الجمهورية الجزائرية الديمقراطية الشعبية

جامعة الدكتور مولاي الطاهر سعيدة

كلية الحقوق والعلوم السياسية

قسم الحقوق

دور الشـــــــرطة القضـــــــائية في مكافحـــــة الجريمـــــة الإلكترونيـــــة

مذكرة تخرج لنيل شهادة الماستر

تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالب:
مخلوف عكاشــة

تحت إشراف الدكتور:
فليح كمال محمد عبد المجيد

أعضاء لجنة المناقشة:

- الدكتور: دربة أمين ..... رئيسًا
- الدكتور: فليح كمال محمد عبد المجيد ..... مشرفًا ومقررًا
- الدكتور: نابي عبد القادر ..... عضوًا
- الدكتور: وقاس ناصر ..... عضوًا

السنة الجامعية: 2016-2017

بسم الله الرحمن الرحيم

الإهـــــــــــداء

الإهـــــــــــــداء

أهدي نجاحي هذا إلى:

ـالمرحوم أبي الغالي الحاج عيسى رحمه الله وطيّب ثراه.

ـأمي الحاجة الخالدية التي علمتنا معنى الصبر والعلم والعمل .

ـمن قال فيها الرسول صل الله عليه وسلم " الدنيا متاع وخير متاعها الزوجة الصالحة" زوجتي العزيزة التي أعانتني في السراء والضراء.

ـأولادي (سليمة، محمد، عيسى، عبير) حفظهم الله ورزقهم العلم النافع.

ـإخوتي وأخواتي .

ـإخوتي التي لم تلدهم أمي.

-أصدقائي على مستوى العمل بمؤسسة الإسمنت بالحساسنة وخاصة مصلحة الضبط والقياس و المراقبة.

ـزملاء الدراسة بكلية التكنولوجيا تخصص أنظمة و مركبات الإتصال.

ـزملاء الدراسة بكلية الحقوق والعلوم السياسية تخصص قانون جنائي وعلوم جنائية .

شـــــكر وإمتنـــــان

شـــكر وإمتنـــان

أتقدم بجزيل الشكر والإمتنان إلى الأستاذ فليح كمال على ما بذله من مجهودات وملاحظات جمة وقيمة لإخراج هذا البحث بهذه الصورة.

كما أتقدم بالشكر لأعضاء لجنة المناقشة الذين قبلوا مناقشة هذا البحث، الأستاذ دربة أمين، والأستاذ وقاص ناصر، والأستاذ نابي عبد القادر، جزاهم الله خير الجزاء ونفع بهم.

كما أشكر صديقي وزميلي يعقوب ناجي وطلبة دفعة 2017 تخصص قانون جنائي والعلوم الجنائية، وطلبة دفعة أنظمة ومركبات الإتصال بكلية العلوم والتكنولوجيا.

والشكر موصول إلى كل من ساعدني لإنجاز هذا البحث.

المقدمـــــة

لقد شهدت البشرية في ظرف وجيز من الزمن ، مقارنة بما سبق من عهد التاريخ البشري تطورا فائقا نقلها نقلة نوعية من عالم إلى أخر ، فتحولت عديد مظاهر الحياة من كل ما هو تقليدي و مادي، إلى ما هو حديث و رقمي ، و ذلك بفعل إنتشار تقنية المعلوماتية في حقبة السبعينيات من القرن الماضي ، فأصبحت الإستعمالات اليومية للحواسيب و شبكات الإتصال أمراً شائعاً داخل أغلب المجتمعات المتحضرة ، و قد تغلغلت التقنية المعلوماتية في كل جوانب الحياة ، فأصبحت و بما توفره من تسهيلات و بفضل ما تشهده من تطور مستمر و دائم ، التقنية الأولى و بدون منازع التي تستعين بها المجتمعات في شتى مجالات حياتهم ، و ذلك من خلال الإعتماد عليها للتحكم في تسيير المرافق الحيوية للدول والحكومات ، كالإدارة الإلكترونية ، و مجلات الدفاع و الأمن ، و الإقتصاد والصحة...إلخ

و هي و بالإضافة لذلك تشهد إنتشاراً واسع النطاق على المستوى الإجتماعي فأفراد المجتمعات أصبحوا يديرون شؤون حياتهم اليومية من خلال مجموعة التطبيقات التي توفرها تقنية المعلوماتية، كالتواصل المباشر و تبادل المعارف و المعلومات والتعاقد عن بعد عن طريق شبكة الأنترنت، بل و قضاء كل ما كان مستعصياً من قبل بفعل العوائق الجغرافية و المادية و التي أصبحت في ظل عالم المعلوماتية مجرد أرقام و رموز إلكترونية ، و التي لا يتطلب أمر تجاوزها سوى الكبس على زر من أزرار لوحة مفاتيح الحاسوب ، و بذلك فقد غيرت هذه التقنية من نمط الحياة البشرية فإرتقت بها و جعلت منها حياة أفضل تميزها السرعة و التطور و اليسر.

غير أن كل هذا التطور و التحول في أسلوب حياة الإنسان حمل معه مظاهر سلبية أثرت على أمن الدول والأفراد بالسلب ، و ذلك من خلال ظهور صور الإستعمال غير المشروع لتقنية المعلوماتية ، و هي التي أصطلح عليها قانونا وصف " الجرائم المعلوماتية" هذا النوع الحديث من السلوكات الإجرامية الماسة بأمن و سلامة النظم المعلوماتية و بحقوق الغير

تشكل خطراً بالغا و ذلك لتعدد أوصافها الإجرامية ، كجرائم سرقة المعلومات المخزنة أو تخريبها ، أو جرائم التحويل غير المشروع للأموال ، أو جرائم التعدي على الغير عبر الشبكات ، أو جرائم الإستغلال الجنسي للقصر و الأطفال...إلخ من جرائم مستحدثة تتسم بطابعها المعنوي الخالص ، و تخلو من الطابع المادي المميز لأغلب الجرائم التقليدية.

إن ظهور كل هذه المفاهيم الإجرامية الحديثة ، قلب مفاهيم النظرية التقليدية للجريمة فقد أدخلت الجريمة المعلوماتية على هذه الأخيرة صوراً جديدة للجريمة بركنها الشرعي وأساليب و طرق حديثة لم تكن معروفة من قبل مست الجريمة من خلال ركنها المادي فالجرائم المعلوماتية جرائم ناعمة ، لا تستوجب لتحقيقها وسائلاً و جهداً ماديا كبيراً وذلك من خلال إعتماد الجناة على وسائل تكنولوجية و أساليب إجرامية حديثة و متطورة تسمح لهم بنيل مبتغاهم بأقل جهد و بأسرع وقت ممكن دون اللجوء إلى العنف المادي ، فمجرمو المعلوماتية يتميزون بالذكاء و المعرفة الواسعة بمجال المعلوماتية و أدق تفاصيلها وهو ما يسمح له كذلك بالتحكم في أثار و أدلة جرائمه من خلال تدميرها و محوها و هو ما يجعل من أمر أغلب الجرائم المعلوماتية خفية لا يمكن إكتشافها أو تتبع أثارها ، بالنظر إلى الطبيعة الخاصة للأدلة الناتجة عن هذا النوع من الجرائم ، و التي أصبحت تشكل التحدي الأكبر الذي يواجه النصوص الجزائية الإجرائية ، التي تنظم سير جملة الإجراءات الخاصة بعمليات البحث و التحقيق و ملاحقة المجرمين ، في إطار شرعي من أجل تقديمهم أمام العدالة فالجريمة المعلوماتية بوصفها " ذلك السلوك الإجرامي المنصب على إستعمال تقنية المعلوماتية بهدف التعدي على أمن سلامة النظم المعلوماتية و جملة المعلومات المتداولة عبرها من خلال شبكات الإتصال ، أو تلك المخزنة على ذاكرة الحواسيب المتصلة بها، تشكل نقطة تعا رض بين التكنولوجيا الحديثة و جملة النصوص القانونية الإجرائية ، فهذه الأخيرة وضعت لمجابهة الجرائم التقليدية ذات الطابع المادي و التي تخلف ورائها أثار مادية محسوسة و لم تتناول في صلب نصوصها الجرائم المعلوماتية ، هذه الأخيرة التي لا ينفك معدل إنتشارها عن الإرتفاع

و تتزايد يوماً بعد يوم ،و ذلك بفعل عجز السلطات المختصة بتنفيذ القانون عن مجابهتها بسبب عدم ملائمة النصوص الإجرائية لطبيعتها الخاصة ، فالنصوص الخاصة بالبحث

و التحقيق في مجال الجرائم التقليدية لا تصلح للتطبيق في مجال الجرائم المعلوماتية ، فالنصوص المتعلقة بإصدار أوامر القبض و الإحضار و على سبيل المثال لا يمكنها أن تجدي نفعا في مواجهة مجرمي المعلوماتية الذين قد يرتكبون فعلهم الإجرامي من نقطة تقع في أقصى بقاع الأرض ، و ذلك بسبب عائق مبدأ إقليمية النص الجنائي ، و هو ما يتسبب في شل أيدي العدالة عن ممارسة أعمال البحث و التحقيق بشأن الجرائم المعلوماتية ، و قد تتم في بعض الأحيان تحت طابع الضرورة و الإستعجال مباشرة الإجراءات بالرغم من عدم توافقها مما قد يتسبب في إهدار حقوق الغير بفعل تعسف السلطات المختصة في تطبيق إجراءات غير منصوص عليها قانونا تخت غطاء ضرورات التحقيق والحفاظ على الأدلة.

_أهمية الموضوع.

1-التزايد المستمر للنشاط الإجرامي عبر النظم المعلوماتية ، وتزايد درجة خطورة هذا النشاط و إرتفاع مستوى التهديدات التي يشكلها على الأمن العام ، في ظل الإعتماد المطلق على تكنولوجيا المعلومات في المجتمعات المعاصرة ، يقابله عجز سلطات البحث و التحقيق عن رسم نموذج موحد لهذه الجرائم والإستقرار على جملة من الإجراءات الخاصة بمتابعتها نظراً لتطورها الدائم و المستمر ، مما ينتج عنه أحياناً غياب أو جمود إجرائي و عجزه عن تفعيل الإجراءات بسبب عدم ملائمته للجريمة محل البحث و التحقيق.

2-تصنيف موضوع إجراءات البحث و التحقيق بشأن الجرائم المعلوماتية من بين أهم المواضيع المطروحة للنقاش على النطاق الدولي و الوطني ، فهي تشغل بإستمرار حيزاً مهما من جهود الباحثين كذلك الفقه و التشريع لأجل وضع إستراتيجيات قانونية و عملية آنية

ومستقبلية، تضمن عدم فقدان السيطرة على تقنية المعلوماتية ، و تحولها من تقنية تساعد على تطور المجتمعات من خلال تبادل المعارف و المعلومات إلى تقنية هدامة.

_أسباب إختيار الموضوع.

_الرغبة في التعمق في دراسة و تحليل الدور التي تلعبه الشرطة القضائية في مكافحة النشاط الإجرامي الإلكتروني ، و التي أسست لها الجهود و المعاهدات الدولية والإقليمية كإتفاقية بودابست لمكافحة الجرائم المعلوماتية ،و الإتفاقية العربية لمكافحة الجرائم المتصلة بتقنية المعلوماتية و كذلك الجهود التشريعية الداخلية ، كما هو عليه الحال في الجزائر التي أقرت بتشريع خاص يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال و مكافحتها، وذلك بتاريخ 05 أوت 2009،بموجب القانون رقم 04/09 وهي القوانين التي تحاول تنظيم فضاء المعلوماتية بصفة عامة و مكافحة الجانب الإجرامي المتصل بها ، من خلال تحديد قواعد إجرائية خاصة تسمح بمتابعة هذا النوع من الجرائم ومرتكبيها بشكل يضمن شرعية الإجراءات المتخذة ، بهدف ردع هذه الفئة من المجرمين التي دأبت على تبني منطق الإفلات من العقاب ، بحجة قدرتهم على تعطيل الإجراءات من خلال إعتمادهم على وسائل و أساليب إلكترونية إجرامية غاية في التعقيد من الناحية التقنية تجعل من أمر تحصيل الأدلة الإلكترونية في مواجهتهم أمراً بالغا في الصعوبة ، نظراً لتسببها في تعطيل النصوص الإجرائية بسبب طابع اللاملائمة بين الإجراءات و طبيعة الجرائم.

_صعوبات البحث.

_إن الوصول إلى وضع خطة متوازنة و معالجة فعالة و دقيقة لموضوع البحث لم يكن بالسهولة المتوقعة بدءا بالنظر إلى طبيعة الموضوع المزدوجة القانونية و الفنية ، و التي تشكل تحدياً بالغ الصعوبة نظراً لما يميز الموضوع من دقة المصطلحات و المفاهيم العلمية منها والقانونية ، و التي يصعب التحكم فيها و توظيفها بشكل متناسب و متلازم، مع مراعاة

عدم تغليب أي من الطابع القانوني على الفني أو العكس من ذلك ، تحت طائلة فقدان البحث لمعالمه المزدوجة.

_قلة الدراسات السابقة في المجال الإجرائي و إتجاه أغلبها لمعالجة الظاهرة الإجرامية المعلوماتية من ناحية السلوك الإجرامي و العقوبات المقررة لها ، دون التركيز على الجانب الإجرائي، وهو ما جعل الباحث أمام حتمية تجميع المعلومات الخاصة بالموضوع في شكل جزئي و إعادة تجميعها بشكل متناسق وفق خطة عمل.

إن التغيير الحاصل على مستوى النشاط الإجرامي بفعل إتصاله بتقنية المعلوماتية، صاحبه تحول كبير على المستوى القانوني و بالخصوص الإجرائي ، فظهرت آليات وإجراءات قانونية مستحدثة في مجال البحث و التحقيق ، أساسها النص القانوني ، و ميدانها الجرائم المعلوماتية غير أن تطور كلا المجالين لا يسري بنفس الوتيرة ، فالجرائم المعلوماتية تتطور بشكل سريع ومذهل ، فيما تعرف النصوص و الإجراءات القانونية وتيرة بطيئة من حيث مسايرتها لواقع الجريمة المعلوماتية ، مما يخلق دوما فجوة بين الجريمة و الإجراءات الموضوعة لمتابعتها قد تتسبب في تعطيل أو شَل عمل الجهات المختصة بمباشرة هذه الإجراءات.

فالإشكالية العامة المطروحة في هذا البحث: ما هو دور ضباط الشرطة القضائية في مكافحة الجرائم الإكترونية؟

وتتفرع عن هاته الإشكالية عدة تساؤلات نذكر منها:

فيما تتمثل الجهود الدولية في مكافحة الجريمة الإلكترونية؟

مدى كفاية القوانين الداخلية للحد من هذه الجرائم؟

وأخيرًا ماهي الأليات التي وضعتها الدولة والمشرع الجزائري لمنع تفشي هذه الجرائم؟

إن البحث في مجال الإجراءات الخاصة بالبحث و التحقيق في مجال الجرائم المعلوماتية يفرض على الباحث إعتماد منهجية علمية خاصة تتماشى و ترتيب الأفكار المطروحة للنقاش حسب خطة البحث ، و لذلك فقد إعتمدنا مناهج بحثية متعددة بدرجات متفاوتة من حيث الأهمية ، إعتلى صدارتها المنهج الوصفي و كذلك التحليلي ، من خلال ما ورد في البحث من وصف لمفهوم النظم المعلوماتية و الجريمة المعلوماتية ، و مختلف الجهود الفقهية والقانونية المتعلقة بمسألة البحث و التحقيق في الجرائم المعلوماتية ، إضافة إلى التعرض لمختلف الجهات المختصة بمباشرة هذه الإجراءات ووسائلها و أساليب عملها ، وصولا إلى نتاج هذه الأعمال والإجراءات ، و كل ذلك في شكل وصف دقيق مصحوب بالتحليل القانوني لأجل الكشف عن مواطن اللبس التي تعتري موضوعنا المتسم بطابعه الإجرائي الدقيق إضافة لذلك فقد كان للمنهج المقارن نصيب وافر من الإستعمال بوصفه منهجاً مساعداً بالدرجة الأولى ، بحيث إستعنا به خلال كامل أطوار البحث لأجل وضع نتائج من خلال المقارنة بين مختلف الأنظمة و التشريعات التي أولت أهمية قصوى لموضوع إجراءات البحث والتحقيق في مجال الجرائم المعلوماتية، وقد قسمنا هذا البحث إلى فصلين، في الفصل الأول تناولنا الإطار المفاهيمي للجريمة المعلوماتية من خلال مبحثين في المبحث الأول مفهوم الجريمة الإلكترونية والمبحث الثاني صور الجريمة الإلكترونية ، أما الفصل الثاني فقد تناولنا فيه الوحدات والإجراءات الخاصة بالبحث والتحقيق في الجرائم الإلكترونية وبدوره ينقسم إلى مبحثين في المبحث الأول وحدات البحث والتحقيق في الجرائم الإلكترونية مركزيًا، أما المبحث الثاني الإجراءات الخاصة المتبعة في إطار تنفيذ إجراءات البحث والتحقيق المعلوماتي.

الفصل الأول

الإطار المفاهيمي للجريمة المعلوماتية

إعتمد الإنسان منذ القدم في نقل المعلومات بشتى أنواعه، على مختلف الوسائل كالرسومات والكتابة على الأحجار وجلود الحيوان والورق ، وكل ذلك بغرض حفظ هذه المعلومات وتخزينهاوتسهيل أمر إسترجاعها ، لأجل مواجهة وضعية مستعصية تحتاج إلى كم من المعلومات تشكل حلًا لها، وتعتبر الكتب والمخطوطات والوثائق والمستندات، من أهم مصادر نقل المعلومة التي إعتمدها الإنسان في العهد القريب.

غيرأنه تخلى عنها في الوقت الحاضر بفعل ما وفرته له تقنية المعلوماتية في مجال التعامل مع المعلومة ،سواء من حيث نقلها أو تخزينها أو إسترجاعها بل حتى إستعمالها للتنبؤ بما قد يحدث مستقبلًا ،وذلك من خلال إنتشار الحواسيب على أعلى نطاق وظهور تقنيات حديثة لتبادل المعلومات وللإتصال في شكل وشبكة الأنترنت ، كل ذلك خلق جانبًا مشرقًا تمثل في تحسين شبكة المعلومات الدولية (The Web).وتيسير عمل الدول والحكومات والمؤسسات في مجال التعامل فيما بينها ، أو مع المجتمعات التي تحكمها وتتعامل معها.

كما ساهمت هذه التقنية في تطور نمط حياة الإنسان الذي أصبح يعتمد بشكل شبه كامل على الحواسيب وشبكات الإتصال و تبادل المعلومات لأجل قضاء حوائجه دون عناء التنقل من مكان لآخر سعيا وراء المعلومة أو المرفق ، غيرأنه وبالموازات مع ذلك ظهر جانب مظلم لهذه التقنية تمثل في سوء تسخير مزاياها لأجل الإعتداء على مصالح الغير المتمثلة في جملة المعلومات ذات الطابع المتاح أو السري المتداولة عبر النظم المعلوماتية من خلال الحواسيب والشبكات ، وذلك من قبل فئة أصطلح عليها وصف مجرمي المعلوماتية[1].

1 –غازي عبد الرحمن هيان الرشيد:الحماية القانونية من جرائم المعلوماتيةالحاسب و الأنترنت،أطروحة لنيل درجة الدكتوراةفي القانون،الجامعة الإسلامية في لبنان،كلية الحقوق،2004،ص 92.

المبحث الأول:مفهوم الجريمة الإلكترونية.

غالبًا ما تستهدف الجريمة بوصفها فعلا محظورًا بموجب نصوص القانون العقابية حقوق الغير فنجد منها ما يستهدف المال أو الشخص في حد ذاته سواء بكيانه المادي أو المعنوي.

غير أنه وفي ظل المتغيرات الإجتماعية التي تحمل في طياتها مفاهيم الحداثة والتطور التكنولوجي، والتي غيرت من نمط معيشة الإنسان إلى ماهو أفضل ومن كافة النواحي كل ذلك بفضل التقنيات التكنولوجية التي توفرها، ظهر نوع جديد من الجرائم يستهدف المال والنفس من خلال الفضاء الرقمي الإلكتروني كنتيجة لإنتشار تقنية المعلوماتية التي أضحت تشكل عصب الحياة الحديثة ونقطة قوة في مسار التقدم الحضاري لأي دولة كانت ، فبدونها لا تستطيع أي دولة إحراز التقدم المرجو واللّحاق بركب المجتمع الدولي، فقد أصبح تبادل المعلومات ومعالجتها بأسرع وقت وأفضل طريقة الشغل الشاغل لإختصاصي هذا المجال بالرغم من درجة التطور والتقدم التي آلت إليه هذه التكنولوجيا .

غير أن هذا الإهتمام كان محل فئة أخرى وهي فئة المجرمين الذين أصروا على إقتحام هذا المجال من خلال الإعتداء على الأنظمة المعلوماتية بأهداف متباينة ، منها ما يهدف إلى إثبات الذات والتحدي ومنها ما يهدف إلى تحقيق ثروة على حساب الغير، ومنها ما يهدف إلى أبعد من ذلك من خلال المساس بأمن وسلامة الفرد والمجتمع ، وهي الظاهرة التي أصطلح على تسميتها الجريمة المعلوماتية هذه الجريمة التي أصبحت تشغل فكر القانونيين[1].

1 –محمّد عبيد الكعبي ،الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت،دار النهضة العربية،القاهرة، بدون سنة نشر،ص 32.

المطلب الأول:مفهوم النظم المعلوماتية.Le Système Informatique

تعتبر المعلومات الهدف الرئيسي للجريمة المعلوماتية بإعتبارها محلها الرئيسي ، فلا يتاح للمجرمين المعلوماتيين الوصول إليها إلا من خلال منفذ وحيد وهو النظام المعلوماتي الذي يشكل الوعاء المنطقي لها ، والذي أنشئ خصيصًا بغرض تداولها وفق نظم معالجة آلية تتحكم فيه أجهزةالحاسوب منفردة أو مجتمعة بواسطة الربط بشبكات الإتصال ، تعمل على تداول ومعالجة المعلومات بأفضل وأسرع طريقة ممكنة بهدف ترقية الأداء المؤسساتي لأجهزة الدولة ،ومصالحها الحيوية كالدفاع والتعليم والإعلام...إلخ ، ضف إلى ذلك تيسير المعاملات بين الأفراد داخل المجتمع ، من خلال تقديم خدمات ذات طابع إلكتروني كالبيع و الشراء والدفع الإلكتروني ، أو خدمات البريد الإلكتروني وما يجاورها من خدمات تستلزم الإدلاء بمعلومات شخصية ذات طابع سري ، مما يجعل من هذه النظم المعلوماتية هدفا يستقطب هواة و محترفي الإجرام المعلوماتي على حد سواء.

الفرع الأول:تعريف المعلوماتية.

أسهمت التطورات التكنولوجية والتقنية المتسارعة في نهاية القرن العشرين وبداية القرن الواحد والعشرين ، في سرعة تحول المجتمعات من عصر الصناعة إلى عصر المعلومات وتحولت أساليب وأنشطة العمل تدريجيًا إلى النمط الإلكتروني بفضل التمازج بين تقنيتي الإتصالات والمعلومات مما أسفر عن إنطلاقة قوية في عالم تقنية المعلومات ، كان نتاجها ظهور تطبيقات حضرية ذات طابع تقني كالحكومة الإلكترونية ،التجارة الإلكترونية ، وذلك بإعتبارها الجانب الإيجابي للتطور التكنولوجي المعاصر ، أما الجانب السلبي المرافق لها فقد تجلى في ظهور الجرائم المعلوماتية كنتيجة حتمية لإساءة إستخدام هذه التقنيات[1].

التعريف اللغوي: أشتق مصطلح " المعلومات " لغة من كلمة" علم "و دلالتها هي المعرفة التي يمكن نقلها وإكتسابها، وأصلها في اللغة الفرنسية والإنجليزية والألمانية والروسية هو كلمة (Informolio) اللاتينية بحسب الأصل والدالة على شيء للإبلاغ والتوضيح .

[1] _عبد الله بن سعود محمد السراني، فعالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، رسالة مقدمة لأجل نيل شهادة الدكتوراه قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2009 ،ص21.

التعريف الإصطلاحي:لقد أشار عديد الباحثين بإختلاف تخصصاتهم إلى تعريف إصطلاحي للمعلومات يمكن جمعها في مفهوم يقصد به " الحقائق أو الرسائل أو الإشارات أو المفاهيم التي تعرض بطريقة صالحة للإبلاغ أو التوصيل أو التفسير بواسطة الإنسان أو أدوات أو معدات آلية "،أو بأنها " الصورة المحولة للبيانات "وقد تم تنظيمها ومعالجتها بطريقة تسمح بإستخلاص النتائج[1].

التعريف القانوني : إهتم جزء قليل من التشريعات بوضع تعريف للمعلومات وفي سبيل ذلك نذكرماجاء به المشرع الفرنسي وفق ما يقرره القانون رقم 625/82 الصادر في 1982/7/26 الخاص بتنظيم الإتصالات السمعية و البصرية بأنها " رنين صور الوثائق والبيانات والرسائل أيًا كانت طبيعتها"[2]

ليلحق به المشرع الأمريكي بموجب القانون الصادر سنة 1999 المنظم للمعاملات التجارية الإلكترونية بالقول في الفقرة 10 من المادة 02 بأن المعلومات هي " كل البيانات والكلمات والصور والأصوات والوسائل وبرامج الكمبيوتر والبرامج المضغوطة سواء على أقراص مرنة أو قواعد بيانات أو ما شابه ذلك"، وبذلك فقد أكسب المشرع الأمريكي الطابع التكنولوجي لمدلول كلمة " معلومة "وهو ما أخذ به كلا من التشريعين البحريني و الإماراتي، اللذان نصا على تعريف مشترك من حيث المفهوم بموجب القانونين الصادرين تبعا سنة 2002 المتعلقين بتنظيم المعاملات الإلكترونية بالقول بأن المعلومات هي " معلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب آلي أو غيرها من قواعد البيانات"[3].

وما يمكن الإشارة إليه هو تعريف المشرع الجزائري الوارد في نص المادة 02 الفقرة "ج "من القانون رقم09/04[4] المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم

---

[1] _ محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2004، ص35،36.

[2] _نقلاً عن محمد علي العريان، نفس المرجع،ص39.

[3] _عبد العال الدريبي، الجرائم الإلكترونية،دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012، ص 44.

[4] _ القانون رقم 09/ 04 المؤرخ في 16 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47.

المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، بالقول بأن المعطيات المعلوماتية هي " أي عملية عرض للوقائع والمعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج التي تجعل من المنظومة المعلوماتية تؤدي وظيفتها[1]".

يمكن القول بأن المعلوماتية ظاهرة إجتماعية ذات بعد تاريخي نشأت وتطورت مع تطور الحضارة يرجع الفضل في إقتراح مصطلح المعلوماتية إلى العالم الفرنسي " دريفيس" الذي إستخدمه أول مرة عام 1962 لتمييز المعالجة الآلية للمعلومات عن غيرها من أنظمة معالجة المعلومات[2].

وقد كان للأكاديمية الفرنسية نصيب في وضع تعريف للمعلوماتية حسب ما ورد في مقرر جلستها المنعقدة في 02 أفريل 1967 بالقول بأنها " العلم التفاعلي العقلاني بواسطة آلات أوتوماتيكية مع المعلومات بإعتبارها دعامة للمعارف الإنسانية وعماداً للإتصالات في ميادين تقنية الإقتصاد والإجتماع"[3].

ولعل أن التعريف الأكثر تداولا لمدلول المعلوماتية ،ذلك الذي عرفها بأنها "علم يعنى بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها ،وإختزانها وإسترجاعها وتفسيرها وبثها وتحويلها وإستخدامها ، كما يتضمن البحث عن تمثيل المعلومات في النظم الطبيعية والصناعية والإدارية ، وإستخدام تقنيات الترميز في نقل الرسالة والتعبير عنها إضافة إلى الإهتمام بأساليب معالجة المعلومات كالنظم المعلوماتية ونظم البرمجة ويمكن تلخيص ذلك بالقول بأن المعلوماتية هي " المعالجة الآلية للمعلومات"[4].

الفرع الثاني:قوام النظم المعلوماتية.

بإزدياد حجم المعلومات وكثافتها إزدادت الحاجة إلى تبادلها ونقلها من مكان إلى آخر، وهو ما أدى إلى إنتشار تقنية المعلوماتية، التي تهدف إلى معالجة المعلومات بصفة آلية

---

[1] –القانون 04/09،الصادر بتاريخ 16 أوت 2009،الجريدة الرسمية رقم47،ص05.

[2] _ تركي بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فعاليته، رسالة مقدمة لأجل نيل شهادة الدكتوراه، قسم العلوم الشرطية ، جامعة نايف للعلوم الأمنية ، الرياض، السعودية،2009، ص14.

[3] _ محمد علي العريان، المرجع سابق، ص38 .

[4] _ تركي بن عبد الرحمان المويشير، المرجع السابق، ص14

بفضل التقنيات التي تتوفر عليها والتي هي نتاج تقاطع علوم الحاسوب وعلم الإتصالات الأمر الذي أدّى إلى إنتشارها بسرعة مذهلة عبر كافة أقطار العالم[1].

البند الأول:تعريف النظم المعلوماتية:

تكفلت نصوص وأحكام الإتفاقيات الدولية والإقليمية إضافة إلى نصوص التشريعات الوطنية بتعريف النظم المعلوماتية ، فعرفت إتفاقية بودابست لمكافحة الجرائم المعلوماتية في مادتها الأولى النظم المعلوماتية بأنها " كل آلة بمفردها أو مع غيرها من الآلات المتصلة او المرتبطة ، والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للبيانات المعلوماتية وتعني هذه الأخيرة كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل وتكون مهيأة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة يجعل الحاسوب يؤدي المهمة"[2].

كما نجد تعريفا آخر جاءت به المذكرة التفسيرية لإتفاقية بودابست الصادرة قبلا وبتاريخ2001/11/08 بمناسبة إنعقاد الدورة رقم 109 لإجتماع لجنة وزراء المجلس الأوربي بالقول بأنها " المقصود بالنظام المعلوماتي هو جهاز يتكون من مكونات مادية و مكونات منطقية ، بغرض المعالجة الآلية للبيانات الرقمية يشمل هذا الجهاز على وسائل الإدخال وإخراج وتخزين البيانات وقد يكون هذا الجهاز منفردا أو متصلا بمجموعة من الأجهزة المتماثلة عن طريق شبكة وتعني كلمة آلية دون تدخل بشري[3].

البند الثاني:المكونات المادية للنظم المعلوماتية.

تعد الحواسيب (Ordinateurs ou computers)من أهم المكونات الرئيسية للنظام المعلوماتي.

أولاً: التعريف الإصطلاحي للحاسوب: " عبارة عن جهاز إلكتروني يتكون من عنصرين مادي ومعنوي ،يشمل الأول كل المكونات المادية في حين يشمل الثاني البرامج حيث يتم

---

[1]_ حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض،السعودية، 2000،ص18.

[2]_المادة الثانية من إتفاقية بودابست التي إنبثقت عن إجتماع المجلس الأوروبي ودخلت حيز النفاذ 1 جويلية 2004.

[3]_ هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها، الطبعة الأولى، دار النهضة العربية ،مصر 2008 ، ص18، 19.

تشغيله على ضوء برنامج يتم تخزينه على ذاكرته ومن ثم يقوم بإستقبال البيانات ومعالجتها على النحو المطلوب منه بغية الوصول إلى نتائج محددة"[1].

ثانياً:التعريف القانوني للحاسوب: للحاسوب نصيب من التعاريف القانونية فقد عرفه المشرع السعودي في نص المادة الأولى (01) من نظام مكافحة الجرائم المعلوماتية السعودي بأنه " أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي ، يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو إستقبالها أو تصفحها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له" .

ثالثا:المكونات المادية للحاسوب(hard ware): يقصد بالمكونات المادية للحاسوب الهيكل المادي المكون لنظام الحاسوب ويتكون أساسا من الوحدات الرئيسية التالية:

1-وحدات الإدخال : تستعمل هذه الوحدات لإدخال المعلومات أو الأوامر أو المعطيات أو البرامج المراد معالجتها إلى ذاكرة الحاسوب وقد تكون في شكل وسائل إدخال مباشرة(On Line)و تمثل لوحة المفاتيح (keyborad) إحدى هذه الوسائل،كما قد تكون في شكل وسيلة إدخال غير مباشرة (Off Line) ، وكغرفة الأقراص المدمجة، الماسح الضوئي[2].

2_وحدة المعالجة المركزية (Central Processing Unit C.P.U) وتعتبر مركز الأنشطة في الحاسوب وتحتوي على دوائر كهربائية تترجم و تنفذ تعليمات برامج التشغيل[3].

3-وحدة الذاكرة:(Memory Unit M .U) هي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز أو النتائج الآتية من وحدة المعالجة المركزية[4].

---

[1]_ محمد حماد الهيتي، التكنولوجيا الحديثة و القانون الجنائي، الطبعة الثانية، دار الثقافة للنشر و التوزيع،عمان، الأردن، 2012 ، ص 144.

[3]_نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2010، ص24.

[3]_ إبراهيم بن سطم بن خلف العنزي ، التوقيع الإلكتروني و حمايته الجنائية، رسالة مقدمة لأجل نيل شهادة الدكتوراه،قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية،2009،ص31 .

[4]_المرجع نفسه ، ص26.

4-وحدات الإخراج : وهي الأجزاء والوحدات التي يتم من خلالها إخراج البيانات المعالجة من وحدة المعالجة المركزية إلى الخارج ومن أهم وحدات الإخراج الشاشة والطابعة[1].

رابعاً :المكونات المنطقية للحاسوب(Software):تتمثل هذه المكونات المنطقية في التطبيقات العملية التي تجري داخل الكيان المادي للحاسوب وتتمثل في جملة البيانات والمعلومات ، إضافة إلى برمجيات الحاسوب ،ولقدعرفها العاملون في مجال الحاسوب بأنها "الأوامر المرتبطة منطقيا والموجهة إلى الحاسوب بعد توجيهها إلى اللغة الوحيدة التي يفهمها وهي لغة الأرقام الثنائية"[2].

البند الثالث:شبكات الإتصال كعنصر للنظم المعلوماتية:

يتكون النظام المعلوماتي من جملة من المكونات منها المتعلقة بالحاسوب من ماديات وبرمجيات ومنهاما يتعلق بالشبكات أي شبكات الإتصال.

أولاً:مفهوم شبكة الإتصال.

لشبكة الإتصال في مجال النظم المعلوماتية تعريف خاص يقصد به " أداة ربط بين حاسوبين أو أكثر وهذه الرابطة قد تكون أرضية بالأسلاك أو الكابلات ، كما يمكن أن تكون لا سلكية ، أو بالأشعة تحت الحمراء ، أو بالقمار الصناعية ، والشبكة يمكن أن تكون مقتصرة جغرافيًا على منطقة صغيرة فتسمى شبكة محلية (Réseau Local) كما يمكن أن تغطي منطقة كبيرة فتكون متسعة النطاق (Réseau Etendu) ،ويمكن أن تكون متصلة ببعضها البعض (Interconnecté)وتعدشبكة الأنترنت(Internet) شبكة عالمية لأنها تتكون من العديد من الشبكات المتصلة ببعضها البعض و التي تستخدم جميعا نفس البروتوكولات ، والنظم المعلوماتية يمكن أن تتصل بالشبكة بوصفها نقاطا نهائيةأو نقاط خروج ، أو كوسيلة لتسهيل نقل المعلومات[3].

ثانيًا : تعريف شبكة الأنترنت :

يعتبر الأنترنت أكبر شبكة موسعة تغطي جميع أنحاء العالم تتصل بين حواسيب شخصية

---

[1] _عبد العال الدربي، المرجع السابق، ص18.

[2] _عبد العال الدربي، المرجع نفسه، ص27.

[3] _ هلالي عبد اللاه أحمد،المرجع السابق، ص23 .

وشبكات محلية و أخرى عامة ، يمكن لأي شخص حول العالم أن يصبح عضوًا في هذه الشبكة من منزله أو مكتبه أو من أي مكان آخر بشكل يمكنه من الوصول إلى قدر هائل من المعلومات، و يكفيه لذلك حاسوب مكتبي أو محمول أوهاتف نقال و تقنية المودم[1].فشبكة الأنترنت عبارة عن وسيط ناقل للمعلومات بين أجهزة الحاسوب المتصلة به بواسطة أنظمة التحكم في البيانات وبروتوكولات (TCP /IP)وعناوين خاصة حيث يتصل مستخدموها عن طريق الخط الهاتفي المتصل بمحول الإشارات المودم(Modem) الذي يقوم بتحويل الإشارات الرقمية ونقل الرسالة بين المرسل ، والمرسل إليه مرورًا بالخادم (Server)[2].

الفرع الثالث: الأمن المعلوماتي.

إن تنامي إستعمالات تقنية المعلوماتية وظهور مفاهيم جديدة ، كالحكومات والإدارات والعقود الإلكترونية ، وإنتشار مواقع التواصل الإجتماعي على شبكة الأنترنت ، وإعتماد كل منا على هذه الوسائل في حياته اليومية ، يحمل نوعا من الخطر يتمثل في صور الإعتداء التي يمكن أن تمس بالمعطيات الرقمية لكل منا ، وما يمكن أن تسببه من ضرر في صورة الأثار السلبية للجريمة المعلوماتية ، وهو ما أدى إلى ظهور وبشكل موازى لتقنية المعلوماتية ما يعرف بالأمن المعلوماتي .

البند الأول:تعريف الأمن المعلوماتي:

يعرف الأمن المعلوماتي بأنه " فرض ضوابط على سبل وأساليب الوصول للمعلومات بهدف إضفاءالشرعية على حدود وصلاحية إستخدام المعلومات "، كما عرف أيضا بأنه " إتخاذ الإحتياطات والتنظيمات التي تهدف إلى المحافظة على المعلومات في الحاسوب ، بمأمن من الأعطال والحوادث أو الجرائم المتعمدة"[3] وتهدف أغلب التعاريف إلى إبراز أن الأمن المعلوماتي ينطوي على:

---

[1] _نهلا عبد القادر المومني، المرجع السابق،ص35.

[2] _علي بن عبد الله غسيري ، الأثار الأمنية لأستخدام الشباب للأنترنت، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض ، السعودية، 2004،ص 13،14.

[3] _عبدالله بن سعود محمد السراني، المرجع السابق،ص23.

•المحافظة على المكونات المادية للحاسوب.

•المحافظة على المعلومات وسلامتها وسريتها وملكيتها والإستفادة منها.

•المحافظة على المعلومات من تداخل إستخدامها أو تخريبها ، أو إستخدام معلومات مضللة أو تحريفها و إستبدالها ، أو سوء تفسيرها و إلغائها أو الفشل في إستخدامها أو سرقتها.

•معالجة جميع الخروقات المتعلقة بالسلامة و السرية ، والملكية لصاحب المعلومة.

و يمكن إيجاز كل ذلك في إطار تعريف موجز واحد مضمونه " الأمن المعلوماتي هو ذلك العلم الذي يبحث في إستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها وأنشطة الإعتداء عليها"[1].

ويتمتع مجال الأمن المعلوماتي بالأهمية البالغة نظرًا لإزدياد أهمية وقيمة المعلومات ودورها الحساس، بالنسبة للدول خصوصا تلك الأمنية و العسكرية و الإقتصادية ذات الطابع الإستراتيجي لذلك إرتبط عنصر السرية بالمعلومات على ضوء ما قد يترتب جراء فقدانها من خسائر[2].

