المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

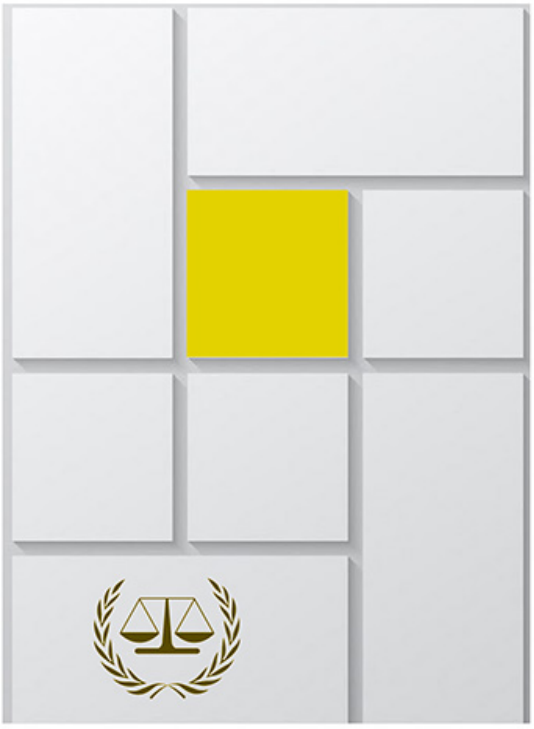
الجرائم الإلكترونية ووسائل الإثبات الرقمي

إعداد:
الدكتور علي حسون
معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العربية

المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

الجرائم الإلكترونية ووسائل الإثبات الرقمي



إعداد:
الدكتور علي حسون
معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العربية

المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

الجرائم الإلكترونية
ووسائل الإثبات الرقمي

إعداد:
الدكتور علي حسون
معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العربية

منشورات المركز العربي للبحوث القانونية والقضائية

العنوان: بيروت -منطقة الأشرفية-شارع بيضون- مقابل فصيلة قوى الأمن الداخلي

الموقع الإلكتروني: www.carjj.org

البريد الإلكتروني: arab.league@carjj.org

تلفون: 009611200283 009611200281 /

فاكس: 009611200280

"إن المواقف والأفكار الواردة في هذا الكتاب تعبّر عن وجهة نظر ورأي المؤلف ولا تلتزم بها أية جهة أخرى"

ملخص الدراسة

تعرف الجرائم الإلكترونية على أنّها أي فعل يتم من خلال أجهزة الكمبيوتر بهدف التعطيل والإتلاف.
كذلك استخدام البيانات والمعلومات الموجودة عليها بغية السرقة والاحتيال لأهداف غير شرعية.
يحدث ذلك من خلال استخدام فيروس يعطل الجهاز ويخترقه من خلال تقنيات خبيثة.
تكمن أهداف ارتكاب الجرائم الإلكترونية وراء الجانب السيئ من الطبيعة البشرية وهو الجشع والطمع والركض خلف المكاسب الشخصية دون الاهتمام بما قد تسببه هذه المكاسب من أذى للآخرين.
لذلك فإن السبب الأول في الجرائم الإلكترونية مؤداه حب التطفل واستغلال الآخرين وضعفهم والمرض النفسي الذي يجعل رؤية الآخر ضعيفًا والنشوة والتلذذ بذلك.
تعد هذه الجرائم الإلكترونية مرضًا يسبب الفتك بالمجتمعات والعلاقات الإنسانية، ويؤخر من عجلة التقدم والتنمية التي يعيشها العالم مؤخرًا.
أول هذه الآثار هي تدمير قيم الأسرة من خلال استغلال أفرادها والإساءة له وصورته التي تؤثر في باقي أسرته لمدة طويلة.
توفر القوانين والتشريعات الخاصة بكل دولة عقوبات على مرتكبي الحرائم للحد من انتشارها وإعطاء جزء بسيط من حق الضحية المسلوب من قبل المجرم.
بالإضافة إلى قوانين كل دولة فإن المجتمع الدولي يطبق عقوبات على مرتكبي الجريمة ويأمر البوليس الدولي بتتبع المجرمين والتواصل مع سفاراتهم ودولهم للقبض عليهم
وللجريمة الالكترونية طرق إثبات خاصة بها تعرف بالدليل الرقمي, والدليل الرقمي ذو هيئة الكترونية غير ملموسة لا تدرك بالحواس, وهذه أهم خاصية تميز الدليل الالكتروني عن غيره من الأدلة الجنائية. ولإثبات الجريمة الالكترونية لابد من إتباع طرق الإثبات المتعارف عليها, والتي تخضع للقواعد العامة للإثبات الجنائي. ولكن مايميز هذه الجرائم أنه عند تطبيق طرق الإثبات في مجالها ينتج دليل خاص بها وهو الدليل الالكتروني, والدي يتميز بكونه دليل دو هيئة الكترونية غير ملموسة, ويخضع شأنه شأن الأدلة الجنائية الأخرى للسلطة التقديرية للقاضي الجزائي.

Résumé de l'étude :

L'avis consultatif rendu par la Cour internationale de Justice le 19 juillet 2024 est un avis historique qui affirme les principes fondamentaux du droit international, en particulier en ce qui concerne l'interdiction de l'acquisition de territoires par la force et le droit des peuples à l'autodétermination, constitue un défi juridique important à la politique d'Israël dans les territoires occupés et expose les actes criminels commis par Israël qui ont privé le peuple palestinien de ses droits et l'ont marginalisé pendant des décennies. L'avis consultatif a affirmé que l'occupation israélienne des territoires palestiniens (connus sous le nom de 67 territoires) est illégale et que ses pratiques de construction de colonies de peuplement, d'augmentation du nombre de colons, de privation des Palestiniens des éléments de base de la vie et d'exploitation des ressources naturelles palestiniennes sont illégales, que l'occupation israélienne commet le crime d'apartheid en Cisjordanie et à Jérusalem-Est, et que l'occupation doit démanteler les colonies.Les Palestiniens ont le droit à l'autodétermination. La communauté internationale ne doit pas continuer d'ignorer les dispositions juridiques concernant les politiques et pratiques illégales d'Israël, et le Conseil de sécurité doit agir maintenant et mettre fin à l'impunité dont Israël jouit depuis des décennies. Bien que les avis de la Cour consultative internationale de Justice ne soient pas juridiquement contraignants, ils ont une autorité morale et juridique considérable et peuvent éventuellement faire partie du droit international coutumier juridiquement contraignant pour les États. L'avis consultatif ouvrira la voie à de nouvelles procédures juridiques et politiques dans les forums internationaux et l'utilisera pour renforcer la pression diplomatique et juridique sur Israël afin qu'il mette fin à son occupation. C'est un pas dans

un long chemin vers la justice pour le peuple palestinien comme pour d'autres peuples qui se sont battus pour leur liberté.

Les conséquences juridiques de l'avis consultatif ne peuvent être négligées ou ignorées, car il est émis par l'organe judiciaire principal de l'ONU, ce qui exige des autres organes de l'ONU qu'ils adoptent des positions et des décisions qui sont conformes à ce qui y est énoncé et qui le reflètent.

الفصل الاول: الجرائم الإلكترونية

الجريمة ظاهرة قديمة، عرفتها المجتمعات البشرية منذ القدم، وظهرت في هذه المجتمعات السلطة الحاكمة إنطلاقاً من رب الأسرة إلى شيخ القبيلة، حيث وضعت بعض القيود على تصرفات الأفراد لإستتباب الأمن لدى الفرد والمجتمع، وإعتبرت أن كل فعل يمس أمن الجماعة أو حياة الفرد أو ماله أو سلامته الجسدية، فعل مجرم يستحق العقاب عليه.

بعد ظهور فكرة الدولة تولت بنفسها سلطة تجريم الأفعال والعقاب عليها، حيث أصدرت تشريعات منها ما هو موضوعي "قانون العقوبات" الذي يجرم الأفعال ويحدد العقوبات عليها، ومنها ما هو إجرائي " قانون الإجراءات الجنائية" الذي يحدد الإجراءات الواجب اتباعها امام الهيئات القضائيه وكذا اجراءات الضبط القضائي، دون أن ننسى ان الشريعة الإسلامية المناسبة لكل زمان ومكان، قد حددت كليات خمس لا تستقيم الحياة الا بها، وهي حفظ الدين، حفظ النفس، حفظ العقل، حفظ النسل، حفظ المال، وبينت ان مسآله المجرم تكون إستناداً لمبدأ الأختيار.

كشفت السنوات الأخيرة النقاب عن تكنولوجيا متطورة، لم تكشفها عقودا من الزمن، وإزاء التطورات السريعة والمذهلة في هذه التكنولوجيا التي جاءت لخدمة الإنسان، إلا انه لم يرق للبعض أن يحسن إستخدامها، فأساء إستخدامها وألحق الضرر بأخيه الانسان، فسبه وقذفه وسرق ماله وأتلف محتويات وأنظمة حاسوبية وكذلك قتله، لنجد أنفسنا أمام صنوف (أصناف) شتى من الجرائم الالكترونيه.

نظراً لحداثة الجرائم الإلكترونيهة، وظهورها مع كل تقنية حديثة يتم إكتشافها وتوفيرها لأفراد المجتمع، نجد إساءة في أستخدامها، ما يستوجب على المشرع مواكبة التطور الحاصل على الصعيد التقني، من خلال استحداث نصوص تشريعية لمكافحة الجرائم الناتجة عن هذه التقنيات ووضع حد لها، وبالتالي العمل على تقليلها إن لم يكن في الإمكان القضاء عليها.

سنتناول في دراستنا الجرائم الإلكترونية ووسائل الأثبات الرقمي في الفصل الاول سنعالج موضوع الجرائم الإلكترونية وفي الفصل الثاني سنتطرف إلى وسائل الأثبات الرقمي.

المبحث الاول: تعريف الجريمة الإلكترونية وخصائصها

لم يتفق الفقه الجنائي على إيراد تسميه موحدة للجريمة الإلكترونية، فهناك عدة تسميات لها منها الجريمة المعلوماتية، جرائم إساءة استخدام تكنولوجيا المعلومات والإتصال، جرائم الكمبيوتر والإنترنت، الجرائم المستحدثة[1]، الجريمة الناعمة، أجرام ذوي الياقات البيضاء[2]. وتجدر الأشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الإنترنت فبينما تتحقق الأولى بالإعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه والمعلومات المخزنة به، فإن جرائم الإنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب الآلي عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى إندماج الميدانين (الحوسبة والأتصالات) وظهور مصطلح cybercrime [3] وقد إنقسم الفقهاء إلى إتجاهين منهم من ينظر إلى الجريمة الإلكترونية بمفهوم ضيق، ومنهم من ينظر اليها بمفهوم واسع كما أن للجريمة الإلكترونية أركان لا تقوم الجريمة إلا بتوافرها.

المطلب الاول: تعريف الجريمة الإلكترونية

عرف القانون الأمريكي الجريمة الإلكترونية بأنها: "الإستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات والإستخدام المتعمد الضار لإجهزه الكمبيوتر أو ملفات البيانات وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى الجناية من الدرجه الثالثة[4].

قد تناول الفقه القانوني تعريفات مختلفه للجريمة الإلكترونية:

الأتجاه الأول: يعرف الجريمة الإلكترونية بأنها: كل أشكال السلوك غير المشروع الذي يرتكب بإستخدام الحاسب[5].

ني: يعرف الجريمة الإلكترونية بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب ومعداته[6].

لث: يعرف الجريمة الإلكترونية بأنها: أي فعل غير مشروع تكون المعرفة بتقنية المعلوماتية أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً[7].

ابع: يعرّف هذا الأتجاه الجريمة الإلكترونية بإنها: الأعتداءات القانونية التي يمكن أن ترتكب بواسطة الوسائل الإلكترونية بغرض تحقيق الربح[8].

وقد عرّفت منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة الجريمة الإلكترونية بأنها: كل فعل أو أمتناع من شأنه الأعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقه مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية[9].

ما يلاحظ على هذين التعريفين أن التعريف الأول، أشترط أن يحقق الفاعل ربحاً، وهذا الأمر غير متحصل دائماً من الجرائم الإلكترونية، كما ان الفعل المرتكب قد لا يكون عمدياً فقد يحصل بطريقه غير مباشرة، كما أن تعريف منظمة التعاون الأقتصادي والتنمية أدرج الأموال المادية، وهذه الأموال كما يرى البعض[10] يمكن حمايتها بموجب نصوص قانون العقوبات التقليدية ولا حاجه لقانون خاص لحمايتها.

س: يعرّف الجريمة الإلكترونية بأنها كل فعل أو أمتناع عبر فعل من مسألة الإعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجاً بطريقة مباشرة أو غير مباشرة لتدخل التقنية الإلكترونية[11].

الفرع الاول: الاتجاه الضيق من تعريف الجريمة الإلكترونية

يعرف أنصار هذا الاتجاه الجريمة الإلكترونية بأنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحسبات الألية بقدر كبير لازم لإرتكابه من ناحية، لملاحقته وتحقيقه من ناحية أخرى[12]". حسب هذا التعريف يجب ان تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لإرتكاب الجريمة، بل كذلك لملاحقتها، والتحقيق فيها. وهذا التعريف يضيق بدرجة كبيرة من الجريمة الالكترونية، بمعنى يجب أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة، والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرها. وهناك من يعرّفها على أنها " الفعل غير المشروع الذي يتورط في إرتكابة الحاسب أو هي الفعل الإجرامي الذي يستخدم في افتراضه

الحاسوب بإعتباره اداة رئيسية. كما يرى الأستاذ تردمان أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة بإستخدام المعالجة الآلية للمعلومات[13]".

ويرى الأستاذ روزنبيلات بإن الجريمة الإلكترونية هي " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه[14]".

حسب هذا التعريف فأن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لإرتكابها تخرج من نطاق التجريم. ويرى الأستاذ باركار بإن الجريمة الإلكترونية كل فعل إجرامي متعمد أياً كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل[15].

الفرع الثاني: الأتجاه الموسع من تعريف الجريمة الالكترونية:

على عكس الأتجاه السابق، يرى فريق أخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل جريمة بوسيلة إلكترونية كالحاسوب مثلاً وذلك بإستخدام شبكات الإنترنت من خلال غرف الدردشة، وإختراق البريد الإلكتروني ومختلف وسائل التواصل الأجتماعية، بهدف الحاق الضرر لفرد أو بمجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الأستهداف الحربي أو الإقتصادي، أو الضرر بسمعتها أو العكس، ويبقى الهدف واحد هو الكشف عن قضايا متستر عليها، أو نشر معلومات لفائدة طرف واحد أو أطراف أخرى من باب التسريب[16] في تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام المخالفة "الجريمة" في كل حالة يتم فيها تغيير معطيات أو بيانات، أو برامج أو محوها، أو كتابتها، أو إي تدخل أخر في مجال إنجاز البيانات أو معالجتها، وتبعاً لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص أو تقصد الحصول على كسب اقتصادي غير مشروع له، أو لشخص أخر[17]".

ودائماً حسب أنصار هذا الإتجاه يرى البعض أن الجريمة الإلكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أنَّ لديه معرفة بتقنية الحاسوب نظامياً حاسوبياً، أو شبكة حاسوبية للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حيازتها، أو توزيعها بصورة غير مشروعة[18]، أما البعض من الفقهاء يعرفونها بإن كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية "الحاسوب الآلي الرقمي وشبكة الإنترنت" بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الاجرامي المستهدف[19].

المطلب الثاني: خصائص الجريمة الإلكترونية والمجرم الإلكتروني

تختلف الجريمة الإلكترونية عن الجريمة التقليدية من حيث خصائصها، فالجريمة الإلكترونية لم تظهر الإ في عصر الحاسب الآلي والإنترنت، وكون هذه الجرائم حديثة ومتطورة فإن لها خصائص منفردة تتميز بها عن غيرها من الجرائم التقليدية، وهذه الخصائص نستخرجها من التعاريف الذي إنتهينا إليها في المطلب السابق، كما أنَّ المجرم الإلكتروني له سمات منفردة به لا نجدها في المجرمين الآخرين[20].

الفرع الاول: خصائص الجريمة الإلكترونية

للجريمة الإلكترونية مجموعة من الخصائص التي تنفرد بها عن الجرائم التقليدية، ومن أهم هذه الخصائص أن الجرائم الإلكترونية تتطلب وجود جهاز إلكتروني ومعرفة كيفية إستخدامه، وإن الهدف من هذه

الجرائم الكيانات المعنوية لهذا الجهاز، كما أن الجريمة الإلكترونية لا حدود لها، وهذه الجرائم صعبة الإثبات والإكتشاف، ولذلك فهي مغرية للمجرمين.

أ: تتميز الجريمة الإلكترونية عن غيرها أن الجهاز الإلكتروني هو أداة الجريمة ووسيلة تنفيذها، أو هو موضوع الجريمة كإتلاف أو سرقة البيانات والمعلومات وهنا تثور المشكلة، أما لو كان موضوع الإعتداء هو الجهاز نفسه أو شاشته أو الكيانات المادية للحاسب الآلي منها تكفي نصوص التجريم التقليدية، ويطبق قانون العقوبات على موضوع الجريمة، فبدون الجهاز الإلكتروني تنتفي الجريمة الإلكترونية، وتتطلب هذه الجريمة دراية كافية وخبرة فائقة بالكمبيوتر والإنترنت في بعض الجرائم، أو معرفة سلوكيات الفعل المرتكب في الجرائم البسيطة منها، كما أنها لا تمتاز بالعنف، وأغلب الجرائم ترتكب عبر الإنترنت[21].

وذلك فإن ما يميز الجريمة الإلكترونية عن غيرها من الجرائم، أنها تتطلب وجود علم كافي بالجوانب الفنية التقنية لإستخدام الحاسوب والإنترنت، وتعتبر العلاقة بين مدى الدراية بالجوانب الفنية والتقنية لإستخدام للحاسوب وبين الجريمة وبين الجريمة الإلكترونية علاقة طردية، فكلما زادت الخبرة لدى الأفراد بمعرفة تقنية الحاسوب، زاد احتمال استخدام خبرتهم بشكل غير مشروع[22].

ثانياً: موضوع الإعتداء و معطيات الجهاز الإلكتروني

تعد البيانات والمعلومات المخزنة على الحاسب الآلي هي موضوع الجرائم الإلكترونية، فهذ البيانات يمكن تخزينها ونقلها من جهاز لآخر عبر الوسائط الصلبة أو المرنة أو عبر البريد الإلكتروني، ولذلك فهي تعتبر مكونات معنوية تقبل الحيازة والنقل، ويمكن سرقته وإتلافه، ولذلك يجب أن يكون هذا الحال محل حماية من قبل القانون الجزائي[23]، وعليه فإن كان موضوع الإعتداء هو الحاسب الآلي أو شاشته أو أحد مكوناته المادية فإنه في هذه الحالة يصلح أن يكون قانون العقوبات هو المرجع الصالح أو لو كان موضوع الإعتداء هو معطيات الحاسوب من البيانات والمعلومات فنحن هنا بصدد جريمة إلكترونية وتحتاج إلى نصوص أكثر دقة في معالجتها.

ولذلك فإن البيانات والمعلومات الحاسوبية تعد مالاً قابل للحيازة والنقل، وله قيمة مادية، وقد نص المشرع الأردني في المادة 54 من القانون المدني الأردني بأن "كل شيء يمكن حيازته مادياً أو معنوياً أو الإنتفاع به إنتفاعاً مشروعاً، ولا يخرج عن التعامل تطبيقه أو بحكم القانون، يصح أن يكون محلاً للحقوق المالية[24].

ثالثاً: الجريمة الإلكترونية لا حدود جغرافية لها:

أزالت الشبكة العنكبوتية(الإنترنت) كل الحدود الجغرافية بين الدول، وجعلت العالم كله كقرية صغيرة يسهل التواصل بين الأفراد ليس في الدول كحسب بل أنه من السهل التواصل بين الأشخاص في القارات المختلفة، وهذا ما جعل الجريمة الإلكترونية عابرة للحدود[25].

ولأن أغلب الجرائم الإلكترونية ترتكب عبر الإنترنت فإنها تتسم بالطابع الدولي، حيث تقع هذه الجرائم فيكون المجرم في دولة والمجني عليه في دولة أخرى، ويمكن أن يكون الضرر قد حدث في دولة ثالثة أو عدة دول، مثل أختراق المواقع والأجهزة وإتلافها، وسرقة البيانات والمعلومات، والأموال

كل ذلك جعل من مكافحة الجريمة الإلكترونية أمراً عسيراً، وذلك لتعدد الأماكن التي تتعلق بالجريمة، وتنازع قوانين الدول الواجبة التطبيق، وإختلاف الإجراءات الجزائية من دولة لأخرى، وصعوبة ملاحقة الجناة، كل ذلك يتطلب وجود تعاون دولي للقبض على الجناة وتقديمهم للمحاكم المختصة بنظر النزاع[26].

فالتحقيق في الجرائم الإلكترونية يتطلب القيام بإجراءات وأعمال التحقيق خارج حدود الدولة، مثل تفتيش المواقع الإلكترونية المادية للقيود على البيانات أو المعلومات، أو إلقاء القبض على المطلوبين، أو معاينة مسرح الجريمة، كل ذلك يحتاج إلى تعاون دولي على أرض الواقع[27].

رابعاً: الجريمة الإلكترونية صعبة الأكتشاف والاثبات:

الجرائم الإلكترونية من الجرائم التي لا تترك آثار خارجية مادية فهي لا تترك بقع دماء كما في جرائم الإعتداء والقتل ولا إتلاف كما في جرائم السطو، فالجريمة الإلكترونية جريمة نظيفه أي لا تترك آثار مادية ملموسة، ولذلك كانت هذه الجريمة صعبة الإكتشاف والإثبات.

ومما جعل الجرائم الإلكترونية صعبة الإكتشاف والإثبات البعد الجغرافي بين الجاني والمجني عليه كما ذكرنا، وأستخدام الجاني وسائل فنية حديثة في جرمه، كما أن هذه الجرائم ترتكب في وقت سريع ويتم محو أثرها في وقت أسرع لا يتعدى الثواني، ومما يزيد الأمر صعوبة عدم وجود خبرة لدى ضباط التحقيق في مثل هذه الجرائم من ناحية التحقيق والبحث على الأدلة والتحفظ عليها، ومن الصعوبات التي تواجه إثبات هذه الجرائم عدم أقتناع القضاة بكثير من الجرائم المستحدثه في هذا المجال[28].

وتعد هذه الخاصيه من السمات التي تتميز بها الجريمة الإلكترونية عن غيرها، فقط إنتشرت مكاتب تقوم بأعمال السرقة والقرصنة من خلالها يقوم بعض الأشخاص بإستئجار قراصنه محترفين لسرقة بيانات الشركات العالمية مقابل مبالغ من المال وبيعها لأشخاص مستفيدين، كل هذه الأعمال غير مشروعة، وإن من الأسباب الكافة في صعوبة إكتشاف وإثبات هذه الجرائم عدم تقديم شكاوي من قبل أصحاب الشركات التي يتم إختراقها، وذلك خوفاً على سمعة الشركة وعلى المستثمرين فيها[29].

خامساً: الجرائم الإلكترونية جرائم الأذكياء:

الجريمة الإلكترونية جريمة ناعمة وذلك لسهولة إرتكابها دون أي مجهود يذكر بخلاف الجريمة التقليدية التي تطلب مجهود بدني مثل القتل والسرقة والإغتصاب، فالجرائم الإلكترونية لا تتطلب سوى علم كافي بالجوانب الفنيه والتقنيه للجهاز الإلكتروني، وتعتبر الجرائم الإلكترونية جرائم مغرية لسرعة تنفيذها وسهولة محو أدلة الأدانة فيها، فهي تنفذ عن بعد دون التواجد في مسرح الجريمة، ولا تتطلب سوى ضغط مفتاح معين في الجهاز لتنفيذها، ومن مغريات هذه الجرائم المكاسب المادية الضخمة التي تحققها في وقت قصير، خاصةً الموظفين الذين يعملون في الشركات التي تعتمد على النظام الإلكتروني في عملها، فمن السهل لديهم اختراق الأجهزة والبرامج وتحقيق مأربهم[30].

