وزارة التعليم العالي والبحث العلمي

جامعة محمد البشير الابراهيمي برج بوعريريج

كلية الحقوق والعلوم السياسية

قسم الحقوق

أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث ل.م.د

تخصص: القانون الخاص

بعنــوان:

خصوصية التحقيق في مواجهة الجرائم المعلوماتية

من إعداد الطالبة:

أومدور رجاء

تحت إشراف الأستاذ الدكتور:

فرشة كمال

أعضاء لجنة المناقشة:

الاسم واللقب	الصفة	الرتبة	الجامعة
د/ هدفي العيد	رئيسا	أستاذ محاضر –أ–	جامعة برج بوعريريج
د / فرشة كمال	مشرفا ومقررا	أستاذ محاضر –أ–	جامعة برج بوعريريج
د/ دوار جميلة	ممتحنا	أستاذة محاضرة –أ–	جامعة برج بوعريريج
د/ رفاف لخضر	ممتحنا	أستاذ محاضر –أ–	جامعة برج بوعريريج
د/ مقدم الياسين	ممتحنا	أستاذ محاضر –أ–	جامعة المسيلة
د/ ماني عبد الحق	ممتحنا	أستاذ محاضر –أ–	جامعة برج بوعريريج
د/ خضري محمد	مدعوا	أستاذ محاضر –أ–	جامعة برج بوعريريج

السنة الجامعية:

2021-2020

إهداء :

الحمد لله الذي أنعم علينا بنور العلم وأعاننا على اتمام هذا العمل المتواضع.

أهدي ثمرة جهدي

الى مصدر قوتي وتشجيعي الوالدين الكريمين

الى مصدر الحب خالتي العزيزة

الى سندي المتين اختي وأخي

الى كل من سر مسمعي بكلمة طيبة

الى كل من يسعى الى العلم والمعرفة

الى كل مجتهد يطمح الى النجاح

رجاء أومدور

شكر وتقدير:

الحمد لله، نحمده ونستعين به ونستهديه،

الصلاة والسلام على سيدنا محمد أشرف المرسلين.

أتقدم بأسمى آيات الشكر مع التقدير والمحبة

الى الدكتور فرشة كمال الذي تفضل بالإشراف على هذه الأطروحة بنصائحه وتوجيهاته القيمة.

الى أعضاء اللجنة الموقرة على قبولهم مناقشة الأطروحة

الى كل من لم يبخل علي وأفادني بمعلومات سديدة

كما أتقدم بفائق الاحترام والتقدير الى كل الأساتذة وكل الأسرة الجامعية في كلية الحقوق والعلوم السياسية بجامعة برج بوعريريج.

رجاء أومدور

قائمة المختصرات:

المختصرات باللغة العربية

ج ر	الجريدة الرسمية
ق ع	قانون العقوبات
ق إ ج	قانون الاجراءات الجزائية
ص	صفحة
ط	طبعة

المختصرات باللغة الأجنبية

CPP	Code de procédure pénal
P	Page
Op. cit	ouvrage précédemment cité
Ibid	le même ouvrage
INCC	Institut National de criminalistique et de Criminologie
CPLCIC	Centre de Prévention et de lutte contre la criminalité informatique et la cybercriminalité
SCIC	Service Centrale d'investigation Criminelle
Adresse IP	Internet Protocol Adresse
MAC	Media Access Control
TCP/IP	Transmission control Protocol/ Internet Protocol
IDS	Système de détection d'intrusion
IPS	Système de prévention d'intrusion

مقـــــــــــــــدمة

مقدمة

ساهمت التكنولوجيا الحديثة في بروز عصر جديد أحدث تحولا جذريا في كافة ميادين الحياة، وسهل الانفتاح على العالم بلا حدود، بأن اختزل المسافات ومكن من التواصل بين الأشخاص والمؤسسات ربحا للوقت وتسريعا لتبادل وتداول المعلومات على نطاق واسع دون جهد التنقل، فأصبح العالم كقرية صغيرة يسهل فيها التعامل والتواصل باستمرار.

ومع تسارع الاستخدام الايجابي للتقنيات الرقمية الحديثة في أغراض ساهمت في تقديم خدمات للأفراد والمجتمعات، الا أن الواقع أظهر امكانية اساءة استخدام هذا التطور في أنشطة غير مشروعة، مما يؤدي الى الاضرار المباشر أو غير المباشر بالمصالح المادية والمعنوية للأفراد والتأثير السلبي على متطلبات حياتهم المعتادة، ناهيك عن امكانية تشكيل خطر على سيادة الدول وكيانات المؤسسات الوطنية والدولية.

نتيجة توسع العصر الرقمي الى مختلف المجالات، لم تبق الجرائم منحصرة في نمطها التقليدي القائم في وسط مادي ملموس، بل أصبحت تستعمل تقنيات جديدة في وسط افتراضي غير ملموس، وظهر بذلك ما يعرف بالجرائم المعلوماتية كإفراز سلبي للتطور الرقمي الذي شهده العالم، لتشكل بذلك انتهاكات خطيرة تطال الحياة الخاصة للأفراد، وتمس حرياتهم وآرائهم الخاصة، الى جانب التأثير في السيادة الوطنية والاستقرار الوطني.

ولعل أي تشريع في العالم يحاول ضمان مواكبة التطورات السريعة التي تتماشى مع التكنولوجيا الحديثة مع عدم اهمال موضوع حماية حقوق الانسان وحق التمتع بالحرية والخصوصية في مباشرة الأعمال دون رقابة أو تجسس على الحياة الشخصية، وكذا المحافظة على أمن واستقرار الدول.

بســـبب الطبيعة الخاصـــة لهذا النمط الاجرامي المســـتجد، كان لزاما على الأنظمة الجزائية أن تتدخل للوقاية الســـابقة واللاحقة عن حدوث هذه الجرائم والبحث عن ســـبل للحد من تطورها مستقبلا، من خلال التوجه نحو استخدام الوسائل والأساليب المتطورة في مجال التحقيق بتلك الجرائم وضـبط مرتكبيها وتتبعها وكشـفها وجمع الأدلة القائمة حولها، وكل ذلك بغرض ضـــمان فاعلية التحقيق ونجاعة الأســـاليب المتبعة بشـــأنه، ليقع على عاتق الهيئات المختصـــة مهمة الاســـتعداد لمواجهة تلك التطورات وتلافي أخطارها على الصـــعيد الأمني والقضائي.

غير أن واقع الحال يظهر عدة صـــعوبات تعيق التحقيق بهذه الجرائم مما يحول دون ضـــمان غاياته، وكل ذلك ناتج عن التعقيد ودقة الوقائع المعلوماتية التي مســـحت ما يعرف بالحدود الوطنية وتجاوزت جغرافية الدول، لتتخذ عبور الحدود الوطنية، وتمتد اضـــرارها عبر أكثر من اقليم، وهو الواقع الذي فرض البحث في إطـار تشـــريعي يمكن معه مواجهـة هذا الوضـــع ومجابهة مخلفاته بتكريس آليات للتعاون الدولي على الصـــعيد الأمني والقضـــائي والفني، تحت مظلة تشريعية دولية متجانسة تعزز سبل التعاون الدولي.

أهمية الموضوع:

تتجلى أهميـة موضـــوعنـا من النـاحيـة العلميـة بدايـة في حداثتـه، فهو مرتبط بجرائم معاصـرة في مجال البحث الأكاديمي والتكريس القانوني، ومازالت النصـوص القانونية بشـقيها الموضوعي والاجرائي تثير العديد من التساؤلات التي تتطلب المناقشة والبحث العلمي.

علاوة على ذلك فهذا الموضـــوع لا يقتصـــر على المقاربة القانونية، بل يشـــمل كذلك المقاربة التقنية، التي تدعم فاعلية النصـوص القانونية، حيث يسـتمد الموضـوع أهميته العلمية من كونـه مرتبط بـأهم اجراء يتخـذ في الـدعوى الجزائيـة، وهو اجراء التحقيق في الجرائم المعلوماتية، الذي يســتلزم البحث في خصــوصــياته المتعلقة بالجرائم المعلوماتية كأســاس

موضـــوع التحقيق المســـتحدث، ومختلف عناصـــر التحقيق فيها، والآليات القانونية والفنية والأمنية اللازمة لمواجهة هذه الجرائم في مجال التحقيق الجنائي.

أما من الناحية العملية فان الموضـــوع يحتل درجة بالغة من الأهمية من خلال عمل أجهزة التحقيق بشكل متكامل ومتناسق لضبط الدليل وتأمينه من التلف أو الضياع واستعمال أســـاليب وأدوات معينة للوصـــول الى مرتكبي الجرائم المعلوماتية وعدم افلاتهم من العقاب ناهيك عن منع تفاقم الاجرام المنظم العابر للحدود.

أسباب اختيار الموضوع:

وقع اختيارنا لهذا الموضوع لعدة أسباب ذاتية تتمثل في:

– الرغبة الشخصية الملحة في دراسة جوانب الموضوع وتبيان أهم الخصوصيات التي يمتاز بها اجراء التحقيق في الجرائم المعلوماتية، خاصة وأن هذا الموضوع يدخل في صميم القانون الجنائي في شقه الاجرائي.

– ضرورة وجود دراسة لتوضيح خصوصيات التحقيق في مواجهة الجرائم المعلوماتية باعتبار هذه الأخيرة جرائم مستحدثة تستدعي دراستها، والتطرق للموضوع بصيغة متخصصة.

– نشر الوعي وإثراء المكتبة ببحث جديد متخصص، قد يساعد باحثين آخرين في المستقبل.

أما الدوافع والأسباب الموضوعية فلم تكن وليدة الصدفة بل لحداثة الموضوع، كونه يصـــب حول ما أحدثته التكنولوجيا الحديثة من تطور وتغير في المنظومة القانونية. وتعميق المعرفة في مجال التحقيق في الجرائم المعلوماتية، من خلال ابراز أهم خصوصياته لمواجهة هذا النوع من الاجرام، من حيث التطرق لأهم عناصـــر وأســـاليب التحقيق في الجرائم المعلوماتية ودور الأجهزة المختصـــة في حســـن ســـيره وأهم الآليات الاجرائية وآليات التعاون الدولي في مجال التحقيق في هذه الجرائم.

أهداف الموضوع:

يهدف الموضوع الى عدة نقاط تتمثل أساسا في:

- تسليط الضوء على خصوصية التحقيق في مواجهة الجرائم المعلوماتية.
- اثراء الرصيد العلمي والمعرفي ببحث جديد في مجال الجرائم المعلوماتية.
- معرفة مدى تطابق القواعد الاجرائية التقليدية مع التحقيق في هذه الجرائم المعلوماتية.
- ابراز أهم التحديات التي تواجه التحقيق في الجرائم المعلوماتية.
- ابراز كيفية التعامل مع الدليل الالكتروني للارتقاء بإجراءات التحقيق.
- تزويد الأشـــخاص المنوط لهم عملية التحقيق بالتقنيات الحديثة للكشـــف عن المجرم المعلوماتي.

الدراسات السابقة:

تعتبر الدراسات السابقة لهذا الموضوع قليلة مقارنة بباقي المواضيع، وذلك راجع لكون الموضوع معاصر وهذه الجرائم من الجرائم المستحدثة التي مازالت تثير العديد من التساؤلات ومواجهتها تفتقر لأساس ثابت وموحد يضمن فاعلية تطويق نطاقها، وحتى تناول الموضوع مازال يصـــب في الجوانب الموضـــوعية، أكثر من الجوانب الاجرائية، وهو ما يحول دون نجاعة التصـدي لها، بخلاف ايجاد بعض أطروحات دكتوراه حسـب توجه كل باحث بتطرقه لما يراه مناسبا في الموضوع.

أطروحة دكتوراه للباحث: احســـان طبال، النظام القانوني للتحقيق الدولي في جرائم الكمبيوتر، جامعة الجزائر 1، ســنة 2014، و كانت الاشـكالية حول متطلبات حماية الحق في محاكمة عادلة للمتهم، و مدى امكانية اضـــفاء قواعد التحقيق المعهودة على جرائم

الكمبيوتر، و امكانية التأسيس لنظام قانوني مستحدث على التحقيق المتعلق بارتكاب انتهاكات و جرائم عبر نشاطات الاعلام الآلي، و يرى الباحث ان التحديات تبقى مستعصية على الحل في غياب خطة واضحة للتعامل مع هذه الطائفة من الجرائم و مرتكبيها لاسيما في الدول التي لم تبادر لتعديل تشريعاتها بما يكفل تجاوز العقبات.

أطروحة دكتوراه للباحث ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، جامعة باتنة، سنة 2016، كانت الاشكالية حول مدى فاعلية الآليات القانونية المستحدثة في مجال دعم أعمال البحث والتحقيق للكشف عن الجرائم المعلوماتية، ويرى الباحث ان التشريع الجزائري يتميز بالجمود والقدم مقارنة لما آلت اليه الجرائم المعلوماتية.

أطروحة دكتوراه للباحث براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، جامعة تيزي وزو، سنة 2018، كانت الاشكالية حول امكانية الاعتماد على اجراءات التحقيق التقليدية لإثبات هذه الجرائم، وإذا كانت هذه الاجراءات كافية لاحتواء متغيرات هذا النمط المستجد من الجرائم، خلص في نهاية الدراسة الى وجود مشاكل وعقبات، وقدم مجموعة حلول مستوحاة من تجارب بعض الدول واتفاقية بودابست على وجه الخصوص.

ويكمن الاختلاف بين ما جاء به كل باحث وموضوع دراستنا من خلال اعتمادنا أساسا على أهم خصوصيات التحقيق في الجرائم المعلوماتية، والتطرق الى المستجدات على الصعيد القانوني باعتبار أن هذه الجرائم معاصرة تتطلب مواجهتها مواكبة التطورات التكنولوجية باستمرار وتحديث الترسانة القانونية.

صعوبات البحث:

لعل أهم الصـــعوبات التي واجهتنا أثناء اعداد هذه الأطروحة هو تشـــعب الموضـــوع وتداخله مع مصطلحات وجوانب تقنية مما دفعنا الى الاستعانة بعدة تخصصات لفهم بعض المصـــطلحات والجوانب التقنية، اضـــافة الى بذل جهد كبير في دراســـة الجوانب الفنية دعما للجوانب القانونية.

كما أن من أهم الصعوبات التي واجهتنا هو ضآلة المراجع الجزائرية المتخصصة في المجال المعلوماتي، ولعل ذلك يرجع الى حداثة الموضـــوع وبداية المشـــرع الجزائري في مواكبة التطورات التكنولوجية، بدليل أن معظم القوانين المنظمة لبعض الجوانب المعلوماتية صـــدرت مؤخرا.

الاشكالية المطروحة

أدخل المشـــرع الجزائري مجموعة من التعديلات على كل من قانون العقوبات وقانون الاجراءات الجزائية، كما اســـتحدث القانون 09-04 المتعلق بالقواعد الخاصـــة للوقاية من الجرائم المتصـــلة بتكنولوجيات الاعلام والاتصـــال ومكافحتها، اضـــافة الى القانون 18-04 المتعلق بالقواعد العامة للبريد والاتصـــالات الالكترونية، والقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وصدرت مجموعة من المراسيم الرئاسية سنة 2020، منها المرسوم الرئاسي الذي أعاد ســـير وتنظيم الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصـــال، والمرسوم الرئاسي المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

وانطلاقا مما سبق، نطرح الاشكالية الرئيسية للموضوع على النحو الآتي:

هل كرس المشرع الجزائري أحكام قانونية تتلاءم مع خصوصية التحقيق لضمان فاعليته في مواجهة الجرائم المعلوماتية والحد من آثارها؟

التساؤلات الفرعية:

انطلاقا من الاشكالية الرئيسية، يمكن طرح مجموعة تساؤلات فرعية تتمثل أهمها فيما يلي:

- بما تتميز الجرائم المعلوماتية؟

- كيف يمكن اجراء التحقيق دون أن يتعارض مع الحق في الخصوصية؟

- ماهي أهم الصعوبات التي يمكن أن تصادف اجراءات التحقيق واثبات هذا النوع من الجرائم؟

- هل تكفي آليات التعاون الدولي في الحد من عبور الجرائم المعلوماتية للحدود الوطنية؟

المنهج المعتمد:

نظرا لطبيعة الموضوع وخصوصيته، تم الاعتماد على المنهج الوصفي التحليلي بطريقة متكاملة ومتناسقة من أجل الالمام والتوسع في الموضوع، وتأصيل عناصره مع تحليل النصوص القانونية المرتبطة بذلك، وفي هذا الإطار قضت الضرورة الاستعانة بالدراسات المقارنة في بعض المواضع لتوضيح نقاط الاختلاف والتشابه بين التشريع الجزائري وبعض التشريعات الأخرى.

الخطة المعتمدة:

للإجابة على اشكالية الموضوع ارتأينا اعتماد خطة ثنائية متوازنة تنقسم الى بابين، على أن يتضمن كل باب فصلين.

وعلى هذا الأســـــاس، تنـاولنـا في البـاب الأول: مكـانـة التحقيق في مواجهـة الجرائم المعلوماتية، تعرضـنا من خلاله الى مبادئ التحقيق في الجرائم المعلوماتية (الفصـل الأول)، ودور أجهزة التحقيق في مواجهة الجرائم المعلوماتية (الفصل الثاني).

أما الباب الثاني خصصناه لتوضيح آليات التحقيق في مواجهة الجرائم المعلوماتية حيث وضّحنا اجراءات التحقيق في الجرائم المعلوماتية (الفصل الأول)، والتعاون الدولي في مواجهة الجرائم المعلوماتية (الفصل الثاني).

الباب الأول:

مكانة التحقيق في مواجهة الجرائم المعلوماتية

الباب الأول: مكانة التحقيق في مواجهة الجرائم المعلوماتية

ان الثورة المعلوماتية اليوم هي بمثابة ثورة صناعية ثانية في حياة البشرية، أساسها الفكر البشري، تعتمد على الابتكار والتطوير، وتحويل الأفكار الى منجزات[1]، مما يساهم في ازدهار وتقدم الدول.

رغم الأثر الايجابي للثورة المعلوماتية الا أنها قد تستغل في زيادة نسبة الجرائم المعلوماتية، هذه الأخيرة التي تنعكس خصوصيتها على اجراءات التحقيق الجنائي، فمن ناحية تعتبر عنصر لا غنى عنه لمباشرة الاجراءات الجزائية، ومن ناحية قد يستصعب الوصول اليها لطبيعتها غير الملموسة، ولطبيعة الدليل المستمد منها.

علاوة على ذلك يتميز مرتكبي هذه الجرائم عما عهدناه في مرتكبي الجرائم التقليدية؛ بالذكاء والقدرة التقنية في اخفاء معالم الجريمة، وهو ما يؤدي الى صعوبة وصول الجهات المكلفة بالتحقيق الى الدليل الذي يفيد في كشف الجريمة، كما قد يساهم الضحية نفسه في اعاقة سير اجراءات التحقيق.

ناهيك عن امكانية تعارض اجراءات التحقيق مع مبادئ مهمة كمبدأ قرينة البراءة والحق في الخصوصية، واشكالية الاثبات الجزائي في الجرائم المعلوماتية.

ولعل اجراءات التحقيق في الجرائم المعلوماتية تحكمها قواعد قانونية وفنية مميزة، فهي تتطلب عناصر أساسية بدونها لا جدوى من فتح تحقيق من أساسه، وتصادفها عدة تحديات لابد من ابراز أثرها على اجراءات التحقيق، وهو ما جعلنا نتعرض في الفصل الأول: مبادئ التحقيق في الجرائم المعلوماتية.

[1]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم المعلوماتية، ط 1، دار الفكر الجامعي، الاسكندرية، 2009، ص 12.

نظرا لطبيعة البيئة المعلوماتية أصبح تطوير أساليب التحقيق ضرورة ملحة لمواجهة مختلف الجرائم المعلوماتية، فنتيجة لوجود مجرم معلوماتي فلابد أن يقابله محقق له خبرة ودراية كافية بالمجال المعلوماتي وهذا ما يعكس المرونة التي يتسم بها اجراء التحقيق حيث لابد أن يضفي المحقق من خبرته وفطنته ومهاراته لمواجهة الجرائم المعلوماتية، خاصة وأن هذه الأخيرة بيئتها مختلفة عن البيئة التقليدية التي تعتمد على كل ما هو مادي ملموس.

وهو ما جعلنا نتساءل عن دور التحقيق في مواجهة الجرائم المعلوماتية؟

واجابة ذلك تطرقنا في الفصل الثاني لدور أجهزة التحقيق في مواجهة الجرائم المعلوماتية.

الفصل الأول:

مبادئ التحقيق في الجرائم المعلوماتية

الفصل الأول: مبادئ التحقيق في الجرائم المعلوماتية

ان التحقيق هو مجموعة القواعد القانونية والفنية التي تباشـــرها الســـلطة المختصـــة لتمحيص الأدلة والكشف عن الحقيقة.

تتأتى الحقيقة في الجرائم المعلوماتية بوجودها كأسـاس موضـوع التحقيق المسـتحدث، وينبغي التطبيق السـليم للقانون من خلال التقدير السـليم للدليل المسـتمد من الجريمة واحترام قواعد الاختصـــاص وعدم تجاوز حدود الحيز المكاني والزماني خاصـــة عند عبور الجريمة حدود الدولة الواحدة، واحترام مختلف عناصـــر التحقيق، وهو ما تناولناه في المبحث الأول تحت عنوان العناصر المتطلبة للتحقيق في الجرائم المعلوماتية.

ان حرية الفرد هي توازن عادل بين ما تفرضـــه الســـلطة العامة من التزامات عادلة، وبين ما يخضـع له الفرد من قيود تحد من حريته[1] ويعتبر مبدأ الشـرعية الاجرائية والحق في الخصـوصـية تحديا أمام سلطات التحقيق في الجرائم المعلوماتية، كما أن قواعد اثبات الجرائم المعلوماتية تعتبر مميزة، وهو ما جعلنا نخصـــص المبحث الثاني ل: تحديات التحقيق في الجرائم المعلوماتية.

[1]– بوكحيل لخضر، الاجراءات الجنائية، مطبعة الشهاب، باتنة، دس، ص 03.

المبحث الأول: العناصر المتطلبة للتحقيق في الجرائم المعلوماتية

ان أهم عنصـــر لصـــحة اجراء التحقيق في الجرائم المعلوماتية هو وجود جريمة من الجرائم المعلوماتية والتي لا تقوم الا بقيام جميع اركانها مجتمعة، ورغم ذلك قد تســتصـــعب اجراءات التحقيق في هذه الجرائم لأسباب معينة.

كما يتطلب لصـــحة اجراء التحقيق فيها توفر مجموعة من الشــروط، مع احترام حيز الجريمة من خلال تحديد القانون واجب التطبيق والاختصـــاص القضـــائي في الجرائم المعلوماتية.

وبناء على ذلك خصصنا هذا المبحث لتوضيح العناصر المتطلبة للتحقيق في الجرائم المعلوماتية بإبراز أهم عنصـــر وهو وجود الجريمة في حد ذاتها من خلال المطلب الأول، وبقية العناصر من خلال المطلب الثاني.

المطلب الأول: العناصر الرئيسية للتحقيق في الجرائم المعلوماتية

تناولنا هذا المطلب من خلال فرعين:

الفرع الأول بعنوان وجود جريمة من الجرائم المعلوماتية، حاولنا فيه تســليط الضـــوء على عدة نقاط وهي مفهوم الجرائم المعلوماتية، أركانها، خصوصيتها.

أما الفرع الثاني بعنوان الصـــعوبات التي تواجه اجراءات التحقيق، والتي تناولناها من خلال عدة نقاط وهي ابراز انعكاس خصوصية الجريمة على اجراءات التحقيق، دور الضحية في اعاقة سير التحقيق، وسائل التقليل من الصعوبات المتعلقة بالجرائم المعلوماتية.

الفرع الأول: وجود جريمة من الجرائم المعلوماتية لمباشرة إجراءات التحقيق

ان أهم عنصر للتحقيق في الجرائم المعلوماتية هو الوجود الفعلي للجريمة، التي تمتاز من حيث تعريفها وخصوصياتها، كما يستلزم استظهار أركانها كعنصر جوهري لصحة اجراء التحقيق.

أولا: مفهوم الجرائم المعلوماتية

تطورت المفاهيم عبر مراحل ويمكن ايجازها في عدة نقاط:

1-انحصار استعمال الحاسب الآلي في نطاق محدد:

كانت أجهزة الحاسب الآلي تستخدم في مجالات ضيقة تشمل المؤسسات العسكرية والمؤسسات الكبرى التابعة للدولة، ثم بدأ في المرحلة الموالية: الاستخدام التجاري لهذه الأجهزة، ليتضح مع نهاية الخمسينات مفهوم اساءة استخدام الكمبيوتر المؤسس على أبعاد أخلاقية، وظل مفهوم الجرائم المعلوماتية منحصر في إطار السلوكيات غير الاخلاقية مع استبعاد النطاق القانوني.[1]

2-بداية استخدام المصطلحات الدالة على الجرائم المعلوماتية:

بدأ الحديث على الجرائم المعلوماتية كظاهرة اجرامية مستحدثة شاع فيها مصطلح "الهاكرز" الذي يقوم باقتحام النظم ونشر الفيروسات والبرامج المدمرة للملفات، واختراق أمن المعلومات، لإظهار تفوقه التقني، حيث كان معظم الهاكرز من فئة صغار السن العباقرة في هذا المجال، لكن مع تزايد خطورة ذلك كان لابد من اعادة تصنيف المجرمين وتحديد

[1]- نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، منشورات دار الخلدونية، الجزائر، 2017، ص 15.

طوائفهم خاصـــة مع تحول الجريمة من مجرد مغامرة وابداء تفوق الى أفعال أكثر خطورة من تجسس واستيلاء على بيانات خاصة. [1]

3-اتساع نطاق الجرائم المعلوماتية في المراحل الموالية:

في مطلع التســعينات بدأت مفاهيم الجريمة المعلوماتية تتطور، وبرزت أنماط جديدة تستهدف مواقع الانترنت التسويقية، و نشطت جرائم نشر الفيروسات والرسائل عبر البريد الالكتروني، وتجدر الاشارة الى أنه لم يكن هناك اهتمام بمسائل الأمن بقدر الاهتمام بالشبكة وتوسيع نطاقها، حيث تركز الاهتمام على الربط و الدخول مما شجع ذلك في تنامي الجرائم المعلوماتية، غير أنه نتيجة تحول الانترنت الى بيئة متكاملة للاســتثمار والعمل والانتاج والاعلام والحصول على المعلومات زادت الحاجة الى توفير معايير الأمن في شبكة الانترنت وبدأ التفكير مليا في الثغرات ونقاط الضعف.[2]

4-المفاهيم الدالة على الجرائم المعلوماتية

-مفاهيم فقهية: تباينت المفاهيم الفقهية حســب منظور كل باحث، فمنهم من عرفها بأنها: " أفعال اجرامية يســتخدم في ارتكابها الحاســب كأداة رئيســية" أو هي" مجموعة افعال غير مشــروعة مرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب." أو هي " أية جريمة يكون متطلبا لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب"[3]

---

[1]- فضيلة عاقلي، الجريمة الالكترونية واجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال المؤتمر الدولي الرابع عشر الجرائم الالكترونية، طرابلس 24-25 مارس 2017، ص 123.

[2]- خالد مختار الفار، إسماعيل بابكر محمد، التحقيق الجنائي في جرائم الحاسوب، ط 1، دار عزة للنشر والتوزيع، السودان، 2010، ص 153 ص 154.

[3]- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، المكتب الجامعي الحديث، الاسكندرية، 2018، ص 21.

وما يلاحظ من هذه التعاريف أنها ترتكز على معيار واحد سـواء بالنظر الى وسـيلة ارتكاب الجريمة، أو الى محل ارتكابها، أو بالنظر الى المعرفة بتقنيات الحسـاب الآلي، ومن هنا تبنى بعض الفقهاء تعريفات أخرى تعتمد على عدة معايير في نفس الوقت، ومنها:

الجرائم المعلوماتية هي اي اجراء غير قانوني يكون الحاسـب الآلي هو اداة أو هدف الجريمة، واي جريمة تهدف وسيلتها او غرضها الى التأثير على وظيفة الحاسب الآلي، حيث يلحق ضرر بالضحية، سواء حقق المجرم ربحا أو كان بإمكانه تحقيقه، ووفقا لخبراء قانونيين يغطي مفهوم الجرائم المعلوماتية الحوسبة كهدف اساسي للجريمة، وتقنية المعلومات كوسيلة لارتكاب الجريمة.[1]

وعرفت منظمة التعاون الاقتصـادي والتنمية OCDE الجرائم المعلوماتية على أنها: " كل سـلوك غير مشـروع أو غير أخلاقي أو غير مصـرح به يتعلق بالمعالجة الالكترونية للبيانات أو نقلها"[2]

كما عرفتها منظمة الأمم المتحدة في مؤتمرها العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد بفيينا سنة 2000 بأنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"[3]

ونعرف بدورنا الجرائم المعلوماتية بأنها: الاستخدام غير المشروع أو غير المصرح به للبيانات والمعلومات، أو نقلها أو تخزينها أو استعمالها عبر الوسائط الالكترونية، بما يشكل اعتداء على الأشخاص والأموال والجوانب الأمنية للدولة واستقرارها.

[1] -Daniel M، Frédéric-Paul M، Cybercrime: menaces، vulnérabilités et ripostes, 2e Edition، presses Universitaires de France, 2001, Paris, France, p 13-14.

[2]– فهد عبد الله العبيد العازمي، الاجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2016، ص 42.

[3]–محمد أمين الشوابكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، ط 4، دار الثقافة، عمان، 2011، ص 10.

– **مفاهيم قانونية:** عرفت بعض التشـــريعات مصـــطلح الجرائم المعلوماتية ومنها: القانون الأمريكي الذي عرفها بموجب القانون رقم 1213 لســـنة 1982 الخاص بمواجهة جرائم الكمبيوتر على أنها: الاســـتخدام غير المصـــرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات، أو الاســتخدام المتعمد الضــار بأجهزة الكمبيوتر أو ملفات البيانات وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية الى جناية من الدرجة الثالثة.[1]

أما عن موقف المشرع الجزائري من مفهوم الجرائم المعلوماتية

لم يشــر المشــرع الجزائري الى المصــطلح بوصــف "جرائم معلوماتية" غير أنه عالج بعض أنماط هذه الجرائم وأطلق عليها تســـمية " الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات" وذلك سنة 2004 أين أضاف قسما جديدا تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، ضمن قانون العقوبات، ليقوم بتعديلات فيما بعد سنة 2006 على كل من قانون العقوبات والاجراءات الجزائية، وسدا منه للفراغات القانونية وضع مجموعة ترتيبات في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصـــال ومكافحتها[2]، وأطلق على الجرائم المعلوماتية: مصـــطلح "الجرائم المتصـــلة بتكنولوجيات الاعلام و الاتصـــال" حيث عرفها بموجب المادة الثانية منه على أنها " جرائم المســـاس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسـهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصـالات الالكترونية" ثم وضـــح في الفقرة الموالية من نفس المادة المقصـــود بمنظومة معلوماتية و المعطيات المعلوماتية و الاتصالات الالكترونية....

[1]– فهد عبد الله العبيد العازمي، مرجع سابق، ص42.

[2]– قانون رقم 09-04، المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 47، الصادرة بتاريخ 16 أوت 2009، ص 5.

وما يلاحظ في هذا الصدد أنه وسع من نطاق هذه الجرائم عندما أضاف عبارة " أي جريمة أخرى" و سبب ذلك هو امكانية ظهور جرائم معلوماتية جديدة تكون محلا للمعالجة الآلية، لكن رغم ابراز أهم المصطلحات التي جاء بها هذا القانون غير أن مفهوم المعالجة الآلية بقي مبهما الى حين صدور القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[1] حيث عرفت المادة الثالثة من هذا القانون المعالجة الآلية بأنها: " العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات و تطبيق تغييرها أو مسحها أو استخراجها أو نشرها".

5-أنواع الجرائم المعلوماتية

ان الجرائم المعلوماتية تتعلق بأي نوع من الجرائم التي ترتكب على أو عن طريق نظام الكمبيوتر والمتصل بشكل عام بشبكة الانترنت، وبالتالي يمكن تصنيف السلوك الاجرامي الى ثلاث فئات[2]:

- فئة المجرمين الذين يستخدمون التقنيات الرقمية باعتبارها الهدف الأساسي للجريمة (يغطي هذا الاعتداء على انظمة البيانات الآلية والتشفير).
- فئة المجرمين الذين يستخدمون التقنيات الرقمية (كوسيلة لإعداد أو مساعدة أو صور الجريمة التقليدية كالاحتيال، التزوير، تبييض الأموال).
- فئة المجرمين الذين يستخدمون التقنيات الرقمية كوسيلة للجرائم التي تنطوي على محتوى غير قانوني (كالمواد الاباحية للأطفال، العنصرية).

[1]- قانون رقم 18-07، مؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، عدد 34، الصادرة في 10 يونيو 2018، ص 11.

[2] - Quéméner M, Ferry J, Cybercriminalité Défi mondial, 2e édition, economica, 2009, paris France, p 02.

وقد صـــنفت الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية (بودابســـت نوفمبر 2001)[1] الجرائم المعلوماتية الى عدة أنواع وهي:

- الجرائم الماسـة بخصـوصـية وسـلامة وتوافر بيانات ونظم الكمبيوتر: وتشـمل جرائم النفاذ غير المشـروع، جرائم الاعتراض والالتقاط غير المشـروع، التدخل في البيانات، التدخل في الشبكات والأنظمة المعلوماتية، اساءة استخدام الأجهزة.
- الجرائم ذات الصلة بالكمبيوتر: وتشمل التزوير بواسطة الحاسوب، الاحتيال بواسطة الحاسوب.
- الجرائم ذات الصلة بالمحتوى: وتشمل الدعارة المتعلقة بالأطفال
- الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة.

وقسمها بعض الباحثين الى عدة أنواع:

النوع الأول: الجرائم الواقعة على الحاســوب وتشــمل جرائم الملكية الفكرية، جرائم الســرقة، التزوير المعلوماتي، الاحتيال المعلوماتي، جرائم التخريب، جرائم التعرض للحياة الخاصة.

النوع الثاني: الجرائم الواقعة بواسطة الحاسوب كالاستغلال غير المشروع لبطاقات الائتمان[2].

النوع الثالث: الجرائم الواقعة باستخدام الانترنت وتقسم الى:

- **الجرائم الواقعة على الأشـــخاص:** كجرائم القدح والذم والتحقير عبر الانترنت، وجرائم الابتزاز الالكتروني، الاستغلال الجنسي للأطفال عبر الانترنت.

[1]- الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية-رقم 185، بودابست، 2001.

[2]- علي جبار الحسيناوي، جرائم الحاسوب والانترنت، اليازوري، الاردن، 2008، ص 70.

-**الجرائم الواقعة على الأموال:** كجرائم تدمير المواقع، نشـــر الفيروســـات، الاختراق، القمار على الانترنت، تزوير البيانات.

غير أن تصـــنيف الجرائم المعلوماتية، غير منحصـــر، حيث من الممكن أن تظهر جرائم مستقبلية تدمج كل نتاج التقدم المذهل في التكنولوجيا[1]، ويستغل المجرمون ذلك لصالحهم.[2]

ثانيا: أركان الجرائم المعلوماتية

من العناصـــر اللازمة لصـــحة اجراء التحقيق هو وجوب اســـتظهار أركان الجرائم المعلوماتية، والمتمثلة في ركنها الشرعي، ركنها المادي وركنها المعنوي.

1-الركن الشرعي:

الركن الشرعي هو نص التجريم الذي يجرم الفعل ويعاقب عليه[3]، وذلك تأسيسا على أول مبدأ في قانون العقوبات وهو مبدأ الشـــرعية الذي يقضـــي بأن "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون".

ولقد خصـــص المشـــرع الجزائري منذ تعديل 2004 وتبعته تعديلات 2006 القســـم الســـابع مكرر من قانون العقوبات تحت عنوان المســـاس بأنظمة المعالجة الآلية للمعطيات والذي يندرج ضـــمن الباب الثاني الجنايات والجنح ضـــد الأفراد، الفصـــل الثالث الجنايات والجنح ضـــد الأموال. (المواد من 394 مكرر الى 394 مكرر7 من قانون العقوبات الجزائري).

[1]- أحمد محمد عبد الباقي، الانترنت-التكنولوجيا وجرائم المستقبل، دار النهضة العربية، القاهرة، 2017، ص 20.

[2] - Bellivier F, Eudes M, Fouchard I, Droit des crimes internationaux, 1 re édition, Thémis droit, France, 2018, p215.

[3]- عبد الرحمن خلفي، محاضرات في القانون الجنائي العام (دراسة مقارنة)، دار الهدى، الجزائر، 2012، ص 48.

2-الركن المادي:

ان النشاط أو السلوك المادي في الجرائم المعلوماتية يتطلب وجود بيئة رقمية واتصال بالإنترنت، ويتطلب معرفة بداية النشـــاط والشـــروع فيه.[1] حيث يتحقق الركن المادي للجريمة بتوفر السلوك الاجرامي، النتيجة وعلاقة السببية.

أ- في جريمة الدخول أو البقاء عن طريق الغش في المنظومة المعلوماتية:

يتمثل الســـلوك الاجرامي اما في الدخول أو في البقاء: حيث يعتبر الدخول ســـلوكا ايجابيا يتمثل في الولوج الى النظام المعلوماتي الغير مفتوح للجمهور ضـــد رغبة المســـؤول عن هذا النظام المعلوماتي، و أشـارت المادة 394 مكرر من قانون العقوبات الجزائري أنه " كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك " وباستقراء نص المادة نجدها لم تشترط صفة معينة في الشخص الذي يدخل أو يبقى في النظام، ولم تشـــترط وســـيلة أو طريقة معنية، المهم هو أن يكون مخالفا لإرادة صـاحب النظام أي لا يوجد ترخيص.[2] أما البقاء فهو سـلوك سـلبي يتمثل في امتناع عن المغادرة والخروج من النظام عند انتهاء فترة التصـريح، حيث أن الدخول مشـروع والبقاء غير مشـروع. ويعتبر سـلوك الدخول والبقاء غير المصـرح بهما من جرائم السـلوك المحض أي جرائم الخطر، وهي جرائم تكتفي بالســـلوك الاجرامي، فعند تحقق بعض النتائج فان العقوبة تشدد فقط كون أن الجريمة قائمة منذ الدخول أو البقاء. وليست كل النتائج محل

[1]- خالد ممدوح ابراهيم، مرجع سابق، ص 53.

[2]- فالمشرع لم يكتف بالدخول وذلك باعتبار أن الشخص من الممكن أن يكون مرخص له بالدخول غير أنه يتجاوز الوقت المحدد له في الترخيص، كما يمكن أن يكون الدخول عن طريق الصدفة دون قصد، بمعنى لا يوجد غش أو احتيال للدخول الى النظام، فاذا لم يقم بالخروج فورا تعتبر جريمة بقاء غير مشروع لتوفر العلم والارادة.

اعتبار، بل فقط ما تنص عليه المادة 394 مكرر من نفس القانون وهي: حذف المعطيات، تغيير المعطيات، تخريب نظام اشتغال المنظومة.[1]

ب- في جريمة التلاعب بالمعطيات:

يتمثل السلوك الاجرامي في الادخال أو التعديل أو الازالة. ورغم أن معظم الجرائم الواقعة على المعطيات هي جرائم خطر لا يشترط أن يترتب على السلوك الاجرامي اعتداء فعلي على المعطيات، بل يكفي الاحتمال أو التهديد بالخطر، لكن في هذه الجريمة (جريمة التلاعب بالمعطيات) هي جرائم ضرر أي جرائم مادية وبالتالي هي ذات نتيجة، لأنه لا يكفي أن تهدد سلامة المعطيات بل يشترط تغيير حالة المعطيات.

ج-في جريمة التعامل في معطيات غير مشروعة:

السلوك الاجرامي له صورتين: اما التعامل في معطيات صالحة لارتكاب جريمة[2] أو التعامل في معطيات متحصلة من جريمة سابقة أي متحصلة من جريمة الدخول أو البقاء غير المصرح بهما أو من جريمة التلاعب بالمعطيات.[3]

---

[1]- ولتحقق الظرف المشدد يجب وجود علاقة السببية بين السلوك المتمثل في الدخول أو البقاء وبين النتيجة المشددة. وهناك نتيجة مهمة يمكن أن تعقب الدخول دون تشديد العقوبة وهي تحميل المعطيات، وما يعاب على المشرع أنه أغفل تجريم سرقة المعلومات.

[2]- في التعامل في معطيات صالحة لارتكاب جريمة: الهدف من التجريم هو الحيلولة دون وقوع الجريمة أصلا أي أن مجرد التعامل في حد ذاته جريمة ولو لم ترتكب، (حماية قبلية وقائية)، والتجريم وقائي لعدم وقوع الجريمة أصلا. ويتمثل السلوك الاجرامي في ستة أشكال للتعامل في معطيات صالحة لارتكاب جريمة وهي: التصميم، البحث، التجميع، التوفير، النشر، الاتجار (المادة 394 مكرر 02 من قانون العقوبات).

[3]- في التعامل في معطيات متحصلة من جريمة سابقة أي متحصلة من جريمة الدخول أو البقاء غير المصرح بهما أو من جريمة التلاعب بالمعطيات: الهدف من التجريم هنا هو الحد من النتائج وآثار الجريمة السابقة، ويتمثل السلوك الاجرامي في فعل الحيازة أي السيطرة الارادية على المعطيات أو فعل الافشاء الذي يقوم على اخذ معلومات سرية وافشائها للغير، فعل النشر الذي يقوم على اخذ معلومات غير مرخص الاطلاع عليها ونشرها، وفعل الاستعمال مهما كان غرضه.

ولا يعتد بالنتيجة فيكفي قيام الجاني بأحد الأفعال المنصوص عليها في المادة 394 مكرر 2، فالغاية من التجريم هنا هي وقائية لأن هذه الجرائم هي جرائم خطر يهدف المشرع من خلال تجريمها الى منع وقوع الضرر في حالة التعامل في معطيات صالحة لارتكاب الجريمة، وفي حالة حدوث هذه الأخيرة يحاول القضاء على آثار الجريمة (التجريم وقائي استباقي).

3-الركن المعنوي:

يقصد بالركن المعنوي هو توضيح الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني.[1]

أ- في جريمة الدخول أو البقاء غير المصرح بهما:

-**الجريمة في صورتها البسيطة:** هي جريمة عمدية تشترط توفر القصد العام المتمثل في العلم والارادة، أي علم الجاني بكل واقعة تدخل في تكوين الجريمة وموضوع الحق المعتدى عليه، وتتجه ارادته الى فعلها، وفي ذلك لا يبحث المشرع الجزائري عن النية الخاصة أو القصد الخاص، بل يكتفي بالقصد العام.

-**الجريمة في صورتها المشددة:** النتيجة تعتبر غير عمدية والظرف المشدد لا يغير من وصف الجريمة والذي يقوم بمجرد الركن المادي وهو حدوث النتيجة المشددة وارتباطها بفعل الدخول أو البقاء الغير مصرح بهما، برابطة السببية، وبالتالي الركن المعنوي لا يوجد هنا والمسؤولية عن النتيجة المشددة هي غير عمدية تقوم على الخطأ.[2]

[1]- خالد ممدوح ابراهيم، مرجع سابق، ص 53.

[2]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007، ص 160.

ب- **في جريمة التلاعب بالمعطيات:** تعتبر جريمة عمدية تتطلب القصـــد العام فقط فبمجرد تعديل أو اضـــافة أو حذف وهو على علم أنه ليس من حقه ذلك وتتجه ارادته الى ذلك، تقوم الجريمة بغض النظر عن النية، وهناك من التشـــريعات من تشترط نية خاصة وهي نية الاضرار بالغير أو قصد تحقيق ربح غير مشروع أو فائدة غير مشروعة، كالتشريع البرتغالي، التركي، الفنلندي.[1]

ج-**في جريمة التعامل في معطيات غير مشـــروعة:** تعتبر جريمة عمدية تتطلب توفر القصـد العام (العلم والارادة)، أما بالنسـبة للقصـد الخاص عند التعامل في معطيات متحصـلة من جريمة سـابقة فيكفي القصـد العام لأن طبيعة المعطيات واضـحة وهي غير مشروعة وبالتالي النية الخاصة غير لازم اثباتها، وبالنسبة للتعامل في معطيات صـالحة لارتكاب جريمة فالمشـرع الجزائري لم يشـر الى ذلك وبالتالي يكفي القصـد العام.

وقد تنقل المشـــرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الارادة ومبدأ العلم، فهو تارة يســـتخدم الارادة كما هو الشـــأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا يأخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي.[2]

وتجدر الاشـارة الى أن الاتفاق في الأصـل غير مجرم لأنه مرحلة نفسـية لا تخرج عن مجرد العزم والقانون لا يعاقب على مجرد النوايا، غير أن هذا الاتفاق إذا تجســـد في أعمال مادية، فهنا يتجاوز مجرد العزم ويبدأ في التحضـــير وان لم يكن تحضـــيرا كاملا، أي يدخل المرحلة التحضـــيرية وبالتالي جرمه المشـــرع، حيث نص في المادة 394 مكرر 5 أن

[1]- محمد خليفة، مرجع سابق، ص 189.

[2]- خالد ممدوح ابراهيم، مرجع سابق، ص 53.

كل من شـارك في مجموعة أو اتفاق تألف بغرض الاعداد لجريمة أو أكثر وكان التحضـير مجسد بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.

ويقوم الركن المـادي في هـذه الجريمـة بـانعقـاد ارادتين أو أكثر واجتمـاعهمـا على موضـوع معين (يتمثل في الاعداد لجريمة أو أكثر سـواء جريمة الدخول أو البقاء، جريمة التلاعب بالمعطيات، جريمة التعامل في معطيات غير مشروعة. وهو ما نصـت عليه المادة 394 مكرر 05 من قانون العقوبات)، ويقوم بغض النظر عن الوقت الذي اسـتغرقه سـواء كان منظما أو عارضا اقتصر اعضاؤه على مجرد العزم[1]، ويشترط لقيام الجريمة تعدد الجناة: الحد الأدنى هو شخصين، كلاهما مسؤول جزائيا، فاذا لم يكن احداهما مسؤولا جزائيا لا يقوم الاتفاق.

أما الركن المعنوي في هذه الجريمة فيقوم وفقا للعلم بماهية الفعل أو الأفعال موضـوع الاتفاق وبما لها من خصـائص يعتمد عليها المشـرع في اضـفاء الصـفة الجرمية عليها. ويجب أن تكون الارادة جادة لدى شـخصـين على الأقل وانتفاؤها لدى أحدهما ينفي الجريمة ككل. من الجرائم العمدية يشترط القصد العام (العلم والارادة).

وهو ما أخذ به المشـرع الفرنسـي كذلك، حيث يشـترط القصـد العام لتوفر الجريمة ومثال ذلك ما جاء في قضـية أحد المسـاهمين مع انونيموس في اتفاق مبرم للقيام بالتلاعب بمعطيات شـركة كهرباء فرنسـا، حيث تمت ادانته على أسـاس المشـاركة عن علم وارادة في الاتفاق على اغراق نظام المعالجة الآلية للمعطيات في الشركة ببيانات جديدة، مما يؤدي الى اعاقة وتشويه سير النظام، وهو ما أيدته محكمة النقض الفرنسية.[2]

[1]– وهو ما ورد في المادة 176 من ق ع ج (اتفاق مهما كانت مدته وعدد اعضائه).

[2] -Cour de cassation، crime, 7, novembre 2018 n 16-84,918 , Thierry J B, Participation à une cyber-association de malfaiteurs , AJ Pénal- mensuel, Dalloz, France, 2018, p 44-45.

ثالثا: خصوصية الجرائم المعلوماتية

تتميز الجرائم المعلوماتية عن الجرائم العادية في عدة نقاط نوضحها كما يلي:

1-خصوصية الجرائم المعلوماتية بحسب وظيفتها:

الجرائم المعلوماتية عابرة للحدود الوطنية: (ذات طابع دولي)

تتسم الجرائم المعلوماتية بالطابع عبر الوطني، فهي جرائم لا تعرف الحدود[1]، وتنتقل فيها البيانات والمعلومات والأموال بسرعة كبيرة مما يرتب صعوبات اجرائية في ملاحقة مرتكبي الجرائم المعلوماتية، ويتطلب تضافر الجهود الدولية في تنظيم أطر المواجهة والتعاون الدولي.[2]

الجرائم المعلوماتية صعبة الاكتشاف والاثبات:

تتميز الجرائم المعلوماتية بأنها صعبة الاكتشاف وان اكتشفت فهي صعبة الاثبات، ولعل سبب صعوبة كشفها هو عدم تركها لآثار مادية، أو صعوبة الوصول الى تلك الآثار المعلوماتية الرقمية التي تتيح لرجال الشرطة رؤية أو الكشف على مسرح الجريمة، والسبب في صعوبة اثباتها ان اكتشفت هو غياب الدليل المرئي، فأغلب البيانات تكون على شكل رموز لا يمكن قراءتها، مما يصعب كشفها أو التعرف على مرتكبها بسبب غياب الدليل.[3]

[1] -Arredondo C G S, l'usurpation d'identité numérique sur internet : Etude comparée des solutions français, mexicaines et nord-américaines, thèse de doctorat en droit, spécialité droit privé et sciences criminelles, université Paris Saclay, France, 2018, p 320.

[2]– رامي متولي القاضي، مكافحة الجرائم المعلوماتية–في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، ط 1، مصر، 2011، ص 53.

[3]– لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، دار الحامد للنشر والتوزيع، عمان الأردن، سنة 2014، ص 27.

-الجرائم المعلوماتية تتسم بالجاذبية:

تعتبر سوق المعلومات والحاسب والإنترنت ثروة كبيرة للمجرم المعلوماتي ولانتشار الاجرام المنظم، حيث أصبحت مصدر لتبييض الأموال وتوظيفها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات، وغيرها.[1]

- الجرائم المعلوماتية مرنة لها سلبيات وخيمة:

تمتاز الجرائم المعلوماتية عن الجرائم التقليدية بأنها غامضة، لا تتسم بالعنف، كما يصعب اكتشافها وضبط مرتكبيها ومحاكمتهم، وقد يتم تدمير المعلومات التي من الممكن ان تستخدم كدليل اثبات في مدة لا تقل عن ثانية واحدة.[2]

حيث أن هذا النوع من الجرائم سريع النمو، ويتسبب في أضرار جسيمة ويشكل تهديدات حقيقية للضحايا في جميع أنحاء العالم.[3]

ومن بين الأسباب التي تزيد من الضرر الناجم عن الجرائم المعلوماتية: هو تداخل الحاسب الآلي في بيئة الأعمال التجارية والمعاملات في القطاع العام والخاص، كذلك انتشار ظاهرة سوء استخدام الحاسب الآلي مثل نشر الفيروسات الضارة وتعميم المعلومات الارهابية وافشاء أسرار أسلحة الدمار الشامل، كذلك عدم الاستقرار السياسي في العالم يضاعف من احتمالات الاعتداء على أجهزة الحاسب الآلي ونظم الاتصالات، خاصة في الدول المتقدمة التي تعتمد كليا على التقنيات العالية.[4]

---

[1]- اسراء جبريل رشاد مرعي، الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي للدراسات الاستراتيجية، الاقتصادية والسياسية، ألمانيا، 2016، بحث منشور على الموقع: https://democraticac.de/?p=35426، تاريخ الدخول: 15-05-2019، الساعة 02.00.

[2]- رامي متولي القاضي، مرجع سابق، ص 53.

[3] -Arredondo C G S, op cit, p 297.

[4]- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط1، مركز الدراسات والبحوث، الرياض، 2004، ص 82.

كما أن عدم القدرة على التحكم في الذباب الالكتروني الذي ينشـــر مواضـــيع متفرقة تمس جهات معينة خاصة عند اعادة نشرها في عدة مجموعات وصفحات، قد يكون سببا في زيادة الأضرار الناجمة عن هذه الجرائم.

2-خصوصية الجرائم المعلوماتية بالنظر الى شخصية المجرم المعلوماتي

تتميز الجرائم المعلوماتية في ارتكابها عادة من طرف عدة أشـــخاص، يقوم بالجانب التقني من المشـروع الاجرامي شـخص متخصـص في تقنيات الحاسـوب والانترنت، ويقوم شـــخص آخر من المحيط أو من خارج المؤســـســـة المجني عليها لتغطية عملية التلاعب وتحويل المكاسـب له، حيث أن الاشـتراك في اخراج الجريمة المعلوماتية الي حيز الوجود قد يكون ســـلبيا وهو الذي يترجم الصـــمت من جانب من يعلم بوقوع الجريمة في محاولة منه تسهيل اتمامها، وقد يكون اشتراكا ايجابيا في الغالب يتمثل في المساعدة الفنية أو المادية.[1]

أ-مميزات المجرم المعلوماتي

- المجرم المعلوماتي هو شـخص ذو مهارات فنية عالية متخصـص في الاجرام المعلوماتي، قادر على اســـتخدام خبراته في الاختراقات وتغيير المعلومات، وعلى تقليد البرامج أو تحويل الأموال. وغيرها، محترف في التعامل مع الوسـائل التقنية والانترنت، اجتماعي يمكنه التكيف مع الآخرين.[2]

- يمتاز بالمستوى المعرفي والذكاء في استعمال وسائل التكنولوجيا الحديثة.

[1]- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 2، دار الثقافة، عمان الأردن، 2010، ص 58.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 40.

-يعود المجرم المعلوماتي للجريمة دائمًا: فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات وقد لا يحقق الاختراق بهدف الايذاء بل بهدف تطوير مهارته وقدرته على الاختراق.[1]

- يعتمد على القوة الفكرية لا العضلية، مما يرتب خسائر فادحة خاصة في الدول المتقدمة.

- استخدام المجرم المعلوماتي لوسائل الدفع الالكتروني يشكل خطرا يفوق ما يترتب عن الجرائم التقليدية.

- مجرم فضولي محترف يعمل على تطوير قدراته التقنية باستمرار.

ب-أنواع المجرمين المعلوماتيين:

يمكن تصنيف أنواع المجرمين المعلوماتيين الى:

-القراصنة:

وتشمل هذه الطائفة القراصنة المحترفون: وهم أشخاص ذوي كفاءة علمية عالية، يفضلون العمل الجماعي وغالبا يكون دافعهم لارتكاب الجريمة هو كسب الأموال بطرق غير مشروعة.

والى جانب ذلك هناك نوع يطلق عليه الاشخاص المبتدئون: هدفهم الأول هو تحقيق المغامرة والاثارة، وأن يتم تقبلهم في مجتمع القراصنة، اضافة الى طائفة مسماة بأطفال النصوص البرمجية: وهو مصطلح أطلقه القراصنة ذوي الخبرة، على الأشخاص الأقل نضجا ولكنهم خطيرين في نفس الوقت، يستغلون الزلات الأمنية في الانترنت، ويستعملون أساليب

[3] - اسراء جبريل رشاد مرعي، الجرائم الإلكترونية " الأهداف - الأسباب - طرق الجريمة ومعالجتها، المركز الديمقراطي العربي، ألمانيا، https://democraticac.de/?p=35426، الدخول يوم 15-05-2019، الساعة 02.00.

وبرامج أو نصـوص برمجية معروفة يسـهل العثور عليها، ليسـتغلوا نقاط الضـعف ومن ثم توجيه هجمات الكترونية.[1]

-الأشخاص المخادعون:

يتمتع هؤلاء بالكفاءة والقدرات الفنية العالية، متخصـصـين في المجال المعلوماتي، تنصـب معظم جرائمهم على شـبكات تحويل الأموال، التلاعب بالحسـابات المصـرفية أو الفواتير أو تزوير البطاقات الرقمية.[2]

-الجواسيس:

هدفهم هو جمع المعلومات لمصـلحة الدولة التي ينتمون اليها أو لمصـلحة بعض الأشخاص أو الشركات المنافسة.[3]

-الأشخاص المتطرفون ذوي المثل العليا:

يشـمل هذا النوع الأشـخاص الذين يدافعون عن توجه معين، وهم على اسـتعداد تام للاشتراك والانخراط مع جماعات اجرامية أخرى من شأنها الاضرار بالأشخاص أو بقطاعات مختلفة في المجتمع، سواء كانت الغاية ذات طابع سياسي، عرقي، ديني، اقتصادي.[4]

[1]- أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية، القاهرة، 2015، ص 193.

[2]- علي جبار الحسيناوي، مرجع سابق، ص37.

[3]- رامي متولي القاضي، مرجع سابق، ص 58.

[4]- طاهر محمود أبو القاسم، الجرائم المعلوماتية: صعوبات وسائل التحقيق فيها وكيفية مواجهتها، منشورات المنظمة العربية للتنمية الادارية جامعة الدول العربية، 2019، ص53.

الفرع الثاني: صعوبة التحقيق رغم وجود جرائم معلوماتية

رغم وجود جرائم معلوماتية فقد تقف خصوصياتها كحجر عائق أمام السلطات المكلفة بالتحقيق في تمحيص الأدلة والوصول الى الحقيقة القضائية.

كما أن طبيعة الجاني والمجني عليه قد تعيق سير اجراءات التحقيق، وذلك باعتبار أن المجرم المعلوماتي يعتبر محترفا مدركا للجوانب التقنية ويعرف كيف يخفي هويته للحيلولة دون تعقبه أو كشفه، حيث تبقى أنشطته مجهولة وبمنأى عن علم السلطات المعنية بمكافحة الجرائم المعلوماتية، أما طبيعة المجني عليه الذي قد يقع في اغلب الأحيان ضحية الجرائم المعلوماتية أي شخص سواء كان شخص طبيعي أو معنوي بسبب جهله بالجوانب الرقمية أو امتناعه عن التبليغ عن الجرائم.[1]

أولا: انعكاس خصوصية الجرائم المعلوماتية على اجراء التحقيق

كما سبق بيانه فجرائم المعلوماتية لها من الخصوصية ما يميزها عن غيرها من الجرائم التقليدية، الا أن التحقيق فيها قد يصادفه عدة اشكالات متعلقة بالجريمة في حد ذاتها.

فاذا نظرنا لخصوصية الجريمة في عبورها حدود الدولة الواحدة فذلك يثير العديد من المشاكل المتعلقة بالسيادة، الاختصاص القضائي، القانون الواجب التطبيق، قبول الأدلة المتحصل عليها في دولة ما أمام قضاء دولة أخرى، متطلبات التحقيق، الملاحقة، التفتيش والضبط؛

[1]– فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، 2003، ص 34.

وفي هذا السياق: قضية الاعتداء على سيتي بنك (City Bank في نيويورك بواسطة Vladimir Levin وأعضاء من المافيا في روسيا وبستراسبورغ، وقد خلق ذلك مشكلة قانونية بالنسبة لمكتب التحقيقات الفيدرالي، لأن المحققين كان عليهم فحص نظم البنوك في سبع دول مختلفة، حيث تم الايداع الالكتروني للنقود وكان تطبيق أوامر التفتيش والتتبع الزمني لهذا الحدث تحديا بالنسبة لمعظم المحققين، وتم القبض على المتهم وحكم عليه بالسجن لمدة ثلاث سنوات وإلزامه بدفع مبلغ 240 ألف دولار لسيتي بنك.[1]

كذلك قضية Thompson RN: حيث قام مبرمج انجليزي يعمل في بنك بالكويت بالتلاعب في معطيات نظام الحاسب الآلي للبنك، عن طريق الخصم من أرصدة العملاء والايداع في حسابه الخاص ثم بعد عودته لبلاده طلب من البنك تحويل الحساب الخاص الى عدة حسابات بنكية في انجلترا، وبعدها حكم عليه بالسجن بتهمة الحصول على أموال الغير بالاحتيال. فقام بالطعن في الحكم استنادا الى عدم اختصاص القضاء الانجليزي لأن فعل السحب والايداع كان بالكويت. غير أن محكمة الاستئناف رفضت طعنه على أساس أن النشاط الاجرامي للمتهم لم يكتمل الا بعد طلب التحويل ثم حصوله على الأموال محل النشاط الاجرامي، وبالتالي المكافحة تتطلب تعاونا كثيفا بين الدول وتوافقا كبيرا بين تشريعاتها.[2]

زيادة على ذلك قد ينعكس أثر خصوصية الجرائم المعلوماتية في اعاقة سير اجراءات التحقيق وتفسير ذلك:

[1] طاهر محمود أبو القاسم، مرجع سابق، ص 159.

[2]– محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، المجلد 1، العدد 1، الجلفة، ص 376.

عدم ترك الجرائم المعلوماتية لأثر خارجي، فلا توجد جثث قتلى ولا آثار دماء، ولا آثار عنف كما في الجرائم التقليدية، وهذا بسبب ارتكاب الجرائم المعلوماتية باستخدام تقنيات تكنولوجية عالية تعتمد على نقل المعلومات المعالجة آليا بالنبضات الالكترونية.[1]

كما أنه ضخامة حجم وكم البيانات والملفات المتواجدة في البيئة المعلوماتية، يصعب من امكانية تحديد الملفات والبيانات المجرمة، ويؤدي في الغالب الى اصطدام مهمة الاكتشاف بحق الفرد في الخصوصية الشخصية.[2]

أما بالنظر الى خصوصية الجرائم المعلوماتية حسب شخصية المجرم المعلوماتي:

فمن الصعوبات التي تواجه السلطات المختصة بالتحقيق هي قدرة الجاني على محو الأدلة القائمة ضده، أو تدميرها في زمن قصير.[3]

كما أن البحث في ملفات الحاسب الآلي تقابله صعوبة غير عادية، لاستطاعة الجاني تحريك الملفات من جهاز لآخر بسرعة فائقة واخفائها في مساحة ضئيلة جدا على ذاكرة الحاسب، أو تخزينها في سيرفر يقع في دولة ذات اختصاص قانوني مختلف في تجريم هذه الجرائم، كذلك صعوبة تتبع المعلومات داخل الجهاز كدليل تسعى الجهات الأمنية لملاحقته وذلك بسبب وجود كم هائل من المعلومات والبرامج والملفات المخزنة التي يتعين فحصها ولها ارتباط بالجريمة لكشف ادلة الجريمة، وتكمن الصعوبة اما في طبيعة المعلومات أو في نقص الخبرة الفنية.[4]

[1]– طاهر محمود أبو القاسم، مرجع سابق، ص 158.