ضف إلى ذلك أن تقنية المعلوماتية قد خلفت و على صعيد الحياة الشخصية سلسلة من التحديات الجديدة ، و التهديدات الخاصة فهي تزيد من كمية البيانات المجمعة المعالجة بإعتبارها مصدر غني بالمعلومات المتعلقة بالحياة الشخصيةللأفراد ، فتوفر عنهم معلومات متعلقة بعاداتهم هوياتهم و سلوكياتهم ،وآرائهم و إتجاهاتهم ، و تتدفق هذه المعلومات عبر الحدود دون أي إعتبار للحدود الجغرافية و السياسية ، و قد تعرض لجهات داخليةو خارجية و ربما لجهات غير معروفة و هذا ما ينجر عنه إساءة إستخدامها في دول لا تتوفر فيها مستويات الحماية القانونية للمعلومات بشكل كاف[3].

---

[1] _عمر بن محمد العتبي ، الأمن المعلوماتي و مدى توافقه مع المعايير المحلية و الدولية ، رسالة مقدمة لأجل نيل شهادةالدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية،2010، ص15 .

[2] _عبدالله بن سعود السراني، المرجع السابق، ص24.

[3] _ بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009،ص 21.

البند الثاني:غايات الأمن المعلوماتي.

تتمثل الغايات الأساسية لإعتماد إستراتيجيات الأمن المعلوماتي في أي منظومة معلوماتية ، في الحفاظ على المعلومة من حيث:

أولا : الإ تاحة :أي إتاحة إستخدامها بصورها الأصلية أينما كانت و كيفما تطلب الأمر أي حفظ المعلومات من مظاهر التخريب أو الخلط مع معلومة أخرى على نحو يلوثها.

ثانيا : التكامل :يقصد بالتكامل هنا تكامل المحتوى أي أن المعلومات المعالجة آليًا كلٌ لا يتجزأ، و الأمن المعلوماتي هو ما يضمن سلامة المعلومة بكل أجزائها منذ بدء المعالجة و إلى نهايتها ، من خلال ضمان عدم التلاعب بالمعلومات سواء بشكل جزئي أو كلي[1].

ثالثا : السرية : أي ضمان حفظ المعلومات المخزنةأو المنقولة عبر الشبكة و عدم الإطلاع عليها أو إستخدامها إلا بموجب إذن ، أي ضمان الإطلاع عليها لفائدة المصرح لهم ، فضلا عن تحديد حدود صلاحية الإستخدام كلية كانت أو جزئية ، سواء ما تعلق منها بالحق في القراءة فقط أوبالحق في الحذف و التعديل[2].

المطلب الثاني:الجريمة الإلكترونية.

إن التطور التكنولوجي و ما صحبه من ثورة في مجال المعلوماتية الناتجة عن الاستخدام المتزايد لأجهزة الحاسوب بمختلف أشكاله وأنواعه، المكتبية، المحمولة، الهواتف الذكية والمتصلة على شبه الدوام بشبكة الأنترنت، أثّر وبشكل كبير على مظاهر حياة الأفراد والمجتمعات بشكل إيجابي، من خلال مختلف الصيغ الإلكترونية المتاحة.

الفرع الأول:التطور التاريخي للجريمة الإلكترونية.

إن التعرض لمفهوم الجريمة المعلوماتية يستلزم منا بالضرورة، التعرض لأهم المحطات التاريخية التي كانت ولازالت تعتبر نقاط تحول في مسار السلوك الإجرامي التقليدي،إلى ذلك السلوك الإجرامي المعاصر والمعلوماتي.و إذا أردنا الحديث عن الجريمة المعلوماتية

[1] _ سلمى مانع، دور الأمن المعلوماتي في مكافحة الجرائم المعلوماتية، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة. المعلوماتية بين الوقاية و المكافحة 16 و 17 نوفمبر 2015 كلية الحقوق، جامعة بسكرة، الجزائر، ص10.

[2] _عبدالله بن سعود محمد السراني، المرجع،ص25.

باعتبارها ذلك النشاط الناشئ عن الإستغلال غير المشروع للحواسيب والشبكات المتصلة بها فيجب علينا الرجوع إلى المحطات التاريخية التالية:

- سنة 1981 أين تم تقديم(إيان مريفي-Ian Murphy)أمام الجهات القضائية الأمريكية بتهمة الولوج غير المشروع للنظام المعلوماتي لشركة (AT&T) و تعمده تغير النظام الفوترة المعمول به .
- سنة 1986 تاريخ ظهور أول فيروس معلوماتي تحت إسم (Brain) والذي يهاجم حواسيب علامة IBM وكان ذلك بالباكستان، وهي نفس السنة التي شهدت إستصدار الكونغرس الأمريكي ، قانون يجرم مسائل الغش المعلوماتي.
- سنة 1988 إطلاق روبير موريس (ROBERT MORIS) لأول فيروس على شبكة الأنترنت. عرف باسم "دودة موريس "والتي تسببت في إتلاف 6000 حاسوب كان متصلا بالشبكة وقد عوقب إثر ذلك بالحبس لمدة 03 ثلاث أشهر وبغرامة 10.000 دولار أمريكي.
- سنة 1990 إنتشار أكثر من 1000 نوع من الفيروسات على شبكة الأنترنت.
- سنة 1994 قيام عالم الرياضيات الروسي (فلاديمير ليفين – VLADIMIRE LEVIN)بالإستيلاء إلكترونيا على مصرف(City bank)من خلال الدخول إلى النظام المعلوماتي المصرفي العالمي (SWIFT)وهو ما حقق له ثروة قدرت ب 10 ملايين دولار أمريكي، وتسبب في خسارة هذا البنك لأكبر 10 زبائن له، وقد ألقي عليه القبض بلندن سنة 1995 وتم تسليمه للولايات المتحدةالأمريكية، التي أصدرت في حقه بالسجن ل(03) ثلاث سنوات[1].لتتوالى في حقبة التسعينات الجرائم المعلوماتية سواء تلك الناتجة عن نشر الفيروسات أو تلك المتعلقة بالتعدي على الأموال ولعل أن أهم هذه الحقبة هو حكم الإعدام الذي صدر في حق مواطنين صنيين أتهما باختراق نظاممالمعلومات الخاص بأحد البنوك الصينية وتحويل ما قيمته 87000 دولار أمريكي

[1] - _Jean- Philippe Humbert- le monde de la cyberdélinquance et l'image sociale du pirate informatique - thèse de doctorat- sciences de l'information est de la télécommunication université Paul Verlaine – Metz – France – 2007- P 95-97

لحسابهماالشخصي. لتأتي بعد ذلك حقبة سنوات الألفين (2000) والتي تميزت بظهور أنواع أخرى وحديثة من مظاهر الإجرام المعلوماتي، تتسم بالخطورة على أمن الفرد والجماعة، من خلال إستهدافها لشتى المجالات،سواء منها الحيوية للدولة أو الأفراد فأصبحت الجريمة المعلوماتية سلوكًا نتعايش معه يوميا في ظل التهديدات التي تشكلها على مصالحنا الخاصة والعامة ، ونظرًا لإعتمادنا المتزايد يوما بعد يوم على تقنية المعلوماتية[1].

الفرع الثاني:تعريف الجريمة المعلوماتية.

إستقطب مفهوم الجريمة المعلوماتية إهتمام الفقهاء والقانونيين والمختصين في مجال المعلوماتية، من أجل وضع تعريف شامل للجريمة المعلوماتية، فحاول كل منهم حسب اختصاصه وضع تعريف ملائم فمنهم من عرفها تعريفا ضيقا وقال بأنها " الجرائم المرتبطة بالحاسوب والتي تشكل انتهاكا للقانون الجنائي "ومنهم من قال بأنها " تلك الجريمة التي يستخدم فيها الحاسوب "وهو تعريف واسع جدًا[2].

و إذا ما حاولنا وضع تعريف متكامل لهذا النوع من السلوك الإجرامي، فإنه يجب علينا الإطلاع بدءًا على مدلولها باللغة الفرنسة (La Cybercriminalité) فأصل الكلمة (Cyber) يوناني (Kubernan) أي التحكم والتسيير، ويقصد به في مجال المعلوماتية، المعالجة الآلية للمعطيات ، وقد شاع إستعمال هذا المصطلح وإتصل بكافة صور الإجرام كالغش المعلوماتي (Cyber fraude)،الإرهاب المعلوماتي (Cyber Terrorisme) .

البند الأول:التعريف القانوني:

أما من الناحية القانونية فلا يوجد مصطلح قانوني موحد للدلالة على الجرائم

[1] _Jean- Philippe Humbert- le monde de la cyberdélinquance et l'image sociale du pirate informatique - thèse de doctorat- sciences de l'information est de la télécommunication université Paul Verlaine – Metz – France – 2007- P 95-97

[2] _عمر بن محمد العتبي، المرجع السابق،ص21.

الناشئة عن سوء إستغلال النظم المعلوماتية أو إساءة إستخدامها فهناك من يطلق عليها وصف جريمة الغش المعلوماتي، وهناك من يطلق عليها وصف جريمة الإختلاس المعلوماتي وهناك من يصفها بجرائم الإحتيال المعلوماتي، غير أن المصطلح الأكثر شيوعا هو مصطلح الجريمة المعلوماتية[1].

وقد ورد تعريف الجريمة المعلوماتية بحسب ما قدمه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي إنعقد" بفينا "سنة 2000 بأنها " كل جريمة يمكن إرتكابها بواسطة نظام حاسوبي أوشبكة حاسوبية أو داخل نظام الحاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية، ومن التعاريف الذي تم التوسع فيها تعريف الخبير الأمريكي (باركر – Parker) الذي حاول إعطائها مفهوماً واسعاً يحيط بكل أشكال التعسف في مجال إستخدام النظم المعلوماتية ، فهي من وجهة نظره " كل فعل إجرامي متعمد ،أي كانت صلته بالمعلوماتية ينشأ خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل"[2].

البند الثاني:التعريف الفقهي:

في إطار مساهمة الفقه في تعريف الجريمة المعلوماتية إنقسم هذا الأخير إلى إتجاهين أساسيين أحدهما إعتمد التضيق والآخر التوسع في إطار وضع تعريف الجريمة المعلوماتية.

-أولا : الاتجاه الفقهي الذي يعرفها بشكل ضيق : تزعم هذا الاتجاه الفقيه (ميروي) من خلال وضعه تعريفا مضمونة " أن الجريمة المعلوماتية هي ذلك الفعل غير المشروع الذي يتورط في إرتكابه الحاسب[3].

كما عرفها روزبلات بأنها" نشاط غير مشروع موجة لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه "أما (سولريز) فعرفها

---

[1] _تركي بن عبد الرحمن المويشير، المرجع السابق،ص15.

[2] _تركي بن عبد الرحمن المويشير، المرجع نفسه ،ص16.

[3] _ محمد أمين الشوابكة، جرائم الحاسوب والأنترنت(الجريمة المعلوماتية)، دارالثقافة للنشر والتوزيع، عمان الأردن،2009،ص8.

بأنها "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات"[1].

–ثانيا :الإتجاه الفقهي الموسع لمفهوم الجريمة المعلوماتية : حاول هذا الإتجاه إعطاء تعريف موسع للجريمة المعلوماتية لهدف تفادي النقص الظاهر على التعاريف السابقة، فعرفت بأنها " كل فعل أو امتناع عمدي ينشأ عن الإستخدام غير المشروع للتقنية المعلوماتية بهدف الإعتداء على الأموال المادية أو المعنوية "،كما عرفت بأنها " كل سلوك سلبي كان أم إيجابي يتم بموجبه الإعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت"[2].

وقد عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02 الفقرة (01)من القانون رقم 09-04الصادر في05أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بالقول بأن"الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي" : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[3]

الفرع الثالث:الطبيعة القانونية للجريمة المعلوماتية.

بالنظر إلى التعاريف التي وردت لمفهوم الجريمة المعلوماتية، وجملة الخصائص والسمات التي تميزها فإنه وبدون شك ستتبادر إلى أذهاننا فكرة التساؤل حول الطبيعة القانونية للجريمة المعلوماتية، فهي في ظاهرها جريمة غير مادية، أي بدون أثر مادي ملموس فمجالها البيئة الإلكترونية مما يجعلها مختلفة كليا عن الجرائم الأخرى التي يرى التشريع الجنائي أنها تهدد مصلحة الغير العامة والخاصة ، وفي هذا الصدد وبالنظر إلى تقاطع مفهوم الجريمة التقليدية والمعلوماتية بالمصالح المحمية قانونا فقد انقسم الفقه حول تكييف طبيعة هذه الجريمة بين الوصف الخاص والعام لها .

---

[1] _ محمد سيد سلطان، قضايا قانونية في أمن المعلومات و حماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الكويت، 2012 ،ص62.

[2] _تركي بن عبدالرحمن المويشير، المرجع السابق،ص17.

[3] –القانون 04/09،القانون السالف الذكر،ص05.

البند الأول :الإتجاه الفقهي الذي يرى بأن الجريمة المعلوماتية جريمة من نوع خاص.

يستند هذا الاتجاه على فكرة، أن مجال الحماية القانونية هو المعلومة في حد ذاتها باعتبارها السند الأساسي للنظم المعلوماتية، وإنطلاقا من أن وصف" القيمة "يضفى على الأشياء المادية القابلة للإستحواذ دون تلك المعنوية التي لا يمكن الإستحواذ عليها، فإن مجال الحماية المقرر لها هو في ضوء حقوق الملكية الفكرية فقط، و لعل أن فكر هذا الإتجاه الفقهي يتعارض و المفاهيم الحديثة للقانون الجنائي الذي يقر بأحقية توفير الحماية القانونية للمعلومة بإعتبارها تكتسب صفة المال و هو ما تبناه أنصار المذهب الثاني[1].

البند الثاني :الإتجاه الفقهي الذي يرى بأن الجريمة المعلوماتية جريمة مستحدثة.

يتخذ هذا الاتجاه موقفا صريحا مفاده أن الجريمة المعلوماتية و بإعتبارها جريمة تستهدف المعلومات، و بإعتبار هذه الأخيرة مجموعة مستحدثة من القيم بإعتبارها قابلة للإستحواد عليها بعيدا عن دعامتها المادية، كما أنها قابلة للتقويم بحسب سعر السوق متى كانت غير محظورة تجاريا، و أنها نتاج مؤلفها وتجمع بينها علاقة ، و هو الرأي الذي جاء به الأستاذ (فيفانتي – vivanti) بقوله أن " فكرة الشيء أو القيمة لها صورة معنوية و أن نوع الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع إقتصادي وأن تكون جديرة بحماية القانون ،ومتى كانت المعلومات و البرامج المعالجة آليا ذات قيمة اقتصادية فإنه يجب معاملتها معاملة المال"[2].

إذًا فالبيانات والمعلومات الموجودة داخل ذاكرة الحاسوب تعتبر من الأموال ولها قيمة مادية، فهي قابلة للنقل من حاسوب لآخر أو لقرص مضغوط أو البريد إلكتروني فهي بالتالي مال منقول وإذا ما نقلت من دون رضا صاحبها فيطبق عليها قانون العقوبات.

ولقد استقر الرأي الراجح من الفقه على أن البرامج والمعلومات تخضع لمبدأ الحماية الجنائية والبرامج والمعلومات ملك لصاحبها، إن سرقة دعامتها من الغير هي سرقة للمعلومات في حد ذاتها لأنه لا يمكن الفصل بين الدعامة والمعلومة محل السرقة[3].

---

[1] _محمد علي العريان، المرجع السابق، ص49.

[2] _محمد علي العريان،المرجع السابق، ص51.

[3] _خالد عياد الحلبي، المرجع السابق، ص57.

المطلب الثالث:المجرم والضحية في الجرائم الإلكترونية.

يطلق وصف المجرم عادة على كل شخص يبادر بمحض إردته إلى الإعتداء على جملة القواعد العامة ذات الطابع العقابي، المنظمة لسلوكات الأفراد والتي يكون الهدف منها حماية المصالح العامة والخاصة على حد سواء، ولطالما شرعت قوانين ونظم لأجل مجابهة هذه السلوكات الإجرامية ومتابعة مرتكبيها.

الفرع الأول:شخصية المجرم المعلوماتي.

يعد الأستاذ باركر واحدًا من أهم الباحثين الذين إهتموا بموضوع الجريمة المعلوماتية عمومًا، وبالمجرم المعلوماتي خصوصًا، من خلال البحوث التجريبية التي قام بها سنة 1976 بالولايات المتحدة الأمريكية، وقد وضع مجموعة من السّمات التي تميز المجرم المعلوماتي، والتي يساعد التعرف عليها مواجهة هذا النمط الحديث من المجرمين ،ويرى الأستاذ باركر أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة إلا أنه في النهاية لا يخرج عن كونه مرتكبًا لفعل إجرامي يتطلب توقيع العقاب عليه[1] .

البند الأول: المجرم المعلوماتي ذو طبع إجتماعي.

يتّسم المجرم المعلوماتي في كونه في العادة كائنا ذو طبع إجتماعي يتميز بقدرته على التكيف في بيئته الإجتماعية، بل أن بعضهم يتمتع بثقة كبيرة في مجال عمله، فالمجرم المعلوماتي لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، فهو يتوافق ويتصالح معه وتزداد خطورته الإجرامية كلما زاد تكيفه الإجتماعي مع توافر الميول الإجرامي لديه، فشعوره بأنه محل ثقة و أنه خارج إطار الشبهات يدفعه إلى التمادي في ارتكاب جرائمه و التي لا تكتشف عادة[2].

و من توابع خصائصه الإجتماعية أنه شخص يشعر بالخوف الدائم من أمر كشف جرائمه وإفتضاح أمره، بالرغم من أن هذا الشعور يخالج كافة المجرمين، إلا أنها تصاحب مجرمي المعلوماتية بصفة خاصة لما يترتب على كشف أمرهم من إرتباك مالي وفقد للمركز

[1] _عبد العال الدربي، المرجع السابق، ص58.

[2] _تركي بن عبد الرحمن المويشير، المرجع السابق، ص28.

الوظيفي، ومرد هذا الخوف أيضًا هو إنتمائهم إلى فئة إجتماعية متميزة، من حيث التعلم والثقافة وطبيعة العمل[1].

البند الثاني :المجرم المعلوماتي ذكي ومحترف.

إذا كان مرتكبي الجرائم التقليدية ليس لمستواهم التعليمي و لا لدرجة ذكائهم دور كقاعدة في نمط جرائمهم ، فإن مجرمي المعلوماتية لا بد أن يكونوا من المختصين في مجال المعلوماتية ولهم دراية وخبرة في مجال التعامل معها أو فك رموزها ، فلا يمكن أن يرتكب هذه الجرائم إلّا من له مهارة و معرفة فنية في مجال المعلوماتية ، ولا يشترط المؤهل العلمي لذلك فيمكن أن يرتكبها شخص ليس له المؤهل العلمي و لكنه على درجة عالية من الذكاء[2].

وتبين إحصائيات العديد من القضايا أن عددًا من المجرمين لا يرتكبون سوى جرائم المعلوماتية، إي أنهم محترفون في هذا النوع من الإجرام دون أن تكون لهم صلة بأي نوع من الجرائم التقليدية[3].

إن المجرم المعلوماتي يمكن أن يكوّن تصورًا كاملا لجريمته وذلك قبيل تنفيذها و ذلك حتى لا يتفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو تسبب في الكشف عنها فالجرائم التي يرتكبها تتطلب منهمقدرة عقلية وذهنية عميقة في مجال المعلوماتية، فلا يلجأ إلى استخدام العنف بل يتبع أسلوب الهدوء لتحقيق أهدافه، و لذلك فإن الإجرام المعلوماتي هو إجرام الأذكياء فالمجرم المعلوماتي يسعى وبشغف إلى معرفة طرق جديدة لا يعرفها سواه سمح له بالاختراق الحواجز الأمنية في البيئة الإلكترونية لأجل نيل مبتغاه[4].

البند الثالث :المجرم المعلوماتي يتميز بقوة التحمل والصبر.

يحتاج المجرم المعلوماتي إلى القدرة على التحمل و الصبر، فقد يستغرق أمرإختراق إلكتروني، أو تحويل أموال ساعات طوال أو أياما لأجل تحسيده، ولذلك فإن قوة التحمل

---

[1] _نهلا عبد القادر مومني، المرجع السابق،ص80.

[2] _محمد حماد الهيتي، المرجع السابق،ص163.

[3] _عبد العال الدربي، المرجع السابق، ص58.

[4] _نهلا عبد القادر مومني، المرجع السابق، ص78،77.

والمثابرة من السّمات التي تساعد المجرم، المعلوماتي على نيل مبتغاه و رفع و تنمية قدراته ومهاراته فتكرار المحاولات يستغرق وقتا طويلًا يحتم عليه التمتع بالصبر[1].

البند الرابع : المجرم المعلوماتي يتمتع بالسلطة.

يقصد بالسلطة في هذا المجال، جملة الحقوق و المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من إرتكاب جريمته، فكثير منهم لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، و تتمثل عادة في إمتلاك شفرة الدخول إلى النظام المعلوماتي، و إجراء المعاملات، وقد تكون هذه السلطة أحيانًا غيرمشروعة في حال سرقة شفرة الدخول[2].

وقد يستغل المجرم المعلوماتي المزايا التي توفرها تكنولوجيا المعلومات وسلطته عليها فيدون بيانات وهمية وغير صحيحية، ويطلب الحاسوب إعتمادها عند إجراء بعض العمليات ومثالها الموظف المشرف على الموظفين على مصالح المحاسبة وصرف الأجور الذي يمكن أن يدرج أسماء بعض الموظفين الوهميين ضمن قائمة الموظفين ثم يمرر عملية صرف الرواتب ويتولى إيداع رواتب الموظفين الوهميين في حسابه الخاص ولذلك فإن المهتمين بمجال المعلوماتية عادةً ما ينبهون أصحاب المؤسسات إلى أخذ الاحتياطات اللازمة عند إختيار المشرفين على هذه المصالح[3].

الفرع الثاني:أصناف وفئات مجرمي المعلوماتية.

يصنف مجرمو المعلوماتية إلى عدة أصناف و ذلك حسب درجة الخطورة التي يتميزون بها أو يشكلونهافي مواجهة أمن نظم المعلومات، وكذلك بالنظر إلى حجم رغباتهم ودوافعهم الإجرامية ما بين الفضول و المزح وتحقيق الغاية الإجرامية و يمكننا تصنيفهم إلى:

البند الأول :صغار مجرمي المعلوماتية أو العابثون.

هم فئة الشباب الذين إنبهروا بالثورة المعلوماتية و الحواسيب ، و تتمثل أفعالهم في الإنتهاك غيرالمسموح به لذاكرات الحواسيب خصوصًا ، ولأجل الإطلاع على ما تحتويه من

---

[1] _عبد الله بن سعود السراني، المرجع السابق، ص36.

[2] _عبد العال الدربي، المرجع السابق، ص60،61.

[3] _الهاشمي الكسراوي" الجريمة المعلوماتية "،مقالة علمية، مجلة القضاء و التشريع ،العدد07، جويلية2006 ، مركز الدراسات القانونية و القضائية، وزارة العدل و حقوق الإنسان، الجمهورية التونسية، ص17.

معلومات بدافع الفضول ، فهؤلاء الشباب لا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي لها أفعالهم غير المشروعة ، فميولهم للمغامرة والتحدي والرغبة في الإكتشاف ، هو ما يميزهم عن المجرمين المحترفين في مجال المعلوماتية[1].

وقد تباينت الآراء حول تصنيف هؤلاء الشباب في طائفة المجرمين لأنهم ينطلقون من ميول المغامرة والتحدي والرغبة في الإستكشاف وهم لا يدركون خطورة أفعالهم ، فنادى البعض بالقول بأن هذه الفئة لا تسبب ضررًا للنظام المعلوماتي، بل يرجع لها الفضل في كشف الثغرات الأمنية في تقنية المعلومات و بالتالي فهي تخدم الأمن المعلوماتي[2].

أما الإتجاه الآخر فيرى أن هذه الفئة تصنف ضمن مجرمي المعلومات مثل غيرهم من المجرمين لأن أفعالهم تعد خطيرة من الناحية العلمية بالنظر إلى تعديها حدود الحواجز الجغرافية، و في الحقيقة فإنه لا يجب التقليل من شأن هؤلاء فقد تتعدى بواعثهم الهواية والعبث لتتحول إلى مراحل متقدمة وهي مرحلة إحترف هذه الجرائم[3].

البند الثاني:قراصنة المعلوماتية.

يمثل القراصنة تهديدًا جديًا وفعليًا على أمن المعلومات، فهم عادة ما يحترفون الجريمة المعلوماتية ويقصدون من ورائها إحداث الضرر بالمجني عليه، أو تحقيق الربح والكسب من خلال التعدي على مواقع وبيانات و معلومات خاصة بالمؤسسات والأفراد ، ويمكن التفرقة بين نوعين من القراصنة حسب درجة خطورتهم و إختلاف بواعثهم:

-أولا : القراصنة الهواة (Hackers):

هم فئة من مجرمي المعلوماتية يمتلكون عادة وسائل تقنية متطورة أكثر من تلك التي يستعملها العابثون، تكون عادة في شكل حواسيب متطورة و متصلة بشبكة الأنترنت إضافة إلى برامج معلوماتية نادرة، يتكون مجتمعهم من مبرمجين معلوماتين أصحاب خبرة في مجال علم الحواسيب و الشبكات، يميزهم الذكاء الحاد، ويمضون نصف أوقاتهم أمام شاشات

---

[1] _سامي على حامد عياد، الجريمة المعلوماتية و إجرام الأنترنت، دار الفكر الجامعي، الإسكندرية، مصر ، 2007، ص63

[2] _تركي بن عبد الرحمن المويشير، المرجع السابق، ص30.

[3] _نهلا عبد القادر المومني، المرجع السابق، ص82.

الحواسيب، فالقرصنة بالنسبة لهم هي حياة ثانية، تأخذ حيزًا مهمًا من الحياة الأولى، هدفهم مهاجمة مواقع الشركات الكبيرة والمؤسسات الحكومية، ومواقع القواعد العسكرية، الهاكرز ليسوا دائما سيئو النية فهم يريدون و بكل بساطة أخذ العبرة بزيارة أماكن ممنوعة على الشبكة ولا يقومون عادة سوى بالإطلاع على المعلومات[1].

إن هؤلاء المجرمين عادة ما يشغلون مناصب محل ثقة ولهم شهادات تعلمية ،ومن أمثلة ذلك الطالب لأمريكي (إيان ميرفي) الذي عمد سنة 1981 إلى إختراق الملفات المخزنة بحاسوب الحكومة الفيدرالية الأمريكية بهدف الإطلاع على المعلومات ذات الطابع السّري فقط[2].

و ما يمكن الإشارة إليه في هذا المقام هو التنظيم الذي أضحى يعمل عليه و يعتمده الهاكرز من خلال تبادل المعلومات والخبرات و الحلول، و تنظيم أنفسهم في مجموعات تعمل أو تدعي العمل للمصلحة العامة كمجموعة (Anonymosse) أو منظمات أخرى تعمل على تعطيل المواقع الإباحية و المواقع التي تنشر صور إباحية للأطفال، و الحقيقة التي يجب عدم إغفالها أن للقراصنة الهواة دورًا يسهم في كشف الفجوات الأمنية، الأمر الذي يدفع إلى تطويرها ضد الإعتداءات[3].

ثانيا : القراصنة المحترفون (Crackers):

يشكل الكراكرز أكبر تهديد للأنظمة المعلوماتية، لأنهم غير معروفين، ويستخدم هؤلاء عادة نفس وسائل القراصنة الهواة لدخول النظام المعلوماتي، لكنهم يختلفون معهم من حيث الباعث والغاية فهم لا يهدفون إلى سرقة المعلومات أو الإطلاع عليها فقط أو تعديلها، و إنما هدفهم هو تدميرها ومسح النصوص و البرامج و المعلومات المسجلة على القرص الصلب للحاسوب[4].

---

[1] _بولين أنطونيوس، المرجع السابق، ص158.

[2] _الهاشمي الكسراوي، المرجع السابق،ص185.

[3] _نهلا عبد القادر ميموني، المرجع السابق،ص83،84.

[4] _بولين أنطونيوس، المرجع السابق، ص186.

تعكس هذه الفئة ميولاتها الإجرامية الخطيرة التي تنبئ عن رغبتها في إحداث التخريب، فهم يتميزون بقدرتهم العالية و خبرتهم الواسعة في مجال النظم المعلوماتية، و عادة ما يعود المجرم المعلوماتي المحترف إلى إرتكاب جريمته مرة أخرى، بحيث تزداد سوابقه القضائية و يعيش غالبًا من عائدات جرائمه، وهذا المجرم لا يهتم بإبداء أراء متطرفة أو الدفاع عن حق الغير، وإنما يهتم فقط بالأفكار التي تدر عليه الأرباح[1].

وتشير الأبحاث والإحصائيات التي أجراها معهد (Stand Ford Resarch) أن الكراكز هم من الجيل الحديث، أي أنهم من فئة الشباب، وتتراوح أعمارهم ما بين 25_45 سنة وأن نسبة إرتكابهم للجرائم مقسمة ب:

- 25% من الجرائم المعلوماتية يرتكبها المحللون المعلوماتيون .
- 18% من الجرائم المعلوماتية يرتكبها المبرمجون المعلوماتيون .
- 17% من الجرائم المعلوماتية يرتكبها أشخاص لهم أفكار خاصة .
- 12% من الجرائم المعلوماتية يرتكبها أشخاص غرباء عن مكان تواجد المعلومات .
- 11% من الجرائم المعلوماتية يرتكبها فنيو التشغيل
- 17% من الجرائم المعلوماتية يرتكبها أشخاص من متصفحي الشبكات[2].

إذا كان هذا التصنيف لمجرمي المعلوماتية هو التصنيف المتعارف عليه في ميدان الجرائم المعلوماتية فإنه هناك أنواع أخرى من مجرمي المعلوماتية يصنفون تصنيفا آخر يمكنهم ذكرهم على سبيل الحصر في فئة:

1_ **الموظفون العاملون في مجال الأنظمة المعلوماتية** :يعتبر هؤلاء وبالنظر إلى المهارات التي يتمتعون بها، فئة مرشحة لأن ترتكب جرائم معلوماتية تحقق أهدافهم الشخصية وأهمها الكسب المادي أو الإنتقام من أرباب العمل.

[1] _نهلا عبد القادر مومني، المرجع السابق،ص 84.

[2] _تركي بن عبد الرحمن المويشير، المرجع السابق،ص32.

2_ **مجرمو المعلوماتية المتطرفون** :ويتألفون عادة من أفراد الجماعات الإرهابية و المتطرفة في إطار الجريمة المنظمة، لهم من المعتقدات والأفكار الإجتماعية والسياسية والدينية، والتي يرغبون في فرضها باللجوء إلى النشاط الإجرامي الذي أصبح يتجه إلى الجرائم المعلوماتية[1].

الفرع الثالث:الضحية في الجريمة المعلوماتية.

إن التسليم بأهمية النظم المعلوماتية و بالنجاح الكبير الذي حققته، لا يغفل معه أثر هذه النظم السلبي على ضمانات الحق في الحياة الخاصة، و يتجلى ذلك بصورة واضحة في اعتماد جل المؤسسات الحكومية و الخاصة على تقنية المعلوماتية، لما لها من قدرة هائلة تجعلها قادرة على عملية جمع و تخزين و معالجة، وإسترجاع و مقارنة كم هائل من البيانات الخاصة بأفراد المجتمع في قطاعاته المختلفة، و لكن ما يثير القلق هو إساءة استخدام المعلومات ذات الطابع السّري، التي تخزن إلكترونيا و هو قلق يزيد من حدته أن هذه المعلومات إذا ما تم الربط بينها واستعمالها فإنه يمكن أن تظهر جوانب يضر كشفها بالمصالح العامةو الشخصية للمعنيين بها[2].

إن الإطلاع أو التعدي على المعلومات بطرق إحتيالية غير شرعية تعتمد على الإختراق عادة، و الذي يشكل كسلوك تعديا على حق الغير و يترتب أثرًا مباشرً في شكل نتيجة إجرامية و مجني عليه، هذا الأخير له وضع خاص في الجرائم المعلوماتية، فالمعتدى عليه في هذا المجال هو من يكون ضحية الإعتداء غير المشروع الذي يستهدف مكونات الحاسوب المادية أو المنطقية، فقد يكون شخصًا طبيعيًا أو معنويًا في شكل شركة حكومية أو خاصة، ويشترط لأن ينطبق عليه هذ الوصف أن يكون الإعتداء قد إستهدف المجني عليه في إحدى المكونات المادية أو المنطقية لحاسوبه أو للشبكة التي يتصل من خلالها. و الملاحظ أنه من الصعب تحديد ضحايا الإجرام المعلوماتي على وجه الدقة لأن هؤلاء لا يعلمون شيئا عنها إلا بعد وقوعها، و في هذه الحالة يفضل أغلبهم أنه من الحكمة عدم الإبلاغ عنها

[1] _نهلا عبد القادر مومني، المرجع السابق،ص78،86.

[2] _بولين أنطونيوس، المرجع السابق،ص98،97.

وبالتالي لا يحبذ أكثرهم أن يعترف بأن نظامه المعلوماتي قد وقع ضحية إعتداء معلوماتي لما قد يشكل هذا الاعتراف من دافع المجرمين في الاستمرار في إعتدائهم[1].

ويبدو إحجام المجني عليه في مجال الجرائم المعلوماتية عن الإبلاغ عن الجريمة أكثر وضوحًا في المؤسسات المالية مثل البنوك، حيث تخشى إدارتها أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم إلى تضاؤل الثقة فيها من قبل المتعاملين معها، و هو ما قد يؤثر سلبًا في السياسة التي يمكن أن توضع لمكافحتها[2].

وتعتبر المعلومات مجموعة من القيم المستحدثة، الهدف الأول للجرائم المعلوماتية، فيمكن تصور وقوع هذا الإعتداء عليها سواء عن طريق بيعها أو مقايضتها أو إتلافها[3].

ويتركز الإتجاه الأساسي لجرئم المعلوماتية وفقا لتحقيق أجرته مجلة (Ressources Informatique أن:

- 19% من أفعال الغش المعلوماتي تستهدف البنوك .
- 16% من أفعال الغش المعلوماتي تستهدف الإ ا ردة .
- 10% من أفعال الغش المعلوماتي تستهدف الإنتاج الصناعي .
- 10% من أفعال الغش المعلوماتي تستهدف المعلومات .

لتأتي بعد ذلك شركات التأمين والشركات الخاصة، و في واقع الأمر فإن الجريمة المعلوماتية تستهدف في المقام الأول المؤسسات المالية و التي تتحكم في القيم الرأسمالية[4].

[1]_خالد بن عياد الحلبي، المرجع السابق،ص37.

[2]_تركي بن عبدالرحمن المويشير، المرجع السابق، ص21.

[3]_محمد علي العريان، المرجع السابق،ص67.

[4]_عبد العال الدربي، المرجع السابق،170.

المبحث الثاني:صور الجريمة الإلكترونية.

الجرائم الإلكترونية هي تلك الجرائم التي تتم بإستخدام الحاسوب و الشبكات، أو تلك الجرائم التي تقع على الحاسوب ذاته،وتتشابه الجريمة المعلوماتية والجريمة التقليدية من حيث المفهوم بإعتبارهما يشكلان تهديدًا على المصلحة العامة أو الخاصة المحمية قانونًا، غير أنهما يختلفان في مواضع كثيرة تتضح خصوصًا في مجال الركن المادي والركن المعنوي الخاص بكل منهما فنجد أن سرقة معدات الحاسوب المادية أو تخريبها، في صورة الشاشة أو الوحدة الرئيسية،أومعدات الإتصال بالشبكة كالكوابل، يعتبر من باب الجرائم التقليدية لأنها تستهدف أموالًا ذات طبيعة مادية قابلة للحيازة، عكس الجرائم الواقعة على المكونات المنطقية للحاسوب والتي تستهدف برمجياته والمعلومات المخزنة بداخله أو تلك المتداولة عبر شبكة الأنترنت، ففي هذه الحالة يكون الحاسوب الخاص بالجاني هو الوسيلة في إرتكاب الجريمة.

إن النشاط أو السلوك المادي في جرائم المعلوماتية بمفهومها الخاص يتطلب وجود بيئة إلكترونية وإتصال بشبكة الأنترنت، كما يتطلب من الجاني معرفةتفاصيل هذا النشاط ونتائجه ،فيقوم في سبيل المثال ذلك بتجهيز الحاسوب، و يحمله ببرامج الإختراق أو يعدها بنفسها وهو ما يعبر عنه بالحالة النفسية للجاني المعلومات[1].

إن الجرائم المعلوماتية هي ظاهرة إجرامية تقرع أجراس الخطر لتنبه العالم إلى حجم المخاطر التي يمكن أن تنجم عنها، وهي جرائم في نسق تطور مستمر ناهيك عن كونها جرائم ذكية وذات طبيعة و منشأ خاص، فهي تنشأ في بيئة إلكترونية، يقترفها أشخاص يميزهم الذكاء والمعرفة التقنية، مما يتسبب في خسائر للمجتمع ككل وعلى كل المستويات الإقتصادية والإجتماعية والثقافية والأمنية، ولذلك فقدإستقطبت هذه الجرائم إهتمام أغلب الدول و قد حازت على قدر مهم من الإهتمام التشريعي ،و ذلك سواء على المستوى الدولي أو الداخلي النابع من جهود التعاون الدولي في مكافحة الجريمة المنظمة، فنجد وعلى سبيل المثال أن إتفاقيةبودابست المؤرخة في 2001/11/23والتي إنضمت إليها أغلب دول

[1] _ محمد علي قطب، المرجع السابق،ص06.

الإتحاد الأوروبي إضافة إلى (17)سبعة عشر دولة خارج الإقليم الأوروبي تجرم في قسمها الأول من بابها الثاني في نصوص المواد من 02 إلى 13 مختلف صور الجرائم المعلوماتية والتي يجب على الدول الموقعة الالتزام بتجريمها ضمن نصوصها الداخلية،وقد أكدت المذاكرة التفسيرية بأن الهدف من القسم الأول من الباب الثاني لهذه الإتفاقية هو تحسين وإصلاح وسائل منع و قمع الإجرام المعلوماتي[1].

وهو ما تضمنه الفصل الثاني من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المؤرخة في 2010/12/21بالقاهرة ، بعد الإجتماع المشترك لوزراء الداخلية والعدل العرب بمقر الأمانة العامة للجامعة العربية والتي صادقت عليه إثنان و عشرون (22) دولة عربية[2] .

المطلب الأول :جرائم التعدي على النظم المعلوماتية.

يقصد بالنظم المعلوماتية أي نظام منفصل أو مجموعة من الأنظمة المتصلة بعضهما البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذ للبرنامج[3].

كما يقصد بالجرائم المعلوماتية بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية[4].

الفرع الأول :جرائم الدخول والبقاء غير المشروع للنظم المعلوماتية(جرائم الإختراق).

تعتبر هذه الجرائم الأكثر شيوعا في مجال الإجرام المعلوماتي ،والسلوك الإجرامي المفضل لمجرمي المعلوماتية ،وسنتناول بالتفصيل كل صورة من هذه الصور الإجرامية على حدى وفق ما يلي :

---

[1] _هلالي عبد اللاه أحمد، المرجع السابق، ص33.

[2] -المرسوم252/14المتضمن التصديق على الإتفاقيةالعربية لمكافحة جرائم تقنية المعلومات،الجريدة الرسمية رقم57،الصادرة بتاريخ 28سبتمبر2014،ص05.

[3] _ المادة 2 فقرة ب من القانون 04/09،المرجع السابق ،ص05.

[4] _المادة 2 فقرة أ من القانون 04/09 نفس المرجع،ص05.

البند الأول: طبيعة جرائم الإختراق المعلوماتي.

تعريف الجريمة:تعرف جرائم الدخول والبقاء غير المشروع ،أو جرائم إختراق النظم المعلوماتية بشكل عام بأنهاالقدرة على الوصول لهدف معين بطريقة غير مشروعة بطريقة الغش، عن طريق ثغرات في نظام الحماية الخاص بالهدف، وهي سمة سيئة يتسم بها المخترق لقدرته على دخول أنظمة الآخرين عنوة ودون رغبة منهم ودون علمهم بغض النظر عن الأضرار التي قد تحدثها، وتعد هذه الأنشطة الجرمية الأكثر إنتشارًا[1].