الفرع الثاني: خصائص المجرم الإلكتروني

المجرم الإلكتروني شخص طبيعي، لدية قدرة على تشغيل الحاسب الآلي واستخدامه، وليس المقصود بالقدرة هنا هو الخبرة العالية، ولكن القدرة هنا تتمثل بمعرفة كيفية إرتكاب الجريمة من خلال الحاسب الآلي[31] وهناك مجموعة من الخصائص التي يتميز بها المجرم الإلكتروني.

أولاً: المجرم الإلكتروني أنسان إجتماعي

المجرم الإلكتروني فئة فريدة من نوعها في عالم الأجرام، كون هذا المجرم إنسان غير عنيف خلافاً للمجرمين التقليديين فهو يتمتع بذكاء حاد مما يساعده على التكيف مع أفراد المجتمع دون قلق أو حيرة، فهو يرتكب جريمته بكل هدوء وتروي ثم يمحو أثارها بسهولة ويسر، فيكون في لحظة إنسان طبيعي وفي لحظة أخرى مجرم محترف.

وكثيراً مما يدفع المجرم الإلكتروني إلى إرتكاب جريمته هو الإنتقام من رب العمل الذي طرده من عمله أو بدافع اظهار قدرته على إختراق الإجهزة والمواقع أو بدافع له أو النصب أو بدافع مادي[32].

ويكون المجرم الإلكتروني متكيف إجتماعياً، فهناك من يرى بأنه كلما زاد خطورته الإجرامية زادت قدرته على التكيف مع المجتمع[33].

وفي كثير من الأحيان يعود المجرم الإلكتروني لإرتكاب جريمتة مرة أخرى، فهو مجرم عائد للإجرام، وذلك رغبة منه في التحدي لسد الثغرات التي أدت إلى تقديمه للمحكمة في المرة الأولى، وقد يؤدي عودته للإجرام تقديمه للمحكمه مرة أخرى، كما أن المجرم الإلكتروني لا علاقة له بالجرائم التقليدية في كثير من الأحيان، فهو يرتكب الجرائم الإلكترونية وحدها دون غيرها[34].

ثانياً: المجرم الإلكتروني مجرم ذكي ومتخصص

من أهم ما يميز المجرم الإلكتروني أنه مجرم يتمتع بذكاء حاد، لا نجد هذا الذكاء في المجرمين التقليديين الذي في الغالب ما يترك أثراً ليدلوا عليهم، بخلاف المجرم الإلكتروني فقد ألم بجميع الجوانب الفنية والتقنية لجريمته، مما يساعد في التخلص من أدلة إدانتة في وقت سريع وبدون جهد يذكر، وهذا هو حال أغلب هؤلاء المجرمين، قد تكون الخبرة لدى المجرم الإلكتروني محدودة فقط في نطاق المامه بظروف الجريمة، فإذا كانت خبرة المجرم قليلة فالجرائم التي يرتكبها لا تتعدى الأتلاف أو نسخ البيانات والبرامج، أما إذا كان المجرم على مستوى عالي من الخبرة فقد يرتكب جريمة إختراق الأجهزة أو جريمة التجسس الإلكتروني أو يزرع الفيروسات أو يسرق الأموال[35] وتبين من خلال الكثير من القضايا أن المجرمين الإلكترونيين هم مجرمين متخصصين، أي أنهم متخصصين في جرائم الإنترنت والكمبيوتر، كما أن هؤلاء المجرمين قد يتمادوا في جرائمهم إلى حد إرتكابهم الجرائم الخطيرة[36].

فالمجرم الإلكتروني يتمتع بذكاء حاد وقدرة ذهنية كبيرة في مجال التكنولوجيا والتي كسبها أما عن طريق الدراسة المتخصصه في هذا المجال، أو عن طريق الخبرة المكتسبة من الممارسة العملية للحاسوب والإنترنت، فهو من خلال قدرته تستطيع إختراق دخول أصعب المواقع والبرامج، والتي تكون في العادة محمية من قبل برامج مكافحة أو عن طريق شيفرة معينة[37].

ومما يؤكد على قدرة بعض الأشخاص الذهنية والعقلية هو إختراق الهاكرز لمواقع (دولة اسرائيل) ومواقعها الحكومية، ومواقع البورصة والجامعات والمصارف، والتي تسببت في إيقاف بعض المرافق الحيوية مثل التيار الكهربائي والإشارات الضوئية والبنوك، وإستخدام هذا الأسلوب الحديث كنوع من أنواع المقاومة في وجه الأحتلال[38].

المبحث الثاني: الأطار القانوني للجريمة الإلكترونية

سنبين من خلال هذا المبحث الملامح التي توضح لنا الأطار القانوني للجرائم الإلكترونية، وهذا يتطلب بيان أركانها وتحديد أطرافها ومحلها وآليات تنفيذها.

المطلب الاول: أركان الجريمة الإلكترونية

تقوم الجريمة بشكل عام على أركان ثلاثة هي:

عي: هو الصفة غير المشروعة للفعل وتشمل قاعدة التجريم والعقاب للجرائم الإلكترونية فيما ورد النص عليه في قانون جرائم أنظمة المعلومات الأردني.

الركن المادي: وهو ماديات الجريمة التي تبرز إلى العالم الخارجي.

الركن المعنوي: وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ[39].

الفرع الأول: الركن المادي في الجرائم الإلكترونية

من المشكلات العملية التي تثيرها الجريمة الإلكترونية طبيعة الركن المادي في الجريمة الإلكترونية، ذلك أن مفهوم ومناط التجريم ينصب على نظام الإلكتروني يساء أستعماله أو يتم أقتحامه على نحو غير مشروع، مما يكون لذلك الأستعمال أو الأقتحام من أثر مادة ملموس يظهر أما في صورة تدمير للمعلومات، وهو ما يشير أمكانية الإتلاف العمدي للمنقولات، أو السرقة ذلك عن طريق إساءة أستعمال بطاقات الإئتمان، أو يثير شبهة التزوير عن طريق التلاعب في بيانات الحاسب الآلي.

إن السلوك الإجرامي في الجريمة الإلكترونية، يرتبط دائماً بالمعلومة المخزنة على الحاسب الآلي، أو تلك التي يتم إدخالها الحاسب الآلي، وصعوبة المشكلة إن السلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب فيتم تدمير النظام المعلوماتي، أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك أو إساءة استعمال بطاقات الإئتمان[40].

إن السلوك الإجرامي يوصفه عنصراً في الركن المادي في الجريمة التقليدية يتم رؤيته رؤى العين، والتأكد منه كفعل القتل أو السرقة أو التزوير، ولكن صعوبة الجريمة الإلكترونية، والركن المادي فيها خاصةً إن الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي لا يمكن الأمساك مادياً بها، تماماً مثل التيار الكهربائي الذي يسري في توصيله دون ان نراه[41].

لذلك يتعين تحليل السلوك الإجرامي في الجريمة الإلكترونية خاصة ما يتعلق فيها بفكرة المال في الجرائم الإعتداء على المال العام أو الخاص، كما لابدّ من العرض لصور السلوك الإجرامي في الجريمة الإلكترونية.

إن النشاط أو السلوك المادي في الجريمة الإلكترونية يتطلب وجود بيئة رقمية وجهاز كمبيوتر وإتصال بشبكة الإنترنت ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، فعلى سبيل المثال يقوم مرتكب

الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج إختراق أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالأداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة أعداد برامج فيروسات تمهيداً لبثها، وليس كل جريمة تستلزم وجود أعمال تحضيرية وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت. حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية. إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج إختراق، ومعدات لفك الشيفرات وكلمات المرور، وحيازة صور دعارة للإطفال، فمثل هذه الأشياء تمثل جريمة في حد ذاتها[42].

إن النشاط والسلوك المادي في الجريمة الإلكترونية يعّد محلاً لتساؤلات عديدة فيما يتعلق ببدايته أو الشروع في إرتكاب الجريمة، ومثل هذا النشاط يختلف عما هو الحال عليه في العالم المادي، فإرتكاب الجريمة عبر الإنترنت يحتاج بالضرورة إلى منطق تقني، وبدونه لا يمكن للشخص حتى الإتصال بالإنترنت، سواء كان بقصد إرتكاب جريمة أم لمجرد التصفح أو الدخول في الإتصال المباشر كالمحادثه وغيرها.

وهذا السلوك المادي الإيجابي المتمثل في المنطق التقني يجعل الجريمة عبر الإنترنت ذات طابع موحد بالضرورة، فهي تباشر من حيث السلوك أو النشاط المادي فيها، كأحدى عناصر الركن المادي يضاف إليه فلسفة الركن المادي في الجريمة، مثل هذا الأمر تداركه المشرّع الأردني حين نص على جرائم يمكن أن ترتكب على الكمبيوتر، ففي مثل هذه النصوص نجد المشرّع الأردني يقرر صراحة عبارة..."إذا أرتكبت الجريمة بإستخدام نظام معلوماتيه أو الشبكه المعلوماتية... أو عبارة ... بإستخدام المعالجة الآلية للبيانات ففي مثل هذه الحالات يكون المشرّع الأردني مدركاً لمسألة الشروع في إرتكاب جريمة عبر الشبكة المعلوماتية المرتبطه بالإنترنت[43].

لذلك يعتبر الدفع بعدم وجود قدرات تقنية حال الإتهام بإرتكاب جريمة عبر الإنترنت من الدفوع الموضوعية الجوهرية التي تلتزم محكمة الموضوع بالرد عليه تفصيلاً وإلا___ عاب حكمها غيباً في التسبب بما يسمح قبول نقضه، ولقد جعلت الطبيعة الموحدة للجريمة عبر الإنترنت من حيث إتحاد جميع أشكالها المادية في ضرورة إستخدام الآلة كوسيط إلى إرتكابها إن أتصفت هذه الجريمة بالضرورة بالطابع التقني[44].

ولكي يتوافر الركن المادي في الجريمة الإلكترونية، فلا بدّ من حصول النتيجة الإجرامية على أن ترتبط بالسلوك الإجرامي بعلاقة سببية.

الفرع الثاني: الركن المعنوي للجريمة الإلكترونية

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالركن المعنى هو المسلك الذهني أو النفسي للجاني بإعتباره محور القانون الجنائي، ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية، من علم وإرادة آثمة وقصد جرمي مع أقرار حق الدولة في العقاب الذي يبنى على هذه المقدمات، لذلك يمكن تعريف الركن المعنوي بأنه: العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها، وهذه العلاقة هي محل الإذناب في معنى إستحقاق العقاب، ومن ثم يوجه إليها لوم القانون وعقابه[45].

ويتوفر القصد الجنائي في حق الجاني في حالات ثلاثة هي[46]:

: إذا كان الجاني يتوقع ويريد أن يترتب على فعله أو إمتناعه حدوث الضرر أو وقوع الخطر الذي حدث والذي يعلق عليه القانون وجود الجريمة.

: إذا نجم عن الفعل أو الإمتناع ضرر أو خطر أكثر جسامة مما كان يقصده الفاعل وهي حالة جواز القصد الذي ينص عليه القانون صراحةً على إمكان إرتكابها بهذا الوصف.

: الحالات التي يعزى فيها القانون الفعل إلى الفاعل نتيجة لفعله أو إمتناعه، أي حالات يفترض فيها القانون توافر القصد الجنائي لدى الجاني إفتراضاً، وهو مستمد من أنه طالما أن النتيجة الجسيمة التي تحققه نشأت عن فعل الجاني، فمقتضى ذلك أن هذا الفعل كان صحيحاً لإحداثها، ولكونه كذلك فإن الجاني يجب ان يتحمل نتائجه، توقعها ام لم يتوقعها.

إن توافر الركن المعنوي في الجرائم الإلكترونية يعدّ من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلتزم تطبيقها، إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع، فمثلاً أن التمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام يعدّ تمييزاً دقيقاً.

ففي جريمة تجاوز صلاحية الدخول، فإنه يلزم لتوافرها أن يكون هناك صلاحية للدخول على نظام ما، على أن تتوافر في داخل هذا النظام أنظمة معينة ليس من حق هذا الشخص الدخول عليها، فيقوم المذكور بالدخول عليه، ففي هذه الحالة لا تتوافر سوى جريمة واحدة، حيث أن المذكور يملك صلاحية الدخول على النظام الأساسي ولا يملك الدخول على أنظمة ضالة فيها، إلا أن تكوين النشاط المادي هنا يلزم أن يكون السلوك الإجرامي مرتكباً في إطار نشاط ثانٍ وليس النشاط الأول، مثل هذا الأمر يجعل جريمة تجاوز صلاحيات الدخول معتبراً من الجرائم التي لا يتطلب فيها ركناً معنوياً، وهذا الأمر محرم قانوناً. ونتيجة لذلك فإن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب بإستخدام الإنترنت من حيث مدى تحديد ما إذا كانت تتطلب قصداً عاماً أم خاصاً، فذلك لا يمانع في تطلب قصد جنائي خاص في جريمة التهديد، إلا أنه يقر من جديد أنه يكفي بالقصد العام عن ذات الجريمة، كما هو الشأن في جريمة التهديد بالبريد الإلكتروني وعبر المجموعات الإخبارية وفق ما هو مقرر في القسم والقصد العام فيها، بينما يتم إستدلال معالمه من النظرة الموضوعية إلى السلوك الشخصي من مجموعة الظروف المحيطة بالجريمة بما في ذلك فحص الحالة العقلية لمرتكب الجريمة[47].

أما في القضاء الفرنسي فإن منطق سوء النية يكتسح النصوص التي تطبق بشأن الإنترنت، حتى أن هذه الجرائم لا يمكن أن تدخل حيز التطبيق ما لم يتوفر سوء النية في منطق القصد الخاص وإرادة الإضرار، ومن ذلك ما هو مقرر في المادة (15 - 2226 عقوبات فرنسي جديد) التي تشترط سوء النية حين وجود عدوان على البريد الإلكتروني، وبما يجعل ذلك بالضرورة متطابقاً مع ما هو مقرر في المادة (5 – 2 – 1 -32 L) من تقنيين البريد والإتصالات الصادر بالقانون المؤرخ 26 / 7 / 1996 التي تلزم وزير الاتصالات الفرنسي بالسهر على مبدأ إحترام سريه الإتصالات[48].

كذلك الحال لدى المشرع البريطاني فالركن المعنوي في الجريمة الإلكترونية يتطلب أن تنصرف إرادة الجاني نحو الدخول إلى البيانات أو المعطيات المخزنة في أي حاسوب، إذ جرم المشرّع البريطاني الدخول غير

المصرّح به للنظام الإلكتروني بموجب المادة الأولى من قانون إساءة إستخدام الحاسوب البريطاني لعام 1990 وكذلك جرم الدخول غير المصرح به إلى النظام الإلكتروني بهدف إرتكاب جريمة أخرى بموجب الماده الثانية من نفس القانون[49].

المطلب الثاني: صور الجريمة الإلكترونية

صنف الفقهاء والباحثين الجرائم الإلكترونية إلى عدة تقسيمات فمنهم من صنفها إلى جرائم بواسطة الحاسب الآلي ومنهم من قسمها إلى جرائم ترتكب على المعلومات والبيانات الحاسوبية ومنهم من قسمها نسبةً إلى الهدف من الجريمة وهناك الكثير من التقسيمات والتصنيفات.

أول: يقصد بجرائم نظام ووسائل شبكات المعلومات الجرائم التي تقع على المكونات المعنوية للحاسب الآلي من بيانات ومعلومات قبل إختراق الحاسب الآلي أو الشبكة إما مجرداً، أو بهدف تخريب المعطيات والأنظمة، أو خلق البرامج الضارة التي تنقل عبر الحاسب الآلي، أو الشبكة إما مجرداً، أو بهدف إرتكاب جريمة أخرى مثل تخريب المعطيات والأنظمة أو خلق البرامج الضارة التي تنقل عبر الحاسب الآلي **والشبكات وغيرها من الجرائم الأخرى**[50].

وأكثر الجرائم التي تتعلق بالأنظمة والمعلوماتية جريمة الدخول غير المصرح به، ويقصد بها وجود هجمات على معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المحتوى، أو تعطيل قدرة وكفاءة الأنظمة للقيام بأعمالها، وتتطلب هذه الجريمة وجود ركن مادي ومعنوي، ويتمثل الركن المادي بفضل الدخول الذي يطلق عليه الدخول المنطقي، وذلك بغرض فتح باب يؤدي إلى نظام الكمبيوتر بمكوناتة المنطقية، أما الركن المعنوي فيتمثل بالقصد الجنائي كون هذه الجريمة من الجرائم العمدية فيجب توافر العلم والإرادة للجاني عند دخوله الغير مصرح به النظام[51].

ومن الجرائم الإلكترونية التي تستهدف أنظمة المعلوماتية نفسها تلك التي تكون الغاية منها الدخول إلى أنظمة المعلومات والمواقع على شبكة الإنترنت بهدف إلغاء أو حذف أو إضافة أو تدمير أو إنشاء أو إتلاف أو حجب، أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو إنتحال صفته أو إنتحال شخصية مالكه فكل هذه التصرفات تعد من الجرائم الإلكترونية التي تضر بالغير[52].

ومن أمثلة جرائم الإختراق التي تتعلق بأنظمة المعلوماتية والشبكات جرائم تدمير المواقع وإختراق المواقع الرسمية، وإختراق الأجهزة الشخصية وإختراق البريد الإلكتروني للآخرين أو الإستيلاء عليه أو إغراقه[53].

وجميع هذه الجرائم تبدأ بإنتهاك خصوصية الشخص وهذا سبباً كافية لتجريمها، فضلاً عن إلحاق الضرر المادي والمعنوي بالمجني عليه[54].

وفي أطار ذلك نص قانون العقوبات الفرنسي على أن جرائم نظم المعلومات هي (إدخال البيانات بطريقة الغش في نظام المعالجة الآلية أو محوها أو التعديل بطريقة الغش للمعطيات التي يحتويها) يعاقب بالحبس لمدة ثلاث سنوات وبغرامة قدرها 300.000 فرانك[55] ونص مشروع القانون العربي لمكافحة سوء إستخدام تكنولوجيا المعلومات والإتصالات على تعريف إتلاف البرامج بأنها: "تدمير البرامج الإلكترونية سواء أكان كلياً

أو جزئياً أو إتلافها على نحو يجعلها غير صالحة للأستعمال[56] وخلاصة القول أن الجرائم المتعلقة بأنظمة المعلومات والشبكات تنصب بدخول المواقع أو الأجهزه بطريقة غير مشروعة أو بطريقة مشروعة، كما لو تمت الجريمة من قبل موظف مختص وإتلاف البيانات أو سرقتها أو نسخها أو تبديلها أو نشر فيروس يؤدي إلى ما ذكر، وقد تتعدد أسماء وأشكال الجرائم التي تستهدف أنظمة المعلومات ولكن كلها تدور في حلقة واحدة، فهذه الجرائم قد تتغير أساليب وطرق إرتكابها مع التطور التكنولوجي، ولكن في النهاية فإنه يعاقب على إرتكابها بنص قانوني واحد إلا إذا ظهرت جريمة جديدة لم تكن متوقعة ولم تغطيها النصوص القانونية.

ومن الفيروسات الشهيرة التي أنتشرت على شبكات الإنترنت وتسببت في خسائر كبيرة لمستخدمي الإنترنت فيروس حصان طرواده، حيث أطلق أسم حصان طرواده على أحد الفيروسات التي هاجمت أجهزة أربع دول وهي أنجلترا النرويج والسويد والدنمارك، ومن نماذج فيروس حصان طرواده التي ظهرت من النصف الأول من عام 1990، وكان هذا الفيروس يصل الأجهزه عن طريق البريد الإلكتروني ويهدد صاحب الجهاز بأن يرسل الفيروس إلى أجهزه أخرى وأن يتم إرسال مبلغ 378 دولار، وإلا يتم محو البيانات والملفات المخزونة على الهارد ديسك، وبالفعل كان يتم محو بيانات الجهاز الذي أصيب بالفيروس[57].

الفرع الثاني: الجرائم الواقعة على الأموال والإتصالات

بيّن الواقع أن الجرائم الواقعة على الأموال والإتصالات من أخطر الجرائم الإلكترونية الحديثة، كون هذه الجرائم توقع خسائر مادية ضخمة، فالجرائم المالية التقليدية لا تتم الإ بالسطو على البنوك والشركات، وهي تحتاج فقط إلى شخص متخصص في برامج الحاسب الآلي، وهي لا تحتاج إلى مجهود جماعي بل يكفي شخص أو أثنين لإرتكاب الجريمة، كما أن الجرائم الإلكترونية توقع خسائر أكبر بكثير من الجرائم التقليدية، وكذلك الأمر بالنسبة للجرائم المتعلقة بالإتصالات.

ومن الجرائم الواقعة على الأموال جرائم سرقة الأموال والبيانات والبرامج والخدمات الإلكترونية، وتتطلب هذه الجرائم توافر الركن المادي المتمثل في فعل الإختلاس لمال منقول مملوك للغير، وكذلك لا بد من توافر الركن المعنوي المتمثل في القصد الخاص للجاني في نيته لتملك الأموال أو البيانات المسروقة[58].

ومن أمثله الجرائم المالية الإلكترونية السحب عن طريقة بطاقة الصراف الآلي، فمن الممكن، أن يقوم شخص بتزوير بطاقة صراف آلي والسحب عليه من خلال البنوك، وتعد هذه الحالة من حالات السرقة والتي تتم عن طريق وسيلة إلكترونية وهي بطاقة الصراف الآلي[59].

وفي فرنسا قضت محكمة الجنح حكماً يتعلق بموظف قام بنسخ برامج معلوماتية تتعلق بشركة بيجو على قرص إلكتروني ومن ثم أستخدم هذا البرامج لدى شركة أخرى عمل لديها بعد أن ترك عمله في شركة بيجو وأدانته المحكمة بالسرقة على أساس سرقة البرامج الإلكترونية[60].

ومن الجرائم المالية الإلكترونية لعب القمار عبر الإنترنت حيث يوجد أكثر من ألف موقع للقمار على شبكة الإنترنت والذي يسمح لمرتاديه بلعب جميع أنواع القمار الموجود في أنديه القمار، وينفق الأمريكيين ما يقارب مليار دولار للعب القمار عبر الإنترنت[61].

وفي التشريع الإماراتي نص المشرّع في المادة 11 من القانون الأتحادي رقم 2 لسنه 2006 في شأن مكافحة جرائم تقنية المعلومات في الإمارات على أن "كل من أستخدم الشبكة المعلوماتية أو أحدى وسائل تقنية المعلومات، في الدخول دون وجه حق، إلى أرقام أو بيانات بطاقه إئتمانية أو غيرها من البطاقات الإلكترونية يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين وتكون عقوبة الحبس مدة لا تقل عن سنة والغرامة لا تقل عن 30 الف درهم أو إحدى هاتين العقوبتين إذا توصل من ذلك إلى الإستيلاء لنفسه أو لغيره على مال الغير[62]".

ومن أخطر الجرائم الإلكترونية المالية جريمة غسل الأموال عبر الإنترنت، حيث بدأت عملية غسل الأموال من تجارة المخدرات والمقامرة والجنس وغيرها من الجرائم، ومن المجالات التي يتم من خلالها غسل الأموال عبر المضاربة في البورصة والتجارة في العقارات والأراضي والشقق ومجال المزايدات والمناقصات الحكومية وشراء التحف الثمينة والهدايا والمجالات في هذا الشأن لاحصر لها[63].

وتنصب الجريمة الإلكترونية على الإتصالات سواء الخلوية أو خطوط الهاتف أو الإنترنت فالمجرم الإلكتروني قد يقوم بتزوير بطاقات الهاتف أو قد يستخرج أرقام بطاقات الشحن التي لم تستخدم من خلال حسابات ومواقع الشركات الخلوية، وقد يصل إلى الحصول على خط إنترنت دون علم الشركة ففي الإمارات أدين مهندس فني كان يعمل في إحدى شركات الحاسب الآلي، حيث أمد شخص بالرقم السرّي للإنترنت الخاص بهذه الشركة والذي إستخدم الإنترنت لمدة شهرين وإدانته المحكمة على هذا الفعل[64].