[2]– رشاد خالد عمر، مرجع سابق، ص 61.

[3]– خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، عمان، 2011، ص 223.

[4]– طاهر محمود أبو القاسم، مرجع سابق، ص 159 ص160.

ثانيا: دور الضحية في اعاقة سير التحقيق في الجرائم المعلوماتية

ان الضحية في الجريمة المعلوماتية هو كل من أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع للتقنيات الالكترونية الرقمية.[1]

نتيجة لقلة خبرة الضحايا، وكشفهم عن بعض المعلومات الشخصية عن حياتهم اليومية أو استعمالاتهم المفرطة لوسائل التواصل الاجتماعي، قد يؤدي الى زيادة ارتكاب الجرائم المعلوماتية خاصة جرائم السب والشتم، والابتزاز الالكتروني، سرقة المعلومات الشخصية والاعتداء على حرمة الحياة الخاصة.

وقد يكون امتناع الضحايا عن التبليغ سببا في عدم مباشرة اجراءات التحقيق في الجرائم المعلوماتية، ومن أهم أسباب الامتناع عن التبليغ عند التعرض لأحد أنواع الجرائم المعلوماتية:

- قد يعود الى الجهل بالقانون: حيث أن عدم الادراك بوجود نصوص تجرم وتعاقب على أشكال الجرائم المعلوماتية قد يكون سببا مباشرا في عدم التبليغ.
- عدم معرفة الضحية بالإجراءات التي يمكنه اتباعها في حالة التعرض للجرائم المعلوماتية كعدم معرفته الجهة التي يلجأ لها للتبليغ وكيفية التبليغ عن الجرائم.
- امتناع الشركات أو المؤسسات عن التبليغ خوفا على سمعتها وكيانها، وقد تكون الخشية بسبب أن التبليغ قد يكون فرصة ذهبية أمام المجرم المعلوماتي لمعرفة ثغرات النظام المعلوماتي للمؤسسة، ومختلف نقاط الضعف فيها.
- تخوف المؤسسات التجارية من استغراق التحقيق لفترة زمنية طويلة، مع احتمالية احتفاظ جهات التحقيق بأجهزة الحاسب مما يؤثر على حسن سير العمل بتلك الشركات والمؤسسات.

[1]– مصطفى محمد موسى، مرجع سابق، ص 158.

- امتناع الشـركات والمؤسـسـات المالية (كالبنوك) عن التبليغ خشـية من اهتزاز ثقة المتعاملين معها وبالتالي سحب ودائعهم واستثماراتهم، ولا يقف الأمر على عدم التبليغ فقط بل يتعداه الى الامتناع عن تقديم اية مساعدة لجهات التحقيق إذا علمت السلطات بالجريمة، الأمر الذي يشـكل صـعوبة في اكتشـاف الجريمة من جهة وصـعوبة في اثباتها من جهة اخرى.[1]

وفي احدى الوقائع تعرض بنك Marchant Bank city في بريطانيا الى سـرقة 08 مليون جنيه استرليني من أحد ارصدته الى رقم في سويسرا، وتم ضبط الفاعل متلبسا بسحب المبلغ المسـروق، وبدلا من محاكمته قام البنك بدفع مليون جنيه له شـرط التزام الفاعل بعدم الاعلام عن جريمته، واعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي.[2]

-**صـعوبة تحديد نطاق الضـحايا:** ويعود السـبب في ذلك الى أنهم في أغلب الأحيان لا يعلمون شـيئا عن الجريمة الا بعد وقوع الفعل وفي هذه الحالة يرون من الحكمة عدم الابلاغ عنها، كما لا يحبذ اكثرهم أن يعترف بأن نظامه المعلوماتي قد وقع ضـحيه اعتداء، وهذا السلوك السلبي يعتبر مغريا لمرتكبي الجرائم للاستمرار في أنشطتهم.[3]

- اعتقاد بعض الضـحايا بعدم قدرة الأجهزة الأمنية على التوصـل لمرتكبي الجرائم بسـبب نقص خبرتهم وعدم توفر الامكانيات اللازمة للتوصل الى المجرمين.

[1]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 130.

[2]- حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، ط 01، دار النهضة العربية، القاهرة مصر، ص 34.

[3]- فتوح الشاذلي، عفيفي كامل عفيفي، مرجع سابق، ص 34.

-التخوف من الاساءة للسمعة والفضيحة خاصة في الجرائم الاباحية والتشهير بالنساء أو في حالات الاعتداء الجنسي على الاطفال، وعرض صور اباحية لهم في مواقع الانترنت؛ كما أن تخوف الموظف من الحرمان من خدمة الانترنت، قد يكون سببا في امتناعه عن التبليغ حين يتعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لمواقع غير مؤمنة أو غير مسموح بزيارتها.[1]

ثالثا: وسائل التقليل من الصعوبات المتعلقة بالجرائم المعلوماتية

- التكوين المستمر للأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية بتقنيات الحاسب الآلي وكيفيات التعامل مع الادلة الالكترونية.
- الاستعانة بالخبرة الفنية العملية في المجال المعلوماتي، لتحديد نوعية الأدلة الالكترونية التي يجب ضبطها والبحث عنها والتي لها أهمية في التحقيق، كما يمكن الاستعانة بنظم المعالجة الآلية للبيانات من أساليب الفحص والتدقيق والمراجعة لاستخراج الدليل الالكتروني.[2]
- تحسيس المواطن بدوره في وجوب التبليغ عن الجرائم المعلوماتية بمختلف أنواعها.
- تحسيس المجتمع خاصة الأولياء بالجانب السلبي للتكنولوجيات الحديثة وبوجوب حماية القصر عبر الانترنت.[3]

ووجوب التبليغ عن التهديدات التي يتعرض لها القصر باي شكل من الأشكال.

[1]- طاهر محمود أبو القاسم، مرجع سابق، ص 174.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 139.

[3]- وقد قامت وزارة البريد والاتصالات السلكية واللاسلكية في الجزائر بنشر دليل عملي للأولياء والأوصياء والمربين يتعلق بحماية الأطفال على الانترنت، في 15-جويلية-2020.

- تفعيل دور وسائل الاعلام المختلفة عن أماكن تلقى البلاغات في الجرائم المعلوماتية، مع اتخاذ السلطات المتخصصة في المجال المعلوماتي تدابير رصد كل من حركة هواة الحاسب الآلي من الشباب، حركة المشبوهين في مجال الجرائم المالية وجرائم المخدرات، وفي مجال جرائم الاتجار غير المشروع في المعلومات وتقنيات الحاسب الآلي، في جرائم الاستغلال الجنسي للأطفال، ورصد مختلف المواقع المشبوهة والاباحية، اضافة الى متابعة المسجلين في جرائم التزوير والاحتيال.[1]

[1]– طاهر محمود أبو القاسم، مرجع سابق، ص 176.

المطلب الثاني: العناصر الثانوية للتحقيق في الجرائم المعلوماتية

خصصنا هذا المطلب لتوضيح أهم العناصر لصحة اجراء التحقيق والتي تستتبع الوجود الفعلي للجرائم المعلوماتية حيث يستوجب استظهار وقت ومكان ارتكابها، وهو ما تناولناه في الفرع الأول تحت عنوان تحديد حيز الجرائم المعلوماتية، كما يستوجب توفر شروط هامة لمباشرة اجراءات التحقيق والمتمثلة في عنصري السرية وتدوين الاجراءات وهو ما تناولناه في الفرع الثاني تحت عنوان شروط التحقيق في الجرائم المعلوماتية.

الفرع الأول: تحديد حيز الجرائم المعلوماتية

ان مسألة النتيجة الاجرامية في مجال الجرائم المعلوماتية تثير العديد من المشاكل من بينها: ما يتعلق بوقت ومكان تحقق هذه النتيجة، فمثلا لو قام أحد المجرمين في دولة معنية باختراق حساب بنكي تابع لدولة أخرى فهذا بطبيعة الحال يثير مشكلة وقت تحقق النتيجة الاجرامية هل هو وقت الدولة الصادر منها الفعل المادي أو وقت البنك الموجود خارج حدود الدولة، وهو ما يثير مشاكل اخرى منها ما يتعلق بمكان ارتكاب الجريمة باعتبارها عابرة للحدود الوطنية، اضافة الى مشكلة القانون الواجب التطبيق.[1]

أولا: القانون واجب التطبيق

لتحديد القانون الواجب التطبيق في الجرائم المعلوماتية لابد من التطرق للمبادئ التي يعتمد عليها لتحديد هذا القانون، ومن ثم تحديد الاختصاص بالنظر في هذه الجرائم.

[1]– خالد ممدوح ابراهيم، مرجع سابق، ص 53.

-مبدأ الاقليمية:

عالج المشـرع الجزائري مسـألة القانون الواجب التطبيق من خلال نص المادة 03 من قانون العقوبات حيث " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضـــي الجمهورية. كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصـــاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الاجراءات الجزائية "

وباسـتقراء نص المادة فالدولة تحدد توزيع الاختصـاص للقضـاء الجنائي الوطني في تطبيق قانون العقوبات على اقليم الجمهورية وهذا بالنسـبة للجرائم التي ترتكب في الداخل و في الخارج -حسـب ما يدخل في نطاق اختصـاص محاكمها الجزائية- وفقا لأحكام قانون الاجراءات الجزائية، حيث أن قانون الاجراءات الجزائية باعتباره قانون اجرائي، يعتبر الوسيلة الوحيدة لتطبيق قانون العقوبات باعتباره قانون موضـوعي، وهذا ما جعله مرتبط في تطبيقه بالنطاق المكاني لهذا الأخير، وبالتالي قاعدة الاقليمية في نص المادة 3 من قانون العقوبات تعكس بدورها النطاق المكاني لقانون الاجراءات الجزائية، مما يجعله يطبق على اقليم الدولة بالنسبة للجرائم التي ترتكب داخل الاطار الاقليمي للدولة.[1]

غير أن اختصـــاص الدولة بالتحقيق في جريمة ما وان كان يخولها تطبيق قانون اجراءاتها بشأن هذا التحقيق بصرف النظر عن مكان وقوع الجريمة مادامت خاضعة لقانون العقوبات الخاص بها الا أن ذلك لا يعني أن تباشـــر اجراءاتها خارج الاقليم، حيث يتعذر على الدولة مباشـرة اختصـاصـها بالتحقيق خارج اقليمها، لان ذلك من مظاهر سـيادتها فلا يسمح لها بممارسته على اقليم دولة اخرى[2] (تعارض مع مبدأ سيادة الدولة الاخرى)

[1]- عبد الرحمن خلفي، الاجراءات الجزائية، ط 3، دار بلقيس، الدار البيضاء الجزائر، 2017، ص 42.

[2]- خالد عياد الحلبي، مرجع سابق، ص 243.

غير أن مبدأ الاقليمية في الجرائم المعلوماتية فيه من الصعوبة ما يحول دون إمكانية تطبيقه وذلك بسبب خصوصية هذا النوع من الجرائم وتميزها بالطابع عبر الوطني، فمن جهة نجد أنفسنا أمام إشكالية تعدد القوانين المطبقة حسب الدول، ومن جهة أخرى نكون أمام إشكالية عدم إمكانية تحديد دقيق لوقت ومكان ارتكاب هذا النوع من الجرائم.

-مبدأ الشخصية:

تبنى المشرع الجزائري مبدأ الشخصية كمكمل لمبدأ الاقليمية و وفي ذلك لا يمكن افلات المجرم المتمتع بالجنسية الجزائرية من العقاب، حتى لو ارتكب جريمة معاقب عليها في القانون الجزائري خارج اقليم الجمهورية، حيث يجوز متابعته في جناية بشرط عودته اختياريا لأرض الوطن و لم يثبت أنه حكم عليه نهائيا في الخارج و أن لا يكون قد عوقب بموجب حكم نهائي،[1] واضافة الى ذلك فاذا كان وصف الجريمة هو "جنحة" يشترط اضافة الى ما سبق أن يكون الفعل جنحة بالنسبة للدولتين و لابد من اخطار النيابة العامة في الجزائر ببلاغ من الطرف المضرور أو من سلطات الدولة الأخرى.[2]

ويستصعب تطبيق هذا المبدأ في الجرائم المعلوماتية نتيجة طبيعة المعلومات وإمكانية تخزينها في سيرفر دول ذات اختصاص قضائي مختلف، مما يجعلنا أمام إشكالية تنازع الاختصاص القضائي الدولي.[3]

[1]- المادة 582 من الأمر 66-155، الموافق ل 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.

[2]- المادة 583 من الأمر 66-155، الموافق ل 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.

[3]- محمد كمال شاهين، الجوانب الاجرائية للجريمة الالكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، دار الجامعة الجديدة، الاسكندرية، 2018، ص 200.

-مبدأ العينية:

حصر المشرع الجزائري بعض الجرائم في المادة 588 من قانون الاجراءات الجزائية، و التي ينظر فيها وفقا لمبدأ العينية و تتمثل في كل جناية أو جنحة ضـــد ســـلامة الدولة الجزائرية أو تزييف النقود أو أوراق مصـرفية وطنية متداولة قانونا في الجزائر، وأي جناية أو جنحة ترتكب اضرار بمواطن جزائري، حيث ينعقد الاختصاص للقضاء الجنائي الوطني على كل من يرتكب أحد هذه الجرائم خارج الاقليم الجزائري بصـفته فاعلا أصـليا أو شـريكا حيث يجوز متابعة الجاني و محاكمته وفقا للقانون الجزائري اذا ألقي عليه القبض في الجزائر أو تم تسليمه بموجب اتفاقية تسليم المجرمين.

وتكمن المشـــكلة هنا في حالة تنازع الاختصـــاص بين دولة ارتكبت فيها الواقعة الاجرامية وفقا لمبدأ الاقليمية ودولة تعتبر الفعل جريمة يختص بها قضـــاؤها وفقا لمبدأ العينية،[1]

اضـافة الى عدم مصـادقة بعض الدول على اتفاقية تسـليم المجرمين، مما يؤدي الى افلات المجرم من العقاب، كما أن خصـوصـية الجرائم المعلوماتية في عدم تركها لآثار مادية أو صـعوبة التوصـل للآثار الرقمية قد تعيق تطبيق هذا المبدأ بسـبب غياب الأدلة الالكترونية وبالتالي قد لا يتوصل الى المجرم المعلوماتي أصلا.

-مبدأ العالمية:

يخول مبدأ العالمية للقضـــاء الجنائي الوطني حق النظر في الجرائم المرتكبة في الخارج من حامل لجنسية أجنبية ضد ضحية أجنبية، ويبقى هذا المبدأ غير مقنن في القانون الجنائي الجزائري بشقيه قانون عقوبات وقانون اجراءات جزائية.

[1]- محمد كمال شاهين، مرجع سابق، ص 190.

ثانيا: مسألة الاختصاص القضائي في الجرائم المعلوماتية

تثير الجرائم المعلوماتية عدة مشـــاكل نتيجة امكانية ارتكابها في مكان معين، وترتب آثارها في مكان آخر داخل أو خارج الدولة، وهنا تنشأ عدة مشاكل أبرزها: [1]

- مشكلة البحث عن الأدلة الجنائية خارج دائرة الاختصاص المسجل فيها البلاغ، والتي تم فيها تحريك الاجراءات الجزائية.
- مشـكلة فحص البيانات في مراكز معلومات دول أخرى الشـيء الذي يتطلب خضـوع اجراءات التحقيق للقوانين الجنائية السارية في تلك الدولة.

بالرجوع الى القانون 09-04 سـالف الذكر، نجد أن المادة 15 منه ضـمن الفصـل السادس المتضمن التعاون والمساعدة القضائية الدولية تناولت مسألة الاختصاص القضائي، فإضـافة الى قواعد الاختصـاص المنصـوص عليها ضـمن قانون الاجراءات الجزائية، منح الاختصـاص للمحاكم الجزائرية بالنظر في الجرائم المتصـلة بتكنولوجيات الاعلام والاتصـال المرتكبة خارج الاقليم الوطني، وذلك عند توفر مجموعة من الشروط تتمثل في:

1. وجود جريمة من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال
2. ارتكاب الجريمة خارج اقليم الدولة
3. أن يكون مرتكب الجريمة أجنبي
4. اسـتهداف الجريمة مؤسـسـات الدولة الجزائرية أو الدفاع الوطني أو المصـالح الاستراتيجية للاقتصاد الوطني.

واكدت المادة 53 من القانون 18-07 سـالف الذكر، اختصـاص الجهات القضـائية الجزائرية بمتابعة الجرائم المتعلقة بمعالجة المعطيات ذات طابع شـخصـي التي ترتكب خارج اقليم الجمهورية، " سـواء من طرف جزائري أو شـخص أجنبي مقيم في الجزائر أو شـخص

[1]- محمد الأمين البشري، مرجع سابق، ص 128.

معنوي خاضـــع للقانون الجزائري. كما تختص الجهات القضـــائية الجزائرية بمتابعة الجرائم المنصوص عليها في هذا القانون وفقا لقواعد الاختصاص المنصوص عليها في المادة 588 من قانون الاجراءات الجزائية."[1]

ويتضح من هذه المادة الرجوع الى القواعد العامة عملا بمبدأ العينية فيما يخص ارتكاب هذه الجرائم خارج الاقليم الوطني، وما نلاحظه أن القوانين مازالت قاصـــرة وتتطلب مرونة أكبر لمواجهة الصعوبات التي تقف حجر عائق أمام الأجهزة المكلفة بالتحقيق.

[1]- أنظر نص المادة 53 من القانون 18-07، سالف الذكر، ص 22.

الفرع الثاني: شروط التحقيق في الجرائم المعلوماتية

ان التحقيق في الجرائم المعلوماتية يتطلب وجوبا احترام قواعد قانونية لازمة ولعل أهمها هو احترام عنصر السرية، ولا يمكن اثبات التحقيق الا بتوفر الكتابة كشرط أساسي لصحة اجراء التحقيق، وإضافة الى ذلك تناولنا شرط آخر متمثل في حق الدفاع عند استعمال المحادثة المرئية عن بعد خلال مرحلة التحقيق، وهو ما ستتناوله في هذا الفرع كما يلي:

أولا: العلنية بالنسبة للخصوم والسرية بالنسبة للجمهور

إذا كان الأصل هو العلانية المطلقة في مرحلة التحقيق النهائي أي مرحلة المحاكمة، بهدف توضيح حسن سير اجراءات الدعوى، ولكي تكون أحكام القاضي ليست محل شك أو أي خضوع لأي جهة، الا أن مرحلة التحقيق الابتدائي –مرحلة التحقيق القضائي–تكون العلانية فيها نسبية بمعنى أنها قاصرة على فئة محددة بهدف حسن سير العدالة وسلامة التحقيق من الآثار السلبية له.[1]

في هذا السياق نصت المادة 11 ق اج (تكون اجراءات التحري والتحقيق سرية ما لم ينص ق على خلاف ذلك، ودون اضرار بحقوق الدفاع) فبتدرج أداء المهام ابتداء من مرحلة التحقيق الأولي (التمهيدي) الى مرحلة التحقيق الابتدائي (القضائي) ثم مرحلة التحقيق النهائي (المحاكمة)، يكون هناك تدرج في ضمانات حقوق الدفاع وهنا نشير الى نقطة مهمة وهي: وجوب التوازن بين فعالية التحقيق وضمان حقوق الدفاع.

[1]– علي عدنان الفيل، اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة) المكتب الجامعي الحديث، مصر، 2011، ص 67.

وبناء على هذه القاعدة، يعتبر التحقيق الجنائي أســـاس توفير العدالة، وتحقيقها بمفهومها العام، يشمل جميع أطراف المجتمع، سواء ضحية أو متهم، وحتى بالنسبة للمحقق الجنائي حيث يســـتهدف التحقيق توفير الحماية الكاملة له حال اتخاذه اجراءاته القانونية الصحيحة، وكلما توافرت الضمانات اللازمة ادى ذلك الى شعور الجميع بالأمان وعدم الوقوع تحت طائلة الظلم.[1]

ولابد لمرحلة التحقيق الابتدائي أن توازن بين ضرورات المصلحة العامة واقتضاء حق الدولة في توقيع العقاب من ناحية، وبين مقتضــيات احترام الحرية الفردية وحقوق الدفاع عن المتهم من ناحية أخرى.[2]

ان أهم ضمانة تحرص عليها أغلب القوانين الجزائية هي جعل التحقيق الابتدائي سري بالنسبة للجمهور، وعلني بالنسبة للخصوم.

حيث أن عدم امتداد العلانية الى الجمهور له هدفين رئيسيين:

يتمثل الهدف الأول في عدم الاساءة والتشهير بالمتهم قبل ادانته والحكم عليه من قبل المجتمع، لتفادي تمديد الاســاءة والتشــهير لعائلته، اذ أن الاتهام الموجه اليه في بداية الأمر ليس ســوى وقائع مادية أو قانونية نســبت اليه، على خلاف الأصــل الذي يتمتع به كل فرد، والذي أســاســه مبدأ قرينة البراءة التي مفادها أن المتهم بريء حتى تثبت ادانته. أما الهدف الثاني هو عدم انتشــار الشــائعات بين أفراد المجتمع، مما يدفعهم للتنبؤ بأحداث القضــية والمبالغة في الوقائع المنســوبة الى المتهم، فيكون هناك رأي عام دافع مؤثر على القضــاء، ومن الممكن حتى أن ينحرف تبعا للرأي العام.[3]

[1]– خالد ممدوح ابراهيم، مرجع سابق، ص 55.

[2]– فوزي عمارة، قاضي التحقيق، اطروحة دكتوراه العلوم، جامعة قسنطينة، 2009–2010، ص 19.

[3]– خالد ممدوح ابراهيم، مرجع سابق، ص 57.

وفي هذه النقطة يمكن الحديث عن طابع الازدواجية أو الموازنة لهدف مبدأ سرية التحقيق فمن جهة يحمي سمعة الأشخاص وشرفهم، ومن جهة يحقق العدالة.

أما العلانية بالنسبة لأطراف الدعوى فهو ضرورة حتمية، ولا شك أن حضور المتهم يمليه حق احاطته بالتهمة المنسوبة اليه، وهو ما يعد أيضا ضمانة من الضمانات المقررة للمتهم، اذ أن حضوره يتيح له الوقوف على كيفية سير التحقيق في جميع مراحله، ومن حقه الرد على التهم المنسوبة اليه، ودفع الأدلة وهو بلا شك اعمال لمبدأ المواجهة.

غير أنه استثناء قد تباشر اجراءات التحقيق دون حضور للخصوم، في حالة الضرورة والاستعجال، غير أنه يبقى لمحامي المتهم حق الاطلاع على ملف القضية، واستمرار منع المتهم من حضور اجراءات التحقيق بعد زوال حالة الضرورة والاستعجال، يعد اخلالا بحقوق الدفاع ويستلزم بطلان الاجراءات[1].

ثانيا: وجوب تدوين اجراءات التحقيق

يعتبر التدوين من القواعد الأساسية في الاجراءات الجزائية، و المقصود به هو اثبات اجراءات التحقيق عن طريق الكتابة التي تعد حجة تنبني عليها النتائج، و دونها يفترض عدم مباشرة التحقيق استنادا الى مبدأ ما لم يكتب لم يحصل، فهي قاطعة للشك؛ و يستوي أن يكون التدوين في محضر واحد أو عدة محاضر، فجميع المحاضر التي يثبت فيها المحقق ما قام به من اجراءات تعتبر من أوراق الدعوى الجزائية و تكتسب حجتها متى كانت مستوفية للشروط القانونية، و من بين هذه الشروط أن يتم التدوين بمعرفة موظف عمومي يسمى كاتب الضبط (كاتب التحقيق)[2] وتجدر الاشارة الى وجوب الانتباه عند تدوين التحقيق، و ذلك لتفادي الوقوع في أخطاء جسيمة تتعلق بصحة الاجراءات أو بتدوين اجابات المستجوبين

[1]– خالد ممدوح ابراهيم، مرجع سابق، ص 58.

[2]– فوزي عمارة، مرجع سابق، ص 23 ص24.

أو اغفال تاريخ تحرير المحاضر. ولابد من ذكر الوقائع بدقة مع تفادي حشر بعض الكلمات والأقوال أو حذف أجزاء منها أو الكشط كما يلزم اعطاء الوصف القانوني للواقعة بدقة.

ثالثا: الحق في الدفاع عند استخدام تقنية المحادثة المرئية عن بعد

يعتبر حق الدفاع مكفول قانونا في شتى مراحل القضية الجزائية باعتباره أحد أهم الركائز التي تضمن المحاكمة العادلة، و لم يعط القانون 15-03 المتعلق بعصرنة العدالة[1]، أهمية للحق في الدفاع عند اجراء التحقيق و المحاكمة الالكترونية، مما يوقع عدة اشكالات اجرائية خاصة بالنسبة لحرية اتصال المحامي بالمتهم مباشرة في اي وقت، اضافة الى سكوت المشرع على ضمانة تمكين الشخص المحبوس من حقه في الدفاع مع تيسير السبل القانونية لاختيار و تأسيس دفاعه، و اغفاله لتوقيع الشخص المصرح و امكانية حضور المحامي الى جانبه في مكان تواجده الفعلي.[2]

وقد تدارك المشرع ذلك من خلال تعديله الأخير لقانون الاجراءات الجزائية الجزائري، حيث نص صراحة على امكانية استعمال وسائل الاتصال المسموعة والمرئية أثناء الاجراءات، وذلك لمقتضيات حسن سير العدالة أو الحفاظ على الأمن أو الصحة العمومية أو أثناء الكوارث الطبيعية أو لدواعي احترام مبدأ الآجال المعقولة.[3]

ففي مرحلة التحقيق القضائي، أجاز المشرع لجهات التحقيق (قاضي التحقيق، غرفة الاتهام، جهة الحكم)، استعمال تقنية المحادثة المرئية عن بعد في استجواب أو سماع

[1]- قانون رقم 15-03، مؤرخ في 01 فيفري 2015، متعلق بعصرنة العدالة، ج ر، عدد 06، الصادرة بتاريخ 10 فيفري 2015، ص 05.

[2]- عبد الحميد عمارة، استخدام تقنية المحادثة المرئية عن بعد في التحقيق والمحاكمة الجزائية، مجلة دراسات وابحاث المجلة العربية في العلوم الانسانية والاجتماعية، مجلد 10، عدد 3، 2018، ص 68 ص69.

[3]- أمر رقم 66-155، الموافق ل 8 جوان 1966، المتضمن قانون الاجراءات الجزائية، المعدل والمتمم بالأمر رقم 20-04 الموافق ل 30 أوت 2020، ج ر، عدد 51، الصادرة بتاريخ 31 اوت 2020، ص 12.

شـــخص أو عند اجراء مواجهة بين الاشـــخاص أو التبليغات التي يســـتوجب القانون تحرير محاضر لأجلها.

فاذا استدعى ذلك استجواب أو سماع أو تبليغ شخص غير موقوف مقيما خارج دائرة اختصـــــاص المحكمة، توجه جهة التحقيق المختصـــــة طلبا الى وكيل الجمهورية للمحكمة الأقرب لمحل اقامته قصد استدعائه للتاريخ المحدد للقيام بالإجراء، و اضـاف شرطا مهما و هو وجوب تطبيق أحكـام المـادة 105 ق ا ج من طرف جهـات التحقيق، و التي تنص صـــراحة على وجوب ســـماع المتهم أو المدعي المدني أو اجراء مواجهة بينهما بحضـــور المحامي، أو بعد دعوته قانونا ما لم يتنازل عن ذلك صراحة، حيث يستدعى المحامي بكتاب موصـى عليه يرسـل اليه بيومين على الأقل قبل اسـتجواب المتهم أو سـماع الطرف المدني، مع امكانية استدعائه شفهيا و اثبات ذلك بمحضر، و لابد أن يوضـع ملف الاجراءات تحت طلب المحامي في أجل 24 ساعة قبل استجواب المتهم أو سماع الطرف المدني.[1]

وأضـاف المشـرع نقطة مهمة في حالة اسـتحالة تحويل المتهم أو الشـخص المحبوس، حيث يمكن سـماعه عن بعد بحضـور أمين ضـبط المؤسـسـة العقابية ويحرر محضـرا بذلك، يوقعه ويرسله بمعرفة مدير المؤسسـة العقابية الى الجهة القضـائية المختصـة، وأجاز المشـرع حضور الدفاع رفقة موكله سواء بمكان سماعه او أمام جهة التحقيق المختصة.

ويوقع الشـخص المسـموع على نسـخة المحضـر المرسـل اليه بأية وسـيلة من وسـائل الاتصـال، بعد توقيعه مباشرة من القاضـي وأمين الضبط لدى الجهة القضائية المختصة، وإذا

[1]– المادة 105 من الأمر 66–155، الموافق ل 8 يونيو 1966، المتضمن قانون الاجراءات الجزائية، المعدل والمتمم بالقانون رقم 01–08 المؤرخ في 26 يونيو 2001، ص 66.

امتنع عن التوقيع أو تعذر ذلك ينوه الى ذلك على نسخة المحضر، وتعاد النسخة الى الجهة القضائية المختصة بنفس وسيلة الارسال لتلحق بملف الاجراءات.[1]

ولابد أن ننوه أن هذا الاجراء مازال يشــوبه العديد من الصــعوبات خاصــة مع نقص تدفق الانترنت، وانقطاع الصوت والصورة.

[1]– المادة 441 مكرر 5 من الأمر 66–155، الموافق ل 8 يونيو 1966، المتضمن قانون الاجراءات الجزائية، المعدل والمتمم بالأمر رقم 20–04 سالف الذكر، ص 12.

المبحث الثاني: تحديات التحقيق في الجرائم المعلوماتية

يعتبر التحقيق في الجرائم المعلوماتية من الموضـــوعات المعاصـــرة التي لاقت صـــعوبات ناجمة عن طبيعة الجرائم المعلوماتية وطبيعة اطرافها، ومن ثم فمواجهة هذا النوع من الجرائم يتطلب الاستجابة للتحديات التي تواجه سلطات التحقيق، ولعل أهم هذه التحديات هو صـــعوبة اكتشـــاف هذه الجرائم المســـتحدثة، وحتى وان اكتشـــفت يصـــعب اثباتها. ولعل الســـبب الكامن وراء صـــعوبة اثباتها هو تمتع المجرم المعلوماتي بالذكاء في اخفاء معالمها، وعدم ترك الجريمة لآثار مادية ملموسـة، ناهيك عن احتياجها لخبرة فنية عالية، وهو ما دفعنا لتناول نظرية الاثبات في المجال المعلوماتي كأهم تحدي للتحقيق في الجرائم المعلوماتية.

زيادة على ذلك فارتباط الحق في الخصـــوصـــية بالبيئة الرقمية في ظل التطورات التكنولوجيـة الحـديثـة يعتبر من أهم التحـديـات التي تواجـه اجراءات التحقيق في الجرائم المعلوماتية، فمن جهة لهذا الحق صـــلة وثيقة بحرمة الفرد وســـريته وحريته في الاحتفاظ بمعلوماته الشخصية دون تطاول الغير عليها، تأسيسا على أنه "لا يجوز تعريض أحد لتدخل بشكل تعسفي في حياته الخاصـة أو شؤون أسرته أو مسكنه أو مراسـلاته ولا لحملات تمس شرفه وسمعته، ولكل شخص حق يحميه القانون من مثل ذلك التدخل أو تلك الحملات"[1]،

و " لا يجوز التدخل بشـكل تعسـفي أو غير قانوني بخصـوصـيات أحد أو بعائلته أو بيته أو مراســـلاته".[2] ومن جهة فالبيئة المعلوماتية قد تكون موقعا اســـتراتيجيا للاعتداء على هذا الحق، لسـهولة تبادل المعلومات أو تخزينها اضـافة الى نشـر الشـخص لبياناته ومعطياته الشـــخصـــية عبر المواقع الكترونية، مما يؤدي الى اســـتغلالها من قبل الغير على غير وجه حق. ومن هذا المنطلق تناولنا الحق في الخصوصية المعلوماتية في المطلب الثاني.

[1]– المادة 12 من الاعلان العالمي لحقوق الانسان لسنة 1948.

[2]– المادة 17 من الاتفاقية الدولية للحقوق المدنية والسياسية.

المطلب الأول: الاثبات في الجرائم المعلوماتية

يعتبر الاثبات من أهم أعمدة العدالة الجنائية بمجرد وضـــع القضـــية أمام الجهة القضـائية، ويرتبط الاثبات بمبدأ مهم وهو مبدأ الشـرعية الاجرائية الذي قمنا بتسـليط الضـوء عليه أولا ثم تطرقنا لقواعد الاثبات في الجرائم المعلوماتية والسلطة التقديرية للقاضـي الجنائي في تقدير الدليل الالكتروني.

الفرع الأول: الشرعية الاجرائية كمكمل للشرعية الجزائية

ان الشرعية الاجرائية مكلمة للشرعية الجزائية، وبدونها لا تكفي الشرعية الموضوعية لحماية الحقوق و الحريات الفردية، حيث أن مبدأ الشـــرعية الموضـــوعية لا يكفي لوحده للتقليص من حدة الضغط على الحريات التي تتضمنها النصوص الموضوعية، وبالتالي جاء قانون الاجراءات الجزائية بمبدأ الشـــرعية الاجرائية ليخلق توازنا بين مصـــلحة المجتمع في معاقبة الجاني و مصلحة الجاني في ضمان حريته من تعسف السلطة، حيث أن الأصل أن المتهم بريء حتى تثبت ادانته، و لا يجوز اتخاذ أي اجراء في مواجهته، الا بناء على قانون يكفل حماية الحرية الشخصية تحت اشراف القضاء.[1]

أولا: قرينة البراءة كركن أساسي للشرعية الاجرائية

ان الاصـل في المتهم هو البراءة حتى تثبت ادانته بحكم حائز لقوة الشـيء المقضـي فيه، وقد تردد هذا المبدأ في الاعلان العالمي لحقوق الانســـان، والعهد الدولي الخاص بالحقوق المدنية والسـياسـية، وتضـمنته الوثائق الاقليمية لحقوق الانسـان وواجباته كالإعلان الأمريكي لحقوق الانسان وواجباته، كما تأكد نص قرينة البراءة في العديد من دساتير الدول،

[1]– عبد الرحمن خلفي، مرجع سابق، ص 46 ص47.

والجدير بالإشـــارة ان ادراج هذا المبدأ في القوانين الاجرائية الجزائية لبعض الدول هو بمثابة الارث المشترك لكل الأمم المتحضرة[1]

وقد نصـــت الفقرة الأخيرة من المادة 11 قانون اجراءات جزائية جزائري على أنه: " تراعى في كل الأحوال قرينة البراءة و حرمة الحياة الخاصـــة" فقرينة البراءة تعتبر من القرائن المكرسة لصالح المتهم و هي أساس المبادئ العامة للدفاع في مجال ضمان الحريات الفردية في قانون العقوبات، و أساس الضمانات الاجرائية المقررة للمتهم أثناء مراحل سير الدعوى، فبما أن المتهم بريء حتى تثبت ادانته بحكم بات فانه لا يجوز متابعته الا بنص جزائي ساري المفعول وقت ارتكاب الجريمة، ولا بد أن تراعى في ذلك الضمانات الاجرائية المقررة في قانون الاجراءات الجزائية.

بناء على ذلك فالتحقيق في الجرائم المعلوماتية لابد أن يكون مبني على الحيادية، فلا يتخذ المحقق أي قرار حول ادناب أو براءة المتهم، بل يقوم بجمع الأدلة والتأكد منها، وبناء عليها يستخرج الحقائق ثم يوثقها. وهذا ما يفسر مبدأ قرينة البراءة الذي تخدمه مبادئ أخرى كسرعة الفصل في اجراءات الدعوى، ومبدأ الشك يفسر لصالح المتهم.

ثانيا: تعارض اجراءات التحقيق مع الشرعية الاجرائية

ان مباشـــرة الاجراءات العادية في بيئة لا تنســـجم مع طبيعة الجرائم المعلوماتية قد يشكل مساسا بالشرعية الاجرائية وبحقوق الأفراد، وبالتالي لابد من افراد قواعد خاصة تكفل الموازنة بين متطلبات فاعلية أنشـــطة الأجهزة المكلفة بمواجهة الجرائم المعلوماتية وبين مقتضيات حماية حريات الأفراد وحقهم في الخصوصية.

[1]– بوكحيل لخضر، مرجع سابق، ص 33.

كما أن تطبيق القواعد التقليدية التي تحدد معايير الاختصـــاص غير كافية حيث يثير مكان ارتكاب الجريمة المعلوماتية عدة مشـــاكل بســـبب اختلافه عن مكان ارتكاب الجرائم العادية باعتبار هذا النوع من الجرائم المستحدثة تتجاوز حدود الدولة الواحدة.

– القواعد الاجرائية التقليدية وضـــعت في الأصـــل لمكافحة الاعتداءات المادية، والجرائم المعلوماتية ذات طبيعة خاصـة غير ملموسـة، اضـافة الى أن القواعد التقليدية تتميز بانعدام أو ضـعف الاسـتجابة لمتطلبات ضـبط الجرائم المعلوماتية وجمع الأدلة والبحث عن مرتكبيها وايقافهم وتقديمهم للعدالـة؛ كما ان الأجهزة المكلفة بالتحقيق لا يمكنها مباشـــرة الاجراءات التقليدية في بيئة افتراضـــية وخاصـــة في حالة تفتيش الشـــبكات أو عمليات اعتراض الاتصـــالات، حيث أن مختلف المعلومات تكون في شـــكل نبضـــات الكترونية ذات طبيعة معنوية.[1]

ثالثا: جزاء تجاوز القواعد الشرعية عند التحقيق في الجرائم المعلوماتية

يعتبر الجزاء الاجرائي عصـــب القانون الاجرائي، ومن بين الجزاءات الاجرائية نجد نظرية البطلان، حيث أن البطلان يعتبر أداة ضـــرورية لترشـــيد الاجراءات وذلك بهدف الوصـــول الى عدالة فعالة، وبالتالي لابد من تنفيذ وتطبيق النصـــوص الاجرائية بطريقة صـــحيحة وأن يكون العمل الاجرائي صـــحيح ومنتج لآثاره القانونية، تفاديا لاعتباره معيبا أو سقوطه في البطلان.

كما تعتبر نظرية البطلان أداة لتبصـــير الاجراءات حيث تطورت هذه النظرية بتطور حقوق الدفاع وحماية الحريات الفردية، ولها أهمية في مرحلة التحقيق الابتدائي، فأي عمل يقوم به قاضـي التحقيق لابد أن يكون في إطار احترام الضـوابط الاجرائية حماية لحقوق الفرد

[1]– يوسف قجاج، خصوصية القواعد الاجرائية في مجال البحث عن الجريمة الالكترونية (دراسة مقارنة)، منشورات مجلة المنارة للدراسات القانونية والادارية. سلسلة البحوث الجامعية، العدد 14، دار السلام، الرباط، سنة 2016، ص 16.

وعدم المساس بحريته ضمانا لحسن سير العدالة، ولابد من اقامة توازن بين حماية حقوق الدفاع من جهة وحسن سير العدالة من جهة أخرى.

فإضافة الى السلطات الممنوحة لقاضي التحقيق من شأنها المساس بحريات الافراد كان لابد أن يقيد المشرع هذه الاجراءات و يحيطها بضمانات تكفل احترامها ولا يكون ذلك الا بتقرير البطلان على اي اجراء مخالف، و نظرا لأهميته نظمه المشرع في قسم خاص في ق ا ج –القسم العاشر في بطلان اجراءات قاضي التحقيق– الا أنه رغم وجود النصوص القانونية التي تنظمه الا أن التطبيق العملي قليل و مؤسف ولعل ذلك يرجع لملل المحامين في الدفع به أمام تقاعس القضاة عن الاخذ به، و عليه يمكن القول أن العمل بالبطلان يعود الى شخصية القاضي و شجاعته في الأخذ به.[1]

ولابد من الاشارة أن الاجراءات الباطلة يمتد بطلانها الى الاجراءات اللاحقة، وتأسيسا على ذلك نصت المادة 170 من قانون الاجراءات الفرنسي قبل تعديلها بالقانون رقم 93 /2 الصادر في يناير 1993 تنص على أن البطلان يلحق الاجراء المعيب والأعمال التالية له، وبالتالي يتعين استبعادهما معا طالما أن الدليل الثاني يرتبط بالأول ويترتب عليه. ويترك لقاضي الموضوع تقدير ما إذا كان الاجراء الباطل يمتد الى الاجراءات اللاحقة عليه أم أن نطاق البطلان يقتصر على الاجراء المعيب وحده، ومع ذلك فان هذه الحرية ليست مطلقة، فالقانون وان اعترف للقاضي بسلطة واسعة في تقدير الدليل الا أنه قيده من حيث القواعد التي تحدد كيفية الحصول عليه وشروطه، ومخالفة ذلك يهدر من قيمة الدليل ويرتب البطلان.[2]

[1]– سامية دايخ، بطلان اجراءات التحقيق الابتدائي في التشريع الجزائري، أطروحة دكتوراه تخصص القانون الاجرائي، جامعة مستغانم كلية الحقوق والعلوم السياسية، سنة 2016–2017، ص 322.

[2]– فهد عبد الله العبيد العازمي، مرجع سابق، ص 404.

الفرع الثاني: القواعد الخاصة بالإثبات في الجرائم المعلوماتية

ان الاصـــل هو حرية الاثبات ومبررات ذلك أن المجرم يتخذ كل الاحتياطات لعدم كشف الحقيقة وعليه يحق للنيابة العامة والقاضـي الجزائي (سواء قاضـي التحقيق أو الحكم) الاستعانة بكل طرق الاثبات. ومن حق المتهم استعمال اي وسيلة مشروعة للإثبات لتحضير دفاعه ولتحقيق التوازن بين الحريات الفردية (حقوق الدفاع) وبين المصـــلحة العامة (اظهار الحقيقة) حق الاعتراف لجهة الادعاء والتحقيق والمحكمة بالاســـتعانة باي وســـيلة لإثبات الجريمة. الا ان المشرع قيد حرية الاثبات في بعض الجرائم،[1] وعليه لا يمكن للقاضي مخالفة القواعد المقررة قانونا، وإذا خالف النص الذي يقيده على الدفاع ابداء النص المخالف قبل الفصل في الموضوع كدفع أولي، غير أن الاثبات يقيد بمبدأ شرعية الاثبات ومبدأ مشروعية الدليل.

أولا: مبدأ شرعية الاثبات في الجرائم المعلوماتية

ان من مسـتلزمات مبدأ شـرعية الاثبات أن يقترن هذا الاخير بقيم العدالة واخلاقياتها ومقتضـــيات الكرامة الانســـانية، وبالتالي لا يجوز قبول اي دليل الكتروني يتم بطرق غير مشـروعة (كالتعذيب والاكراه وتحريض اعوان الشـرطة والقضـاء، الاسـتجواب المرهق ونية الخداع فيه، التسجيل الصوتي والتنصت (ماعدا احوال المادة 65 مكرر من قانون الاجراءات الجزائية الجزائري)، التنويم المغناطيسي، جهاز كشف الكذب ...وغيرها).

[1]– نص المادة 212 قانون اجراءات جزائية: " يجوز اثبات الجرائم باي طريق من طرق الاثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه طبقا لاقتناعه الشخصي".

ولكي ينتج هذا المبدأ أثره لابد من اقتران مبدأ شـرعية الاثبات بمبدأ المشـروعية، فاذا كانت ادلة الادانة مقترنة بمبدأ الشـــرعية، فأدلة البراءة غير مقيدة بمبدأ الشـــرعية (مبدأ عدم جواز تقييد المتهم في الدفاع عن نفسه) اذ لا يضر العدالة تبرئة مذنب بقدر ما يضرها ادانة بريء ويبقى الشك يفسر لصالح المتهم.

ثانيا: مشروعية الدليل الالكتروني في الاثبات

تعددت التعاريف الموضحة لمفهوم الدليل الالكتروني نذكر منها:

الدليل الالكتروني هو الدليل المشـــتق من أو بواســـطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال اجراءات قانونية وفنية، لتقديمها للقضـاء بعد تحليلها علميا أو تفسـيريا في شـكل نصـوص مكتوبة، أو رسومات أو صور وأشكال وأصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الادانة فيها.[1]

وهو الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شـــكل مجالات ونبضـــات مغناطيسية أو كهربائية، من الممكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصـة في شـكل صـور أو تسـجيلات صـوتية أو مرئية، ويتم تقديمها في شـكل دليل يمكن اعتماده أمام القضاء.[2]

وهو المعلومات المخزنة أو المنقولة في شكل ثنائي والتي قد يمكن الاعتماد عليها في المحكمة.[3]

---

[1]– عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الاثبات الجنائي بالأدلة الرقمية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، الرياض، 2007، ص 13.

[2]– ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006، ص 88.

[3] -Lazetik G B, Koshevaliska O, Digital Evidence in Criminal Procedures(A comparative approach), Balkan Social Science Review, 2 (1), 2013, p16.

وهو الدليل الذي يحتاج الى معالج رقمي لقراءته أو فهم محتواه.[1]

من التعاريف السابقة نعرف الدليل الالكتروني على أنه بيانات ومعلومات رقمية مستمدة من الأجهزة الالكترونية وشبكات الاتصال، تكون في شكل نبضات مغناطسية أو كهربائية، فيمكن من خلالها تسهيل قراءته وكشف محتواه لتقديمه للقضاء كدليل لإثبات الجريمة.

-ان العبرة في الاثبات هي الاحتكام الى دليل يؤكد ارتكاب المتهم للجرم المنسوب اليه، ويجب أن يكون هذا الدليل مشروعا ومتحصلا عليه بطرق مشروعة.

1-مشروعية وجود الدليل الالكتروني

عرف القانون المقارن ثلاثة نظم للإثبات أولها نظام الاثبات المقيد وثانيها نظام الاثبات المعنوي أو الحر، وآخرها نظام الاثبات المختلط، ودون الخوض في تفاصيل كل هذه الانظمة، نشير الى أن اغلب التشريعات الجنائية الحديثة أخذت بنظام الاثبات الحر ومنها -التشريع الجزائري والمصري والفرنسي-، ومبدأ حرية الاثبات هو ميزة من مميزات النظرية العامة للإثبات في القانون الجنائي.[2]

باختلاف الأنظمة يختلف موقفها من الأدلة التي تقبل كأساس للحكم بالإدانة، حسب الاتجاه الذي تتبناه، فوفقا لنظام الاثبات الحر، يتمتع القاضي الجزائي بحرية مطلقة في اثبات الوقائع، و يختار من بين ما يطرح عليه ما يراه صالحا للوصول الى الحقيقة، و على اساسها يقبل الدليل أو يرفضه، في حين أن المشرع لا يتدخل في تحديد القيمة الاقناعية للدليل، ففي هذا النظام للقاضي دور ايجابي في مجال الاثبات، و عليه لا تثور مشكلة مشروعية الدليل الالكتروني من حيث الوجود، و تبقى مسألة قبول الدليل الالكتروني يخضع

[1]- حازم محمد حنفي، مرجع سابق، ص 09.

[2]-بوكحيل لخضر، مرجع سابق، ص 42.

للتقدير القضائي، فالأصل في الأدلة مشروعية وجودها، و الدليل لابد أن يكون مشروعا من حيث الوجود[1]

2-مشروعية تحصيل الدليل الالكتروني:

مشـروعية تحصـيل الدليل الالكتروني، تتطلب الصـدق في مضـمونه، و ذلك باتخاذ اجراءات تتفق و القواعد القانونية و الانظمة الثابتة في وجدان المجتمع المتحضر،[2] حيث أن الدليل غير المشـروع لا يقبل في الاثبات الجنائي ولا يدخل في عناصـر الاثبات التي يبني عليها القاضـي تقديره، و يعتبر الدليل غير المشروع دليلا متحصـلا عليه على حساب قيم و اخلاقيات العدالة من جهة و على حساب الحفاظ على الكرامة الانسانية للشخص و حقه في الدفاع من جهة اخرى (كالحصـول على الاعتراف بالتهديد و الاكراه المادي) وبالتالي يقع باطلا كل دليل الكتروني متحصـل عليه بطرق غير مشـروعة أو مخالفة للقانون، أو جاء نتيجة اجراء جنائي تخلفت كل أو بعض شروطه.

ومن أمثلة الطرق غير المشـروعة التي يمكن ان تسـتخدم في الحصـول على الدليل الالكتروني، اكراه المتهم المعلوماتي (ماديا أو معنويا) من اجل الافصـاح عن مفاتيح الشـفرة أو كلمات المرور للولوج داخل النظام المعلوماتي الخاص به، أو الاسـتجوابات المنهكة لقوى المتهم المعلوماتي كأن يستدعى للتحقيق معه لمدة طويلة، كذلك تتسم بعدم المشروعية أعمال التحريض على ارتكاب الجرائم المعلوماتية كالتحريض على التجسـس المعلوماتي أو المراقبة الالكترونية كمراقبة البريد الالكتروني والاتصالات الالكترونية دون اذن.[3]

[1]- خالد عياد الحلبي، مرجع سابق، ص 128.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 361.

[3]- محمد كمال شاهين، مرجع سابق، ص 372.

و لا يمكن اعتماد تسجيل الاصوات دون اذن من السلطة المختصة كحجة ، وتأسيسا على ذلك قضـــت محكمة التعقيب في تونس برفض التســـجيل الصـــوتي المنجز دون اذن السـلطة المختصـــة لا يمكن اعتماده كدليل ادانة[1] كما أن اي دليل ناجم عن اجراءات تتعامل مع منطقة اللاوعي أو الوعي كالتســجيل الصــوتي او الضــوئي او التنصــت، أو اي دليل الكتروني متحصــل عليه من افشــاء للســر المهني يعد باطلا حتى ولو كان صــادقا او كان نتيجة اسـتعمال طرق قانونية كاعتراض المراسـلات و تسـجيل و مخالف للقانون، وتأسـيسـا على ذلك فالتسـجيل الهاتفي بطريقة غير مشـروعة و دون علم صـاحبها، ليس دليل يسـتند عليه في الاثبات (يفقد حجيته في الاثبات)، في هذا الاطار أصـــدرت محكمة النقض الفرنسـية قرار يقضـي بأن تسـجيل المكالمات الهاتفية بطريقة غير مشـروعة يؤدي الى عدم قبوله كدليل، وذلك تأســيســا على المادة 06 الفقرة الأولى من اتفاقية المحافظة على حقوق الانسـان و الحريات الأسـاسـية (حيث أن تسـجيل مكالمة هاتفية من قبل أحد الأطراف دون علم صاحب الأقوال يشكل وسيلة ماكرة، مما يمنع قبول تقديمه كدليل)[2].

حيث أن الاستعانة بأدلة غير مشروعة في الاثبات من الممكن ان تكون جريمة بذاتها او على الاقل اســـاليب احتيالية تمس بحقوق الدفاع ولا تقبل الادلة إذا لم تحترم القواعد الموضوعية والشكلية التي قررها المشرع.

مسألة التسجيل في الاماكن العامة ليس له قوة ثبوتية الا بمرجعية القاضي فهو مجرد دلائل يمكن تعزيزها بغيرها من الأدلة.

[1]– قرار تعقيبي صادر عن محكمة التعقيب بتونس، عدد 6811، الصادر بتاريخ 22.02.2007.

[2]– قرار محكمة النقض الفرنسية، الغرفة التجارية، رقم الطعن: 07-17147 07-17196، بتاريخ 3 يونيو 2008. منشور في النشرة

ثالثا: عبء الاثبات في الجرائم المعلوماتية

ان اثبات الركن المادي للجريمة واسنادها لمرتكبها يقع على سلطة الاتهام وهي بصفة اصـــلية النيابة العامة ولابد ان تبين عند المتابعة الأدلة التي من شـــأنها اثبات قيام اركان الجريمة وعدم وجود عذر معفي أو أحد اسـباب انقضـاء الدعوى العمومية، ويمكن للمتهم ان يقدم دفوعا وإذا تمسـك او ادعى وجود وسـائل الدفاع لصـالحه مرتبطة بالدعوى مثل سـبب اباحة، موانع العقاب، سبب لانقضاء الدعوى يتحول المتهم الى مدعي يقع عليه عبء اثبات ما يدعيه اســتنادا الى قاعدة البينة على من ادعى. ان دور النيابة العامة هو اظهار الحقيقة بقصـــد ادانة المذنب او تبرئة البريء، لذلك خول لها قانون الاجراءات الجزائية صـــلاحيات وامتيازات واســـعة تجعل منها طرفا ممتازا في الخصـــومة الجنائية حيث تعتبر وكالة باســـم المجتمع.

و قد تلعب هذه السلطة دورا مهما، في حالة ما اذا كانت الدعوى قد رفعت بواسطته، و في هذه الحالة لابد من اثبات عناصـر الجريمة، و رابطة السـببية التي تربط بين السـلوك الاجرامي و النتيجة الاجرامية، فسـلطة الاتهام كما يقول الفقيه الفرنســي PATARIN) ليســت مجرد مدع عادي، بل هي تحمي البريء كما تحمي المتهم، ولذلك يجب عليها جمع عناصـر الاثبات التي في صـــالح المتهم اذا ظهرت لها، و تقدمها الى القضـــاء لأنها باعتبارها نائبة عن المجتمع تهتم ببراءة البريء و ادانـة المتهم، لـذلـك على النيـابـة العـامـة اثبـات جميع العناصر المكونة للجريمة.[1]

كما يقع عبء الاثبات على الطرف المدني عندما يبادر بتحريك الدعوى العمومية أو عندما يتأسس بعد تحريك الدعوى العمومية.

[1]– طاهر محمود أبو القاسم، الجرائم المعلوماتية، مرجع سابق، ص 133.

الفرع الثالث: القيمة الاقناعية للدليل الالكتروني في الاثبات الجزائي

ان دور القاضـــي في البحث عن الدليل الجزائي التقليدي يختلف عن دوره في الجرائم المعلوماتية، وذلك لارتكاب هذه الاخيرة في وسـط افتراضـي وبالتالي الحصـول على الدليل الالكتروني وتقديمه للقضـــاء لا يكفي لاعتماده كدليل ادانة، اذ ان الطبيعة الفنية لهذا الدليل تمكن من العبث في مضـــمونـه على نحو يحرف الحقيقـة، دون أن يكون في قـدرة غير المتخصص إدراك ذلك العبث، ولذلك تثور فكرة الشك في مصداقيته كدليل اثبات جزائي.[1]

أولا: شروط قبول الدليل الالكتروني في الاثبات

ليعد الدليل الالكتروني أساسا يستند عليه للوصول الى الحقيقة في الدعوى يتطلب توفر شرط اليقين والمناقشة.

1-يقينية الدليل:

ان جميع قواعد الاثبات الجنائي تهدف الى البحث فيما إذا كان من الممكن أن يتحول الشـك الى يقين، فالاتهام يبدأ في صـورة الشـك فيما إذا كان شـخص ما قد ارتكب الجريمة وأصبح مسؤولا عنها، وتستهدف قواعد الاثبات تمحيص هذا الشك وتحري الوقائع التي انبعث عنها، والقول في النهاية بما إذا كان قد تحول الى يقين تبنى عليه الادانـة، وإذا لم يفلح في ذلك، يبقى الشك على حاله، ومن ثم تستحيل الادانة.[2]

وحتى يتحقق اليقين لدى سـلطة التحقيق أو القاضـي الجنائي في الجريمة المعلوماتية، لابد أن يكون الدليل الالكتروني ذا علاقة بموضوع الجريمة، وهذا الشرط يشار اليه في قانون

[1]- مليكة أبو ديار، الاثبات الجنائي في الجرائم الالكترونية، المجلة الالكترونية للأبحاث القانونية، العدد 2، المغرب، 2018، ص 107.

[2]- طاهر محمود أبو القاسم، مرجع سابق، ص 133.

الاثبات الفيدرالي الأمريكي بمبدأ العلاقة الكاشـفة بين الدليل والواقعة محل الدعوى، ويسـمى الدليل هنا بالدليل الكاشـف الذي يعرف على أنه: الدليل الذي يملك بذاته غاية محددة ممثلة في قدرته على ابراز حقائق يمكنها التأثير في اتجاه الدعوى الى الحد الذي يمكن ان يحدث تطويرا فيها بحيث لا يمكن حدوث هذا التطور دونها.[1]

2-وجوب مناقشة الدليل الالكتروني:

ان مناقشـة الدليل الالكتروني تسـتلزم أن يكون الدليل ذاته يصـلح للمناقشـة بمعنى أن يكون دليلا منتجا في الدعوى، كما يشـترط أن تكون سـلطة التحقيق على دراية بتقنية المعلومات و تكنولوجيا الحاسوب و الانترنت حتى يمكنها طرح الدليل الالكتروني و مناقشته و عرضـه أمام القاضـي الجزائي و امكانية مناقشـة المتهم الخبير المعلوماتي، هذا فضـلا عن ضرورة التدريب الفني للقاضي نفسه خاصة على كيفية التعامل مع تقنية المعلومات و أنظمة معالجة البيانات، و مع الأدلة الناتجة عن الحاسـب و الانترنت، حتى يمكنه فهم و مناقشـة الدليل الالكتروني المطروح أمامه في الدعوى الجنائية.[2]

وقد نص قانون الاجراءات الجزائية الفرنسـي على هذا الشـرط حيث لا يجوز للقاضـي أن يؤسـس حكمه الا على أدلة طرحت عليه أثناء المناقشـات والتي تمت مناقشـتها أمامه في مواجهة الأطراف.[3]

[1]– محمد كمال شاهين، مرجع سابق، ص 374.

[2]– محمد كمال شاهين، المرجع نفسه، ص 376.

[3] – article 427 (Le juge ne peut fonder sa décision que sur des preuves qui lui apportées au cours des débats et contradictoirement discutées devant lui.) CPP - Dernière modification le 02 janvier 2021 - Document généré le 01 février 2021 Copyright (C) 2007-2021 Legifrance.

وهو نفســـه ما أخذ به المشـــرع الجزائري بموجب المادة 212 من قانون الاجراءات الجزائية في الفقرة الثانية، بنصه: " ولا يسوغ للقاضي أن يبني قراره الا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه."

ثانيا: حجية الدليل الالكتروني أمام القضاء الجزائي

ان مجرد الحصـــول على دليل الكتروني وتقديمه للقضـــاء لا يكفي لاعتماده كدليل ادانـة، اذ أن الطبيعـة الفنيـة للدليل الالكتروني تمكن من العبث بمضـــمونـه، ولا يمكن لغير المختص إدراك ذلك العبث، فضـــلا عن ذلك فان نســبة الخطأ في اجراءات الحصــول على الدليل محتملة بدرجة كبيرة، ومن هنا هل يمكن اســـتبعاد الدليل الالكتروني من دائرة ادلة الاثبات الجزائي لتعارضه مع قرينة البراءة؟[1]

لقد أصــبح الفقه الجزائي المعاصــر اليوم ينحاز الى مبدأ حرية القاضـــي في الاثبات حيث يعطى لـه حريـة قبول الدليل وتقدير قيمتـه، ووجود مبدأ حريـة القاضـــي في الاقتنـاع يخفف من عبء الاثبات الذي يقع على عاتق النيابة العامة وفقا لمبدأ قرينة البراءة،

و على اختلاف النظم القانونية التي تأخذ بنظام الاثبات الحر كالقانون الفرنســـي، و المصــري، و الجزائري فالقاضـــي له الســلطة التقديرية في قبول الدليل أو رفضـــه، وفي هذا الاطار جاء في المادة 427 من قانون الاجراءات الجزائية الفرنســـي أن تثبت الجرائم بجميع طرق الاثبات و يحكم القاضـــي تبعا لاقتناعه الشـــخصـــي، و عليه تعد الأدلة الالكترونية ومخرجات الحاســـب الآلي مقبولة في الاثبات الجنائي من حيث المبدأ، و تأكيدا على ذلك قضـى بقبول التسـجيلات الممغنطة، أمام القضـاء الجزائي الفرنسـي و ذلك على أسـاس توافر

[1]– خالد عياد الحلبي، مرجع سابق، ص 246.