ويعد الدخول و البقاء غير المشروع أو غير المصرح به للنظم المعلوماتية، سابقة ضرورية كنشاط إجرامي لأجل إرتكاب جرائم معلوماتية أخرى كإتلاف المعطيات أو سرقتها،أو التحايل الإلكتروني أو التعدي على الأشخاص غير أن مرتكب هذا الفعل قد يقصده دون سواه وهو ما أثار خلافا بين الفئة حول مدى إنطباق وصف الجريمة المعلوماتية على هذا النوع من السلوكات ويمكن تخليص موقف الفقه في الإتجاهات التالية:

أولًا :الإ تجاه الداعي إلى عدم تجريم هذا النوع من السلوكات:

يرى أنصار هذا الإتجاه أنه ومن غير الداعي إلى تجريم مجرد الدخول أو البقاء داخل النظام المعلوماتي، و خاصة إذا لم لكن الفاعل نية إرتكاب جرائم لاحقة.

ثانيًا :الإ تجاه الداعي إلى ضرورة تجريم فعل الدخول والبقاء غير المشروع :

يرى أنصاره حتمية تجريم هذه السلوكات حتى ولولم يكن لدى الفاعل نية إرتكاب جرائم لاحقة، مستندين في ذلك إلى حجم الخسائر المادية التي قد تترب على مجرد حالة الدخول غير المشروع أو حتى محاولة ذلك، مستهدفين بالخسائر التي لحقت بأحد المصانع الأمريكية المتخصصة في صناعة الأسلحة النووية والتي بلغت 100.00 دولار كتكلفة أبحاث بهدف منع أحد الأشخاص من الدخول إلى نظمها المعلوماتية بصفة متكررة[2].

ولعل أن هذا الإتجاه هو الأكثر شيوعًا وعملًا به من قبل أغلب التشريعات التي لا ترى في وجوب تحليل نية المخترق في إرتكاب جرائم لاحقة، أمرًا ضروريًا لأجل تجريم الدخول

[1]_خالد عياد الحلبي، المرجع السابق، ص89.

[2]_نهلا بعد القادر، المرجع السابق، ص156،157.

غير المشروع كما هو عليه الحال في التشريع الجزائري حسب نص المادة 394 مكرر من القانون 15/04.[1] قانون عقوبات جزائري.

البند الثاني: أساليب و دوافع جرائم الإختراق المعلوماتي.

يعتمد المجرم المعلوماتي أساليب معلوماتية متنوعة لأغراض إجرامية ،مدفوعا بأغراض ودوافع شخصية تنبأ عن ميولاته الإجرامية ،ويمكن ذكر أهم أساليب الإجرامية وحصرها في:

أولا –أساليبها:

يعتمد هذا النوع من السلوكات على مبدأ التواصل غير المصرح به مع نظام الحاسوب أو شبكة المعلومات، من خلال إستخدام وسيلة اتصال عن بعد،أو خلال التواصل عبر نقاطالإتصال الموجودة على الشبكة للدخول إلى نظام حاسوب معين، بغرض الإطلاع على البيانات أو البرامج المخزنة فيه، و يتطلب ذلك عادة تجاوز أو كسر إجراءات الحماية المعلوماتية للنظام[2].

كما يعتمد المخترقون عادة على خطط أخرى لأجل تنفيذ أفعالهم وهي محاولة السيطرة على جدران الحماية (fire wall) وكذلك الهجوم على خادم الملفات العامة(serveur)، وقد يستعمل المخترق طرق غير هجومية عن طريق الدخول كمستعمل عادي حائز على التصريح، ثم الولوج إلى شبكة المنشأة ثم الإتصال بالخادم و الحصول على المعلومات[3].

ثانيا : دوافعها :

لجرائم الإختراق دوافع و أسباب عدة و لوأن العبث و قضاء وقت الفراغ يعد من أبرز عوامل نشوء هذه الظاهرة الإجرامية و بروزها للوجود، غير أن خبراء الأمن المعلوماتي لخصوا دوافعها في ثلاث نقاط:

---

[1] –القانون 15/04،المؤرخ بتاريخ10نوفمبر2004،المعدل والمتمم للأمر66–156 المتضمن قانون العقوبات،الجريدة الرسمية رقم71،ص11،12.

[2] _خالد عياد الحلبي، المرجع السابق، ص89.

[3] _عبدالله بن سعود السراني، المرجع السابق، ص31.

1_**الدافع العسكري** :إن الاعتماد شبه الكامل على أنظمة الحاسوب في المجال العسكري والصراع القائم بين الدول في مجال الدفاع فتح الطريق أمام ظاهرة الإختراق المعلوماتي بهدف التجسس لتوفير المعلومات السرية السياسية العسكرية والاقتصادية.

2_ **الدافع التجاري** :كما هو الحال بالنسبة للصراع بين الدول، تعيش الشركات التجارية حربا مشتعلة في مجال المنافسة وهو ما يجعلها عرضة لمحاولات الإختراق يوميا.

3_ **الدافع الشخصي** :ويشكل هذا الدافع نوعا من أساليب التباهي بالنجاح في إختراق أنظمة الحاسوب، وهو الدافع المشترك بين فئة طلاب الجامعات والمهتمين بمجال المعلوماتية[1].

البند الثالث: أركان جريمة الإختراق المعلوماتي.

تقوم جرائم الدخول غير المشروع والبقاء، على مبدأ عدم إحداث أي تأثير سلبي على الأنظمة المعلوماتية، ويقوم بهذا النوع من الأنشطة ما يطلق عليهم المخترقون ذوي القبعات البيضاء، الذين يقومون بالدخول بطريقة غير مشروعة لأنظمة الحاسوب وشبكات المعلومات ومواقع الأنترنت، مستغلين الثغرات الأمنية لتلك النظم ومخترقين إجراءات الأمن المعلوماتي وذلك بهدف الوصول إلى معلومات محاطة بالخصوصية والسرية، وقد يتعدى ذلك إلى إتلاف المعلومات وهي جرائم تقوم على[2]:

أولا :الركن الشرعي:

نص المادة394مكرر من القانون15/04.[3]

ثانيا :الركن المادي :

لا يقوم الركن المادي لفعل الدخول إلى النظام المعلوماتي على مدلول الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل هو الدخول بإستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول الإلكتروني[4].

---

[1] _خالد عياد الحلبي، المرجع السابق، ص90.

[2] _محمد علي قطب، المرجع السابق، ص7.

[3] -المادة394مكرر من القانون15/04،المرجع السابق،ص11،12.

[4] _نهلا عبد القادر مومني، المرجع السابق، ص158.

وتعتبر جريمة الإختراق شكلية أي أنها تحقق بمجرد تحقق السلوك الإجرامي، إذ لا يلزم لتحققها نتيجة ما، وقد يترتب عليها لاحقا من أضرار بالمعطيات المعلوماتية، و التي تعتبر في نظر العديد من التشريعات ظرفا مشددا للعقاب ولو لم يكن لدى الجاني النية في تحقيق أي نتيجة[1].

أما بالنسبة لجريمة البقاء غير المشروع داخل نظام معلوماتي فإنهما عادة ما تكون نشاطا لاحقا لجريمة الدخول غير المشروع، أو تعديا على الحق الممنوح بالدخول إلى النظام المعلوماتي من خلال تحديد مدة البقاء القصوى، ويظهر ركنها المادي على أنه نشاط مكمل لجريمة الدخول غير المشروع، ويقصد به الحالات التي يكون فيها الدخول إلى أنظمة المعالجة الآلية للمعطيات مشروعا متبوعا ببقاء غير مشروع ويتجلى ذلك في حرمان الفاعل من حق البقاء داخل النظام المعلوماتي[2].

و يتحقق الركن المادي الجريمة البقاء غير المشروع عن طريق الصدفة، أو الخطأ، فقد يجد الشخص نفسه داخل النظام صدفة فيقرر البقاء وعدم قطعالإتصال به، ويعتبر هذه الجريمة شكلية لا تشترط تحقيق أية نتيجة كما أنها جريمة مستمرة ماإستمر البقاء بصفة غير مشروعة داخل النظام المعلومات[3].

ثالثا –الركن المعنوي:

إن الركن المعنوي في الجريمة هنا، هو عبارة عن القصد الجنائي بعنصريه، العلم والإرادة فالفاعل لا بد له من أن يكون على علم بأنه يقوم بفعل الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، ولابد من ان تكون إرادته متجهة لارتكاب هذا الفعل.

البند الرابع: العقوبات المقررة لجريمة إختراق النظم المعلوماتية.

بالرغم من كون هذا النوع من الجرائم ذات طابع شكلي،إلّا أن أغلب التشريعات قابلتها بجزاءات عقابية حتى ولو لم يترتب عليها ضرر، وهو حال المشرع الجزائري الذي نص في مضمون المادة 394 مكرر 15/04 على ما يلي " يعاقب بالحبس من ثلاثة 03 أشهر

---

[1] _خالد عياد الحلبي، المرجع السابق، ص96.

[2] Myriam Quéméner- Yves Charpenel – La cybercriminalité- op cit -p 73.

[3] _نهلا عبد القادر، المرجع السابق، ص161.

إلى سنة 01 و بغرامة من 50.00 دج إلى 100.000 دج كل من يدخل أو يبقى بطريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك[1]".

الفرع الثاني :جرائم الإتلاف المعلوماتي:

بعد تعرضنا لجرائم الدخول والبقاء غير المشروع داخل النظم المعلوماتية، نستعرض نوعا آخر من الجرائم المعلوماتية يعرف بوصف جرائم الإتلاف المعلوماتي، والتي تعتبر عادة نتيجة حتمية للجريمة الأولى .

البند الأول: تعريف جرائم الإتلاف المعلوماتي:

هي تلك الجرائم التي ينتج عنها إتلاف المكونات المادية كالإتلاف الذي يقع على الشاشة أو الطابعة أو الأقراص المضغوطة، أو أسلاك ربط الشبكة،وهذه الصورة تنطبق عليها نصوص قانون العقوبات التقليدية التي تتناول بالتجريم فعل الإتلاف الذي يؤدي إلى إلحاق الضرر بالمال المنقول[2].

ولقد أورد المشرع الجزائري(الركن الشرعي) تعريفا لهذا النوع من الجرائم وذلك وفق ما نصت عليه في المادة 394 مكررمن 15/04 قانون عقوبات جزائري بالقول " : يعاقب بالحبس من 06 من ستة أشهر إلى ثلاثة سنوات 03 وبغرامة من 50.000 إلى 200.000 دج كل من أدخل بطريق الغش معطيات في نظام أو أزال أو عدل بطريق الغش المعطيات التي تضمنها[3]".

البند الثاني: الركن المادي لجريمة الإتلاف المعلوماتي.

لجريمة الإتلاف المعلوماتي وعلى غرار الجرائم الأخرى الخاضعة لمبدأ شرعية الجرائم والعقوبات ركن مادي تقوم عليه الجريمة وذلك بالرغم من الطابع المنطقي لها وصور الركن المادي لهذه الجريمة هي:

أولا : إعاقة السير العادي للنظم المعلوماتية :

أولا نشير إلى أن المشرع لم يتعرض في نص 394 مكرر01 من القانون 15/04

[1] -المادة394مكرر من القانون 15/04،المرجع السابق،ص12،11.

[2] _نهلا عبد القادر مومني، المرجع السابق، 123.

[3] _ المادة 394 مكرر من قانون العقوبات الجزائري.

قانون عقوبات جزائري[1]، إلى مفهوم إعاقة السير العادي للنظم المعلوماتية ، وهو السلوك الإجرامي الذي أولته إتفاقية بودابست أهمية بالغة وقد تجلى ذلك في نص القانون الفرنسي. يقصد بإعاقة سير عمل النظام المعلوماتي، "ذلك الفعل الذي يسبب تباطؤًا في عمل النظام أو ارتباكا، مما يؤدي إلى تغير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت"[2].

ثانيا: المساس بسلامة المعلومات :

إن المساس بسلامة المعلوماتAtteintes a l'intégrité des donnés كسلوك مجرم محصور في فعل الإدخال، التعديل، الحذف للمعطيات المعلوماتية المخزنة في ذاكرة الحاسوب، أو على الشبكة هو ما أتفقت عليه أغلب التشريعات كما جاء في نص المادة 394 مكرر01 من القانون15/04 قانون عقوبات جزائري، المادة 05 من نظام مكافحة الجريمة المعلوماتية السعودي، ويقوم الركن المادي لهذه الجريمة من خلال:

1- حذف أي محو البيانات كليا وتدميرها إلكترونيا،كمحو الذاكرة الرئيسية للحاسوب، أوإستعمال برمجيات خفية تعمل على محو محتوى الحاسوب أو الشبكة.

2- تعديل البرامج والمعطيات المعلوماتية من خلال:

أ -التلاعب بالبرامج أي بالنظام المعلوماتي بشكل يؤدي إلى إخفاء البيانات كليًا أو جزئيًا.

ب -اختلاس البرامج ويكون عن طريق نسخها عن طريق أسلوب التجسس.

ج -تغيير نظم عمل البرامج أي بتزويدها بتعليمات إضافية تتيح الوصول إلى جميع المعطيات التي يتضمنها الحاسوب.

3- إدخال برامج جديدة : أي إصطناع برنامج كامل أو ناقص في الناحية الفنية يخصص لارتكاب فعل الغش المعلومات[3].

البند الثالث: الركن المعنوي لجرائم الإتلاف المعلوماتي.

يتحقق الركن المعنوي بتحقيق السلوك المادي المقترن وجوبا بالقصد الجنائي (الإرادة العمدية)، بإستثناء الحالات المرخص لها إدخال تعديل أو حذف جزء من النظام المعلوماتي

---

[1] -القانون15/04،المرجع السابق،ص11،12.

[2] _محمد أمين الشوابكة، المرجع السابق، ص223.

[3] _محمد أمين الشوابكة، نفس المرجع، ص224.

ويعتبر قائمًا هذا الركن من لحظة إدخال أو تعديل أو حذف المعلومات المقترنة بإرادة إحداث تعديل على النظام المعلوماتي، مهما كانت النتيجة المتوقعة أو غير المتوقعة على النظام[1].

أما فيما يخص عنصر العلم فإنه يتحقق إذا ما كان الفاعل يعلم بأن المحل المعتدى عليه النظام المعلوماتي ملك للغير، و أن فعله بالإدخال أو الحذف والتعديل هو فعل من شأنه إحداث تلف أو إعاقة للنظام المعلوماتي عن أداء مهامه بشكل طبيعي.

الفرع الثالث: جرائم إساءة إستخدام المعلوماتية.

تعريف جريمة إساءة إستخدام المعلوماتية.

وجدت هذه الجرائم مجالا تعريفيا في نصوص القانون، فقد عرفها المشرع الجزائري من خلال نص المادة394 مكرر02 قانون عقوبات جزائري بالقول" : يعاقب بالحبس من شهرين (02) إلى ثلاث 03سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدًا أو عن طريق الغش بما يأتي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم[2]".

ولعل أن مفهومها يتضح بشكل أفضل وفق نص المادة 09 من الإتفاقية العربية لمكافحة جرائم التقنية الحديثة[3] بوصفها لجرائم إساءة إستخدام وسائل تقنية المعلومات على أنها:

-إنتاج أو بيع أو شراء أو توزيع أو توفير:

- أية أدوات أو برامج مصممة أو مكيفة لغايات إرتكاب الجرائم المبينة في المواد من 06 إلى 08من نص الإتفاقية .
- كلمة سر أو شفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد إستخدامها لأي من الجرائم المبينة في المواد من 06 إلى 08 من نص الإتفاقية.

---

[1] _ Myriam Quéméner- Yves Charpenel –La cybercriminalité- op cit- p 77.

[2] _المادة 394 مكرر 2 من القانون 15/04 ،المرجع السابق ،ص12.

[3] -المرسوم252/14، المصادقة على الإتفاقية العربية لمكافحة الجرائم،المرجع السابق،ص05.

• حيازة أي أدوات أو برامج مذكورة في الفقرة أعلاه، بقصد إستخدامها لغايات إرتكاب أي من الجرائم المذكورة في المواد من 06 إلى 08 من نص الإتفاقية[1].

و قد تعرضت إتفاقية بودابست قبل ذلك إلى تجريم هذا النوع من السلوكات باعتماد نفس الصياغة و ذلك وفق ما جاء في نص مادتها السادسة (06) .

البند الثاني:أركان جريمة إساءة إستخدام المعلوماتية.

إضافة إلى الركن الشرعي حسب نص المادة 394 مكرر02 تقوم هذه الجرائم على ركنين هامين هما:

أولا :الركن المادي :

يشكل هذا السلوك الإجرامي جريمة جنائية منفصلة و مستقلة، تتمثل في إرتكاب أفعال غير مشروعة ذات طبيعة خاصة ترتبط ببعض الأجهزة أو البرامج أو بيانات الدخول، في صورة إساءة إستخدامها بغرض إتاحة جرائم معلوماتية أشد وأخطر،إن إرتكاب هذه الجريمة يستلزم عادة وفي غالب الأحيان حيازة وسائل الولوج مثل أدوات وبرامج القرصنة أو أي وسائل أخرى بغرض إستعمالها لأغراض إجرامية، الأمرالذي يؤدي في النهاية إلى خلق نوع من السوق لإنتاج وتوزيع مثل هذه الأدوات [2].و يمكن حصر الركن المادي لهذه الجريمة في تحقق السلوكات التالية:

• تصميم برامج تساعد على الدخول غير المشروع داخل النظام المعلوماتية.
• تصميم برامج تساعد على إتلاف المعلومات كبرامج الفيروسات.
• البحث و تجميع المعلومات والبرامج التي تساعد على إرتكاب الجرائم الأخرى.
• توفير و نشر كل ما من شأنه المساعدة على إرتكاب الجرائم المعلوماتية.
• الإتجار في كل وسائل إرتكاب الجرائم المعلوماتية.

ثانيا :الركن المعنوي :

تعتبر هذه الجرائم ذات طابع عمدي وهو ما نستنتجه من نصوص قانون العقوبات التي أكد فيها المشرع على ضرورة توفر عنصر القصد في نص المادة 394 مكرر 02 قانون

[1] _ المرسوم252/14، المصادقة على الإتفاقية العربية لمكافحة الجرائم،المرجع السابق،ص05.
[2] _هلالي عبد اللاه أحمد، المرجع السابق، ص 84،85.

الجنائي الجزائري من خلال إستخدامه لعبارة" عمدًا أو عن طريق الغش "و بالتالي فإنه تستبعد من مجال التجريم الحالات التي لا يتوفر فيها القصد الجنائي أي صور الخطأ.

وعلى كل حال فإنه يشترط لقيام هذه الجريمة أن ترتكب عمدًا و بدون وجه حق أي يتوفر القصد الجنائي العام، أضف إلى ذلك يجب توفر نية خاصة أو قصد جنائي خاص يتمثل في إستخدام جهاز الحاسوب والشبكة لأجل إرتكاب الجريمة المشار إليها، وإستنادًا من ذلك نخرج من دائرة التجريم الأدوات والبرامج المصرح بها لأجل إستخدامها من أجل اختبار أو حماية جهاز الحاسوب[1].

البند الثالث :العقوبات المقررة لجرائم إساءة إستخدام المعلوماتية:

أقر المشروع الجزائري بعقاب كل من يتعمد أو يستعمل طريق الغش لأجل إرتكاب جرائم إساءة إستخدام المعلوماتية بعقوبة الحبس من (02) شهرين إلى (03) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج وتضاعف هذه العقوبة إذا ما مست بأمن الدفاع الوطني أوالهيئات والمؤسسات الخاضعة للنظام العام، دون الإخلال بمبدأ تطبيق عقوبات أشد إذا تعدت من حيث النتيجة أو القصد ما كان مقررًا بدءا[2].

المطلب الثاني :الجرائم المعلوماتية الواقعة على الأموال.

يمكن تعريف المال المعلوماتي المشمول بالحماية القانونية بأنه" كل مال إلكتروني قابل للنقل و التملك "أو بأنه "المال الموجود على الحاسوب، سواء في صورة معلومات أو بيانات إلكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية، فهو بذلك كل المدخلات الإلكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك و تكتسي الحماية القانونية[3]".

---

[1] _ هلالي عبد اللاه أحمد، المرجع السابق ، ص88،89.

[2] _ المادتين 394 مكرر 2 و 394 مكرر 3 من قانون العقوبات الجزائري.

[3] _ نايل نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2012، ص32.

أما تعريف المجلس الأروبي لغش الحاسوب فهو"تغيير أو محو أو كبت معطيات أو بيانات أو برامج الحاسوب، أو أي تدخل في مجال انجاز أو معالجة البيانات من شأنه التسبب في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على مكسب اقتصادي غير مشروع له أو لشخص آخر[1]".

الفرع الأول :جرائم التحويل غير المشروع للأموال أو جرائم الإحتيال الإلكتروني.

يعرف النصب أو الإحتيال على أنه من جرائم الإعتداء على ملكية مال منقول يلجأ فيها الجاني بواسطة إحدى وسائل الإحتيال المعينة قانونا، إلى حمل المجني عليه على تسليم المال المنقول[2].

البند الأول: الركن الشرعي:

وقد نص المشرع الجزائري على مفهوم جريمة النصب في نص المادة 372 من قانون العقوبات الجزائري بالقول" :كل من توصل إلى إستلام أو تلقي أموال والتي أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الإلتزامات أو إلى الحصول على أي منها أو شرع في ذلك،وكان ذلك بالإحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما بإستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث أمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة (01)على الأقل إلى خمس (05) سنوات على الأكثر وبغرامة من 500 إلى 20.000 دج[3]. ".

البند الثاني: الركن المادي.

يقوم الركن المادي لفعل الإحتيال على فعل التظاهر والإيحاء، الذي يكون صالحا للإيقاع بالمجني عليه في الغلط، بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي[4]

---

[1] _خالد عياد الحلبي، المرجع السابق، ص100،101.

[2] _محمد العريان، المرجع السابق، ص123.

[3] _ المادة 372 من قانون العقوبات الجزائري.

[4] --أحسن بوسقيعة،الوجيز في القانون الجزائي الخاص،الجزء الأول،الطبعةالخامسة عشر،دار هومة،الجزائر،2013، ص352.

والإحتيال لا يقع على الشخص الطبيعي فقط بل المعنوي أيضا، فالشركات والمؤسسات العامة و الخاصة هي من الأشخاص الاعتبارية في نظر القانون وحيث أن الحاسوب وشبكات الإتصال الداخلية والخارجية تعد من فروع ومكونات الشركة أو المؤسسة فإنها تكون صالحة لوقوع فعل الخداع والتحايل عليها، و قدإعتبر الفقه ممارسة أفعال الإحتيال من خلال التلاعب بالبرامج و البيانات و ما يترتب على ذلك من إيهام للمجني عليه بصحتها من أساليب الاحتيال،وحسب هذا الإتجاه فإن الحاسوب ليس سوى مجرد وسيلة للتحايل أما الفقه الفرنسي فاعتبر أن غش الأنظمة المعلوماتية للاستيلاء على الأموال يحقق جريمة الاحتيال[1].

و يشترط ليتحقق الركن المادي لجريمة الإحتيال تحقق الأفعال التالية:

أولا :فعل النصب :

أي تنفيذ فعل التلاعب بمدخلات النظام المعلوماتي أي تغذيته ببيانات غير صحيحة أو من خلال التلاعب ببرامجه، إضافة إلى فعل الإدخال والإتلاف والمحو والطمس التي سبق وتفصيل معناها[2]. وقد قدم مكتب التحقيقات الفيدرالي الأمريكي مجموعة من النصائح لمستعملي الأنترنت لأجل وقاية مستعمليه من الوقوع ضحايا جرائم الإحتيال وهي:

- تجنب المشاركة في المزايدات على شبكة الأنترنت إلا بعد التأكد من صحتها ودور البائع والمزايد فيها.
- عدم تقديم أرقام الضمان الإجتماعي في مجال البيع بالمزايدة على الأنترنت.
- عدم تقديم أرقام بطاقات الإئتمان إلا بعد التأكد من تأمين الموقع[3].

ثانيا:إستعمال الطرق الاحتيالية :

يستعين مرتكبو جرائم الإحتيال المعلوماتي بشبكة الأنترنت أساسا، من أجل تحصيل مبتغاهم و ذلك من خلال اعتماد أسلوب إرسال الرسائل الإلكترونية لضحاياهم، في شكل رسائل صادرة عن مؤسسات موثوق فيها، يطلب فيها من الضحايا المحتملين تقديم معلومات

[1] _محمد أمين الشوابكة، المرجع السابق، ص185.

[2] _هلالي عبد اللاه، المرجع السابق، ص102.

[3] _نايرعمرنبيل، المرجع السابق، ص84.

شخصية خاصة بهم، وهو ما يسمح لهؤلاء بتتبع ضحاياهم والعمل على الإيقاع بهم ،ولعل أن الأسلوب الأحدث هو الإحتيال على الطريقة النيجيرية التي تعتمد على إرسال رسائل بريدية إلكترونية مفادها طلب المساعدة على تحويل العشرات من ملايين الدولارات من قبل الضحية، بدعوى أن المرسل يعاني من مشاكل سياسية في بلده الأصلي و أنه مستعد تقديم ما قيمته 10 إلى15 % من قيمة الأموال المحولة بشرط فتح حساب و تدعيمه بقيمة أولية لأجل إتمام العملية[1].

يكتمل الركن المادي لهذه الجرائم إذا ما سبب بصفة مباشرة للغير ضررًا اقتصاديا أو ماديا، أي أن يكون الجاني قد نفذ الجريمة بغية الحصول على منفعة اقتصادية غير مشروعة له أو للغير،ومصطلح الضرر الاقتصادي أو المادي واسع جدا بمفهومه فهو يشمل النقود والأشياء المادية وغير المادية ذات القيمة الاقتصادية[2].

البند الثالث: الركن المعنوي لجريمة الإحتيال الإلكتروني.

تعتبر جريمة النصب أو الإحتيال من الجرائم العمدية، التي يتخذ فيها الركن المعنوي صورة القصد الجنائي حسب ما أورده المشرع الجزائري في نص المادة 372 قانون العقوبات،وتبعا لذلك فإنه يستلزم أن يتوافر قصد جنائي خاص يتمثل في إنصراف نية الجاني إلى تملك الشيء بطريق الإحتيال. و القصد العام في هذه الجريمة هو نتاج إجتماع عنصري العلم والإرادة معا، فعلم الجاني بأن فعله ينطوي على الإستيلاء على هذا المال.

الفرع الثاني :جرائم الإستخدام غير المشروع لأدوات الدفع الإلكتروني.

تعتبر تقنية الدفع الإلكتروني للأموال من أهم التطبيقات الحديثة للمعلوماتية ، فقد كسرت حاجز التعامل بالنقود وكذلك عوائق المبادلات المالية ،فأصبحت تتم بسهولة وسيولة كبيرة ولا تستغرق من الزمن سوى لحظات ، غير أنها و بقدر تطمينات المؤسسات المالية بمدى أمنها إلا أنها تبقى الهدف الأول لمجرمي المعلوماتية ، نظرًا لما تدره من أرباح دون اللجوء إلى الأساليب التقليدية للسرقة وما جاورها.

---

[1] Myriam Quéméner- Yves Charpenel – La cybercriminalité – op cit – p 135.

[2] _هلالي عبد اللاه، المرجع السابق، ص103.

توفر البطاقات الخاصة بالدفع الإلكتروني خاصية التعامل بالأموال في شكلها الإلكتروني دون عناء التنقل لتسليمها أو تسلمها في سبيل إتمام المعاملات ،وهو ما عزز نطاق المعاملات التجارية حول العالم ،وتتخذ البطاقات الخاصة بالدفع الإلكتروني لأشكالًا وأنواعًا عديدة وذلك كنتيجة لشيوع إستعمالها و يمكن إيجاز ذلك فيما يلي:

البند الأول :طبيعة العمل ببطاقات الدفع الإلكتروني :

يعتمد نظام عمل بطاقة الدفع الإلكتروني على عمليات التحويل الإلكتروني للأموال من حساب بطاقة العميل الخاصة بالبنك أو المؤسسة المالية المصدرة للبطاقة إلى حساب التاجر بالبنك أو المؤسسة المالية التي يوجد به حسابه من خلال شبكة التسوية الإلكترونية للهيئات الدولية، وأشهر بطاقات الدفع في هذا المجال MASTER CARD VISA CARD.[1]

تعطي البطاقة خدمة الحصول على السلع والخدمات لحاملها، بطريقتين:

الأولى :بحضور العميل بحيث يحصل التاجر على بصمة البطاقة مطبوعة على إشعار بالبيع من خلال قراءتها مع الحصول على توقيع العميل (DOS) .أو (ATM) على جهاز

الثانية :الحصول على السلع والخدمات عن طريق تصريح كتابي أو تلفوني، بخصم القيمة على حساب البطاقة عن طريق إستخدام شبكة الأنترنت[2].

فيكفي دخول العميل إلى الموقع الإلكتروني الخاص بالتاجر على شبكة الأنترنت، ثم يختار السلع المراد شراؤها، ثم يملأ النموذج الإلكتروني بإدخال بيانات البطاقة الإلكترونية وعنوانه،ويقوم بعدها التاجر بخصم قيمة السلع من رصيد البطاقة وإرسال نسخة من الفاتورة للمشتري[3].

البند الثاني: أنواع بطاقات الدفع الإلكتروني:

تختلف بطاقات الدفع باختلاف طبيعتها و تصنف إلى:

1-بطاقات الوفاء:

---

[1] _محمد أمين الشوابكة، المرجع السابق، ص193

[2] _خالد عياد الحلبي، المرجع السابق، ص119.

[3] _محمد أمين الشوابكة، المرجع السابق، ص193.

وهي الأكثر شيوعا ويطلق عليها بطاقات الخصم الشهري وتستخدم في الوفاء بمقابل السلع والخدمات التي يحصل عليها حاملها من التجار المعتمدين لدى المؤسسة المالية المصدرة لها.

2-بطاقات الائتمان:

يستطيع حاملها أن يسدد بها مجموع إلتزاماته مباشرة حتى ولو لم يكن يمتلك حسابًا أو رصيدًا لدى البنك مصدر البطاقة، ولكنه يلتزم بتسديد ما عليه من ديون تجاه البنك في أجل محدد بالاتفاق المسبق بينه و بين البنك، وكلما سدد ديونه في الأجل المحدد تجدد الاعتماد مرة أخرى، و أشهرها هي بطاقات Master cardوVisa card ..

3-بطاقات الصرف الآلي:

تعطي لحاملها إمكانية سحب مبالغ نقدية من حسابه الموجود لدى البنك مصدر البطاقة بحد أقصى متفق عليه.

4-بطاقات ضمان الشيكات :

تتيح هذه البطاقة لحاملها تحرير شيكات للمستفيد، مع تولي البنك مصدر البطاقة الوفاء بقيمة الشيكات المحررة[1].

البند الثالث: صور الإستخدام غير المشروع لبطاقات الدفع الإلكتروني.

تمثل جرائم الإستخدام التعسفي لبطاقات الدفع الإلكتروني، أشهر الجرائم التي تستهدف الأموال المتداولة و تتمثل صور هذا عبر النظم المعلوماتية، وخصوصا مع تنامي التجارة الإلكترونية الإستعمال التعسفي الذي يشكل جريمة في ذلك الإستعمال غير الشرعي من قبل الغير، أي من غير حامل البطاقة، لأن الجرائم التي يرتكبها حاملها يمكن أن تصنف على أنها جريمة خيانة أمانة، و يقصد بالجرائم هنا و المرتكبة من قبل الغير بأنها تلك الجرائم التي يرتكبها طائفة تهتم بمجال المعلوماتية، وتستهدف أمنها وأمر مرتاديها، فتركز جهودها على التقاط وقرصنة البيانات المالية الشخصية للأفراد أو المؤسسات البنكية من اجل إعادة إستخدامها بدون وجه حق ولأجل اقتناء سلع وخدمات وتحميل الغير مسؤولية دفع

[1] _ محمد علي قطب، الجريمة المعلوماتية و طرق مواجهتها، الجزء الثالث، بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني، أكاديمية الشرطة البحرينية، مملكة البحرينية، 2011، ص 8.

مقابلها.وتتكون بطاقة الدفع الإلكترونية من مكونين: (البطاقة نفسها، البيانات السرية الخاصة بحاملها).

و قد يقع فعل الإعتداء إما على البطاقة نفسها أو على مكوناتها المعنوية في إحدى الأشكال التالية:

أولا :في حال سرقة البطاقة أو ضياعها :

تتخذ البطاقة الخاصة بالدفع الإلكتروني شكلًا خاصًا مصنوعًا من مادة البلاستيك، مطبوع عليها بعض المعلومات المتعلقة بحاملها، مع شريط ممغنط يحتوي على بيانات غير مقروءة تتعلق بالبنك والعميل، فإذا ما سرقت أو ضاعت هذه البطاقة من حاملها فعليه إبلاغ البنك الذي أصدرها فورًا لمنع إستعمالها من قبل الغير أو إلغائها،وهو ما ينطبق أيضا على رقمها السري، وتصبح الجهة التي سحبت منها المبالغ بعد الإخطار هي المسؤولة ويتحمل الشخص الذي عثر أو سرق هذه البطاقة مسؤولية فعل سحب المبالغ من رصيدها[1].

ثانيا :في حالة سرقة أو ضياع بيانات البطاقة :

جرت العادة أن لا يمنح البنك الرقم السري الخاص بالبطاقة إلا لحاملها، حتى لا يكون عرضة للسرقة أو الإحتيال من قبل الغير و بالتالي تنحصر مسؤولية الإدلاء بأرقام البطاقة البنكية عبر شبكة الأنترنت على حاملها، كما يمكن أن يتعرض إلى سرقة رقمه السري وبيانات بطاقته من خلال ملئه لنموذج الشراء الإلكتروني على شبكة الأنترنت[2].

كما يمكن أن يتعرض لسرقة بنياته السرية من خلال بعض الأساليب التي يعتمدها لصوص التجارة الإلكترونية و هي:

1- إنشاء موقع إلكتروني وهمي على الشبكة مطابق لموقع بعض الشركات الكبرى وإستعماله في الحصول على البيانات السرية للمتعاملين ثم إغلاقه.

2- التسلل إلى مواقع الشركات التجارية والمالية والحصول على معلومات عملائها.

أي إغراق الموقع المستهدف بالرسائل البريدية و بالتالي تحميله

---

[1] _خالد عياد الحلبي، المرجع السابق،134،135.

[2] _محمد أمين الشوابكة، المرجع السابق، ص100.

3- إستعمال تقنية (Mail BomBing) ما لا يستوعب من معلومات مما يؤدي إلى انفجاره عبر الشبكة، و بعثرة المعلومات المخزنة فيه و منها البيانات السرية الخاصة بالعملاء[1].

ثالثا :حالة تزوير بيانات بطاقات الائتمان :

يتم تزوير بطاقات الدفع الإلكتروني على نطاق شبكة الأنترنت، من خلال تشكيل أرقام بطاقات خاصة ببنك معين،وذلك بعد تزويد الحاسوب بالرقم الخاص بالبنك مصدر البطاقة عن طريق برامج تشغيل خاصة،ومن ثم إستخدام البطاقة المزورة التي لها مستخدم أصلي،والقيام بعمليات الشراء بواسطتها مما يعرض العملاء الحقيقيين لمشكلات مع البنوك بسبب إستخدام بطاقاتهم،أو بطاقات مطابقة لبطاقاتهم، و هو ما يفسر إكتشاف البنوك لإعترضات من حاملي بطاقات الدفع الإلكتروني، على عمليات لم يقوموا بها

لتبين التحريات بعدها أن هذه العمليات تم إجراؤها عن طريق شبكة الأنترنت من قبل لصوص المعلوماتية الذين يستعملون تقنيات خاصة تمكنهم من الحصول على أرقام البطاقات الخاصة بالعملاء وإستخدامها في عمليات البيع و الشراء.

و تشير الإحصاءات في فرنسا أن:

71 % من الفرنسيين يقدرون بأنه ليس هناك حماية كافية عل شبكة الأنترنت .

75% من عينة البحث أبدوا تخوفا من عمليات الشراء عبر شبكة الأنترنت بسبب خطر قرصنة بياناتهم الشخصية ،وأغلب من فكروا في عمليات الشراء عبر الأنترنت يفضلون المواقع الفرنسية على حساب الأجنبية كمعيار ضمان[2].

الفرع الثالث :جرائم الإعتداء على حقوق الملكية الفكرية.

مع تقدم عصر الثورة المعلوماتية، طفت إلى السطح تحديات تتناسب مع هذا التطور فقد برزت مشاكل التعامل مع نوع جديد من أنواع الملكية الفكرية يمكن وصفها بالملكية الرقمية،وهي تلك الملكية التي تنصب على برامج الحاسوب وبياناتها والمصنفات الرقمية المنشورة على شبكة الأنترنت، التي بذل في إنتاجها وجمعها وإظهارها جهد فكري إبداعي

[1]_محمد علي قطب، الجريمة المعلوماتية وطرق مواجهتها،المرجع السابق، ص12 .

[2]_عبدالله بن سعود السراني، المرجع السابق، ص42.

جعل من الواجب حمايتها، كحق ملكية فردية وجماعية ،إن مسيرة التحول نحو مجتمع المعلومات تقضي السماح للأفراد بالنفاذ إلى هذه المعلومات مع كفالة حماية حقوق المؤلفين بمظاهر حماية حديثة تشمل الملكية الرقمية[1].

البند الأول: تعريف المصنفات الرقمية.

إنتقلت المصنفات الفكرية في ظل عصر المعلوماتية من صورة المنشورات الورقية التقليدية ،إلى الإلكترونية أو الرقمية المتاحة عبر الشبكة ،وهو ما جعلها عرضة لمخاطر الجريمة المعلوماتية ، بإعتبارها مصدر ربح مادي خصوصا إن كانت الأصالة والحداثة تميزها.

أولا :تعريفها :

يعرف المصنف الرقمي بأنه كل" مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات "فبرنامج الحاسوب مصنف رقمي، وكذلك قاعدة البيانات وطبوغرافيا الدوائر المتكاملة باعتبارها نتائج تطور علم الحاسوب، بخلاف أسماء وعناوين الأنترنت والبريد الإلكتروني التي تعتبر من المصنفات التي إرتبط ظهورها بشبكة الأنترنت[2].

وتتصف المصنفات عموما بطابع الأصالة إما من حيث الإنشاء أو التعبير، أي أنه نتاج ذهني بطابع معين يبرز شخصية صاحبه سواء في مضمون و جوهر الفكرة أو في مجرد طريقة عرضها[3].

البند الثاني: صور الجرائم المعلوماتية الواقعة على المصنفات الرقمية.

إهتمت غالب التشريعات بوضع نصوص تجرم المساس بالحقوق المعنوية والفكرية للغير وبالتالي تضمن للمصنفات الحماية القانونية اللازمة، ومنها المصنفات الرقمية من كافة أنواع الإعتداءات وهو ما تكلفت به وعلى نحو مفصل ودقيق إتفاقية بودابست لمكافحة الجريمة

---

[1] _عبد الكريم عبدالله ، الحماية القانونية للملكية الفكرية على شبكة الأنترنت، دار الجامعة الجديدة،2008،مصر، ص24 .

[2] _يوسف مسعودي، " النظام القانوني لحماية المصنفات الرقمية " ، مجلة الدراسات القانونية ، العدد 04 أوت 2009، مركز البصيرة للبحوث و الاستشارات و الخدمات التعليمية ، الجزائر ، ص113 .

[3] _محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، مصر، 2003، ص21 .

