وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

المرجع:.....

قسم: القانون العام

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجرائم الالكترونية عبر وسائل الاتصال

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق.

التخصص: قانون جنائي وعلوم جنائية

من إعداد الطالب(ة):

بوزايدة فاطيمة كوثر

تحت إشراف الأستاذ(ة):

أ/ زاوي عبد اللطيف

أعضاء لجنة المناقشة

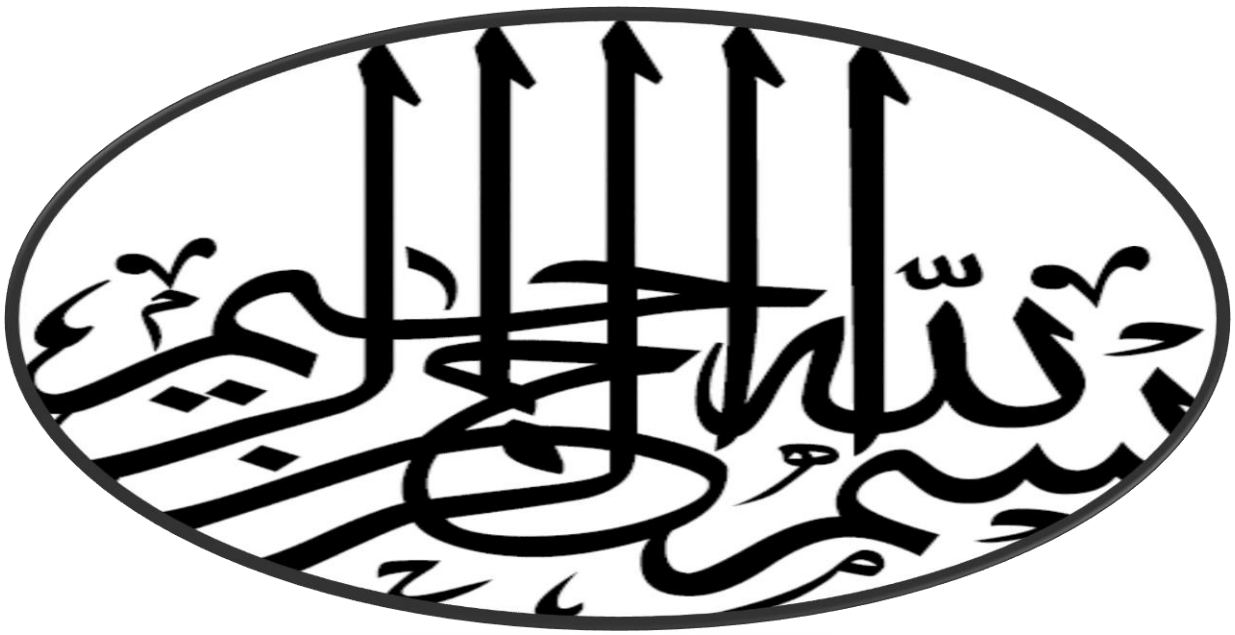
الأستاذ(ة).....بلبنة محمد.....رئيسا

الأستاذ(ة)..... زاوي عبد اللطيف ..... مشرفا مقررا

الأستاذ(ة).....مشرفي عبد القادر.....مناقشا

السنة الجامعية: 2023/2022

نوقشت يوم: 2023/07/04



الإهـــــداء

إلى من شرفني بحمل اسمه من كان يصنع من شقائه سعادتي إلى الذي كلما طلبت أعطاني مبتسما دون مقابل إلى سندي وموجهي ومسهل دربي إلى الذي بطيبته وحنانه الوافر وعطائه بدون حدود وصلت إلى ما أنا فيه إلى من انتظر ثمرة جهدي والذي مهما قلت ووصفت لن أعطيه حقه

أبي الغالي أطال الله في عمره وأدامه.

إلى التي ليس لها مثيل وإلى حبها في قلبها كبير والتي تحزن لحزني وتفرح لفرحي إلى التي يتسع صدرها حين تضيق بي الدنيا إلى التي شجعتني ولا تزال تشجعني على المواصلة الدرب فاستحقت أن تكون الجنة تحت أقدامها حفظها الله وأبقاها سندا لي

أمي الحبيبة

وإلى من هو سر قوتي وسبب فرحتي وسندي في الحياة الى من اقتسمت معهم الحلو والمرة

إخوتي الأعزاء

إلى كل من علمني حرف إلى كل من أضاءوا بعلمهم عقولنا أساتذتي الأفاضل أسال الله أن يحفظهم ويرعاهم ويجعلهم نورا للأمة

تشكرات

الله لا يطيب الليل إلا بشكرك ولا يطيب النهار إلا بطاعتك... ولا تطيب اللحظات إلا بذكرك... ولا تطيب الآخرة إلا بعفوك... ولا تطيب الجنة إلا برؤيتك

فالحمد الله الذي أعاننا وثبتنا لإتمام هذا البحث المتواضع حمدا يليق بجلال وجه وعظيم سلطانه والصلاة والسلام على أشرف المرسلين سيدنا محمد عليه أفضل الصلاة والسلام.

أتقدم بالشكر الجزيل للأستاذ المشرف " زاوي عبد اللطيف " الذي لم يبخل علي بإرشاداته وتوجيهات ونصائحه فله مني الشكر والاحترام.

وأشكر كل من ساعدني في هذا البحث من قريب ومن بعيد ولو بكلمة طيبة.

الى كل هؤلاء أرجو من الله العزيز القدير أن يجزيهم عنا خير الجزاء

قائمة المختصرات

باللغة العربية

ص: صفحة

ط: طبعة

د.ط: دون طبعة

ب.ن: بلد النشر

س.ن: سنة النشر

باللغة الأجنبية:

p: p
I: ed
D.T.: Without a print
B.N.: Country of publication
SN: Year of publication

مـــقـدمـــة

يعتبر الاتصال من السلوكات الانسانية المعقدة، تستعمل فيه كل الحواس وإمكانات الانسان الذهنية والنفسية في ان واحد استعمالا متناسقا ومنسجما حتى يتم تبليغ واستلام الرسالة، وتكمن أهميته في أنه المحرك الأساسي لكل العمليات الاجتماعية داخل المجتمع والمؤسسة، وبدونه لا يمكن تصور أي حركة إجتماعية وأي شكل من أشكال التبادل، ونصبح أمام حالة صامتة نجتهد فيها لفهم وفك الرموز.

يعد الاتصال عملية ووظيفة هامة من ضمن الوظائف الأساسية بالمؤسسة الاقتصادية، التي تتميز اليوم بتوجهها نحو الكبر والتعقيد بعدما كانت الوحدات الحرفية والمؤسسات الرأسمالية التي يملكها ويديرها نفس الشخص ذات أحجام ومهام بسيطة غير معقدة، فلما كانت المؤسسة في أطوارها الأولى بسيطة في إدارتها وفي الوسائل المادية والبشرية المستعملة، كانت عملية الاتصال سهلة ومستمرة ويومية، بين النظم والمالك وبقية الافراد العاملين معه، وفق طرق ووسائل شفوية عادة ومباشرة، إلا أن هذه الطرق ما فتئت تتطور وتتعقد بالمؤسسة الحديثة لتعقد تنظيمها ومستوياتها الادارية وزيادة عدد افرادها وضخامة مواردها، وهذا ما جعل المهتمين بالاتصال بين الكائنات البشرية يتجهون إلى دراسة هذا الموضوع فيها.

والعصر الحديث جعلها ضرورة من ضروريات التقدم الإنساني و المحرك الأساسي لها في مختلف مجالات الحياة، لأن هذا التقدم واكبه من جهة أخرى تطور الفكر والعقل البشري الإجرامي، لأن استخدامه لا يقتصر بين جانب الخير و جانب الشر نما في هذه الثورة، ويقتصر على الإنسان الشرير الذي قد يوصف كمجرم لسعيه وراء أطماعه لتحقيق أغراضه المشروعة منها والغير مشروعة لاسيما و أن هذه الظاهرة الإجرامية المتزايدة قد دقت ناقوس الخطر عن حجم المخاطر و الخسائر التي يمكن أن تخلقها خاصة و أنها جرائم ذكية تنشأ و تحدث في بيئة خاصة ألا و هي الإلكترونية الرقمية ومرتكبوها أشخاص متميزون و أذكياء ذوي الخبرة.

هذه الظاهرة الإجرامية ظاهرة تقنية تنشأ في الخفاء فأصبحت حكرا على الدول المتقدمة و تعددت إلى غير ذلك (الدول النامية)، مما زاد من أهمية هذه التكنولوجيا و التي عرفت بعصر المعلومات، وهذا ما دفع بالدول للعمل على الحد منها و الوقاية، من خلال قيام بمجالات نوعية و خلق وسائل شتى لمحاربتها بحيث أصبح تهديدها المباشر واضحا لهذا تكاثفت الجهود الدولية كالمنظومة الحقوقية لمواجهة الآثار الناجمة عن هذه الظاهرة و المترتبة على إساءة استخدام تقنية الاتصالات و المعلومات، ووضع سياسات جنائية تتنوع بين الوقاية و المواجهة من خلال سن مجموعة القوانين من أجل وضع حد لها.

فالجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان سلبي أو إيجابي فهي أيضا معنية بالمكافحة فكان لا بد من إيجاد طار قانوني مناسب لسد الفراغ الإجرائي، لذلك وضعت مجموعة من الإجراءات منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية عن طريق تعديل قانون الإجراءات الجزائية لتقني اجراءات خاصة تتماشى وأن وسائل وطبيعة الجرائم المستحدثة، ومنها الجريمة الإلكترونية، ومنها الإجراءات التي تطبق على الجريمة الإلكترونية فقط.

هذه الأخيرة قد أحدثت انقلابا هاما في النظريات التقليدية بما فيه نظرية الإثبات الجنائي و تحديد ما إذا كانت النصوص الجنائية التقليدية نواجه الأفعال الغير مشروعة التي ترتكب عبر شبكة الأنترنت، ومما سبق نطرح الإشكالية التالية:

كيف ساهمت وسائل الاتصال في مكافحة الجريمة الالكترونية؟

أهمية الموضوع:

تكمن أهمية البحث أساسا في كون الجريمة الإلكترونية جريمة يمتد تأثيرها إلى جميع الأصعدة الارتباطات بتطور تكنولوجيا الإعلام والاتصال والتي تستخدم في جميع مجالات

الحياة سواء من طرف الأفراد أو المؤسسات، واتخاذ تدابير اللازمة لحماية المجتمع من هذه الجريمة ومكافحة المجرمين وهذا الصنف من الأشخاص.

أسباب اختيار الموضوع:

تم اختيار الموضوع بناء على:

أ- أسباب ذاتية:

- رغبة وميول شخصي لدراسة الموضوع
- موضوع يقع ضمن التخصص مناسب له.

ب- أسباب موضوعية:

- معرفة مدى الحماية التي يوفرها المشرع الجزائري للجريمة الالكترونية خاصة ما تعلق بوسائل الاتصال
- اثراء المكتبة الوطنية بمراجع في الموضوع.

4- المنهج المتبع:

نزولا عند متطلبات البحث العلمي، كما هو متعارف عليه في المواضيع القانونية التي تفرض علينا نوع المنهج المتبع، فقد اخترنا منهجا يلم بكل جوانب الموضوع هو المنهج الوصفي التحليلي الذي يهدف الى الالمام بالموضوع محل الدراسة من كل جوانبه.

تقسيم البحث: تم تقسيم البحث وفق الخطة الثنائية الى:

الفصل الأول: ماهية وسائل الاتصال والجريمة الالكترونية

الفصل الثاني: أليات مكافحة الجرائم الالكتروني

الفصل الأول:ماهية وسائل الاتصال والجريمة الالكتروني

تمهيد:

عرفت البشرية في نهاية القرن الماضي اتساعات وتزايدا مطردا لنطاق استخدام تقنية المعلوماتية في المجتمع، ونظرا للتطور السريع لهذه التقنية، فقد مكنت من استعمالات متعددة وفي جميع المجالات، مما أدى إلى ظهور نوع جديد من الجرائم أطلق عليها تسمية الجرائم المعلوماتية.

ولقد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة ونظرا لجسامة أخطارها وفداحة خسائرها وسرعة انتشارها، أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفئتين والمهتمين بأمن الصرح المعلوماتي، لتحديد مفهومها وخصائصها، والتمييز بينها وبين ما يقترب منها من ظواهر، ومعرفة العوامل المختلفة التي تتدخل في هذا التحديد.

المبحث الأول: مفهوم الجريمة الالكترونية

لقد ترتب على الاستخدام المتزايد لنظم المعلومات إلى نشوء ما يعرف بالجريمة الالكترونية، ولقد استخدمت عدة مصطلحات للدلالة على هذه الظاهرة الإجرامية فمنهم من يطلق عليها: الغش المعلوماتي، والبعض الآخر يطلق عليها اسم جرائم الحاسب الآلي، والآخر جرائم الكمبيوتر والانترنت أو الجريمة الالكترونية.[1]

إن الجريمة الالكترونية جريمة مستحدثة يعتمد مرتكبها على وسائل تقنية ويكون ذا دراية كافية باستخدام النظم المعلوماتية لذا فإن الإحاطة بمفهومها الدقيق لا يزال محل خلاف فقهي، فهي ظاهرة إجرامية مستحدثة تتميز عن الجريمة التقليدية، وتختلف عنها من حيث المفهوم.

المطلب الأول: تعريف الجريمة الالكترونية

تعددت التعريفات التي تناولت الجريمة الالكترونية، ويرجع ذلك إلي الخلاف الذي أثير بشأن تعريف هذه الجريمة، فالجرائم الالكترونية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة، وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات، وقد أحاط

[1]: قربوز حليمة ،الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2006_2009، ص12.

بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها. [1]

على الرغم من تنامي جهود التصدي لظاهرة الإجرام المعلوماتي إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة الالكترونية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق وجانب أخر عرفها على نحو موسع.

أولا: التعريف الضيق للجريمة الالكترونية

يعرف الفقيه الفرنسي (Mass) جريمة الكمبيوتر بأنها:" الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[2] وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال استخدم لهذا التعريف معيارين هما: الوسيلة، وتحقيق الربح المستمد من معيار محل الجريمة المتمثل في المال.

ويعرفها الفقيهان الفرنسيان (Vivant و Le Stant) بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب" هذا التعريف مستند من بين معيارية على احتمال جدارة الفعل بالعقاب وهو معيار غير منضبط ولا يستقيم مع تعريف قانوني وان كان يصلح هذا التعريف في نطاق علوم الاجتماع وغيرها.

[1] :أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الطبعة الرابعة، 2007، ص 104.

[2]: ابرهيمي سهام،مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2004، 2007، ص7.

وعرفها (كلاوس تايدومان) بأنها:"كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلي".[1]

ويرى البعض أن تعريف كلا من (Marwe)و(Ros Blat) جاءا مقصورين على الإحاطة بالظاهرة الإجرامية أما تعريف كلاوس تايدومان فيؤخذ عليه أنه بالغ في العمومية والاتساع، لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع.[2]

ثانيا: التعريف الموسع للجريمة الالكترونية

ذهب الفقيهان (Michel و Credo) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته.[3]

---

[1] :المرجع نفسه، ص 8.

[2]: عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت،الطبعة الأولى، دار الفكر الجامعي، مصر ،2006،ص98.

[3]: طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي ،جامعة الجزائر 1، كلية الحقوق ،2011،2012، ص6.

ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها:"كل سلوك اجرامى يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر".

ويعرفهاTièdementبأنها ":كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب " .

من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة المعلوماتية، حيث أن مجرد مشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة المعلوماتية.[1]

ويعرفها (David Tompson):"جريمة يكون متطلبا لاقترافها أن يتوفر لدى فاعلها معرفة تقنية الحاسب".[2]

والدكتور هلالي عبد الله أحمد يرى أنها:"عمل أو امتناع يأتيه إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا".

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الألي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدة سمات وحقائق، والتي انعكست بدورها على مرتكب

[1]: المرجع نفسه، ص 7.

