غرداية

كلية الحقوق والعلوم السياسية

قسم الحقوق

خصوصية الجريمة المعلوماتية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق تخصص قانون جنائي

إعداد الطالب:

-بوعرعارة إبراهيم زياد

إشراف الأستاذ:

-د. حمو فخار

الأستاذ المساعد:

-د.ماشوش مراد

لجنة المناقشة:

لقب واسم الأستاذ	الرتبة	الجامعة	الصفة
حاج إبراهيم عبد الرحمان	أستاذ التعليم العالي	جامعة غرداية	رئيسا
بن فردية محمد	أستاذ التعليم العالي	جامعة غرداية	مناقشا

نوقشت بتاريخ..../.../...

الموسم الجامعي:1442-1443هـ/2021-2022م

غرداية

كلية الحقوق والعلوم السياسية

قسم الحقوق

خصوصية الجريمة المعلوماتية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق تخصص قانون جنائي

إعداد الطالب:

-بوعرعارة إبراهيم زياد

إشراف الأستاذ:

-د. حمو فخار

الأستاذ المساعد:

-د. ماشوش مراد

لجنة المناقشة:

لقب واسم الأستاذ	الرتبة	الجامعة	الصفة
حاج إبراهيم عبد الرحمان	أستاذ التعليم العالي	جامعة غرداية	رئيسا
بن فردية محمد	أستاذ التعليم العالي	جامعة غرداية	مناقشا

نوقشت بتاريخ..../.../...

الموسم الجامعي:1442-1443هـ/2021-2022م

"يصبح أي تمييز، مثل المنعطفات الحادة في الطريق، أمرًا بالغ الأهمية بسبب السرعة الهائلة التي نسافر بها في عالم التكنولوجيا الفائقة لاقتصاد الخدمات."

-كلارنس توماس

"نحن نفتقر إلى الحكمة، نحن في مستوى عالٍ من التكنولوجيا. إلى أين ستقود؟"

-بول ماكريدي

"نحن قادمون على عصر القرود، فبرغم هذا الكم من التكنولوجيا التي وصل إليها الإنسان، إلا أننا أصبحنا أمام إنسان أقل رحمة، أقل مودة، أقل عطفا، أقل شهامة، أقل مروءة، وأقل صفاء من الإنسان المتخلف."

-مصطفى محمود

اهداء

الى جدتي رحمة الله عليها

إلى من لا يمكن للكلمات

أن توفي حقهما

أبي وأمي

إلى أخي وأخواتي

وإلى كل الأهل والأقارب

إلى أساتذتي

وجميع الأصدقاء والزملاء

نهدي لهم ثمرة جهدنا المتواضعة.

شكر وتقدير

أولا الحمد والشكر لله تعالى الذي ألهمني وأعانني ووفقني على إتمام بحثي هذا والذي آمل أن أكون قد حققت الغاية المرجوة منه، كما أخص بالشكر والتقدير والاهتمام الأستاذ فخار حمو الذي تفضل بالإشراف على هذه المذكرة والأستاذ ماشوش مراد الذي قدم النصح والإرشاد ولم يبخل علينا بتوجيهاته ونصائحه القيمة التي كانت عون لنا في اتمام هذا البحث طوال فترة إعداد المذكرة فلهما مني فائق الاحترام والتقدير.

وقبل أن نمضي نقدم أسمى آيات الشكر والامتنان والتقدير والمحبة إلى الذين حملوا أقدس رسالة في الحياة إلى الذين مهدوا لنا طريق العلم والمعرفة إلى جميع أساتذتنا الأفاضل، واخص بالذكر كل أولئك الذين خدموا وساهموا في توفير وخلق الجو المناسب.

قائمة المختصرات

IP	Internet Protocol
IC3	Internet Crime Complaint Center
IFCC	Internet Froude Complaint Ccenter
NWC	National White Collar Center
ICROS	Internet Crime Reporting Online System
TCP	Tram Mission Control Protocol

المقدمة

ما لا شك فيه، أن الانسان قد طوّر من نفسه على مرِّ العصور. حيث يعيش الانسان اليوم في اوج عطائه، سواء اقتصادياً، علمياً، تنظيمياً، وعلى جميع الأصعدة. حيث أصبحت الحياة أكثر مرونة وسلاسة من أي وقت سبق. كل الفضل قد يعود للتكنولوجيات الحديثة، خاصة تلك المتعلقة بمجال التقنية المعلوماتية. اذ تمكنت الحواسيب الالية وشبكة الانترنت من فرض نفسها على جميع المجالات نظرا لدقتها والسرعة التي تتمتع بها.

لكن لا يمكننا انكار أن الجريمة ظاهرة قديمة عرفتها المجتمعات البشرية منذ القدم هي الأخرى، وكانت دائما تجد طريقها من خلال استغلال هذه التطورات للدفع بقدراتها، نشاطها، امتدادها، وفعاليتها. فبقراءة تاريخ العالم وتطوراته على مر الزمان، سنلاحظ ملحمة من سفك الدماء، الجشع، والغباء الذي رافق هذه التطورات والذي يستحالُ تجاهله. ومع ذلك، لا يزال الانسان يطمح بطريقة ما الى تأسيس مستقبل مشرق، حيث تحاول التشريعات جاهدة في وضع بعض القيود على تصرفات الافراد لإستثبات الأمن والحفاظ على الحقوق لدى الفرد والمجتمع وبناء ثقة أكبر.

بعد ما غزت تقنية المعلوماتية جميع المجالات وازدادت تأصلاً في مجتمعاتنا وأصبح التمتع بايجابياتها في متناول الجميع، كان لا بد من بداية ملاحظة الانعكاس السلبي لها، اذ برزت طائفة جديدة من الجرائم التي لم يتفق الفقه الجنائي على ايراد تسمية موحدة لها نظرا لأن الجريمة المعلوماتية جريمة حديثة نسبيا. كما كانت هناك اتجاهات مختلفة في تعريفها كونها تتسم بمجموعة من الخصائص والسمات التي لا تتميز بها غيرها من الجرائم التقليدية والجرائم الأخرى، سواء من حيث كشفها، نطاق وقوعها، عدد ضحاياها، طرق تنفيذها، او استراتيجيات مكافحتها.

امتد بروز هذه الجرائم لخلق طائفة جديدة من المجرمين يتسمون هم الاخرون بدورهم بخصائص وسمات تميزهم عن غيرهم من المجرمين، المجرم المعلوماتي في الغالب لا يمت لأنماط المجرم التقليدي بصلة، حيث يكون شخصاً عادياً في اغلب حياته، يعيش في منزل

جميل بضاحية جميلة، يربي حيوانات اليفة، يدرس في مدرسة جيدة، مهذب، مثقف، وذو تربية حسنة. لكن في نفس الوقت، يعيش حياة موازية خبيثة فاسدة ومليئة بالفوضى والاجرام.

تمنح المعلوماتية سهولة في الاتصال والوصول للمعلومات وإمكانيّات لا حصر لها، ما يجعل من إمكانية التحكم في هذا النوع من الجرائم امرا بالغ الصعوبة ان لم يكن بالأمر الشِبه مستحيل. حيث خلقت الجريمة المعلوماتية عائقاً للتشريعات في وضع استراتيجيات فعالة ومناسبة لمكافحتها من جهة، وتحدياً لرجال انفاذ القانون في التعامل معها من جهة أخرى، مما أوجب سعي اغلب التشريعات الى فهمها وسن إجراءات وقوانين تتماشى مع طبيعتها.

وسعى رجال انفاذ القانون هم الأخرون للرَّفع من مستوى قدرات أعضائهم على المستوى الفني والتقني، وتوظيف أحدث الوسائل المتاحة واكثرها تطوراً، لبناء أجهزة أمنية ذات مستوى اعلى كفاءة لمجابهة الجريمة وإزالة الغموض عنها وكشف حقائقها، بل قد يتعدى الأمر ذلك بالاستعانة بأشخاص أكثر خبرة في المجال السيبراني في حالة عدم توفر الأجندة اللازمة لدى مصالح انفاذ القانون.

خاصة أن عدد كبير من مجرمي المعلوماتية يعتمدون على خاصية الاختفاء او التقاعد المبكر بعد جمع مبالغ مالية ضخمة، مِما يجعلهم متقدمون بخطوة في اغلب الأحيان عن الأجهزة الأمنية، حيث يتمكنون من الإفلات بفعلتهم والهروب من مسؤوليات الضرر المترتب عن أفعالهم، مما يجعل الأنظمة القانونية امام تهديد هدم الثقة.

تتجلى أهمية هذه الدراسة في تغيير المعتقد السائد بين الناس أن الجرائم المعلوماتية تُرتكب في عالم آخر بعيد عن عالمهم، وفي الواقع، يمكن لهذه الجرائم أن تضر بهم يوميا حتى من دون أن يشعروا بذلك. وفي إدراك كيف أصبحت المعلوماتية جزء لا يتجزأ من العالم الذي نعيشه، يلجأ الانسان لاستعمالها في جميع الأماكن وكل الأوقات وشتى المجالات، حيث

تبدو لوهلة بانها مجرد عالم افتراضي، لكن في باطنها هي عالم جديد موازي يشكك في كل ما بناه أسلافنا في العالم الواقعي.

إن تعلقنا بالحواسب والأنظمة المعلوماتية أمر لا ريب فيه، واحد من الأسباب الوجيهة لاختيار دراسة موضوع الجريمة المعلوماتية واثارته، حيث يندرج الموضوع ضمن اهتماماتي الشخصية، وإن غموضها وحداثتها يثيران الفضول والرغبة في محاولة معاصرة هذه الجرائم وتحليلها وإزالة بعض الغموض عنها. أحيانا تكون أفضل طريقة لتفادي العاصفة هي المرور عبرها او التجول حولها. كما انه لا بد من النظر اليها من الجانب القانوني، بناء على التغيرات السريعة والمتنامية التي تطرأ عليها. خاصة وأن الموضوع حديث من الجانب الموضوعي لتجريم الأفعال او الاعتداءات الماسة بأنظمة المعالجة الألية للمعطيات، والقواعد الإجرائية الخاصة للحماية منها.

تهدف دراستنا للجريمة المعلوماتية الى بعض النقاط الأساسية وهي:

-اثراء النقص في المراجع المتخصصة في الجرائم المعلوماتية.

-اظهار خصوصية الجريمة المعلوماتية وخصوصية المجرم المعلوماتي ومدى امكانياته.

-اظهار مدى خطورة الجريمة المعلوماتية والحاجة الى مكافحتها وضرورة التصدي لها.

-تحديد أجهزة التحقيق في الجريمة المعلوماتية.

-رؤية مدى كفاءة السلطات في التعامل معها، واستعداد التشريعات القائمة على مواجهة هذا الخطر المجهول.

-تغطية موضوع لم يتم استكشافه الا قليلا في القانون الجزائري، هناك إطار دائم التوسع للجريمة والإجراءات الجنائية في القانون الدولي، وهناك العديد من الأسئلة تدخل سلطات الدولة في الحياة الخاصة أو القيود التي يجب وضعها.

-يهدف هذا البحث الى التركيز على جرائم المعلوماتية العامة التي يمكن ان تؤثر على المواطنين والشركات في حياتهم اليومية، ولا يمتد لتهديدات الإرهابية، او الهجمات على أمن الدولة، أو التجسس بين الدول، كما لا تتناول الدراسة الجوانب العسكرية لتهديدات السيبرانية ولا على صلاحيات واختصاصات جهاز المخابرات في هذا المجال.

استندنا في دراستنا لخصوصية الجريمة المعلوماتية الى عدة دراسات سابقة تميزت بدراستها للجانب الإجرائي، خلاف الدراسات السابقة التي كانت تصب جل اهتمامها على الناحية الموضوعية فقط. ومن بين هذه الدراسات:

-عميش رحاب، الجريمة المعلوماتية.

-بويقرة خيرة، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري.

-بوعمرة محمد، بنينال سيد علي، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري.

غير أنه واجهتنا بعض الصعوبات في انجاز البحث، كون الموضوع حديث نتج عنه نقص في المراجع الذي تعالج الموضوع بوضوح وتعمق من كل جوانبه. كما ان الموضوع يتمتع بجانب تقني وفني يستلزم متخصصا ملم بالموضوع، وغياب التعريفات والتسميات الموحدة لهذا الموضوع، أدى الى تواجد العديد من الآراء ووِجهات النظر المختلفة.

ان ظهور الاجرام المعلوماتي اثار العديد من المشاكل في الجانب الموضوعي والجانب الإجرائي خاصة باعتبار ان تلك الجرائم لها خصوصيات وسمات تجعل منها جرائم صعبة بالخصوص وأنها تقوم على المسرح المعلوماتي الغير مادي والذي يختلف عن مسرح الجريمة التقليدي إضافة على غرار ان ثورة الاتصالات والمعلومات استحدثت أنواع جديدة من الجرائم الا انها استحدثت أنواع من المجرمين اللذين يتسمون بدورهم بخصائص و سمات خاصة كما انهم يفلتون في اغلب الأحيان من العقوبات، ومنه كان لا بد من مواكبة

هذا التطور الملحوظ في الجرائم المعلوماتية موضوعيا واجرائيا لمواجهة هذه المخاطر،، بالتالي ومن خلال مشكلة الدراسة يمكننا أن نتساءل عن:

فيما تتمثل الخصوصية الموضوعية والإجرائية للجريمة المعلوماتية التي تثيرها في واقعنا العملي؟

هذه الإشكالية يمكن أن نتفرع منها لعدة تساؤلات منها:

1-ما هي الطبيعة الخاصة للجريمة المعلوماتية؟

2-ما الطبيعة الخاصة للمجرم المعلوماتي؟

3-ما هي الهيئات المكلفة بالتحقيق في الجريمة المعلوماتية وخصائصها؟

4-فيما تتمثل اليات التحقيق في الجريمة المعلوماتية؟

وعلى هذا الأساس اعتمدنا على المنهج الوصفي المقارن، الذي يقوم بوصف هذه الظاهرة ومقارنتها، وذلك لأن الدراسة تهتم بخصوصية الجريمة المعلوماتية عن غيرها من الجرائم من الناحية الموضوعية والإجرائية.

حتى نتمكن من معالجة الإشكالية المطروحة ارتأينا تقسيم الخطة إلى فصلين معتمدين على تقسيم ثنائي للخطة.

ففي الفصل الأول سنتناول فيه الخصوصية الموضوعية للجريمة المعلوماتية والذي أدرجناه في مبحثين تناول كل منهما الطبيعة الخاصة للجريمة المعلوماتية كمبحث أول، والطبيعة الخاصة للمجرم المعلوماتي كبحث ثاني.

أما الفصل الثاني فتطرقنا إلى الخصوصية الإجرائية للجريمة المعلوماتية وأدرجناه كذلك في مبحثين هما: المبحث الأول: التحقيق في الجريمة المعلوماتية، أما المبحث الثاني: إجراءات الحصول على أدلة الإثبات للجريمة المعلوماتية.

الفصل الأول:

الخصوصية الموضوعية للجريمة المعلوماتية

الجريمة المعلوماتية هي جريمة تستند او تقوم على النظم المعلوماتية، هي ما يفصل بين الجريمة التقليدية والجريمة المستحدثة. لكن فيما قد تتجلى الخصوصية الموضوعية للجريمة المعلوماتية، هل هي ببساطة نمط اجرامي مثل باقي الأنماط المألوفة والمتفق عليها، أم أنها جرائم مختلفة وغير ملموسة للطبيعة الخاصة للبيئة المُرتكَبة عليها.

قد يمتلك معظم الناس فكرة خاطئة عن الجريمة المعلوماتية فالجريمة عموما في القانون الجنائي العام هي ذلك السلوك للفرد فعلا كان او امتناعا والذي يقابله عقاب جزائي. دعونا نقترح خيارا ثالثا خصوصية الجريمة المعلوماتية كأداة للقياس. فخصوصية الجريمة المعلوماتية لا تعتمد في الغالب على ارتكاب السلوك المحظور، بل تعتمد على سهولة ارتكابها، صعوبة اكتشافها، مجال امتدادها، عدد ضحاياها، الضرر الناجم عنها، وافلات مرتكبيها من تحمل مسؤوليات جرائمهم.

انتحال الشخصية، تهديد الأفراد، تحريض على أعمال غير مشروعة، السرقة، التزوير، الاحتيال، اختراق الأنظمة، تدمير النظم، التجسس، القاسم المشترك بينها أنها جرائم. الجريمة المعلوماتية لا تعني انها جريمة مغايرة، لا تعني انها غير مرتبطة بالسلوكيات الاجرامية التقليدية. الجريمة المعلوماتية في جوهرها هي ذلك القياس للخصوصية والسمات التي تحظى بها هذه الجريمة.

لكن قد تختلف الجريمة المعلوماتية عن الجريمة التقليدية في نوع الشخص المرتكب للفعل المجرم، حيث يختلف المجرم المعلوماتي عن نظيره المجرم التقليدي في الخصائص، الدوافع، المستوى الذي ترتكب به الجريمة، مستوى ذكائه ودرايته، قدرته للوصول لأكبر عدد ممكن من الضحايا، وقدرته على التواري عن الأنظار اثناء ارتكابه للجريمة أو بعدها.

المبحث الأول: الطبيعة الخاصة للجريمة المعلوماتية

تعتبر الجريمة الإلكترونية من الظواهر الحديثة لارتباطها بتكنولوجيا الحديثة، ولقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، حيث لم يتفق الفقه على تعريف محدد بل بعض الفقهاء، ذهب إلى ترجيح عدم وضع تعريف بحجة أن مثل هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني[1].

إن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب المادة 02 من القانون 09 -04 على أنها «: جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية«.

ويلاحظ على هذا التعريف ما يلي:

-أن المشرع قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكترونية، وثانيها معاير موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثا معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات[2].

المطلب الأول: خصائص الجريمة المعلوماتية

[1]- الشوابكة محمد أمين، **جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009،
ص08.

[2]- بوظياف إسماهان، **الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر**، العدد 11، سبتمبر 2018، ص 352-353.

لقد خلقت تكنولوجيا المعلومات أشكالا جديدة لارتكاب الجرائم، فهناك تشابه كبير بين الجرائم المعلوماتية وبين الجرائم التقليدية، فهي جميعاً تحتاج الى إجراءات تتشابه في عمومها مثل: المعاينة، التفتيش، المراقبة، التحريات والاستجواب بالإضافة الى جمع وتحليل الأدلة.

فقد لا يعني مصطلح الجريمة المعلوماتية بالضرورة وجود سلوك اجرامي جديد، بل هو مصطلح مبني الى حد كبير على أساس ان هذا السلوك السيبراني، هو عبارة عن طرق جديدة لارتكاب السلوك الاجرامي، او يمكن القول انه نموذج أقرب الى الطريقة التقليدية من حيث تحديد وتصنيف الجرائم. إلا أن الجرائم المعلوماتية تتميز عن غيرها من الجرائم التقليدية، من حيث اثباتها بشكل عام، وإجراءاتها وطبيعتها بشكل خاص.

إن استخدام تقنيات الاتصال، لا يسمح فقط للجريمة بالازدهار بل بالتطور بطريقة أكثر ضررا. وفي ظل البيئة المتقاربة التي نعيش فيها، يكاد يكون من المستحيل للضحية الاختباء من التعرض لي هذا النوع من الجريمة.

هذه المميزات التي أصبحت تمثل حاجزا للسلطات القضائية ونظام العدالة الذين يهتمون بمصداقيتهم. في اكتشاف هذه الجرائم واثباتها والوصول لمرتكبيها ناهيك عن تقييم نطاقها. ومع ذلك، يجب التأكيد على بعض الاختلافات. لهذا سنقسم هذه الخصائص الى الخصائص المتعلقة بكشف الجريمة المعلوماتية، أي من حيث صعوبة كشفها واثباتها، والخصائص المتعلقة بطبيعتها.

بالتالي نتناول هذا المطلب من خلال تقسيمه الى فرعين: نتحدث في الأول عن الخصائص المتعلقة بكشف الجريمة المعلوماتية، وفي الفرع الثاني نتطرق الى الخصائص المتعلقة بطبيعتها.

الفرع الأول: الخصائص المتعلقة بكشف الجريمة المعلوماتية

يصعب متابعة جرائم الحاسب الآلي والإنترنت وكذا الكشف عنها، ومعظم هذه الجرائم تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها، وتعود اسباب صعوبة اكتشاف وإثبات هذا النوع من الجرائم إلى الأمور التالية:

أولا–صعبة الاكتشاف: تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإذا اكتشفت فان ذلك يكون بمحض الصدفة عادة[1]. تشير الدراسات أن ما يتم اكتشافه من جرائم المعلومات يصل الى نسبة 1% والذي يتم الإبلاغ عنه من هذه النسبة لا يكاد يصل الى 5% فقط[2].

حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية ان الوسيلة المستخدمة لارتكاب الجريمة هي نبضة الكترونية ينتهي دورها خلال أقل من ثانية واحدة، وأن الجاني يقوم بتدمير الدليل بمجرد استعماله، ويقوم بذلك بكل هدوء ودون احداث أي ضجة، وذلك على خلاف الكثير من الجرائم التي نعرفها[3].

وعدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية. فبيانات الكمبيوتر متقلبة للغاية، يكفي الضغط على مفاتيح قليلة او استخدام برنامج ألي لمحوها، مما يجعل من المستحيل تتبع صاحب المخالفة، او اتلاف دليل ذنبه. يتم تخزين بعض أنواع البيانات لفترات قصيرة فقط قبل اتلافها. في حالات أخرى، إذا لم يتم جمع الأدلة بسرعة، فقد يعاني الأشخاص او الممتلكات من ضرر كبير[4]. كما ان الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، اذ ان الجريمة المعلوماتية جريمة عابرة للدول[5].

---

[1]– الصغير، جميل عبد الباقي، **القانون الجنائي والتكنولوجيا الحديثة**، ط1، دار النهضة العربية، القاهرة، 1992، ص17.

[2]– القطاونة مصعب، **الإجراءات الجنائية الخاصة في الجرائم المعلوماتية**، بحث مقدم لشبكة قانوني الأردن، 2010، ص05.

