الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة حمه لخضر بالوادي

كلية الحقوق و العلوم السياسية

قسم: الحقوق

العقبات الإجرائية في إثبات الجريمة المعلوماتية

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة ماستر ل.م.د في الحقوق

التخصص: جريمة وأمن

إعداد الطالبين:

- محمد تومي
- وحيد عبد الليلة

إشراف الدكتور:

- صادق جراية

لجنة المناقشة:

الاسم واللقب	المؤسسة	الصفة
د/ كمرشو الهاشمي	جامعة الشهيد حمه لخضر . الوادي	رئيسا
د/ صادق جراية	جامعة الشهيد حمه لخضر . الوادي	مشرفا ومقررا
د/ جوادي إلياس	جامعة الشهيد حمه لخضر . الوادي	مناقشا

السنة الجامعية: 2024/2023


بسم الله الرحمن الرحيم

قال الله تعالى:

صدق الله العظيم سورة التوبة - الآية 105

شكر وعرفان

إمتثالا لقول رسول الله صلى الله عليه وسلم «من لم يشكر الناس لم يشكر الله» .

كان لزاما علينا تسجيل الشكر وإعلامه ونسبة الفضل لأصحابه، استجابة:

علامة شكر المرء إعلان حمده فمن كتم المعروف منهم فما شكر

فالشكر أولا لله عز وجل على أن هدانا لسلوك طريق البحث والتشبه بأهل العلم وإن كان بيننا وبينهم مفاوز .

كما نخص بالشكر أستاذنا الكريم ومعلمنا الفاضل المشرف على هذا البحث الأستاذ الدكتور : جراية الصادق ، فله منا وافر الثناء وخالص الدعاء .

كما نشكر السادة الأساتذة المناقشين وكل الزملاء وكل من قدم لنا فائدة أو أعاننا بمرجع،

نسأل الله أن يجزيهم عنا خيرا وأن يجعل عملهم في ميزان حسناتهم .

الإهداء

بسم الله مسبب الأسباب، وفاتح الأبواب، وخالق آدم وحواء من تراب، أما بعد . . .

أهدي ثمرة عملي هذا إلى التي أفضلها عن نفسي، فهي التي ضحت من أجلي، والتي لم أراها يومًا ما تدخر جهدًا في سبيل إسعادي دائمً وأبدًا، إليك أمي الحبيبة.

دائمًا ما نسير في دروب الحياة، ويبقى معنا من يسيطر على أذهاننا في كل طريق نسلكه، فلك أنت يا صاحب الوجه الطيب والأفعال الحسنة، فلم أراك تبخل على بأي شيء طيلة حياتي، والدي العزيز أطال الله في عمره.

إلى أخواني و أخواتي ، وإلى جميع أصدقائي و زملائي في هذا العمل إلى كل من علمني حرفا لكم جميعًا يا من ساعدوني وكانوا دائمًا بجانبي

إلى شهدائنا الأبرار، إلى فلسطين الأبية، إلى غزة المحاصرة.

أهديكم ثمرة عملي

محمد

الإهـــداء

إلى من علمني النجاح و الصبر . . . إلى من علمني العطاء بدون انتظار . . . أبي رحمة الله عليه .

إلى من علمتني و عانت الصعاب لأصل إلى ما أنا فيه . . . إلى من كان دعاؤها سر نجاحي و

حنانها بلسم جراحي . . . أمي العزيزة أطال الله في عمرها .

إلى جميع أفراد عائلتي الكريمة كل باسمه .

إلى زميلي الذي شاركني هذا العمل المتواضع تومي محمد

إلى كل من كان لهم أثر على حياتي، وإلى كل من أحبهم قلبي ونسيهم قلمي .

إليكم أهدي ثمرة هذا العمل المتواضع .

وحيد

قائمة المختصرات:

المختصر	المعنى
ق . ع . ج	قانون العقوبات الجزائري
ق . ا . ج	قانون الاجراءات الجزائية
ط	طبعة
ص	صفحة
ق	قانون
د	دكتور


مقدمة

ان خصوصية الجرائم المعلوماتية بالنظر إلى طبيعتها الرقمية التي تميزها عن غيرها، فرضت منطقا مختلفا في التعامل معها واستيعابها على مستوى مراحل حياتها المختلفة، من خلال تطوير أساليب البحث والتحري بما يتلاءم والمستوى التقني المتطور والعقد هذه الجرائم، وهو نفس المنطق الذي جعل المشرع الجزائري يسارع إلى استحداث إجراءات تحري خاصة (تمثل في السرب واعتراض المراسلات السلكية واللاسلكية المنصوص عليها في المادة 65 مكرره وما يليها من قانون الإجراءات الجزائية) بموجب القانون 06-22 المؤرخ في 29 ذي القعدة 1427 الموافق ل 20 ديسمبر 2006 المتمم للأمر 66-156 المؤرخ في 18 متر 1386 الموافق : 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية (يتبع السحر المركزي للشرطة العلمية والتقنية أربع مخابر جهوية موزعة عبر التراب الوطني وهي: المخير الجهوي بوهران، المخير الجهوي بقسنطينة المدير الجهوي ببشار، المدير الجهوي بتمنراست) وإصدار القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق : 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها رافي تشريع هذه الرسالة من القوانين.

إنشاء عدة هيئات وأجهزة للوقاية من الحيمة المعلوماتية، منها ما هو تابع لوزارة العدل ومنها ما هو تابع لمصالح الأمن المصلحة المركزية قارية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الشايع للمديرية العامية للأمن الوطني والمعهد الوطني للشرطة الجنائية أو المخم المركزي للشرطة العلمية والتقنية (منشور في الجريدة الرسمية للجمهورية الجزائرية، العدد 48 الصادرة بتاريخ من ذي الحجة 1427 الموافق ل:24 ديسمبر 2006 ص 30) وأخرى تابعة لجهاز الدرك الوطني كالمعهد الوطني للأدلة الجنائية وعلم الإحرام للدرك الوطني، الذي تم إنشاؤه بالمرسوم الرئاسي رقم 183-04 الصادر بتاريخ 26 جوان 2004، ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني، كما تم بموجب المادة 13 من القانون 09 - 04 (بالرجوع إلى نص المادة 13 من القانون 09-04 نجد أنها تنص على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أن تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق السليم وبتاريخ 08 أكتوبر 2015 صدر المرسوم الرئاسي رقم 15 -261 المتضمن تشكيل وتنظيم وكيفيات سير الهنة، حيث نصت المادة الثانية وما يليها منه على أن الهيئة سلطة إدارية مظلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل

ويأتي على رأس مهام هذه الهيئة، اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (تولي هذه الهيئة تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالإضافة إلى مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة والوقاية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص، كما تتولى الهيئة تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية (راجع في هذا الشأن المادة 04 من المرسوم الرئاسي رقم 15 – 261 الصادر بتاريخ 08 أكتوبر 2015 المتضمن تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

من جهة أخرى نجد أن المشرع الجزائري لم يخرج عن هذه القاعدة، حيث قام بنص قانون خاص يتبني تجريم أفعال الاعتداء علي الانظمة المعلوماتية وهذا من خلال ما يحتويه القانون رقم 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وقام بإصدار قانون الاجراءات الجزائية بموجب الأمر رقم: 06/22 المؤرخ في: 20 /12/ 2006، والذي بدوره يحتوي على أساليب خاصة في التحري والبحث في مثل هذا النوع من الجرائم .

1) الهدف من الدراسة:

– الوقوف على أساليب البحث و التحري عن الجرائم وأدلة الاثبات المتاحة في القانون الجزائري، ومدي مواجهتها في اثبات الجرائم الالكترونية.

– محاولة الوصول إلى تشخيص الدليل الالكتروني ومدي حجيته كدليل إثبات أمام الجهات القضائية.

– الكشف عن العراقيل والتحديات الاجرائية التي تثيرها عليمة البحث والتحري والاثبات والتي تفرضها خصوصية هذا النوع من الجرائم.

– المساهمة في اثراء الدارسات وبحوث علي الاجتماع سيسيولوجيا العنف والقانون العام الجنائي.

2) أهمية الموضوع:

– ان التعامل الالكتروني الحديث اصبح مرغما على كل الدول لما توفره من مزايا متعددة وكثيرة، كالنجاعة والفاعلية، اقتصاد التكاليف اختزال الوقت، الأمن والحماية.

– إن توجه الدول في اعتمادها على فكرة الادارة الالكترونية يتطلب وجود أنظمة معلوماتية أمنة ومحصنة ضد أي اعتداء أو سوء استغلال، و ذلك من خلال إيجاد حلول وبرامج وقائية وهي غير كافية من الناحية الواقعية، كما يتطلب الأمر إيجاد وسائل حماية ردعية، تتمثل أساسا في ألية التجريم والعقاب.