الفرع الثالث: جرائم الأعتداء على الأشخاص والجرائم الجنسية

إن جرائم الأعتداء على الأشخاص وحياتهم الخاصة من أكثر الجرائم الإلكترونية إنتشاراً، وتتنوع الجرائم التي تمس بالأشخاص، فلها عدة صور وأشكال، ولكن أكثرها ما يدور حول الذّم والتهديد والتشهير عبر الإنترنت، مثل أن يقوم شخص بنشر صور فاضحة لشخص أخر بهدف تشوية سمعته والإساءة له، ولكن قد يتخذ الأعتداء على الأشخاص صور أخطر من ذلك قد تؤدي إلى القتل، فمثلاً عند قيام شخص باللعب بالنظام الإلكتروني لمستشفى حديث فقد يؤدي ذلك إلى وفاة أحد المرضى.

وتهدف الجرائم التي تمس بالأشخاص الحط من مكانتهم الإجتماعية والإساءة المباشرة أو غير المباشرة لهم، ويتمثل الركن المادي في هذه الجريمة بتصرف مادي يصدر عن الفاعل الأمر الذي يتطلب مشاهدة وإدراك هذا التصرف من الغير وهو وما يشار إليه بمصطلح العلانية[65].

وإن أكثر الجرائم التي تنتشر عبر الإنترنت هي جرائم الذم والتهديد والتشهير، حيث يعد الإنترنت أفضل بيئة لمثل هذه الجرائم نظرا لسرعة التنفيذ والبعد المكاني بين الجاني والمجني عليه، ويفضل الكثير من المجرمين إرتكاب هذه الجريمة عبر الإنترنت لصعوبة الكشف عن هويتهم وإيقاعهم تحت طائلة المسؤولية، وترتكب مثل هذه الجرائم للطعن في شرف الغير أو بدافع الإنتقام أو لدفع الناس للحقد وبغض شخص معين، كما أن هذه الجرائم ترتكب على عدة أشكال كتابية أو سمعية أو مرئية[66].

ومن صور جرائم الإعتداء على الأشخاص، جريمة الإعتداء على حرمة الحياة الخاصة، فللحياة الشخصية خصوصية وحرمة لا يجوز لإي شخص أن يقتحمها، ومثل ذلك الإعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الإطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة خلال الإطلاع على البيانات والمعلومات الخاصة بشخص ما أو تسجيل مكالمات أو فيديو أو مراقبته[67].

الفرع الرابع: جرائم الأمن العام وتجاره الرقيق والمخدرات

تعد حرب المعلومات من الحروب الجديدة التي ظهرت بظهور الحاسب الآلي والإنترنت، فتتنافس اليوم الدول العظمى فيما يعرف بالحرب الإلكترونية بشأن إختراق كل دولة أجهزة الدولة الأخرى للحصول على المعلومات التي تتعلق بالشؤون العسكرية والأمنية والأقتصادية، وكما نعلم أن الإنترنت خرج من رحم المؤسسة العسكرية وظهر معه المحتوى المعلوماتي الرقمي العسكري والذي يتعلق بكل كبيرة وصغيرة داخل المؤسسة العسكرية والتي هي اليوم الهدف الأساسي في الحرب الإلكترونية[68]. ومن خلالها ظهرت صور التجسس الإلكتروني والذي يهدف إلى التجسس على الدول للحصول على المعلومات التي تتعلق بالأسلحة الجديدة وغيرها من المعلومات الأمنية والعسكرية.

ومن الجرائم التي تهدد الأمن العام جريمة التجسس الإلكتروني والذي يتخذ الركن المادي فيها صورة سلوك الجاني في إستعمال نظام إلكتروني معين قادر من خلاله الدخول إلى حافظة السر الإلكتروني، وتمكنه من الأطلاع عليها أو نسخها، أما الركن المعنوي فيتمثل بالقصد العام وكذلك تتطلب هذه الجريمة وجود قصد خاص يرغب من خلالها الفاعل إيقاع ضرر بالدولة أو بالنظام العام فيها أو الإساءة لها[69].

ومن الجرائم التي تهدد الأمن العام إنشاء مواقع على الإنترنت تعمل على نشر الفتنة والتفرقة بين أفراد المجتمع، من خلال بث الأفكار المكتوبة أو المسموعة أو المرئية، والتي تفرق بين أفراد المجتمع من الناحية السياسية أو العقائدية أو الدينية وكذلك إنشاء المواقع التي تنشر الأفكار المعادية للدولة وتنظم الجماعات المأجورة وتروج لإفكارها وتدعو للإنضمام معها وهي في الحقيقة لا تخدم الا العدو[70].

وكشف الباحثون عن إستخدام بعض عصابات الإنترنت في تجارة الرقيق الأبيض، ومن خلال عقد صفقات لبيع فتيات من 40 دولة نامية في أوروبا الشرقية في دول الغرب، لإستخدام هؤلاء في المتعة والجنس، ويتم ذلك بإرسال كتالوجات متضمنة صور الفتيات صفاتهن وأسعارهن، وقد يتم عقد لقاءات بين الفتيات والأشخاص الراغبين بالشراء، وتربح هذه العصابات الملايين من الدولارات التي يتم إستخدامها فيما بعد في عمليات غسل الأموال[71].

وفي إطار ذلك عقد المؤتمر الدولي لمكافحة إستغلال الأطفال في الجنس عبر الإنترنت، في الفترة من 29 سبتمبر الأول من أكتوبر 1999 في مدينة فيينا بالنمسا، وأكد المؤتمر على ضرورة التعاون الدولي لمكافحة هذا النوع من الجرائم، والعمل على ضبط شبكات الإنترنت من موردي الخدمة، مع توفير خطوط إتصال للأبلاغ عن مثل هذه الحالات[72].

وفي التشريع السعودي نص المشرع في المادة 6 على أنه يعاقب بالسجن مدة لا تزيد عن خمس سنوات وبغرامة لا تزيد عن ثلاث ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيا من الجرائم

المعلوماتية الأتيه، إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للإتجار في الجنس البشري، أو تسهيل التعامل به[73].

وفي العصر الحديث ظهرت طرق لم تكن في الحسبان تدفع الشخص لإدمان المخدرات، فقد ظهر على الإنترنت مواقع تختص للتحفيز على تعاطي المخدرات والترغيب إليها، ولم يصل الأمر إلى ذلك فقط بل تعدى إلى نشر طرق زرع المخدرات بكافة أنواعها، وكيفية تحضيرها بأبسط الطرق[74].

وفي التشريع السوداني نص المشروع في المادة 21 على أنه "كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أحد أجهزه الحاسوب أو ما في حكمها بقصد الإتجار أو الترويج للمخدرات أو المؤثرات العقلية أو ما في حكمها أو يسهل التعامل فيها، يعاقب بالسجن مدة لا تتجاوز 20 سنه أو بالغرامة أو بالعقوبتين معاً[75].

المطلب الثالث: صور الجريمة الإلكترونية في دولة الإمارات العربية المتحدة

أصدر المشرع الإماراتي قانون مكافحة الشائعات والجرائم الإلكترونية في سبتمبر عام 2021 عرف بموجبه بأنواع الجرائم الإلكترونية وأبرز صور هذه الجرائم نوردها كالتالي:

السب والقذف عبر وسائل التواصل الإجتماعي

لعل أهم ما يميز دولة الإمارات العربية المتحدة أن لديها مجموعة متكاملة ودقيقة من أدوات التصدي لكل صور الجرائم الإلكترونية وفي مقدمة ذلك قوانين وتشريعات تنظم الأنشطة المنفذة على شبكة الإنترنت. ودائماً وأبداً كانت دولة الإمارات المتحدة تحارب الجرائم، وتضرب بيد من حديد بوضعها القوانين والتشريعات التي تساعد على الحد من الجريمة، وكان من بين هذه القوانين قانون مكافحة الجرائم الإلكترونية الذى جاء للحد خاصةً من جرائم السب والقذف عبر وسائل التواصل الإجتماعي.

الأستفزاز الإلكتروني

رغم أن هذا القانون نجح بالفعل في الحد من هذه الجرائم، إلا أن البعض من مشتغلي الظهور ببرامج التواصل الإجتماعي أساء أستخدامه، والتحايل على أحكام القانون من خلال الأستفزاز الإلكتروني، وذلك ببث مواد أعلامية من شأنها إثارة المتابعين مثل:

الظهور في مظهر يخدش الحياء أو يخالف العادات والتقاليد في المجتمع، من شأنها أن تستفزهم وتخرجهم عن شعورهم وحملهم على كتابة التعليقات التي من شأنها أن تضعهم تحت المساءلة القانونية دون توافر للقصد الجنائي لديه.

وبالفعل نجد أنه على مستخدمي مواقع التواصل الإجتماعي أن يتوخوا الحذر بمشاركاتهم من خلال هذه المنصات حتى لا يقعوا في مصيدة تحايلهم. وأن يكونوا أكثر وعياً وإدراكاً بالعواقب الوخيمة التي تنتظرهم.

وهنا يأتي دور ناشر المادة محل التعليق ليقوم بتوجيه الإتهام للمتابعين؛ مستغلاً قانون مكافحة الجرائم الإلكترونية مستهدفاً بذلك الحصول على تعويضات مادية نظير التنازل عن توجيه الإتهام للمتابعين.

جريمة سرقة الهوية

تشتمل الجرائم الإلكترونية أيضاً على جريمة سرقة الهوية، وهي جريمة تتمثل في إستخدام مرتكب هذا الجرم للمعلومات الشخصية بدون وجه حق مثل الصور الشخصية وأرقام بطاقات الإئتمان الخاصة بشخص أخر دون موافقة مسبقة منه، للحصول على فائدة مالية أو أي فائدة أخرى أو تحقيق عوائد غير قانونية.

وعادة ما يحدث من خلال قيام مرتكب هذا الجرم بإرسال رسائل إلكترونية غير حقيقية على أنها من جهة ذات ثقة، مثل شركة ما، أو مصرف، مثل طلب تحديث البيانات الشخصية للمستخدم وفور الإرسال يقوم مرتكب هذا الجرم بسرقة الهوية الشخصية.

ترويج المخدرات عبر وسائل التواصل الإجتماعي

تصدى قانون مكافحة المخدرات والمؤثرات العقلية رقم 30 لسنة 2021 والذي تبنى سياسة جنائية صارمة ومتكاملة لمكافحة إنتشار وتعاطي المواد المخدرة والمؤثرات العقلية تقوم على مبدأ العقوبة والردع والعلاج والتأهيل للجاني.

وتصدى للأساليب المستحدثة من ترويج المخدرات وشراءها عبر "وسائل التواصل الاجتماعي" وتضمن عقوبات رادعة.

وأعتبر فعل أيداع الأموال أو تحويلها إلى البائع أو المروج للمواد المخدرة متى كانت بقصد شراء المواد المخدرة أو المؤثرات العقلية بهدف التعاطي أو الأستعمال الشخصي جنحة يعاقب مرتكبها بالحبس أو بالغرامة التي لا تقل عن خمسين ألف درهم.

ويهدف المشرع إلى ردع من كل من تسول له نفسه إرتكاب جريمة التعاطي وزجره في حال أنصياعه إلى أصدقاء السوء أو من تسول له نفسه الأمارة بالسوء شراء المواد المخدرة بقصد تعاطيها أو تجربتها بدافع الفضول وذلك عن طريق إيداع الأموال أو تحويلها.

الأبتزاز الإلكتروني

الأبتزاز الإلكتروني يتكون من نوعين: معنوي أو مادي.

: إنه يبتزك بصورك أو مقاطع فيديو أو مقاطع تسجيلات صوتية أو حتى مستندات يمتلكها ضدك.

: بأنه يهددك أويتوعدك بإن يفضح أو ينشر أسرارك.

وهذه الجريمة جرمها المشرع الإماراتي وفقاً لقانون الشائعات والجرائم الإلكترونية وتحديداً في المادة 42.

وما هي عقوبة الابتزاز الإلكتروني؟

أن عقوبة الابتزاز الإلكتروني وفقاً للمادة 16 من المرسوم بقانون إتحادي رقم 5 لسنة 2021 في شأن مكافحة جرائم تقنية المعلومات، هي الحبس وغرامة لا تقل عن 250 ألف درهم.

وتنص المادة على أن يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن 250 ألف درهم ولا تجاوز 500 ألف درهم، أو بإحدى هاتين العقوبتين، كل من أبتز أو هدد شخصا أخر لحمله على القيام بفعل أو

الأمتناع عنه، بإستخدام الشبكة المعلوماتية أو وسيلة تقنية معلومات، وأن العقوبة تكون السجن مدة لا تزيد على عشر سنوات، إذا كان التهديد بإرتكاب جناية أو بإسناد أمور خادشة للشرف أو الأعتبار.

جريمة إنتهاك حقوق الملكية الفكرية

نتيجة الانفتاح الثقافي وإزدياد المنتجات الصناعية، أنتشرت ظاهرة إنتهاك حقوق الملكية الفكرية بشكل كبير، ومن الأمثلة التي ترتبط بها القرصنة أو تقليد علامة أو مادة أو تصميم دون إذن صاحب الملكية. ونجد أنه من المهم وقوع العقاب على من يرتكب تلك الجريمة، وحماية الملكية الفكرية لأصحاب الحق فيها خصوصاً في ظل ما يطرأ على جرائم الملكية الفكرية من تزايد كبير.

جرائم التشهير والتجسس الإلكتروني

فيما يتعلق بالتشهير الإلكتروني يقوم مرتكب تلك الجريمة بإستخدام وسائل التواصل الإلكترونية المختلفة عبر الإنترنت ووسائل التواصل الإجتماعي بنشر معلومات غير حقيقية أو تضر بشكل مباشر شخصاً، ما بصورة تلحق الضرر بسمعته من خلال نشر صور فاضحة أو خادشه، أو فيديوهات مخزية سواء حقيقية أو مزيفة أو ترويج أقوال تسيء للشخص أو الشركة أو المؤسسة عبر المنصات والوسائل الإلكترونية. أما في التجسس الإلكتروني فيقوم مرتكب جريمة التجسس بإستخدام الوسائل التكنولوجية بهدف إختراق متعمد لجهاز الشخص المستخدم، أو الأشخاص الذين يعملون الصالح مؤسسة أو شركة، والقيام بنقل المعلومات والتجسس عبر برامج أو عن طريق "التهكير" غير الأخلاقي.

الفصل الثاني: طرق الإثبات التقليدية لإستخلاص الدليل الرقمي

أمد القانون القاضي وبالأخص في المسائل الجنائية بسلطة واسعة وحرية كاملة في سبيل تقصي ثبوت الجرائم من عدمها لذلك تتعدد طرق الإثبات التقليدية، وإن كان القاضي ليس مجبراً على قبول الدليل المستمد من إجراء محدد فإن هناك إجراءات قانونية تتجسد في المعاينة والتفتيش والضبط والشهادة وندب الخبراء تستخدم بصفة عامة في سبيل التحقيق في الجريمة.

ونظراً لكون الجريمة التقليدية تختلف عن الجريمة المعلوماتية في عدة أشياء منها وقوع هذه الأخيرة في بيئة رقمية وأن أدلتها هي أدلة رقمية وليس مادية لذلك سوف يتم تبيين كيفية القيام بالإجراءات التقليدية في البيئة الرقمية لإستخلاص الدليل الرقمي.

وتختلف وسائل الإثبات التقليدية من وسائل ذات طبيعة مادية لا تظهر فيها الصفة الشخصية للشخص المتوسط بين الإجراء والدليل الذي ينجم عنه ويبرز فيها الأثر المادي دون ذاك الشخص، وإجراءات ذات طابع شخصي حيث يظهر فيها صفة الشخص الذي يتوسط بين القيام بالإجراء والدليل المتحصل عليه لذلك في إطار هذه الدراسة سيتم التركيز على الوسائل التقليدية التي تصلح للتطبيق في البيئة الرقمية ليتم إستبعاد الأعتراف والإستجواب كونها أموراً غير تقنية لا تصلح في البيئة الرقمية والحصول على دليل رقمي.

المبحث الأول : الوسائل المادية للحصول على الدليل الرقمي

يمكن القول بأن وسائل الإثبات المادية هي تلك الوسائل التي لا يظهر فيها العنصر الشخصي بقدر ما يظهر فيها العمل المادي التقني، فهي التي لا يتوقف قيامها على شخص محدد بمواصفات محددة يكون له الأثر البالغ في التقصي عن الدليل أو الحصول عليه، وإنما العمل المادي هو الذي يكون ظاهراً وأساسياً في هذا النوع من الإجراءات وهو الذي يهدف للحصول على الدليل، وتتناول في هذا الإطار كلا من المعاينة التقنية وكذا التفتيش والضبط.

المطلب الأول: المعاينة التقنية:

يعتبر المكان الذي أرتكبت فيه الجريمة الوعاء الأساسي الذي يحوي على أدلة الجريمة، لذا كان من الواجب على مأمور الضبط القضائي "ضابط الشرطة القضائية" الأنتقال إلى ذلك المكان لمعاينته وإثبات الآثار المادية للجريمة[76]، وبالتالي كل ما يؤدي إلى كشف الحقيقة، وكذا ضرورة إخطار النيابة العامة فوراً بإنتقاله لكي تنتقل بدورها إلى محل الجريمة في الجرائم المتلبس بها[77].

الفرع الأول: المقصود بالمعاينة في هذا الإطار سيتم التطرق إلى:

تعريف المعاينة: المعاينة في اللغة تعني النظر إلى الشيء، ويقال عاينه معاينة وعياناً أي لم يشك في رأيته إياه، ورأيت فلان عيانا أي واجهته، وهي بذلك تعني المناظرة والمشاهدة[78].

المعاينة اصطلاحاً: لم يحدد المشرع المقصود من المعاينة الأمر الذي دعا الفقه للتصدي لها، حيث عرفها البعض رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة[79]، كما عرفها البعض الآخر بأنها "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة[80].

والمعاينة من الوجهة القانونية إجراء استقصائي كاشف لأبعاد الجريمة وأركانها، وتعد المعاينة من أهم إجراءات التحقيق فهي عصبه ودعامته، كونها تعبر تعبيراً صادقاً لا تكذب ولا تحابي ولا تخدع، فتعطي للمحقق صورة صحيحة واقعية لمكان الجريمة، وللمعاينة أهمية في عالم التحقيق في وقوع الجرائم، فهي تؤكد وقوع هذه الأخيرة أو نفيها، وصدق أقوال أطراف الواقعة وتحديد الوصف القانوني للواقعة، ومن الناحية العملية تساعد المحقق على معرفة وقت إرتكاب الجريمة، ومعرفة العلاقة بين الجاني والمجني عليه، وكذا أسلوب إرتكاب الجريمة[81].

ويمكن تعريفها في هذا الإطار بأنها إجراء من إجراءات الأستدلال أو التحقيق يقوم بها أشخاص محددون في القانون (ضباط الشرطة القضائية أو النيابة العامة أو قضاة التحقيق) بغية المحافظة على مسرح الجريمة وإستخلاص الأدلة منه، في سبيل التوصل لإثبات الجريمة.

وتختلف المعاينة في إطار قانون الإجراءات الجزائية عنها في إطار القانون المدني، ففي فرنسا والجزائر يتولى إجراؤها الخبير أو المحضر القضائي كما يمكن للقاضي أيضا إجراء المعاينة بنفسه وهذا طبقا للمادة 146 من قانون الإجراءات المدنية والإدارية الجزائري[82].

أما في إطار الجرائم فإن المعاينة تتولاها النيابة العامة وقضاة التحقيق، وهو ما يتضح من خلال المادة 79 من ق.إ.ج الجزائري وتقابلها المادة 90 من ق.إ.ج المصري[83].

أهمية المعاينة: وتكمن أهمية المعاين في أمرين الأول جمع الأدلة الناتجة عن الجريمة (آثار الجريمة)، والثانية وقوف المحقق بنفسه على مسرح الجريمة لتتكون لديه فكرة واضحة عن كيفية وقوع الجريمة، وبهذا توصف المعاينة بأنها دليل مباشر تفوق في أهميتها اعتراف المتهم إذ هي أقوى الأدلة الجنائية التي يطمئن إليها المحقق لكونها لا تكذب ولا تحابي وتعبر عن الواقع تعبيراً صادقاً[84].

والمعاينة رغم أهميتها إلا أنها ليست لازمة في كل الجرائم، فهي ليست إجراء تلقائي في مباشرتها بل إجراء هادف غايته الكشف عن العناصر المادية التي تتعلق بالجريمة، فإذا انعدم ذلك الهدف كما هو الحال في جريمة السب مثلاً لم يكن ثمة مجال لإجرائها[85].

وإذا كانت المعاينة تتم بالإنتقال إلى محل الواقعة الإجرامية كقاعدة عامة إجرائية مقررة إلا أنه في إطار جرائم الإنترنت فإن الإنتقال لا يكون بالضرورة عبر العالم المادي وإنما عن طريق العالم الأفتراضي، فيستطيع عضو التحقيق أن يقوم بالمعاينة من مكتبه بالمحكمة من خلال الحاسب الآلي الخاص به أو من خلال مقهى الإنترنت أو من مقر مزود الخدمة الذي يعتبر أفضل مكان يتم من خلاله إجراء المعاينة، كما يجب أن يعجل بإجرائها خشية ضياع الأدلة[86].

وقد أجاز المشرع الأمريكي لعضو النيابة العامة أن يعجل بإجراء المعاينة خشية ضياع الأدلة وذلك بإرسال رسالة إلى مزود خدمة الإنترنت يلزمه فيها بتتبع السجلات المطلوبة إلى حين صدور أمر المحكمة بذلك[87].

ورغم أهمية المعاينة في إطار الجرائم التقليدية إلا أنها لا تتمتع بنفس الأهمية في مجال الحصول على الدليل الرقمي لعدة إعتبارات منها:

أن الجرائم المعلوماتية لا يترتب عنها غالباً أثار مادية فالدليل هنا رقمي وغير مرئي.

تردد عدد كبير من مستعملي الشبكة المعلوماتية على مسرح الجريمة مما قد يؤدي إلى جهل هوية الفاعل الحقيقي.

مشكلة تبخر الدليل الإلكتروني الذي يمكن تعديله أو إزالته بسهولة ومن على بعد[88].

الفرع الثاني: إجراءات معاينة مسرح الجريمة الإفتراضي: والمعاينة في جرائم الإنترنت أشكال مختلفة بحسب نوعية الجريمة المرتكبة على أن هناك طرقاً عامة تتوافق مع طبيعة الإتصال بالإنترنت مثل تصوير شاشة الحاسوب impression de captures d'écran والتي قد تكون بواسطة آلة تصوير تقليدية أو عن طريق إستخدام برمجية حاسوبية متخصصة في أخذ الصور لما يظهر على الشاشة وهو ما يصطلح عليه بتجميد مخرجات الشاشة frozen، أو عن طريق حفظ الموقع بأستخدام خاصية الحفظ save as المتوافرة في نظام التشغيل، كما يمكن حفظ ذلك عن طريق خاصية history حيث أن الحاسب كلما تم الولوج إلى الإنترنت فإنه يقوم بإستنساخ نسخة من كل صفحة أو موقع يتم استدعاؤه ويقوم بحفظها، كما قد تتم المعاينة عن طريق إنزال نسخة من المصنف في جرائم العدوان على الملكية الفكرية أو التحفظ على نسخة من الصور في جرائم العنوان على الصور والعلامات، وذلك بطباعتها واستخراجها في هيئة ورقية، أو عن طريق المعاينة على الأسلوب الإرشادي لجرائم العالم الأفتراضي الذي يحدد هوية المتسلل أنطلاقاً من النقطة الأولى وهي اقتفاء الأثر[89].

وعموماً فإنه لإجراء المعاينة في الفضاء الرقمي ينبغي مراعاة عدة خطوات وإرشادات فنية لنجاح العملية والمحافظة على الدليل وهي:

القيام بتصوير جهاز الحاسب الآلي وكل ما يتعلق به من أجهزة وملحقات ويراعى تسجيل وقت وتاريخ ومكان التقاط الصور.

ملاحظة بطريقة مدققة لكيفية إعداد نظام الحاسب والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام.