[3]–المطردي مفتاح بوبكر، الجريمة الالكترونية، ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان،23–25 أيلول، 2012، ص8

[4] JEAN-LUC PUTZ, **CYBERCRIMINALITE**, criminalité informatique en droit luxembourgeois, 2019, page38

[5]–الصغير جميل عبد الباقي، مرجع سابق

غالبا لا تتطلب جرائم المعلوماتية استثمارات او معدات كبيرة، فقط عن طريق الكمبيوتر والاتصال بالأنترنت، يمكن التصرف على مستوى العالم. من ناحية أخرى يمكن ان يكون عائد الاستثمار مثيرا للاهتمام ايضا[1]. كذلك فإن قدرة الجاني على تدمير دليل الإدانة في اقل من الثانية الواحدة يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم[2].

الجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه او لا يدري حتى بوقوعها والإمعان في حجب السلوك المكون لها واخفائه عن طريق التلاعب غير المرئي في النبضات او الذبذبات الالكترونية التي تسجل البيانات عن طريقها امرا ليس عسيرا في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبها[3].

كما ان المجني عليه يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك او تمْنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها[4].

إلى جانب ذلك فإن المجني عليه يتردد أحيانا في الإبلاغ عن هذه الجرائم خوفا من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي الى تكرار وقوعها بناء على تقليدها من قبل الاخرين كما ان الإعلان عن هذه الجرائم يؤدي أحيانا الى الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه[5].

الشعور بالعجز وبالتالي يمكن ان يولد شعور بالعجز داخل السلطات، وأيضا داخل الجمهور. لن يتقدم الضحية بشكوى، مدركا ان ذلك لن يؤدي الى شيء ملموس. الشرطي لن يغتنم الخدمات المتخصصة، معتبرا ان عمليات البحث منذ البداية محكوم عليها بالفشل. لن

[1] JEAN-LUC PUTZ, **CYBERCRIMINALITE**.p41

[2] – الصغير جميل عبد الباقي، مرجع سابق

[3] رستم، هشام محمد فريد، **الجوانب الإجرائية للجرائم المعلوماتية**، ط1، مكتبة الآلات الحديثة، أسيوط، 1994، ص16.

[4] المومني نهلا عبد القادر. **الجريمة المعلوماتية**، ط2، دار الثقافة للنشر والتوزيع، عمان، 2010، ص54

[5] الهيتي محمد حماد، **التكنولوجيا الحديثة والقانون الجنائي**، ط1، دار الثقافة للنشر والتوزيع، عمان, 2004، ص 166.

يسعى قاضي التحقيق للحصول على مساعدة جنائية متبادلة مع دولة أخرى للحصول على عنوان IP مدركا ان هذا سيوجهه فقط الى دولة ثالثة ثم الى دولة رابعة[1].

ثانيا–صعبة الاثبات: تتعلق عملية اثبات الجرائم بصفة عامة بإقامة الدليل, وذلك بالنظر الى نوع الجريمة والى الإجراءات التي يتم اتباعها للحصول على الدليل, وهذه الخطوات هي المتبعة في كل الجرائم بما فيها الجرائم المرتكبة عبر الانترنت, غير أن في هذه الأخيرة تكون عملية استخلاص الدليل صعبة للغاية نظرا لكون الأدلة في هذا النوع من الجرائم يتميز بخصوصيته المعنوية, بالإضافة الى ذلك الإجراءات المتبعة في اثبات هذه الأدلة اثبتت قصورها, فاذا كانت ذات فائدة في الجرائم التقليدية, فهي غير مجدية في جرائم الانترنت في غالب الأحوال, خاصة في ظل الطابع العالمي لهذه الجريمة[2].

اكتشاف الجريمة المعلوماتية امر كما سبق وأشرنا ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن اثباتها امر يحيط به كذلك الكثير من الصعاب[3]. وتعني الصعوبة في اثبات وقوع الجريمة بعد اكتشافها، أو بعبارة أخرى الصعوبة في إثبات التنفيذ، فبعد اكتشاف الجريمة والعلم بوقوعها، هناك صعوبة في إثبات أحداثها، والسبب من ذلك هو أن هذا النوع من الجرائم غالبا ما يتم تنفيذه بطرق مركزية صعبة ومهارات تخصصية عالية، ويتم في الوقت نفسه إخفاء أو مسح أي آثار قد يتركها الجاني[4].

الجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الامن وأجهزة التحقيق والملاحقة. ففي هذه البيئة تكون البيانات ولمعلومات عبارة عن نبضات

[1] JEAN-LUC PUTZ, **CYBERCRIMINALITE**, p44

[2]– صغير يوسف، **الجريمة المرتكبة عبر الانترنت**، مذكرة لنيل شهادة الماجيستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة تيزي وزو، تاريخ المناقشة:06-03-2013، ص124.

[3] –المومني نهلا عبد القادر، مرجع سابق، ص 56

[4]–بن شهرة شول، ماشوش مراد، **السمات الخاصة للجريمة المعلوماتية**، مجلة المستقبل للدراسات القانونية والسياسية، معهد الحقوق والعلوم السياسية–المركز الجامعي افلو، المجلد04، العدد01, 2020، ص 06

الكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل امر طمس الدليل ومحوه كليا من قبل الفاعل امرا في غاية السهولة[1].

تجدر الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح غالبا في إثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف آثارا مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائية الكشف عن الجريمة وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة المعلوماتية يتضاءل دوره والإفصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين[2]:

الأول: إن الجريمة المعلوماتية لا تخلف آثار مادية، يكون دليل الاثبات في الجريمة التقليدية مرئيا من ذلك السلاح الناري او الأداة الحادة المستعملة في القتل او الضرب، وكذلك المادة السامة التي تستعمل في القتل، او المحرر ذاته الذي تم تزويره، او النقود التي زيفت وأدوات تزييفها، وفي كل هذه الأمثلة يستطيع رجل الضبط او التحقيق الجنائي رؤية الدليل المادي وملامسته بإحدى حواسه[3].

لكن في الجرائم التي تقع على العمليات الالكترونية المختلفة خاصة التي تقع عبر شبكة الانترنت مثل التي تقع على عمليات التجارة الالكترونية، أو على العمليات الالكترونية للأعمال المصرفية، أو على اعمال الحكومة الالكترونية، يكون محلها جوانب معنوية تتعلق بالمعالجة الالية للبيانات، فإذا وقعت جرائم معينة على هذه الجوانب المعنوية، كجرائم السرقة او الاختلاس أو الاستيلاء أو الغش أو التزوير او الإتلاف فإنه قد يصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة[4].

---

[1] المومني نهلا عبد القادر، مرجع سابق.

[2]–المومني نهلا عبد القادر، المرجع السابق، ص 57

[3]–صغير يوسف، المرجع السابق، ص124

[4]–علي محمود علي حمودة، **الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الاثبات الجنائي**، مقال متوفر على الموقع التالي: http//www.arablawinfo.com

الثاني: إن كثيرا من الأشخاص يردون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها هي فترة طويلة نسبية، الأمر الذي يعطي مجالا للجاني أو للأخرين أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستسقاة من المعاينة في الجريمة المعلوماتية[1].

بالإضافة إلى ذلك فإن نقص الخبرة الفنية والتقنية لدى الأجهزة الأمنية يشكل عائقا أساسيا أمام إثبات هذه الجريمة ذلك لأنها تتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والإنترنت، ونتيجة لنقص الخبرة كثيرا ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة المعلوماتية فلا تبذل لكشف غموضها وضبط مرتكبيها جهودا تتناسب وهذه الأهمية. بل إن المحقق قد يدمر الدليل بمحوه محتويات الأسطوانة الصلبة عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة[2].

الصعوبة في تحديد مرتكبيها: وتعني الصعوبة تحديد الشخص أو الجهة التي ارتكبت الجريمة، فبعد اكتشاف وقوع الجريمة وبعد التثبت من أنها نفذت بالفعل، هناك صعوبة تحديد الشخص أو الجهة التي نفذت، والسبب من ذلك هو أن جرائم المعلوماتية غالبا ما تنفذ بطرق احترافية لا يوجد فيها روابط واضحة تربط الأحداث بمن نفذ هذه الأحداث، ويطلق بعضهم على جرائم المعلوماتية "جرائم ذوي الياقات البيضاء" لأنه قد يرتكبها أناس مؤهلون تأهيلا عاليا، وربما يحملون درجات علمية متقدمة تبعد الشكوك عنهم، ولا تدل مظاهرهم على أنهم مجرمون وهذا ما يصعب عملية الربط بين هؤلاء الأشخاص والجرائم التي يرتكبها، حتى لو كان الدافع من وراء ذلك هو إبراز المهارة وممارسة الهواية فقط[3].

يتطلب لارتكابها وجود جهاز إلكتروني: تتميز الجريمة الإلكترونية عن غيرها أن الجهاز الإلكتروني هو أداة الجريمة ووسيلة تنفيذها، أو هو موضوع الجريمة كإتلاف أو سرقة البيانات

---

[1]– بن شهرة شول، ماشوش مراد، مرجع سابق.ص07

[2]–بن شهرة شول، ماشوش مراد، مرجع سابق. انظر كذلك، القبائلي سعد حماد، **ضوابط الحماية الإجرائية لبرامج الحاسب الالي**، بحث مقدم لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، اريد, 2004، ص24.

[3]–القحطاني ذيب بن عايض، **امن المعلومات**، مكتبة مدينة الملك فهد للعلوم والتقنية، الرياض, 2015، ص332.

والمعلومات، كما تتطلب هذه الجريمة دراية كافية وخبرة فائقة بالكمبيوتر والإنترنت في بعض الجرائم، أو معرفة بسلوكيات الفعل المرتكب في الجرائم البسيطة منها، كما أنها لا تمتاز بالعنف، وأغلب الجرائم الإلكترونية ترتكب عبر الإنترنت[1].

إن ما يميز الجريمة الإلكترونية عن غيرها من الجرائم، أنها تتطلب وجود علم كافي بالجوانب الفنية والتقنية لاستخدام الحاسوب والإنترنت، وتعتبر العلاقة بين مدى الدراية بالجوانب الفنية والتقنية للحاسوب وبين الجريمة الإلكترونية علاقة طردية، فكلما زادت الخبرة لدى الأفراد بمعرفة تقنية الحاسوب، زاد احتمال استخدام خبرتهم بشكل غير مشروع[2].

كما أثبت الواقع العملي أن الجرائم الإلكترونية قد ترتكب من خلال الهواتف المحمولة، خاصة بعد ظهور أجهزة الهاتف الذكية والتي هي في الحقيقة عبارة عن أجهزة كمبيوتر صغيرة، والتي من خلالها يتم الاتصال بشبكة الإنترنت، ويسهل تخزين ونقل المعلومات من خلالها[3].

ليس كما ذكر بعض الباحثين بأن الحاسب الآلي هو الأداة الوحيدة في ارتكاب الجريمة الإلكترونية، ففي أيامنا هذه ترى أنه يمكن تصنيف الهواتف المحمولة الذكية ضمن أجهزة الكمبيوتر، وذلك لأنه لا يختلف عن الحاسوب سوى في الحجم، بل إن الهواتف الذكية يمكن من خلالها الاتصال المباشر بخلاف الحاسب الآلي، أما بالنسبة للوظائف الأخرى فتتم ممارسة جميع وظائف الحاسب الآلي من خلال الهاتف الذكي[4].

الفرع الثاني: الخصائص المتعلقة بطبيعتها

لقد أتاحت شبكة الانترنت إمكانية الاتصال بين عدة حاسبات ألية مهما كانت المسافة الفاصلة بينهما. حيث لم يعد هناك ما يحول دون تبادل المعلومات ونقلها بكميات مذهلة وبسرعة هائلة، وقد أدى ذلك الى نتيجة مفادها ان عدة أماكن متفرقة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة وفي ان واحد، حيث غالبا ما يكون الجاني في بلد والمجني عليه

[1]–القاضي رامي متولي، **مكافحة الجريمة المعلوماتية**، ط1، دار النهضة العربية، القاهرة, 2011، ص14.

[2] عبابنة محمود احمد، **جرائم الحاسب وابعادها الدولية**، ط2، دار الثقافة للنشر والتوزيع، عمان, 2017، ص22.

[3] القاضي رامي متولي، مرجع سابق، ص 16.

[4]–بن شهرة شول، ماشوش مراد، مرجع سابق. ص08

في بلد اخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه، وعليه تعتبر الجريمة المعلوماتية شكلا جديدا من الجرائم العابرة للحدود الوطنية او الإقليمية او القارية[1].

كما اتاحت في نفس الوقت سهولة في ارتكاب هذا النوع من الجرائم، ومرونة في التنفيذ فبمجرد توفر جهاز حاسب الي وخدمة انترنت، يصبح للمؤلف إمكانية التصرف على مستوى العالم.

أولا–الطبيعة الدولية للجريمة المعلوماتية :يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعددة الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة[2].

ومن القضايا التي لفتت النظر إلى البعد الدولي للجريمة المعلوماتية، قضية عرفت باسم مرض نقص المناعة (الإيدز)، وتتلخص وقائعها عام 1989 عند قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج التي يهدف في ظاهرها إلى اعطاء بعض النصائح الخاصة بهذا المرض، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)[3].

---

[1]–المناعسة أسامة احمد. الزغبي جلال محمد. **جرائم تقنية المعلومات الالكترونية**، دراسة مقارنة، ط1، دار الثقافة، عمان, 2014، ص95.

[2] - ENDRELIN, Clément.**Les moyens juridiques de lutte contre la cybercriminalité**, Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen,2011 , p15

[3]–عبابنة محمود احمد، **جرائم الحاسوب وأبعادها الدولية**، دار العلم والثقافة للنشر والتوزيع، عمان, 2006، ص45

وكان يترتب تعطيل الجهاز بمجرد تشغيله، ثم تظهر عبارة على الشاشة يقوم فيها الفاعل بطلب مبلغ مالي يرسل على عنوان حتى يتمكن المجني عليه من الحصول على مضاد لهذا الفيروس. وفي الثالث من فبراير 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة، وتقدمت المملكة المتحدة بطلب تسليمه لمحاكمته لديها باعتبار أن النشاط الإجرامي المتمثل في إرسال البرنامج تم في أراضيها، وأياً ما كان الأمر فإن لهذه القضية الأثر البالغ من ناحيتين[1]:

-الأولى: أنها المرة الأولى التي تتم فيها تسليم متهم في جريمة معلوماتية.

-الثانية: أن يتقدم شخص للمحاكمة **بتهمة إعداد برنامج مخرب.**

لقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي، أم تلك التي توجد بها المعلومات محل الجريمة، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب " إن المشرع الجزائري قد عقد الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبي وتستهدف الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، المادة 15 من القانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها".

كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة، ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما

[1] ماشوش مراد، مرجع سابق. ص09

يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية"[1].

وتعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية وتجنب خلق ما يسمى "بملاذات جرائم المعلوماتية " Computer Crime Havens"، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي بطبيعة الحال التنسيق بين قوانين الدول المختلفة لضمان تحقق "مبدأ ازدواجية التجريم" فيما يتعلق بجرائم المعلوماتية[2].

نجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم وإن كان مشرعنا قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات[3]، والذي استحدث نصوصًا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات بالإضافة إلى قانون 04/09 المؤرخ في 05 08 2009 المتضمن القواعد الخاصة للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته وسنّ أحكام خاصة بالتعاون والمساعدة القضائية الدولية (وقد علق المشرع الجزائري التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال على شرط احترام الاتفاقيات الدولية و الاتفاقيات الثنائية والمعاملة بالمثل)[4].

---

[1]– قورة نائلة عادل محمد. **جرائم الحاسب الاقتصادية دراسة نظرية وتطبيقية**، ط1، دار النهضة العربية، القاهرة, 2006، ص54.

[2]–ماشوش مراد. مرجع سابق، ص 10.

[3]–قانون 04–15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الامر 66–155 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج. ر، العدد 71، الصادر 10 نوفمبر 2004.

[4]–سوير سفيان. **جرائم المعلوماتية**، مذكرة ماجيستر في علم الاجرام والعقاب، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر, 2010، ص22.

ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المختلفة في محورين[1]:

-الأول: داخلي بحيث تتلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.

-الثاني: دولي عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرمو المعلوماتية عن عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى.

ثانيا-جريمة هادئة: ان الجرائم المعلوماتية هي جرائم هادئة بطبيعتها، لا تحتاج الى العنف[2]، يتصرف المجرم المعلوماتي خارج العتبة حيث تقلل تقنيات المعلومات من عتبة الإجراءات. لم يعد الجاني يجد نفسه وجها لوجه مع الضحية، يصبح الضحية مجهول الهوية بالنسبة له. إذا، لم يعد هناك خطر التعرض الجسدي للضحية او السلطات[3].

كل ما تحتاج اليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، كما تحتاج كذلك الى وجود الانترنت مع وجود مجرم يوظف خبرته او قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كاختراق خصوصيات الغير او التجسس او الاحتيال[4].

من ناحية أخرى لا تكون المهارات التقنية الخاصة مطلوبة دائما، ولكن يمكن الحصول عليها عبر الأنترنت بدلا من ذلك. كما يمكن تنزيل الأدلة والبرامج العملية مجانا أو مقابل الدفع، او يمكن الوصول الى الخدمات الأخرى التي تسهل ارتكاب الجريمة. وبالتالي، يمكن شراء المعلومات المتعلقة بأحدث الثغرات الأمنية في البرامج، او حتى البيانات الشخصية[5].

---

[1]-بن شهرة شول، ماشوش مراد. مرجع سابق، ص11.

[2]-المومني نهلا عبد القادر، مرجع سابق، ص58

[3]JEAN-LUC PUTZ، مرجع سابق، ص39

[4]- المومني نهلا عبد القادر، مرجع سابق.

[5] JEAN-LUC PUT، مرجع سابق، ص40

تتميز الجريمة السيبرانية بقلة عدد الحالات التي تم اكتشافها بالفعل إذا ما قارنا ذلك على ضوء ما يتم اكتشافه من الجرائم التقليدية. ويرى البعض أن من بين الأسباب وراء صعوبة اكتشاف هذه الجرائم يرجع إلى تميزها بأنه لا يشوب ارتكابها أي عمل من أعمال العنف[1].

في الجريمة التقليدية سيجد السارق الذي يفشل في فتح الخزنة صعوبة في العثور على متخصص في الحال لتقديم المساعدة له، على الأنترنت من ناحية أخرى يتم انشاء اليات تعاقد من الباطن، حيث يمكن للمرء شراء خدمات أحيانا تكون مشروعة وأحيانا غير مشروعة للتحضير لإرتكاب الجريمة او تسهيل ارتكابها. بالقياس الى مجالات تكنولوجيا المعلومات الأخرى التي تميل الى التعاقد تسمى هذه الظاهرة **الجريمة كخدمة**[2].

ولا يتمثل الاختلاف بين الجريمة السيبرانية والجريمة التقليدية في معدل ارتكابها ومقدار الخسائر الناجمة عنها فقط، بل تتميز الجريمة السيبرانية أيضا بكونها لا تتسم بالعنف الذي تتسم به غيرها من الجرائم التقليدية. فحالات الإتلاف المعلوماتي التي قد يصاحبها استخدام للعنف قليلة نسبيا إذا قورنت بغيرها من الجرائم، حتى إنه يمكن القول إنه لا يوجد شعور حقيقي بعدم الأمان في مواجهة الجريمة السيبرانية كالذي يوجد بصورة دائمة في مواجهة غيرها من الجرائم[3].

لا تتم تجربة الهجوم على البيانات بنفس طريقة الهجوم على السلع المادية، ربما يكون عدد الأشخاص الذين قاموا بتنزيل فيلم بشكل غير قانوني أعلى بكثير من عدد الأشخاص الذين سرقوا قرص DVD من المتجر. الناس اقل ترددا في محو القرص الصلب من اشعال النار في السيارة، رغم ان الضرر المالي قد يكون نفسه[4].

---

[1]–شيخه حسين الزهراني. **الطبيعة القانونية للهجوم السيبراني وخصائصه**، مجلة جامعة الشارقة للعلوم القانونية، جامعة الشارقة، المجلد 17، العدد 01,2020، ص776.

[2] JEAN-LUC PUTZ،مرجع سابق،ص42

[3]– شيخه حسين الزهراني، مرجع سابق

[4] JEAN-LUC PUTZ,مرجع سابق. ص41

المطلب الثاني: أنواع الجريمة المعلوماتية

ذهب الفقه الراجح إلى تقسيم الجرائم المعلوماتية إلى طائفتين رئيسيتين على محل الجريمة المعلوماتية التي تنصب على معطيات الحاسوب التي تطال المعلومات نفسها بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة، إذ تقتضي في ارتكاب النشاطات الإجرامية استخدام الحاسب الآلي. وتتمثل الطائفة الأولى في الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي أما الطائفة الثانية تتمثل في الجرائم المعلوماتية الواقعة على النظام المعلوماتي.

وقسمها آخرون بالاعتماد على معيار أنماط السلوك المختلفة التي تمثل الجريمة المعلوماتية ومدى اتفاقها أو اختلافها مع القواعد التي تحكم القانون الجنائي إلى ثلاث طوائف تتمثل في الدخول والاستعمال غير المصرح بهما لنظام الحاسب الآلي، أما الثانية تتمثل في الاحتيال المعلوماتي وسرقة المعلومات والطائفة الأخيرة تتمثل في الجرائم التي يساعد الحاسب الآلي على ارتكابها[1].

لكن ومن الملاحظ أن هذه التقسيمات لم تراع بعض أو كل خصائص هذه الجرائم من خلال موضوعها والحق المعتدى عليه لاعتمادها على معيار واحد للتقسيم متناسية معايير أخر، بحيث يرى بعض من الفقهاء أنه يجب مراعاة في كل محاولة للتقسيم اعتباران وهما:

- التطور المستمر للجريمة المعلوماتية
- معيار الجريمة المعلوماتية نفسها أي كل ما يدخل في إطار المعلوماتية وما يخرج منها[2].

كما أطلق المشرع الجزائري تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الجريمة المعلوماتية، ولقد عرفها في المادة الثانية من القانون رقم 09 -04 المؤرخ في

[1]– قورة. نائلة عادل محمد، المرجع السابق، ص256

[2] David Fayon. **L'informatique**, Vuibert, 1999 .p 15.**(**on appelle Entrées-Sorties les échanges d'informations entre le processeur et les périphériques qui lui sont associés on appelle Entrées-Sorties les échanges d'informations entre le processeur et les périphériques qui lui sont associés, Les sorties sont les données émises par l'unité centrale à destination d'un périphérique (disque, réseau, écran…). **)**

2009/08/05 بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية[1]". هذا بخصوص تعريف الجريمة الالكترونية أما فيما يتعلق بأنواعها والتي حددها قانون العقوبات الجزائري في القسم السابع ضمن المواد 394 مكرر إلى 394 مكرر 6.