عدة شـروط أهمها: الحصـول عليها يكون بطريقة مشـروعة و نزيهة، و أن تتاح مناقشـتها وجاهيا من قبل الخصوم.[1]

وبالنسـبة للنظم التي تأخذ بنظام الاثبات المقيد كالمملكة المتحدة بريطانيا و الولايات المتحدة الأمريكية، حيث لا يمكن في ظلها الاعتراف بأي قيمة اثباتية للدليل الالكتروني، ما لم ينص القانون صـراحة على ذلك ضـمن قيمة أدلة الاثبات، وقد نص قانون الاثبات في المواد الجزائية البريطاني على قبول الدليل الالكتروني و حدد قيمته الاثباتية اتفاقا، وما يعاب على هذا النظام أنه يقيد سـلطة القاضـي فمن الممكن أن يحكم بما يخالف قناعته، فبدأ هذا النظام ينحصـر نطاقه حتى في الدول التي اعتنقته، فنجد بريطانيا مثلا ظهر فيها ما يعرف بقاعدة الادانة دون أدنى شـك، و التي مفادها أن القاضـي يسـتطيع أن يكون عقيدته من أي دليل و ان لم يكن من ضـمن الأدلة المنصـوص عليها متى كان هذا الدليل قاطعا في دلالته.[2]

وقد نص المشرع الأمريكي صراحة على حجية الدليل الالكتروني في الاثبات الجزائي في العديد من القوانين الخاصة، منها قانون الحاسب الآلي الصادر في 1984 في ولاية ايوا حيث نصت المادة 16/1716 على أن مخرجات الحاسب الآلي تكون مقبولة بوصفها أدلة اثبات بالنسـبة للبرامج و البيانات المخزونة فيه، كما اعترف قانون الاثبات الصـادر في 1983 في ولاية كاليفورنيا بحجية الدليل الالكتروني في الاثبات و ذلك باعتبار النسـخ المستخرجة من البيانات التي يحتويها الحاسب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات البيانات، و أكد القضاء الأمريكي ذلك باعتبار الأدلة المستخرجة من الحاسب الآلي و الانترنت يجب أن تكون مقبولة كأدلة اثبات طالما توافر فيهم شرطان: أن يكون الحاسوب

[1]– محمد كمال شاهين، مرجع سابق، ص 380.

[2]– خالد عياد الحلبي، مرجع سابق، ص 237.

المســـتخرج منه الدليل يؤدي وظائفه بصـــورة ســـليمة و أن يتوفر في القائم عليه الثقة و الطمأنينة [1]

أما بالنســبة لنظام الاثبات المختلط (والذي يجمع بين النظام الحر و النظام المقيد)، فيعتمد على أدلة معينة لإثبات الوقائع دون بعضـها الآخر، أو يشـترط في الدليل شـروطا في بعض الأحوال أو يعطي للقاضـــي الحرية في تقدير الأدلة القانونية، مثل القانون الاجرائي الياباني، حيث حصـر المشـرع الياباني طرق الاثبات المقبولة في تصـريحات المتهم، واقوال الشـهود، و القرائن، و الخبرة، أما بالنسـبة لأدلة الحاسـب و الانترنت، فيقرر الفقه الياباني أن السـجلات الالكترو–مغناطيسـية تكون غير مرئية في حد ذاتها، و لذلك لا يمكن أن تسـتخدم كدليل في المحكمة، الا اذا تم تحويلها الى صـورة مرئية مقروءة عن طريق مخرجات الطباعة لمثل هذه الســـجلات، و في مثل هذه الحالة يتم قبول هذه الادلة الناتجة عن الحاســـوب و الانترنت، سواء كانت هي الاصل أن نسخة من هذا الاصل.[2]

وتجدر الإشارة الى أن بعض الفقه اليوناني وسايره البعض من الفقه المصري يلجؤون الى حيلة للتوصـــل الى إمكانية قبول الأدلة المســتمدة من الحاســب في اثبات وقائع الدعوى المتعلقة بالجرام المعلوماتية من خلال التفرقة بين وســـائل الاثبات وطرق الاثبات، فيرون أن الأولى محددة على سبيل الحصر، في حين أن الثانية متنوعة وتتزايد باستمرار.[3]

ثالثا–موقف القاضي من اخضاع الدليل الالكتروني للتقييم الفني:

تســـاهم الوســـائل التقنية في ارســـاء مبدأ الحق في الاثبات لدورها في جمع الادلة الالكترونية وعرضـــها امام القاضـــي المختص، بكافة مفرداتها وعناصـــرها ليختار منها ما

[1]– محمد كمال شاهين، مرجع سابق، ص 384.

[2]– فهد عبد الله العبيد العازمي، مرجع سابق، ص 377.

[3]– لينا محمد الأسدي، المرجع السابق، ص 110.

يتلاءم مع ظروف الدعوى، ومواجهة الاطراف بالأدلة المخزنة سواء في صورة مخرجات ورقية أو وسائط ممغنطة أو رسائل الكترونية أو برقيات تبادلها عن طريق الفاكس والتلكس، لإظهار الحقيقة أمام القاضي لتسهل مهمته في الاثبات وتمكنه من اصدار حكمه باقتناع ويقين[1]

ان الاقتناع الشخصي للقاضي لابد أن يكون مبنيا على الوعي الذي يخضع فيه لقواعد المنطق و عقليا متطابقا مع الحقيقة الواقعية، كما أن اقتناعه بالإدانة يجب أن يكون على درجة من اليقين الذي يخلو من الشك، و ذلك لعدم اهدار مصلحة المتهم المتوفرة في مبدأ قرينة البراءة، و من حيث الدرجة اللازمة للإثبات فاليقين القضائي يتقرر من خلال الضمانة الثابتة للمتهم، و تكمن في درجة الاثبات التي ينبغي أن يدركها القاضي حتى يتمكن من اعلان مسؤولية المتهم، غير أن الظن يتعارض مع اليقين حيث أن الاقتناع في العقل لا يؤسس على فكرة الظن بل على الأدلة الموضوعية وعلى يقين قائم على تسبيب يقيني، و بالتالي فحرية القاضي في الاقتناع ليست مطلقة لأن الاقتناع المطلوب في المواد الجنائية هو الاقتناع العقلي المؤسس على أكبر قدر من اليقين، و بالتالي تقيد حرية القاضي في الاثبات، حيث أن مبدأ مشروعية الدليل هو قيد حقيقي لأن الدليل المقبول يجب أن يكون مشروعا تطبيقا للمبادئ التي تلزم القاضي الجنائي أن لا يأخذ الا بالإدانة المشروعة.

وعليه يجب أن تكون عقيدة القاضي و اقتناعه بالإدانة مستمدا من أدلة الكترونية تم الحصول عليها بطرق قانونية، و ليس بناء على معلوماته الشخصية أو على ما قد يكون رآه بنفسه، لأن القاعدة أن لا يحكم الا بناء على التحقيقات، كما ينبغي أن لا يؤسس القاضي الجزائي حكمه على دليل ناتج عن حاسب الكتروني لحقه سبب يبطله و يعدم أثره، ففي القانون الفرنسي نجد أن الاثبات الجزائي حر شرط أن يكون الحصول عليه مشروعا، فرغم

[1]– فهد عبد الله العبيد العازمي، مرجع سابق، ص 389.

أن قانون الاجراءات الجزائية الفرنسي لا يتضمن أية نصوص تتعلق بمبدأ الامانة و النزاهة في البحث عن الحقيقة القضائية، الا أن الفقه و القضاء كانا بجانب هذا المبدأ سواء في التنقيب عن الجرائم التقليدية أو في مجال الجرائم المعلوماتية، كأن يستخدم رجال الشرطة طرق معلوماتية للتنصت على المحادثات التلفونية، لذا يشير أحد الفقهاء أن القضاء قد قبل استخدام الوسائل العلمية في البحث و التنقيب عن الجرائم الا أنه أكد على أن يكون الحصول عليها بطرق مشروعة.[1]

ويعتبر الشك في الدليل الالكتروني غير متعلق بمضمونه كدليل، وانما بعوامل مستقلة عنه، ولكنها تؤثر في حجيته، ومثلما يخضع الدليل الالكتروني لقواعد معينة تحكم طرق الحصول عليه، فانه يخضع لقواعد اخرى للحكم على حجيته الاثباتية، وذلك يرجع لطبيعته الفنية، فهناك وسائل فنية من طبيعة الدليل تمكن من فحصه للتأكد من سلامته وصحة الاجراءات المتبعة في الحصول عليه، وهذا الدليل الالكتروني بوصفه دليلا علميا فان دلالته قاطعة بشأن الواقعة المستشهد به عنها، وإذا سلمنا بإمكانية الشك في سلامته بسبب قابليته للعبث ونسبة الخطأ في اجراءات الحصول عليه، فتلك مسألة فنية القول فيها لأهل الخبرة، فيجب عدم الخلط بين الشك الذي يشوب الدليل الالكتروني بسبب إمكانية العبث فيه أو لوجود خطأ في الحصول عليه وبين القيمة الإقناعية لهذا الدليل، فاذا سلم الدليل من العبث والخطأ فلا يمكن للقاضي التشكيك في حجيته في الاثبات.[2]

حيث أن الخبرة تحتل دورا كبيرا في التثبت من صلاحية الدليل الرقمي، وتزيد من أهمية الدليل العلمي في الاثبات الجنائي، كما تزيد من اهمية دور القاضي الجزائي في الاثبات بحيث يبقى متمتعا بسلطته التقديرية في تقدير الأدلة بحسبان أنها قد لا تكون مؤكدة

[1]– فهد عبد الله العبيد العازمي، مرجع سابق، ص 362.

[2]– خالد عياد الحلبي، مرجع سابق، ص 248 ص 252.

على سبيل القطع أو قد تكون مجرد امارات أو دلالات وقد يحيط بها الشك، وهنا تظهر أهمية السلطة التقديرية لأنه من خلالها تظهر مواطن الضعف في قرائن وأن الشك يفسر لصالح المتهم.[1]

المطلب الثاني: الحق في الخصوصية المعلوماتية

في عام 1973 اعتمدت السويد قانون البيانات (Datalag). وفي العام التالي تبنت الولايات المتحدة قانون الخصوصية، وتعد فرنسا من أوائل الدول التي أدركت أن الخصوصية، مثل الحريات، يمكن أن تتعرض للخطر بواسطة أجهزة الكمبيوتر. اعتبارًا من 1970/1969، في التقرير السنوي لمجلس الدولة، تساءل المدعي العام حول "عواقب تطوير معالجة البيانات على الحريات العامة والقرارات الإدارية". وفي عام 1974، أنشأت لجنة لتقديم المقترحات في هذا الشأن. وكانت هذه المقترحات هي أصل قانون 6 يناير 1978 المسمى "الحوسبة والحريات"، والذي تم تعديله عدة مرات منذ ذلك التاريخ واستكمل بمراسيم مختلفة.[2]

الفرع الأول: ماهية الحق في الخصوصية المعلوماتية

لقد كرست معظم الدساتير والقوانين الداخلية للدول في العالم الحق في الخصوصية باعتباره أحد أهم المبادئ التي تحكم المجتمع، ومن بينها الدستور الجزائري ضمن الباب

---

[1]– مليكة أبو ديار، مرجع سابق، ص 108.

[2]– الغرض الرئيسي من القانون، الذي يُعهد بتطبيقه إلى سلطة إدارية مستقلة، اللجنة الوطنية لحماية البيانات (2) (CNIL)، هو التحكم في جمع ومعالجة واستخدام المعلومات والبيانات "الاسمية"، أي تلك التي تسمح بأي شكل من الأشكال، بشكل مباشر أو غير مباشر، بتحديد الأشخاص الطبيعيين الذين تنطبق عليهم "

Bertrand A, droit à la vie privé et droit à l’image, Litec, paris, 1999, p 124.

الثاني (الحقوق الأساسية والحريات العامة والواجبات)، في الفصل الأول (الحقوق الأساسية والحريات العامة).[1]

وفي ظل التطورات التكنولوجية الحديثة وبيئة المعلوماتية، أصبح الاعتداء على الحق الخصوصية والحريات من أكثر المخاطر التي تفسد تطوير تكنولوجيا المعلومات[2].

اولا: مفهوم الحق في الخصوصية المعلوماتية

لابد من اجراء دراسة معمقة للقضايا المتصلة بالحماية القانونية الفعالة والضمانات الاجرائية والرقابة الفعالة، لتعزيز الحق في الخصوصية وحمايته في العصر الرقمي من خلال توفير مزيد من التوجيهات العملية، بشأن مبادئ الضرورة والتناسبية والمشروعية فيما يخص ممارسة المراقبة، وبشأن تدابير رقابة فعالة ومستقلة ومحايدة.[3]

1-تعريف الحق في الخصوصية

مازال الفقه والقضاء غير مستقر على تعريف جامع مانع لهذا الحق نظرا لديناميكية مصطلح الخصوصية وارتباطه بالتطورات في مجال التكنولوجيات الحديثة،

[1]- المادة 47 من دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي 96-438، المؤرخ في 07 ديسمبر 1996، ج ر، عدد 76، الصادر بتاريخ 08 ديسمبر 1996، المعدل والمتمم الى غاية المرسوم الرئاسي 20-442، المؤرخ في 30 ديسمبر 2020، ج ر، عدد 82، الصادرة بتاريخ 30 ديسمبر 2020، ص 13.

[2] -Pradel J, Danti-Juan M, droit pénal spécial, 6e édition, éditions Cujas, 2014, paris, France, p 213.

[3]- تقرير مفوضية الأمم المتحدة السامية لحقوق الانسان حول الحق في الخصوصية في العصر الرقمي، الصادر بتاريخ 30 جوان 2014، تحت رقم A/HRC/27/37، ص 16.

وبقصـــد تكييف العدالة مع متطلبات المجتمع الحديث واضـــفاء طابع قضـــائي على العدالة الاجتماعية[1]، تم التطرق على المستوى القضائي لبعض الانتهاكات الماسة بهذا الحق حيث:

حصـــرها القضـــاء الأمريكي في حالة التجســـس على الحياة الخاصـــة (انتهاك خلوة الشخص)، نشر وقائع خاصة، نشر وقائع تشوه الحقيقة في النظر، الحق في عدم استعمال الغير بعض العناصر العائدة له بغرض الحصول على الربح؛

وتعرض القضـــاء الفرنســـي الى: الحياة العاطفية والزوجية والعائلية، الذمة المالية للشخص، الحالة الصحية للشخص، الآراء السياسية، الصورة، قضاء أوقات الفراغ، محل الاقامة، الحياة الوظيفية، الاسم...[2]

أما على المستوى الفقهي:

يعرف الحق في الخصوصية على أنه "حق الفرد في أن يختار سلوكه الشخصي وتصرفاته في الحياة عندما يشارك في الحياة الاجتماعية مع الآخرين".[3]

[1] -Roché S, En quête de sécurité causes de la délinquance et nouvelles réponses, Armand colin, 2003, Paris, France, p 229.

[2]– علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة (دراسة مقارنة)، المكتب الجامعي الحديث، 2019، ص 41.

[3]– محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية (دراسة مقارنة)، ط 1، مركز الدراسات العربية، مصر، 2016، ص 26

والحق في الخصـوصـية في مجال المعلوماتية والانترنت هو "حق الفرد في أن يقرر بنفسه متى وكيف يمكن للمعلومة الخاصة به أن تصل الى الغير عبر الانترنت، ومنها رقمه السري، رقم بطاقته الالكترونية، عقود الشراء عبر الخط".[1]

كما أن هذا الحق غير محصـور في الفرد فحتى المجموعات والمؤسـسـات لهم الحق في أن يحددوا لأنفسـهم متى وكيف والى أي مدى يمكن للمعلومات الخاصـة بهم أن تصـل للآخرين.[2]

ويرى البعض أن خصـوصـية المعلومات: هي حق الفرد في ضـبط عملية جمع المعلومات الشـخصـية عنه، وعملية معالجتها آليا، وحفظها وتوزيعها واسـتخدامها في صـنع القرار الخاص به والمؤثر فيه، سـواء وضـعت هذه المعلومات في بنوك المعلومات، أو في البريد الالكتروني أو على مواقع التواصل الاجتماعي.[3]

وتتضـمن خصـوصـية المعلومات القواعد التي تحكم جمع وادارة البيانات الخاصـة كمعلومات بطاقات الهوية، المعلومات المالية، السجلات الطبية والسجلات الحكومية، وهناك خصوصية الاتصالات التي تعطي سرية وخصوصية للمكالمات الهاتفية والبريد اضافة الى الخصوصية المادية التي تعطي حماية جسدية للأفراد كفحص الجينات وفحص المخدرات.[4]

---

[1]– فتحي بن جديد، حماية الحق في الخصوصية أثناء التعاقد عبر الانترنت، مجلة القانون، العدد الثالث، 2012، ص 265.

[2]– خدوجة الذهبي، حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 08، المجلد الأول، 2017، ص 143.

[3]– سوزان عدنان، انتهاك حرمة الحياة الخاصة عبر الانترنت (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد 03، 2013، ص 433.

[4]– محمد نصر محمد، مرجع سابق، ص 24.

وما نلاحظه أنه نظرا لعدم وجود تعريف جامع مانع فيبقى بذلك المجال مفتوح لوضع تعريفات تتماشى مع التطورات الحاصلة في مجال التكنولوجية الحديثة، وبإيجاز يمكن تعريف الحق في الخصوصية المعلوماتية بأنه حق كل فرد أو مؤسسة أو مجموعة في المحافظة على أي معلومة شخصية مرتبطة بخصوصيتهم وعدم السماح للغير بالتطاول على هذه الحق.

ثانيا: نطاق الاعتداء على الحق في الخصوصية المعلوماتية

يمكن تحديد نطاق الاعتداء على الحق في الخصوصية في عدة مواضع.

1-في شبكات التواصل الاجتماعي:

تحوز شبكات التواصل الاجتماعي (مثل Facebook، Twitter، Linkedin، Instagram) عدة معلومات حول الاشخاص المستخدمين، ومن بينها معلوماتهم الشخصية من هوية، اقامة، منطقة، اصدقاء، ميول، افكار، توجهات، نشاطات وتفاعلات، وكذا ادوات الاتصال والمراسلة من رسائل على التطبيقات او ربط للبريد الالكتروني، وكذا الهاتف، واستخدام تقنيات الفيديو، فان نقاط الاتصال والدخول الى هذه الشبكة تعد عملية مراقبة مستمرة وتسجيل دائم يتبع المستخدم.[1]

مازال موضوع الخصوصية عبر وسائل التواصل الاجتماعي يثير العديد من الاشكالات، ولم يستقر الاجتهاد حول العديد من المسائل، خاصة ما تعلق بالملكية والقيمة

[1]- عبد الوهاب جعيجع، الامن المعلوماتي وادارة العلاقات الدولية، دار الخلدونية، الجزائر، 2017، ص123.

التجارية للبيانات الشـــخصـــية المتداولة عبر مواقع التواصـــل الاجتماعي، وامكانية تعارض الحق في الخصوصية مع حرية التعبير والحق في الوصول الى المعلومة.[1]

كما أن شبكات التواصل الاجتماعي تملكها شركات تجارية خاصة، وأرباحها تأتي من جمع بيانات الأفراد وبيعها عادة الى شـــركات دعاية، وبالتالي كل ما يتعلق بالمعلومات الشخصية والبيانات وكل ما يدور من حياة خاصة أو عامة أو صور وفيديوهات يقوم الفرد بإنزالها عبر الموقع تكون معرضة لمخاطر الخصوصية، والسبب في ذلك الخوادم التي تحفظ ارقام IP، والكوكيز التي تحفظ معلومات حول المستخدم، هذا عدا مزود خدمة الانترنت التي تمر كل المعلومات القادمة والمرسلة من المستخدم عبره.[2]

2-في وسائل الاتصال الالكترونية

أصـــبح البريد الالكتروني لغة تخاطب آنية وهي أكثر وســـائل الاتصـــال الالكترونية شيوعا في عصرنا الحالي، ويقدر عدد الرسائل الالكترونية التي يتبادلها المستخدمون عبر الانترنت بنحو 110 مليار رسالة سنوية، اما بالنسبة لحجم المعلومات التي تسري ضمن البريد الالكتروني المتنقل في بيئة الفضـــاء المعلوماتي، فقد بلغ حجم الرســـائل اليومية نحو 1829 تيرابايت، مما يعني ان حجمها السنوي سيبلغ قرابة 3.35 بيتابايت [3]

يعتبر البريد الالكتروني أحد الوســـائل الحديثة في المعاملات الالكترونية التي تقدمها شبكة الانترنت، عن طريق التبادل الفوري للرسائل، وبهذا يعد اختراق البريد الالكتروني من أهم المخاطر التي تواجه الحق في الخصوصية، وتعرض الفرد الى انتهاك سرية المعاملات

[1]- مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، المجلد السابق، العدد 13، الجزائر، 2018، ص 477.

[2]- محمد نصر محمد، مرجع سابق، ص 52.

[3]- عبد الوهاب جعيجع، مرجع سابق، ص 107.

والمراســـلات التي تدخل في شـــتى المجالات، ولهذا من المقرر وفقا للقواعد العامة تكريس ضـمانات لحماية سـرية المراسـلات في حدود وضـوابط معينة بغض النظر عن الأسـاليب المستخدمة سواء تقليدية أو حديثة[1]

3-في محركات البحث

في ظل انتشـار المعاملات التجارية الالكترونية، أصـبحت معظم الشـركات تلجأ الى جمع البيانات الشـخصـية عبر مواقعها على شـبكة الانترنت، دون التصـريح عن الغرض من ذلك، كما لا تلتزم بإشـعار المسـتخدمين بالتجميع عن طريق بيان سـياسـة الخصـوصـية التي يفترض أن تكون في الموقع، كما تقوم محركات البحث(Google مثلا) بجمع أكبر قدر من البيانات الشـــخصـــية بما في ذلك عناوين بروتوكولات الانترنت IPو طلبات البحث، ومن الممكن تحديد هوية و معتقدات الشـخص أو ميوله الجنسـي، وفي هذا الخصـوص قضـت محكمة الدرجة الأولى في باريس بتاريخ 06 نوفمبر 2013 بالزام Google، بالاســتناد الى الحق في حرمة الحياة الخاصـــة، بوقف عرض صـــور تكشـــف الحياة الجنســـية لأحد الأشخاص.[2]

4-في المعاملات التجارية الالكترونية

ان انتشـــار المعاملات التجارية الالكترونية كبيع وشـــراء أو عرض الخدمات و المعلومات قد تشكل مساسا بالحق في الخصوصية، فهي من جهة تتطلب الثقة بين التاجر و الزبائن: خاصة عند تقديم رقم بطاقة الاعتماد أو معلومات شخصية أو عنوان البريد، ومن جهة قد يتم الاسـتيلاء و الاسـتغلال غير المشـروع لهذه البيانات، مما يجعل هذه المعاملات مصدر آخر للخطر الذي يتهدد الحياة الخاصة، كما أن وسائل الدفع هي مصدر أخطر، لما

[1]- خدوجة الذهبي، مرجع سابق، ص 149.

[2]- مفيدة مباركية، مرجع سابق، ص 468.

قد يقابل سرعة المعاملات المالية من تهديد لسرية هذه المعاملات، وقد تستخدم البيانات الشخصية للمتعامل لأغراض اجرامية من خلال تداولها مع مؤسسات مالية و مقدمي السلع و الخدمات و الوسطاء حيث يتم الاستيلاء عليها. [1]

5-في قواعد بيانات الحاسب

بظهور الحكومة الالكترونية، أصبح تسيير مختلف المؤسسات يتم عبر الانظمة المعلوماتية، مما يتطلب تبني قواعد البيانات التي تحتوي على بيانات شخصية تعود لعمال أو موظفين أو تلاميذ، أو مرضى، أو متابعين قضائيا في المحاكم، وهي كلها بيانات تستوجب الحماية.[2]

كشفت انترنت الاشياء عن عدد كبير من المخاطر –من بينها ما يتعلق بالخصوصية– اضافة الى المخاطر و التحديثات الأمنية التي قد تستهدف الكثير من الأجهزة و الانظمة الأساسية بالإضافة الى أنظمة التشغيل و الاتصالات، لذا من الضروري ايجاد تقنيات حديثة و مبتكرة لأمن الشبكات و الأجهزة المتصلة لحمايتها من الهجمات التي تستهدف البيانات و المعلومات، و أن تقوم هذه التقنيات بتشفير جميع الاتصالات للتصدي للتحديات الجديدة المتمثلة في انتحال هوية الأشياء أو الهجمات التي تستنزف استهلاك البطاريات، و في رؤيا مستقبلية حول حماية البيانات و المعلومات، فمن المتوقع ظهور تهديدات جديدة و هو ما يحتم تحديث البرمجيات و الهاردوير الخاص بهذه الأجهزة حتى تعمل بكفاءة طول مدة خدمتها.[3]

[1]– صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل، المجلد 24، عدد 02، عنابة، 2018، ص 130.

[2]– مفيدة مباركية، مرجع سابق، ص 466.

[3]– أحمد محمد عبد الباقي، الانترنت–التكنولوجيا وجرائم المستقبل، مرجع سابق، ص 551.

الفرع الثاني: أوجه الحماية الجزائية للحق في الخصوصية المعلوماتية

ان أهم أوجه الحماية الجزائية للحق في الخصوصية المعلوماتية تتجسد من حيث حماية حرمة الحياة الخاصة للأشخاص وحرمة شرفهم، وسرية اتصالاتهم ومراسلاتهم، إضافة الى حماية معطياتهم الشخصية.

أولا: عدم جواز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه

وفي هذا السياق فتهديد الأشخاص و الابتزاز عبر الانترنت (خاصة عبر مواقع التواصل الاجتماعي) يعتبر من صور الاعتداء على الحق في الخصوصية، و مواجهته هي محل اشكال في القانون الجزائري، الذي مازال متأخرا في اصدار قواعد خاصة تحكم هذه الأمور، لكن هذا لا يعني افلات المجرم من العقاب، فعلى المستوى القضائي تعالج هذه الجرائم وفقا لأحكام قانون العقوبات، حسب الغاية أو الهدف من الجرائم المرتكبة، فاذا استهدفت الجريمة تهديد الأشخاص و ابتزازهم، هنا يمكن المتابعة وفقا لأحكام قانون العقوبات وفقا للمواد من 284 الى 287 قانون عقوبات[1]، التي تعاقب على جنحة التهديد، كما قد يكون قاصدا بذلك الاعتداء على حرمة الحياة الخاصة، بالتقاط أو تسجيل، أو نشر صور أو احاديث خاصة، وفي هذه الحالة يمكن المتابعة وفقا لأحكام المادة 303 مكرر قانون عقوبات، التي تعاقب بالحبس من 6 أشهر الى 3 سنوات و غرامة من 50.000 دج الى 300.000 دج.

كما يحدث الاعتداء على الحياة الخاصة من خلال جمع أو تبادل أو استخدام المعلومات بطريقة غير مشروعة، وقد جرم المشرع الجزائري بموجب المادة 303مكرر 1 من قانون العقوبات، الاحتفاظ أو الوضع أو السماح بأن توضع في متناول الجمهور أو الغير، أو الاستخدام بأي وسيلة كانت التسجيلات والصور أو الوثائق بواسطة تقنية:

[1]– أمر رقم 66–156، مؤرخ في 1966، متضمن قانون العقوبات، المعدل والمتمم.

التقاط أو تسجيل أو نقل مكالمات وأحاديث خاصة أو سرية بغير اذن صاحبها أو رضاه أو بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير اذن صاحبها أو رضاه[1]

وما يلاحظ من أحكام المواد سالفة الذكر أن النيابة والقضاء مازالت تسقط أحكام قانون العقوبات في هذه المسائل، وحماية لحرية الأفراد وخصوصيتهم، لابد من تعديل هذه المواد بما يتماشى مع التطورات التكنولوجية واضافة الآليات الالكترونية المستعملة في هذه الجرائم، أو سن قانون مستقل خاص بالجرائم المعلوماتية.

ثانيا: ضمان سرية المراسلات والاتصالات الالكترونية

قد يتعارض ضمان سرية المراسلات والاتصالات كأحد اوجه حماية الحق في الخصوصية مع اجراءات التحقيق في الجرائم المعلوماتية، وبالرجوع الى القانون 09-04 سالف الذكر، نجد أن المشرع من جهة أكد على وجوب مراعاة سرية المراسلات والاتصالات، ومن جهة أكد أنه لمقتضيات التحري والتحقيق يمكن وضع مجموعة ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.

كما أكد بموجب المادة 10 منه على وجوب التزام مقدمي خدمات الانترنت بكتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

من هذا المنطلق يمكن أن نلتمس ارادة المشرع في التوفيق بين القواعد الاجرائية الناجعة للوقاية من الجرائم المعلوماتية ومواجهتها، بين تكريس الحق في الخصوصية[2].

[1]- أمر رقم 66-156، مؤرخ في 1966، متضمن قانون العقوبات، المعدل والمتمم.

[2]- مفيدة مباركية، مرجع سابق، ص 482.

وقد أصدر المشرع الجزائري مؤخرا القانون 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية[1]، وبتحليلنا للنصوص القانونية المتعلقة به، نجد أن المشرع قد أحاط سرية المراسلات بحماية خاصة من أي انتهاك، وذلك بنصه في المادة 160 من نفس القانون على أن يلتزم المتعاملون وكذا مستخدموهم، باحترام سرية المراسلات الصادرة عن الاتصالات الالكترونية وشروط حماية الحياة الخاصة والمعلومات الاسمية للمشتركين.

ويقصد بالاتصالات الالكترونية كل ارسال أو تراسل أو استقبال علامات أو اشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية.

وقد عالج المشرع الجزائري النظام القانوني للاتصالات الالكترونية حيث أجاز انشاء و-أو استغلال شبكات الاتصالات الالكترونية مهما كان نوع الخدمات المقدمة، على أن يخضع انشاء واستغلال شبكات الاتصالات الالكترونية المفتوحة للجمهور وتقديم خدمات الاتصالات الالكترونية للجمهور الى احترام عدة شروط أهمها:

- احترام شروط خصوصية البيانات والمعلومات التي تم ايصالها بواسطة شبكات الاتصالات الالكترونية
- احترام شروط الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي.

كما عالج أنظمة استغلال الاتصالات الالكترونية، وأورد شرط مهم عند استعمال شبكات أو خدمات الاتصالات الالكترونية التي لابد ألا تمس:

- النظام العام والدفاع الوطني والأمن العمومي
- الكرامة وحفظ الحياة الخاصة للآخرين

[1]- قانون رقم 18-04، مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر، عدد 27، الصادرة بتاريخ 13 ماي 2018، ص 03.

- الأطفال، خصوصا فيما يتعلق باستعمال خدمات الانترنت

ولضمان سرية المراسلات والاتصالات الالكترونية تطرق المشرع الجزائري بموجب هذا القانون الى عدة جرائم وفي مقدمتها جريمة انتهاك سرية المراسلات حيث أفرد المشرع عقوبة جنحية في حالة انتهاك سرية المراسلات عن طريق البريد أو الاتصالات الالكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل اليه أو يخبر بوجودها، وفي هذه الحالة يعاقب بالحبس من سنة الى خمس سنوات وبغرامة من 500.000 دج الى 1.000.000 دج[1] حسب ما جاء في المادة منه146.

كذلك جريمة تحويل المراسلات أو الأمر أو المساعدة في ارتكاب الجريمة: وما يلاحظ في هذه الجريمة عدم تحديد طريقة التحويل أو طبيعته، حيث يعاقب على ارتكابها مهما كان شكلها:

1-إذا تم تحويل المراسلات الصادرة أو المرسلة عن طريق الاتصالات الالكترونية أو الأمر أو المساعدة في ارتكاب الجريمة فالعقوبة الاصلية تتمثل في الحبس و-أو الغرامة المالية، اضافة الى امكانية نطق الجهة القضائية بواحدة او أكثر من العقوبات التكميلية المنصوص عليها في المادة 9 من قانون العقوبات.

2-إذا تم تحويل المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الالكترونية من قبل مستخدم لدى متعامل للاتصالات الالكترونية أو يأمر أو يساعد في ارتكاب الافعال، فالعقوبة جنحية تتمثل في الحبس من ستة أشهر الى سنتين وغرامة من 500.000 دج الى 1.000.000 دج أو بإحدى هاتين العقوبتين

[1]- المادة 146 من قانون رقم 18-04، مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، سالف الذكر، ص 28.

ويعاقب الاشـخاص الآخرين الغير مذكورين في المواد 165 و166 من هذا القانون بالحبس من شهرين الى سنة وغرامة من 200.000 دج الى 1.000.000 دج وهو ما ورد في نص المادة 197 من هذا القانون.

اضافة الى جزاءات أخرى.

ثالثا: حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

تعتبر المعطيات ذات الطابع الشـخصـي جزءا لا يتجزأ من الحياة الخاصـة، ولم تكن هذه المعطيات محمية من قبل الى غاية صدور القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشـخصـي، وان جاء هذا القانون متأخرا نوعا ما الا أنه من الجيد اسـتحداثه، لحماية أكبر للحقوق اللصـيقة بالشـخص والتي تتطلب المحافظة عليها وعدم جمعها أو التشهير بها دون موافقة الشخص المعني أو دون مبرر.

ففي ظل العولمة وسـهولة الحصـول على البيانات وتداولها، تتضـاعف أهمية ارسـاء نظام فاعل للحماية، وفرض اجراءات قانونية صـارمة، ضـد اسـاءة اسـتخدام البيانات الشخصية، والاعتداء على الخصوصية، فلابد من الالتزام بتطبيق ومواكبة أرقى المعايير في هذا المجال، حفاظا على امكانات وفرص الافادة، مما يمكن أن تقدمه التقنيات الحديثة في معالجة البيانات، سـواء على مسـتوى تطوير الاقتصـاد، أو على مسـتوى الانماء الاجتماعي والثقافي، ولابد من الانسجام على المستوى القانوني[1]

حيث يقصد بالمعطيات ذات الطابع الشخصي: كل معلومة بغض النظر عن دعامتها متعلقة بشـخص معرف أو قابل للتعرف عليه بصـفة مباشـرة أو غير مباشـرة لاسـيما بالرجوع

[1]-منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية (الهم الأمني وحقوق الأفراد)، ط1، المركز العربي للبحوث القانونية والقضائية، بيروت لبنان، سنة 2018.

الى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيو مترية أو النفسية أو الاقتصادية أو الاجتماعية.

وقد توسع المشرع الجزائري في بسط الحماية الجنائية للحياة الخاصة فلم يشترط مصدر أو شكل معين حتى تتم معالجة المعطيات ذات طابع شخصي، حيث يجب أن تتم المعالجة مهما كان مصدرها أو شكلها، المهم هو أن تكون في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم، وفي حالة خرق ذلك قرر المشرع عقوبة جنحية تتمثل في الحبس من سنتين الى خمس سنوات وغرامة من 200.000 دج الى 500.000 دج.

و أضاف المشرع شرطا مهما للقيام بالمعالجة وهو الموافقة المسبقة للشخص المعني و يجب أن تكون هذه الموافقة صريحة، كما يمكن أن يتراجع عنها الشخص المعني في أي وقت، على أن لا تكون هذه الموافقة واجبة في حالات معينة أوردها نص المادة 07 من القانون ، وفي حالة معالجة المعطيات ذات الطابع الشخصي دون احترام ما جاء في المادة 07، أو دون موافقة الشخص المعني أو اعتراضه، عندما تستهدف هذه المعالجة الاشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب مشروعة، يعاقب كل من قام بذلك بالحبس من سنة الى ثلاث سنوات و بغرامة من 100.000 دج الى 300.000 دج وهو ما جاء في نص المادة 55 من هذا القانون. وشدد المشرع العقوبة من سنتين الى خمس سنوات وغرامة من 200.000 الى 500.000 دج في حالة معالجة المعطيات الحساسة دون موافقة صريحة من الشخص المعني.[1]

[1]– المادة 57 من القانون قانون رقم 18–07، مؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، عدد 34، الصادرة في 10 جوان 2018، ص 22.

ولبسط حماية أكبر لمعالجة المعطيات ذات الطابع الشخصي قام المشرع بتجريم العديد من الأفعال بموجب هذا القانون (المواد من 54 الى 74) ومنها تجريم الجمع غير المشروع للمعطيات الشخصية، (كجريمة استعمال الأساليب غير المشروعة في جمع المعطيات الشخصية، أو جمع المعطيات الشخصية المتعلقة بالوضعية الجزائية للشخص المعني)، كذلك في حالة خرق سرية وسلامة المعالجة، وغيرها من الجرائم المنصوص عليها في هذا القانون[1].

لا يمكن معالجة المعطيات ذات طابع شخصي المتعلقة بالجرائم والعقوبات وتدابير الأمن الا من قبل السلطة القضائية والسلطات العمومية والأشخاص المعنويين الذي يسيرون مصلحة عمومية، ومساعدي العدالة في إطار اختصاصهم، ولابد أن تتم المعالجة بموجب تصريح أو ترخيص مسبق من السلطة الوطنية المختصة.

[1]– للتوسع في الموضوع: أنظر عز الدين طباش، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري (دراسة في ظل قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، العدد 02، سنة 2018، ص 26-60.

الفصل الثاني:

دور أجهزة التحقيق في مواجهة الجرائم المعلوماتية

الفصل الثاني: دور أجهزة التحقيق في مواجهة الجرائم المعلوماتية

ان أجهزة التحقيق في الجرائم المعلوماتية عبارة عن ادارة متخصصة يحكم وظائفها مبدأ التخصص والتمييز الذي تكون فيه المعرفة الالكترونية وتطبيقها بسرعة وسرية عنصر أساسي لفاعلية التحقيق في الجرائم المعلوماتية، ويكون لهذه الأجهزة تركيبة بشرية يتصل أفرادها وفقا لقواعد أمن المنشأة بمعنى (أمن الأفراد، المعلومات، وسائل الاتصال والتنقل) وذلك بهدف الحد من الجريمة وضبطها وضبط الأدلة الالكترونية.[1]

ويلعب المحقق دورا هاما في حسن سير اجراءات التحقيق، من خلال اتسامه بالمعرفة الالكترونية وتجاوزه للأخطاء المتعلقة بتدوين الاجراءات أو بعدم الدقة أو اغفال اجراءات جوهرية في التحقيق، ويلتزم المحقق بالمحافظة على سرية التحقيق، والسرعة في اجراءات جمع الأدلة والتعامل معها بدقة واحترافية.

وطبقا لذلك وضحنا الأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية ضمن المبحث الأول، ثم تطرقنا لدور المحقق في حسن سير اجراءات التحقيق ضمن المبحث الثاني.

[1]– مصطفى محمد موسى، مرجع سابق، ص 287.

المبحث الأول: الأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية

ان الولايات المتحدة الأمريكية هي في مقدمة الدول التي أنشـــأت و اســـتحدثت عدة مكاتب متخصـصـــة في مكافحة الجرائم المعلوماتية و التحري و التحقيق فيها ضـمن مكتب التحقيقات الفيدرالي FBI، وأنشأت ايضا قسم مكافحة جرائم الحاسوب و جرائم حقوق الملكية الفكرية التابع لوزارة العدل الأمريكية عام1991، تليها فرنســـا التي أنشـــأت هي الأخرى مجموعة من المكاتب و الأجهزة المتخصـصـــة في مكافحة هذه الجرائم و التحري و التحقيق فيها، مثل: المكتب المركزي لمكافحة الاجرام المرتبط بتكنولوجيا المعلومات و الاتصـــالات عام 2000، و قســـم الانترنت التابع للمصـــلحة التقنية للبحوث القانونية و الوثائقية عام 1998.[1]

وتتعدد أســباب انشــاء أجهزة مكلفة بالتحقيق في الجرائم المعلوماتية وأول ســبب هو حماية أفراد المجتمع من مخاطر هذه الجرائم والحد منه اضافة الى ضبط الجرائم المعلوماتية والحصـول على مختلف الأدلة الالكترونية التي تسـاعد في اثبات الجريمة. كما يعتبر التهديد الذي يطال أمن الدول سببا ثانيا لإنشـاء أجهزة متخصـصـة في التحقيق في مثل هذه الجرائم نتيجة اســتخدام تقنية المعلومات والتفاعل معها من قبل مختلف فئات المجرمين من ارهابيين ومهربي الأسلحة والمتاجرين بالمخدرات ومبيضي الأموال وجماعات الجريمة المنظمة. [2]

وسـنتناول في هذا المبحث الهيئات المكلفة بالتحقيق ضـمن المطلب الأول والوحدات المكلفة بالتحقيق ضمن المطلب الثاني.

[1]– رشاد خالد عمر، مرجع سابق، ص 68.

[2]– مصطفى محمد موسى، مرجع سابق، ص 288.

المطلب الأول: الهيئات المكلفة بالتحقيق في الجرائم المعلوماتية

بدأت التشريعات –ومن بينها التشريع الجزائري –تواجه خطورة الجرائم المعلوماتية من خلال استحداث هيئات قضائية وغير قضائية وهو ما سنتناوله في هذا المطلب.

الفرع الأول: الهيئات القضائية الجزائية المتخصصة

يعتبر انشاء هيئات قضائية جزائية متخصصة توجها جديدا لتطويق نطاق الجرائم الخطيرة ومن بينها الجرائم المعلوماتية.

أولا: انشاء الهيئات القضائية الجزائية المتخصصة

نشأت هيئات قضائية جزائية متخصصة منذ تعديل قانون الاجراءات الجزائية الجزائري بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم ل ق ا ج ج.

باستقراء نص المادة 37 و40 منه، يتضح أن المشرع الجزائري خروجا عن القواعد العامة للاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق والمحددة بـ:

- مكان وقوع الجريمة.
- محل اقامة أحد الأشخاص المشتبه في مساهمتهم فيها.
- المكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر.

فقد أجاز المشرع بموجب الفقرة الثانية من المادة 37 ق ا ج تمديد اختصاص وكيل الجمهورية في جرائم محددة على سبيل الحصر ومن بينها الجرائم المتعلقة بالمعالجة الآلية للمعطيات الى دائرة محاكم أخرى محددة عن طريق التنظيم، وهو نفسه بالنسبة لتمديد اختصاص قاضي التحقيق بموجب الفقرة الثانية من المادة 40 ق ا ج.

كما نصت الفقرة الأخيرة من المادة 329 من قانون الاجراءات الجزائية جزائري، على تمديد الاختصاص المحلي للمحكمة في الجرائم المحددة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

وما يفسر خروج المشرع عن معايير الاختصاص الأصلي[1] في الجرائم المعلوماتية هو:

- اتساع مكان ارتكاب الجرائم المعلوماتية خارج حدود الاختصاص الاقليمي التقليدي، وانتشار الأعمال المكونة هذه الجرائم داخل وخارج حدود الدولة.
- التمسك بالمعايير الأصلية للاختصاص يشكل عائقا أمام مواجهة الجرائم المعلوماتية.
- الطبيعة الخاصة لهذه الجرائم.

وقد حدد المشرع سنة 2006، بموجب المرسوم التنفيذي رقم 06-348 تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق حيث يمتد الاختصاص المحلي لمحكمة سيدي محمد ومحكمة قسنطينة ومحكمة ورقلة ومحكمة وهران ووكلاء الجمهورية وقضاة التحقيق في هذه المحاكم، الى محاكم المجالس القضائية التابعة لمختلف ولايات الوطن (48 ولاية) حسب الجهة.[2]

وما يعاب على المشرع الجزائري في مسألة تمديد الاختصاص أنه لجأ الى ذلك الا أنه لم يستحدث أقساما متخصصة و لا تشكيلة خاصة لدى الجهات القضائية و لا قضاة متخصصين في الجرائم المحددة حصرا في هذه المواد و من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، عكس ما ذهب اليه القانون الفرنسي في المادة 706-75 من ق ا ج فرنسي أن المحاكم ذات الاختصاص الموسع تشمل على فرع للنيابة وتشكيلات للتحقيق

[1]- كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11، العدد 01، سنة 2015، ص 121.

[2]- أنظر المادة 2-3-4-5 المرسوم التنفيذي رقم 06-348، المؤرخ في 5 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر، عدد 63، الصادرة في 8 أكتوبر 2006، ص 30.

و المحاكمة متخصـــصـــة بالنظر في الجرائم محل الاختصـــاص الذي وضـــح أن تمديد الاختصاص للمحاكم لا يخص الا القضاة المعينين في فروع متخصصة في حين أن قانون 04-14 جاء عاما حيث جعل من تمديد الاختصـــاص لكل القضـــاة الموجودين في المحاكم ذات الاختصاص الموسع[1].

ثانيا: توسيع صلاحيات ضباط الشرطة القضائية

تجدر الاشـارة أن المادة 16 من ق اج ج عالجت مسـألة تمديد اختصـاص ضـباط الشـرطة القضـائية الى كامل التراب الوطني فيما يتعلق بالبحث ومعاينة جرائم محددة بنص المادة ومن بينها الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات، وأجازت المادة 47 التفتيش والمعاينة والحجز في هذه الجرائم في أي ســـاعة من النهار والليل بإذن من وكيل الجمهورية كما يجوز لقاضـــي التحقيق بالتفتيش والحجز ليلا أو نهارا في كامل التراب الوطني، أو يأمر ضباط الشرطة القضائية المختصين بذلك.

كما مكن المشـرع الجزائري بموجب المادة 51 من نفس القانون، تمديد آجال التوقيف للنظر مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، وهنا لابد من مراعاة ضمانات المتهم خلال مرحلة التوقيف للنظر.

[1]- كريمة علة، مرجع سابق، ص 123.

الفرع الثاني: الهيئات غير القضائية

تتمثل الهيئات غير القضـــائية المكلفة بالتحقيق في الجرائم المعلوماتية في الهيئة الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيات الاعلام والاتصـال، اضـافة الى السـلطة الوطنية لمعالجة المعطيات ذات طابع شخصي، ووكالة أمن الأنظمة المعلوماتية.

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

1-مفهوم الهيئة

في سبيل ضمان فاعلية التحقيق أنشأ المشرع الجزائري بموجب المادة 13 من القانون 09-04 الهيئة الوطنية للوقاية من الجرائم المتصـلة بتكنولوجيات الاعلام و الاتصـال، وترك تحديد تشـــكيلتها و تنظيمها و كيفيات ســـيرها عن طريق التنظيم، حيث نظمت وفقا لعدة مراسيم بداية بالمرسوم الرئاسـي 15-261 المؤرخ في 8 اكتوبر 2015[1]، الذي عرف الهيئة بموجب المادة 02 منه على أنها: ســـلطة ادارية مســـتقلة تتمتع بالشـــخصـــية المعنوية و الاسـتقلال المالي توضـع لدى الوزير المكلف بالعدل ثم جاء المرسـوم الرئاسـي 19-172 المؤرخ 6 يونيو 2019 [2]و أعاد تعريف الهيئة بموجب المادة 02 منه، على أنها: مؤسـســة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية و الاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني، و أعيد تنظيم الهيئة من جديد بموجب المرســوم الرئاســي 20-183

[1]- مرسوم رئاسي رقم 15-261، مؤرخ في 8 اكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 53، الصادرة بتاريخ 8 اكتوبر 2015، ص 16.

[2]- مرسوم رئاسي رقم 19-172، مؤرخ في 6 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر، عدد 37، الصادرة بتاريخ 9 جوان 2019، ص 05.

المؤرخ في 13 يوليو 2020[1]، حيث عرفت الهيئة بأنها: سلطة ادارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة رئيس الجمهورية.

وما يلاحظ أنه وقع تعديل فيما يخص الجهة الوصية حيث أصبحت الهيئة توضع تحت سلطة رئيس الجمهورية، بعدما كانت توضع تحت سلطة وزارة العدل سنة 2015، ولدى وزارة الدفاع الوطني سنة 2019، كما تم استرجاع مصطلح سلطة ادارية مستقلة كما كان سابقا في المرسوم الرئاسي 15-261، وذلك بعدما استعمل مصطلح مؤسسة عمومية ذات طابع اداري في المرسوم الرئاسي 19-172 عندما وضعت تحت سلطة وزارة الدفاع الوطني.

وموقف المشرع الجزائري اتجاه هذه السلطات الجديدة كان يسوده الغموض فلم يسلم بمبدأ استقلاليتها بسهولة رغم نصه على تمتعها بالاستقلالية الادارية والمالية، اذ أنه لم يوفر الأدوات القانونية التي تؤكد ذلك، فلم تكن رؤيته واضحة اتجاه مفهوم السلطة الادارية المستقلة، فالمصطلح يثير اشكالات قانونية عديدة ويحمل في طياته ما يشبه التناقض بين صفة السلطة الادارية التي تتمتع بالتبعية وتخضع لرقابة رئاسية أو وصائية والى رقابة القضاء الاداري وبين صفة الاستقلالية.[2]

وما نلاحظه أن المرسوم الرئاسي لسنة 2019 غير المصطلح من سلطة ادارية مستقلة الى مؤسسة عمومية ذات طابع اداري عندما ألحق الهيئة بوزارة الدفاع باعتبارها وزارة سيادية تتنافى وصفة الاستقلالية التي تتمتع بها الهيئة، و حسن فعل بتعديل المصطلح في المرسوم الأخير لسنة 2020، باعتبار الهيئة في ميدان الضبط الاداري أين يستعمل

[1]- مرسوم رئاسي رقم 20-183، مؤرخ في 13 جويلية 2020، يتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 40، الصادرة بتاريخ 18 جويلية 2020، ص 05.

[2]-سلطان عمار، السلطات الادارية المستقلة في الجزائر، مجلة جيل للأبحاث القانونية المعمقة، العدد 33، سنة 2019، ص 53.

مصـــطلح ســـلطة أو هيئة مســـتقلة، و تتمتع الهيئة الوطنية للوقاية من الجرائم المتصـــلة بتكنولوجيات الاعلام و الاتصـال بالشـخصـية المعنوية و الاسـتقلال المالي، و بوضـع الهيئة تحت سلطة رئاسـة الجمهورية فالهيئة هي امتداد للسلطة التنفيذية و باعتبار رئيس الجمهورية هو رئيس السلطة التنفيذية فهو المتحكم في هذه الهيئات.

2-مقر الهيئة:

كان مقر الهيئة مقتصـر في مدينة الجزائر في المرسـوم الرئاسـي لسـنة 2015، ثم أضـــيفت امكانية تمديد مقر الهيئة الى أي مكان آخر من التراب الوطني بموجب المرســـوم الرئاسي لسنة 2019، و أبقى المرسوم الرئاسي لسنة 2020 على أن مقر الهيئة كأصل عام يحدد بمدينـة الجزائر مع امكانيـة نقل المقر الى أي مكـان آخر من التراب الوطني، و يكمن الاختلاف بين المادة 03 في المرسومين الأخيرين أن نقل مقر الهيئة في مرسوم 2019 كان بموجب قرار من وزير الدفاع الوطني، و أصـــبح نقل مقر الهيئة الى كامل التراب الوطني بموجب المرسوم الرئاسي الأخير يتم بموجب مرسوم رئاسي.

3-مهام الهيئة:

أبقى المرسـوم الرئاسـي لسـنة 2020 على مهام الهيئة تحت رقابة السـلطة القضـائية والمتمثلة في: [1]

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها،
- تنشـيط وتنسـيق عمليات الوقاية من الجرائم المتصـلة بتكنولوجيات الاعلام والاتصـال ومكافحتها،

[1]- أنظر المادة 04 من المرسوم الرئاسي 20-183 سالف الذكر، ص 05 ص06.

- مساعدة السلطات القضائية المختصة ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، لاسيما من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية
- ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الارهابية والتخريبية والمساس بأمن الدولة.
- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الاجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الاعلام والاتصال.
- المساهمة في تحيين المعايير القانونية في مجال اختصاص الهيئة.

4-تنظيم الهيئة:

وضع المرسوم الرئاسي لسنة 2020 كل من مجلس التوجيه ومديرية عامة، تحت السلطة المباشرة لرئيس الجمهورية، ويقدمان له عرضا عن نشاطاتهما.[1]

مجلس التوجيه: أبقى المرسوم الرئاسي الجديد على نفس الصلاحيات الممنوحة لمجلس التوجيه بموجب المرسوم الرئاسي لسنة 2019، غير أنه عدل التشكيلة برئاسة رئيس الجمهورية و يمكنه أن يفوض ممثله، حيث يتشكل مجلس التوجيه من الوزير المكلف

[1]- المادة 05 من المرسوم الرئاسي رقم 20-183، سالف الذكر، ص 06.

بالعدل، الوزير المكلف بالداخلية، الوزير المكلف بالمواصلات السلكية واللاسلكية وقام المرسوم بإضافة كل من المدير العام للأمن الداخلي وقائد الدرك الوطني والمدير العام للأمن الوطني و ممثل عن رئاسة الجمهورية وممثل عن وزارة الدفاع الوطني ويعين رئيس الجمهورية ممثلي رئاسة الجمهورية ووزارة الدفاع الوطني.

وأضافت المادة 08 منه أن اجتماع مجلس التوجيه في دورة عادية مرتين في السنة، بناء على استدعاء من رئيسه، ويمكنه أن يجتمع في دورة غير عادية، كلما كان ذلك ضروريا، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

المديرية العامة: يريدها مدير عام، تعيينه أو انهاء المهام يكون بموجب مرسوم رئاسي.

أسندت للمديرية العامة نفس الصلاحيات المنصوص عليها في مرسوم 2019، غير أن الاختلاف يكمن في أن المرسوم الجديد جعل من صلاحيات المديرية العامة مقيدة بوجوب موافقة مجلس التوجيه، على مشروع ميزانية الهيئة واعداد وتنفيذ برنامج عمل الهيئة، ووجوب رفع التقرير السنوي لنشاطات الهيئة لمصادقة مجلس التوجيه.

كما أضاف مصطلح –الهوية–وأبقى على نفس الصلاحية المنصوص عليها في المرسوم السابق، حيث أن من بين صلاحيات المديرية العامة تبادل المعلومات مع مثيلاتها في الخارج بغرض تجميع كل المعطيات المتعلقة بتحديد مكان وهوية مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والتعرف عليهم، كذلك اعادة عبارة مراقبة انشطة مكونات المديرية العامة[1] في المرسوم الجديد بعدما كانت سابقا مراقبة انشطة هياكل الهيئة.

[1]– المادة 10 من المرسوم الرئاسي رقم 20–183، سالف الذكر، ص 7.

كذلك أعيدت صياغة اسماء المديريات والمصالح التابعين للمديرية العامة، حيث تضم الهيئة:[1]

-**مديرية للمراقبة الوقائية واليقظة الالكترونية:** حيث أضافت المادة 15 صلاحية اليقظة الالكترونية في مجال الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وهو سبب تغيير المصطلح الذي كان في المرسوم الرئاسي لسنة 2019 "مديرية تقنية"

-**مديرية للإدارة والوسائل:** لم يتغير محتوى المادة في المرسوم الجديد

-**مصلحة الدراسات والتلخيص:** حيث أضاف المرسوم الرئاسي الجديد صلاحيات هذه المصلحة بموجب المادة 19 منه.

-**مصلحة التعاون واليقظة الالكترونية:** حيث أضاف المرسوم الرئاسي الجديد صلاحيات هذه المصلحة بموجب المادة 20 منه.

5-سير الهيئة:

أضاف المرسوم الرئاسي الاخير المواد من 21 الى 30 تنظم كيفيات سير الهيئة، وأهم ما جاء في هذه المواد:

- اضافة صلاحية مهمة للهيئة حيث تكلف حصريا بمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في الحين، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.
- امكانية طلب اي وثيقة أو معلومة ضرورية لإنجاز مهامها من أي جهاز أو مؤسسة أو مصلحة.

[1]- المادة 11 من المرسوم الرئاسي رقم 20-183، سالف الذكر، ص 7.

- إمكانية طلب المساعدة من الوزارات المعنية للأعوان العموميين المختصين في مجال تكنولوجيات الاعلام والاتصال.
- وجوب المحافظة على السر المهني.
- استعمال الوسائل والتجهيزات الالكترونية أو استيراد أو اقتناء أو حيازة لا يكون الا من طرف الهيئة في حدود اختصاصها. أو عند الاقتضاء سلطة ضبط الاتصالات السلكية واللاسلكية، والمؤسسة العمومية المكلفة بشبكات الاتصالات.
- تفتيش أي مكان أو هيكل أو جهاز بلغ الى علم الجهات المختصة بأنه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية...

ثانيا-السلطة الوطنية لحماية المعطيات ذات طابع شخصي

1-استحدث المشرع الجزائري بموجب القانون 18-07 سلطة وطنية تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي وهي عبارة عن سلطة ادارية مستقلة تتمتع بالشخصية المعنوية وبالاستقلال المالي والاداري تضمن عدم انطواء استعمال تكنولوجيات الاعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة. توضع لدى رئيس الجمهورية وذلك بهدف حماية المعطيات.

2-المهام المسندة للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

-تلقي التصريحات المسبقة المتعلقة بمعالجة المعطيات ذات الطابع الشخصي: حيث تضمنت المواد من 13 الى 16 من القانون كل ما يخص اجراء التصريح الذي يجب أن يودع مسبقا لدى السلطة الوطنية، وباستقراء نص للمادة 13 من القانون نجد أن طريق تقديم التصريح المسبق يكون بأي شكل من الأشكال، حيث يمكن تقديمه الكترونيا، ويسلم وصل ايداع أو يرسل فورا بالطريق الالكتروني في مدة محددة ب 48 ساعة.

-**اخضـــاع المعالجة لنظام الترخيص:** وقد تضـــمنت المواد من 17 الى 21 كل ما يخص نظام الترخيص، حيث لابد للسلطة الوطنية إذا تبين لها أن المعالجة محل التصريح تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص. كذلك تمنح السلطة الوطنية الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا شروط محددة قانونا. كما تقوم بنشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني.

-**الاعلام وتقديم الاستشارات والاقتراحات اللازمة:** حيث تسهر السلطة على اعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم. وتسهر على تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي، أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي الى مثل هذه المعالجة. كما تختص بتقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي، لمعالجة هذه المعطيات.

-**اصـــدار أوامر:** حيث تأمر بالتغييرات اللازمة من أجل حماية المعطيات ذات الطابع الشخصي المعالجة، كما تأمر بإغلاق معطيات أو سحبها أو اتلافها.

-**تطوير علاقات التعاون مع الســـلطات الأجنبية المماثلة:** ويشـــترط في ذلك مراعاة مبدأ المعاملة بالمثل.

-وضع معايير وقواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات، بالإضافة الى اصدار عقوبات ادارية وفقا لأحكام المادة السادسة والأربعون.

-تختص بالإعلام الفوري للنائب العام المختص، في حالة معاينة وقائع تحتمل الوصـــف الجزائي.

-**اعداد تقرير سنوي:** حيث تقوم السلطة الوطنية بإعداد التقرير السنوي حول نشاطاتها، وترفعه الى رئيس الجمهورية.

لقد اشترط القانون 18-07 الموافقة المسبقة من الشخص الطبيعي الذي تكون المعطيات ذات الطابع الشخصي المتعلقة به محل معالجة، وله الحق في التراجع عن موافقته في أي وقت، كما لا يمكن اطلاع الغير على المعطيات محل المعالجة الا بعد الموافقة المسبقة منه. وإذا كان عديم أو ناقص الأهلية تكون الموافقة وفق القواعد المقررة قانونا.[1]

ولا يمكن القيام بالمعالجة للمعطيات ذات الطابع الشخصي المتعلقة بالطفل الا بعد حصول موافقة من ممثله الشرعي، أو بترخيص من القاضي المختص. [2]

ويخرج عن مجال تطبيق هذا القانون كل من المعطيات ذات الطابع الشخصي: سواء المعالجة من طرف شخص طبيعي لغايات لا تتجاوز الاستعمال الشخصي أو العائلي، شرط عدم احالتها للغير أو نشرها.

أو المحصل عليها والمعالجة لمصلحة الدفاع والأمن الوطنيين. أو المعالجة لأغراض الوقاية من الجرائم ومتابعة مرتكبيها وقمعها كذلك المحتوية في قواعد البيانات القضائية التي تخضع الى النص الذي أحدثت بموجبه والى أحكام المادة 10 من القانون 18-07.

وتجدر الاشارة أنه لا يمكن معالجة المعطيات ذات الطابع الشخصي المتعلقة بالجرائم والعقوبات وتدابير الأمن، الا من قبل السلطة القضائية والسلطات العمومية والأشخاص المعنوية المسيرة لمصلحة عمومية، ومساعدي العدالة في إطار اختصاصاتهم القانونية. كما

[1]- أنظر نص المادة 07 من القانون 18-07 سالف الذكر.

[2]- أنظر نص المادة 08 من القانون 18-07 سالف الذكر.

يجب تحديد المسؤول عن المعالجة والغاية منها والأشخاص المعنيين بها، والغير الذي يمكنه الاطلاع على المعلومات ومصدرها والاجراءات الواجب اتخاذها لضمان سلامة المعالجة.[1]

ثالثا: وكالة أمن الأنظمة المعلوماتية

استحدثت منظومة وطنية لأمن الأنظمة المعلوماتية توضع لدى وزارة الدفاع، والتي تتكون من المجلس الوطني لأمن الأنظمة المعلوماتية، والوكالة الوطنية لأمن الأنظمة المعلوماتية التي من بين مهامها اجراء التحقيقات الرقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية[2]

وتعتبر وكالة أمن الأنظمة المعلوماتية مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلال المالي، يقع مقرها في مدينة الجزائر.

سير الوكالة:

تدير الوكالة لجنة توجيه وتزود بلجنة علمية، وتتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وادارية موضوعة تحت سلطة المدير العام الذي يسير بدوره الوكالة ويسهر على تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنفيذ المخططات والبرامج المسطرة من قبل لجنة التوجيه.

[1]- أنظر نص المادة 10 من القانون 18-07 سالف الذكر.

[2]- مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، عدد 04، الصادر في 26 جانفي 2020، ص 05.

المطلب الثاني: الوحدات المكلفة بالتحقيق في الجرائم المعلوماتية

ان الأجهزة التابعة للأمن والدرك الوطني تسهر على المواجهة التنظيمية للجرائم المعلوماتية بشكل عمودي كل في مجال اختصاصه.

الفرع الأول: وحدات الدرك الوطني

تلعب مؤسسة الدرك الوطني دور فعال في مواجهة الجرائم المعلوماتية وتطويق نطاق الجرائم المعلوماتية من خلال استحداثها لتقنيات خاصة، وانشاء وحدات خاصة.

أولا: المعهد الوطني للأدلة الجنائية وعلم الاجرام INCC /GN

وهو جهاز تابع للدرك الوطني أنشأ سنة 2004 بموجب المرسوم الرئاسي رقم 04-183[1]، يتكون من 11 دائرة متخصصة في عدة مجالات تضمن الخبرة والتكوين والتعليم وتقديم المساعدات التقنية والبحوث والدراسات والتحاليل في علم الجريمة.