[2]: عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002،ص4

هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي، وقد كان ظهور شبكة المعلومات وتطورها إلى الصورة التي أصبحت الآن عليها فيما يعرف بالأنترنت أثره في إعطاء شكل جديد للجريمة المعلوماتية: [1]

1- السمات الخاصة بالجريمة الالكترونية :

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح،سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة.

- **خصوصية الجريمة الالكترونية:** تتسم الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها، ويرجع ذلك إلى عدة أسباب من بينها:

وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.[2]

[1] : كحولة محمد وأخرون، جرائم المعلوماتية، مذكرة ماجيستير، مرجع سبق ذكره، ص 75.

[2] : كحولة محمد وأخرون، جرائم المعلوماتية، مذكرة ماجيستير، مرجع سبق ذكره، ص 76.

- **الطبيعة المتعدية الحدود للجريمة الالكترونية:**

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

كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة.[1]

فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة بينها ألاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في أن واحد، كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني

[1]: نائلة عادل، محمد فريد قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005، ص 29.

عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة.[1].

ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية".

تعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي التنسيق بين قوانين الدول المختلفة لضمان تحقق "مبدأ ازدواجية التجريم" فيما يتعلق بجرائم المعلوماتية.[2]

[1]: نائلة عادل، محمد فريد قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية وتطبيقية، المرجع السابق، ص 30.

[2] : المرجع نفسه، ص 31.

ونجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم. وإن كان المشرع قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات.

والذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

2- السمات الخاصة بالمجرم المعلوماتي:

لم يكن لارتباط الجريمة الالكترونية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين، وقد اختلف الباحثون في تحديد هذه السمات، ويعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة ، بالمجرم المعلوماتي بصفة خاصة. إلا أنه لا يخرج في النهاية عن كونه مرتكبالفعل إجرامي يتطلب توقيع العقاب عليه.[1]

فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه على درجة من العلم و المعرفة، وإن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي.[1]

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و يرمز إليها الأستاذ Parker بكلمة S.K.R.A.M و هي تعني :[1]

1. **المهارة:**

المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي ،والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين. إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال، بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.[2]

[1] :محمد خريط، مذكرات في قانون الاجراءات الجزائية الجزائري، دار هومة للنشر والطباعة، الطبعة 4، الجزائر، 2009، ص 47.

[2] : حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2005_2006. ص9

2. المعرفة:

فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته. كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي. فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

3. الوسيلة:

فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها.

4. السلطة:

فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها. وقد تتمثل هذه السلطة في الحق في استعمال الحاسب

الآلي أو إجراء بعض التعاملات، وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر. [1]

5. الباعث:

وراء ارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية،ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الانتقام من رب العمل أو أحد الزملاء، حيث يفرق مرتكبي هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية لأخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.

[1] : المرجع نفسه، ص 10.

المطلب الثاني: أركان الجريمة الالكترونية

تعد الجرائم الالكترونية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الأونة الأخيرة، وذلك بسبب الاستعمال السيئ للثورة التكنولوجية، مما دفع الكثير من الحكومات إلى إظهار اهتمام متزايد لمكافحة الجرم المعلوماتي وسد ثغرات الأنظمة المعلوماتية، والجريمة المعلوماتية كغيرها من الجرائم التقليدية تقوم على أركان وأساس قانوني سوف نتعرف عليه من خلال :

أولا: الركن المفترض

يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان جريمة من جرائم الاعتداء على هذا النظام.

ويؤدي توافر هذا الشرط إلى الانتقال للمرحلة التالية، إذ أن هذا الشرط يعتبر عنصرا لازما، ولذلك يكون من الضروري تعريف نظام المعالجة الآلية للمعطيات ومدى خضوع هذا النظام لحماية فنية.

1- تعريف نظام المعالجة الآلية للمعطيات:

هو تعبير فنِّ ي تقني متطور، يخضع للتطورات السريعة والمتلاحقة في مجال الإعلام الآلي، ولذلك لم يعرف المشرع الجزائري على غرار المشرع الفرنسي نظام المعالجة الآلية للمعطيات، فأوكل بذلك مهمة تعريفه لكل من الفقه و القضاء.

حيث قدمت المادة الأولى من الاتّفاقية الدولية للإجرام المعلوماتي تعريفا للنّظام المعلوماتي على النحو التالي:[1]

"يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتّصلة ببعضها البعض أو ذات صلة بذلك، ويقوم إحداهما أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات". ويقصد بـ "بيانات الكمبيوتر" أية عملية عرض للوقائع ،أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر، بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها".

ويكون نظام المعالجة الآلية للمعطيات في طور التّشغيل عند إرسال إشارة كهربائية نحو وحدة المعالجة المركزية، والتي تقوم بدورها بإرسال البرنامج المسئول عن تشغيل ذاكرة القراءة، هذه الأخيرة تقوم بالبحث عن المعطيات التي تسمح بتشغيل النِّظام المسئول عن البحث، ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة التي تقوم بمتابعة المراحل اللاّحقة .[2]

2- الحماية الفنية لأنظمة المعالجة الآلية للمعطيات:

تكفل بعض القواعد الأمنية الحماية لنظم المعالجة الآلية للمعطيات، كوضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من الأجهزة المختلفة، والتي يمكن عن طريقها معرفة

[1] :صغير يوسف، الجريمة المرتكبة عبر الأنترنت، المرجع السابق، ص 93.

[2]: عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2003، ص 187.

محتوى المعلومات التي يتم نقلها، ويتأتّى ذلك عن طريق حماية الكابلات والوصلات الكهربائية لارتباطها بالأجهزة، ومن بين هذه القواعد، أُسلوب يعتمد على توزيع العمليّات التي يقوم بها نظام المعالجة الآلية للمعطيات ونقلها إلى نظام احتياطي (مركز للمساعدة) عند الضرورة، ويلجأ إلى هذا الأسلوب عادة البنوك وشركات التّأمين، ويظلّ هذا الموقع سرا ويخضع لدرجة عالية من الحماية، ومن الأساليب المستعملة كذلك، الاعتماد على الاختبارات الفيزيولوجية للدخول إلى النِّظام عن طريق التحقّق من شخصية القائم بعملية الدخول عن طريق بصمة الأصبع أو نبرة الصوت أو شكل الأذن أو شبكية العين .[1]

لكن يبقى نظام التشفير لحماية المعلومات هو الأسلوب الواسع الانتشار، خاصة البيانات المتناقلة عبر الشبكات، كشبكات الإنترنت، لما تنطوي عليه من سرية البيانات الشخصية كالرسائل الإلكترونية وكذا البيانات الخاصة بالأعمال التجارية الرقمية.

ويقوم نظام التّشفير على تحويل المعلومات والبيانات إلى شكل رمزي غير مفهوم بدون مفتاح لحلِّ رموزه، يعرفه عادةً مرسل المعلومات والمرسل إليه، وفي داخل جهاز الكمبيوتر توجد أجهزة مهمتها التحقُّق من شخصية القائم بعملية الدخول عن طريق الشفرة .

[1]: خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، طبعة 1، الاسكندرية، 2009، ص 280.

فبالرجوع إلى نص المادة 394 مكرر[1] من قانون العقوبات، لا نجد إشارة إلى ضرورة خضوع النّظام للحماية الفنية حتى يتمتع بالحماية الجنائية، وكذلك الشأن بالنسبة للمادة 323-1 من قانون العقوبات الفرنسي، و يظهر من خلال الأعمال التّحضيرية لقانون 1988، المتعّلق بالمعلوماتية والمقتبسة منه المادة 323-1 ، أنه كان من المقترح ضرورة شمول النّص بهذا الشرط، ولكن اشتراط وجود حماية أمنية في نظام المعالجة الآلية للمعطيات لم يتم الاتّفاق عليه في المناقشات الأخيرة في البرلمان الفرنسي، ولذلك جاء النص خالياً من هذا الشرط، ووجد أن هذا الشّرط قد يؤدي إلى الحد من الحماية الجنائية للنظم غير المشمولة بتجهيزات أمنية داخل النظام.

ولذلك اكتفى المشرع الفرنسي في النَّص النِّهائي بأن يكون التوصل قد تم "بطريق الغش"، وهذا التَّعبير يترك تفسيره لقاضي الموضوع.[2]

وهذا ما فتح أبواب النِّقاش حول هذه النُّقطة من خلال ظهور رأيين مختلفين:

الرأي الأول: يقول بعدم جدارة الأنظمة التي لا تحميها نظم أمنية بالحماية الجنائية، كون أنه من غير المعقول حماية معلومات هامة تركها المسئولون عنها دون أي إجراءا تتكفل لها الحماية.

[1]: تنص المادة394مكرر من قانون العقوبات:"يعاقب بالحبس والغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

[2]: صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،2003 ، ص117.

ويقيس أنصار هذا الرأي جريمة الدخول غير المشروع في أنظمة المعالجة الآلية للمعطيات على جريمة انتهاك حرمة المنزل، حيث لا تقوم الجريمة لمجرد أن الدخول إلى المسكن قد تم بغير رضاء صاحبه، كترك مسكنه دون حماية بسبب عدم وجود أقفال أو أبواب أو نوافذ، فيجب أن يكون الدخول مصحوباً باستعمال وسائل تدلّ على عدم رضا صاحب المسكن.[1]

ويستند أنصار هذا الرأي إلى عدة أسباب تنصب جميعها في اتجاه واحد هو ضرورة أن يكون هناك نظم أمنية يتم اختراقها لامتداد الحماية الجزائية للمعلومات، وأول هذه الأسباب يتعلّق بالمادة 28 من القانون 78–17 لسنة 1978 الخاص بالمعلوماتية وحماية الحريات الفرنسي، حيث تتطلّب أن تكون الأنظمة مشمولة بتدابير أمنية لحمايتها ،والسبب الثاني يكمن في إقامة الدليل على قيام الركن المادي للجريمة وكذا التّحقُّ ق من توافر القصد الجنائي لدى مرتكبها، لأن اختراق الأنظمة الأمنيّة من طرف الفاعل يترك أثراً، و يؤكِّد طريق الغش والاحتيال الذي سلكه.

الرأي الثاني: فهو يذهب إلى أنه ينبغي حماية أنظمة المعالجة الآلية للمعطيات جزائيا بغض النظر إن كانت تتمتع بحماية النظم الأمنية من عدمه، ويقيس أنصار هذا الاتِّجاه جريمة الدخول غير المشروع على جريمة السرقة، حيث أن تمتُّع المال المسروق بحماية

[1] : عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، مرجع سبق ذكره، ص189.

صاحبه أو عدم تمتُّ عه بهذه الحماية لا يؤثّر في قيام جريمة السرقة، بغض النظر عن مقدار الصعوبة التي واجهت الجاني في تنفيذها، كما أن تطُّلب مثل هذا الشرط يضيق من تطبيق الحماية الجزائية، ويتجاهل الحالات التي يتم فيها الدخول إلى النّظام نتيجة خطأٍ قام به المبرمجون، أو المسئولون عن أمن النِّظام.

هذا الرأي هو الأقرب إلى الصواب استنادا إلى المبادئ العامة المستقرة في القانون الجنائي كحرفية النص، وعدم جواز تقييد النص المطلق أو تخصيص النّص العام، إلاّ إذا وجد نص يجيز ذلك، ولا يوجد في حالتنا نص خاص يقيد إطلاق النّص أو يخصص عمومه، وبالتالي يجب التزام حرفية النّص في التّفسير، فعدم ذكر المشرع لشرط الحماية الفنّية يعني أن المشرع أراد استبعاده.[1]

وأكدت محكمة استئناف باريس في حكم صادر لها في 1994/04/05 ،على أنه من غير الضروري لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية، وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسئول عن النظام.

[1]: صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، المرجع السابق، ص118.

ثانيا: الأركان الأساسية للجريمة المعلوماتية

متى ثبت توفر الشرط الأولي لقيام الجريمة المعلوماتية ألا وهو نظام المعالجة الآلية للمعطيات أمكن الانتقال إلى المرحلة التالية وهي البحث في توافر أركان أية جريمة من جرائم المعلوماتية.

1- الركن المادي:

يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات وهناك ثلاثة أشكال للاعتداء نذكرها فيما يأتي:

1- الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات :

نصت عليه المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي بالإضافة للمادة 394مكرر من قانون العقوبات بقولها: "يعاقب بالحبس من ثلاثة أشهر إلى سنة بغرامة من 50.00دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.0000 دج إلى 150.000دج ."

وعليه فإن هذا الشكل من الاعتداء على نظام المعالجة الآلية للمعطيات يتكون من صورة بسيطة للجريمة وأخرى مشددة، فأما الصورة البسيطة تقوم بمجرد الدخول أو البقاء غير المشروع.

ويقصد **بفعل الدخول** ظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات وبالتالي لا نقصد بالدخول الدخول بمفهومه المادي[1].

وتجدر الملاحظة أن المشرع لم يحدد وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ومنه تقع الجريمة بأية وسيلة أو طريقة تمت بها الدخول، فيستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر.

كما أن هذه الجريمة تقع من كل إنسان أيا كانت صفته، وكفاءته المهنية والفنية، فهذه الجريمة ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة.

في حين أنه يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.[2]

[1]:علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، مصر، 1999، ص120.

[2] : عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، مرجع سبق ذكره، ص192.

وتجدر الإشارة إلى أنه قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام، وقد يجتمعان، ويكون البقاء معاقبا عليه وحده حين يكون الدخول إلى النظام مشروعا.

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، في الحالة التي لا يكون فيها للجاني الحق في الدخول إلى النظام، ويدخل إليه رغم ذلك ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق الاجتماع المادي للجريمتين الدخول والبقاء غير المشروعين. [1]

إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، فإنها تحقق أيضا، وبصورة غير مباشرة حماية المعطيات أو المعلومات.[2]

أما الصورة المشددة تتحقق بتوافر الظرف المشدد المتمثل في حصول نتيجة الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

[1]: علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص121.

[2]: عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، مرجع سبق ذكره، ص193.

وقد نصت المادة 394 مكرر 2+3من قانون العقوبات على أن " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150000 دج.[1]

[1] : المادة 394 مكرر 2 و 3 من القانون رقم 20-06 مؤرخ في 28أبريل سنة 2020 المتضمن تعديل قانون العقوبات.

وعليه نستنتج من خلال ذلك أن هناك ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، وتربط بين هذين الظرفين علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع والنتيجة الضارة وإن لم تكن مقصودة.

ومنه فظرف التشديد يعتبر ظرف مادي يكفي أن توجد بينه وبين الجريمة الأساسية المتمثلة في الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره، إلا إذا أثبت الجاني انتفاء تلك العلاقة ويثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ.[1]

2- الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

نصت على هذا الشكل من الاعتداء المادتين الخامسة والثامنة من الاتفاقية الدولية للإجرام المعلوماتي، في حين أن المشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام، ويمكن رد ذلك لكون أن المشرع الجزائري قد اعتبر من خلال الفقرة ج من المادة الثانية من القانون 04/09 على أن برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية. [2]

[1]: صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، مرجع سبق ذكره، ص122.

[2]: تنص الفقرة ج من المادة الثانية من القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 07 لـ 2009.على ما

وقد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات والاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية، فإذا كان الاعتداء مجرد **وسيلة** فان الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء **غاية** فان الفعل يشكل جريمة الاعتداء العمدي على المعطيات.