الفرع الأول: أنواع الجريمة المعلوماتية

أدى التطور المستمر للسلوك البشري نتيجة الابتكارات التكنولوجية الى خلق فرص لا مثيل لها للجريمة وسوء الاستخدام، تحت ضوء الطرق المختلفة التي تُولِد بها التكنولوجيا الجريمة والانحراف بالإضافة الى تعزيز التكتيكات الفريدة للإجرام، تتزايد الجرائم الالكترونية بسرعة. يبلغ متوسط الخسارة المرتبطة بسرقة الإنترنت 1.3 مليون دولار، في حين ان متوسط الخسارة في العالم المادي، حيث يكون لديك سلاح، يتراوح بين 6000 و8000 دولار فقط[2].

هناك ثلاثة أنواع رئيسية للهجمات السيبرانية يمكن تلخيصها في[3]:

1-الهجوم الموزع: في إطار هذا النوع من الهجوم، يتم تثبيت البرامج الضارة على أجهزة كمبيوتر متعددة. هناك طرق مختلفة يمكن ان يصل بها الهجوم الموزع الى جهاز الكمبيوتر او الجهاز المحمول. مثال التشفير وبرامج الفدية يقوم المتسللون بتشفير ملفاتك والاحتفاظ ببيانتك للحصول على فدية. لا تدفع الفدية في كثير من الأحيان، سيأخذون اموالك ولا يزالون لا يفتحون بياناتك. مما سبق ذكره نتطرق الى أكثر ثلاث هجمات موزعة شيوعا[4]:

1.1 -التعامل مع المتصفح: يمكن للبرامج الضارة التلاعب بما تراه على متصفحك وسرقة بياناتك. على سبيل المثال، عندما يتم ارسال بضعة أسطر إضافية من رمز البرامج

---

[1]-الجمهورية الجزائرية الديمقراطية الشعبية: **الجريدة الرسمية**، العدد47، المتضمن قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها, 2009/08/16، ص05.

[2] A.J.WRIGHT. **THE ELITE CYBER CRIMINALS STORIES**. The Secret world of cyber criminals and strategies for addressing Cyber Crime.2020.p06

[3]-المرجع نفسه، ص06، 09، 10.

[4]-المرجع نفسه.ص07, 08

الضارة الى موقع ويب أحد البنوك، يبدو موقع الويب كما هو، لكن البرنامج الضار يسرق بيانات البنك.

2.1 –مفتاح المسجل: يوجد هذا النوع من البرامج الضارة في خلفية جهاز الكمبيوتر الخاص بك ويلتقط ما تكتبه لمعرفة سلوكك وربما التقاط بياناتك الشخصية. يمثل أداة تسجيل المفاتيح تهديدا لمعلوماتك الشخصية. يتم عرض معلوماتك الحساسة مثل اسم المستخدم وكلمات المرور وما الى ذلك لمؤلف مسجل المفاتيح. هذا يؤدي الى سرقة الهوية والمعاملات غير المصرح بها.

3.1–رفض خدمة الموزع(DDOS): يقصف المهاجم موقع الويب الخاص بك بحركة المرور حتى ينهار الخادم ويصبح غير متصل بالإنترنت. يمكن ان يكون البرنامج الضار في شكل تنزيل موقع ويب أو مربع منبثق، على سبيل المثال، انت الفائز في نوع الرسائل او مرفقات البريد الالكتروني او محرك أقراصUSB.

2–الهجوم المركزي: في هذا النوع من الهجوم يتم اختراق نظام مركزي في محاولة للحصول على بيانات العملاء عادة لتحقيق مكاسب مالية. بدلا من ذلك، قد يتم تنفيذ هجوم مركزي باسم القرصنة او القرصنة لأسباب أخلاقية او اجتماعية او سياسية.

3–الهجوم الشخصي: هذا يعني بالضبط ما تقوله. انه هجوم شخصي على بياناتك. أكثر أنواع الهجمات الشخصية شيوعا هي:

–انتحال البريد الالكتروني–انتحال الهواتف–انتحال الرسالة.

ومما سبق ذكره ذهب الفقه الراجح إلى تقسيم الجرائم المعلوماتية إلى طائفتين رئيسيتين على محل الجريمة المعلوماتية التي تنصب على معطيات الحاسوب التي تطال المعلومات نفسها بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة إذ تقتضي في ارتكاب التي النشاطات الإجرامية استخدام الحاسب الآلي. وتتمثل الطائفة الأولى في الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي أما الطائفة الثانية تتمثل في الجرائم المعلوماتية الواقعة على النظام المعلوماتي، وهذا ما سنتطرق إليه خلال دراستنا لهذا الفرع.

أولا-الجرائم الواقعة بواسطة النظام المعلوماتي: يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية ويعد فيها الحاسب الآلي في هذه الطائفة من الوسائل التي تسهل بها النتيجة الإجرامية ومضاعفة جسامتها، حيث يهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة من خلال اعتدائه على أموال الغير، فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته كوسيلة لتنفيذ جريمته[1].

1-الجرائم المعلوماتية الواقعة على الأشخاص: تقع هذه الجرائم على الأشخاص من خلال نوع الحق المعتدى عليه ودور النظام المعلوماتي في اقترافها.وتتمثل هذه الاعتداءات في الجرائم الواقعة على حقوق الملكية الفكرية والأدبية، أما النوع الثاني تكمن في الجرائم الواقعة على حرمة الحياة الخاصة للفرد وكما نشير أنه هذه الحرمة يدخل في نطاقها أمواله.

1.1-طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية والأدبية: يمكن أن يكون النظام المعلوماتي وسيلة فعالة للاعتداء على الملكية الفكرية والأدبية، ومثال ذلك استخدام النظام المعلوماتي في السطو على قاعدة معلومات التي تتضمن معلومات أياً كان نوعها ملكاً لشخص آخر دون إذنه أو علمه كمن يعتدي بنسخ مقال أو بحث في صدد الإنجاز من جهاز أو دعامات التخزين les supports de stockage[2]. أخرى دون إذن صاحبها وينسبها لنفسه حيث تمثل اعتداء على حق من حقوقه والأدبية ومنها المادية كون أن للمعلومات قيمة من خلال نشرها أو تسويقها، ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع أذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع[3].

2.1-طائفة الجرائم المعلوماتية الواقعة على الحياة الخاصة: لقد كفلت جل الدول الحياة لمواطنيها بالحماية ولا شك أن الحاسبات الآلية بما لها قدرة فائقة على تخزين مقدار كبير من المعلومات، ولأهمية المعلومات التي تحتويها هذه الانظمة، أصبحت هذه الحسابات هدفاً لما لها

[1]- قورة نائلة عادل محمد، المرجع السابق، ص265.

[2] David Fayon، المرجع السابق، ص21

[3]- الملط، أحمد خليفة، **الجرائم المعلوماتية**، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، مصر،2006، ص 184

من دور مهم في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مادية ومعنوية مختلفة[1].

وعليه يمكن استخدام النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد، كأن يقوم شخص بإعداد ملف معلوماتي يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه ، كما يقوم بنشر معلومات على شكل صور أو حقائق من خلال اختراقه لحساب شخص وتشويه السمعة أو الاطلاع على معلومات بعلم الشخص المعني ويقوم بحفظها واطلاع الغير عليها أو أسرار مكتوبة أو سير ذاتية ، مذكرات قصد التشهير بشخص أو جماعة معينة أو بيعها لتحقيق مصالح مختلفة كالحصول على عائد مادي أو للضغط على أصحابها مقابل القيام بعمل أو الامتناع عنه[2].

كما تعاقب مختلف التشريعات كل من يقوم بالدخول غير المصرح له إلى النظام المعلوماتي وإفشاء معلومات توجد داخلها، حيث حمت تلك التشريعات الأسرار المهنية حيث ألزمت أصحاب المهن على غرار المحامي والطبيب بالمحافظة على الأسرار التي يقرها له الزبون أو العميل[3].

2-الجرائم المعلوماتية الواقعة على النظم المعلوماتية الأخرى: هذا النوع من الجرائم لا يستلزم تدخلاً لإتلاف الوظائف التقنية للنظام المعلوماتي ولا تعديلا على المعلومات المعالجة، بل يقتصر في غالب الأحيان الولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة الكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى.

1.2-الولوج غير المشروع للمعلومات المعالجة آلياً: تقوم هذه الصورة بوجود المجرم داخل أحد المراكز المعلوماتية بهدف الولوج إلى المعلومات التي تمت معالجتها آلياً والاطلاع عليها دون تصريح وقد يكون هذا الولوج إما مباشرًا أو غير مباشر .

---

[1]-قورة نائلة عادل محمد، مرجع سابق، ص 275

[2]- الملط أحمد خليفة، مرجع سابق، ص 190

[3]-المرجع نفسه، ص 200

أما المباشر فيعد من أكثر الأفعال المرتكبة وأسهلها تنفيذاً ويتخذ عدة صور إذ يستطيع الجاني الاستيلاء على المعلومات المخزنة لدى الأنظمة بعدة طرق باستخدام آلة الطباعة أو بالقراءة المباشرة أو باستخدام مكبر الصوت، ومن أمثلة ذلك الولوج المباشر، قيام شخص سابق بأحد البنوك الأمريكية الذي كان يعمل في النظام المعلوماتي الخاص بالبنك نقل معلومات المالية المخزنة في النظام ونقلها لرئيسه الجديد بعد حصوله على كلمة السر من زميل سابق له[1].

وأما الولوج غير المباشر ظهر بظهور تقنيات مستحدثة، لها الصلة بالنظام المعلوماتي كالمعالجة عن بعد، إذ هذه التقنيات أدت إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للولوج والاستفسار عن بعد من المراكز المعلوماتية، إذ أنه أثناء بثها تكون عرضة للالتقاط والتسجيل غير مشروعين في كل فترة من فترات هذا التحويل ما بين المرسل والملتقط، ولعل من أبسط هذه التقنية هي تقنية البلوتوث Bluetooth[2].

2.2-إساءة استخدام البطاقات الائتمانيـة: أدى إدخال النظام المعلوماتي في مجالات عمليات البنوك إلى ظهور هذا النوع الجديد من الجرائم المعلوماتية، التي تعد من أخطر الجرائم لاسيما في المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور والحداثة، ويتخذ هذا النوع من الجرائم على صورتين:

الصورة الأولى تتمثل في الاساءة في استخدام الحسابات المصرفية أو البطاقات الائتمانية وذلك عن طريق عدم احترام العميل المصدرة إليه البطاقات الائتمانية شروط العقد المبرم بينه وبين المؤسسة المصرفية كأن يستعمل بطاقة منتهية الصلاحية أو بطاقة تم إلغاؤها أو الشراء بأكثر من قيمتها[3].

---

[1]- الشوا محمد سامي. **ثورة المعلومات وانعكاساتها على قانون العقوبات**، دار النهضة العربية، القاهرة، 1994، ص97

[2]-David Fayon ص25، مرجع سابق،

[3]- الملط أحمد خليفة، المرجع السابق، ص 192

أما الصورة الثانية تتمثل في استخدام الغير لتلك الحسابات أو البطاقات كأن يقوم المجرم استعمال البطاقة للحصول على سلع أو خدمات او سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي مثلاً أو السحب باستخدام بطاقات ائتمانية مزورة[1].

ثانيا-الجرائم الواقعة على النظم المعلوماتية: إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية بالتصنيف الذي يقوم على محل الجريمة ويتمثل في الجرائم الواقعة على النظام المعلوماتي نفسه التي قد تستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية والمعلومات المدرجة بالنظام.

نظرا لان الجرائم الواقعة على المكونات المادية للنظام المعلوماتي مشمولة بالحماية الجزائية، فهي تندرج ضمن الجرائم التقليدية وتقوم على أفعال مادية، ارتأينا الاهتمام بالجرائم الواقعة على المكونات المنطقية للنظام المعلوماتي المستلزم لمعرفة فنية عالية في مجال البرمجة، والتي تقع على البرامج التطبيقية او برامج التشغيل.

1-جرائم الاعتداء على المكونات المنطقية للنظام المعلوماتي: تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة، وقد تقع هذه الجرائم إما على البرامج التي منها البرامج التطبيقية أو برامج التشغيل.

1.1- الجرائم الواقعة على البرامج التطبيقية: يقوم الجاني في هذه الصورة بتحديد البرنامج أولاً ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية.

1.1.1-تعديل البرنامج: الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود وتكثر هذه الجرائم في مجال الحسابات[2].

ومن أمثلة ذلك قيام مبرمج في أحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zwick وحصل على إثر ذلك على مئات الدولارات كل شهر

[1]-المرجع نفسه، ص196

[2]-الملط أحمد خليفة، المرجع السابق، ص173

وكان من الممكن أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل ليكتشف بعدها حقيقة هذا المبرمج[1].

2.1.1-التلاعب في البرامج: يأخذ التلاعب في البرامج عدة أشكال فقد يتم عن طرق استعمال القنبلة المنطقية[2] أو عن طريق قيام أحد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي، وبهذا يصعب اكتشاف هذا البرنامج لصغره ودقته.

2.1-الجرائم المعلوماتية الواقعة على نظام التشغيل: تقوم الجريمة في هذه الصورة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[3]، ويتحقق هذا النوع من الجرائم في نوعين:

1.2.1-المصيدة: تتمثل هذه الصورة من خلال إعداد برنامج به أخطاء وعيوب عمداً، لا يكتشف بعضها عند استخدام البرنامج، إذ يترك المبرمج ممرات خيالية وتفرعات في البرنامج حتى يستطيع بعدها تنفيذ التعديلات الضرورية للولوج داخل النظام المعلوماتي والوصول إلى كل المعلومات التي تحتويها الذاكرة.

2.2.1-تصميم برنامج وهمي: وتقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه معد خصيصاً لارتكاب الجريمة، ومن أمثلة ذلك قيام إحدى شركات التأمين الأمريكية بواسطة مبرمجيها من تصميم برنامج وهمي يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 46000 بعد تقاضي هذه الشركة من اتحاد شركات التأمين عمولات من نظيراتها[4].

---

[1] - Duleroy ,**Les escrocs a l'informatique** ,le nouvel économiste , octobre 2002 , p 202

[2]-الملط أحمد خليفة، مرجع سابق ، ص 545

[3]-المرجع نفسه، ص175

[4]-Duleroy ، المرجع السابق ، ص 210

3.1-جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي: للمعلومة في حد ذاتها باعتبارها الأساس الذي يقوم عليه النظام المعلوماتي، وبهذا اصبحت هدفاً للجريمة المعلوماتية من خلال التلاعب فيها أو عن طريق إتلافها.

1.3.1-التلاعب في المعلومات: يتم التلاعب في المعلومات الموجودة داخل النظام بالطريق المباشر أو غير المباشر، أما الطريق المباشر يتم عن طريق ادخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، ويتم هذا التلاعب بإضافة معلومات غير مؤسسة كإضافة أسماء مستخدمين غير موجودين في العمل أو الإبقاء على مستخدمين تركوا العمل.

في حين أن الطريقة غير المباشرة يتم عن طريق التدخل غير المباشر لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين أو الدعامات، فقد قام في هذا الصدد أحد الموظفين بأحد فروع الشركة Isoverst Gobain بإرسال شريط ممغنط يحتوي على 139 إذن دفع، وعند معالجته بالبنك تم رفض نسخه لعيب في الشريط، وقد علق الخبراء أنه لو نجحت العملية لتم النصب على البنك بحوالي 21 مليون فرنك[1].

2.3.1-إتلاف المعلومات: قد يهدف الجاني من خلال ارتكابه للجريمة المعلوماتية المخزنة داخل النظام، وقد يأخذ هذا التلاف عدة صور الحذف التغير استبدال المعلومة.

ويشكل استبدال المعلومة نوع من أنواع جرائم الغش والتزوير المعلوماتي وهو على درجة كبيرة من الخطورة لأنه في حال نجاحه يستمر لوقت طويل قبل اكتشافه ويتولد عليه اضرار كبيرة كتغير رقم بآخر أو اسم بغيره[2]، فقد قام شخص يدعى Vladimir Loriblitt يعمل بوزارة المالية بتغير فواتير وهمية للنظام وتحويل ما تم سداده لحساب شركات وهمية الذي جنى منها 10 ملايين دولار قبل أن يتم اكتشافه[3].

---

[1]-المرجع نفسه، ص 212

[2]-الملط أحمد خليفة، مرجع سابق، ص 175

[3]-Duleroy ، مرجع سابق ، ص215

أما محو المعلومات فهو من أسهل طرق الاتلاف كون أنه من خصائص الجرائم المعلوماتية في قدرة المجرم المعلوماتي من محو آثار الجريمة في فترة وجيزة لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو عن طريق الفأرة.

الفرع الثاني: أنواع الجرائم المعلوماتية في القانون الجزائر

عمد المشرع الجزائري على تطبيق نصوصا قانونية خاصة على السلوكيات المنحرفة في مجال المعلوماتية بإفراده نصوصا تجريميه وذلك عندما تطرق إلى تجريم المساس بأنظمة الحاسب الآلي، مما دفعه إلى تعديل قانون العقوبات بالإضافة إلى تقنينه قانون خاص يتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي جمع بين القواعد الاجرائية المكملة لقانون الاجراءات الجزائية وبين القواعد الوقائية.

تأخذ صور الاعتداء على النظام المعلوماتي في قانون العقوبات الجزائري صورتين أساسيتين هما[1]، الدخول والبقاء في منظومة معلوماتية، أما الصورة الثانية هي المساس بمنظومة معلوماتية.

كما تضمن قانون العقوبات صور أخرى للغش في حين أبقى خارج دائرة التجريم بعض الأفعال منها: المساس بحقوق الأشخاص عن طريق المعلوماتية، كجمع المعلومات حول شخص وتحويل المعلومات الاسمية عن مقصدها[2].

1-الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات: نصت عليه المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير

[1]-. بن عقون حمزة، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة ماجستير في القانون، كلية حقوق، جامعة الحاج لخضر باتنة، الجزائر، 2012، ص182.

[2]- بوسقيعة أحسن، **الوجيز في القانون الجزائي الخاص**، الجزء الأول، الطبعة العاشرة، دار هومة، الجزائر، 2009، ص 445.

لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج".

1.1-فعل الدخولL'accès : لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، وإنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات[1]، ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[2].

2.1-فعل البقاءLe maintien : يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، وقد يجتمعان.

ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورًا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي.

ويكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والاطلاع فقط ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، والتي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة.

---

[1]- بن قارة عائشة مصطفى، **حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، دار الجامعة الجديدة، الاسكندرية، 2010، ص42

[2]- قهوجي علي عبد القادر، **الحماية الجنائية لبرامج الحاسب الآلي**، دار الجامعة الجديدة، الاسكندرية، 1999، ص 121

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الاجتماع المادي للجرائم.

وإذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضا وبصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة، وذلك بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له الحق السيطرة على النظام، ويقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج[1].

أما عن الصورة المشددة لهذه الجريمة، نصت المادة 394 مكرر 3/2: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظمة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج"، على ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، ويتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه.

ويكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة، ولا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلّب مثل هذا الشرط يكون غير معقول، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة.

كما لا يشترط أن تكون تلك النتيجة مقصودة، أي على سبيل الخطأ غير العمدي، فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة العمدية الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتفاء تلك

[1]– بن قارة عائشة مصطفى، المرجع السابق، ص42

العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

تجدر الإشارة إلى أن الولوج والتجول والبقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا إن تمّا عمداً، كما أن الركن المعنوي لهذه الجريمة يأخذ صورة القصد الجنائي بعنصريه العلم والإرادة، حيث يلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع.

كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصريه العلم والإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام[1].

2-المساس بمنظومة معلوماتية: يأخذ السلوك الإجرامي لهذه الجريمة إما الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات أو الاعتداء العمدي على المعطيات[2].

حيث لم يورد المشرع الجزائري نصاً خاصاً بالاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام وقد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات والاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية، فاذا كان مجرد وسيلة فان الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء غاية فان الفعل يشكل جريمة الاعتداء العمدي على المعطيات[3].

---

[1]- قهوجي علي عبد القادر، مرجع سابق، ص 136

[2]- حاجب هيام، **الجريمة المعلوماتية**، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر، 2008، ص47

[3]-المرجع نفسه، ص48

يتمثل هذا السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات من أداء نشاطه العادي والمنتظر منه القيام به، وإما في فعل إفساد نشاط أو وظائف هذا النظام، ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية جهاز الحاسب الآلي نفسه، شبكات الاتصال، أجهزة النقل ...الخ، أما المعنوية مثل البرامج والمعطيات[1].

وتتمثل النشاطات غير المشروعة لهذه الجريمة في:

1.2-التعطيل (العرقلة): يفترض وجود عمل إيجابي دون أن يشترط المشرع أن يتم التعطيل بوسيلة معينة سواء مادية أو معنوية وسواء اقترنت بالعنف أم لا، فأما عن الوسيلة المادية فمثلها كسر الأجهزة المادية للنظام أو تحطيم أسطوانة، أما عن الوسيلة المعنوية فهي التي تقع على الكيانات المنطقية للنظام كالبرامج والمعطيات. وذلك بإتباع إحدى التقنيات التالية: إدخال برنامج فيروسي، استخدام قنابل منطقية مؤقتة، جعل النظام يتباطأ في أدائه لوظائفه إلى غيرها من التقنيات.

2.2-الافساد: هو كل فعل وإن كان لا يؤدي إلى التعطيل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها. والافساد من هذه الزاوية يقترب من التعييب الذي يعتبر ظرفا مشددا لجريمة الدخول والبقاء غير المشروع. والفارق بينهما يكمن في أن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون عمديا بينما يتطلب هذا الشرط بالنسبة لجريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات.

[1]- فشار عطاء الله، **مواجهة الجريمة المعلوماتية في التشريع الجزائري**، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص13

ومن بين صور الإفساد أو التعييب نجد تقنية استخدام القنبلة المعلوماتية التي تدخل عن طريقها مجموعة معطيات تتكاثر داخل النظام تجعله غير صالح للاستعمال كاستخدام البرنامج المسمى بـ " حصان الطروادة " والذي يقوم بتغيير غير محسوس في البرامج أو المعطيات[1].