المعلوماتية في نص مادتها العاشرة ،وهو مادعمته المادة 17من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة2010 .[1]

و هي الجهود التي توجها المشرع الجزائري حيث أشار إلى مفهوم المصنفات الرقمية في الأمر 08/03المؤرخ في 2003/07/19في نصوص المواد 02-03-04-05 المتضمن لقانون حماية الدوائر الشكلية و المتكاملة[2]، إضافة إلى نص المادة03 و المادة 27من الأمر 05/03المؤرخ في 2003/07/19المتضمن قانون حماية المصنفات و حقوق المؤلف الشكلية والدوائر المتكاملة[3] ، إن كل هذه النصوص تجسد مفاهيم جرائم التعدي على المصنفات الرقمية والأكثرتداولاً منها وهي:

الإعتداء على حقوق المؤلف من خلال جرائم التقليد: (lacontrefaçon):

جرائم التقليد الفعال هي التي تعتمد على إعادة إنتاج أو عرض، أو نشر بأية وسيلة كانت عملًا فكريًا من خلال التعدي على حقوق المؤلف[4].

إن إعادة إنتاج وبث أو نشر الأعمال المحمية عبر الأنترنت بدون موافقة حائز حق المؤلف هو أمر شائع للغاية والأعمال المحمية تشمل عمومًا الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية، وجدير بالذكر أن السهولة التي يتم من خلالها عمل نسخ غير مصرح بها عن طريق التكنولوجيا الرقمية، والنطاق الذي بمقتضاه يتم إعادة إنتاجها و توزيعها هي الشبكات الإلكترونية[5].

فجرائم المعلوماتية هي أكثر الجرائم مساسا بحق المؤلف وخصوصا جرائم التحميل غير المشروع عبر شبكة الأنترنت، فملايين المتصفحين لشبكة الأنترنت إعتادوا على تحميل الأفلام والموسيقى دون شرائها من مصدرها الأساسي، مستغلين في ذلك برامج متخصصة في

---

[1] _المادة 17 من المرسوم 14-252 الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ،المرجع السابق ،ص06.

[2] -الأمر08/03المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة،بتاريخ2003/07/23الجريدة الرسمية،36ص44.

[3] - الأمر05/03المتعلق بحقوق المؤلف والحقوق المجاورة،بتاريخ2003/07/23الجريدة الرسمية44،ص04و07.

[4] _2Myriam Quéméner- Yves Charpenel – La cybercriminalité- op cit -p 145.

[5] _هلالي عبد اللاه، المرجع السابق، ص132.

فك شفرات الحماية، وذلك إما بغرض استعمالها الشخصي أو بغرض إعادة نشرها وطرحها للغير على شبكة الأنترنت أو للبيع على وسائط تخزين خارجية كالأقراص المضغوطة.

و هو الأمر الذي إستدعى تدخل المحكمة العليا للولايات المتحدة الأمريكية سنة 2005بحيث أشارت إلى أن الشركات التي تطور وتقدم برامج لتحميل الملفات يمكن محاكمتها بتهمة مساعدة متصفحي الأنترنت على انتهاك حقوق الملكية الفكرية[1].

و يقوم الركن المعنوي في هذه الجرائم في حال إرتكابها عمدا وبدون وجه حق أي أنها جرائم تشترط التعمد لأجل قيام المسؤولية الجزائية، و عليه تستبعد أفعال الاستعمال المشروع لهذه الحقوق إذا تعلقت بحق الغير في الإستعمال، ودون الإخلال بحقوق المؤلف، كاستعمالها داخل إطار علمي داخل منشأة علمية، أو نسخها بمعرفة مالكها لأجل حفظها من مخاطر التلف، أو دراستها بغرض نقدها وتطويرها، أو إذإستعملت من قبل هيئات الإذاعة المقروءة أو المسموعة أو المرئية[2].

المطلب الثالث :جرائم الإعتداء على الأفراد.

قابل الوجه المشرق لتقنية المعلوماتية، وجه سلبي يشكل خطرًا و تهديدًا على الحياة العامة والخاصة والحريات الفردية، وهو موضوع مستحدث شغل مؤخرًا حيزًا مهمًا من إهتمامات العام والخاص، خصوصا بعد ازدياد الطلب على المعلومات الشخصية من قبل مؤسسات الدولة أو المؤسسات الخاصة بل حتى من قبل الأفراد أنفسهم في ظل الاتجاه نحو مجتمع المعلومات[3].

و يتمثل الخطر خصوصا في غايات إستعمال هذه التكنولوجيا سواء كانت بصفة آلية أو دورية أو بشكل ظاهر أو خفي،مباشر أو غير مباشر من خلال تنفيذ عمليات تتمثل في جمع وتخزين ومعالجة ونشر معطيات تتعلق بأشخاص طبيعيين، في شكل كتابات أو صور

---

[1] _عبد الكريم عبدالله ، المرجع السابق، ص 214،215.

[2] _محمد حسين منصور، المرجع السابق، ص234،235.

[3] _العربي جنان،معالجة المعطيات ذات الطابع الشخصي،الحماية القانونية في التشريع المغربي والمقارن، المغرب2010 ،ص19.

أو أصوات، وتوفير الإمكانيات التقنية للتصرف فيها إما على حالتها الأصلية أو بعد معالجتها وبالتالي التحكم في الغايات المستوحاة منها[1].

الفرع الأول :الجرائم الماسة بالحريات العامة.

سوف نتحدث في هذا الفرع عن أهم الجرائم التي تمس الأداب العامة للمجتمع.

البند الأول:جرائم المعلوماتية الماسة بالآداب العامة.

تتلخص عموما هذه الجرائم في تلك السلوكات الماسة بالأخلاق ولو أن التعرض لجرائم الأخلاق ليس بالأمر الهين، بالنظر إلى تباين القيم الاجتماعية من مجتمع لآخر، بل وحتى بين طبقات المجتمع نفسه فما يعد إنحلالا خلقيا في مجتمع ما قد يكون غير ذلك في مجتمع آخر،وجرائم الأخلاق هي تلك التي تتضمن العدوان على القيم الاجتماعية والأخلاقية المتعارف عليها في النظم الإجتماعية[2].

ويشترط القانون في غالبه للقول بوجود جريمة معلوماتية ماسة بالآداب العامة أن تستوفي جملة من الشروط الأساسية وهي أن تكون علنية أي أن تترتب نتائج يعترف بها القانون ويرتب عليها آثاره، إضافة إلى أن تكون معروضة على الجمهور.

وقد تعرض المشرع الجزائري لمفهوم هذه الجرائم في بعض نصوص قانون العقوبات دون أن يحدد نطاقها المتصل بتقنية المعلوماتية، إلا أنه يمكن لنا إعمال هذه النصوص على جرائم المعلوماتية بالنظر إلى عمومية وشمولية النصوص، فنجد نص المادة 333 قانون عقوبات جزائري[3]، تشير إلى عقاب كل شخص إرتكب فعلا مخلا بالحياء بصفة علنية وذلك بالحبس من شهرين 02 إلى سنتين 02 وبغرامة من 500 إلى 2000 دج إضافة إلى نص المادة 333 مكرر التي تنص على نفس المقدار من العقاب في حق كل من صنع أو حاز أوإستورد أو سعى إلى ذلك، أو وزع أو أجر أو ألصق أو أقام معارض أو عرض أو شرع في ذلك أو باع أو شرع في البيع أو وزع أو شرع في ذلك، كل مطبوع أو محرر

[1] _ العربي جنان،معالجة المعطيات ذات الطابع الشخصي ،المرجع السابق، ص9.

[2] _ عبد العال الدريبي، المرجع السابق، ص235.

[3] -المادتين 333 و 333 مكرر من قانون العقوبات الجزائري.

أو رسم أو إعلان أو صور أو لوحات زيتية أو صور فوتوغرافية أو أنتج أي شيء مخل بالحياء.

من خلال إستقراء نصوص المواد السالفة الذكر نجد أن المشرع الجزائري لم يذكر بالتخصيص الجرائم التي تقع بواسطة النظم المعلوماتية والتي تستهدف المساس بالآداب العامة و إنما يمكن تطبيق نصوص هذه المواد على الجريمة المعلوماتية باعتبارها وفي الوقت الراهن من أبرز الوسائل الإجرامية المستعملة من قبل مجرمي المعلوماتية الذين وجدوا في هذه التقنية وسيلة ذات كفاءة عالية لأجل نشر إعلاناتهم الإلكترونية التي تمس بالآداب العامة،فالأفعال المجرمة حسب نص المادةتشمل:الصناعة أوالحيازةأو الاستيراد،العرض أو الشروع في العرض للجمهور،البيع أوالتوزيع أو الشروع فيهما[1]. فيمكن تصنيع وتركيب الأفلام والصور بواسطة الحاسوب وكذلك تخزينها وتعديلها ونشرها إما على شبكة المعلومات أو على وسائط تخزين خارجية كالأقراص المضغوطة، وبالتالي إتاحتها للجمهور والتأثير على قيمهم الاجتماعية، خصوصا بالنسبة للمجتمعات العربية الإسلامية وهو الأمر الذي شددت عليه الإتفاقية العربية لمحاربة جرائم التقنية المعلوماتية[2] وفق ما جاء في نص المادة (12)الثانية عشر منها بوصفها لهذه الجرائم بجرائم الإباحية والتي صاغها المشرع السعودي أحسن صياغة في نص المادة 06 الفقرة 10من قانون مكافحة الجرائم المعلوماتية السعودي بقولها :يعاقب بالسجن لمد ة لا تزيد عن 05 سنوات و بغرامة لا تزيد عن 03 ثلاث ملايين ،أو بإحدى العقوبتين كل شخص يرتكب الجرائم إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة.

الفرع الثاني :جرائم الإعتداء على حرمة الحياة الخاصة.

الحق في إحترام الحياة الخاصة أي مبدأ الخصوصية للأفراد، هو أحد الحقوق اللصيقة بالشخصية التي تثبت للإنسان لمجرد كونه إنسانًا و يعتبر هذا الحق من أهم الحقوق وذلك لما له من إرتباط وثيق بحرية الفرد، غير أن المعلوماتية بتقنياتها الحديثة المتمثلة في أجهزة الحاسوب، والشبكات الخاصة للإتصال العالمية منها والمحلية، وبما توفره من قدرة هائلة على

[1] -أحسن بوسقيعة،المرجع السابق،ص125.

[2] – هلالي عبد اللاه، المرجع السابق، ص134.

جمع المعلومات والبيانات الشخصية، وتخزينها وإسترجاعها وتصنيفها وتحليلها ومعالجتها، ومن ثم تبادلها وتناقلها دون أي عائق تقني، يشكل تهديدًا حقيقيًا على حق الأفراد في إحترام حياتهم الخاصة خصوصا مع ظهور ما يعرف ببنوك المعلومات، ومن هنا كان من الواجب التصدي للإجرام المعلوماتي الذي أصبح يشكل تهديدًا صريحًا على حقوق الإنسان وهو الحق في الحياة الخاصة[1].

يعتبر تعريف الحياة الخاصة أمرًا صعبًا نظرًا لمفهومها الفضفاض ومع ذلك فقد حاول بعض الفقه وضع تعريف لها على شاكلة الفقيه(مارتن) الذي قال :" هي الحق في الحياة الأسرية والشخصية والداخلية والروحية لشخص عندما يعيش وراء باب مغلق "، وأورد مؤتمر ستوكهولم الخاص برجال القانون المنعقد سنة 1967 تعريفا جاء فيه " هي الحق في أن يكون الفرد حراً وأن يعيش كما يريد دون أدنى حق للتدخل الخارجي "، وفي ظل صعوبة تحديد مفهوم الحياة الخاصة فإنه يمكن تحديد معالمها من خلال معا لم الزمان والمكان وتقاليد المجتمع مما يعني بأن هذا الحق يختلف تبعا لإختلاف الزمان والمكان[2].

و تشكل جرائم الإعتداء على حرمة الحياة الخاصة للأفراد جزءًا مهمًا من النشاط الإجرامي المعلوماتي و يمكن حصر صورها في الأوصاف التالية:

البند الأول: جرائم القذف و التشهير عبر الأنترنت.

للشخص الحق في الشرف الذي يكفل له إحترام سمعته وشرفه، وإعتباره وكرامته من التعدي والإيذاء، ويقصد بالشرف مجموع القيم التي يضيفها الشخص على نفسه وتشكل سمعته التي ستتبع تقدير الناس له، و يتمثل الإخلال بالشرف في الحط من مكانة الإنسان وتعريضه للإحتقار والإزدراء من قبل الغير عن طريق الأقوال والتشهير أو نسب الأفعال[3].

وتعد جرائم الذم والقدح والتحقير من أكثر الجرائم شيوعًا في نطاق شبكة الأنترنت، إذا أسيء إستخدامها بهدف النيل من شرف الغير وكرامته وإعتباره، ففي إطار مجتمع

---

[1]_نهلا عبد القادر المومني، المرجع السابق، ص165.

[2]_أسامة أحمد المناعسة، جلال محمد القاضي، جرائم تقنية نظم المعلومات الإلكترونية،دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان ،الأردن،2010، ص225.

[3]_محمد حسين منصور، المرجع السابق، ص372.

المعلومات الإلكترونية يجد العابثون حرية في نشر وبث رسائل تحتوي عبارات الذم والقدح والتحقير إتجاه آخرين مستهدفين بذاتهم، بصفة وجاهية أو غيابية أو بواسطة الوسائط الإلكترونية السمعية أو السمعية البصرية[1].

وغالبًا ما تقع هذه الجرائم بوصفها الحديث الإلكتروني تحت سلطة النصوص التقليدية مما يخلق إشكالًا في أمر إثباتها وهو ما ينطبق على أحكام التشريع العقابي الجزائري، بحيث يخلو من نصوص تتعلق بتجريم الإعتداءات على شرف وإعتبار الأشخاص ذات الطبيعة الإلكترونية، وتبقى المواد296 ، 297من قانون العقوبات مجرد نصوص توضيح الفعل المادي المكون لجريمة القذف والسب والقدح والتحقير، إضافة إلى العقوبات المقررة لها، بدون أي ربط مباشر مع تقنية المعلوماتية بالرغم من إقرار القانون رقم 04/15 المؤرخ في 10نوفمبر 2004 المعدل والمتمم لنصوص قانون العقوبات، وهو على عكس المشرع السعودي الذي تكفل في نصوص قانون مكافحة الجرائم المعلوماتية بإيضاح هذا النوع من الجرائم بالتفصيل كما هو نص الفقرة من المادة 03 من نفس القانون، وذلك تفسيرًا لما ورد في نص المادة أربعةعشر (14)من مضمون الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية[2] ،ويمكن حصر هذه الجرائم في الأنماط والسلوكات التالية:

أولا :إستهداف شخص معين بذاته بالذم والقدح والتشهير :

يكون ذلك إما بإستخدام البريد الإلكتروني بحيث يعمد الجاني من خلاله، إسناد مادة معينة إلى شخص ما قد يكون معنيا بذاته بحيث نال من شرفه أو كرامته و تعرضه إلى بغض الناس وإحتقارهم، خصوصًا إذا ما إعتمد الجاني في ذلك على توزيع مضمون الرسالة الإلكترونية إلى عدد غير محدد من المتعاملين مع الأنترنت عن طريق رسائل البريد الإلكتروني[3].

---

[1]_محمد أمين الشوابكة، المرجع السابق، ص31.

[2]_عرفت المادة 14 من الإتفاقية العربية لمكافحة جرائم المعلوماتية جريمة الإعتداء على حرمة الحياة الخاصة بإعتبارها جريمة معلوماتية بأنها " : الإعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات "،المرجع السابق ،ص06.

[3]_محمد أمين الشوابكة، المرجع السابق، ص33.

وقد يجد الجاني في شبكة الويب العالمية (Web)وسيلة في إسناد مادة كتابية أو صوتية أو مرئية مسيئة لشخص ما فتنال من شرفه وكرامته وتعرضه للإحتقار والذم من قبل الغير، كما أنها قد ترتكب عن طريق مواقع التواصل الاجتماعي (Facebook) ،أو موقع غرف المحادثة والدردشة (Chat Rooms)أو من خلال الوجاهية بفضل إستعمال تقنيات الاتصال السمعي البصري (Twitter) التي يوفرها خدمة (Skype) .

ثانيا :إستهداف مجموعة من الأفراد وحث الغير على كراهيتهم :

يمكن أن تستهدف هذه الجرائم مجموعة من الأفراد جملة واحدة من خلال إنتماءاتهم الدينية أو العقائدية أو العرقية، وهي النقطة الأساسية التي شكلت موضوع البروتوكول الإضافي لإتفاقية الجريمة الإلكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية، والتي تحرض على كراهية الأجانب والتي ترتكب عن طريق أنظمة الكمبيوتر المؤرخة في 28 جانفي2008 بسترا جبورغ بفرنسا والتي جاءت بفصلين الأول تضمن الأحكام العامة التي تبين الغرض الأساسي من هذا البروتوكول والثاني تكفل ببيان هذه الجرائم المعلوماتية وحصرها في السلوكات التالية:

- نشر المواد التي تتعلق بالعنصرية وكراهية الأجانب عبر أنظمة الكمبيوتر.
- التهديد الذي تحركه دوافع التمييز العنصري وكراهية الأجانب.
- الإهانة التي تحركها دوافع التمييز العنصري وكراهية الأجانب.
- الانكار أو التقليل أو الموافقة أو تبرير جرائم الإبادة الجماعية وجرائم ضد الإنسانية.

وهي الصور المجرمة نفسها تقريبا التي جاءت بها الفقرة 04 من المادة 15 من الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية.[1]

البند الثاني: جرائم التعدي على البيانات الشخصية.

تعد الحياة الخاصة قطعة أساسية من كيان الإنسان، لا يمكن إنتزاعها منه، وإن إحترامها يعد من المبادئ الدستورية الثابتة، بحيث يعد الدستور بأن لحياة المواطنين الخاصة حرمة يحميها القانون فلكل شخص الحق في أن تظل أسرار حياته الخاصة محجوبة عن العلنية

[1] -المادة15 من المرسوم14-252 ،الإتفاقية العربية لمكافحة جرائم المعلوماتية، المرجع السابق ،ص06.

ومضمونة من تدخل الغير وإستطلاعه[1]. وتشكل الجريمة المعلوماتية مظهرًا حديثا، يهدد بخطر محدق البيانات الشخصية للأفراد من عدة زوايا نوجزها فيما يلي:

أولاً:جمع البيانات وتخزينها على نحو غير مشروع:

يتمثل فعل انتهاك الحق في الحياة الخاصة للأفراد، في عملية جمع وتخزين بيانات صحيحة عنهم ولكن على نحو غير مشروع، ويستمد هذه الصفة غير المشروعة من الأساليب المستخدمة لأجل الحصول على هذه البيانات أو من حيث طبيعة هذه البيانات.

أما من حيث الأساليب فقد يعتمد الجاني على أسلوب التقاط إرتجاجات الجدران وترجمتها إلى عبارات وكلمات وذلك بواسطة معدات خاصة تغذي الحاسوب المزود ببرنامج خاص لترجمة كل ذلك، أو من خلال إعتراض الرسائل الإلكترونية، أو إختراق النظام المعلوماتي للضحية.

أما من حيث طبيعة البيانات فان البيانات الإسمية الخاصة يجب أن يحظر جمعها وتخزينها ومعالجتها داخل الحاسوب من قبل الغير، إضافة إلى المعلومات المتعلقة بالسجل القضائي التي لا يحق إلا للسلطة القضائية جمعها و تخزينها حفاظا على سمعة الأشخاص[2].

وهي الجرائم المنصوص عليها في نصوص المواد 303 مكرر و 303 مكرر 01 من قانون العقوبات الجزائري[3].

ثانيا :إساءةإستعمال البيانات والمعلومات الإسمية إنتحال الشخصية:

ترتكز جريمة إنتحال الشخصية على مبدأ التعدي على البيانات الإسمية للغير من أجل التخفي والتهرب من المسؤولية، أي الإفلات من المتابعة الجزائية، أي هي إستخدام بيانات شخصية للغير من أجل الوصول إلى هدف غير مشروع، يتمثل في جريمة تحقق الربح المادي لمقترفها، دون أن يكون هو المتابع بشأنها، وقد أشارت الإحصائيات السنوية لسنة 2009أن حوالي 210,000 شخص في فرنسا قد وقعوا ضحايا هذا النوع من الإجرام

[1] _محمد حسين منصور، المرجع السابق، ص373.

[2] _نهلا عبد القادر مومني، المرجع السابق،ص173،174.

[3] -القانون06/23،الصادر بتاريخ20ديسمبر2006المعدل والمتمم الأمر66-156المتضمن قانون العقوبات،الجريدة الرسمية رقم84،ص23.

عبر الأنترنت،ويقدر معدل نموها على مستوى الدول الغربية ب 40% وتشكل هذه الجريمة جزءًا من جرائم الاحتيال المعلوماتي، فالفرد أصبح معرضًا أكثر من أي وقت مضى لمخاطر انتحال هويته من قبل الغير بسبب إعتماده المطلق أو شبه الدائم على تقنية المعلوماتية وشبكة الأنترنت خصوصًا، ضف إلى ذلك أن وسائل التحقق من الشخصية عبر الأنترنت هي غير تلك المتبعة أمام الجهات الرسمية فاسم المستعمل وكلمة السر والعنوان المنطقي، ورقم البطاقة البنكية هي وسائل إثبات الهوية المعلوماتية وهي الأجدر بالحماية، مقارنة بالاسم واللقب والصورة، وقد عرفت هذه الجرائم إنتشارًا رهيبا في السنوات الأخيرة من خلال إنتشار تقنية المعلوماتية وقد علق عليها الأستاذ أوليفي إيتاني(Olivier Iteanu)بالقول :"لقد دخلنا مرحلة الهوية المستعملة "أي أنها قابلة للاستبدال بمجردإستعمالها أول مرة[1].

ثالثا :إفشاء الأسرار و البيانات و المعلومات الاسمية:

إن هذا النوع من السلوكات الإجرامية، قد يكون نتيجة حتمية للجرائم السالف ذكرها، بأن البيانات الخاصة قد إنتقلت من السر إلى العلانية، بمجرد تخزينها بعد تجميعها على نحو غير مشروع أو حتى بصفة مشروعة، وبالتالي فإنها تكون عرضة للاطلاع عليها من قبل عدد غير محدد العدد من الأشخاص في حال عرضها على شبكة الأنترنت أو على الأقل من قبل عدد محدد متمثل في الأشخاص العاملين في فضاء المعلوماتية.

الفرع الثالث :جرائم الاستغلال الجنسي للأطفال عبر الأنترنت.

تعتبر هذه الجرائم نتاج نطاق عالمية الأنترنت الذي يتيح نشر الأعمال المخلة بالآداب العامة والأخلاق، والتي يتباين مفهومها من بلد لآخر، فإستخدام التقنية المعلوماتية في نشر المواد الإباحية التي تستهدف شريحة البالغين، قد لا تستثني شريحة الأطفال الذين قد يكونوا عرضة إما لهذه المواد الإباحية أو محلا لها مما يشكل إعتداءا ماديا ومعنويا على الأطفال،ولقد

[1] Myriam Quéméner- Yves Charpenel – La cybercriminalité - op.cit -p 89-90

صادقت الجزائر على البروتوكول الإختياريالملحق باتفاقيةحقوق الطفل ولقد فصلت المادتين(02)و(03)من 299/06 إستغلال الطفال في البغاء[1].

وتشكل تقنية المعلوماتية تهديدا على فئة القصر والأطفال من ثلاث 03 نواحي:

1- إمكانية ولوج الأطفال إلى مضمون المواقع الإباحية أو المواقع التي تظم دعارة الأطفال.

2- تخليد الانتهاكات الجنسية ضد الأطفال من خلال نشر هذه المواد على شبكة الأنترنت.

3- تشكل شبكة الأنترنت مرتعا للأشخاص الخطيرين المنجذبين لفئة الأطفال، وبالتالي فانه يمكن الإيقاع بهم[2].

و مما يزيد من مخاطر الأنترنت على الأطفال هو إعتبارهم الفئة الأكثر انجذابا لهذه التقنية والأكثر تصفحا للإنترنيت فقد قدمت وكالة كاليستو لاتحاد صوت الطفل إحصائيات تفيد بأن 12 %من هذه الفئة تقضي أكثر من 03 ساعات يوميا في تفقد الرسائل الإلكترونية وأن أكثر من87%منهم قد تفاجأوا بمضامين إغرائية فاضحة، وبالتالي فإن الأطفال هم الفريسة الأسهل على شبكةالأنترنت[3].

البند الأول: مظاهر الحماية القانونية للأطفال عبر الأنترنت.

ظهرت المساعي الأولى لمكافحة الاستغلال الجنسي للأطفال عام 1999 بمناسبة مؤتمر فينا لمكافحة الاستغلال الجنسي للأطفال، وقد نصت المادة " 34 " من إتفاقية حقوق الطفل على أن يتعهد الأطراف على حماية الطفل من جميع أشكال الإستغلال الجنسي والإنتهاك الجنسي وذلك من خلال إتخاذ جميع التدابير الوطنية والثنائية والجماعية لمنع الأطراف:

- حمل أو إكراه الطفل على تعاطي نشاط جنسي غير مشروع.
- الإستخدام الاستغلالي للأطفال في الدعارة.

---

[1] -المرسوم06-299 المؤرخ في 02 سبتمبر2006،التصديق على البروتوكول الإختياري الملحق باتفاقية حقوق الطفل،الجريدة الرسميةرقم55،ص04.

[2] _محمد أمين الشوابكة، المرجع السابق، 106،107.

[3] _ Myriam Quéméner- Yves Charpenel – La cybercriminalité - op.cit – p 103.

- الإستخدام الاستغلالي للأطفال في العروض والدعارة...

أما على المستوى الإقليمي فنجد أن إتفاقية بودابست لسنة 2001 قد أفردت في نص مادتها التاسعة 9 مجموعة من الأحكام تلتزم بها الدول الموقعة تحت عنوان :الجرائم المتصلة بالمواد الإباحية للأطفال والتي جرمت السلوكات التالية:

- إنتاج مواد إباحية طفولية بغرض نشرها على نظام معلوماتي.
- تقديم أو إتاحة مادة إباحية طفولية عبر نظام معلوماتي.
- التزود أو تزويد الغير بمادة إباحية طفولية عبر نظام معلوماتي.
- حيازة مادة إباحية طفولية في نظام معلوماتي أو أية وسيلة تخزين.

و هي نفس التوصيات التي قدمتها الإتفاقية العربية لمواجهة جرائم تقنية المعلومات في نص الفقرة 02 و 03من نص المادة 12 الثانية عشر الموسومة بالجريمة الإباحية ضد الأطفال.

أما على مستوى التشريع الجزائري فتجريم هذا النوع من السلوكات جاء متأخرًا جدا وذلك بموجب القانون 01/14 المؤرخ في 04 فيفري 2014 الذي إستحدث نص المادة 333مكرر 1 ضمن قانون العقوبات الجزائري والتي جاء فيها "بأنه يعاقب بالحبس من 05 سنوات إلى 10 سنوات و بغرامة من 500 ألف إلى 1 مليون دج كل من صور قاصرًا لم يكمل سن 18 سنة بأي وسيلة كانت و هو يمارس أنشطة جنسية بصفة مبينة ،حقيقية أو غير حقيقية ، أو صور الأعضاء الجنسية للقاصر جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو إستيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر. في حال الإدانة تأمر الجهة القضائية بمصادرة الوسائل المستعملة لأرتكاب الجريمة والأموال المتحصل عليها مع مراعاة حقوق الغير حسن النية"[1].

البند الثاني: صور الإستغلال الجنسي.

إذا كان واقع الحال من الناحية التشريعية هو توحد الرؤى والنظرة تجاه ظاهرة الاستغلال الجنسي للأطفال عبر الأنترنت فان المظاهر المادية لهذه الظاهرة في إتساع و تزايد مستمر ويمكن حصرها تحت أوصاف عامة في شكلين أساسيين هما:

[1]-القانون 01/14،الصادر بتاريخ04فبراير2014،الجريدة الرسمية رقم07،ص07.

أولا :جريمة إغراء الأطفال عبر الأنترنت لغرض إباحي :

تتحقق هذه الجريمة حسب ما أورده المشرع الفرنسي وهو بقيام الجاني بربط الاتصال مع الأطفال بغرض إغوائهم جنسيا و يكون الربط بواسطة إلكترونية و الغرض منها هو عقد لقاء معهم يقوم على هدف المعاشرة الجنسية يشارك فيها الطفل ويتحقق ركنها المعنوي من خلال إلمام الجاني بعنصري العلم والإرادة فيعلم أن سلوكه محظور وأن الضحية قاصر و تتجه إرادته إلى الإغواء بهدف إشباع رغبته الجنسية، كما قد يكون الغرض أوالسلوك مقتصرًا على عرض مشاهد إباحية على الطفل[1].

ثانيا :جريمة استغلال صورة الطفل عبر الأنترنت في مواد إباحية :

تتحقق هذه الجريمة وفق قانون العقوبات الجزائري نص المادة 333 مكرر 1من القانون14 /01[2]، من خلال ركنها المادي القائم على التقاط صور أو تصوير صور لطفل أو حيازتها أو نشرها أو تخزينها أو تزويد الغير بها لغرض إباحي، ويكون ذلك باستعمال الحاسوب وشبكة الاتصال،سواء كانت حقيقة أو مصطنعة، كما يتحقق ركنها المعنوي من خلال توفر القصد الجنائي أي علم الجاني بخطورة فعله و إتجاه إرادته إلى تحقيق هذه الحيازة أو النشر أو الإنتاج للمواد التي تستغل فيها صورة الطفل في أعمال إباحية.

[1] _محمد أمين الشوابكة، المرجع السابق، ص130.

[2] – القانون 01/14، المرجع السابق،ص07.

الفصل الثانـــي

الوحدات والإجراءات الخاصة بالبحث والتحقيق في الجرائم الإلكترونية

يختص على المستوى الوطني بمهام مباشرة أعمال البحث والتحقيق في الجرائم المعلوماتية وحدات متخصصة منها التابعة لوزارة العدل، وأخرى تابعة لسلك الأمن الوطني منها ما هي تابعة لسلك الدرك الوطني ، و هي وحدات أغلبها حديثة النشأة نظراً لحداثة المجتمع الجزائري مع عهد الجرائم المعلوماتية ، و التي تعرف إنتشاراً متزايداً تماشياً وإنتشار تكنولوجيا المعلومات المرتبطة أساسا بإستعمال الحواسيب و شبكة الانترنت ،و كذلك الهواتف الذكية المرتبطة بشبكة الأنترنت للجيل الثالث. ونظراً لطبيعة الجرائم المعلوماتية الخاصة فإنها تتطلب إجراءات و أساليب خاصة و نوعية للبحث والتحقيق، لأجل اكتشاف الدليل الرقمي و تحصيله من قبل الفنيين المختصين، وكل ذلك يستدعي اتخاذ إجراءات سريعة.

وعليه سوف نقسم هذا الفصل إلى مبحثين في المبحث الأول نتناول فيه الوحدات المختصة بإجراءات البحث والتحقيق في الجرائم المعلوماتية على المستوى الوطني، والمبحث الثاني الإجراءات الخاصة المتبعة في إطار تنفيذ إجراءات البحث والتحقيق المعلوماتي.

المبحث الأول: وحدات البحث والتحقيق في الجرائم الإلكترونية مركزيًا.

أفرز الإنترنت جرائم لم تكن في الحسبان الأمر الذي دعى الجزائر أن تتخذ كافة الإحتياطات والتدابير للحد منها، فعلى الرغم من الضعف بهذا المجال إلا أنها أنشأت وحدات على كافة الأصعدة لمجابهتها.وعليه سوف نقسم هذا المبحث إلى ثلاثة مطالب في المطلب الأول نتناول الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام، والمطلب الثاني الوحدات التابعة لسلك الأمن الوطني أما المطلب الثالث فخصصناه للوحدات التابعة للدرك الوطني الجزائري.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام.

تعود فكرة إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال إلى سنة2009 و بالضبط منذ تاريخ 05 أوت 2009 تاريخ صدور القانون 04/09.[1] المتعلق بتحديد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، بحيث جاء في نص المادة 13 من القانون على انه تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحته، تحدد تشكيلة الهيئة و تنظيمها و كيفية سيرها عن طريق التنظيم.

وقد إستلزم الأمر لصدور التنظيم الذي طرحته نص المادة 13 السالفة الذكر الإنتظار لمدة 06سنوات كاملة، أين صدر المرسوم رقم 15/ 261.[2] والذي تضمن في فصوله تحديد تشكيلة و تنظيم وكيفيات سيرالهيئةالوطنيةللوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

الفرع الأول:التعريف بالهيئة وإختصاصاتها.

البند الأول: تعريف الهيئة.

تعتبر " الهيئة " كما يصطلح عليها في صلب نصوص المرسوم الرئاسي حسب أحكام المواد من 01 إلى 04 منه بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و

[1] -القانون 04/09 المتعلق بتكنولوجيا الإعلام والإتصال،المرجع السابق.

[2] -المرسوم261/15 الصادر بتاريخ08أكتوبر2015،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، رقم53.

الإستقلال المالي توضع لدى الوزير المكلف بالعدل، و يقع مقرها بالجزائر العاصمة، تتولى الهيئة المهام المنصوص عليهاحسب نص المادة 14من القانون 04/09[1] و ذلك تحت رقابة السلطة القضائية و طبقا لأحكام قانون الإجراءات الجزائية.

البند الثاني: إختصاصات الهيئة:

بينت البند الثانية 02 من المادة 04 من المرسوم الرئاسي261/15[2] المهام الأساسية التي تكلف بها الهيئة و هي و على سبيل الحصرمهام الهدف منها هو الوقاية من الجرائم المعلوماتية، و مكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث و التحقيق ومد يد العون لمصالح الشرطة القضائية و أبرز مهام هذه الهيئة هي:

1_ إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

2-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحته.

3- مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.

4- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية و الماسة بأمن الدولة و ذلك تحت سلطة قاضي مختص.

5- تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مسارها من أجل إستعمالها في الإجراءات القضائية.

6- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا المعلومات

7- تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المعلوماتية.

8- تنفيذ الطلبات الصادرة عن الدول الأجنبية و تطوير سبل التعاون و التبادل معها.

---

[1] - الفانون 04/09 المتعلق بتكنولوجيا الإعلام والإتصال،المرجع السابق.

[2] - المرسوم261/15،يحدد تنظيموكيفيات سير الهيئة الوطنية، المرجع السابق.

9- المساهمة في تحديث المعايير القانونية في مجال إختصاصها.

الفرع الثاني:تشكيل الهيئة وطبيعة عملها.

تتشكل الهيئة من لجنة مديرة إضافة إلى مديرية عامة ، تتشكل اللجنة المديرة من الوزير المكلف بالعدل رئيسا إضافة إلى الوزير المكلف بالداخلية و الوزير المكلف بتكنولوجيات الإعلام و الإتصال وقائد الدرك الوطني و كذلك المدير العام للأمن الوطني ،وممثلين أحدهما عن رئاسة الجمهورية والأخر عن وزارة الدفاع يكملها قاضيان من المحكمة العليا، أما المديرية العامة فيرأسها مدير عام يعين بموجب مرسوم رئاسي ، و تتجلى مهام هذه المديريات في ضبط برامج عمل الهيئة ودراسة مشروع الميزانية و تقديم تقارير خاصة بنشاط الهيئة، و بالتالي فهي لا تساهم في الإجراءات الخاصة بالوقاية أو بمكافحة الجرائم المعلوماتية[1].

البند الأول: تشكيلة الهيئة التقنية

إضافة إلى اللجان الإدارية تضم الهيئة مديريات تتسم من حيث مهامها وتشكيلتها بالطابع التقني، بإعتبارها المختصة بإنجاز المهام التقنية المتعلقة بالوقاية و وبمكافحة الجرائم المعلوماتية و هذه المديريات هي:

-أولًا : مديرية المراقبة الوقائية و اليقظة الإلكترونية

لم يشر الأمر الرئاسي 261/15 إلى تشكيلة المديرية ،غير أنه و من خلال تحليل نص المادة 18 منه يمكن لنا تحديد تشكيلتها في مجموعة من ضباط و أعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، من سلك الأمن الوطني و كذلك الدرك الوطني و المصالح العسكرية للإستعلام و الأمن، يعينون بموجب قرارات مشتركة بين

[1] _المواد 6، 7، 8 ،9، 10 من المرسوم الرئاسي 261/15 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإتصال والإعلام ومكافحتها،المرجع السابق.

.

الوزراء المكلفين بالعدل و الدفاع و الداخلية ، يساعدهم مستخدمي الدعم التقني و الإداري من نفس الأسلاك. تعمل هذه المديرية على إنجاز المهام التالية:

1- تنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية و القيام بإجراءات التفتيش والحجز داخل الأنظمة المعلوماتية إذا ما تعلق الأمر جرائم الإرهاب او التخريب و الجرائم الماسة بأمن الدولة بناءًا على رخصة مكتوبة من السلطة القضائية و تحت رقابة القاضي المختص.

2_ إرسال المعلومات المحصل عليها إلى السلطات القضائية و مصالح الشرطة القضائية.

3- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئةوجمع المعطيات التي تسمح بتحديد مكان تواجد مرتكبي الجرائم المعلوماتية و التعرف عليهم.

4- جمع و مركزة كل المعلومات و إستغلالها من اجل الكشف عن الجرائم المعلوماتية.

5- المشاركة في حملات التوعية حول مخاطر تكنولوجيا الإعلام و الإتصال.

6- تزويد السلطات القضائية و مصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات و المعطيات المتعلقة بالجرائم المعلوماتية.

إذًا وبالنظر إلى تشكيلة و المهام الملحقة بهذه المديرية فإنه يمكن وصفها بأنها المركز العملياتي للهيئة بما أنها تتولى الجانب التقني الخاص بإنجاز الأعمال المتعلقة بالبحث والتحقيق في الجرائم المعلوماتية و لعل أن ما يزيد من دورها الفعال هو تنصيبها على رأس مركز العمليات التقنية و كذلك الملحقات مما يبرز دورها الفعال في تسيير و تأطير الأعمال المتعلقة بالوقاية أوبمكافحة الجرائم المعلوماتية[1].

[1]_المواد 11 ،13 ،14 ،18 ،21 من المرسوم الرئاسي 261/15 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإتصال والإعلام ومكافحتها،المرجع السابق.

_ثانيًا: مديرية التنسيق التقني :

لم ينص المرسوم الرئاسي 261/15 على مديرية التنسيق التقني مما يترك المجال للقول بأنها تشكيلتها تكون بناء على قرارات مشتركة بين وزراء العدل و الدفاع و الداخلية على شاكلة مديرية المراقبة الوقائية و اليقظة الإلكترونية ، غير أنها تختلف عنه من حيث المهام الموكلة إليها ، فتتمثل مهامها أكثر في الدور الوقائي و الإعلامي من خلال توليها على :

1 – إنجاز الخبرات القضائية في مجال إختصاص الهيئة.

2– تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي.

3– إعداد الإحصائيات الوطنية للإجرام المعلوماتي.

4– تسيير المنظومة المعلوماتية و إدارتها[1].

إذًا فمن خلال إستعراض الهيكل العام للهيئة و مجمل إختصاصاتها، يتضح لنا جلياً مدى إقتناع الهيئة التشريعية بضرورة تفعيل دور الهيئة في مجال الوقاية و مكافحة الجرائم المعلوماتية ولو بشكل متأخر، نظراً لتوسع تطبيقات تقنية المعلوماتية في المجتمع الجزائري على الصعيدين الحكومي والإجتماعي، و هو ما ينبئ بتنامي الإجرام المعلوماتي وإزدياد حجم التهديدات التي يشكلها على سلامة الأنظمة المعلوماتية وأمن المعطيات المخزنة و المتداولة عبرها.

المطلب الثاني:الوحدات التابعة لسلك الأمن الوطني.

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة ، كافة الإمكانيات البشرية و التقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم و بالخصوص تلك

[1] _المادة 12 من المرسوم الرئاسي 261/15 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإتصال والإعلام ومكافحتها،المرجع السابق.

المستحدثة منها كالجرائم المعلوماتية،و التي تعتبر نتاج التطور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والإتصال ، و ذلك بهدف حماية المصلحة العامة و كذلك المصالح الخاصة المرتبطة بإستعمال هذا النوع من التكنولوجيات.

الفرع الأول:على مستوى المديرية العامة.

