو ما جعله يقوم بعمليات التحويل والسحب بسرعة..

ونتيجة لما قامت به هيئة التحقيق من إثبات الجريمة على المدعي عليه (أ)، وهو بكامل أهليته المعتبرة شرعاً يعد فعلاً محرماً شرعاً ومجرماً نظاماً وفقاً للمادة الرابعة من نظام مكافحة جرائم المعلوماتية؛ يطبق على هذا المتهم أحكام المادة الرابعة من نظام مكافحة الجريمة الإلكترونية، حيث أوضحت هذه المادة أنه يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين كل شخص يقوم بالاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، وأيضاً الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية أو

بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما
تنتجه من خدمات.

القضية العاشرة

قرار اتهام رقم هـ ر ١/٤/..... لعام..... ١٤هـ في قضية جريمة معلوماتية

رقم (.....) المتهم فيها كل من:

١ - ٢٧ سنة سعودي الجنسية بموجب السجل المدني رقم (.....) مطلق سراحه بالكفالة.

٢ - ٢٥ سنة سعودي الجنسية بموجب السجل المدني رقم (.....).

٣ - ٢٤ سنة بموجب السجل المدني رقم (.....) مطلق سراحه بالكفالة.

الحمد لله وحده وبعد:

بتاريخ...../...../..... ١٤هـ حضر لمركز شرطة.....المبلغ /..... سعودي الجنسية مبلغاً عن قيام أحد الأشخاص بالدخول للشبكة العنكبوتية (الإنترنت) لحساب شقيقه /..... المنوم في مستشفى الملك فهد (رعاية طويلة الأمد) ودخوله لحسابه الجاري والاستثماري وبيع جميع الأسهم وتحويل المبالغ إلى الثاني والثالث.

وبسماع أقوال الأول:..... أنكر قيامه بدخول حساب المدعو/..... وبمواجهته بأقوال زميله وكذلك أخذ بطاقة صراف زميله/..... أفاد بأنه قام بذلك بناء على طلب ××× لكي يقوم بسحب مبلغ مالي له وبإعادة سماع الأقوال أصر على أقواله السابقة. وبسماع أقوال الثاني:..... أنكر قيامه بدخول لحساب وكذلك معرفته بالمدعو /..... وأفاد أنه سبق وأن حضر له زميله الأول..... وأخبره بأن أحد أقاربه سوف يقوم بتحويل مبالغ مالي وأنه لا يوجد لديه حساب في بنك..... وطلب منه بطاقة الصراف الآلي ورقم حسابه في..... وأعطاه إياه.

وبسماع أقوال الثالث:..... أفاد بأنه سبق وأن ورد له حوالات على حسابه في مصرف الراجحي من حساب زميله الأول /..... ولا يعلم عنها شيء كون المبلغ حول من حساب..... إلى حسابه ثم تحولت مباشرة إلى حساب الأول..... في نفس الوقت.

وبالإطلاع على كشف دراسة حساب المتهم الثاني /..... تبين أن جميع العمليات التي استفاد منها نفذت عن طريق الإنترنت حسب المرفق الـ (IP ADDRESS) ولم يتضح للثالث أي حساب في بنك.....

وبالإطلاع على الحساب الثالث..... تبين وجود حوالات من حسابه إلى حساب الأول /..... بمبالغ مختلفة.

ولما أشير إليه

أقرر توجيه الاتهام ل..... ويتواطؤ الثاني والثالث بارتكاب جريمة معلوماتية وذلك بالدخول إلى البيانات البنكية له في الاستيلاء على مبلغ () عن طريق الإنترنت دون مسوغ نظامي المعاقب عليها بموجب المادة ٢/٤ من نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/١٧) وتاريخ ١٤٢٨/٣/٨هـ.

وذلك للأدلة والقرائن التالية

- ١- ما ورد في تقرير مؤسسة النقد العربي السعودي لفة رقم ().
 - ٢- وجود حوالات صادرة من الأول على حساب الثاني في بنك..... مما يثبت وجود علاقة بينهما في الاستيلاء على المبالغ المالية العائدة للمبلغ.
 - ٣- إقرار المتهم الثاني بطلب الأول بطاقة الصراف ورقم حسابه في بنك..... وإجراء عمليات عليها.
- وحيث أن ما أقدم عليه المذكور فعل مجرم ومعاقب عليه نظاماً ما يستدعي إحالته إلى المحكمة الجزئية لإثبات ما اسند إليه والحكم عليه بالعقوبة المنصوص عليها في المادة (٢/٤) من نظام مكافحة الجرائم المعلوماتية المشار إليه علماً بأن الحق الخاص ما زال قائماً.

وبالله التوفيق،،، عضو هيئة التحقيق والادعاء العام

المحقق/

التحليل:

بالنظر إلى هذه القضية يلاحظ أنها ترتبط بالجريمة الإلكترونية، وذلك من خلال تناولها وعرضها لجريمة الاعتداء على الأموال عن طريق الأنظمة الإلكترونية الحديثة، حيث يتضح من خلال تفاصيل هذه القضية أنها تمت من خلال بلاغ المدعي عن المتهمين بالدخول للشبكة العنكبوتية (الإنترنت) لحساب شقيقه المنوم في مستشفى الملك فهد (رعاية طويلة الأمد) ودخوله لحسابه الجاري والاستثماري وبيع جميع الأسهم وتحويل المبالغ إلى المتهم الثاني والثالث.