أما الاعتداءات العمدية على المعطيات فلقد نص المشرع الجزائري عليها في المادة 394 مكرر2 في قانون العقوبات "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها"، تأخذ الصورة الأولى الاعتداءات العمدية على المعطيات الموجودة داخل النظام، فالنشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية[2]:

-الإدخال(L'intrusion) ، المحو(Effacement) ، التعديل.(Modification)

أما الصورة الثانية فهي جريمة المساس العمدي بالمعطيات خارج النظام التي وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها من خلال تجريمه السلوكيات المذكورة في نص المادة 394 مكرر 2 والتي تستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة، كأن تخزن في أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

المبحث الثاني: الطبيعة الخاصة للمجرم المعلوماتي

[1]- قهوجي علي عبد القادر، مرجع سابق، ص143

[2]- حاجب هيام، مرجع سابق، ص 49

المعلوماتية ينظر اليها دائما بوصفها أداة محايدة وأن مصدر ضعفها وانتهاكها هو الانسان ذاته، والذي غالبا ما يهيئ فرصة استغلال الوسيلة المعلوماتية عن حسن أو سوء نية. فجوهر المشكلة يرتبط بالإنسان وشخصيته ودوافعه وكما هو معروف فانه لا يمكن لأي عقوبة ان تحقق هدفها سواء في مجال الردع العام أو الردع الخاص ما لم تضع في الاعتبار شخصية المجرم، والذي ينبغي إعادة تأهيله اجتماعيا حتى يعود مرة أخرى مواطنا صالحا في مجتمعه[1].

سنتطرق للسمات المميزة للمجرم المعلوماتي في (المطلب الأول)، ونعرض بعد ذلك دوافع ارتكاب الجريمة في (المطلب الثاني).

المطلب الأول: السمات المميزة للمجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين[2].

ولقد اختلف الباحثون في تحديد هذه السمات، ويعد الأستاذ Parkerواحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة، وبالمجرم المعلوماتي بصفة خاصة لأنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه، فكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء.

إذا فان المجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه على درجة من العلم والمعرفة وإن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو الحال في جرائم ذوي الياقات البيضاء[3]. كما يتفق مجرمو

[1]–الشوا، سامي، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، ط1، دار النهضة العربية، القاهرة، 1994، ص 33، 34.

[2]– قورة نائلة عادل محمد، المرجع السابق، ص54

[3] - Eduin H, Suthreland. **White collar criminality**, 1998.p125

المعلوماتية مع ذوي الياقات البيضاء في أن الفاعل في الحالتين يبرر جريمته، بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.

يتميز المجرم المعلوماتي بعدد من السمات والخصائص والأصناف. والتي سنقوم بتقسيمها لفرعين. الفرع الأول نتناول فيه خصائص المجرم المعلوماتي، اما الفرع الثاني نذكر فيه أصناف المجرم المعلوماتي.

الفرع الأول: خصائص المجرم المعلوماتي

يتميز المجرم المعلوماتي بعدد من السمات والخصائص وهي:

أولا–المهارة والمعرفة والذكاء: يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين، إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال[1].

إن المجرم المعلوماتي يمكن أن يكّون تصورا كاملا لجريمته، فالفاعل يستطيع ان يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته، وذلك حتى لا يفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها[2].

الاجرام المعلوماتي هو اجرام الاذكياء بالمقارنة بالإجرام التقليدي الذي يميل الى العنف[3] فالمجرم المعلوماتي مجرم شغوف يصبو دائما لابتكار طرقه الخاصة لاختراق الحواجز الأمنية ونيل مبتغاه.

[1]–ماشوش مراد، السمات الخاصة للجريمة المعلوماتية، مرجع سابق، ص13

[2]–قورة نائلة عادل محمد، مرجع سابق، ص 52.

[3]– الشوا، سامي، مرجع سابق، ص34

ثانيا–تبرير ارتكاب الجريمة: يوجد شعور لدى مرتكب فعل الاجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم أو بمعنى أخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم[1].

ثالثا–انسان اجتماعي: المجرم المعلوماتي انسان مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف ولا يعني ذلك تقليل من شأن المجرم المعلوماتي بل إن خطورته الاجرامية قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الاجرامية لديه[2]. فاكتسابه لثقة مجتمعه يجعل منه انسان خارج إطار الشبهات، مما يتيح له مجالا كبيرا للتمادي في ارتكاب جرائمه والتي قد لا تكتشف في الغالب.

رابعا–الخوف من كشف جريمته: بالرغم من خوف المجرمين بصفة عامة لكشف جرائمهم، الا انها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب عليها من خسائر لهم، وذلك لانتمائهم في غالب الأحيان لوسط اجتماعي متميز من حيث التعليم والثقافة وطبيعة العمل.

يساعد مجرمي المعلوماتية على الحفاظ على سرية افعالهم طبيعة الأنظمة المعلوماتية نفسها، ذلك أن أكثر ما يعرض المجرم الى اكتشاف امره هو ان يطرأ أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحواسيب انما تؤدي عملها غالبا بطريقة ألية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة الى أخرى وهو ما يساعد

[1]– قورة نائلة عادل محمد، مرجع سابق، ص54

[2]–الرومي محمد أمين، **جرائم الكمبيوتر والانترنت**، ط1، دار النهضة العربية، القاهرة، 2003، ص23

على عدم كشف الجريمة طالما ان جميع خطوات التنفيذ معروفة مسبقا حيث لا يحتمل أن تتدخل عوامل غير متوقعة يكون من شأنها الكشف عن الجريمة[1].

أثبتت الدراسات أن غالبية مرتكبي الجرائم المعلوماتية غير قادرين على ارتكاب الجرائم التقليدية خاصة تلك التي تتطلب مواجهة مع المجني عليه فالمجرم المعلوماتي لا يستطيع الاعتداء على المجني عليه بطريقة مباشرة الا انه لا يرى غضاضة في أن يكون هذا الاعتداء عن طريق البيئة الالكترونية[2].

خامسا-السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها، وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات[3].

الفرع الثاني: أصناف المجرم المعلوماتي

بناء على ما تقدم يمكن أن نقسم مجرمي المعلوماتية Cyber criminals إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية ويمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة وتتمثل هده الطوائف فيما يأتي[4]:

*الطائفة الأولىPranksters : الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث).

[1]- قورة نائلة عادل محمد، مرجع سابق، ص 56

[2]-هذا ما توصل له الأستاذ باركر خلال دراسته للأنماط المختلفة لمجرمي المعلوماتية، انظر، المرجع نفسه.

[3]- ماشوش مراد، السمات الخاصة للجريمة المعلوماتية، مرجع سابق، ص14

[4]- قورة نائلة عادل محمد، مرجع سابق، ص 58

*الطائفة الثانيةHackers : فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

*الطائفة الثالثةMalicious Hackers : هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترقي فيروسات الحاسبات الآلية وموزعيها.

*الطائفة الرابعةPersonnel Problem Solvers : فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.

*الطائفة الخامسةCareer Criminals : مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على فعالهم وصف الجريمة المنظمة، أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل[1]، ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.

*الطائفة السادسةExtrem Advocates : فتدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، ويركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه.

وان اعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفًا جذابًا لهذه الجماعات، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات

[1]– رستم، هشام محمد فريد، ص69

الإرهابية المعروفة في أوربا باسم "The Red Brigades" بتدمير ما يزيد عن 60 مركزا للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها ومعتقداته.

*الطائفة السابعةThe Criminally Negligent : والتي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية وفي أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح؛ ففي نيوزلندا على سبيل المثال قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائرة لهذا التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60 راكبا على متنها، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ[1].

المطلب الثاني: دوافع ارتكاب الجريمة

الدافع او بمصطلح أخر الباعث: وهو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام"[2].

وتنقسم هذه الدوافع، لدوافع متعلقة بشخص المجرم، ودوافع متعلقة بالجريمة وهو ما سنتطرق إليه في الفرعين المواليين، حيث سنتناول في (الفرع الأول) الدوافع المتعلقة بشخص المجرم، ثم دوافع ارتكاب الجريمة في (الفرع الثاني).

الفرع الأول: الدوافع المتعلقة بشخص المجرم

لدراسة هذا الفرع ارتأينا ذكر الدوافع على المستوى الفردي أولا والدوافع على مستوى المجتمع ثانيا.

أولا: على المستوى الفردي: وهي تلك الدوافع التي تجعل من الشخص يقوم بارتكاب عدد من المخالفات جوهرها حب الاستطلاع والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات.

[1]– عبابنة محمود احمد، مرجع سابق، ص45

[2]– قورة نائلة عادل محمد، مرجع سابق، ص 58

1-الرغبة في التعلم: الرغبة في تعلم كل ما يتعلق بأنظمة الحاسوب والشبكات الالكترونية قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية ويشير الأستاذ (ليفي) مؤلف كتاب قراصنة الأنظمة الى اخلاقيات هؤلاء القراصنة التي ترتكز على مبدأين أساسيين:

*ان الدخول الى أنظمة الحاسوب يمكن ان يعلمك كيف يسير العالم.

*ان عملية جمع المعلومات يجب أن تكون غير خاضعة للقيود[1].

بشكل عام يرى هؤلاء المجرمون أن جميع المعلومات المفيدة يجب أن تتاح حرية نسخها والاطلاع عليها، الا أنهم يقرون بضرورة اغلاق بعض نظم المعلومات وعدم السماح بالوصول الى بعضها خاصة بعض المعلومات السرية التي تخص الأفراد[2].

2-الدوافع المادية (الربح وكسب المال): تجدر الإشارة الى انه في حال نجاح المجرم في ارتكاب جريمته المعلوماتية فإن ذلك قد يدر عليه أرباحا تكون هائلة في زمن قياسي.

ويمكن ان نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة لاقترافه هذا النوع من الاجرام من خلال ما يرويه أحد هؤلاء المجرمين المحترفين في سجن كاليفورنيا بقوله[3]:(لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الامريكية وبإمكاني ان اكرر ذلك في أي وقت لقد كان شيئا سهلا فانا اعرف أسلوب عمل جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني)

إذا فإن بناء ثروة هائلة في زمن قياسي من أول وأكثر البواعث المؤدية لإقدام هذا النوع من المجرمين لارتكاب جرائمهم.

3-المتعة والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات: مجرمو المعلوماتية يتملكهم شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة الى

---

[1]-محمود عبد الله حسين، **سرقة المعلومات المخزنة في الحاسب الالي**، (ط2)، دار النهضة العربية، القاهرة، 2002، ص69

[2]- محمود عبد الله حسين، المرجع السابق، ص69

[3]-مشار الى هذه الواقعة في، المرجع نفسه، ص57

تعويضهم عن الإحساس بالدنيوية ففي بعض الأحيان وجد أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي. وفي هذا الشأن ننجد المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها وقد يندفع تحت تأثير رغبة قوية من اجل تأكيد قدراته التقنية لإدارة المنشأة الى ارتكاب الجريمة المعلوماتية[1].

ثانيا-على المستوى المجتمع: وتتمحور في الاختراقات للأجهزة الشخصية والتعرف على نقاط ضعف الأخرين.

1-**الرغبة في الانتقام:** يكون الدافع في هذه الحالة لارتكاب الجريمة المعلوماتية الانتقام. سواء كان من شخص طبيعي او معنوي. على سبيل المثال، دفع الانتقام بمحاسب شاب الى ان يتلاعب بالبرامج المعلوماتية بحيث تختفي كل البيانات الحسابية الخاصة بديون هذه المنشأة بعد رحيله بعدة أشهر وقد تحقق هذا الأمر في التاريخ المحدد[2].

2-**دوافع أخرى:** قد لا تكون الدوافع السابقة الوحيدة بل هناك عدة دوافع قد تدفع بحدوث الجريمة المعلوماتية. فمثلا يعد التحضر أحد دوافع الجريمة المعلوماتية عامة، والجريمة المعلوماتية شأنها شأن الجريمة التقليدية هي الأخرى ترتبط بالبطالة والظروف الاقتصادية الصعبة. كما يعد التسابق الفضائي والعسكري بين الدول دافعا لهذه الجريمة، فقد قام القراصنة بالإغارة على شبكات معلوماتية تابعة لوكالة الفضاء ناسا ومواقع أسلحة ذرية تابعة لحكومة الولايات المتحدة الامريكية[3].

كما ان مناهضة العولمة قد تكون احدى الدوافع لارتكاب هذا الفعل، فقد تم اختراق النظام المعلوماتي للمنتدى الاقتصادي العالمي في دافوس بسويسرا، وتمت عملية سرقة معلومات سرية

[1]- الشوا سامي، مرجع سابق، ص53

[2]-المرجع نفسه، ص52

[3]-احمد هلالي عبد الله، الجوانب الموضوعية والاجرائية لجرائم المعلوماتية، (ط2)، دار النهضة العربية، القاهرة، ص 21، 22.

تتعلق بعدد من الشخصيات الثرية المؤثرة التي شاركت في المؤتمر وأرسلت الى احدى الصحف السويسرية[1]

كما وجدت مجموعات تطلق على نفسها مجموعات الكراهية على الانترنت تزدري كل القيم الدينية والأخلاقية والاجتماعية السائدة في المجتمعات وبصفة خاصة تلك المرتبطة بالأسرة. وهناك مواقع الالحاد التي تطالب بإلغاء الدين والدولة والاسرة وتحرير الانسان من تلك الأصفاد والقيود[2].

الفرع الثاني: الدوافع المتعلقة بالجريمة

مثل ما هناك دوافع تتمحور حول شخص المجرم، فلا يمكن انكار الدوافع المتعلقة بالجريمة في حد ذاتها. لقد تطرقنا سابقا في المبحث الاول للطبيعة الخاصة للجريمة المعلوماتية خاصة تلك الخصائص المتعلقة بطبيعتها، فيمكننا القول انها قد تمثل دافعا كبيرا في قيام هذه الجريمة.

ومما سبق، سنحاول ان نبين ما قد تمثله الصبغة الدولية والجريمة نفسها حافزا للمجرم القائم عليها.

أولا-الصبغة الدولية للجريمة كحافز: تتصف الجريمة المعلوماتية بكونها جريمة ذات بعد عالي أو دولي، لكن لا ينبغي أن يفهم من ذلك أنها جريمة دولية[3].

1-**جريمة متعدية الحدود:** المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود[4].

2-**سهولة حركة المعلومات:** جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الاجرامي في دولة أخرى[1].

---

[1]-**www.news.bbc.co.uk/hi/arabic/news/newsied1153000/1153/24,stm.**

[2]-احمد هلالي عبد الله، المرجع السابق، القاهرة، ص24

[3]-شوقي يعيش تمام، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، سلسلة مطبوعات المخبر 06، جامعة بسكرة، (ط1)، مطبعة الرمال(الوادي)، الجزائر، 2019، ص28

[4]- نهلا المومني، مرجع سابق، ص 50.

3-**مشكل تحديد الدولة صاحبة الاختصاص:** خلقت الجريمة المعلوماتية العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة الى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام[2].

4-المفهوم المشترك بين الدول: تكمن أهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية في أنه لا يوجد هناك مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة. بالإضافة الى أن نقص الخبرة لدى الشرطة وجِهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة ان وجدت وجمع الأدلة عنها للإدانة فيها يشكل عائقا كذلك أمام التعاون في مجال مكافحة هذا النوع من الجرائم[3].

ثانيا: الجريمة نفسها كحافز

1-صعوبة اكتشافها: تتميز الجريمة المعلوماتية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة[4].

1.1-عدم تركها لأثر خارجي: الجاني يمكنه ارتكاب هذه الجريمة في دول أو قارات أخرى، اذ أن الجريمة المعلوماتية كما سبق وأشرنا جريمة عابرة للدول[5].

2.1-سهولة تدمير الدليل: إن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة[6] يشكل حافزا إضافيا في ارتكاب هذا النوع من الجرائم.

---

[1]-Ulrich Sieber، **جرائم الكمبيوتر والجرائم الأخرى في مجال المعلومات**، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي (ترجمة سامي شوا)، دار النهضة العربية، القاهرة، 1993، ص58

[2]- نهلا المومني، مرجع سابق، ص51 .

[3]-عوض محمد محي الدين، **مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)**، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 361، 362.

[4]-الصغير جميل عبد الباقي، مرجع سابق، ص17

[5]- نهلا المؤمني، مرجع سابق، ص55

[6]-رستم هشام محمد فريد، مرجع سابق، ص16

3.1-عدم الإبلاغ عنها: تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها[1].

2-صعوبة اثباتها: حتى في حال اكتشاف وقوع الجريمة والإبلاغ عنها فإن اثباتها أمر يحيط به كذلك الكثير من الصعاب، فهي تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة[2].

3-جريمة أقل عنفا وجهدا في التنفيذ: لا تتطلب جرائم المعلومات عنفا لتنفيذها، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والايذاء، كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع والكسر وغير ذلك.

على هذا الأساس تتميز الجرائم المعلوماتية بانها من الجرائم الهادئة، أو الناعمة، حيث لا تحتاج الى العنف، وكل ما تحتاج اليه هو عامل الخبرة والذكاء والقدرة على التعامل مع جهاز الحاسوب بمستوى تقني في ارتكاب الأفعال غير المشروعة، فهي من الجرائم النظيفة التي تستخدم الأرقام والبيانات وليس لها أثر خارجي مادي[3]. وهذا ما يعطي حافزا لارتكاب هذا النوع من الجرائم.

[1]-المرجع نفسه، ص25، 26.

[2]-المومني نهلا، مرجع سابق، ص56.

[3]-صغير يوسف، مرجع سابق، ص16.

الفصل الثاني:

الخصوصية الإجرائية

للجريمة المعلوماتية

إن طبيعة الجرائم المعلوماتية بخصوصياتها ووسائل ارتكابها قد تدفع جميع التشريعات لإعادة النظر في كثير من المسائل، والتعامل معها بحذر سواء في مرحلة التحقيق الأولية والتي تتعامل معها الضبطية القضائية والتي تتلخص في الاستدلال الى مرحلة التحقيق الابتدائية التي تكون من طرف قاضي التحقيق والتي تتلخص في التفتيش.

دفع المشرع الجزائري بدوره الامعان في النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون، ذلك أن الدليل الذي قد يقوى على إثبات هذا النوع من الجرائم لا بد أن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل قادرة على القيام به، مما يستوجب تدخل المشرع لتكريس اليات وقواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة المعلوماتية الاعتماد عليها في الوصول إلى الدليل المناسب في إثبات الجريمة المعلوماتية.
وتكوين جهات خاصة تباشر البحث والتحري إثر وقوع الجريمة المعلوماتية ليعتمد المشرع عليها في اثبات وإقامة العدل.

المبحث الأول: التحقيق في الجريمة المعلوماتية

ما لا شك فيه هو أن ادانة المتهم من عدمه مرتبطة باستجلاء الحقيقة. بالتالي فإن التثبت من حقيقة وقوع الجريمة، وإقامة الإسناد المادي على مرتكبها بأدلة الاثبات على اختلاف أنواعها يعتبر الوسيلة المنشودة لتحقيق ذلك. هنا تكمن اهمية التحقيق فهو إجراء من أهم الإجراءات التي تُتخذ بعد وقوع الجريمة.

والثابت أن الدعوى الجزائية تمر بمرحلتين: مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضا، مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي، فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي[1]، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق[2]، وإننا نؤيد الرأي أو الاتجاه[3] الذي يقسم التحقيق إلى:

–تحقيق أولي و الذي يناط به رجال الضبطية القضائية.

–تحقيق قضائي ويناط به رجال القضاء، و هذا الأخير يقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق وتحقيق نهائي و يكون في مرحلة المحاكمة من طرف قضاة الحكم.

وفي جميع أنواع التحقيق هذه، يكون للقائمين عليه من ضبطية قضائية وقضاة، صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية، وهو الأمر الذي يفهم صراحة من خلال استقراء نص المادتين 57 و63 من قانون الإجراءات الجزائية الواردتين في

---

[1]–المادة 51 من قانون الإجراءات الجزائية: "يتمتع ضابط الشرطة القضائية بـ:

–رؤساء البلديات، ضباط الدرك الوطني، محافظو الشرطة، ضباط الشرطة، ذوو الرتب في الدرك الوطني و رجال الدرك الذين أمضوا في سلك الدرك أكثر من ثلاث سنوات و يتم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع، مفتشو الأمن لوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الأقل و عينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية وكذا ضباط الصف التابعين للمصالح العسكرية.

[2]– يبدوا أن المشرع يخلط بين التحقيق الأولي والتحقيق الابتدائي وذلك من خلال نص المادة 36 من قانون الإجراءات الجزائية التي تنص على أن ضباط الشرطة القضائية يقومون بالتحقيقات الابتدائية...." وفي نفس الوقت تنص المادة 33 الواردة في الباب المتعلق بالأحكام الخاصة بقاضي التحقيق على أن التحقيق الابتدائي في الجنايات وجوبي وهو بذلك يعتبر أن التحقيق الذي يمارسه سواء رجال الضبطية القضائية أم قضاة التحقيق يعد تحقيقا ابتدائيا على حد السواء.

[3]– زهير كاظم عبود، بحث مقدم للأكاديمية العربية المفتوحة في الدنمارك، كلية القانون والسياسة قسم القانون للدراسات العليا 2007 بدون ترقيم.

الباب الأول من هذا القانون تحت عنوان «في البحث والتحري عن الجرائم" حيث تنص المادة 57 الفقرة الثالثة أنه" يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات..." وتنص في نفس الوقت المادة 63 من نفس القانون أنه "يناط بقاضي التحقيق إجراءات البحث والتحري..." وعليه فإنه يمكن القول إن إجراءات البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أو ابتدائيا، وبهذا المفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولي، بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا[1].

وإذا كان التحقيق عموما يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطويرا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة[2].

المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية.