وتشمل صورة الاعتداء العمدي على سير النظام فعلين يتمثلان في الآتي:

يتمثل **الأول** منها في فعل التعطيل، والذي يفترض وجود عمل إيجابي، مع العلم أن المشرع لم يشترط أن يتم التعطيل بوسيلة معينة فيستوي أن يتم التعطيل بوسيلة مادية ككسر الأجهزة المادية للنظام أو تحطيم أسطوانة أو عن طريق وسيلة معنوية تتم بموجب الاعتداء على الكيانات المنطقية للنظام كالبرامج والمعطيات وذلك بإتباع إحدى التقنيات المستعملة في هذا المجال مثل إدخال برنامج فيروسي، استخدام قنابل منطقية مؤقتة، جعل النظام يتباطأ في أدائه لوظائفه كما يستوي أن يقترن التعطيل بالعنف أم لا. [1]

أما الفعل **الثاني** يتمثل في **الإفساد** الذي يتم بكل فعل إلى تعطيل نظام المعالجة الآلية للمعطيات يؤدي إلى جعله غير صالح للاستعمال السليم وذلك من شأنه أن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها

3- الاعتداءات العمدية على المعطيات:

يلي:"منظومة معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"

[1]: أحسن بوسقيعة، التحقيق القضائي، دار هومة للطبعة للنشر والطباعة، طبعة 10، الجزائر، 2009، ص 124.

نصت عليها المواد 03،40،08، من الاتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع الجزائري في المادة394مكرر 1و394مكرر 2من قانون العقوبات[1]. فجرم في المادة الأولى الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، وجرم في المادة الثانية المساس العمدي بالمعطيات الموجودة خارج النظام، ويظهر هذا فيما يلي:

أ_ جرائم الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي

باستقراء المادة**394مكرر1**[2]نجد أن لهذه الجريمة صورتين تتمثل الأولى في الاعتداءات العمدية على المعطيات الموجودة داخل النظام أما الصورة الثانية تتمثل في المساس العمدي بالمعطيات خارج النظام نجد الاعتداءات العمدية على المعطيات الموجودة داخل النظام تتجسد في إحدى الأفعال الثلاثة:

الإدخال (L'intrusion)، المحو(L'effacement)، التعديل(modification La)

الإدخال l'intrusion: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل ويتحقق هذا الفعل في الفرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب

[1]: المواد 394 مكرر 1 و 2 من القانون رقم 20-06 مؤرخ في 28أبريل سنة 2020 المتضمن تعديل قانون العقوبات.

مبلغا من النقود أكثر من المبلغ الموجود في حسابه وكذلك الحامل الشرعي لبطاقة الائتمان والتي يسدد عن طريقها مبلغا (التاجر أو شخص يتعامل معه) أكثر من المبلغ المحدد له.[1]

وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب(فيروس–حصان طروادة – قنبلة معلوماتية زمنية)يضيف معطيات جديدة.

المحو l'effacement :يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

التعديل modification: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة gomme d'effacementأو برامج الفيروسات بصفة عامة، وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل.

مع الملاحظة أن المشرع لم يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يقوم الركن المادي، كما أن أفعال الإدخال والمحو والتعديل

[1] : www.despace.univ.dz تم زيارة الموقع بتاريخ 2023/05/22 على الساعة 23:45.

تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل.

ب_ أما صورة المساس العمدي بالمعطيات خارج النظام نص عليها المشرع الجزائري بموجب أحكام المادة394مكرر2 من قانون العقوبات[1]، وكرس بموجبها المشرع الحماية الجزائية للمعطيات في حد ذاتها لأنه لم يشترط أن تكون المعلومات داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا.

إذ نصت الفقرة الأولى من المادة394مكرر 2أن محل الجريمة يتمثل في المعطيات سواء كانت مخزنة في أشرطة أو أقراص أو معالجة آليا أو مرسلة عن طريق منظومة معلوماتية ، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

في حين أن الفقرة الثانية من المادة394مكرر 2جرمت أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من

[1]: تنص المادة 394مكرر2من بقانون العقوبات:" يعاقب بالحبس وبغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات محزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات فقد يكون الهدف من ذلك المنافسة غير المشروعة ،الجوسسة، الإرهاب، أو التحريض على الفسق ...الخ.[1]

2- الركن المعنوي:

بعد التطرق للركن المادي لجرائم الاعتداء الماس بالأنظمة المعلوماتية بمختلف أشكاله، نتطرق فيما يأتي للركن المعنوي الذي يتخذ كل الأشكال السابق ذكرها صورة القد الجنائي و نية الغش.

ففي صورة الدخول والبقاء غير المشروع داخل نظام المعالجة الألية للمعطيات فإن كل م فعل الولوج والتجول والبقاء داخل نظام المعالجة الألية للمعطيات لا يجرمان إلا إذا تم عدما، وقد نصت المادة الثانية من الاتفاقية الدولية للجرائم المعلوماتية في هذا الصدد أنه يمكن السماح للدولة العضو أن تشترط لقيام هذه الجريمة مجرد خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله.[2]

وبالتالي يلزم توفر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو فعل البقاء مع علمه بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوفر الركن المعنوي إذا كان دخول الجاني أو بقائه داخل النظام مسموح به، أو مشرع أو إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في البقاء أو نطاق هذا الحق كأن

[1] : أحسن بوسقيعة، الوجيز في القانون الجنائي العام، دار هومة للنشر والطباعة، طبعة أولى، الجزائر، 2010، ص 34.

[2] : المرجع نفسه، ص 35.

يجهل وجود خطر من جراء الدخول أو البقاء أو كان يعتقد أنه مسموح له بالدخول، فإذا توفر القصد الجنائي بعنصريه العلم والإرادة لا يتأثر بالباعث على الدخول أو البقاء فيضل القصد قائما ، حتى ولو كان الباعث هو الفضول أو اثبات القدرة على المهارة والانتصار على النظام.

وبالنسبة للنية تبرز من خلال طريقة التي يتم بها الدخول عن طريق خرق جهاز الرقابي الذي يحمي النظام، أما بالنسبة للبقاء فإنها تستنتج من خلال العمليات التي تمت داخل النظام، أما جريمة الاعتداءات على سير النظام المعالجة الآلية للمعطيات فإنها تعد بطبيعتها جريمة عمدية، إذ أنه من المفترض أن أفعال العرقلة لا تكون إلا عمدية، وهذا ما يميزه عن الاعتداء غير عمدي لسير النظام الذي يشكل ظرفا مشددا للجريمة والدخول والبقاء غير المشروع داخل النظام.

وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة، ويظهر ذلك جليا من خلال الأفعال المشكلة لهذه الجريمة، حيث لا يتصور أن يقوم الفاعل بالاعتداء على سير النظام المعالجة الآلية للمعطيات بعرقلته أو تعطيله أو إفساده عن غير قصد.[1]

كما أن جريمة الاعتداءات العمدية على المعطيات تعد بدورها جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم ولإرادة، إذ يجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه

[1] :خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سبق ذكره، ص 57.

الإجرامي يترتب عليه التلاعب في المعطيات، ويعلم أن ليس له الحق في القيام بذلك، وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.

كما يشترط بالإضافة إلى القصد الجنائي العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير، بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل، مع العلم بذلك واتجاه إرادة الجاني إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.[1]

وأخيرا جريمة استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية التي تتم بالقيام بأحد الأفعال المنصوص عليها في المادة 394 مكرر 2 من قانون العقوبات المتمثلة إما في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الانجاز في معطيات مخزنة أو معالجة مرسلة عن طريق منظومة معلوماتية أو حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، فإنه لا يمكن أن يتم هذا الاستخدام بغير علم وإرادة الفاعل مما يجعله لا محالة عمديا، إلا أن المشرع اشترط أن يكون ذلك بطريق الغش، وبالتالي فإن المشرع الجزائري يشترط توافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش في هذه الصورة كذلك.[2]

[1] : أحسن بوسقيعة، التحقيق القضائي، مرجع سبق ذكره، ص 65.

[2] : خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سبق ذكره، ص 63.

المبحث الثاني: مفهوم وسائل الاتصال

وسائل الاتصال هيَ الطُّرُق والأجهزة التي تُقرّب النّاس، وتسهّل حدوث التّواصل فيما بينهم و التي تسمى بالرسالة والتي عرفت توسّعًا كبيرًا خُصوصاً في الفترة الأخيرة من القرن الحادي والعشرين؛ أين ظهرت تقنياتٌ حديثةٌ ومتطوّرة في مجال الاتّصالات، فبعد الرسالة والتيلكس والفاكس والهاتف الذي تطور من الثابت الى الخلوي ظهرت شبكة الإنترنت وما تُتيحه من أساليب للاتّصال المتطورة والآنية على غرار مواقِع التّواصُل الاجتماعيّ، وتطبيقات المُحادثات، ورسائِل البريد الإلكترونيّة .

المطلب الأول: تعريف وسائل الاتصال

يختلف مفهوم الاتصال من تخصص لاخر، فعلماء الانتروبولوجيا يعرفونه على انه شبكة معقدة من المفاهيم الكاملة أو الجزئية بين أعضاء وحدات تختلف في حجمها وفي درجة تعقيدها، وتتراوح هذه الوحدات من أسرة صغيرة أو شخصين بينهما اتصال من نوع ما إلى جماعة هائلة العدد تربط بينها وسائل اتصال ممكنة أو متاحة، وأن هذه الشبكة المعقدة قد تبدو ظاهريا في شكل مؤسسات اجتماعية في صفتها الثابتة لكنها في الواقع ذات طبيعة اتصالية، وكل نموذج ثقافي وكل حركة وكل سلوك اجتماعي يتضمن اتصالا ضمنيا او صريحا[1].

وهناك تعاريف عدة للاتصال نورد من ضمنها التالي:

– يعرفه" Henry Albert "على أنه: نقل المعنى من شخص لاخر، من خلال العلامات أو الإشارات، أو الرموز من نظام لغوي مفهوما ضمنيا للطرفين.

– كما يعتبر ميلر" Miller.G"أن الإتصال يحدث عندما توجد معلومات في مكان ما، أو لدى شخص ما، ونريد ايصالها إلى مكان اخر أو شخص اخر.

[1] : زيدان عبد الباقي، أساليب ووسائل الاتصال، دار الأنجلو مصرية، القاهرة، ط1، 1991، ص38.

-يعرف" Cherry.C "الاتصال بأنه إستعمال الكلمات أو الرسائل، أو أية وسيلة مشاة للمشاركة في المعلومات حول موضوع أو حدث[1].

– كما يمكن تعريف الاتصال هو تلك العملية التفاعلية بين المرسل والمستقبل في إطار بيئة اجتماعية معينة، وهذا التفاعل يجعل من غير الممكن فهم جانب واحد من جوانب تلك العملية بمعزل عن الجوانب الاخرى، وان التفاعل والمشاركة بين المرسل والمستقبل يميز مفهوم الاتصال عن مفهوم الاعلام، ويجعل مفهوم الاعلام معبرا عن العملية الاتصالية لأنه يكون ذو اتجاه واحد.

– -ويعرف الاتصال ايضا بأنه العملية التي يتم من خلالها نقل رسالة ما من المرسل إلى المرسل إليه سواء كانت هذه العملية بين فردين أو بين جماعتين أو بين فرد وجماعة، أو بين تنظيمين عن طريق مجموعة من الرموز المعروفة لدى الطرفين، وذلك من خلال وسائل الاتصال المختلفة بحيث يكون غرضها تحقيق هدف معين يرمي إليه المرسل والذي قد يكون إخباريا أو إقناعيا، أو استعلاميا أو إصدار أوامر أو غيرها.[2]

والاتصال داخل المؤسسة او ما يعرف بالاتصال التنظيمي الذي يشمل كل العمليات التي يتم من خلالها إبلاغ الرسالة بين أطراف التنظيم جماعات وأفراد، سواء داخل التنظيم الرسمي أو التنظيم غير الرسمي، ولايمكن أن نتصور مؤسسة مهما كان نوعها بدون شبكة إتصال رسمية وحتى غير رسمية تستعمل مختلف الوسائل لتحريكها من أجل تحقيق أهداف معينة، وعملية الاتصال جزء ضروري من عملية التفاعل التي تتم بين الأفراد داخل التنظيم حتى أنه اعتبر ركيزة أساسية داخل التنظيمات الحديثة، ذلك أن نسبة كبيرة من وقت العمل اليومي تستغرق في عملية الاتصال بكل أشكاله[3].

---

[1] : المرجع نفسه، ص39.

[2] : زيدان عبد الباقي، أساليب ووسائل الاتصال، المرجع السابق، ص40.

[3] : ملفين. ل. دليفر، نظريات وسائل الاتصال، ترجمة كمال عبد الرؤوف، القاهرة، الدار الدولية للنشر والتوزيع، 1999، ص 211.

ومنه الاتصال هو العملية التي يتم من خلالها تبادل الرسائل بين طرفين أو أكثر بحيث يتفاعلون بمقتضاها فيما بينهم من خلال منبهات مختلفة يتم الرد عليها برموز متفق عليها سلفا، ويكون موضوع الاتصال قضية معينة أو معنى مجردا او واقعا معينا.

لا يمكن تصور أي مؤسسة بدون أي شكل من أشكال الاتصال، فالاتصال هو جوهر نشاط المؤسسة وهو الروح التي تحركها، بحيث أي نقص أو غياب أو أي تشويه للمعلومات يعني إضطراب وظائف المؤسسة، فالاتصال هو محور كل العمليات في المؤسسة رسمية كانت او غير رسمية، بحيث يترتب عليه فعالية الأداء من حيث اتخاذ القرارات وبناء الهيكل التنظيمي وفعالية القيادة وحركية الجماعات والدافعية والبيئة التنظيمية والتغيير التنظيمي والعلاقات العامة.

وعن طريق الاتصال يتم إصدار التعليمات الخاصة بانجاز المهام وتلقي التوجيهات والإرشادات، والرد على تساؤلات المرؤوسين وتقديم الاقتراحات لحل مشاكلهم وإمدادهم بالمعلومات الضرورية لوضع الاستراتيجيات وتنفيذها، وإمدادهم بالآليات الضرورية للتصحيح الذاتي للأخطاء واكتشافها[1].

ومن جهة أخرى يعتبر الاتصال نشاطا إداريا وتقنيا وعقليا ونفسيا واجتماعيا، وفي نفس الوقت يتوجب على القائمين عليه مراعاة التوازن بين هذه الاتصالات لضمان عملية الاستقرار في المؤسسة وتحقيق أقصى قدر من الفعالية، وهو نشاط رسمي وغير رسمي في ان واحد، ونشاط جماعي تفاعلي نلاحظه من خلال اندماج الأفراد في الجماعات، وتأثرهم وبخصائصها السلبية والايجابية، سواء المتعلقة منها بانجاز المهام أو بالعلاقات الاجتماعية المختلفة، لذا فأي عملية تغيير تنطلق من بناء إستراتيجية للاتصال داخل المؤسسة، ويمكن أيضا ابراز الاهمية التالية للاتصال[2]:

[1] : ملفين. ل. دليفر، نظريات وسائل الاتصال، المرجع السابق، ص212.

[2] : ملفين. ل. دليفر، نظريات وسائل الاتصال، المرجع السابق، ص213.

– يسمح الاتصال بنقل المعلومات، حيث أن هذه الأخيرة تؤدي دورا محددا في عملية إتخاذ القرار بالمؤسسة، فالمعلومات بالكمية والنوعية ترتبط بشكل مباشر بشبكة الاتصال وقنواēا وأعوانها

– يسمح بممارسة مختلف العمليات الادارية بالمؤسسة، فانطلاقا من عملية التخطيط، التنظيم، التنسيق، القيادة والرقابة وغير ذلك من الأنشطة التي تتوقف على الاتصال، والمرتبط بشكل كبير بالهيكل التنظيمي للمؤسسة، الذي يوضح المهام ومواقع المسؤولية وغيرها.

– ايصال مختلف المشاكل التي قد تنشئ نزاعات اجتماعية بين الافراد والجماعات بالمؤسسة، وكذا عملية الحل لهذه النزاعات.

– ربط المؤسسة بالعالم الخارجي، فالمؤسسة كنظام مفتوح بمحيطها الأمر الذي يستوجب ضرورة توفير شبكة اتصال تقوم باستقطاب المعلومات، التي تعتبر متغيرة ومستمرة والتي تفيد في التخطيط الاستراتيجي وفي أداء مختلف الأنشطة.[1]

المطلب الثاني: خصائص أنواع وسائل الاتصال

أولا: خصائص وسائل الاتصال

للاتصال جملة من الخصائص أو الميزات يمكن ابرازها في النقاط التالية[2]:

– أن الاتصال يمكن أن يتم بعدة طرق وليس فقط الطرق الكتابية أو اللغوية، حيث يمكن أن يكون إبراز أحاسيس أو معاني، تتم بواسطة سلوكات أو إشارات معينة.