وقد قامت جهة التحقيق بالتحري من أجل محاولة إثبات الجريمة على المتهمين من قبل المدعي، ولذلك فقد قامت جهة التحقيق بمواجهة المتهم الأول بأقوال زميله وكذلك أخذه لبطاقة صراف زميله، وقد أفاد بأنه قام بذلك بناء على طلب أحد زملائه لكي يقوم بسحب مبلغ مالي له وبإعادة سماع الأقوال أصر على أقواله السابقة، وبسماع أقوال المتهم الثاني أنكر قيامه بدخول لحساب وكذلك معرفته بالمدعي، وأفاد أنه سبق وأن حضر له زميله الأول وأخبره بأن أحد أقاربه سوف يقوم بتحويل مبالغ مالي وأنه لا يوجد لديه حساب في بنك وطلب منه بطاقة الصراف الآلي ورقم حسابه وأعطاه إياه، وبسماع أقوال المتهم الثالث أفاد بأنه سبق وأن ورد له حوالات على حسابه في مصرف الراجحي من حساب زميله الأول ولا يعلم عنها شيء كون المبلغ حول من حساب إلى حسابه ثم تحولت مباشرة إلى حساب في نفس الوقت، وبالإطلاع على كشف دراسة حساب للمتهم الثاني تبين أن جميع العمليات التي استفاد منها نفذت عن طريق الإنترنت، وبالإطلاع على الحساب الخاص بالمتهم الثالث تبين وجود حوالات من حسابه إلى حساب الأول بمبالغ مختلفة.

ونتيجة لذلك فقد أقرت جهة التحقيق بأن ما قام به المتهمون فعل مجرم ومعاقب عليه نظاماً ما يستدعي إحالته إلى المحكمة الجزئية لإثبات ما أسند إليه والحكم عليه بالعقوبة المنصوص عليها في المادة (٢/٤) من نظام مكافحة الجرائم المعلوماتية حيث أوضحت هذه المادة أنه يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين كل شخص يقوم

بالاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، وأيضاً الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات.

وتنفذ عقوبة هذه المادة على المتهمين طبقاً للأدلة التالية:

١- ما ورد في تقرير مؤسسة النقد العربي السعودي عن وجود حوالات صادرة من المتهم الأول على حساب المتهم الثاني مما يثبت وجود علاقة بينهما في الاستيلاء على المبالغ المالية العائدة للمبلغ.

٢- إقرار المتهم الثاني بطلب الأول بطاقة الصراف ورقم حسابه في بنك وإجراء عمليات عليها، ولذلك فإن إقرار المتهم على نفسه، يؤكد إثبات الاتهام الموجه إليه، وذلك من خلال عجز المتهم المذكور عن إثبات سبب شرعي، أو مسوغ نظامي لوجود المبلغ المالي في الحساب؛ وتصرفه فيه بالسحب والتحويل.

ومن خلال تلك الأدلة الموضحة، يتضح أن العقوبة التي تقرها المادة الرابعة هي التي تتناسب مع المتهمين الثلاثة، نظراً لأنها توضح وصول المتهمين دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات.

الفصل السادس

ملخص نتائج الدراسة والتوصيات والمقترحات

الفصل السادس

نتائج الدراسة والتوصيات

آمل وأدعو الله سبحانه وتعالى أن تكون هذه الدراسة قد وفقت في تحقيق أهدافها، التي تتمثل أهميتها في أنها تكمن في مراجعة النصوص النظامية التي تجرم الاستخدام غير المشروع للحاسب الآلي وملحقاته وشبكات الإنترنت من خلال تصنيف هذه الجرائم وتحديد العقوبات المترتبة عليها في النظام السعودي، وفي ما تقدمه هذه النصوص من دعم في مجال مكافحة الجرائم الإلكترونية والتصدي لها. والإسهام في عرض وتحليل آليات إثبات الجريمة الإلكترونية، وتساهم في تبصير رجال القضاء والمحامين على أهمية التأكد من وقوع الجريمة الإلكترونية وإثبات حدوثها ومن ثم إدانة المتهم بارتكابها.

وقد توصلت هذه الدراسة إلى العديد من النتائج والتوصيات التي اتضحت من خلال تحليل وتفسير البيانات التي تم الحصول عليها، وفي هذا الفصل سيتم عرض ملخص لأهم النتائج التي توصلت إليها إلى جانب مجموعة من التوصيات التي من خلال هذه النتائج، وذلك على النحو التالي:

أولاً: النتائج:

هناك العديد من النتائج التي توصلت إليها هذه الدراسة، وقبل عرض هذه النتائج لابد من إيضاح أن ما نتوصل إليه من نتائج تتعلق بالتقنية مثل إثبات الجرائم الإلكترونية تشكل صعوبة ما لأنها متغيرة ومتطورة، وما نتوصل إليه من نتائج الآن ربما يتغير مستقبلاً بحكم طبيعة الجريمة الإلكترونية المرتبطة بالتقنية التي تتطور بشكل كبير، ويمكن إيجاز هذه النتائج كما يلي:

- ١ - تتسم الجريمة الإلكترونية بصعوبة اكتشافها، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة الإلكترونية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية،

كما إن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، إذ أن الجريمة الإلكترونية جريمة عابرة للدول (دولية).

٢ - يعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية، ويزداد الإثبات صعوبة في الجرائم الإلكترونية، حيث أن اكتشاف الجريمة الإلكترونية أمر ليس بالسهل، وفي حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كثير من الصعاب مما يستلزم الكثير من الجهد والخبرة الفنية.

٣ - هناك نقص في الخبرة الفنية والتقنية لدى الشرطة وجهات الإدعاء والقضاء، وهذا يشكل عائقاً أساسياً أمام إثبات الجريمة الإلكترونية، ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والإنترنت، ونتيجة لنقص الخبرة والتدريب كثيراً ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة الإلكترونية.

٤ - إن الجريمة الإلكترونية قد تكون جزءاً من جريمة تقليدية، بمعنى أن تكون هناك جريمة تقليدية تضم جانب إلكتروني، لا سيما في ظل ارتباط الناس بالتقنيات الحديثة التي بدأت تنتشر بشكل كبير وأهمها الحاسبات الآلية والهواتف الذكية، وقد تكون جريمة إلكترونية مستقلة.