بادرت المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية بغية خلق وحدات متخصصة تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها ، ولذلك قامت المديرية العامة للشرطة القضائية بإستحداث أربع 04 مصالح مختصة في شكل نيابة مديرية و هي:

- ✓ نيابة مديرية الشرطة العلمية.
- ✓ نيابة مديرية الإقتصادية و المالية.
- ✓ نيابة القضايا الجنائية.
- ✓ مصلحة البحث و التحليل.

وفيما يتعلق بمكافحة الجريمة المعلوماتية فقد أسندت المهمة لنيابة مديرية الشرطة العلمية والتقنية هذه الأخيرة التي تضع لخدمة هذا الهدف مصالح عملية مختصة بذلك،تتولى أعمال البحث و التحري والتحقيق بشأن الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، و هذه الوحدات هي:

- ✓ المخبر المركزي للشرطة العلمية و الكائن مقره بالجزائر العاصمة.
- ✓ المخبر الجهوي للشرطة العلمية– قسنطينة.
- ✓ المخبر الجهوي للشرطة العلمية – وهران.
- ✓ المخبر الجهوي للشرطة العلمية –بشار.
- ✓ المخبر الجهوي للشرطة العلمية –تمنراست.

بالإضافة إلى مخابر أخرى قيد الإنجاز ورقلة مثلًا ينتظر تسليما قريبًا لأجل تعميم هذا النوع من النشاط على كافة ربوع الوطن[1].

يتولى كل مخبر سواء المركزي أو الجهوي لولاية قسنطينة أو وهران، مهام البحث والتحقيق و تحليل الأدلة الجنائية بمختلف أنواعها ، و لأجل ذلك يضم كل مخبر دائرتين هما:

أولًا:الدائرة العلمية

تتولى أعمال البحث والتحقيق و تحليل الأدلة المتصلة بالمجال البيولوجي و الطب الشرعي و الكيمياء و المخدرات ، وكذلك تلك المتعلقة بمجال التسميم و الحريق والمتفجرات كل منها على مستوى مخبر خاص.

ثانيًا: الدائرة التقنية

وتتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة و القذائف بمختلف أنواعها، وكذلك جرائم التزوير، إضافة إلى الجرائم المعلوماتية، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى.

[1] ـ في سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية ،خلقت المديرية العامة للأمن الوطني سنة 2010 ما يقارب 25 خلية لمكافحة الجرائم المعلوماتية موزعة على النحو التالي 8 : خلايا على مستوى الشرق، 8 خلايا على مستوى ولايات الوسط ، 6 خلايا على مستوى ولايات الغرب، 1 خلية على مستوى ولايات الجنوب لتقوم بعدها المديرية العامة بتعميم الخلايا هذه على جميع أمن ولايات الوطن، تعمل على رصد و كشف هذا النوع من الجرائم و تحويل مسائل البحث و التحقيق المعقدة تقنيا بشأنها إلى المخابر المركزية و الجهوية للشرطة العلمية ، و قدأحصت المديرية العامة للأمن الوطني في ال 10 أشهر الأولى من سنة 2015 مايقارب 410 قضية معالجة تورط فيها 347شخص . أنظر في ذلك : عبد الرحمان حملاوي،دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية،بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة،16و17نوفمبر2015،كلية الحقوق ، جامعة بسكرة، الجزائر، ص10،09.

الفرع الثاني:على المستوى الجهوي :

يضم المخبر الجهوي للشرطة العلمية مخبراً خاصا بتولي أعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية ، و ذلك تحت تسمية" **دائرة الأدلة الرقمية والآثار التكنولوجية** "و التي لم تكن عند إستحداثها سنة 2004 سوى قسم ،غير أن الإرتفاع الملحوظ لعدد القضايا الناتجة عن الجرائم المعلوماتية بسبب الإنتشار المتزايد لتقنية المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية هي:

- قسم إستغلال الأدلة الرقمية الناتجة عن الحواسيب و الشبكات.
- قسم إستغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات ينشط هذا القسم على مستوى المخبر المركزي بالجزائر العاصمة .

تضم الدائرة في صفوفها ثمانية 08 أعضاء محققين أربعة 04 منهم أعوان شرطة رسميون يتمتعون بصفة ضابط شرطة قضائية ، والبقية هم أعوان شبيهون، يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي ، إضافة إلى إلمامهم بالجانب القانوني ، و مما يزيد من فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث والتحقيق في الجرائم المعلوماتية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الإطلاع على كل المستجدات القانونية منها و التقنية في مجال الإجرام المعلوماتي[1].

ومن مهام هذا المخبر ضمان الدعم التقني لمختلف مصالح الشرطة و الأجهزة القضائية في مجال التحريات الالكترونية ، و ذلك من خلال القيام بعمليات البحث عن المعطيات المشبوهة و المعلومات الرقمية على مختلف أشكالها : ملفات، رسائل إلكترونية،

[1] –عبد الرحمان حملاوي،المرجع السابق.

برامج، صور، هذا البحث يتم عن طريق إستعمال برامج ووسائل خاصة تمكن من إسترجاع كل المعطيات المحذوفة، و الإطلاع على محتوى كل الوسائط الرقمية.

تلعب الدائرة دورًا مهمًا للغاية في الكشف عن أسرار الجرائم المعلوماتية ، من خلال مختلف الإجراءات التي تباشرها إما أثناء مرحلة البحث والإستدلال ، أو أثناء مرحلة التحقيق القضائي.

فأما أثناء مرحلة البحث و التحري فإن أعضاء الدائرة عادة ما يستجيبون للطلبات التي يقدمها لهم أعوان الشرطة التابعون لخلايا مكافحة الجرائم المعلوماتية الموزعة على كل مديريات الأمن الوطني، أولطلبات وكيل الجمهورية أو قاضي التحقيق التي تردهم في شكل إنابة قضائية ، من أجل دعمهم و مساعدتهم أثناء مرحلة المعاينة لمسرح الجريمة و كذلك لحجز الأدلة المتواجدة عليها.

أما أثناء مرحلة التحقيق القضائي فإن دور الدائرة لا يتعدى لأن يكون دور خبير ذلك من خلال إعداد تقارير خبرة بناءًا على طلبات وكيل الجمهورية وبالخصوص قاضي التحقيق ، كنتيجة لقيام المحققين بأعمال تحليل الأدلة المحجوزة و العمل على إستخراج الأدلة الإلكترونية منها كتحليل محتوى الأقراص الصلبة للحواسيب المستعملة في الجريمة ، أو حواسيب الضحايا ، و كذلك كل دعامات التخزين الإلكترونية بمختلف أنواعها وأشكالها و كذلك المواقع التي تم إختراقها و إستهدافها وصولًا إلى تحديد المواقع الجغرافية وعناوين المجرمين ، و ذلك بالإستعانة بوسائل مادية خاصة منها حواسيب متطورة ذات عالية[1] .

إضافة إلى أجهزة أخرى كأجهزة التخزين مهما كان نوعها ، و عمل نسخة طبق الأصل عنها من أجل العمل عليها بالتحليل و ذلك حفاظًا على النسخة الأصلية من أي

[1] –عاقلي فضيلة،الجريمة الإلكترونية وإجراءات موجهتها من خلال التشريع الجزائري ،بحث مقدم إلى أعمال الملتقى الدولي الرابع عشر بطرابلس،24و25مارس2017،جامعة باتنة1،ص131،132.

تحريف أو فقدان إضافة إلى وسائل برمجية أخرى تتمثل في برامج التتبع الإلكتروني لتحديد موقع الهجوم ، أو برامج إعادة بناء المعلومات بعد حذفها أو تخريبها، و هي كلها برامج خاصة موضوعة تحت تصرف أعضاء الدائرة لخدمة أعمال البحث والتحقيق عن الأدلة الإلكترونية، التي عادة ما تختتم بإعداد تقارير خبرة تقدم لقضاة التحقيق أو لقضاة الحكم في أبسط شكل ممكن حتى يتم إستيعاب مضمونها و الإستناد عليها لتسبيب الأحكام والقرارات.

و بالرجوع إلى المعطيات الإحصائية المقدمة فإن سنة 2014 شهدت ما يقارب 250قضية محل تحقيق من قبل أعضاء الدائرة ، أبرزها قضيتان وردتا على سبيل الإنابة القضائية الدولية و بالتحديد عن طريق مكتب الأنتربول تتعلق كلاهما بقيام شابين من ولاية قسنطينة بالإعتداء على الأنظمة المعلوماتية الخاصة بموقع وزارة الخارجية الكويتية و تعطيله ، و كذلك القيام بجريمة إحتيال إلكتروني على أهداف بالولايات المتحدة الأمريكية، أما فيما يخص الثلاثي الأول لسنة 2015 فإنه تم تسجيل 60 قضية طرحت أمام محققي دائرة الأدلة الرقمية و الأثار التكنولوجية للنظر فيها ، تتعلق أغلبها بسوء إستخدام مواقع التواصل الإجتماعي من خلال قضايا المساس بالأشخاص في صورة الإبتزاز و القذف والتشهير[1].

و في الأخير فإن ما يمكن قوله بهذا الخصوص أن المديرية العامة للأمن الوطني تولي أهمية بالغة في مجال مكافحة الإجرام المعلوماتي ، غير أنها و بالنظر إلى الدول الأجنبية الأخرى لا تزال متأخرة بعض الشيء من حيث قلة عدد وعتاد هذه الوحدات هذا من جهة، إضافة إلى العقبات التشريعية التي تحد من عمل أعضاء هذه الوحدات كشرط الحصول على تسخيرة من قبل الجهات القضائية المختصة لأجل الإنطلاق في أعمال البحث والتحقيق المعلوماتي ولو وصل إلى علم أعضائها تبليغات من قبل الضحايا أنفسهم ، أو معلومات

[1] –عاقلي فضيلة،المرجع السابق،ص132.

بوقوع جريمة معلوماتية ، و هو ما يضيق من مجال عملهم ويحد من مدى فعاليتهم في دعم أعمال البحث والتحقيق نظراً لطول مدة إستيفاء الإجراءات القانونية و ما يصاحبها من فقدانٍ للأدلة الإلكترونية[1] ، نظراً لقدرة الجاني على التخلص من أثارها ومحوها قبل وصول أيدي هؤلاء إليها ، وهو ما يدعونا إلى لفت إنتباه القائمين على شؤون مؤسسة الأمن الوطني بالتنسيق مع الجهات القضائية إلى ضرورة مطالبة المشرع لوضع نصوص ملائمة تمنح حرية أكبر في مسائل مباشرة الإجراءات الخاصة بالمتابعة والتحقيق في الجرائم المعلوماتية ،نظراً لسرعة تنفيذ و محو أدلة هذه الأخيرة.

المطلب الثالث:الوحدات التابعة للدرك الوطني الجزائري.

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن و النظام العام و محاربة الجريمة بكافة انواعها، وحدات متنوعة و عديدة على مستوى القيادة العامة ، أو على مستوى القيادات الجهوية والمحلية و هي تباعًا:

- ✓ قيادة الدرك الوطنية.
- ✓ الوحدات الإقليمية.
- ✓ الوحدات المشكّلة.
- ✓ وحدات الإسناد .الوحدات المتخصّصة.
- ✓ هياكل التكوين.
- ✓ المعهد الوطني للأدلّة الجنائية وعلم الإجرام.
- ✓ المصالح المراكز العلمية والتقنية.
- ✓ المصلحة المركزية للتحريات الجنائية.

[1] -بحث مقدم من طرف قيادة الرك الوطني:مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة16و17 نوفمبر2015،الجزائر،ص4،5.

✓ المفرزة الخاصّة للتدخل[1].

تعمل مؤسسة الدرك الوطني جادة إلى التطلع بمختلف الجرائم المرتكبة على شبكة الإنترنت و هذا لتسهيل مهمة البحث و المعاينة و التفتيش في أنظمة الحواسيب و العمل على مراقبة مختلف الشبكات، و بالتالي فقد تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، و ذلك حسب الإختصاص و الصلاحيات وطبيعة الجريمة إلى ثلاث 03 مستويات مركزية، جهوية ، محلية.

الفرع الأول:على المستوى المركزي.

تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم المعلوماتية و دعم أعمال البحث والتحقيق بشأنها من خلال الهيئات التالية:

أولًا: مديرية الأمن العمومي و الإستغلال :

وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية و المركز التقني العلمي، في مجال أعمال البحث و التحري في الجرائم المعلوماتية.

ثانيًا :المصلحة المركزية للتحريات الجنائية :

وهي هيئة ذات إختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام و الإتصال.

ثالثًا : المعهد الوطني للأدلة الجنائية و علم الإجرام:

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام، مؤسسة عمومية ذات طابع إداري تم إنشاؤه بمرسوم رئاسي رقم 183/04[2] بتاريخ 26جوان2004 في إطار عصرنة قطاع الدرك

---

[1] _ الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 مارس 2017 الرابط الإلكتروني :
http://www.mdn.dz/site_cgn/index.phpL=ar&P=undefined

[2] _ المرسوم الرئاسي رقم 04/ 183 الصادر 27 يونيو 2004، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 41،ص18.

الوطني، وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية و التحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، يعد المعهد بمثابة هيئة مختصة في إجراء الخبرات و المعاينة و ذلك بمختلف دوائره ، بما فيها "**دائرة الإعلام الآلي والإلكترونيك**" ،التي أوكلت لها مهام تحليل الأدلة الخاصة بالجرائم المعلوماتية ، و ذلك بتحليل الدعامات الإلكترونية وإصلاح الدعامات التالفة ، إنجاز المقاربات الهاتفية ، تحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل إستغلالها.

إن الخدمة الاساسية التي يقدمها هذا المعهد هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية ، ولهذا فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يساهم بشكل فعال في مكافحة الجرائم المعلوماتية من خلال مهامه الخاصة بمتابعة أو دعم إجراءات البحث والتحقيق في الجرائم المعلوماتية فهو يتولى في هذا الشأن:

- القيام بالخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح، بما فيها تلك المتعلقة بالجرائم المعلوماتية.
- مساعدة المحققين للسير الحسن للمعاينات، عن طريق دعمهم الأفراد المؤهلين أثناء الحاجة.
- تنفيذ مناهج الشرطة العلمية و التقنية لجمع وتحليل الأدلة المأخوذة من مسرح الجريمة.
- ضمان المساعدة العلمية في التحريات المعقدة كحال التحريات الخاصة بالجرائم المعلوماتية.
- المشاركة في الأبحاث والتحاليل المتعلقة بالوقاية للتقليل من جميع أشكال الإجرام بما فيها المعلوماتي.
- مشاركة ومساهمة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المكلفة بالتحاليل والخبرات في ميدان علم الإجرام في وضع سياسة مكافحة الإجرام[1].

[1]_الموقع الرسمي لقيادة الدرك الوطني تاريخ التصفح 31 مارس 2017.

رابعًا : مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية :

أنشئ هذا المركز حديثا ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية، إذ يوفر المساعدة التقنية للمحققين ويساهم في توجيه التحقيقات المرتبطة بتكنولوجيا الإعلام و الإتصال ، فهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي و الإستعمال لقيادة الدرك الوطني[1] و يحقق المهام التالية:

1_ ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت.

2_ القيام بمراقبة الإتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني و الجهات القضائية.

3_ مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والإتصال و البحث عن الأدلة في شبكة الأنترنت.

4_المشاركة في عمليات التحري والتسرب عبر شبكة الأنترنت لفائدة وحدات الدرك الوطني و السلطات القضائية.

5_ المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

الفرع الثاني:على المستوى الجهوي.

[1]_عالج هذا المركز في ال 10 أشهر الأولى من سنة 2015 ما يقارب 240 قضية متعلقة بالجرائم المعلوماتية ، تنوعت بين جرائم التهديد، المساس بالنظام العام، جرائم الإختراق، التحرش الجنسي بالقصر و تحريضهم على الفسق و الدعارة، إهانة هيئات و رموز وطنية ، النصب و الإحتيال، الإعتداء على حرمة الحياة الخاصة . أنظر في ذلك : عز الدين –قيادة الدرك الوطني –الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها – بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة 16 و 17 نوفمبر 2015 كلية الحقوق ، جامعة بسكرة، الجزائر ص29.

تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بمهمة تنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية و كذلك دعمها بالوسائل الخاصة للتحريات و الأبحاث المعقدة كالجرائم المعلوماتية.

يلعب الدرك الوطني دورًا هامًا في ميدان الشرطة القضائية نظراً لإنتشار وحداته على مستوى كامل التراب الوطني، ونظراً للوسائل المادية الموضوعة تحت تصرفه وعدد أفراده الهائل والصلاحيات التي خولها لهم القانون ، وهم في الواقع حسب الرّتب والوظائف ضباط وأعوان الشرطة القضائية.

الفرع الثالث:على المستوى المحلي.

يحوز الدرك الوطني على فصائل للأبحاث التي ينتمي إليها أفراد ذوي خبرة وإختصاص واسعين في ميدان الشرطة القضائية، هذه الفصائل مكلفة خصيصًا لمكافحة الأشكال الخطيرة للإجرام المنظم كالجرائم المعلوماتية ، وذلك عن طريق القيام بتحقيقات تتطلب تحريات معقدة ، هذه الوحدات المختصة تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني.

وأعيد تنظيم فرقة الدرك الوطني بتاريخ 21 جويلية 2007 بموجب التعليمة رقم 4-223-2007 الصادرة عن ديوان قيادة الدرك الوطني ، و ذلك للتماشى مع طبيعة الجرائم محل المعاينة ، و هو ما سمح بإنشاء خلية متخصصة لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام و الإتصال في سبعة عشر مجموعة ولائية ، و هو ما يسمح بتطبيق سياسة فعالة في مكافحة الجرائم المعلوماتية من خلال توفير الخلايا المتخصصة في مجال أعمال البحث والتحقيق في هذا النوع من الجرائم[1].

[1]_معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني – سعيدة -الجزائر.

إن كل المعطيات التي إستعرضناها في هذا المبحث توضح وبشكل جلي مدى تكاثف و تعزيز الجهود المتعلقة بترقية و دعم أعمال البحث والتحقيق بشأن الجرائم المعلوماتية ، من خلال تصنيفها على حدى وتخصيص أجهزة أمنية خاصة بمباشرة الأعمال المتعلقة بالبحث والتحقيق بشأنها وذلك نظراً لخصوصيتها من جهة ولخصوصية مرتكبيها وأدلتها من جهة أخرى ، غير أن الملاحظ بشأن ذلك هو مدى التفاوت الحاصل بين الجهود المبذولة والنتائج المحصلة في هذا المجال فعلى المستوى الإقليمي الأوربي فإننا نلاحظ مدى الإهتمام بترقية ودعم مجال أعمال البحث والتحقيق في الجرائم المعلوماتية من خلال حجم الوحدات ذات الإختصاص الدولي و الإقليمي و الداخلي ، التي أصبحت تعمل على مكافحة هذا النوع من الجرائم ، عكس ذلك هناك شبه غياب للتعاون على المستوى الإفريقي و العربي بهذا الخصوص ، و ذلك راجع أساسًا إلى ضعف الإمكانيات المادية و البشرية في هذا المجال بالرغم من الإنتشار الفائق لتقنية المعلوماتية ، وهو ما ينعكس على معدلات تنامي الإجرام المعلوماتي في هذه الدول و إزدياد عدد حالاتها.

المبحث الثاني:الإجراءات الخاصة المتبعة في إطار البحث والتحقيق المعلوماتي.

مما لاشك فيه أنه لا يوجد ما يسمى بالجريمة الكاملة مهما حاول الجاني إخفائها و ذلك إستنادا لقاعدة " **لوكارد**[1]" لتبادل المواد، التي تنص على أنه عند إحتكاك جسمين يبعضهما البعض فإنه لابد أن ينتقل جزء من الجسم الأول إلى الثاني والعكس كذلك

[1] - Le principe d'échange de Locard, énoncé pour la première fois par EdmondLocard en 1920 s'applique au lieu du crime, à l'auteur, à lavictime, il peuts'exprimer de la manière suivante :-l'auteur et/ou son matériel abandonnent des indices sur la victime et sur la scènede crime. L'auteur et /ou son matériel emportent des indices appartenant a la victime et a lascène de crime. Plus d'information voir :
-Jean Claude martin – investigation de scènes de crimes -fixation de l'état lieux et traitement des traces d'objet- presse polytechnique et des universitaireRomandes- France- 2004. P 08.

وبالتالي ينتج عن هذا الإحتكاك الدليل الجنائي ، وفي مجال الجريمة المعلوماتية ينتج لدينا ما يعرف بالدليل الالكتروني أو ما يطلق عليه بالدليل الرقمي[1].

ونظراً لطبيعة الجرائم المعلوماتية الخاصة فإنها تتطلب إجراءات وأساليب خاصة ونوعية للبحث والتحقيق، لأجل اكتشاف الدليل الرقمي و تحصيله من قبل الفنيين المختصين، وكل ذلك يستدعي إتخاذ إجراءات سريعة[2] .

إجراءات البحث التحقيقي الجنائي العام هي الأساس في البحث والتحقيق في جرائم المعلوماتية تماماً كما هو الحال في باقي الجرائم الأخرى، أما عناصر البحث والتحقيق الجنائي الأخرى من عملية و فنية و غيرها فإن إستخدامها يتوقف على ظروف كل جريمة فالملاحظ أن إجراءات التحقيق في الجرائم المعلوماتية تتصف بالخصوصية من حيث طريقة كشفها والتبليغ عنها، والعناية بمسرح الجريمة وكيفية تكوين فريق الضبط والتفتيش، وصولًا إلى خصوصية التعامل مع الأدلة الجنائية[3].

وعليه سوف نقسم هذا المبحث إلى ثلاثة مطالب في المطلب الأول نتناول الشروط الخاصة بالمحقق في الجرائم الإلكترونية، والمطلب الثاني الإجراءات الخاصة بالبحث والتحري في الجرائم المعلوماتية، أما المطلب الثالث الإجراءات الفنية لمعاينة مسرح الجريمة الإلكترونية.

المطلب الأول: الشروط الخاصة بالمحقق في الجرائم الإلكترونية.

لا تجيز الجريمة المعلوماتية وبحكم خصوصيتها وطبيعتها، لأي كان من جهات الضبطية القضائية أو جهات التحقيق أو النيابة العامة أمر البحث والتحقيق بشأنها، فهي

---

[1] _عائشة بن قارة،حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة الجديدة ، الإسكندرية ، مصر، 2010،ص78.

[2] _عبد الله بن سعود محمد السراني، المرجع السابق،ص65.

[3] _ –ضياء علي أحمد النعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى،المطبعة الوطنية، المملكة المغربية ، 2001،ص363.

جريمة تستلزم محققًا من نوع خاص قادر على التعامل مع مميزاتها بالشكل اللّازم الذي يسمح له بمعرفة هوية مرتكبها و تحديد معالمها وآثارها، وذلك من خلال تتبع آثارها الإلكترونية ودلائلها، كل ذلك في إطار الشرعية الإجرائية، تجنبا لطائلة البطلان وإحترام الحقوق وحريات الأفراد.

إن الإجراءات الخاصة بالبحث والتحقيق في مجال الجرائم المعلوماتية، المحددة وفق القواعد العامة لقانون الإجراءات الجزائية أو بعض القوانين الأخرى المكملة له على شاكلة القانون09 /04[1] المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال وسبل مكافحتها، سواء تلك المتعلقة بالإختصاص النوعي والإقليمي، تعتبر في مجملها قاصرة في مجال تحديد الصفات الملائمة لرجال البحث والتحقيق في الجرائم المعلوماتية وذلك بسبب وجوب توفر شروط أخرى خاصة في شخص المحقق ذاته حتى يكون على إستعداد لمواجهة تحديات الجرائم المعلوماتية، و هي الشروط المتعلقة بالمعرفة الفنية للنظم المعلوماتية ، و التي تعتبر مكملًا أساسيًا لجملة الشروط القانونية التقليدية، وهو ما سنستعرضه في الفرعين المواليين اللذان خصصنا أولهما لتحديد الشروط القانونية المشترطة في شخص المحقق المعلوماتي، و ثانيهما لجملة الشروط المعرفية والفنية بالنظم المعلوماتية التي يجب أن يحيط بها المحقق حتى يحسن التعامل مع الجريمة المعلوماتية.

الفرع الأول:الشروط المتعلقة بالإختصاص القضائي.

تعتبر شروط الإختصاص القضائي من مسائل النظام العام التي يمكن إثارتها في أي مرحلة كانت عليها الدعوى فتتعرض الإجراءات برمتها للبطلان في حال عدم إستيفائها، و شروط الإختصاص في مسائل البحث والتحقيق نوعان اختصاص نوعي وآخر إقليمي محلي، فلا يمكن لمن يتولى أعمال البحث والتحقيق مباشرة أعماله و هو غير مختص نوعا ، كما لا

[1] –القانون04/09،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام، المرجع السابق.

يمكن لمن يتولى الإجراءات نفسها وهو يتمتع بصفة الإختصاص النوعي ممارسة أعماله خارج نطاق إختصاصه الإقليمي[1].

البند الأول :تحديد مفهوم شروط الإختصاص النوعي في مسائل الجريمة المعلوماتية.

تعتبر إجراءات البحث والتحقيق من الإجراءات التي تمس بحقوق وحريات الأفراد ولذلك فقد حرص المشرع الجزائري على إسنادها لجهة قضائية لأجل ضمان كفالة حقيقية لجملة الحقوق و الحريات الفردية، و تتمثل عادة هذه الجهة القضائية في هيئة الضبطية القضائية إذا كانت الإجراءات المتعلقة بمرحلة البحث والتحري ، وفي هيئة قضاء التحقيق إذا كانت الإجراءات متعلقة بمرحلة التحقيق القضائي ممثلة في شخص قاضي التحقيق.

و كما سبق وأن وضّحنا سابقًا فإن الإختصاص العملي و الفني في مجال أعمال البحث والتحقيق في الجرائم المعلوماتية يعود وبالدرجة الأولى إلى دائرة مكافحة الجرائم المعلوماتية التابعة للمديرية العامة للأمن الوطني، وكذلك الفرق التابعة لمركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابعة لسلك الدرك الوطني، و إلى مديرية المراقبة الوقائية واليقظة الإلكترونية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها و تحت إشرافها والتي تم الإعلان عنها رسميا بموجب صدور المرسوم الرئاسي رقم261/15 [2]المؤرخ في 8 أكتوبر 2015 هذه الوحدات الخاصة تتكون أساسا من جملة من المستخدمين يتولى ممن تتوفر لديهم صفة ضباط للشرطة القضائية مباشرة إجراءات البحث والتحقيق في الجرائم المعلوماتية، إما من تلقاء أنفسهم أو

[1] ـ راجع المادة 40 من الأمر 155/66 المؤرخ في 8 يونيو 1966 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري،الجريدة الرسمية رقم48،ص04.

[2] – المرسوم الرئاسي 261/15 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإتصال والإعلام ومكافحتها،المرجع السابق.

بناء على طلبات وأوامر تردهم من قبل وكيل الجمهورية أو قاضي التحقيق ، مما يجعل منهم العنصر البارز في متابعة هذه الإجراءات بصفة فعلية دون غيرهم.

البند الثاني :إختصاص ضباط الشرطة القضائية بالبحث والتحري

يتولى عادة ضباط الشرطة القضائية مسائل البحث والتحري في كافة الجرائم ، بما في ذلك الجرائم المعلوماتية فلا يوجد مانع قانوني يحد من ممارسة هؤلاء لأعمالهم المتعلقة بالبحث والتحري في مجال الجرائم المعلوماتية بعد تبليغهم بوقوعها، سوى أن يتوفر فيهم شرط الإختصاص النوعي والذي يمكن تحديده في التمتع بصفة ضابط الشرطة القضائية، وذلك تقيدا بما تفرضه نص المادة 05 من الفصل الثالث المتعلق بالقواعد الإجرائية الخاصة بتفتيش النظم المعلوماتية الوارد في نص القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال وسبل مكافحتها و التي تنص على أنه" يجوز للسلطات القضائية المختصة وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية ...الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها" .

وبناءًا على ذلك فإن الأشخاص المذكورين في نص المادة 15 من قانون الإجراءات الجزائية الجزائري، والتي تحدد قائمة حصرية لصفة الأشخاص المنوط بهم هذه الصفة، هم الأشخاص المخولون قانونًا بمباشرة أعمال البحث وتنفيذ أوامر التحقيق بشأن الجرائم المعلوماتية[1].

---

[1] _جاء في نص المادة 15 من قانون الإجراءات الجزائية الجزائري المعدلة بموجب الأمر15 2015انه ": يتمتع بصفة ضابط الشرطة القضائية:

- رؤساء المجالس الشعبية البلدية.
- ضباط الدرك الوطني.
- الموظفون التابعون للأسلاك الخاصة المراقبين و محافظي و ضباط الشرطة للأمن الوطني.

إذًا فمن أجل حق ممارسة أعمال البحث والتحري (التحقيق الإبتدائي) في الجرائم المعلوماتية، فإن الشرط الأساسي هو التمتع بصفة ضابط الشرطة القضائية وذلك حسب ما هو وارد في هذا الشأن بموجب المادة63 من القانون 22/06 قانون الإجراءات الجزائري بقولها:"يقوم ضباط الشرطة القضائية ، وتحت رقابتهم أعوان الشرطة القضائية ، بالتحقيقات الإبتدائية بمجرد علمهم بوقوع الجريمة إما بناء على تعليمات وكيل الجمهورية أو من تلقاء انفسهم . "[1].

كما يجوز لضباط الشرطة القضائية القيام بكل أعمال التحقيق القضائي اللازمة لكشف الحقيقة في مجال الجرائم المعلوماتية ، إذا ما تعذر على قاضي التحقيق القيام بها بنفسه ، وذلك بعد ندبهم من قبل هذا الأخير حسب الشروط القانونية المنصوص عليها في المواد من 138 إلى 142 من قانون الإجراءات الجزائية ، و على قاضي التحقيق عند إنتهاء هؤلاء من أعمالهم مراجعة عناصر التحقيق.

ولقد أجاز المشرع حسب مضمون البند الأخير من المادة 05 من القانون 04/09[2] المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وسبل مكافحتها ، وفي سبيل تخطي عقبات إنعدام المعرفة الفنية بالنظم المعلوماتية من قبل ضابط الشرطة القضائية لهؤلاء أن يقوموا بتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث بقصد

•ذوو الرتب في الدرك، و رجال الدرك الذين أمضوا في سلك الدرك ثلاث سنوات غلى الأقل و الذين تم تعينهم بموجب قرار مشترك بين وزير العدل ووزير الدفاع الوطني ، بعد موافقة لجنة خاصة.

•الموظفون التابعون للأسلاك الخاصة للمفتشين و حفاظ و أعوان الشرطة للأمن الوطني الذين أمضوا ثلاث03 سنوات على الأقل و عينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية و الجماعات المحلية بعد موافقة لجنة خاصة.

•ضباط و ضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر بين وزير الدفاع و وزير العدل."

[1] _ المادة 63 من قانون الإجراءات الجزائية الجزائري،المؤرخ في 20ديسمبر2006،الجريدة الرسمية رقم84.

[2] – القانون04/09،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام، المرجع السابق.

مساعدتهم وتزويدهم بكل المعلومات الضرورية لإنجاز مهامهم دون أن تتعرض الإجراءات المتخذة للبطلان ،وهو ما أكدته المادة 65 مكرر8 من القانون 22/06 من قانون الإجراءات الجزائية.

البند الثالث :الإختصاص النوعي للجهات القضائية (النيابة العامة – قضاء التحقيق).

أولا :جهة النيابة العامة :

تعتبر النيابة العامة السلطة المختصة بمباشرة الدعوى العمومية باسم المجتمع و تتولى مهمة المطالبة بتطبيق القانون، ويتولى النائب العام مهمة تمثيل النيابة العامة أمام المجالس القضائية، فيما يمثلها لدى المحكمة وكيل الجمهورية أو أحد مساعديه وتتولى النيابة العامة ممثلة في شخص وكيل الجمهورية إدارة نشاط الضبطية القضائية كما يتمتع هو نفسه بكافة السلطات والصلاحيات المرتبطة بصفة ضابط شرطة قضائية، فيتولى مباشرة أو الأمر بمباشرة جميع الإجراءات اللازمة للبحث و التحري عن الجرائم بما في ذلك الجرائم المعلوماتية.

وله في حال مباشرة الإجراءات الخاصة بالبحث والتحري في الجرائم المعلوماتية حسب أحكام المادة 35 مكرر من قانون الإجراءات الجزائية المستحدثة بموجب الأمر 02/15 المؤرخ في 23 جويلية 2015[1]، ومضمون البند الأخير من المادة 5 من القانون 04/09المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وسبل مكافحتها، أن يستعين بمساعدين متخصصين في مجال المعلوماتية تحت مسؤوليته ،من أجل مساعدته في المسائل الفنية المتعلقة بالجريمة محل المتابعة، وذلك بعد إطلاعهم على ملف الإجراءات المتخذة، وبعد أداءهم القسم المتعلق بالحفاظ على سرية المعلومات ،يقدمون

[1] –الأمر02/15 المعدل والمتمم للأمر155/66 المتضمن قانون الإجرااات الجزائية،المؤرخ في2015/07/23،الجريدة الرسمية رقم 40،ص30

أعمالهم في شكل تقارير تلخيصية أو تحليلية تتضمن النتائج المتوصل إليها بناء على إلتماسات النيابة العامة .

ثانيًا :إختصاص جهة التحقيق :

يختص قاضي التحقيق بإجراءات البحث والتحري إختصاصًا أصيلًا حسب ما تقتضي به المادة 38 الأمر 75/69 قانون الإجراءات الجزائية ويختص بالتحقيق في الجرائم إما بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و 73 من نفس القانون.

ووفق ما تنص عليه المادة 68 من قانون الإجراءات الجزائية يقوم باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الإقناع وأدلة النفي، وإذا كان من المتعذر عليه القيام بها بنفسه جاز له أن ينيب ويندب ضابط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشروط المنصوص عليها قانونا حسب المواد 138 إلى 192 قانون الإجراءات الجزائية، بما في ذلك الجرائم المعلوماتية، بما أن النص كان عامًا وشاملاً ولم يهدف بالتحديد والتخصيص لنوع الجرائم الجائز التحقيق فيها[1].

البند الرابع:الإختصاص الإقليمي في مجال الجرائم المعلوماتية.

تعتبر الجريمة المعلوماتية نوعا خاصا من الجرائم فهي لا تعترف بمبدأ الإقليمية ولا بالحدود الجغرافية ، فهي بمفهومها وطابعها الدولي قد قلبت مفاهيم الإختصاص الاقليمي للنص الجنائي و كذلك الإجرائي ، فهي قد تقع في آن واحد وعلى مستوى عدة دول وذلك بسبب الطابع اللامادي للمعلومات وللمعطيات محل الجريمة، الذي نتج عنه مبدأ عدم

[1]_حسب ما تنص عليه الفقرة الأخيرة من المادة 05 من القانون 04/09 (المتعلق بالوقاية من الجرائم بتكنولوجيات الإعلام و الاتصال و سبل مكافحتها فإن قاضي التحقيق و في حال توليه إجراءات التحقيق بنفسه بشان الجريمة المعلوماتية فله أن يستعين بكل شخص له دراية بعمل المنظومة المعلوماتية محل التفتيش بقصد مساعدته على إنجاز مهمته.

إشتراط وقوع الجريمة المعلوماتية ضمن نطاق الإختصاص الإقليمي للنص الجنائي حتى ينشأ الحق في المتابعة والتحقيق،وهي كلها معطيات أثارت إشكاليات ماسة بالمسائل الإجرائية[1].

ومن الشروط التي يجب أن تتوفر في المحقق في الجرائم التقليدية صفة الإختصاص المكاني، أي أن لا يمارس إجراءات البحث والتحقيق خارج دائرة الإختصاص المكاني، وقد يمتد التحقيق في جريمة ما إلى ما خارج دائرة الإختصاص وفق ما يستلزم من ظروف التحقيق ومقتضياته، وتبقي بذلك الإجراءات صحيحة لا بطلان فيها.

إن إعمال الشروط التقليدية لقاعدة الإختصاص المكاني أمر لا مفر منه من أجل البحث والتحقيق في مجال الجريمة المعلوماتية، لكن كل ذلك غير كاف نظراً للطابع المميز لها، فهي بذلك تثير إشكالات عدة تجعل من اختصاص المحقق مكانيا غير مجد،نظراً لوجود محل البحث والتحقيق خارج نطاق الإختصاص الإقليمي المكلف به.

الفرع الثاني:المهارات الفنية لرجال البحث والتحقيق المعلوماتي.

عند الحديث عن المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المتعلقة بالمعلوماتية فإننا لا نقصد بها المهارات التقليدية التي يجب أن يتمتع بها المحقق فهي مهارات أساسية يفترض توافرها في المحقق بالضرورة، فمهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود تعتبر من أساسيات أعمال التحقيق الذي لا يتوقع أحد عدم توافرها لدى المحقق، ولذلك فالمهارات المقصودة عند رجال البحث والتحقيق المعلوماتي هي تلك المهارات التي تتسم بالحداثة في مجال تقنية المعلوماتي[2].

فمن الصعوبات التي تواجه رجال البحث والتحقيق المعلوماتي مسألة عدم التخصص ونقص الخبرة بصفة عامة، وذلك فيما يتعلق بثقافة الحاسوب وجرائم المعلوماتية وكيفية التعامل معها، وذلك بالخصوص في الدول العربية، نظراً لحداثة الإعتماد على النظم

---

[1] - Myriam Quéméner- Yves Charpenel - La Cybercriminalité - op.cit- p 159

[2] _حسين بن سعيد الغافري، "التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت"، بحث منشور على الموقع الإلكتروني الرسمي للمركز العربي للبحوث القانونية و القضائية للجامعة العربية، ص 02 ،تاريخ التصفح 2017/02/20.على الموقع الإلكتروني:www.carjj.org/node.

المعلوماتية مقارنة بأوروبا والولايات المتحدة الأمريكية، إضافة إلى الوقت الذي يستغرقه بتشكيل أجهزة مكافحة هذه الجرائم الذي يعتبر بطيئا مقارنة بنسق إنتشار الجرائم المعلوماتية، وهي الفوارق التي ينعكس أثرها سلبا على قيمة إجراءات البحث والتحقيق ،وهو ما يستدعي تأهيل سلطات البحث والتحقيق لأجل التحكم في هذه الجرائم.

إن إكتشاف هذه الجرائم والتوصل إلى فاعلها بملاحقتهم قضائيا لا يتطلب الإلمام بأصول البحث الجنائي وقواعد التحقيق القانونية فقط ،فهو أمر مفترض عملا بقاعدة الشرعية الإجرائية ولكن يجب كذلك الإلمام بأصول التحقيق الجنائي الفني في الجرائم المعلوماتية من خلال إكتساب مهارات خاصة تسمح بإستيعاب تقنيات الحاسوب من حيث برامجه وكيفيات إختراقه، ومصطلحاته ونفسية الجناة على إعتبار أنهم فئة خاصة يتعين التعامل معهم بأسلوب خاص[1].

ومن بين هذه المواصفات الخاصة التي تجعل من رجال البحث والتحقيق مختصين في مجال الجرائم المعلوماتيةنذكر ما يلي:

البند الأول:ضرورة التعرف على المكونات المادية للنظم المعلوماتية و عمل الشبكات.

يجب أن يحيط رجال البحث والتحقيق في مجال الجرائم المعلوماتية علما بالجانب النظري للنظم المعلوماتية، وذلك من خلال معرفة الجوانب التالية:

أولا :المكونات المادية للحاسوب :

يجب على المحقق التعرف على الشكل المعين للحواسيب وملحقاتها ومسمى كل منها، والهدف من إستخدامه، وذلك حتى يستطيع وضع إحتمالات توظيفه في المجال الإجرامي، فعدم معرفته بالمكونات المادية للحاسوب قد يؤدي به إلى إهمالها أو حتى إتلافها بدون قصد أو يتسبب في تدمير أو تعديل البيانات المخزنة عليه نتيجة الجهل به، بل يجب

[1] _عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية –دراسة مقارنة .على ضوء القواعد العامة للإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، مصر،2009 ،ص82،83.