– أن الاتصال له مستقبل ومرسل، وهدف هذا الاخير في العملية هو التأثير على المستقبل

[1] : المرجع نفسه، ص214.

[2] : مي عبد الله سنو، الاتصال في عصر العولمة، الدور والتحديات الجديدة، لبنان، الدار الجامعية للطبع والنشر، 1999، ص 29.

– ذا خلا الاتصال من وجود معنى ينتقل بين المرسل والمستقبل فلا يمكن القول أن هناك اتصالا، كما أن هناك ضرورة اتمام عملية الاستقبال للطرف الثاني كشرط لاتمام عملية الاتصال

– هدف الاتصال أيضا إلى تحقيق التكامل والتفاهم بين المتصلين، وهي من بين المهام ذات الاعتبار في المجتمعات الحديثة وخاصة في المؤسسة الاقتصادية[1].

ثانيا: أنواع وسائل الاتصال

توجده عده وسائل أو أساليب للاتصال، وسوف نقتصر هنا على ثلاثة وسائل مهمة:

1– **الوسائل الشفهية:**

وهي الوسائل لتي يتم بواسطتها تبادل المعلومات بين المتصل والمتصل به شفاهه عن طريق الكلمة المنطوقة لا المكتوبة مثل (المقابلات الشخصية، والمكالمات الهاتفية، والندوات والاجتماعات، المؤتمرات)، ويعتبر هذا الأسلوب أقصر الطرق لتبادل المعلومات والأفكار وأكثرها سهوله ويسراً وصراحة، إلا أنه يعاب أنه يعرض المعلومات للتحريف وسوء الفهم.[2]

2– **الوسائل الكتابية**:

هي الوسائل لتي يتم بواسطتها تبادل المعلومات بين المتصل والمتصل به عن طريق الكلمة المكتوبة مثل (الأنظمة والمنشورات والتقارير والتعاميم والمذكرات والمقترحات والشكاوى ...الخ) ، ويعتبر هذا الأسلوب هو المعمول به في أغلب المنظمات الحكومية ، و توجد شروط للرسالة المكتوبة وهي أن تكون كاملة، ومختصرة، واضحة وصحيحة.

[1] : المرجع نفسه، ص30.

[2]: مي عبد الله سنو، الاتصال في عصر العولمة، الدور والتحديات الجديدة، المرجع السابق، ص31.

وتتميز الوسائل الكتابية بمزايا أهمها: إمكانية الاحتفاظ بها والرجوع لها عند الحاجة و حماية المعلومات من التحريف وقلة التكلفة ، أما أهم عيوبها فهي : البطء في إيصال المعلومات ، تأكد احتمال الفهم الخاطئ لها خصوصاً عندما يكون للكلمة أكثر من معنى[1].

3- **الوسائل غير اللفظية**:

وهي الوسائل التي يتم بواسطتها تبادل المعلومات بين المتصل والمتصل به عن طريق الإشارات أو الإيماءات والسلوك (تعبيرات الوجه وحركة العينين واليدين وطريقة الجلوس ...ألخ) ، ويطلق عليها أيضاً لغة الجسم ، وقد تكون هذه التلميحات مقصودة أو غير مقصودة من مصدر الاتصال وتصل نسبة استخدامها في الاتصال ما يقرب من 90% من المعاني وبصفة خاصة في الرسائل التي تتعلق بالأحاسيس والشعور ، ويختلف فهم الرسائل غير اللفظية بسبب اختلاف الثقافات داخل المنظمة (المدرسة) وداخل المجتمع أيضاً.

[1]: المرجع نفسه، ص32.

الفصل الثاني: أليات مكافحة الجريمة الالكترونية عبر وسائل الاتصال

تمهيد:

إن طبيعة الجرائم الالكترونية بعناصرها ووسائل ارتكابها، قد تدفع المشرع الجزائي إلى إعادة النظر في كثير من المسائل الجزائية، خاصة فيما يتعلق بمسألة التحري والتحقيق وكذا الإثبات، ذلك أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لا بد أن يكون من طبيعة إلكترونية، وهو الأمر الذي يقودنا إلى الحديث عن مسألة قبول هذا الدليل أمام القضاء ومدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف والأخطاء، وكذا مصداقيته ومشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية، وقد تتأثر جرائم الفضاء الرقمي أثناء التحري والتحقيق فيها معوقات وصعوبات والتي سوف نتطرق إليها من خلال هذا الفصل.

المبحث الأول :وسائل التحري و التحقيق في الجريمة الالكترونية

لم يكن لدى الدول خيار آخر للتصدي لظاهرة الإجرام الالكتروني في بداية ظهورها إلا الاعتماد على النصوص الجزائية القائمة بمختلف فروعها الموضوعية و الإجرائية، وذلك تفاديا لإفلات الجناة من العقاب من جهة، وعدم وجود قواعد قانونية أخرى تتلاءم و طبيعة هذه الجرائم المستحدثة من جهة أخرى، ولكن بعد التطور السريع الحاصل في مجال المعلوماتية وما صاحبه من انعكاسات على الجرائم في الوسائل المستعملة لارتكابها والمحل الذي تقع عليه ونوع الجناة الذين يرتكبونها، جعل هذه القوانين غير مواكبة لها، وبالتالي أضحت غير مجدية .

ومما لا شك فيه، أن المشرع حينما أراد توسيع نطاق تطبيق إجراءات التحقيق التقليدية لمتابعة جرائم الفضاء الرقمي، فانه يقصد بها تلك الإجراءات التي تثير إشكالات وعقبات عملية تعود إلى خصوصية هذه الجرائم، كالتفتيش والضبط والمعاينة والخبرة، والتي هي في حاجة إلى تطوير وتحسين لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها، كسماع المتهم أو الشهود، الاستجواب والمواجهة، فإنها مستبعدة نظرا وجود أية صعوبات في اتخاذها استرشادا بذلك.

المطلب الأول :إجراءات التحري والتحقيق العامة ومدى سريانها على الجريمة الالكترونية

أولا: التفتيش في البيئة الرقمية

يقصد بمحل التفتيش، المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره و خصوصيته، والسر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة، كالمسكن أو سيارة أو رسائل، بالتالي فمحل التفتيش قد يكون أحد المواقع المذكورة مع مراعاة الإجراءات والشروط القانونية المقررة لكل موقع على حدة، وكلما كان المحل في جرائم الفضاء الرقمي هو الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية وحدات(Hard Ware) كوحدات المعالجة المركزية (processeur) ، وحدات الإدخال والإخراج، ووحدات التخزين ما يسمى بوحدة التحكم (Unité De Contrôle) ومكونات أخرى منطبق برامج النظام الأساسية والبرامج التطبيقية والبيانات المعالجة آليا، كما له أن

شبكات اتصالات بعدية سلكية ولاسلكية متواجدة على مستوى المحلي و الدولي، فان الأمر يتطلب منا البحث في مدى قابلية جميع هذه المكونات للتفتيش؟[1]

1- تفتيش المكونات المادية للحاسب:

ليس هناك خلاف على أن الولوج إلى المكونات المادية للحاسوب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الالكترونية و مرتكبيها يخضع للإجراءات التفتيش المألوفة، لأن حكم تفتيش هذه الكيانات المادية يتوقف أساسا على طبيعة المكان الذي تتواجد ما فيه إذا كان عاما أو خاصا، فإذا كانت موجودة في مكان خاص ك سكن المتهم أو أحد ملحقاته كان له حكمه، بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن و ملحقاتها وبالإجراءات والضمانات المقررة قانونا .

أما القانون الجزائري تشترط المواد من 44 إلى 47[2] من قانون الإجراءات الجزائية للقيام بإجراءات تفتيش المسكن في الجرائم المتلبس بها، و هذا بالحصول مسبقا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار بهذا الإذن قبل الدخول إلى المسكن والشروع في التفتيش في الفترة الممتدة من الخامسة صباحا إلى الثامنة على أن يتم التفتيش مساءا وبحضور صاحب المسكن أو ممثله وإن تعذر ذلك استدعى ضابط الشرطة القضائية القائم بالتفتيش شاهدين من غير الموظفين الخاضعين لسلطته.

كما يجب التمييز إذا كانت مكونات الحاسب منعزلة أم أنها متصلة بحواسيب أو أجهزة متواجدة في مكان آخر كمسكن الغير، ففي هذه الحالة يجب على المحقق وضع القيود والضمانات التي يشترطها القانون لتفتيش هذه الأماكن إذ أما كانت المكونات المادية للحاسوب متواجدة في أماكن عامة، سواء أكانت عامة بطبيعتها كالحدائق العامة والطرق

[1] : حملاوي عبد الرحمن، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، جامعة محمد خيضر، بسكرة، 2016، ص 02.

[2] : المواد من 44 إلى 47 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات

العامة، أم أماكن عامة بالتخصيص كمقاهي الانترنت ومحلات بيع وصيانة الحواسب، فإجراءات تفتيشها تكون وفقا للأصول الخاصة بتلك الأماكن.[1]

كذلك بالنسبة للمكونات الموجودة بحوزة شخص ما، فبغض النظر عن صفة هذا الشخص، مبرمجا كان أو عامل صيانة أو موظفا في شركة تنتج جرائم الحاسب الآلي، فإن تفتيش هذه المكونات يخضع لأحكام تفتيش الأشخاص، وبالشروط والضمانات القانونية المحددة لذلك.

ومما سبق يتضح أن تفتيش المكونات المادية لجهاز الحاسب و ملحقاته مثل لوحة بناء المفاتيح أو الشاشة أو الطباعة أو غيرها من الأشياء المادية المحسوسة، لا يثير أية مشاكل إجرائية أمام سلطات الاستدلال، إذ يسري عليه ما يسري على تفتيش الأشياء والأدوات المادية الأخرى من شروط وضمانات، وقت التفتيش والإذن بالتفتيش و الأشخاص القائمين بالتفتيش، والأشخاص المطلوب حضورهم عند التفتيش، مراعاة مع الاختصاص المكاني .

كما أن أجهزة القضاء المخول لها القيام بإجراء التفتيش سواء بصفة أصلية أو استثنائية يمكنها تفتيش المكونات المادية في الجريمة الالكترونية دون الحاجة إلى أن تكون متخصصة في الجوانب التقنية.[2]

2 – مدى صلاحية مكونات الحاسب المنطقية للتفتيش :

تعرف الكيانات المنطقية للحاسب بأنها" مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات"، وإذا كان الأمر قد انتهى إلى صلاحية مكونات الحاسب المادية كمحل يرد عليه التفتيش، فان امتداد ذلك إلى المكونات غير المادية أو المنطقية هو محل جدل فقهي كبير حول مدى صلاحيتها لأن تكون محلا للتفتيش تمهيدا لضبط الأدلة كون التفتيش وسيلة للبحث وضبط الآثار المتعلقة بالجريمة وتقديمها إلى المحكمة كدليل إدانة، لذلك يثور الشك والتساؤل حول إمكانية اعتبار البحث عن أدلة الجريمة الالكترونية في نظم الحاسب نوعا من التفتيش باعتبار أن البيانات

[1] : هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة بسكرة، 2015، ص 5.

[2] : هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المرجع السابق، ص 06.

الالكترونية أو البرامج في حد ذاتها تفتقر إلى مظهر مادي محسوس في المحيط الخارجي، ويستشعر الفقه صعوبة المسألة بالنظر إلى غياب الطبيعة المادية للمعلومات والبيانات، بما يجعلها تتنافى مع الهدف الذي يصبو إليه التفتيش ألا وهو البحث عن الأدلة المادية.[1]

ولقد سعى جانب من الفقه إلى التشكيك وفيه و تجنبه على نحو يسمح بتضمين التفتيش بمعناه التقليدي، البحث والتنقيب في نظم برامج الحواسب عن أدلة الجريمة الالكترونية وان كانت هذه النظم البرامج عبارة عن نبضات أو ذبذبات إلكترونية حجتهم في ذلك هي أنه أو موجات كهرومغناطيسية إلا أنها قابلة للتسجيل والتخزين والتحميل على وسائط و دعائم مادية معينة، ولها كيان مادي محسوس من خلال استشعارها وقياسها، لذلك فمن الممكن جدا إخضاعها لقواعد التفتيش التقليدية .[2]

وعلى النقيض من ذلك، يرى جانب آخر من الفقه بأنه من غير الممكن إخضاع مكونات الحاسب المنطقية لقواعد التفتيش التقليدية، لأن هذه القواعد وضعت في وقت لم تكن نظم المعالجة الآلية والحواسيب موجودة وتطبيقاتها غير معروفة، بالتالي فطبيعة هذه المكونات تتطلب إحداث قواعد تفتيش جديدة خاصة بها، أو على الأقل تعديل قواعد التفتيش المألوفة بشكل يجعلها تتلاءم أحكامها مع متطلبات هذه التقنية الجديدة .[3]

ولم يبق المشرع الجزائري مكتوف الأيدي تجاه المتغيرات التي تحدث في عالم التكنولوجيات الحديثة، بل قام بدوره باستحداث نصوص قانونية جديدة أجاز من خلالها تفتيش المكونات المنطقية والمعطيات المعلوماتية للحاسب، ومن بين هذه النصوص المادة 05 من القانون رقم 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4]، التي تسمح للسلطات القضائية المختصة ولضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص

---

[1] : محمد قدري حسن عبد الرحمن، جرائم الاحتيال الالكتروني، مجلة الفكر الشرطي، عدد 79 ، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011 ، ص159.

[2] : محمد قدري حسن عبد الرحمن، جرائم الاحتيال الالكتروني، المرجع السابق، ص160.

[3] : المرجع نفسه، نفس الصفحة.

[4] : المادة 05 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

عليها في المادة 04 من هذا القانون، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات.

رغم اعتبار التفتيش من الإجراءات الجوهرية في عملية التحقيق البحث عن حقيقة الجرائم إلا أن معظم القوانين الإجرائية حرصت على إحاطته بجملة من الضمانات القانونية، وذلك تفاديا لتعسف سلطات البحث والاستدلال وما يمكن أن يحدثه من اعتداء على حقوق وحريات الأفراد و حرمة مساكنهم وحياتهم الخاصة من جهة، وإحقاقا لحق الدولة ممثلة المجتمع في كشف غموض الجرائم ومتابعة مرتكبيها وتوقيع العقاب عليهم من جهة أخرى.

ثانيا:ضبط الأدلة في الجريمة الرقمية

يعتبر الضبط من إجراءات جمع الأدلة، وهو النتيجة الطبيعية التي ينتهي إليها التفتيش والأثر المباشر الذي يسفر عنه، ويقصد به وضع اليد على الأشياء المتعلقة بجريمة وقعت والتي تفيد في كشف الحقيقة عنها و عن مرتكبيها، و وضعها في إحراز مختومة وتقدم إلى الجهة القضائية المختصة كدليل إثبات. [1]

وتحصيل الأدلة في الجرائم الالكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته و الأقراص الصلبة و الأقراص والأشرطة الممغنطة و الطابعة و البرامج اللينة والمراشد، البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الانترنت مثل المودم، ففي هذه الحالة فلا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي، وقد يرتبط الدليل الالكتروني بالمكونات وإخضاعها لإجراءات الضبط والتحريز التقليدية المعنوية للحاسب، كمختلف برامج والبيانات المعالجة آليا والمراسلات والاتصالات الالكترونية التي يجري تبادلها عبر شبكة الانترنت والبريد الالكتروني، وهنا تثير الطبيعة المجردة لهذه المكونات جدلا فقهيا واختلافا تشريعيا كبيرا حول مدى إمكانية

[1] : ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار الحقوق، تخصص قانون جنائي، 2014، ص 71.