ان التزايد المستمر للجرائم المعلوماتية قد طرح عدة تحديات لأجهزة الضبط القضائي، مما ترك أثرا بالغا لضرورة تطوير هذه الأجهزة لمواكبة التطور الحاصل في مجال الجريمة، ونتيجة لذلك قامت معظم الدول بإحداث أجهزة متخصصة لمكافحة الجريمة المعلوماتية، والتي تتولى مهمة التحري عن جرائم العالم الافتراضي وإزالة الغموض عنها، وقد حملت هذه الأجهزة تسميات مختلفة منها شرطة الأنترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات.

[1]–بوبقرة خيرة، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2020/2019، ص43

[2]–المرجع نفسه

إلا ان دور هذه الأجهزة لا يقتصر على المستوى الوطني، بل هناك أجهزة خصصت للمستوى الدولي بدورها، سنحاول في هذا المطلب ذكر بعض الأجهزة سواء كان ذلك على المستوى الوطني او الدولي كالتالي:

الفرع الأول: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الداخلي(الوطني):

ذهبت أغلب الأنظمة القانونية الإجرائية في التشريعات المقارنة إلى أن تحيل مسألة البحث والتحري في هذا النوع من الجرائم لأجهزة متخصصة، تكون لها من الكفاءة والتدريب والوسائل البشرية والمادية ما يؤهلها للتعامل مع هذا النوع المستحدث من الإجرام، بالنظر إلى الطبيعة التقنية التي يتميز بها وسوف نحاول أن نلقي الضوء على هذه الأجهزة الموجودة في بعض الدول وفي بلادنا.

1-الأجهزة المختصة في الدول الأجنبية: كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة إذ أن مكافحة الجرائم المعلوماتية مرتبط بمدى تقدم الدول من الناحية التقنية وبمدى توفر الإمكانات المادية اللازمة لإنشاء هذه الأجهزة ونذكر على سبيل المثال في هذا الصدد الدول التالية:

1.1-الولايات المتحدة الأمريكية: قامت الولايات المتحدة الأمريكية بإنشاء عدة أجهزة لمكافحة الجريمة المعلوماتية ومنها[1]:

* **شرطة الوابWebpolice** : وتعتبر نقطة مراقبة على الأنترنت إضافة إلى أنها تتلقى الشكاوى من مستخدمي الشبكة وملاحقة الجناة والقراصنة، والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة[2].

* **مركز تلقي شكاوى الأنترنتIC3** : والذي تم إنشاؤه من طرف مكتب التحقيقات الفدرالي **FBI** في سنة 2000، ثم في عام 2003 تم دمج مركز شكاوى الاحتيال عبر

[1]- بوبقرة خيرة، المرجع السابق، ص45، 46.

[2]- جميل عبد الباقي الصغير، **الجوانب الإجرائية للجرائم المتعلقة بالأنترنت**، دار النهضة العربية، القاهرة، 2002، ص77

الأنترنت المعروف بIFCC مع هذا المركز، ويعمل مركز ic3 بصورة تشاركية مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاءNWC ، ويقوم هذا المركز بتلقي الشكاوى عبر موقعه على الأنترنت أين يقوم الشاكي بماء استمارة الكترونية ثم يقوم المختصون في هذا المركز بتحليل الشكاوى وربطها بالشكاوى الأخرى المستلمة من قبل.

* **قسم جرائم الحاسوب والعدوان على حقوق الملكية الفردية الفكرية:** ويختص هذا القسم بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها.

* **نيابة جرائم الحاسوب والاتصالات CTC:** وتتألف من مجموعة من قضاة النيابة العامة ممن تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات وتم منحهم صلاحيات واسعة في مجال الجرائم المعلوماتية والعدوان على حقوق الملكية الفردية.

* **المركز الوطني لحماية البنية التحتية:** التابع للمباحث الفدرالية الأمريكية وقد حدد هذا المركز البنى التحتية التي تعتبر هدفا للهجومات والاعتداءات عبر الأنترنت وعلى رأسها شبكات الاتصالات.

وإضافة إلى هذه الأجهزة يوجد أيضا في الولايات المتحدة الأمريكية وحدة متخصصة بمكافحة الإجرام المعلوماتي تابعة لقسم العدالة الأمريكي تتكون من خبراء في نظام الحوسبة والأنترنت ومن مستشارين قانونيين[1].

2.1-بريطانيا: قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتحري عن الجرائم المعلوماتية وتضم هذه الوحدة نحو ثمانين عنصرا على درجة عالية من الكفاءة في المجال التقني، وقد بدأت هذه الوحدة نشاطها عام 2001[2].

3.1-فرنسا: قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية ونذكر[3] هذه الأجهزة:

---

[1]- نبيلة هبة محمد هروال، **الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص108.

[2]- بوبقرة خيرة، مرجع سابق، ص46.

[3]-المرجع نفسه.

***القسم الوطني لقمع جرائم المساس بالأموال والأشخاص:** ويتكون هذا القسم من محققين

مختصين في التحقيق بجرائم العالم الافتراضي وقد بدأ هذا القسم مهامه عام 1997.

***المكتب المركزي لمكافحة الإجرام المرتكب بتكنولوجيات المعلومات والاتصالات:** ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة الجرائم المعلوماتية، وقد تم إنشاؤه في:2000/05/15.

4.1-الصين: قامت السلطات في هذا البلد بإنشاء وحدة متخصصة على مستوى جهاز الشرطة تعرف باسم "القوة المضادة للهكرة" وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الأنترنت[1].

5.1-مصر: قامت وزارة الداخلية في مصر بإنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم من خلال الشبكة المعلوماتية نعرضها على النحو التالي:

***إدارة مكافحة جرائم الحسابات وشبكات المعلومات:** أُنشئت هذه الإدارة بموجب قرار وازري[2]، وهي تابعة للإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها فنيا مصلحة الأمن العام التابعة لوزارة الداخلية، وتضم ثالث أقسام رئيسية هي: قسم العمليات، قسم التأمين وقسم البحوث والمساعدات الفنية، وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم المعلوماتية، فهي تتكون من ضباط متخصصين في مجال تكنولوجيا الحسابات والشبكات وتختص بمكافحة جرائم الأنترنت على مختلف أنواعها[3].

***قسم مكافحة جرائم الحاسبات وشبكات المعلومات:** وقد أنشأ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، ويتبع إدارة المعلومات والحاسب الآلي ويخضع من حيث

---

[1]– عمر محمد أبو بكر بن يونس، **الجرائم الناشئة عن استخدام الأنترنت**، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004، ص812.

[2]–قرار وزير الداخلية المصري رقم13507 لسنة 2002 الصادر بتاريخ: 2002/07/07.

[3]–نبيلة هبة مجمد هروال، مرجع سابق، ص141.

الإشراف الفني لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جريمة عليها باستخدام الأساليب والتقنيات العملية الحديثة، ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات[1].

2-الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الوطني:

أما الوضع في بلادنا فإنه وبالنظر إلى الخصوصية التي تتميز بها الجريمة المعلوماتية كان الأمر محتما لتوفير كوادر وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة المعلوماتية وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني.

فعلى مستوى جهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاموناف بالجزائر العاصمة ومِخبرين جهويين بكل من قسنطينة ووهران، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر[2].

أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية، بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني وهو قيد الإنشاء[3].

يعتبر جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الاستثناء إلى بعض الجهات والهيئات الخاصة بحكم خبرتها في مجال معين وباعتبارها الأقدر من غيرها على كشف الجرائم الواقعة ضمن حدود اختصاصها الفني أو

[1]- بوبقرة خيرة، مرجع سابق، ص46، 47.

[2]- بوبقرة خيرة، المرجع السابق، ص48.

[3]-المرجع نفسه.

التقني، والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال ضبط الجرائم والتحري بشأنها[1].

الفرع الثاني: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الدولي والإقليمي:

سبق وأن أسلفنا الذكر بأن الجرائم المعلوماتية تتميز بأنها عابرة للحدود الوطنية يمكن أن يتعدى أثرها عدة دول، لذلك كان لا بد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإجرام، ومن أساليب التعاون الدولي الأمني الذي يمكن أن يحقق أهدافه لا قِبل للشرطة الإقليمية من تحقيقها، ومن أبرز هذه الأجهزة في مجال مكافحة الجرائم المعلوماتية على هذا الصعيد نذكر[2] ما يلي:

1-على الصعيد الدولي: تعد المنظمة الدولية للشرطة الجنائية (الإنتربول)[3] ، من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ومنها الجرائم المعلوماتية، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتية، وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين:

الاولى: تجمع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

---

[1]- عثماني عزالدين، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية-مخبر المؤسسات الدستورية والنظم السياسية، المركز الجامعي مرسلي عبد الله-تيبازة، المجلد الثاني، العدد04، 2018، ص52.

[2]- المرجع نفسه، ص49، 50، 51.

[3]- بعد انتهاء الحرب العالمية الثانية عقد في بروكسل(بلجيكا) مؤتمر دولي في الفترة من 9-6/9 عام 1946 انتهى إلى إحياء اللجنة الدولية للشرطة الجنائية (ICPO)ونقل مقرها إلى باريس وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية الإنتربول ووضع ميثاق هذه المنظمة في الفترة من7-1956/06/13 واعتبر نافذا اعتبارا من 1956/06/13.

الثانية: التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

وتعمل المنظمة الدولية للشرطة الجنائية في مجال الجرائم المعلوماتية بوضع قائمة اسمية لضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية بوضع قائمة اسمية لضباط مختصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين[1]، ولقد أنشأت هذه المنظمة وحدة متخصصة في مكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته.

2-الأجهزة على المستوى الإقليمي:

***الشرطة الأوروبية أو الأوروبول:** هو جهاز على مستوى الاتحاد الأوروبي تم إنشاؤه في لوكسمبورغ عام 1992 ومقره في مدينة لاهاي بهولندا ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة وكذا الإجرام المعلوماتي، ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة لمختلف الدول الأعضاء، وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتية.

وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه اسم (Internet Crime Reporting online System) في سنة 2010 بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء.

* **الأوروجست Eurojust:** وهو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، تم إنشاؤه عام 2002 وينعقد اختصاصه

[1] - Myriam QUEMENER، Cybercriminalité -droit pénal appliqué، econonica, Septembre 2010, p208.

عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الاتحاد الأوروبي، ويعد الأوروجست وحدة للتعاون القضائي، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات ومباشرة متابعات جزائية.

المطلب الثاني: خصائص التحقيق والمحقق في الجريمة المعلوماتية

تعد مرحلة التحقيق الابتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات، مرحلة هامة في سبيل البحث والتحري عن الجرائم وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة المعلوماتية لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم ففي كثير من الجرائم المعلوماتية لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإحباط والإعجاب معا[1].

الفرع الأول: خصائص التحقيق في الجريمة المعلوماتية

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة. وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزائها شيئا سوى الخضوع والامتثال أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثير[2].

أولا–منهج أو أسلوب التحقيق الابتدائي في الجريمة المعلوماتية: والهدف من التحقيق الابتدائي هو التأكد أولا من وقوع جريمة يعاقب عليها القانون، ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وما هي الوسائل التي استعملت في

[1]–الخن محمد طارق عبد الرؤوف، **جريمة الاحتيال عبر الانترنت**، منشورات الحلبي الحقوقية،2010، ص230.

[2]–خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2010، ص56.

ارتكابها، ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي عن غيره بالنسبة للجرائم الأخرى[1].

1-وضع خطة عمل التحقيق: يبدأ المحقق عمله عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو[2] الآتي:

-وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة.

-التخطيط الفني للتحقيق و ذلك من أجل الوصول إلى أفضل الطرق والأساليب للتعامل مع هذه الجرائم بالتفصيل والوضوح.

-عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق.

-تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل وهو ما يؤدي إلى ضمان مستوى جيد من الأداء.

-تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبرة أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة[3].

ويجب أن ترتكز خطة العمل على مجموعة من البنود الأساسية يتم الارتكاز عليها أثناء تنفيذ الخطة، وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب استيضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال

---

[1]- بوبقرة خيرة، مرجع سابق، ص52.

[2]-المرجع ننفسه، ص52، 53.

[3]-محمد نصير السرحاني، **مهارات التحقيق الفني في الحاسوب والأنترنت**، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص72.

التحقيق[1]، بالإضافة إلى مراعاة الظروف والملابسات المحيطة بالواقعة ذلك أن من هذه الظروف ما يشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل[2] ومنها:

-مدى أهمية الأجهزة و الشبكات المتضررة لعمل المنظمة.

-مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها.

-مستوى الاختراق الأمني الذي تسبب فيه الجاني.

ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش وذلك من خلال تحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها.

2-تشكيل فريق التحقيق: يجب أن يتشكل فريق التحقيق من فنيين وأخصائيين ذوي خبرة في مجال الحاسوب والأنترنت، يمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والأنترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة[3].

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما تطلبه من مهارات فنية وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا ومن الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم المعلوماتية من:

-المحقق الرئيسي ويكون ممن لهم خبرة في التحقيق الجنائي.

-خبراء الحاسوب و شبكات الأنترنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم.

-خبراء ضبط و تحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.

-خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.

---

[1]-هشام رستم، **الحواسب الإجرائية للجرائم المعلوماتية**، مكتبة الآلات الحديثة، أسيوط، 2000، ص59.

[2]-بوبقرة خيرة، مرجع سابق، ص53.

[3]-عبد الله حسين محمود، **إجراءات جمع الأدلة في الجريمة المعلوماتية**، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003، ص612.

– خبراء التصوير والبصمات والرسم التخطيطي[1].

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك[2].

الفرع الثاني: العناصر الأساسية للتحقيق الابتدائي في مجال الجريمة المعلوماتية

ونقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي[3].

1-الإجراءات التي يجب على الضبطية القضائية مراعاتها قبل البدء في التحقيق:

ويمكن أن نسرد الأهم منها[4] كما يأتي:

-تحديد نوع نظام المعالجة الآلية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات.

-وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل واحد منهم.

-إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه، و هل هناك حواسيب آلية خارج هذه الشبكة ولها إمكانية الاتصال بها أم لا؟

---

[1]– عبد الله حسين محمود، المرجع السابق، ص612.

[2]– انظر المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]–عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، ط1، ص84.

[4]–بوبقرة خيرة، مرجع سابق، ص55، 56.

-مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.

-مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

-يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته.

-فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها، و التحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها لطمس البيانات.

-التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها و تضليل أجهزة المراقبة و أجهزة التحقيق بعد ذلك.

-إبعاد الموظفين عن أجهزة الحاسب الآلي بعد الحصول منهم على كلمة السر و كذا الشفرات في حالة وجودها.

-تصوير الأجهزة المستهدفة (التي وقعت بها أو عليها الجريمة) من الأمام و الخلف و ذلك لإثبات أنها كانت تعمل و كذلك للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق.

2-الإجراءات التي يجب مراعاتها أثناء التحقيق: عند البدء في عملية التحقيق الابتدائي سيما عند القيام بعملية تفتيش جهاز الحاسوب فإنه على رجال الضبطية القضائية وبرفقتهم الخبراء الذين يستعينون بهم بمراعاة[1] ما يلي:

-عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانة المرنة قبل استخدامها و التأكد فنيا من دقة النسخ عن طريق الأمر (disque comp).

-نزع غطاء الحاسب الآلي المستهدف و التأكد من عدم وجود أقراص صلبة إضافية.

[1]- بوبقرة خيرة، المرجع السابق، ص56، 57.

-أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص تحليل المعلومات الموجودة بغرض التوصل إلى معرفة الملفات الممسوحة، ويمكن استعادتها من سلة المهملات مع ملاحظة أن هناك بعض الملفات التي إن مسحت وضغط على أزرار معينة مثل Shift delete في وقت واحد لا يمكن استعادتها وكذا من أجل معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.

-العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلوماتي.

-العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

-حفظ المعدات والأجهزة التي تضبط بطريقة فنية و سليمة.

الفرع الثالث: خصائص المحقق المعلوماتي

أمام التطور التقني والتكنولوجي الذي صاحب الجريمة المعلوماتية فإن المختصين بالتحقيق في هذا النوع من الإجرام المستحدث يختلفون عن أولئك المختصين بضبط الجرائم التقليدية من حيث الخصائص وطريقة التكوين.

ذلك أن التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن الجرائم المعلوماتية وكشف النقاب عنها.

وإذا كان قد سبق وأن طرحنا خصائص الجريمة المعلوماتية وكذا خصائص المجرم المعلوماتي فإنه في اعتقادنا يلزم الأمر معرفة الخصائص التي يجب أن يتوفر عليها من يتصدى لمهمة البحث والتحري عن هذا النوع من الجرائم والمجرمين.

أولا-الخصائص الفنية للمحقق في الجريمة المعلوماتية: والمشكلة الأساسية التي تواجه المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فمتخصص الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دواع الجريمة وجمع الأدلة لتقديم

المتهم للمحاكمة، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول جريمة معلوماتية ما، ولكن من الناحية القانونية يتبين فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم[1].

وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلازمه عند مباشرته التحقيق في الجريمة المعلوماتية معرفة العديد من الجوانب الفنية ليقوم بعمله على أحسن وجه ونذكر[2] منه:

-معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والأنترنت و التي تتعلق بالجريمة المرتكبة ذلك أن افتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل، على اعتبار أن جهله بارتكاب أساليب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات[3].

-إتباع الإجراءات الصحيحة و المشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقع الجريمة، و تخزينها في الأقراص المعدة لذلك و منع حذفها و الحرص على عدم تعريض وسائط التخزين كالأقراص المرنة أو المدمجة لأية مؤثرات خارجية كالقوى الكهرومغناطيسية أو موجات الميكروويف حتى لا تتلف محتوياتها.

---

[1]- في حادثة طلب أحد المحققين من المشتبه فيه أن يريه الملف الذي قام بتزويره انطلاقا من الحاسب الشخصي له فما كان للمشتبه فيه إلا أن قام عمدا بحذف هذا الملف وبذلك أضاع الدليل الرئيسي في الجريمة وفي حادثة أخرى تم القبض على بعض المهتمين وضبط الحاسوب ثم قامت جهات التحقيق بتفكيك الحاسوب باعتباره دليل على الجريمة وقامت بنقله إلى مركز الشرطة ثم بعدها تبين أن تشغيل الجهاز لفحص مكوناته يحتاج إلى إعادة توصيل الكابلات التي تم نقلها دون أن يتم ترقيمها وكان الأمر يبدو شبه مستحيل وضاع حتى الدليل أيضا.

[2]-بوبقرة خيرة، مرجع سابق، ص59، 60.

[3]- جميل عبد الباقي، الصغير، **أدلة الإثبات الجنائي والتكنولوجيا الحديثة**، دار النهضة العربية القاهرة، 2002، ص115.

-كما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والأنترنت وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي من اختراق للشبكات واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنها تعطي للمحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات التي تحول دون ذلك[1].

-يتوجب على المحقق أن يستطيع التمييز بين الأنظمة المختلفة لتشغيل الحاسوب وأن يلم بجميع الأنظمة التشغيلية لأجهزة الحاسوب وما تتسم به من خصائص ومميزات كل نظام على حدي لأنه ملزم بالتعامل معها.

كذلك أنظمة الملفات التي يعتمدها كل نظام حتى يتمكن من إجراء التحقيق في الجرائم المعلوماتية وفي كشف المجرمين ومعاينة مسرح الجريمة وإذا كان التعامل المباشر مع هذه الأنظمة والقيام بفحصها ورفع الأدلة الجنائية الرقمية الموجودة فيها يعتبر مهمة الخبير «إلا أن معرفة المحقق الجنائي الأولية بهذه الأنظمة ضرورية لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة المعلوماتية.

-كما يتعين على المحقق كذلك التعرف على معطيات الحاسوب المختلفة ليصبح قادرا على معرفة صيغ الملفات وما يمكن أن تحتويه من معطيات، ومعرفته لأهم التطبيقات التي يمكنه من خلالها قراءة أو مشاهدة محتوى هذه الملفات[2]، والتي تعد أمرا في غاية الأهمية، لأنها تعتبر الوعاء الحقيقي لأدلة الإدانة في كثير من القضايا ذات الصلة بالحاسوب والأنترنت بما تحتويه من معلومات.

---

[1]- حسين سعيد بن سيف الغافري، **الجهود الدولية في مواجهة جرائم الأنترنت**، ورقة مقدمة للاتحاد العربي للتحكيم الإلكتروني،2007، ص02.

[2]-يتم حفظ البيانات الرقمية داخل الحاسوب على شكل مجموعات أو كتل من البيانات تمثل وحدة واحدة تسمى الملفات ويتميز كل ملف ببنية وصيغة خاصة تميزه عن غيره، وغالبا ما ترتبط صيغة بنوع محدد من المحتوى كأن يحتوي الملف على بيانات تمثل صورا أو أصواتا أو مستندا خطيا منسق أو غير منسق.

–و من الأمور الفنية التي يتوجب على المحقق معرفتها أيضا أن يكون ملما بالأساليب المستخدمة في ارتكاب الجرائم المعلوماتية و تقنيات الأمن المعلوماتي، ذلك أن معرفة رجال التحقيق لهذه الأساليب يعد من الأمور المهمة التي تساعدهم في معرفة الجناة ومواقع ارتكاب الجريمة ومن أي طرفية الكترونية صدر السلوك الإجرامي وكذلك في مناقشة الشهود وسماع المشتبه فيهم و محاصر تهم بالأسئلة التي تتعلق بكيفية ارتكاب الجريمة وطرق تنفيذها.

ثانيا–تأهيل وتدريب المحقق المعلوماتي: في مكافحة الجرائم المعلوماتية بصفة عامة لا بد من وضع سياسة جنائية رشيدة تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التأهيل والتدريب إلى العاملين بأجهزة الضبطية القضائية.

وقد تنبهت الدول إلى هذا الأمر وظهر هذا الاهتمام في توصيات العديد من المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين، ومنها ما جاء في القاعدة 1/22 من قواعد بيكين التي أكدت على الحاجة إلى التخصص المهني والتدريب.

ولهذا فإنه من الضروري إعداد المحققين في الجرائم المعلوماتية باعتبارهم يواجهون أنشطة إجرامية معقدة وتنفذ بطرق دقيقة وذكية، ويتأتى ذلك من خلال الإسراع في أن يطور رجال البحث الجنائي وسائلهم البحثية وقدراتهم العلمية وليس بالضرورة أن يكون المحقق في الجريمة المعلوماتية خبيرا في الحاسوب والنظم المعلوماتية ولكن لا بد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي وحسن استغلالهم في كشف الجرائم وجمع الأدلة كما أنه من الضروري أن يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة و التدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة عملية وسليمة[1].