عليه أن يلم بكيفية التعامل معها وملحقاتها كذلك بإعتبارها أدلة محتملة، وأن يحرص على عدم تعريضها لأي من المؤثرات الخارجية التي تؤدي إلى تدمير محتوياتها كالقوى المغناطيسية، وإكتساب هذه المهارات هو نتاج الدورات التدريبية كما هو الحال في الولايات المتحدة الأمريكية وكندا[1].

ثانيًا:أساسيات عمل شبكات الإتصال :

يتوجب على رجال البحث والتحقيق الجنائي المعلوماتي معرفة آليات عمل الشبكات المتصلة بالحاسوب، وخصوصا شبكة الأنترنت بإعتبارها شبكة دولية تربط بين ملايير الحواسيب عبر العالم فعليه أن يجيد التعامل والتحكم في مبادئ الإتصال الشبكي وأنواعه وكيفية إنتقال البيانات من جهاز لآخر، ومبادئ البروتوكولات الرسمية الخاصة بالإتصال بالشبكة وتبرز أهمية تحكم المحقق بمبادئ عمل الشبكات في كونها ضرورة لبناء تصور شامل عن كيفية إرتكاب الفعل الإجرامي المعلوماتي، إضافة إلى إعتراض البيانات أثناء إنتقالها عبر الشبكة والتجسس عليها وتحويل مسارها، كما أنها تمنحه أكثر من ذلك وهي إمكانية تتبع مصدر الإعتداء[2].

البند الثاني:تمييز أنظمة التشغيل الحاسوبية ومبادئ التعامل معها وشبكة الأنترنت:

لايكفي أن يكون المحقق على علم بالمكونات المادية للحاسوب فقط ،حتى يستطيع القول بأنه مؤهل للتحقيق في الجرائم المعلوماتية بل يجب عليه أن يحيط علما كذلك بكل الجوانب المنطقية للأنظمة الحاسوبية ويمكن إيجازها في:

أولا :تمييز أنظمة التشغيل الحاسوب ومبادئ التعامل معها :

يجب أن يكون لدى المحقق على الأقل فهم مبدئي بأنواع الأنظمة التشغيلية لأجهزة الحاسوب وخصائص ومميزات كل نظام تشغيلي، وكذلك أنظمة حفظ ومعالجة البيانات والملفات التي تعتمد عليها، وذلك حتى يتمكن من المشاركة في متابعة وفحص وتفتيش مسرح

---

[1] _حسين بن سعيد الغافري، المرجع السابق،ص02.

[2] _خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع ، عمان، الأردن، 2001،ص186.

الجريمة فقد يجد نفسه أمام حتمية إتخاذ قرار صعب بعد المشاورة مع الخبير، وبدون المعرفة التقنية فإن هذا القرار سيكون بيد الخبير وحده، وأكثر أنظمة التشغيل شيوعا والتي يتدرب عليها رجال البحث والتحقيق هي :ويندوز – لينكى[1].

ثانيا :التعرف على الصيغ المختلفة لتطبيقات الحاسوب

يتوجب على المحقق كذلك أن تتوفر فيه صفة المعرفة بالصيغ المتنوعة لتطبيقات الحاسوب، وذلك ليصبح قادرًا على معرفة مكان الملفات المخزنة وما تتضمنه من معطيات كما يشترط معرفته لأهم التطبيقات التي تمكنّه من قراءة أو مشاهدة محتوى هذه الملفات على أساس أنه ملف في غاية الأهمية، وبإعتبارها الوعاء الحقيقي لأدلة الإدانة لما تحتويه من معلومات في شكل رقمي محفوظة على شكل ملفات، يتميز كل ملف ببينة وصيغة خاصة تميزه عن غيره.

ثالثا :التعامل بالشكل الصحيح مع شبكة الأنترنت:

يعتبر الأنترنت أداة تحري مناسبة لرجال البحث والتحقيق المعلوماتي، فهي تسمح لهم توضيح غموض بعض الجرائم ، فمن الضروري إستخدامها حتى يستطيع التصدي لها من خلال تبادل الملفات ونقل الرسائل الإلكترونية كما تتيح لهم الإطلاع على مستجدات جرائم المعلوماتية وطرق مكافحتها[2].

البند الثالث:ضرورة معرفة الأساليب الإجرامية في مجال المعلوماتية.

معرفة رجال البحث والتحقيق بأساليب إرتكاب الجرائم المعلوماتية أمر غاية في الأهمية خاصة فهي تساعدهم على معرفة طبيعة المجرم، والموقع الإحتمالي لإرتكاب الجريمة، كما تساعد من يتولى مسائل مناقشة الشهود وإستجواب المتهمين في طرح الأسئلة المباشرة المتصلة بالسلوك الإجرامي، كما أنها تساعد المحقق على التواصل مع خبير الحاسوب، عند شرح هذا

[1] _حسين بن سعيد الغافري،المرجع السابق،ص3.

[2] _خالد عياد الحلبي،المرجع السابق، ص 187،188.

الأخير لما توصل إليه من أدلة وقرائن ، والأساليب المستخدمة في إرتكاب الجريمة والأدوات المستعملة في ذلك[1].

كما أن الإلمام بتقنيات الأمن المعلوماتي من الأمور المهمة التي لابد من معرفتها من قبل المحقق، فمعرفتها وإستعمالاتها تساعده ميدانياً في عمله، فعندما يباشر تحقيقا في جريمة إختراق نظام معلوماتي لشركة أو مؤسسة فهو يسأل القائمين على نظامها المعلوماتي عن نوع البرامج الحمائية والأمنية المستخدمة وكيفية عملها وهو ما يسمح له بإستخلاص الوصفة التفاعلية بينها وبين الفعل الإجرامي، من خلال ما يرد في التقارير التي يعدها الخبير من خلال قراءة أنظمة تقنية الجدار الناري(Fire wall) ونظام خادم الوكيل(Proxy server)[2].

الفرع الثالث :ضرورة الخضوع لدورات تدريبية وتكوينية في مجال المعلوماتية.

إضافة إلى جملة المعارف التي يشترط أن يحيط بها المحقق علما من أجل أن يكون مؤهلًا لمباشرة أعمال البحث والتحقيق في شان الجرائم المعلوماتية ، فإنه لابد أن يكون محل تكوين نظري وتدريب عملي مستمر ودائم وذلك كنتيجة حتمية لطابع التطور المستمر للجريمة المعلوماتية ، وللتدريب أهمية ومنهج خاص نبينه فيما يلي:

البند الأول : أهمية التدريب في مجال مواجهة الجرائم المعلوماتية.

التدريب والتكوين يعد جزءا من عملية التنمية الإدارية، فهو بهدف بالدرجة الأولى إلى زيادة الكفاءة والفعالية والقدرة على إنجاز العمل ومن ذلك فقد حرصت الكثير من المنظمات العامة والخاصة على العناية به، بإعتباره أحد الأدوات الرئيسية لرفع مستوى الأداء، والهدف من عملية التدريب هوإدخال وإستحداث تعديلات جوهرية على سلوك المتدربين تكون أثارها واضحة في سلوكهم لأداء الأعمال التي يكلفون بإنجازها كل في مجال تخصصه بشكل أفضل بعد عملية التدريب لا قبلها[3].

---

[1] _حسين بن سعيد الغافري، المرجع السابق،ص5.

[2] _خالد عياد الحلبي، المرجع السابق،ص190.

[3] _يوسف حسن يوسف ، الجرائم الدولية للانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية ، القاهرة، مصر،2001،ص176.

ويميل الفقه الجنائي إضافة إلى الواقع العملي إلى القول بأن التحقيق في مجال الجرائم المعلوماتيةفي حاجة إلى خبرة ومهارات خاصة لا تتأتى إلا بالتدريب المتخصص يراعى فيه عدة عناصر تتعلق بشخص المتدرب ومنهج التدريب ، فبخصوص المتدرب لا بد أن يكون مؤهلا لذلك سواء أكان من ضباط الشرطة القضائية أو سلطات التحقيق أو النيابة العامة فيجب أن تتوافر فيه قدرات ذهنية ونفسية خاصة، غير أن تدريب المتخصص في معالجة البيانات ونظم التشغيل يؤتي ثماره بسرعة مقارنة بأولئك المنتمين لسلك الشرطة أو العدالة[1].

كما يشترط كذلك في المتدرب أن يكون على قدر من الخبرة، فقد ذهب بعض الخبراء إلى تحديد شرط 05 سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات من أجل وضع الشخص ضمن قائمة المتدربين[2].أما بالنسبة للمنهج التدريبي فيجب أن يتضمن المحتوى الجوانب التالية:

- الواقع الحالي والإتجاهات المستقبلية للجرائم المعلوماتية، ومن أجل التعرف على الفئات المختلفة

التي ينقسم إليها مجرمو المعلوماتية.

- الجانب التشريعي من أجل فهم ومعرفة الشيء القانوني المتعلق بهذه الجرائم والإلمام بإتجاهات

القوانين والتشريعات.

- دراسة وتحليل القضايا المشهورة للإستفادة من تجارب العدالة في مواجهة هذه الجرائم.
- الوقوف على الأبعاد الدولية وآليات التعاون المشترك بين الدول والتعرف على الإتفاقيات والمعاهدات الدولية[3].

البند الثاني : المحاكاة الحاسوبية كأسلوب تدريب ملائم في مجال الجرائم المعلوماتية.

[1]_عبد الفتاح بيومي حجازي،المرجع السابق، ص89.

[2]_يوسف حسن يوسف،المرجع السابق،ص177.

[3]_حسين بن سعيد الغافري،المرجع السابق،ص3.

إن ما يجب الإشارة إليه في هذا الصدد هو تقنيات التدريب المعروفة بإسم المحاكاة الحاسوبية التي تعرف بأنها تقليد محكم يطابق ويماثل الأصل تماما، بحيث يتم التعايش مع ظروف وملابسات وإحتمالات الواقع العملي للمواقف والأحداث بصورة تزيد من القدرة على التعامل مع هذه المواقف في الحياة العملية[1].إن إتباع الأسلوب التدريبي سيؤدي إلى إكتساب الأفراد العاملين في مجال البحث والتحقيق المعلوماتي وفي حالة الإعداد الجيد للنموذج المحاكي للواقع الميداني لعملهم، لمعارف وإتجاهات ومهارات مرتبطة بكيفية أداء العمل وإستخلاص النتائج والربط بينها وكيفية التصرف في موقف محدد بأعلى قدرة من الفعالية[2].

إذًا فمسألة الإختصاص في مجال أعمال البحث والتحقيق المعلوماتي ليست مسألة ذات طابع قانوني، بل هي أوسع من ذلك لتمتد إلى شروط الإختصاص الفني والعلمي بمجال النظم المعلوماتية، فبدونها لا يمكن مباشرة أعمال البحث والتحقيق من قبل الجهات المختصة ولو إستوفت شروط الإختصاص النوعي والإقليمي، نظرًا لما تطرحه غياب ثقافة التعامل مع النظم المعلوماتية، من إشكاليات عملية، وهو الأمر الذي لم يستدركه بعد التشريع الجزائري وفق نصوص قانون الإجراءات الجزائية، وترك أمر تنظيمه للقوانين الخاصة بأسلاك الأمن الوطني والدرك الوطني اللتان تبذلان مجهودات معتبرة في هذا المجال من أجل التكييف مع الواقع الحديث للإجرام، وذلك من خلال عزمها على تعميم الفرق المختصة بمكافحة الجرائم المعلوماتية على المستوى الوطني مع تجهيزها بأحدث التقنيات والعمل على رفع كفاءة موظفيها من خلال تكوينهم الدائم والمستمر في الدول التي أحرزت تقدما ملحوظا في هذا المجال.

المطلب الثاني: الإجراءات الخاصة بالبحث والتحري في الجرائم المعلوماتية.

[1] _ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر 2007 ، ص150

[2] _ممدوح عبد الحميد عبد المطلب،المرجع نفسه،ص147.

الجريمة المعلوماتية وكغيرها من أنواع الجرائم الأخرى، تمر بذات مرحلتي الإستدلال والتحقيق القضائي،وما يترتب على ذلك من إجراءات قانونية وفنية وشكلية ويعتبر إجراء التحقيق القضائي،هو الأساس في مجال البحث والتحقيق المعلوماتي، وذلك لما يكتسبه هذا الأخير من أهمية قصوى في مجال إستخلاص الحقائق بشأن الجريمة، لكن تبقى الإجراءات الأخرى الخاصة بمرحلة الإستدلال أو التحري الفنية منها خصوصا ضرورية لأجل إستكمال متطلبات التحقيق القضائي في مجال الجريمة المعلوماتية[1]. وعليه سوف نقسم هذا المطلب إلى ثلاثة فروع في الفرع الأول آليات الكشف والتبليغ عن الجرائم، والفرع الثاني وضع خطة تكوين فريق العمل، أما الثالث الخطوات الأولية لمباشرة أعمال البحث والتحري عن الجرائم الإلكترونية.

الفرع الأول:آليات الكشف والتبليغ عن الجرائم.

إن المشكل الذي يواجه أجهزة الأمن والمحققين من رجال الضبطية القضائية، هو أن الجرائم المعلوماتية لا تصل إلى علم السلطات المعنية بالصور العادية، وذلك لصعوبة إكتشافها من قبل الأشخاص العاديين وحتى المؤسسات والشركات لا تكتشف هذه الجرائم فور وقوعها على إعتبار أن أغلبها لا يراجع حساباته بشكل يومي، وحتى وإن تم ذلك بشكل يومي أو شهري فإنه يصعب عليها التأكد من الفوارق في الأرقام التي تبدو عادة خسائر أو ديون أو حتى في حال إكتشافها فإن أغلب تلك الشركات تتردد في التبليغ خوفا على سمعتها[2].

وهنا تظهر أهمية دور الأجهزة الأمنية في رصد حركة مرتكبي جرائم المعلوماتية وإكتشاف هذه الجرائم من خلال الرصد الميداني لحركة المعاملات التجارية ومراقبة المشبوهين داخل المؤسسات المالية وحولها، فالقدرة على الملاحظة وقراءة تصرفات الأشخاص العاملين في مجال المعلوماتية، والمهتمين بالبرامج، وهواة صناعة الأنظمة هي أولى خطوات السيطرة الأمنية على نشاط مرتكبي جرائم الحاسوب ويتعزز كل ذلك من خلال تكثيف المراقبة من قبل الوحدات الخاصة لمكافحة الجريمة المعلوماتية في الأماكن وحول الفئات التالية:

[1] _عبد الفتاح بيومي حجازي،المرجع السابق،ص67.

[2] _ضياء علي أحمد النعمان، المرجع السابق، ص364.

- أماكن بيع أجهزة الحواسيب والبرامج المعلوماتية.
- الرصد الدقيق لحركة المترددين على المواقع المذكورة أعلاه.
- الرصد الدقيق لحركة المشبوهين في مجال جرائم الأموال وتجارة المخدرات.
- الرصد الدقيق لحركة معتادي جرائم التزوير والإحتيال ومعتادي الإجرام المعلوماتي.

إن هذا القدر من التواجد الميداني المنظم يضمن تغطية أمنية على منافذ المعلومات والحاسوب وله أثر وقائي ورادع في نفس الوقت، كما يسمح بتوفير المعلومات الأولية عن الجرائم المعلوماتية قبل وقوعها كما يضمن سرعة التبليغ عنها وإتخاذ الإجراءات بحقها[1].

البند الثاني :كيفية التعامل مع التبليغ بشأن الجرائم المعلوماتية.

التبليغ هو إخطار السلطات المختصة بوقوع جريمة، وهذا الإخطار واجب أدبي يتقيد به المواطن الصالح سواء وقعت الجريمة عليه أو على غيره ، إن أهمية التبليغ تعطي للمجني عليه ولغيره من الأفراد في الجرائم المعلوماتية دور لا يستهان به لأنه قد يكون السبيل الوحيد لكشف هذه الجرائم، وهو دور يعطي الفرصة لأجهزة الضبطية القضائية فرصة التحرك بسرعة من أجل مواجهة الجريمة المعلوماتية ويعتبرعدم الإبلاغ سببا رئيسيا في تفاقم الجرائم المعلوماتية[2].

فالتبليغ هو المشكلة الحقيقية التي الجهات المختصة بمواجهة الجريمة المعلوماتية ، فغالبية الهيئات فالمؤسسات تخشى الإبلاغ عن الجرائم المعلوماتية خوفًا من فقدان عملائها وهو ما ينتج عنه إفلات مرتكب الجريمة بفعلته.[3] والتبليغ هو إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع ، أو كان هناك إتفاقا جنائيا، أو أدلة أو قرائن أو عزمًا على إرتكابها، أو وجود شك أو خوف من أنها إرتكبت[4].

---

[1] _عبد الفتاح بيومي حجازي، المرجع السابق،ص 72-75.

[2] _خالد عياد الحلبي، المرجع السابق،ص192.

[3] -عبد الله بن سعود محمد السراني، المرجع السابق،ص67.

[4] _ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة الإستدلالات، دار الفكر الجامعي، مصر،2007،ص177.

وفي هذا الصدد نصت الفقرة الأولى من المادة 17 المعدلة بموجب الأمر02/15 قانون الإجراءات الجزائية الجزائري على أنه " يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و 13 و يتلقون الشكاوى والبلاغات ويقومون بجمع الإستدلالات و إجراء التحقيقات الإبتدائية" تقابلها نص المادة 17 من قانون الإجراءات الجزائية الفرنسي والمادة 24من نظيره المصري و 27 من نظام الإجراءات الجزائية السعودي.

والتبليغ عن الوقائع الجنائية حق لكل شخص بل هو واجب مفروض عليه فلا يصبح معاقبته وإقتضاء التعويض منه، إلا إذا تعمد الكذب، وتوافرت في شأنه أركان جريمة البلاغ الكاذب[1].

ويتكفل ضباط الشرطة القضائية بتلقي البلاغات ومباشرة الإجراءات المتعلقة بالتحقيقات الإبتدائية، ولهم الحق في سبيل ذلك طلب مساعدة القوة العمومية أثناء تنفيذ مهامهم، وتختم أعمالهم بإعداد محاضر ترسل إلى وكيل الجمهورية لأجل إخطاره بالجنح والجنايات التي تصل إلى عملهم ويستحب أن يكون المبلغ في الجريمة المعلوماتية على درجة مقبولة من الإلمام والمعرفة بالجوانب الفنية للحاسوب، حتى يتمكن من تقديم معلومات تصف الحادث بالشكل الذي يمكن معه لضباط الشرطة القضائية من مباشرة البحث والتحري عنها، وهو ما يستلزم أن يكون متلقي البلاغات على قدر من المعرفة بالجوانب المعلوماتية، حتى سيضع مناقشة المبلغ في الكثير من جوانب الجريمة محل البلاغ[2].ويتم التبليغ باعتباره أولى خطوات إجراءات البحث والتحقيق المعلوماتي من خلال:

- تلقي جهات الضبطية القضائية معلومات أمنية تشير إلى ممارسته شخص معروف أو غير معروف أنشطة معلوماتية محظورة.
- توفر معلومات عن انتشار الفيروسات التخريبية عبر شبكة الإنترنت.
- ضبط شخص بحيازة مستندات أو محررات مزورة أو بطاقات إئتمان مزورة[3].

[1] _راجع المواد 91 و 92 من قانون العقوبات الجزائري.

[2] _خالد عياد الحلبي، المرجع السابق،ص195.

[3] _عبد الله بن سعود محمد السراني، المرجع سابق، ص182،183.

ا

لبند الثالث : كيفية التبليغ عن الجرائم المعلوماتية.

إن التبليغ عن جرائم المعلوماتية لا يختلف عما هو عليه الحال في مجال الجرائم التقليدية ،غير أنه يتمتع بنوع من الخصوصية يتماشى و طبيعة هذه الجرائم ،فالبلاغ في هذه الحالة قد يتم عن طريق شبكة الأنترنت أو ما يعرف بالبلاغ الإلكتروني ،وذلك بإطلاع الهيئات المختصة بالبحث والتحري بواسطة رسالة إلكترونية عن وجود أعمال غير مشروعة ،أوعن موقع ينشر صورًا جنسية للأطفال و هو ما يوفره البريد الإلكتروني للدرك الفرنسي من خلال البريد الإلكتروني:

بإعتباره الجهة المختصة بالتحري والتحقيق في judiciare@gendaremeriedefense.gov.fr

شأن هذه الجرائم في فرنسا، و كذلك الحال في مصر من خلال الإتصال بموقع شرطة إدارة مكافحة جرائم الحاسب و شبكات المعلومات في مصر.

قد يكون التبليغ من خلال ملئ المبلغ لإستمارة رقمية على الموقع المخصص لتلقي البلاغات و الشكاوي كذلك التى يوفرها الموقع الرسمي لأنترنت الأحداث في فرنسا www.intrenet.miners.gov.fr ،أو تلك المتوفرة على موقع إدارة مكافحة جرائم الحاسبات و شبكات المعلومات المصري على الرابط التالي: www.ccd.gov.eg.[1]

وهي الإمكانية المتاحة على المستوى الوطني من خلال إمكانية التبليغ التي تتيحها المواقع الخاصة بالجهات الأمنية كجهاز الشرطة والدرك الوطني، هذا الأخير الذي يضع تحت تصرف المواطنين البريد الإلكتروني لأجل التواصل مع هذه الجهات والتبليغ عن كافة الجرائم والجرائم المعلوماتية، وذلك عبر البريد الإلكتروني من خلال العنوان الإلكتروني-ccom : cgn@mdn_dzأو من خلال الخدمة التي أصبحت متاحة منذ 07 أفريل 2015 المتعلقة بإيداع الشكاوى أو المعلومات المتعلقة بالجرائم عبر الموقع الإلكتروني المستحدث من قبل هيئة الدرك الوطني على العنوان التالي:

[1]_نبيلة هروال، المرجع السابق،ص182،183.

https://ppgn.mdn.dz، و هو مايوفره كذلك موقع المديرية العامة للأمن الوطني على موقعه الذي يمكن لأي شخص من التبليغ وبصفة تضمن سرية هويته ، عن أي جنحة أو جناية وذلك بهدف تشجيع الغير على التبليغ عن الجرائم بما فيها المعلوماتية ، ويبقى للمبلغ حرية الإختيار في الأخير بين الأسلوب التقليدي أو الإلكتروني.

وتظهر أهمية تلقي البلاغات في أنها تساعد رجال البحث والتحري على تحديد نوع الجريمة المبلغ عنها إن كانت تندرج ضمن الجرائم المعلوماتية ،وكذلك وضع تصور مبدئي لخطة العمل المناسبة للبحث والتحري بشأن الجريمة،وبالتالي تحديد نوع الخبرة المطلوبة لأجل المعاينة وتحريز الأدلة وما يجب التأكيد عليه أن جهة تلقي البلاغ يجب عليها أن تحرص على أن يقوم المبلغ بالخطوات التالية:

- تجهيز قائمة بأسماء العاملين في المؤسسة أو المشتبه فيهم.
- تجهيز نسخة إحتياطية من بيانات الأجهزة المتضررة.
- عدم تبليغ أي أحد آخر بالجريمة الواقعة[1].

الفرع الثاني:وضع خطة تكوين فريق العمل.

إن أمر تقصي الحقيقة و تتبع الدليل الإلكتروني الناتج عن الجريمة المعلوماتية ، يحتاج إلى تضافر الجهود من أجل الإحاطة بكل جوانب الجريمة من القانونية إلى المعلوماتية إلى تلك الفنية ،وهو ما يستدعي تشكيل فريق من المختصين كل في مجاله لأجل التكفل بمهام البحث والتحقيق المعلوماتي وذلك وفق خطة محددة مسبقًا تهدف إلى تنظيم العمل وتحقيق الهدف المنشود ،وسنحاول إبراز كل ذلك في الفقرات اللاحقة.

البند الأولى :وضع خطة العمل.

بعد الإنتهاء من جمع المعلومات الأولية المتعلقة بالجريمة المبلغ عنها، أو تلك محل الشكوى، يبدأ رجال البحث والتحري بناء على ضوء المعطيات المستقاة بتحديد خطة العمل المناسبة وتشكيل فريق العمل اللازم للتحري في الحادثة، وهذه الخطة يجب أن تكون قد إكتملت في ذهن المحقق بمجرد إنتهائه من أخذ الإفادة من المبلّغ أو الضحية وإتضحت لديه

[1]_خالد عياد الحلبي، المرجع السابق،ص195.

الصورة الأولية عن الحادثة الجرمية قبل التنقل إلى مسرح الجريمة لأجل مباشرة إجراءات المعاينة والضبط وذلك من خلال الإرتكاز على النقاط التالية[1]:

• تحديد حجم الجريمة محل البحث والتي تحدد حجم ونوع الفريق اللازم للتدخل فجرائم المعلوماتية تتنوع مابين بسيطة ومعقدة وذلك حسب طبيعتها الفنية الخاصة، التي تفرض على أعضاء فريق التحقيق إمتلاك مهارات فنية خاصة وضرورية للتعامل معها.

• تحديد الظروف المحيطة بالجريمة و بالخصوص:

- مدى أهمية محل الجريمة ومدى نسبة الضرر التي لحقت بالضحية
- مدى تضرر الأجهزة الحاسوبية والشبكات.
- إعداد قائمة بأسماء المتهمين المحتملين.
- تحديد مستوى الإختراق الأمني الذي يتسبب فيه الجاني.
- تحديد مستوى مهارة المجرم المعلوماتي.
- تحديد طبيعة مسرح الجريمة والأسلوب الأمثل للتعامل معها، وهذه النقطة مهمة جدًا وإخفاق المحقق في تحديد طبيعة الأسلوب المناسب للتعامل مع الجريمة قد يؤدي إلى عدم الحصول على أية نتيجة أو الحصول على كم هائل من النتائج بدون فائدة[2].

• مراعاة الضوابط القانونية فالإجراءات المسبقة التحديد تساعد على ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل البحث تتم وفق ضوابط إجرائية شر عية ولا تعرض الإجراءات لطائلة البطلان في مراحل متقدمة من سير الدعوى[3].

• تعيين الأشخاص الذين سيتم إستجوابهم وتحديد الأسئلة والنقاط التي يجب إستيضاحهم بشأنها وكذلك تقدير مدى الحاجة إلى الإستعانة بأصحاب الخبرة والإختصاص التي يفتقدها فريق التحقيق بعد وضع الخطة يشترط كذلك وبصفة آلية تعيين فريق التحقيق

---

[1]_علي عدنان الفيل، إجراءات التحري و جمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، دار الكتاب الجامعي الحديث، الإسكندرية، مصر، 2012، ص13.

[2]_حسين بن سعيد الغافري، المرجع السابق،ص7.

[3]_خالد عياد الحلبي، المرجع السابق،ص198.

وتشكيله من أجل مباشرة الأعمال المتعلقة بالتحري والبحث في مدى صحة البلاغات والشكاوي الواردة بشأن الجريمة المعلوماتية[1].

البند الثاني :تشكيل فريق العمل.

يجب وفي مجال البحث والتحري بشأن الجرائم المعلوماتية، تشكيل فريق تحقيق يمزج بين الخبرة في مجال البحث والتحري في الجرائم العادية، وبين التخصص في مجال المعلوماتية، فهناك عادة محققون ذوو خبرة طويلة في مجال البحث الجنائي، و هناك أخصائيون في مجال المعلوماتية ذوي معرفة واسعة ولكن من النادر أن يوجد محقق تتوفر فيه الصفتين معًا، لا سيما وأن عالم المعلوماتية متشعب وعلى درجة كبيرة من التعقيد ولذلك وجب أن يتضمن فريق العمل في مجال التحري والبحث خبراء وفنيين من هذا المجال، وذلك حسب ما تفرضه وقائع كل قضية، كما أن فريق التحقيق قد يتطلب الإستعانة ببعض خبراء مسرح الجرائم التقليدية كخبير البصمات و ممن ليس لهم دور وثيق الصلة بالطبيعة الخاصة بجرائم المعلوماتية غير أنه لا يتصور خلو أي فريق منهم نظرًا لما يحققونه من فائدة من خلال أدوارهم الثانوية[2]. وعلى كل حال فإن فريق العمل يجب أن يتكون من :

أولًا :المشرف على التحقيق :

والمحقق الرئيسي والذي يجب أن يكون من ذوي الخبرة الطويلة في مجال التحقيق الجنائي في الجرائم المعقدة، مع إلمامه بالجوانب المعلوماتية، ويتولى مهمة الإشراف على إدارة الفريق وتوزيع المهام على أعضائه[3].

ثانيًا :فريق خبراء الحاسوب والشبكات :

قد يضم شخصا واحدًا أوأكثر حسب ظروف الجريمة وهو شخص لديه خبرة ومعرفة بوسائل وأساليب التحقيق وإجراءاته، مع إلمامه بطبيعة الجرائم المعلوماتية وكيفية التفتيش عن الأدلة الإلكترونية والتعامل معها وأخذ الإفادة من ذوي العلاقةمع مسرح الجريمة.[1]

---

[1] _علي عدنان الفيل، المرجع السابق،ص16.

[2] _حسين بن سعيد الغافري، المرجع السابق،ص7.

[3] _عبد العال الدريبي المرجع السابق،ص310.

2 _علي عدنان الفيل، المرجع السابق،ص17.

ثالثًا :خبراء تدقيق الحسابات الإلكترونية :

هو شخص أو أكثر لديه إختصاص في مجال المراجعة المحاسبية على درجة عالية من الخبرة في التعامل مع البرمجيات المستخدمة، والآليات التي يتم بموجبهاتبادل الأموال إلكترونيًا، ينصب عمله على تحديد أسلوب الجريمة وأساليب التلاعب بالأنظمة وتقدير الخسائر الناتجة عن الجريمة.

رابعا :فريق ضبط وتحريز الأدلة :

يتكون هذا الفريق من خبراء رفع البصمات كإجراء عام في معظم الجرائم وذلك من خلال التركيز على المكونات المادية للحاسوب والشبكات المتضررة، أو المستعملة في الجريمة، وبالخصوص لوحة المفاتيح والفأرة والشاشة والطابعة[2].

خامسًا :فريق الرسم والتصوير :

يضم شخصًا أو أكثر يقوم ون بتصوير أو رسم تخطيطي (كروكي) لمسرح الجريمة وتحديد موقع الأجهزة والملفات والأشخاص، وإلتقاط الصور الفتوغرافية والتصوير بالفيديو.

سادسًا :فريق التفتيش العلمي :

يتولى هذا الفريق عملية البحث الدقيق على مسرح الجريمة وفق النظم القانونية التي تتبع التفتيش في الأماكن، فيقومون بالمرور على كل الغرف والأماكن مع فحصها بشكل دقيق لأجل الكشف عن أشياء مخفية، ويستحب أن يكون هؤلاء من خبراء الحاسوب.

سابعًا :فريق التأمين والقبض :

توكل لهذا الفريق مهمة السيطرة الأمنية على مسرح الجريمة وضبط مداخلها ومخارجها وحركة الموجودين بها، والمباني المجاورة لها وتنفيذ عملية القبض على المشبه فيهم ويتكون عادة من رجال الأمن بالزي الرسمي[3].

---

[2]_حسين بن سعيد الغافري، المرجع السابق،ص3.

[3]_عبد العال الدربي، المرجع السابق،ص310،311.

ثامنًا :الخبير الإستشاري :

يعمل الخبير الإستشاري على تحقيق هدفين في مجال مساعدة فريق التحقيق المعلوماتي و هما:

- القيام بدور توضيحي للواقعة.
- إزالة الغموض عن وقائع معينة.

فمثلا في جرائم الأنترنت يكمن عمل الخبير في توضيح طريقة عمل شبكة الأنترنت ثم يطرح رأيه الخاص حول النقاط الغامضة المتعلقة بالجريمة، ما قد يحل إشكالًا عالقًا وعمله كخبير إستشاري هو ترجمة لمهاراته الفائقة التي قد لا تتوفر عند المحقق والخبير المعلوماتي[1].

إذًا تعتبر خطة العمل وتشكيلة فريق العمل من القيم الأساسية والثابتة في مجال البحث والتحقيق المعلوماتي، فأي محاولة لتتبع أثارها من دون التشكيل الضروري والخطة المناسبة سيكون مصيره الفشل لا محالة ،نظرًا لسرعة تنفيذ الجريمة المعلوماتية وسهولة محو الدليل،وإعتمادها على أساليب قد تتعدى قدرة الفريق مجتمعًا، وهو ما يستدعي ضرورة بقاء أفراده على إتصال دائم بعالم المعلوماتية لأجل تحصيل المستجدات،التي تمكنهم من الوصول إلى نتائج جد فعالة في مجال القبض على مجرمي المعلوماتية من خلال تعقبهم وملاحقتهم.

الفرع الثالث:الخطوات الأولية لمباشرة أعمال البحث والتحري عن الجرائم المعلوماتية.

تعتبر الجريمة المعلوماتية من قبيل الجرائم الخفية، أي أنها عبارة عن أنشطة إجرامية تتم في سرية بتخطيط وإعداد مسبق وتنفيذ بطريقة مدروسة من قبل مجرمين متمرسين في عالم الجريمة تجمعهم مصلحة عدم إبلاغ السلطات المختصة عن نشاطهم الإجرامي[2].وفي حالة الإبلاغ أو تقديم شكوى عن نشاط هؤلاء المجرمين لدى السلطات المختصة ممثلة في المصالح الأمنية والقضائية، فإن هذه الأخيرة تباشر أعمال الإستدلال والتحري بشأن الجرائم محل

[1] _خالد عياد الحلبي، المرجع السابق،ص202.

[2] _ محمد عنب، إستخدام التكنولوجيا الحديثة في الإثبات الجنائي، دون ذكر دار النشر، مصر ،2007، ص176 .

البلاغ أو الشكوى فيبادرضباط الشرطة القضائية بدءا وقبل كل شيء بالتأكد من الفرضيات التالية في إطار أداء مهامهم:

البند الأول : الإجراءات الأولية لكشف حقيقة الجريمة.

قبل مباشرة إي إجراء وإتقاءًا لتضييع الجهد بشأن جريمة لم تقع ،أو كانت محل تبليغ كاذب يباشر ضباط الشرطة القضائيةإلى التأكد من:

أولا : التأكد وقوع جريمة فعلية :

فلا بد من أجل ضمان صحة الإجراءات الخاصة أن نكون أصلا بصدد جريمة إلكترونية سواء تحت وصف جنحة أو جناية، أي استيفاء الركن الشرعي.

ثانيًا : توفر دلائل تشير إلى إتهام شخص معين :

ينبغي أن تتوفر في الشخص المشبه فيه دلائل كافية تدعوا للإعتقاد بأنه ساهم في إرتكاب الجريمة مما يستوجب إتهامه فيها، وفي مجال الجرائم المعلوماتية يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر والصفات التي تقوم على المضمون المنطقي لملابسات الجريمة وخبرة المحقق.

ثالثًا : حيازة المشتبه فيه لدلائل قوية في كشف الحقيقة :

فلا يكفي لمباشرة تحريات جدية، الحصول على الإذن القانوني فقط، بل يجب أن تتوفر لدى المحقق أسباب كافية بأنه يوجد في مكان ما أولدى المشتبه فيه أدوات إستخدمت في الجريمة المعلوماتية أو أدلة إلكترونية لها فائدة في إستجلاء الحقيقة[1].

وفي حال توفر هذه الشروط جاز لأعضاء فريق التحقيق المعلوماتي مباشرة أعمالهم بشأن الجريمة المعلوماتية من خلال تحديد ملابساتها وهوية مرتكبها من خلال إجراءات تسبق عملية الإنتقال لأجل المعاينة المادية لمسرح الجريمة لسبب وحيد وهو أن غالبية الجرائم المعلوماتية هي جرائم غير ملتبس بها، أي أن أعمال البحث والتحقيق بشأنها عادة ما تنطلق متأخرة

[1] -نزيهة مكاري، "وسائل الإثبات في جرائم الاعتداء على حق المؤلف عبر الانترنت"، مقالة منشورة بمجلة 14سنة 2009دون ذكر المعلومات المتعلقة بهيئة النشر، المناهج القانونية، العدد المزدوج13المملكة المغربية، ص64.

بعد وقوعها فهي جرائم خفية تحتاج الى خبرات فنية هائلة للكشف عنها ويتبع فريق التحقيق مجموعة من الإجراءات العملية الخاصة نوضحها في البنود الموالية.

البند الثاني:إجراء الإرشاد الجنائي.

يعد الإرشاد الجنائي من أهم المصادر التي يعتمد عليها ضباط الشرطة القضائية في عمليات البحث و التحري لجمع المعلومات و خصوصًا في مجال الجرائم المعلوماتية فنجد أن هيئات الضبطية أصبحت تجند عناصرها للدخول إلى العالم الإفتراضي و بالخصوص إلى مواقع التواصل الإجتماعي و قاعات الدردشة خصوصًا تلك المعروف عنها تطرفها و ميولها العدواني، و ذلك تحت أسماء مستعارة بقصد البحث عن الجرائم ومرتكبيها، فضباط الشرطة القضائية ما عليهم سوى الإتصال بالشبكة و إعتماد أسلوب النقاش والدردشة الإلكترونية مع الغير ومختلف الهيئات وبمجرد بروز مؤشرات عن هوية المجرم المعلوماتي أوجرائم المعلوماتية كالإحتيال أو الإستغلال الجنسي للأطفال ،يبادر هؤلاء إلى سؤاله مثلًا عن طرق الحصول على بطاقات الإئتمان المزورة أو عن مواعيد إستدراج الأطفال وهي المعلومات التي يستعين بها مزود الخدمة بالإنترنت الذي يمكن أن يوفر بواسطة برمجيات خاصة مكان وجود المجرم و مثال ذلك ما قامت به المباحث الفيدرالية الأمريكية(FBI) التي إستطاعت الإطاحة بشبكة(FAST-LAND)التي تمتهن القرصنة المعلوماتية والمتاجرة بها عبر شبكة الأنترنت،وذلك من خلال دس مرشد معلوماتي ضمن أعضاء هذه الشبكة[1].

وقد أتاح التشريع الجزائري اللجوء إلى هذا الأسلوب حسب ما نصت عليه المادة 65 مكرر05 من القانون06-22[2] إلى غاية المادة 65 مكرر 18 من قانون الإجراءات الجزائية، وذلك في حالة الجرائم المعلوماتية، بعد الحصول على إذن مسبب من وكيل الجمهورية أو قاضي التحقيق وتحت رقابة الأول لمدة (04)أشهر قابلة للتجديد.

البند الثالث :إجراء الوضع تحت المراقبة الإلكترونية.

[1] _نبيلة هروال، المرجع السابق،ص 196،197.

[2] -الأمر22/06المعدل والمتمم للأمر 155/66،المرجع السابق.

يجب الإشارة أولًا أن المراقبة على أي وسيلة من وسائل الإتصالات تعد بمثابة إعتداء على حرمة الحياة الخاصة فهو حق محمي دستورياً ، ومشمول بالحماية القانونية التي تقر بأن الإتصالات مهما كان شكلها مكفولة سرًا و لا يجوز مصادرتها أو الاطلاع عليها إلا بأمر قضائي مسبب، ويعد فعل مراقبتها أو تسجيلها أو بثها جريمة معاقب عليها، و المراقبة الإلكترونية هي عملية يقوم فيها المراقبة بتتبع المشتبه فيه بواسطة الأجهزة الإلكترونية، وإفراغ ما تسفر عنه في تقارير أمنية، وتلك التقارير تفرغ في ملف إلكتروني يحدد فيه الزمان والمكان الذي تمت فيه و النتيجة التي أسفرت عنها[1].

والحقيقة أن المشتبه فيه المراقبة من قبل فريق التحقيق هو شبكة الانترنت أو البريد الالكتروني، إذ يتم من خلالها مراقبة إتصالاته الإلكترونية المشتبه فيها، و التقنية المستخدمة في هذا المجال هي التقنية الالكترونية البحتة، و التي تعني مجموعة الأجهزة المتكاملة مع بعضها بغرض تشكيل مجموعة من السمات المتعلقة بالمجرمين أو المشتبه فيهم ،وفق برنامج موضوع مسبقا لتحديدهم من أجل ضبطهم وجمع الأدلة قبلهم لإثبات إدانتهم وتقديمهم أمام المحكمة[2].