حفظ الموقع باستخدام خاصية الحفظ save as أو تحميل الدليل أو نسخة منه أو طباعتها واستخراجه في هيئة ورقية أو قرص صلب أو مرن.

التأكد من سلامة الحاسب الخادم للتأكد من دقة مصدر الدليل الإلكتروني[90].

عدم التسرع في نقل المادة المعلوماتية حتى يتم توفير البيئة المناسبة لها، خاصةً التأكد من عدم وجود مجال مغناطيسي لكي لا يؤدي إلى إتلافها.

اقتصار عملية المعاينة على الأشخاص الأكفاء ممن تلقوا تدريباً كافياً لمواجهة هذا النوع من الأدلة[91].

التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة.

يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات[92].

والجدير بالذكر أنه يجب تحرير محضر بالمعاينة عن طريق كاتب، ويجب عند إجرائها إخطار الخصوم بمكان المعاينة وزمانها، علما بأن المعاينة كإجراء تحقيق يمكن أن تكون إجراء إستدلالي لو قام بها مأمور الضبط القضائي[93].

المطلب الثاني: التفتيش والضبط في البيئة الرقمية

إن الولوج إلى الأنظمة المعلوماتية للتحري والتنقيب في مجموعة البرامج والبيانات والملفات المخزنة وتلك المتصلة بنشاط إجرامي لهو في حقيقة الأمر إجراء إقتضته مصلحة وظروف التحقيق، يفيد في كشف حقيقة قيام الجريمة وإسنادها إلى فاعلها، وبالتالي يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه، ثم إن من أثار التفتيش إجراء الضبط.

الفرع الأول: التفتيش في البيئة الرقمية: رغم تعدد التعريفات الفقهية المصطلح التفتيش إلا أنها تجمع على أنه إجراء من إجراءات التحقيق، يهدف إلى البحث عن أدلة مادية الجنحة أو جناية وقعت في محل خاص يتمتع بحرمة المسكن أو الشخص[94]، ونسبتها إلى فاعلها، وفقا لإجراءات قانونية محددة.

ويعد التفتيش من أكثر الأساليب الجنائية قوة وجدلاً، كونه وسيلة فعالة للحصول على الدليل من جهة، ومن جهة أخرى يؤدي إلى إباحة انتهاك الحق في الخصوصية، فهو من أقصى الصلاحيات التي تمارسها السلطة العامة ضد المواطنين، ويعد أحد مظاهر تقييد الحريات الأساسية، لذا نجد أن أغلب التشريعات تنظمه قانوناً بل وتنص عليه في دساتيرها[95].

ونتيجة الثورة التكنولوجية وتعدد الجرائم المعلوماتية التي يتم إرتكاب أغلبها بواسطة الحاسب الآلي وشبكاته، يطرح التساؤل حول مدى قابلية الحاسب الآلي بمكوناته وشبكاته للتفتيش بغية الحصول على الأدلة

الرقمية؟ وعليه سيتم دراسة هذا الإجراء وفق ما يلي:

تعريف التفتيش: تعددت التعريفات الفقهية التي تناولت مصطلح التفتيش، فقد عرفه البعض بأنه "إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضوع التحقيق، وكل ما يفيد في كشف الحقيقة، وهو ينطوي على مساس بحق المتهم في سرية حياته الخاصة[96]".

كما عرفه آخرون بأنه "إجراء من إجراءات التحقيق يهدف إلى التوصل إلى أدلة جريمة أرتكبت فعلاً، وذلك بالبحث عن الأدلة في مستودع السر، سواء أجري على شخص المتهم أو في منزله دون توقف على إرادته[97]".

أما المجلس الأوربي فقد عرف التفتيش في الجرائم المعلوماتية بأنه: "الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني بإستخدام الوسائل الإلكترونية[98]".

أما الفقه الفرنسي فقد عرفه بأنه "بحث بوليسي أو قضائي عن عناصر الدليل عن جريمة ما، ويمكن وفقاً لقواعد قانونية خاصة أن ينفذ في المسكن الخاص بأي شخص، أو في أي مكان أخر حيث يمكن أن توجد أشياء يكون إكتشافها مفيدا في إظهار الحقيقة[99]".

وعليه يمكن القول بأن التفتيش عبارة عن إجراء من إجراءات التحري والتحقيق يقوم به موظف قضائي، أو تحت سلطة القضاء، بموجب إجراءات محددة في قانون الإجراءات الجزائية يهدف إلى الحصول على الدليل الجنائي، ومن ثم تقديمه إلى القضاء.

مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش يتكون الحاسب الآلي من مكونات مادية[100] وأخرى منطقية[101] كما أن له شبكات اتصال بعدي سلكية واللاسلكية محلية ودولية، وبالتالي وفي نطاق إجراء التفتيش الوارد على الحاسوب تكون أمام ثلاث صور وهي كالتالي :

مدى قابلية مكونات الحاسب الآلي المادية للتفتيش:

يجمع الفقهاء على أن مكونات الحاسب المادية تصلح أن تكون محلاً للتفتيش، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، حيث أن لهذا الأخير أهمية خاصة في مجال التفتيش[102]، فإذا كان موجود في مكان خاص éun lieu priv كمسكن المتهم أو أحد ملحقاته فهنا لا يجوز تعديل هذه المكونات إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم، ومع كل الضمانات التي يقررها القانون في هذا الشأن، أما إذا كانت موجودة في أماكن عامة سواء تلك العامة بطبيعتها les lieux publics par nature كالطرق العامة والحدائق ...، أو كانت من الأماكن العامة بالتخصيص les lieux publics par destination كالمقاهي والمطاعم والسيارات فإنه إذا وجد الشخص وفي حوزته هذه المكونات المادية للحاسوب فإن تفتيشه لا يجوز إلا في الحالات التي يجوز فيها تفتيش الأشخاص[103].

ومن التشريعات التي تجيز تفتيش مكونات الحاسب الآلي من خلال ما تخوله التقنيات الإجرائية لسلطة التحقيق من إتخاذ أي إجراء لجمع الأدلة، نجد المادة 487 من ق.ع الكندي[104].

كما أنه في ذات الإطار نجد نص المادة 251 من قانون الإجراءات اليوناني التي تجيز تفتيش مكونات الحاسب الآلي المادية[105].

أما قانون إساءة استخدام الحاسب الإنجليزي Computer Misuse Act الصادر في 29 جوان 1990 فإن الجرائم المدرجة في القسم الثاني[106] والثالث[107] تجيز القبض على المتهم وتفتيش محل إقامته بحثاً عن أدلة مادية دون الحاجة إلى أمر قضائي، أما الجرائم المدرجة في القسم الأول[108] فإن التفتيش لا يجوز فيها إلا بناء على أمر قضائي وعلى أسباب منطقية، وأن ثمة أدلة متعلقة بالجريمة يمكن الحصول عليها[109].

ومن القوانين من تقدم قواعد تفصيلية للتفتيش تطبق على مكونات الحاسب وبياناته مثال ذلك القسم الفرعي رقم 16/1 من قانون المنافسة الكندي الذي يسمح لحامل إذن التفتيش إمكانية أن يستخدم أي نظام الحاسب الآلي بغرض التفتيش، ويمكن أن يسجل أي بيانات في شكل مطبوعات ومخرجات[110].

مدى قابلية مكونات الحاسب المعنوية للتفتيش: أثارت هذه الصورة خلافةً بين الفقه المقارن بين مؤيد ومعارض، فإذا كان التفتيش يتم المكونات الحاسب المادية فهل الشيء الذي يتم ضبطه هو الشيء المادي أم أنه يتضمن كذلك الأشياء غير المادية.

ذهب رأي إلى أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل البيانات الإلكترونية من برامج وتطبيقات[111] ففي اليونان نجد المادة 251 من قانون الإجراءات تعطي السلطات التحقيق إمكانية فعل أي شيء يكون ضرورياً لجمع وحماية الأدلة، ويفسر الفقه اليوناني مصطلح أي شيء أنه يشمل ضبط البيانات المخزنة في حاملات البيانات المادية، وهو أيضا ما نصت عليه المادة 487 من القانون الجنائي الكندي - السالفة الذكر – طالما تتوافر أسس معقولة على قيام الجريمة[112]، وكذلك الأمر في لكسمبورج طبقاً لقاعدة أن الضبط يشمل بصفة عامة كل الأشياء التي تفيد في إظهار الحقيقة، كما أن بعض الفقهاء في فرنسا أشاروا إلى أن للبرامج كيان مادي يتمثل في نبضات إلكترونية ومغناطيسية وبالتالي فهي قابلة للتفتيش[113].

وفي ألمانيا فإنه طبقا للقسم 94 من قانون الإجراءات الجنائية فإن الأدلة المضبوطة يجب أن تكون أشياء ملموسة، وهذا لا يشمل فقط نظام الحاسب بل حتى حاملات البيانات، وهذه البيانات تنقصها بالضرورة الخاصية المادية وبالتالي لا تشكل مواد يمكن تفتيشها وضبطها، ولكن إذا تم طبع هذه البيانات أو تصويرها فوتوغرافيا فهنا تشكل محلاً للضبط وهو ما يدخل تحت القسم 161 من قانون الإجراءات الجنائية[114].

وفي رومانيا فإن التفتيش والضبط ينصب على الدعامة المادية المدون عليها بيانات الحاسب كالأشرطة المغناطيسية أو الأقراص، أما البيانات فلا يتم ضبطها، ونفس الأمر في اليابان حيث أن السجلات الإلكترومغناطيسية تكون غير مرئية ومن ثم لا يمكن ضبطها إلا إذا حولت إلى صورة مرئية عن طريق مخرجات الحاسوب مثل الطابعة، وبهذا المفهوم أخذ كل من الفقه في البرازيل والمجر وفنلندا وكذا فرنسا، حيث أن بعض الفقهاء يرون أن النبضات المغناطيسية والإشارات الإلكترونية لا

تعد من قبيل الأشياء المادية وبالتالي لا تكون محلا للتفتيش، إلا أن المشرع الفرنسي قد تنبه لهذه الإشكالية فقام بتعديل نصوص التفتيش بالقانون رقم 545 -2004 الصادر في 21 جوان 2004، حيث قام بإضافة عبارة المعطيات المعلوماتية في المادة 94 من ق.إ.ج لتصبح المادة كما يلي: يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة[115].

وقريباً من هذا موقف الفقه السائد في أمريكا والمملكة المتحدة حيث أنه لا يعتبر هذا مشكلة مادام يمكن ضبط السجلات المعالجة ذاتها للمستندات الناتجة عنها أو الحاسب في حد ذاته بافتراض أنه دليل[116], حيث أنه في و.م.أ جرى تعديل القاعدة رقم 34 وهي من القواعد الفيدرالية الخاصة بالإجراءات الجنائية سنة 1970 فأصبحت تنص على السماح بإمكانية تفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية بما يدخل ضمنها البريد الإلكتروني وجميع الوثائق التي تتضمن النسخ الضوئية ومطبوعات الكمبيوتر وفواتير التليفون وسجلات العناوين والمذكرات والمراسلات، وعليه فإنها تخضع جميعها لإمكانية ضبطها[117].

ومن التشريعات العربية التي أجازت صراحة التفتيش في نظم المعالجة الآلية للبيانات القانون الأردني في نص المادة 31/1 من ق.إ.ج وجا فيها: " مع مراعاة الشروط والأحكام المقررة في التشريعات ذات العلاقة يجوز لموظفي الضابطة العدلية الدخول إلى أي مكان يشتبه بإستخدامه لإرتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل المشتبه في استخدامها ...".

أما المشرع الجزائري فتناول هذا الإجراء في المادة 11 من القانون رقم 09-04 المؤرخ سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها [118] في الفصل الثالث المادة الخمسة (05) بعنوان القواعد الإجرائية تعاملات المنظريات. المعلوماتية، حيث أشارت المادة إلى أنه يجوز للسلطات القضائية المختصة ولضباط الشرطة القضائية في الحالات المنصوص عليها في العادة 04 من هذا القانون[119] التفتيش ولو عن بعد في:

منظومة معلوماتية أو معطيات معلوماتية مغرية فيها.

منظومة تخزين معلوماتية.

وهنا إشارة صريحة إلى التفتيش في المكونات المعنوية الحاسب الآلي.

أما الإتفاقية الأوربية المتعلقة بالإجرام المعلوماتي الموقعة في بودابست في 2001 فقد نصت على التفتيش في البيئة المعلوماتية للحصول على الأدلة الرقمية وهذا في المادة 19 الفقرة الأول والتي جاء فيها: "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى برى أنها ضرورية من أجل تخويل سلطاته المخلصة سلطة التفتيش أو الولوج بطريقة مشابهة,

لنظام معلوماتي أو لجزء منه وكذلك للبيانات المعلوماتية المخزنة فيه وعلى أرضه.

لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية[120].

من خلال الفقرة الأولى من المادة 19 نلاحظ أنها تعطي لسلطات صلاحيات التفتيش والولوج إلى البيانات المعلوماتية التي تم احتواؤها سواء في داخل نظام معلوماتي[121] أو في جزء منه أو على دعامة تخزين مستقلة، وعليه فإن تطبيق إجراء التفتيش المعلوماتي يستلزم بالإضافة إلى تفتيش النظام أن يتم تفتيش كل دعامة تخزين مشتركة كالأقراص التي تكون مجاورة لهذا النظام المعلوماتي، ويمكن التساؤل في هذا الإطار هل المادة 19 في فقرتها الأولى تنطبق على البيانات المعلوماتية المخزنة لأن الإشكال الذي يثور هو إذا ما كانت رسالة إلكترونية غير مفتوحة ومنتظرة في صندوق الخطابات مقدم خدمات الإنترنت حتى يقوم المرسل إليها بإدخالها في نظامه المعلوماتي هل تعتبر كأنها بيانات معلوماتية مخزنة وبالتالي تطبق عليها المادة 19 أم أنها بيانات في مرحلة النقل والتحويل وبالتالي تنطبق عليها أحكام المادة 21 الخاصة بإعتراض البيانات المتعلقة بالمحتوى، ويلاحظ في هذا الإطار أنقسام التشريعات ففي حين تتجه بعضها إلى أن هذه الرسالة تعتبر مشابهة للبيانات المخزنة وبالتالي ينطبق عليها نص المادة 19، ويذهب الأتجاه الآخر بإعتبارها جزءا من الاتصال لا يمكن الحصول عليها إلا عن طريق سلطة الإعتراض[122].

مدى قابلية شبكات الحاسب للتفتيش: وفي هذه الصورة يمكن التفرقة بين حالتين:

لى: اتصال حاسب المتهم بنهاية طرفية موجودة خارج منزله وضمن حدود الدولة: يرى الفقه في

ألمانيا وإستناداً إلى مقتضيات القسم 103 من قانون الإجراءات الجنائي أن التفتيش يمكن أن يمتد إلى سجل البيانات المتصلة به النهاية الطرفية الحاسب المتهم والتي تكون في موقع آخر، وهذا عندما يكون موقع التخزين الفعلي خارج المكان الذي يتم فيه التفتيش[123]. كما تعرض مشروع قانون جريمة الحاسب في هولندا إلى هذه الفرضية في القسم الخامس المادة 125 التي تنص على إمكانية أن يمتد التفتيش إلى الأجهزة المعلوماتية الموجودة في موقع آخر، شريطة أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة[124]، كما نصت المادة 17 فقرة أ من القانون الفرنسي رقم 239 لسنة 2003 بشأن الأمن الداخلي الصادر في 18 مارس 2003 على مكانية التفتيش في الشبكات حيث ورد نصها كما يلي: "يجوز لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم التفتيش على البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر، مادامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي، أو يتم الدخول إليها، أو تكون متاحة ابتداء من النظام الرئيسي[125]".

كما أن المشرع الجزائري وبموجب المادة 05 فقرة 02 من القانون 09-04 السالف الذكر والتي تجيز التفتيش عن بعد في حالة اتصال حاسب المتهم بنهاية طرفية خارج منزله وداخل إقليم الدولة وقد جاء فيها: "في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول

إليها إنطلاقاً من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها، بعد إعلام السلطة القضائية المختصة مسبقا بذلك".

كما تسمح الإتفاقية الأوربية لجرائم الإنترنت 2001 في الفقرة الثانية من المادة 19 من القسم الرابع للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز الكمبيوتر معين إلى غيره من الأجهزة المرتبطة به عن طريق شبكة اتصالات إذا كان في هذا الأخير معلومات يتم الدخول إليها من خلال الجهاز محل التفتيش، وقد ورد فيها ما يلي: " يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل التأكد مما إذا كانت سلطاته تقوم بالتفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي معين أو جزء منه على أرضه، وأن هذه البيانات يمكن الوصول إليها بشكل قانوني سواء من خلال النظام الأولى أو من خلال كونها مهيأة من أجله، وأن هذه السلطات المذكورة ستكون قادرة على التوسع العاجل لنطاق التفتيش أو الولوج بطريق مشابه لنظام آخر[126]".

وعلى العكس من هذا فإن دول أخرى مثل بلجيكا وسويسرا تقصر أثر إلى التفتيش على الأجهزة الموجودة في مكان محدد دون امتدادها إلى الأجهزة المرتبطة[127].

الحالة الثانية: اتصال حاسب المتهم بنهاية طرفية خارج إقليم الدولة: من بين أهم الصعوبات التي تواجهها سلطات التحقيق حسب رأي الأستاذ ULIRCH SIEBER في جمع الأدلة وهذا في تقريره المقدم إلى مؤتمر A.I.D.P. قيام مرتكبي الجرائم المعلوماتية بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الحدود الجغرافية للدولة عن طريق شبكات الاتصال البعدية Telecommunications network بهدف عرقلة التحقيقات[128]، ولقد أشرنا إلى أن القانون في هولندا يسمح وهذا بشرط أن يكون التدخل مؤقتاً وأن تكون البيانات لازمة لإظهار الحقيقة، ويتحفظ بعض الفقهاء الهولنديين على نص المادة 125 السالفة الذكر كونها تعتبر اختراق السيادة دولة وبالتالي يفضل عدم تطبيقها[129]، كما يجد هذا الرأي موافقة في ألمانيا بإعتبار أنه في غياب الاتفاق الخاص بين الدول يعتبر ذلك خرقاً لحقوق السيادة لدولة أخرى وخرقا للقوانين الثنائية الوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائية[130]، أما عملياً فإنه في إحدى قضايا الغش المعلوماتي أسفر البحث عن وجود نهاية طرفية في ألمانيا متصلة بشبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها، ولم تستطع السلطات الألمانية الحصول على هذه البيانات إلا من خلال التماس المساعدة المتبادلة[131].

هذا وتجيز المادة 17 من قانون الأمن الداخلي الفرنسي السابق الذكر في فقرتها الثانية والتي أضيفت إلى قانون الإجراءات الجزائية وعدلت المادة 57 أنه لضباط الشرطة القضائية أن يقوموا بتفتيش الأنظمة المتصلة حتى ولو كانت ممتدة إلى خارج الإقليم الوطني، مع الالتزام بمقتضيات المعاهدات الدولية في هذا الإطار[132].

كما أن المشرع الجزائري وموجب المادة 05 فقرة 03 من القانون 09-04 السالف الذكر تجيز التفتيش عن بعد في حالة اتصال حاسب المتهم بنهاية طرفية خارج إقليم الدولة وجاء فيها: "إذا تبين مسبقاً بأن

المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة، طبقاً للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل". وفي نفس الإتجاه صدر عن المجلس الأوربي توصيات تسمح بامتداد التفتيش خارج إقليم الدولة وهو ما نصت عليه التوصية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات والتي ورد فيها "لسلطة التحقيق عند تنفيذ تفتيش المعلومات وفقا لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة إختصاصها إلى غير ذلك من الأجهزة، ما دامت مرتبطة بشبكة واحدة، وأن تضبط البيانات المتواجدة فيها مادام أنه من الضروري التدخل الفوري للقيام بذلك، كما أن التوصية رقم 17 نصت كذلك بأمتداد نطاق التفتيش خارج إقليم الدولة إذا كان من الضروري إتخاذ إجراءات عاجلة في هذا الشأن، واشترطت أن يتواجد أساس قانوني يجيز ذلك ينبني على أساس موافقة الدولة التي يمتك التفتيش إليها[133].

كما تجدر الإشارة إلى أن قواعد القانون الجنائي سواء الموضوعية منها والإجرائية ذات طابع إقليمي لا يمكن أن تنفذ خارج إقليم الدولة بما فيها التفتيش والقبض، وتضيف اللجنة الأوروبية للمشكلات الجنائية التابعة للمجلس الأوروبي أنه إذا ما وقعت هذه الإجراءات على إقليم دولة أخرى تعتبر غير مشروعة إلا إذا كان القانون الدولي يجيزها[134].

ومع ذلك فقد أجازت المادة 32 من الإتفاقية الأوروبية بشأن الجرائم المعلوماتية إلى إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين:

الأولى: إذا تعلق التفتيش بمعلومات مباحة للجمهور.

الثانية: إذا رضي صاحب هذه البيانات بهذا التفتيش[135].

الفرع الثاني – الضبط في البيئة الرقمية: من نتائج التفتيش الصحيح في بيئة رقمية عملية الضبط، التي يقصد بها وضع اليد على شيء يتصل بجريمة معلوماتية وقعت، يفيد في كشف الحقيقة عنها وعن مرتكبيها[136]، ترد على منقولات يصطلح عليها بالمنقولات المعلوماتية والتي تتمثل في مكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به (وقد تم تناولها في إطار التفتيش) كما أنه يمكن نقل البيانات المعالجة إلكترونياً أو المعلومات من حاسب معين إلى حواسب أخرى سواء عن طريق شبكات الإتصال التي تربط بينها أو عن طريق الأقراص والشرائط الممغنطة، وهو ما يطلق عليها المراسلات الإلكترونية، وإذا كنا قد توصلنا إلى إمكانية التفتيش في المكونات المعنوية للحاسوب وبالتالي إباحة ضبطها فإن الأمر قد يواجه صعوبات مفادها عدم وجود نصوص تشريعية صريحة تجيز الضبط في البيئة المعلوماتية، فمثلاً المشرع المصري لم ينص صراحةً على إمكانية ضبط المكونات المعنوية للحاسوب بخلاف المشرع الفرنسي الذي تدارك الوضع وقام بسد الفراغ التشريعي وذلك بموجب قانون الأمن الداخلي 239 / 2003 والذي استحدث المادة 57-1 /فقرة 3 التي تقضي بأن البيانات التي يتم الحصول عليها من جراء تفتيش النظام المعلوماتي يتعين نسخها على دعامات ويتم تحريز هذه الدعامات في أحراز مختومة[137] وسنتناول هذه النقاط بالتحليل كما يلي:

ضبط مكونات الحاسب الآلي: من المعلوم بأن مكونات الحاسب الآلي تختلف من مكونات مادية وأخرى معنوية، وقد يقال أنه طالما وصف المنقول ينطبق على مكونات الحاسب الآلي فإنه من السهل ضبطها، والواقع أن المسألة ليست بهذه البساطة فإذا كان الأمر لا يثير مشاكل بالنسبة لضبط المكونات المادية للحاسب من وحدة المدخلات ووحدة الذاكرة الرئيسية ووحدة الحساب والمنطق ووحدة التحكم ووحدة المخرجات ووحدات التخزين الثانوية، وكذلك بالنسبة الشبكات الإتصال الخاصة به، فإن ضبط مكونات الحاسب المعنوية قد أثار خلافاً كبيراً في الفقه المقارن، حيث أنه إذا كانت الغاية من التفتيش ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل قواعد البيانات الإلكترونية بما تحتويه هي الأخرى من سجلات أو حقول أو برامج تطبيقات[138].