– تطبيق ألية العقاب لا يكون الا من خلال ايجاد حلول ومقترحات قانونية كفيلة بضمان الحريات والحقوق الاساسية للمواطن وتكريس قرينة البراءة.

3)دوافع اختيار الموضوع:

إن اختيارنا لهذا الموضوع ناتج عن دوافع موضوعية ودوافع شخصية.

<u>بالنسبة للدوافع الموضوعية:</u> فتتمثل في

– ان ظاهرة المجرم الالكتروني هي ظاهرة حديثة كشفت عن ضعف في النصوص الجنائية الموضوعية والاجرائية. التي صارت عاجزة عن احتواء ومواجهة مختلف الانشطة المنطوية تحت لواء الجريمة.

– من خلال هذه الدراسة يمكن ان نقف على اهم بواطن الضعف والنقص الذي تتخلله قواعد القانون الجنائي في اثبات الجرائم المعلوماتية،

– تبين هاته الدراسة أهم العراقيل التي تحول دون اثبات مثل هذا النوع من الجرائم.

– أنه موضوع جدير بالبحث والتحليل نظرا لما يسببه من أضرار مختلفة وارتباطه بالتحولات الاجتماعية العلمية والاقتصادية التي تحدث في المجتمع.

– محاوله فهم المشكلات التي يعاني منها المراهقين.

محاوله ازالة الغموض واللبس فيما يخص تأثير مواقع التواصل الاجتماعي علي المراهقين.

– دراسة سيسيولوجيا لمواقع التواصل الاجتماعي.

– استخدام مواقع التواصل الاجتماعي بشكل كبير بين مختلف الفئات من المراهقين في الجزائر.

<u>بالنسبة للدوافع الشخصية:</u> فتتمثل في أن البحث في هذا الموضوع من شانه أن يعزز و يثري معارفنا القانونية ويمكننا من الاستفادة منه مستقبلا خاصة في مسارنا المهني.

4)منهج الدراسة:

يعرف المنهج mèthode أو الطريقة التي يستعملها الباحث للوصول الى المعلومات التي يريد الحصول عليها بطريقة علمية وموضوعية مناسبة.

وبصفة عامة المنهج هو إتباع الاساليب والقواعد العامة التي يسعى بفضلها الباحث لاكتشاف الحقيقة العلمية والموضوعية، فالمنهج هو طريقة موضوعية يتبعها الباحث في دراسته أو يتبع ظاهرة من الظواهر

بقصد تشخيصها أو وصفها وصفا دقيقا وتحديد ابعادها بشكل شامل يجعل من السهل التعرف عليها وتمييزها.

ومن هذا المنطق وبناء على الاشكالية التي تم تحديدها، وبما اننا في دراستنا هذه نسعى الى جمع معلومات حول مستدمي مواقع التواصل الاجتماعي وكيف يؤثر هذا الاستخدام على المراهقين، فقد اعتمدنا على المناهج التالية:

4-1 المنهج الوصفي التحليلي: Descriptive and Analytical method

يتمثل في وصف الظاهرة أو المشكلة الاجتماعية ثم يقوم بتحليلها من حيث الخصائص التي تميزها وتحديد العوامل التي تدفع له.

ان هذا المنهج لا يقوم فقط على الوصف الدقيق للظاهرة، وإنما للكشف عن الاسباب الحقيقية والخصائص المميزة لها وصولا الى الحلول من خلال التحليل السيسيولوجيا الذي ينطلق من المعطيات ناتجة عن الوصف الشامل الذي يعتمد على تقنيات ووسائل منهجية تزود الباحث بمعطيات تمكنه من القيام بتحليل موضوعي علمي.

4-2 أدوات جمع البيانات:

يجب على الباحث أن تتوافر لديه بعض الحقائق والمعلومات عن موضوع الذي يجب دراسته من اجل اتخاذ القرارات المناسبة ، وهذا حتى تكون البيانات المتواصل إليها دقيقة والمعلومات صحيحة ، وللوصول إليها يجب الاعتماد على مصادر موثوقة تعتبر أساسية في التوصل الى نتيجة علمية أو حكم موضوعي صادق ومعبر عن جوهر أي قضية .

لهذا يتعين على كل باحث أن يكون ملما بقواعد وأساليب جمع البيانات اذا كانت الدراسة ميدانية وان المعلومات المتعلقة بموضوع دراسة الباحث توجد خارج المكتبة ، فأنه يتعين عليه أيضا ان يعتمد على منهجية علمية للحصول على معلومات الأساسية لداسته ذلك باستعمال ن وسائل جمع البيانات التي من بينها اجراء المقابلات.

1) الاشكالية:

من خلال ما سبق يمكننا معالجة هذا الموضوع وذلك من خلال طرح الإشكال الآتي:

فيما تتمثل العراقيل الإجرائية التي تحول دون اثبات الجريمة المعلوماتية وفق القانون؟

بحيث نطرح جملة من التساؤلات أهمها:

- مفهوم الجريمة المعلوماتية؟

– فيما تتمثل خصائص الجريمة المعلوماتية؟ وماهو الدليل الالكتروني؟

– إلى أي مدى وقف المشرع الجزائري في وضع طرق وأساليب البحث عليها؟

– ما هو القانون الواجب تطبيقه على الجريمة المعلوماتية؟

– ماهي الحلول التشريعية للحد منها؟

تم معالجة هذا الموضوع من خلال الاعتماد على المنهج التحليلي الوصفي، الذي بدوره يقف على أهم بواطن الموضوع، وتبعا لذلك ارتأينا أن نتبع الخطة التالية:

الفصل الأول الإطار المفاهيمي للجريمة المعلوماتية

المبحث الأول : ماهية الجريمة المعلوماتية

المطلب الاول : مفهوم الجريمة المعلوماتية وأركانها

المطلب الثاني: خصائص وتصنيفات الجريمة المعلوماتية

المطلب الثالث : مفهوم مبدأ الشرعية الجزائية وتطوره

المبحث الثاني : مفهوم الدليل الالكتروني

المطلب الأول : تعريف الدليل الالكتروني

المطلب الثاني: التعاريف المتحصل عليه من الوسائل الإلكترونية

المطلب الثالث: المصلحة المركزية المختصة كآلية للحماية والحد من الجريمة المعلوماتية

الفصل الثاني: العراقيل الاجرائية في استخدام وسائل اثبات الجريمة المعلوماتية

المبحث الأول : وسائل الاثبات والتحري في الجرائم الإلكترونية في ظل التشريع الجزائري

المطلب الأول: التفتيش الالكتروني

المطلب الثاني: الخبرة

المطلب الثالث: اعتراض المراسلات

المبحث الثاني : الحلول القانونية للحد من العراقيل الإجرائية في اثبات الجرائم المعلوماتية

المطلب الأول: عراقيل تقنية وعراقيل بشرية

المطلب الثاني: عراقيل قضائية

المطلب الثالث: الحلول القانونية قصيرة المدى وطويلة المدى

المطلب الرابع: الحلول القانونية طويلة المدى

الفصل الأول

الطبيعة الخاصة للجريمة المعلوماتية

إن التطور الملحوظ في المجال التقني نتج عنه استخدام هاته الوسائل بطرق غير شرعية وغير قانونية، الأمر الذي ينجر عنه إرتكاب جرائم لها صلة بهذا المجال، بحيث تكون أكثر خطورة وحدة وهو مايعرف بالجريمة الإلكترونية، ونظرا لحداثة هذا النوع من الجرائم إختلف فقهاء القانون في وضع مفهوم محدد وموحد لها وهذا راجع أن هاته الجرائم تمتاز بخصائص مميزة عن باقي الجرائم الأخرى، حيث عرفت نوعا خاص من المجرمين الالكترونيين الذين لهم دوافع شخصية وخارجية، بحيث قمنا بتقسيم الفصل الأول إلى مبحثين:

المبحث الأول : ماهية الجريمة المعلوماتية

المطلب الاول : مفهوم الجريمة المعلوماتية وأركانها

المطلب الثاني: خصائص وتصنيفات الجريمة المعلوماتية

المطلب الثالث : مفهوم مبدأ الشرعية الجزائية وتطوره

المبحث الثاني : مفهوم الدليل الالكتروني

المطلب الأول : تعريف الدليل الالكتروني

المطلب الثاني: التعاريف المتحصل عليه من الوسائل الإلكترونية

المطلب الثالث: المصلحة المركزية المختصة كآلية للحماية والحد من الجريمة المعلوماتية

المبحث الأول : ماهية الجريمة المعلوماتية

للوقوف على ماهية الجريمة المعلوماتية كان لزاما منا التطرق في البداية إلى التعرف على مفهومها عن طريق وضع تعاريف عديدة وتوضيح خصائصها وأركانها كما هو مبين في المطلب الأول والذي نتطرف فيه إلى مفهوم الجريمة الالكترونية وأركانها وخصائصها بينما تطرقنا في المطلب الثاني إلى مفهوم مبدأ الشرعية الجزائية وتطورها، بحيث يتمحور المطلب الثالث حول تصنيفات الجريمة المعلوماتية كما هو مبين على النحو التالي:

المطلب الاول : مفهوم الجريمة المعلوماتية وأركانها وخصائصها

أولا: مفهوم الجريمة المعلوماتية

1) من الجانب الفني

لم يتفق الفقه الجنائي على ايراد تسمية موحدة للجريمة المعلوماتية ، فهناك من يطلق عليها تسمية الجرائم الالكترونية ، وهناك من يطلق عليها تسمية جرائم المعلوماتية ، في حين يذهب اخرون الى تسميتها جرائم اساءة استخدام تكنولوجيا المعلومات والاتصال ، ويسميها اخرون جرائم الكومبيوتر والانترنيت ، وهناك من يطلق عليها الجرائم المستحدثة.