وقد نص التشريع الإجرائي الجنائي الجزائري على إمكانية الوضع تحت المراقبة الالكترونية في مجال مكافحة الجرائم المعلوماتية حسب نصوص المواد 65 مكرر 5 إلى مكرر 10 قانون 06-22 و ذلك تحت الفصل الرابع الموسوم باعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، بحيث يجوز لوكيل الجمهورية وكذلك لقاضي التحقيق في حال فتح تحقيق قضائي ، منح إذن لضابط الشرطة القضائية المكلفين بالبحث و التحري عن الجرائم المعلوماتية، يتضمن إعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية دون موافقة المعنيين بها، ويشترط في الإذن أن يكون مكتوبًا ومتضمنا لكافة العناصر الأساسية التي تسمح بالتعرف على الإتصالات المطلوب إلتقاطها وذلك لمدة أقصاها (04)أشهر قابلة للتجديد، ولصاحب الإذن الحق في تسخير أي عون عمومي أو

[1] _ناير نبيل عمر ، المرجع السابق،ص149.

[2] _نبيلة هروال، المرجع السابق،ص 199،200.

خاص لدى هيئة الإتصالات السلكية أو اللاسلكية من أجل التكفل بالجوانب التقنية المتعلقة بالعملية، وتختتم العملية بإعداد محضر من قبل ضابط الشرطة القضائية يتضمن مضمون العملية مع توضيح تاريخ وساعة بداية العملية وإنتهائها، وقد تعزز اللجوء إلى هذا الأسلوب سنة 2009 بموجب نص كل من المادتين 03 و04 الواردتين ضمن فصول القانون04/09 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها[1] اللتان عبرتا صراحة عن إجازة مباشرة إجراء الرقابة الإلكترونية فيما تعلق بالجرائم المعلوماتية ،ولكن دون ذكر الهيئة المكلفة بتولي ذلك و قد إستمر الوضع كذلك إلى غاية صدور المرسوم الرئاسي15-261الذي يحدد تشكلية وتنظيم و كيفيات سيرالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[2] بتاريخ 08 أكتوبر2015 .

هذه الأخيرةأصبحت الهيئة المختصة بتنفيذ عمليات المراقبة الإلكترونية للإتصالات الإلكترونيةحسب مضمون الفقرة 05 من نص المادة 04 من المرسوم الرئاسي15-261 وذلك من خلال إستحداث مديرية المراقبة الوقائية واليقظة الإلكترونية التي يدخل في صميم إختصاصاتها القيام بمهام المراقبة الإلكترونية للإتصالات من أجل الكشف عن الجرائم المعلوماتية بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها ،حسب ما تقره المادة 11من المرسوم الرئاسي15-261 ،كما منحها القانون حسب نص المادة 21 من المرسوم السالف الذكر الصفة الحصرية لتولي مهام المراقبة الإلكترونية في حال تصنيف الجريمة المعلوماتية ضمن الجرائم الإرهابية والتخريبية والماسة بأمن الدولة دون سواها من الهيئات الوطنية الأخرى و ذلك تحت سلطة قاض مختص.

وتنفذ عادة عملية المراقبة و التتبع الإلكتروني في مجال الجرائم المعلوماتية من خلال الإستعانة ببعض الوسائل التقنية نذكر منها:

[1] -القانون04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها،المرجع السابق.

[2] - يحدد تشكلية وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال،المرجع السابق.

أولًا :تقنية تتبع عنوان :TCP-IP:

عنوان **IP** هو العنصر المسؤول عن تراسل الحزم البيانية عبر شبكة الانترنت وتوجيهها إلى أهدافها، ويعتبر بمثابة عنوان الحاسوب المتصل بالشبكة ويتكون من شفرة رقمية تتكون من أربع (04)أجزاء، يشير الأول إلى المنطقة الجغرافية و الثاني لرمز مقدم الخدمة، و الثالث لمجموعة الحواسيب المرتبطة و الرابع يخص الحاسوب الذي يتم الإتصال منه، ولذلك وفي حالة وجود جريمة معلوماتية فإن ضباط الشرطة القضائية يقومون بتتبع عنوانIP للجهاز مصدر الجريمة وتحديد موقعه[1].

ثانيًا :إستخدام تقنية فحص البروكسي : (PROXY)

البروكسي هو الوسيط العامل بين الشبكة و المستخدم، تستخدمه الشركات المقدمة لخدمة الإتصال لأجل إدارة الشبكة،وضمان أمنها وتوفير حزمة الذاكرة الجاهزة (**Cashe Memory**) يعمل البروكسي على تلقي طلب المستخدم للبحث عن صفحة ما ،فيتحقق البروكسي ضمن الذاكرة الجاهزة عما إذا جرى تنزيل الطلب من قبل فيقوم بإعادة إرسالها دون الحاجة إلى طلبها من الشبكة العالمية للمعلومات (**web**) من أجل تزويد المستخدم بها، ومن مزاياه أن ذاكرته هذه يمكن أن تحتفظ بتلك المعلومات والعمليات ، وهو ما يمنح لضباط الشرطة القضائية فحصها وإستخلاص الدلائل ضد المتهم وذلك من خلال تقفي أثاره بمساعدة مزود الخدمات[2].

ثالثًا :إستعمال برامج التتبع المعلوماتية:

تقوم برامج التتبع على شاكلة برنامج (HACK-TRACER)بالتعرف على محاولات الإختراق ومن قام بها، وإشعار الجهة المتضررة بذلك، وهذه البرامج عادة ما تكون ساكنة في خلفية المكتب، عندما ترصد أي محاولة للقرصنة أو الإختراق وتسارع بغلق منافذ

[1] _عبدالله بن سعود محمد السراني،المرجع السابق،ص51.

[2] _علي عدنان الفيل، المرجع السابق،ص70،71.

الدخول للمخترق، ثم تبدأ بعملية مطاردته واقتفاء أثره وصولا إلى تحديد عنوانه الإلكتروني (IP) واسم الشركة المزودة بخدمة الإنترنت ومعلومات أخرى[1].

رابعًا: الإستعانة بنظام كشف الإختراق: INTRUSION DETECTION SYSTEM وهو النظام الذي يرمز له ب I.D.S ويعتمد على مجموعة من البرامج التي تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الشبكة مع تحليلها بحثًا عن أي إشارة قد تدل على وجود مشكلة تهدد أمن الحاسوب و الشبكة من خلال مقارنة نتائج التحليل مع الصفات المشتركة للاعتداءات المعلوماتية، ففي حالةوجودها يبادربتسجيلها في سجلات حاسوبية خاصةوهذه السجلات التي يسعى لها ضباط الشرطة القضائية لتحليل أسلوب إرتكاب الجريمة وربما مصدرها[2].

خامسا :العمل بنظام جرة العسل:

هو نظام حاسوبي مخصص لكي يتعرض للهجمات الإلكترونية عبر الشبكة، من خلال خداع من يقوم بذلك وذلك بإبداء سهولة في الاعتداء عليه وذلك لإغرائه، وذلك حتى يتمكن من جمع أكبر قدر من المعلومات عن أسلوب الهجوم وتحليله وهو ما يسمح باتخاذ الإجراءات الوقائية التي تزود فريق التحقيق بالمعطيات اللازمة التي توضح معالم الجريمة[3].

سادسًا :جمع الأدلة من خلال إعتراض رسائل البريد الالكتروني :

وذلك من خلال الإستعانة ببرامج (DCS)مصممة للبحث في مضمون الرسائل الالكترونية المتبادلة على شاكلة برنامج كارنيفور و 1000 الذي يتعقب ويفحص رسائل البريد الالكتروني المرسلة الذي طورته المباحث الفيدرالية الأمريكية (FBI)والواردة عبر أي حاسوب خادم تستخدمه أي شركة توفر خدمة الانترنت وهو برنامج مستخدم في التحقيق في قضايا الأمن القومي الأمريكي[4].

---

[1] _خالد عياد الحلبي، المرجع السابق،ص207.

[2] _علي عدنان الفيل، المرجع السابق،ص71.

[3] _خالد عياد الحلبي، المرجع السابق، ص209.

[4] _نبيلة هروال، المرجع السابق،201.

كل هذه الأساليب و البرامج و الأنظمة هي وسائل تساعد ضباط الشرطة القضائية في أعمال البحث و التحري ولكن يبقى أمرإستخلاص نتائجها أمرًا مرهونًا بمدى إلتزام مقدم خدمة الإنترنت بمد يد العون لأجل تحديد مكان إرتكاب الجريمة وهوية مرتكبها.

البند الرابع:إلتزامات مقدمي خدمات الإنترنت:

يقصد بمزود الخدمات أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات لأجل التواصل بواسطة تقنية المعلوماتية، ويقوم بتخزين ومعالجة المعطيات بما فيها المعلومات الخاصة بالمشترك كنوع خدمة الإتصالات المستخدمة لديه، هويته، عنوانه البريدي، رقم هاتفه وذلك بناء على إتفاق ترتيب الخدمة القائم بينهما، حسب تعريف المادة 02 الفقرة 02 و 09 من الإتفاقية العربية مكافحة الجرائم المتصلة بالتقنية المعلوماتية[1] بأنه نوعان كما يعرفه قانون حماية الحياة الخاصة في مجال الإتصالات الالكترونية الأمريكية

- الأول مزودو خدمة الإتصالات الالكترونية وهو كل من يقدم خدمة إلى مستخدمي الشبكة، ويعمل على تسهيل إرسال واستقبال الإتصالات السلكية واللاسلكية والالكترونية.
- الثاني مزودو خدمة معالجة المعلومات عن بعد ، وهو كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بواسطة وسائل الإتصالات الالكترونية.

وبناء على ذلك فإذا أرسل أي شخص لآخر رسالة عن طريق البريد الإلكتروني فإنها تمر وبالضرورة على مزود الخدمة وتخزن لديه[2].

إن القانون قد سمح للسلطات المختصة بمتابعة الجرائم المعلوماتية حق طلب التحفظ على البيانات المخزنة لديها وحق كذلك تزويدها بالمعلومات الخاصة بالمشترك ونشاطه في إطار عملها

المتعلق بأعمال البحث و التحري عن الجرائم المعلوماتية.

الإجراء و الالت ا زم الذي نجد له أصلا قانونيا على المستوى الدولي حسب ما تقرره أحكام

[1] -المرسوم252/14المتضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات،المرجع السابق.

[2] _عائشة بن قارة، المرجع السابق،ص155،156.

المادتين16و17 من إتفاقية بودابست لمكافحة الجرائم المعلوماتية، تقابلها المواد25،23،24من الإتفاقية العربية لمكافحة الجرائم المتصلة بالتقنية المعلوماتية، وقد وردت هذه الإلتزامات على المستوى الوطني حسب ما جاء في نص المادة 10 من الفصل 04من قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ،التي توجب على مقدمي خدمة الإنترنت مساعدة السلطات في إطار التحريات القضائية من خلال جمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة وكل ذلك تحت غطاء السرية ،كما ألزمت المادة 11 من نفس القانون مقدمي الخدمات حفظ المعطيات التالية:

- المعطيات التي تسمح بالتعرف على مستخدمي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة.
- المعطيات التي تسمح بالتعرف على المرسل إليه وعناوين المواقع المطلع عليها.

ويلزم حفظ هذه المعطيات لمدة سنة منذ تاريخ تسجيلها، وهي مدة طويلة مقارنة بمقترحات الإتفاقية العربية التي قدرتها ب 90 يومًا وهو الأجل الذي يسمح لضباط الشرطة القضائية بالرجوع إليها من أجل تحديد هوية وأماكن إرتكاب الجرائم المعلوماتية وذلك نظرًا للإعتبارات التالية:

- قابلية البيانات المعلوماتية للتلاشي والتلاعب والتغير.
- إرتكاب غالبية الجرائم عن طريق نظم الإتصالات وهو ما يساعد على تحديد هوية مرتكبي هذه الجرائم .
- التحفظ على هذه البيانات يعتبر أحد أهم عناصر الإثبات التي يمكن أن تكشف عن هوية مرتكبي هذه الجرائم [1].ولضباط الشرطة القضائية إمكانية تقديم طلبات لمزودي الخدمة بالانترنت لأجل تزويدهم بالمعلومات المخزنة و من ضمن هذه الطلبات:

[1]_هلالي عبد اللاه ،المرجع السابق ،ص196،197.

- طلب التحفظ المعجل على البيانات المخزنة وذلك حتى يتفادى المزود شطب التسجيلات و القضاء على الدليل.
- طلب تقديم بيانات معلوماتية خاصة بالمشترك.
- طلب إعتراض الإتصالات الالكترونية.

إذًا تعتبر هذه الإجراءات أهم الإجراءات ذات الطابع الإجرائي الفني و المعلوماتي في مجال أعمال البحث و التحري عن الجرائم المعلوماتية التي يباشرها ضباط الشرطة القضائية تنفيذا لتعليمات وكيل الجمهورية أو قاضي التحقيق أوإختصاصا منهم، وذلك من خلال ممارسة مهامهم بعيدًا عن مسرح الجريمة أي في مرحلة تسبق التنقل للمعاينة والتفتيش المادي وضبط الأدلة الالكترونية والمادية وهي الإجراءات التي تختلف نوعا ما من حيث الوسائل و الطرق.

المطلب الثالث :الإجراءات الفنية الخاصة بمعاينة مسرح الجريمة المعلوماتية.

بعد أن تطرقنا إلى المسائل الخاصة بإجراءات البحث والتحري الأولية بشأن الجريمة المعلوماتيةوالتي يبادر إليها ضباط الشرطة القضائية، بمجرد الوصول إلى علمهم بوقوع الجريمة تنتقل إلى تفصيل المسائل الخاصة بالإجراءات العملية ذات الطابع الخاص المتعلقة بمرحلة المعاينة والتفتيش والتي يتمعادة على مسرح الجريمة، والتي تقتضي تنقل الجهات المختصة من أجل تحقيق الهدف الرئيسي وهوإحراز الأدلة المادية والإلكترونية، والتي من شأنها إثبات وإدانة أو براءة المتهم، وعادة ما يتولى مهمة التنقل إلى مسرح الجريمة المعلوماتية، الفرقة الخاصة بالبحث والتحقيق في مسائل الجرائم المعلوماتية.

وعليه سوف نقسم هذا المطلب إلى ثلاثة فروع في الفرع الأول الإجراءات الخاصة بالإنتقال إلى مسرح الجريمة وتأمينه ، والمطلب الثاني الإجراءات الخاصة بالتفتيش وضبط الأدلة، أما المطلب الثالث الأساليب الخاصة في التعامل مع الأشخاص ذوي العلاقة بالجريمة الإلكترونية.

الفرع الأول: الإجراءات الخاصة بالإنتقال إلى مسرح الجريمة وتأمينه.

إذا ثبت بناء على أعمال البحث والتحري الأولية التي قام بها ضباط الشرطة القضائية بشأن صحة فحوى البلاغات الواردة إليهم بشأن وقوع جريمة معلوماتية أو بناء على توفر حالة تلبس بالجريمة، أنه هناك أدلة قوية تشير إلى حيازة المشتبه فيه لأدلة تفيد في استجلاء الحقيقة، مخزنة على حاسوبه أو على وسائط خارجية أو مخبأة في مسكنه أو مقر عمله فإن هذا الأمر يستدعي و بالضرورة الانتقال إلى مسرح الجريمة المفترض لأجل إتمام أعمال البحث والتحري أو القيام بتنفيذ الأوامر القضائية الواردة من قاضي التحقيق كالأمر بالتفتيش، وإن كانت الإجراءات الخاصة بالانتقال إلى مسرح الجريمة المعلوماتية نوعية بعض الشيء إلا أنها تخضع وبالضرورة لمجموعة من الشروط القانونية قبل كل شيء.

البند الأول:ضرورة إستيفاء الشروط القانونية لتنفيذ أمر الانتقال.

إن الانتقال إلى مسرح الجريمة وما يصاحبه من ضرورة المعاينة والتفتيش، يقتضي التعدي على حرمة الحياة الشخصية للأفراد ومساكنهم، يستوجب أن يتم في إطار قانوني لأجل ضمان شرعية الإجراءات وعدم تعريضها للبطلان الذي قد يهدم الدليل ويتسبب في إفلات المتهم من العدالة، إضافة إلى ضمان عدم التعسف في مواجهة الغير من الأفراد بحجة ضرورة التحقيق، وتجنبا لكل ذلك يستوجب القانون على ضابط الشرطة القضائية إحترام مجموعة من الشروط القانونية المبينة في قانون الإجراءات الجزائية وأخرى في القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ، لأجل إتمام هذه الإجراءات ضمن إطار شرعي وذلك حسب الأحوال التالية:

أولا: حسب أحوال حالة التلبس :

توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب إرتكابها، كما تعتبر كذلك إذا كان الشخص المشتبه فيه في وقت قريب جدا من وقوعها أو تبعته العامة بالصياح أو كان حائزًا لأشياء أو دلائل تدعوا إلى إفتراض مساهمته في الجريمة كما توصف كذلك إذا ما إرتكبت الجناية أو الجنحة في منزل أو كشف صاحب المنزل عنها عقب وقوعها وبادر باستدعاء ضابط الشرطة القضائية لأجل إثباتها[1].

[1]_المادة 41 من الأمر66-155قانون الإجراءات الجزائية،المرجع السابق.

إن تطبيق هذه الأحوال على الجريمة المعلوماتية يكاد أن يكون أمرًا مستحيلا، غير أنه يمكن إفتراض وقوعها ولو في نادر الأحوال وهو ما يترتب عنه إتخاذ الإجراءات التالية:

- على ضابط الشرطة القضائية الذي بلغ بجناية أو جنحة متلبس بها مهما كان نوعها، أن يخطر وعلى الفور وكيل الجمهورية،ثم ينتقل وبدون تمهل إلى مسرحها قصد اتخاذ الإجراءات اللازمة للتحري، والتي تسمح بالحفاظ على الآثار التي يخشى اختفائها[1].
- لا يجوز الإنتقال إلى مسكن الأشخاص الذين يظهر أنهم ساهموا في الجريمة المتلبس بها سواء لتنفيذإجراءات التحري أوالتحقيق بالجرائم المعلوماتية إلا بناء على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهاره قبل الدخول إلى مسكن المشتبه فيه ويترتب على تنفيذ الإجراء في غياب الإذن ،أو غياب أوصاف محل البحث ، أو عناوين أماكن البحث ، عن مضمون الإذن البطلان المطلق للإجراء برمته[2].

فبمجرد توفر هذين الشرطين جاز لرجال البحث والتحقيق بناء على حالة التلبس مباشرة أعمالهم المتعلقة بالمعاينة و التفتيش، ولهم الحق في إتمام أعمالهم في أي ساعة من ساعات الليل أو النهار وذلك حسب ما تورده المادة 47 من قانون الإجراءات الجزائية.

ثانيا: حسب ظروف الأحوال العادية :

يقصد بها الحالات التي تكون خارج حالة التلبس وهي الظروف التي تميز الجريمة المعلوماتية والتي تحتاج إلى تقدير فني كبير لأجل التأكد من مدى صحة وقوعها، واتخاذ تقرير الإجراءات الكفيلة بمتابعة مرتكبيها واثبات الأدلة في مواجهتهم، ويتم الإنتقال إلى مسرح الجريمة تنفيذا عادة لأوامر وكيل الجمهورية في إطار إتمام إجراءات البحث والتحري[3]، أو تنفيذا لأوامر قاضي التحقيق.

---

[1]_المادة 42 من من الأمر66-155قانون الإجراءات الجزائية،المرجع السابق.

[2]_المادة 44 من القانون 22/06 المعدل والمتمم للأمر66-155 قانون الإجراءات الجزائية،المرجع السابق.

[3]_المادة 36 فقرة 4 المعدلة بموجب الامر 02/15 المعدل والمتمم للأمر66-155 قانون الإجراءات الجزائية.

ويشترط في هذه الحالة إحترام جملة الشروط المتعلقة بالإذن المكتوب سواء الصادر من قبل وكيل الجمهورية أوقاضي التحقيق حسب الأحكام الواردة في المواد من 44 إلى 47 مكرر من قانون الإجراءات الجزائية تحت طائلة البطلان.

إذاً فمن الناحية القانونية فإن الشروط المتعلقة بالمعاينة و التفتيش في إطار الجريمة المعلوماتية هي نفس الشروط المتبعة في باقي الجرائم الأخرى ولا داعي لتكرارها، بحيث ينبغي تركيز البحث حول طبيعة الإجراءات المتبعة والاحتياطات الخاصة التي يطبقها ضباط الشرطة القضائية لأجل معاينة الجرائم المعلوماتية والتي تعرف تحت إسم إجراءات تأمين موقع الجريمة المعلوماتية.

البند الثاني :الإلتزام بإجراءات تأمين موقع الجريمة المعلوماتية.

قد يقوم كل من ضباط الشرطة القضائية أو وكيل الجمهورية أو قاضي التحقيق ، عند الانتقال إلى مسرح الجريمة بأعمال المعاينة المادية والميدانية للجريمة في حد ذاتها، والمعاينة هي فحص مكان أوشيء أو شخص له علاقة بالجريمة، وإثبات حالته كمعاينة مكان إرتكاب الجريمة أو أداة إرتكابها أو محلها أو معاينة جسم أو ملابس الجاني أو المجني عليه لإثبات ما بالجسم من جراح أو ما على الثياب من دماء أو آثار أخرى[1].

إن الإنتقال من أجل إجراء المعاينة يعتبر أول إجراء من إجراءات البحث و التحري ، فهو الإجراء الأكثر أهمية لآنه يسمح بالمعاينة المادية للوقائع المشكلة للجريمة ، والإنطلاق بشكل سريع ومباشر في عملية البحث و ضبط الأدلة ، التي تساعد على معرفة وقت وكيفية إرتكاب الجريمة وهوية فاعلها، و عادة ما تسند هذه المهمة لأفراد الشرطة العلمية والتقنية ،نظرًا لضرورة التدخل بسرعة و بطريقة مدروسة تتلائم و طبيعة الجريمة محل المعاينة ، من خلال القيام بسلسلة من العمليات التي تستلزم خبرة ميدانية و وسائل من نوع خاص[2].

[1] _عبد العال الدريبي، المرجع السابق،ص294.

[2] _Charle Diaz – La Police Techenique et Scientifique-2eme Edition- Edition Presse universitaire de France - France – 2006- p54.

غير أن دورها يتضاءل في مجال الجرائم المعلوماتية، فهي لا تحقق نفس الأهداف كما هو الحال في الجرائم التقليدية، كما أنها لا ترقى إلى درجة أهميتها كإجراء في تلك الجرائم وذلك راجع إلى:

1- أن الجرائم التي تقع على نظم المعلومات و الشبكات قلما تخلف عقب إرتكابها أثار مادية.

2- إن عددا كبيرًا من الأشخاص قد يتردد على مسرح الجريمة خلال الفترة الزمنية التي تتوسط مرحلة إرتكابها واكتشافها، مما يفسح المجال أمام حدوث تلف أو تغيير أو عبث بالآثار المترتبة عنها[1].

وحتى تكون للمعاينة في جرائم المعلوماتية فائدة تسهم في كشف الحقائق وجب على المحقق اتباع مجموعة الإرشادات العملية ذات الطابع التأميني نوجزها فيما يلي:

أولا: قبل التنقل إلى إجراء المعاينة :

يجب إتباع الخطوات التالية من قبل رجال البحث والتحقيق قبل التحرك إلى مسرح الجريمة المعلوماتية لإجراء المعاينة وهي:

1- توفير معلومات مسبقة عن مكان الجريمة، وكذلك عن نوع وعدد الأجهزة المتوقع مداهمتها، ونوع الشبكات المتصلة بها، وذلك لتحديد خطة التعامل معها.

2- إعداد خريطة الموقع الذي سيتم الانتقال إليه مع ضرورة وضع خطة وتقسيم الأدوار على فريق التحقيق وتحديد المهام واختصاص كل واحد منهم حتى لا تتداخل الإختصاصات.

3- الحصول على الاحتياجات الضرورية من الأجهزة و البرامج الحاسوبية للاستعانة بها في الفحص.

4- تأمين مصدر التيار الكهربائي حتى لا يتم التلاعب به عن طريق قطعه أو تعديله بهدف تعطيل عمل فريق المعاينة.

5- مراجعة الخطة واستحضار الإذن القضائي[1].

[1] _علي عدنان الفيل، المرجع السابق،ص33.

ثانيا :عند معاينة مسرح الجريمة:

المعاينة إجراء من أهم إجراءات التحقيق الجنائي لأهمية الأدلة المستقاة منها التي تكون غالبا ذات دلالة قاطعة في الإثبات ،وقد أكدت المعاينة الفنية في كثير من الأحيان فعاليتها في إظهار حقيقة الجريمة ومعرفة كيفية وأسباب وقوعها وهوية مرتكبيها ، لذلك يترتب على المحقق مراعاة الدقة والترتيب وبذل أقصى ما يمكن من العناية والإهتمام عندإجرائها ،للحيلولة دون فقدان ما يمكن إستخلاصه من معلومات قيمة قد تفيد في تنوير التحقيق ،ويرى الفقه الجنائي ضرورة إتباع ضوابط خاصة لأجل معاينة مسرح الجريمة المعلوماتية هي[2]:

1- تحديد أجهزة الحواسيب الموجودة وتحديد مواقعها بأسرع وقت ممكن، إضافة إلى البحث عن النهاية الطرفية المزود للخدمة بالانترنت (MODEME) من أجل قطع الإتصالات الخارجية التي يمكن أن تخرب الأدلة أو تمحوها من على ذاكرة الحاسوب،كما يراعى ضرورة تصوير الأجهزة الموجودة وخاصة الأجزاء الخلفية التي تحمل الأرقام التعريفية للأجهزة.

2- ضرورة وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة، مع رصد الإتصالات الهاتفية من و إلى مسرح الجريمة مع إبطال مفعول الهواتف النقالة التي تساعد عن طريق تقنية الجيل الثالث في تدمير الأدلة من خلال إتصالها بالأجهزة محل المعاينة[3].

3- ملاحظة وإثبات الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الإتصال وطريقة الولوج

---

[1]_نبيلة هروال، المرجع السابق،ص220.

[2]_عبد الفتاح عبد اللطيف الجبارة ، إجراءات المعاينة الفنية لمسرح الجريمة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن 2010 ، ص171.

[3]_عبد الفتاح بيومي حجازي، المرجع السابق،ص578.

للنظام إضافة إلى ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بالنظام حتى يمنح فرصة لإجراء المقارنة حين يعرض الأمر على القضاء[1].

4- عدم التسرع في نقل أي" مادة معلوماتية "من مسرح الجريمة وذلك قبل إجراء اختبار اليقين من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي والتي قد تؤدي إلى إتلاف البيانات المخزنة مباشرة في حالة تعرضها لها.

5-حفظ ما تحتويه سلة المهملات من أوراق ممزقة أو كربون نسخ أو أقراص ممغنطة سليمة أو محطمة مع فحصها ورفع البصمات عنها وكذلك التحفظ على مستندات الإدخال والمخرجات الورقية و التي عادة ما تكون ذات صلة بالجريمة[2].

6_ حصر عملية المعاينة في فئة المختصين والمحققين الذين يتوافرون على الكفاءة العلمية والخبرة الفنية في مجال النظم المعلوماتية، والذين تلقوا تدريبا فنيًا كافيًا على التعامل مع الأدلة المعلوماتية، ففي فرنسا مثلا يقوم فريق التحقيق المتكون من ثلاث عشر (13) شرطيا بالإشراف على تنفيذ المهام التي يأمر بها وكيل الجمهورية أو قاضي التحقيق، فيرافقون المحققين أثناء عمليات المعاينة ويعملون على فحص الأجهزة ونسخ محتوياتها وإعداد تقارير فنية ترسل إلى قاضي التحقيق[3].

الفرع الثاني :الإجراءات الخاصة بالتفتيش وضبط الأدلة طبقاً لقانون الإجراءات الجزائية.

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، والضبط غاية التفتيش القريبة أي الأثر المباشر الذي يسفر عنه الإجراء، وهدف التفتيش سواء تعلق بالأشخاص أوالمساكن هو ضبط الأشياء التي تفيد في كشف الحقيقة أي الأشياء التي تعد

---

[1]_عبد الله حسين علي محمود" إجراءات جمع الأدلة في مجال سرقة المعلومات "،بحث مقدم للمؤتمرالعلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، مركز البحوث والدراسات،أكاديمية شرطة دبي، الإمارات العربية المتحدة،من 26 إلى 28 أفريل 2003، ص2.

[2]_فتوح الشادلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودورالشرطة، منشورات الحلبي الحقوقية،بيروت ، لبنان، دون ذكر سنة النشر، ص357.

[3]_علي عدنا الفيل، المرجع السابق،ص35.

في ذاتها دليلا على الجريمة، أو يمكن إستخدامها كدليل، وقد تكون هذه الأشياء هي وسيلة الجريمة أو تكون السبب الذي ارتكبت من أجله الجريمة، ولما كان الضبط هو الأثر المباشر للتفتيش، وبإعتباره أحد إجراءات التحقيق فتنطبق عليه القواعد التي تنطبق على التفتيش فإذا بطل التفتيش بطل الضبط، والتفتيش يعتبر وسيلة تهدف للوصول إلى الحقيقة وليس غاية في حد ذاته، ولعل أن الشكل الذي يتبادر إلى الذهن في هذه الحالة هو مدى قابلية النظم المعلوماتية للتفتيش بإعتبارها بيانات مادية[1].

البند الأول :الضوابط القانونية للتفتيش والضبط.

إن الحديث عن مسألة الضوابط القانونية للتفتيش و الضبط في مجال الجرائم المعلوماتية يقودنا إلى إبرازها وفق التسلسل المنطقي التالي:

أولا : حسب شروط الإختصاص النوعي و المحلي :

على عكس أغلبية التشريعات العربية التي خولت سلطة التحقيق وحق التفتيش للنيابة العامة، فإن التشريع الإجرائي الجزائري ساير نظيره الفرنسي وجعل الإختصاص الأصيل بالتفتيش والضبط لقاضي التحقيق، ولا يحق ذلك للنيابة العامة ممثلة في وكيل الجمهورية إلا وفق حالة التلبس بالجنحة أو الجناية.فلقاضي التحقيق أن يقوم وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها مناسبة وضرورية

للكشف عن الحقيقة بالتحري عن أدلة الاهتمام وأدلة النفي ،ويجوز له بناء على ذلك الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويباشر قاضي التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة (79،80،81)من قانون الإجراءات الجزائية.

[1] _علي حسن أحمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة،عالم الكتب الحديث، اربد، الأردن ، 2004،ص135.

وإذا كان من المتعذر على قاضي التحقيق أن يقوم بنفسه بجميع إجراءات التحقيق جاز له أن يندب ضابط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشر وط القانونية المنصوص عليها في المواد من 138 إلى 142 من قانون الإجراءات الجزائية[1].

وباعتبار التفتيش والضبط إجراء يستهدف جرائم عادة ما تقع إما داخل الإختصاص المحلي لقاضي التحقيق أو خارجه، فإن هذا الأخير ملزم بإتباع قواعد الإختصاص الإقليمي فهو مختص ضمن دائرة وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه فيهم،أو بمحل القبض على أحدهم ويمتد إختصاصه تلقائيا إلى دائرة اختصاص محاكم أخرى فيما يتعلق بالجرائم المعلوماتية فإختصاصه في هذه الحاة وطني حسب ما هو مكرر في المادة 40 من قانون الإجراءات الجزائية وكذلك الفقرة الأخيرة من نص المادة 47، وهو نفس الإختصاص المقرر إقليمياً المطبق على ضباط الشرطة القضائية في حال تنفيذ أوامر قاضي التحقيق[2].

ثانيا :من حيث المواعيد : عندما يتعلق الأمر بالجرائم المعلوماتية فإنه يجوز التفتيش في كل محل سكني أ و غير سكني في كل ساعة من ساعات النهار أو الليل بناء على إذن مسبق من وكيل الجمهورية المختص.يمكن لقاضي التحقيق أن يقوم بنفسه بعملية التفتيش و الضبط ليلًا أو نهارًا وفي أي مكان علىامتداد التراب الوطني أو يندب ضابط الشرطة القضائية المختص بذلك(البند 03 و 04 المادة 47) من قانون الإجراءات الجزائية الجزائري.

غير أنه إذا ما تعلق الأمر بجناية فلا يجوز سوى لقاضي التحقيق القيام بالتفتيش وبحضور وكيل الجمهورية(المادة 82 ق إ ج)، و الملاحظ أن هذا الاستثناء هو بمثابة نص مضاد لما هو وارد في نص المادة 47 البند 03 و 04 و التي تمنح الحق لضباط الشرطة القضائية المختصين بالجرائم المعلوماتية بالتفتيش في مسرح الجريمة المعلوماتية، فكان من الأولى توسيع مجال إختصاصهم وليس تضييقه من خلال حصر الإختصاص في شخص قاضي التحقيق الذي قد لا يكون على علم بتقنيا ت التفتيش الخاصة بالجرائم المعلوماتية.

[1] _ المادة 68 من الأمر 01-08،المؤرخ في 26يونيو2001،الجريدة الرسمية رقم 34،ص07.

[2] _البند الأخير من المادة 16 المعدل والمتمم للأمر66- 155قانون الإجراءات الجزائية ،المرجع السابق.

أما فيما تعلق بمسألة حضور المشتبه فيه عملية التفتيش والضبط سواء في مسكنه أو مسكن شخص آخر فإن البند الأخيرة من نص المادة (45 ق إج) لا تستوجب حضوره، ففي مجال الجرائم المعلوماتية لقاضي التحقيق أو لضباط الشرطة القضائية مباشرة أعمالهم دون مراعاة هذه المسألة مع ضرورة الالتزام بأحكام ضمان السر المهني والتقييد بقواعد الحجز.

وإذا ما كان الشخص موقوفا للنظر أو محبوسا مؤقتا أو غائبا لسبب آخر وكان من الخطر نقله لمكان التفتيش فإنه يجوز إجراء التفتيش بعد الحصول على الموافقة المسبقة لوكيل الجمهورية، أولقاضي التحقيق مع ضرورة حضور شاهدين (المادة 47 مكرر ق إ ج)[1].

البند الثاني :القواعد الفنية المتبعة عند التفتيش والضبط.

إذا ما استنفذت الشروط القانونية لمباشرة إجراء التفتيش، جاز لقاضي التحقيق أو لضباط الشرطة القضائية المختصين، مباشرة عملية التفتيش والضبط، بغرض حجز كل ما من شأنه إظهار الحقيقة المتعلقة بالجريمة المعلوماتية سواء أكانت مادية كالحاسوب وملحقاته أو منطقية كالمعلومات والبيانات المخزنة عليه، أو على الشبكة،ولابد أن يرعى في ذلك القواعد التالية:

أولا :القواعد الاحتياطية قبل بدء التفتيش المعلوماتي:

1- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان وجود النظام المعلوماتي من خلال غلق المداخل والمخارج.

2- السيطرة على الدائرة المحيطة بمسرح الجريمة بوضع حراسة ملائمة.

3- السيطرة على محيط مسرح الجريمة من خلال التحفظ على الأشخاص الموجودين.

4- وضع حراسة على الأجهزة حتى لا يتمكن أي كان من لمسها.

5- إختيار مكان لمقابلة المتهمين والشهود بعيدًا عن الأجهزة.

6- توثيق مسرح الجريمة أو محل التفتيش جيدا من خلال جرد محتوياته وذلك لاحتمال توفر إحدى هذه المصادر على الدليل وهي الأوراق التي تم طباعتها، جهاز الحاسوب وملحقاته أقراص ودعائم البرامج، وسائط التخزين المتحركة، الطابعات[1].

[1] -القانون رقم06-22،المعدل والمتمم للأمر66- 155قانون الإجراءات الجزائية ،المرجع السابق.

ثانيا :قواعد تفتيش وضبط ماديات الجريمة المعلوماتية :

يخضع تفتيش المكونات المادية للحاسوب للإجراءات القانونية الخاصة بالتفتيش، أي أنه يجب أن يراعى مكان وجود ذلك الحاسوب أثناء مباشرة الإجراء فيما كان مكانًا عامًا أو خاصًا واستنفاذ الشروط القانونية السالفة الذكر[2].ويراعى عند التفتيش لأجل ضبط الأدلة المحتملة القواعد التالية:

1- التركيز حول مكان شاشة الحاسوب التي تعتبر الموضع المفضل عند مجرمي المعلوماتية للصق بعض القصاصات التي تحمل المعلومات المهمة كأرقام الهاتف أو فهرس المعلومات داخل الحاسوب كالكلمات السرية و المرور.

2- التفتيش بجوانب التوصيلات الهاتفية، فعادة ما يدون مجرمو المعلوماتية محادثاتهم الهاتفية في شكل مخططات يتركونها بجوار الهاتف.

3- تفتيش المفكرات الالكترونية، وهي من أهم الأدلة التي يجب التحفظ عليها وضبطها فهي تحمل أرقام الهاتف وعناوين البريد الإلكتروني والمواعيد والملخصات وغيرها من المعلومات المفيدة في التحقيق.

4- تفتيش جيوب المتهم، فمجرمو المعلوماتية معهم عادة أقراص مرنة، أو بطاقات ذاكرة تحمل معلومات متعلقة بالجريمة عادة[3].

ويحق لرجال التحقيق الإطلاع على محل التفتيش وحجزه أو ضبطه وتوضع عادة الأشياء المحجوزة في وعاء أو كيس، يغلق ويختم عليها بختم قاضي التحقيق أو ضابط الشرطة القضائية.

ثالثا :قواعد تفتيش وضبط المكونات المنطقية :

يجوز للسلطات القضائية المختصة (قاضي التحقيق)، ولضباط الشرطة القضائية حسب ما يجيزه القانون 04/09 وفي إطار إجراءات التحقيق المعلوماتي، الدخول بغرض

---

[1] _علي عدنان الفيل، المرجع السابق،ص36،37.

[2] _نبيلة هروال، المرجع السابق،ص237.

[3] _حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف للعلوم الأمنية، الرياض، المملكة العربية السعودية 2000 ، ص 228.

التفتيش ولو عن بعد إلى كل منظومة معلوماتية أو جزء منها وإلى كل منظومة تخزين معلوماتية.

وإذا كانت هناك أسباب تدعوا للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى غير تلك الأولى جاز لهم تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعدإعلام السلطة القضائية المختصة مسبقا ، وإذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية خارج الإقليم فإن الحصول على إذن يكون من خلال طلب مساعدة دولية حسب المبادئ و الأعراف الدولية في مجال التعاون القضائي[1].

وهي آلية التفتيش عن بعد أو التفتيش المباشر التي تستهدف الكيانات المعنوية والمنطقية للحاسوب دون المادية منها، وإن كانت هذه الأخيرة ضرورية لأجل ولوج النظم المعلوماتية أو الشبكات بهدف التفتيش عن بعد وإلى حجز المعطيات المعلوماتية، فعندما تكتشف السلطة المختصة بالتفتيش المعلوماتي وجود معلومات مهمة من شأنها الكشف عن الجريمة ومرتكبها ويقدر بأنه لا حاجة لضبط وحجز ماديات المنظومة المعلوماتية، فإنه يقوم بنسخ المعطيات والمعلومات الضرورية لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز وفقًا للقواعد المقررة في قانون الإجراءات الجزائية، مع السهر على سلامة المعطيات الأصلية المخزنة على المنظومة المعلوماتية محل التفتيش[2].

أما إذا إستحال أمر حجز هذه المعطيات لأسباب تقنية كان للسلطة المختصة بالتفتيش و الحجز أن تستعمل تقنيات المنع من الوصول إلى المعطيات أو نسخها كما يجوز لها أن تأمر باتخاذ جميع الإجراءات اللازمة لمنع الإطلاع عليها وحجبها من خلال تكليف أي شخص مؤهل وذلك باستعمال وسائل تقنية لذلك[3].