٥ - تتطلب طبيعة الجريمة الإلكترونية بصفة عامة أساليب غير تقليدية في التحقيق لاكتشاف الدليل الرقمي ودعمه من قبل الفنيين المختصين، وذلك يستدعي اتخاذ إجراءات سريعة؛ لأن الدليل الإلكتروني غير مادي، ويمكن التخلص من أية أدلة أو آثار من قبل مرتكبي الجرائم الإلكترونية، كما تختلف أساليب تلقي البلاغ وإجراء المعاينة والقيام بالتحريات والتفتيش والاستجواب عنها في الجرائم التقليدية نظراً لطبيعة الجرائم الإلكترونية وخصائصها.

٦ - تواجه طرق التحقيق في إثبات الجريمة الإلكترونية صعوبات متعددة، حيث تستدعي هذه الطرق في المقام الأول اكتشاف الجريمة الإلكترونية، ومحلها، وبيئتها، ومن ثم البلاغ عنها، وأخذ إذن الجهات المختصة قبل القيام بالمعاينة

والتفتيش للموقع أو الجهاز المشتبه به، وذلك للبحث عن الدليل الرقمي الإلكتروني بالطرق الفنية، ومن ثم إجراء التحريات، التي تساعد في عملية الإثبات.

٧ - تتسم الجرائم ذات الصلة بالحاسب الآلي، بحدثة أساليب ارتكابها، وسرعة تنفيذها، وسهولة إخفائها، ودقة وسرعة محو آثارها. هذه الخصائص العامة تقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها، وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها.

٨ - تعتبر علانية التحقيق في الجريمة الإلكترونية من الضمانات اللازمة لتوافر العدالة، ولهذا فالعلانية في الجريمة الإلكترونية لا يقتصر فيها الأمر على وضع الاطمئنان في قلب المتهم، بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلاً للشك أو الخضوع تحت التأثير، كما أن فيها اطمئناناً للجمهور على أن الإجراءات تسير في طرق طبيعية.

٩ - تمثل الشهادة أهمية كبيرة في إثبات الجريمة الإلكترونية في المواد الجزائية فهي ترد على وقائع مادية وترشد القاضي إلى تحري قيمتها ولذا يقال أن الشهادة عماد الإثبات والشهود عيون المحكمة وآذانها، في إثبات الجريمة، حيث يكون غالباً للشهادة أثناء التحقيق أثر كبير فيما يتعلق بالبراءة والإدانة ولها أهميتها في الكشف عن الأدلة التي تساعد في إثبات الجريمة الإلكترونية.

١٠ - تساعد الخبرة الفنية في إثبات الجريمة الإلكترونية، حيث تكمن أهمية الخبرة في أنها تنير الطريق للقاضي الذي يهتدي به لتحقيق العدالة لا سيما في المجال الجنائي، لذا فقد اهتمت لقوانين المختلفة بأهمية الاستعانة بالخبراء للمحقق، ولم يحظر كل من القانونيين على المحاكم أن تستعين بالخبراء وبالتالي فإنه يجوز دائماً للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم.

١١ - يعتبر صعوبة ظهور الدليل المادي من أهم المعوقات التي تواجه إثبات الجريمة الإلكترونية، فالدليل المادي للجريمة الإلكترونية يكون عن طريق ارتكاب الجريمة بواسطة الحاسب الآلي، حيث تتم الجريمة في بيئة أو إطار، لا علاقة له بالأوراق أو المستندات، أو شبكة المعلومات الدولية، ويمكن للجاني عن طريق (نبضات اليكترونية)، لا ترى، العبث في بيانات الحاسب أو برامجه، وذلك في وقت قياسي قد يكون جزءاً من الثانية، وهذا يعد من أهم المعوقات التي تواجه إثبات الجريمة الإلكترونية.

١٢ - يعتبر فقدان الأثر من أهم المعوقات التي تواجه إثبات الجريمة الإلكترونية، حيث تظل الجريمة الإلكترونية عن طريق الحاسب الآلي مجهولة ما لم يبلغ عنها للجهات الخاصة بالاستدلالات أو التحقيق الجنائي، والمشكلة التي تواجه أجهزة العدالة الجنائية أن هذه الجرائم لا تصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، لا تخلف أثراً مادية كتلك التي تخلفها الجريمة العادية.

ثانياً: التوصيات:

في ضوء النتائج التي تم التوصل إليها، يمكن وضع عدد من التوصيات التي يمكن أن تساهم في تفعيل إثبات الجريمة الإلكترونية وذلك كما يلي:

- ١ - زيادة الاهتمام بتدريب الكوادر والاستعانة بالخبرة الفنية، حيث تستدعي عملية التحقيق في مجال الجرائم الإلكترونية وأن يتم تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن رجل الشرطة، والمحقق من كشف الجريمة، والتعرف على مرتكبيها بالسرعة والدقة اللازمة لذلك. ولتحقيق ذلك يجب تدريب الكوادر التي تباشر التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية المتميزة في هذا المجال.
- ٢ - العمل على التحفظ على الأجهزة المشتبه بها في ارتكاب الجريمة الإلكترونية، وكذلك تقنيات الاتصال المرتبطة بها التي يشك المحقق في استخدامها في عمليات الاختراق والتعدي والتزوير الإلكتروني، لكي لا يقوم الجاني بتدميرها أو إتلافها، مع ضرورة تحرير جميع المضبوطات بعد إجراء الفحص عليها وتدوين ذلك في محضر الضبط، وتحرير ما يجب تحريره من الأجهزة والتقنيات.
- ٣ - وفيما يتعلق بمعاينة الجريمة الإلكترونية، يمكن عمل ما يلي:
 - تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة، وتحديد مواقعها بأسرع وقت ممكن، وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملفات، بهدف تعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها، مع تصوير الأجهزة الموجودة، وبصفة خاصة أجزائها الخلفية.
 - ضرورة ملاحظة طريقة إعداد أنظمة الحاسب الآلي أو الإلكتروني بعناية فائقة، مع إثبات الحالة التي تكون عليها توصيلات الحاسب، وهذا لتسهيل عملية تحليل النظام عند عرض الموضوع أمام المحكمة المختصة.
 - وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة، ورصد الاتصالات الهاتفية من وإلى مسرح الجريمة مع إبطال