ضبطها وفقا لقواعد الضبط المألوفة، مع العلم أن الضبط بمفهوم هذه الأخيرة لا يرد إلا على الأشياء المادية .[1]

تنبه المشرع الجزائري بدوره لهذا القصور، وتبني في القانون رقم 04 -09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05[2] إجراءات مستحدثة خاصة بضبط وتحريز المعطيات والبيانات المعلوماتية، وغيرها من الأدلة الرقمية بما يتناسب وطبيعتها اللامادية، تحت عنوان" حجز المعطيات وخصص المعلوماتية "، و لها عددا من المواد التي نذكرها على النحو التالي :

- نصت المادة (06)على أنه " عندما تكتشف السلطات التي تباشر التفتيش في منظومة معلوماتية معطيات محزنة مفيدة في الكشف عن الجرائم ومرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع وفقا للقواعد المقررة في قانون الإجراءات الجزائية ".[3]
- أضافت المادة (07) [4]فيما يخص الحجز عن طريق منع الوصول إلى المعطيات بأنه " إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (06)أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى

[1] :سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، محكمة سيدي محمد، ص 11.

[2] : القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] : المادة السادسة من القانون رقم 04 -09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05.

[4] : المادة السابعة من القانون رقم 04 -09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05.

نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

أما بخصوص المعطيات المحجوزة ذات المحتوى المجرم فنصت الماد (08)[1]على أنه " يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك ".

بالإضافة إلى هذه التدابير، وضع المشرع الجزائري على عاتق مقدمي خدمات الانترنت جملة من الالتزامات تساعد سلطات التحقيق على ممارسة مهام التفتيش والضبط على الكيانات المعنوية للحاسب الآلي عندما تستدعي ذلك ضرورة التحقيق.

ويتضح من خلال النصوص السابقة، بأن المشرع الجزائري أدرك خطورة الجرائم الالكترونية وأن الجزائر ليست بمنأى عنها، فقام بتلافي القصور الموجود في قانون الإجراءات الجنائية فيما يخص ضبط الكيانات المنطقية للحاسب أسوة بالاتفاقية الأوروبية وتشريعات الدول المتقدمة، بل حتمية لا واعتقد أن موقفه هذا ليس اختيارا مفر منها ما دام قد أنه أجاز تفتيش هذه الكيانات، وهو ما يقتضي بحكم المنطق القانوني والعقلي ضرورة إباحة ضبطها لأن الغاية من التفتيش هو ضبط ما كل يفيد في كشف الحقيقة، بالتالي لا يعقل أن ينظم المشرع مرحلة ا م من رحل التحقيق ويغفل عن الأخرى .

والجدير بالذكر، أنه رغم محاولة استحداث قواعد وإجراءات جديدة تواكب الطبيعة الخاصة للأدلة المستمدة من البيئة الرقمية والالكترونية وتسمح بضبطها وتحريزها بشكل سليم.[2]

[1] : المادة الثامنة من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05.

[2] : أحمد مسعود مريم ، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال في ضوء القانون 09-04 مذكرة لنيل شهادة ماجستير في القانون الجنائي، كلية قصدي مرباح بجامعة ورقلة،2013، ص103.

ثالثا: المعاينة في الجريمة الالكترونية

تعرف المعاينة بأنها إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على ما كل قد يفيد من، فهي بذلك تعد من إجراءات التحقيق الابتدائي التي يجوز لسلطات الآثار في كشف الحقيقة .[1]

وأثناء التحقيق يتم اللجوء إليها من تلقاء نفسها كلما ترى في ذلك ضرورة لإجلاء الحقيقة، أو بناء على طلب من الخصوم، والأصل أن تجرى المعاينة بحضور أطراف الدعوى الجزائية، غير أنه يجوز للمحقق إجراءها في غيابهم نظرا لضياع أو تعديل الأدلة أصيلا من مصادر الأدلة، وللمعاينة أهمية بارزة في مجال التحقيق الجنائي لكونها مصدر المادية والفنية الراسخة والثابتة التي تكون دائما محل ثقة سلطات التحقيق و القضاء، ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة، فهي ناطقة بما أتاه شاهد على ما فعله الجاني دون انحياز أو تعديل أو نقصان، وحتى تأتي المعاينة بثمارها وتفي بأغراضها المنشودة، أحاطها المشرع بجزاءات جنائية توقع على كل من يتجرأ ويقوم بإحداث تغييرا على حالة الأماكن التي وقعت فيها الجريمة أو ينزع شيء منها قبل الإجراءات الأولية للتحقيق القضائي.[2]

باستثناء ما إذا كانت تلك التغيير أو نزع الأشياء للسلامة والصحة العمومية أو ستلزمها معالجة الضحية وفي هذا الشأن تنص المادة 43[3] من قانون الإجراءات الجزائية الجزائري على " :يحظر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، وإلا عوقب بغرامة من 200دج إلى 1000دج".

وتتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة،

---

[1] : نائلة عادل، محمد فريد قورة، جرائم الحاسب الألي، منشورات الحلبي الحقوقية، 2005، ص 233.

[2] : المرجع نفسه، ص 234.

[3] : المادة 43 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات

ذا كانت الجريمة واقعة على المكونات المادية للأجهزة الالكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص الممغنطة ، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعد أدلة مادية تدل على وقوع الجريمة وانتسابها لشخص معين، ثم ضبطها وضعها في أحد زرا مختومة تقدم للنيابة العامة .[1]

أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الالكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الانترنت فيكون الانتقال للمعاينة هنا افتراضيا الكترونيا، ويمكن للمحقق إجراء المعاينة الافتراضية أو الالكترونية بالولوج والانتقال إلى مسرح الجريمة عبر الانترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه، أو من خلال مقهى الانترنت أو إحدى أرقام مزود خدمات الانترنت.[2]

ويلتزم المحقق عادة قبل البدء في المعاينة الالكترونية بجملة من التدابير الفنية والتحفظية التي تساعده في القيام بمهامه على أحسن وجه هي كالتالي:[3]

-الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد ومواقع الأجهزة الالكترونية وشبكاتها وسائر ملحقاتها والنهايات الطرفية المتصلة بها المتوقع مداهمتها . -توفير الوسائل والإمكانات اللازمة من أجهزة برامج وأقراص صلبة ولينة التي يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتامين وحفظ المعلومات .

-تأمين التيار الكهربائي بشكل لا يتم التلاعب أو التخريب عن طريق قطع التيار او تعديل الطاقة الكهربائية التأكد من خلو المحيط الخارجي لمسرح الجريمة الالكترونية من أية مجالات لقوى مغناطيسية اتصالات التي يمكن أن تتسبب في محو البيانات المسجلة أو إتلاف الآثار الأخرى للجريمة .

---

[1] : أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط 2، 2007، ص100.

[2] : المرجع نفسه، ص 101.

[3] : علي عدنان الفيل ، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث ، القاهرة ، 2012 ، ص 69.

-التحفظ على محتويات سلة المهملات ومستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة قد ما يوجد عليها من بصمات إعداد فريق من المتخصصين و أهل الخبرة في مجال تكنولوجية الإعلام الآلي للاستعانة بهم عند الحاجة.[1]

رابعا: ندب الخبراء في الجريمة الالكترونية

تعرف الخبرة الفنية بأنها إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء، من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع جريمة أو نسبتها إلى المتهم . فهي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها بمعرفة فنية وعلمية لا تتوفر لديه .

وللخبرة الفنية دور كبير في إثبات الجريمة الالكترونية، لأنها تنير الدرب لسلطات التحقيق والقضاء و سائر الجهات المختصة بالدعوى الجزائية للوصول إلى الحقيقة وتحقيق العدالة الجنائية، لذلك ومنذ تفشي جرائم الفضاء الرقمي، تستعين سلطات التحقيق والإستدلال و المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال التقنية الالكترونية من اجل كشف غموض الجريمة وتجميع أدلتها والتحفظ عنها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق، حيث تعددت أنواع ونماذج نظرا الحواسيب وشبكات الاتصال بينها.[2]

وأصبحت العلوم والتقنيات المتعلقة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتشعبة، والتطورات في مجالها سريعة و متلاحقة لد رجة قد يصعب على المتخصص تتبعها واستيعابها، بل يمكن القول لا انه يوجد حتى الآن خبير يملك معرفة متعمقة في سائر أنواع الحاسبات وبرامجها و شبكاتها، أو قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها، لذلك ترك المشرع للمحقق الحرية الكاملة، وفي أية مرحلة رام من حل التحقيق ندب أي خبير يرى فيه الكفاءة الفنية اللازمة للاستعانة

---

[1] : علي عدنان الفيل ، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 70.

[2] : www.policemc.gov.bh/reports/2009/...7.../633843953272369688.doc تم زيارة الموقع بتاريخ 2023/05/21 على الساعة 23:15.

بخبرته، كما لأنها يوجد في القانون ما يلزمه بالاستجابة للمتهم ولا غيره من الخصوم إذا طلبوا ندب خبير، تنص الفقرة الثانية من المادة (143) من قانون الإجراءات الجزائية الجزائري[1] ، على ضرورة ندب قاضي التحقيق لخبير مختص، فإذا كانت الاستعانة بخبير فني في المسائل الفنية التقليدية أمرا واجبا على جهة التحقيق أو الحكم، فهي أوجب في مجال استخلاص الدليل الرقمي لإثبات جرائم الفضاء الرقمي، لتعلقها بمسائل فنية آية في التعقيد لا يكشف غموضها إلا بمتخصص بارع في مجال تخصصه، ذلك لأن الذكاء والفن لا يكشفه ولا يفهمه إلا ذكاء وفن مماثلين.

وتبرز أهمية الاستعانة بالخبير الفني لإثبات جرائم الفضاء الرقمي بشكل أكبر عند غيابه، فقد تعجز سلطات التحقيق والاستدلال عن إسقاط اللثام عن الجريمة وجمع الدليل بخصوصها لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة، وهو قد ما يؤدي إلى تدمير الدليل أو محوه بسبب الجهل أو الإهمال عند التعامل معه .

ولم يتخلف المشرع الجزائري إذ نص في المادة (05)[2] الفقرة الأخيرة من 04-09المتضمن القواعد الخاصة بالوقاية من الجرائم المتصل بتكنولوجيا الإعلام والاتصال ومكافحتها بأنه " يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص يراد له بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها قصد مساعدتها وتزويدها لبك المعلومات الضرورية لانجاز مهمتها "

وإن صياغة المشرع الجزائري لهذا النص بصيغة العموم " كل شخص له دراية"، أمر مقصود حتى يوسع دائرة المساعدة القضائية في مجال مكافحة جرائم الفضاء الرقمي لتشمل إلى جانب الخبير، جميع المتخصصين والمعاملين في مجال تكنولوجيات الإعلام

[1] : المادة 143 من القانون رقم 04 -09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05.

[2] : المادة 05 من القانون رقم 04 -09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05.

والاتصال، مثل مهندسي وذوي الشهادات العليا في الإعلام الآلي، ومقدمي خدمات الاتصالات الالكترونية، كمزودي خدمة العبور إلى الانترنت، مزودي خدمة الإيواء، مزودي خدمة الحوسبة و كل من دراية له في هذا المجال .[1]

ولم يتوقف المشرع الجزائري عند هذا الحد، بل قامت بإنشاء هيئات وأجهزة متخصصة في مواجهة جرائم الفضاء الرقمي مزودة بوسائل متطورة وتقنيات عالية، وجعلت من مهامها الأساسية انجاز الخبرات التي تحتاج إليها السلطات القضائية، نذكر منها مركز الوقاية من الإعلام الآلي والجرائم المعلوماتية ومكافحتها الذي أنشأته قيادة الدرك الوطني في عام2009 والمعهد لوطني للبحث في علم التحقيق الجنائي الذي أنشأ بموجب المرسوم الرئاسي رقم 432-04 المؤرخ في 20 ديسمبر 2004[2] وتم تنظيم المصالح والأقسام والمخابر فيه بموجب قرار وزاري والذي تضمن مصلحة الخبرات الخاصة بالدلائل مشترك مؤرخ في 2007/04/14 .

ونذكر كذلك القسم الخاص بالخبرة الرقمية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية المتواجد على مستوى المديرية العامة للأمن الوطني وتمتد مصالحها إلى بعض الولايات والذي يتولى تقديم الخبرة الفنية المتميزة في القضايا ذات الطابع الرقمي، بالإضافة إلى إنشاء مؤخرا ثلاث مخابر جنائية جهوية بشمال البلاد تابعة للأمن الوطني تضم عدة أقسام متخصصة بما فيها قسم الأدلة الالكترونية والرقمية.[3]

مما لا شك فيه أن الخبرة التقنية باعتبارها من إجراءات التحقيق تخضع لضوابط قانونية و أخرى فنية، وهذا ما سوف يتم إبرازه بالشكل التالي :

أولا : الجوانب القانونية للخبرة الإلكترونية

نظرا في مجال الإثبات الجنائي، حرصت معظم التشريعات على تنظيمها و إحاطتها بمجموعة من الضوابط حتى يكون لنتائجها حجية أمام القضاء، ومن ضمن هذه

[1] : ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري، مرجع سبق ذكره، ص 72.

[2] : المرسوم الرئاسي رقم 432-04 المؤرخ قي 20 ديسمبر 2004 وتم تنظيم المصالح والأقسام والمخابر فيه بموجب قرار وزاري والذي تضمن مصلحة الخبرات الخاصة بالدلائل مشترك مؤرخ في 2007-04-14 .

[3] : ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري، مرجع سبق ذكره، ص80.

الضوابط ما يتعلق بالخبير و منها ما يتعلق بالخبرة، فأما الضوابط الخاصة بالخبير، فهي كالتالي :[1]

-أ اختياره الخبير من جدول الخبراء: الأصل أن يختار الخبراء حسب التخصص من الجداول التي تعدها المجالس القضائية بعد استطلاع رأي النيابة العامة، ولكن استثناء في حالة عدم توفر الخبرة المطلوبة في جداول الخبراء وجهات التحقيق ليسوا مقيدين في أي من هذه الجداول.

ب- أداء اليمين القانونية:أوجب المشرع الجزائري على ضرورة أداء الخبير لليمين القانونية قبل مباشرة مهامه لا في المادة (145) من قانون الإجراءات الجزائية[2] وإن كان عمله باطلا على الخبير في كل مرة يختار فيها وقبل أداء مهامه أن يحلف اليمين القانونية، غير انه إذا كان الخبير المعين مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى ما قد دام أدى اليمين عند تقييده بالجدول أول مرة.

ولعل العبرة من حلف الخبير هي حمله على الصدق والأمانة في عمله، وبث الطمأنينة في نتائج خبرته التي يقدمها سواء بالنسبة لتقدير القاضي و الثقة ببقية أطراف القضية، علاوة على ذلك، يتعين على الخبير بعد تفرغه من أبحاثه وفحوصاته إعداد تقرير مفصل حول المسألة محل البحث ويبين فيه خلاصة ما توصل إليه من النتائج، وعلى الخبير إيداع تقرير خبرته لدى كتابة الجهة القضائية التي أمرت بالخبرة خلال الآجال المحددة في أمر التعيين وأجازا استبداله بغيره لم ما يطلب الخبير تمديد هذه الآجال منفصلا .

وفي حالة تعدد الخبراء ولم يصلوا إلى نتائج مشتركة يقدم المرجع كل منهم تقريرا وتقرير الخبير لا يكون ملزما للنيابة العامة أو المحكمة، إلا أن عدم الموافقة على التقرير يجب أن يكون مسببا، وفي هذه الحالة يجوز طلب خبرة تكميلية من الخبير نفسه وتمكينه الاستعانة بفنيين من أصحاب الاختصاص إذا تطلب الأمر ذلك بموجب طلب يقدمه لقاضي التحقيق ويعينوا بأسمائهم ويؤدون اليمين، ويرفق تقري رهم بتقرير الخبرة.

---

[1] : ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري، المرجع السابق، ص81.

[2] : المادة 145 من القانون رقم 04 -09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05.