وإذا كانت الشركات الخاصة تستعين بمحققين هم خبراء في الحواسيب، فالجهات الحكومية أولى بإعداد كوادرها للضبط والتحقيق في الجرائم المعلوماتية، فالتقدم المتواصل في

[1]– البشري محمد الأمين، **التحقيق في جرائم الحاسب الآلي**، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة الفترة من01 إلى03 ماي 2000.

تكنولوجيا الحاسب الآلي والأنترنت يفرض على جهات تطبيق القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات وهذا الأمر يتطلب الإلمام بالتقنيات الجديدة حتى يمكن مواجهة مجرمي المعلوماتية.

ويرى الفقه الجنائي أنه حال التدريب على التحقيق في الجريمة المعلوماتية يتعين مراعات عناصر أساسية تتمثل في شخص المتدرب ومنهج الدورة التدريبية وصفة وأسلوب التدريب[1].

ويجب أن يشمل منهج التدريب خصوصا تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة والأساليب التي تتعلق بالكشف عنها وكيفية إثباتها ومعاينتها والتحفظ عليها وكيفية فحصها فنيا.

وقد كان هناك من يرى أن صعوبة التحقيق الجنائي في الجرائم المعلوماتية تتطلب أن يعهد بهذا التحقيق إلى بيوت خبرة متخصصة في هذا المجال، لكن هذا الأمر له خطورته إذ من شأنه أن يضحي بمصلحة الفرد والمجتمع ويضعها تحت رحمة هذه الشركات التي يكون همها تحقيق الربح المادي على حساب إظهار الحقيقة، فضلا عن الإخلال بمبدأ سرية التحقيق سيما لو تعلق التحقيق بجرائم عرض الأشخاص وأسرارهم الشخصية أو تعلق الأمر بأمن الدولة[2].

المبحث الثاني: إجراءات الحصول على أدلة الإثبات للجريمة المعلوماتية

تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورا ملموسا يواكب حركة الجريمة وتطور أساليب ارتكابها، فبعد أن كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الاستعانة بالأساليب العلمية واستخدام شبكة الإنترنت هي الصفة المميزة والغالبة، ومراد ذلك هو حدوث طفرة علمية في مجال تكنولوجيا المعلومات و الاتصالات و استخدام الوسائط الإلكترونية في شتى مجالات

[1]– رستم هشام محمد فريد، **الجرائم المعلوماتية**، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، ص115.

[2]–البشري محمد الأمين، مرجع سابق، ص25.

الحياة، فكلما اكتشف العلم شيئا حديثا وجد الاكتشاف طريقه إلى مجال الإثبات الجنائي و التدليل.

وقد اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها بموجب القانون 09-04 المؤرخ في 05 غشت2009 على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

المطلب الأول: إجراءات كشف الجريمة المعلوماتية

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعوانها، حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية[1] فقط.

إذ بوقوع جريمة ينشأ حق الدولة والمجتمع في معاقبة مرتكبيها، وهذا لا يتم إلا من خلال اجراءات التحقيق في الجريمة بكافة الوسائل والطرق المتاحة حتى يمكن إدانة مرتكبها، وبموجب ذلك، فإن النيابة العامة هي المختص الوحيد بتحريك الدعوى العمومية، وذلك بإجراء التحقيق فيها بنفسها أو من تفوضه من مأموري الضبط القضائي وفقا لأحكام القانون.

من ثم بعد انتهاء التحقيق في الجريمة، تحال إلى المحكمة المختصة للنظر بها واصدار حكم قطعي. فإجراءات التحقيق المتبعة في كافة الجرائم تأخذ بجميع عناصر التحقيق الجنائي المتكامل وتمر بذات المراحل الفنية والشكلية، وتعد هذه الإجراءات في أي جريمة تماما كما هو

[1]-أحمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم09-04**، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة ورقلة، السنة الجامعية 2012-2013، ص66.

الحال في الجرائم الأخرى أو كانت جريمة الكترونية فالمحصل النهائي في التحقيق هو العثور على أدلة واضحة يمكن أن تستدل المحكمة بها وتصدر العقوبة عليها[1].

إن أهمية جهاز الضبطية القضائية في الكشف عن الجريمة الإلكترونية والتعرف على المجرم الإلكتروني، تبعه استعداد المشرع الجزائري لأساليب التحري الخاصة المستعملة بما تناسب ومتطلبات ضبط الوجه الجديد للإجرام حتى يسمح للقضاء والضبطية أن يتكيف دورها في مهامها مع الإجرام الجديد مستمدة شرعيتها من المواثيق الدولية التي صادقت عليها الجزائر، وخاصة المادة 20 من اتفاقية باليرمو لمكافحة الجريمة المنظمة عبر الحدود الوطنية التي أدرجت الجريمة الإلكترونية كشكل من أشكال الجريمة المنظمة[2].

ونظرا لأهمية التحقيق في هذا النوع من الجرائم وكشفها قسمنا هذا المطلب إلى فرعين تناولنا في الفرع الأول الإجراءات التقليدية، وفي الفرع الثاني الإجراءات المستحدثة.

الفرع الأول: الإجراءات التقليدية

من المعلوم أن الأنظمة الإجرائية لمختلف الدول تحتوي على مجموعة من الأساليب والوسائل التقليدية التي تلجأ اليها سلطات البحث والتحري للكشف عن مختلف الجرائم مثل الخبرة والتفتيش، حيث تعتبر تلك الوسائل من الأساليب العامة والتقليدية المستعملة للتحقيق في أي جريمة كانت، لدى وباعتبارها أي الجريمة المعلوماتية من الجرائم، فإنه وجب الاستعانة بتلك الوسائل رغم تقليديتها من أجل التحقيق[3].

طبعا ولأن البيئة الاجرامية مختلفة والجاني والمجني عليه مختلفان كذلك عن نظيريهما في الجرائم التقليدية، بالإضافة الى الوسائل المرتكبة بواسطتها الجريمة المعلوماتية، فإنه أصبح من

[1]–البشري محمد الأمين، مرجع سابق، ص 349.

[2]– نبيلة هبة هروال، **الجوانب الإجرائية لجرائم الأنترنت**، الطبعة 2، دار الفكر الجامعي، مصر، 2011، ص 76.

[3]– بن بادة عبد الحليم، **إجراءات البحث والتحري عن الجريمة المعلوماتية**، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، المجلد الثاني، العدد 23، 2015، ص78.

الضروري إعادة تحيين تلك الوسائل التقليدية بما يتوافق مع الطبيعة الخاصة للجريمة المعلوماتية حتى تتمكن من انتاج دليل يعتد به قضائيا[1].

وتمر هذه الإجراءات بمرحلتين مهمتين تتمثلان في مرحلة جمع الأدلة ومرحلة التحقيق فيها.

أولا-مرحلة جمع الأدلة في الجريمة المعلوماتية: تعتمد مرحلة الاستدلال على تلقي التبليغات او الشكاوى عن الجريمة، كما تعتمد على الاستجواب والاستماع للشهود، لدى سنحاول من خلال دراستنا التطرق للإجراءات الواجبة التطبيق لهذه المرحلة.

1-تلقي البلاغات والشكاوى

1.1-تلقي البلاغات في الجريمة المعلوماتية: ويقصد بالتبليغ عن الجريمة مجرد الإخبار عنها، ويكمن أن يكون التبليغ من مصدر معلوم أو جهة غير معلومة، ويعقب تلقي التبليغات جمع الاستدلالات مباشرة، والواقع أن التبليغ يصدر به إخبار الجهات المختصة بالتحقيق عن جريمة معينة وقعت أو على وشك الوقوع قيد التحضير أو وجود اتفاق أو عزم على ارتكابها[2].

الأصل أنه يجب على رجال الضبطية القضائية قبول البلاغات أو الشكاوى التي تقدم إليهم سواء كانت كتابية أو شفهية، وعند ورودها للقسم تقيد في دفتر خاص بتلقي البلاغات، كما يجب على المتحري أو المحقق إخطار رئاسته في حالة الجرائم الإلكترونية، واخطار الجهات المختصة مثل: إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، ومن الأخطاء الشائعة في هذا المجال، الامتناع عن قبول البلاغ أو الشكوى بدعوى عدم الاختصاص

[1]-المرجع نفسه.

[2]- فضل سليمان احمد، **المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الإنترنت**، دار النهضة العربية، القاهرة، 2013، ص 276.

المكاني أو النوعي بها، في حين أن الواجب اتخاذ الإجراءات المقررة بشأنها، ثم إخطار جهة الاختصاص وإحالة المحضر إليها[1].

ويقوم المتحري بجمع الأدلة وفحص البلاغ أو الشكوى إجراءات معينة تتمثل في المعاينة وجمع الأدلة والتحقيق[2].

كما يتم الإبلاغ عن الجريمة الإلكترونية عن طريق الانترنت أو ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق، كإبلاغها عن وجود صفحات أو مواقع غير مشروعة بإرسال رسالة إلكترونية مثلا تتضمن التبليغ عنى وجود موقع منشور فيه صور الاستغلال الجنسي للأطفال[3].

والمعلومات التي يجب معرفتها من المبلغ والتي ينبغي أن يدونها المحقق عند تلقي البلاغ، يمكن الحصول عليها من خلال طرح أسئلة عن تاريخ وقت تلقي البلاغ، المعلومات الخاصة، طبيعة ونوع الجريمة الإلكترونية، محل البلاغ، إلى غيرها من الأسئلة المتعلقة بالجريمة[4].

2.1-الشكوى في الجريمة المعلوماتية: قد يترتب على الجريمة ضرر خاص قد يصيب أحد الأفراد ماديا أو معنويا، فينشأ له حق تحريك الدعوى العمومية بتقديم شكوى أمام الجهة المختصة بالتحقيق حيث نص المشرع الجزائري في قانون الإجراءات الجزائية أنه يحق لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص وقد عرفت الشكوى بأنها البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طلبا لتحريك الدعوى العمومية بشأن جريمة معينة[5].

---

[1]- بوعمرة محمد، بنينال سيد علي، **جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري**، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أكلي أولحاج البويرة، السنة الجامعية:2020/2019، ص 42.

[2]-خالد عباد الحلي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، دار الثقافة، الأردن، 2011، ص .79

[3]- بوعمرة محمد، بنينال سيد علي، مرجع سابق، ص 42.

[4]-المرجع نفسه.

[5]-المرجع نفسه، ص43

ولقد خصصت العديد من المراكز لمعالجة هذه الشكاوى على سبيل المثال مركز تلقي الشكاوى عن جرائم الاحتيال عبر الأنترنت المؤسسة في فيرجينيا الغربية بالولايات المتحدة الأمريكية من طرف مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء[1] من أجل مكافحة ظاهرة الاحتيال عبر الانترنت[2].

2-الاستجواب وسماع الشهود في الجريمة المعلوماتية:

1.2-الاستجواب: وهو أن يمثل أمام المحقق حتى يتحقق من هويته ومحيطه علما بكل الوقائع المنسوبة إلي وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخبر المتهم في أن له الحق في توكيل محامي وإن لم يقدر يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إذا ما طرأ تغيير عنوانه أن يخطر المحقق بذلك[3].

2.2-سماع الشهود: سماع الشهود هو إجراء من الإجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة، بحيث يستدعي أشخاص ليست لهم علاقة بالجريمة، إلا أن وجودهم ضروري للكشف عن الجرائم والقبض عن مرتكبها يختلف الشاهد في الجريمة الإلكترونية عن

---

[1]-الياقات البيضاء: يشار اليه على انه متسلل أخلاقي يتعرف ظاهرياً على الثغرات الأمنية. حيث يجادل قراصنة الياقة البيضاء بأن الانترنت أصبح أكثر أمانا بسبب أنشطتهم. السؤال الرئيسي هو: **ما إذا كان الاختبار يجب أن يؤذن؟** من السهل تصوير شخص ما على انه يتصرف بشكل أخلاقي من خلال اختبار الأنظمة، ولكن لا يمكن انكار أنه **يمتلك مستوى عالٍ من المعرفة المتخصصة جنبا الى جنب مع الايمان بأخلاقيات حرية الوصول**. بعبارة أخرى أحد عيوب مفهوم تحسين الأمان هو: **ما يحدث للمعلومات المكتسبة في الهجوم؟** عند تقديم المعلومات بهدوء وسرية، يشير ذلك الى أنه تصرف أخلاقي، ويحاوَلُ بشكل شرعي تحديد العيوب المحتملة واغلاقها بسرعة. وإذا أعلن المتسلل للعالم عن خرق أمنى يسمح للأخرين باستغلال الخلل حتى يتم غلقه، يعتبر هذا تصرف غير أخلاقي. هذه نقطة أساسية: **كيف يمكن للمتسلل معرفة ما هو ضار وما هو غير ضار؟** ما يعتبره شخص ما غير ضار، قد يعتبره الأخر انتهاكا صارخا للخصوصية. إذا قرر شخص ما إلقاء نظرة غير مدعوة حول المنزل، والحجة أن الباب كان مفتوحا أو لم يتطلب الكثير من الدفع، لن يكون من المتوقع أن يعتبر ذلك مبررًا لفعله. أي انه من الصعب تحديد الدافع بعد الواقعة، فمن السهل على شخص تم القبض عليه ان يدعي انه فعل ذلك لسبب أخلاقي ولم يكن ينوي فعل المزيد، خاصة في حالة عدم توفر أدلة كافية. هذه مشكلة تتجاوز تصنيف الياقات البيضاء وستكون صحيحة لجميع الياقات. لهذا السبب فان فكرة الياقات معيبة وهناك حاجة الى طرق بديلة لتصنيف القراصنة.

[2]- بوعمرة محمد، بنينال سيد علي، مرجع سابق.

[3]- خالد عباد الحلي، المرجع السابق، ص80.

الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية[1].

ثانيا-التحقيق في الجريمة المعلوماتية: عند تلقي المحقق البلاغ أو الشكوى بوقوع جريمة ما، فإنه ينتقل مباشرة إلى مكان وقوعها مع إخطار وكيل الجمهورية، وذلك بهدف التنقيب عن الأدلة وحمايتها إلا أنه تجدر الإشارة إلى أن مسرح الجريمة الإلكتروني بالإضافة إلى المسرح المادي يوجد مسرح إلكتروني متمثل في البيئة الإلكترونية التي يجد فيها المحقق صعوبة استخلاص الدليل منها، مما يدفعه للاستعانة بالخبراء الفنيين في هذا المجال، في معاينة مسرح الجريمة أو القيام بالعمليات التفتيش والضبط وفحص آثار الجريمة، لا تشكل خللا فنيا أو قانونيا، كما هو الحال في التحقيق مع الشهود والمتهمين، إذ أن أخذ أقوال الشهود واستجواب المتهمين يعتمد على خبرات المحققين، ويعتبر الاستجواب مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق، ومطالبته له رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما، وذلك قصد محاولة الكشف عن الحقيقة واستظهارها بالطرق القانونية[2].

تتولى سلطة مختصة إجراء الاستجواب، إذ يجب على جهات التحقيق أن تكون مؤهلة للتحقيق في الجرائم المعلوماتية حتى يمكن استيعاب واقعة التحقيق، إن طريقة توجيه الأسئلة وترتيب أولوياتها واستنتاج الحقائق من الطريقة التي يتحدث بها المتهم وقراءة لغة الجسد لديه، أمور مهنية لا يوفيها حقها إلا المحققون الذين اكتسبوا الخبرة والمعرفة العلمية[3].

[1]- بوعمرة محمد، بنينال سيد علي، مرجع سابق، ص43.

[2]بوعمرة محمد، بنينال سيد علي، المرجع السابق، ص44.

[3]- حزيط محمد، **قاضي التحقيق في النظام القضائي الجزائري**، دار هومة، الجزائر، 2010، ص 102.

1-التفتيش: يذهب اغلب فقهاء القانون الجنائي الى القول إن التفتيش هو أحد إجراءات التحقيق يباشره موظف مختص يهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة خاصة وذلك وفقا للضمانات والقيود القانونية المقررة[1].

وهناك من يعرف التفتيش بأنه إجراء من اجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبها إلى المتهم بارتكابها[2].

يتضح من خلال التعريفين الأهمية البالغة لهذا الإجراء كالخصوصية الكبيرة التي يتمتع بها نظرا لما يمثله من الاعتداء على حرمة الحياة والأماكن الخاصة لهذا قيده المشرع الجزائري بمجموعة من الضوابط لا من حيث الأوقات التي يتم فيها[3]، ولا من حيث الأماكن التي يمكن أن تخضع للتفتيش[4]، ولا من حيث الجهات المخول لها القيام بعملية التفتيش[5].

قسم الفقهاء مسرح الجريمة المعلوماتية إلى نوعين[6] مسرح تقليدي وأخر افتراضي:

*المسرح التقليدي: يتمثل هذا المسرح من الجريمة المعلوماتية في الوسائل الموجودة كالملموسة في المكان الذي ارتكبت فيه الجريمة مثل أجهزة الإعلام الآلي، أقراص التخزين، الصور، البصمات وبالتالي فهذا المسرح ال يختلف عن المسرح في الجريمة التقليدية.

*المسرح الافتراضي: هذا المسرح هو الذي يصنع الفرق والخصوصية بين الجريمة المعلوماتية وباقي الجرائم، كونه تتجلى فيه فنيات وتقنيات ارتكاب الجريمة المعلوماتية ومن

---

[1]-سعيداني نعيم، **اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، السنة الجامعية: 2013/2012، ص143.

[2]-هلالي عبد الله أحمد، تفتيش نظم الحاسوب الالي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997، ص73.

[3]-انظر المادة 47 من قانون الإجراءات الجزائية الجزائري.

[4]- انظر المادة 335 من قانون العقوبات الجزائري.

[5]- انظر المادة 44 من قانون الإجراءات الجزائية الجزائري.

[6]-بن بادة عبد الحليم، مرجع سابق، ص78.

خلاله يمكن الحكم على وسائل البحث والتحري التقليدية فيما مدى نجاحها في الكشف عن مثل تلك الجرائم، ويتمثل هذا المسرح في داخل الحاسوب من خلال المكونات الرقمية التي تتواجد فيه وفي مختلف مكوناته (الذاكرة، الأقراص الصلبة...)، ولا يمكن أن يتعامل مع هذا المسرح الا شخص خبير ذو دراية واسعة بفنيات وتقنيات الحاسب الآلي.

1.1-إجراءات التفتيش في الجرائم الماسة بالمعطيات الرقمية: تعد إجراءات التفتيش والضبط من إجراءات التحقيق التي تختص بها سلطة التحقيق ويناط لضابط الشرط القضائية القيام بهما في حالات استثنائية ويعتبر التفتيش وسيلة للحصول من خلاله على أدلة في بيان وظهور الحقيقة، ولا يكفي في التفتيش مجرد توافر شروطه سواء الموضوعية أو الشكلية، بل يلزم أيضا ضرورة مراعاة حدوده الداخلية و التي يتمثل أهمها في ضرورة التقيد بالغرض من التفتيش أثناء تنفيذه وفقا لما نص عليه قانون الإجراءات الجزائية والذي يقضي بأن الأصل في التفتيش هو البحث عن الأشياء المتعلقة بالجريمة موضوع التحقيق، ويلاحظ أنه في الحالات التي يجوز فيها لضابط الشرط القضائية القيام بإجراء التفتيش و الضبط فإن مشروعية هذا الإجراء تتوقف على محل ارتكاب الجريمة ومدى تبعيته للمجني عليه[1].

1.1.1-إجراءات تفتيش النظام المعلوماتي الخاص بالمتهم: إذا كان محل ارتكاب الجريمة ينصب على نظام المعلومات الخاص بالمتهم دون لزوم التدخل في نظام معلوماتي لشخص آخر، وفي هذا الفرض إذا كانت الشروط الإجرائية للتفتيش صحيحة وفقا لما نص عليه القانون فإن التفتيش وما يسفر عنه من ضبط أي من الأدلة، سواء أكانت هذه الأدلة هي أجهزة الكمبيوتر أم أحد الوسائط المتعددة، يكون مشروعا، وهذا الحال يكثر في جرائم التزوير والتزييف حيث يتم التفتيش وملحقاته من طابعات ملونة أو أجهزة ماسح ضوئي، و يتم نقل البرنامج الداخلي الذي يوجد عن طريق إتمام عملية التزوير أو التزييف في أي من الوسائط المتعددة و بذلك يتم الحصول على دليل ارتكاب الجريمة، وهذا ما يتم أيضا في جرائم النسخ و

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص228.

التقليد حيث يتم ضبط الوسائط المتعددة المحملة بالبرامج المنسوخة و الأجهزة المستخدمة في ذلك[1].

2.1.1-إجراءات التفتيش في نظام معلوماتي غير خاص بالمتهم: يظهر هذا الفرض في الجرائم التي ترتكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة من أي جهاز من أجهزة الحاسبات الآلية الأخرى المتصلة بالحاسب الذي ارتكبت في نظامه المعلوماتي الجريمة وفي هذا الفرض فإن إجراءات التفتيش والضبط تتطلب الدخول في نظام معلوماتي لشخص آخر. ويلاحظ أن قانون الإجراءات الجزائية نص على أنه لا يجوز لرجال الشرطة القضائية الدخول في أي محل مسكون إلا في الأحوال المبينة في القانون، أو في حالة طلب المساعدة من الداخل ... وهو ما دعا المشرع إلى مد تلك الحماية إلى المحل الخاص بحيث أقر له ذات الحماية الخاصة بالمسكن وكذلك السيارة الخاصة إذا كانت توجد في مسكن المتهم، أما إذا وجدت في الطريق العام فلها نفس حرمة الشخص بحيث لا يجوز تفتيشها إلا إذا جاز تفتيش الشخص قانونا[2].

3.1.1-تطبيقات في إجراءات تفتيش نظم الحاسبات الآلية الخاصة بالأشخاص: طبقا لمعيار الخصوصية التي يحميها المشرع يتبين أنه قد تناول المسكن والسيارة والمحل وكل ما يتعلق بالشخص ويمثل خصوصياته، ولذلك فإن نضام المعلومات وما يحتويه من خصوصيات للأشخاص تخضع أيضا بالتبعية لمعيار الخصوصية من حيث عدم جواز التدخل فيها بدون إذن من وكيل الجمهوري[3].