- مفعول أجهزة الهاتف المتحرك التي قد تساعد عن طريق تقنية معينة على تدمير أدلة الجريمة الإلكترونية متى ما تم توصيلها بالأجهزة محل المعاينة.
- يجب التأكد من عدم وجود أي مجالات كهرومغناطيسية في المحيط الخارجي لمسرح الجريمة حتى لا يتم أي إتلاف للبيانات المخزنة، وهذا يتطلب إجراء اختبارات وفحوصات تقنية قبل نقل أي مادة معلوماتية من مسرح الجريمة.
- يجب فحص كل ما تحويه سلة المهملات في الجهاز ورفع البصمات التي قد تكون لها دلالة على مرتكب الجريمة، بالإضافة إلى ضرورة القيام بحفظ كل المستندات الخاصة بالإدخال والإخراج والتي قد تكون على صلة بالجريمة.
- ٤ - زيادة الاهتمام بتطوير دور الخبرة الفنية، لما لها من دور فعال في إثبات الجريمة الإلكترونية، وهناك بعض العناصر التي أوصي بها بأن تتوفر في الخبرة الفنية حتى تساعد في سهولة إثبات الجريمة الإلكترونية، وهذه العناصر كما يلي:
- الإلمام بتركيب الحاسب وصناعته وطرأه ونظم تشغيله الرئيسية والفرعية، والأجهزة الطرفية الملحقة به، وكلمات المرور أو السر وأكواد التشفير.
- طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.
- قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك أي مشاكل أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.
- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعائمتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمتها الممغنطة.

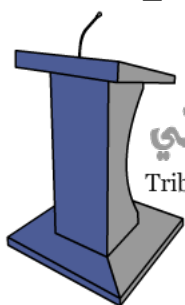
- ٥ - أهمية إنشاء أقسام أو إدارات في جهات الضبط الجنائي والتحقيق متخصصة في مجال الجريمة الإلكترونية، ويكون من ضمن اختصاصاتها متابعة ما يستجد من تطورات في مجال التقنية الحديثة للتعامل مع الجرائم المستحدثة في هذا المجال.
- ٦ - إنشاء قاعدة بيانات لجرائم المعلومات من حيث أساليبها وأنواعها للرجوع إليها عند اللزوم.
- ٧ - أهمية التنسيق المستمر بين الجهات القضائية والأمنية من جهة، والجهات ذات العلاقة بالتكنولوجيا من جهة أخرى لمسايرة ما يستجد في هذا المجال.

قائمة المصادر والمراجع

١. أبكر، سليمان مصطفى. (١٤٢٢هـ). جرائم الحاسب الآلي. مجلة الأمن والحياة. العدد ٢٤٢، الرياض، أكاديمية نايف العربية للعلوم الأمنية.
٢. أبكر، سليمان مصطفى. (١٤٢٠هـ). جرائم الحاسوب وأساليب مواجهتها. مجلة الأمن والحياة، العدد (٢١٠).
٣. أبو العينين، عبد الفتاح محمد. (١٩٩٢م). القضاء والإثبات في الفقه الإسلامي مع المقارنة بقانون الإثبات اليمني. القاهرة، جامعة الأزهر.
٤. أبو زهرة، محمد (١٩٩٨م). الجريمة والعقوبة في الفقه الإسلامي. القاهرة، دار الفكر العربي.
٥. أبو عامر، محمد زكي. (١٩٩٩م). الإثبات في المواد الجنائية. الإسكندرية، الدار الفنية للطباعة والنشر.
٦. أحمد، هلالى عبد الله. (٢٠٠٣م). الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر، ٢٠٠١. القاهرة، دار النهضة العربية.
٧. آل معجون، خلود سامي (١٤١٠٣هـ) إثبات جريمة الزنا بين الشريعة والقانون، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، الرياض.
٨. بحر، عبد الرحمن. (١٩٩٩م). معوقات التحقيق في جرائم الإنترنت: دراسة مسحية على ضباط الشرطة في دولة البحرين. رسالة ماجستير منشورة، الرياض، أكاديمية نايف العربية للعلوم الأمنية.
٩. البداينة، ذياب. (١٩٩٩م). جرائم الحاسب والإنترنت: الظواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض، أكاديمية نايف العربية للعلوم الأمنية.
١٠. البشري، محمد الأمين. (٢٠٠٠م). التحقيق في جرائم الحاسب الآلي. القاهرة، مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من ١ - ٢ مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون.

١١. البشري، محمد الأمين. (٢٠٠١م). التحقيق في جرائم الحاسب والإنترنت. المجلة العربية للدراسات العربية والتدريب، العدد (٣٠)، الرياض، أكاديمية نايف العربية للعلوم الأمنية.
١٢. بصله، رياض فتح الله. (٢٠٠١م). حدود الإثبات العلمي في قضايا التزييف والتزوير. القاهرة، دار نوبار للطباعة.
١٣. البقمي، ناصر محمد (٢٠٠٨م). مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، أبو ظبي، مركز الإمارات للدراسات والبحوث الإستراتيجية.
١٤. بوادي، حسنين المحمدي، (٢٠٠٦م)، إرهاب الإنترنت "الخطر القادم"، ط ١، دار الفكر الجامعي، الإسكندرية.
١٥. تاج الدين، مدني عبد الرحمن. (٢٠٠٤م). أصول التحقيق الجنائي وتطبيقاتها في المملكة العربية السعودية. الرياض، معهد الإدارة العامة.
١٦. جاد، نبيل عبد المنعم. (٢٠٠٥م). جرائم الحاسب الآلي. ندوة المواجهة الأمنية للجرائم المعلوماتية، مركز دعم اتخاذ القرار بالقيادة العامة لشرطة دبي، مطبعة بن دسمال.
١٧. جهاد، جودة حسين محمد. (٢٠٠٠م). المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، دراسة مقارنة، مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من ١ - ٢ مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون.
١٨. الحبشي، فادي. (١٩٩٠م). المعاينة الفنية لمسرح الجريمة والتفتيش. الرياض، جامعة نايف العربية للعلوم الأمنية.
١٩. حجازي، سهير. (١٩٩٤م). التهديدات الإجرامية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي، دولة الإمارات العربية المتحدة، العدد (٩١).