فإذا كانت مصادرة أجهزة الحاسب الآلي التي ارتكبت بها الجريمة المعلوماتية أهم وسائل الضبط فإن مثل هذا الإجراء قد لا يكون متاحاً دائماً كما لو كان الضبط يتم عن بعد، فهنا إتجهت التشريعات المقارنة إلى أساليب أخرى تتلاءم مثل هذه الحالات نجد من بينها أسلوب النسخ copier حيث يتم نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها، وهنا يكون أسلوب النسخ ذات أهمية كبيرة حيث ينتج عنه دليل رقمي مقبول أمام القضاء، كما نجد أيضاً أسلوب التجميد في حالة إذا كان القرص الصلب يحتوي على ملفات مشفرة وتحتاج بالتالي إلى فك شفرتها للتعرف على محتوياتها الإجرامية فالتجميد يساعد خبراء المعمل الجنائي على القيام بعملهم دون الخشية من ضياع الأدلة[139]. أما من حيث الاختلاف التشريعي فقد سبق تناوله سالفاً في إطار التفتيش وكل ما ينطبق عن التفتيش ينطبق عن الضبط (وبالتالي لا داعي للإعادة)[140].

ويواجه عملية الضبط للبيانات المعالجة إلكترونياً صعوبات تتمثل في إتساع حجم الشبكة المعلوماتية، وكذا وجود البيانات المراد ضبطها في شبكات أو أجهزة تابعة لدولة أجنبية مما يستدعي التعاون من طرف جهات الشرطة والتحقيق للوصل إلى عملية ضبطها، كما أن التفتيش والضبط قد ينطوي على كثير من الأحيان على اعتداء على حقوق الغير لاسيما الحياة الخاصة وبالتالي وجوب إتخاذ الضمانات اللازمة لحماية هذه الحقوق[141].

أما الضبط وفقا للإتفاقية الأوروبية لجرائم المعلوماتية 2001 فقد أوردت الفقرة الثالثة من المادة 19 هذا الإجراء وجاء فيها: "يجب على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تخويل سلطاته المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين 1 و 2، وهذه الإجراءات تشمل السلطات التالية:

ضبط أو الوصول بطريقة مشابهة إلى نظام معلوماتي أو جزء منه أو إلى دعامة تخزين معلوماتية.

التحقق والتحفظ على نسخة من هذه البيانات المعلوماتية.

المحافظة على سلامة البيانات المخزنة.

منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتي[142].

يلاحظ في إطار هذه الفقرة أنها تناولت مسألة الضبط أو الحصول بوسيلة مشابهة على البيانات المعلوماتية التي كانت موضوع تفتيش والتي تشتمل على الأجزاء المادية للحاسب وكذا دعامات التخزين المعلوماتية، كما يلاحظ أن المادة قد استخدمت بالإضافة إلى المصطلح التقليدي الضبط مصطلح الحصول بطريقة مشابهة وذلك من أجل الأخذ في الاعتبار الطرق الأخرى لرفع البيانات غير المادية والتي لا يسهل الوصول إليها، وعليه فإن الضبط أو الحصول على البيانات عن طريق وسيلة مشابهة له وظيفتان الأولى تتمثل في جمع الأدلة والثانية مصادرة هذه الأدلة بجعلها غير قابلة للوصول إليها[143].

كما أن المشرع الجزائري تناول هذا الإجراء (أي الضبط) في المادة السادسة 06 من القانون رقم 09-04 السالف الذكر بعنوان حجز المعطيات المعلوماتية[144].

ضبط المراسلات الإلكترونية: يدخل تحت وصف المراسلات كل من الرسائل والجرائد والطرود والبرقيات والمحادثات السلكية واللاسلكية، ولقد عرف قانون الاتصالات الإلكترونية الأمريكي لسنة 1986 الاتصالات الإلكترونية بأنها "كل انتقال بشكل كلي أو جزئي لإشارات أو الصور أو الأصوات أو المعطيات أو المعلومات أياً كان نوعها عن طريق الكابل أو الراديو أو النظام الكهرومغناطيسي أو التصوير الكهربائي أو الصور المرئية"، في حين عرف قانون البريد والاتصالات الإلكترونية الفرنسي:

Code des postes et des communication électroniques décret n° 567 – 80

الاتصالات الإلكترونية بأنها كل انتقال أو إرسال أو استقبال الإشارات أو علامات أو كتابة أو صور أو أصوات عن طريق النظام الكهرومغناطيسي[145].

ولقد حرصت كافة التشريعات على تقرير الحماية القانونية للمراسلات والاتصالات بصفة عامة لأنها تعتبر الوسيلة لنقل الأسرار الخاصة بالشخص أو بحياته الخاصة، غير أن تقرير هذه الحماية لا يحول دون خضوعها للضبط تحقيقاً للمصلحة العامة للمجتمع[146]، وتتفق أغلب التشريعات على أن الضبط أو الإطلاع أو المراقبة أو التسجيل يجب أن يكون تحت إذن مسبب ولمدة محدودة، كون أن للمراسلات البريدية والبرقية والمحادثات التليفونية وغيرها من وسائل الإتصال حرمة وأن سريتها مكفولة ومن بين هذه التشريعات المادة 45 من الدستور المصري[147] والتي تقابلها المادة 39 من الدستور الجزائري، كما أن المادة 303 مكرر من قانون العقوبات الجزائري والمضافة بموجب القانون رقم 06-23 المؤرخ في 20/12/2006 عاقبت على اعتراض الاتصالات السلكية واللاسلكية دون إذن[148]، كما أنها مددت الحماية والعقاب في حق كل من أحتفظ أو وضع أو سمح بأي وسيلة كانت التسجيلات المتحصل عليها بأحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون، على أنه مما يثير لبساً وغموضاً في إطار ضبط المراسلات الإلكترونية الضبط الواقع على البريد الإلكتروني وكذا الضبط الوارد على شبكات الحاسب الآلي وهذا مما سنعالجه في النقطة التالية:

ضبط البريد الإلكتروني: يقصد بالبريد الإلكتروني Electronic Mail صندوق عبارة عن ملف متواجد على وحدة الأقراص الممغنطة يستخدم في استقبال الرسائل، وحتى تتم عملية

إرسال واستقبال البريد الإلكتروني فإن ذلك يتم عن طريق مقدم خدمة الإنترنت والذي يتولى تقديم الخدمة من المرسل إلى المرسل إليه، وحتى تتم هذه الخدمة ينبغي توافر عدة معلومات وهي:

إسم مزود إرسال البريد الإلكتروني ويرمز له بالرمز "SMTP".

إسم مزود استقبال البريد الإلكتروني "POP".

العنوان البريدي للمستخدم في الإنترنت.

إسم مزود إرسال البريد الإلكتروني.

العنوان البريدي في الإنترنت[149].

وإذا أراد أي مستخدم الحصول على الرسائل الخاصة به فإنه يتجه إلى أقرب وحدة طرفية ويقوم بعدها باستدعاء الرسائل المتواجدة على بريده، ويمكن توصيل الرسائل إلى أي مكان في العالم باستخدام خطوط التليفون أو الموجات اللاسلكية أو الأقمار الصناعية[150]، أما بخصوص ضبط الرسائل الواردة بالبريد الإلكتروني فإن الإشكال الذي يمكن إثارته في هذا الجانب هل أن هناك وجه شبه بين الرسائل الإلكترونية والرسائل التقليدية، بمعنى هل يمكن إخضاع الرسائل الإلكترونية إلى ما تخضع له الرسائل الورقية من قواعد خاصة في إطار الضبط؟

تشير أغلب الآراء التشريعية والفقهية أن مخرجات الحاسب من قبيل المستندات المطبوعة، ويعللون ذلك أن التقدم العلمي قد تجاوز المفهوم التقليدي للمستند الذي يتجسد في الورق المكتوب، ومن بين التشريعات التي تأخذ بهذا التعديل الذي أدخل على قانون العقوبات الفنلندي والذي بمقتضاه تمت المماثلة بين مخرجات الحاسب الآلي من خرائط ورسومات وأفلام وشرائط صوتية والمستندات التقليدية، بعد أن كانت قبل التعديل لا تدخل في مفهوم المستند، ونفس النهج انتهجه الفقه في كل من المجر والبرازيل، كما يذهب الفقه في الشيلي إلى أن التصوير الفوتوغرافي والتصوير بالأقمار الصناعية والتصوير بالأشعة والهاتف السلكي واللاسلكي وضيع تسجيلات الصوت والصورة تعد من قبيل المستندات، لأن التقدم الفني قد تجاوز المفهوم التقليدي للمستند الذي يعرفه على أنه مجرد ورقة مكتوبة[151].

أما عن كيفية ضبط البريد الإلكتروني فإنه على المحقق أولا اختيار الصندوق البريد الخاص بالمتهم محل التفتيش لتظهر، لتظهر القائمة المنسدلة والتي بها عدة خيارات، كالوارد، الصادر، المهملات... وعلى المحقق أن يختار الأمر الذي هو محل للبحث ولقراءة الرسالة سواء الواردة أو الصادرة، وذلك بالضغط على زر الإدخال لتظهر الرسالة كاملة أمامه، وفي كل الحالات للمحقق أيضاً طباعة الرسالة الإلكترونية.

التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي: رغم ما تثيره هذه النقطة من إشكاليات إلا أن أغلب تشريعات العالم تكاد تتفق أن التنصت مسموح به تحت ظروف معينة، ففي فرنسا يجيز القانون 10 يوليو 1991 اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل

المعلومات[152]، وعلى أن السلطة القضائية هي المخولة بمنح إذن للقيام بهذا الاعتراض طبقاً للمادة 100 من ق.إ.ج الفرنسي[153] والمحدد بأربعة أشهر كحد أقصى[154].

وكذا نفس النهج نجده لدى التشريع الهولندي الذي يجيز لقاضي التحقيق أن يأمر بالتصنت على شبكات اتصالات الحاسب إذا كانت هناك جرائم خطيرة تفيد ضلوع المتهم فيها، وتشمل هذه الإمكانية الفاكس والتلكس ونقل البيانات.

وفي أمريكا يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسب بشرط الحصول على إذن تفتيش صادر من القاضي[155].

أما في اليابان فقد أقرت محكمة مقاطعة KOFU سنة 1991 وهذا في غياب نصوص صادرة من المشرع إلى شرعية التصنت على شبكات الحاسب الآلي للبحث عن دليل الإدانة[156]، وفي فلندا يجيز القانون التصنت على شبكات الحاسوب عن بعد بمقتضى إذن يقدم في كل حالة على حدا[157]، وبالنسبة للقانون الجزائري فإن المادة 65 مكرر 5 من ق .إ.ج قد نصت صراحة على اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية في جرائم محددة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[158].

المبحث الثاني: الوسائل الشخصية للحصول على الدليل الرقمي:

بعد معرفة الوسائل المادية التقليدية التي تصلح كإجراءات مؤدية للحصول على الدليل الرقمي سيتم الإنتقال إلى الوسائل الشخصية التي تستعملها سلطات التحقيق للحصول على الدليل الرقمي، وقد تم إدراج هذه الوسائل تحت هذه التسمية لوجود شخص يتوسط بين الإجراء وبين الدليل بحيث يؤدي غياب هذا الشخص إلى انعدام الدليل، أي أنه يعتبر وسيلة للحصول عليه.

المطلب الأول: الشاهد المعلوماتي والشهادة الإلكترونية: تعرف الشهادة عموماً بأنها الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق، أو القضاء بشأن جريمة وقعت[159]. وتعتبر الشهادة الطريق العادي للإثبات الجنائي، مقابل ذلك فالكتابة تعتبر الطريق العادي للإثبات المدني[160]، وللشهادة في مجال الإجراءات أهمية بالغة لأن الجريمة عمل غير مشروع يجتهد الجاني في التكتم عند إرتكابها ويحرص على إخفائها عن الناس، ولهذا فإن العثور على شاهد يعتبر مكسباً كبيراً للعدالة، ومن هنا جاءت قاعدة "عدم رد الشهود"[161]، وتختلف الشهادة الإلكترونية عن الشاهد المعلوماتي ففي حين يقصد بالشهادة الإلكترونية بأنها تلك الشهادة التي لا يكون فيها الشاهد حاضراً جلسة التحقيق بذاته وإنما تتم عبر وسائل إلكترونية[162]، فإن الشاهد المعلوماتي هو ذلك الشخص الذي يدلي بشهادته في جلسة المحاكمة.

الفرع الأول : الشاهد المعلوماتي: وفي هذا الإطار سيتم تناول كل من:

المقصود بالشاهد المعلوماتي: يقصد بالشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية المعلومات، والذي يمكنه الدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب ذلك، لذلك يطلق عليه بالشاهد المعلوماتي Le Témoin informatique تمييزاً له عن الشاهد التقليدي[163] وينحصر الشاهد المعلوماتي في:

مشغلو الحاسب الآلي: وهم الأشخاص الذين يتمتعون بقدر عال من الخبرة في تشغيل نظم الحاسب الآلي وكيفية إدخال البيانات ونقلها إلى وسائط التخزين، ويجب أن تكون لهم خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات مع ما تتوافر لهم من معلومات عن قواعد كتابة البرمجة[164].

المحللون: وهم الذين يقومون بعملية تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات، كما يمكنهم تتبع البيانات داخل النظام عن طريق مخطط تدفق البيانات[165].

خبراء البرمجة: أو ما يسمون بمخططي البرامج، وهم الأشخاص المتخصصون في كتابة أوامر البرامج وينقسمون إلى مخططي برامج النظام ومخططي برامج التطبيقات[166].

مهندسو الصيانة والاتصال: وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب وشبكات الاتصال[167].

مديرو النظم: وهم الذين تسند لهم مهمة الإدارة في النظم المعلوماتية[168].

إلتزام الشاهد بالإعلام في الجريمة المعلوماتية: ويقصد به أنه متى كان الشاهد حائزاً لمعلومات جوهرية لازمة لاختراق نظام المعالجة الآلية للبيانات بحثاً عن أدلة جوهرية تتطلبها مصلحة التحقيق فإنه يكون مطالباً بأن يعلم سلطات التحقيق على سبيل الإلزام وإلا تعرض للعقوبات المقررة لجريمة الامتناع عن الشهادة[169].

وإلتزام الشاعد بالإعلام يحوي مجموعة من السمات الجوهرية تتمثل فيما يلي:

التزام الشاهد بالإعلام التزام قانوني : يقتضي أن يتوافر نص صريح يلزم الخبراء والحرفيين في مجال المعلوماتية بالإعلام عن الجرائم في حالة وقوعها.

استقلالية هذا الالتزام: إن تقديم المعلومات الجوهرية الهامة التي تتصل بموضوع النظام المعلوماتي محل التحقيق واجباً جديداً والتزاماً مستقلاً عن التزامات الشاهد التقليدية.

التزام وقائي: يعتبر الالتزام بالإعلام في الجرائم المعلوماتية دوراً وقائي في بيئة تكنولوجيا المعلومات فهو يؤدي إلى عدم التحفظ على الشبكة بأكملها وبالأخص الشبكات الكبيرة وإنما على نوع محدد من البيانات التي تثير البس والشكوك[170].

علة الالتزام بالإعلام في الجريمة المعلوماتية: تبدو الحكمة من إلزام الشاهد المعلوماتي بالإعلام في الجرائم المعلوماتية من عدة جوانب:

تحقيق مبدأ التوازن في المعلومات الأساسية المتعلقة بالمجال المعلوماتي من برامج ونظم معلوماتية بين شهود ومستخدمي الحاسبات الآلية وسلطات التحقيق والتحري، ذلك أن نقص المعلومات المتخصصة في هذه الجرائم لازال هو التحدي الخطير بالنسبة للتحقيقات الجنائية، فعدم الإفصاح عن هذه المعلومات من قبل الشاهد المعلوماتي لسلطات التحري سوف يؤدي إلى اختلال التوازن المعرفي بين هذه السلطات ومستخدمي الحاسب الآلي، إذ

يستحيل على السلطات بدون معرفة كلمات المرور السرية والشفرات الخاصة بالبرامج المختلفة الولوج إلى الأوعية المعلوماتية محل الواقعة[171].

تحقيق التضامن بين المتعاملين في البيئة المعلوماتية: إذ أن الزام الشاهد المعلوماتي بالإعلام عن الجرائم المعلوماتية سيؤدي إلى تفادي هذه الأخيرة، وبالتالي التصدي لكل من يحاول إساءة استخدام الحاسبات والشبكات المعلوماتية على مختلف تنوعها، مما يؤدي إلى شيوع الروح التعاونية حفاظاً على الثروة المعلوماتية من الضياع.

تدارك أوجه العجز والقصور الذي تمتاز به الوسائل التقليدية: يلاحظ أن الالتزام بأداء الشهادة المعلوماتية يختلف عنها في التقليدية، حيث أن الشاهد المعلوماتي يجاوز في شهادته الشاهد التقليدي من حيث أنه يقوم بطبع ملفات البيانات المخزنة في ذاكرة الحاسوب أو في الإفصاح عن كلمات المرور السرية، لذا يعتبر هذا الالتزام أكثر فعالية في مواجهة القصور الذي تمتاز به الشهادة التقليدية[172].

مضمون الالتزام بالإعلام من قبل الشاهد المعلوماتي: على الشاهد المعلوماتي أن يمنح سلطات التحقيق كل ما يحوزه من معلومات جوهرية لازمة للولوج إلى النظام المعلوماتي الخاص به لأجل البحث عن أدلة للجريمة المعلوماتية وفي سبيل ذلك فإنه يلتزم بـ:

طبع ملفات البيانات المخزنة في ذاكرة الحاسوب أو حاملات البيانات الثانوية وتسليمها إلى المحقق متى اقتضت المصلحة العامة ذلك.

الإفصاح عن كلمات المرور السرية: حيث أن كلمة المرور السرية تعتبر وسيلة تأمين لبرامج الحاسب الآلي من الاستخدام عن طريق شخص مجهول فيقوم الشاهد بالإفصاح عنها لمصلحة التحقيق.

الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة[173].

وقد اختلف الفقه المقارن بين مؤيد ومعارض لهذه الالتزامات فذهب فريق أنه لا يلزم على الشاهد المعلوماتي تقديم هذه الالتزامات، في حين أيد الفريق الآخر هذه الالتزامات.

الاتجاه الأول: حيث يذهب القائلون بهذا الاتجاه إلى أنه ليس من واجب الشاهد وفقاً للالتزامات التقليدية للشاهد أن يقوم بالإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة (الالتزامات السابقة الذكر)، ونجد هذا المعنى أساساً له في الفقه الألماني الذي يرى أن طبع البيانات المخزنة في ذاكرة الحاسب الآلي لا يدخل في أداء الشهادة[174] وكذا نفس الحال في تركيا حيث لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة[175]، أما في الشيلي فيرى الفقه هناك أنه في ظل غياب النصوص التشريعية الصريحة فإنه ليس من الملائم الحديث عن الواجب القانوني لالتزام بعض الأفراد على طبع سجلات الحاسب والكشف عن كلمات المرور السرية، بل يجب أن يؤخذ في عين الاعتبار جريمة إنتهاك الأسرار[176].

أما بالرجوع إلى قانون الإجراءات المصري فنجده في نص المادة 29 ق. إ.ج.ج قد خول المأمور الضبط القضائي سلطة سماع أقوال من تكون لديهم معلومات عن الواقعة الجرمية المرتكبة، وزادت في نص المادة 31 من نفس القانون أنه إذا كان في حالة تلبس أن يسمع أقوال الأشخاص الحاضرين في محل الواقعة، وأن يطلب من الحاضرين عدم مبارحة مكان الجريمة، ويرى جانب من الفقه المصري أن الالتزامات التي فرضها قانون الإجراءات الجزائية لا تتسحب على الشاهد المعلوماتي، وعليه لا يمكن إلزام الشاهد بالإدلاء بما لديه من معلومات لازمة للولوج إلى النظام المعلوماتي إذ أنه غير ملزم بالتعاون فيما يجاوز علمه والإدلاء بمثل هذه المعلومات[177].

الاتجاه الثاني: يرى أصحاب هذا الاتجاه أن على الشاهد الإفصاح عن كلمات المرور والشفرات الخاصة بالبرامج والقيام بطبع ملفات البيانات، ومن أنصار هذا الاتجاه الفقه الفرنسي، حيث يرى البعض أن المشرع طالما لم ينظم هذه المسألة فإنه لا مناص من تطبيق القواعد العامة في الشهادة، وعليه يلتزم الشهود بالكشف عن كلمات المرور وشفرات التشغيل ما عدا حالات المحافظة على سر المهنة فإنهم يكونون في حل من ذلك[178].

وفي هولندا يجيز مشروع الحاسب الآلي لسلطات التحري والتحقيق إصدار الأمر القائم بتشغيل النظام وهذا بتقديم المعلومات اللازمة للولوج إلى النظام المعلوماتي كالإفصاح عن كلمات المرور والشفرات الخاصة بتشغيل النظام، ويتم تكليف القائم على تشغيله بحل رموز هذه البيانات[179].

وفي اليونان يمكن الحصول من القائم على تشغيل نظام الحاسب على كلمة المرور السرية للولوج إلى النظام المعلوماتي، كما يمكن الحصول على بعض الإيضاحات الخاصة بنظامه الأمني، لكن ليس على الشاهد أي التزامات بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسب، وذلك لأنه يجب أن يشهد على معلومات حازها بالفعل وليس الكشف عن معلومات جديدة[180].

وفي إنجلترا وطبقا للقانون الصادر 1984 بشأن البوليس والأدلة الجنائية يعطي هذا الأخير المحققين الحق في أن يطلبوا من الغير تمكينهم من الدخول إلى المعلومات المختزنة في الحاسب الآلي أو الإطلاع عليها[181].

موقف اتفاقية بودابست من الالتزام بأداء الشهادة المعلوماتية: نصت الفقرة الرابعة من المادة 19 من الاتفاقية الأوربية للجرائم المعلوماتية وجاء فيها: "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل تحويل سلطاته المختصة سلطة إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من أجل حماية البيانات المعلوماتية التي تضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات المشار إليها في الفقرتين 1 و 2.

نجد في إطار هذه المادة أنها تتعلق بإلزام مديري النظم بالتعاون مع سلطات التحري والتحقيق بحكم اللزوم العقلي والمنطقي وهذا للقيام بعمليات التفتيش والضبط، إذ أنه بدون هذه المساعدة يصعب على سلطات التحري تتبع مسار الجريمة المعلوماتية وبالتالي صعوبة أو استحالة الوصول على الأدلة الجرمية أثناء

عملية التفتيش، أما المعلومات التي يمكن إلزام مديرو النظام بتقديمها هي المعلومات الضرورية التي تسمح بتطبيق إجراءات التفتيش والضبط أو أي طريقة تهدف إلى الحصول على الدليل الرقمي الذي يثبت قيام الجريمة وإسنادها إلى فاعلها.

أما بالنسبة للمشرع الجزائري فقد تناول هذه المسألة في المادة 10 من القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث ألزم مقدمي الخدمات بالتعاون مع سلطات التفتيش والتحري من أجل إمدادهم بكل ما يحتاجونه في هذا الإطار، كما يتعين عليهم كتمان سر العمليات التي ينجزونها تحت طائلة العقوبات[182].

الفرع الثاني: الشهادة الإلكترونية: تفترض هذه النوعية من الشهادة حصولها أمام قاضي الموضوع حيث يكون الشاهد غير حاضر جسدياً في جلسة المحاكمة إلا أنه يظهر بشكل سمعي ومرئي وتسمى بالشهادة الإلكترونية الفورية وتتم عن طريق ما يعرف بتقنية conferenceévid o.[183]

ولقد أخذت بهذه التقنية الكثير من الدول وعلى رأسهم إيطاليا وهذا بقصد حماية الشهود من مخاطر الانتقام في حالة ظهورهم شخصياً في جلسات التحقيق، كما أقرته كندا وأستراليا في مجال محاكمة الأحداث لتلافي الآثار النفسية العنيفة عليهم جراء حضورهم الشخصي، أما في القضاء الأمريكي وحتى مرحلة ظهور الدوائر الاتصالية المتكاملة كان يرفض بقوة إمكانية إحداث اتصال صوتي بين الشاهد والجلسة ويعتبرها من شهادة السماع كونها تحدث خارج الجلسة، لذلك كان حضور الشاهد بذاته أمر إجباري، أما بعد ظهور فكرة الدوائر الاتصالية من مغلقة ومفتوحة فقد أثير مدى إمكانية قبول الشهادة الفورية لاسيما وأن الشاهد يظهر بهيئته الكاملة كما لو كان حاضراً بجسده، ولقد كانت بداية الأخذ بهذا النظام عندما واجه القضاء مشكلة إدلاء الشهادة من قبل أشخاص وضعوا في برنامج حماية الشهود وهو ما أقرته المحكمة الفيدرالية الأمريكية طالما أن هناك أسباب تدعو للأخذ به، ويميز القضاء الأمريكي بين نوعين من الشهادة الإلكترونية المرئية، فمن ناحية يوجد نظام الشهادة المرئية ذات الاتجاه الواحد حيث أن الشاهد يدلي بشهادته ولا يرى سوى الكاميرا المسلطة عليه، في حين في نظام الشهادة المرئية ذات الاتجاهين وفيها يرى الشاهد قاعة المحاكمة ويراه من في المحكمة[184]، وسيتم تناول هذه التقنية وفق ما يلي:

نظم تقنية vidéo conférence : هناك أربعة نظم مختلفة لتطبيق هذه التقنية في مرحلة المحاكمة عن بعد وهي:

نظام الاتصال من نقطة إلى أخرى: وفيه يتم الاتصال المرئي والمسموع بين قاعة المحكمة ومكان آخر يتواجد فيه الشاهد[185].