ان مسألة وضع تعريف للجريمة المعلوماتية كانت محلاً لاجتهادات الفقهاء ، لذا ذهب الفقهاء في تعريف الجريمة المعلوماتية مذاهب شتى ووضعوا تعريفات مختلفة ، وبالتالي فلا نجد تعريفاً محدداً للجريمة المعلوماتية نتيجة للاجتهادات الفقهية المتشعبة في هذا المجال فمن يتصدى لتعريف هذه الجريمة قد يتناول تعريفها من زاوية تقنية (فنية) او من زاوية قانونية. فالقائلون بالتعريف التقني يذهبون الى القول بأن الجريمة المعلوماتية هي (نشاط اجرامي تستخدم فيه تقنية الحاسب الالي بطريقة مباشرة او غير مباشرة كوسيلة او هدف لتنفيذ الفعل الاجرامي المقصود) [1].

ويذهب اتجاه اخر في الفقه الى التركيز على الجانب الموضوعي في تعريف الجريمة المعلوماتية باعتبار ان هذه الجريمة ليست الجريمة التي يستخدم الحاسب الالي كأداة في ارتكابها حسب بل تقع على الحاسب الالي او في داخل نظامه [2].

2) من الجانب القانوني:

تعرف بأنها: " مجموعة من الأفعال والأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية.

---

[1] د . عبد الرحيم محمد سلطان العلماء ـ جرائم الانترنيت والاحتساب عليها ـ بحث مقدم لمؤتمر القانون والكمبيوتر والانترنيت ـ مايو 2005 ص5

2 مشار الى هذا التعريف لدى د . علي عبد القادر القهوجي ـ الحماية الجنائية لبرامج الحاسب ـ دار الجامعة الجديدة ـ 1998 ص. 2

وبمعني آخر هي: " نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي ..

كما أن هناك من عرفها بأنها " الجريمة التي يتم ارتكابها إذا قام ش خص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني "

كما قسم رجال القانون العرب الجريمة الالكترونية في جانبها القانوني إلى:

أ- الجرائم التي تستعمل فيها الوسائل التكنولوجية من أجل القيام بالفعل الإجرامي مثل: تزوير أموال عن طريق الماسح الضوئي فهذا النوع له إطاره القانوني في معظم التشريعات العالمية.

ب- الجرائم التي تستخدم التقنية الحديثة لارتكابها، حيث عن طريق الأنترنت يمكن إنشاء مواقع إباحية، أو الإنضمام إلى مجموعات إرهابية، أو المتاجرة بالأسلحة أو المخدرات أو المتاجرة بأسرار الناس عن طريق خرق مواقعهم أو جهاز الكمبيوتر أو انتحال الشخصية باستخدام بطاقات الائتمان وسنركز دراستنا على هذا النوع من الجرائم.

ففي وسط عالم إفتراضي رقمي فرضه التطور التكنولوجي قد يجد الشخص نفسه وسط تيار جارف تختلس فيه أمواله من دون أي دليل ملموس، فمن خلال كل ما ذكر يمكن تعريف الجريمة الإلكترونية بأنها سلوك غير مشروع أو غير أخلاقي أو غير مسرح به[1].

ثانيا: أركان الجريمة المعلوماتية

للجريمة الإلكترونية أركان تتمثل في:

1) الركن المادي

يتكون الركن المادي للجريمة الالكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية مع العلم أنه يمكن تحقق الركن المادي تون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقق نتيجتها ، مثل إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة ورغم عدم تحقق النتيجة إلا أنه لا مناص من معاقبة الشخص ويتخذ الركن المادي عدة صور بحسب كل جريمة:

- **جريمة الغش المعلوماتي** : الركن المادي فيها شر تغيير الحقيقة في مستند رسمي أو محرر رسمي، ولكن المستند هذا ليس مستند عادي يدخل ضمن أدلة الإثبات، بل هي عبارة عن تسجيلات أو محررات إلكترونية

- **جريمة الإرهاب الإلكتروني والمواقع الإباحية ومواقع القمار**: الركن المادي في هذه الجرائم هو إطلاق المواقع التي تحث إما على الانضمام إلى الجماعات الإرهابية ، كما تورد كيفية صنع القنابل اليدوية -

[1] فرعون محمد الصديق، بوعلي العربي، إثبات الجريمة المعلوماتية، ملازمي الأوائل للشرطة، الدفعة 2018 – 2020، ص 15.

أما المواقع الإباحية فتزود مواقعها بالصور وافكار الشئون الجنسي وهناك مواقع تنشر فكرة الانتحار أو تشويه صورة الإسلام.

أما مواقع القمار فهي لغسيل الأموال فالركن المادي هذا سلوك المجرم المعلوماتي في تزويد المواقع بالمعلومات اللازمة للانحراف أو القتل وهذا المجرم أقل م ن المخترق أو المتسلل، هذا فيما يخص السلوك الاجرامي أما النتيجة فهي الأثر المادي المتمثل في انحراف المجتمع وتدمير الأخلاق والمعتقدات وظهور عادات عربية على المجتمع زيادة إلى تقشي العنف التصميم الموقع من طرف المجرم مرتبطة بالتأثيرات الخطيرة التي تحمل عبرها المجتمع من انحراف وهذا ما يعرف بالعلاقة السينية[1].

2) الركن المعنوي

بعرف بأنه العلم بعناصر الجريمة وإرادة ارتكابها وبالتالي يتكون هذا الركن من عنصرين هما العلم والارداف فالعلم:

هو إدراك الأمور على نحو مطابق للواقع ، بسبق الإرادة و أما الإرادة : فهي إنجاء لتحقيق السلوك الإجرامي. ويتخذ القصد الجنائي عدة صور منها القصد العام والقصد الخاص

– **القصد الجنائي العام:** هو الهدف الفوري والمباشر للسلوك الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما يعتاد

– **القصد الجنائي الخاص:** هو ما يتطلب توفره في بعض الجرائم فلا يكفي بمجرد تحقيق الغرض من الجريمة بل هو أبعد من ذلك أني انه يبحث في تواليا المجرم بطرحنا السؤال:

ما هو الهدف الذي يريد الجاني تحقيقه من الجريمة؟ فأي قصد يجب توافره في الجريمة الالكترونية؟ إن المجرم الالكتروني يتوجه من أجل إرتكاب فعل غير مشروع أو غير مسموح مع علمه أركان الجريمة، وبالرغم من أن بعض المخترقون يرون أفعالهم بأنهم مجرد فضوليون وأنهم قد تسللوا صدفة فلا ينتقي العلم كركن للقصد الجنائي، كان يجب عليهم أن يتراجعوا بمجرد دخولهم ولا ب تمروا في الإطلاع على أسرار الأفراد والمؤسسات أن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية فالقصد الجنائي متوافر في جميع الجرائم الالكترونية دون أي استثناء ولكن ه ذا لا يمنع أن هناك بعض الجرائم الالكترونية تتطلب أن تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الأنترنيت.

[1] فرعون محمد الصديق، بوعلي العربي، مرجع سابق، ص 19 – 20

أما جرائم نشر الفيروسات عبر الشبكة فهي تتوفر على القصد الجنائي الخاص فالمجرم يهدف إلى تعطيل عمل الشبكة وفي جميع الحالات المشرعه هو من يختص بتحديد الحالات اللاتي يشترط فيها توافر القصد الجنائي الخاص[1].