٢٠. حجازي، عبد الفتاح بيومي. (٢٠٠٥م). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت. دار الكتب القانونية، مصر.
٢١. حجازي، عبد الفتاح بيومي. (٢٠٠٥م). القانون الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر.
٢٢. حجازي، عبد الفتاح. (٢٠٠٢م). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر.
٢٣. حسن، سعيد عبد اللطيف. (١٩٩٩م). إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت: الجرائم الواقعة في جرائم تكنولوجيا المعلومات. القاهرة، دار النهضة العربية.
٢٤. حسني، محمود نجيب. (١٩٨٨م). شرح قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية، الطبعة الثانية.
٢٥. حسين، محمود عبد الله (٢٠٠٢م). سرقة المعلومات المخزنة في الحاسب الآلي. القاهرة، دار النهضة العربية.
٢٦. الحسيني، عمر الفاروق. (١٩٩١م). تأملات في بعض صور الحماية الجنائية لنظام الحاسب الآلي. تقرير مقدم إلى الدورة التدريبية التي ينظمها اتحاد المصارف العربية في الفترة من ٧-٩ مايو ١٩٩١، في الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في أعمال البنوك.
٢٧. الحمدان، عبد الرحمن بن عبد العزيز. والقاسم، محمد بن عبد الله. (٢٠٠٤م). أساسيات أمن المعلومات. الرياض، مطابع الحميضي.
٢٨. حمودة، علي محمود. (٢٠٠٣م). الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي. بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية - مركز البحوث والدراسات أكاديمية شرطة دبي - محور القانون الجنائي في الفترة من ٢٦ - ٢٨ أبريل ٢٠٠٣.



٢٩. الحميد، محمد دباس، ونينو، ماركو إبراهيم. (٢٠٠٧م). حماية أنظمة المعلومات. عمان، دار الحامد للنشر والتوزيع.
٣٠. الخطيب، الشربيني (١٤٢٥هـ) مغني المحتاج إلى معرفة معاني ألفاظ المنهاج. بيروت، دار العلم للملايين.
٣١. الخليفة، هند سليمان. (٢٠٠٧م). الحاسب الجنائي في الدول الغربية: دراسة استطلاعية. دراسة مقدمة لمؤتمر تقنية المعلومات والأمن الوطني المنعقد بالرياض خلال الفترة من ١ - ٤ ديسمبر ٢٠٠٧.
٣٢. الخماسي، فتحي بن الطيب. (١٤٢٥هـ) الفقه الجنائي الإسلامي. دمشق، سوريا، دار قتيبة.
٣٣. خيال، محمود السيد عبد المعطي. (١٩٩٨م). الإنترنت وبعض الجوانب القانونية. القاهرة، دار النهضة العربية.
٣٤. درويش، عبد الكريم أبو الفتوح. (٢٠٠٣م). الإدارة الإستراتيجية لمكافحة الجرائم المستحدثة. الإمارات العربية المتحدة، شرطة دبي.
٣٥. رستم، هشام فريد. (١٩٩٤م). الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مصر، مكتبة الآلات الحديثة.
٣٦. رستم، هشام محمد فريد. (١٩٩٢م). قانون العقوبات ومخاطر تقنية المعلومات. القاهرة، مكتبة الآلات الحديثة.
٣٧. رمضان، عمر السعيد. (١٩٩٠م). مبادئ قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية، المجلد الأول.
٣٨. رمضان، مدحت. (٢٠٠٤م). الحماية الجنائية لموقع الإنترنت ومحتوياته، ورقة عمل مقدمة لندوة التجارة الإلكترونية المنعقدة في المعهد العالي للعلوم القانونية والقضائية بدبي، ١٠-١١ مايو ٢٠٠٤.
٣٩. الرويلي، محمد بن محسن بن باعث (٢٠١٠م) تجريم الأفعال الإباحية الإلكترونية والعقاب عليها، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، قسم العدالة الجنائية.

٤٠. الزرقاني، محمد بن عبد الباقي بن يوسف. (١٤١١هـ). شرح الزرقاني على موطأ الإمام مالك بيروت، دار الكتب العلمية، ١٠٦/٨.
٤١. زين العابدين، ابن إبراهيم. (١٨٩٣). البحر الرائق شرح كنز الحقائق. القاهرة، المطبعة العلمية، ٦٨/٥.
٤٢. السبهان، فهد إبراهيم. (١٩٩٥م). استجواب المتهم بمعرفة سلطة التحقيق. الإمارات العربية المتحدة، مطبعة بن دسمال.
٤٣. السراي، عبد الله بن سعود بن محمد (٢٠٠٩م) فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، رسالة دكتوراه بجامعة نايف العربية للعلوم الأمنية، قسم العلوم الشرطية.
٤٤. السرحاني، محمد نصير. (٢٠٠٤م). مهارات التحقيق الجنائي الفني في جرم الحاسب الآلي والإنترنت. رسالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية.
٤٥. السعيد، كامل. (١٩٩٣م). جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات. بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في الفترة من ٢٥-٢٨ أكتوبر، ١٩٩٣، القاهرة.
٤٦. سفر، حسن بن محمد. (٢٠٠٣م). الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي. بحث مقدم لمجمع الفقه الإسلامي الدولي، الدورة الرابعة عشر، الدوحة، قطر.
٤٧. سلامة، مأمون محمد. (٢٠٠١م). الإجراءات الجنائية في التشريع المصري. القاهرة، دار النهضة العربية.
٤٨. السنباطي، عطا عبدالعاطي محمد (١٤٢٢هـ)، موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت، دار النهضة العربية، الطبعة الأولى.
٤٩. الشاذلي، فتوح عبد الله. (١٩٩٨م). قانون العقوبات: القسم العام. الإسكندرية، دار المطبوعات الجامعية.