نظام المتحدث الناشط (السويتش): وفي هذا النظام تتعدد الأماكن التي يتم فيها الاتصال المرئي المسموع، حيث توجد قاعة المحكمة وعدة أماكن أخرى يتواجد فيها الشهود، كما توجد شاشة لعرض الصورة في كل مكان من هذه الأماكن مع أجهزة سماع الصوت، ولا تظهر على شاشة العرض سوى صورة الشخص الذي يتكلم، وإذا حدث وأن تكلم عدة أشخاص في وقت واحد فإن صورة الذي يتكلم بأعلى صوت هي تظهر[186].

نظام الحضور المستمر الثابت: وفي هذا النظام يكون الاتصال بين خمسة أماكن متفرقة وهي قاعة المحكمة من جهة وأربعة أماكن أخرى متفرقة يتواجد فيها المتهمون والشهود، وفي كل مكان يوجد شاشة لعرض الصورة مقسمة إلى أربعة أجزاء، وإمكانية سماع صوت من يتكلم من المشاركين في الجلسة وفي أن واحد.

نظام الحضور المستمر المتقدم[187]: وهو النظام الحدث في هذه التقنية ويتم الاتصال بين قاعة المحكمة وبين عدد كبير من الأماكن الأخرى، ويتم إعداد هذه الأماكن بتزويدها بشاشات عرض الصورة والصوت، ويتم تقسيم شاشة عرض الصورة الموجودة في كل مكان إلى أربعة أقسام يتم تثبيت القسم الأول لعرض بانوراما قاعة المحكمة وقسمين آخرين في مكانين من الأماكن المتصلة بهذه القاعة، أم القسم الرابع فيقوم تلقائياً بنقل صورة الشخص الذي يتكلم.

مدى حجية تقنية vidéo conférence في مجال المحاكمة الجزائية: ذهب غالبية الفقه الحديث إلى تأييد استخدام هذه التقنية نظرا لما يترتب على استخدامها مزايا عديدة منها تبسيط وسرعة إجراءات المتابعات الجزائية، بالإضافة إلى حماية الشهود والمجني عليهم وغيرهم من المتعاونين في مجال العدالة، وتدعيم وسائل المساعدة القضائية بين الدول، إلا أن جانب آخر من الفقه ذهب إلى عكس ذلك واستند في ذلك إلى عدة حجج منها مبدأ المواجهة بمفهومه الواسع يقتضي حضور الجميع في قاعة المحكمة حيث يمكن القاضي من مواجهة الأطراف بعضها ببعض، وتمكن القاضي من تلمس الحقيقة عن قرب من خلال الانفعالات النفسية أثناء جلسة المحكمة، إلا أنه يمكن الرد على هذه الحجة أن القاضي هو المتحكم في هذه التقنية فله أن يوجه الحديث إلى من يريده وأن يركز كاميرا المراقبة على من يشاء بل أنه عن طريق هذه التقنية قد نتوصل إلى هدوء نفسي من طرف القاضي تمكنه بالحكم من دون أي ضغوط، كما أنه يلاحظ عن كثب انفعالات المتهمين والشهود عن كثب من خلال الشاشة، كما يرى المعارضون لهذه التقنية أنها باهظة التكاليف ليس بمقدور الدول النائية مجابهتها، كما أنها تثير مشكلة تطبيق قواعد الاختصاص المكاني المنصوص عليها في قانون الإجراءات ويمكن الرد على هذه الحجة بتعديل في قانون الإجراءات بما يتلائم وهذه التقنية.

المطلب الثاني: الخبرة التقنية في البيئة الرقمية

قد يصادف المحقق أثناء التحري عن الجريمة والبحث عن أدلتها بعض المشاكل الفنية التي يتوقف على حسمها استمرار التحقيق وبلوغ غرضه، ولما كان المحقق غير ذي اختصاص فني وفر له القانون وسيلة الاستعانة بأهل الخبرة لحسم هذه الأمور ولتناول موضوع الخبرة في الوسط.

الفرع الأول: المقصود بالخبرة التقنية وأحكامها: وفي هذا الإطار سيتم تناول كل من الخبرة التقنية، وكذا أحكامها وفق ما يلي:

تعريف الخبرة التقنية: تعرف الخبرة عموماً على أنها الاستشارة الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقييم الأدلة التي تحتاج إلى معرفة فنية ودراية علمية لا تتوافر لدى عضو السلطة القضائية المختص بحكم تكوينه وعمله[188]، فقد عرفها المستشار فرج علواني هليل "بأنها إبداء رأي فني من شخص مختص فنياً في شأن واقعة ذات أهمية في الدعوى الجنائية[189]"، كما أن تطورات التكنولوجيا وتعددها في مجال الحاسبات الرقمية والوسائل التكنولوجية الفنية وتعدد وسائل الاتصال الحديثة ودور الإنترنت كقوة مؤثرة من جهة وفشل جهات التحقيق في جمع الأدلة لعدم درايتها بالدليل الفني كل هذه الأسباب أدت بالخبرة إلى أن تكون ضرورة لا يمكن الاستغناء عنها في هذا الإطار[190] وعليه يمكن القول أن الخبرة التقنية أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات والإنترنت حيث تؤدي دوراً بارزاً أمام نقص المعرفة القضائية الشخصية في البيئة الرقمية[191].

والأصل في الخبرة أنها إجراء من إجراءات التحقيق الابتدائي كونها تهدف إلى الوصول إلى الحقيقة، وهو ما أشارت إليه المادة 85 من ق.إ.ج مصري[192]. وعليه يستشف منها أنه لا يجوز للقاضي أن يقضي في المسائل العملية إلا بعد الاستعانة بأهل الخبرة في المسائل الفنية[193].

أما في القانون الجزائري فقد نصت المادة 143 ق.إ.ج. على أن ندب الخبير هو من سلطات جهات التحقيق أو قد يكون بناء على طلب من النيابة العامة أو الخصوم[194].

أحكام الخبرة: تخضع الخبرة التقنية في أغلب التشريعات إلى نفس أحكام الخبرة القضائية من حيث القواعد القانونية التي تحكم عمل الخبير وإجراءاته، إلا أن هناك بعض التشريعات نظمت أعمال الخبرة في مجال الجرائم الإلكترونية مثل القانون البلجيكي الصادر في 23/11/2000 حيث نصت المادة 88 منه "يجوز لقاضي التحقق وللشرطة القضائية أن يستعين بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق[195]".

وقد تناول المشرع الجزائري على سبيل المثال، أحكام الخبرة في القسم التاسع من الباب الثالث في المواد من 143 إلى 155 ندرجها في النقاط الآتية:

ندب الخبراء يكون من جهات التحقيق أو بناءً على طلب النيابة العامة أو من الخصوم المادة 145.

يختار الخبراء من الجدول الذي تعده المجالس القضائية ويحلف الخبير يميناً أمام القاضي المختص المواد 144-145.

تحديد مهمة الخبير وكذا مهلة إنجاز مهمته كل هذا تحت سلطة قاضي التحقيق أو القاضي الذي أنتدبه المواد 146 – 148.

يجوز للخبير الاستعانة بفنيين بعد إذن القاضي وهذا بعد حلف اليمين المادة 149.

يجوز للخبير أن يتلقى أقوال غير المتهم كما يحق له أن يستوجب المتهم ولكن بحضور قاضي التحقيق أو القاضي المعين من المحكمة، غير أن للأطباء توجيه أسئلة للمتهم الخاضع للفحص بغير حضور قاضٍ أو محامٍ المادة 151.

يقدم الخبراء نتائج خبرتهم كتابة بتقرير لدى كاتب الجهة القضائية التي أمرت بالخبرة.

يعرض الخبراء بالجلسة نتائج أعمالهم الفنية بعد حلف اليمين، ويجوز لكل من رئيس الجلسة أو المحامي أو الخصوم توجيه أسئلة لهم المادة 155.

الفرع الثاني: أهمية الخبرة التقنية وأساليبها في الوسط الرقمي: للخبرة التقنية أهمية كبيرة كما أنها تتميز بمجموعة أساليب يقوم بها الخبير التقني للحصول على الدليل الرقمي وهذا كما يلي:

أهمية الخبرة التقنية: مما يستدعي اللجوء إلى الخبرة التقنية أن جهات التحري والتحقيق كثيراً ما تفشل في جمع الأدلة الرقمية، بل إن المحقق في كثير من الأحيان ما يتسبب في تدمير الدليل الرقمي إما نتيجة خطأ أو إهمال أو جهل في التعامل معه، وعموماً يراعى في الخبير أن تتوافر لديه القدرات الفنية والإمكانيات العلمية في المسألة موضوع الخبرة[196]، والتي تهدف إلى:

الكشف عن الدليل الرقمي وإجراء الإختبارات اللازمة على الدليل الرقمي للتأكد من أصالته ومصدره كدليل يمكن قبوله أمام القضاء.

إصلاح الدليل وتهيئته وإعادة تجميعه من المكونات المادية للحاسب، مع عمل نسخة أصلية من الدليل الرقمي للتأكد من سلامته أثناء عملية استخلاصه.

استخدام الخوارزميات للتأكد من أن الدليل لم يتم العبث به، وتحريزه لإثبات أصالته وتحديد الخصائص المميزة لكل جزء من الأدلة الرقمية كالمستند الرقمي، الصور، الاتصالات[197].

ومن أهم المسائل التي يستعين بها القاضي بالخبرة في المجال المعلوماتي ما يلي[198]:

وصف الحاسب (نوعه، صناعته ...) والأجهزة الملحقة بها ونوع نظام التشغيل، وأهم الأنظمة الفرعية التي يستخدمها.

وصف البيئة المتواجدة فيها الحاسب ونوع الشبكة المتصل بها ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائل الاتصالات وتردد موجات البث....

وصف الوضع المحتمل لأدلة الإثبات والشكل والهيئة التي يمكن أن تكون عليها.

بيان كيفية عزل النظام المعلوماتي مع المحافظة على الأدلة وسلامة الأجهزة.

كيفية نقل الأدلة إلى أوعية ملائمة دون تلفها أو تغيير محتواها.

بيان كيفية نقل الأدلة الرقمية إلى صورة مادية مطابقة للأصل[199].

أساليب عمل الخبير التقني في الوسط الرقمي: الأصل أن للخبير التقني كامل الصلاحيات ومطلق الوسائل في سبيل الحصول على الحقيقة، على أن المحكمة يمكن أن ترفض ذلك بشرط أن تسبب قرارها وإلا تعرض حكمها للنقض، وهناك أسلوبان في عمل الخبير التقني حيث يتمثل الأول في القيام بتجميع تحصيل لمجموعة المواقع التي تشكل جريمة في حد ذاتها كما هو الشأن في بث صور فاضحة بقصد الدعاية للتحريض، أو في جرائم النصب والسب والتهديد، ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها برمجياً وبالتالي نسبتها إلى مسارها الذي أعدت فيه، ثم التوصل في النهاية إلى معرفة بروتوكول الإنترنت IP الذي ينسب إلى جهاز الحاسوب الذي صدر عنه هذا الموقع، أما الأسلوب الثاني فيتمثل في القيام بتجميع لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم مثل المواقع التي تساعد الغير على التعرف على جرعات المخدرات التي تتناسب مع وزن الإنسان بادعاء أنه لو أتبع النصائح فإنه لا يتعرض للإصابة بحالة الإدمان، وأيضاً كيفية زراعة المخدرات بعيداً عن أعين الناس...، ويتم في إطار تصنيف المواقع المذكورة استخدام برمجيات متطورة مهمتها الكشف عن هذه المواقع باستمرار، ومعرفة الجديد فيها[200]، وهناك العديد من القضايا الإجرامية التي طبقت فيها مثل هذه الأساليب[201] وعليه فإنه للقيام بتحديد الدليل الرقمي والوصول إليه وجب على الخبير أن يتخذ خطوات لاشتقاق الدليل الإلكتروني كمرحلة أولى، ثم إتخاذ الأدوات المناسبة للحصول على هذا الدليل كمرحلة ثانية.

خطوات اشتقاق الدليل الرقمي: لما كانت عملية تجميع الأدلة الرقمية من أصعب الأمور التي تواجه عمل الخبير فقد كان لزاماً عليه أن يتبع خطوات محددة من أجل اشتقاق هذا الدليل والتي تتمثل في المراحل التالية[202].

خطوات ما قبل التشغيل والفحص: ويمكن إيجازها في النقاط التالية:

- التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها.
- التأكد من سلامة وحدات تشغيل النظام.
- تسجيل بيانات مكونات هذه الوحدات المضبوطة كالنوع والطراز والرقم ....

خطوات التشغيل والفحص: وتتمثل هذه الخطوات في:

- استكمال تسجيل باقي بيانات الوحدات من خلال قراءات الجهاز.
- عمل نسخة من كل وسائط التخزين المضبوطة وهذا حفاظا على الأصل أثناء عملية الفحص المبدئي.
- تحديد أسماء وأنواع المجموعات البرمجية التي لها علاقة بموضوع الجريمة.
- استخدام التقنيات لإظهار الملفات المخبأة وتلك التي تم محوها.
- تجريد كل الأدلة المتحصل عليها وعمل نسخة إلكترونية لها للمحافظة عليها.

- تحويل الدليل الإلكتروني على هيئة مادية إما عن طريق الطباعة في حالة كونها عبارة عن صور أو مستندات أو وضعها في أي وعاء آخر يتفق ونوع الدليل المتحصل عليه.

تحديد مدى الترابط بين الدليل المادي والدليل الإلكتروني: حيث أن في هذه المرحلة يتم فحص كل من الدليل المادي المضبوط والدليل الإلكتروني في شكله المادي ومن ثم الربط بينهما ليكون دليلاً مقبولاً أمام القاضي أثناء المحاكمة.

مرحلة التدوين: وتعتبر هذه آخر خطوة حيث يتم إعداد تقرير بجميع مراحل خطوات اشتقاق الدليل مع كل ما يفيد من إيضاحات مصورة أو مسجلة، ثم تسلم إلى الجهة القضائية المختصة.

أدوات الخبير: يستعين الخبير في ظل البحث عن الأدلة الجنائية في الفضاء الرقمي إلى وسائل مادية وإجرائية للوصول إلى الدليل الجنائي الرقمي[203].

الوسائل المادية: وهي الأدوات الفنية التي تستخدم في القضاء الرقمي وهي:

- عنوان الإنترنت Internet Protocol Address:IPعنوان بروتوكول الإنترنت هو المسئول عن تراسل حزم البيانات عبر شبكة الإنترنت، ويوجد عنوان IPبكل جهاز مرتبط بالإنترنت، وهو يتكون من أربعة أجزاء وكل جزء يتكون من أربع خانات حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الكمبيوتر الذي تم الاتصال منه، وفي حالة ارتكاب جريمة فإن أول ما يقوم به الخبير هو البحث عن رقم الجهاز وتحديد موقعه مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل اتصال بالشبكة[204].
- البروكسي PROXY: يعمل البروكسي كوسيط بين الشبكة ومستخدميها ويقوم على فكرة مفادها أنه إذا تلقى مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما المحلية المتوفرة يتحقق البروكسي فيما إذا كانت هذه الصفحة Cacheضمن ذاكرة قد جرى تنزيلها من قبل، فيقوم بإرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم IPأحد عناوين ، ومن أهم مزاياه أن ذاكرته الخفية يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة[205].
- برامج التتبع: فائدة هذه البرامج أنها تقوم بالتعرف على محاولات الاختراق التي تتم وتقديم بيان شامل بها إلى المستخدم يحتوي على شكل الاختراق، وتاريخ حدوثه، الذي تمت من خلاله عملية الاختراق، وأسم الشركة المزودة لخدمة IPوعنوان

الإنترنت، ومعلومات أخرى تؤدي إلى تتبع المخترق والجهاز الذي تمت منه عملية الاختراق[206].

- نظام كشف الاختراق: وهو فئة من البرامج تتجسد مهمتها IDS اختصارا يرمز له ( ) في مراقبة العمليات التي تتم على مستوى الكمبيوتر والشبكة مع تحليلها بحثاً عن أية إشارة قد تدل على وجود مشكلة ويقوم مبدأ عملها على تحليل رزم البيانات أثناء إنتقالها عبر الشبكة ومقارنتها بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسبية والتي يطلق عليها مصطلح التوقيع، وفي حالة اكتشاف البرنامج أحد هذه التوقيعات يقوم بإنذار مدير النظام ويسجل البيانات الخاصة بهذا الاعتداء في سجلات كمبيوترية خاصة.
- أدوات فحص ومراقبة الشبكات: يلجأ الخبير في سبيل الحصول على الدليل الرقمي إلى أدوات لفحص ومراقبة الشبكات من بين هذه الأدوات ما يلي:

أداة وظيفتها تحديد مكان الحاسوب الفيزيائي على الشبكة، وهو **ARP** يحتفظ بجميع أرقام كروت الشبكة مما يتيح له معرفة عناوين IP ؟ UGN HGQFM

برنامج وهو برنامج يلتقط أي عملية فحص أجريت **Visual Route** على الشبكة، فيقوم بإعطاء تفاصيل كاملة عن تبين العمليات التي تم فيها المسح وبالتالي معرفة عنوان وأسم الجهة المختصة بوضع البرنامج IP.

أداة ترسم مساراً بين جهازين تظهر فيها كل التفاصيل عن **Tracer** مسار الرزم والعناوين التي زارها الجاني ، كما تسمح برؤية المسار الذي اتخذه من مضيف إلى آخر IP.

أداة وهي أداة مخصصة للفحص متعلقة بالبروتوكول **Netstat** TCP/IP ولها عدة مهام منها عرض جميع الاتصالات الحالية ومنافذ التنصت، وعرض كامل جدول التوجيه[207].

الوسائل الإجرائية: ويقصد بها الإجراءات التي تهدف إلى البحث عن الدليل ومن ثم يمكن للمحقق وبمساعدة من الخبير تحديد شخصية مرتكبه من بين هذه الإجراءات[208]:

- اقتفاء الأثر: يمكن تقصي أثر المجرم أثناء ارتكابه الجريمة معلوماتية في حالة إذا لم يقم بمسح آثار جريمته، ويمكن تقفي الأثر بعدة طرق سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.
- الإطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته: ينبغي على المحقق وهو بصدد التحقيق في إحدى الجرائم المعلوماتية أن يطلع على النظام المعلوماتي وشبكاته والإطلاع على جميع العمليات التي وردت على قاعدة البيانات وإدارتها، وخطة

تأمينها ومعرفة مواد النظام والملفات، وإلى غير ذلك من الإجراءات التي تهدف إلى إحاطة كاملة بالنظام المعلوماتي للتعرف على الجريمة المرتكبة.

- يمكن الاستعانة بهذه التقنية في حصر الحقائقالاستعانة بالذكاء الاصطناعي: والاحتمالات والأسباب والفرضيات ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بجهاز الحاسوب وفق برامج صممت خصيصاً لهذا الغرض[209].

المراجع

1. عادل يوسف عبد النبي الشكري: بحث بعنوان "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، جامعة الكوفة، ٢٠٠٨.
2. مليكة عطوي: الجريمة المعلوماتية حوليات، جامعة الجزائر، مجلة علمية، ٢٠١٢ العدد ٢١.
3. مفتاح ابو بكر المطردي: الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدولة العربية لجمهورية السودان ٢٣/٥/٢٠١٢.
4. علي محمد العريان: الجرائم المعلوماتية دار الجامعة الجديدة، الإسكندرية، ط 2.
5. سامي الشوا: الغش المعلوماتي كظاهرة إجرامية مستحدثة بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، ٢٥ و28 اكتوبر.
6. عبد الكريم عبد الله: جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية منشورات الحلبي الحقوقية، بيروت، ٢٠١١، ط١.
7. احمد محمود عبانبة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ط ١.
8. حمزة بن عقون: السلوك الاجرامي للمجرم المعلوماتي، بحث لنيل شهادة الماجستير في القانون، جامعة باتنة، 2011
9. محمد أمين أحمد الشوابكة: جرائم الحاسوب والإنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن، 2004، ط 1
10. سميرة بيطام: الجريمة الإلكترونية وتقنية الإجرام.
11. كامل مزيد السالك: الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب 23/12/2000.
12. علي كحلوش: جرائم الحاسوب وأساليب مواجهتها، مديرية الأمن الوطني الجزائري العدد 84 / 2007 .
13. عبد العال الديربي، محمد صادق اسماعيل: الجرائم الإلكترونية، الطبعة الاولى، المركز القومي للإصدارات القانونية، القاهرة 2012.
14. رامي متولي القاضي: مكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة 2011.
15. احمد محمود عبابنة: جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ط ١.
16. خالد عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان الأردن 2011.
17. خالد ممدوح ابراهيم: حوكمة الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية 2011.

18. أسامة احمد المناعسة, جلال محمد الزعبي، هايل فاضل الهواوشة: جرائم الحاسب الآلي والإنترنت، دار وائل للنشر، عمان الاردن، 2001.
19. نهله عبد القادر الموفي: الجرائم المعلوماتية، رساله ماجستير، ط 2، دار الثقافة، عمان الاردن، 2010.
20. عبد العال الديربي ومحمد صادق إسماعيل: الجرائم الإلكترونية، الطبعة الأولى، المركز القدمي للاصدارات القانونية، القاهرة 2012.
21. ابراهيم خالد ممدوح: الجرائم المعلوماتية، ط 1، دار الفكر الجامعي، الإسكندرية، 2009.
22. محمد الجبور: الوسيط في قانون العقوبات - القسم العام، دار وائل، عمان، ط 1، 2012.
23. سميرة المعاشي: ما هية الجريمة المعلوماتية، مجله المنتدى القانوني، العدد السابع، جامعة محمد خضر بسره، الجزائر.
24. عبد الفتاح حجازي: التزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ط 1، 2008.
25. ابراهيم خالد ممدوح: حوكمت الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011.
26. موسى مصطفى محمد: دليل التحري على شبكه الإنترنت، دار الكتب القانوني، مصر، 2010.
27. سامي الرواشدة واحمد الهياجنة: مكافحة الجرائم المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، الأردن، 2009، المجلد واحد، العدد 3.
28. جمال محمد غيطاس: أمن المعلوماتية والأمن القومي، مصر للطباعة والنشر، القاهرة، 2007.
29. يوسف حسن يوسف: الجرائم الدولية للإنترنت.
30. علي جبار الحسيناوي: جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، 2009.
31. جميل عبد الباقي الصغير: الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002.
32. عادل عزام الحيط: جرائم الذم والقدح والتحقير المرتكبه عبر الوسائط الإلكترونية، ط 1، دار الثقافة، عمان، 2011.
33. خالد ممدوح إبراهيم: الجرائم المعلوماتية.
34. هدى حامد مشقوش: جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة.
35. علي عبد القادر القهوجي: الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديده للنشر، الإسكندرية، 1994.