3) المجرم المعلوماتي

إن المجرم المعلوماتي هو شخص يختلف عن المجرم العادي فلا يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة للمعلوماتية، فينال ثلاثة أنواع بارزة لهؤلاء المجرمين أو بالأحرى ثلاث تصنيفات:

1.3. الهاكرز : هر شخص بارع في استخدام الحاسب الآلي وبرامجه وهو فضولي في بعض الأحيان يكون عادة من المراهقين المولعين بالشبكة العنكبوتية ولديه فضول في استكشاف حسابات الأخرين وبطرق غير مشروعة، حيث يدفعهم الفضول الى معرفة كلمة سر بعض الأشخاص والدخول على نظامهم المعلوماتي، لكن لا تتوفر لديهم في الغالب مواقع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي والثبات الذات وتلف هذه الطائفة أساسا من مراهقين وشباب مطلبية وتلاميذ ثانويات وشباب عاطل عن العمل.

2.3. الكراكرز : هم أشخاص متسللون يتابعون عن كثب آخر الأخبار وبرامج الحماية الأمنية للأجهزة والمعلومات، الى حد أنهم ينشئون النوادي لتبادل المعلومات[2].

وهؤلاء المجرمون يستطيعون الإجتياز الأمني لمختلف المواقع بقصد التخريب والاختلاس والتزوير، ومن أهم هذه الجماعات في جماعة القراصنة الروس الذين يعتبرون الأفضل على الإطلاق، ففي استطلاع للرأي أكد أنهم متمكنون من الخرق الآلي للأنظمة بنسبة 82 بالمائة حتى أن الولايات المتحدة الأمريكية وجهت الاتهام لروسيا بمحاولة سرقة برامج نظام تمركز الصواريخ العالي، لأن بعض الهاكرز الروس قاموا بمهاجمة موقع الأطلسي. للعلم فإن هناك بعض المجلات التي تصدر، مهمتها الدفاع عن هذه الفئة التي لا تعتبرها مجرمة بل تقول إنهم يبلون حسنا، وأنهم يكتشفون الثغرات الأمنية في الأنظمة المعلوماتية

3.3. مصممو المواقع الإرهابية والإباحية: وحتى التونسية لجلب الأفراد المهتمين بالتسوق مثلا من أجل معرفة شفرة بطاقة الائتمان واستعمالها الحاجات شخصية ولكن الملاحظ أن هذه الفئة اقل خيرة من الفئة السابقة التنكر.

[1] فرعون محمد الصديق، بوعلي العربي، مرجع سابق، ص 21

[2] فرعون محمد الصديق، بوعلي العربي، مرجع سابق، ص 22

ثالثا: خصائص الجريمة المعلوماتية

تعتبر الجرائم الالكترونية من الجرائم المستحدثة بحيث لها مجموعة من الصفات قد تتطابق بعضها مع صفات طوائف اخرى من الجرائم هذا من جهة، ومن جهة اخرى فإن اختلاف هذا النوع من الجرائم عن الجرائم التقليدية من حيث الافعال الاجرامية اكسبها خصوصية غير عادية

1) المجرم المعلوماتي:

قد يكون المجرم المعلوماتي شخصاً طبيعياً يعمل لحسابه الخاص، والهدف منه تحقيق مصلحة خاصة به من وراء الجرم الذي ارتكبه عن طريق الاستعانة بأحد نظم المعالجة الالية للبيانات والمعلومات، وأحيانا قد يعمل لحساب شخص ما سواء كان شخصا معنويا كشركة خاصة أو عامة أو شخص آخر.

2) الهدف والدافع من وراء ارتكاب جرائم المعلوماتية:

هناك عدة دوافع الى ارتكاب الجريمة المعلوماتية، قد يقف وراءها مصدر واحد هو الرغبة الاجرامية ويمكن ايجاز هذه الدوافع بالاتي :

1.2. الدوافع الشخصية:

يمكن حصر الدوافع الشخصية لدى المجرم الالكتروني هو السعي لتحقيق الربح ، فهذا الدافع المادي يعد من اهم البواعث الى ارتكاب الجريمة المعلوماتية لما يحققه من ثراء شخصي فاحش ، وقد يكون الدافع في سبيل انتقام وتحقيق انتصار شخصي على نفس الانظمة المعلوماتية.

2.2. الدوافع الخارجية:

بفطرة الانسان هو مخلوق هش من الناحية السيكولوجية، بحيث يمكن أن يواجه بعض المواقف التي قد تؤثر عليه سلبا ، ولعل من ابرزها عنصر الزمن وتوفير سنوات عدة من البحث، واغراءات الملايين من الدولارات في مجال البحث العلمي، اذ تدفع الحاجة بعض المنشآت بل وحتى بعض الدول الى الاتصال بالأفراد الذين يشغلون اماكن حساسة في احدى المنشآت كي يعملوا لصالح منشآت اخرى منافسة بهدف الاطلاع على بعض المعلومات والتقنيات المتوفرة لديها للاستفادة منها، وتستخدم في ذلك عدة اساليب منها الرشوة او الاقناع والاغراء المقترن بالتهديد، والذي قد يصل في بعض الاحيان الى زرع[1] جواسيس في تلك المنشآت.

[1] ـ د . خليفة الملط احمد ـ الجرائم المعلوماتية ـ دار الفكر العربي ـ الاسكندرية ـ ص 98، بتصرف.

3.2. ارتكاب الجرائم المعلوماتية في مراحل تشغيل نظام المعالجة الآلية للبيانات:

يمتاز المجرم المعلوماتي على غيره من المجرمين بقدرات تمكنه في أي مرحلة من المراحل بتشغيل نظام المعالجة الالية للبيانات في الحاسب الالي (الادخال ـ المعالجة ـ الاخراج) ، غير ان لكل مرحلة من هذه المراحل تمتاز بنوعية خاصة من الجرائم بحيث أنه يمكن النظر لطبيعتها بارتكاب الجريمة المعلوماتية الا في وقت محدد، فنجد أنه في مرحلة الادخال تترجم المعلومات إلى لغة مفهومه من قبل الالة، بحيث يسهل إدخال معلومات غير صحيحة او عدم إدخال الوثائق الأساسية والمعلومات المطلوبة، وفيما يخص مرحلة المعالجة الالية للبيانات فيمكن ادخال أي تعديلات على برامج الحاسب الالي تحقق الهدف الاجرامي عن طريق التلاعب في برامج النظام المعلوماتي كدس تعليمات غير مصرح بها أو تشغيل برامج جديدة تلغي كلياً او جزئياً عمل البرامج الاصلية، وتتطلب الجرائم المرتكبة في هذه المرحلة أن يكون الجاني الإلكتروني على دراية فنية، كما ان اكتشافها يكون صعب للغاية، وكثيراً ما تقف الصدفة وراء اكتشافها، اما في المرحلة المتعلقة بالمخرجات بحيث يمكن أن يقع بها التلاعب في النتائج التي يخرجها النظام المعلوماتي (الحاسب الالي) وهذا من خلال بيانات صحيحة ادخلت وعولجت بطريقة صحيحة.

4.2. كيفية وقوع الجريمة في بيئة الإلكترونية :

إن من شروط لقيام الجريمة الإلكترونية هو كيفية التعامل الصحيح والدقيق مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي وهذا لهدف معالجتها الكترونياً بحيث يمكن للمستخدم ان قوم بكتابتها من خلال العمليات المتبعة والتي بدورها تمكن من توافر امكانية تصحيحها او تعديل محتواها او امسحها او تخزينها اواعادت استرجاعها او طباعتها بحيث تعتبر هذه العمليات همزة الوصل في إرتكاب الجرائم المعلوماتية ، اين يشترط من الجاني الالكتروني ان يمكون ملما وعالما لها اثناء ارتكابها وخاصة في جرائم التزوير واستعمال مزور والتقليد والتشهير[1].

5.2. تواطؤ البعض على القيام بالاضرار:

يتمحور الدور الاساسي للبعض في التواطؤ على الاضرار بحيث نجد ان اصحاب الياقات البيضاء فغالباً من له مصلحه لتغطية عملية التلاعب بحيث يقوم باعانة المجرم الاكتروني على القيام بإلحاق الضرر بالمجني عليها لتغطية عملية التلاعب وتحويل المكاسب المالية اليه حيث يقومون

[1] – الشحات منصور حاتم عبد الرحمن ـ الاجرام المعلوماتي ـ دار النهضة العربية ـ القاهرة ط ١ـ 2003ـ ص 37 ، بتصرف .

باختيار في هدا النوع من الجرائم على شخص متخصص في الانظمة المعلوماتية يقوم الجانب الفني من المشروع الاجرامي .