٥٠. الشاذلي، فتوح، وعفيفي، عفيفي كامل. (٢٠٠٣م). جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون. بيروت، منشورات الحلبي الحقوقية.
٥١. الشاعر، عبد الرحمن إبراهيم. (٢٠٠٤م). تقنية المعلومات والاتصال. الرياض، دار ثقيف للنشر والتأليف.
٥٢. شاهين، إسماعيل عبد النبي. (٢٠٠٠م). أمن المعلومات في الإنترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من ١ - ٢ مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون.
٥٣. شتا، محمد محمد (٢٠٠٠م). فكرة الحماية الجنائية لبرامج الحاسب الآلي. القاهرة، دار الجامعة الجديدة للنشر.
٥٤. شمس الدين، أشرف توفيق. (٢٠٠٦م). الحماية الجنائية للمستند الإلكتروني "دراسة مقارنة". القاهرة، دار النهضة العربية، الطبعة الأولى.
٥٥. الشوا، محمد سامي. (٢٠٠٠م). ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة، دار النهضة العربية.
٥٦. الشوابكة، محمد أمين (٢٠٠٢م)، الجرائم المرتكبة عبر الإنترنت، رسالة ماجستير غير منشورة، جامعة الدول العربية، المنظمة العربية للتربية والثقافة والعلوم، قسم البحوث والدراسات القانونية.
٥٧. الشوابكة، محمد أمين. (٢٠٠٦م). جرائم الحاسوب والإنترنت: الجريمة المعلوماتية. عمان، دار الثقافة للنشر والتوزيع.
٥٨. صابر، نويب حسين. (٢٠١٠م). مؤتمر البيئة المعلوماتية الآمنة. الرياض، جمعية المكتبات والمعلومات السعودية.
٥٩. صالح، نائل عبد الرحمن. (٢٠٠٠م). واقع جرائم الحاسوب في التشريع الأردني. بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في العين بدولة الإمارات العربية المتحدة في الفترة من ١ - ٣ مايو ٢٠٠٠.

٦٠. الصغير، جميل عبد الباقي. (١٩٩٢م). القانون الجنائي والتكنولوجيا الحديثة. القاهرة، دار النهضة العربية.
٦١. الصغير، جميل عبد الباقي. (٢٠٠٢م). الإنترنت والقانون الجنائي. القاهرة، دار النهضة العربية.
٦٢. الصيفي، عبد الفتاح مصطفى. (٢٠٠٢م). تأصيل الإجراءات الجنائية. الإسكندرية، دار المعرفة الجامعية.
٦٣. الطخيس، إبراهيم عبدالرحمن (١٩٩٤م)، دراسات في علم الاجتماع الجنائي، ط١، دار العلوم للطباعة والنشر، الرياض.
٦٤. طنطاوي، إبراهيم حامد. مرسى. (١٩٩٧م). سلطات مأمور الضبط الجنائي. القاهرة، دار النهضة العربية، الطبعة الثانية.
٦٥. عبد الحميد، أحمد فاروق. (١٤٢٠هـ). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. الرياض، جامعة نايف العربية للعلوم الأمنية.
٦٦. عبد اللاه، هلالى. (٢٠٠٠م). التزام الشاهد بالإعلام في الجرائم المعلوماتية. القاهرة، دار النهضة العربية.
٦٧. عبد الله، الأزرق. (٢٠١٠م). مؤتمر البيئة المعلوماتية الآمنة. الرياض، جمعية المكتبات والمعلومات السعودية.
٦٨. عبد المطلب، ممدوح عبد الحميد. (٢٠٠١م). جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية: الجريمة عبر الإنترنت. الشارقة، مكتبة دار الحقوق.
٦٩. عبد المطلب، ممدوح عبد الحميد. (٢٠٠٦م). البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت. مصر، دار الكتب القانونية.
٧٠. عبد المطلب، ممدوح عبد الحميد. (٢٠٠٧م). أدلة الصور الرقمية. ورقة عمل مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة: الجرائم الإلكترونية الملامح والأبعاد، المنعقدة بكلية الملك فهد المنية بالرياض في الفترة من ٢٢ إلى ٢٤ أبريل، ٢٠٠٧. الرياض، كلية الملك فهد الأمنية.

٧١. العبيدي، خالد بن عبد الله بن معيض (٢٠٠٨م). الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية، دراسة تحليلية مقارنة، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، قسم العدالة الجنائية.
٧٢. العرابي، علي زكي (١٩٤٠م) المبادئ الأساسية للتحقيقات والإجراءات الجنائية.
٧٣. عرب، يونس. (٢٠٠٢م). جرائم الكمبيوتر والإنترنت. ورقة عمل مقدمة إلى مؤتمر الأمن العربي المنعقد في الفترة من ١٠-١٢ / ٢ / ٢٠٠٢، أبو ظبي، المركز العربي للدراسات والبحوث الجنائية.
٧٤. عرب، يونس. (٢٠٠٦م). تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية. ورقة عمل مقدمة لمؤتمر هيئة تنظيم الاتصالات في الفترة من ٢-٤ أبريل ٢٠٠٦، سلطنة عمان، مسقط.
٧٥. العريان، محمد علي. (٢٠٠٤م). الجرائم المعلوماتية. الإسكندرية: الدار الجامعية الجديدة للنشر.
٧٦. عقيدة، محمد أبو العلا (٢٠٠٣م)، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد في أكاديمية شرطة دبي، مركز البحوث والدراسات بتاريخ: ٢٦ - ٢٨ نيسان، دبي، الإمارات العربية المتحدة.
٧٧. العكيلي، عبد الأمير، وحرية، سليم إبراهيم. (١٩٨١م). أصول المحاكمات الجزائية. المجلد الأول، الموصل، دار الكتب للطباعة والنشر.
٧٨. علي، نبيل علي. (١٩٩٤م). العرب وعصر المعلومات. الكويت، عالم المعرفة.
٧٩. عمار، زكريا أحمد (١٤٢٩هـ) ، الحلقة العلمية: الدليل الرقمي والتحقيق في الجرائم الإلكترونية، جامعة نايف العربية للعلوم الأمنية، كلية علوم الأدلة الجنائية، من ٢٢ إلى ٢٦ / ١٢ / ١٤٢٩هـ.