حيث تكلف دائرة الاعلام الآلي والالكترونيك بمعالجة تحليل وتقديم كل دليل الكتروني وتماثلي للعدالة، كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة.

يسهر أفراد الدائرة على تأمين اليقظة التكنولوجية من أجل تحيين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية.

ولإنجاز المهام المنوطة بها تنقسم الدائرة الى ثلاثة مخابر وكل مخبر مزود بفصيلة مهمتها اقتناء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل:

[1]- مرسوم رئاسي 04-183 المؤرخ في 26 جوان 2004، يتضمن احداث المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية، عدد 41، الصادرة في 27 جوان 2004، ص 18.

1. **مخبر الاعلام الآلي:** يختص بتحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش)، كما يقوم بتحديد التزوير الرقمي للبطاقات البنكية.
2. **مخبر الفيديو:** يختص بإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد، كما يعمل على تحسين نوعية الصورة (فيديو، صورة) بمختلف التقنيات، ومقارنة الأوجه وشرعية الصور والفيديو.
3. **مخبر الصوت:** يختص بمعرفة وتحديد المتكلم، وتحديد شرعية التسجيلات الصوتية، ويعمل على تحسين نوعية اشارة الصوت بنزع التشويش وتعديل السرعة.[1]

ثانيا: مركز الوقاية من جرائم المعلوماتية ومكافحتها GN/ CPLCIC

وهو مركز تابع لأجهزة الدرك الوطني بدأ عمله منذ سنة 2004، والذي يكلف بمهمتين رئيستين:

المهمة الأولى: قبلية تتعلق بالتدقيق والوقاية،

المهمة الثانية: بعدية تتعلق بردع الجرائم الماسة بالطفولة.

وحديثا أنشأ مكتب خاص بحماية الأحداث عبر الانترنت بغرض تقديم الدعم التقني للوحدات الاقليمية في التحري وجمع الأدلة الجنائية.

في 2017 عالج المركز 100 جريمة تتعلق بالأطفال و المراهقين، و 20 جريمة مالية، حيث أن الجرائم المالية مازالت محدودة لأن التجارة الالكترونية و الدفع الالكتروني مازال في بدايته، ويتوقع زيادة هذا النوع من الجرائم خلال السنوات المقبلة بعد تعميم التجارة الالكترونية، مما يتطلب الاستعداد لمواجهة من الجرائم المتعلقة بالتجارة الالكترونية عن

[1]– عرض مقدم من طرف: هواري عياش، المعهد الوطني للأدلة الجنائية، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16–17 نوفمبر 2015، بسكرة، الجزائر.

طريق انشاء مكتب خاص بالجريمة الاقتصادية و مختلف تحديات الفضاء السيبراني، وهذا يستدعي اطار قانوني متكامل من الجوانب العملية و التقنية و ذلك عن طريق تكوين مختصين في الجرائم المعلوماتية في كل مجالاتها. [1]

ثالثا: المصلحة المركزية للتحريات الجنائية SCIC /GN

تعد المصلحة المركزية للتحريات الجنائية مصلحة تابعة لأجهزة للدرك الوطني تقوم بالتحقيق التقني والعملي، ويبقى اجراء التحقيق في الجرائم المعلوماتية ليس بالأمر السهل، باعتبار أن هذا النوع من الجرائم المعاصرة لا يعترف بحدود المكان والزمان، كما أن اجراءات جمع الأدلة وتحديد هوية مرتكبي هذه الجرائم أو المشتبه بهم تبقى معقدة في ظل التكنولوجيات الحديثة.

وجدير بالذكر أن المحققين على المستوى المحلي من فصائل الأبحاث التي تشمل محققي جرائم الاعلام الآلي، يختصون بالتحقيق ومقاربة تقنية أولية.[2] وهو كذلك بالنسبة لخلايا الشرطة العلمية والتقنية على المستوى المحلي.

[1]– مباركة بن عمراوي، العقيد في الدرك الوطني جمال بن رجم للإذاعة: 95 بالمائة من الجرائم الالكترونية تم حلها بنجاح، موقع الاذاعة الجزائرية، الدخول يوم 25-05-2019، على الساعة 05:34.

[2]– عرض مقدم من طرف: عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، بسكرة، الجزائر.

الفرع الثاني: وحدات الأمن الوطني

تتولى المديرية العامة للأمن الوطني التحقيق في الجرائم المعلوماتية عن طريق قسمين يشمل القسم الأول المخابر، ويشمل القسم الثاني الفرق، وفي سبيل نجاعة التحقيق لها دور فعال في مواجهة الجرائم المعلوماتية.

أولا-المخابر

يوجد مخبر مركزي للشرطة العلمية في الجزائر العاصمة، ومخبر جهوي في قسنطينة ووهران[1] وقد استحدثت أقسام متخصصة في تتبع الأدلة الرقمية من خلال استغلال أجهزة الكترونية قصد استخراج وتتبع ما من شأنه أن يفيد في التحقيق ويساعد العدالة في تقرير الأحكام في القضايا التي تكون من هذا النوع، وأهم الأجهزة المستغلة من طرف هذه الأقسام:

1-أدوات التخزين الرقمية (أجهزة التصوير، بطاقات الذاكرة، الأقراص الصلبة)

2-أجهزة الكمبيوتر ولواحقها[2]

وحسب المعطيات الاحصائية لدائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية بقسنطينة، فقد شهد سنة 2014 ما يقارب 250 قضية محل تحقيق، أبرزها قضيتين تتعلق بالإنابة القضائية الدولية عن طريق مكتب الانتربول أقدم فيهما شابين من ولاية قسنطينة بالاعتداء و تعطيل نظام معلوماتي خاص بموقع وزارة الخارجية الكويتية، و القيام باحتيال الكتروني على أهداف بالولايات المتحدة الأمريكية، وسجل الثلاثي الأول سنة

[1]- وتجدر الاشارة أن هناك مخابر أخرى قيد الانجاز في ورقلة، بشار، تمنراست.

[2]- حملاوي عبد الرحمن، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16-17 نوفمبر 2015، بسكرة، الجزائر، ص 08.

2015، 60 قضية تتعلق أغلبها بسوء استخدام مواقع التواصل الاجتماعي من خلال قضايا المساس بالأشخاص في صورة الابتزاز، القذف و التشهير..[1]

ثانيا: وجود فرقة على مستوى كل أمن ولاية

في سبيل ضمان فاعلية التحقيق في مواجهة الجرائم المعلوماتية تم انشاء ما يعرف بالمصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال، و هي مصلحة تابعة لمديرية الشرطة القضائية مقرها على مستوى الجزائر العاصمة، ثم أنشأت خلايا تابعة للفرق الاقتصادية و المالية على مستوى أمن الولايات، تشمل خلية مكافحة الجرائم المعلوماتية، ثم مع تطور الجرائم و اعتماد Modem و 3g، تم ترقية الخلية لتصبح فرقة في حد ذاتها، حيث أصبحت مستقلة و تابعة للفرق الولائية للشرطة القضائية، و توجد فرق على مستوى 48 ولاية.

وكمثال عن بعض الاحصائيات على مستوى الفرق، كانت القضايا المنجزة من خلال فرقة مكافحة الجرائم المعلوماتية في أمن ولاية قالمة تقدر 153 قضية منجزة خلال الثلاث سنوات الأخيرة والموضحة في الجدول التالي:

[1]– حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، جامعة باتنة 1، 2016، ص 181.

السنة	عدد القضايا المنجزة	عدد المتورطين	
		الراشدين	الأحداث
2018	40	40	00
2019	55	56	05
2020 الى غاية نوفمبر	58	67	01
المجموع	153	163	06

جدول يوضح مثال عن الاحصائيات المتعلقة بالجرائم المعلوماتية خلال السنوات الأخيرة (مقدم من طرف أمن ولاية قالمة)

وما يلاحظ من خلال ذلك أن القضايا في تزايد من عام لآخر، خاصة في السنوات الأخيرة، كما تختلف الفئات العمرية للمتورطين في الجريمة بين بالغين وأحداث، ولعل السبب في ارتفاع معدل الجريمة المعلوماتية يرجع الى عدة عوامل، من بينها: الانفتاح على العالم الافتراضي، اغفال الأولياء عن مراقبة الطفل القاصر، التأثيرات السلبية لمواقع التواصل الاجتماعي، الانفلات الأخلاقي وغيرها من العوامل الاقتصادية والاجتماعية.

وأغلب القضايا المعالجة في الفرقة تتعلق بمواقع التواصل الاجتماعي خاصة (فايسبوك)، في قضايا المساس بحرمة الحياة الخاصة للأشخاص، والسب والشتم والتهديد، وقضايا النصب والاحتيال.[1]

[1]– وهو ما تم تسجيله في إطار زيارة ميدانية للفرقة المختصة بمكافحة الجرائم المعلوماتية على مستوى أمن ولاية قالمة.

ثالثا: دور المديرية العامة للأمن الوطني في مواجهة الجرائم المعلوماتية

للمديرية العامة للأمن الوطني دور أســـاســـي في مواجهة الجرائم المعلوماتية ويتجلى ذلك من خلال دورها الوقائي، والردعي والتحسيسي.

يتجلى الدور الوقائي من خلال عقد دورات افتراضية على مستوى شبكات المعلومات عموما ومواقع التواصل الاجتماعي خصوصا.

أما دورها الردعي يعتبر امتداد لدورها الوقائي في حالة الاخلال بالنظام العام، أو في حالة منشورات هدامة تمس النظام العام كعرض أجهزة حساسة أو ممنوعات للبيع عبر مواقع التواصـــل الاجتماعي، حيث يتم التدخل وتحديد هوية صـــاحب الحســـاب واتخاذ الاجراءات القانونية في هذا الشأن مع انجاز ملف قضائي ضده.

زيادة على ذلك للمديرية العامة دور تحسـيسـي كالتنقل لمختلف المؤسـسـات التربوية وتنظيم نشاطات والتحسيس حول سوء استعمال شبكات التواصل الاجتماعي أو سوء استخدام الانترنت، وحماية الأطفال القصر من مخاطر الانترنت.

كما تعمل المديرية على تلقي الشـــكاوى التي قد تكون مباشـــرة، أو غير مباشـــرة عن طريق ارسال النيابة العامة للقضية للتحقيق فيها.

أما على المستوى الدولي لم تغفل مديرية الأمن الوطني استغلال عضويتها الفعالة في الانتربول الذي يتيح لها مجالات للتبادل المعلوماتي وتسـهيل الاجراءات القضـائية المتعلقة بتسـليم المجرمين، وكذا مباشـرة الانابة القضـائية الدولية ونشـر أوامر القبض للمبحوث عنهم دوليا.[1]

ومن خلال الهيكل التنظيمي للمكتب المركزي الوطني –انتربول الجزائر–[2]يوجد مكتب الربط للانتربول ل 48 ولاية، واسـتخدام قاعدة المعطيات I24/7، حيث يعمل جهاز I24/7 على تحديد المعلومات اللازمة حول الأشخاص والمركبات موضوع التحقيق.

[1]– حملاوي عبد الرحمان، مرجع سابق، ص 09.

[2]– الملحق 01: الهيكل التنظيمي للمكتب المركزي الوطني انتربول –الجزائر–

المبحث الثاني: دور المحقق في حسن سير اجراءات التحقيق

ان شخصية المحقق لها دور كبير في نجاح التحقيق، فالتهيب من استخدام الكمبيوتر أو الانترنت، أو عدم الاهتمام بالمستجدات الحاصلة في المجال المعلوماتي وتطور الجرائم المعلوماتية، أو نقص المعرفة الفنية سواء بأساليب ارتكاب الجرائم المعلوماتية، أو بمتطلبات أمن المعلومات أو نقص المهارات الفنية المطلوبة للتحقيق في الجرائم المعلوماتية، وعدم فهم المصطلحات الخاصة بالمجال الرقمي قد يؤدي الى فشل التحقيق.[1]

وقد تناولنا في المطلب الأول: اتسام المحقق بمهارات تعتمد على التأهيل التكنولوجي، ثم تناولنا في المطلب الثاني: تعامل المحقق مع الأدلة الالكترونية

المطلب الأول: اكتساب مهارات التأهيل التكنولوجي

ان الهدف من منهجية البحث والتحقيق هو قبول الخطوات والمناهج التي اكتسبها المحقق، كما يجب الدقة والربط المنطقي بين السبب والنتيجة الاجرامية وتوثيق أقوال الشهود.[2] ولسلامة المعلومات لابد من سرية عملية المعالجة وتخزينها، اضافة الى التكاملية وسلامة المحتوى من أي تغيير أو نقص أو زيادة أو عبث سواء خلال النقل المعالجة التخزين[3]

[1]– علي عدنان الفيل، مرجع سابق، ص 84.

[2]– طاهر محمود أبو القاسم، مرجع سابق، ص 188.

[3]– عبد الوهاب جعيجع، مرجع السابق، ص 78

الفرع الأول: المعرفة الالكترونية

ان المعرفة هي خلاصـــة تجميع وترتيب مجموعة من المعلومات التي تمت معالجتها، حيث تمثل حصيلة خبرة طويلة لها قيمة وفائدة في اتخاذ القرار.[1]

أولا: دور المعرفة الالكترونية في حسن سير التحقيق في الجرائم المعلوماتية

تعد المعرفة الالكترونية أسـاس فاعلية التحقيق في الجرائم المعلوماتية وتصـنف نسـبة المعرفة من خلال معيار القدرة على الخلق والابتكار اضـــافة الى قدرة أجهزة التحقيق على مسايرة التطورات التكنولوجية.[2]

وقدرة المحقق على الالمام بالجوانب التقنية والفنية للحاسب الآلي ومعرفة مجموعة من العناصـــر أهمها المكونات المادية للأجهزة الرقمية وطريقة التعامل معها اضـــافة الى تمييز أنظمة التشـغيل والتعرف على صـيغة الملفات وتطبيقات الحاسـب الآلي، ومعرفة أسـاليب وأدوات ارتكاب الجرائم المعلوماتية اضـــافة الى الالمام بمهارة تقييم الجريمة المعلوماتية ومعرفة أهم ما يميزها.[3]

ثانيا: المهارات المكتسبة عن طريق التدريب

من بين المهارات التي تكتســـب عن طريق التدريب المهارات التقنية التي تتضـــمن أســاســيات صــيانة الحاســب الآلي والأجهزة والخبرة في مجال الشــبكات والمعرفة اللازمة بالإجراءات القانونية والقضـائية المطبقة والالمام بأمن الشـبكات، أو مهارات العرض والتوثيق

[1]– عباس لحمر، البعد الاستراتيجي لتكنولوجيا المعلومات والاتصال، دار هومة، 2018، الجزائر، ص 238.

[2]– مصطفى محمد موسى، مرجع سابق، ص 297.

[3]–نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة الأندلس للعلوم الانسانية والاجتماعية، العدد 13، المجلد 15، سنة 2017، ص 310.

حيث يلتزم المحقق بكتابة التقارير مفصلة ومباشرة وواضحة سهلة الفهم حول الحقائق التي عثر عليها.

اضافة الى المهارات المهنية التي تزيد من مصداقية وحيادية المحقق بتعامله بشكل مهني مع من يطلب منه المشـــورة، فليس كافيا أن يكون المحقق قادرا على تحليل الأدلة بل يجب أن يكون قادرا على شـرح وعرض وتوثيق هذه الأدلة بطريقة مفهومة لأشـخاص قد لا يكونون مختصين في مجال تقنية المعلومات.[1]

وتعتبر الولايات المتحدة أول دولة عنيت بتوفير التدريب اللازم لمواجهة الجرائم المعلوماتية و التحقيق فيها من خلال عقد دورات متخصـــصـــة من قبل أكاديمية مكتب التحقيقات الفدرالية لتزويد محققي الشـرطة والعاملين في الادارات الجنائية بمعارف و مهارات حول برمجة الحاسب و تشغيله، مع استخدام تطبيق بنكي مصغر وحاسب آلي، من خلال عقد حملات تدريبية تقوم على رفع نســـبة المعرفة الالكترونية، حيث أنه بعد تصـــاعد الاعتداءات على مواقع الانترنت لشـــركات أمريكية كبرى، التزمت وزارة العدل الأمريكية و مكتب التحقيقات الفدرالي بملاحقة المسـؤولين عن هذه الأعمال و التأكد من تنفيذ العقوبات عليهم حتى تظل شبكة الانترنت بيئة آمنة لممارسة الأعمال و التجارة الالكترونية، و اعتبرت الحكومة الأمريكية هذه الاعتداءات هجوما على المصـــالح الأمريكية لحرمانها من عائدات الانترنت.[2]

[1]–عبد الله القحطاني، التحقيق الجنائي الرقمي 06، المجموعة السعودية لأمن المعلومات، hemaya groupe https://www.youtube.com/watch?v=JKxEccd8feA ، تاريخ الدخول 06–06–2019، ساعة 10.21 الى 10.30.

[2]– محمد نصر محمد، مرجع سابق، ص 66–67.

ثالثا: اتقان استخدام الوسائل المساعدة في التحقيق

ان الأجهزة المكلفة بالتحقيق تستعين بمجموعة من الوسائل والأدوات التي تساعد على كشف المتورطين[1]، ومن ثم تساعد في ضمان فاعلية التحقيق والتي يجب على المحقق اتقان استخدامها، وتنقسم الى وسائل مادية ووسائل اجرائية.

1-الوسائل التقنية المادية

تتعدد الوسائل التقنية المادية المساعدة في التحقيق وأبرزها ما يلي:

-**عنوان IP:** هو رقم تسلسلي يمنح لكل جهاز الكتروني مرتبط بشبكة الاتصال، قد يكون دائم أو مؤقت مثال: شكل الIP الداخلي(192.168.3.1) وشكل الIP الخارجي (105.103.56.45) IPv4 و هناك اصدار 6 و هو أطول (IPV6)، و تسمح هذه العناوين بتسليم معلومات الى جهاز معين.[2]

عند ارتكاب جريمة معلوماتية فأول ما يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة مرتكب الجريمة، ويمكن لمزودي خدمات الانترنت مراقبة المشترك، كما يمكن للشبكة التي تقدم خدمات الاتصال الهاتفي ان تقوم بمراقبة المعني إذا توفرت برامج واجهزة خاصة بذلك.[3]

-**عنوان التحكم بالنفاذ الوسطAdresse MAC:** وهو عبارة عن عنوان دائم و فريد لجهاز الحاسب الآلي مخزن في كل بطاقة شبكة، بمثابة هوية الجهاز يتم من خلاله تعريف بطاقة

[1] -Broadhead.S, The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law and Security Review, 34 (6), 2018, p 18.

[2] -Perez C, Sokolova K, La Cybersécurité, Studyrama, 2018, France , p57.

[3]- خالد عياد الحلبي، مرجع سابق، ص 206.

الشـبكة و المودم و غيرها من طرق الاتصـال بالإنترنت. حيث يمكن تتبع أي شـخص عبر جهاز الحاسب الآلي، أو الهواتف الذكية عبر عنوان Mac.

-**الخادم الوكيل** (Proxy): وهو عبارة عن جهاز له وظيفة التوسـط بين أجهزة الكمبيوتر على الشـبكة المحلية (وتسـتعمل في بعض الأحيان بروتوكول TCP/IP، و الانترنت)، ويسـتعمل الخادم الوكيل Proxy في معظم الاحيان الويب وبالتالي هو وكيل HTTP، وقد يكون هناك خوادم أخرى لكل بروتوكول مثال تطبيق (FTP).. وهذا الخادم الوكيل Proxy يمنح مسـتوى عال من الأمن[1]

ويسـتعمل الخادم الوكيل عادة للوصـول الى الأماكن المحجوبة بواسـطة قيود معينة، ويمكنه كذلك تخزين الصفحات التي غالبا ما يستشيرها المستخدمون[2].

-**أدوات الضـبط:** وهي من الوسـائل المادية التي تحتاجها جهات التحقيق وجمع الاسـتدلالات، كمعظم برامج الحماية وأدوات المراجعة، وأدوات مراقبة المسـتخدمين للشـبكة، وأدوات التنصـت على الشـبكة، ومختلف التقارير التي تنتجها نظم أمن البيانات ومراجعة قاعدة البيانات وبرامج النسـخ الاحتياطي والتسـجيل، ومختلف أدوات الضـبط الأخرى كنظام كشف الاختراق ويمكن استخدام عدة أدوات مثال أدوات جمع المعلومات عن الزائرين للمواقع كبرمجيات Java Appletsأو Cookies.[3]

-اضـافة الى برامج التتبع التي تفيد في كشـف الاختراق، وعدة أدوات لفحص بروتوكول الانترنت TCP/IP (كأداة ARP، برنامج Visual Route، أداة Tracer، أداة stat Net.) والتي تفيد

[1] -Pierre Emmanuel Périllon, L'usage des proxy dans une infrastructure réseau, travail de recherche bibliographique, université Claude Bernard, Lyon 1, 2007-2008, p 19.

[2] -Charles Perez، Karina Sokolova, op cit, p 62.

[3]- خالد عياد الحلبي، مرجع سابق، ص 210.

في فحص الشـــبكات ومراقبتها، وعدة أدوات أخرى تســـاعد التحقيق في الجرائم المعلوماتية كالمستخدمة في التدقيق والمراجعة لمختلف عمليات الحاسب الآلي.

- نظم كشف الاختراق IDS وIPS

نظام كشـــف الاختراق IDS : وهو عبارة عن برنامج تحليلي لرزم البيانات المتنقلة عبر الشبكة و من بعض ملفات نظام التشغيل الخاصة بتسجيل الاحداث فور وقوعها على اجهزة الحاسب الآلي أو الشبكة، و من ثم مقارنة نتائج التحليل مع مجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها: مصطلح التوقيع، ففي حالة اكتشاف احد التواقيع يقوم بإرسال تحذير الى مدير الشبكة بوجوب الكشف عن الثغرات الموجودة في نظام الحماية، و تحديد الأخطاء و تصحيحها و يسجل البيانات الخاصة بهذا الاعتداء في سجلات خاصة على الحاسب الآلي.[1] ثم ظهر **نظام كشف الاختراق IPS:** وهو نسخة مطورة من النظام الســابق يقوم بعملية الكشــف أولا ثم التنفيذ وفقا لردة فعل معينة، و تســاعد هذه الوســيلة المحقق في معرفة مصــدر الجريمة المعلوماتية ، أو الأســلوب أو الطريقة الذي ارتكبت بها.

-نظام جرة العســل (Honey Pot): هو عبارة عن جهاز وهمي يســاعد في عملية التحقيق الجنائي، يقوم بعمله على الشــبكة المحلية للإطاحة بالمخترق أو ادانته قانونيا، حيث عند استهداف المخترق لجهاز معين وشن هجماته وأخذ ما يريده من بيانات مزيفة، يقوم المحقق بتتبع أثره ومعرفة طريقة تفكيره، ومعرفة غايته وماذا ســيفعل بالجهاز وتحليل هجماته على الجهاز الوهمي.[2]

---

[1]- خالد ممدوح ابراهيم، مرجع سابق، ص 307.

[2]- مركز iscur1tyللدورات التدريبية، مجتمع عربي مختص بأمن المعلومات، /مقال-دور-honeypot-بالإختراق/isecur1ty.org، تاريخ الدخول 07-06-2019، ساعة 11.00 الى 11.30.

2-الوسائل الاجرائية:

تعتمد الاجهزة المكلفة بالتحقيق على مجموعة من الوسائل الاجرائية اللازمة لضمان فاعلية التحقيق ومن أبرزها:

-حماية النظام المعلوماتي

لعل أهم وسيلة هي حماية النظام المعلوماتي حيث يتطلب للتحقيق في الجرائم المعلوماتية الاطلاع على النظام المعلوماتي بمكوناته (من شبكات، تطبيقات، خدمات) وبعملياته (كقاعدة البيانات، ادارتها، تأمينها، معرفة مواد النظام، المستفيدين منه، الملفات، الاجراءات، تصنيف الموارد العامة وغيرها)

ولابد من معرفة نوع برامج الحماية والاستعانة بها، الاستفادة من مختلف التقارير التي تنتجها نظم أمن البيانات وتقارير الجدران النارية.[1]

وهنا تظهر اشكالية رئيسية تتمثل في تكلفة الهجمات الالكترونية حيث نكون أمام احتمالين اما أن ندفع مقابل الحماية من شراء البرامج ونظم الحماية الالكترونية اللازمة أو نتحمل النتائج الوخيمة التي ترتبها الهجمات.

-التأكد من الجريمة وتقصى آثرها في مسرح الجريمة

ان أول نصيحة يقدمها البعض عبر مواقع خاصة للمخترقين هي مسح الآثار التي من الممكن أن تؤدي الى اكتشافهم، وغالبا يكون التقصي للأثار متوقفا على نوع الدليل وقوته، وقد يعتمد على الخبرة والقوانين المعترف بها، فالمحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملما بمهارات هذه التقنية، كالقدرة على استخدام برنامج

[1]- خالد عياد الحلبي، مرجع سابق، ص 214.

Timestamp، وهي البرامج التي يتم من خلالها تحديد زمن ارتكاب السلوك الاجرامي، كما ينبغي أن يكون الخبير ملما بمهارات تحليل البيانات والتشفير. [1]

وتجدر الاشارة أن تقصي الأثر يكون بعدة طرق: سواء عن طريق بريد الكتروني تم استقباله، أو عن طريق تتبع أثر الجهاز المستخدم في عملية الاختراق.[2]

وينبغي على جهات التحقيق التثبت من الجريمة ودراسة مختلف عناصرها من استظهار لأركان الجريمة ووقت ومكان ارتكابها اضافة الى احترام مختلف المبادئ الأساسية للتحقيق في الجرائم المعلوماتية.

-الاستعانة بالذكاء الاصطناعي

ان الذكاء الاصطناعي هو البحث عن الوسائل التي من المحتمل أن تزود أنظمة الحاسب الآلي بقدرات فكرية مماثلة لتلك التي لدى البشر[3]

ويمكن الاستعانة به في مجال التحقيق في الجرائم المعلوماتية حيث يتم من خلاله التوصل لنتائج مبنية على حقائق واحتمالات واسباب وفرضيات، تستنتج عن طريق معاملات حسابية يتم تحليلها بالحاسب الآلي وفقا لبرامج خاصة مصممة لهذا الغرض[4]

[1]- احسان طبال، النظام القانوني للتحقيق الدولي في جرائم الكمبيوتر، اطروحة دكتوراه في الحقوق، كلية الحقوق، جامعة الجزائر 1، 2013.2014، ص 83.

[2]- علي عدنان الفيل، مرجع سابق، ص 77.

[3] Sabouret N, comprendre l'intelligence artificielle, ellipses, 2019, France, p 18.

[4]- خالد عياد الحلبي، مرجع سابق، ص 214.

وتعتمد نظرية الذكاء الاصـــطناعي على الآثار الموجودة في مســـرح الجريمة وأقوال الشهود والقرائن التي يتم تحليلها تحليلا منطقيا بالقدر الذي يتوافق مع الحقائق والأسباب.[1]

الفرع الثاني: أساس تطبيق المعرفة الالكترونية

ان السرية والسرعة باعتبارهم أساس تطبيق المعرفة الالكترونية إضافة الى التكوين الجيد في مجال التحقيق في الجرائم المعلوماتية أمر لازم لضمان فاعليته.

أولا: احترام مبدأ السرعة

تعتبر الســـرعة أســـاس تطبيق المعرفة الالكترونية، فنتيجة للتطورات المتســـارعة للتكنولوجيا الحديثة وظهور أساليب الكترونية وأشكال جديدة من الجرائم المعلوماتية، استدعى اعتماد الســرعة الالكترونية في مجال التحقيق في الجرائم المعلوماتية ويقصـــد بذلك ســـرعة دوران البيانات والمعلومات عبر الوسائط الالكترونية.

ويبرز دور المحقق من خلال قوة الملاحظة وسرعة البديهة في تتبع المتهمين والشهود والالتزام بتسـريع الاجراءات الواجبة واخطار الخبراء الفنيين، حيث تضـمن السـرعة الوصـول الى الحقيقة دون تلف الدليل أو ضياعه ودون طمس لمعالم الجريمة الالكترونية وآثارها.

ثانيا: كتمان السر المهني

ان اضفاء السرية على اجراءات التحقيق في الجرائم المعلوماتية يضمن الوصول الى الحقيقة، حيث يلتزم المحقق بالســـرية فيما يخص جميع المراحل ســـواء ما يتعلق بتدابير

[1]– محمد الأمين البشري، الأدلة الجنائية الرقمية مفهومها ودورها في الاثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد 33، ص 126.

الكشـــف عن الجريمة المعلوماتية أو التحقيق فيها أو المحاكمة، وهذا بغرض حصـــر نطاق الجريمة وعدم افلات المجرمين من العقاب.

وقد نصـــت للمادة 11 من قانون الاجراءات الجزائية الجزائري في الفقرة الثانية على وجوب الالتزام بالسر المهني.

وبالتالي تعتبر ســـرية أي أخبار أو معلومات متعلقة بالتحقيق في الجرائم المعلوماتية كما هو الشـــأن في المعلومات المتصـــلة بتحريك الدعوى والأمر بالقبض على أحد الجناة الالكترونيين أو التفتيش لشخصه أو مسكنه أو حاسوبه الشخصي، كذلك المعلومات المتعلقة باستجواب المتهمين أو أقوال الشهود أثناء التحقيق، اجراءات المعاينة والمواجهة وقرار الاتهام أو الامر ان لا وجه لإقامة الدعوى لما تتضمنه من معلومات مستمدة من التحقيق.[1]

ثالثا: التكوين المستمر

ان قلة خبرة أجهزة الضبط القضائي والجهات القضائية في مجال الجرائم المعلوماتية لتمحيص عناصـر الجريمة و جمع المعلومات و الأدلة عنها، قد تكون سـببا في اعاقة سـير التحقيق، حيث تجد الجهات المكلفة بالتحقيق نفســـها غير قادرة على التعامل بالوســـائل الاســـتدلالية، و الاجراءات التقليدية مع هذه الجرائم، خاصـــة أن المجرمين المعلوماتيين محترفون في تخزين البيانات المتعلقة بنشـــاطاتهم الاجرامية في أنظمة تقنية المعلومات باستخدام شفرات أو رموز سرية لإخفائها عن أجهزة العدالة، مما يثير مشاكل في جمع الأدلة الجنائية، وتصطدم الأجهزة المكلفة بالتحقيق بصعوبة في الوصول الى الدليل.[2]

[1]– مصطفى محمد موسى، مرجع سابق، ص 307.

[2]– فهد عبد الله العبيد العازمي، مرجع سابق، ص 139.

لذا لا بد من ايجاد أســـلوب خاص للتحقيق يجمع بين الخبرة الفنية و الكفاءة المهنية من خلال تبادل المعلومات بين المحقق و خبير المعلوماتية، و حصـــر النقاط المطلوب اســـتجلائها من قبل الخبير و المحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب النقاط، أخذ أقوال الشهود و استجواب المتهمين من قبل المحقق بحضور الخبير الذي يجوز له توجيه أسئلة فرعية، التنسيق بين المحقق و الخبير في الحصول على البيانات المخزنة في الحاسب الآلي و ملحقاته الخاصة بالشاهد أو المتهم الذي تم التحقيق معه مع مراعاة عدم اجباره على تقديم دليل ضده.[1]

كما ينبغي رسم أطر قانونية محكمة تضم الجانب التقني والجانب العملي معا وذلك من خلال تكوين متخصصين في مواجهة الجرائم المعلوماتية.

[1]– علي عدنان الفيل، مرجع سابق، ص 85.

المطلب الثاني: تعامل المحقق مع الأدلة الالكترونية

ان الأدلة الجنائية عبارة عن وقائع مادية أو معنوية من شأنها أن تكشف عن الجريمة وتزيل الغموض حولها، فهي برهان لصحة الوقائع موضوع التحقيق، وهي وسيلة تعتمد عليها الشرطة وأجهزة العدالة في اثبات وتقصي الحقائق حول الوقائع، الأشخاص والأشياء، وصولا الى العدل كغاية يتطلع لها أفراد المجتمع.[1]

ولقد تطرقنا في هذا المطلب لكيفية التعامل مع الأدلة الالكترونية، وابراز أهم الاشكالات التي تعيق سير اجراءات التحقيق.

الفرع الأول: كيفية التعامل مع الأدلة الالكترونية

ان التعامل بالأدلة الالكترونية يفرض تحديد خصوصياتها وتقسيماتها، باعتبارها ذات طبيعة خاصة يتطلب التعامل معها اتباع خطوات أساسية للوقاية من تلفها أو ضياعها.

أولا: خصوصية الأدلة الالكترونية

ان الدليل الالكتروني متميز عن الدليل العادي من عدة جوانب يمكن اجمالها في النقاط التالية:

-**الدليل الالكتروني دليل علمي:** فالعلوم الجنائية تقدم لنا الأدوات والتقنيات والأساليب النظامية التي يمكن استخدامها لتحليل الأدلة الرقمية، والاستفادة منها في اعادة تكوين ما حدث أثناء ارتكاب الجريمة وصولا الى الربط بين الجاني والضحية ومسرح الجريمة، وعلى

[1]- محمد الأمين البشري، الأدلة الجنائية الرقمية مفهومها ودورها في الاثبات، مرجع سابق، ص 93.

هذا النحو يمكن النظر الى الدليل الرقمي كعمل علمي يندرج تحت العلوم القضـائية ويسـري عليه الكثير من قواعد القانون والأحكام المنظمة للأدلة.[1]

ولا يمكن الحصـول على الدليل الالكتروني أو الاطلاع على فحواه أو حفظة سـوى باسـتخدام أسـاليب مبنية على أسس علمية، حيث تفيد هذه الخاصـية سـلطات التحقيق بالتعامل مع هذا الدليل سعيا وراء اثبات الحقيقة.[2]

-**الدليل الالكتروني دليل تقني:** لابد أن يتعامل معه تقنيين متخصـصـين في الأدلة الجنائية العلمية و البيئة الافتراضـية خصـوصـا، ولابد من توافق بين الدليل المسـتخلص و البيئة التي تكون فيها، لأن التقنية لا تبرز مسـرح الجريمة و ما فيه من أدلة وانما تبرز الدليل في حد ذاته القائم على نبضـات مغناطيسـية أو كهربائية، تشـكل لنا معلومة يمكن اعتمادها كدليل اثبات، وهذا الدليل يتكون من بيانات ومعلومات ذات طبيعة الكترونية غير ملموسة، لا تدرك بالحواس العادية بل يتطلب ادراكها الاسـتعانة بأجهزة و معدات و أدوات الحاسـب الآلي (Hardware)، و استخدام نظم برامجية حاسوبية (Software)[3].

- **دليل قابل للتطور باسـتمرار:** حيث يواكب الدليل الالكتروني التطورات الحاصـلة في المجال الالكتروني، ليصبح ناجعا في اكتشاف الجرائم ومرتكبيها واثباتها، فهو في تطور دائم وغير محصور في مكان وزمان معين.

[1]- محمد الأمين البشري، مرجع سابق، ص 126.

[2]- حازم محمد حنفي، مرجع سابق، ص 17.

[3]- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص 14.

-**دليل غير محصور في نطاق معين:** فاذا كان مسرح الجريمة وملحقاتها، مستودعا للأدلة الجنائية التقليدية، فالأدلة الجنائية الرقمية مستودعها هو محيط واسع من الشبكات المعلوماتية والبرامج وأجهزة الحاسوب المنتشرة في نطاق غير محدود.[1]

-**الدليل الالكتروني سريع الانتقال:** حيث ينتقل الدليل الالكتروني بشكل سريع ويتعدى بذلك الحدود المكانية والزمانية، ويمكن أن يتسع مسرحه عالميا، مما يمكن الجناة من تبادل المعارف الرقمية بسرعة كبير في عدة دول، ويصعب من اجراء التحقيق.

-**دليل متنوع:** فمصطلح الدليل الالكتروني يشمل كافة أنواع وأشكال البيانات الرقمية الممكن تداولها في المجال المعلوماتي، ويمكن لهذا الدليل أن يظهر في هيئات مختلفة كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات أو الخوادم، وقد يكون واضحا كالوثائق المعدة بنظام المعالجة الآلية للكلمات أو تكون مخزنة في البريد الالكتروني، وقد يكون مرتبط بالتشفير للحد من العدوان على حقوق المؤلف الذي يعد مسألة مكتسحة للعالم الافتراضي.[2]

يكون الدليل الالكتروني في الواقعة الافتراضية التي تبدأ وتنتهي في العالم الافتراضي، بحيث يكون كل من الدليل الرقمي والجريمة الافتراضية صورة للآخر، ويحقق القانون صفة التجريم والواقعة الافتراضية، وكذلك يمكن أن يستعان بالدليل الرقمي في الواقعة المزدوجة وهي الواقعة المادية الممزوجة بطابع رقمي.[3]

[1]- محمد الأمين البشري، الأدلة الجنائية الرقمية مفهومها ودورها في الاثبات، مرجع سابق، ص 92.

[2]- حازم محمد حنفي، مرجع سابق، ص 20.

[3]- ميسون خلف الحمداني، علي محمد كاظم الموسوي، الدليل الرقمي وعلاقته بالمساس بالحق في الخصوصية المعلوماتية أثناء اثبات الجريمة، جامعة النهرين، العراق، 2016، ص21.

-**دليل ذو وظيفة مزدوجة:** حيث يرصد معلومات عن المجرم ويسجل كل تحركاته وسلوكياته في سجلات خاصة في النظام المعلوماتي ويحلل هذه المعلومات والبيانات المسجلة في نفس الوقت. ويكون ذلك بتحويل المعلومات المسجلة الى أرقام ثم معالجتها.

حيث تترجم النصوص والحروف والأرقام والصور والفيديوهات الى صيغ رقمية ذات طبيعة ثنائية تتكون من سلسلة من رقم (0 و1)، يمثل الصفر (0) وضع الاغلاق off، والواحد (1) وضع التشغيل on، ويمثل الرقم (0 و1) ما يعرف بالبيت bit، ويشكل عدد 8bitsما يعرف بالبايت byte.

- **دليل يصعب التخلص منه:** ففي حالة محاولة اصدار أمر بإزالة ذلك الدليل فمن الممكن اعادة اظهاره من خلال ذاكرة الآلة التي تحتوي على الدليل، وكذلك فمحاولة الجاني محو الدليل الرقمي يسجل عليه كدليل، حيث أن قيامه بذلك يسجل في ذاكرة الآلة وهو ما يمكن استخراجه واستخدامه كدليل ضده، وتمكن الطبيعة الفنية للدليل الرقمي من اخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا تم العبث والتحريف. [1]

وتجدر الاشارة الى أنه يمكن استخراج عدة نسخ من الأدلة الجنائية الرقمية مطابقة للأصل، ولها نفس القيمة العلمية والحجية الثبوتية[2]. وبهذا يكون الدليل الالكتروني متميز عن الدليل المادي الذي يمكن التخلص منه بإخفاء معالم الجريمة كمسح البصمات من مسرح الجريمة، أو تمزيق أو حرق أوراق معينة تدين شخص في جريمة معينة.

[1]- طارق محمد الجملي، الدليل الرقمي في مجال الاثبات الجنائي، المؤتمر المغاربي الأول حول المعلوماتية والقانون، يوم 28-29-10-2009، أكاديمية الدراسات العليا، طرابلس، ص 03.

[2]- ميسون خلف الحمداني، علي محمد كاظم الموسوي، مرجع سابق، ص 24.

ثانيا: تقسيمات الأدلة الالكترونية

أشـارت وزارة العدل الأمريكية الى انقسـام الادلة الالكترونية الى ثلاث فئات: يشـمل النوع الأول السـجلات المحفوظة في الحاسـب الآلي و تشـمل الوثائق المكتوبة و المحفوظة كالبريد الالكتروني ورسـائل غرف الدردشـة و ملفات معالجة البيانات، في حين يشـمل النوع الثاني السجلات التي يتم انشاؤها بواسطة الحاسب الآلي و لم يشارك الاشخاص في اعدادها، كسـجلات الهواتف و فواتير أجهزة السـحب الآلي للنقود، و تشـمل الفئة الثالثة: السـجلات المختلطة تم حفظ جزء منها بالإدخال و تم انشـاء الجزء الآخر عن طريق الحاسـب الآلي كأوراق العمل المالية التي تم حفظها بالإدخال ثم معالجتها عن طريق برنامج Excel لإجراء العمليات الحسابية عليها.[1]

في حين أن هناك من قسم الأدلة الالكترونية الى أدلة أعدت لتكون وسيلة اثبات وأدلة لم تعد لتكون وسيلة اثبات:

وفي ذلك تشـمل الأدلة التي أعدت لتكون وسـيلة اثبات السـجلات التي تنشـأ تلقائيا، تعتبر من مخرجات الحاسـب الآلي كسـجلات الهاتف وفواتير البطاقات البنكية، أو فواتير أجهزة السحب الآلي ATM[2]

اضـافة الى السـجلات المتكونة من جزأين: جزء أنشـأه الحاسـوب تلقائيا وجزء أدخل فيه، كالوثائق المكتوبة ورسـائل البريد الالكتروني، ورسـائل في مواقع الدردشـة المختلفة على الانترنت.

[1]– عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص 14.

[2]– طارق محمد الجملي، مرجع سابق، ص 04.

أما الأدلة لم تعد أساسا لتكون وسيلة اثبات: تتعلق بالآثار المعلوماتية الالكترونية ومنها ما يعرف بالبصمة الالكترونية، حيث لا تتجه ارادة الجاني الى ترك آثار عند اتصاله بشبكة الانترنت، غير أن الوسائل الفنية الخاصة، يمكنها ضبط اي اتصال أو محادثة تمت عبر شبكة الانترنت.

ولعل الدليل الالكتروني كما يمكن استخلاصه من جهاز الكمبيوتر وملحقاته فأيضا يمكن استخلاصه من أي تقنية حديثة كالهاتف النقال الذكي والايباد(ipad) وغيرها من وسائل الاتصال الحديثة، أو من الآلات الطابعة ومخرجاتها، والمودم، ووسائط التخزين كالأقراص المدمجة cd، أو من ذاكرة فلاش USB، أو الشريط الممغنط magnetic tapes، أو من القرص الثابت، وأيضا من البطاقات الممغنطة.

وتجدر الاشارة الى أن جهاز كمبيوتر واحد يمكن أن يحتوي على أدلة لوجود نشاط إجرامي يجري على شبكة الإنترنت، أو يمكن أن يكون في جهاز الكمبيوتر نفسه، مثل المواد الإباحية، والتعدي على حقوق المؤلف والابتزاز والتزوير وأكثر من ذلك بكثير. فتتواجد الأدلة الالكترونية على القرص الصلب والمعدات والطرفية الثابتة للكمبيوتر، بما في ذلك الوسائط القابلة للإزالة[1].

وتصلح الأجهزة المحمولة كدليل في كثير من الجرائم، حيث أنها تسمح للمجرم بالقيام بعدة جرائم أو المساعدة والمشاركة في ارتكابها، وبالتالي تتبع أي خطوة يخطوها الجاني في سبيل اتمام جريمة أو مساعدة على اتمامها، فهذه الأجهزة وبعدما كانت غير متطورة وتستخدم للاتصال فقط، فالآن أصبحت لالتقاط الصور الرقمية، تصفح شبكات الانترنت

[1]- iscurity، دليل مبسط للتعامل مع الأدلة الرقمية، مركز تدريب في أمن المعلومات، https://www.isecur1ty.org، تاريخ الدخول 07-06-2019، ساعة 11.00 الى 11.30.

وارسال رسائل فورية وأصبح دورها لا يقل شأنا عن جهاز الكمبيوتر، كذلك الايباد وهو جهاز كمبيوتر مصغر يمكن أن يحتوي أدلة رقمية تثبت جرائم معينة.

هذا ويعتبر جهاز الكمبيوتر متصـل بموفر خدمة الانترنت (ISP) والذي يعد جزءا من شـبكة مزود خدمات الانترنت، وكل مزود خدمة يتصـل بشـبكة أخرى فتعتبر شـبكة الانترنت بذلك عبارة عن مجموعة شـبكات حيث يمكن ارسـال واسـتقبال المعلومات من أي نقطة الى اخرى على هذه الشـبكة، وهذه المجموعة العالمية من الشـبكات لا يوجد لها مالك أو شـبكة مسيطرة، فهي تعمل كالمجتمع له ايجابيات وسلبيات.[1]

ثالثا: خطوات التعامل مع الأدلة الالكترونية

ان التحقيق في الجرائم المعلوماتية، يسـتدعي أن يعتمد الدليل الالكتروني من قبل المحاكم والجهات المختصـة، وفي سـبيل ذلك يتخذ مجرى التحقيق مجموعة من الخطوات الأساسية تتمثل في:

- جمع الأدلة
- فحص الأدلة
- تحليل ومراجعة الأدلة
- عمل تقرير بجميع الاثباتات الرقمية المستخرجة من الأدلة[2]

حيث ينبغي على المحقق السيطرة التحكم بالأدلة ولابد من تمييز الأدلة وتوثيق كل ما يعثر عليه في مسـرح الجريمة والاسـتمرار في التوثيق خلال فترة التحقيق كاملة، وفي هذا

[1]– iscurity، دليل مبسط للتعامل مع الأدلة الرقمية، مركز تدريب في أمن المعلومات، https://www.isecur1ty.org، تاريخ الدخول 07-06-2019، ساعة 11.00 الى 11.30.

[2]– أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، مرجع سابق، ص 260.

يلتزم بتحديد مصدر الدليل الالكتروني المتوقع حتى يتم الحصول عليه بصورة رقمية تمهيدا لفحصه وتحليله.

وهناك من يرى أن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي ترتبط بها الأجهزة محل التحقيق و لعل أبرز الأماكن التي يحتمل وجود الأدلة الجنائية المتعلقة بالجرائم المعلوماتية فيها هي: الورق، المكونات المادية، البرامجSoftware، وسائط التخزين المتحركة، دليل الاستخدام Manuals الخاص بالمكونات المادية و المنطقية للحاسب الآلي و التي تفيد في معرفة التفاصيل الدقيقة لكيفية عملها، و كذلك مجلات الحاسب و الأوراق المطبوعة، كما أن كلمات السر أو ارقام الهاتف التي قد تكون مكتوبة على أوراق ملصقة بالحواسب أو بقربها قد تكون خاصة بحسابات الاتصال بشبكة الانترنت أو بعض خدمات الانترنت المختلفة أو بفك تشفير بعض البيانات التي قد تحتوي أدلة تفيد في الوصول الى الحقيقة.[1]

بعد القيام بهذه الاجراءات المحقق برسم خطة توضح الطريقة التي سيقوم باتخاذها حيث يحدد الأدوات المناسبة وكيفية استخدامها للحصول على الدليل الالكتروني، ثم يبدأ في استخراج البيانات التي يكون مصدرها مختلف قد يكون قرص صلب، ذاكرة عشوائية، أقراص خارجية... وغيرها، ليقوم فيما بعد بالتأكد من سلامة البيانات المستخرجة.

بعد هذه المرحلة يكون على المحقق الدقة في تحليل الأدلة حيث تعتبر هذه المرحلة الأكثر تحديا تستغرق الكثير من الوقت وتحتاج قدرا عاليا من المهارة التقنية خلال فترة التحقيق الجنائي، تحدد فيها الاستنتاجات وتربط الأحداث والمشتبه فيهم.

[1]– حازم محمد حنفي، مرجع سابق، ص 60.

عند الانتهاء من تحليل الأدلة، على المحقق كتابة تقريرين: التقرير الأول هو تقرير تقني لعملية التحقيق مع النتائج، والتقرير الثاني هو تقرير عام للشخص العادي الذي لا يملك خبرة فنية.[1]

ومن هنا يبرز دور المحقق في التعامل مع الأدلة الالكترونية، من خلال قدرته على السيطرة والتحكم بالأدلة، مع التزامه بتحليلها بدقة، وكتابة التقارير المتحصل عليها.

الفرع الثاني: إشكالية التعامل مع الأدلة الالكترونية

ان أساس أي قضية تنطوي على أدلة الكترونية هو التعامل الصحيح مع الأدلة[2]، وتبقى مجموعة صعوبات تواجه المحقق في ذلك.

أولا: صعوبات التعامل مع الأدلة الالكترونية

ان من أبرز الصعوبات التي تواجه المحقق عند التعامل بالأدلة الالكترونية:

- مشاكل الدليل باعتباره غير مرئي ولا وجود لآثار مادية تقليدية مع صعوبة الوصول الى الدليل بسبب استخدام وسائل حماية فنية ككلمات السر حول المواقع تمنع الوصول اليها أو تدميرها أو تشفيرها لإعاقة الوصول لها والاطلاع على محتواها أو استنساخها.[3]

- سهولة محو الدليل الالكتروني أو تدميره في مدة قصيرة تعتبر من الصعوبات التي تواجه مكافحة هذه الجريمة ومن التطبيقات العملية ما قام به مجرم معلوماتي في ألمانيا حيث برمج نظامه الأمني لحماية البيانات المخزنة في حاسوبه من محاولات الوصول اليها، بطريقة

[1]– أحمد محمد عبد الباقي، مرجع سابق، ص 264.

[2] - Mugisha D , Digital Forensics : Digital Evidence in judicial System, international journal of cyber Criminology, 2019, p17.

[3]– على عدنان الفيل، مرجع سابق، ص 81.

تعمل على محو كل هذه البيانات بالكامل وذلك إذا تم اختراقه من شـــخص غير مرخص له بالدخول.[1]

– وجود كم هائل من المعلومات والبيانات المتعين فحصـــها، وعبورها لحدود الدولة الواحدة، حيث أن المجرم المعلوماتي من الممكن أن يكون في مكان والضـــحية في مكان آخر، وعدم معرفة مكونات الجريمة.[2]

– اضافة الى صعوبات اخرى كإمكانية تخزين البيانات والمعلومات المتعلقة بالجريمة بأنظمة وشـــبكات الكترونية موجودة في دول مختلفة، ارتكاب الجريمة عن بعد، ســـرعة تنفيذ الجرائم المعلوماتية، مساس اجراءات التفتيش بخصوصيات الأفراد.[3]

– القواعد القائمة في مجال قبول ومصـداقية الأدلة يمكن أن تثير مشـاكل عند تطبيقها، نظرا لتقييم تســـجيلات الحاســـبات في الاجراءات القضـــائية لذا ينبغي ادخال بعض التغييرات التشريعية في حالة الضرورة.[4]

ثانيا–الحلول الواردة لحسن سير اجراءات التحقيق في الجرائم المعلوماتية

–التعامل مع الأدلة الالكترونية بدقة واحترافية أكبر.

–اسناد التحقيق لشخص متخصص وعدم توزيع التحقيق في نفس الجريمة بين عدة محققين.

–تفادي الأخطاء الشائعة في التحقيق كإغفال اجراءات جوهرية أو التباطؤ في التحقيق.

–عدم اهمال المحقق لإجراء من اجراءات التحقيق وعدم اعتماده على غيره في التحقيق.

[1]– فهد عبد الله العبيد العازمي، مرجع سابق، ص 134.

[2]– خالد ممدوح ابراهيم، مرجع سابق، ص 66.

[3]– يوسف قجاج، مرجع سابق، ص 21.

[4]– خالد عياد الحلبي، مرجع سابق، ص 268.

-المتابعة المستمرة للتطورات التكنولوجية ومعرفة الوسائل التقنية والاجرائية لمواجهة الجرائم المعلوماتية.

-التدريب المستمر وتبادل الخبرات بين المتخصصين في هذا المجال سواء على المستوى الدولي أو الوطني.

-عقد ندوات دورية وابراز مختلف الجوانب القانونية المتعلقة بالتحقيق في الجرائم المعلوماتية وكيفية التعامل مع الأدلة الالكترونية.

-احداث توازن بين الواقع العملي والعلمي في اكتساب مهارات التأهيل التكنولوجي.

-تفعيل دور التعاون الدولي لاكتساب المهارات والخبرات من الدول المتقدمة.

-التقيد بالقوانين والالتزام بالإجراءات القانونية عند القيام باستخلاص الأدلة الالكترونية.

خلاصة الباب الأول:

ان مكانة التحقيق في مواجهة الجرائم المعلوماتية لا تبرز الا من خلال احترام الأجهزة المكلفة بالتحقيق للمبادئ المعترف بها قانونا وضـــمان الموازنة بين فعالية التحقيق من جهة وضـــمان حقوق الدفاع من جهة أخرى، ناهيك عن الالتزام بتدوين الاجراءات، واحترام الحيز الزماني والمكاني للجريمة، ولا يمكن القول بتحقق جريمة من الجرائم المعلوماتية الا بوجودها فعلا وتحقق مختلف عناصرها واركانها من ركن شرعي ومادي ومعنوي.

ورغم الالتزام بتحديد العناصـــر اللازمة للتحقيق الا أن طبيعة الجريمة المعلوماتية قد تحول دون نجاعة اجراء التحقيق فيها، نتيجة الصعوبات التي تواجه الأجهزة المكلفة بالتحقيق بســـبب خصـــوصـــية هذه الجريمة في امكانية عبورها لحدود الدولة، أو نتيجة حيل المجرم المعلوماتي في تحريك البيانات المجرمة وقدرته على محو الأدلة أو اخفائها، أو لجهل الضـــحايا وتخوفهم من التبليغ عن الجريمة مما يتطلب التحســـيس بوســـائل تضـــمن فاعلية التحقيق في هذه الجرائم.

ويعتبر اثبات الادلة الالكترونية اشـــكالية اخرى تصـــادف القائمين على التحقيق في الجرائم المعلوماتية، فمن جهة لابد من التقيد بمبدأ شـــرعية الاثبات والذي يقترن بقيم العدالة واخلاقياتها ومقتضيات الكرامة الانسانية، ومبدأ مشروعية الأدلة الالكترونية في الاثبات من حيث الوجود والتحصـــيل، ومن جهة أخرى تبقى مســـألة مقبولية هذه الادلة في الاثبات محل اختلاف بين التشـــريعات لاعتمادها على نظم قانونية مختلفة، ولإمكانية العبث بمضـــمون الأدلة الالكترونية مما اســـتدعى النظر في امكانية اعتمادها كدليل في الاثبات الجنائي ومدى تعارضـــها مع مبدأ قرينة البراءة، فاذا ســـلمت الادلة من العبث و الخطأ فلا يمكن للقاضـــي التشكيك في مصداقيتها.

ومن جانب آخر من الممكن أن تتعارض اجراءات التحقيق مع مبدأ الحق في الخصوصية، وفي سبيل ذلك عمدت التشريعات و من بينها المشرع الجزائري، الى الموازنة بين تكريس الحق في الخصوصية و بين تنظيم القواعد الاجرائية للوقاية من الجرائم المعلوماتية و مواجهتها، هذا و حددنا نطاق حماية الحق في الخصوصية في مواقع التواصل الاجتماعي وفي المعاملات التجارية وفي محركات البحث والبريد الالكتروني وقواعد البيانات وغيرها، حيث لابد من عدم انتهاك حرمة المواطن الخاصة، مع ضمان سرية المراسلات والاتصالات وحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

زيادة على ذلك وفي سبيل حماية الأفراد والمجتمعات وضبط الجرائم المعلوماتية والحصول على الأدلة الالكترونية التي تفيد في اثبات هذه الجرائم المستحدثة، أنشأت أجهزة متخصصة للتحقيق في هذه الجرائم كالهيئات القضائية الجزائية المتخصصة والهيئات غير القضائية والوحدات التابعة لقطاع الدرك وقطاع الأمن.

لعل فاعلية التحقيق في الجرائم المعلوماتية تتحقق بإلمام المحقق في هذه الجرائم بمهارات التأهيل التكنولوجي، وقدرته على مسايرة التطورات التكنولوجية واتقان استخدام الوسائل التقنية المادية والاجرائية، وحسن التعامل مع الأدلة الالكترونية، وهذه الأخيرة التي قد تطرح صعوبات باعتبارها غير مرئية تتطلب السرعة والدقة في التعامل معها، وتتطلب التكوين المستمر للأجهزة المكلفة بالتحقيق بما يضمن حسن سير التحقيق وفعاليته.

الباب الثاني:

آليات التحقيق في مواجهة الجرائم المعلوماتية

الباب الثاني: آليات التحقيق في مواجهة الجرائم المعلوماتية

ان أسلوب التحقيق في الجرائم المعلوماتية يتطلب تنسيقا على المستوى الوطني، و قد تدخلت القوانين الداخلية للدول من خلال اعتماد آليات اجرائية تتناسب مع خصوصية هذه الجرائم وخصوصية مرتكبيها، وتمكن الجهات المختصة من التوصل الى الجريمة و الدليل المناسب لإثباتها، واباحة المساس بالحريات الفردية و الحياة الخاصة في حدود ما ينص عليه القانون و في نفس الوقت احترام ضمانات الحق في الخصوصية، و تجريم أي اعتداء يمس حقوق و حريات الافراد دون وجه حق، وبناء على ذلك تطرقنا في الفصل الأول الى اجراءات التحقيق في الجرائم المعلوماتية.

زيادة على ذلك يجعلنا عبور الجرائم المعلوماتية لحدود الدولة الواحدة، أمام مسألة أخرى وهي وجوب التنسيق بين مختلف الدول، حيث يغدو في ذلك التعاون الدولي أمرا متحتما، والذي لا يكون فعالا الا باحترام الآليات الأمنية والفنية والقضائية.

كما لا يمكن اقامة الدليل عند التحقيق في هذه الجرائم المعاصرة الا من خلال احترام القواعد القانونية الدولية، وفقا لمبدأ المعاملة بالمثل، وابرام اتفاقيات دولية تحد من هذه الجرائم أو الانضمام الى اتفاقيات دولية سابقة كاتفاقية الاتحاد الاوروبي المتعلقة بالجريمة الالكترونية (بودابست).

وفي نفس السياق، ورغبة في تعزيز التعاون بين الدول العربية، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الانسان، أبرمت الدول العربية اتفاقيات ثنائية وجماعية، وفي ذلك تبنت الدول العربية سياسة جنائية مشتركة من خلال المصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية، والتي تهدف من ورائها الى حماية المجتمع العربي من هذه الجرائم التي تهدد أمن ومصالح الدول الأعضاء، ولذلك خصصنا الفصل الثاني لآليات التعاون الدولي في سبيل مواجهة الجرائم المعلوماتية.

الفصل الأول:

اجراءات التحقيق في الجرائم المعلوماتية

الفصل الأول: اجراءات التحقيق في الجرائم المعلوماتية

نتيجة التطورات المستمرة الحاصلة في مجال التكنولوجيا الحديثة و ما صاحبها من عصرنة القطاعات و المؤسسات، و عصرنة الاتصالات و المواصلات، والتي سهلت من حركة الأشخاص و الأموال و المعلومات (سرعة المعاملات، ربح الوقت، جهد أقل) ، و هو ما استدعى مواكبة التشريعات الداخلية و الدولية لهذه التطورات لتجنب الجرائم المعاصرة و من بينها الجرائم المرتبطة بتكنولوجيات الاعلام و الاتصال، و أصبح على كل دولة اتخاذ التدابير التشريعية و الاجراءات الضرورية لغرض التحقيق في الجرائم المعلوماتية، مع اقامة توازن بين المصالح المختصة بالكشف عن الجرائم المعلوماتية من جهة، واحترام حقوق الانسان و الحريات.

وفي سبيل نجاعة التحقيق في مواجهة الجرائم المعلوماتية تدخلت القوانين الداخلية للدول من خلال سن قواعد اجرائية تمكن الجهات المختصة من اعتمادها في سبيل الوصول الى الجريمة المعلوماتية والدليل المناسب لإثباتها،

وهو ما استدعى التساؤل حول ما يتماشى مع طبيعة العالم الافتراضي خاصة وأن استخلاص الأدلة يحكمها قواعد إجرائية معينة كالتفتيش والضبط والمعاينة والخبرة والتي تعد قواعد ذات نطاق عام صالحة لكل الجرائم، الا أن تنظيمها للجرائم المعلوماتية لابد أن يتناسب مع طبيعتها وخصوصيتها، ومع طبيعة الدليل الذي يصلح لإثباتها وهو ما استدعى البحث عن درجة ملاءمة القواعد الاجرائية التقليدية للتحقيق في الجريمة المعلوماتية ضمن المبحث الأول.

مع كل الصعوبات التي تكتنف التوصل الى الجرائم المعلوماتية ومرتكبيها خاصة مع سهولة محو آثار الجريمة وسرعة تدمير الأدلة الناجمة عنها لم تبق القوانين الاجرائية مكتوفة الأيدي وبقيت المحاولات مستمرة في سبيل في تخطي شبح الجرائم المعلوماتية وهو ما

استدعى تدعيمها بإجراءات خاصة استحدثت لتتماشى مع الجرائم الخطيرة وهو ما تم تناوله في المبحث الثاني.

المبحث الأول: الاجراءات العادية للتحقيق في الجرائم المعلوماتية

ان طبيعة الوسط الافتراضي، يتطلب اعادة تقييم منهج الاجراءات التقليدية، خاصة وأن الوسائل المستخدمة في ارتكاب الجرائم المعلوماتية تختلف عن الوسائل التقليدية، مما يتطلب مواكبة الاجراءات للتطورات الحاصلة في المجال المعلوماتي، لتسهيل التعامل مع الحاسب الآلي وكافة الأجهزة الحديثة والمحافظة على الأدلة المستخلصة منها، مع مراعاة عدم المساس بالحريات وحقوق الانسان، الا لمقتضيات التحري والتحقيق مع مراعاة الضمانات المقررة قانونا بشأنها.

وتطرقنا في هذا المبحث للتفتيش وآثاره من ضبط وحجز وبطلانه في حالة مخالفة الضمانات المحددة قانونا خاصة في حالة الاعتداء على حرمة الحياة الخاصة، من خلال المطلب الأول: تحت عنوان: اجراء التفتيش.