6.2. النتائج المترتبة عن اضرار الجرائم المعلوماتية :

ان ارتكاب الجرائم المعلوماتية يتمحور ويتبلور في نطاق تقنية وتكنولوجيا متقدمة يتزايد استخدامها يوماً بعد اخر من خلال تطور البرامج واعلام في ادارة مختلف المعاملات الاقتصادية والمالية حيث تمس هذه الجرائم المركز الحسابي والاداري وتنقلات الاموال والاستثمارات سواء في المنشآت العامة او الخاصة ، ايضا تمس المعلومات الشخصية المخزنة في ذاكرة الميتة والحية للحواسيب الالية للبنوك وشركات التأمين وحتى لدى المحامين والمستشفيات ومراكز الشرطة والدرك والامن العسكري والاحزاب السياسية ، وقد تهدد هذه الاعتداءات مباشرة قدسية وسرية وحرمة الحياة الخاصة او الحرية السياسية ، ناهيك عن الخطورة التي تشكلها هذه الجرائم اذا ما تعلقت بالمعلومات الخاصة بإدارة الدولة وعمل الحكومة وخاصة في ميادين الامن والدفاع والمشروعات النووية والتصنيع الحديث للأسلحة وامن البلاد ، وهدا النوع يطلق عليه مايعرف باسم (المعلومات السوداء).

7.2. صعوبة تحليل وكشف الجريمة المعلوماتية واثباتها :

مثل هدا النوع من الجرائم يكون على مستوى المسرح الافتراضي للجريمة بحيث لا تحتاج جرائم الاعتداء على برامج ومعلومات الحاسب الالكتروني الى أي عنف او جثث او سفك للدماء او اثار اقتحام لسرقة الاموال ، وانما هي قاعدة معلومات وبيانات تقوم على تغيير و تعديل ويمكن ان تصل الى حد القيام المحي الكليً او الجزئيً من السجلات المخزونة في ذاكرة الحاسب الالكتروني ، هنا تكمن صعوبة اكتشافها ومن ثم القيام بتطبيق الجزاء الجنائي على مرتكبها هنا ايضا نجد صعوبة اخرى تتمحور في إثبات الجرائم المعلوماتية حيث ان هذه الجرائم لا تترك أي اثر خارجي ومرئي لها حيث انها تعتمد في الاساس على الدليل الاكتروني الافتراضي والدي يعتبر سهل الاتلاف والاخفاء، ايض من بين الصعوبات الموجودة في اثبات هذا النوع من الجرائم هو ان المجرمين الذين يخططون يتمازون هم دائماً اصحاب ذكاء ودهاء وخبرة ودراية واحتراف في مجال تقنية المعلومات وبالتالي فهم يخططون لهذه الجرائم بطرق محكمة وسرية تضمن نجاحهم في ارتكاب الجريمة وفرارهم من اعين العادلة والسلطات المحققة وهذا من خلال استخدامهم وسائل تقنية متطورة يصعب على الغير معرفتها والتعامل .

8.2. صفات المجرم المعلوماتي :

ان مرتكبي جرائم الكومبيوتر والإنترنت (الجرائم المعلوماتية) هم في الاصل عبارة عن مجموعة من الصفات او الخصائص تميزهم عن سواهم من الجناة المتورطين في انماط الانحراف الاخرى ، ولعل من ابرز هذه السمات:

أ ـ المجرم المعلوماتي صغير السن:

تصل اعمار مقترفي الجريمة المعلوماتية بين (18 ـ 46) سنة ، والمتوسط العمري لهم 25 سنة مما يدل على ان المجرم المعلوماتي يكون من صغار السن بحكم التطور الذي تعيشه هاته الفئة العمرية لان كبار السن لم يألفوا التعامل مع الحاسب الالي .

ب ـ المجرم المعلوماتي الفطن :

يوصف الاجرام المعلوماتي بأنه اجرام الاذكياء والفطناء وهذا بالمقارنة بالإجرام التقليدي الذي يميل الى العنف، فنجد ان المجرم المعلوماتي انسان على مستوى عالي من الدهاء و الذكاء ، اضافة الى انه مجرم يتكيف اجتماعياً مع كل الظروف .

ج ـ المجرم المعلوماتي بطبيعته مجرم متخصص:

ان الجناة او مرتكبي الجرائم المعلوماتية على دراية تامه من المعرفة المعلوماتية ، أي انهم متخصصون في هذا الشكل من الانحراف والاجرام الالكتروني .

د ـ المجرم المعلوماتي بطبيعته مجرم محترف:

يشترط في ارتكاب الجرائم الالكترونية توافر شروط في مرتكبي الجرائم المعلوماتية يتمثل في انهم يمتازون بقدر عالي من المعرفة المعلوماتية ، ولكن هذه السمة ليست عامة ومطلقة وانما تقتصر على الجرائم التي يستلزم ارتكابها التعامل مع الحاسب الالي ومعالجة المعلومات[1] .

[1] ـ محمد عبد الله ابو بكر سلامة ـ المرجع السابق ص. 97 ، بتصرف .

المطلب الثاني : مفهوم مبدأ الشرعية الجزائية وتطوره

نصت المادة الاولى 01 من قانون العقوبات على انه (لا جريمة ولا عقوبة الا بنص قانوني) ضماناً لمصلحة الافراد فهو السور الحقيقي لحماية حقوق الافراد وكفالة حرياتهم الفردية، ذلك ان اسناد مهمة تحديد الجرائم والعقوبات الى السلطة التشريعية يعد ضماناً لعدم الاعتداء على حقوق الافراد وحرياتهم من قبل السلطات الاخرى فلا تمتلك السلطة القضائية ملاحقة افعال لم يجرمها المشرع ولا تقرير عقوبات غير التي حددتها النصوص العقابية[1]

كما يعد مبدأ (قانونية الجرائم والعقوبات) من المبادئ الاساسية المقررة في اغلب التشريعات الجنائية الحديثة ويقصد به ان المشرع وحده هو الذي يملك تحديد الافعال المعاقب عليها والمسماة (بالجرائم) وتحديد الجزاءات التي توقع على مرتكبيها والمسماة (بالعقوبات) ويفترض هذا المبدأ ضرورة الفصل بين السلطات الثلاث (التشريعية والتنفيذية والقضائية) وان مهمة بيان الافعال التي تعد جرائم وتقرير الجزاء الجنائي الذي يترتب على وقوع كل منها من شأن السلطة التشريعية وحدها ، لانها صاحبة الاختصاص الاصيل في تشريع القوانين هذا كله من اجل ضمانً مصلحة الافراد فهو السور الحقيقي لحماية حقوق الافراد وكفالة حرياتهم الفردية، ذلك ان اسناد مهمة تحديد الجرائم والعقوبات الى السلطة التشريعية يعد ضماناً لعدم الاعتداء على حقوق الافراد وحرياتهم من قبل السلطات الاخرى فلا تمتلك السلطة القضائية لفكرتي العدالة والاستقرار ، اذ تتحقق فكرة العدالة في المساواة بين افراد المجتمع وعدم التمييز بينهم على اساس طائفي او طبقي من حيث التجريم والعقاب ، كما يتحقق الاستقرار بسيادة القانون وعدم اغتصاب سلطة لاختصاصات سلطة اخرى وفي هذا تأكيد لمبدأ الفصل بين السلطات وفي هذا المبدأ تحقيق للمصلحة العامة لما يحققه من وحدة للقضاء الجزائي وعدم تناقضه او تفاوته تفاوتاً يذهب بهذه الوحدة.

و من جهة نجد ان مبدأ الشرعية الجزائية لانتقادات ساقها معاضوه منها ، حيث انه يقيد سلطات القاضي الجزائي ويقف حجر عشرة امام حق المجتمع وواجبه في مواجهة الأفعال الخطيرة التي تلازم التطور الاجتماعي والتقدم العلمي والتقني ، فالمشرع حين يجرم الأفعال الضارة او الخطرة التي تمس بمصالح المجتمع انما يضع في حسبانه المصالح القائمة وقت اصدار التشريع ، وكذلك صور الافعال التي يمكن ان تضر بتلك المصالح حسب تصوراته وقت اصداره للقاعدة القانونية .

[1] ـ د . الشحات منصور حاتم عبد الرحمن ـ المرجع السابق ص. 89 ، بتصرف .