٨٠. العنزي، سلمان. (٢٠٠٢م). وسائل التحقيق في جرائم نظم المعلومات. رسالة ماجستير غير منشور، الرياض، جامعة نايف العربية للعلوم الأمنية.
٨١. عودة عبد القادر (١٤٠١هـ)، التشريع الجنائي الإسلامي، م ١، بيروت: مؤسسة الرسالة.
٨٢. عوض، محمد محيي الدين. (١٩٦٣م). القانون الجنائي: مبادئه الأساسية ونظرياته العامة في التشريعين المصري والسوداني. القاهرة، المطبعة العالمية.
٨٣. عوض، محمد محيي الدين. (١٩٩٣م). مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات. ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة.
٨٤. غنام، محمد غنام. (٢٠٠٠م). عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر. بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من ١-٢ مايو ٢٠٠٠، الإمارات، كلية الشريعة والقانون.
٨٥. فرغلي، عبد الناصر محمد، والمسماري محمد عبيد. (٢٠٠٧م). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة. المؤتمر العربية الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية.
٨٦. فلييسون، ستيفن. (٢٠٠٠م). الجريمة الإلكترونية في القرن الحادي والعشرين. ترجمة آمنة علي يوسف، دبي، مركز البحوث والدراسات بإدارة شرطة دبي.
٨٧. فوزي، شريف. (١٩٨٦م). مبادئ التشريع الجنائي الإسلامي. القاهرة، مكتبة الخدمات الحديثة.
٨٨. الفيروز آبادي (١٤٠٧هـ)، القاموس المحيط، مؤسسة الرسالة، بيروت، لبنان، ط ٢.

٨٩. القحطاني، فيصل بن معيض (١٩٩٩م) هيئة التحقيق والادعاء العام ودورها في نظام العدالة الجنائية في المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية.
٩٠. القحطاني، منصور بن سعيد. (٢٠٠٨م). مهددات الأمن المعلوماتي وسبل مواجهتها. الرياض، جامعة نايف العربية للعلوم الأمنية.
٩١. قشقوش، هدى حامد. (٢٠٠٠م). الإلتلاف العمدي لبرامج وبيانات الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، في الفترة ١-٣ مايو سنة ٢٠٠٠.
٩٢. قطب، محمد علي. (٢٠١٠م). الجرائم المعلوماتية وطرق مواجهتها. مملكة البحرين، وزارة الداخلية، الأكاديمية الملكية للشرطة.
٩٣. قورة، نائلة. (٢٠٠٤م). جرائم الحاسب الاقتصادية. القاهرة، دار النهضة العربية، الطبعة الأولى.
٩٤. الكاساني، علاء الدين أبو بكر. (١٩٨٢م). بدائع الصنائع في ترتيب الشرائع. بيروت، دار الكتاب العربي، ٦٧/٧.
٩٥. كامل، محمد فاروق عبد الحميد. (١٩٩٩م). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. الرياض، جامعة نايف العربية للعلوم الأمنية.
٩٦. كلزي، ياسر حسن (٢٠٠٧م) حقوق الإنسان في مواجهة سلطات الضبط الجنائي، دراسة مقارنة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية.
٩٧. ماركيزية، جان (١٩٨٣م) الجريمة، ترجمة عيسى عصفور، منشورات عويدات، بيروت.
٩٨. المالكي، برهان الدين بن فرحون. (١٩٩٥م). تبصرة الحكام في أصول الأقضية ومناهج الأحكام. تخريج جمال مرعشلي. بيروت، دار الكتب العلمية.
٩٩. الماوردي، علي بن محمد. (١٤٢٥هـ). الأحكام السلطانية. بيروت، دار الكتب العلمية.

١٠٠. مجلة مجمع الفقه الإسلامي التابع لمنظمة المؤتمر الإسلامي. (١٤١١هـ).
جدة، المجمع الفقه الإسلامي برابطة العالم الإسلامي، العدد الخامس، المجلد الثالث.
١٠١. مجمع اللغة العربية، جمهورية مصر العربية، معجم القانون، القاهرة، الهيئة العامة لشئون المطابع الأميرية، ١٤٢٠هـ.
١٠٢. محمود، عبد الله حسين. (٢٠٠٢م). سرقة المعلومات المخزنة في الحاسب الآلي. القاهرة، دار النهضة العربية، الطبعة الثانية.
١٠٣. محمود، عبدالله ذيب عبدالله (٢٠٠٩م) حماية المستهلك في التعاقد الإلكتروني: دراسة مقارنة، رسالة ماجستير غير منشورة، جامعة النجاح الوطنية، فلسطين.
١٠٤. المرزوقي، محمود محمد. (٢٠٠٣م). جرائم الحاسب الآلي. المجلة العربية للفقه والقضاء، العدد ٢٨، الأمانة العامة لجامعة الدول العربية.
١٠٥. المزمومي، محمد بن حميد. (٢٠٠٧م). جريمة الاعتداء على الأموال عن طريق الحاسب الآلي. رسالة ماجستير غير منشورة، جامعة الملك عبد العزيز بجدة.
١٠٦. مصري، عبد الصبور (٢٠١٠م)، الجريمة الإلكترونية، دار العلوم، للنشر والتوزيع، القاهرة.
١٠٧. مصطفى، محمود محمود. (١٩٧٧م). الإثبات في المواد الجنائية في القانون المقارن. القاهرة، مطبعة جامعة القاهرة.
١٠٨. موسى، مصطفى محمد. (٢٠٠٣م). أساليب إجرامية للتقنية الرقمية: ماهيتها، مكافحتها، القاهرة، دار النهضة العربية.
١٠٩. المويشير، تركي بن عبد الرحمن. (٢٠٠٩م). بناء أنموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته. الرياض، جامعة نايف العربية للعلوم الأمنية.