ورغم أن المشرع وفي جل القوانين التي نصها حاول حماية خصوصية الأفراد بما فيها البيانات والمعلومات الشخصية وكذلك السجلات والدفاتر أو الحاسبات الآلية والملحقات السرية بعدم جواز الاطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون،

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص230.

[2]- عثماني عزالدين، مرجع سابق، ص61.

[3]- خالد ممدوح إبراهيم، مرجع سابق، ص331

وهذا ما أكده أيضا بامتداد الحق في التفتيش إلى سجلات البيانات التي تكون في موقع إلكتروني آخر عندما يكون التخزين الفعلي خارج المكان الذي يتم فيه التفتيش[1].

وكذلك ذهب جانب آخر من الفقه بأن البيانات لها طابع مادي على أساس أنها نبضات أو ذبذبات إلكترونية وإرشادات أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط متعددة ويمكن قياسه[2].

ولأن البحث عن الدليل على ارتكاب الجريمة، من حيث كونه وسيلة للإثبات ومحلا للإقتناع وفقا لنظرية الإثبات الجنائي يتطلب الإقرار بإمكانية أن تكون المعلومات محلا للتفتيش وضبط الأدلة المتحصل عليها، يلاحظ أن الأمر يختلف من حيث صدور إذن بالتفتيش في النظام المعلوماتي لأحد الأشخاص عنه في الإذن بالتفتيش في الجرائم التقليدية الأخرى.

لأن الإذن قد يصدر في حق شخص ارتكب جناية أو جنحة وقامت قرائن قوية على ارتكابه للجريمة وعند القيام بتنفيذ إذن التفتيش، فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما اتبع للمتهم، أو أن للمتهم أكثر من جهاز في أمكان مختلفة كأن يكون المتهم مالكا لجهاز في منزله وجهاز أخر في عمله، أو أن يكون الشخص له شريك في الأجهزة مما يتطلب الحصول على إذن آخر من وكيل الجهورية[3].

ويتم ذلك عن طريق تحديد مجال هذا التفتيش وما يستتبعه بالضرورة من تتبع لشبكات المعلومات، ويخضع ذلك للسلطة التقديرية للقاضي من حيث توافر حالة الضرورة أو عدم توافرها، وهذا النظام اتبعته بعض الدول مثل الولايات المتحدة الأمريكية وكندا، حيث نصتا على أن يكون إذن التفتيش متضمنا[4] ما يلي:

-البحث عن أدلة محصلة من كيان الحساب المنطقي و التي يدخل فيها برامج التطبيق و نظم التشغيل.

[1]- عثماني عزالدين، مرجع سابق، ص61، 62.

[2]- خالد ممدوح إبراهيم، مرجع سابق، ص228

[3]- عثماني عزالدين، مرجع سابق، ص62.

[4]- خالد ممدوح إبراهيم، مرجع سابق، ص323.

-البيانات المستخدمة بواسطة برنامج الكمبيوتر أو كيانه المنطقي.

-السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات.

- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

2.1-محل التفتيش في البيئة الرقمية: يرد التفتيش في نظم المعالجة الألية للمعلومات على المكونات المادية(HARD WARE) ، والمكونات المنطقية(SOFT WARE) ، وعلى شبكات اتصالات بعدي (NETWORKS TELECOMM-UNICATION)، على شبكات اتصالات بعدية[1].

1.2.1-تفتيش المكونات المادية لحاسوب: لا تثار أي مشكلة في تفتيش مكونات المادية للحاسوب، كونها ترد على أشياء مادية الإجراءات الجزائية ورد بالمعنى أن تفتيش ورد على الأشياء، وهو تصرف على الأرجح على المكونات المادية، وهو ما أكدته المادة 64 من نفس قانون سواء كان الحاسوب وملحقاته المادية موجود في أماكن خاصة أو عامة ، المنزل أو محمول باليد أو مقهى الانترنت، إلا أن المشرع الجزائري استثني في تعديل قانون رقم 22/06 في المواد 3/45 و 2/47 و 3/64 من قانون الإجراءات الجزائية تطبيق هذه الضمانات فيما يخص الجرائم المعلوماتية؛ أي أن هذه الضمانات لا تراعي في جرائم المعلوماتية، ويرجع السبب في ذلك إلى سهولة التلاعب بالأدلة في الجرائم لمعلوماتية، و سهولة التخلص من الأدلة و إتلافها و محوها بسرعة كبيرة[2]

2.2.1-تفتيش المكونات المعنوية للحاسوب: فقد أجاز المشرع الجزائري صراحة تفتيش النظم المعلوماتية بموجب نص المادة 05 من القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها؛ حيث جاء فيه" يجوز السلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات

[1]- ابراهيم الدسوقي، **الأمن المعلوماتي**، دار الجامعة الجديدة، الاسكندرية، 2009، ص371.

[2]- نعيم سعيداني، مرجع سابق، ص145.

الجزائية وفي الحالات المنصوص عليها في المادة 4أعلاه الدخول، بغرض التفتيش، ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات لمعلوماتية المخزنة فيها.

3.2.1-تفتيش الشبكات المعلوماتية المتصلة بالحاسوب: الشبكة المعلوماتية هي اتصال جهاز حاسوب أو أكثر ببعضها سلكي أو لاسلكيا. فإذا كانوا في نفس الموقع سمي" شبكة محلية"، أي إذا تفرقت سمي" شبكة بعيدة المدى"، ومع ظهور الانترنت، أعطت الاتصال بعدا دوليا، هذا تثار إشكالية في إجراء التفتيش خاصة ما يتعلق بالاختصاص؛ فهنا نجد أن المشرع الجزائري أجاز صراحة تفتيش نظم المعلومات المتصلة بالحاسوب محل التفتيش، وتسجيل كل البيانات، اللازمة كأدلة إثبات ضد المتهم وفقا المادة 05 من قانون 09-04.

3.1-المعاينة: المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يرى المحقق أن لها صلة بالجريمة، والأصل أن إجراء المعاينة متروك لتقدير المحقق، لا يقوم بها إلا إذا كان هناك فائدة من ورائها، كما أن هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية ملتبس بها، يجب على القائمين بالمعاينة تأمين الأجهزة والمعدات التي يتم الاستعانة بها خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة واخطاره مسبقا حتى يستعد من ناحية الفنية والعملية ويعد خطة مناسبة للمعاينة مع مراعاة ما جاء في القوانين الجنائية حول المعاينة تحقيقا لمبدأ الشرعية[1].

4.1-الخبرة: تعتبر الخبرة من أهم الإجراءات التي تتخذ للتثبيت عن الأدلة التي تساعد عن الكشف عن الجريمة الإلكترونية، كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها[2].

---

[1]- عبد الفتاح بومي حجازي، **مكافحة جرائم الكمبيوتر والانترنت**، دار الفكر الجامعي، مصر، الطبعة الأولى، بدون سنة، ص237.

[2]- ضريفي نادية، **سلطات القاضي الجنائي في تقدير الدليل الإلكتروني**، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص 124.

الفرع الثاني: الوسائل المستحدثة

لقد أوضحت توصيات المؤتمر الدولي الثاني للاتجاهات الحديثة في الإثبات والتحقيق الجنائي المنعقد في أمستردام في عام 1999 والذي شارك فيه(170) من العلماء كرجال القانون والخبراء وأكدت هذه التوصيات على ضرورة مواكبة مشكلات الإجرام وخصوصا الجرائم الإلكترونية، وتأهيل رجال الأمن والأجهزة الشرطية وتخطيط عمل دؤوب لوضع برنامج تدريبي ووضع أساليب حديثة لتعليمهم[1].

أوضحت الدراسات معوقات استخدام وسائل التحقيق في الجرائم الإلكترونية، وأفادت هذه أن نسبة المعوقات تتراوح بنسب متفاوتة ما بين 3.5%إلى 93% و تقوم هذه الى عدم معرفة المحققين بمكونات عناصر الجريمة المعلوماتية، وعدم التدريب على استخدام التقنية المساعدة في كشف المجرمين، وعدم قناعة العاملين في مجال المعلومات في تدخل المحققين من رجال القانون بدعوى عدم المعرفة التخصصية الفنية، وعدم استخدام أدوات وبرامج التحقيق وقلة التنسيق بين الأجهزة الأمنية والمؤسسات المستخدمة لنظم المعلومات، وعدم توافر المتخصصين والخبراء في بالبحث والتحري عن الجرائم الإلكترونية[2].

أولا–تسجيل واعتراض المراسلات: الجريمة المعلوماتية أو الإلكترونية هي من بين الجرائم التي يمكن اللجوء فيها لأسلوب التسرب واعتراض المراسلات إذا دعت ضرورة التحقيق لذلك[3].

1–التسرب: تعتبر الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات من بين الجرائم التي تناولتها وعّدتها المادة 65 مكرر 5 من قانون الإجراءات الجزائية والتي يجوز فيها اللجوء إلى أسلوب التسرب.

[1]– العنزي سليمان مهجع، **وسائل التحقيق في جرائم نظم المعلومات**، رسالة ماجستير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية.2003، ص6.

[2]– العنزي سليمان مهجع، المرجع السابق، ص243–244.

[3]–بن بادة عبد الحليم، مرجع سابق، ص85.

والتسرب هو تلك العملية التي يقوم بموجبها ضابط الشرطة القضائية بالتوغل داخل المجموعات الإجرامية وإيهامهم بأنه شريك معهم أو خاف وذلك من اجل الإيقاع بهم.

ومن المعلوم فإن التسرب يخضع لعدة شروط شكلية وموضوعية في حالة مخالفتها يحكم على العملية بالبطلان، وقد تناولت تلك الإجراءات بالتفصيل المواد من 65 مكرر 11 إلى 65 مكرر 15 لهذا لا يمكن التفصيل فيها نظرا لأنه ليس محلها هنا.

ويمكن افتراض عملية التسرب في مجال الجريمة المعلوماتية من خلال قيام ضابط أو عون الشرطة القضائية بالتوغل والدخول إلى العالم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات الكترونية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر ذلك الفاعل معيهم والمشارك، مستخدما الأسماء والصفات المستعارة والوهمية من اجل الإيقاع بيهم[1].

2-اعتراض المراسلات: جاء في المادة 03 من القانون 09-04 انه مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات كالاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

وان كانت المراسلات تتمتع بالخصوصية التي حماها المشرع بسن قوانين تعمل على توفير قد كبير من الحماية الجزائية لها، إلا أن هذا الأمر لم يكن على الاطلاق، بل قام المشرع بالسماح باعتراض المراسلات وكشف السرية عنها وذلك إذا اقتضت ضروريات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويعتبر هذا هو السند الشرعي المبرر لإباحة هذا الإجراء بسبب انو يشّكل اعتداء صارخ على

[1]-بن بادة عبد الحليم، المرجع السابق، ص85.

حرمة الحياة الخاصة وسرية المراسلات فيباح استثناء وفي حدود ضيقة وذلك للفائدة المنتظرة منه والتي تتعلق بإظهار الحقيقة وكشف الغموض عن الجريمة وضبط الجناة[1].

وتبرز عمليات اعتراض المراسلات أكثر في مجال المراسلات الإلكترونية أو البريد الإلكتروني بخدمة قائمة التراسل (mailingList)، وهو نظام تراسل جماعي يمنح صلاحية بث رسالة إلى مجموعة من الأشخاص المسجلين في القائمة ويحتوي البريد الإلكتروني برامج متخصصة لكتابة الرسائل الإلكترونية وارسالها استعراضها وتخزينها[2].

وتخضع عملية اعتراض المراسلات إلى مجموعة من الشروط والضوابط[3] مثل:

-ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ.

- تحديد طبيعة المراسلة ومدة الاعتراض.

ثانيا-المراقبة الالكترونية: هذا الإجراء تم استحداثه بموجب المادة 03 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتهما، أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم، اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها.

المشرع الجزائري لم يعترض التعريف المقصود بالمراقبة الالكترونية مثله مثل باقي التشريعات، الا أن الفقه قد تصدى لذلك وعرفه بأنه إجراء مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم بموجبه المراقب باستخدام التقنية الإلكترونية لجميع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض أخر[4].

---

[1]-محمد أو العلاء عقيدة، **مراقبة المحادثات التلفونية**، دراسة مقارنة، دار النهضة العربية، 2008، ص192.

[2]-بن بادة عبد الحليم، مرجع سابق، ص86

[3]-المرجع نفسه.

[4]-بن بادة عبد الحليم، المرجع السابق، ص86.

إجراء مراقبة الاتصالات الإلكترونية؛ هو إجراء يدخل كذلك في إطار التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية[1].

فإلى جانب إمكانية القيام بإجراء مراقبة الاتصالات الإلكترونية في إطار التحريات والتحقيقات القضائية من اجل الوصول إلى أدلة لم يكن بالمقدور الوصول إليها لولا استعمال هذه الوسيلة، بالإضافة إلى انه يمكن استغلال هذه التقنية للعمل في بيئة الرقابة من اجل الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة[2].

هو ما قررته المادة الرابعة من القانون 04/09 من خلال نصها على انو يمكن القيام بعمليات المراقبة الإلكترونية للاتصالات للوقاية من الافعال الموصوفة بجرائم الارهاب والتخريب والجرائم الماسة بأمن الدولة، وكذا توفر معلومات حول إمكانية الاعتداء على منظومة معلوماتية على نحو يهدد لنظام العام والدفاع الوطني.

يجب الاعتراف للمشرع الجزائري انه قد قام بخطوة جريئة من خلال نصه على إجراء الرقابة الالكترونية للاتصالات، على اعتبار أنه من أخطر الإجراءات في النظام الإجرائي عبر العالم الافتراضي كونه يمس بخصوصية الانسان وحرمة حياته[3].

المطلب الثاني: آليات التحقيق عن الجرائم المعلوماتية في الاتفاقات الدولية

استنادا لكثرة استعمال الشبكة العنكبوتية، وسرعة وصولها واتصالها من دولة إلى أخرى ظهرت لنا هذه التقنيات بعدة مشاكل ومن أهمها الاختراقات التي تتم بواسطة الحاسوب الآلي ويمكن لهذه الجرائم أن تتعدى حدود الدولة الوطنية لتشمل الحدود الدولية، ومن هنا جاء الاهتمام الدولي بشأن هذه الجرائم؛ كون المجتمع أصبح يعاني من هذه الجرائم.

أصبح الأمر في غاية الأهمية لعقد اتفاقيات دولية بين الدول للتعاون بهذا الشأن للحد من هذه الجرائم ومكافحتها ومن هذه الاتفاقيات الذي سوف نجمل الحديث عنها. من وسائل الحد

[1]–المرجع نفسه.

[2]–سعيداني نعيم، مرجع سابق، ص184.

[3]–سعيداني نعيم، المرجع السابق، ص184.

من الجرائم الإلكترونية إبرام اتفاقيات دولية في مجال حماية شبكات الأنترنت خاصة، بعدما سهلت شبكات الأنترانت والحصول على المعلومات خلال ثوان وضرورة التنويه إلى عقد اتفاقات دولية واطلاع الجهات التي تضررت جراء المخاطر الواقعة على المعلومات[1].

التعاون الدولي مهم عند التعامل مع الجرائم الإلكترونية، لما سيلحقه تطور في أساليب متشابهة لتحقيق قانون جنائي واجرائي لحماية شبكات المعلومات الدولية؛ لأن هذه الجرائم هي عابرة للقارات ولا حدود لها، وعدم التعاون فيما بين الدول سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما يعطي المجرمين إمكانية الافلات من العقوبة ومضاعفة أنشطتهم الإجرامية[2].

ولأهمية التعاون بين الدول، يعتبر التفتيش العابر للحدود والذي يجب أن يتم وفقا لاتفاقيات دولية مبرمة ما بين الدول من أجل السماح بالتفتيش ولا يجوز القيام بالتفتيش العابر للحدود في غياب تلك الاتفاقيات أو على الأقل يجب أن نحصل على إذن من الدول الأخرى للقيام بالإجراءات القانونية وفقا للمعايير الوطنية[3].

وقد نظمت اتفاقية بودابيست مجموعة من الإجراءات الخاصة بالبحث والتحري أيضا جاءت مضامين الاتفاقية العربية مطابقة لأحكام اتفاقية بودابيست خاصة على القواعد الجرائية من خلال نص المواد (16) إلى (21) ويمكن إجمالها فيما يلي[4]:

-سرعة التحفظ على بيانات الكمبيوتر المخزنة

-اجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة

-تفتيش وحجز بيانات الكمبيوتر المخزنة

---

[1]- بن يونس عمر محمد أبو بكر، **الجرائم الناشئة عن استخدام الأنترنت**، جامعة المنصورة كلية الحقوق، مصر، 2004، ص.809

[2]- الشنيفي عبد الرحمن عبد العزيز، **امن المعلومات وجرائم الحاسب الآلي**، الطبعة الاولى، الرياض، السعودية، 1414 هجري، ص 113.

[3]- توبة عبد الحكيم رشيد، **جرائم تكنولوجيا المعلومات**، دار المستقبل للنشر والتوزيع، عمان، 2008، ص235.

[4]- قجاج يوسف، **الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية**، مجلة الفقه والقانون، عدد 196/28- 182، 2015، ص 186.

-التجميع الفوري لبيانات الكمبيوتر وامكانية اعتراض هذه البيانات.

التعاون القضائي هو تعاون السلطات القضائية الدولية لمكافحة الجريمة الإلكترونية، ويهدف التعاون إلى تقريب من الإجراءات الجنائية الدولية من حيث إجراءات البحث كالتحري عن وقوع جريمة إلكترونية ويتم التنسيق ما بين السلطات القضائية الدولية للاتفاق على معايير موحدة[1] وفقا للاتي:

-التمسك بمبدأ التجريم المزدوج كشرط لتسليم المجرمين.

-استخدام التكنولوجيا الحديثة مثل الدوائر التلفزيونية وأن يتاح للقاضي الانتقال من دولة إلى أخرى لسبيل التحقيق في الجريمة ولاكتشاف محتوياتها.

-أن يراعى تنفيذ الأحكام الأجنبية وفقا لضوابط تتفق عليها الدول فيما بينها.

-ويراعى تطبيق برامج آمنه لحماية الشهود، لأن هذه الجرائم تحتوي على مجموعات كبيرة ومخطط لها مسبقا بحيث من يقوم بارتكاب هذه الجريمة شخص له علاقات كبيرة داخل وخارج الدولة.

ولأهمية التعاون ما بين الدول قامت جامعة الدول العربية بعقد اجتماع لصياغة ميثاق لقانون مكافحة جرائم تقنية المعلومات بمقر الأمانة العامة بالقاهرة الموافق 2010/2/21، وتحدثت عن التعاون الدولي والقضائي في الفصل الرابع منه، وفي المادة (30) تحدثت عن الاختصاص للدول بأن كل دولة تلتزم بتبني الإجراءات في حال تحققت الجريمة في إقليم الطرف وعلى متن سفينة تحمل علم الدولة الطرف، وتطرقت إلى موضوع تسليم المجرمين.

تهدف الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وذلك من أجل الحفاظ على أمن الدول العربية ومصالحها وسلامة الأفراد فيها، وتقتضي هذه الاتفاقية بتطبيق بنودها بهدف منع الجرائم الإلكترونية والتحقيق فيها، مثل

[1]- قشقوش هدى حامد، **الجريمة المنظمة**، دار النهضة العربية، القاهرة، 2000، ص85.

الاعتداء على سلامة البيانات، ونشر افكار جماعات إرهابية والدعوة لها، وجرائم إساءة استخدام تقنية المعلومات، والتزوير الاحتيال[1]..

بينما ظهرت اتفاقية بودابست تهدف إلى توحيد السياسة التشريعية من أجل مكافحة الجرائم الإلكترونية المرتكبة في الفضاء الافتراضي والى تنسيق التعاون بين التشريعات الوطنية لتسهيل مكافحة الإجرام المعلوماتي، وتطبيق إجراءات تتلاءم لتحقيق وملاحقة الفضاء الافتراضي ووضع نظام تعاون دولي يتميز بالسرعة والفعالية في التنفيذ[2].

وحتى يمكن تطبيق قواعد تعاون الدولي بإجراءات سليمة وصحيحة ويمكن تطبيقها كتالي[3]:

*التمسك بمبدأ التجريم المزدوج كشرط لتسليم المجرمين وينص عليه المشرع صراحة في قانون دول الأطراف الذي وقع الفعل عليها، ولكن يمكن التخلي عن تسليم الجاني في حال كان هناك إجراءات تمس بحقوق الإنسان والحريات العامة، كما نصت الاتفاقية على عدم استبعاد الاختصاص الجنائي الذم ينص عليه أحد الاطراف وفقا لقانونه الوطني ومطالبة الدول الأطراف في الاتفاقية بالتشاور حول الاختصاص القضائي الاكثر ملاءمة لمحاكمة مرتكبي الجرائم الإلكترونية في حالة تعدد المطالبة من طرف الاطراف باختصاصه القضائي حول واقعة معينة.

*أن يتوفر بين الدول نظام للمساعدة القضائية في المواد الجنائية مثلا اقتضت العدالة في التحقيق أن ينتقل القاضي الى الدولة الذي أرتكب فيها الفعل ان يكون متوفر في الدولة المساعدة للقاضي بحرية الانتقال والتحقيق أو اعطاء إنابة قضائية الى قاضي لمتابعة سير التحقيقات ويجب أن تنفذ وفقا للمعايير الدولية وبجميع الاحوال أن يكون هناك توافقا في الإجراءات في كل من الدولتين كما تسمى توأمة التشريع.

---

[1]–المالكي محمد بن احمد خضران، **رؤية استراتيجية لربط المعلومات الأمنية بين دول مجلس التعاون لمكافحة الجرائم الإلكترونية**، رسالة ماجستير منشورة. جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2015، ص 92–93.

[2]–قجاج يوسف، مرجع سابق، ص186.

[3]–قشقوش هدى حامد، مرجع سابق، ص85–86.

ويلاحظ غالبا أن ما يتم استبعاد الإنابة في الشق السياسي والعسكري والضريبي، لأنها من شأنها المساس بالسيادة والنظام العام والمصالح الأساسية للدول، حيث يبقى النظام معيبا لارتباطه بالطرق الدبلوماسية والتي تتسم بالبطء وكثرة البروتوكولات وما يتعارض من الإجراءات السريعة لهذه الجرائم من شأن الإجراءات المعقدة أن تؤدي إلى ضياع الأدلة والبيانات واختفائها[1].