ونتيجة الصعوبات التي تقف حجر عائق أمام اثبات الجرائم المعلوماتية فقد يقتضي التحقيق كشف وصيانة عناصر الجريمة من خلال اجراء المعاينة أو استعانة القضاة بخبراء بغرض الاستشارة الفنية لتقدير بعض المسائل المتعلقة بموضوع الدعوى وهو ما تطرقنا له بموجب المطلب الثاني تحت عنوان: المعاينة والخبرة.

المطلب الأول: اجراء التفتيش المعلوماتي

التفتيش بوجه عام هو اجراء قضائي يهدف الى الحصول على أدلة تساعد في كشف الحقيقة، ويتميز بخاصيتي الجبر والاكراه، أي أن الانسان يخضع له مجبرا، إذا لم يوافق على اجرائه برضاه، ويتضمن هذا الاجراء مساسا بمستودع سر الانسان، سواء كان مسكنا أو في جسمه، وهو اجراء يهدف الى جمع الأدلة التي تساهم في كشف الحقيقة[1]

أما فيما يتعلق بالتفتيش المعلوماتي: عرفه بعض الفقهاء بأنه: الاطلاع على محل منحه القانون حماية خاصة باعتباره مستوع سر صاحبه، يستوي أن يكون هذا المحل جهاز حاسب آلي أو شبكة انترنت. وقد عرفه المجلس الاوروبي بأنه: اجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني.[2]

ويمكن تعريف التفتيش المعلوماتي على أنه: اجراء من اجراءات التحقيق يهدف الى الوصول الى أدلة منبثقة من جناية أو جنحة لإثبات ارتكابها ونسبتها الى المتهم، بشرط أن يكون تحقق وقوعها فعلا داخل نظم المعالجة الآلية للمعطيات.

الفرع الأول: القواعد القانونية لإجراء التفتيش المعلوماتي

يتميز اجراء التفتيش عن الجرائم المعلوماتية من حيث ضوابطه الشكلية والموضوعية، ويثار التساؤل حول مدى إمكانية تفتيش مكونات الحاسب الآلي وشبكاته؟

[1]– سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية (دراسة مقارنة)، دار الكتب القانونية، القاهرة مصر، 2011، ص 55.

[2]– عربوز فاطمة الزهراء، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل للأبحاث القانونية المعمقة، العدد 34، ص 105.

أولا: تفتيش الحاسب الآلي

يشـــتمل الحاســـب الآلي على مجموعة من المكونات المادية المتمثلة في الوحدات المختلفة (وحدات الادخال كلوحة المفاتيح والماســح الضــوئي والميكروفون، وحدات الاخراج كالشـاشـة والطابعة والسـماعات)، كما يشـتمل على مجموعة من المكونات المعنوية المتمثلة في المعلومات والبيانات المعالجة آليا، غير أن التسـاؤل يثور حول مدى قابلية هذه المكونات للتفتيش؟

أ-بالنسبة لتفتيش مكونات الحاسب الآلي المادية:

لا يوجد اشـــكال حول إمكانية خضـــوعها للتفتيش غير أن ذلك يتوقف على طبيعة المكان: فاذا كان المكان خاصـــا؛ لا يجوز تفتيشـــه الا بنفس الضـــمانات المقررة قانونا في التفتيش التقليدي، أما إذا كان المكان عاما؛ لا يجوز التفتيش الا بنفس الضـــمانات والقيود المرتبطة بتفتيش الأشـــخاص.[1] وهناك بعض التشـــريعات تبين ضـــوابط التفتيش لمكونات الحاسب الآلي، ومنها قانون المنافسة الكندي، حيث يتيح للقائم بالتفتيش امكانية استخدام أي نظام لأجهزة الحاسب الآلي لتفتيش أي بيانات، وبإمكانه أن يعمل على تسجيل تلك البيانات في شكل مطبوعات أو مخرجات أخرى.[2]

ب-بالنسبة لتفتيش مكونات الحاسب الآلي المعنوية:

هي محل خلاف فقهي، حيث يرى جانب من الفقه أن المكونات المعنوية لا تصـــلح بطبيعتها لأن تكون محلا للتفتيش والضـبط باعتبار أن التفتيش يهدف الى ضـبط أدلة مادية وهذا يقتضـي أحكاما خاصـة تكون أكثر ملائمة لتفتيش وضبط تلك البيانات غير المحسوسة،

[1]- خالد عياد الحلبي، مرجع سابق، ص 159.

[2]- يوسف بن سعيد الكلباني، الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري (دراسة مقارنة)، ط 1، دار النهضة العربية، القاهرة، 2017، ص341.

واقترح بعض الفقهاء أن تضاف للنصوص التقليدية عبارة المواد المعالجة عن طريق الحاسب الآلي أو بياناته، ويرى بعض الفقهاء في فرنسا أن النبضات والاشارات الالكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تأخذ حكم الأشياء المادية عند التفتيش.[1]

وهناك من يرى أن المكونات المعنوية تخضـــع للتفتيش مثلها مثل المكونات المادية، وعلة ذلك أن القوانين الاجرائية عندما تمنح سـلطات التحقيق امكانية ضـبط أي شـيء يكون ضــروريا لجمع الأدلة فان ذلك يجب تفســيره ليشــمل ضــبط البيانات المخزنة أو المعالجة الكترونيا، كما يشمل بيانات الحاسب الآلي غير المحسوسة [2]

اما عن موقف المشـــرع الجزائري يمكن اعتباره جعل التفتيش يمتد ليشـــمل جميع المكونـات المـاديـة والمعنويـة، وتبرير ذلـك نص المـادة 81 من قـانون الاجراءات الجزائيـة" يباشـــر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشـــياء يكون كشـــفها مفيدا لإظهار الحقيقة" حيث استعمل في نص المادة مصطلح "أشياء"

ولقد ثار خلاف حول مدى انطباق لفظ شـــيء على الكيانات المعنوية، حيث ذهب البعض الى أن لفظ شـــيء يخص ما كان ماديا ملموســـا، ولذا يقترح هذا الرأي لمواجهة القصـــور التشـــريعي أن يتم تعديل النصـــوص الخاصـــة بالتفتيش، ويضـــاف اليها ما يجعل التفتيش يشمل البحث في الوسط الافتراضـي وضبط المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب، وأخذت بعض الاتجاهات بهذا الرأي ونصـت صـراحة أن اجراءات التفتيش تشـمل أنظمة الحاسـوب ومن ذلك قانون اسـاءة اسـتعمال الحاسـوب في انجلترا لعام 1990، والمادة 3-1/19 من اتفاقية بودابســـت لســـنة 2001.[3] وذهب رأي آخر الى أن الكيانات

[1]- محمد كمال شاهين، مرجع سابق، ص 281.

[2]- يوسف بن سعيد الكلباني، مرجع سابق، ص 342.

[3]- خالد عياد الحلبي، مرجع سابق، ص 240.

المنطقية والبيانات والبرامج تشـغل حيزا ماديا في ذاكرة الحاسـوب و يمكن قياسـها بمقياس معين، وهي تأخذ شـكل نبضـات الكترونية تمثل الرقمين 0 و 1، فإنها ذات كيان مادي تتشـابه مع التيار الكهربائي الذي اعتبره الفقه والقضـاء في فرنسـا و مصـر من قبيل الاشـياء المادية، ويرى اتجاه آخر أن المشـكلة ليس مشـكلة مصـطلح، وانما امكانية اتخاذ الاجراء، وبالتالي فان تفتيش الوسط الافتراضـي يكون صحيحا اذا اسفر عن وجود بيانات اتخذت فيما بعد شـكلا ماديا، وهذا الاتجاه اخذ به قانون الاجراءات الألماني في القسـم 94 منه حينما نص على أن الادلة المضـبوطة يجب ان تكون ملموسـة، ولذلك فان البيانات اذا تمت طباعتها تعد أشياء ملموسة يمكن ضبطها.[1]

وما يسعنا القول في هذا الصدد أن هذا المصطلح جاء واسعا وغير محصور، المهم هو ان يكون مفيدا في اظهار الحقيقة والتوصـل الى الأدلة وبالتالي يمكن تطبيق القواعد العامة على الجرائم المعلوماتية ليمتد التفتيش الى جميع المكونات المادية والمعنوية للحاسـب الآلي التي تفيد في اظهار الحقيقة، كما تناول المشرع من خلال المادة 05 من القانون 09-04 القواعد الاجرائية لتفتيش المنظومات المعلوماتية من خلال إجازته للسـلطات القضـائية المختصـة وكذا ضـباط الشـرطة القضـائية الدخول بغرض التفتيش و لو عن بعد الى كل منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها أو الدخول بغرض التفتيش ولو عن بعد الى منظومة تخزين معلوماتية. [2] وهو ما يؤكد صـراحة أن المشـرع جعل من المكونات المعنوية للحاسب الآلي محل تفتيش.

[1]- خالد عياد الحلبي، مرجع سابق، ص 242.

[2]- المادة 05 من قانون رقم (09-04) المؤرخ في 5-04-2009 سالف الذكر، ص 6.

ثانيا-تفتيش شبكات الحاسب الآلي:

قد تمتد شبكات الحاسب الآلي في الدولة نفسها أو الى عدة دول:

أ-في حالة اتصال حاسب المتهم بحاسب آخر في نفس الدولة:

يرى الفقه و القانون حلا للصـــعوبات التي تثيرها القواعد التقليدية، حيث أن الفقه الألماني يرى امكانية امتداد التفتيش الى سـجلات البيانات التي تكون في موقع آخر اسـتنادا الى مقتضـــيات القســـم 103 من قانون الاجراءات الجنائية الألماني، كما ذهبت بعض التشـريعات الى جواز امتداد التفتيش الى نظام معلوماتي آخر غير النظام محل التفتيش ومن بينها: قانون تحقيق الجنايات البلجيكي الصـادر في 23 نوفمبر سـنة 2000 حيث جاء في المادة 88 منه على أن يتم الامتداد اذا كان الولوج ضـروريا لكشـف الحقيقة بشـأن الجريمة محل البحث، واذا وجدت مخاطر تتعلق بضـياع الأدلة نظرا لسـهولة محو أو اتلاف أو نقل البيانات محل البحث[1]

وقد تطرق المشـرع الجزائري لتوسـيع الصـلاحيات في تفتيش الجرائم المعلوماتية الى كامل امتداد التراب الوطني، حيث يجوز اجراؤه في كل محل سكني أو غير سكني، وفي أي وقت، بناء على اذن مســبق من وكيل الجمهورية المختص، كما يمكن لقاضـــي التحقيق أن يقوم بـأي عمليـة تفتيش ليلا أو نهـارا وفي أي مكـان على امتـداد التراب الوطني أو يـأمر ضـباط الشـرطة القضـائية المختصـين بذلك، مع امكانية اتخاذ تدابير اخرى أو الامر باتخاذ تدابير تحفظية بناء على تسخير النيابة العامة أو طلب من ضباط الشرطة القضائية.[2]

[1]- محمد كمال شاهين، مرجع سابق، ص 284.

[2]- انظر الفقرة 03 و04 من المادة 47 من الأمر 66-155، المؤرخ في 8 يونيو 1966، المتضمن قانون الاجراءات الجزائية، المعدل والمتمم.

ب-في حالة اتصال حاسب المتهم بحاسب آخر خارج حدود الدولة:

امتداد التفتيش لخارج الاقليم الوطني أو ما يعرف بالتفتيش العابر للحدود الوطنية، يتعارض مع مبدأ سيادة الدولة على اقليمها، لهذا لابد أن يتم بموجب اتفاقيات ثنائية أو دولية تجيز هذا الامتداد أو على الأقل الحصـــول على اذن من الدولة الأخرى بذلك، وقد اعتبر الفقه الالماني السماح باسترجاع بيانات تم تخزينها بالخارج أمر مشكوك فيه، خاصة في ظل غياب اتفاق متبادل بين الدول والذي يعد خرقا لحقوق الســيادة لدولة اخرى، ونفس الرأي أيده القضـــاء الالماني عندما عرضـــت عليه واقعة تتعلق بالغش المعلوماتي، حيث كانت طرفية أحد الحواسيب الموجودة في ألمانيا متصلة بسويسرا وعندما حاولت سلطات التحقيق الألمانية ضبط هذه البيانات لم تتمكن من ذلك الا من خلال التماس المساعدة المتبادلة.[1]

وقد انتهج المشـــرع الجزائري امكانية امتداد التفتيش الى خارج الاقليم الوطني وذلك وفقا لمبدأ المعاملة بالمثل وبمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات ذات الصلة وهذا في حالة اتصال حاسب المتهم بحاسب آخر خارج الدولة.[2]

وفي نفس الســـياق وبالرجوع الى الاتفاقية الاوروبية المتعلقة بالجريمة الالكترونية (بودابســـت 2001) نجد أنها أجازت النفاذ (التفتيش) العابر للحدود الى بيانات الكمبيوتر المخزنة دون ترخيص من الدولة الطرف وذلك في حالة تفتيش بيانات مخزنة ومتاحة للجمهور بغض النظر عن مكان توجد البيانات جغرافيا، كما اجازت الدخول بغرض التفتيش

[1]- محمد كمال شاهين، مرجع سابق، ص 290.

[2]- ونصت في ذلك المادة 5 فقرة 3 من القانون 09-04 على أنه: (... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول اليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الاقليم الوطني، فان الحصول عليها يكون بمساعدة السلطات المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل...)

الى بيانات مخزنة في دولة طرف، من خلال موافقة قانونية وطوعية للشـــخص الحائز على المعلومات أو البيانات اللازمة في اجراء التفتيش.[1]

غير أننا نرى أنه بالنظر الى الأبعاد الدولية فلا يمكن مواجهة الجرائم المعلوماتية خارج الاقليم الا بتعزيز آليات التعاون الدولي على المستوى الأمني والقضائي والفني، بشرط عدم اتاحة فرصـــة التحكم والتجســـس من قبل الدول الرائدة في المجال المعلوماتي على الأنظمة المعلوماتية للدول الأخرى.

ثالثا-ضمانات التفتيش المعلوماتي

ان اجراء التفتيش يعد انتهاكا لحرمة الأفراد ومساسا بحياتهم الخاصة، غير أن هذا الانتهاك يكون بموجب القانون، حيث تغلب المصـــلح العامة (مصـــلحة المجتمع)، على المصلحة الخاصة (مصلحة الفرد)، لتحقيق عدة اعتبارات تتمثل أساسا في تحقيق العدالة، وحق الدولة في العقاب. ولابد في ذلك من مراعاة عدة ضمانات:

1-الضمانات الموضوعية

أ-يجب الحصول على اذن بالتفتيش[2]: وهذا الاذن يجوز أن يشمل البحث عن معلومات في الكمبيوتر تتعلق بجريمة من الجرائم، ويســـتوي أن تكون هذه المعلومات في أي شـــكل كان سواء كان الكترونيا أو مغناطيسيا، في صورة ديسك أو أسطوانة أو مسجلة على الهارد ديسك أو في شـــكل ورقي تم طباعته بناء على ذلك.[3] وإذن التفتيش يمتد الى ما هو موجود في

[1]- المادة 32 من اتفاقية الاوروبية المتعلقة بالجريمة الالكترونية، سالفة الذكر، ص 18.

[2]- الملحق رقم 02: نموذج اذن بالتفتيش لمنظومة معلوماتية.

[3]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 686.

المكان أو بحوزة الشخص ويساعد في كشف الجريمة، فاذا وجد في المسكن: يجب اصدار اذن بتفتيش المسكن، وإذا كان الحاسوب محمولا: يجب اصدار مذكرة لتفتيش هذا الشخص.[1]

ب-يجب أن يكون سبب التفتيش معلوما ومحل التفتيش محددا بدقة: يشترط لصحة اجراء التفتيش أن ينصب محله على نظم الحاسب الآلي بجميع مكوناته و شبكاته، و أن تكون الجريمة قد وقعت فعلا، وليس مجرد احتمال ارتكابها، و يشترط تكييفها القانوني الى جناية أو جنحة، وتستبعد المخالفات نظرا لضآلتها، و عدم خطورتها، ولذا فانه يشترط فيما يتعلق بصحة التفتيش المعلوماتي أن يكون الفعل المراد الحصول على دليل بشأنه يشكل جريمة، فذا كان التفتيش يتعلق بالجرائم المعلوماتية بالمفهوم الضيق، فانه قد لا يوجد نص في قانون دولة ما على تجريم هذا النمط من السلوك، وهو ما يجعل التفتيش غير مشروع لانتفاء صفة الجريمة عن الفعل وفقا لمبدأ الشرعية الجنائية.[2]

كما يشترط وجود دليل كافي يؤكد التورط في ارتكاب جريمة معلوماتية أو الاشتراك فيها، و وجود امارات قوية و قرائن على وجود أشياء أو أجهزة أو معدات تفيد في كشف الجريمة لدى المتهم؛ حيث أن المعيار لإجراء التفتيش أو اصدار الاذن به هو أن يكون هناك دلائل قوية تجمعت حول الجريمة و تدعو للاعتقاد المعقول بوقوعها، وتقدير تلك الدلائل من اختصاص السلطة المكلفة بالتحقيق، و لا يكفي مجرد تقدير الدليل الذي يبرر المساس بحريات الاشخاص و بالخصوصية المعلوماتية لإلقاء المصداقية عليه وانما يجب أن يكون التقدير متصفا بالتعقل و متفقا مع ما جاءت به الخبرة و تحت رقابة محكمة الموضوع[3]

[1]- سامي جلال فقي، مرجع سابق، ص 341.

[2]- خالد عياد الحلبي، مرجع سابق، ص 244.

[3]- محمد كمال شاهين، مرجع سابق، 297.

واجاز المشرع الجزائري تمديد التفتيش الى منظومة أخرى أو جزء منها إذا كان هناك اعتقاد بتخزين معطيات في منظومة معلوماتية أخرى.[1] كما يمكن للإطارات المختصين التابعين للهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال –الذين لهم صفة ضبطية قضائية–القيام بتفتيش أي مكان أو هيكل أو جهاز بلغ الى علمهم أنه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية.[2]

2- الضمانات الاجرائية

أ–**الحدود المكانية: ان** نظم الحاسب الآلي إذا كانت في حوزة شخص المتهم فإنها تعتبر من توابعه، ولو لم تكن ملكه، فيكفي أن تكون بحوزته وعليه فان تفتيشها يخضع لنفس الضمانات الاجرائية المقررة لتفتيش الشخص. أما إذا وجدت في مسكن المتهم أو في مكان له حرمة خاصة فان حكم تفتيش مكونات الحاسب الآلي وشبكات الانترنت يخضع لأحكام وضمانات تفتيش المساكن.

حيث أن الغرض من اضفاء حكم تفتيش الأشخاص والأماكن على تفتيش نظم الحاسب الآلي وشبكات الانترنت هو الاستفادة من الضمانات الاجرائية المقررة لها، غير أن ذلك لا يعني عدم الحاجة لنصوص اجرائية جديدة تتماشى مع طبيع الجرائم المعلوماتية، بل هو أمر يفرضه الواقع العملي في ظل غياب نصوص اجرائية جديدة.[3]

كما تجدر الاشارة أن المشرع الجزائري استثنى شرط حضور صاحب المسكن المراد تفتيشه، بموجب المادة 45 من قانون الاجراءات الجزائية، حيث يمكن لضباط الشرطة

[1]– أنظر الفقرة 02 من نص المادة 05 من القانون 09–04 سالف الذكر، ص 06.

[2]– أنظر المادة 30 من المرسوم الرئاسي رقم 20–183 سالف الذكر، ص 09.

[3]– محمد كمال شاهين، مرجع سابق، ص 299.

القضائية اجراء التفتيش المعلوماتي دون التقيد بشرط حضور صاحب المسكن أو من ينوبه أو الشاهدين.

غير أنه يثور تساؤل حول الحكم المطبق لو كانت نهاية طرفية النظام المعلوماتي المراد تفتيشه تمتد لمسكن غير مسكن المتهم فهل يمكن تفتيشه في هذه الحالة؟ ولقد حسمت بعض القوانين هذه المسألة بإجازة التفتيش كالقانون الهولندي المادة 25/أ من قانون جرائم الحاسوب ودون الحاجة للحصول على اذن مسبق من أية جهة بشرط ألا تكون النهاية الطرفية خارج اقليم الدولة[1]

ب-الحدود الزمانية: اختلف التشريعات الاجرائية في تنظيمها لوقت اجراء التفتيش من قبل القائم بالتفتيش، ففي قانون الاجراءات الجنائية المصري لم يحدد وقتا محددا للتفتيش فيمكن اجراؤه في اي وقت نهارا أو ليلا، اما قانون الاجراءات الجنائية الكرواتي وضع قيودا زمنية على اجراء التفتيش فلم يسمح به الا في وقت محصور بين الساعة السابعة صباحا و التاسعة مساء، و كذلك قانون الاجراءات الجنائية الفيدرالي الأمريكي حصر المدة بين الساعة السادسة صباحا و العاشرة مساء، في حين أن المشرع الأردني لم يحدد وقتا للتفتيش الا أن محكمة النقض الاردنية لا تسمح بتفتيش المنازل الا نهارا[2]

وحصر المشرع الجزائري مدة التفتيش والمعاينة بين الساعة الخامسة صباحا الى الثامنة ليلا في الجرائم العادية كقاعدة عامة، وحدد مجموعة من الجرائم من بينها الجرائم المعلوماتية التي مدد فيها اجراء التفتيش الى اي ساعة من ساعات النهار والليل[3]،

[1]- خالد عياد الحلبي، مرجع سابق، ص 245.

[2]- سامي جلال فقي حسين، مرجع سابق، ص 164.

[3]- انظر المادة 47 قانون اجراءات جزائية جزائري سالف الذكر.

وبالمقارنة مع التشريعات الأخرى نوافق ما جاء به المشرع الجزائري من تمديد ميقات التفتيش لأي ساعة من النهار أو الليل إذا تعلق الأمر بالجريمة المعلوماتية، وذلك نظرا لطبيعتها بالدرجة الأولى، وسهولة محو واتلاف الدليل المعلوماتي مما يعيق اجراء التحقيق القضائي.

ج-تحرير محضر تفتيش

يشترط لصحة اجراء التفتيش أن يفرغ في محضر يدون فيه كافة المعلومات المتعلقة بالتحقيق سواء توصل الى الدليل أو لم يتوصل اليه، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي لا يشترط لصحته سوى ما تقتضيه القواعد العامة عموما التي تقضي أن يكون المحضر مكتوبا باللغة الرسمية، ويحمل تاريخ تحريره وتوقيع محرره، ويتضمن كافة الاجراءات التي اتخذت بشأن الوقائع التي يثبتها.[1]

د-امكانية الاستعانة بالخبرة الفنية

يختلف التفتيش في الجرائم المعلوماتية عن التفتيش عن الجرائم العادية، حيث يحتاج التفتيش في الجرائم المعلوماتية لخبرة فنية كبيرة بتقنيات الحاسب الآلي، لذا يجب أن يكون القائم بالتفتيش خبيرا مختصا في المجال المعلوماتي، وهناك تشريعات-ومن بينها المشرع الجزائري-أجازت الاستعانة بخبير بغرض التفتيش عن هذه الجرائم.[2]

وقد يصادف القائم بالتفتيش عدة صعوبات من بينها:

[1]- نجاة بن مكي، مرجع سابق، ص 222.

[2]- أنظر الفقرة الأخيرة من المادة 05 من القانون 09-04 سالف الذكر.

- تشفير الحاسوب أو تشفير المعلومات المخزنة داخل الحاسوب، أو اخفائها، أو مكانها غير معروف.[1]
- لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم المعلوماتية، فمن بين الجرائم التي انتشرت عبر الانترنت التجسس والارهاب الالكتروني، ويشمل مفهوم الارهاب الالكتروني في التشريعات المقارنة الأعمال الارهابية عبر المواقع الالكترونية (الانترنت) التي تعرض افكارا عن العمليات الارهابية وكيفية تنفيذها.[2]
- في الجرائم المعلوماتية العابرة للحدود لا يمكن تفتيش حاسوب يقع خارج حدود الدولة حتى ولو عبر العالم الافتراضي، ويتم حل هذا الاشكال عبر التعاون الدولي وبطريق الانابة القضائية، حيث تعتبر الاتفاقية الأوروبية للجرائم المعلوماتية عام 2001 نموذجا للتعاون القضائي الدولي.[3]

الفرع الثاني: آثار التفتيش المعلوماتي

يعد ضبط الأدلة المعلوماتية هو الأثر المباشر للتفتيش عن الجرائم المعلوماتية، كما قد يترتب عن هذا التفتيش حجز المنظومة المعلوماتية، وقد تتعارض هذه الإجراءات مع الحق في الخصوصية أو قد تتنافى مع الشروط المقررة قانونا مما يتطلب الدفع ببطلان إجراءات التحقيق.

أولا: ضبط الدليل المعلوماتي

يترتب عن التفتيش اما عدم ضبط اي دليل معلوماتي بعد تفتيش الحاسوب والشبكة المرتبطة به، أو نشوء الحق في ضبط الأشياء التي تفيد في الكشف عن الجريمة.

---

[1]- سامي جلال فقي، مرجع سابق، ص 343.

[2]- فهد عبد الله العبيد العازمي، الاجراءات الجنائية، مرجع سابق، ص 687.

[3]- سامي جلال فقي، مرجع سابق، 343.

غير أن التساؤل يثور حول نوع الأشياء محل الضبط في الجرائم المعلوماتية، خاصة لطبيعة هذه الجرائم وأن محلها (البيانات والبرامج) تتسم بصورة معنوية غير محسوسة؟

واجابة على ذلك الأشياء في نطاق التفتيش في وسائل التقنية الحديثة قد تكون أشياء مادية (منقولات كالأجهزة، أو عقارات كالأماكن الكائن بها منقولات معنوية)، وقد تكون أشياء معنوية (كالمراسلات والاتصالات الالكترونية والمعلومات المعالجة الكترونيا وغيرها من الأشياء المعنوية) [1]

فالأصل ان الأشياء المادية التي يحوزها المتهم تكون محلا للضبط أما الأشياء المعنوية كالبيانات والبرامج فهي محل اشكال فقهي، غير أنه باعتبارها تسجل وتحفظ على وسائط المادية فقد تكون محلا للضبط ايضا، ففي حالة العثور على الدليل المعلوماتي، وكون الأدلة عبارة عن نبضات مغناطيسية يجب تفريغها على دعامة مادية كالأقراص المغناطيسية وغيرها من وسائط التخزين، أو تفريغها على الورق، ويتم تثبيت تفاصيل الأدلة المعلوماتية في محضر ضبط.[2]

ويثير اجراء ضبط البيانات المعالجة الكترونيا عدة صعوبات من بينها: كبر حجم الشبكات التي تحتوي على المعلومات المطلوب ضبطها، كالبحث في نظام الشركة متعددة الجنسيات، اضافة الى مشكلة وجود البيانات في شبكات أو أجهزة تابعة لدول اجنبية، مما يتطلب التعاون مع أجهزة العدالة التابعة لهذه الدول.[3]

[1]– بكري يوسف بكري، مرجع سابق، ص 157.

[2]– سامي جلال فقي، مرجع سابق، ص 344.

[3]– رامي متولي القاضي، مرجع سابق، ص 124.

تعارض اجراء الضبط مع الحق في الخصوصية:

يمثل التفتيش و الضبط أحيانا الاعتداء على حرمة الحياة الخاصة للأشخاص، و هو ما يستدعي اقرار ضمانات لازمة لحماية الحقوق و الحريات، و من بين التشريعات المقارنة التي حرصت على تحقيق مثل هذه الضمانات للمتهم في الاجراءات الجنائية القانون البلجيكي: حيث أجاز للنيابة العامة سلطة الأمر بغلق البيانات لمنع الوصول اليها، أو الى نسخة مستخرجة منها و الموجودة لدى من يستعملون هذا النظام، و ذلك لضمان الحفاظ على البيانات محل البحث و ضمان امكانية مقارنتها مع النسخة المستخرجة من جهاز المتهم، كما اجاز لسلطات التحقيق سحب البيانات التي سبق اخذ نسخة منها من الجهاز اذا كانت محلا للجريمة او ناتجة عنها، او اذا كانت مخالفة لآداب العامة او النظام العام، او اذا مثلت خطرا على الانظمة الالكتروني، أو خطرا بالنسبة للمعلومة المخزنة او المرسلة بهذه الانظمة[1]

ثانيا: حجز المنظومة المعلوماتية

قد يترتب عن التفتيش حجز المنظومة المعلوماتية في حالة اكتشاف السلطة التي تباشر اجراء التفتيش عن وجود معطيات مخزنة تفيد في الكشف عن الجريمة ومرتكبيها، ففي هذه الحالة من الممكن أن تحجز المنظومة برمتها، كما يمكن أن يحجز جزء منها فقط، ذلك باعتماد مجموعة من الاجراءات حسب ما يفهم من نص المادة 06 من القانون 09-04 سالف الذكر، وتتمثل في:

- نسخ المعطيات على دعامة تخزين الكترونية تكون قابلة للحجز (سواء المعطيات محل البحث أو المعطيات اللازمة لفهم المعطيات محل البحث)
- الوضع في احراز وفقا لما هو مقرر في قانون الاجراءات الجزائية

[1]– رامي متولي القاضي، مرجع سابق، ص 124.

- السهر على سلامة المعطيات في المنظومة المعلوماتية
- امكانية استعمال وسائل تقنية لتشكيل أو اعادة تشكيل المعطيات لتكون قابلة للاستغلال لأغراض التحقيق بشرط عدم المساس بمحتوى المعطيات.

وتجدر الاشارة انه في حالة تعذر اجراء الحجز لأسباب تقنية، يتعين على السلطة التي تباشر اجراء التفتيش ان تستخدم تقنيات مناسبة لمنع نسخ أو الوصول الى المعطيات التي تحتويها المنظومة المعلوماتية، والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال المنظومة،[1] والهدف من هذا الاجراء الاحترازي هو الحفاظ على الأدلة في محيطها الالكتروني، لمنع اي محاولة لطمسها أو اخفاء معالمها، مما يساهم في نجاح اجراء التفتيش والحجز باعتباره أثر للتفتيش.[2]

ثالثا: بطلان اجراء التفتيش

يبطل اجراء التفتيش إذا كان متعلقا بالنظام العام غالبا في الشروط الموضوعية يؤدي الى بطلان مطلق للإجراء، ويمكن للقاضي أن يثيره من تلقاء نفسه، أما إذا كان متعلقا بالشروط الشكلية فغالبا البطلان نسبي يجوز لصاحب المصلحة التمسك به أو التنازل عن حقه في التمسك به، ويترتب على البطلان في معظم التشريعات استبعاد الدليل الناجم عن هذا التفتيش، وجميع الآثار المترتبة على اقرار البطلان في التفتيش عن الجرائم العادية تترتب على بطلان التفتيش في الجرائم المعلوماتية. وقد نص المشرع المصري والايطالي صراحة على البطلان [3]

[1]– وهذا حسب ما جاء في المادة 07 من القانون 09-04 سالف الذكر.

[2]– هميسي رضا، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، عدد 05، جامعة الوادي، الجزائر، جوان 2012، ص 174.

[3]– سامي جلال فقي، مرجع سابق، ص 345.

هذا وتبقى المحافظة على الحريات الفردية وحرمة الحياة الخاصة من أصعب الحقوق الواجب احترام ضمانات حمايتها، وعدم المساس بها الا لمقتضيات التحقيق في الجريمة وباحترام الشروط القانونية (الشكلية والموضوعية) تحت طائلة البطلان في حالة التعسف في استعمال الحق في التفتيش أو الحجز، ففي سبيل ضمان عدالة التفتيش المعلوماتي يمكن للمتضرر رفع دعوى قضائية قوامها المساس بحقه طبقا لأحكام قانون العقوبات من الناحية الموضوعية، والدفع ببطلان اجراء التفتيش المخالف للشروط المقررة قانونا من الناحية الاجرائية.

المطلب الثاني: المعاينة والخبرة في الجرائم المعلوماتية

تعتبر الخبرة والمعاينة من أكبر العقبات التي تواجه الاثبات في الجرائم المعلوماتية، فالمعاينة قد تكون شخصية تتعلق بشخص المجني عليه، كما قد تكون مكانية تتعلق بمكان ارتكاب الجريمة، وتتعلق المعاينة العينية بالأشياء والادوات المستخدمة في ارتكاب الجريمة وقد يقتضي الأمر الاستعانة بخبير وفي هذه الحالة نكون أمام اجراء آخر من اجراءات التحقيق وهو الخبرة التي تعد اهم وسائل جمع الأدلة[1]

الفرع الأول: المعاينة في الجرائم المعلوماتية

المعاينة هي اجراء يتضمن وصف مكان الحادث بما فيه من أشياء، اشخاص، مع الفحص الدقيق لكافة المحتويات بهدف كشف مخلفات وآثار الجاني بالمكان، والتي تشير الى شخصيته وشركائه، وما يفيد في اثبات ارتكاب الجريمة وتوضح قدرا من الاستنتاجات التي تشكل في حد ذاتها الأساس الذي يقوم عليه التحقيق.[2]

ويقصد بمعاينة مسرح الجريمة المعلوماتية معاينة الآثار والبصمات الالكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت، وتشمل الرسائل المرسلة منه، أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسب الآلي والشبكة العالمية، او التي من الممكن ان يطلق عليها البصمات المعلوماتية، وذلك مع ضرورة مراعاة مبدأ الشرعية والخصوصية المعلوماتية للأفراد ودون البحث في المحتوى الا في حدود السلطات القصرية الممنوحة لجهات التحقيق.[3]

---

[1]– محمد نصر محمد، مرجع سابق، ص 96.

[2]– حازم محمد حنفي، مرجع سابق، ص 55.

[3]– محمد كمال شاهين، مرجع سابق، ص 259.

أولا: الهدف من المعاينة في الجرائم المعلوماتية

ان الهدف من المعاينة هو تطوير عملية البحث والتحقيق الجنائي، واتاحة المجال لكشف آثار الجريمة والتحفظ عما يفيد في التحقيق.

وتبدأ المعاينة في الجرائم المعلوماتية بمعاينة المسرح التقليدي وذلك من خلال الانتقال الى مكان تواجد الأجهزة ومعاينة المكونات المادية للحاسب الآلي، تفاديا لأية تلف أو ضياع للأدلة المتحصل عليها، ومن ثم الانتقال الى المسرح الالكتروني الذي يشمل برامج وبيانات الحاسب الآلي.

وتعد المعاينة اجراء هادف غايته كشف وصيانة العناصر المادية للجريمة محل المعاينة، فاذا انعدمت تلك الغاية تنتفي معها جدوى المعاينة وفائدتها بالنسبة للتحقيق، وفي ذلك قضت محكمة النقض المصرية بأن المعاينة اجراء من اجراءات التحقيق يترك لزوم القيام به الى سلطة التحقيق[1]

وقد تكون الجرائم المعلوماتية مستمرة كما هو الحال في الجرائم الاقتصادية كجرائم السرقة والاحتيال، وفي هذه الحالة يكون الهدف من المعاينة هو المداهمة وضبط الادلة على الطبيعة، كما قد يكون مسرح الجرائم المعلوماتية كما في الجرائم الاخرى كالتزوير اتلاف البرامج وتفجير المباني والمنشآت، وفي هذه الحالة بعد وقوع الجريمة الأمر متوقف على اعترافات المتهمين إذا تم ضبطهم، وكذلك شهادة الشهود والقرائن،[2]

و تنصب المعاينة في الجرائم المعلوماتية: على المكونات المادية، و ذلك بانتقال المحقق الى مسرح الجريمة و التحفظ على أجهزة الحاسب الآلي و مستلزماته و ملحقاته من وسائل اتصال بالشبكة العنكبوتية، كالرواتر، الطابعة، جهاز الماسح الضوئي، و جميع

[1]– محمد كمال شاهين، مرجع سابق، ص 260.

[2]– حازم محمد حنفي، مرجع سابق، ص 58.

الأشـياء التي من الممكن أن تكون أدلة الكترونية كشـرائط الفيديو الرقمية Dvd، Cd، Flash Disque، و يتطلب ذلك سـرعة الانتقال الى محل الجريمة للمحافظة على آثار الجريمة قبل العبث بمضمونها، أو اتلافها أو التخلص منها، كما تنصب المعاينة على المكونات المعنوية و التي تتمثل في البرامج و البيانات الموجودة في جهاز الحاسب الآلي.[1]

ثانيا: الاجراءات المتخذة قبل وأثناء اجراء المعاينة

يشـير الفقه الى أن ارتكاب الجريمة على المكونات المادية للحاسـب الآلي مثل جرائم الاعتداء على أشرطة الحاسب و كابلاته و شاشة العرض الخاصة به و مفاتيح التشغيل و الأقراص و غيرها، لا تثير صـعوبة في معاينتها و التحفظ على الأشـياء التي تعد أدلة مادية تدل على ارتكاب الجريمة و نسـبتها الى مرتكبها، في حين أن المكونات المعنوية كالجرائم الواقعة على برامج الحاسـب الآلي و بياناته أو بواسـطتها، تثير العديد من الصـعوبات أهمها قلة الآثار المادية التي قد تتخلف عن هذه الجرائم، كذلك تردد عدد كبير من الأشخاص على مسـرح الجريمة خلال مدة زمنية طويلة نسـبيا تتوسـط عادة بين زمن ارتكاب الجريمة و بين اكتشـافها، مما يمنح فرصـة لحدوث تغيير أو عبث بالآثار المادية أو زوال بعضـها،[2] كذلك امكانية التلاعب بالبيانات عن بعد أو حذفها، مما يتطلب الحذر عند اجراء المعاينة و اتخاذ مجموعة من الاجراءات قبل و أثناء المعاينة.

1-الاجراءات الواجب اتباعها قبل معاينة مكان الجريمة المعلوماتية

ان أهم اجراء لابد من اتباعه قبل معاينة مكان الجريمة المعلوماتية هو توفير معلومات مسبقة عن مكان الجريمة، ونوع وعدد الأجهزة المتوقع مداهمتها وشبكاتها.[3]

---

[1]- حازم محمد حنفي، مرجع سابق، ص 56.

[2]- رامي متولي القاضي، مرجع سابق، ص 109.

[3]- خالد ممدوح ابراهيم، مرجع سابق، ص 157.

ونظرا لخطورة الجرائم المعلوماتية وامكانية تلف الأدلة أو ضياعها فينبغي قبل المعاينة الاعداد الجيد لعدم تسرب الأدلة أو ضياعها، واصطحاب خبراء متخصصين لمرافقة فريق التحقيق، كما ينبغي اصطحاب وسيلة توليد كهرباء بديلة وآمنة، حتى لا ينقطع التيار الكهربائي أثناء الفحص لتفادي تلف الأدلة، اضافة الى ضرورة وجود مجموعة من البرامج المساعدة على فحص مكونات الحاسب الآلي كالمتعلقة باستعادة الملفات المحذوفة، وبرامج كسر كلمات المرور وبرامج فحص الهواتف المحمولة.[1]

2-الاجراءات الواجب اتباعها أثناء القيام بالمعاينة

تصوير الجهاز والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة، وملاحظة طريقة اعداد نظام الحاسب بعناية، واثبات حالة التوصيلات والكابلات المرتبطة بالحاسب والتي تكون متصلة بمكونات النظام، وهذا لتسهيل القيام بالمقارنة والتحليل عند عرض الموضوع على المحكمة، وينبغي عدم التسرع في نقل أية مادة معلوماتية من مكان وقوع الجريمة لعدم اتلاف البيانات المخزنة[2]

كذلك لابد من فحص سلة المهملات لمعرفة الملفات المحذوفة مؤخرا بالإضافة الى استخدام برامج استعادة الملفات المحذوفة، التحفظ على المستندات الخاصة بالإدخال وملحقات الحاسب الآلي المادية الورقية المرتبطة بالجريمة وكل الآثار التي تفيد التحقيق، الحرص على عدم اتلاف اي بيانات يتم استخراجها من الجهاز وكذلك التأكد من وجود نسخة منها محفوظة على الحاسب نفسه، والفحص بدقة لكل ملفات الجهاز، خاصة ملفات

[1]- حازم محمد حنفي، مرجع سابق، ص 57.

[2]- رامي متولي القاضي، مرجع سابق، ص 110.

Log file للتعرف على العمليات التي قام بها المستخدم والمواقع التي ارتادها على شبكة الانترنت.[1]

ثالثا: ضوابط المعاينة بعد وقوع الجريمة في المجال الالكتروني

- استعداد فريق التحقيق الذي سيتولى اجراء المعاينة من الناحية الفنية والعملية، ولابد من قصر المعاينة على ذوي الخبرة في المجال المعلوماتي.
- اعداد خطة عمل للمعاينة وكيفية اجرائها.
- تأمين جميع الاجهزة الالكترونية بما في ذلك الشخصية والمحمولة وابعاد اي شخص لا علاقة له بمهمة التحقيق.
- تصوير الحاسب الآلي والاجهزة الطرفية المتصلة به، مع تسجيل وقت ومكان التقاط كل صورة، مع التركيز بصفة خاصة على الأجزاء الخلفية للحاسب الآلي وملحقاته، ومراعاة وقت وتاريخ ومكان التقاط كل صورة.[2]
- دقة ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، ليتمكن المحقق من المقارنة والتحليل فيما بعد عند عرض الأمر على المحكمة.
- مراعاة عدم نقل أية مادة معلوماتية من مسرح الجريمة قبل اجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من اي مجال لقوى مغناطيسية يمكن ان تتسبب في محو البيانات المسجلة على الوسائط المعلوماتية.[3]
- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة او أوراق الكربون المستعملة، والشرائط والاقراص الممغنطة، وفحصها ورفع البصمات ذات الصلة بالجريمة، كذلك التحفظ على مستندات الادخال والمخرجات الورقية للحاسب ذات

[1]– حازم محمد حنفي، مرجع سابق، ص 57.

[2]– خالد ممدوح ابراهيم، مرجع سابق، ص 164.

[3]– محمد كمال شاهين، مرجع سابق، ص 247.

الصـــلة بالجريمة، ولابد ان تتم الاجراءات وفقا لمبدأ المشـــروعية وفي إطار ما تنص عليه القوانين الاجرائية.[1]

- تحريز الأدلة الالكترونية المتحصـــلة من مســـرح الجريمة من خلال ضـــبط وتحريز الدعائم الأصلية للبيانات وعدم الاكتفاء بضبط النسخ، مراعاة ظروف الحرارة والرطوبة لتخزينها والالتزام بالقواعد الفنية المتعلقة بنقلها، مع تأمين البرامج المضـــبوطة قبل تشغيلها فنيا وعمل نسخ احتياطية سليمة وكاملة، وتمييز كل دليل الكتروني عن غيره بوضع علامة مادية خاصة به.[2]

وجدير بالتنويه الى قضـــية في مجال النصـــب و الاحتيال عبر الانترنت، و ذلك عن طريق ارسـال بريد الكتروني، الى الضـحية (أ) مفاده بيع و شـراء بذرة تسـتخدم في تحضـير بعض الأدوية و العطور اسـمها (لسـان الثور)، ثم التواصـل مع الضـحية عبر السـكايب و الهاتف النقال قصـد اسـتدراجه بواسـطة شـخصـية وهمية تسـمى BERCY، و تمكن من سـلبه مبلغ مالي معتبر جراء التعامل معه، و بعد التحقيق من قبل رجال الدرك الوطني بالتنســـيق مع مركز الوقـايـة من جرائم الاعلام الآلي و الجرائم الالكترونيـة ببئر مراد رايس تبين ان المشـــتبه فيه XX يقيم في مرقد بمدينة وهران، و هذا المرقد يســـمح لأي نزيل فيه باســـتخدام بشبكة انترنت (ويفي)،

وبناء على التحقيقات تم حجز كمية معتبرة من البذرة، وجهاز كمبيوتر يســـتعمل في ارسـال رسـائل البريد الالكتروني بالشـخصـية المزعومة BERCY، ودفاتر فيها اسـماء جزائريين من مختلف ربوع الوطن، وشـرائح تسـتعمل في الاتصـال بالضـحايا، واتضـح وجود ضـحايا آخرين منهم الضـــحية (ب)، و (ج) حيث صـــرح الضـــحية (ب) بعد اســـتدعائه أنه تعرض للنصـــب والاحتيال عن طريق شـــبكة الانترنت باســـتعمال البريد الالكتروني في قضـــية ابرام

[1]– حازم محمد حنفي، مرجع سابق، ص 59.

[2]– خالد ممدوح ابراهيم، مرجع سابق، ص 177.

صفقة شراء وبيع لسان الثور لفائدة متعامل أوروبي مزعوم BERCY اين تم سلبه هو ايضا مبلغ 406 مليون سنتيم. وتم تحديد الضحية (ج) الذي تم سلب منه مبلغ 360 مليون سنتيم من قبل نفس الشبكة. وبعد اطلاع المحكمة على ملف الدعوى واتباع الاجراءات القانونية اللازمة قضت المحكمة بإدانة المتهم ب 3 سنوات حبسا نافذا وغرامة نافذة[1]، وبموجب قرار جزائي صادر عن غرفة استئنافات الجنح والمخالفات لمجلس قضاء قالمة، تم رفع العقوبة المحكوم بها في هذه القضية على المتهم الى 5 سنوات حبسا نافذا وغرامة نافذة.[2]

الفرع الثاني: الخبرة في مجال الجرائم المعلوماتية

الخبرة هي عبارة عن اجراء من اجراءات التحقيق التي تستوجب الالمام بمجموعة من المعلومات الفنية التي تساعد في استخلاص الأدلة اللازمة للتوصل الى الحقيقة القضائية.

وتعرف الخبرة القضائية على أنها استشارة فنية يستعين بها قاضي التحقيق لتقدير المسائل الفنية التي يحتاج تقديرها الى معرفة فنية أو دراية علمية لا تتوافر لديه بحكم تكوينه، ولعل دواعي اللجوء الى الخبير كثيرة وهي في تزايد مستمر نتيجة المستجدات على الساحة العلمية ولجوء الجناة الى وسائل عصرية متطورة في ارتكاب الجريمة، حيث لا يمكن كشفها الا بواسطة ذوي الاختصاص وما يزيد في الحاجة الى الخبير هو طبيعة تكوين قضاة التحقيق الذي يغلب عليه العمومية.[3] في حين أن للخبير كفاءة في اختصاص معين بذاته.

[1]– حكم، محكمة قالمة، قسم الجنح، رقم الجدول 16/01976، رقم الفهرس 16/02413، تاريخ الحكم 30-06-2016.

[2]– قرار جزائي، مجلس قضاء قالمة، الغرفة الجزائية، رقم الملف 03219/ 16، رقم الفهرس 16/03722، تاريخ القرار 11-09-2016.

[3]– أحسن بوسقيعة، التحقيق القضائي، ط 10، دار هومة، 2012، ص 107-108.

وفي ذلك يعد الخبير التقني شـــخص مؤهل علميا وعمليا يتميز بالكفاءة والتخصـــص في التعامل مع شبكة الانترنت وأنظمة وبرمجيات الحاسب الآلي وفهم لغته.[1]

أولا: ندب الخبراء

تعتبر الخبرة في مجـال التحقيق الجنـائي أحـد ذروع المحقق الجنـائي في الجرائم المعلوماتية وتظهر أهميتها بصـــفة عامة في كونها اجراء تحقيق تتحرك به الدعوى الجنائية وذلك بـانتداب الخبير، وتظهر أهميـة انتداب هذا الاخير في الجرائم المعلومـاتيـة في كونـه مؤثرا في ســير الدعوى الجنائية، فبعد أن يدلي برأيه شــفاهية لســلطة التحقيق أن تقرر عدم احالة المتهم الى المحاكمة وأن تأمر الا وجه لإقامة الدعوى الجنائية، هذا فضـــلا عن كون الخبير التقني أحد اعضاء فريق التحقيق في الجرائم المعلوماتية ابتداء.[2]

يكتســي ندب الخبراء أهمية قصــوى في اجراءات جمع أدلة المكونات المعنوية في كل وحدات التخزين و تحليلها و كشـــف أي تلاعب في البرامج و المعلومات، غير أن ذلك لا يعني عدم الاكتراث بمسـألة تأهيل سـلطات الملاحقة و تزويد أفرادها بالمعرفة العلمية والتقنية ليكونوا على دراية فيما يســـتلزم ندب الخبراء وفهم ما يقدمونه من آراء، لذلك نجد الكثير من الدول المتقدمة قد اهتمت بتدريب المحققين في الجرائم المعلوماتية، وقد قام المجلس الأوروبي في احدى توصياته سنة 1999 بالدعوة الى ضرورة تدريب الشرطة واجهزة العدالة بما يواكب التطور المتلاحق لتقنية المعلومات واستخدامها لتحقيق التوازن بين وسـائل ارتكاب الجريمة و بين ســـبل مواجهتها، وعقدت المنظمة الدولية للشـــرطة الدولية العديد من الدورات التدريبية لمحققي جرائم الحاسب الآلي.[3]

---

[1]– محمد كمال شاهين، مرجع سابق، ص 333.

[2]– محمد كمال شاهين، المرجع نفسه، ص 335.

[3]– حازم محمد حنفي، مرجع سابق، ص 63.

ولقد أوجبت المادة 143، 146 من قانون الاجراءات الجزائية الجزائري على قاضي التحقيق أن يحدد بدقة في الأمر بندب خبير المهمة المطلوبة منه والأسئلة الفنية أو العملية التي يطلب الاستفسار فيها، وأن هذه المهمة لا يجوز ان تتعلق الا بفحص مسائل ذات طابع فني، ولا يفوض فيها أي جزء من جوانب اختصاصه، لأن ذلك قد يعرض أمره للبطلان، ولابد أن تجرى الخبرة تحت مراقبة واشراف قاضي التحقيق، ويتعين على الخبير اطلاع القاضي بكل ما توصل اليه من نتائج ويعلمه بتطورات الأعمال التي يقوم بها، لاتخاذ الاجراءات اللازمة.[1]

ثانيا: دور الخبرة في مجال الجرائم المعلوماتية

للخبير التقني دور وقائي وهو حماية وتأمين النظام محل الاعتداء من استمرار التهديد المعلوماتي ضده، كالحد من استمرار انتشار الفيروسات التي يمكن ان تنتقل وتسجل اوتوماتيكيا على الحاسبات والتي يمكن ان تدمر ما تبقى من النظام المعلوماتي، أو ان يساعد على وقف التجسس المعلوماتي بنسخ الملفات أو بمنع سرقة وقت الآلة.[2]

كما تساعد الخبرة في مجال الجرائم المعلوماتية في الكشف عن الدليل الالكتروني وتحديد خصائصه المميزة وخصائص كل جزء منه كالمستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور، الأصوات وغيرها، و يقوم الخبير بعمل نسخة اصلية منه للتأكد من عدم وجود معلومات مفقودة اثناء استخلاصه، و يمكن اجراء اختبارات عليه للتحقق من أصالته و مصدره كدليل يمكن تقديمه لأجهزة انفاذ القانون، كما تساعد الخبرة في اصلاح

[1]– محمد حزيط، مذكرات في قانون الاجراءات الجزائية الجزائري، ط 8، دار هومة، 2013، ص 184.

[2]– محمد كمال شاهين، مرجع سابق، ص 335.

الدليل و اعادة تجميعه من المكونات المادية للحســـاب الآلي، وفي جمع الآثار المعلوماتية الرقمية، و استخدام خوارزميات للتأكد من ان الدليل لم يتم العبث به أو تعديله.[1]

يكون عمل الخبير بحضور و تحت اشراف المحقق، و يرى الفقه ان حضور المحقق هو بمثابة رقابة اجرائية لتســهيل مهمة الخبير و مســاعدته في تعيين مكان البحث و توفير الظروف الموضـــوعية، غير انه لا يجوز للمحقق التدخل في الاعمال الفنية التي يجريها الخبير، و ينحصر دور الخبير في ابداء رأيه في المسائل الفنية التي حددها له المحقق، وله ان يســـتعين بغيره من الخبراء نظرا لعدم وجود خبير لديه معرفة متعمقة في ســـائر انواع الحاسبات و برمجياتها، ولا خبير قادر على التعامل مع كافة انماط الجرائم التي تقع بواسطة او على الحاسب الآلي.[2]

وبالإســقاط على ما جاء في قانون الاجراءات الجزائية الجزائري فقاضـــي التحقيق أو القاضي الذي تعينه الجهة القضائية له ان يراقب اعمال الخبرة، وإذا ظهر للخبير مسألة تقنية خارجة عن اختصــاصــه فيجوز للقاضــي ان يصــرح لهم بضــم فنيين متخصــصــين، ويؤدي الفنيون المعينون على هذا الوجه نفس يمين الخبراء ويرفق تقريرهم بكامله بتقرير الخبراء[3]

حجية تقرير الخبرة:

عند الانتهاء من الخبرة يحرر الخبراء تقريرا، وبالرجوع الى المادة 153 من قانون الاجراءات الجزائرية الجزائري فتقرير الخبرة لابد أن يشتمل على وصف ما قام به الخبراء من أعمال ومختلف النتائج التي تم التوصل اليها، وعليهم ان يشهدوا بقيامهم بالأعمال المطلوبة

[1]– خالد ممدوح ابراهيم، مرجع سابق، ص 302.

[2]– محمد كمال شاهين، مرجع سابق، ص 338.

[3]– المادة 149 من قانون الاجراءات الجزائية.

منهم شخصيا، ومن ثم يقومون بالتوقيع على تقرير الخبرة ويودع لدى كاتب الجهة القضائية التي أمرت بالخبرة ويثبت الايداع بموجب محضر.

و مؤكد أن المحكمة تعتبر هي الخبير الاعلى و لذلك تخضع تقارير الخبرة لتقديرها، فلها ان تأخذ برأي خبير دون آخر، كما ان لها الحق في ترجيح رأي احد الخبراء دون الآخر وفقا لاقتناعها وحسب ما تراه مؤيدا لوقائع الدعوى، و هي ليست ملزمة ببيان اسباب الترجيح، كما لها السلطة التقديرية في الاخذ ببعض ما ورد في تقرير الخبرة، و تترك الباقي دون ابداء أسباب ذلك الا في المسائل الفنية فلا يجوز لها تفنيدها الا بأسانيد فنية، وفي ذلك قضت محكمة النقض المصرية في ارساء حدود السلطة التقديرية لمحكمة الموضوع لا يجوز للمحكمة أن تحل نفسها محل الخبير الفني في مسألة فنية،[1]

ثالثا: متطلبات اعمال الخبرة القضائية في مجال الجرائم المعلوماتية

ان اعمال الخبرة القضائية تستدعي المام الخبير بالمعلومات الفنية ليتمكن من استخلاص الأدلة اللازمة، وتستدعي الخبرة استخدام الخبير التقني لمجموعة الأساليب العلمية التي يقوم عليها تخصصه.

ومن بين الأساليب التي يقوم بها في سبيل التوصل للجرائم المعلوماتية، قيامه بتجميع و تحصيل المواقع التي تشكل جريمة في ذاتها ثم تحليلها للتوصل الى معرفة بروتوكول الانترنت الذي ينسب الى الحاسب الآلي الذي صدر عن هذه المواقع كمواقع التهديد، النصب، السب أو جرائم النسخ، بث صور مخلة بالحياء قصد الدعاية لارتكاب جرائم الدعارة، الاتجار بالبشر، او دعارة الاطفال و غيرها، او من خلال تجميع و تحصيل للمواقع التي لا يشكل موضوعها جريمة في حد ذاته بل تؤدي من خلال تتبع موضوعها الى قيام

[1]– الطعن رقم 486، سنة 34 ق، جلسة 29.06.1964، الطعن رقم 2397 لسنة 33 ق، جلسة 27.01.1964 م، ص 384. عن حازم محمد حنفي، مرجع سابق، ص 64.

احد الافراد بارتكاب الجريمة، كالمواقع التي تساعد الغير على كيفية زراعة المخدرات أو كيفية اعداد أو التعامل مع القنابل.[1]

ولابد للخبير التقني ان يكون ملما بمكونات وبرمجيات الحاسب الآلي ونظم تشغيله، ومختلف ملحقاته، وأن يكون قادرا على:[2]

- التحكم في وسائل وبرامج فحص نظم الحاسب الآلي كبرامج كشف وازالة الفيروسات، وبرامج استرجاع البيانات والمعلومات وبرامج فك الشفرات وكلمات السر
- القدرة على نسخ البرامج والملفات وعمل نسخ من القرص الصلب طبق الاصل.
- القدرة على اتقان استخدام الوسائل والبرامج دون تدمير أو اتلاف الأدلة المستمدة منها ومعرفة كيفية الربط بين الدليل المادي والدليل الالكتروني في الوقائع محل البحث.
- القدرة على تفسير الملاحظات والربط بين الاشياء واستخلاص نتائج علمية فنية قضائية.
- التمكن من نقل أدلة الاثبات وتحويلها الى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة، واثبات مطابقة المخرجات الورقية لما هو مسجل على الحاسب الآلي أو النظام أو الشبكة.

ويتعين على الخبير المعلوماتي التنسيق مع المحقق الجنائي قبل محاكمة الجاني عن الجريمة المعلوماتية المرتكبة، على ان يشمل اللقاء كافة الخبراء الذين ساهموا مع سلطات الضبط او التحقيق في تلقي البلاغات او اجراء الضبط والتفتيش او فحص البرامج وجمع الادلة الجنائية، على ان يتم في هذا اللقاء حصر الادلة وترتيبها، ولابد للمحقق ان يشرح

[1]– خالد ممدوح ابراهيم، مرجع سابق، ص 301.

[2]– حازم محمد حنفي، مرجع سابق، ص 68.

للخبراء الجوانب القانونية لطبيعة عملهم والتأكيد على ربط الادلة بالخبرة العلمية وعناصـــر واركان الجريمة محل الدعوى الجنائية.[1]

وتجدر الاشـارة أن اجراءات الخبرة والمعاينة تتطلب ادارة متخصـصـة تشـمل مجموعة من المتخصـصـين في المجال المعلوماتية ويحوزون صـفة الضـبطية القضـائية، فلا يكفي مجرد تدريب القائمين على ادارة الخبرة الجنائية، أما بالنسـبة لرجال القضـاء والنيابة وضـباط الشـرطة القضـائية فهم يحتاجون الى التدريب على اسـتخدام الوسـائل التكنولوجية واسـتخدام اجهزة الحاســب الآلي اضــافة الى رفع الكفاءة القانونية لدى رجال القضــاء والنيابة العامة وتوفير الموسوعات القانونية التي تتطلب الربط بين كافة المؤسسات القضـائية بقواعد بيانات قانونية.[2]

في الواقع أنه على الرغم من الجهود المبذولة للتوصل للجرائم المعلوماتية الا أنه تبقى بعض العقبات تواجه الخبير في جمع الأدلة الالكترونية ومن بينها:

فقدان الخبير لأدلة جوهرية بسبب اغلاق جهاز الحاسب الآلي بطريقة غير صحيحة، أو عند القطع المفاجئ للتيار الكهربائي، كما قد يقوم الجاني بتهيئة جهاز الحاســب الآلي للتفجير أو التدمير بمجرد تشغيله بالضغط على زر توصيل الطاقة ومهارته في تدمير الادلة أو تحريفها أو تعديل البيانات أو اخفاء الهوية والمعلومات قد تشـكل عائقا أمام عمل الخبير، كما قد يصعب الحصول الأدلة الالكترونية في حالة توزيع مسرح الجريمة بين أكثر من دولة بسبب تعقيد الاجراءات أو وجود مشاكل عملية وتشريعية في بعض الدول، وضـخامة حجم

[1]–حازم محمد حنفي، مرجع سابق، ص 70.

[2]– محمد نصر محمد، مرجع سابق، ص 100.

البيانات التي تمر عبر الشـبكات مما يكون له تأثير عكسـي في حالة البحث عن دليل ادانة أو براءة[1]

المبحث الثاني: الاجراءات المستحدثة للتحقيق في الجرائم المعلوماتية

مع التعقيدات والصـعوبات التي تواجه السـلطات المختصـة أثناء اسـتخلاص الأدلة الالكترونية، كان من اللازم مواكبة التطورات التكنولوجية واستحداث اجراءات خاصة تتناسب مع خصـوصـية التعامل مع البيئة التقنية، وذلك بغية تسـهيل التوصـل الى مرتكبي الجرائم المعلوماتية وجمع الأدلة ضدهم.

وفي سياق ذلك اتجهت الاتفاقيات الدولية وغالبية التشريعات الى أن يكون استحداث هذه الاجراءات الخاصة مراعيا لإقامة توازن بين الحق في استخدام الوسائل الحديثة للكشف عن الجريمة وجمع الأدلة فيها، وبين الحرية الشخصية للأفراد واحترام خصوصيتهم، وذلك من خلال الالتزام بالضوابط القانونية الملائمة في ذلك، على أن تكون اباحة المساس بالحياة الخاصـة لمقتضـيات التحقيق في إطار قانوني واحترام الشـروط العامة والخاصـة المحددة قانونا.

المطلب الأول: الاجراءات المتعلقة بالبيانات الالكترونية المتحركة

جاء النص على شرعية المراقبة التقنية لضرورات التحقيق لجمع الأدلة الأولية، نتيجة التطورات الهائلة في مجال التكنولوجيا الحديثة وما صـاحبها من امكانية اخفاء هوية المجرم وصعوبة تتبع تحركاته. حيث خصصنا الفرع الأول لهذه النقطة تحت عنوان المراقبة السرية للمراسلات والاتصالات الالكترونية.

[1]– حازم محمد حنفي، مرجع سابق، ص 67.