ومنطق مبدأ المشروعية يقضي بعدم تجريم فعل الا بنص القانون ولو ترك الامر للتطبيق القضائي فهذا يعني اعطاء سلطة التشريع الى القضاء. كما ان منطق مبدأ المشروعية يقضي سلفاً تحديد الافعال المنهي عنها والتي تعد جرائم حتى يستطيع الافراد تكييف سلوكهم بما يتفق وأوامر المشرع ونواهيه ، هذا اضافة الى ان الاثر التهديدي للعقوبة يفقد مفعوله اذا لم تكن الجرائم والعقوبات محددة سلفاً بمقتضى نصوص قانونية ، ولأجل هذه الاعتبارات نجد ان الكثير من التشريعات التي الغت هذا المبدأ في ظروف سياسية معينة عدلت عن ذلك وضمنت قوانينها النص عليه صراحة.

لقد تطور مبدأ المشروعية ، حيث اصبح يعطي للقاضي مرونة وسلطة تقديرية فيما يتعلق بتقدير العقوبة التي تتفق وظروف الجريمة ، فمثلاً تطور التشريع فجعل للعقوبة حداً اقصى وحداً ادنى يتخير القاضي من بينهما ما يراه اكثر ملائمة للحالة المعروضة امامه ، كما وضع لكثير من الجرائم عقوبات تخييرية يتخير القاضي من بينهما ما يراه اكثر ملائمة مع وضع الجاني بل ذهب الى ابعد من ذلك حين اعطى للقاضي سلطة الامر بوقف تنفيذ العقوبة متى ما تبين له من ماضي المتهم واخلاقه وظروفه ان هذا اجدى في اصلاح الجاني وتأهيله كما اعطى للسلطة التنفيذية حق التدخل في تنفيذ العقوبة بما تراه محققاً للغاية منها فقرر حق العفو وتخفيف العقوبة والافراج الشرطي عن المسجون قبل انتهاء مدة عقوبته اذا ثبت صلاح.

ومع ذلك فأن المرونة التي طرأت على مبدأ قانونية الجرائم والعقوبات قد وردت على المبدأ في شقه الثاني وهو تقدير العقوبة دون الشق الاول الخاص بخلق الجرائم ، فقد بقى هذا الشق على جموده ومنع القاضي من اية سلطة تقديرية في شأن تقدير الجرائم ، مع التخفيف من ذلك الجمود احياناً بإعطاء السلطة التنفيذية ذلك الحق بتفويض بناءاً على قانون [1].

[1] ـ د. القهوجي علي عبد القادر ـ قانون العقوبات ـ القسم العام ـ الدار الجامعية ص. 41 بتصرف .

المطلب الثالث: تصنيفات الجريمة المعلوماتية

أولا: استنادا الى قانون العقوبات:

من جهة التشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الاولية للمعطيات (ق رقم 04-05 مؤرخ- 10-11-2004)[1].

القسم السابع مكرر 1 من قانون العقوبات باب المساس بأنظمة المعالجة الآلية للمعطيات

المادة 394 مكرر : يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك تضاعف العقوبة إذا ترتب على 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 50.000 دج إلى 150.000 دج[2].

المادة 394 مكرر 1 : يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها[3].

المادة 394 مكرر2: يعاقب بالحبس من شهرين (2)إلى ثلاث (3) سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج، 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[4].

---

[1] قانون رقم 04-05 مؤرخ في 14 أغسطس 2004، يعدل و يتمم القانون رقم 90-29 المؤرخ في أول ديسمبر سنة 1990 و المتعلق بالتهيئة و التعمير.

[2] الأمر رقم 66-156 المؤرخ في مؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة يونيو سنة 1966 ،الذي يتضمن قانون العقوبات، المعدل والمتمم قانون العقوبات، المعدل والمتمم، طبعة 2012، ص113.

[3] المرجع نفسه.

[4] الأمر رقم 66-156 ، المرجع السابق، ص113.

المادة 394 مكرر 3 : تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد[1].

المادة 394 مكرر 4: يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[2].

المادة 394 مكرر 5: كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها[3].

المادة 394 مكرر6: مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا له هذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها[4].

المادة 394 مكرر 7: يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها[5].

ثانيا: استنادا الى انتشارها:

هناك من يصنفها على حسب انتشارها نجد وزارة العدل الامريكية سنة 11/2000 اقرت على نوع من الجرائم وهي:

– جرائم السطو على البيانات الكومبيوتر– جرائم الانجاز بكلمة السر– جرائم عمليات الهاكر والقرصنة وسرقة الاسرار التجارية باستخدام الكومبيوتر– جرائم تزوير الماركات التجارية – جرائم تزوير العملة باستخدام الكومبيوتر. الصور الجنسية لاستغلال الاطفال – جرائم الاحتيال عبر شبكات الانترنيت – جرائم الماسة بأمن البلاد المتمثلة في تهديدات القنابل بواسطة الانترنيت و الانجاز بالمتفجرات الاسلحة و النارية أو المخدرات وغسل الاموال غير شبكة الانترنت.

ثالثا: تصنيف مكتب التحقيقات الفيديرالي الامريكي FBI:

– اقتحام شبكات الهواتف العامة أو الرسمية و اقتحام المواقع الرسمية

---

[1] المرجع نفسه.

[2] المرجع نفسه.

[3] المرجع نفسه.

[4] المرجع نفسه.

[5] الأمر رقم 66-156 ، المرجع السابق، ص113.

- انتهاك سرية بعض المواقع و البرامج[1]
- أما بالنسبة للباحث أحمد صيداني فقد أورد 5 أنواع من الجرائم هي:
- الاعتراف غير المسموح به
- اتلاف المعلومات أو البرامج
- تعطيل نظام الكومبيوتر وتخريب شبكة الاتصالات
- اختراق غير مسموح به المعلومات داخل النظام وخارجة.
- التجسس على الكومبيوتر[2].

[1] فرعون محمد الصديق، بوعلي العربي، مرجع سابق، ص18

[2] فرعون محمد الصديق، بوعلي العربي، المرجع السابق، ص19

المبحث الثاني : مفهوم الدليل الالكتروني

تهدف هذه الدراسة إلى تحديد الضبط المفاهيمي للدليل الإلكتروني وتسليط الضوء على حجيته في الإثبات الجنائي، وذلك من خلال الوقوف على مفهوم الدليل الإلكتروني كوسيلة إثبات في المجال الجنائي، وتحديد خصائصه و طبيعته التي تميزه عن باقي الأدلة الجنائية التقليدية، بالإضافة إلى تحديد أشكال وتقسيمات الدليل الإلكتروني، وذلك من خلال التطرق في المطلب الأول إلى تعريف الدليل الإلكتروني والمطلب الثاني التعاريف المتحصل عليها من الوسائل الالكترونية، بينما خصصنا المطلب الثالث في الحديث عن المصلحة المركزية المختصة كآلية للحد والحماية من الجريمة المعلوماتية، وهذا كما يلي:

المطلب الأول : تعريف الدليل الالكتروني

يقوم مبدأ الإثبات الجنائي علي قاعدة هامة مفادها أن القاضي لا يقضي بعلمه الشخصي وأن إحاطته بوقائع الدعوى يجب أن يتم من خلال ما يُطرح عليه من أدلة يتم مناقشتها أمامه، فالدليل هو الوسيلة التي ينظر من خلالها القاضي للواقعة موضوع الدعوى، وعلى أساسه يبني قناعته. لذلك اهتمت مختلف الأنظمة القانونية علي اختلاف الأسس التي تقوم عليها، بتنظيم الأدلة الجنائية وتحديد شروط مشروعيتها واجراءات الحصول عليها وتقدير قوتها الاثباتية وحجيتها. وأن استحداث أي نوع من الأدلة يجب أن يخضع للضوابط و الشروط التي يحددها النظام القانوني الذي يقوم في ظله هذا الدليل.

لقد قيلت العديد من التعاريف في الأدلة الرقمية، فهناك من عرفها بانها:« بيانات يمكن إعدادها وتراسلها وتخزينها رقميا، بحيث تمكن الحاسوب من تأدية مهمة ما »[1] إن هذا التعريف يربط بين البيانات المخزنة وبين جهاز الحاسوب، وفي ذلك تضييق وحصر شديد لمعني الأدلة الرقمية. فهو يربط البيانات بالحاسوب، ويكون قد أقصي من التعريف، طيفا واسعا من الأدلة المتحصلة من أجهزة اخري غير الحاسوب علي غرار الهواتف النقالة الذكية والتي يمكن من خلالها الولوج الي شبكة الانترنيت والقيام بعدة عمليات اتصال معقدة. وكذلك الات التصوير الرقمية المتطورة...الخ.