١١٠. النمر، أبو العلا. (١٩٩١م). الأدلة الجنائية في ضوء الفقه وأحكام النقض الجنائي، دراسة تحليلية للدليل الجنائي فقهاً وعملاً.. القاهرة، دار الصداقة.
١١١. الهيتي، محمد حماد. (٢٠٠٤م). التكنولوجيا الحديثة والقانون الجنائي. عمان، جاز الثقافة للنشر والتوزيع.
١١٢. الهيتي، محمد حماد. (٢٠٠٥م). جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها. عمان، دار المناهج للنشر والتوزيع.
١١٣. واصل محمد، والهاللي حسين بن علي (٢٠٠٤م). الخبرة الفنية أمام القضاء "دراسة مقارنة". عمان، المكتب الفني بالمحكمة العليا بوزارة العدل.
١١٤. اليوسف، عبد الله بن عبد العزيز. (١٩٩٩). الظواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض، جامعة نايف العربية للعلوم الأمنية.

الملحق

نظام مكافحة الجرائم المعلوماتية



نظام مكافحة جرائم المعلوماتية

المادة الأولى :

يقصد بالالتفاظ والعبارات الآتية - أينما وردت في هذا النظام - المعاني المبينة أمامها ما لم يقتض السياق خلاف ذلك:

- ١- الشخص: أي شخص ذي صفة طبيعية أو اعتبارية ، عامة أو خاصة .
- ٢- النظام المعلوماتي: مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.
- ٣- الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت).
- ٤- البيانات: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بواسطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.
- ٥- برامج الحاسب الآلي: مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.
- ٦- الحاسب الآلي: أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات ، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها ، يؤدي وظائف محددة بحسب البرامج ، والأوامر المعطاة له.
- ٧- الدخول غير المشروع: دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع، إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



المملكة العربية السعودية
 هيئة الخبراء بمجلس الوزراء

الرقم : _____
 التاريخ : _____ / _____ / ١٤٠٤ هـ
 المرفقات : _____

٨- الجريمة المعلوماتية: أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

٩- الموقع الإلكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

١٠- الالتقاط: مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح .

المادة الثانية :

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها ، وبما يؤدي إلى ما يأتي :

- ١ - المساعدة على تحقيق الأمن المعلوماتي.
- ٢ - حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية .
- ٣ - حماية المصلحة العامة، والأخلاق، والآداب العامة.
- ٤ - حماية الاقتصاد الوطني.

المادة الثالثة :

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية:

- ١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.
- ٢- الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً .
- ٣- الدخول غير المشروع إلى موقع الكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه .



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



المملكة العربية السورية
هيئة الخبراء بمجلس الوزراء

الرقم :
التاريخ : / / ١٤
المرفقات :

٤- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا ، أو ما في حكمها .

٥- التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة .

المادة الرابعة :

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

- ١- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة .
- ٢- الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

المادة الخامسة :

يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية :

- ١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها .
- ٢- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
- ٣- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت .

المادة السادسة :

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



المملكة العربية السعودية
هيئة الخبراء بمجلس الوزراء

الرقم :
التاريخ : ١٤ / / ١٤٢٨
المرفقات :

١- إنتاج ما من شأنه المساس بالنظام العام ، او القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعدادة ، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي .

٢ - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره ، للاتجار في الجنس البشري، أو تسهيل التعامل به.

٣- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها .

٤- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره ، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها .

المادة السابعة :

يعاقب بالسجن مدة لا تزيد على عشر سنوات وغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية :

١- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية .

٢- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني .

المادة الثامنة :

لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات

الآتية:





- ١- ارتكاب الجاني الجريمة من خلال عصابة منظمة .
- ٢- شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.
- ٣- التهديد بالقصر ومن في حكمهم، واستغلالهم .
- ٤- صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم معادلة.

المادة التاسعة :

يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية .

المادة العاشرة :

يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة .

المادة الحادية عشرة :

للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

المادة الثانية عشرة :

لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة ما يتعلق بحقوق الملكية الفكرية، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفاً فيها.





المادة الثالثة عشرة :

مع عدم الإخلال بحقوق حسني النية ، يجوز الحكم بمصادرة الأجهزة ، أو البرامج ، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام ، أو الأموال المحصلة منها . كما يجوز الحكم بإغلاق الموقع الإلكتروني ، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكة.

المادة الرابعة عشرة:

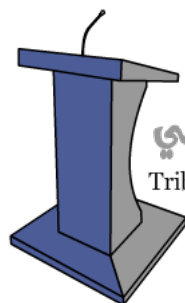
تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة .

المادة الخامسة عشرة :

تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام.

المادة السادسة عشرة :

ينشر هذا النظام في الجريدة الرسمية ويعمل به بعد (مائة وعشرين) يوماً من تاريخ نشره .



مدونة المنبر القانوني

Tribunejuridique.blogspot.com