كما يعتبر نظام التسـرب أسـلوبا جديدا جاء به المشـرع الجزائري بغرض دعم فعالية الأسـاليب العادية للبحث والتحقيق في مواجهة الجرائم المسـتحدثة ومن بينها الجرائم المعلوماتية، وهو في حقيقته مساهمة أو مشاركة في الجريمة سمح بها المشرع لاختراق عالم الجريمة والتوصـل الى المجرم، وقد تضـمنه المشـرع الجزائري في المنظومة القانونية وفقا للمواد من 65 مكرر 11 الى مكرر 18 من قانون الاجراءات الجزائية. وسـنتناول هذا الأسلوب بموجب الفرع الثاني تحت عنوان التسرب.

الفرع الأول: المراقبة السرية للمراسلات والاتصالات الالكترونية

نتيجة القصـور في مواجهة الجرائم المعلوماتية من الناحية الموضـوعية في قانون العقوبات ومن الناحية الاجرائية في قانون الاجراءات الجزائية جاء المشـرع الجزائري بموجب القانون 09-04 بإجراء جديد يتمثل في وجوب وضـع ترتيبات تقنية لمراقبة الاتصـالات الالكترونية وتجميع وتسـجيل محتواها آنيا، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، وذلك لمقتضيات حماية النظام العام ولمستلزمات التحري والتحقيق القضائي.

ويقصد بالمراقبة السرية هي العمل الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع بيانات ومعلومات حول شخص أو شيء محل التحقيق، ومن ضمن أشكالها:

- مراقبة الشبكات المعلوماتية بهدف اكتشاف الجرائم المعلوماتية ومرتكبيها: حيث لا يجوز لجهات الضبط القضائي مراقبة محتوى الاتصالات الالكترونية، غير ان المراقبة جائزة ولو بصـفة سـرية للمواقع والمحادثات وغرف الحوار والدردشـة المفتوحة للجمهور، ويمكنها أن تستعين في هذا المجال بتقنية تعقب المواقع الاباحية على شبكة الانترنت، أو اية تقنية اخرى

قادرة على ايجاد المواقع الالكترونية التي تحتوي على بيانات الكترونية غير مشروعة كالمواقع التي تحرض على الارهاب واستعمال المخدرات وغيرها.[1]

وعموما ما يثير الاشكال في هذا المجال: أن القيام بالمراقبة السرية الالكترونية للشبكات المعلوماتية ليس بالأمر السهل، فينبغي أن تتوفر لدى جهات الضبط القضائي القائمة بها المؤهلات العلمية والتقنية اللازمة لأداء المهمة، وهذه الأمور لا يمكن تحقيقها الا من خلال اسناد مهمة التحقيق لجهات ضبط قضائي خاصة مؤسسة ومعدة لهذا الغرض تختص بمكافحة الجرائم المعلوماتية، ملمة بما يدخل من البيانات الالكترونية ضمن مفهوم الحياة الخاصة التي لا يجوز مراقبتها الا بإذن قضائي. وهذا ما يستدعي تزويد الجهات المختصة بالثقافة القانونية اللازمة لهذا الغرض عبر تنظيم دورات خاصة لهم.[2]

– مراقبة محتوى الاتصالات الالكترونية: والتي تعد من قبيل الاجراءات التحقيقية بالنظر لمساسها بحق الأفراد في الخصوصية.

ويثار في ذلك التساؤل حول امكانية اعتبار المراقبة الالكترونية تفتيشا؟

خاصة مع اتجاه بعض الآراء الفقهية الى اعتبار المراقبة تفتيشا باعتبار أن الهدف فيهما واحد وهو البحث و ضبط ما يفيد في التوصل الى الحقيقة، في حين اتجه رأي آخر الى التفريق بينهما على أساس أن التفتيش غايته هي العثور على الدليل المادي و ضبطه بوضع اليد عليه لمصلحة العدالة، في حين ان مراقبة الاتصالات الالكترونية ليست ملموسة وانما يسمع فيها سر المتحدث قوليا، حيث أن أسلاك الهاتف أو التسجيل ليس دليل في حد

[1]– رشاد خالد عمر، مرجع سابق، ص 74.

[2]– رشاد خالد عمر، المرجع نفسه، ص 75.

ذاته و انما هو وسيلة أو أداة لسماع الحديث و لا تتأثر طبيعته بالأداة أو الوسيلة المستعملة للحصول عليه.[1]

وفي هذا الصدد لا نعتبر بدورنا المراقبة السرية الالكترونية للاتصالات الالكترونية ومن ضمنها المحادثات الهاتفية نوعا من انواع التفتيش، لأن المراقبة الالكترونية ترد على البيانات الالكترونية المتحركة التي تتجسد هنا بالاتصالات الالكترونية حال اجرائها، دون تلك التي انتهت وخزنت، في حين أن التفتيش يرد فقط على البيانات الالكترونية الساكنة أو المخزنة التي تتجسد هنا بالاتصالات الالكترونية المنتهية والمخزنة.[2]

أولا: اعتراض المراسلات السلكية واللاسلكية:

ان اعتراض المراسلات هو مراقبة الاتصالات الالكترونية أثناء بثها وليس الحصول على اتصالات الكترونية مخزنة، ويترتب على المراقبة السرية للاتصالات الالكترونية تسجيل محتوى تلك الاتصالات وتخزينها على وسائط مادية قابلة للنقل، بغية استخدامها فيما بعد لإثبات جريمة وقعت، ولكن تختلف نوعية التسجيل هنا بحسب ما إذا كانت المحادثة الالكترونية المراقبة اتصال صوتي فقط أو اتصال صوتي مرئي، ففي الأول يكون التسجيل صوتي، وفي الثاني يكون صوتي مرئي.[3]

وقد استحدث المشرع الجزائري بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006 الفصل الرابع في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ويشمل المواد من 65 مكرر 5 الى 65 مكرر 10.

[1]- يوسف مناصرة، الدليل الالكتروني في القانون الجزائي، مرجع سابق، ص 430.

[2]- نجاة بن مكي، مرجع سابق، ص 231.

[3]- نجاة بن مكي، المرجع نفسه، ص 231.

وحصـر اسـتخدام هذه الأسـاليب في جرائم محددة على سـبيل الحصـر وتتمثل في: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات، الجرائم الارهابية، جرائم تبييض الأموال، الجرائم المتعلقة بالتشـريع الخاص بالصرف، اضافة الى جرائم الفساد.

وقد منح المشرع لضباط الشرطة القضائية (في هذه الجرائم) رخصة للقيام بمجموعة من الأعمال إذا اقتضت ضرورات التحري أو التحقيق الابتدائي ذلك.

حيث يجوز لوكيل الجمهورية أن يأذن باعتراض المراســـلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، كما يأذن بإجراء ترتيبات تقنية من أجل التقاط وتثبيت وبث وتسجيل الكلام والتقاط الصور.

ويعد التحقيق الابتدائي هو التحري الأولي للضـــبطية، ونظرا لأن هذه التدابير عملا من أعمال التحري، وليست عملا قضائيا، فهي غير قابلة للطعن، وبالتالي فليس مطلوبا أن يكون القرار بشـأنها مسـببا، ومن باب المقارنة مع التشـريعات الأخرى، فقانون الاجراءات الجزائية في كل من فرنسا والمغرب لا يعطي للنيابة هذه السلطات بل هي متروكة لقاضي التحقيق أو قضاة الحكم، في حين أن المشرع الجزائري سمح بها لكل من وكيل الجمهورية وقاضي التحقيق.[1]

1-الشروط اللازمة لعملية اعتراض المراسلات وتسجيل والتقاط الصور

رغم أن جميع القوانين تفرض حماية الحياة الخاصـــة للأشـــخاص ومن ذلك حماية المراسلات والمكالمات والأحاديث الخاصة، غير أن القانون سمح بصفة استثنائية الخروج عن هذه القاعدة وذلك بغرض مواجهة التطور الاجرامي، من خلال استحداث أحكام خاصة

[1]- جمال نجيمي، قانون الاجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، ط 1، دار هومة، الجزائر، 2015-2016، ص 157.

تتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور على أن يكون ذلك تحت مراقبة مباشرة من طرف رجال القضاء بما فيهم ممثلو الادعاء العام، (اللجوء لهذا الاجراء بتم بوجود شروط خاصة ولا يمكن لضباط الشرطة القضائية اتخاذ هذه التدابير في التحريات العادية)، بينما قوانين الاجراءات الجزائية في فرنسا والمغرب لم تعط هذه السلطة للنيابة.[1]

أ-الاذن

أول ما يجب توفره كشرط أساسي لتكون اجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور صحيحة قصد التحقيق في الجرائم المعلوماتية هو توفر الاذن من وكيل الجمهورية ويباشر تحت مراقبته، ويشترط في الاذن أن يتضمن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة والجريمة موضوع المتابعة والتي تبرر اللجوء الى هذا الاجراء.

وقد أعطى المشرع الجزائري حماية قانونية خاصة لسرية لمراسلات و الاتصالات و للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، من خلال الدستور حيث لا يجوز المساس بهذه الحقوق دون أمر معلل من السلطات القضائية، و يعاقب القانون على أي انتهاك لذلك، و يقصد بذلك وجوب احترام الاذن بالمراقبة الالكترونية بعد اخطار النيابة العامة المتمثلة في وكيل الجمهورية، و عزز فيما بعد بالقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، و بتحليلنا لأحكام هذا القانون نجد أنه نص صراحة على وجوب الموافقة المسبقة حيث لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي الا بالموافقة الصريحة للشخص المعني، و استثنى من مجال تطبيق هذا القانون المعطيات ذات الطابع الشخصي المحصل عليها و المعالجة لمصلحة الدفاع و الأمن الوطنيين، أو المحصل عليها لأغراض الوقاية من الجرائم

[1]- جمال نجيمي، مرجع سابق، ص 159.

و متابعة مرتكبيها أو لمواجهة هذه الجرائم و المتضمنة في قواعد البيانات القضائية حيث لا يمكن معالجة المعطيات ذات الطابع الشخصي المتعلقة بالجرائم و العقوبات و تدابير الأمن الا من قبل السلطة المختصة و السلطات العمومية و الأشخاص المعنويين الذين يسيرون مصلحة عمومية و مساعدي العدالة في اطار اختصاصهم، مع اشتراط ان تحدد عند المعالجة المسؤول عنها و الغاية منها و الأشخاص المعنيين بها و الغير الذي يحق له الاطلاع على المعلومات و مصدرها و الاجراءات اللازمة لضمان سلامة المعالجة، و في هذا الاطار لابد أن يلتزم المسؤول عن المعالجة بسريتها تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول.

ب-طبيعة الجريمة:

خص المشرع اجراء اعتراض المراسلات اضافة الى تسجيل والتقاط الصور، في التحري عن الجرائم المتلبس بها أو في التحقيق الابتدائي في الجرائم المحددة على سبيل الحصر من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ولعل الغرض من ادراج هذه الجرائم هو خطورتها الاجرامية وأثرها على السياسة العامة للدولة وعلى اقتصادها.

وإذا رأت المحكمة أن الواقعة لا تشكل جريمة في نظر قانون العقوبات أو أنها غير ثابتة تقضي ببراءة المتهم بغير عقوبة أو مصاريف، وهو ما قضت به محكمة قالمة في قضية نشر الصور على شبكة الانترنت على موقع XX حيث تبين للمحكمة أنه لا يوجد في الملف ما يثبت ان هذا الموقع خاص بالمتهم وأنكر هذا الاخير ملكيته للموقع، وبالتالي نشر الصور ووضعها في متناول الجمهور غير ثابت في حق المتهم مما يتعين براءته من الجرم المتابع به، وجعل المصاريف على الخزينة العمومية.[1]

[1]- حكم، محكمة قالمة، قسم الجنح، رقم الجدول: 10/07102، رقم الفهرس: 11/02248، تاريخ الحكم: 28-03-2011.

ج-تحرير محضر:

حيث يشترط تحرير محضر من ضابط الشرطة القضائية المأذون له أو المناب، مع ذكر تاريخ وساعة بداية العملية وانتهائها.

يتعلق المحضر الأول بالجانب التقني و بتاريخ و ساعة بداية العملية و انتهائها، و يوجد محضر ثاني يدرج فيه مضمون اعتراض المراسلات أو الصور أو المحادثات، والتي تفيد في تقصي الحقائق، دون تلك الواقعة بين المتهم ودفاعه الا اذا تعلقت بمساهمة المحامي في الجريمة، مع الاحتفاظ بالتسجيل برمته جعله في حرز مختوم يضمن سلامته، ولم يمنع القانون من أخذ نسخ احتياطية لذلك التسجيل، وما يلاحظ أن المشرع الجزائري لم يتطرق لمصير السند المادي للتسجيل، خلافا للمشرع الفرنسي الذي نص على تحطيمه بعد انقضاء الدعوى العمومية نهائيا، بينما المحاضر تبقى مدرجة في ملف الدعوى.[1]

د-الالتزام بكتمان السر المهني:

حيث يشترط عدم الاخلال بالسر المهني واتخاذ جميع التدابير اللازمة لضمان احترام ذلك السر، وذلك تأسيسا على نص المادة 65 مكرر 6 التي تقضي بأن تتم العمليات المحددة في المادة 65 مكرر 5، دون المساس بالسر المهني المنصوص عليه في المادة 45 من القانون 06-22.

ثانيا: تنفيذ عملية اعتراض المراسلات والتقاط الصور وتسجيل الأصوات

وفقا لنص المادة 65 مكرر 5 يسمح الاذن بهذه العملية بوضع الترتيبات التقنية للدخول الى المحلات السكنية وغيرها ولو خارج المواعيد المحددة في المادة 47 من القانون 06-22، وبغير علم أو رضا الأشخاص الذي لهم حق على تلك الأماكن.

[1]- جمال نجيمي، مرجع سابق، ص 161.

وتنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص، وعند فتح تحقيق قضـــائي تتم العمليات بناء على اذن من قاضـــي التحقيق وتحت رقابته المباشرة في إطار انابة قضائية.

فلابد من الســـهر على التنســـيق بين العدالة وضـــباط الشـــرطة القضـــائية، فلوكيل الجمهورية وقاضـي التحقيق (كل حسـب اختصـاصـه) في إطار اعتراض ومراقبة الاتصـالات السهر على التنسيق بينه وبين عناصر الشرطة القضائية لأن لهما سلطة المراقبة على انجاز وتنفيذ التعليمات حول كل ما سـجل خلال العملية ومصـير ملف القضـية حيث ألزم المشـرع ضابط الشرطة القضائية بالتقيد بما ورد في طلبات القضاة.[1]

ثالثا: حالات اللجوء الى المراقبة الالكترونية

المراقبة الالكترونية، هي اجراء تدخلي في الحياة الخاصـــــة، ومنه قيدها المشـــــرع الجزائري بجملة من الاجراءات الضرورية لصحتها وذلك بهدف الوقاية من الجرائم المعلوماتية وذلك من خلال نصه في المادة 04 من القانون 09-04 على حالات محددة حصرا يتم فيها اللجوء الى المراقبة الالكترونية وتتمثل هذه الحالات في:

1. الوقاية الأفعال الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
2. في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية بما يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
3. لمقتضـــيات التحري والتحقيق القضـــائي في حالة صـــعوبة الوصـــول الى نتيجة تهم البحث دون اللجوء الى هذا الاجراء.
4. في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

[1]- أعمر قادري، أطر التحقيق وفق أحكام نصوص الاجراءات الجزائية، ط 2، دار هومة، 2015، ص 70.

1-في الجرائم الارهابية أو التخريبية أو الماسة بأمن الدولة:

لدواعي المحافظة على الأمن والنظام العام والوقاية من الجرائم الخطيرة تضمن القانون 09-04 سالف الذكر، استثناء فيما يخص امكانية اللجوء الى المراقبة الالكترونية للوقاية من الجرائم الإرهابية أو التخريبية أو الماســـة بأمن الدولة، على أن يختص النائب العام لدى محكمة الجزائر بمنح ضباط الشرطة القضائية المنتمين الى الهيئة اذنا لمدة ستة أشهر قابلة للتجديد على أســاس تقرير يبين طبيعة الترتيبات التقنية المســتعملة والأغراض الموجهة لها، وتكون هذه الترتيبات حصريا لتجميع وتسجيل معطيات ذات صلة بهذه الجرائم[1].

وتكلف مديرية المراقبة الوقائية واليقظة الالكترونية التابعة للهيئة الوطنية للوقاية من الجرائم المتصـــلة بتكنولوجيات الاعلام والاتصـــال حســـب الفقرة الأولى من المادة 15 من المرسوم الرئاسي 20-183، بالمراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الارهابية والتخريبية والاعتداء على أمن الدولة.

وفي إطار التنســـيق مع المصـــالح الأمنية، تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال قصد الوقاية من الجرائم الارهابية والتخريبية والماسة بأمن الدولة حصريا في مجال اختصاصها، بمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.[2]

[1]- المادة 04 من القانون 09-04 سالف الذكر، ص 06.

[2]- المادة 22 من المرسوم الرئاسي رقم 20-183، سالف الذكر، ص 08.

2-في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:

أجاز المشـــرع الجزائري اللجوء الى اجراء المراقبة الالكترونية في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.[1]

وتكلف مديرية المراقبة الوقاية واليقظة الالكترونية التابعة للهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام و الاتصـــال حســـب نص المادة 15 من المرســـوم الرئاسي رقم 20-183، بمساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها، بما في ذلك الخبرات القضـــائية في اطار مكافحة الجريمة المرتبطة بتكنولوجيات الاعلام و الاتصـــال والجرائم التي تتطلب اللجوء الى هذا أســـاليب التحري الخاصـــة للهيئة، اضـــافة الى جمع و تســـجيل و حفظ المعطيات الرقمية و تحديد مصـــدرها وتتبعها بغرض اســـتعمالها في الاجراءات القضـــائية، واليقظة الالكترونية في مجال الجرائم المتصـــلة بتكنولوجيات الاعلام و الاتصال.

وفي كل الحالات التي تســـمح باللجوء الى اجراء المراقبة، ينبغي على الهيئة الوطنية للوقاية من الجرائم المتصـــلة بتكنولوجيات الاعلام والاتصـــال حســـب المادتين 24-25 من المرســـوم الرئاســـي 20-183، حفظ المعلومات المحصـــل عليها أثناء عمليات المراقبة، مع تســـجيل الاتصـــالات الالكترونية التي تكون موضـــوع مراقبة وتحرير محضـــر وفقا للشـــروط والأشكال المنصوص عليها في قانون الاجراءات الجزائرية.

[1]- المادة 04 من القانون 09-04، سالف الذكر، ص 06.

ويمكن للإطارات المختصين التابعين للهيئة الحائزين على صفة الضبطية القضائية أثناء ممارستهم ووظائفهم أو بمناسبتها، القيام بالتفتيش أي مكان أو هيكل أو جهاز بلغ الى علمهم أنه يحوز و–أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية.[1]

وبناء على ما جاء في القانون 09–04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها والمرسوم الرئاسي الأخير 20–183، الذي يحدد اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، يتضح لنا أن عملية المراقبة الالكترونية تعتبر من الاجراءات الخطيرة والتي تتطلب اجراءات مشددة وهو ما سار عليه المشرع الجزائري وذلك بغية توفير حماية أكبر للحق في حرمة الحياة الخاصة الرقمية والمحافظة على الحريات الفردية في البيئة الرقمية.

الفرع الثاني: التسرب

يعرف التسرب على أنه اجراء يقوم به ضابط الشرطة القضائية أو أحد أعوانه تحت مسؤوليته بتنسيق العملية لمراقبة الأشخاص المشتبه فيهم بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.[2]

وهو اجراء جديد جاء به المشرع الجزائري إذا اقتضت ضرورة التحري والتحقيق اللجوء له في الجرائم السبعة المحددة على سبيل الحصر وتتمثل في: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، الجرائم

[1]– المادة 30 من المرسوم الرئاسي رقم 20–183، سالف الذكر، ص 09.

[2]– المادة 65 مكرر 12 من القانون 06–22 المتضمن قانون الاجراءات الجزائية المعدل والمتمم.

الارهابية، جرائم تبييض الأموال، الجرائم المتعلقة بالتشـريع الخاص بالصـرف، اضـافة الى جرائم الفساد.

أولا: شروط صحة التسرب

عندما تقتضـي ضرورات التحري والتحقيق في احدى الجرائم المحددة حصرا في المادة 65 مكرر 5 يجوز لوكيل الجمهورية أو قاضـــي التحقيق، بعد اخطار وكيل الجمهورية أن يأذن تحت رقابته بمباشرة عملية التسرب.

1-الاذن:

يجب أن يصـدر الاذن من وكيل الجمهورية المختص أو قاضـي التحقيق بعد اخطار وكيل الجمهورية[1]، والاذن يمنحه هذا الأخير بصـفته مدير الضـبطية القضـائية وممثل النيابة وقاضـي التحقيق في إطار انابة قضـائية.[2] ولابد أن يكون الاذن مكتوبا ومسـببا ومحدد المدة تحت طـائلـة البطلان، ويجـب أن يـذكر في الاذن الجريمـة التي تبرر اللجوء لهـذا الاجراء وهوية ضابط الشرطة القضائية الذي يقوم بعملية التسرب.

وتجدر الاشـــارة الى أنه يمكن أن تجدد العملية حســب مقتضـــيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية.

والمدة الزمنية هي 4 أشـــهر قابلة للتجديد، يجوز للقاضـــي الذي رخص بها أن يأمر بوقفها في أي وقت قبل انقضـاء المدة، وللمتسـرب مواصـلة النشـاط هنا للوقت الضـروري الكافي لتوقيف العملية في ظروف تضـمن أمنه دون مسـؤوليته جزائيا، بشـرط ألا تتجاوز 4

[1]- المادة 65 مكرر 11 من القانون 06-22 المتضمن قانون الاجراءات الجزائية المعدل والمتمم.

[2]- المادة 138 من القانون 06-22 المتضمن قانون الاجراءات الجزائية المعدل والمتمم.

أشــهر، كما يمكن تمديد المدة لمدة 4 أشــهر أخرى إذا لم يتمكن العون المتســرب من انهاء نشاطه في ظروف تضمن أمنه.

2-تحرير محضر

حيث يعد تقريرا يتضــمن العناصــر الضــرورية لمعاينة الجرائم غير تلك التي تعرض أمن الضابط أو العون المتسرب للخطر.

ثانيا: تنفيذ عملية التسرب

يهدف التســرب الى جمع البيانات والمعطيات الخاصــة التي تشــير الى كافة الأعمال الاجرامية، وتمكين المصـــالح الأمنية من معرفة الامكانيات المادية والبشـــرية المســـتعملة، وكذلك الأساليب ووسائل الاتصال والتنقل المستغلة من أجل ارتكاب أفعال مشبوهة.[1]

بتوفر الشـروط سـالفة الذكر يباشـر عضـو الضـبط القضـائي مهامه وتنفذ العملية في إطار اجرائي محكم.

حيث أن مباشـرتها تكون باسـم مسـتعار ولا يجوز اظهار الهوية الحقيقية للضـابط أو المتسرب في أي مرحلة من مراحل الاجراءات، ويعاقب كل من يكشف عن هويته.

وقد أجاز المشـــرع لـه الاســـتعانة بمجموعة من الوســـائل والقيام ببعض الافعال المنصـــوص عليها في المادة 65 مكرر 14 من القانون 06-22، دون أن يكون مســـؤولا جزائيا، وتتمثل في:

-اقتناء أو حيازة أو نقل أو تسليم أو اعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجريمة أو مستعملة في ارتكابها.

[1]- أعمر قادري، مرجع سابق، ص 75.

-استعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الايواء أو الحفظ أو الاتصال.

ثالثا: معوقات عملية التسرب

على الرغم من تسخير المشرع الجزائري لمجموعة من القوانين المنظمة لأسلوب التسرب، غير أن ذلك قد يحول دون نجاعة العملية على أرض الواقع نتيجة لعدة عراقيل والتي نذكر منها:

- لا يزال التسرب الالكتروني في الجزائر في مراحله الأولى من الناحية التطبيقية وذلك لقلة الأحكام القضائية التي تثبت اللجوء اليه في شبكة المعلومات الانترنت، مقارنة بتشريعات أخرى، ولربما سيكون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال دور في تفعيل هذا الاجراء.[1]
- اغفال المشرع الجزائري النص على كيفية تمويل المتسرب: ففي كثير من الأحيان يضطر المتسرب الى سد بعض المصاريف الخاصة بعملية التسرب الالكتروني من حسابه الخاص، وهو ما يستدعي النص على انشاء حساب أو صندوق على مستوى الخزينة لتمويل العملية مواجهة هذه الاشكالية.
- عدم تنظيم عملية استخراج الهوية المستعارة للمتسرب: حيث أغفل المشرع التطرق الى هذه المسألة، حيث يستصعب اثبات المتسرب لهويته بموجب وثائق ادارية لبعث روح الاطمئنان في نفوس الجماعات الاجرامية، وفي ظل اغفال الجهة المانحة لهذه الهوية ينبغي معالجة هذا الفراغ القانوني بنص قانوني صريح.
- اغفال مسألة القبض على العضو المتسرب ضمن الجماعات الاجرامية:

[1]- يوسف مناصرة، الدليل الالكتروني في القانون الجزائي، مرجع سابق، ص 477.

سـواء داخل أو خارج حدود الدولة ففي أغلب الحالات وخاصـة في الجرائم المحددة على سبيل الحصر ومن بينها الجرائم المتعلقة بالمعالجة الآلية للمعطيات والتي تتسم بعبورها لحدود الدولة الواحدة، قد يقع المتسـرب في اشـكالية القبض عليه، مما يتطلب توفير الحماية الكافية له بوضـع نصـوص قانونية تنظم هذه المسـألة ومنح ضـمانات أكبر له، مع عقد اتفاقيات دولية ثنائية أو جماعية.

– في حالة تعرض المتسرب الى العجز يتعذر سماعه كشاهد: فعلى الرغم من جوازية سماع ضابط الشرطة القضائية منسق عملية التسرب كشاهد في أي مرحلة من مراحل التحقيق[1]، كان لزاما على المشـرع تضـمين مسـألة الشـهادة ضـمن أحكام القانون 15–03 المتعلق بعصرنة العدالة والذي استحدث تقنية جديدة للإدلاء بتصريحات عن بعد عن طريق الشاشة الالكترونية ولو بتقنية تغيير الصوت والصورة.

والجدير بالذكر أن المادة 56 من القانون 06–01 المتعلق بالوقاية من الفسـاد ومكافحته، تطرقت الى أساليب التحري الخاصـة والمتمثلة في الترصـد الالكتروني والاختراق دون تعريفهما، وذلك بعد اذن من وكيل الجمهورية.

كذلك المادة 40 من الأمر 05–06 المتعلق بمكافحة التهريب المعدل والمتمم الذي أجازت امكانية اللجوء الى أسـاليب تحري خاصـة، لما لها من نجاعة في مواجهة الجرائم المسـتحدثة خاصـة مع آفاق عولمة الاقتصـاد وتوجهه نحو اقتصـاد السـوق، وهو ما ادى بالمشرع الى مواكبة اشكال الاجرام المستحدث ومواءمته مع التشريعات المقارنة، غير أنه لا يمكن الجزم بأن النصوص المذكورة أعلاه تجيز صراحة اللجوء الى التسرب الالكتروني، لذا

[1]– المادة 65 مكرر 18 من القانون 06–22 المتضمن قانون الاجراءات الجزائية المعدل والمتمم.

من المستحسن تعديل فقرات المادة 65 مكرر 12 من قانون الاجراءات الجزائية لرفع اللبس في تفسيرها.[1]

المطلب الثاني: الاجراءات المتعلقة بالبيانات الالكترونية المخزنة

قبل البداية في التحقيق في الجرائم المعلوماتية تتخذ مجموعة من الاجراءات التمهيدية لجمع الأدلة والتي يقوم بها غالبا مقدمي خدمات الكمبيوتر والانترنت بتكليف من السلطة المختصة، ويكون الهدف من هذه الاجراءات مراقبة ومتابعة استخدام وسائل تقنية الاتصالات الحديثة، وتسجيل كل البيانات المخزنة بالأجهزة المستخدمة في الاتصالات (كمبيوتر، انترنت)، وذلك لتسهيل مهمة سلطة التحقيق في كشف الجرائم المعلوماتية والبحث عن الأدلة وضبطها.[2]

وللبيانات الالكترونية المخزنة أهمية بالغة في مجال التحقيق في الجرائم المعلوماتية، وبناء على ذلك ينبغي المحافظة عليها وحمايتها من كل ما يؤدي الى تلفها أو تعديلها؛ وتكمن الأهمية خصوصا بالنسبة للبيانات المتعلقة بالاتصالات الالكترونية التي يتم الاحتفاظ بنسخة منها في الخادم المعلوماتي لدى مزود خدمة الاتصال والانترنت، في أنه يمكن استخدامها من طرف سلطات التحقيق كأدلة اثبات في حالة تلاعب الجاني أو غيره بالبيانات الالكترونية الأصلية، والتي تشكل دليلا في مواجهته، كما يمكن من خلالها تتبع أثر المجرم المعلوماتي ومعرفة هويته، كما قد تشكل هذه البيانات دليلا للإثبات خاصة فيما يتعلق بالاتصالات الالكترونية ذات المحتوى غير المشروع.[3]

[1]– يوسف مناصرة، الدليل الالكتروني في القانون الجزائي، مرجع سابق، ص 481.

[2]– رامي متولي القاضي، مرجع سابق ص 125.

[3]– رشاد خالد عمر، مرجع سابق، ص 194.

ويقصد بمقدمي الخدمات:

1-أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و / أو نظام للاتصالات،

2-وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.[1]

الفرع الأول: الاجراءات العامة لمقدمي الخدمات

يلتزم مقدمي الخدمات بمجموعة من الإجراءات العامة والمتمثلة فيما يلي:

أولا: اجراء الرقابة الموجهة والمؤقتة:

تعتبر المراقبة الالكترونية اجراء تطفلي على الحياة الخاصة، ولذلك سعى القانون 09-04 لتوفير اجراءات صارمة لضمان توازن بين مصالح العدالة والحقوق الأساسية للإنسان، من خلال الاستشراف القضائي على عمليات المراقبة وتحديد حالات محددة حصرا يجوز فيها اللجوء الى هذا الاجراء، وعليه حفاظا على النظام العام و لدواعي أمنية أو للوقاية من الجرائم الخطيرة، يجيز القانون وضع ترتيبات تقنية وبرامج معلوماتية على مستوى متعاملي الانترنت من أجل القيام بعمليات الرقابة على الاتصالات الالكترونية وتسجيل محتواها في الوقت الحقيقي، وهي عبارة عن مراقبة موجهة (تتم في حالات محددة حصرا)، ومؤقتة ومأذون بها حصريا من طرف السلطة القضائية في شكل ترخيص مكتوب من الجهة القضائية المختصة[2]

[1]- المادة 02 من القانون 09-04 سالف الذكر، والمادة الأولى من الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست).

[2]- يوسف مناصرة، الدليل الالكتروني في القانون الجزائي، مرجع سابق، ص 315.

ويعد تجميع معطيات المرور المتعلقة بالاتصـالات الالكترونية في وقتها الفعلي عبارة عن قيام مقدم الخدمة بناء على طلب من سـلطات البحث والتحقيق بتسـجيل بيانات أو معلومات اتصـال معين في فترة الانتاج ونسـخ صـور منها ثم تجميعها لحظة النقل عبر الاتصـال، وتتم عملية التجميع هنا في شـكل ذبذبات صـوتية أو الكترونية دون أن يؤثر ذلك على حركتها أو تنقلها أو اعاقة وصولها الى المرسل اليه.[1]

ويقابل هذا الالتزام ما جاء في المادة 20 من اتفاقية بودابسـت بشـأن جمع بيانات الكمبيوتر في الوقت الحقيقي، حيث تعتمد كل دولة طرف على اتخاذ التدابير اللازمة لتمكين سـلطاتها المختصـة من ... اجبار مزود الخدمة في نطاق قدرته الفنية على جمع أو تسـجيل من خلال تطبيق وسائل فنية أو التعاون مع السلطات المختصة ودعمها في جمع أو تسجيل بيانات الحركة في الوقت الحقيقي، على أن يلتزم مزود الخدمة بالسـرية عند قيامه بهذا الاجراء.

ثانيا: مساعدة السلطات

باسـتقراء نص المادة 10 من القانون 09-04، فانه يتعين على مقدمي الخدمات تقديم المسـاعدة اللازمة للسـلطات المكلفة بالتحريات القضـائية لجمع وتسـجيل المعطيات المتعلقة بمحتوى الاتصـالات في حينها وبوضـع المعطيات المتعلقة بحركة السـير، تحت تصرف السلطات المختصة.

واسـتنادا للمعطيات المكشـوف عنها من طرف مقدم الخدمة، يتسـنى للسـلطات المختصـة من اتخاذ القرار المناسـب، و من ثم يتمكن المحقق من تحديد مصـدر أو مسـتقبل الاتصـال مع امكانية التعرف على مرتكبي الجريمة محل التحقيق، و يقابل هذا الالتزام ما تضـمنته المادة 18 من اتفاقية بودابسـت من التزام مقدم الخدمة بتقديم بيانات أو معطيات

[1]–براهيمي جمال، مرجع سابق، ص 112.

محددة (تعتمد كل دولة طرف ما يلزم من تدابير تشـــريعية و غيرها من التدابير لتمكين سلطاتها المختصة اصدار أمر الى: ...أي مزود خدمة بعرض خدماته داخل أراضي الدولة الطرف بتقديم معلومات عن المشـترك ذات الصـلة بتلك الخدمات الموجودة بحوزته أو تحت ســيطرته)، حيث يعد تقديم المعطيات الى المحققين وســيلة من وســائل التعاون الفعالة في اقامة الدليل الالكتروني.[1]

ويقصد بعبارة معلومات عن المشترك: أي معلومات مدرجة في شكل بيانات الكمبيوتر أو في شكل آخر يحفظها مقدم الخدمة وتتعلق بالمشتركين في الخدمات التي يزودها بخلاف بيانات الحركة أو المضمون والتي بموجبها يمكن تحديد:

- نوع خدمة الاتصال المستخدمة والشروط الفنية المرتبطة بها ومدة الخدمة
- هوية المشـــترك وعنوانه البريدي أو الجغرافي، ورقم هاتفه وغيره من أرقام الولوج والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق أو ترتيبات الخدمة
- أي معلومات أخرى عن موقع تركيب أجهزة ومعدات الاتصـــال المتاحة بموجب اتفاق أو ترتيبات الخدمة[2]

كما أنه وفي إطار مســـاعدة الســـلطات يتعين على مقدمي الخدمات كتمان ســـرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصـــلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

[1]– يوسف مناصرة، الدليل الالكتروني في القانون الجزائي، مرجع سابق، ص 318.

[2]– المادة 18 من الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست)، 2001، الصادرة عن مجلس أوروبا، مجموعة المعاهدات الأوروبية–رقم 180، ص 10.

ثالثا: حفظ المعطيات المتعلقة بحركة السير

لتلافي كل المشـــكلات التي تصـــادف الأدلة التقنية و الناجمة عن مرونة العالم الافتراضـي وامكانية ازالة الأدلة التقنية أو تخلفها نهائيا استلزم وضـع اطار قانوني من خلال اتباع نظام الزام مزودي الخدمات بحفظ البيانات، وهو ما تضـمنه قرار الجمعية العامة للأمم المتحدة رقم (63-55) المؤرخ في 22 يناير 2001، المتعلق بمكافحة اســـاءة اســـتعمال تكنولوجيا المعلومات لأغراض اجرامية حيث ألزمت المادة الأولى منه، الدول بأن تســـمح بحفظ البيانات الالكترونية المتعلقة بالتحقيقات الجنائية الخاصة و سرعة الحصول عليها،[1] و أكدت المادة 10 من القانون 09-04 ذلك من خلال الزامية مسـاعدة السـلطات. ان التحفظ الســـريع يعتبر اجراء من اجراءات جمع البيانات الالكترونية المخزنة، توجه الســـلطات المختصـة بموجبه أمرا الى مقدمي الخدمة، وذلك بغرض القيام بالتحفظ على وجه الاستعجال على بيانات الكترونية ساكنة ومخزنة لديه أو في أي مكان آخر خاضـع لسيطرته، الى حين اتخاذ اجراءات قانونية كطلبها أو تفتيشها.

كما يعد هذا الاجراء أداة تحقيق مســـتحدثة وهو اجراء أولي تمهيدي الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها، ويقصـــد به: توجيه الســـلطة المختصـــة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته وتحت سـيطرته في انتظار اتخاذ اجراءات قانونية أخرى كالتفتيش، أو الأمر بتقديم بيانات معلوماتية.[2]

وعرفت المادة 02 من القانون 09-04 المعطيات المتعلقة بحركة الســير بأنها: (أي معطيات متعلقة بالاتصـــال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا

[1]- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط 1، منشورات الحلبي الحقوقية، بيروت لبنان، 2012، ص 446.

[2]- نجاة بن مكي، مرجع سابق، ص 230

في حلقة اتصالات، توضح مصدر الاتصال، والجهة المرسل اليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة)

وباستقرائنا لنص المادة 11 من نفس القانون، نجد أن المشرع الجزائري حدد المعطيات التي يلتزم مقدمو الخدمات بحفظها على سبيل الحصر وتشمل:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها
- المعطيات التي تسمح بالتعرف على المرسل اليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.
- بالنسبة لنشاط الهاتف يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

وللحد من المشاكل التي تصادف الأدلة التقنية فرضت بعض التشريعات على مقدمي الخدمة وجوب الاستجابة لطلب التحفظ الصادر من السلطات المختصة على وجه السرعة، وتختلف مدة التحفظ من تشريع لآخر، حيث أن المشرع الأمريكي فرض الالتزام بالتحفظ على البيانات الالكترونية المخزنة لديه أو في أي مكان آخر تحت سيطرته لمدة لا تزيد عن 90 يوما، مع امكانية تجديد هذه المدة الى 90 يوما أخرى بناء على طلب الجهة المختصة.[1]

[1]– رشاد خالد عمر، مرجع سابق، ص 195.

فيما حدد المشـرع الفرنسـي التحفظ لمدة لا تزيد عن سـنة واحدة بطلب من السـلطات المختصة[1].

وقد وضـــع المشـــرع الجزائري مدة محددة لحفظ البيانات أو المعطيات والمقدرة بســـنة واحدة ابتداء من تاريخ التسجيل، ولعل ذلك هو ضمانة أخرى لحرمة الحياة الخاصة للأفراد.

وفي نفس السياق نصت المادة 16 من اتفاقية بودابست على انه يجب على كل دولة طرف ان تتبنى الاجراءات التشريعية وأية اجراءات اخرى ترى أنها ضرورية لتخويل سلطاتها المختصة أن تأمر بالتحفظ العاجل على البيانات المخزنة.

ولعل الغرض من ذلك هو تمكين السـلطة المختصـة بالتحقيق في الجرائم المعلوماتية من معرفة مضـمون البيانات المرسـلة أو المسـتقبلة سـواء عند اجراء التفتيش أو بطلبها من مقدمي الخدمة، ويلتزم هذا الأخير بالحفاظ على البيانات وحمايتها من الضياع أو التعديل أو التلف، مع الحفاظ على عنصر السرية ومنع الغير من الحصول أو الوصول اليها.[2]

ويثور التساؤل حول الجهة المختصة بإصدار الأمر بالتحفظ السريع على البيانات المخزنة؟

بالرجوع الى الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية نجد أنها أشارت فقط الى أنه "يختص بإصدار التحفظ السلطة المحددة في التشريع الداخلي لكل دولة"، حيث لم تحدد الجهة المختصـة، وأشـارت فقط الى مصـطلح (السـلطات المختصـة)، وذلك راجع لاختلاف هذه السـلطات المختصـة من دولة الى أخرى حسـب نوعية الاجراء إذا كان اجراء تحقيقي أو اجراء استدلالي، وحسب نوع النظام المعمول به في تلك الدولة.

[1] –Guy de Felcourt, L’usurpation d’identité ou l’art de la fraude sur les données personnelles, CNRS éditions, 2011, Paris, France, p 212.

[2]– رامي متولي القاضي، مرجع سابق، ص 126.

وبالرجوع الى المشرع الفرنسي نجد أنه خول لضباط الشرطة القضائية اصدار هذا الأمر، وذلك بناء على امر مسبق له من النائب العام المختص وذلك بإذن من قاضي محكمة الجنح، وهذا عكس المشرع الأمريكي والذي وسع من نطاق الجهة المخولة بإصدار الأمر بالتحفظ المستعجل، حيث أجاز اصداره من قبل أيه جهة حكومية.[1]

بالنظر الى المادة 10 ف 1 من القانون 09-04 سالف الذكر، نجد أن المشرع الجزائري سمح بتسجيل محتوى الاتصالات في حينها، و هو اجراء تسخير من طرف السلطات القضائية لمقدمي الخدمات المعنيين بجمع تسجيل المعطيات المتعلقة بمحتوى الاتصالات بمختلف انواعها، غير أن المشرع الجزائري على عكس مثيله الفرنسي، كما لم يحدد الأشخاص المسموح لهم بتسخير مقدمي الخدمات، و ترك المجال مفتوحا للاجتهاد، في حين أن المشرع الفرنسي سمح لضباط الشرطة القضائية بتسخير من وكيل الجمهورية مع ترخيص مسبق من طرف قاضي الحريات و الحبس بتكليف مقدمي الاتصالات للقيام بكل الاجراءات التي تؤمن الحفظ لمدة لا تزيد عن سنة واحدة لمحتويات البيانات المتعلقة بمستعملي الخدمات[2]

و تجدر الاشارة الى أنه و رغم تعدد طرق الوصول الى الانترنت الا أنه في كل الأحوال لابد من وجود مقدم خدمة، وقد ثار التساؤل حول امكانية قيام مسؤولية مقدم الخدمة باعتباره فاعل أصلي في الجريمة؟ ، وفي هذا الصدد يرى بعض الفقهاء بعدم مسؤوليته تأسيسا على أن عمله فني و لا يمكنه مراقبة المحتوى المقدم، كما لا يمكنه مراقبة تصرفات مستخدمي الانترنت، وأيد هذا الموقف القضاء الفرنسي على أساس أن مجرد قيام مستخدم

[1]- رشاد خالد عمر، مرجع سابق، ص 196.

[2]- براهيمي جمال، مرجع سابق، ص 102-103.

الشبكة ببث رسالة غير مشروعة لا يكفي لقيام مسؤولية مقدم الخدمة، و ذلك لوجود كم هائل من الرسائل المتداولة يوميا، اضافة الى العدد اللانهائي من المشتركين.

في حين أن هناك رأي آخر يرى بضرورة مسائلة مقدم الخدمة على أساس مسؤوليته التوجيهية، حيث يتعين عليه منع نشر محتوى صفحات الشبكة المتعارضة مع القوانين والنظم واللوائح أو المصلحة العامة، وتأسيسا على ذلك نص التوجيه الأوروبي لسنة 2000 على التزام الدول الأعضاء بتوحيد المعاملة القانونية لمسؤولية الوسطاء المقدمين لخدمة الانترنت، ولابد لهم من ايقاف اي عمل غير مشروع.[1]

وبالرجوع الى القانون الجزائري نجد أن المشرع حدد مسؤولية مقدي الخدمات بموجب المادة 11 من القانون 09-04 سالف الذكر، ففضلا على العقوبات الادارية المترتبة على عدم احترام الالتزامات المفروضة عليهم، تترتب مسؤوليتهم الجزائية في حالة الاخلال بحسن سير التحريات القضائية، وفي ذلك يعاقب الشخص الطبيعي بعقوبة سالبة للحرية وتتمثل في الحبس من 6 أشهر الى 5 سنوات، اضافة الى عقوبة مالية تتراوح بين 50.000 دج الى 500.000 دج، أما النسبة للشخص المعنوي يعاقب بغرامة وفقا للقواعد المقررة في قانون العقوبات.

الفرع الثاني: الاجراءات الخاصة بمقدمي خدمات الانترنت

زيادة على الالتزامات المفروضة على جميع مقدمي الخدمات والمتمثلة في تقديم المساعدة للسلطات وحفظ المعطيات المتعلقة بحركة السير، فقد أضاف المشرع بموجب المادة 12 من القانون 09-04، بعض الالتزامات الخاصة الملقاة على عاتق مقدمي خدمة الانترنت وتتمثل في: التدخل الفوري ووضع الترتيبات التقنية اللازمة.

[1]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 440.

أولا: التدخل الفوري

ويقصد بذلك التزام مقدمي خدمات الانترنت بالتدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها[1] بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول اليها غير ممكن:

وتبعا لنص المادة 394 مكرر 8 من قانون العقوبات، يتضح أن المشرع الجزائري أدرج الاخلال بهذا الالتزام تحت طائلة التجريم، حيث من الممكن قيام المسؤولية الجزائية لمقدمي خدمات الانترنت في حالة عدم وضع حد للأنشطة غير المشروعة سواء تم اخطارهم بالصفة الجرمية عبر قرار قضائي من الجهات القضائية، أو بناء على اعذار من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

حيث يتطلب سحب أي محتوى غير مشروع بسرعة ودون تمهل أو منع الوصول اليه كمختلف الممارسات الاباحية ضد الأطفال، فيروسات والبرامج الضارة بالمعطيات، حالة تزوير البطاقات البنكية أو جرائم الاحتيال وغيرها. وقد تداركت اتفاقية بودابست القصور في تحديد مفهوم المحتوى غير المشروع كون الفكرة في حد ذاتها مختلفة من دولة لأخرى، وذلك عن طريق البروتوكول الاضافي المتعلق بتجريم أفعال التمييز والتحريض على الكراهية بواسطة منظومة معلوماتية.[2]

ثانيا: وضع ترتيبات تقنية لمنع وصول الجمهور الى الأنشطة المعلوماتية المجرمة

حيث ألزم المشرع الجزائري وفقا للمادة 12 من القانون 09-04 بحصر امكانية الدخول الى الموزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة من

[1]- عادل بوزيدة، المسؤولية الجزائية لمتعهدي مواقع الانترنت، أطروحة دكتوراه تخصص القانون الجنائي الاقتصادي، جامعة تبسة، 2017، ص 28.

[2]- يوسف مناصرة، الدليل الالكتروني في القانون الجزائي، مرجع سابق، ص 321.

خلال وضـــع ترتيبات تقنية تمنع من الوصـــول الى الأنشـــطة المعلوماتية المجرمة، كما ألزم مقدمي خدمات الانترنت أيضـــا بإخبار المشـــتركين لديهم بوجودها. وما يلاحظ أنه تم النص على هذا الالتزام وتقرير مضـــمونه وفقا لنص المادة 14 من المرســـوم التنفيذي 98-257 (المعدل بالمرسوم التنفيذي 2000-307 الذي يضبط شروط وكيفيات اقامة خدمات انترنت واستغلالها)، حيث يحدد الالتزامات الواقعة على متعهدي الوصول لخدمة الايواء المعلوماتي، وجاء فيه بضـــرورة اتخاذ متعهدي الوصـــول كافة الاجراءات اللازمة لتأمين حراســـة دائمة لمضـــمون الموزعات المفتوحة لمشـــتركيهم، قصـــد منع النفاذ الى الموزعات التي تتضـــمن معلومات متعارضة مع النظام العام.[1]

وفي الأخير ينبغي الاشـــارة الى أن شـــركات تقديم خدمات الانترنت تحتاج لمعرفة حقوقها كحقوقها بالنســـبة لرخص الاســـتخدام والخطوط والترددات ونطاق الخدمات ومقابل تقديم الخدمة، كما تحتاج لمعرفة مسـؤوليتها، والتزاماتها تجاه المسـتخدمين، كمسـؤولية عدم الوصـول الى البريد الالكتروني أو عند قيام أحد مشـتركيها بإرسـال رسـالة تهديد أو مسـاس بسـمعة الغير او أي عمل غير قانوني عبر الشـبكة، وبالتالي فمعرفة دور القانون في حالة طلب السلطات المختصة تزويدها بهذه المعلومات أمر حتمي وضروري.[2]

[1]- عادل بوزيدة، مرجع سابق، ص 28.

[2]- فهد عبد الله العبيد العازمي، مرجع سابق، ص 439.

الفصل الثاني:

التعاون الدولي في مواجهة الجرائم المعلوماتية

الفصل الثاني: التعاون الدولي في مواجهة الجرائم المعلوماتية

لقد أدرك المجتمع الدولي اليوم خطورة الجرائم المعلوماتية، وأساليب ارتكابها ومختلف الصفات المميزة لها، خاصة في ظل امتداد آثارها الى دول متعددة، حيث أصبح من الضروري ايجاد توافق دولي محكم لمواجهة هذه الجرائم العابرة للحدود الوطنية مع وجوبية التنسيق بين مختلف الدول لفعالية اجراءات التحقيق على المستوى الدولي، ولعل هذا لا يتأتى الا من خلال تعزيز التعاون الدولي بوضع آليات دولية تتماشى وخصوصية هذه الجرائم.

وفي هذا السياق يعد التعاون الدولي على المستوى الأمني والفني ضرورة ملحة، الى جانب ذلك فالتعاون القضائي الدولي يعد من الآليات الفعالة لمواجهة الجرائم المعلوماتية، خصوصا وأن الظواهر الاجرامية لا تقف على حدود اقليمية لدولة واحدة بل تتعداها الى أبعد من ذلك، سواء من خلال تنظيمها أو من حيث أهدافها.

وبناء على ما سبق، فيم تتمثل مساعي التعاون الدولي لمواجهة هذه الجرائم؟ وفي ذلك خصصنا المبحث الأول للموضوع للإجابة على الاشكالية على ذلك.

ومن ناحية أخرى وفي إطار المساعدة القضائية في مجال الجرائم المعلوماتية أو تسليم المجرمين بين الدول، وباعتبار هذه الاجراءات حساسة وقد تكون محلا للجدل، خصصنا مبحث ثاني بعنوان: التعاون القضائي الدولي في مواجهة الجرائم المعلوماتية للتطرق لأهم النقاط المتعلقة بالموضوع.

المبحث الأول: مساعي التعاون الدولي في مواجهة الجرائم المعلوماتية

في عالم مزدحم بشـــبكات الاتصـــالات فدقيقة تنقل وتســـتقبل المعلومات من مناطق جغرافية متباعدة باســـتخدام تقنيات لا تكفل للمعلومات أمنا كاملا، يتاح في ظلها التلاعب عبر الحدود بالبيانات المنقولة أو المخزنة، مما قد يســـبب لبعض الدول أو الأفراد أضـــرارا فادحة، يغدو التعاون الدولي واسع المدى في مجال مكافحة الجرائم المعلوماتية.[1]

بغرض تحسـين وسـائل وسـبل التعاون الدولي سـعت الاتفاقيات الدولية الى مواجهة الجرائم المعلوماتية، كما سعت المنظمات الدولية الى ذلك من خلال عقدها لمؤتمرات ودورات تبرز من خلالها أهمية مواجهة هذه الجرائم.

المطلب الأول: المعالجة القانونية الدولية للتعاون الدولي في مواجهة الجرائم المعلوماتية

في إطار مواجهة الجرائم المعلوماتية وتحقيق وحدة أكبر بين الدول وتعزيز التعاون الدولي، خاصة في ظل الحاجة الملحة الى اتباع سياسة جنائية مشتركة حماية للمجتمع من الجرائم المعلوماتية، ودعما للتعاون الدولي، عالجت مجموعة من الاتفاقيات الدولية موضـــوع الجرائم المعلوماتية بما فيها الأحكام المتعلقة بالتعاون الدولي في ســـبيل مواجهة الجرائم المعلوماتية العابرة للحدود الوطنية، كما ساهمت الأمم المتحدة من خلال قراراتها بمعالجة هذا الموضوع.

[1]– محمد نصر محمد، مرجع سابق، ص 57.

الفرع الأول: الاتفاقيات الدولية بشأن التعاون الدولي في مواجهة الجرائم المعلوماتية

ان الاتفاقيات الدولية هي الأداة التي يمكن أن تنبع عنها الالتزامات بين الدول[1]، وقد تم اعتماد اتفاقية بودابست من طرف لجنة الوزراء بالمجلس الأوروبي، كما سنت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك في بهدف تعزيز التعاون بين الدول العربية وتدعيمه في مجال مواجهة الجرائم المعلوماتية.

أولا: الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية

تهدف هذه الاتفاقية الى تعزيز فعالية التحقيق في الجرائم المعلوماتية والتمكين من جمع الأدلة المناسبة لمواجهة هذه الجرائم، حيث رحبت بما يعزز سبل التعاون الدولي في مجال مواجهة هذه الجرائم بما في ذلك اجراء الذي اتخذته منظمة الامم المتحدة ومنظمة التعاون والتنمية الاقتصادية والاتحاد الأوروبي ومجموعة الثمانية.

وركزت في ذلك على مجموعة من التوصيات والقرارات منها:

- توصيات لجنة الوزراء رقم 10.85 بشأن التطبيق العملي للاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية بشأن اعتراض الاتصالات السلكية واللاسلكية،
- التوصية رقم 90 .4 بشأن حماية البيانات الشخصية في مجال خدمات الاتصالات (خاصة الخدمات الهاتفية)،

[1]– عادل عبد العال ابراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون، دقهلية، عدد 16، مجلد 1، 2014، ص 203.

- التوصية رقم 9.89 بشأن الجرائم ذات الصلة بالكمبيوتر والتي توفر مبادئ توجيهية للهيئات التشريعية الوطنية بشأن التعريف ببعض الجرائم الكمبيوتر.
- التوصية رقم 13.95 بشأن المشاكل التي يطرحها قانون الاجراءات الجنائية وعلاقته بتكنولوجيا المعلومات.
- كما راعت الاتفاقية القرار رقم 1 الذي تبناه وزراء العدل الأوروبيون في مؤتمرهم 21 الذي أوصى لجنة الوزراء بدعم الجهود التي تبذلها اللجنة الأوروبية المعنية بمشاكل الاجرام في مجال الجرائم المعلوماتية لتقريب أحكام القوانين الجنائية الوطنية من بعضها، وتمكين استخدام الوسائل الفعالة لإجراء التحقيق في هذه الجرائم.
- القرار رقم 3 المعتمد خلال المؤتمر الثاني لوزراء العدل الأوروبيين بلندن الذي اقر بالحاجة الى نظام سريع وفعال للتعاون الدولي في مواجهة الجرائم المعلوماتية.

أوجه التعاون الدولي بموجب الاتفاقية فيما يخص التحقيق في الجرائم المعلوماتية:

شددت الاتفاقية على الحاجة الى التعاون الدولي في الكشف عن الجرائم المعلوماتية والتحقيق فيها ومقاضاة مرتكبيها، كما اعترفت بالحاجة الى حماية المصالح المشروعة في استخدام وتطوير تقنية المعلومات، والأهم من ذلك أكدت على حقوق الانسان بما في ذلك الحق في حرية التعبير والخصوصية وأقرت بالحاجة الى حماية البيانات الشخصية.[1]

وفي سبيل اجراء التحقيقات والمتابعات بشأن الجرائم المعلوماتية وجمع الأدلة فيها أكدت الاتفاقية على وجوب تطبيق الصكوك الدولية الخاصة بالتعاون الدولي في المسائل الجنائية والترتيبات المتفق عليها بموجب التشريعات الموحدة أو وفقا لمبدأ المعاملة بالمثل والقوانين الوطنية.

[1] - Kerr I , Gilbert D, Information ethics in the electronic age, Tom Mendina and Johannes J.Britz, 2004, p 168.

كما تطرقت الى أهم المبادئ ذات الصلة بتسليم المجرمين في الجرائم المنصوص عليها في هذه الاتفاقية، والتي سبق تناولها في الباب الأول والمتمثلة في:

- الجرائم الماسة بخصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر: وتشمل جرائم النفاذ غير المشروع، جرائم الاعتراض والالتقاط غير المشروع، التدخل في البيانات، التدخل في الشبكات والأنظمة المعلوماتية، اساءة استخدام الأجهزة
- الجرائم ذات الصلة بالكمبيوتر: وتشمل التزوير بواسطة الحاسوب، الاحتيال بواسطة الحاسوب.
- الجرائم ذات الصلة بالمحتوى: وتشمل الدعارة المتعلقة بالأطفال
- الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة
- المحاولة أو المساعدة أو التحريض على ارتكاب هذه الجرائم.

كما أنه ولأغراض التحقيقات و المتابعات المتعلقة بالجرائم المعلوماتية و جمع الأدلة فيها، فانه على كل دولة طرف أن توفر المساعدة المتبادلة و تتخذ ما يلزم من تدابير تشريعية أو ما يلزم من التدابير المؤقتة (التعجيل في حفظ البيانات، تعجيل الكشف عن البيانات)، وتتخذ ما يلزم في حالة المساعدة المتبادلة ذات الصلة بالتحقيق(في حالة النفاذ الى بيانات الكمبيوتر المخزنة أو النفاذ العابر للحدود الى بيانات متاحة للجمهور أو عند جمع بيانات الحركة في الوقت الحقيقي، او في حالة المساعدة المتبادلة ذات الصلة بالاعتراض على بيانات المحتوى).

كما يتعين ضمان المساعدة الفورية على مدار الساعة و7 ايام في الاسبوع، اضافة الى الاجراءات المتعلقة بطلبات المساعدة القضائية في حالة عدم وجود اتفاقية دولية واجبة التطبيق، والمنصوص عليها في 27 من الاتفاقية.

ولابد أن ننوه أن الاتفاقية نظمت قواعد الاختصاص سواء ارتكبت الجريمة داخل اقليم اي دولة طرف أو على متن سفينة ترفع علم الدولة الطرف أو على متن طائرة مسجلة بموجب قوانين تلك الدولة الطرف أو من قبل أحد مواطنيها إذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي في مكان ارتكابها أو في حالة ارتكاب الجريمة خارج مجال ولايتها القضائية.[1]

ثانيا: البروتوكول الاضافي بشأن تجريم الافعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر

قد يشكل سوء استخدام الإنترنت وسيلة لدعم العنصرية و كراهية الأجانب، مما يستوجب اقرار مبدأ التعاون الدولي للتحقيق مع مرتكبي هذه الجرائم و ملاحقتهم قضائيا، و في هذا الاطار تم صياغة بروتوكول اضافي بشأن تجريم الافعال المرتبطة بالتمييز العنصري و كراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر كمكمل لاتفاقية بودابست، و ذلك بهدف مواءمة القانون الجنائي الموضوعي لمواجهة أشكال التمييز العنصري و كراهية الأجانب عبر الانترنت، و تحسين التعاون الدولي في هذا المجال، حيث يساعد هذا النوع من الموائمة في التخفيف من عبء المكافحة على الصعيد الوطني و الدولي، و تعزيز تبادل الخبرات المشتركة من الناحية العملية و بهذا يصبح التعاون الدولي خاصة تسليم المجرمين و المساعدة القانونية المتبادلة ميسرا.[2]

ويحدد هذا البروتوكول النطاق الذي يعتبر فيه نشر أي تعبير أو فكر ينطوي على التمييز العنصري أو العدائي للأجانب انتهاكا لحقوق الغير، وأشارت المادة الثامنة منه على

[1]– المادة 22 من الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، بودابست 2001، سالفة الذكر، ص 12.

[2]– التقرير التفسيري للبروتوكول الاضافي لاتفاقية الجريمة الالكترونية بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، المنعقدة في ستراسبورغ في28 يناير 2003، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 189، ص 02.

العلاقة بين الاتفاقية وهذا البروتوكول على أن تطبق أحكام الاتفاقية في ماعدا بعض الأحوال التي تقتضي اجراء بعض التعديلات.

ثالثا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تهدف الاتفاقية الى تعزيز التعاون وتدعيمه بين الدول العربية[1] في مجال مكافحة الجرائم المعلوماتية ومواجهة خطورتها وذلك بهدف المحافظة على مصـــالح الدول العربية وأمنها وســلامة الفرد والمجتمع، وذلك أخذا بالمبادئ الدينية والأخلاقية والتراث الانســاني في هذه الدول.

أوجه التعاون الدولي بموجب الاتفاقية فيما يخص التحقيق في الجرائم المعلوماتية:

تطرقت الاتفاقية الى التعاون القانوني والقضائي من خلال سن قواعد قانونية تتماشى مع طبيعة الجرائم المعلوماتية وذلك من خلال:

- تمديد الاختصــاص في الجرائم المنصــوص عليها في هذه الاتفاقية: في حالة ارتكاب الجريمة (سواء كلها أو جزء منها أو تحققت) في اقليم دولة طرف أو على متن سفينة علم الدولة الطرف أو على متن طائرة مســـجلة تحت قوانين الدولة الطرف أو من طرف أحد مواطني الدولة الطرف إذا كانت الجريمة معاقبا عليها حســـب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصـــاص القضـــائي لأية

[1]– وقد صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، بموجب المرسوم الرئاسي رقم 14–252، المؤرخ في 08 سبتمبر 2014. أنظر الجريدة الرسمية عدد 57، الصادرة بتاريخ 28 سبتمبر 2014.