كما أنه هناك من عرفها بأنها: « الدليل الذي يجد له أساسا في العالم الافتراضي ويقود الي الواقعة غير المشروعة ومرتكبها »[2] وهو تعريف يستند الي عنصرين، هما منشأ الدليل الرقمي و محيطه وهو العالم الافتراضي، والهدف أو الغاية من وجوده وهي الواقعة غير المشروعة ومرتكبها. أن التعريف باستعمال المنشأ والغاية أو الهدف، وإن كان يؤدي الي معني ينطبق علي مفهوم الأدلة الرقمية، إلا أنه

[1] وهو التعريف الذي أخذ به التقرير الأمريكي المقدم الى ندوة الانتربول العلمية حول الدليل الرقمي سنة 2001 ، ص05.

[2] د/ عمر بن محمد يونس، الجرائم الناشئة عن استخدام الانترنت، ط الاولى، دار النهضة العربية القاهرة، سنة 2004، ص 4 .

تعريف يبقي قاصرا عن الإحاطة بالمعني الكامل لها، ما دام أنه لم يتطرق الي تحديد مكونات الأدلة الرقمية ، ما دامت تلك المكونات معلومة وبإمكانها اضفاء ووضوح أكثر علي التعريف.

وعليه فإنه هناك من عرف الدليل الرقمي بأنه: « الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهى مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ و تطبيق القانون»[1].

والذي يلاحظ على هذا التعريف أنه يقصر مفهوم الدليل الرقمي على ذلك الذي يتم استخراجه من الحاسوب الآلي، ولاشك أن ذلك فيه تضييف لدائرة الأدلة الرقمية، فهي كما يمكن أن تستمد من الحاسوب الآلي، فمن الممكن أن يُتحصل عليها من أية آلة رقمية أخرى، فالهاتف و ألآت التصوير وغيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدراً للدليل الرقمي، فضلاً عن ذلك فإن هذا التعريف يخلط بين الدليل الرقمي ومسألة استخلاصه، حيث عرَّفه بأنه الدليل المأخوذ من الكمبيوتر. وهذا يعني أن الدليل الرقمي لا تثبت له هذه الصفة إلا إذا تم أخذه أو استخلاصه من مصدره وهذا ليس صحيحا، إذا من شأن التسليم بذلك القول إن تلك المجالات المغناطيسية أو الكهربائية قبل فصلها عن مصدرها بواسطة الوسائل الفنية لا تصلح لأن توصف بالدليل الرقمي، أي أن مخرجات الآلة الرقمية لا تكون لها قيمة إثباتية مادامت في الوسط الافتراضي الذي نشأت فيه أو بواسطته. كما أن هناك من عرفه بأنه: « مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية »[2].

هذا التعريف يعطي صورة أدق وأوضع للدليل الرقمي، فهو علي خلاف التعريفات السابقة، يبرز مكونات الأدلة الرقمية ويشير الي أنها، المجالات أو النبضات المغناطسية أو الكهربائية، كما أنه لا يربط تلك المجالات او النبضات المغناطسية أو الكهربائية، بأداة تقنية معينة كالحاسوب أو الهواتف الذكية أو غير ذلك، مما يجعل التعريف مرنا قابل للتكييف مع التطور التقني ما يتوصل اليه العلم من مخترعات أو انماط جديدة من الاستغلال. لكنه في رأينا يظل ناقصا، لأنه لا يمكن اعتبار جميع النبضات المغناطسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية، أدلة رقمية، إلا إذا كانت تدل علي واقعة غير مشروعة يعتبرها القانون جريمة وعلي مرتكبها.

---

[1] د/ ممدوح خالد إبراهيم، الدليل الالكتروني في جرائم المعلوماتية، بحث منشور على الانترنت الرابط:http://www.f-law.net ، ص 02

[2] د/ الجملي طارق محمد ، الدليل الرقمي في مجال الاثبات الجنائي، بحث منشور علي الانترنيت.

وعليه فان التعريف الملائم للأدلة الرقمية هو: « أنها مجموعة البيانات التي تتخذ شكلا إلكترونيا أو رقميا كالنبضات المغناطسية أو الكهربائية أو غير ذلك من الأشكال والتي تكون محفوظة و يمكن استغلالها و تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية و / أو مرئية، تدل علي واقعة غير مشروعة يعتبرها القانون جريمة وعلي مرتكبها». إن هذا التعريف يشمل العديد من المزايا، فهو يتطرق الي كنه الأدلة الرقمية وهي البيانات باختلاف أنواعها، سواءا كانت بيانات تتعلق بالمضمون ، أو بيانات خاصة بالاشتراكات أو بيانات خط السير، والتي تتخذ شكلا الكترونيا أو رقميا أو غير ذلك من الأشكال التي قد تظهر وتتجسد مع التطور التقني وتتلائم مع العالم الافتراضي الذي توجد فيه.

المطلب الثاني: الدليل الجنائي بواسطة الوسائل الإلكترونية

أولا: مفهوم الدليل الجنائي.

تعتبر الأدلة بصفة عامة من المسائل الهامة في القانون والفقه، حيث حظيت باهتمام الكثير من الدراسات الفقهية والقانونية كما تعد الأدلة الجنائية من أهم أنواع الأدلة علي الإطلاق لما لها من أهمية بالغة في إثبات الجرائم ومعاقبة مرتكبيها، وحماية المصلحة العامة والدماء والأموال و الممتلكات والحرمات من الانتهاك، وفي نفس الوقت ضمان حقوق الانسان وحرياته من الضياع لهذا فالدليل هو الوسيلة التي يستعين بها القاضي من أجل الوصول إلى الحقيقة التي ينشدها فهو كل وسيلة مرخص بها أو مسموح بها قانونا لإثبات وجود أو عدم وجود الواقعة المرتكبة أو صحة أو كذب وقوعها. لهذا يعتبر الدليل وهو جوهر الإثبات الجنائي فماهي الأدلة الجنائية وما أنواعها وما هو الفرق بينها وبين المفاهيم

ثانيا: تعريف الادلة الجنائية:

التعريف اللغوي : الأدلة جمع دليل، والدليل هو ما يستدل به، والدليل الدال أيضا، وهو المرشد والكاشف والدلالة، ويطلق علي ما يقتضي الصدق لا محالة، ومنه الحجة: وهو ما تثبت به الدعوي من حيث الغلبة علي الخصم.[1]

1) التعريف الاصطلاحي :

يعرف الدليل الجنائي عند فقهاء الشريعة الإسلامية بأنها: « ما يلزم من العلم به، العلم بشيء أخر. فاذا أعلم المدعي القاضي بحجة على دعواه، لزم من علم الفاضي بتلك الحجة مع إقتناعه بها علمه بصدق دعوى المدعي فيما ادعاه

[1] د/ عواد محمد كمال ، الضوابط الشرعية والقانونية للأدلة الجنائية، سنة 2011، دار ريم للنشر والتوزيع، ص 26.

أما فقهاء القانون الوضعي عرفوه : « أنها الواقعة التي يستمد منها القاضي البرهان علي إثبات اقتناعه بالحكم الذي ينتهي اليه »[1].

ومنها: « أنها الوسيلة الاثباتية المستخدمة في تحقيق اليقين لدي القاضي أو في ترجيح موقف الشك لديه»[2].

إن اختلاف التعاريف السابقة وإن اختلفت صيغها، نجدها تصب في مفهوم واحد، وهو أن الأدلة الجنائية هي الوسيلة والطريقة والسبيل و الأداة الوحيدة التي يتم عبرها إثبات أو نفي صحة واقعة ما وإسنادها لشخص معين.

ثانيا: الفرق بين الأدلة الجنائية و المفاهيم المشابهة لها.

يمكن ان يكون خلط لدى البعض بين الأدلة وبين بعض المفاهيم المقاربة لها، علي غرار الاثبات والاستدلال والدلالة و اجراءات الحصول علي الدليل، اين سنقوم بالتطرق فيما يلي الى محاولة توضيح وتحليل الاختلاف الموجود بين مفهوم الادلة وبين تلك المفاهيم.

1) الفرق بين الأدلة الجنائية وألدة الاثبات الجنائي:

لقد درج الفقهاء علي استعمال لفظي الدليل والإثبات كمترادفين، رغم أنه قد يكون لهما مدلولين مختلفين، فمعني الإثبات كألية يختلف عن معني الإثبات كنتيجة فالإثبات الجنائي كألية، يعني إقامة الدليل لدي الجهات المختصة علي حقيقة واقعة ذات أهمية قانونية بالطرق والقواعد التي يحددها القانون. فالإثبات الجنائي بذلك يكون أوسع مدلولا من مفهوم الدليل، بل إن الدليل الجنائي في هذه الحالة هو خلاصة عملية الاثبات الجنائي التي تمر بعدة مراحل، التي تنطلق بعملية البحث والتحري ثم التحقيق الجنائي وصولا الي المحاكمة الجنائية و هي المرحلة الاخيرة التي يكون فيها القاضي قناعته بما توصلت اليه عملية الاثبات الجنائي وما تمخضت عنه من أدلة إثبات أو نفي .