---

[1]_المادة 5 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال.

[2]_ المادة 6 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال.

[3]_المادة 7 ،8 ،9 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

البند الثالث :وسائل تحليل الأدلة المحجوزة.

إن عملية التفتيش عادة ما تسفر عن نوعين من المضبوطات مادية ومنطقية، فالأولى في شكل الحاسوب ذاته وملحقاته، والثانية في شكل ملفات وبيانات ومعلومات كانت مخزنة على القرص الصلب للحاسوب أو على الشبكة، وهي المضبوطات التي تحتاج إلى تحليل من أجل استخلاص الدليل منها وذلك من خلال الإستعانة ببرامج ووسائل خاصة نوجزها فيما يلي:

أولا :وسائل استعادة الدليل وفك التشفير:

قد يقدم المتهم على تخريب القرص الصلب لحاسوبه بمجرد علمه باكتشاف أمره ولذلك يستعين أعضاء فرقة البحث والتحقيق المعلوماتي، في مجال معالجة الأدلة التالفة ببرنامج view disk، أما في مجال فك التشفير الذي قد يعمد الجاني إلى إستعماله لمنع الإطلاع على البيانات المخزنة على حاسوبه فتستعمل برامج شركة acces data corporationتحت إسم pass out أو password recovery[1].

ثانيا :برامج إذن التفتيش :

هو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة، لترقيم الأدلة وتسجيل البيانات عنها، ويقوم هذا البرنامج بإصدار وصلات إستلام الأدلة، و البحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو ظروف ضبط هذا الدليل، وعادة ما يكون بحوزة المحقق على قرص مرن أو قرص صلب محمول.

ثالثا :برنامج بدء تشغيل الحاسوب:

وجود قرص بدء تشغيل الحاسوب مع المحقق، يمكنه من تشغيل الحاسوب المراد تفتيشه إذا كان هذا الأخير محميا بكلمة مرور، ويجب أن يكون مزودًا ببرنامج مضاعفة المساحة، فربما قام المتهم باستخدام هذا البرنامج مسبقا لمضاعفة مساحة القرص الصلب

رابعا : برنامج معالجة الملفات كبرنامج (xtree gold):

[1] _ ممدوح عبد الحميد عبد المطلب، المرجع السابق،ص84،85.

وهو برنامج معالجة آلية للملفات أي مكان على الشبكة، أو القرص الصلب ويستخدم لتقسيم محتويات القرص الصلب الخاص بالمتهم، أو الأقرص المرنة المضبوطة ويستخدم لق ا رءة البرامج و الملفات في صورتها الأصلية.

خامسا : برنامج نسخ البيانات كبرنامج lap link :

هو برنامج يمكن المحقق من نسخ كل البيانات من حاسوب المتهم إلى قرص آخر من خلال تقنية المنفذ المثالي أو المنفذ الموازي، وهو برنامج مفيد جدا يسمح بنسخ المعطيات بكل أمان ودقة قبل أي محاولة لتدميرها..

سادسا :برامج فحص الشبكة :

هي أدوات تستخدم في فحص البرتوكول TPC/IP لمعرفة المشكلات المتعلقة بالشبكات والعمليات التي تعرضت لها، ويرجع فعاليتها إلى قدرتها على دخول الشبكات وتحديد نوع برامج التجسس و الفيروسات التي إستعملت في عمليات الإختراق و تحديد مصدرها بدقة[1].

ومن بين هذه الأدوات:

1_ أداة arp وظيفتها تحديد مكان الحاسوب على الشبكة.

2_ برنامج visual route وهو برنامج يلتقط أي كلمة لعملية ضد الشبكة فيبين وقت وزمن الهجوم ومصدره.

3_ أداة tracer هو برنامج يعمل على رسم مسار بين حاسوب الجاني و العناوين التي زارها والفترات التي قضاها هناك.

4_ أداة nat sat هو برنامج يعرض حالة الاتصال الحالية ومنافذ التصنت في شكل عرض كامل[2]

إضافة لذلك يستعين المحققون بنوع آخر من البرامج كبرامج عرض الملفات بكل أشكالها وصورها ، إضافة إلى إعادة تشكيلها عبر ما يعرف بالإستعانة بتقنيات الذكاء

[1] _عبدالله بن سعود محمد السراني،المرجع السابق،ص55.

[2] _علي عدنان الفيل، المرجع السابق،ص75،76.

الاصطناعي، فجمع الأدلة في مجال الجرائم المعلوماتية يعتمد على تقنيات خاصة ومدى نجاعتها، فهي السبيل لحصر الإحتمال ات والأسباب والفرضيات، وهي تتم عن طريق عمليات حسابية يقوم بها الحاسوب وفق برامج مصممة لذلك، تعمل على حصر الإحتمالات ثم إقصاء الأضعف منها وصولا إلى الإحتمال الأقوى[1].

سابعا : برامج كشف الفيروسات وتدميرها :

يجب على المحقق أن يحمي أدواته وحاسوبه الخاص بالتحقيق بواسطة برامج كشف فيروسات فقد يعمد المتهم إلى تفخيخ حاسوبه بالفيروسات التي تنتقل إلى حاسوب المحقق وتدميره بمجرد ربطه بحاسوب المتهم لنسخ البيانات[2].

الفرع الثالث :الأساليب الخاصة في التعامل مع الأشخاص ذوي العلاقة بالجريمة المعلوماتية.

نعني بالتحقيق مع الأشخاص ذوي العلاقة مع الحاسوب، تلك الإجراءات المتعلقة بتدوين أقوال الشهود، وإستجواب المتهمين وإجراءات مواجهة المتهمين بالأدلة المتوفرة ضدهم وما يتبع ذلك من إجراءات مواجهة بين المتهمين بالأدلة المتوفرة من جهة، وبين المتهمين و الشهود من جهة أخرى، و العودة بالشهود و المتهمين إلى مسرح الجريمة عند الضرورة لمناقشتهم حول أجهزة الحاسوب وملحقاته[3].

البند الأول : أهمية إتباع أسلوب خاص في إستجواب المجرم المعلوماتي.

من أكبر المعوقات التي تقف حائلا في نجاح المحقق في إستكمال المتطلبات الإجرائية الخاصة في مواجهة المتهم ،هي شخصية المحقق في حد ذاته،والمتمثلة في التهيب من إستخدام الحاسوب الانترنت، إضافة إلى عدم اهتمامه بالمستجدات في مجال المعلوماتية.

إضافة إلى معوقات متعلقة بنقص المهارة الفنية للمحقق في التعامل مع الحاسوب

---

[1] _خالد عياد الحلبي، المرجع السابق،ص214.

[2] _حسن طاهر داود، المرجع السابق،ص229،230.

[3] _ محمد الأمين البشيري، التحقيق في الج ا رئم المستحدثة،مركز الدراسات و البحوث، جامعة نايف للعلوم الأمنية، الرياض، السعودية ،2004، ص120 .

و الانترنت، وعدم معرفة أساليب الجرائم المعلوماتية، وعدم الإلمام باللغة المعلوماتية لا سيما وأن هذا المجال غني واكتسب مصطلحات علمية خاصة أصبحت تشكل لغة خاصة لمحادثات و أساليب التفاهم بين المجرمين، ليس هذا وحسب بل إختصرت هذه المصطلحات بالعبارت والحروف الأولى لتعرف باسم لغة المختصرات وهي لغة متطورة ومتجددة ، إذ يجب أن تتوفر في المحقق الخبرة الفنية والكفاءة لأجل نجاحه في مجال التعامل مع مجرمي المعلوماتية[1].

عادة ما يطلق مجرمو المعلوماتية على أنفسهم صفة النخبة(les élies) بحجة أنهم الفئة الأكثر في معرفة بأسرار المعلوماتية، وعالم الحاسوب، وشبكة الانترنت ويطلقون على رجال السلطة القضائية ورجال القضاء صفة الضعفاء والقاصرين، نظرًا لقلة خبرتهم ومعرفتهم بمجال النظم المعلوماتية، ولذلك فقد أصبحت توكل مهام التحقيق في الجرائم المعلوماتية لهيئات خاصة في هذا المجال، وشركات خاصة في مجال المعلوماتية، ويرى البعض أنه من الخطورة تخلي أجهزة العدالة والقضائية عن دورها في التحقيق في مثل هذا النوع من القضايا لصالح الهيئات والشركات الخاصة فبذلك ضياع لحقوق المجتمع تحت رحمة شركات خاصة همها الوحيد تحقيق الكسب المالي وهي غير مكلفة بتحقيق العدالة.

وحتى تكتمل قدرات الجهات الأمنية و القضائية في هذا الشأن، وجب الإستعانة بخبراء الحاسوب في كل مراحل البحث والتحقيق ، كما هو عليه الحال في التحقيق مع المتهمين والشهود، إذ أن أخذ أقوالهم وإستجوابهم يعتمد على منهجية معينة، وقدرات ومواهب لا تتوفر إلا لدى المحقق الذي إكتسب خبرة مهنية في مجال التعامل مع المجرمين إضافة إلى المعرفة الفنية للخبير في مجال المعلوماتية[2].

البند الثاني : ضمانات الإستجواب.

يتولى عادة وفق التشريع الإجرائي الجزائي الجزائري قاضي التحقيق مهمة إستجواب المتهم، وبذلك فهو إجراء ذو طابع قضائي لا يصح إلا من خلال إحترام وتوافر الشروط المحددة قانونا والتي يمكننا إيجازها في النقاط التالية:

---

[1] _علي عدنان الفيل، المرجع السابق،ص85.

[2] _ضياء علي أحمد النعمان، المرجع السابق،377،378.

- الإستجواب إجراء من إجراءات التحقيق، يقصد من وراءه التحقق من شخصية المتهم ومناقشته مناقشة تفصيلية في التهمة المنسوبة إليه ومطالبته بالرد على الأدلة القائمة في مواجهته بنفيها أو التسليم بها ، وهو بذلك إجراء يحقق وظيفتين الأولى إثبات شخصية المتهم ومناقشته بالأدلة والثانية تحقيق دفاع المتهم من خلال فتح السبيل أمامه لتفنيد الأدلة القائمة ضده، وبالتالي مساعدة القضاء على معرفة الحقيقة وكشف ملابسات وشخصية الفاعل الحقيقي[1].
- يختلف إستجواب المتهم عن مجرد سؤاله بواسطة أحد ضباط الشرطة القضائية خلال فترة البحث و التحري، ففي هذه الحالة يكون السؤال متعلق بالوقائع المنسوبة للمشتبه فيه فقط دون مناقشة تفصيلية ودون تحقيق لدفاع المشتبه فيه[2].
- يشترط لبدء الإستجواب إستيفاء الشروط القانونية المنصوص عليها وفق قانون الإجراءات الجزائية والمقررة حسب نصوص المواد من 100 إلى 105 إضافة إلى التقييد بقواعد الموضوعية وإحترام الكرامة الإنسانية للشخص المستجوب، وهي كلها ضمانات قانونية تضمن شرعية الإجراء، ولكن ما هي الضمانات التي تجعل من الإستجواب في الجرائم المعلوماتية إجراء كاشفا للحقيقة؟

البند الثالث :الأسلوب الأمثل لإستجواب مجرمي المعلوماتية.

إن التعامل مع الجريمة المعلوماتية بالبحث والتحقيق يتطلب وسائل خاصة وكذلك التعامل مع المجرم المعلوماتي في إطار إستجوابه فيجب على قاضي التحقيق اتباع أسلوب خاص غير ذلك المعتاد في إستجواب المتهمين في جرائم القانون العام الأخرى ويمكن حصر أسلوبه في مرحلتين:

أولا : قبل البدء في الإستجواب:

قبل البدء في إستجواب المتهم في الجريمة المعلوماتية وجب على قاضي التحقيق التقييد بالقواعد التالية:

[1] _عبد الفتاح حجازي بيومي،المرجع السابق،ص679.

[2] _عبد الفتاح حجازي بيومي، نفس الملرجع،ص681.

1- تبادل المعلومات مع الخبير المعلوماتي من خلال تولي قاضي التحقيق مهمة شرح أهمية ترتيب المتهمين و طريقة توجيه الأسئلة إليهم،وكذلك يقوم الخبير شرح الأبعاد التقنية التي ينبغي إستجلاءها من كل شخص موضع الإستجواب.

2- يزود الخبير قاضي التحقيق بكافة المصطلحات الضرورية التي يمكن إستخدامها أثناء الحوار مع بيان معانيها للاستفادة منها عند الضرورة.

3- وضع خطة الإستجواب بناء على المعطيات السابقة[1].

ثانيا : عند البدء في الإستجواب :

تراعى عند البدء في أخذ أقوال المتهم من قبل قاضي التحقيق التعليمات التالية:

1- إتاحة فرصة حضور الخبير لجلسة الإستجواب،ومنح هذا الأخير توجيه أسئلة فرعية وفق خطة مسبقة وكيفية متفق عليها مسبقا بمعرفة قاضي التحقيق.

2- يفضل في سبيل تحقيق التعاون بين الخبير وقاضي التحقيق أن يستعين الأول بأوراق يضعها أمام قاضي التحقيق تحدد وقت طرح السؤال ونوعه وموضوعه كما يمكن لقاضي التحقيق أن يتيح للخبير فرصة إستجواب المتهم.

3- مراعاة القوانين الإجرائية التي تمنع بعضها حضور الخبير جلسة الإستجواب،ويستحب في هذه الحالة تشكيل لجان تحقيق من أجل ضمان حضور الخبير في عضويتها.

4- تفادي إضاعة الوقت في إستجواب المتهم حول جريمة لا يمكن إكتشافها.

5- تحرير محضر الإستجواب بكل دقة و وضوح[2].

البند الرابع :الشهادة في مجال الجريمة المعلوماتية.

تعرف الشهادة بصفة عامة بأنها أقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء تتعلق بثبوت الجريمة و ظروف إرتكابها و إسنادها إلى المتهم أو براءته فيها ،وقد قال بشأنها بنتام (Bentham): "الشهود هم عيون القضاء وأذانها" وكثيرًا ما يكون للشهادة أثناء جمع الاستدلالات أوالتحقيق الأثر الأكبر في القضاء

[1] _ضياء أحمد النعمان، المرجع السابق،ص380.

[2] _محمد الأمين البشيري، المرجع السابق،ص123،124.

بالإدانة أو البراءة لأن الأقوال التي تتضمنها قد أدلي بها فور وقوع الحادث، قبل أن تمتد يد العبث إليها، أو قد يطول عليها الوقت فتضعف معا لم الجريمة والوقائع التي تنصب عليها[1].

ولا تقل أهمية الشهادة في مجال المعلوماتية عن نظيرتها في مجال الجرائم الأخرى، غير أن ما يمكن الإشارة إليه في موضوع الدراسة أن الشاهد المعلوماتي يختلف عن غيره من الشهود فهو صاحب معرفة علمية وتقنية بمجال المعلوماتية، وهو ما يفرض عليه إلتزامات من نوع خاص أمام جهة التحقيق.

أولا :المقصود بالشاهد المعلوماتي:

سماع الشاهد إجراء كسائر إجراءات التحقيق في المواد التقليدية وهو أمر متروك لتقدير قاضي التحقيق ومرتبط بظروفه،والأصل أن يطلب الخصوم سماع شهادة من يرونوكذلك الحال لقاضي التحقيق الذي له أن يسمع شهادة أي شاهد يتقدم ولو من تلقاء نفسه ولا بد له أن يتحرى الصدق في أقواله[2].

والشاهد في مجال المعلوماتية هو ذلك الشخص صاحب الخبرة والتخصص في تقنيات الحاسوب والذي له معلومات ومكاسب عن شبكات الحاسوب والإتصال والخدمات الخاصة بذلك ، إذا كانت مصلحة التحقيق تقتضي البحث عن الأدلة داخلها، والشاهد المعلوماتي عدة أصناف يجوز لقاضي التحقيق إستدعاء من شاء منهم لسماعه[3].

1- القائم على تشغيل الحاسوب :وهو المسؤول عن تشغيل الحاسوب والمعدات المتصلة به وهو شخص تتوفر فيه الخبرة الكافية في مجال تشغيل الجهاز وإستخدامه.

2- المبرمجون :و هم الأشخاص المختصمون في كتابة البرامج المعلوماتية وهم فئتان:

أ .مخططو برامج التطبيقات:يقوم هؤلاء بالحصول على خصائص ومواصفات النظام المعلوماتي المطلوب من محلل النظم ثم تحويلها إلى برامج دقيقة لتحقق هذه المواصفات.

---

[1] _عائشة بن قارة، المرجع السابق،125.

[2] _عبد العال الدربي، المرجع السابق،ص312.

[3] _نزيهة مكاري، المرجع السابق،ص75.

ب .مخططو برامج النظم :يقوم هؤلاء بتصحيح وإختبار وتعديل برامج نظم الحاسوب الداخلية أي تلك الخاصة بالوظائف المتعلقة بتجهيز الحاسوب بالبرامج والأجزاء الداخلية منه.

3- المحللون :هم فئة من الأشخاص مهمتهم تحليل الخطوات وجمع ببيانات النظام المعلوماتي ثم تحليلها، أي تقييمه لوحدات منفصلة و إستنتاج العلاقات الوظيفية بين هذه الوحدات.

4- مهندسو الصيانة و الإتصالات : هم فئة المسؤولين عن أعمال الصيانة الخاصة بالحاسوب والشبكات المتصلة به.

5 – مديرو النظم :وهم من توكل لهم إدارة النظم المعلوماتية[1].

ثالثا :إلتزامات الشاهد المعلوماتي:

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج إلى أنظمة تشغيل الحواسيب أو الشبكات، التي تحتوي على الأدلة الإجرامية غير أن هذا الطرح يبقى نسبيا نظرًا للتوصيات المقدمة من قبل المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات المنعقد بريو دي جانيرو – البرازيل و الذي أوصى بضرورة التعاون الفعال بين المجني عليهم والشهود وغيرهم من مستخدمي التكنولوجيا المعلومات في سبيل مكافحة هذا النوع من الجرائم وينقسم الفقه إلى إتجاهين:

1-الإتجاه الأول :يرى أنصاره أنه ليس من الواجب على الشاهد وحسب المنظور التقليدي لإلتزاماته، أن يقوم بطباعة البيانات المخزنة في ذاكرة الحاسوب ولا بتحليل ذاكرة النظام المعلوماتي فهذا العمل الخبير وهو ما عمل به التشريع الألماني والتركي[2].

2-الإتجاه الثاني :يرى أنصاره أن الشاهد المعلوماتي يستطيع القيام بطبع المعلومات وتحليل البيانات والكشف عن كلمات السر وهو ما أخذ به التشريع الفرنسي والهولندي[3].

---

[1]_– رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة، 16 و 17 نوفمبر 2015 ، كلية الحقوق ، جامعة بسكرة، الجزائر ،ص4،5.

[2]_عائشة بن قارة، المرجع السابق،ص129،130.

[3]_عبد العال الدربي، المرجع السابق،ص316.

خاتمة

بعد إستعراضنا لموضوع البحث يتضح جلياً مدى التحول الذي لامس البحث في مجال العلوم الجنائية، فقد تأثرت هذه الأخير بالتطور التكنولوجي وبالخصوص تقنيات المعلومات. ويمكن إجمال النتائج التي تم التوصل إليها في هذا البحث إلى :

1-إن التقنية المعلوماتية أصبحت من أساسيات حياة الدول و الشعوب و لا يمكن تصور فكرة التخلي عنها، نظراً لتزايد مجالات إستعمالاتها في كافة المجالات ، و ذلك بالرغم من كافة التهديدات التي تشكلها الجريمة المعلوماتية على أمن و سلامة نظمها و مستعمليها.

2- يستحيل القضاء على الظاهرة الإجرامية المعلوماتية بشكل نهائي ، و ذلك لإتصالها المباشر بتقنية المعلوماتية ، ففكرة التخلي عن هذه التقنية هي الحل الوحيد لمشروع القضاء على الجريمة المعلوماتية ، و ذلك بالرغم من درجة التطور التي آلت إليها المنظومة القانونية العقابية منها و الإجرائية في مجال مكافحة الجريمة المعلوماتية.

3-ظهور فئة جديدة من المجرمين و الضحايا تحت و صفي " مجرمي المعلوماتية " و"ضحايا الإجرام المعلوماتي " فالفئة الأولى أهم ما يميزها هو الذكاء و العلم و المعرفة ، و الخطورة الإجرامية في مجال المعلوماتية ، و ذلك بالرغم من خلو ملامحهم الشخصية من ملامح المجرمين المتعارف عليها في أصول علم الإجرام ، و هو ما يزيد من درجة خطورتهم وتهديدهم نظراً لكونهم خارج مجال الشك و الريبة مما يعزز ثقتهم في انفسهم على مواصلة نشاطهم الإجرامي و السعي إلى تطوير أساليبهم الإجرامية ، أما الفئة الثانية فعادة ما يميزها قلة المعرفة و التقدير بمجال المعلوماتية و هو ما يجعل منها أهدافا سهلة لمجرمي المعلوماتية.

4-تصنيف الجرائم المعلوماتية في صورة الإستغلال الجنسي للأطفال و كذلك جرائم الحض على الكراهية و التمييز العنصري ، من بين أخطر الجرائم نظراً لقلة حيلة و ضعف الضحايا في هذه الخالة لما قد تتسبب فيه من قيام نزعات بين الشعوب.

5-إن إجراءات البحث و التحقيق المعلوماتي هي إجراءات من نوع خاص يشترط لمباشرتها التقييد بمجموعة من الشروط أهمها شرط التقييد بالنص الإجرائي الملائم ، لما قد تنطوي عليه هذه الإجراءات من مساس بالحريات الفردية و إطلاع على مستودع سر الإفراد كالتصنت الإلكتروني وإعتراض البريد الإلكترون، و حجز للمعطيات و البيانات الشخصية و كل ذلك حفاظا على سلامة الإجراءات من طائلة البطلان و كذلك حفاظا على حريات الأفراد وكرامتهم.

6- تخضع إجراءات البحث و التحقيق المعلوماتي لإختصاص جهات متخصصة في التعامل مع الجرائم المعلوماتية ، تعتمد في تكوينها على مجموعة من المختصين في مجال المعلوماتية وكذلك في مجال التحقيق الجنائي ، مما يجعل منهم أفضل الأشخاص الذين يستطيعون التكفل بمهام البحث والتحقيق في الجرائم المعلوماتية ، نظراً لتقديرهم العلمي و المعرفي بالأساليب الإجرامية المعلوماتية وكذلك القواعد القانونية للتعامل بالشكل الشرعي مع الجريمة المعلوماتية ، إضافة إلى مراعاتهم لجملة من القواعد العملية الإحتياطية منها و الأصلية عند مباشرة الإجراءات التي تهدف إلى جمع الأدلة بشكل يكون الهدف منه ضمان حسن سير الإجراءات و الحفاظ على سلامتها من طائلة البطلان و كذا سلامة الأدلة من مخاطر التلف و الفقدان.

7-تعتمد إجراءات البحث و التحقيق في مجال الجرائم المعلوماتية على القواعد الفنية العملية أكثر منه على القواعد الإجرائية القانونية ، فلا جدوى من النص دون توفر المهارة اللازمة في التعامل مع الجريمة المعلوماتية، كما ان حسن سير الإجراءات ذات الطبيعة الفنية و العملية يعتمد مباشرة على مدى توفر الوسائل المادية الضرورية من حواسيب متطورة و شبكات إتصال مؤمنة ، و برامج خاصة تسمح بتحصيل الدليل الإلكتروني ، تسهل من مهمة الخبير في مجال البحث و التحقيق المعلوماتي.

بعد إستعراض النتائج تم التوصل إلى مجموعة من التوصيات:

1- تعزيز عمل الجهات الأمنية و القضائية في مجال مكافحة الجرائم المعلوماتية ، و ذلك من خلال حسن تدريب الكفاءات العاملة على طبيعة الإجراءات المتخذة في مجال الجرائم المعلوماتية ومدى خصوصية هذا النوع من الجرائم و المجرمين في آن واحد ، إضافة إلى تعزيزهم بأحدث الوسائل التكنولوجية في مجال المعلوماتية من حواسيب و برامج معلوماتية تسمح لهم بتأدية مهامهم على اكمل وجه.

2- ضرورة العمل على تحسيس ضحايا الجرائم المعلوماتية بضرورة التبليغ عن أي جريمة معلوماتية قد يقعون ضحايا لها ، و ذلك من أجل السماح للجهات المكلفة بالبحث والتحقيق بالإطلاع على مدى جسامة و حقيقة الجريمة المعلوماتية ، إضافة إلى الإطلاع على كافة الأساليب الإجرامية الحديثة المستعملة في مجال الجريمة المعلوماتية ، و التي يمكن ان تبقى محل خفاء في حال عدم تبليغ الضحايا عن الجرائم المعلوماتية التي تستهدفهم.

3- وضع سجل أمني إلكتروني يتضمن قائمة بمجرمي المعلوماتية يسمح بوضعهم تحت المراقبة الأمنية أي رصد نشاطاتهم المعلوماتية المشبوهة عبر الشبكة، و التي تنذر بوقوع جريمة معلوماتية.

ملحق

قاموس المصطلحات المعلوماتية

مودم	Modem	إختصار لكلمةModulateur و هو جهاز يربط الحاسوب بشبكة الأنترنت و منه ببقية الحواسيب المتصلة الشبكة يعمل من خلال نقل البيانات بعد تحويلها من رقمية إلتناظرية قابلة للنقل عبر خط الهاتف في حال إرسالها والعكس من ذلك في حال إستقبالها
الخادم	serveur	برنامج أو جهاز حاسوب يوفران المعلومات بالنسبة للحواسيب أو البرامج العميلة المتصلة به
بروتوكول	protocol	مجموعة من القواعد المتفق عليها و التي تتيح إتصال البرامج و الأجهزة المختلفة و غير المتوافقة مع بعضها البعض ، فهي اللغة التي تتخاطب بها الحواسيب المتصلةعبر الشبكة بهدف تبادل المعلومات ، فهو و بلغة تقنية الوصف الرسمي للقواعد التي ينبغي على حاسوبين إتباعهالتبادل المعلومات و الرسائل
خادم البروكسي	Proxy serveur	إحتياط أمني يتيح للمستخدم الموجود خلف الجدار الناري من إستعراض محتويات الويب دون تعريض محتويات الشبكة الخاصة لخطر الإطلاع عليها
مزود الخدمة	Service provider	الشركة التي توفر الوصول المباشر للأنترنت
تطبيق معلوماتي	Application	برنامج موضوع خصيصا من أجل مساعدة المستخدم على تنفيذ بعض المهام الخاصة على الحاسوب كمعالجة النصوص مثلا

بروتوكول التحكم بنقل البيانات / بروتوكول أنترنت	Transmission Control Protocol/internet protocol (tcp/ip)	مجموعة من البروتوكولات التي تحدد نظام نقل البيانات عبر شبكة الأنترنت ، توصف بأنها الغراء الذي يشد أجزاء الأنترنت بعضها لبعض ، فتحقق الترابط بين شبكات متباعدة فيزيائيا بصورة مباشرة لتشكل معا شبكة إفتراضية واحدة تعرف بإسم " الأنترنت"
فيروس	virus	برنامج يقوم بإحداث تلف متعمد على الحاسوب و عادة ما يكون في صورة برنامج خفي على الشبكة أو لصيق بأحد البرامج.
الويب	web	عبارة عن مجموعة من المستندات(وثائق ، صور ،فيديوهات.....) المتصلة في شكل نصوص تشعبية HTML ، متواجدة على أجهزة خادم الويب يمكن الوصول إليها عن طريق عناوين الأنترنت URL و قد تم إستحداث الويب كمصدر للمستندات المباشرة بواسطة علماء الفيزياء في المعمل الأوربي للفيزياء الجزيئية بسويسرا
عنوان الموارد الموحد	Uniform Resource Locator (URL)	مؤشر يدل على مكان وجود صفحة أو أي نوع أخرمن الموارد ضمن فضاء الويب.
عنوان بروتوكول الأنترنت	Adresse internet Protocol (Adresse IP)	يعرف أيضا بالعنوان الرباعي المنقط ، و هو عنوان رقمي خاص بكل حاسوب يضمن التعريف به على شبكة الانترنت و تحديد موقعه ، يتكون من أربعة مجموعات من الأرقام تفصل بينها النقاط
ثنائي	Binaire	نظام رقمي يعتمده الحاسوب يستخدم فيه لغة رقمي الصفر و الواحد كأساس للعد

جدار النار أو حاجز النار	Fire Wall Par Feu	أحد الإحتياطات الأمنية على شبكة الأنترنت يحمي المعلومات أو يمنع الوصول إليها ، كما يضمن عدم إلحاق الضرر بالمستخدمين من خلال حماية نظم التشغيل الخاصة بهم ، يعمل الجدار الناري في شكل نظام أمني ينظم حركة مرور المعلومات عند حدوث إتصال بين شبكتين على الأقل ، فيسمح لحزم البيانات بالمرور أو يمنعها بين الشبكتين ، و ذلك إعتمادا على مجموعة من القواعد التي يحددها مدير الشبكة مثل إسم المستخدم و كلمة السر
رقمي	Digital Numérique	كل تمثيل للقيم المسموعة أو المرئية إلى بتات Bits، فالقرص المظغوطCD هو وسيط تخزين رقمي لأن الأصوات التي يتم تحويلها إلى بتاتBits ثم يتم تخزينها عليه ، و عند تشغيله يقوم المشغلPlayer بإعادة تحويل تلك البتاتBits إلى إشارات تناظرية Analogثم يرسلها عبر السماعات في شكل أصوات.
عنوان بريد إلكتروني	Adresse Electronique	و عبارة عن عنوان إلكتروني مشابه للعنوان البريدي يتداول عبره البريد الإلكتروني ، يتكون من إسم المستخدم و عنوان على شبكة الأنترنت مفصولين بعلامة مميزة هي@
ADSL تقنية	ADSL	تقنية ربط بالشبكات(شبكة الأنترنت) ، عن طريق استعمال الهاتف الثابت ، تمنح قوة تدفق أقرب لتلك التي توفرها تقنية الالياف البصرية.

الفهـــــــــرس

المصـــــادر

والمـــــراجع

أولاً: المصادر القانونية.

أ_ الإتفاقيات والمعاهدات الدولية.

1-إتفاقية بودابست لمكافحة الجرائم المعلوماتية، المنبثقة عن اجتماع المجلس الأوربي ببودابست ، المحر تحت رقم 185، بتاريخ 21 نوفمبر 2001.

2-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المنبثقة عن اجتماع مجلس الوزراء الداخلية و العدل العرب بصفة مشتركة، بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة مصر بتاريخ 21/12/2010.

ب_ القوانين.

1-الأمر رقم 165/66 المعدل والمتمم بالقانون رقم 02/15 المؤرخ في 23 يوليوسنة 2015، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 40.

2- القانون رقم 04/09 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادرة في 16 أوت 2009.

3-القانون 03/ 2000 المؤرخ في 5 أوت 2000 المحدد للقواعد المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 48، الصادرة 6 أوت 2000.

4-الأمر05/03المتعلق بحقوق المؤلف والحقوق المجاورة،بتاريخ الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد44،الصادرة ب2003/07/23.

5- الأمر08/03المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة،بتاريخ الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ،العدد36،الصادرةب2003/07/23.

6- القانون23/06،الصادر بتاريخ20ديسبر2006المعدل والمتمم الأمر66-156المتضمن قانون العقوبات،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، العدد 84.

7- الأمر02/15 المعدل والمتمم للأمر155/66 المتضمن قانون الإجرات الجزائية،المؤرخ في2015/07/23،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ،العدد 40.

8- القانون 15/04،المؤرخ بتاريخ10نوفمبر2004،المعدل والمتمم للأمر66-156 المتضمن قانون العقوبات،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد71.

ج_ المراسيم.

1- المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر 2015 و المتضمن تحديد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم ، 53 الصادرة بتاريخ 08 أكتوبر 2015.

2-المرسوم الرئاسي رقم 183/04 الصادر بتاريخ 27 يونيو 2004 ، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 41.

3- المرسوم06-299 المؤرخ في 02 سبتمبر2006،التصديق على البروتوكول الإختياري الملحق باتفاقية حقوق الطفل،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، العدد 55.

ثانياً: المراجع.

(أ): الكتب

1- أحسن بوسقيعة،الوجيز في القانون الجزائي الخاص،الجزء الأول،الطبعةالخامسة عشر،دار هومة،الجزائر،2013.

2-محمّد عبيد الكعبي ،الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت،دار النهضة العربية،القاهرة، بدون سنة نشر.

3-محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2004.

4- عبد العال الدريبي، الجرائم الإلكترونية،دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر،2012.

5- حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض،السعودية، 2000.

6- هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها، الطبعة الأولى، دار النهضة العربية ،مصر . 2008

7- محمد حماد الهيتي، التكنولوجيا الحديثة و القانون الجنائي، الطبعة الثانية، دار الثقافة للنشر و التوزيع،عمان، الأردن،2012.

8- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2010.

9- علي بن عبد الله غسيري ، الأثار الأمنية لأستخدام الشباب للأنترنت، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض ، السعودية، 2004.

10- بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية دراسة مقارنة، الطبعة الأولى،منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.

11- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت(الجريمة المعلوماتية)، دارالثقافة للنشر والتوزيع، عمان الأردن،2009.

12- محمد سيد سلطان، قضايا قانونية في أمن المعلومات و حماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الكويت،2012.

13- سامي على حامد عياد، الجريمة المعلوماتية و إجرام الأنترنت، دار الفكر الجامعي، الإسكندرية، مصر ، 2007.

14- ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2012.

15- عبد الكريم عبد الله، الحماية القانونية للملكية الفكرية على شبكة الأنترنت، دار الجامعة الجديدة،مصر، 2008.

16-محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، مصر، 2003.

17- العربي جنان،معالجة المعطيات ذات الطابع الشخصي،الحماية القانونية في التشريع المغربي والمقارن، المغرب2010.

18- أسامة أحمد المناعسة، جلال محمد القاضي، جرائم تقنية نظم المعلومات الإلكترونية،دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان ،الأردن،2010.

19-عائشة بن قارة،حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة الجديدة ، الإسكندرية ، مصر، 2010.

20-ضياء علي أحمد النعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى،المطبعة الوطنية، المملكة المغربية ، 2001.

21-عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الإبتدائي في الجرائم المعلوماتية- دراسة مقارنة. على ضوء القواعد العامة للإجراءات الجنائية، الطبعة الأولى، دار النهضة العربية، مصر، 2009.

22- خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع ، عمان، الأردن، 2001.

23-يوسف حسن يوسف ، الجرائم الدولية للانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية ،القاهرة، مصر،2001.

24-ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر 2007.

25-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة الإستدلالات، دار الفكر الجامعي، مصر،2007.

26-علي عدنان الفيل، إجراءات التحري و جمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، دار الكتاب الجامعي الحديث، الإسكندرية، مصر، 2012.

27- محمد عنب، إستخدام التكنولوجيا الحديثة في الإثبات الجنائي، دون ذكر دار النشر، مصر، ،2007.

28-عبد الفتاح عبد اللطيف الجبارة ، إجراءات المعاينة الفنية لمسرح الجريمة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن 2010.

29- فتوح الشادلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودورالشرطة، منشورات الحلبي الحقوقية،بيروت ، لبنان، دون ذكر سنة النشر.

30- علي حسن أحمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة،عالم الكتب الحديث، اربد، الأردن ، 2004.

31-حسن طاهر داود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف للعلوم الأمنية، الرياض، المملكة العربية ،السعودية 2000.

32- محمد الأمين البشيري، التحقيق في الجرائم المستحدثة،مركز الدراسات و البحوث، جامعة نايف للعلوم الأمنية، الرياض، السعودية ،2004.

(ب): الأطروحات.

1- غازي عبد الرحمن هيان الرشيد:الحماية القانونية من جرائم المعلوماتيةالحاسب و الأنترنت،أطروحة لنيل درجة الدكتوراةفي القانون،الجامعة الإسلامية في لبنان،كلية الحقوق،2004.

2- عبد الله بن سعود محمد السراني، فعالية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، رسالة مقدمة لأجل نيل شهادة الدكتوراه قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2009.

3- تركي بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية و قياس فعاليته، رسالة مقدمة لأجل نيل شهادة الدكتوراه، قسم العلوم الشرطية ، جامعة نايف للعلوم الأمنية ، الرياض، السعودية،2009.

4-إبراهيم بن سطم بن خلف العنزي ، التوقيع الإلكتروني و حمايته الجنائية، رسالة مقدمة لأجل نيل شهادة الدكتوراه،قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية،2009.

5-عمر بن محمد العتبي ، الأمن المعلوماتي و مدى توافقه مع المعايير المحلية و الدولية ، رسالة مقدمة لأجل نيل شهادةالدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية،2010.

(ت): المقالات العلمية.

1- الهاشمي الكسراوي "الجريمة المعلوماتية" ،مقالة علمية، مجلة القضاء و التشريع ،العدد07، جويلية 2006، مركز الدراسات القانونية و القضائية، وزارة العدل و حقوق الإنسان، الجمهورية التونسية.

2- نزيهة مكاري،" وسائل الإثبات في جرائم الاعتداء على حق المؤلف عبر الانترنت"، مقالة منشورة بمجلة14 سنة 2009 دون ذكر المعلومات المتعلقة بهيئة النشر، المناهج القانونية، العدد المزدوج13المملكة المغربية.

(ث): الملتقيات والبحوث:

1-سلمى مانع، دور الأمن المعلوماتي في مكافحة الجرائم المعلوماتية، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة. المعلوماتية بين الوقاية و المكافحة 16 و 17 نوفمبر 2015 كلية الحقوق، جامعة بسكرة، الجزائر.

2-محمد علي قطب، الجريمة المعلوماتية و طرق مواجهتها، الجزء الثالث، بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني، أكاديمية الشرطة البحرينية، مملكة البحرينية، 2011.

3-يوسف مسعودي، " النظام القانوني لحماية المصنفات الرقمية " ، مجلة الدراسات القانونية ، العدد 04 أوت 2009، مركز البصيرة للبحوث و الاستشارات و الخدمات التعليمية ، الجزائر.

4-عبد الرحمان حملاوي– دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية-

بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16 و 17 نوفمبر 2015 –كلية الحقوق – جامعة بسكرة- الجزائر.

5- عبد الله حسين علي محمود "إجراءات جمع الأدلة في مجال سرقة المعلومات" ،بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، مركز البحوث والدراسات،أكاديمية شرطة دبي، الإمارات العربية المتحدة،من 26 إلى 28 أفريل 2003.

6-عز الدين– قيادة الدرك الوطني- الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها - بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة- 16 و 17 نوفمبر 2015 -كلية الحقوق – جامعة بسكرة- الجزائر.

7-حسين بن سعيد الغافري،" التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت"، بحث منشور على الموقع الإلكتروني الرسمي للمركز العربي للبحوث القانونية و القضائية للجامعة العربية.

8- عاقلي فضيلة،الجريمة الإلكترونية وإجراءات موجهتها من خلال التشريع الجزائري ،بحث مقدم إلى أعمال الملتقى الدولي الرابع عشر بطرابلس،24و25مارس2017،جامعة باتنة1.

(ج): المواقع الإلكترونية:

1-الموقع الرسمي لقيادة الدرك الوطني – تاريخ التصفح 31 مارس 2017الرابط الإلكتروني

13Thttp://www.mdn.dz13T,

المراجع باللغة الأجنبية:

1__Jean- Philippe Humbert- le monde de la cyberdélinquance et l'image sociale du pirate informatique - thèse de doctorat- sciences de 'information est de la télécommunication université Paul Verlaine –Metz – France_2007 .

2_ Myriam Quéméner- Yves Charpenel – La Cybercriminalité- Edition Economica- Paris- France- 2010.

okacha

Digitally signed by okacha
DN: cn=okacha gn=okacha c=France i=FR
Reason: I am the author of this document
Location:
Date: 2017-06-12 20:55+02:00