دولة، كما تلتزم الدولة لمد اختصـــاصـــها إذا كانت الجريمة تمس بأحد مصـــالحها العليا.[1]

- امكانية تبادل المجرمين بين الدول الاطراف مع احترام الشـــروط المقررة بنص المادة 31 من الاتفاقية.
- تبادل المسـاعدة لأقصـى حد ممكن لفاعلية التحقيقات أو الاجراءات المتعلقة بالجرائم المعلوماتية أو جمع الأدلة الالكترونية.
- امكانية تقديم معلومات متعلقة بالتحقيق بين الدول الاطراف دون طلب مسبق إذا رأت أنها تســـاعد الدولة الطرف في القيام بتحقيقاتها أو تؤدي الى طلب للتعاون، غير أنه يمكن للدولة المبادرة بالمســـاعدة أن تطلب من الدولة الاخرى الحفاظ على ســـرية المعلومات المقدمة.
- اتباع مجموعة من الاجراءات المتعلقة بطلب التعاون والمساعدة المتبادلة مع ضمان الحفاظ على سرية المعلومات.
- اتخاذ ما يلزم من التدابير المؤقتة المتعلقة بالحفظ العاجل للمعلومات المخزنة أو الكشف العاجل للمعلومات المحفوظة.
- اتخاذ اي اجراء ذو صـــلة بالتحقيقات ســـواء في إطار التعاون والمســـاعدة الثنائية للوصـــول الى معلومات تقنية المعلومات المخزنة أو للوصـــول الى تقنية المعلومات عبر الحدود دون تفويض من دولة طرف اخرى، أو في إطار التعاون والمســـاعدة الثنائية بخصـــوص الجمع الفوري للمعلومات، ولتوفير معلومات متعلقة بمحتوى الاتصالات.

[1]– المادة 30 من المرسوم الرئاسي رقم 14–252، سالف الذكر، ص 9.

الفرع الثاني: دور الأمم المتحدة في مجال التعاون الدولي لمواجهة الجرائم المعلوماتية

تلعب منظمة الأمم المتحدة دورا أساسيا في حفظ السلام والأمن الدوليين، وتسعى الى رسم سياسات العدالة الجنائية وتوطيد التعاون الدولي في مواجهة الجرائم العابرة للحدود الوطنية ومن بينها الجرائم المعلوماتية.

أولا: تدعيم التعاون الدولي بعقد منظمة الأمم المتحدة لمؤتمرات دورية

تعقد منظمة الأمم المتحدة مؤتمرات دورية كل خمسة سنوات: من بينها:

-**المؤتمر السابع لمنع الجريمة و معاملة المجرمين** (المنعقد في ميلانو-ايطاليا عام 1985) و الذي أكد على وجوب تطبيق التطورات التكنولوجية الحديثة في كل مكان لصالح الجمهور، و بالتالي منع الجريمة على نحو فعال، كما أكد على أن التكنولوجيا قد تولد أشكالا جديدة من الجريمة مما ينبغي اتخاذ تدابير ملائمة للتصدي لها، و أشار بدوره الى مسألة الخصوصية التي من الممكن الاعتداء عليها عن طريق الاطلاع على البيانات الشخصية المخزنة داخل نظم الحاسب الآلي، مما يشكل انتهاكا لحقوق الانسان، و اعتداء على حرمة الحياة الخاصة و بالتالي لابد من اعتماد ضمانات ملائمة لضمان السرية، و انبثق عن هذا المؤتمر مجموعة من القواعد التوجيهية تؤكد على تشجيع التشريعات الحديثة التي تجرم و تتناول الجرائم المعلوماتية باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال و الاحتيال المنظم.[1]

-**المؤتمر الثامن لمنع الجريمة و معاملة المجرمين** (المنعقد بهافانا-كوبا عام 1990) والذي جاء بعدة مبادئ أهمها: تحديث القوانين الجنائية الوطنية بما في ذلك التدابير

[1]- نجاة بن مكي، مرجع سابق، ص 115.

المؤسساتية و تحسين أمن الحاسب الآلي و التدابير الفنية، و اعتماد اجراءات تدريب كافية للموظفين و الوكالات المسؤولة عن منع الجرائم الاقتصادية و الجرائم المعلوماتية، و زيادة التعاون الدولي لمواجهة هذه الجرائم و ذلك من خلال مضاعفة الأنشطة التي تبذلها الدول الأعضاء على الصعيد الدولي بما في ذلك تسليم المجرمين و المساعدة في المسائل الخاصة بالجرائم المعلوماتية.

- **المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين** (المنعقد في القاهرة عام 1995) ومن أهم توصياته: حماية حياة الانسان الخاصة وملكيته الفكرية[1] في مواجهة مخاطر التكنولوجيا وتعزيز التعاون الدولي والمساعدة الفنية العملية لتعزيز سيادة القانون تحت شعار السعي نحو الأمن والعدالة للجميع، حيث منح المؤتمر أولوية كبيرة للتعاون الفني والخدمات الاستشارية التي تقدمها الأمم المتحدة لمساعدة الدول الأعضاء في تحقيق أهداف منع الجريمة داخل الدول وتحسين مواجهة الجريمة والتصدي لها.

وواصلت المجهودات من خلال عقدها لعدة مؤتمرات اخرى من بينها:

- **المؤتمر الحادي عشر** (المنعقد في بانكوك–تايلند عام 2005) والذي يهدف الى تدعيم جهود التعاون والتنسيق الدولي من أجل منع الجريمة ومن بينها الجرائم المعلوماتية واتخاد التدابير اللازمة لمواجهتها.

[1]– عمدت التشريعات الى تقرير حماية دولية لمواجهة الجرائم المعلوماتية العابرة للحدود الوطنية، ومن بين الاطر القانونية المعتمدة لمواجهة خطورتها، (حماية الملكية الفكرية) و ذلك عن طريق الحماية المقررة لبرامج الحاسب الآلي و قواعد البيانات، و مختلف اشكال المصنفات الرقمية، و للتصدي بوجه أكبر للجرائم المعلوماتية، جاء التأكيد على حقوق الملكية الفكرية، من خلال ابرام عدة اتفاقيات دولية ، أولها اتفاقية برن لحماية المصنفات الأدبية و الفنية، واتفاقية تريبس، كما ساهمت المنظمات الدولية كمنظمة الويبو و اليونسكو في ارساء قواعد قانونية دولية تحكم المعاملات في مجال الملكية الفكرية في البيئة الرقمية.

- **المؤتمر الثاني عشر** (المنعقد في السلفادور–البرازيل عام 2010) والذي أقر اعلان السلفادور الذي فتح المناقشة بشأن الاستجابة الوطنية والدولية الجديدة لجرائم الانترنت ومن أهم موضـــوعاته منع الجريمة ومن بينها جرائم الانترنت والتعاون الدولي في مكافحة الجريمة.
- **المؤتمر الثالث عشر** (المنعقد بالدوحة–قطر عام 2015) والذي يهدف الى مكافحة الجريمة المنظمة عبر الوطنية من خلال تحســين التعاون الدولي و مختلف أشــكال الجريمة المســتجدة و دور عامة الناس في منع الجريمة و العدالة الجنائية، وأكد هذا المؤتمر على وجوب تعزيز التدابير المتخذة في مجال منع الجريمة و العدالة الجنائية من أجل التصدي للأشكال المتطورة من الجريمة، و أشار بعض الدول من خلال هذا المؤتمر الى ضــرورة اعتماد صــك دولي جديد ملزم قانونا بشــأن مكافحة الجرائم المعلوماتية، و ســد الثغرات في التشــريعات و التجريم بشــكل فعال، كما أن تنظيم الفضاء السيبراني ضروري للمنع من انشاء أنواع جديدة من الانتهاكات التي يصعب فهمها، كالتشهير و سرقة الهوية و الجرائم الجنسية.[1]

وكان آخر مؤتمر لها: **المؤتمر الرابع عشــر** (المنعقد بكيوتو–اليابان عام 2020) والذي كان بين مواضيعه التعاون الدولي وتقديم المساعدة التقنية من أجل منع الجرائم بجميع أشكالها والتصدي لها،

[1] –BOOS R, La lutte contre la cybercriminalité au regard de l'action des états, thèse de doctorat, spécialité droit privé et science criminelles, faculté de droit, université de Lorraine, France, 2016, p 368.

ومن أبرز حلقات هذا المؤتمر الاتجاهات الراهنة للجريمة والتطورات الأخيرة والحلول المستجدة لاسيما التكنولوجيا الحديثة بوصفها وسائل لارتكاب الجريمة وادوات لمكافحتها[1]، ومن بين توصياته:

-تعزيز الدول الاعضاء معايير وقواعد الأمم المتحدة في مجال منع الجريمة والعدالة الجنائية ووضع آليات مناسبة لوضع وتنفيذ استراتيجيات وطنية ومحلية فعالة لمنع الجريمة والتشجيع على الاستخدام المسؤول للتكنولوجيا في منع الاجرام مع ضمان أن تكون السياسات والأطر التنظيمية ذات الصلة تتوافق مع المعايير الدولية لحقوق الانسان.[2]

ثانيا: دور المنظمة العالمية للملكية الفكرية (WIPO) في مواجهة الجرائم المعلوماتية

تعتبر المنظمة العالمية للملكية الفكرية من المنظمات الدولية الحكومية، وهي من بين الوكالات المتخصصة التابعة لهيئة الأمم المتحدة (مقرها في جنيف)، تهتم بحماية مختلف عناصر الملكية الفكرية تحت مظلة اتفاقية باريس الخاصة بحماية الملكية الصناعية واتفاقية برن الخاصة بحماية المصنفات الأدبية والفنية واتحادهما.

[1]- **مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية 1955-2020**، منشورة على موقع الأمم المتحدة، الدخول يوم 14-01-2021، على الساعة 00.23 الى 00.40
https://www.un.org/ar/events/crimecongress2015/pdf/sixty.years.booklet.pdf

[2]- **مؤتمر الامم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية**، كيوتو اليابان، افريل 2020، ورقة عمل اعدتها الامانة العامة، البند 3 من جدول الاعمال المؤقت الاستراتيجيات الشاملة لمنع الجريمة من اجل تحقيق التنمية الاجتماعية والاقتصادية. منشورة على موقع الأمم المتحدة، الدخول يوم 14-01-2021، على الساعة 00:55، 01.15، https://undocs.org/pdf?symbol=ar/A/CONF.234/4

وقد تم انشاء هذه المنظمة بإستكهولم في 14 يوليو 1967، وصادقت عليها الجزائر بموجب الأمر 75-2 مكرر في 09 جانفي 1975.[1]

وتهدف المنظمة الى دعم حماية الملكية الفكرية في جميع أنحاء العالم عن طريق التعاون بين الدول وبين المنظمات الدولية الأخرى عند الضرورة، مع ضمان التعاون الاداري بين اتحادات الملكية الفكرية المنشـــأة بموجب المعاهدات التي تديرها، وتضـــطلع بعدد من الأنشطة[2]:

- **أنشـطة تنظيمية:** تهدف الى وضـع القواعد والمعايير اللازمة لحماية الملكية الفكرية وانفاذها بإبرام معاهدات دولية.
- **أنشطة البرامج:** تقدم المساعدة القانونية والفنية الى الدول في مجال الملكية الفكرية.
- **أنشـطة التصـنيف والتوحيد الدوليين:** تشـمل التعاون بين مكاتب الملكية الصـناعية بشأن وثائق البراءات والعلامات التجارية والرسوم والنماذج الصناعية.
- **أنشـطة التسـجيل والابداع:** تضـم خدمات الطلبات الدولية المودعة للحصـول على براءة اختراع وتسجيل العلامات والرسوم والنماذج الصناعية الدولية.

ومن أجل مساعدة الدول على استكمال تشريعاتها فيما يتعلق بحماية برامج الحاسب الآلي والقضاء على مشاكل نقل المعلومات عن بعد، شكلت المنظمة عددا من الخبراء تهدف الى حماية برامج الحاسب الآلي، واستمرت في دراسة الأسلوب المناسب لحماية هذه البرامج

[1]- الأمر رقم 75-2 مكرر المؤرخ في 9 جانفي 1975، المتضمن المصادقة على اتفاقية انشاء المنظمة العالمية للملكية الفكرية الموقعة باستكهولم في 14 يوليو 1967، ج ر عدد 13، الصادرة بتاريخ 14 فيفري 1975، ص 198.

[2]- ملخص عن اتفاقية إنشاء المنظمة العالمية للملكية الفكرية (اتفاقية الويبو) (لسنة 1967)، منشور على موقع المنظمة العالمية للملكية الفكرية WIPOعلى الرابط التالي:

https://www.wipo.int/treaties/ar/convention/summary_wipo_convention.html، الدخول يوم: 15-01-2021، الساعة 14.00 الى 14.15.

ومسائلها الفنية وعبر عدة اجتماعات ساد اتجاه لدى أغلب الدول الصناعية ودول العالم الثالث الى خضوع برامج الحاسب الآلي لقوانين حماية حق المؤلف، وأضافت غالبية التشريعات برامج الحاسب الآلي الى المصنفات الأدبية المحمية.[1]

وفي ذلك أدرج المشرع الجزائري برامج الحاسب الآلي ضمن المادة 04 من الأمر 03-05[2]، واعتبرها من المصنفات الأدبية أو الفنية المحمية وخصصها في الفقرة الأولى على أنها مصنفات أدبية مكتوبة، كما استبعد برامج الحاسب الآلي من نطاق الاختراعات بموجب المادة 07 من الأمر 03-07[3] المتعلق ببراءة الاختراع، بنصه: " (لا تعد من قبيل الاختراعات في مفهوم هذا الأمر: ....6) برامج الحاسوب.).

ولعل هذا الاستبعاد جاء لإسباغ الحماية الكاملة لقانون حق المؤلف على البرمجيات، والاعتداء عليها يعتبر اعتداء على الحقوق الذهنية والملكية الفكرية، لكونهما من الحقوق التي ترد على أشياء معنوية غير محسوسة من ابداع الذهن ونتاج الفكر[4]

وجدير بالذكر أن المنظمة العالمية للملكية الفكرية تعمل بالتنسيق مع منظمات أخرى أهمها المنظمة العالمية للتجارة العالمية والتي دخلت حيز التنفيذ في 1995، ويكمن الهدف المشترك بينهما في حماية حقوق الملكية الفكرية بكافة جوانبها، ومساعدة بلدان العالم على التقدم وتحقيق التنمية، من خلال التوعية والتدريب وتقديم المساعدات الفنية لمختلف الدول.

---

[1]- نجاة بن مكي، مرجع سابق، ص 108.

[2]- الأمر 03-05، يتعلق بحقوق المؤلف والحقوق المجاورة، المؤرخ في 19 يوليو 2003، ج ر عدد 44، الصادرة بتاريخ 23 يوليو 2003، ص4.

[3]- الأمر 03-07، يتعلق ببراءات الاختراع، المؤرخ في 19 يوليو 2003، ج ر، عدد 44، الصادرة بتاريخ 23 يوليو 2003، ص 29.

[4]- نجاة بن مكي، مرجع سابق، ص 81.

ونتيجة المستجدات الحاصلة في العالم، وبغرض توسيع نطاق الحق في الاتصالات، صدرت معاهدتي الانترنت، حيث تمت صياغة معاهدة حقوق الطبع والنشر التابعة للمنظمة الدولية لحقوق الملكية الفكرية، والتي سميت بمعاهدة الانترنت الأولى، ومعاهدة عمليات الاداء والتي سميت بمعاهدة الانترنت الثانية[1]

ثالثا: دور الاتحاد الدولي للاتصالات (ITU) في مواجهة الجرائم المعلوماتية

يعتبر الاتحاد الدولي للاتصالات من الوكالات المتخصصة التابعة للأمم المتحدة، يقع مقره في جنيف سويسرا، بجانب مقر الأمم المتحدة، وتهدف أنشطته الى تعزيز دوره في بناء الثقة والأمن في استعمال تكنولوجيا الحديثة في مجال المعلومات والاتصالات.

ولعل دور الاتحاد في مواجهة الجرائم المعلوماتية يبرز من خلال:

- اتخاذ مجموعة من التدابير القانونية تهدف الى المساعدة على تحقيق تناسق في الأطر القانونية للدول.
- تعاون الاتحاد مع مجموعة من الشركاء التابعين لمكتب الأمم المتحدة المكلف بالمخدرات والجريمة، أو غيره من الجهات التي لها خبرة في هذا المجال، وذلك بغرض توفير الأمن المعلوماتي ومكافحة الرسائل الاقتحامية.
- اتخاذ مجموعة من التدابير التقنية والاجرائية لحماية المعلومات والاتصالات.
- المشاركة في المنتديات والمؤتمرات الدولية بشأن مواجهة الجرائم المعلوماتية وحماية الأطفال عبر الانترنت وابراز كيفيات استخدام التكنولوجيا الحديثة بطريقة آمنة ومسؤولة.

[1]– كوثر مازوني، قانون الملكية الفكرية في مواجهة التكنولوجيات الحديثة التجربة الجزائرية، دار هومة، الجزائر، 2016، ص 30.

- –تعاون الاتحاد مع المنظمات والمبادرات الاقليمية والدولية، ومنها:

مبادرة الكومنولث بشـــأن الجريمة الســـيبرانية، الوكالة الأوروبية لأمن الشـــبكات والمعلومات (ENISA)، المنظمة الدولية للشرطة الجنائية (INTERPOL)، الجماعة الاقتصادية لدول إفريقيا الغربية (ECOWAS)، والبنك الدولي، منتدى أفرقة التصـــدي للحوادث قبيل وأمن المعلومـات (FIRST)، الرابطـات الإقليميـة لأفرقـة التصـــــدي للحوادث الأمنيـة الحاســـوبية (CSIRT)/أفرقة الاســـتجابة لحالات الطوارئ الحاســـوبية (CERT) مثل فريق الاستجابة لحالات الطوارئ الحاسوبية في منطقة آسيا والمحيط الهادئ (AP CERT) وفريق الاستجابة لحالات الطوارئ الحاسوبية في منطقة إفريقيا (AFRICA CERT) وفريق الاستجابة لحالات الطوارئ الحاسوبية لمنظمة التعاون الإسلامي (OIC CERT).[1]

[1]– تقرير الأمين العام، أنشطة الاتحاد الدولي للاتصالات بشأن تعزيز دوره في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، مجلس الاتحاد الدولي للاتصالات، الوثيقة C18/18–A، جنيف، 2018.

المطلب الثاني: أجهزة التعاون الدولي في مجال الجرائم المعلوماتية

ان التعاون الأمني الدولي في مواجهة الجرائم المعلوماتية مبني على أســـاس توفير المعلومات والبيانات اللازمة حول الجريمة ومرتكبيها، وليتم ذلك على نحو فعال لابد من انشاء مركز دولي للمعلومات والبيانات الخاصة بهذه الجرائم بكافة صورها وأنماطها بما في ذلك أسماء المتورطين والاجراءات المتخذة والتحقيقات والأحكام الصادرة بشأنهم، كما يفترض اعداد مدونة دولية توحد معايير وأركان الجريمة مع ضـــمان أن يشـــكل نطاق التجريم كافة جوانبها ومراحلها.[1]

ولنجاعة التعاون الدولي في مواجهة الجرائم المعلوماتية لابد من تنســـيق دولي على المستوى الأمني وتحقيق تكامل بين الأجهزة الأمنية والتي سنوردها في هذا المطلب.

الفرع الأول: الانتربول

في إطار مواجهة الجرائم العابرة للحدود الوطنية يبحث العديد من القضـــاة أو ضـــباط الشـــرطة القضـــائية أو الدرك عن أدوات وخدمات عملية تســـمح لهم بإجراء تحقيقاتهم خارج الأراضي الوطنية.[2]

وتعتبر المنظمة الدولية للشـــرطة الجنائية (الانتربول INTERPOL)، من الأجهزة التابعة لمنظمة الأمم المتحدة وهي منظمة شرطة دولية مقرها في ليون فرنسـا، تم انشـاؤها في 07-09-1923، تباشر مهامها بأربع لغات رسمية (الانجليزية، الفرنسية، الاسبانية، العربية) [3]

---

[1]- عادل عبد العال ابراهيم خراشي، مرجع سابق، 193.

[2] -Olivier B, Les investigations judiciaires internationales, Berger-levrault, 1er édition, 2014, p 237.

[3]- الانتربول منظمة مستقلة تهدف لتأكيد التعاون الدولي بين سلطات الشرطة للدول الأعضاء، ومكافحة جرائم القانون العام، والتعاون في إطار الاعلان العالمي لحقوق الانسان بغض النظر عن الابعاد السياسية والدينية والعنصرية، والعمل على منع الجرائم الدولية والحد منها. لها عدة تسميات منها: البوليس الدولي أو الشرطة الدولية، المنظمة الجنائية للشرطة الدولية CPOI، انتسبت الجزائر له في 1963.

أولا: دور الانتربول في مواجهة الجرائم المعلوماتية

يبرز دور الانتربول في مواجهة الجرائم المعلوماتية من خلال ما يلي:

- تأكيد وتشـــجيع التعاون بين أجهزة الشـــرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة من خلال جمع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية للشـــرطة الجنائية الدولية على مســـتوى اقليم الدول الأعضاء، وتتبادلها فيما بينها.[1]
- دعم جهود الشـــرطة في مواجهة الجرائم العابرة للحدود الوطنية، وتقديم الخدمات في مجال الأدلة الجنائية.[2]
- التعاون في ملاحقة المجرم وتسليمه الى الدولة التي طلبته فهي مختصة بالجرائم ذات الطابع الدولي خاصـــة جرائم الاســـتغلال الجنســـي للأطفال عبر الانترنت والاحتيال المعلوماتي، اضـــافة الى دعم اجراءات البحث والتحقيق في الجرائم المعلوماتية من خلال –جمع وتخزين المعلومات المتعلقة بالجرائم– وتوفيرها للدول الأعضـــاء عبر شبكة الاتصالات الشرطية الرابطة بين الدول الأعضاء (I24 /7)[3] والتي تم تطويرها ودعمها بمنظومة (I-Link) التي تعتبر مركز رئيســـي لتبادل المعلومات الجنائية والتواصل بين الدول الأعضاء، لها عدة وظائف تضمن فعالية نقل وتبادل المعلومات الشرطية: حيث تسير قاعدة البيانات الجنائية الدولية، وتقدم الدعم لمصالح الشرطة على المستوى الدولي والداخلي، مع تكوين رجال الشرطة لتحسين مهاراتهم في مجال

---

[1]– محمد أحمد سليمان، مرجع سابق، ص 53.

[2]–عادل عبد العال ابراهيم خراشي، مرجع سابق، ص 197.

[3]– منذ 2003 نفذ الانتربول شبكة اتصالات جديدة تسمى I24 /7 تربط هذه الشبكة بين الدول الاعضاء مما يسمح لهم بالتواصل في الوقت الحقيقي وبشكل أساسي بين المكاتب المركزية الوطنية والهيئات الفنية الدائمة بطريقة آمنة، وللتواصل بين الهيئات الفنية التابعة للانتربول مباشرة حيث تضمن هذه الشبكة الوصول الكامل أو الجزئي الى قواعد بيانات الانتربول والمعلومات التي تنشرها هذه المنظمة.

Olivier B, op.cit, p 240.

الاتصـالات، كما تقوم بعمليات نوعية تسـتهدف الاجرام المعلوماتي، كعملية Anmask.[1]

ثانيا: استراتيجيات عمل الانتربول

يقوم الانتربول بعملية ملاحقة مجرمي المعلوماتية بصفة عامة وشبكة الانترنت بصفة خاصـة عن طريق تعقب الأدلة الالكترونية وضـبطها، والقيام بعمليات التفتيش العابر للحدود لمكونات الحاسـب الآلي المنطقية والأنظمة المعلوماتية شـبكات الاتصـال، وذلك بغرض البحث عما قد تحتويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية، وكلها أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، وهي من شأنها تطوير واكتساب مهارات وخبرات القائمين على مواجهة هذه الجرائم والحد من انتشارها[2]

وقد وضـع الانتربول بالتعاون مع مجموعة الدول الثمانية الكبرى G8 اسـتراتيجيات لمواجهة الجرائم المعلوماتية من خلال: انشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة و7أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف، اضافة الى استخدام وسائل حديثة لمواجهة هذه الجرائم كاستخدام قاعدة البيانات المركزية للصور الاباحية المحولة من قبل الدول الأطراف والتي تسـتخدم برامج معينة للتحليل ومقارنة أوتوماتيكية للصـور، هذا ناهيك عن تزويد شـرطة الدول الأطراف بإرشـادات حول الجرائم المعلوماتية و كيفيات التدريب على مكافحتها و التحقيق فيها.[3] وبهذا يتوالى عمل الانتربول بالتعاون بينه وبين الدول الأطراف.

[1]– حسين ربيعي، مرجع سابق، ص 149 ص151.

[2]– المركز العربي للبحوث القانونية والقضائية، ضرورة التعاون الاقليمي والدولي في مكافحة جرائم المعلوماتية، ورقة عمل مقدمة الى الاجتماع السادس للمختصين بتقنية المعلوماتية في النيابات العامة في الدول العربية، بيروت، 2018، ص 04.

[3]– عادل عبد العال ابراهيم خراشي، مرجع سابق، ص 198.

وعلى غرار هذه المنظمة **أنشأ المجلس الأوروبي في لكسمبورج عام 1991** شرطة أوروبية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة لملاحقة الجناة في الجرائم العابرة للحدود ومنها: الجرائم المعلوماتية.

أما على المستوى العربي: فنجد مجلس وزراء العرب أنشأ المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشـــرطة في الدول الأعضـــاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القانون والأنظمة المعمول بها في كل دولة، اضافة الى تقديم العون في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.[1]

[1]– نجاة بن مكي، مرجع سابق، ص 150.

الفرع الثاني: الأجهزة الأمنية الدولية الأخرى

بغرض نجاعة التعاون الدولي على المســـتوى الأمني اعتمدت عدة وكالات لمواجهة الجرائم المعلوماتية ومن بينها اليورو بول واليورو جســـت على مســـتوى الاتحاد الأوروبي، والافريبول على المستوى الافريقي.

أولا: اليورو بول

يعد **اليورو بول** من أكبر الهيئات الاســتشــارية لمكافحة الجرائم المعلوماتية، يقع مقره في لاهاي هولندا، و قد تم اختياره من قبل الاتحاد الدولي للأمن المعلوماتي لإنجاز مختلف الدراسات الخاصة بالجرائم المعلوماتية الى غاية سنة 2020، بهدف تحليل دوافعها و وضع تصـــور مســـتقبلي لتطورها، وهو ما يفســـر الثقة الموضـــوعة فيه من قبل اللجنة الأوروبية باعتباره مركز اعلام حول هذه الجرائم حيث يختص بالبحث والتحقيق فيها، –خاصـــــة ما يتعلق باستغلال الأطفال في المواد الاباحية أو الارهاب الالكتروني–، ويكمن دوره أساسا في العمل على تسهيل الاجراءات أمام رجال الشرطة، و مدهم بمختلف النشرات الأمنية والتقارير حول هوية المتهمين و الأدلة المحصلة خارج حدود اختصاصهم.[1]

ويهدف اليورو بول الى تحقيق تنمية اقتصـــــادية وتوازن اجتماعي وتطوير البرامج الرقمية والوصول الى الثقافة وأمن المواطنين[2]

ومن صلاحيات اليورو بول ما يلي:

- مكافحة جرائم الكمبيوتر أو أشـــكال الجريمة التي يســـهل ارتكابها بواســـطة التقنيات الرقمية، ومع ذلك لابد أن تشمل هذه الجرائم هيكلا أو منظمة اجرامية وعضوين على الاكثر.

[1]– حسين ربيعي، مرجع سابق، ص 154.

[2] -Freyssinet E, La cybercriminalité en mouvement, Lavoisier, 2012, France, p 184.

- توفير الخبرة والمساعدة الفنية للتحقيقات والعمليات داخل الاتحاد الأوروبي EU
- نشر نظام معلومات محوسب داخل الدول الاعضاء لتمكين ادخال البيانات والوصول اليها وتحليلها، ويمكنه تخزين واستخدام البيانات اللازمة لأداء وظائفه.

وقد تم الاعلان عن منصة مشتركة لتتبع الجرائم المعلوماتية في 24 اكتوبر 2008 في لوكسمبورغ: تضمن التعاون الشرطي بين مختلف اعضاء الاتحاد، وتبسيط اجراءات الشرطة في القضايا التي تشمل عدة دول، ولعل من اهم المهام المسندة لها مكافحة استغلال الاطفال في المواد الاباحية أو الارهاب أو الجريمة المنظمة. وقد تم تمويله من اليورو بول بميزانية 300.300 اورو.[1]

ثانيا-اليورو جست:

اليورو جست هو هيئة تابعة للاتحاد الأوروبي مسؤولة عن تحسين كفاءة السلطات المختصة في الدول الاعضاء في مكافحة الجريمة المنظمة العابرة للحدود ومنها: الجريمة المعلوماتية عبر الوطنية، مقره في لاهاي بهولندا.

ويكمن دوره في مواجهة الجرائم المعلوماتية من خلال دعم وتعزيز التنسيق والتعاون بشأن الجرائم الخطيرة التي تؤثر على دولتين فأكثر، ومن بين صلاحياته:

- تحفيز وتحسين تنسيق التحقيقات والملاحقات القضائية بين السلطات المختصة في الدول الأعضاء.[2]
- دعم الدول الاعضاء لزيادة كفاءة التحقيقات والملاحقات القضائية.
- تنسيق التحقيقات وتنفيذ طلبات التسليم من قبل السلطات الوطنية من اجل تعزيز فعالية المساعدة القانونية الدولية.

[1] -Quéméner M, Joel Ferry , Op. cit, p 238.

[2] -Olivier B, op. cit, p 237.

- يشارك في عمليات مكافحة استغلال الاطفال في المواد الاباحية
- يعمل اليورو جست بالتعاون مع المكتب الأوروبي لمكافحة الاحتيال
- يجري مناقشة خطة عمل لمكافحة الجرائم المعلوماتية داخل فضاء الاتحاد.[1]
- لـه دور في تطوير آليـات مكـافحـة الجرائم المعلومـاتيـة من خلال تبـادل المعلومـات بصـــفة دوريـة مع محاكم الاتحاد الأوروبي، كما يمثل دعامة في فعالية التحقيق في الجرائم المعلوماتية، ويمهد لليورو بول عمله في مجال التحقيق.[2]

ثالثا: الافريبول

بـدأت فكرة انشـــائـه تتجســـد ابتداء من مؤتمر الانتربول الاقليمي الافريقي الثـاني والعشـرين، سـنة 2013 بمدينة وهران. ويكمن دوره في المسـاعدة على تعزيز القدرة التحليلية للشرطة الافريقية لتقييم التهديدات الاجرامية وتطوير الاستجابة الملائمة، وتعزيز التنسيق بين قوات الشرطة المنتشرة في عمليات دعم السلام، اضـافة الى مهامه في تطوير قدرة السياسـة الشـــرطية الافريقية لمســـايرة الجرائم المســـتحدثة، ومن بينها مواجهة الجرائم المعلوماتية من خلال تبادل الخبرات وتكثيف الدورات التدريبية، والمســـاعدة التقنية المتبادلة في مجال تبادل المعلومات واستخدام التكنولوجيا الحديثة لاستخراج الأدلة الالكترونية.[3]

[1] -Quéméner M, Ferry J,op.cit , p 238 p 239.

[2]– حسين ربيعي، مرجع سابق، ص 155.

[3]– يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها) –دراسة مقارنة) –، مرجع سابق، ص 284.

المبحث الثاني: التعاون القضائي الدولي في مواجهة الجرائم المعلوماتية

نتيجة تفاقم الاجرام العابر للحدود أصبح من الضروري تكثيف الجهود الدولية للحد من الكم الهائل من الجرائم الخطيرة التي عبرت القارات، حيث يعد التعاون القضائي الدولي من الآليات الفعالة لمواجهة الجرائم المعلوماتية، خصوصا وأن الظواهر الاجرامية لا تقف على حدود اقليمية لدولة واحدة بل تتعداها الى أبعد من ذلك، سواء من حيث تنظيمها أو أهدافها.

اضافة الى الاتفاقية سالفة الذكر و تتويجا للتعاون القضائي بين جميع الدول العربية حررت اتفاقية الرياض العربية للتعاون القضائي حيث جاء بمقدمة هذه الاتفاقية، اقتناعا منها بأن التعاون القضائي بين الدول العربية ينبغي أن يكون تعاونا شاملا لكل المجالات القضائية على نحو يستطيع أن يسهم بصورة ايجابية في تدعيم الجهود القائمة في هذا المجال، وحرصا منها على توثيق علاقات التعاون القائمة بين الدول العربية في المجالات القضائية و العمل على دعمها و تنميتها و توسيع نطاقها تنفيذا للإعلان الصادر عن المؤتمر العربي الأول لوزراء العدل المنعقد في الرباط عام 1977 و بنتيجة ما تقدم: لاشك بأن الاجرام لم يعد يقلق أجهزة الدولة على النطاق الداخلي وانما اصبح من المعضلات الخطيرة التي تواجه المجتمع الدولي في هذه المرحلة بصرف النظر عن طبيعة النظام السياسي للدول و درجة تطورها[1]

[1]– محمد كرام، النصب المعلوماتي بين اكراهات النص القانوني والواقع العملي، ط 2، سلسلة النوازلي الالكترونية 05، مراكش، 2017، ص 118.

المطلب الأول: المساعدة القضائية الدولية كآلية للتعاون الدولي في مواجهة الجرائم المعلوماتية

في إطار التحقيق في الجرائم المعلوماتية، منح القانون للسلطات المختصة امكانية تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني،[1] على أن يرفض أي طلب مساعدة يمس بالسيادة الوطنية أو النظام العام[2]

الفرع الأول: صور المساعدة القضائية الدولية

تتمثل صور المساعدة القضائية الدولية في تبادل المعلومات ونقل الإجراءات والانابة القضائية الدولية.

أولا: تبادل المعلومات

قد تقع دولتين مختصتين في نفس الجريمة، غير أن احدى الدولتين لا ترغب في مباشرة التحقيق بشأنها، كما قد تتطوع بتزويد دولة التحقيق بالبيانات التي تم ضبطها وفقا لنظام تبادل المعلومات أو المساعدات.

حيث أن لتبادل المعلومات أهمية قصوى و من الضروري لجميع المشاركين في الأمن السيبراني أو مواجهة الجرائم المعلوماتية المشاركة في تبادل المعلومات التقنية حول الحقائق الدقيقة مما يتيح لهم زيادة المعلومات و التزود بأخبار بتكلفة أقل[3]، و لابد من تطوير الأطر و القواعد القانونية التي تسمح بتبادل المعلومات التي تساهم في مكافحة الجرائم المعلوماتية، و يشترط في ذلك تقديم المعلومات بطريقة مفهومة، و اقامة شراكة بين الجهات الفاعلة التي

[1]– أنظر الفقرة 1، المادة 16، من القانون 09-04، سالف الذكر ص 08.

[2]– انظر الفقرة 1، المادة 18، قانون 09-04، سالف الذكر، ص 08.

[3] -Freyssinet E, La cybercriminalité en mouvement, Lavoisier, 2012, France, p 195.

يكون لديها معلومات مفيدة خاصـــة مع وجود اطار قانوني شـــفاف لتعزيز تبادل المعلومات بسرية بين الجهات المعنية باحترام خصوصية المواطنين.

وفي هذا نصـت اتفاقية بودابسـت بموجب المادة 25 في فقرتها الأولى على أن توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض على أوسع نطاق ممكن، وذلك لأغراض التحقيقات أو الاجراءات المتعلقة بالجرائم التي لها علاقة بنظم وبيانات الحاسوب، أو بالنسبة لجمع الأدلة الخاصة بالجريمة في شكل الكتروني.[1]

لتليها المادة 26 وتشير الى قاعدة جوازية ارسال المعلومات بين الدول الاطراف دون طلب مسبق لكن بمراعاة القانون الوطني، حيث ترسل المعلومات التي يتم الحصول عبها في إطار التحقيقات وذلك بغرض التعاون ومســـاعدة الدولة الطرف في القيام بتحقيقاتها حول الجرائم المعلوماتية، واكدت في الفقرة الموالية على وجوبية المحافظة على ســـرية تلك المعلومات أو استخدامها وفقا لشروط معينة تطلبها الدولة مقدمة المعلومات.

وهو نفســـه ما اعتمد في الاتفاقية العربية المتعلقة بمكافحة جرائم تقنية المعلومات، حيث جاءت الفقرة الأولى من المادة 32 لتؤكد على وجوب توفير الدول الأطراف للمســـاعدة بأقصـــى مدى ممكن لغاية اجراء التحقيقات أو الاجراءات المتعلقة بجرائم المعلومات و تقنية المعلومات أو لجمع الأدلة في هذه الجرائم، ونصـت المادة 33 على جواز ارسـال معلومات محصل عليها من الدولة المرسلة خلال تحقيقاتها الى الدولة المرسل اليها اذا رأت أن كشف هذه المعلومات من الممكن أن يساعد الدولة الطرف المرسل اليها خلال تحقيقاتها أو أن هذه المعلومات قد تؤدي الى طلب التعاون من قبل تلك الدولة الطرف، وبطبيعة الحال يشـــترط الحفاظ على سرية المعلومات و هو ما تطلبه الدولة الطرف قبل اعطاء هذه المعلومات.

[1]– خالد عياد الحلبي، مرجع سابق، ص 244.

ويولي المجتمع الدولي لتبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الجرائم عموما والجرائم المعلوماتية خصوصا، لما توفره المعلومات الصحيحة من مساندة لأجهزة تنفيذ القانون، ويشمل مبدأ تبادل المعلومات: تقديم البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة معلوماتية.[1]

ونتيجة إدراك الاجرام المنظم لكيفية الاستفادة من تقنيات الكمبيوتر والاتصالات السلكية واللاسلكية للتواصل وتنظيم وتحديد الضحايا والفرص، وما نجم عنه من زيادة كفاءة الجريمة المنظمة في الاتجار بالمخدرات والاتجار بالبشر، وفي التجارة غير المشروعة في بيع المنتجات المقلدة وفي الجرائم الاقتصادية، وغيرها.[2] وهو ما استدعى تأكيد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر وطنية، على تسهيل تبادل المعلومات المتعلقة بكافة جوانب النشاط الاجرامي.

كما أن المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي أكدت على ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية، كما صاغ اتفاق شنجن للاتحاد الأوروبي نظاما متكاملا لتبادل المعلومات.

وبالرجوع الى المشرع الجزائري نجد نص المادة 17 من القانون 04-09 فيما يخص تبادل المعلومات واتخاد الاجراءات التحفظية، والتي جاء فيها:" تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي اجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل."

[1]– صورية بوربابة، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، المركز الديمقراطي العربي، العدد الأول، ألمانيا، 2019، ص 96.

[2] - Ghernaouti-Hélie S, La Cyberctiminalité le visible et l'invisible, Le savoir suisse, France, 2009 , P 117.

كما يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في طلب المساعدة[1]

ثانيا: نقل الاجراءات

يقصد بهذه الصورة قيام دولة ما بمقتضى اتفاقية او معاهدة باتخاذ اجراءات جنائية و هي بصدد التحقيق في جريمة معلوماتية ارتكبت في اقليم دولة اخرى و لمصلحة هذه الدولة متى توفرت مجموعة من الشروط أهمها التجريم المزدوج و الذي يقصد به: أن يكون الفعل المنسوب الى الشخص يشكل جريمة في الدولة الطالبة و الدولة المطلوب نقل الاجراءات اليها بالإضافة الى شرعية الاجراءات المطلوب اتخاذها، وقد تناولت كل من معاهدة الأمم المتحدة النموذجية بشأن نقل الاجراءات في المسائل الجنائية و اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر وطنية هذا الاجراء.[2]

ويحقق نقل الاجراءات الجنائية تقليص الآثار السلبية الناجمة عن تنازع الاختصاص بين الدول غير أنه رغم ذلك فان الاتفاقيات تمثل آليات تقليدية في مواجهة الجرائم و ملاحقة مرتكبيها، و هو ما قد لا يكون مجديا في اطار الجرائم المعلوماتية لطبيعتها العابرة للحدود الوطنية و صعوبة اقامة الدليل على ارتكابها و مدى قبول تشريعات الدول للأدلة المستمدة من الحاسب الآلي، كذلك ما يتعلق بمسائل الضبط و التفتيش في البيئة الافتراضية، و تتبع المسارات الالكترونية، و هو ما يؤدي الى صعوبة اثبات هذه الجرائم و نسبتها الى مرتكبيها، مما استدعى التعاون الدولي في مجال تفتيش أجهزة الحاسب الآلي.[3]

[1]- أنظر الفقرة 2 من نص المادة 18، قانون 09-04 سالف الذكر، ص 8.

[2]- صورية بوربابة، مرجع سابق، ص 97.

[3]- عادل عبد العال ابراهيم خراشي، مرجع سابق، ص 208.

ثالثا: الانابة القضائية الدولية

الانابة القضـائية الدولية: هي اجراء قضـائي من اجراءات الدعوى الجنائية تتقدم به الدولة الطالبة الى الدولة المطلوب اليها، وذلك لضـرورة الفصـل في مسـألة معروضـة على السـلطة القضـائية في الدولة الطالبة و يتعذر عليها القيام به بنفسـها، الهدف منه تسـهيل الاجراءات الجنائية بين الدول بما يكفل اجراءات التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السـيادة الاقليمية التي تمنع الدولة الأجنبية من ممارسـة بعض الأعمال القضائية داخل أقاليم الدول الأخرى كسماع الشهود و اجراء التفتيش وهي مسألة تتم بالطرق الدبلوماسية.[1]

حيث أن مشـكلة الحصـول على الدليل بشـأن بعض الجرائم إذا كان الدليل المراد الحصـول عليه يوجد في جهاز موجود في دولة اخرى، اذ لن تتمكن سـلطات التحقيق من الوصول اليه، ولذا تبدو اتفاقيات الانابة القضائية هي السبيل لتحصيله، بحيث تفوض الدولة الأخرى في جمع هذا الدليل وارسـاله لدولة التحقيق، وقد نصـت المادة 25/أ من قانون الحاسـوب الهولندي على الاعتداد بالدليل المتحصـل عليه في اقليم دولة اخرى إذا تم ذلك تنفيذا لاتفاقيات التعاون الأمني والقضائي[2].

[1]– محمد كرام، مرجع سابق، ص 119.

[2]– خالد عياد الحلبي، مرجع سابق، ص 244.

الفرع الثاني: معالجة المشاكل التي تواجه اجراء المساعدة القضائية الدولية

يصادف اجراء المساعدة القضائية الدولية العديد من العقبات التي يتطلب التطرق اليها وإيجاد حلول تعزز من سبل التعاون الدولي في مجال التحقيق في الجرائم المعلوماتية.

أولا: قصور التشريعات وتعارض المصالح بين الدول

ان من بين الصعوبات التي تواجه آليات التعاون الدولي في مواجهة الجرائم المعلوماتية والحد من آثارها، تعود أساسا الى القصور التشريعي للدول والتعارض بين مصالحها، فمن ناحية يعد افتقار الدول لنموذج موحد للنشاط الاجرامي طبقا لقوانينها، من أهم العقبات وهذا بسبب عدم وجود اتفاق عام ومشترك بين الدول حول نماذج اساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها، فما هو مباح في بعض الأنظمة مجرم في أنظمة اخرى[1]

ومن ناحية فان قصور غالبية النظم القانونية في وضع نظام قانوني خاص بالجرائم المعلوماتية، يجعل سبل التعاون الدولي صعبة، ذلك أن ترك القواعد العامة تنطبق على هذه الجرائم بشكل لا يتلاءم مع طبيعتها التقنية، يؤدي الى افلات المجرم من العدالة واهدار حقوق المجني عليه، كما أن تغليب كل دولة ما تحتاجه مصالحها ولو كان متعارضا مع مصالح الدول الأخرى يزيد من احتمال فشل سبل التعاون الدولي لاسيما عند وجود ايديولوجيات أو تعارض في مستويات احترام حقوق الانسان وحرياته.[2]

سعيا للتغلب على المشكلات المتعلقة بعدم وجود اتفاق عام مشترك بين الدول حول نماذج اساءة استخدام نظم المعلومات الواجب تجريمها، و عدم الوصول الى مفهوم عام حول

[1]– محمد احمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، 2016، ص 60.

[2]– عادل عبد العال ابراهيم خراشي، مرجع سابق، ص 235.

النشـاط الذي يمكن الاتفاق على تجريمه، واختلاف مفاهيم الجريمة باختلاف الحضـارات، و عدم وجود معاهدات دولية لمواجهة المتطلبات الخاصـــة بالجرائم المعلوماتية، مع تعقد المشـاكل النظامية و الفنية الخاصـة بتفتيش نظام معلوماتي خارج حدود الدولة ، أو ضـبط معلومات مخزنة فيه، أو الأمر بتســهيلها، أهاب مؤتمر الأمم المتحدة الثامن لمنع الجريمة و معاملة المجرمين المنعقد في هافانا، في قراره المتعلق بالجرائم ذات الصـلة بالحاسـب الآلي، الدول الأعضاء أن تكثف جهودها بغرض مكافحة اساءة استعمال الحاسب الآلي ويستدعي ذلك تطبيق جزاءات جنائية على الصـعيد الوطني، والنظر اذا ادعت الضـرورة في: تحديث الأنظمة و الاجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضـمان أن تكون الجزاءات بشأن سلطات التحقيق و قبول الأدلة على نحو ملائم. كما ينبغي النص على اجراءات تتعلق بالتحقيق والأدلة للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الاجرامي.[1]

ويعتبر تنوع واختلاف النظم القانونية الاجرائية من العقبات المصـادفة لإجراء التعاون الدولي فطرق التحري والتحقيق والمحاكمة التي تثبت فاعليتها في دولة ما، تكون عديمة الفائدة في دولة أخرى أو قد لا يسـمح بإجرائها كما هو الحال بالنسـبة للمراقبة الالكترونية أو التسـليم المراقب وغيرها.[2] فمن الممكن أن تكون طريقة التحري والتحقيق المشـروعة في دولة ما، غير مشروعة في دولة أخرى، كما قد لا تسمح دولة ما باستخدام دليل اثبات جرى جمعه بطرق ترى هذه الدولة انها طرق غير مشروعة.[3]

وكحل لهذه العقبات لابد من استخدام بعض من تقنيات التحقيق الخاصة، مما يخفف من غلو و اختلاف النظم القانونية والاجرائية و يزيد من فاعلية التعاون الدولي حيث أن المادة 20 من اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر وطنية تشير الى التسليم

[1]– محمد نصر محمد، مرجع سابق، ص 59.

[2]– محمد أحمد سليمان عيسى، مرجع سابق، ص 60.

[3]– صورية بوربابة، مرجع سابق، ص 100.

المراقب و المراقبة الالكترونية و غيرها من اشكال المراقبة و العمليات المستترة، والتي تعتبر من أهم التقنيات المستخدمة للجماعات الاجرامية المنظمة، بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول الى عملياتها و تجميع المعلومات و أدلة الاثبات لاستخدامها فيما بعد في الملاحقات القضائية في دول أطراف في سياق المساعدة القانونية المتبادلة.[1]

وفي ذلك قضت المادة 28 من الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، على ضرورة المحافظة على سرية المعلومات أثناء تبادل المعلومات أو اثناء المساعدة المتبادلة بين الاطراف، كما قضت المادة الموالية على وجوب السرعة في حفظ البيانات المعلوماتية المخزنة، حيث يجوز لكل طرف أن يطلب من الطرف الاخر الحفظ السريع للمعلومات المخزنة عن طريق احدى الرسائل الالكترونية الموجودة داخل النطاق المكاني لذلك الطرف الاخر.[2]

ثانيا: عدم القدرة على جمع الأدلة والمعلومات

ان عدم وجود قنوات اتصال تسمح للجهات المختصة القائمة على التحقيق بالاتصال بجهات أجنبية لجمع الأدلة أدلة معينة أو معلومات مهمة، يؤدي الى اعاقة التعاون الدولي فعدم وجود مثل هذا النظام ينجم عنه عدم القدرة على جمع الأدلة و المعلومات العملية التي غالبا ما تكون مفيدة لمواجهة الجرائم المعلوماتية و بالتالي لا ينجح التعاون الدولي، و في هذا المقام فغالبا ما تشجع الصكوك الدولية الدول على التعاون وانشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها و دوائرها المتخصصة، وذلك بهدف تسهيل الحصول على

[1]– محمد نصر محمد، مرجع سابق، ص 118.

[2]– المادة 29 من الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، بودابست 2001، سالفة الذكر، ص 17.

المعلومات و تبادلها، كما هو معمول به في الاتفاقية الاوروبية المتعلقة بالجريمة الالكترونية، و في اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[1]

ثالثا: بطء اجراءات المساعدة القضائية الدولية

ان أهم ما قد يحول دون نجاعة التعاون الدولي هو العقبات المصادفة لإجراء الانابة القضائية الدولية كصورة من صور المساعدة القضائية الدولية، حيث تتمسك كل دولة بسيادتها على اقليمها، بحسبان ان كل دولة عادة تقوم بالفصل في المنازعات التي تثار عبر اراضيها، فمن غير المقبول ان تطلب محكمة دولة معينة من دولة أخرى اجنبية ان تقدم لها المساعدة في القيام بإجراء التحقيق على اقليمها، كما أن تسليم طلبات الانابة القضائية يكون بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبطء و التعقيد وهو ما قد يتعارض مع طبيعة اعمال الانترنت وما تتميز به من سرعة. [2]

كما أن من بين العقبات هو التباطؤ في الرد من الدولة متلقية طلب المساعدة القضائية، والذي قد يرجع سببه الى نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية، أو الفوارق في الاجراءات التي تعقد الاستجابة وغيرها من الاسباب[3]

وكحل لهذه المشكلة لابد من اقرار اجراءات مستحدثة في مجال المساعدة القضائية الدولية: نتيجة للقصور في اجراءات المساعدة القضائية التقليدية بالرغم من أهميتها، الا أنها تتم بالطريق الدبلوماسي الذي يتسم بالبطء والتعقيد، وهو مما يجعله في اغلب الاحيان غير مجد في مواجهة الجرائم الالكترونية التي تتميز بالسرعة الفائقة، ونتيجة لهذا الوضع ظهرت

[1]– محمد أحمد سليمان عيسى، مرجع سابق، ص63.

[2]– عادل عبد العال ابراهيم خراشي، مرجع سابق، ص 244.

[3]– محمد أحمد سليمان العيسى، مرجع سابق، ص 61.

الحاجة الماسة الى البحث عن سبل بديلة للتعاون القضائي الدولي، وأهمها ما جاء في الاتفاقية الأوروبية حول الجريمة الالكترونية وتتمثل في:[1]

-**طلب الحفظ العاجل للمعطيات المخزنة:** والذي من مميزاته أنه بمثابة تدبير تحفظي احترازي سريع تسعى من ورائه الدول الى حماية بيانات الجريمة من أي تغيير أو ازالة أو محو قد يمسها من قبل المجرم، خاصة بعد علمه بوجود اجراءات تحقيق ومتابعة اتخذت ضده، كما يكفل المحافظة على سرية البيانات التي تهم الشخص المعني.

-**طلب الكشف السريع عن البيانات المحفوظة:** حيث يجوز لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق احدى الوسائل الالكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار اليها.[2]

-طلب دولة من اخرى البحث في بيانات أو النفاذ اليها أو مصادرتها، أو الكشف عناها، في حالة وجود البيانات مخزنة في نظام معلوماتي يوجد داخل أراضي الدولة المطلوب منها المساعدة، بما في ذلك البيانات التي تم حفظها بموجب المادة 29 من الاتفاقية، وتتم الاستجابة بشكل معجل إذا كانت هناك أسباب تدعو للاعتقاد بأن البيانات معرضة للضياع أو التعديل، أو في حالة وجود نص يقضي بالتعجيل في التعاون.[3]

-**المساعدة المتبادلة المتعلقة بجمع بيانات الحركة في الوقت الحقيقي:** وهو ما ورد في نص المادة م 33 من الاتفاقية والتي نصت على المساعدة المتبادلة بين الدول الأطراف

[1]- جمال براهيمي، مرجع سابق، ص 329.

[2]- محمد نصر محمد، مرجع سابق، ص 118.

[3]- المادة 30 من الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، سالفة الذكر، ص 18.

لجمع بيانات الحركة في الوقت الحقيقي والمرتبطة باتصـــالات محددة في أقاليمها التي يتم نقلها بواسطة نظام الكمبيوتر، وفقا للضمانات والاجراءات المحددة في القوانين الوطنية.[1]

-المســـاعدة المتبادلة المتعلقة باعتراض بيانات المحتوى من خلال التعاون في مجال جمع بيانات المحتوى في الوقت الحقيقي أو تسجيلها إذا تعلقت باتصالات محددة يتم نقلها بواسطة نظام معلوماتي بقدر ما تسمح به المعاهدات والقوانين الوطنية.[2]

وتجدر الاشارة أن المشرع الجزائري لم ينص بشكل صريح على هذه الاجراءات، غير أنه يمكن ان نجد لها مكان في تفسير نص المادة 16 من القانون 09-04 [3] والتي نصت على أنه يجوز في حالة الاســتعجال قبول طلب المســاعدة القضــائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس، البريد الالكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

كما انه و لأجل القضاء على الصعوبات التي تواجه اجراء الإنابة القضائية فلابد من ايجاد وسيلة أو طريقة تتسم بالسرعة وتسلم من خلالها طلبات الانابة كالسماح بالاتصال المباشر بين الجهات المختصة في نظر مثل هذه الطلبات للقضاء على مشكلة بطء و تعقيد تسليم طلبات الانابة القضائية، وهو ما اوصت به م 35 من الاتفاقية الاوروبية حيث أوجبت الدولة الاطراف فيها بضرورة تحديد نقطة اتصال تعمل 24 ساعة يوميا طوال أيام الاسبوع

[1]- المادة 33 من الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، سالفة الذكر، ص 19.

[2]- المادة 34، الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، سالفة الذكر، ص 19.

[3]- جمال براهيمي، مرجع سابق، ص 329.

لكي تؤمن المساعدة المباشرة للتحقيق في جرائم البيانات و الشبكات أو استقبال الأدلة في شكل الكتروني.[1]

زيادة على ذلك و باعتبار أن التذرع باعتبارات السيادة قد يكون سببا في تهرب المجرمين من العدالة وتهريب متحصلات الجريمة من أموال، مما يؤدي الى الاضرار بعدة دول، وبالتالي لابد من الاقرار بأن سيادات الدول بلا حدود ولابد من الاستجابة لمقتضيات التكافل و التعاون بين الدول، كما ينعكس أثر تقنية التحقيق عن بعد في التخفيف من فكرة السيادة حيث تسمح هذه التقنية بالتغلب على المشاكل التي تقلل من فاعلية الانابة القضائية الخارجية، وتتميز عن هذه الأخيرة في أن الدولة الطالبة هي التي تباشر اجراءات التحقيق باستخدام هذه التقنية، و يقتصر دور الدولة المطلوب اليها على توفير الوسائل الفنية و المادية لتنفيذ الاجراءات.[2]

[1]– محمد أحمد سليمان العيسى، مرجع سابق، ص 63.

[2]– عادل عبد العال خراشي، مرجع سابق، ص 286 ص287.

المطلب الثاني: تسليم المجرمين كآلية للتعاون الدولي في مواجهة الجرائم المعلوماتية

أصبح في وقتنا الحالي نظام تسليم المجرمين ضرورة ملحة وحتمية دولية تستدعيها الخطورة الاجرامية والتطور الذي وصلت اليه الجريمة اليوم بعبورها حدود الدولة الواحدة.

الفرع الأول: نظام تسليم المجرمين في مواجهة الجرائم المعلوماتية

معلوم أن تعاون الدول يتمثل في تطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية والاجراءات المتفق عليها بمقتضى القانون الخاص بالتماثل أو المعاملة بالمثل القوانين الوطنية والمحلية، ولأقصى درجة ممكنة للأغراض الخاصة بالعمليات المتعلقة بالتحقيق والبحث أو الاجراءات المتعلقة بالجرائم أو الخاصة بنظم وبيانات الكمبيوتر أو لتجميع الأدلة الخاصة بالجريمة في صورة الكترونية، وهي مسألة تتعلق بعمليات تسليم المجرمين[1]

أولا: تعريف نظام تسليم المجرمين

ان نظام تسليم المجرمين هو نظام قانوني تسلم بموجبه دولة ما شخص معين الى دولة اخرى، ويجد هذا النظام أساسه من خلال الاتفاقيات الدولية، مبدأ المعاملة بالمثل، أو التشريعات الداخلية، وتجدر الاشارة أنه في حالة تعارض الاتفاقية مع التشريع الداخلي تسري أحكام الاتفاقية، أما في حالة عدم وجود اتفاقية، فاذا كانت الدولة تقر بمبدأ المعاملة بالمثل بإمكانها الاستجابة لطلب التسليم، أما إذا كانت لا تقر به فلها الخيار في قبول الطلب أو رفضه.

[1]– محمد كرام، مرجع سابق، ص 119.

ومن القضـــايا العملية في مجال تســـليم المجرمين نجد –عملية محطم الجليد Icebreaker، قامت بها اليوروبول Europol في 14 يونيو 2005، حيث تم من خلالها مداهمة وتفتيش أماكن في 13 دولة أوروبية (النمسا، بلجيكا، فرنسا، ألمانيا، المجر، ايسلندا، ايطاليا، هولندا، بولونيا، البرتغال، سـلوفاكيا، السـويد، بريطانيا العظمى)، كما تم توقيف افراد في كل من فرنسـا، بلجيكا، المجر، ايسـلندا، السـويد، ثم تم تسـليم المتهمين الى بريطانيا التي قامت بتقديمهم للمحاكمة الجنائية وحكم القضاء بإدانتهم.[1]

ثانيا: أساس نظام تسليم المجرمين

لقد تضـمنت اتفاقية بودابسـت المبادئ ذات الصـلة بتسـليم المجرمين، من خلال نص المادة 24 منها، والتي تضـمنت جميع الأحكام الخاصـة بتسـليم المجرمين فيها، كذلك نصـت الاتفاقية العربية على التعاون القانوني والقضـائي بما فيها اجراء تسـليم المجرمين وفقا لنص المادة 31 منها.[2]

وأخضـع المشـرع الجزائري بعض جوانب نظام تسـليم المجرمين الى أحكام دسـتورية، والتي قضت بعدم جواز تسليم أحد خارج التراب الوطني الا بناء على قانون تسليم المجرمين، وعدم جواز تسليم اللاجئين السياسيين.[3]

---

[1]– فهد عبد الله العبيد العازمي، مرجع سابق، ص 565.

[2]– أنظر المادة 31 من المرسوم الرئاسي رقم 14–252، المؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية، العدد 57، المؤرخة في 28 سبتمبر 2014، ص 09.

[3]– وفي هذا الصدد لابد للاتفاقيات المبرمة فيما يخص نظام تسليم المجرمين ان تأخذ بعين الاعتبار التنظيم الداخلي لنظام تسليم المجرمين.

كما تضـــمن قانون الاجراءات الجزائية نظام تســـليم المجرمين في الكتاب الســـابع المتعلق بالعلاقات بين السلطات القضائية الاجنبية، ووضح شروط تسليم المجرمين بموجب المواد من 694 الى 701، وآثار التسليم من المواد 702 الى 713، وآثار التسليم في المواد من 714 الى 718 من قانون اجراءات جزائية جزائري. ويفهم من المادة 718 من هذا القانون أنه لا يجوز للدولة ان تقوم بإعادة تسليم شخص تم تسليمه اليها الى دولة أخرى وهو ما يعرف في الاتفاقيات الدولية بمبدأ عدم جواز اعادة التسليم.

ثالثا: شروط تسليم المجرمين

هناك تباين في تحديد شـروط نظام تسـليم المجرمين حيث تقسـم الى شـروط عامة، وشروط خاصة

-الشروط العامة:

- **الشق المتعلق بالأشخاص:** فالقاعدة العامة هي جواز تسليم كامل الأشخاص سواء كانوا فاعلين اصليين أو مشاركين في الجريمة، غير أنه استثناء لا يجوز تسليم رعايا الدولة. أما إذا كان مرتكب الجريمة يحمل جنسـية الدولة الطالبة يتم تسـليمه بطريقة عادية وهو ما جاء في نص المادة 696 قانون اجراءات جزائية. وإذا كان شخص يحمل جنسية دولة ثالثة يسلم الأجنبي الى الدولة الطالبة على أساس مبدأ الاقليمية، وقد يكون على أساس مبدأ العينية.

وفي حالة تعدد الجنسـيات يفرق بين حالتين: فاذا كانت من بين الجنسـيات جنسـية جزائرية سواء أصلية أو مكتسبة لا يجوز تسليمه، أما إذا كانت الجنسيات ليست من بينها جنسية جزائرية والدولتين طالبتي التسليم على اساس مبدأ الشخصية فهنا يجوز تسليمه.

- **الجرائم التي يتم على أساسها التسليم:** حيث أنه كمبدأ عام يتم التسليم في كل الجرائم ماعدا المسـتثنية في الاتفاقيات و المعاهدات الدولية مثل: الجرائم السـياسـية، كما لا يجوز

تسليم أو طرد لاجئ سياسي، أما اذا تعلق الأمر بالجرائم العسكرية التي تشكل اخلالا بالنظام العسكري لا يجوز التسليم في اطار الواجبات العسكرية كالفرار من الخدمة العسكرية، العصيان، الخيانة، غير أنه يجوز تسليمهم اذا ارتكبوا جرائم خارج القانون العسكري و يسلم وفقا للقانون العام اذا كانت الدولة تسلم رعاياها، أما المدنيين الذين يرتكبون جرائم في أماكن خاصة بالجيش يحاكمون أمام القضاء العسكري لكن يجوز تسليمهم).

ومما سبق فيمكن تسليم المجرمين في الجرائم المعلوماتية بشرط أن تكون هذه الجرائم معاقب عليها في قوانين الدول الاطراف ومن بينها[1] الدخول غير المشروع أو الاعتراض غير المشروع أو الاعتداء على سلامة البيانات أو اساءة استخدام أجهزة الحاسب الآلي أو الاستخدام غير المشروع لأدوات الدفع الالكتروني، كذلك في جرائم التزوير و الاحتيال المرتبط بالحاسب الآلي أو جرائم الارهاب الالكتروني أو في الجرائم المنظمة المرتكبة بواسطة تقنية المعلومات كتبييض الأموال و الترويج للمخدرات و المؤثرات العقلية أو الاتجار بالأشخاص و الأعضاء البشرية و المتاجرة بالأسلحة، اضافة الى الجرائم الاباحية خاصة المتعلقة بإباحية الأطفال و القصر أو الاعتداء على حرمة الحياة الخاصة، و الجرائم المتعلقة بالانتهاكات الخاصة بحقوق النشر و التأليف وما له صلة بذلك.