وإذا توفرت الخبرة على الشروط المذكورة أعلاه تكون لها حجية نسبية أمام القضاء، لأن نتائج الخبرة ما هي في الواقع إلا استدلالات لإنارة قاضي الموضوع، أراء الخبير تقدم دائما بصفة استشارية ولا تلزم المحكمة فإن شاء القاضي أخد بالخبرة، ولم يشأ استبعاده، كما له أن يفاضل بين تقارير الخبرات ويأخذ منها بما يطمئن إليه ويطرح جانبا ما عداه ، فالكلمة الأخيرة تعود لقاضي الموضوع وحده عملا بمبدأ " القاضي خبير الخبراء."[1]

وتجدر الإشارة إلى انه وإن كان القاضي يملك سلطة تقديرية واسعة بالنسبة لتقرير الخبرة الذي يتعذر عليه تفنيدها والرد عليها يرد إليه، غير أن ذلك لا يمتد إلى المسائل الفنية البحتة التي، إلا بأسانيد فنية قد يصعب عليه فهمها واستنباطها بدون خبرة فنية أخرى للطبيعة الفنية و العلمية البحتة التي تتميز بها.[2]

ثانيا –الجوانب الفنية للخبرة الإلكترونية

نظرا للطبيعة الفنية و العلمية البحتة التي يتميز بها الجرائم الإلكترونية، فإن عملية تحري الحقيقة وتجميع الأدلة الرقمية فيها تعد من أصعب التحديات التي تواجه الخبير التقني، لذلك لازما عليه اعتماد تقنيات ومهارات علمية مهمة والاستعانة بوسائل متطورة لرفع هذا التحدي.

–أ **الوسائل العلمية لانجاز الخبرة الإلكترونية** : يعتمد الخبير حر ش في ملابسات الجريمة الالكترونية واستخلاص الدليل الرقمي الذي يساعده على الكشف عن المجرم الالكتروني على جملة من الوسائل العلمية، والتي تمثل في الغالب أدوات فنية تستخدم في بنية نظام المعلومات.[3]

[1] : أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سبق ذكره، ص129.

[2] : المرجع نفسه، ص130.

[3] : فهد الله عبد العبيد العازمي ، الإجراءات الجنائية المعلوماتية ، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق .بجامعة القاهرة، 2012 ، ص 266.

ونذكر منها ما يلي :[1]

- **برتوكول الانترنت (IP):** يسمى بعنوان الانترنت هو نظام يشبه عنوان البريد: العادي يعمل على تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها، فهو موجود بكل جهاز الكتروني مرتبط بشبكة الانترنت ويتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات، ويشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الأجهزة الالكترونية المرتبطة، والجزء يحدد الجهاز الذي تم الاتصال منه، وفي حالة وقوع جريمة الكترونية فيمكن للخبير إتباع المسار التراسلي سلي للبحث عن رقم الجهاز المستعمل في ارتكاب الجريمة، ومن ثم تحديد موقعه (IP) للبرتوكول ومنه معرفة الجاني .

-**نظام البروكسي (PROXY):** يشتغل هذا النظام كوسيط بين شبكة الانترنت ومستخدميها يضمن توفير خدمات الذاكرة الجاهزة، ويقوم هذا النظام على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق نظام البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، ويقوم بإرسالها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشبكة العالمية مرة أخرى، أما لم إذا يتم تنزيلها من قبل، فيقوم بتحويل ومن أهم مزايا هذا (IP) الطلب إلى الشبكة العالمية مستعينا في ذلك بأحد عناوين النظام أن الذاكرة المتوفرة لديه تحتفظ وتخزن كل عمليات التنزيل التي تمت عليه والتي يمكن أن تساعد الخبير على اقتناء أدلة إثبات مهمة، مما يجعل دور البروكسي قويا و فعالا في عملية إثبات الجريمة الالكترونية .

-**برنامج(Trace route):** يتم عادة إدراج هذا البرنامج ضمن نظم تشغيل الحاسب الرئيسية، ويعتبر ذا أهمية بالغة في الكشف الجنائي، إذ يحدد بدقة الأجهزة الالكترونية التي اشتركت في نقل البيانات على الانترنت بتحديد مسا تهارا وصولا إلى المرسل إليه، كما يمكنه أن يستدعى، ويحيط بالملفات التي تم الولوج إليها وكافة عمليات الاختراق والعبور أو التجاوز خلال الإعداد للجريمة، وكافة المعلومات المتعلقة بدخول أشخاص مواقع معينة وتحديد

[1] : www.osamabahar.com تم زيارة الموقع بتاريخ 2023/05/27على الساعة 00: 15.

مسارات تنقلاتهم فيها إلى غاية خروجهم من هذه المواقع، وعليه فكل هذه المسارات تتضم عادة آثار أو أدلة رقمية يمكن الاستدلال بها على الجريمة.[1]

-**أنظمة كشف الاختراق(IDS):** يكمن دور هذه الفئة من برامج مراقبة في العماليات التي تحدث على الأجهزة الالكترونية المرتبطة بشبكة الانترنت وتسجيلها فور وقوعها في سجلات خاصة داخل هذه الأجهزة، ومن بين هذه الأنظمة برنامج(hack Tracer) الذي يتكون من شاشة رئيسية تقدم للمستخدم بيانا شاملا بعملية الاختراق التي تتعرض لها جهازه، يذكر فيه اسم وتاريخ الواقعة والعنوان (IP) الذي تمت من خلاله عملية الاختراق واسم مزود خدمة الانترنت المستضيف للمخترق ورقم المنفذ والبوابة الخاصة وبيانات الشبكة التي يتبعها مزود الخدمة للمخترق بما فيها أرقام هواتفها .

- **برامج مراجعة العمليات الحاسوبية واسترجاعها:**برامج تستعمل المراقبة مختلف العمليات التي تجري على ملفات وأنظمة تشغيل حاسب معين بسواء حذفها أ وتسجيلها في ملفات برنامج (Recover).

تسمى(Logs) أ واسترجاع هذه الملفات في حالة محوها و ومن أمثلتها، وتأتي هذه البرامج إما مضمنة في أنظمة التشغيل البرامج أو مستقلة يتم تركيبها على أنظمة التشغيل، وفي كلتا الحالتين بد لا من تفعيلها وإعدادها للعمل مسبقا قبل وقوع الجريمة الالكترونية حتى تتمكن من تسجيل كل المعلومات المتعلقة بهذه الجريمة والتي من شانها أن تساعد الخبير في استنباط الأدلة المفيدة لإثبات الجريمة وانس بها إلى مرتكبها .

-**برنامج الدمج وفك الدمج (pkzip):** يستعين الخبير الالكتروني بهذا البرنامج عادة لفك البرامج التي قام المجرم الالكتروني بدمجها قصد التعرف على طبيعة البيانات التي يحتويها وتحليلها، ودمج البرامج هي تقنية عالية يستعملها المجرم الالكتروني لإخفاء معلومات معينة لا يمكن الاطلاع عليها إلا بعد فك الدمج .[2]

---

[1] : الموقع الإلكتروني السابق.

[2] : عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة والقانون، دار النهضة العربية، القاهرة، 2013 ، ص 44.

-**الذكاء الصناعي:** نقصد بالذكاء الصناعي تقنيات برامج الحاسب الآلي التي يستعين بها الخبير الالكتروني لحصر الأسباب والفرضيات المتعلقة بالجريمة، وجمع الأدلة الجنائية وتحليلها واستخلاص الحقائق منها، عن طريق عمليات حسابية يتم حلها بواسطة البرامج الحاسب الآلي صممت خصيصا لهدا الغرض، كبرنامج (Xtree Progold) الذي يستخدم للعثور على الملفات المبحوث عنها في أي مكان على الشبكة أو الأقراص الصلبة أو الأقراص المرنة المضغوطة، قراءة محتوياتها في صورتها الأصلية من اجل التحليل والتقوى.[1]

المطلب الثاني :الإجراءات الخاصة بالتحري والتحقيق في الجريمة الالكترونية

إذا كانت الثورة المعلوماتية قد أثرت على نوعية الجرائم التي صاحبتها بظهور أنماط مستحدثة التحقيق في هذه من الجرائم عرفت بالجرائم المعلوماتية، فإنها في المقابل أثرت على وسائل الجرائم، إذ أصبحت الطرق التقليدية التي جاءت بها نصوص قانون الإجراءات الجزائية غير كافية لاستخلاص الدليل بخصوص هذا النوع الإجرامي المستجد الذي يحتاج إلى طرق وتقنيات جديدة تتناسب مع طبيعته، يمكنها فك رموزه و ترجمة نبضاته و ذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لان تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة.

واعتبارا للطبيعة الخاصة للجرائم الالكترونية في عناصرها و وسائل وتقنيات ارتكابها، اضطر المشرع الجزائي إلى إعادة النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة التحري والتحقيق والإثبات، باعتبارها أهم موضوعات هذا القانون لأن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية والفنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية للتحقيق واستخلاص الدليل قادرة على القيام به، مما قد يؤدي في الغالب إلى إفلات العديد من المجرمين من العقاب[2].

[1] : : فهد الله عبد العبيد العازمي ، الإجراءات الجنائية المعلوماتية، مرجع سبق ذكره، ص 267.

[2] : أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سبق ذكره، ص134.

أولا :التسرب الالكتروني

تعرف المادة 65 مكرر 12 من القانون الإجراءات الجزائية الجزائري[1] التسرب على :انه "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكل بتنسيق العملية مراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل انطلاقا من هذا التعريف، يتبين أن التسرب عملية معقدة جدا تتطلب معهم أو شريك أو خاف"أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية .

لذلك اعتبار لهذه الضرورة تفطن المشرع الجزائري وجرد الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب.

ليس هذا فحسب، بل أحاط المشرع المسرب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضائها، منها ما ورد في المادة 65 مكرر 16[2] من قانون الإجراءات الجزائية بأنه" لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراء " .

وما تضمنته كذلك المادة 65 مكرر 17 من[3] القانون نفسه بأنه " إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب واصلة النشاطات المذكورة في المادة 65 مكرر 14[4] أعلاه للوقت الضروري

[1] : المادة 65 مكرر 12 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات

[2] : المادة 65 مكرر 16 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات

[3] : المادة 65 مكرر 17 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات.

[4] : المادة 65 مكرر 14 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات.

الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائية، على لا أن يتجاوز ذلك 4 أشهر. "

وعلى هدى ذلك، لا يجوز اللجوء لعملية التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة 65[1] مكرر وهي جرائم : المخدرات الجريمة المنظمة العابرة للحدود جرائم، تبييض الأموال و جرائم التخريب والإرهاب، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ويمكن تصور عملية التسرب في جرائم الفضاء الرقمي في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي ومشاركته في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو أنه طهرا في مجموعات أو نوادي الهاكر، فيها بمظهر طبيعي كما لو كان واحد مستخدما في ذلك أسماء وصفات مستعارة وهمية ظاهرا مثلهم قصد إستدارجهم والكشف عنهم وعن أعمالهم الإجرامية.[2]

أمر المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي:[3]

أولا-**الضوابط الإجرائية:** تتلخص الضوابط الإجرائية للتسرب الالكتروني في الإذن القضائي وكل ما يجب أن يتضمنه من أحكام، لا إذ يجوز للضابط أو عون الشرطة القضائية الغوص في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة والمتمثلة حسب أحكام المادة 65 مكرر 11 ق، إ، ج[4] في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لت فادي حدوث تجاوزات وتعسفات في استعمال هذا الحق .

---

[1] : المادة 65 مكرر من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات.

[2] : بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مرجع سبق ذكره، ص92.

[3] : المرجع نفسه، ص93.

[4] : المادة 65 مكرر 11 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات.

ولا يكفي أن يصدر الإذن بالتسرب من الجهة المختصة فحسب، بل لابد أن يكون مكتوبا، وإن كان هذا الإجراء باطلا، لأن الأصل في العمل الإجرائي الكتابة، وهو ما أكدته المادة 65 مكرر 15 ق، إ، ج[1] بنصها " يجب أن يكون الإذن المسلم طبقا تحت طائلة البطلان."

كما يشترط أن يتضمن الإذن بالتسرب جملة من البيانات التي يتوقف على تحديدها صحة الإجراء ذاته، كذكر نوع الجريمة محل عملية التسرب واسم ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وتحديد المدة المطلوبة لهذه العملية، والتي يجب ألا تتجاوز أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن الشروط نفسها، وفي الوقت ذاته يجوز للقاضي الذي أذن بهذا الإجراء أن يأمر بوقفه في أي حين قبل انقضاء الآجال المحددة.[2]

ثانيا-الضوابط الموضوعية :إلى جانب الضوابط الإجرائية المذكورة أعلاه أحاط المشرع عملية التسرب بضوابط أخرى موضوعية يمكن إيجازها في عنصرين أساسين :هما

-**العنصر الأول** : هو عنصر التسبيب، تضمنته المادة 65 مكرر 15 ق، إ، ج، ويتمثل في المبررات والحجج التي أقنعت الجهات القضائية المختصة لمنح الإذن بإجراء التسرب،وكذا الدوافع والأسباب التي جعلت ضابط الشرطة القضائية يلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكون ضمن موضوع طلبه الإذن.

- **أما العنصر الثاني:** فيتعلق بتحديد نوع الجريمة التي ينصب عليها الإذن بالتسرب والتي يجب 65 مكرر5على سبيل الحصر، وألا تخرج عن نطاق الجرائم السبع التي حددتها المادة إليها أعلاه.

[1] : المادة 65 مكرر 15 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات.

[2] : بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مرجع سبق ذكره، ص94.

2- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

قد عرف المشرع الجزائري الاعتراض بالتفصيل في المادة 65 مكرر5 من قانون الإجراءات الجزائية[1]، إذ اعتبر عملية مراقبة المراسلات بأنها " اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للانتاج والتوزيع، التخزين، الاستقبال والعرض ".

نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، أشكال، صور أو) الدعامة التي تنصب عليها (ورقية أو رقمية أو ،) الوسيلة المستعملة لإرسالها سلكية كانت (كالفكس أو تليغرام)، أم لاسلكية(البريد الالكتروني، الهاتف النقال ،) باستثناء الكتب والمجلات والرسائل والحوليات .[2]

والتي تعد مراسلات خاصة، وهذا ما أكدته المادة 02 فقرة " 6 من القانون رقم04 – 09[3] التي عرفت الاتصالات الالكترونية بأنها " أو سل إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة وبغض الكترونية "النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون أو علم موافقة المعنيين، وذلك لغرض التصنت، والتقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل المواجهة المتهم.

[1] : المادة 65 مكرر 5 من الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات.

[2] : بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مرجع سبق ذكره، ص95.

[3] :المادة 02 الفقرة 06 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ولعل من أهم المراسلات الالكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض غنيا لأدلة إثبات جرائم الفضاء الرقمي، المراسلات عبر البريد والمراقبة والتي تمثل المصدر الالكتروني، كون هذه التقنية من أكثر الوسائل الحديثة استخداما للاتصال عبر الانترنت ومجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون حواجز.[1]

فهو بمثابة نظام تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، كما يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي المستخدم، ولا يمكن الدخول إليه بسهولة لأنه محاط بحماية فنية.[2]

ثالثا: الحفظ و الإفشاء العاجلان للمعطيات المتعلقة بالسير

يعد الحفظ والإفشاء العاجلان للمعطيات المعلوماتية من الإجراءات المستحدثة و الوقائية التي بما ارتأت له أغلبية الدول فرضت بموجب القانون على مزودي خدمة الانترنت و هذا استنشادا الغربية لمتابعة الجريمة الإلكترونية و توقيع العقاب على الجاني، واسترشادا بذلك تضمن القانون الجزائري رقم04 -09[3] الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وبالتحديد في المادة (10) عددا من الالتزامات تفرض على مزودي خدمات الانترنت بتقديم المساعدة بخصوص العمليات التي ينجزونها للسلطات المكلفة بالبحث والاستدلال لأغراض التحقيق من بينها :حفظ المعطيات المعلوماتية المتعلقة بالسير ووضعها تحت تصرف القائمين بعملية التحقيق.

[1] : محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مرجع سبق ذكره، ص23.

[2] : محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مرجع سبق، ص24.