*استخدام التكنولوجيا الحديثة مثل الدوائر التلفزيونية أن يكون للقاضي حرية الانتقال من دولة إلى أخرى للتحقيق في القضية المعروضة عليه وهذا ليس مقتصرا التحقيق على مرحلة التحقيق الابتدائي ولكن في مرحلة الحكم أيضا.

*كما يجب تطبيق برامج آمنه لحماية الشهود على المستوى الدولي.

*مراعاة في تطبيق الأحكام الأجنبية وفقا لضوابط تتفق عليها الدول فيما بينها، والاتفاق على كيفية مصادرة الأموال محل الجريمة عبر الحدود أو إرسال المسجونين. تبادل المعلومات: وهي تشمل تقديم كل البيانات والوثائق التي تطلبها سلطة قضائية اجنبية بصدد متابعة جريمة ما والرد على الاتهامات التي وجهت الى رعاياه في الخارج وتبيان الإجراءات التي اتخذت بحقهم[2].

*نقل الإجراءات: يقصد بها قيام دولة بناء على اتفاقية باتخاذ اجراءات جنائية بصدد جريمة ارتكبت في اقليم دولة اخرى ولمصلحة هذه الدولة وهذا إذا ما توافر عدة شروط وهي[3]:

-ان يكون الفعل المنسوب الى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب منها.

-ان يكون الاجراء المطلوب اتخاذه مقرر في قانون الدولة المطلوب اليها عن الجريمة ذاتها.

---

[1]-لموسخ محمد، **تنازع الاختصاص في الجرائم الالكترونية**، دفاتر السياسة والقانون، عدد2/143-157، لا يوجد سنة نشر، ص155.

[2]-المرجع نفسه.

[3]-المرجع نفسه

–ان يكون الاجراء المطلوب اتخاذها يؤدي الى كشف الحقيقة كأن تكون الادلة موجودة بالدولة المطلوب اليها.

لتزايد الجرائم الإلكترونية وما تثيره هذه الجرائم من إشكاليات عملت منظمة الأمم المتحدة بدورها إلى عقد اتفاقيات خاصة بمكافحة استعمال التكنولوجيا لسنة 2000، بمعنى أنها أكدت على الحاجة إلى تعزيز التعاون والتنسيق بين الدول في مكافحة استعمال تكنولوجيا المعلومات، بالإضافة إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المنعقدة في فينا في أكتوبر 2000، حيث بين المؤتمر فهرس الأمثلة المتعلقة بتسليم المجرمين وتحقيق سبل التعاون وتبادل المساعدة القانونية[1].

[1]– مزغيش سمية، **جرائم المساس بالأنظمة المعلوماتية**، بحث منشور. جامعة محمد خيضر، بسكرة، الجزائر، 2014، ص54–55.

الخاتمة

العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية، حيث أصبحت حياتنا اليومية تستدعي اللجوء إليها، فقد مكنت طرق المعالجة الآلية المجتمعات من تجاوز فكرة الحدود الإقليمية، نظرا لكون التكنولوجيا عابرة للحدود. لكن في مقابل هذا التطور ظهر ما يسمى بالجريمة المعلوماتية، وذلك نتيجة للاستخدام السيئ للمعلوماتية أو الحاسب، فنتج عن هذا الأخير عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن المعطيات من جهة وتمس بحرية الأفراد والمؤسسات من جهة أخرى.

كما تميزت الجريمة المعلوماتية بطبيعة خاصة فنتج عن ذلك صعوبة في وضع تعريف عام، جامع وموحد لها، فقد اختلفت المفاهيم حولها باختلاف الزاوية التي يُنظر إليها بها. فالبعض يُعرفها باعتبار انها وسيلة لارتكاب الجريمة، والأخر باعتبار محل أو موضوع الجريمة، والبعض الآخر يقوم بتعريفها استنادا لشخصية الجاني، وهناك من جمع بين التعريفات جميعا. في حين أنه قد ينصرف مفهوم الجرائم المعلوماتية إلى الأفعال التي تشكل الاعتداء على نظم المعالجة الآلية للمعطيات، والتي تستهدف بشكل خاص المعلومات المختلفة في البيئة الرقمية، بالإضافة إلى كل جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية، وهذه الأخيرة في الغالب ما تكون جرائم تقليدية.

إن الطبيعة الخاصة لها، والمتمثلة في أنها جريمة لا تعترف بالحدود نظرا لارتكابها بواسطة الحاسب أو في مجال النظم المنطقية للحاسب الآلي، وتميزها بالسرعة في التنفيذ والتطور المتسارع في ارتكابها أعطاها خصوصية. بالتالي فإن مرتكبها يتميز بخصائص هو الأخر، إذ أن المجرم المعلوماتي وأشكاله، لا يلجؤون إلى العنف كما هو الحال بالنسبة للمجرم التقليدي، بل يتميز بالذكاء والمهارة والسلطة والمعرفة. لذا فإن أصل الجرائم المعلوماتية هي جرائم تقليدية في ظاهرها، لكن باطنها قد لا يوحي بذلك. وعندما ترتكب فإن الضرر الناجم عنها يكون غير تقليدي أيضا، وقد يكون الضرر الناجم عن جريمة المعلوماتية كبيرا جدا، مع عدم القدرة على وقفها أحيانا، ويمتد إلى عدد كبير من الضحايا، وذلك بناء على أهداف الجريمة نفسها، وقد يكون الضرر ماديا أو معنويا، وقد يشملهما معا.

ان طبيعة الجريمة المعلوماتية تتطلب إجراءات خاصة، وهو ما دعت اليه أغلب التشريعات لإعادة تقييم القواعد الإجرائية المتاحة في استخلاص الدليل كالتفتيش والضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية وهو ما كان فعال بموجب القانون 04/06 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فضلا عن استحداث نوع من القواعد الإجرائية الأخرى و التي تتلاءم مع الطبيعة الرقمية التي يكون الدليل المناسب في إثبات هذا النوع من الجرائم كاعتراض المراسلات و المراقبة الإلكترونية. كما تسعى الاتفاقات الدولية لإنشاء اليات تحقيق مشتركة وذلك لمواجهة مشكل نطاق الجريمة والقانون الواجب التنفيذ، والذي قد يعتبر بالأمر الصعب فما يعتبر ممنوعا في أحد الدول قد يكون مباحا في أخرى، مما يطرح اشكالا في تجريم الفعل من عدمه حتى قبل مباشرة التحقيق فيه.

كما لاحظنا من خلال بحثنا ان هناك خلط، حيث ان المشرع قد نسب التحقيق الابتدائي في الجريمة المعلوماتية لضباط الشرطة القضائية وفقا للمادة 63 من قانون الإجراءات الجزائية، وفي نفس الوقت تنص المادة 66 الواردة في الباب الرابع المتعلقة بأحكام قاضي التحقيق على أن التحقيق الابتدائي في الجنايات وجوبي، بذلك فانه يعتبر التحقيق الممارس من رجال الضبطية او قضاة التحقيق تحقيقًا ابتدائيًا. كما ان استخلاص الدليل في البيئة الرقمية قد يؤدي الى المساس بخصوصية الحياة الخاصة، وإمكانية اطلاع المحققين على اسرار خاصة بأشخاص قد لا يكون لهم يد في الجريمة، فحرص المشرع كل الحرص على ان يشترط اللجوء الى هذه الإجراءات إذا دعت الى ذلك ضرورة التحري والتحقيق والتي يجب ان تقدر بقدرها. لكن متى يمكن القول انها ضرورة في غياب متطلبات السرعة، وزيادة قوة حجم البيانات وعرض النطاق الترددي للشبكات مع الجهل بعدد الضحايا والاضرار؟

النتائج:

-صعوبة التعريف بالجريمة المعلوماتية.

-الجريمة المعلوماتية نوعان الأول يعتمد على المعلوماتية لارتكابها والثاني تسهل المعلوماتية ارتكابها.

-أعداد متزايدة من الأفراد المتصلين بالإنترنت وعيهم بالأمن الرقمي متدنٍ.

-انتقال المدن والمساكن الى الانترنت أوجد أشكال ضعف جديدة.

-الإحجام عن التبليغ عن الجرائم المعلوماتية.

-الافتقار الى تجريم الجرائم المعلوماتية والتعقيدات لدى تداخل الولايات القضائية.

-الجريمة المعلوماتية ستشكل تحديا لسلطة الدولة، خاصة في مراقبتها والتحكم فيها سواء من حيث اعتراض البيانات او من حيث التدفقات المالية.

-صعوبة اكتشاف الجريمة المعلوماتية، ومعرفة مرتكبها أو نطاق ارتكابها، وتقييم الضرر الناجم عنها، كونه ضررا يمس الكيان المنطقي ذو القيمة المنطقية أو القيم المادية او كلاهما على حد السواء.

-السهولة والقابلية لارتكابها، أو الوقوع ضحية لها. ذلك بسبب صعوبة الرقابة الأمنية، وعدم إدراك ضحاياها لمدى خطورتها.

-سهولة إخفاء واتلاف معالم الجريمة واثارها والدلائل التي توحي بارتكابها.

-لا تتطلب جهدا بدنيا، أو عنفا جسديا، او تواجدًا جسمانيا في محل الجريمة مثل الجريمة التقليدية.

-لا تتقيد بمكان أو زمان أو شكل محدد.

-تعتمد على الذكاء والدراية بأنظمة الكمبيوتر في ارتكابها، أو يمكن ارتكابها بالاعتماد على المصادر التي توفر التقنيات اللازمة لارتكابها كخدمة.

-صعوبة التحقيق والتعامل مع هذه الجرائم بالنسبة للمحقق التقليدي خاصة من حيث متابعتها والكشف عنها وإقامة الدليل عنها، فهي جرائم تقنية.

-اختلاف التحقيق فيها عن التحقيق في الجرائم التقليدية.

-التحقيق فيها يتطلب محقق يمتلك الخبرة، ويمكن الاستعانة بمزودي الخدمة في حالة عدم تمكن السلطات القضائية المختصة في إزاحة الغموض عنها.

-اجراء التفتيش في الجريمة المعلوماتية لا يتحدد بزمن معين مثل المسكن.

-الجرائم المعلوماتية هي جريمة ماسة للمعطيات، يمكن استغلال الإجراءات المستحدثة في حال التحقيق في جريمة مرتكبة او محتملة الحدوث

التوصيات:

-تفعيل أحدث التقنيات والوسائل للكشف عن الجريمة ومرتكبيها.

-الاعتماد على مبدأ العالمية بالنظر لطبيعة الجرائم المعلوماتية العابرة للحدود.

-تكوينات متخصصة لمجابهة الظاهرة.

-سن قوانين جديدة تتلاءم وطبيعة الجريمة.

-الفصل بين الإجراءات المتخذة في الجرائم التقليدية مع نظيرتها المعلوماتية.

-اعتماد مقياس جديد في الجامعات يقوم بدراسة المعلوماتية.

-الاستعانة بالمجتمع المدني للتوعية بمخاطر الشبكة المعلوماتية والجريمة المعلوماتية وتأثيرها على القصر والأحداث.

-إعادة النظر في تسيير مقاهي الانترنت، وعدم اعتبارها نشاط تجاري كغيره، وفرض التزامات على مقدمي الخدمة كتوفير كاميرات مراقبة تظهر التاريخ، الوقت، وزاوية تلتقط كل ما يتواجد داخل المقهى خاصة ملامح كل شخص مستغل للخدمة الموَّفرة.

-الاستفادة من التجارب الدولية في المجال لكسب المهارات وصقلها.

-العمل على توحيد القوانين والإجراءات الدولية.

-تقنين التجارة الالكترونية لتسهيل ضبطها.

-الأخذ بعين الاعتبار أن العالم الالكتروني هو عالم موازي للعالم الحقيقي بالمعنى الحرفي.

قائمة

المصادر

والمراجع

المصادر :

- **الجمهورية الجزائرية الديمقراطية الشعبية: الجريدة الرسمية، العدد47، المتضمن قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها, 2009/08/16.**
- **قانون 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الامر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج. ر، العدد 71، الصادر 10 نوفمبر 2004.**
- **المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.**
- **المادة 335 من قانون العقوبات الجزائري.**
- **المادة 44 من قانون الإجراءات الجزائية الجزائري.**
- **المادة 47 من قانون الإجراءات الجزائية الجزائري.**
- **المادة 51 من قانون الإجراءات الجزائية.**
- **-قرار وزير الداخلية المصري رقم13507 لسنة 2002 الصادر بتاريخ: 2002/07/07**

المراجع

الكتب:

-رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم لمعلوماتية، ط1، مكتبة الآلات الحديثة، أسيوط، 1994.

-الشوا محمد سامي. ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994.

- الصغير جميل عبد الباقي، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2002.

-الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، ط1، دار النهضة العربية، القاهرة، 1992.

-القاضي رامي متولي، مكافحة الجريمة المعلوماتية، ط1، دار النهضة العربية، القاهرة, 2011.

-الملط، أحمد خليفة، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، مصر،2006.

-المومني نهلا عبد القادر. الجريمة المعلوماتية، ط2، دار لثقافة للنشر والتوزيع، عمان، 2010

-جميل عبد الباقي، الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية القاهرة، 2002.

-فضل سليمان احمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الإنترنت، دار النهضة العربية، القاهرة، 2013.

-قهوجي علي عبد القادر، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الاسكندرية، 1999.

-ابراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، الاسكندرية، 2009.

-احمد هلالي عبد الله، الجوانب الموضوعية والاجرائية لجرائم المعلوماتية، (ط2)، دار النهضة العربية، القاهرة.

-الخن محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية،2010.

-الرومي محمد أمين، جرائم الكمبيوتر والانترنت، ط1، دار النهضة العربية، القاهرة، 2003.

-الشوا، سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط1، دار النهضة العربية، القاهرة، 1994.

-القحطاني ذيب بن عايض، امن المعلومات، مكتبة مدينة الملك فهد للعلوم والتقنية، الرياض, 2015

-المناعسة أسامة احمد. الزغبي جلال محمد. جرائم تقنية المعلومات الالكترونية، دراسة مقارنة، ط1، دار الثقافة، عمان, 2014.

-الهيتي محمد حماد، التكنولوجيا الحديثة والقانون الجنائي، ط1، دار الثقافة للنشر والتوزيع، عمان, 2004

- بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة العاشرة، دار هومة، الجزائر، 2009.

-توبة عبد الحكيم رشيد، جرائم تكنولوجيا المعلومات، دار المستقبل للنشر والتوزيع، عمان، 2008.

- الشنيفي عبد الرحمن عبد العزيز، امن المعلومات وجرائم الحاسب الآلي، الطبعة الاولى، الرياض، السعودية، 1414 هجري

-حجازي، مكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، الطبعة الأولى، بدون سنة.

-حزيط محمد، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2010.

-خالد عباد الحلي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، 2011.

-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2010.

-عبابنة محمود احمد، جرائم الحاسب وابعادها الدولية، ط2، دار الثقافة للنشر والتوزيع، عمان, 2017،

-عبابنة محمود احمد، جرائم الحاسوب وأبعادها الدولية، دار العلم والثقافة للنشر والتوزيع، عمان, 2006.

-عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، ط1.

-عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004.

-قشقوش هدى حامد، الجريمة المنظمة، دار النهضة العربية، القاهرة، 2000.

-قورة نائلة عادل محمد. جرائم الحاسب الاقتصادية دراسة نظرية وتطبيقية، ط1، دار النهضة العربية، القاهرة, 2006.

-محمد أو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنة، دار النهضة العربية، 2008.

-محمود عبد الله حسين، سرقة المعلومات المخزنة في الحاسب الالي، (ط2)، دار النهضة العربية، القاهرة، 2002.

-نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.

-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، الطبعة 2، دار الفكر الجامعي، مصر، 2011، ص 76.

-هلالي عبد الله أحمد، تفتيش نظم الحاسوب الالي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.

بن قارة عائشة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الاسكندرية، 2010.

البحوث الجامعية:

-العنزي سليمان مهجع، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية.2003.

-بن يونس عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الأنترنت، جامعة المنصورة كلية الحقوق، مصر، 2004.

-أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم09-04، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة ورقلة، السنة الجامعية 2012-2013.

-المالكي محمد بن احمد خضران، رؤية استراتيجية لربط المعلومات الأمنية بين دول مجلس التعاون لمكافحة الجرائم الإلكترونية، رسالة ماجستير منشورة. جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2015.

-بن عقون حمزة، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير في القانون، كلية حقوق، جامعة الحاج لخضر باتنة، الجزائر، 2012.

-بوبقرة خيرة، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة نهاية الدراسة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2020/2019.

-بوعمرة محمد، بنينال سيد علي، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أكلي أولحاج البويرة، السنة الجامعية:2020/2019 .

-حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر، 2008.

-سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، السنة الجامعية : 2013/2012.

-سوير سفيان. جرائم المعلوماتية، مذكرة ماجيستر في علم الاجرام والعقاب، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر, 2010.

-صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجيستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة تيزي وزو، تاريخ المناقشة:06-03-2013.

-محمد نصير السرحاني، مهارات التحقيق الفني في الحاسوب والأنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

-مزغيش سمية، جرائم المساس بالأنظمة المعلوماتية، بحث منشور. جامعة محمد خيضر، بسكرة، الجزائر، 2014.

المقالات العلمية:

-بن بادة عبد الحليم، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، المجلد الثاني، العدد 23، 2015.

-بن شهرة شول، ماشوش مراد، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية والسياسية، معهد الحقوق والعلوم السياسية-المركز الجامعي افلو، المجلد04، العدد01, 2020.

-شوقي يعيش تمام، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، سلسلة مطبوعات المخبر 06، جامعة بسكرة، (ط1)، مطبعة الرمال(الوادي)، الجزائر، 2019.

-ضريفي نادية، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019.

-عثماني عزالدين، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية-مخبر المؤسسات

الدستورية والنظم السياسية، المركز الجامعي مرسلي عبد الله–تيبازة، المجلد الثاني، العدد04، 2018.

–علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الاثبات الجنائي، مقال متوفر على الموقع التالي: http//www.arablawinfo.com

–قجاج يوسف، الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون، عدد 28/196–182، 2015.

–لموسخ محمد، تنازع الاختصاص في الجرائم الالكترونية، دفاتر السياسة والقانون، عدد2/143–157، لا يوجد سنة نشر.

المؤتمرات والندوات العلمية:

– رستم هشام محمد فريد، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت.

–Ulrich Sieber، جرائم الكمبيوتر والجرائم الأخرى في مجال المعلومات، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي (ترجمة سامي شوا)، دار النهضة العربية، القاهرة، 1993.

–البشري محمد الأمين، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة الفترة من01 إلى03 ماي 2000.

–القبائلي سعد حماد، ضوابط الحماية الإجرائية لبرامج الحاسب الالي، بحث مقدم لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، اريد, 2004.

-القبائلي سعد حماد، ضوابط الحماية الإجرائية لبرامج الحاسب الالي، بحث مقدم لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، اربد, 2004.

-القطاونة مصعب، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن، 2010.

-المطردي مفتاح بوبكر، الجريمة الالكترونية، ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية،

-حسين سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الأنترنت، ورقة مقدمة للاتحاد العربي للتحكيم الإلكتروني،2007.

-زهير كاظم عبود، بحث مقدم للأكاديمية العربية المفتوحة في الدنمارك، كلية القانون والسياسة قسم القانون للدراسات العليا 2007

-عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003 .

-عوض محمد محي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993 .

-فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009.

المواقع الالكترونية:

www.news.bbc.co.uk/hi/arabic/news/newsied1153000/1153/24,stm.

الكتب الأجنبية:

-A.J.WRIGHT. THE ELITE CYBER CRIMINALS STORIES. The Secret world of cyber criminals and strategies for addressing Cyber Crime.2020.

-David Fayon. L'informatique, Vuibert, 1999.

-Duleroy ،Les escrocs a l'informatique ،le nouvel économiste، octobre 2002.

-ENDRELIN، Clément. Les moyens juridiques de lutte contre la cybercriminalité، Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen, 2011

-JEAN-LUC PUTZ، CYBERCRIMINALITE، criminalité informatique en droit luxembourgeois, 2019.

-Myriam QUEMENER ،Cybercriminalité -droit pénal appliqué ،econonica, Septembre 2010.

الفهرس

الفهرس

الملخص

الملخص

إن العالم أكثر ترابطا على الصعيد الرقمي اليوم منه في أيّ وقت مضى. ويستغل المجرمون هذا التحول الإلكتروني لاستهداف نقاط الضعف في المنظومات والشبكات والبنى التحتية عبر الإنترنت. ويخلّف هذا الوضع تبعات اقتصادية واجتماعية هائلة على الحكومات والشركات والأفراد في العالم أجمع. وما التصيد الاحتيالي وبرمجيات انتزاع الفدية وانتهاكات البيانات سوى أمثلة قليلة على التهديدات الجريمة المعلوماتية الراهنة، بينما تظهر على الدوام أشكال جديدة من الجريمة السيبرية. ومرتكبو الجرائم الالكترونية هم أكثر فأكثر مرونة وتنظيما، ويستغلون التكنولوجيا الجديدة ويكيفون اعتداءاتهم ويتعاونون فيما بينهم بطرق مبتكرة. يطلق عليهم البعض اسم القراصنة، وآخرون أصحاب الياقات وتسميات أخرى عديدة. لكن يتفق على إطلاق تسمية المجرم المعلوماتي كمصطلح عام لمرتكب هذه الجريمة.

الكلمات المفتاحية: الجريمة المعلوماتية–الجريمة السيبرانية–الجريمة الاكترونية.

تقنيات المعلومات–الحاسب الآلي–المجرم المعلوماتي

Abstract

The world is more interdependent on the digital front today than ever before. Criminals exploit this electronic transition to target weaknesses in online systems, networks and infrastructure. This situation has enormous economic and social consequences for Governments, corporations and individuals worldwide. Phishing, ransomware and data violations are only a few examples of current information crime threats, while new forms of cybercrime are constantly emerging. Perpetrators of cybercrime are more and more flexible and organized, exploiting new technology, adapting their attacks and cooperating with each other in innovative ways. Some are called pirates; others are collars and many other labels. But he agrees to call the information criminal a general term for the perpetrator of this crime.

Keywords :

cybercrime -cybercrime. Information Technologies-Computer-Information Criminal