36. علي عدنان الفيل: النظام القانوني للمعاملات الإلكترونية في الوطن العربي، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011.
37. يوسف حسن يوسف: جريمة غسل الأموال بالطرق التقليدية عبر شبكات الإنترنت ويندك الويب، ط 1، المركز القومي للإصدارات القانونية، القاهرة، 2011.
38. عبد الفتاح بيومي حجازي: الجريمة في عصر العولمة،ط 1، دار النهضة العربية، القاهرة، 2010.
39. نبيلة هبة هروال: الجوانب الإجرائية الجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2007.
40. محمود نجيب حسني: شرح قانون الإجراءات الجزائية، دار النهضة العربية، القاهرة، 1982.
41. مأمون محمد سلامة: الإجراءات الجنائية في التشريع المصري، ج 1، دار النهضة العربية، القاهرة، 2000.
42. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009.
43. محمد حماد الهيتي: التحقيق الجنائي والأدلة الجرمية.
44. حسن محمد إبراهيم: الحماية الجنائية لحق المؤلف عبر الإنترنت، رسالة دكتوراه في الحقوق جامعة عين شمس، 2000.
45. محمد الأمين بشري: التحقيق في جرائم الحاسب الآلي, المجلة العربية للدراسات الأمنية والتدريب, العدد 30 جامعة نايف العربية للعلوم الأمنية, الرياض, نوفمبر, 2000.
46. أحمد سعد محمد الحسيني: الجوانب الاجراية الإجرامية الناشئة. عن استخدام الشبكات الإلكترونية, رسالة دكتوراه في القانون, كلية الحقوق جامعة عين شمس, القاهرة, 2012.
47. أيمن عبد الحفيظ: حدود مشروعية أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، العدد 25، يناير 2004.
48. هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي
49. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت.
50. منى فتحي عبد الكريم: الجريمة عبر الشبكة الدولية للمعلومات, رسالة دكتوراه في الحقوق, كلية الحقوق, جامعة القاهرة, 2012.
51. هلالي عبد اللاه أحمد: الجوانب الموضوعية والإجرائية للجرائم المعلوماتية.
52. أحمد محمود مصطفى: جرائم الحاسبات الآلية في التشريع المصري، ط1، دار النهضة العربية، القاهرة، 2010.
53. عائشة بن قارة مصطفى: حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة الإسكندرية, 2010.

54. بكري يوسف بكري: التفتيش عن المعلومات في وسائل التقنية الحديثة، ط 1، دار الفكر الجامعي، الإسكندرية، 2011.
55. فرج علواني هليل: التحقيق الجنائي والتصرف فيه والأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2007.
56. عبد الفتاح بيومي حجازي: الجوانب الإجرائية الأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2009.
57. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت, رسالة دكتوراه في القانون الجنائيي, كلية الحقوق جامعة عين شمس, 2004.
58. فهد عبد الله العبيد العازمي: الإجراءات الجنائة المعلوماتية، رسالة دكنوراه في الحقوق، جامعة عين شمس، 2012.
59. عبد الله حسين علي محمود: سرقة المعلومات المخزنة في الحاسب الآلي، رسالة دكتوراه في الحقوق كلية الحقوق، جامعة عين شمس، 2001.
60. عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب المصرية، القاهرة، 2009.
61. بن فردية محمد: الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني، السنة الخامسة، المجلد 09 عدد 01-2014، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة بجاية.
62. FRANCILLON (jacques), les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France R.LD.P. (vol.64) 1 et 2 trimestres 1993.
63. WISE (Edward M): computer crimes and other crimes against information technology in The United States R.I.D.P. 1993.
64. YAMAGUCHI (ATSUSHI) computer crimes and other crimes against information technology in Japan R.L.D.P. (vol.64) 1e et 2e trimestres 1993.
65. PIHLAJAMAKI (A ntti): computer crimes and other crimes against information technology in Finland R.L.D.P. (vol.64) 1e et 2e trimestres 1993.
66. MOHRENSCHLAGER (Manfred): computer crimes and other crimes against information technology in Germany R.1.D.P. (vol.64) 1e et 2e trimesters, 1993.
67. KASPERSEN (W.K.Henrik) computer crimes and other crimes against information technology in the Netherlands R.I.D.P. (vol.64) 1e et 2e trimesters, 1993.

68. Sieber (Ulrich) computer crimes and other crimes against information technology “commentary and preparatory questions for the colloquium of the A.I.D.P. in Wurzburg" R.I.D.P. (vol.64) 1e et 2e trimestres 1993.
69. PIRAGOFF (Donald K): «computer crimes and other crimes against information technology in Canada » R.I.D.P. (vol.64) 1e et 2e trimestres 1993.
70. VASSILAKI (Irini): « computer crimes and other crimes against information technology in Greece » R.I.D.P.1993.
71. Durham Cole: «the emerging structures of criminal information law: tracing the contours of a new paradigm R.I.D.P (vol.64) 1e et 2e trimestres .
72. Daniel Morris tracking a computer hacker us attorneys bulletin 2/2001 p 3 available at: http//www.usa.gov/criminal/cybercrime us a may 2001 htm.
73. Erman (Sahir) les crimes informatique et d'autre crimes dans le domaine de la technologie informatique en Turquie, R.I.D.P (vol.64) 1e et 2e trimestres 1993.
74. KUNSEMULLER (CARLOS): “computer crimes and other crimes against information technology in Chile” R.I.D.P. (vol.64) 1e et 2e trimestres 1993.
75. Fabrizio l'aménagement en vidéo conférence des audiences relatives à la grande criminalité par la loi italienne du 07/01/1998.
76. le procés à distance au moyen de la vidéo conférence: l'expérience italienne, dixième congrès des nations unies.
77. Thierry Garé, Catherine Gineste, Droit pénal - procédure pénale,: 7 édition DALLOZ 2012.
78. Meunier (c): la loi du 28 novembre 2000 relative à la criminalité informatique. Revue de droit Pénal Criminel 2002.
79. Waterplas. J.R. informatique et délinquance: un nouveau deffi pour les magistrats et les policiers R.D.P.C Aout-Septembre 1985.

Notes

[←1]

دل يوسف عبد النبي الشكري: بحث بعنوان "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، جامعة الكوفة، ٢٠٠٨، ص ١١٢.

[←2]

. مليكة عطوي: الجريمة المعلوماتية حوليات، جامعة الجزائر، مجلة علمية، ٢٠١٢ العدد ٢١، ص ٨٠.

[←3]

مفتاح ابو بكر المطردي: الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدولة العربية لجمهورية السودان ٢٠١٢/٥/٢٣، ص ١٣.

[←4]

نظر القانون الامريكي: 12 – 13 لسنه ١٩٨٦ م، الخاص بمواجهة جرائم الكمبيوتر، مشار اليه في كتاب رامي متولي القاضي: مكافحة جرائم المعلوماتية، الطبعة الاولى، دار النهضة العربية، القاهرة، ٢٠١١م، ص ٢٣.

[←5]

نظر محمد منير الجنيهي ومحمد ممدوح الجنيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي الإسكندرية، ط١، ص ١٤، وكذلك محمد هشام رستم: جرائم الحاسب المستحدثة، دار الكتب القانونية، مصر، ط1، ص ١١٠.

[←6]

. علي محمد العريان: الجرائم المعلوماتية دار الجامعة الجديدة، الإسكندرية، ط 2، ص ١٧٠.

[←7]

سامي الشوا: الغش المعلوماتي كظاهرة إجرامية مستحدثة بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، ٢٥ و28 اكتوبر، ص ٥١٦.

[←8]

عبد الكريم عبد الله: جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية منشورات الحلبي الحقوقية، بيروت، ٢٠١١، ط١، ص ١٥.

[←9]

. أورد هذا التعريف د.احمد محمود عبابنة: جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ط 1، ص ١٧.

[←10]

. احمد محمود عبانبة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ط ١، ص١٩.

[←11]

. احمد محمود عبانبة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ط ١، ص١٩.

[←12]

ة بن عقون: السلوك الاجرامي للمجرم المعلوماتي، بحث لنيل شهادة الماجستير في القانون، جامعة باتنة، 2011 – 2012،
نقل عن فورة نائلة، جرائم الحاسب الاقتصادية، القاهرة، 2004، ص 21.

[←13]

مزة بن عقون: السلوك الاجرامي للمجرم المعلوماتي، بحث لنيل شهادة الماجستير في القانون، جامعة باتنة، 2011 – 2012، نقل عن فورة نائلة، جرائم الحاسب الاقتصادية، القاهرة، 2004، ص 21.

[←14]

مزة بن عقون: السلوك الإجرامي للمجرم المعلوماتي، بحث لنيل شهادة الماجستير في القانون، جامعة باتنة، 2011 – 2012، نقل عن فورة نائلة: جرائم الحاسب الاقتصادية، القاهرة، 2004، ص 21، نقلاً عن يونس عرب: دليل امن المعلوماتية والخصوصة، ص 213.

[←15]

د أمين أحمد الشوابكة: جرائم الحاسوب والإنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن، 2004، ط 1، ص 8 - 9.

[←16]

. سميرة بيطام: الجريمة الإلكترونية وتقنية الإجرام، المستحدث ص 1 – 4.

[←17]

ليكة عطوي: الجريمة الإلكترونية وتقنية الإجرام، المستحدث ص 9.

[←18]

. كامل مزيد السالك: الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب 23/12/2000، بدون صفحة.

[←19]

. علي كحلوش: جرائم الحاسوب وأساليب مواجهتها، مديرية الأمن الوطني الجزائري العدد 84 / 2007 ص 51.

[←20]

العال الديربي، محمد صادق اسماعيل: الجرائم الإلكترونية، الطبعة الاولى، المركز القومي للإصدارات القانونية، القاهرة 2012، ص 47.

[←21]

ي متولي القاضي: مكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة 2011، ص 52 – 53 وانظر ايضاً محمد محمد الألفي: المواجهة الأمنية والتشريعية لجرائم الإرهاب عبر الإنترنت المكتبة المصرية الحديثة، القاهرة ص 92.

[←22]

. احمد محمود عبابنة: جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ط ١، ص 36.

[←23]

د عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان الأردن 2011، ص 55.

[←24]

ة 54 من القانون المدني الأردني رقم (43) لسنة 1976 مشار إليه في الموقع الرسمي للتشريعات الأردنية ديوان الرأي.

[←25]

. خالد ممدوح ابراهيم: حوكمة الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية 2011 ، ص 360.

[←26]

. أحمد محمود عبابنة: جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ط ١، ص 35.

[←27]

. رامي متولي القاضي: مكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011، ص 35.

[←28]

امة احمد المناعسة: جلال محمد الزعبي، هايل فاضل الهواوشة: جرائم الحاسب الآلي والإنترنت، دار وائل للنشر، عمان الاردن، 2001، ص 106 – 107.

[←29]

. نهله عبد القادر الموفي: الجرائم المعلوماتية، رساله ماجستير، ط 2، دار الثقافة، عمان الاردن، 2010، ص 54.

[←30]

ـة احمد المناعسة، جلال محمد الزعبي، هايل فاضل الهواوشة: جرائم الحاسب الآلي والإنترنت، دار وائل للنشر، عمان الاردن، 2001، ص 106 – 107.

[←31]

ـة احمد المناعسة، جلال محمد الزعبي: جرائم تقنية نظم المعلومات الإلكترونية ط 1، دار الثقافة للنشر والتوزيع، 2010 ص 71.

[←32]

. محمد علي العريان: الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011، ص 77.

[←33]

. رامي متولي القاضي: مكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة 2011، ص 55.

[←34]

د العال الديربي ومحمد صادق إسماعيل: الجرائم الإلكترونية، الطبعة الأولى، المركز القدمي للاصدارات القانونية، القاهرة 2012، ص 58 - 59.

[←35]

. ابراهيم خالد ممدوح: الجرائم المعلوماتية، ط 1، دار الفكر الجامعي، الإسكندرية، 2009، ص 134 – 135.

[←36]

عياد الحلبي: إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الاولى، دار القافة للنشر والتوزيع، عمان الأردن 2011، ص 32 – 33.

[←37]

. نهله عبد القادر الموفي: الجرائم المعلوماتية، رساله ماجستير، ط 2، دار الثقافة، عمان الاردن، 2010، ص 77.

[←38]

ير بعنوان: الحرب الإلكترونية تقلق اسرائيل" مشار إليها عبر الموقع الرسمي لقناة الجزيرة الفضائية بتاريخ 13/6/2013
عبر الرابط التالي HTTP://www.aljazeera.net/ .

[←39]

. محمد الجبور: الوسيط في قانون العقوبات - القسم العام، دار وائل، عمان، ط 1، 2012، ص 59.

[←40]

يرة المعاشي: ما هية الجريمة المعلوماتية، مجله المنتدى القانوني، العدد السابع، جامعة محمد خضر بسره، الجزائر، ص 280.

[←41]

. عبد الفتاح حجازي: التزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ط 1، 2008، ص 58 – 59.

[←42]

. عبد الفتاح حجازي: التزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ط 1، 2008، ص 113.

[←43]

. راجع نصوص المواد 4 – 5 – 6 – 9 – 10 من قانون جرائم أنظمة المعلوماتية الأردني، رقم 30، لسنة 2010.

[←44]

. ابراهيم خالد ممدوح: حوكمت الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011، ص 100.

[←45]

. محمد الجبور: الوسيط في قانون العقوبات - القسم العام، دار وائل، عمان، ط 1، 2012، ص 238 وما بعدها.

[←46]

. محمد الجبور: الوسيط في قانون العقوبات - القسم العام، دار وائل، عمان، ط 1، 2012، ص 238 وما بعدها.

[←47]

. ابراهيم خالد ممدوح: حوكمت الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011، ص 109.

[←48]

. موسى مصطفى محمد: دليل التحري على شبكه الإنترنت، دار الكتب القانوني، مصر، 2010، ص 143.

[←49]

ع سامي الرواشدة واحمد الهياجنة: مكافحة الجرائم المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، الأردن، 2009، المجلد واحد، العدد 3، ص 128، وما بعدها.

[←50]

ال محمد غيطاس: أمن المعلوماتية والأمن القومي، مصر للطباعة والنشر، القاهرة، 2007، ص 212.

[←51]

. خالد ممدوح إبراهيم: الجرائم المعلوماتية المرجع السابق، ص 242 وما بعدها.

[←52]

. قانون جرائم أنظمة المعلوماتية الأردني، رقم 30، لسنة 2010 (الماده 3 فقرة ب).

[←53]

. يوسف حسن يوسف: الجرائم الدولية للإنترنت، المرجع السابق، ص 116.

[←54]

. علي جبار الحسيناوي: جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، 2009، ص 104.

[←55]

. جميل عبد الباقي الصغير: الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص 47.

[←56]

ن عزام الحيط: جرائم الذم والقدح والتحقير المرتكبه عبر الوسائط الإلكترونية، ط 1، دار الثقافة، عمان، 2011، ص 443.

[←57]

. محمد علي العريان: المرجع السابق ص 109 – 110.

[←58]

. خالد ممدوح إبراهيم: الجرائم المعلوماتية، المرجع السابق ، ص 297.

[←59]

. هدى حامد مشقوش: جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، ص 114 – 115.

[←60]

. علي عبد القادر القهوجي: الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديده للنشر، الإسكندرية، 1994، ص 63.

[←61]

. يوسف حسن يوسف: الجرائم الدولية للإنترنت، المرجع السابق، ص 116.

[←62]

ي عدنان الفيل: النظام القانوني للمعاملات الإلكترونية في الوطن العربي، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص 305.

[←63]

ف حسن يوسف: جريمة غسل الأموال بالطرق التقليدية عبر شبكات الإنترنت ويندك الويب، ط 1، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص 35.

[←64]

. جميل عبد الباقي الصغير: الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 47.

[←65]

. أسامة احمد المناعسه وجلال محمد الزعبي: جرائم تقنيه نزم المعلومات الإلكترونية، المرجع السابق، ص 285.

[←66]

. عادل عزام الحيط: المرجع السابق، ص 198 – 199.

[←67]

. خالد ممدوح ابراهيم: حوكمت الإنترنت، المرجع السابق، ص ٤١٠ – ٤١١.

[←68]

. جمال محمد غيطاس: المرجع السابق، ص 63 وما بعدها.

[←69]

. أسامة احمد المناعسة، وجلال محمد الزعبي: جرائم تقنية نظم المعلومات الإلكترونية، المرجع السابق، ص 265.

[←70]

. محمد محمد الالفي: المرجع السابق ص 94.

[←71]

. جميل عبد الباقي الصغير: الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 33.

[←72]

. عبد الفتاح بيومي حجازي: الجريمة في عصر العولمة،ط 1، دار النهضة العربية، القاهرة، 2010، ص 193.

[←73]

ع المادة 6 / 2 من نظام مكافحة جرائم المعلوماتية السعودي رقم 2 / 17 لسنه 1428 هـ مشار إليه في الموقع الرسمي لمجلس الوزراء السعودي على الرابط التالي /HTTP//www.boe.gov.so

[←74]

. يوسف المصري: المرجع السابق، ص 85.

[←75]

، المادة رقم 21 من قانون جرائم المعلوماتية السوداني لسنه 2007، مشار إليه في الملحق رقم 4 في كتاب محمد علي العريان المرجع السابق 313.

[←76]

ت المادة 35 ق. إجراءات إماراتي " على مأموري الضبط القضائي وعلى مرؤوسيهم إجراء المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلمون بها بأي كيفية كانت".
وتنص المادة 43 من القانون نفسه على مأموري الضبط القضائي في حالة التلبس بجريمة أن ينتقل فورا إلى محل الواقعة، ويعاين الآثار المادية للجريمة ويحافظ عليها، ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة ... وعليه إخطار النيابة العامة فوراً بإنتقاله وعلى النيابة العامة الأنتقال فوراً إلى محل الواقعة بمجرد إخطارها بجناية متلبس بها.
كما تنص المادة 90 من ق.إجراءات مصري "ينتقل قاضي التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة الأماكن والأشياء والأشخاص ووجود الجريمة مادياً وكل ما يلزم إثبات حالته ...."
كما نصت المادة 42 من ق.إجراءات جزائري "أنه يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور، ثم ينتقل بدون تمهل إلى مكان الجناية، ويتخذ جميع التحريات اللازمة، وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي، وأن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة ...".

[←77]

لة هبة هروال: الجوانب الإجرائية الجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2007، ص 212.

[←78]

. محمد حماد الهيتي: التحقيق الجنائي والأدلة الجرمية، المرجع السابق، ص 74.

[←79]

. محمود نجيب حسني: شرح قانون الإجراءات الجزائية، دار النهضة العربية، القاهرة، 1982، ص ٦٥٥.

[←80]

ـن محمد سلامة: الإجراءات الجنائية في التشريع المصري، ج 1، دار النهضة العربية، القاهرة، 2000، ص 642، راجع كذلك في هذا الإطار كامل السعيد: شرح قانون أصول المحاكمات الجزائية، ط3، دار الثقافة للنشر والتوزيع، عمان، 2010، ص 437 وما بعدها.

[←81]

. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص 153.

[←82]

ن المادة 146 ق.إ.م.إ.الجزائري وجاء فيها: "يجوز للقاضي من تلقاء نفسه أو بطلب من الخصوم القيام بإجراء معاينات أو تقييمات أو تقديرات أو إعادة تمثيل الوقائع التي يراها ضرورية مع الانتقال إلى عين المكان إذا أقتضى الأمر ذلك...".

[←83]

س المادة 79 ق.إ. ج. الجزائري: "يجوز لقاضي التحقيق الأنتقال إلى أماكن وقوع الجريمة لأجراء المعاينات اللازمة أو للقيام بتفتيشها ..." ، وتقابلها المادة 90 ق.إ.ج المصري: "ينتقل قاضي التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً ..."

[←84]

. محمد حماد الهيتي: التحقيق الجنائي والأدلة الجرمية، المرجع السابق، ص 75.

[←85]

. نبيلة هبة هروال: المرجع السابق، ص 216.

[←86]

من محمد إبراهيم: الحماية الجنائية لحق المؤلف عبر الإنترنت، رسالة دكتوراه في الحقوق جامعة عين شمس، 2000، ص 154، وانظر كذلك عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه في القانون الجنائيي, كلية الحقوق جامعة عين شمس, 2004.، ص 895، وانظر كذلك خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم المعلوماتية، المرجع السابق، ص 156 – 157.

[←87]

. Daniel Morris tracking a computer hacker us attorneys bulletin 2/2001 p 3 available at: http//www.usa.gov/criminal/cybercrime us a may 2001 htm.

[←88]

زيد راجع حسن محمد إبراهيم: المرجع السابق، ص 155، وراجع أيضاً منى فتحي أحمد عبد الكريم: المرجع السابق، ص 179، كذلك عبد الله حسين علي محمود: سرقة المعلومات المخزنة في الحاسب الآلي، رسالة دكتوراه في الحقوق كلية الحقوق، جامعة عين شمس، 2001، ص 357.

[←89]

لة هبة هروال: المرجع السابق، ص 218، وأنظر كذلك عمر محمد بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص 896، انظر أيضاً منى فتحي أحمد عبد الكريم: المرجع السابق، ص 178، وأنظر أيضاً: محمود عمر محمود: المسؤولية الجنائية الناشئة عن جرائم المحمول، رسالة دكتوراه في الحقوق، كلية الحقوق جامعة عين شمس، 2011، ص 141، وانظر أيضاً: أيمن عبد الحفيظ: حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة بحوث الشرطة العدد 25، يناير 2004، ص 367.

[←90]

. Sousan Brenner, model code of cybercrime, investigation procedure p 24 unit Dayton school of law available online at http//cybercrimes.net.mccib.htm 2014/07/05تاريخ الإطلاع

[←91]

ي الو.م.أ توجد نيابة متخصصة في أعمال التحقيق في جرائم الحاسب والاتصالات، وهي مشكلة من مجموعة من أعضاء النيابة العامة ممن تلقوا تدريباً كافياً على نظام المعالجة الآلية للبيانات، ولهم خبرة في هذا المجال أي كيفية التعامل مع الدليل الرقمي وكيفية بناء عريضة الإتهام أمام المحكمة، كما تم منحهم صلاحيات كبيرة في مجال الإستعانة بغيرهم من خبراء وزارة العدل لاسيما قسم جرائم الحاسب والإعتداء على حقوق الملكية الفكرية. للمزيد راجع أيمن عبد الحفيظ: المرجع السابق، ص 367، وانظر كذلك محمد الأمين بشري: التحقيق في جرائم الحاسب الآلي، المجلة العربية للدراسات الأمنية والتدريب، العدد 30، جامعة نايف العربية للعلوم الأمنية، الرياض نوفمبر 2000، ص 30.

وفي فرنسا نجد فريق من الشرطة يقوم بالإشراف على تنفيذ المهمات التي يعهد بها إليه وكلاء النيابة والمحققين وجميعهم ممن تلقوا تدريباً كافياً في هذا المجال، وهم يقومون بمرافقة المحققين أثناء المعاينة حيث يقومون بفحص كل جهاز ونقل نسخة من الأسطوانة الصلبة وبيانات البريد الإلكتروني ثم يقومون بعمل تقرير يرسل إلى القاضي الذي يتولى التحقيق.

راجع صالح أحمد البربري: دور الشرطة في مكافحة جرائم الإنترنت في إطار الإتفاقية الموقعة في بودابست، 23/11/2001، منشور بموقع الدليل الإلكتروني للقانون العربي بتاريخ 2/9/2006: http//www.arablawinfo.com

[←92]

مد الأمين بشري: التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص 30، راجع بشأن القواعد والإرشادات الفنية التي وجب اتخاذها في إطار المعاينة عبد الله حسين علي محمود: المرجع السابق، ص 358 - 359، وأنظر كذلك أحمد سعد محمد الحسيني: الجوانب الإجرائية للجرائم الناشئة عن إستخدام الشبكات الإلكترونية، رسالة دكتوراه في القانون كلية الحقوق، جامعة عين شمس، القاهرة، 2012، ص 80-81.

[←93]

. أحمد سعد محمد الحسيني: المرجع السابق، ص 78.