[3] : المادة 10 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

1. مفهوم الحفظ العاجل لمعطيات السير:

اعتماد على ما سبق ذكره يمكن اعتبار الحفظ على المعطيات الالكترونية بأنه قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل قصد تمكين جهات الاستدلال من الاستفادة منها واستعمالها لأغراض التحري و التحقيق .[1]

فعملية الحفظ إذا هي من مهام مقدمي الخدمات، الغرض منها حماية المعطيات التي سبق وجودها في شكل مخزن من ما كل يمكن أن يتسبب في إتلافها أو تجريدها من صفتها أو حالتها الأصلية، ولا تهم الطريقة التي يتم من خلالها الحفظ على المعطيات الالكترونية ولا الوسيلة القانونية المقررة لذلك، فالأمر متروك لكل دولة لتقدير النماذج التي رأتها ملائمة لوضع عملية الحفظ موضع التنفيذ، وينبغي التنويه في هذا الإطار إلى أن عملية الحفظ لا هنا تخص كل المعطيات الالكترونية بمختلف نماذجها، إنما تخص معطيات المرور فقط أو كما يسميها البعض حركة السير، التي عرف ها المشرع الجزائري في المادة (02)الفقرة الأخيرة من القانون رقم 04 -09[2] بأنها " أية معطيات متعلقة بالاتصالات عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات، مصدر الاتصال، الوجهة المرسلة إليها، والطريق الذي يسلكه، ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة".

[1] : قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مرجع سبق ذكره، ص 39.

[2] : الفقرة الأخيرة من المادة 02 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إلا أنه بالنظر إلى نص المادة 10فقرة1من القانون04-09[1] فإن المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتوى الاتصالات بشرط أن يكون في حينه ، وهو إجراء تسخير من طرف السلطات القضائية لمقدمي الخدمات المعنيين لجمع وتسجيل المعطيات المتعلق بمحتوى اتصالات أيا كانت (محادثات هاتفية أو مكالمات فيديو عبر مواقع الانترنت أو مراسلات كتابية على شكل SMS-MMS .[2]

ومن ضمن معطيات المرور التي يتعين على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية المختصة لأغراض التحقيق، تلك التي حددها المشرع الجزائري في المادة11من القانون04-09على النحو التالي:[3]

_المعطيات التي تسمح بالتعرف على مستعملي الخدمة

_المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال (كرقم التسلسلي لجهاز الاتصال ونوعه).

_الخصائص التقنية وكذا تاريخ و وقت و مدة الاتصال .

_المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها .

_المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم (كأرقام الهاتف مثلا أو عناوين بروتوكول الانترنت ، تحديد مكانهم)...

وإذا كان تحديد معطيات المرور قد يبدو أمرا سهلا عندما تكون تلك المعطيات مرتبطة بمقدم خدمة واحد، فالأمر غير ذلك عندما ترتبط بأكثر من مقدم خدمة، فغالبا ما يساهم عدد من مقدمي خدمات في نقل اتصال معين، ويحتفظ كل واحد منهم بجزء من معطيات المرور أو بعض أجزاء اللغز، مما يجعل تحديد مصدر هذا الاتصال ومنتهاه أم لا وهذه الأجزاء ضمها بعضها إلى البعض و اختبارها.

[1] : الفقرة الأولى من المادة 10 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] : قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مرجع سبق ذكره، ص 40.

[3] : المادة 11 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

لذلك عندما ترتبط معطيات المرور بأكثر من مقدم خدمة فالحفظ العاجل لهذه المعطيات يتم من خلالهم جميعا، سواء بناء على أمر منفصل لكل مقدم خدمة على انفراد أمر واحد يشملهم جميعا يتم إخطارهم به بالتعاقب، أو بناء على أمر يضم كل مقدمي الخدمات، ثم يطلب من كل مقدمي خدمة يصله الأمر بالحفظ، أن يقوم بإخطار من يليه بفحوى هذا الأمر.[1]

2. الإفشاء العاجل لمعطيات السير:

يعد هذا الإجراء من الالتزامات المترتبة على مقدمي خدمات الانترنت في إطار مساعدة السلطات المكلفة بالبحث والتحقيق في جرائم الفضاء الرقمي، فهي عملية مكملة لإجراء الحفظ العاجل لمعطيات المرور، كما أوضح المشرع الجزائري إجـ ءرا الإفشاء العاجل لمعطيات السير لغرض التحقيق وجعله مازالت على عاتق كل مقدمي الخدمات، وذلك من خلال نصه في المادة (10) من القانون04 -09[2] على انه " :في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ... و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) أدناه، تحت تصرف السلطات المذكورة "...[3]

بناء على ما سبق فكما تلزم سلطة التحقيق مقدمي الخدمات بالحفظ العاجل على معطيات المرور فإنها تلزمهم بالإفشاء السريع لها، أو لمن تعينه من قبلها عن تلك المعطيات المهمة المتعلقة بالمرور ووضعها تحت تصرفهم لفحصها قبل أن يتم التلاعب بها، قصد الوصول إلى تحديد هوية كل مقدمي الخدمة الآخرين، والطريق الذي بمقتضاه تم الاتصال، وبهذه الطريقة يكون بمقدور السلطة المكلفة بالبحث والتحري أن تكشف

[1] : معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مرجع سبق ذكره، ص 135.

[2] : المادة 10 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] : المادة 11 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

منبع الاتصال ومصبه، وهي المعلومات التي قد تقوده إلى معرفة هوية الأشخاص المتورطين في ارتكاب الجريمة.[1]

المبحث الثاني :معوقات التحري والتحقيق في الجريمة الالكترونية

إذا كانت ظاهرة الإجرام الإلكتروني أثارت بعض المشكلات فيما ما يتعلق بالقانون عن إمكانية تطبيق نصوصه التقليدية علي هذا النوع الجنائي الموضوعي بحث المستحدث من الجرائم، والتفسير الضيق للنصوص الجنائية فقد أثارت في نفس الوقت العديد من المشكلات فعلي نطاق القانون الجنائي الإجرائي، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحري فيها وجميع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الموضوعية بشأن الجريمة والمجرم.

وتبدأ المشكلات الإجرائية في مجال جرائم الفضاء بتعلقها في كثير من الأحيان وكيانات منطقية غير مادية وبالتالي يصعب من ناحية ببيانات معالجة إلكترونيا كشف هذه الجرائم ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة، ومما يزيد من صعوبة الإجراءات في هذا المجال سرعة ودقة تنفيذ الجرائم بشأنها إخفاء الأدلة المتحصلة عليها عقب التنفيذ، مكانية محو آثارها الإلكترونية، ويواجه التفتيش وجمع الأدلة صعوبات كثيرة في هذا المجال، وقد يتعلق ببيانات مخزنة في أنظمة أو شبكات إلكترونية موجود بالداخل.

ويثير مسألة الدخول إليها ومحاولة جمعه _ تحويلها إلي الدولة التي يجري فيها التحري، مشكلات تتعلق بسياسة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات وفي هذه الحالة يحتاج الأمر إلي تعاون دولي في مجالات البحث والتفتيش والتحري وجمع الأدلة وتسليم المجرمين، بل وتنفيذ الأحكام الأجنبية الصادرة في هذا المجال.[2]

[1] : معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، المرجع السابق، ص 136.

[2] : خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر و التوزيع، عمان، 2011، ص 17.

المطلب الأول: الصعوبات المتعلقة بعمل جهة البحث والتحقيق

إن التحقيق في الجرائم المعلوماتية وملاحقة مرتكبيها جنائيا يتسم بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق في بيئة رقمية قد تؤدي إلى وجود نتائج سلبية تنعكس على نفسية المحقق بفقده الثقة في نفسه وفي عمله، بالإضافة أنها تصعد من قيمة مكافحة هذا النوع من الجرائم.

فالإثبات هو إقامة الدليل على وقوع الجريمة و نسبتها إلى المتهم و ذلك و فق طرق مشروعة و محددة قانونا، و الإثبات في مجال الجرائم االلكترونية ينطبق عليه المفهوم العام للإثبات، و تبعا لذلك فهو يواجه العديد من الإشكاليات بغية استخلاصه نظرا للخصوصيات المتعلقة بطبيعة الجريمة باعتبارها غير مرئية و يسهل محو آثارها، و يصعب الوصول إلى أدلة إدانتها، والسمات المتعلقة بخصوصية التحقيق في هذه نظرا لصعوبة التحري في كشف غموضها وضعف التعاون الدولي في الجرائم مكافحتها.

أولا: عدم وجود تعاون دولي

في ظل الصراعات الحاصلة، يصعب إيجاد تعاون دولي حقيقي لمكافحة وكشف الجريمة الإلكترونية، فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين و تتحقق النتيجة في بلد أخر كقيام مجموعة من المجرمين بتشويه معلومات معينة و ليس بالضرورة أن ينتج هذا السلوك وأثاره في بلد المجرمين، فما هو محظور في الجزائر من الناحية الأخلاقية مباح في دول أخرى.[1]

والتطور السريع للجريمة والمعالجة البطيئة للحالات، ساعد المجرم المعلوماتي على الاستفادة من هذه العقبات للعبث والتخريب.

إن التعاون والتنسيق بين الأفراد والشركات يلعب دورا رئيسيا في إثبات الجريمة الإلكترونية، وعلى العكس من ذلك فإن غياب سياسة التعاون الدولي والتنسيق بين الدول في مقاومة الجريمة الإلكترونية يقابله في ذات الوقت تعاون واضح بين محترفي الإجرام المعلوماتي فضلا عن البرامج إلي يستعين بها القراصنة في أنشطتهم الإجرامية فإنهم يتعاونوا فيما بينهم ويتبادلون النصائح والخبرات فيما يتعلق بأنشطتهم، مما يزيد فاعلية و خطورة

[1] : عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص218.

هجومهم و خصوصا في ظل قصور وعدم فاعلية سياسة الدفاع الخاصة والمنصوص ضد هذه الجريمة.

لذلك تنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في حركة المعلومات بأنه بالإمكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الإجرامي في دولة أخرى.

كما أنه ورغم المناداة بضرورة التعاون الدولي في مكافحة هذه الجريمة، إلا أن هناك عوائق تحول دون ذاك وتجعل هذا التعاون صعبا، وأهمها:[1]

1 –**عدم وجود نموذج موحد للنشاط الإجرامي:** فالأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية لا يوجد فيها اتفاق عام مشترك حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا في بعض الأنظمة يكون محرما في أنظمة أخرى، ويرجع ذلك إلى عدة عوامل كاختلاف العادات والتقاليد والديانات والثقافات من مجتمع لآخر.

2– **اختلاف النظم القانونية الإجرائية:** بسبب تنوع واختلاف النظم القانونية الإجرائية نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى.

3–**عدم وجود معاهدات ثنائية أو جماعية بين الدول:** وحتى في حالة وجودها فإنها تكون قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الإنترنت.

4 –**مشكلة الاختصاص في جرائم الإنترنت:** وتثار هذه المشكلة بالنسبة للاختصاص على المستوى الدولي وذلك الاختلاف التشريعات والنظم القانونية من دولة لأخرى، حيث ينجم عنها تنازع الاختصاص بين هذه الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود، فيحدث أن ترتكب داخل إقليم دولة معينة، إلا أنها تمتد إلى خارج إقليم دول أخرى مما يعني خضوعها لأكثر من قانون جنائي.

[1] : معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مرجع سبق ذكره، ص144.

5-**عدم وجود قنوات اتصال:** أن من أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين هي الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العلمية التي غالبا ما تكون مفيدة في التحري لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون لذاك أصبح أمر التعاون الدولي ومكافحة الجرائم الإلكترونية أمرا حتميا يستلزم ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة هذه الجرائم، والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، ويجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، سبل المكافحة، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دول أخرى، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو إبرام الاتفاقيات الدولية.

وفي مجال الإجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاما من أجل التسيير دون عقبة لطلب المساعدة القانونية الوطنية، ويسهل من عملية القبض على مرتكبي هذه الجرائم، و ذلك دون مساس هذه الإجراءات بسيادة الدول الأخرى وأمنها ونظامها العام أو أي مصلحة أخرى من مصالحها الأساسية.[1]

ثانيا: المعوقات المتعلقة بخصوصية الدليل الإلكتروني

إن الإثبات الجنائي عملية متكاملة تستهدف البحث عن الأدلة الجنائية التي تثبت حدوث الواقعة الجنائية المرتكبة وظروف ارتكابها وأسبابها وتنسيقها إلى مقترفيها، وذلك لتقديمهم للعدالة، بحيث تواجه الجرائم الإلكترونية في هذا المجال عدة صعوبات عند إثباتها والتي انعكست بدورها على الأدلة المتحصل عليها من هذه الجرائم.

[1] : معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، المرجع السابق، ص155.

وتقف وسائل الإثبات الجنائي التقليدية عاجزة عن مواجهة الجرائم الإلكترونية التي تنصب على المعلومات والبيانات المخزنة في نظم المعلومات والبرامج، مما أدى إلى بروز ظاهرة جديدة وهي الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاسوب والانترنت نتج عنها ما يسمى بالدليل الإلكتروني أو الدليل الرقمي لإثبات وقوع الجرائم الإلكترونية ونسبتها لمرتكبيها.

والدليل الإلكتروني هو طريقة خاصة لإظهار الحقيقة والذي يتم فيه اللجوء إلى إحدى الوسائل الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص.

إن الدليل الإلكتروني المراد استخلاصه من بيئة إلكترونية يستمد طبيعته من ذات العمليات الإلكترونية وال يمكن كشفه بالطرق التقليدية و نما قد يحتاج إلى استخدام تقنيات علمية متطورة يجب إتباعها للوصول إليه، لكونه دليل غير مادي ملموس، وغير مرئي وغير مقروء، بحيث تتجلى هذه الخصوصية من خلال ما يلي:

أ[1]- أنها أدلة غير مرئية:

حيث أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التي تقع عليها أو بواسطتها ما هي إلا بيانات غير مرئية لا تفصح عن شخصية معينة، وهذه البيانات مسجلة إلكترونيا بكثافة بالغة وبصورة مرمزة غالبا على دعائم أو وسائل للتخزين إن كانت قابلة للقراءة من قبل ضوئية كانت أو ممغنطة لا يمكن للإنسان قراءتها والأدلة نفسها وال يترك التعديل أو التلاعب فيها إي اثر مما يقطع إي صلة بين المجرم وجريمته ويحول دو ن كشف شخصيته وكشف وتجميع أدلة بهذا الشكل لإثبات وقوع الجريمة و نسبتها إلى مرتكبيها هو أحد أهم المشاكل التي يمكن أن تواجه جهات التحري و الملاحقة.

ب- أن أغلب الآثار المتخلفة عن هذه الجرائم هي آثار إلكترونية:

وهذه الآثار بدورها إنما هي عبارة عن نبضات إلكترونية غير مرئية بالعين المجردة فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة بحيث أنه لا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية تظهرها للعيان، إضافة إلى أن ضخامة

[1] : خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، مرجع سبق ذكره، ص29.

حجم و كم البيانات والملفات الإلكترونية المجرمة من بين ذلك الكم الهائل لفصلها عن تلك البريئة منها.