وما يجدر الاشارة له في هذا الصدد أن نهج الاتفاقيات الدولية والقوانين الوطنية يختلف من حيث تعريف وتصنيف الجرائم محل التجريم حيث أن المنهج الأول يقوم على التعداد الحصري للجرائم محل التسليم، في حين يقوم نهج ثاني بوضع قائمة سلبية للجرائم التي لا يجوز فيها التسليم.[2]

[1]– أنظر الفقرة الأولى من المادة 31، المرسوم الرئاسي رقم 14–252 سالف الذكر، ص 31.

[2]– عادل عبر العال ابراهيم خراشي، مرجع سابق، ص 221.

الشروط الخاصة:

-**ازدواجية التجريم:** وهنا لا ننظر الى تكييف الجريمة وانما إذا كان الفعل مجرم، حيث نلاحظ أن المشرع الجزائري أخذ بهذا الشرط حينما عدد الأفعال التي يجوز فيها التسليم سواء كان الشخص مطلوبا أو مقبولا بعد استيفائه للشروط المنصوص عليها في المادة 696 من نفس القانون[1]، و قد أجاز المشرع التسليم في جميع الأفعال المعاقب عليها بجناية حسب قانون الدولة الطالبة، و أيضا في الجنح متى توافر مجموعة من الشروط أولها ارتكاب شخص لجنحة في قانون الدولة الطالبة وكان الحد الأقصى للعقوبة هي الحبس لمدة سنتين أو اقل، أما الحالة الثانية إذا كان مرتكب الجنحة قد حكم عليه بعقوبة تساوي أو تجاوز الحبس لمدة شهرين.[2]

-**شرط الاختصاص:** ويستند مبدأ الاختصاص الى أن تكون الدولة طالبة التسليم مختصة قانونا انطلاقا من مبدأ العينية، الشخصية، الاقليمية وانتفاء الاختصاص التشريعي بالنسبة للدولة المطلوب اليها التسليم، أما إذا تعددت طلبات التسليم ميز المشرع الجزائري بين حالتين: الحالة الاولى هي حالة تعدد الطلبات حول نفس الجريمة فالأولوية للدولة التي لحقها ضرر أكبر، أما الحالة الثانية في حالة تقارب الأضرار فالأولوية للدولة التي ارتكبت الجريمة على أراضيها.

[1]- مليكة درياد، احكام تسليم المجرمين في قانون الإجراءات الجزائية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 01، 2019، ص 11.

[2]- المادة 697 من قانون الإجراءات الجزائية الجزائري سالف الذكر.

الفرع الثاني: معالجة المشاكل التي تواجه نظام تسليم المجرمين في الجرائم المعلوماتية

يعد نظام تسليم المجرمين من الآليات القضائية التي تصادفها العديد من المشاكل مما يحول دون ضمان غايات التعاون الدولي في مواجهة الجرائم المعلوماتية.

أولا: ازدواجية التجريم

يعتبر التجريم المزدوج من أهم الشـــروط الخاصـــة بنظام تســـليم المجرمين، و هو منصـوص عليه في اغلب التشـريعات الوطنية و الصـكوك الدولية المعنية بتسـليم المجرمين، وبالرغم من أهميته نجده عقبة أمام التعاون الدولي في مواجهة الجرائم المعلوماتية، لاسـيما و أن معظم الدول لا تجرم هذه الجرائم، بالإضـــافة الى أنه من الصـــعوبة تحديد فيما اذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تطبق على الجرائم المعلوماتية الامر الذي يعيق تطبيق الاتفاقيات الدولية في مجال تســـليم المجرمين ويحول دون جمع الأدلة ومحاكمة مرتكبي الجرائم المعلوماتية.[1]

ولأجل القضـاء على مشكلة ازدواجية التجريم، ركزت الاتجاهات والتطورات التشـريعية الخاصـــة بتســـليم المجرمين على تخفيف التطبيق الصـــارم لهذا الاجراء، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين من خلال سرد الأفعال التي تتطلب أن تجرم كجرائم أو افعال مخلة بمقتضـى قوانين الدولتين معا، أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة[2]

[1]– محمد أحمد سليمان عيسى، مرجع سابق، ص 61.

[2]– محمد نصر محمد، مرجع سابق، ص 121.

ثانيا: تعدد طلبات التسليم

قد يرتكب الشـخص المراد تسـليمه لجريمة أو أكثر من الجرائم المعلوماتية وتمس في نفس الوقت بمصالح أساسية لعدة دول، ففي هذه الحالة قد تتزاحم طلبات التسليم المقدمة من الدول المتضـررة الى الدولة المطلوب اليها، وفي ذلك لابد أن تقدم الدولة المتضـررة الأدلة الكافية التي تثبت قيام الشخص المراد تسليمه بارتكاب جريمة من الجرائم المعلوماتية، وكذلك ارسـال طلبها فعلا وليس مجرد تصـريح شـفاهي أو ابداء رغبة في اسـتلامه، و في ذلك لم يسـتقر الاتجاه الدولي على تحديد و ترتيب طلبات التسـليم في حالة تعددها، حيث توجد اختلافات كبيرة في ترتيب الأولويات، وحسـما لمشـكلة تعدد الطلبات فلابد من عقد اتفاقيات دولية يتبعها المجتمع الدولي ككل حيث تتضـمن ضـوابط موضـوعية وآليات محددة بصـفة مجردة و تكون الأولوية في التسـليم للدولة التي أضـرت الجريمة بمصـالحها ثم الدولة التي ارتكبها الجريمة على اقليمها ثم الدولة التي ينتمي اليها الشخص المطلوب تسليمه، وفي حالة طلبات التسـليم حول عدة جرائم فالأولوية للدولة التي ارتكبت على اقليمها الجريمة الأشـد خطورة وفقا لقانون الدولة المطلوب اليها التسـليم، و في حالة تسـاوي الخطورة تكون الاولوية للدولة التي قدمت طلبها أولا.[1]

ثالثا: تنازع الاختصاص القضائي الدولي

قد يحدث أن ترتكب جريمة في اقليم دولة معينة من قبل أجنبي، وهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا على مبدأ الاقليمية، وتخضع لاختصاص

[1]– عادل عبد العال ابراهيم خراشي، مرجع سابق، ص 297.

الدولة الثانية استنادا لمبدأ الشخصية، وقد تهدد الجريمة أمن وسلامة دولة أخرى فينعقد اختصاصها استنادا لمبدأ العينية.[1]

كما تثار مشكلة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الاقليمية، كما لو قام الجاني ببث صور خليعة ذات طابع اباحي من اقليم دولة معينة وتم الاطلاع عليها في دولة اخرى، ففي هذه الحالة ينعقد الاختصاص وفقا لمبدأ الاقليمية لكل دولة من الدول التي مستها الجريمة. [2]

وبالنسبة لمشاكل الاختصاص القضائي الدولي فينبغي ابرام اتفاقيات دولية ثنائية أو جماعية يتم فيها تحديد وجهات النظر فيما يتعلق بالاختصاص القضائي في مواجهة الجرائم المعلوماتية، بالإضافة الى تحديث القوانين الجنائية –الموضوعية والاجرائية–بما يواكب التطورات التكنولوجية المستمرة.

حث مؤتمر الأمم المتحدة الثامن لمنع الجريمة و معاملة المجرمين، المنعقد في هافانا، المتعلق بالجرائم ذات الصلة بالحاسب الآلي، على مضاعفة الدول الأعضاء للأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسب الآلي، بما في ذلك دخولها اطرافا حسب الاقتضاء في المعاهدات المتعلقة بتسليم المجرمين و تبادل المساعدات الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب الآلي، و أن يسفر بحث الأمم المتحدة في هذا الصدد عن فتح آفاق جديدة للتعاون الدولي لاسيما من حيث تطوير معايير دولية لأن المعالجة الآلية للبيانات، و تدابير ملائمة لحل مشاكل الاختصاص القضائي التي

[1]– بمقارنة كل من مبدأ العينية ومبدأ الشخصية نجدهما يشتركان في أن كلاهما يكون العنصر الأجنبي ضروري، وكلاهما ترتكب الجريمة في الخارج، وكلاهما يشترطان الوصف الاجرامي للواقعة (جناية، جنحة)، وكلاهما يشترط التأكد من الواقعة هل فصل فيها أو هل تم التقادم فيها أو العفو فيها، أو هل صدر فيها حكم، غير أن يشترط جنسية رعايا الاقليم، وتسليم المجرمين فيه يكون ارادي، أما مبدأ العينية يشترط المساس بالمصالح العليا للمجتمع وتسليم المجرمين فيه اجباري.

[2]– محمد أحمد سليمان العيسى، مرجع السابق، ص 61.

تثيرها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية، وضع اتفاقيات دولية تنطوي على نصـوص تنظيم اجراءات التفتيش و الضـبط المباشـر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، و الأشكال الاخرى للمساعدة المتبادلة، مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول.[1]

اضافة الى ذلك ينبغي التنويه أن اتفاقية بودابست أوجدت حلولا فعالة لتجاوز العقبات المصـــادفة لإجراء التحقيق في الجرائم المعلوماتية عبر الوطنية، خاصـــة ما تعلق منها باختلاف النظم الاجرائية أمام التعاون الدولي، و مشكلة الاختصـاص و الولايات القضـائية، ومشكلة التجريم المزدوج، وعدم وجود قنوات اتصال دولية مباشرة بين سلطات انفاذ القانون، و الصـعوبات المرتبطة ببطء اجراءات المسـاعدة القضـائية، لذا على الدول الاسـراع خاصـة المتخلفة منها في تبني الحلول المنصـوص عليها، وذلك اما بإدراجها ضـمن قوانينها الداخلية و الالتزام بالعمل بها، أو من خلال الانضمام الى الاتفاقية الأوروبية مادام أنها متاحة للتوقيع من جميع الدول، و من ثم يسري عليها من هذه الأحكام ما يسري على الأطراف الأخرى.[2]

وفي الأخير تجدر الاشـارة الى أن التعاون القضـائي الدولي لا يكفي لوحده بل لابد من ايجاد آليات تعاون تقني دولي في مجال تدريب أجهزة مواجهة الجرائم المعلوماتية،

حيث أن أبرز ما توصل اليه مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية المنعقد في الدوحة في يوم 12-19 أفريل 2015، أن للمســـاعدة التقنية والتعاون التقني أهمية بالغة في اتاحة امكانية تقاســـم ممارســـات التحري والتحقيق الجيدة والتجارب المكتســـبة وتعميم الأســـاليب الجديدة مثل الاحتيال المالي بواســـطة الانترنت أو الاتجار بالمخدرات عبر الانترنت أو اســـتخدام العملات الافتراضـــية في تبييض الأموال مما يتيح

[1]- محمد نصر محمد، مرجع السابق، ص 59.

[2]- جمال براهيمي، مرجع سابق، ص 329.

للسلطات المختصة في بلدان متعددة سرعة اكتساب المهارات الضرورية لمواجهة الأخطار المستجدة[1].

فالجرائم المعلوماتية اليوم تحولت من مجرد انتهاكات فردية لأمن النظم و المعلومات الى ظاهرة تقنية عامة، ينخرط فيها الكثير ممن تتوفر فيهم قدرات معينة في مجال الحاسب الآلي و الاتصال بشبكة الانترنت، و تتم المراقبة التقنية بعدة وسائل منها: تشفير البيانات المهمة المنقولة عبر الانترنت، ايجاد نظام أمني متكامل يقوم بحماية البيانات و المعلومات، توفير برامج الكشف عن الفيروسات و المقاومة لها لحماية الحاسب الآلي والبيانات و المعلومات، عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية، مع عمل وسائل التحكم في الدخول الى المعلومات و المحافظة على سريتها، توزيع مهام العمل.[2]

ولعل الأجهزة العدالة الجنائية في الكثير من الدول ليست لديها نفس درجة الاستعداد لمواجهة الجرائم المعلوماتية لعدة اسباب من بينها: الافتقار الى الموارد الكافية مادية كانت او بشرية، أو أن سلطات التحقيق لديها محدودة، أو لأن لديها قوانين و نظم سبقها الزمن أو تفتقر لقانون مواجهة الجرائم المعلوماتية، وبالتالي لابد من تعاون الدول فيما بينها لمواجهة الجرائم المعلوماتية، و من الاتفاقيات التي دعت بشكل صريح على ضرورة وجود تعاون بين الدول في مجال التدريب و نقل الخبرات نجد نص المادة 29 من اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000 (بالرمو) من بين المجلات المنصوص عليها في المادة و المتعلقة منها بشق المعلوماتية لابد ان يشمل مجال التدريب جمع الأدلة، المعدات و التقنيات الحديثة لإنفاذ القانون، بما في ذلك المراقبة الالكترونية و التسليم المراقب

[1]– يوسف مناصرة، جرائم المساس بأنظمة المعالج الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها) دراسة مقارنة، دار الخلدونية، 2018، الجزائر، 270–271.

[2]– محمد نصر محمد، مرجع سابق، ص 61.

و العمليات الســـرية، الطرائق المســـتخدمة في مكافحة الجريمة المنظمة عبر الوطنية التي ترتكب باستخدام الحواسيب أو شبكات الاتصال السلكية و اللاسلكية أو غيرها من اشكال التكنولوجيا الحديثة.[1]

وللحد من الصـــعوبات الفنية التي تواجه التعاون الدولي في مجال التدريب لابد من زيادة البرامج التي تعمل على بيان مخاطر الجرائم المعلوماتية و الأضـــرار التي تســـببها وبأهمية تدريب رجال العدالة على مواجهتها، و التنســـيق بين الأجهزة المعنية بتدريب رجال تنفيذ القانون و ايجاد برامج تدريبية مشـــتركة تناســـب جميع الفئات، كما يتعين الاهتمام بالمســاعدين القضــائيين، و منهم رجال الأدلة الجنائيين، وما تم اســتحداثه مؤخرا من وظيفة محلل جنائي.[2] ، اضـــافة الى التدريب المســـتمر و عقد دورات تدريبية و تكوينية في الخارج والمشاركة من كل المعنيين بمواجهة الجرائم المعلوماتية من كل الدول.

[1]– فهد عبد الله العبيد العازمي، مرجع سابق، ص 609.

[2]– محمد نصر محمد، مرجع سابق، ص 123.

خلاصة الباب الثاني:

ان فاعلية التحقيق في الجرائم المعلوماتية تتطلب تناسب الآليات الاجرائية مع طبيعة الجرائم المعلوماتية وخصوصية مرتكبيها مع اقامة توازن بين المصالح المختصة بالتحقيق واحترام حقوق وحريات الأفراد.

بالنظر الى درجة ملائمة القواعد الاجرائية التقليدية مع طبيعة هذه الجرائم و مرتكبيها نخلص الى أن القواعد الاجرائية التقليدية غير كافية، فرغم استحداث بعض النصوص القانونية التي تخص الاجراءات العادية للتحقيق في الجرائم المعلوماتية الا أن امكانية استخلاص الأدلة بواسطة اجراء التفتيش و الضبط و الحجز في المنظومة المعلوماتية قد يصادفه عدة اشكاليات من الناحية العملية، فنتيجة وجود أدوات تشفير للحاسب و المعلومات، و قدرات المجرم على تخزينها قد يحول دون نجاعة اجراء التفتيش، كما أن عبور التفتيش خارج الحدود الوطنية يتطلب تنسيق دولي في اطار الاتفاقيات الدولية أو المعاملة بالمثل، ولعل كبر حجم الشبكات المحتوية على معلومات التي يتطلب ضبطها قد لا يتم ضبطها حقيقة، هذا اضافة الى امكانية تعذر اجراء الحجز في المنظومة المعلوماتية.

كما أن المكونات المعنوية للحاسب الآلي قد تثير عدة صعوبات عن اجراء المعاينة وهذا لتردد عدد كبير من الأشخاص على مسرح الجريمة وذلك خلال مدة زمنية طويلة نسبيا مع امكانية التلاعب بالبيانات عن بعد وامكانية حذفها، وهو ما يتطلب اتخاذ اجراءات قبل واثناء وبعد اجراء المعاينة. وقد يسبب سهو الخبير أو اغلاق الحاسب الآلي بطريقة غير صحيحة الى فقدان أدلة جوهرية، كما أن الجاني قد يقوم بتعديل أو اخفاء المعلومات والبيانات أو تحريفها، وقد يهيئ الجهاز للتفجير أو التدمير بمجرد تشغيله وهو ما يحول دون استخلاص الدليل اللازم في اجراء التحقيقات.

مع كل الصعوبات سالفة الذكر كان من اللازم تدعيم الاجراءات العادية التحقيق في الجرائم المعلوماتية بإجراءات خاصة وفي ذلك استحدث المشرع الجزائري اجراء المراقبة الالكترونية والذي يعد من الاجراءات الخطيرة التي تستوجب اجراءات مشددة بغرض توفير حماية للحق في الحياة الخاصة، كما استحدث اجراء التسرب والذي مازال في بداياته من الناحية العملية، كما تم فرض التزامات على مقدمي خدمات الانترنت والتي تعد اجراءات تمهيدية تسهل مهمة سلطات التحقيق في كشف الجرائم المعلوماتية والبحث عن الأدلة وضبطها.

جعل تميز الجرائم المعلوماتية بالطابع عبر الوطني، المجتمع الدولي يركز على وجوب اعتماد آليات للتعاون الدولي في مواجهة هذه الجرائم، وفي ذلك سعت الاتفاقيات الدولية الى تعزيز سبل التعاون الدولي لمنع الجريمة، ومنها الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، والاتفاقية العربية المتعلقة بتقنية المعلومات، ولعل الأمم المتحدة سعت لتحسين وسائل وسبل التعاون الدولي من خلال عقدها لمؤتمرات دورية كل 5 سنوات آخرها كان في 2020، وللوكالات التابعة لها دور رئيسي في مواجهة الجرائم المعلوماتية.

وقد أصبح التعاون الدولي على المستوى الأمني والقضائي ضرورة حتمية لمواجهة هذه الجرائم، ولعل تحقيق التكامل وخدمة السياسة الجنائية في مواجهة الجرائم المعلوماتية يتطلب تبادل الخبرات والتدريب المستمر للأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية، مع الاستفادة من خبرات الدول الرائدة في المجال المعلوماتي ولابد من المساعدة الفنية بين الدول.

ورغم الجهود المبذولة لمواجهة الجرائم المعلوماتية الا أن التعاون القضائي الدولي مازال يعتريه صعوبات تتعلق بالمساعدة القضائية المتبادلة وأخرى تتعلق بإجراءات تسليم المجرمين، مما يستدعي تحديث هذه الآليات، ويبدأ ذلك من خلال تطوير القوانين الوطنية بما يواكب تطور أساليب ارتكاب الجرائم المعلوماتية، والانضمام الى الاتفاقيات الدولية الثنائية أو الجماعية لتطويق نطاق هذه الجرائم، وسن قانون مستقل خاص بالجرائم المعلوماتية.

خاتـــــــــــمة

خاتمة:

ان ما أحدثته تكنولوجيا المعلومات من توفير خدمات نوعية وسريعة تلبي حاجيات الأفراد والمجتمعات والدول، يستدعى تحديث المنظومة القانونية لمواجهة أي استخدام سلبي لذلك، مما استوجب على المشرع الجزائري ملاءمة النصوص القانونية للتطورات الحديثة والأخذ في الحسبان خصوصية التحقيق لضمان فاعليته بغرض الوصول الى الحقيقة، وقد توصلنا الى مجموعة من النتائج والتوصيات التي نوردها على النحو الآتي:

النتائج:

1- ان اجراءات التحقيق في الجرائم المعلوماتية تتمتع بخصوصية من حيث طبيعة هذه الجرائم باعتبارها أساس موضوع التحقيق المستحدث، وكنتيجة فلم يتفق على تحديد مفهوم جامع مانع لهذه الجرائم، وعرفناها بأنها الاستخدام غير المشروع أو غير المصرح به للبيانات والمعلومات، أو نقلها أو تخزينها أو استعمالها عبر الوسائط الالكترونية، بما يشكل اعتداء على الأشخاص والأموال وضرب استقرار الدولة وأمنها.

2- تظهر خصوصية التحقيق في هذه الجرائم من حيث أهمية الأجهزة المكلفة بهذه المهمة، واعتمادها على وسائل مستحدثة تساعد على كشف الجريمة والتوصل الى المجرم المعلوماتي باعتماد تقنيات علمية وعملية تستدعي الالمام بمختلف الجوانب المعلوماتية والتمكن من أجهزة الحاسب الآلي.

3- استحدث المشرع الجزائري هيئات غير قضائية جاءت لتدعم الهيئات القضائية المتخصصة و الوحدات الخاصة بالأمن و الدرك الوطني، لمواكبة التطورات التكنولوجية الحديثة و تطويق نطاق الجرائم المعلوماتية حيث تم انشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام و الاتصال بموجب القانون 09-

04، ليترك تشكيلها و تنظيما و كيفيات سيرها عن طريق التنظيم وقد تم اصدار مرسوم رئاسي سنة 2020 يتضمن اعادة تشكيلة و تنظيم و سير هذه الهيئة؛ كما تم انشاء سلطة وطنية لمعالجة المعطيات ذات طابع شخصي بموجب القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي؛ وتم استحداث وكالة خاصة بأمن الأنظمة المعلوماتية بموجب مرسوم رئاسي سنة 2020، وكل ذلك في سبيل توفير حماية أكبر للأفراد و المجتمعات وضبط الجرائم المعلوماتية والحصول على الأدلة التي تفيد في اثبات هذه الجرائم.

4- وكنتيجة لا غنى عنها، فان الأجهزة المكلفة بالتحقيق لابد عليها أن تراعي احترام المبادئ الدستورية والعالمية لضمان فاعلية التحقيق في مواجهة الجرائم المعلوماتية من خلال تطوير قدرات المعرفة الالكترونية وكتمان السر المهني اضافة الى السرعة في اتخاذ الاجراءات اللازمة، عند القيام بكافة خطوات التحقيق كضمانة لمواجهة فعالة لهذا النوع المستحدث من الجرائم وضمان جمع الأدلة وتحليلها بدقة واحترافية لسلامة التقارير المنجزة.

5- يجب تحديد العناصر اللازمة للتحقيق من خلال استظهار أركان الجريمة وتحديد نطاقها المكاني والزماني بما يسهل توضيح القانون الواجب تطبيقه في هذه الجرائم سواء داخل أو خارج النطاق الاقليمي للدولة، ومراعاة قواعد الاختصاص القضائي؛ كما يشترط تدوين اجراءات التحقيق والتفريق بين ما يلزم فيه السرية وما يلزم فيه العلنية تحقيقا لقاعدة التوازن بين ضمان حقوق الدفاع وفاعلية التحقيق الذي يسعى الى الحقيقة.

6- رغم تعدد الآراء الفقهية والقانونية بشأن امكانية تطابق القواعد الاجرائية التقليدية للتحقيق في الجرائم المعلوماتية الا أنه من وجهة نظرنا فالتحقيق في هذا النوع من

الجرائم يتطلب وجوبا قواعد اجرائية خاصة تتناسب مع طبيعة هذه الجرائم المعاصرة بما يضمن: –تحت طائلة بطلان الاجراءات؛

- عدم المساس بالشرعية الاجرائية؛
- تفادي اي انتهاك لحقوق وحريات الأفراد؛
- ضمان عدم المساس بالحق في الخصوصية.

7- يعد الحق في الخصوصية من التحديات التي تواجه اجراءات التحقيق، وهو ما استدعى تفطن المشرع الجزائري وموازنته بين تكريس هذا الحق وبين تنظيم قواعد اجرائية للوقاية من الجرائم المعلوماتية ومكافحتها.

8- نلتمس ارادة المشرع في التوفيق بين القواعد الاجرائية الناجعة لمواجهة الجرائم المعلوماتية و بين تكريس ضمانات الحق في الخصوصية، من خلال تسلسل القوانين الخاصة بمواجهة الجرائم المعلوماتية ابتداء من تعديل قانون الاجراءات الجزائية سنة 2006، وتضمينه على أساليب التحري و التحقيق الخاصة في الجرائم المعلوماتية، والمتمثلة في اعتراض المراسلات والتقاط الصور وتسجيل الاصوات، اضافة الى اجراء التسرب، والتي لا يمكن اللجوء اليها الا بموجب توفر شروط خاصة منها طبيعة الاذن واحترام مدته، و تحديد الجريمة ووجوب تحرير محضر عند نهاية التحقيق؛ وقد عززت المواجهة بإصدار القانون 09-04 والذي يعتبر أهم ما يمكن اعتماده في مجال التحقيق في هذه الجرائم، لتضمنه لإجراءات تتماشى مع طبيعة الجرائم المعلوماتية، وتتم بموجب اذن خاص، وتتمثل هذه الاجراءات في اجراء تفتيش المنظومة المعلوماتية، وحجزها، اضافة الى اجراء المراقبة الالكترونية؛ كما ضمن هذا القانون إجراءات تمهيدية لجمع البيانات و المعلومات يقوم بها غالبا مقدمي الخدمات من خلال التزاماتهم العامة بهدف مساعدة سلطات التحقيق وحفظ المعطيات المتعلقة بحركة السير، اضافة الى الالتزامات الخاصة لمقدمي

خدمات الانترنت بوجوب التدخل الفوري وضرورة وضع ترتيبات تقنية تمنع وصول الجمهور الى الأنشطة المعلوماتية المجرمة.

9- أخذ المشرع الجزائري في تدعيم المنظومة القانونية بإصدار القانون 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية، الذي أكد على سرية المراسلات و الاتصالات الالكترونية وواجب المحافظة على المعلومات الاسمية للمشتركين، تحت طائلة العقوبات المنصوص عليها بموجب هذا القانون في حالة الانتهاكات التي قد تطال الحق في الخصوصية؛ كما أصدر القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث تعتبر المعطيات ذات الطابع الشخصي جزء من الحياة الخاصة، تستوجب الحماية الجزائية، وتضمن هذا القانون اجراءات قانونية صارمة في حالة اساءة استخدام هذه المعطيات، تحت طائلة العقوبات المقررة في هذا القانون.

10- أخذ المشرع الجزائري بنظام الاثبات الجزائي الحر، المرتكز على شرعية الاثبات المقترن بقيم العدالة وأخلاقياتها ومقتضيات الكرامة الانسانية، ومشروعية الدليل، وفي ذلك يقتضي عند الاثبات بالدليل الالكتروني التقيد بهذه المبادئ.

11- تبقى الصعوبات التي تواجه أجهزة التحقيق في الجرائم المعلوماتية قائمة في ظل توسع دائرة الجرائم المعلوماتية كلما زادت التطورات التكنولوجية، ومن أهم الصعوبات يمكن أن نذكر ما يلي:

- مشاكل الدليل الالكتروني وحجيته في الاثبات الجزائي؛ فالدليل الالكتروني يتطور باستمرار بما يتماشى مع التطورات التكنولوجية، ولم يتدخل المشرع في تحديد القيمة الاقناعية للدليل أمام القضاء، ويكون بذلك للقاضي حرية قبول الدليل وتقدير قيمته، بشرط يقينية الدليل ومناقشته وفقا لمبدأ شفوية المرافعات، ويبقى الشك في الدليل الالكتروني ناتج عن عوامل تؤثر في حجيته نتيجة مبناه العلمي وأساسه التقني، فطبيعته

الفنية تتطلب الاستعانة بوسائل تمكن من فحصه للتأكد من سلامته وصحة اجراءات الحصول عليه.

- صعوبة التعامل مع المتعاملين الاقتصاديين بسبب نقص معلومات الشرائح وعشوائية بيعها خاصة في مراحلها الأولى لتقديم الخدمات والتنافس بين المتعاملين، وهو ما انجر عنه صعوبات في تحديد هويات مستعملي بروتوكول الانترنت، وصعوبة تحديد عنوان IPخاصة عند استعمال تقنية 3G، 4G.
- الاشكاليات التي تصادف اجراءات التحقيق من الناحية العملية، بسبب وجود ادوات تشفير للحاسب الآلي أو المعلومات، وقدرات المجرم على اخفاء أو ازالة الأدلة، أو تهيئة الجهاز للتفجير بمجرد تشغيله مما يحول دون استخلاص الدليل اللازم في التحقيقات، أو كبر حجم الشبكات المحتوية على معلومات يتطلب ضبطها، كما أن تجاوز الجريمة اقليم واحد مما يتطلب مباشرة التفتيش خارج الحدود الوطنية، والذي لا يمكن اللجوء له الا في إطار وجود اتفاقيات دولية أو وفقا لمبدأ المعاملة بالمثل بين الدول.
- تميز الجرائم المعلوماتية بخاصية اللاحدودية، توقع الدول بما فيها الجزائر في صعوبات التعاون الدولي في اجراء التحقيق في هذه الجرائم، منها اشكالية السيادة في حالة ارتكاب الجريمة في أكثر من اقليم.
- القصور في اجراءات المساعدة القضائية وبطء الاجراءات حيث أن المشرع الجزائري لم ينص على سبل بديلة للتعاون القضائي الدولي وان كان قد نص على انه إذا تعلق الامر بالجرائم المعلوماتية يجوز في حالة الاستعجال قبول طلب المساعدة القضائية الدولية إذا ورد عن طريق وسائل الاتصال السريعة كالفاكس والبريد الالكتروني.

- عدم وجود قنوات اتصال بين أجهزة التحقيق في الجرائم المعلوماتية بين مختلف الدول، وهو ما يستدعي انشاءها لتسهيل جمع الأدلة والمعلومات التي تفيد في التحقيق في الجرائم المعلوماتية.
- اختلاف النظم القانونية الاجرائية يوقع الدول في مشكلة امكانية استخدام الدليل الالكتروني في الاثبات، مما يتطلب اللجوء الى تقنيات خاصة في مجال التحقيق في الجرائم المعلوماتية.
- تعتبر آليات التعاون الدولي في مجال التحقيق في الجرائم المعلوماتية غير كافية ولابد من تطويرها من خلال تحديث الأنظمة والقوانين الجنائية –الموضوعية والاجرائية–بما يواكب التطورات التكنولوجية الحديثة.

التوصيات:

1- تدعيم الأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية في كل مرة بآليات وتقنيات ووسائل وأساليب جديدة تضمن المواجهة الفعالة.

2- تفعيل دور المجتمع المدني ووسائل الاعلام في التحسيس بخطورة الجرائم المعلوماتية وضرورة التبليغ عنها.

3- تحيين النصوص القانونية بما يضمن مواكبة السرعة والتطورات التكنولوجية الهائلة، لتفادي أي قصور تشريعي وتجاوز الثغرات القانونية التي قد تحول دون ضمان غايات المواجهة الفعالة للجرائم المعلوماتية.

4- ضرورة اعتماد المشرع الجزائري على نصوص خاصة بالأدلة الالكترونية والنص عليها صراحة كأداة للإثبات الجنائي، مع ضرورة النص على معايير وتقنيات تساعد أجهزة العدالة الجنائية، للتعامل مع هذه الأدلة دون تلفها أو ضياعها.

5- تعديل مواد قانون العقوبات خاصة المتعلقة بتهديد الأشخاص وابتزازهم، والمتعلقة بحرمة الحياة الخاصة، بما يتماشى مع التطورات التكنولوجية واضافة الآليات الالكترونية المستعملة في هذه الجرائم، أو سن قانون مستقل خاص بالجرائم المعلوماتية.

6- مواكبة التطورات التقنية في المجال المعلوماتي بتطوير نظم العدالة الجنائية، وعقد تدريبات وتكوينات متخصصة للأجهزة المكلفة بالتحقيق في الجرائم المعلوماتية، وتطوير مهارات المحققين في سبيل الكشف عن الجرائم المعلوماتية كسبيل ناجع للحد من الاجرام المنظم العابر للحدود.

7- ينبغي على مقدمي خدمات الانترنت في كل ولاية أو قطاع، اعتماد نقاط بيع محددة ومعتمدة، ودون عشوائية، واقامة حد اقصى لعدد الشرائح المستخدمة من قبل الشخص الواحد.

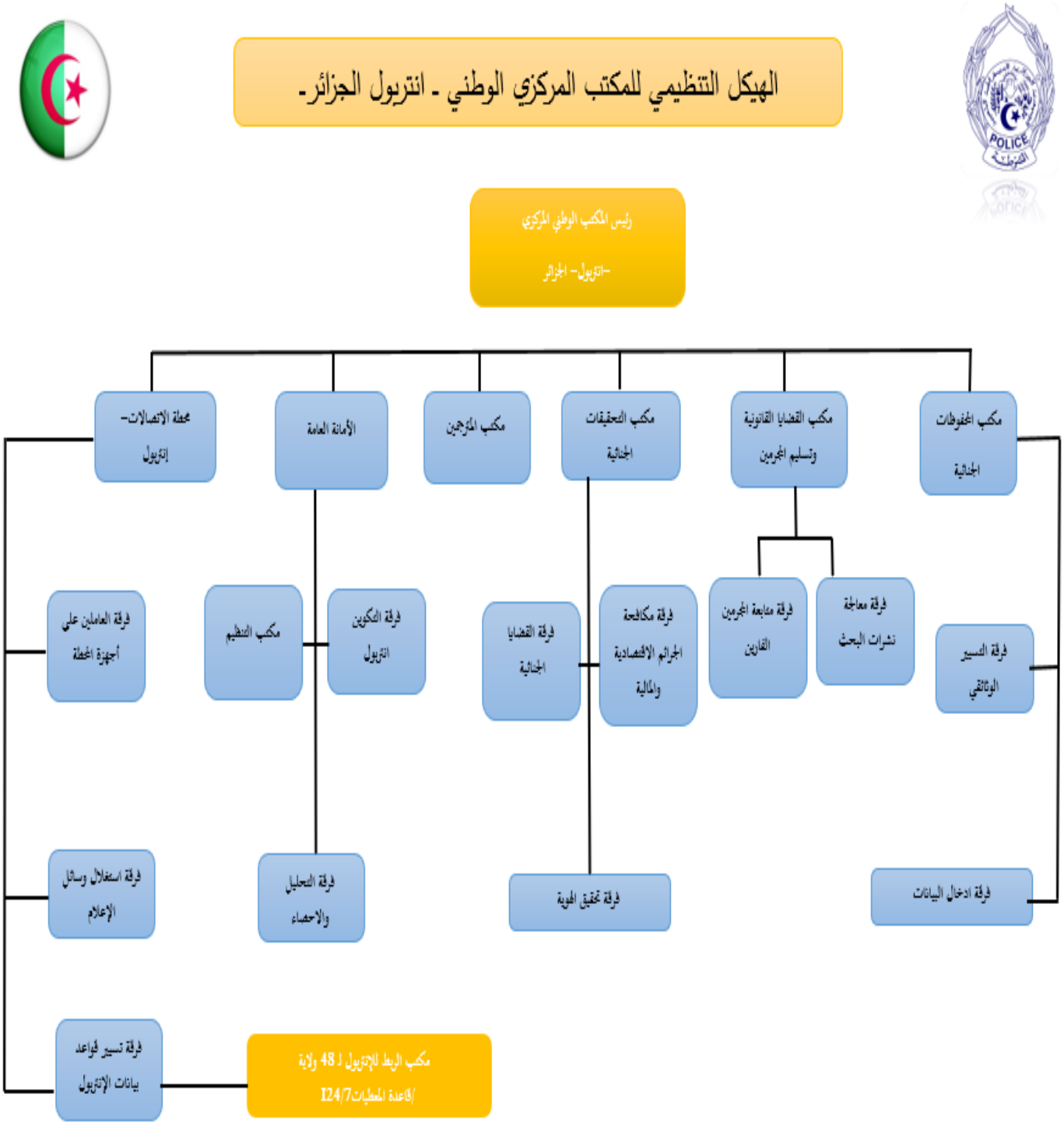
8- تظافر الجهود الوطنية والدولية في تسهيل جمع الأدلة الالكترونية مع مراعاة النواحي الفنية والقانونية.

9- الاستفادة من تجارب الدول المتقدمة الرائدة في المجال المعلوماتي.

10- تفعيل دور التعاون الدولي في مجال تسليم المجرمين والمساعدة القضائية المتبادلة، عن طريق ابرام اتفاقيات دولية واقليمية، ثنائية أو جماعية، واستخدام تقنيات تحقيق خاصة واقرار اجراءات مستحدثة في مجال المساعدة القضائية بين الدول، والاستجابة لمقتضيات التكافل والتعاون بين الدول في مجال التحقيقات.

11- وجوب توفر نظام اتصال قوي بين أجهزة التحقيق الوطنية والأجنبية لضمان التوصل الى المجرم المعلوماتي خاصة وأن بعض الدول لا تسمح بالدخول في نطاق قواعد البيانات التابعة لها.

الملاحـــــــق



ملحق 01: الهيكل التنظيمي للمكتب المركزي الوطني انتربول-الجزائر-

الجمهورية الجزائرية الديمقراطية الشعبية

مجلس قضاء .... وزارة العدل

محكمة...

نيابة الجمهورية

رقم:..... /إ ب / 2020

اذن بالتفتيـــش لمنظومة معلوماتية

-نحن السيد/ وكيل الجمهورية لدى محكمة...

-بعد الاطلاع على ارسالية فرقة البحث والتدخل لأمن ولاية... تحت رقم xx/xx الصادر بتاريخ 15-11-2020.

بخصوص التحقيق في قضية نقل وتخزين المخدرات بعرض عرضها للبيع على الغير بطريقة غير مشروعة في إطار جماعة اجرامية منظمة.

-بعد الاطلاع على طلب الاذن بالتفتيش داخل المنظومة المعلوماتية لغرض تفتيش حسابات الهواتف النقالة التي حجزت من المشتبه فيهم التالية:

هاتف نقال نوع oppoلون ازرق خاص بالمسمى xxx

هاتف نقال نوع plume p8 prأبيض اللون خاص بالمسمى xxx

هاتف نقال نوع condorp8 proأسود اللون خاص بالمسمىxxx

هاتف نقال نوع oppoاخضر اللون خاص بالمسمى xxx

اضافة الى حسابات موقع التواصل الاجتماعي فيس بوك المدمجة بالهاتف.

-بعد الاطلاع على المواد: 04-05-06-07-09 من القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

-حيث أن مقتضيات التحري والتحقيق القضائي تستدعي اللجوء الى المراقبة الالكترونية عل مواقع التواصل الاجتماعي فيسبوك بغرض تحديد وتفتيش حسابا الهواتف النقالة المملوكة للمشتبه فيهم والمذكورة أعلاه.

لهذه الأسباب:

نأذن لضابط الشرطة القضائية قائد فرقة البحث والتدخل لأمن ولاية ... بتفتيش المنظومة المعلوماتية الخاصة بموقع التواصل الاجتماعي فيسبوك المدمجة بالهواتف النقالة المذكورة أعلاه.

وتتبع المعطيات محل البحث وكذا المعطيات اللازمة لفحصها مع ضرورة استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة الالكترونية في الحدود الضرورية للتحريات والتحقيقات القضائية.

حرر ب ... في 15-11-2020

وكيل الجمهورية

ملحق 02: نمـــــــــــــــوذج اذن بالتفتيـــــــش لمـــــــــنظومة معـــــــــــــلوماتية

قائمة المصادر والمراجع

المصادر والمراجع باللغة العربية:

أولا: المصـــــــــــــــــادر:

- **الدستور:**

دستور الجمهورية الجزائرية الديمقراطية الشعبية ، الصادر بموجب المرسوم الرئاسي رقم 96-438، مؤرخ في 07 ديسمبر 1996، المتضمن ، ج ر، عدد 76، الصادرة بتاريخ 08 ديسمبر 1996، المعدل و المتمم، بالقانون رقم 02-03، المؤرخ في 10 أفريل 2002، ج ر، عدد 25، الصادرة بتاريخ 14 أفريل 2002، المعدل و المتمم بالقانون رقم 08-19، المؤرخ في 15 نوفمبر 2008، ج ر، عدد 63، الصادرة بتاريخ 16 نوفمبر 2008، المعدل و المتمم بالقانون رقم 16-01، المؤرخ في 06 مارس 2016، ج ر، عدد 14، الصادرة بتاريخ 07 مارس 2016، المعدل و المتمم بموجب المرسوم الرئاسي 20-442، المؤرخ في 30 ديسمبر 2020، ج ر، عدد 82، الصادرة بتاريخ 30 ديسمبر 2020.

- **الاتفاقيات:**

1-الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، بودابست، 2001.

2-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 08 سبتمبر 2014. أنظر ج ر عدد 57، الصادرة بتاريخ 28 سبتمبر 2014.

3-اتفاقية انشاء المنظمة العالمية للملكية الفكرية الموقعة باستكهولم في 14 يوليو 1967، والتي صادقت عليها الجزائر بموجب الأمر رقم 75-2 مكرر المؤرخ في 9 جانفي 1975، ج ر عدد 13، الصادرة بتاريخ 14 فيفري 1975.

-القوانين:

1-قانون رقم 09-04، المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 47، الصادرة بتاريخ 16 أوت 2009.

2-قانون رقم 15-03، المؤرخ في 01 فيفري2015، يتعلق بعصرنة العدالة، ج ر، عدد 06، الصادرة بتاريخ 10 فيفري 2015.

3-قانون رقم 18-04، المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر، عدد 27، الصادرة بتاريخ 13 ماي2018.

4-قانون رقم 18-07، مؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، عدد 34، الصادرة في 10 جوان 2018.

-الأوامر:

1- أمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

2- أمر رقم 66-155، الموافق ل 8 يونيو 1966، المتضمن قانون الاجراءات الجزائية، المعدل والمتمم.

3- أمر رقم 03-05، يتعلق بحقوق المؤلف والحقوق المجاورة، المؤرخ في 19 جويلية 2003، ج ر عدد 44، الصادرة بتاريخ 23 جويلية 2003.

4- أمر رقم 03-07، يتعلق ببراءات الاختراع، المؤرخ في 19 جويلية2003، ج ر، عدد 44، الصادرة بتاريخ 23 جويلية 2003.

-المراسيم:

1-مرسوم رئاسي رقم 04-183 المؤرخ في 26 جوان 2004، يتضمن احداث المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر، عدد 41، الصادرة في 27 جوان 2004.

2-مرسوم رئاسي رقم 15-261، المؤرخ في 8 اكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 53، الصادرة بتاريخ 8 اكتوبر 2015.

3-مرسوم رئاسي رقم 19-172، المؤرخ في 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر، عدد 37، الصادرة بتاريخ 9 يونيو 2019.

4-مرسوم رئاسي رقم 20-183، المؤرخ في 13 يوليو 2020، يتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 40، الصادرة بتاريخ 18 يوليو 2020.

5-مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، عدد 04، الصادر في 26 جانفي 2020.

6-مرسوم تنفيذي رقم 06-348، المؤرخ في 5 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر، عدد 63، الصادرة في 8 أكتوبر 2006.

- **القرارات القضائية:**

1- قرار جزائي، مجلس قضاء قالمة، الغرفة الجزائية، رقم الملف 03219/ 16، رقم الفهرس 16/03722، تاريخ القرار 11-09-2016.

2- قرار تعقيبي صادر عن محكمة التعقيب بتونس، عدد 6811، الصادر بتاريخ 22-02-2007.

3- قرار محكمة النقض الفرنسية، الغرفة التجارية، رقم الطعن: 07-17147 07-17196، بتاريخ 3 يونيو 2008.

- **الأحكام القضائية:**

1-حكم، محكمة قالمة، قسم الجنح، رقم الجدول 16/01976، رقم الفهرس 16/02413، تاريخ الحكم 30-06-2016.

2-حكم، محكمة قالمة، قسم الجنح، رقم الجدول: 10/07102، رقم الفهرس: 11/02248، تاريخ الحكم: 28-03-2011.

ثانيا: المـــــــــــــــــــــراجـع

- الكتب:

- الكتب العامة:

1- أحسن بوسقيعة، التحقيق القضائي، ط 10، دار هومة، الجزائر، 2012.

2- أعمر قادري، أطر التحقيق وفق أحكام نصوص الاجراءات الجزائية، ط 2، دار هومة، الجزائر، 2015.

3- جمال نجيمي، قانون الاجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، ط 1، دار هومة، الجزائر، 2016.

4- عبد الرحمن خلفي، محاضرات في القانون الجنائي العام (دراسة مقارنة)، دار الهدى، الجزائر، 2012.

5- عبد الرحمن خلفي، الاجراءات الجزائية، ط 3، دار بلقيس، الدار البيضاء الجزائر، 2017.

6- لخضر بوكحيل، الاجراءات الجنائية، مطبعة الشهاب، باتنة الجزائر، دون سنة.

7- محمد حزيط، مذكرات في قانون الاجراءات الجزائية الجزائري، ط 08، دار هومة، الجزائر،2013.

-الكتب المتخصصة:

1- أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية، القاهرة، 2015.

2- أحمد محمد عبد الباقي، الانترنت-التكنولوجيا وجرائم المستقبل، دار النهضة العربية، القاهرة، 2017.

3- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الاسكندرية، 2011.

4- حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، ط 1، دار النهضة العربية، القاهرة، 2017.

5- خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، عمان، 2011.

6- خالد مختار الفار، إسماعيل بابكر محمد، التحقيق الجنائي في جرائم الحاسوب، ط 1، دار عزة للنشر والتوزيع، السودان، 2010.

7- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم المعلوماتية، ط 1، دار الفكر الجامعي، الاسكندرية، 2009.

8- رامي متولي القاضي، مكافحة الجرائم المعلوماتية–في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط 1، دار النهضة العربية، مصر، 2011.

9- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، المكتب الجامعي الحديث، الاسكندرية، 2018.

10- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط 1، منشورات الحلبي الحقوقية، بيروت لبنان، 2012.

11- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية (دراسة مقارنة)، دار الكتب القانونية، القاهرة مصر، 2011.

12- طاهر محمود أبو القاسم، الجرائم المعلوماتية: صعوبات وسائل التحقيق فيها وكيفية مواجهتها، المنظمة العربية للتنمية الادارية جامعة الدول العربية، 2019.

13- عبد الوهاب جعيجع، الامن المعلوماتي وادارة العلاقات الدولية، دار الخلدونية، الجزائر، 2017.

14- علي جبار الحسيناوي، جرائم الحاسوب والانترنت، ليازوري، الاردن، 2008.
15- علي عدنان الفيل، اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة) المكتب الجامعي الحديث، مصر، 2011.
16- علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة (دراسة مقارنة)، المكتب الجامعي الحديث، مصر، 2019.
17- فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، 2003.
18- فهد عبد الله العبيد العازمي، الاجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2016.
19- كوثر مازوني، قانون الملكية الفكرية في مواجهة التكنولوجيا الحديثة التجربة الجزائرية، دار هومة، الجزائر، 2016.
20- لحمر عباس، البعد الاستراتيجي لتكنولوجيا المعلومات والاتصال، دار هومة، الجزائر، 2018.
21- لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، دار الحامد للنشر والتوزيع، عمان الأردن، 2014.
22- محمد أمين الشوابكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، ط 4، دار الثقافة، عمان، 2011.
23- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، الرياض، 2004.
24- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007.

25- محمد كرام، النصب المعلوماتي بين اكراهات النص القانوني والواقع العملي، ط 2، سلسلة النوازلي الالكترونية 05، مراكش، 2017.

26- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006.

27- منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية (الهم الأمني وحقوق الأفراد)، ط 1، المركز العربي للبحوث القانونية والقضائية، بيروت لبنان، 2018.

28- نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، منشورات دار الخلدونية، الجزائر، 2017.

29- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 2، دار الثقافة، عمان الأردن، 2010.

30- يوسف بن سعيد الكلباني، الحماية الجزائية للبيانات الالكترونية في التشريعين العماني والمصري (دراسة مقارنة)، ط 1، دار النهضة العربية، القاهرة، 2017.

31- يوسف مناصرة، الدليل الالكتروني في القانون الجزائي الطريق الى تحول أدلة الاثبات في المادة الجزائية –دراسة مقارنة–، دار الخلدونية، الجزائر، 2018.

32- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها) –دراسة مقارنة–، دار الخلدونية، الجزائر، 2018.

- **أطروحات الدكتوراه:**

1- احسان طبال، النظام القانوني للتحقيق الدولي في جرائم الكمبيوتر، أطروحة دكتوراه في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2013.2014.

2- جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2018.

3- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015-2016.

4- سامية دايخ، بطلان اجراءات التحقيق الابتدائي في التشريع الجزائري، أطروحة دكتوراه تخصص القانون الاجرائي كلية الحقوق والعلوم السياسية، جامعة مستغانم، 2016-2017.

5- فوزي عمارة، قاضي التحقيق، اطروحة دكتوراه العلوم، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، 2009-2010.

6- عادل بوزيدة، المسؤولية الجزائية لمتعهدي مواقع الانترنت، أطروحة دكتوراه تخصص القانون الجنائي الاقتصادي، كلية الحقوق والعلوم السياسية، جامعة تبسة، 2017.

- **المقالات:**

1- اسراء جبريل رشاد مرعي، الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي للدراسات الاستراتيجية، الاقتصادية والسياسية، ألمانيا، 2016.

2- خدوجة الذهبي، حق الخصوصية في مواجهة الاعتداءات الالكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 08، المجلد الأول، 2017.

3- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد 05، جامعة الوادي، الجزائر، 2012.

4- سوزان عدنان، انتهاك حرمة الحياة الخاصة عبر الانترنت (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد 03، 2013.

5- صبرينة جدي، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل، المجلد 24، العدد 02، عنابة، 2018.

6- صورية بورباية، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، المركز الديمقراطي العربي، العدد الأول، ألمانيا، 2019.

7- عادل عبد العال ابراهيم خراشي، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون، دقهلية، العدد 16، مجلد 1، 2014.

8- عبد الحميد عمارة، استخدام تقنية المحادثة المرئية عن بعد في التحقيق والمحاكمة الجزائية، مجلة دراسات وابحاث المجلة العربية في العلوم الانسانية والاجتماعية، مجلد 10، العدد 3، 2018.

9- عربوز فاطمة الزهراء، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل للأبحاث القانونية المعمقة، العدد 34، 2019.

10- عز الدين طباش، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري (دراسة في ظل قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال

معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، العدد02، 2018.

11- عمار سلطان، السلطات الادارية المستقلة في الجزائر، مجلة جيل للأبحاث القانونية المعمقة، العدد 33، 2019.

12- فتحي بن جديد، حماية الحق في الخصوصية أثناء التعاقد عبر الانترنت، مجلة القانون، العدد الثالث، 2012.

13- كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11، العدد 01، 2015.

14- محمد الأمين البشري، الأدلة الجنائية الرقمية مفهومها ودورها في الاثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد 33، السعودية، 2002.

15- محمد أحمد سليمان، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 2، 2016.

16- محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، المجلد 1، العدد 1، الجلفة، 2016.

17- مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، المجلد 1، العدد 13، الجزائر، 2018.

18- مليكة أبو دبار، الاثبات الجنائي في الجرائم الالكترونية، المجلة الالكترونية للأبحاث القانونية، العدد 2، المغرب، 2018.

19- مليكة درياد، احكام تسليم المجرمين في قانون الإجراءات الجزائية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 1، 2019.

20- ميسون خلف الحمداني، علي محمد كاظم الموسوي، الدليل الرقمي وعلاقته بالمساس بالحق في الخصوصية المعلوماتية أثناء اثبات الجريمة، جامعة النهرين، العراق، 2016.

21- نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة الأندلس للعلوم الانسانية والاجتماعية، العدد 13، المجلد 15، اليمن، 2017.

22- يوسف قجاج، خصوصية القواعد الاجرائية في مجال البحث عن الجريمة الالكترونية (دراسة مقارنة)، منشورات مجلة المنارة للدراسات القانونية والادارية. سلسلة البحوث الجامعية، العدد 14، دار السلام، الرباط، 2016.

- المداخلات:

1- المركز العربي للبحوث القانونية والقضائية، ضرورة التعاون الاقليمي والدولي في مكافحة جرائم المعلوماتية، ورقة عمل مقدمة الى الاجتماع السادس للمختصين بتقنية المعلوماتية في النيابات العامة في الدول العربية، بيروت، 2018.

2- طارق محمد الجملي، الدليل الرقمي في مجال الاثبات الجنائي، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، يوم 28-29-10-2009.

3- فضيلة عاقلي، الجريمة الالكترونية واجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال المؤتمر الدولي الرابع عشر الجرائم الالكترونية، طرابلس 24-25 مارس 2017.

4- هواري عياش، المعهد الوطني للأدلة الجنائية، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة، الجزائر، يومي 16-17 نوفمبر 2015.

5- عبد الرحمن حملاوي، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة الجزائر، يومي 16-17 نوفمبر 2015.

6- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الاثبات الجنائي بالأدلة الرقمية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، الرياض، 2007.

7- عز الدين عز الدين، الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة الجزائر، يومي 16-17 نوفمبر 2015.

- التقارير:

1-التقرير التفسيري للبروتوكول الاضافي لاتفاقية الجريمة الالكترونية بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، المنعقدة في ستراسبورغ في28 يناير 2003، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 189.

2-تقرير الأمين العام، أنشطة الاتحاد الدولي للاتصالات بشأن تعزيز دوره في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، مجلس الاتحاد الدولي للاتصالات، الوثيقة C18/18-A، جنيف، 2018.

3-تقرير مفوضية الأمم المتحدة السامية لحقوق الانسان حول الحق في الخصوصية في العصر الرقمي، الصادر بتاريخ 30 جوان 2014، تحت رقم A/HRC/27/37.

- **مواقع الانترنت:**

1- موقع الأمم المتحدة
https://www.un.org/ar/events/crimecongress2015/pdf/sixty.years.booklet.pdf، الدخول يوم 14-01-2021، على الساعة 00.23 الى 00.40.

https://undocs.org/pdf?symbol=ar/A/CONF.234/4، الدخول يوم 14-01-2021، على الساعة 00:55، 01.15.

2- موقع المنظمة العالمية للملكية الفكرية WIPO،
https://www.wipo.int/treaties/ar/convention/summary_wipo_conventio n.html، الدخول يوم: 15-01-2021، الساعة 14.00 الى 14.15.

3- عبد الله القحطاني، التحقيق الجنائي الرقمي 06، المجموعة السعودية لأمن المعلومات، hemaya groupe الرابط على اليوتوب: https://www.youtube.com/watch?v=JKxEccd8feA، تاريخ الدخول 06-06-2019، ساعة 10.21 الى 10.30.

4- مركز تدريب مختص بأمن المعلومات، على الرابط التالي:
https://www.isecur1ty.org، تاريخ الدخول 07-06-2019، ساعة 11.00 الى 11.30.

5- مباركة بن عمراوي، العقيد في الدرك الوطني جمال بن رجم للإذاعة: 95 بالمائة من الجرائم الالكترونية تم حلها بنجاح، موقع الاذاعة الجزائرية، https://www.radioalgerie.dz/news/ar/article/20180214/133919.html الدخول يوم 25-05-2019، على الساعة 05:34.

المصادر والمراجع باللغة الأجنبية:

Sources et Références en Français

- Sources

Code de procédure pénale - Dernière modification le 02 janvier 2021 - Document généré le 01 février 2021 Copyright (C) 2007-2021 Legifrance

https://www.legifrance.gouv.fr

- Références

1-Livres

1- Bellivier F, Eudes M, Fouchard I, Droit des crimes internationaux, 1 re édition, Thémis droit, France, 2018.
2- Bertrand A, Droit à la vie privée et droit à l'image, Litec, Paris, France, 1999.
3- Freyssinet E, La cybercriminalité en mouvement, Lavoisier, France, 2012.
4- Pradel J, Danti-Juan M, droit pénal spécial, 6e édition, éditions Cujas, paris, France, 2014.
5- Ghernaouti-Hélie S, La Cyberctiminalité le visible et l'invisible, Le savoir suisse, France, 2009.
6- Guy de Felcourt, L'usurpation d'identité ou l'art de la fraude sur les données personnelles, CNRS éditions, Paris, France, 2011.
7- Martin D, Frédéric-Paul M, Cybercrime : menaces, vulnérabilités et ripostes, 2e Edition, presses Universitaires de France, Paris, France, 2001.
8- Olivier B, Les investigations judiciaires internationales, Berger-levrault, 1er édition, France, 2014.
9- Quéméner M, Ferry J, Cybercriminalité Défi mondial, 2e édition, economica, paris France, 2009.
10- Roché S, En quête de sécurité causes de la délinquance et nouvelles réponses, Armand colin, Paris, France, 2003.
11- Sabouret N, comprendre l'intelligence artificielle, ellipses, France, 2019.
12- Sokolova K, Perez C, La Cybersécurité, Studyrama, France, 2018.

2-Thèses

1- BOOS R , La lutte contre la cybercriminalité au regard de l'action des états, thèse de doctorat, spécialité droit privé et science criminelles, faculté de droit, université de Lorraine, France, 2016.
2- Arredondo C, l'usurpation d'identité numérique sur internet : Etude comparée des solutions français, mexicaines et nord-américaines, thèse de doctorat, spécialité droit privé et sciences criminelles, faculté de droit, université Paris-Saclay, France, 2018.

3-Articles

1- Périllon P, L'usage des proxys dans une infrastructure réseau, travail de recherche bibliographique, université Claude Bernard, Lyon 1, 2008.
2- Thierry J B, Participation à une cyber-association de malfaiteurs, AJ Pénal-mensuel-, Dalloz, France, 2018.

References in English

-Articles

1- Broadhead.S, The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law and Security Review, 34 (6), 2018.
2- Kerr I, Gilbert D, Information ethics in the electronic age, Tom Mendina and Johannes J.Britz, 2004.
3- Lazetik G B, Koshevaliska O, Digital Evidence in Criminal Procedures (A comparative approach), Balkan Social Science Review, 2 (1), 2013.
4- Mugisha D, Digital Forensics: Digital Evidence in judicial System, international journal of cyber Criminology, 2019.

فهرس المحتويات

ملخص بالعربية:

ان خصوصية التحقيق في مواجهة الجرائم المعلوماتية، تظهر من خلال احترام المبادئ القانونية التي تضمن الموازنة بين فاعلية التحقيق وضمان حقوق الدفاع، وبين تنظيم القواعد الاجرائية لمواجهة الجرائم المعلوماتية وتكريس الحق في الخصوصية، ومراعاة قواعد الشرعية الإجرائية، ومشروعية الدليل الالكتروني في الاثبات الجزائي. وفي سبيل ذلك أنشأت أجهزة متخصصة تتطلب الالمام بمهارات التأهيل التكنولوجي واتقان استخدام الوسائل التقنية المادية والإجرائية، وحسن التعامل مع الأدلة الالكترونية لضمان فاعلية التحقيق في مواجهة الجرائم المعلوماتية.

وفي سبيل نجاعة التحقيق في مواجهة الجرائم المعلوماتية تدخل المشرع الجزائري باعتماد قواعد اجرائية مستحدثة تدعم الإجراءات العادية بغرض تمكين الجهات المختصة من الوصول الى الجريمة المعلوماتية والدليل المناسب لإثباتها. ولما تتميز به الجرائم المعلوماتية من امكانية عبورها للحدود الوطنية يقتضي تطوير سبل التعاون الدولي مع تبادل الخبرات والتدريب المستمر.

الكلمات المفتاحية:

التحقيق، الجرائم المعلوماتية، الأدلة الالكترونية، الحق في الخصوصية، التعاون الدولي

Résumé en Français :

La spécificité de l'enquête face à la cybercriminalité se traduit par le respect des principes juridiques qui assurent un équilibre entre l'efficacité de l'enquête et la garantie des droits de la défense d'une part et l'organisation de règles de procédure et la consécration du droit à la vie privée ainsi que le respect des règles de légalité procédurale et la légitimité des preuves électroniques d'autres part. À cette fin, des organes spécialisés, qui exigent une maîtrise de la gestion des moyens techniques et procéduraux et une bonne utilisation des preuves électroniques pour garantir l'efficacité de l'enquête, ont été créés.

Dans un souci d'efficacité de l'enquête face à la cybercriminalité, le législateur algérien a adopté de nouvelles règles procédurales qui soutiennent les procédures normales dans le but de permettre aux autorités compétentes d'élucider ces crimes et recueillir les preuves appropriées. La cybercriminalité peuvent être caractérisé par la possibilité de franchir les frontières nationales, il est donc nécessaire de développer des moyens de coopération internationale avec l'échange d'expériences et la formation continue.

Mots clés:

Enquêtes, Cybercriminalité, Preuves électroniques, Droit à la vie privé, Coopération internationale

Summary in English:

The specificity of the investigation to fight cybercrimes appears through respecting the legal principles that ensure an equilibrium between the effectiveness of the investigation and the guarantee of the rights of the defense. The organization of procedural rules and the consecration of the right to privacy, as well as respect for the rules of procedural legality and the legitimacy of electronic evidence must be consecrated. And for that, specialized organs require a mastery of the management of technical and procedural means and a good use of electronic evidence to ensure the effectiveness of the investigation.

For the sake of efficiency of the investigation of cybercrime, the Algerian legislator intervened by adopting new procedural rules that support normal procedures with the aim of enabling the competent authorities to elucidate crimes and collect the appropriate evidence. Cybercrimes have the characteristic of crossing national borders, so it is necessary to establish an international cooperation that exchanges experiences and continuous training.

Key words:

Investigation, Cybercrimes, Electronic Evidence, Right of privacy, International cooperation