[←94]

حظ أنه في حين يستخدم النظام الأنجلو أمريكي مصطلح search كمصطلح واحد للدلالة على تفتيش المسكن والشخص نجد أن النظام الفرنسي يستخدم مصطلح fouille a corps في حالة تفتيش الشخص ومصطلح perquisition في حالة تفتيش المسكن للمزيد أنظر: هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ط 1، دار النهضة العربية، القاهرة، 1997، ص 47.

[←95]

ت المادة 41 من الدستور المصري الصادر في 11 سبتمبر 1971 "الحرية الشخصية حق طبيعي وهي مصونة لا تمس، فيما عدا حالة التلبس لا يجوز القبض على أحد أو تفتيشه أو حبسه أو تقييد حريته بأي قيد أو منعه من التنقل إلا بأمر تستلزمه ضرورة التحقيق وصيانة أمن المجتمع ويصدر هذا الأمر من القاضي المختص أو النيابة العامة وذلك وفقا لأحكام القانون"، كما نصت المادة 44 من نفس الدستور " للمساكن حرمة فلا يجوز دخولها ولا تفتيشها إلا بأمر قضائي مسبب وفقا لأحكام القانون" ونص التعديل الدستوري لسنة 1996 الصادر بموجب المرسوم الراسي رقم 96 - 438 المؤرخ في 26 رجب 1417 الموافق 07 ديسمبر 1996 جريدة رسمية 76 الصادرة في 08 ديسمبر 1996 في المادة 40 منه على التفتيش وجاء فيها " تضمن الدولة عدم إنتهاك حرمة المسكن. فلا تفتيش إلا بمقتضى القانون، وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

[←96]

. أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1980، ص 449.

[←97]

. فوزية عبد الستار: شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1986، ص 278.

[←98]

. Conseil de L'Europe: problèmes de procédure pénale lies à la technologie de l'information. Recommandation N.R (95) 13 et expose des motifs. Ed. Conseil de l'Europe، 1996 p 28.
راجع رامي متولي القاضي: مكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2012، ص 92.

[←99]

. la perquisition: "recherche policière ou judicaire des éléments de preuve d'une infraction، strictement réglementée elle peut être réalisée au domicile de toute personne ou en tout autre lieu ou pourraient se trouver des objets dont la découverte serait utile à la manifestation de la vérité".

راجع بكري يوسف بكري: التفتيش عن المعلومات في وسائل التقنية الحديثة، ط 1، دار الفكر الجامعي، الإسكندرية، 2011، ص 58.

[←100]

. تنقسم المكونات المادية للحاسب الآلي إلى ست وحدات:

. وحدة الإدخال: input unit وهي تلك الوسائل التي تستخدم في إدخال البيانات والبرامج إلى وحدة التشغيل المركزية وأهمها لوحة المفاتيح، الفأرة القلم الضوئي ...

. وحدة الذاكرة الرئيسية: main memory وتستخدم لحفظ البيانات والمعلومات والبرامج حفظا دائما ومؤقتاً.

. وحدة الحساب والمنطق: arithmetic and logic unit وهي المسؤولة عن معالجة البيانات حسابياً ومنطقياً وتتكون من مجموعة من الدوائر الإلكترونية والمنطقية ومجموعة من المسجلات.

. وحدة التحكم : control unit وهي أساس عمل وحدة المعالجة المركزية وهي التي تقوم بالتنسيق بين مختلف وحدات الحاسب وضبط كافة العمليات التي تتم داخل وحدة المعالجة.

. وحدات الإخراج: out unit وهي تلك الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات الشاشة، الطابعة الراسم...

وحدات التخزين الثانوية secondary storage units وهي أوساط تخزين ثانوية مثل الأقراص المغناطيسية، الأشرطة المغناطيسية للمزيد راجع هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 71-72.

[←101]

نات المنطقية للحاسب computer software وهي عبارة عن تعليمات مكتوبة بلغة ما وتنقسم إلى نوعين برامج النظام وبرامج التطبيقات، هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 72.

[←102]

عبد الحفيظ: حدود مشروعية أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، العدد 25، يناير 2004، ص 380، راجع كذلك على محمود على حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، أبريل 2003، المجلد الأول ص 269 وما يليها.

[←103]

. هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 73-74.

[←104]

. PIRAGOFF (Donald K): «computer crimes and other crimes against information technology in Canada » R.I.D.P. (vol.64) 1e et 2e trimestres 1993 p239-241.

[←105]

. VASSILAKI (Irini): « computer crimes and other crimes against information technology in Greece » R.I.D.P.1993 p368-371.

[←106]

. وهي جريمة الولوج غير المصرح به على نظام الحاسب الآلي لتسهيل إرتكاب أفعال غير مشروعة عن قصد ويعاقب عليها لمدة أقصاها 5 سنوات

An offence of unauthorized access with Internet to commit or facilitate commission of further offences has also been created which carries a maximum sentence of 5 years imprisonment.

[←107]

وهي جريمة التعديل غير المصرح به لنظام الحاسب الآلي ويعاقب بنفس العقوبات الواردة في القسم الثاني أعلاه .

An offence of unauthorized modification of computer material in created which carries the same penalties as the section 2 offence above.

[←108]

. وهي مجرد الولوج غير المرخص به إلى نظام الحاسب دون ارتباطه بجريمة أخرى يعاقب عليها بالحبس مدة أقصاها ستة شهور

An offence of unauthorized access to computer material، the offence carries a maximum 6 month period of imprisonment.

[←109]

. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 197، أنظر أيضا هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 76.

[←110]

التقرير العام لمؤتمر A.I.D.P الجمعية الدولية القانون العقوبات Association international de droit penal
مأخوذ من هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 76.

Durham Cole: «the emerging structures of criminal information law: tracing the contours of a new paradigm R.I.D.P (vol.64) 1e et 2e trimestres 1993 p 93-113.

[←111]

. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 378.

[←112]

فتحي عبد الكريم: المرجع السابق، ص 188، وكذلك هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي المرجع السابق ص 82.

[←113]

. SAGROS (pierre) et MASSE (Michel) le droit pénal et l'informatique journées d'étude du 15 nov 1980 publication d'institut de science criminelle de la faculté de droit de Poitiers éd. Cujas Tom IV p25-29.

[←114]

. هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 85.

[←115]

. article 94 du C.P.P.F، dispose que: "les perquisitions sont effectuées dans tous les lieux ou peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité."

[←116]

. هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 87.

[←117]

. رامي متولي القاضي: المرجع السابق، ص 96.

[←118]

. قانون رقم 09 – 04 السالف الذكر.

[←119]

. الحالات التي ذكرتها المادة 04 من القانون 09-04 والتي من غيرها لا يمكن إجراء التفتيش هي:
الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
في حالة توفير معلومات عن الجمال الإعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
المقتضيات التحريات والتحقيقات الفضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

[←120]

. Article 19-Perquisition et saisie de données informatiques stockées

1. Chosque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autonités compétentes à perquisitionner ou à accéder d'une façon similaire:
    a. à un système informatique ou à une partie de celui-ci ainsi qu 2'aux données informatiques Qui y sont stockées; et sur son territoire.
    b. à un support de stockage informatique permettant de stocker des données informatiques.

[←121]

يقصد بالنظام المعلوماتي حسب هذه الاتفاقية كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذاً لبرنامج معين بأداء معالجة آلية للبيانات.

Système informatique: "désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou don't un ou, plusieurs éléments assurent en exécution d'un programme, traitement automatisé de données"

[←122]

. هلالي عبد اللاه أحمد: الجوانب الموضوعية والإجرائية للجرائم المعلوماتية, المرجع السابق, ص 234.

[←123]

. MOHRENSCHLAGER (Manfred): computer crimes and other crimes against information technology in Germany R.1.D.P. (vol.64) 1e et 2e trimesters, 1993 P343-351

[←124]

. KASPERSEN (W.K.Henrik) computer crimes and other crimes against information technology in the Netherlands R.I.D.P. (vol.64) 1e et 2e trimesters, 1993 P479-486

[←125]

. loj 18 mars 2003 pour la sécurité intérieur article 17 www.legifrance.gouv.fr/w.Aspad/un texte dejorf2 numéro-21/06/2003. Article 57-1/1

- Créé par Loi 2003-239 2003-03-18 art. 17 1° JORF 19 mars 2003
- Créé par Loi n°2003-239 du 18 mars 2003 - art. 17.

Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre systéme informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

[←126]

. Article 19-2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci. Conformément au paragraphe 1 (a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un d'un accès d'une façon similaire à l'autre système.

[←127]

. حسن محمد إبراهيم: المرجع السابق, ص 162.

[←128]

. Sieber (Ulrich) computer crimes and other crimes against information technology “commentary and preparatory questions for the colloquium of the A.I.D.P. in Wurzburg" R.I.D.P. (vol.64) 1e et 2e trimestres 1993 P70-77.

[←129]

. KASPERSEN (W.K.Henrik): op.cit P503-504

ولذا فإن السائد في هولندا هو نظام التفويض الإلتماسي letters rogatory وذلك لحث سلطات الدول الأخرى على نسخ البيانات الموجودة على أراضيها وإرسالها إلى السلطات الهولندية مع المعاملة بالمثل مأخوذ من هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق ص 78.

[←130]

. MOHRENSCHLAGER (Manfred): op.cit P351.

[←131]

. MOHRENSCHLAGER (Manfred): op.cit P356.

[←132]

. Article 57-1/2

- Créé par Loi 2003-239 2003-03-18 art. 17 1° JORF 19 mars 2003
- Créé par Loi n°2003-239 du 18 mars 2003 - art. 17=

S'il est préalablement avéré que ces données‹ accessibles à partir du système initial ou disponibles pour le système initial‹ sont stockées dans un autre système informatique situé en dehors du territoire national‹ elles sont recueillies par l'officier de police judiciaire‹ sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

[←133]

. حسن محمد إبراهيم: المرجع السابق، ص 162.

[←134]

. conseil de L'EUROPE, la criminalité informatique recommandation no R 89 sur la criminalité en relation avec ordinateur et rapport final du comité européen pour les problèmes criminels, Strasbourg, conseil du Europe.

راجع حسن محمد إبراهيم، المرجع السابق ص 163.

[←135]

. **Article 32 Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public**

Une Partie peut, sans l'autorisation d'une autre Partie:

A. Accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données

B. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

[←136]

. حسن محمد إبراهيم: المرجع السابق، ص 173.

[←137]

. Article 57-1/3: Les données auxquelles il aura été permis d’accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code.

[←138]

. هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 197-199.

[←139]

. حسن محمد إبراهيم: المرجع السابق، ص 174.

[←140]

. هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 197.

[←141]

. أحمد محمود مصطفى: جرائم الحاسبات الآلية في التشريع المصري، ط1، دار النهضة العربية، القاهرة، 2010، ص 158 – 159.

[←142]

. Article 19-3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1ou 2. Ces mesures incluent les prérogatives suivantes:

a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci ou un support de stockage informatique.
b. réaliser et conserver une copie de ces données informatiques.
c. préserver l'intégrité des données informatiques stockées pertinentes.
d. rendre inaccessibles ou enlever ces données informatiques du systéme infirmatique consulté.

[←143]

. هلالي عبد اللاه أحمد: الجوانب الموضوعية والإجرائية الجرائم المعلوماتية، المرجع السابق، من 241.

[←144]

ء فيها: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف من الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقاً للقواعد المقررة في قانون الإجراءات الجزائية".

[←145]

ة بن قارة مصطفى: حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة الإسكندرية, 2010, ص 164.

[←146]

. بكري يوسف بكري: المرجع السابق، ص 137.

[←147]

علواني هليل: التحقيق الجنائي والتصرف فيه والأدلة الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2007، ص 625.

[←148]

، المادة 303 مكرر من ق.ع.ج على أنه يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة لأشخاص بأي تقنية كانت وذلك

بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاء.

بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

[←149]

لفتاح بيومي حجازي: الجوانب الإجرائية الأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2009، ص 791 – 792.

[←150]

لور البريد الإلكتروني بتطور شبكات الاتصال المعلوماتية فمع إنشاء شبكة وكالة المشروعات البحثية المتقدمة لتابعة لوزارة الدفاع الأمريكية أربانيت ARPANET وهي مختصر لAdvanced research projects agency Network سنة 1969 بدأ الاتصال بين الحاسبات على شكل نقل أو إرسال ملفات من جهة إلى أخرى ومع ازدياد عدد مستخدمي الشبكات في السبعينات وتوصيل شبكة الجامعات والمراكز البحثية في و.م.إ بشبكة الأربانيت ظهرت الحاجة إلى إضافة تطبيق آخر للشبكة مفاده إمكانية قيام أحد مستخدمي الشبكة بإرسال رسالة إلكترونية إلى مستخدم آخر من المشتركين فيها وازدهرت هذه النوعية من الخدمات في الثمانينات ثم ازداد اتساعا بربط الشبكة الأمريكية بشبكة الأبحاث الأوروبية ERAN وربط هاتين الشبكتين بشبكة الاتصالات الإنترات المزيد راجع هلالي عبد اللاه أحمد: تقليل نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 212.

[←151]

. هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، من 215.

[←152]

. FRANCILLON (jacques), les crimes informatiques et d’autres crimes dans le domaine de la technologie informatique en France R.LD.P. (vol.64) 1 et 2 trimestres 1993 PP 302-309.

[←153]

. **Article 100** En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou Supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de L'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.
La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

[←154]

. **Article 100-2** Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

[←155]

.WISE (Edward M): computer crimes and other crimes against information technology in The United States R.I.D.P. 1993 P666.

[←156]

. YAMAGUCHI (ATSUSHI) computer crimes and other crimes against information technology in Japan R.L.D.P. (vol.64) 1e et 2e trimestres 1993 P443-448.

[←157]

. PIHLAJAMAKI (A ntti): computer crimes and other crimes against information technology in Finland R.L.D.P. (vol.64) 1e et 2e trimestres 1993 P286-290.

[←158]

. نصت المادة 65 مكرر 5 من ق.إ.ج جزائري: " إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال والإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:...=

=...

اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

- وضع الترتيبات التقنية دون موافقة المعنيين من أجل النقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص".

[←159]

. حسن محمد إبراهيم: المرجع السابق، ص 176.

[←160]

أن الاثبات الجنائي ينصب في المعتاد على حوادث عابرة تقع فجأة فلا يسبقها تراض أو إتفاق أما الإثبات المدني فإنه ينصب عادة على إثبات واقعة تقابل الإيجاب مع القبول وهي واقعة معدة ومرتبة مقدماً. للمزيد راجع فرج علواني هليل: المرجع السابق، من 514.

[←161]

ـ محكمة النقض الشهادة على أنها تقرير الشخص لما يكون قد رأه أو سمعه بنفسه أو أدركه يوجه العموم بحواسه للمزيد راجع سرقة المعلومات المخزنة في الحاسب الآلي، المرجع السابق، ص 334، جاء في أحد أحكام محكمة النقض المصرية بتاريخ 13/3/2000 ما يلي: "لا يشترط في شهادة الشاهد أن تكون واردة على الحقيقة المراد إثباتها بأكملها ويجمع تفاصيلها على وجه دقيق بل يكفي أن تكون من شأن تلك الشهادة أن تؤدي إلى هذه الحقيقة بإستنتاج سائغ تجربه محكمة الموضوع يتلائم به ما قاله الشاهد بالقدر الذي رواه مع عناصر الإثبات الأخرى المطروحة أمامها راجع احمد سعد محمد الحسيني، المرجع السابق، ص 128، راجع كذالك فيما يخص الشهادة وأحكامها في القانون الفرنسي:
Jean Larguier, Philippe conte, op.cit, p 341-346.

[←162]

. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص 945.

[←163]

. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 339.

[←164]

. فهد عبد الله العبيد العازمي: الإجراءات الجنائية المعلوماتية، رسالة دكنوراه في الحقوق، جامعة عين شمس، 2012، ص 447.

[←165]

. عبد الله حسين علي محمود: المرجع السابق، ص 380.

[←166]

. احمد محمود مصطفى: المرجع السابق، ص 144.

[←167]

. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 340.

[←168]

ر قانون الدليل الخاص بولاية كالفورينيا شهود الجريمة المعلوماتية في 1. محلل النظم الذي صمم وحده برنامج الكمبيوتر الذي أنتج الدليل، 2. المبرمج الذي قام بتحرير البرنامج واختباره، 3. المشغل الذي يقوم بتشغيل البرنامج، 4. طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها، 5. أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة والاسطوانات التي تشتمل على البيانات المصدرية الصحيحة، 6. مهندس الصيانة الإلكترونية الذي يقوم على صيانة الجهاز الأصلي والتأكد من جاهزيته، 7. موظفو المدخلات والمخرجات المسؤولون على معالجة المدخلات والمخرجات يدوياً قبل وبعد أداء العمل، 8. مبرمجو صيانة النظام والمسئولون عن سرية عمل الكمبيوتر، 9. المستخدم النائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نواتجها. راجع عبد الله حسين علي محمود: المرجع السابق، ص 380، راجع أيضاً خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 264 – 265.

[←169]

. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 340.

[←170]

ت التوصية الرابعة للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات إلى أن تنفيذ المكنات القسرية المنوطة برجال السلطة العامة يجب أن يكون متناسباً مع الطابع الخطير لانتهاك، ولا يسبب سوى الحد الأدنى من إعاقة الأنشطة القانونية للفرد. للمزيد في هذا الإطار راجع عبد الفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 614-616.

[←171]

. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 344.

[←172]

. عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 345.

[←173]

الفتاح بيومي حجازي: الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 619.

[←174]

. MOHRENSCHLAGER (Manfred): op.cit P351, Ulrich Sieber, op.cit p77.

[←175]

. Erman (Sahir) les crimes informatique et d'autre crimes dans le domaine de la technologie informatique en Turquie, R.I.D.P (vol.64) 1e et 2e trimestres 1993 pp 617-624.

[←176]

. KUNSEMULLER (CARLOS): “computer crimes and other crimes against information technology in Chile” R.I.D.P. (vol.64) 1e et 2e trimestres 1993 p256-259.

[←177]

. حسن محمد إبراهيم: المرجع السابق، ص 178، أنظر كذلك فهد عبد الله العبيد العزمي: المرجع السابق، ص 454.

[←178]

. FRANCILLON (jaques), op.cit, p 309.

[←179]

. KASPERSEN (W.K.Henrik), op.cit P496.

[←180]

. VASSILAKI (Irini): op.cit P371.

[←181]

. أحمد سعد محمد الحسيني: المرجع السابق، ص 138.

[←182]

ي المادة 10 من القانون 09-04 مايلي: "في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

[←183]

هذه التقنية وسيلة اتصال سمعي مرئي متعدد الأطراف، حيث يستطيع بمقتضاها شخصين أو أكثر المشاركة في حديث ومناقشة رغم اختلاف الأماكن التي يتواجدون فيها للمزيد راجع

Gasli, la participation a distance dans le proces penal p17.

راجع حسن محمد إبراهيم: المرجع السابق، ص 180.

[←184]

ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 262 - 263، أنظر أيضا حسن محمد إبراهيم: المرجع السابق، ص 180.

[←185]

. Fabrizio l'aménagement en vidéo conférence des audiences relatives à la grande criminalité par la loi italienne du 07/01/1998. راجع أحمد سعد محمد الحسيني المرجع السابق ص142

[←186]

. le procés à distance au moyen de la vidéo conférence: l'expérience italienne, dixième congrès des nations unies

راجع أحمد سعد محمد الحسيني المرجع السابق، ص 143

[←187]

. أحمد سعد محمد الحسيني: المرجع السابق، ص 144.

[←188]

. Thierry Garé, Catherine Gineste, Droit pénal - procédure pénale,: 7 édition DALLOZ 2012 p 244.

[←189]

. فرج علواني هليل: المرجع السابق، ص 508.

[←190]

حسن محمد إبراهيم: المرجع السابق، ص 181، راجع كذلك في ما يتعلق بالخبرة وأحكامها أحمد سعد محمد الحسيني: المرجع السابق، ص 83.

[←191]

. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص 1031.

[←192]

في نص المادة 85 ق.إ.ج مصري "إذا استلزم إثبات الحالة الاستعانة بطبيب أو غيره من الخبراء يجب على قاضي التحقيق الحضور وقت العمل وملاحظته ...:"

[←193]

. وفي هذا تقرر محكمة النقض المصرية بحكم صادر في 28/5/1985 بموجب الطعن رقم 04 سنة 42 قضائية ما يلي: لا يجوز للمحكمة أن تقضي في المسائل الفنية بعلمها بل يجب الرجوع فيها إلى رأي أهل الخبرة ... "للمزيد راجع مصطفى يوسف: مشروعية الدليل في المسائل الجنائية، دار الجامعة الجديدة، الإسكندرية، 2011، ص 117.

[←194]

. ورد في نص المادة 143 ق.إ.ج.جزائري "الجهات التحقيق أو الحكم عندما تعرض لهل مسألة ذات طابع فني أن تأمر بندب خبير إما بناءً على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم ...".

[←195]

. Meunier (c): la loi du 28 novembre 2000 relative à la criminalité informatique. Revue de droit Pénal Criminel 2002 p 680-683.

[←196]

لفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب المصرية، القاهرة، 2009، ص 97.

[←197]

سعد محمد الحسيني: المرجع السابق، ص 86-87، في نوفمبر سنة 2000 قامت الولايات المتحدة الأمريكية بتأسيس فرع جديد في المباحث الفيدرالية الأمريكية (FBI) أطلق عليه المعمل الأقليمي الشرعي للحاسب الآلي مقره سان ديجو ذو خبرة متعدد النواحي، غرضه مكافحة ...= ...= التصعيد الخطير في الجريمة عبر الإنترنت، بحيث يتم إعداد محللين شرعيين للحاسب الآلي مهمتهم تحليل وتصنيف الدليل الرقمي. راجع أحمد سعد محمد الحسيني: المرجع السابق، ص 87.

[←198]

لله حسين محمود: المرجع السابق، ص 182، راجع كذلك عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 330.

[←199]

. Waterplas. J.R. informatique et délinquance: un nouveau deffi pour les magistrats et les policiers R.D.P.C Aout-Septembre 1985 p 735.

[←200]

. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص 1043-1044.

[←201]

ضية تتلخص وقائعها في تلقي إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بلاغاً يفيد بإكتشافها وصول عدة أقراص مدمجة تحمل صوراً خاصة لها ومكالمات هاتفية مع خطيبها مما سبب لها أضراراً جسيمة، كما اكتشفت صور لها مركبة على جسد فاضحة بموقع الفيس بوك، وقد كشفت عمليات التتبع والفحص الفني عن طريق الخبراء الجاني الذي تبين أنه خطيبها السابق. وفي قضية أخرى تتلخص وقائعها في نجاح رجال المباحث الجنائية الكويتية من ضبط مراهق كويتي لم يتعد عمره 18 بعد اتهامه بأنه يقف وراء بث شريط الفيديو المسيء لقيادات في وزارة الداخلية، وتم كشف هويته بعد أن أوضح المصدر أن رجال الدعم الفني بدأوا بمتابعة المقطع، حيث وعن طريق ال IP تم تتبع مصدر المقطع وصولاً إلى الجهاز الذي تم منه النشر ثم تحديد هوية الجاني. للمزيد راجع أحمد سعد محمد الحسيني: المرجع السابق، ص 89 -90.

[←202]

. عائشة بن قارة مصطفى: المرجع السابق، ص 148 – 149.

[←203]

دية محمد: الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، المجلة الأكاديمية للبحث القانوني، السنة الخامسة، المجلد 09 عدد 01-2014، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة بجاية، ص 248.

[←204]

. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 303 – 304.

[←205]

عباد الحلبي: المرجع السابق، ص 206 - 207، وكذلك راجع خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 305.

[←206]

، أمثلة هذه البرامج برنامج hack tracer v1.2 وهو يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الاختراق يحتوي على أسم وتاريخ الواقعة وعنوان IP الذي تمت منه عملية الاختراق وأسم الدولة والشركة مزودة الخدمة ورقم المنفذ والشبكة التي تتبعها الشركة ... راجع خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 306.

[←207]

. خالد عياد الحلبي: المرجع السابق، ص 210 – 212.

[←208]

. محمد الأمين بشري: التحقيق في جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص 186.

[←209]

. خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 308.