ج- أن الجرائم التقليدية يكون فيها الدليل مادي ومرئي ومقروء:

بحيث إن كل الوقائع المتعلقة بهاته الجرائم خاضعة لسيطرة أجهزة العدالة، وتخلف آثار مادية كالسكين والسلاح وبقع الدم في جريمة السرقة مثال، عكس الجرائم الإلكترونية التي تكون فيها البيانات والمعلومات عبارة عن نبضات إلكترونية وتتم دون مشاهدة أو رؤية دليل الإدانة وسهولة محوه أو تدميره في مدة قصيرة وفي حالة قصور أجهزة عدالة غير متخصصة، والتي غالبا ما تنتفي قدراتهم على أن يتولوا بطريقة مباشرة فحص واختبار البيانات المشتبه فيها وتزداد جسامة هذه المشكلة بوجه خاص في حالة التلاعب في برامج الحاسب نظرا لتطلب الفحص الكامل للبرنامج اكتشاف التعليمات غير المشروعة المخفية داخله قدرا كبيرا من الوقت والعمل و غالبا و ما لا يكون له من حيث التكلفة الاقتصادية مبررا.[1]

د- إن إستخلاص الأدلة يعد تحديا لرجال الأمن:

لذلك يرى المختصين في جرائم الحاسب الآلي أن هذا الجهاز و ما يقع عليه من جرائم معلوماتية يعد تحديا هائلا لرجال الأمن ذلك أن رجل الأمن غير المتخصص و الذي انحصرت معلوماته في جرائم قانون العقوبات بصورة تقليدية من قتل وضرب وسرقة لن يكون قادرا على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية عالية ولذلك فغالبية الجرائم الإلكترونية تكشف مصادفة وليس بطريق الإبلاغ عنها.[2]

كما يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم وهذا يتطلب توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم المعلوماتية، وبمعنى آخر يتعين استقطاب و جذب الكفاءات المهنية المتخصصة في هذا المجال للاستعانة بها في تحقيق هذه الجرائم ويتعين عدم التذرع بالميزانيات المالية كسبب يحول دون قيام الدولة بواجباتها نحو تحقيق العدالة الجنائية وحتى يتم ذلك يرى هذا لجانب ضرورة الاستعانة

[1] : خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، المرجع السابق، ص30.

[2] : المرجع نفسه، ص31.

بالنبضة المتخصصة في الحاسب الآلي حال تحقيق الجرائم المعلوماتية وذلك لضبط هذه الجرائم واكتشافها وتقديم أدلة الإدانة فيها.

ومنه، يمكن القول أن الدليل المادي يمكن رؤيته وملامسته بأحد الحواس من طرف سلطات التحقيق والاستدلال عكس الدليل الإلكتروني الذي تكون المعلومات والبيانات فيه عبارة عن نبضات إلكترونية غير مرئية تنساب النظام المعلوماتي، مما يجعل أمر طمس هذا الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة.[1]

ثالثا :الصعوبات المتعلقة بجهات التحقيق ونقص في الخبرة

1- مشاكل متعلقة بجهاز التحقيق:

إن التحقيق في الجرائم الالكترونية أو ما يعرف بالتحقيق الرقمي هو عبارة عن مجموعة من الأساليب المتبعة من أجل معرفة وتقديم معطيات الإعلام مخزنة، ويتسم بعدة بوسيلة إلكترونية ممغنطة أمام جهة قضائية وهناك معوقات يمكن أن تعرقل عملية التحقيق وتؤدي إلى نتائج سلبية يمكن أن تنعكس على نفسية المحقق في حد ذاته بفقدانه الثقة في نفسه وفي أدائه، وعلى المجتمع بفقدانه الثقة في أجهزة العدالة الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وعلى المجرم نفسه بزيادة الثقة لديه بحيث يستطيع الإفلات من الجهات الأمنية الغير قادرة على اكتشاف أمره، بسبب صعوبة التحري في كشف غموض الجريمة وضعف التعاون الدولي في مكافحة الجرائم الإلكترونية.

إن التحري في كشف غموض الجريمة الإلكترونية تعترضه عدة عقبات، وتتمثل في ما يلي:[2]

أ- الكم الهائل للبيانات:

يشكل الكم الهائل للبيانات التي يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات والتي قد لا تثبت كلها تقريبا شيئا على الإطلاق.

---

[1] : خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، المرجع السابق، ص32.

[2] : رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، 2013، ص 56.

ب- مميزات الجرائم الإلكترونية:

أن الجرائم الإلكترونية تتميز بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها و دقة و سرعة محو آثارها وهي تعتمد في الأساس على الخداع في ارتكابها و التضليل في التعرف على مرتكبيها وتحتاج لخبرة فنية يصعب على الخبير التقليدي التعامل معها.

ومن تم يقتضي أن تكون جهات التحري والتحقيق بل و المحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسبة الإلكترونية وطريقة تشغيلها وأساليب ارتكاب الجرائم عليها أو بواسطتها مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها و ضبط الأدوات التي استخدمت في ارتكابها، لذلك فقد وجدت صعوبات جمة في كشف غموضها و إجراء التفتيش والضبط اللازمين أو التحقيق فيها على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الموارد من الناحية الفنية على نحو تمكينها من تحقيق المهمة المطلوبة وبكفاءة عالية. [1]

ففي الفترة الأولى لظهور هذا النوع من الجرائم وقعت الشرطة في أخطاء جسيمة أدت إلى الإضرار بالأجهزة أو الملفات أو الأدلة الرقمية الخاصة بإثبات الجريمة، ونعطي مثالا لهذا الخطأ من عمل الشرطة بالواليات المتحدة الأمريكية فقد حدث أن طلبت إحدى دوائر الشرطة بالواليات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة و قد حدث نتيجة ذلك أن تسببت دائرة الشرطة بدون قصد في إتلاف ما كان قد سلم من الملفات والبرامج.

- قد تكون شخصية (معوقات تتعلق بالمحقق) مثل: التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الانترنت، عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية .

[1] : المرجع نفسه، نفس الصفحة.

– صعوبات تتعلق بالنواحي الفنية كنقص المهارة المطلوبة للتحقيق في هذا النوع من الجرائم، نقص المهارة في استخدام الكمبيوتر والأنترنت، عدم توفر المعرفة بأساليب ارتكاب الجريمة الجرائم المعلوماتية.

– قلة الخبرة في مجال التحقيق في الجرائم المعلوماتية.[1]

2– نقص الخبرة:

إن صعوبة اكتشاف الجريمة بالدرجة الأولي مرده إلى نقص خبرة المحققين مما يضعنا أمام معادلة غير متكافئة طرفها أجهزة التحقيق بنقص خبرتها في مجال الكمبيوتر و الانترنت والطرف الآخر قراصنة محتلون و منحلون أخلاقيا يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية، وقد وصل بعض المجرمون المعلوماتيين الإطلاق على أنفسهم، ومن العوامل المساعدة اسم النخبة أما رجال الشرطة فقد أطلقوا عليهم اسم الضعفاء في نقص الخبرة في الجرائم المعلوماتية هي :[2]

– عدم تخصيص أموال من أجل التأهيل الجيد للمحققين و كذا حداثة الجريمة و خصوصيتها التي لم يعتد عليها رجال الشرطة، مما جعلهم قاصرين في مواجهتها.

– ضخامة المعلومات على الشبكة و انتشار أجهزة الكمبيوتر مما يصعب عملية التحقيق.

– الإنترنت بيئة خصبة للسلوك الإجرامي .

– التطور السريع للتقنية الحديثة و عدم وجود هيئات قضائية مختصة .

– وجود مواقع على الشبكة تسهل عملية إرسال البريد الالكتروني دون الحاجة إلى ذكر البيانات و يميل الفقه الجنائي إلى القول بضرورة تنمية الخبرة و المهارات للمتخصصين لوضع مدروسة للتدريب على التحقيق مع مراعاة خصوصية التطور التقني السريع دون إهمال التعاون الدولي في مثل هذه الحالات.[3]

---

[1] : رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 58.

[2] : جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، 2001 ، ص111.

[3] :المرجع نفسه، ص112.

المطلب الثاني: صعوبات متعلقة بطبيعة الجرائم المعلوماتية والجهة المتضررة

أولا : صعوبات تتعلق بالدليل الرقمي

من الصعوبات المتعلقة بالدليل الرقمي:

- إخفاء الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه .
- افتقاد أكثر الآثار التقليدية .
- إعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية كاستخدام كلمات السر .
- سهولة محو الدليل أو تدميره في زمن قصير جدا.
- صعوبة فهم الدليل الرقمي.

ثانيا :صعوبات تتعلق بالجهة المتضررة

- عدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين بالمؤسسات تعد إحدى معوقات التحقيق.
- لأحجام عن الإبلاغ عن الأشخاص الميسورين أو صغار السن خوفا من المجتمع
- المحيط بهم وخشية الفضيحة بعد معوقا من معوقات التحقيق .
- عدم الإبلاغ عن الجرائم.[1]

[1] : جميل عبد الباقي الصغير ، المرجع السابق، ص113.

الخـــاتمـة

ختاما مبدأ المشروعية يعتبر بمثابة الأساس القانوني التي تقوم عليه الدولة، وبقية السلطات من سلطة قضائية أو سلطة تشريعية، فهذا المبدأ يعتبر حجر الأساس الذي يربط وبحكم عمل هذه السلطات، ويفحص مدى قيام كل من هذه السلطات باحترام القانون وبمدى جعل القانون المرجع الأسمى للحكم في الخلافات والاستفسارات التي تعترض عمل هذه السلطات.

ولما كانت هذه الدراسة تنصب أولا على تناول مضمونها في ظل القانون الإداري وتحديد المعنى الواضح والسليم الذي لا يعتريه أي غموض في التفسير فكان من اللازم تحديد المصادر الأساسية التي يستقي منها وجوده، فتناولنا فيها أهم مصادر القانون الجزائري بشيء من التفصيل وفقا لمبدأ تدرج القاعدة القانونية، وبينها بشقيها المكتوبة والمتمثلة في التشريع الأساسي والتشريع العادي والتشريع التنظيمي، أو اللوائح وكذا المصادر غير المكتوبة والمبادئ العامة للقانون والأحكام القضائية ومدى الأخذ بها في النزاعات المعروضة على القضاء وكيف ساهمت في بروز معالم مبدأ المشروعية بعيدا عن الشك والتأويل وهذا ما أخذت به جل الأنظمة في تشريعاتها.

وبعد دراستنا للموضوع خرجنا بجملة من النتائج أهمها:

– أهمية وخطورة هذا الموضوع نظرا لما يترتب على عدم إخضاع هذه الأعمال للرقابة القضائية مشاكل جسيمة، فهو يواجه من ناحية امتيازات السلطة التنفيذية التي تصدر أعمالا تقتضي المصلحة العامة، عدم مناقشتها في القضاء

– مبدأ المشروعية هو العلامة المميزة للدولة القانونية وهو ضمانة أساسية للحقوق والحريات العامة، حيث يعتبر معيارا دقيقا و حاسما في وصف طبيعة السلطة هل ديمقراطية أم مستبدة

– تعتبر رقابة القضاء الإداري على أعمال الإدارة الجزاء الأكيد لمبدأ المشروعية، و الضمانة الفعالة لسلامة وتطبيقه و التزام حدود أحكامه.

– تعتبر مبدأ الفصل بين السلطات من أهم شروط تطبيق مبدأ المشروعية، حيث ينجم عن تخلفه غياب ما يسمى بمبدأ إساءة القانون، و اختفاء معالم الدولة القانونية.

ومن أهم التوصيات التي نقترحها في ختام هذا البحث:

– تكريس دولة القانون والعدل ليس بالأمر الهين، بل نحتاج إلى تضافر جهود كل مؤسسات الدولة وسلطاتها و كذا مواطنيها بما لهم من وعي.

– الحث على نشر الاجتهادات القضائية التي تساعد في تدعيم مبدأ المشروعية.

– تنظيم ندوات و أيام دراسية لإثراء الموضوع و مواكبة التحولات التي تمر بها بلادنا.

– بد من الضغط على السلطات الإدارية المرتكبة لعدم المشروعية، حتى يكون هناك قدر من المسؤولية لدى رجال الإدارة وحثهم على احترام المشروعية مما يساهم في زيادة الوعي الإداري و القضائي، ومن خلال ذلك تتجسد دولة القانون.

قائمة المصادر و المراجع

قائمة المصادر والمراجع

أولا: الكتب

1.أحسن بوسقيعة، التحقيق القضائي، دار هومة للطبعة للنشر والطباعة، طبعة 10، الجزائر، 2009.

2.أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الطبعة الرابعة، 2007.

3.أحسن بوسقيعة، الوجيز في القانون الجنائي العام، دار هومة للنشر والطباعة، طبعة أولى، الجزائر، 2010.

4.أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط 2، 2007.

5.جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، 2001 .

6.خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر و التوزيع، عمان، 2011.

7.خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، طبعة 1، الاسكندرية، 2009.

8. رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، 2013.

9. زيدان عبد الباقي، أساليب ووسائل الاتصال، دار الأنجلو مصرية، القاهرة، ط1، 1991.

10.صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،2003.

11.عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2003.

12.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت،الطبعة الأولى، دار الفكر الجامعي، مصر ،2006.
13.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، دار الفكر الجامعي، الإسكندرية، 2006.
14.عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة والقانون، دار النهضة العربية، القاهرة، 2013 .
15.علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، مصر، 1999.

16.علي عدنان الفيل ، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث ، القاهرة ، 2012.
17.محمد خربط، مذكرات في قانون الاجراءات الجزائية الجزائري، دار هومة للنشر والطباعة، الطبعة 4، الجزائر، 2009.
18.ملفين. ل. دليفر، نظريات وسائل الاتصال، ترجمة كمال عبد الرؤوف، القاهرة، الدار الدولية للنشر والتوزيع، 1999.
19. مي عبد الله سنو، الاتصال في عصر العولمة، الدور والتحديات الجديدة، لبنان، الدار الجامعية للطبع والنشر، 1999.
20.نائلة عادل، محمد فريد قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005.

ثانيا: القوانين والأوامر

1.القانون رقم 20-06 مؤرخ في 28أبريل سنة 2020 المتضمن تعديل قانون العقوبات.
2.القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
3.المرسوم الرئاسي رقم 432-04 المؤرخ قي 20 ديسمبر 2004 وتم تنظيم المصالح والأقسام والمخابر فيه بموجب قرار وزاري والذي تضمن مصلحة الخبرات الخاصة بالدلائل مشترك مؤرخ في 2007-04-14 .

4.الأمر رقم 21-11 المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات.

ثالثا: الرسائل الجامعية والبحوث

1.ابرهيمي سهام،مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2004، 2007.

2. أحمد مسعود مريم ، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال في ضوء القانون -04 09 مذكرة لنيل شهادة ماجستير في القانون الجنائي، كلية قصدي مرباح بجامعة ورقلة،2013.

3.حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2005_2006.

4.طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي ،جامعة الجزائر1، كلية الحقوق ،2011،2012.

5.فهد الله عبد العبيد العازمي ، الإجراءات الجنائية المعلوماتية ، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق .بجامعة القاهرة، 2012 .

6.قربوز حليمة ،الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2006_2009.

7.ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار الحقوق، تخصص قانون جنائي، 2014.

رابعا: المجلات العلمية

1.حملاوي عبد الرحمن، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، جامعة محمد خيضر، بسكرة، 2016.

2.سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، محكمة سيدي محمد.

3.عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002.

4.محمد قدري حسن عبد الرحمن، جرائم الاحتيال الالكتروني، مجلة الفكر الشرطي، عدد 79 ، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011 .

5.هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة بسكرة، 2015.

خامسا: المواقع الالكترونية

www.despace.univ.dz

www.policemc.gov.bh/reports/2009/…7…/633843953272369688.doc

www.osamabahar.com

الفهرس

مـلخص مذكرة الماستر

يتلاءم موضوع الدراسة مع التطورات الحاصلة في مجال المعلوماتية التي أصبحت تشكل أداة لارتكاب الجريمة أو مجالا لها، وذلك بإساءة استخدامها واستغلالها على نحو غير مشروع، وقد سعيت من خلال هذه الدراسة توضيح الأحكام الجزائية والقواعد الإجرائية التي على مداها يمارس العاملون في مجال البحث والتحري عن الجريمة المعلوماتي عملهم من أجل الحصول على الدليل المناسب لاثبات هذه الجرائم، من خلال التشريع الجزائري.

الكلمات المفتاحية:

1/ الجريمة الإلكترونية 2/ التشريع الجزائري3/الحاسب الألي 4/ النظام المعلوماتي

Abstract of Master's Thesis

The subject of the study is consistent with the developments taking place in the field of informatics, which has become a tool for committing crime or an area for it, by misusing it and exploiting it illegally. Informatics their work in order to obtain the appropriate evidence to prove these crimes, through the Algerian legislation.

key words:

1/ Cybercrime 2/ Algerian legislation 3/ Computer 4/ Information system