2) الفرق بين الأدلة الجنائية والاستدلال الجنائي :

يقصد بالاستدلال الجنائي، القيام بجمع المعلومات بشأن واقعة جنائية معينة قصد معاونة سلطة التحقيق علي اتخاذ قرارها بتحرك الدعوي العمومية أو حفظها. [3] فعملية الاستدلال الجنائي إذن، هي عملية سابقة عن عملية التحقيق القضائي، وهي بذلك لا ينتج عنها أي دليل ، لأن الدليل لا ينشأ الا في ظل الضوابط و الضمانات التي يقررها القانون. فمثلا لا يمكن اعتبار التصريحات التي يدلي بها

[1] د/ سلامة مأمون ، قانون الاجراءات الجنائية، ط الاولي، دار الفكر، سنة: 1980، ص 764.

[2] د/ أحمد ضياء الدين محمد خليل، رسالة دكتوراه: مشروعية الدليل في المواد الجنائية، جامعة عين شمس، سنة 1982، ص 366.

[3] د/ النمر أبو العلاء علي ، دراسة تحليلية، الاثبات الجنائي، دار النهضة العربية، ط الثانية، ص: 05.

المشتبه فيه أمام عناصر الضبطية القضائية بارتكابه لجريمة ما اعترافا جنائيا، لأنها لم تنشأ في ظل الضوابط والضمانات القانونية التي يجب أن ينشأ فيها الدليل الجنائي على غرار حقوق الدفاع ، وضمانات الحياد... الخ،

3) الفرق بين الأدلة الجنائية وبين الدلالة :

تعرف الدلالة على انها جمع دلائل، وهي عملية الاستنتاج العقلي الذي يمارسه القاضي لإيجاد الصلة بين واقعتين، بهدف التوصل الي معرفة حكم الواقعة المعلومة أو الثابتة بالنسبة له[1]. وهي بهذا المعني تشبه القرينة إلا أنها أقل درجة في الاثبات منها. فالقرينة هي ما يستنبطه المشرِّعُ أو القاضي من أمر معلوم على أمر مجهول أو هي استنتاج شيء معيّن إذا توافرت الوقائعُ التي يعتبرها القانون أساسًا لهذا الاستنتاج بدلاً من الاعتماد على الوقائع والظروف المحتملة. في حين أن الدلالة تحتمل صور شتي من التأويل والاحتمال.

4) الأدلة الجنائية وكيفية الحصول عليها:

قد يلتبس الأمر لدي البعض، بخصوص التمييز بين الأدلة الجنائية وبين الوسائل الإجرائية التي قررها القانون للحصول عليها، فيعتقد أن تلك الوسائل الاجرائية أدلة جنائية ، والحقيقة خلاف ذلك. ذلك لأن الوسائل الإجرائية ما هي الا شكليات قررها القانون وحدد لها ضوابط وأحاطها ببعض الضمانات الغرض منها البحث عن الأدلة الجنائية خلال مباشرة عملية التحقيق القضائي. وبمعني أخر، فإن الوسائل الاجرائية هي الايطار الشكلي للأدلة الجنائية .

ثالثا: أقسام الأدلة الجنائية.

انقسم الفقه بشأن مسألة إطلاق أو تقييد او تقسيم الأدلة الجنائية إلي ثلاثة اتجاهات رئيسية، اتجاه يري عدم جواز تقييد حرية الاثبات في المسائل الجنائية واتجاه ثاني يري بعدم جواز اطلاق الاثبات في المسائل الجنائية، واتجاه ثالث توافقي بين الاتجاهين الاول والثاني .

1) الاتجاه الاول :

الذي يطلق عليه المذهب الحر أو المطلق2 و القائل بحرية الاثبات في المسائل الجنائية، يري أن تقييد حرية الاثبات في المسائل الجنائية قد يؤدي الي اهدار الكثير من الحقوق والاضرار بمصلحة المجتمع في مواجهة الجريمة. ذلك أنه لا يمكن توقع مكان وزمان وقوع الجريمة أو الظروف التي سترتكب فيها ، حتي يتم تصور ووضع الايطار القانوني اللازم لإثباتها.

[1] د/ عواد كمال محمد ، الضوابط الشرعية والقانونية للأدلة الجنائية، دار ريم للنشر والتوزيع، سنة 2011، ص 41.

[2] د/ عواد كمال محمد ، المرجع السابق، ص:46.

ويري أصحاب هذا الرأي، أن حرية الإثبات في المسائل الجنائية وإن كانت تعني حرية القاضي في تكوين اقتناعه بناءا علي الأدلة الجنائية التي تقدم اليه، لكن ذلك لا يعني أنه حر في إتباع أهوائه وميولاته الشخصية .

2) الاتجاه الثاني:

ويطلق عليه اسم المذهب المقيد[1]، فيري أصحابه بضرورة تقييد حرية الاثبات في المسائل الجنائية، وذلك بالنص علي طرق محددة في الاثبات يتقيد بها خصوم الدعوي الجنائية والقاضي علي حد السواء، بحيث لا يمكن اثبات الجريمة واسنادها لمرتكبها ولا يمكن للقاضي الوصول الي الادانة الا من خلال تلك الوسائل التي قررها القانون فلا مجال لإعمال السلطة التقديرية للقاضي ولا مجال للأخذ باقتناعه الشخصي.

فاذا كان القانون هو الذي يحدد عناصر الواقعة الاجرامية فمن الأجدر أن يقوم بتحديد أدلة وطرق اثبات تلك العناصر، فالقانون لا يعترف بالحقيقة الواقعية الا اذا تم اثباتها بالطرق التي حددها وتصير بذلك عبارة عن حقيقة قضائية[2].وهذا مايراه اصحاب هذا الاتجاه .

3) الاتجاه الثالث:

يطلق عليه تسمية النظام المختلط [3]، لأخذه بالاتجاهين السابقين معا فهو يأخذ بنظام الاثبات المقيد في اثبات بعض الجرائم، وفي نفس الوقت يأخذ بنظام الاثبات الحر في البعض الاخر من الجرائم. فنجد أن بعض الجرائم يحدد لها القانون طرق ووسائل اثبات محددة بحيث لا يجوز اثباتها بخلاف الأدلة التي يتطلبها القانون فالقاضي مقيد في تكوين اقتناعه بالأدلة المنصوص عليها قانونا كما هو الحال بالنسبة لا ثبات جريمة الزنا. وفي جرائم أخري لا يخول للقاضي السلطة التقديرية في تقييم الدليل بل عليه الأخذ به كما نص عليه في القانون إلا في حالة الطعن بالتزوير

4) تقسيمات الأدلة من حيث مصدرها :

ان الفقه سعى الى تقسيم الأدلة الجنائية، وخرج بالعديد من التقسيمات من حيث مصدرها ومن ابرزها اربعه تقسيمات وهي :

[1] د/ عواد كمال محمد ، المرجع السابق، ص77.

[2] د/ حسني محمود نجيب ، شرح قانون الإجراءات الجنائية، دار النهضة العربية، ط الثالثة، سنة 1997، ص 407.

[3] د/ عواد كمال محمد ، المرجع السابق، ص 46.

1.4. الدليل المادي : وهو نوع من الادلة التي لها وجود مادي، أي أنها تستند إلي عناصر مادية يمكن إدراكها باستعمال الحواس أو بالاستعانة بأداة علمية، فهي أدلة مباشرة، كمثل الأدوات التي استعملت في ارتكاب الجريمة والبصمات.

2.4. الدليل القولي : تعتبر مختلفة عن الأدلة المادية، فإن الأدلة المعنوية هي التي تصل إلى علم المحقق على لسان الغير، ومثالها الاعتراف والشهادة.

3.4. الدليل الفني : وهو الدليل الناتج عن الخبرة، بحيث يشترط رأي خبير بشأن وقائع معينة. فالأدلة الفنية مناطها الخبرة والتجربة .

4.4. الدليل القانوني : وهو الذي ينص عليه القانون في إثبات بعض الجرائم، بحيث لا تقترن الإدانة إلا بتوفر الدليل وبصحته علي غرار الإقرار القضائي في جريمة الزنا.

5) تقسيم الأدلة من حيث علاقتها بالواقعة المراد إثباتها.

تنقسم اعتبارا بالواقعة المراد إثباتها، إلي أدلة مباشرة وأدلة غير مباشرة.

1.5. الأدلة المباشرة : هي أدلة قاطعة في إثبات الجريمة، والوقائع المرتكبة من طرف الجاني، فالقاضي يكون اقتناعه في إثبات الوقائع ولا يحتاج إلى أدلة أخرى، وهذه الأدلة تنقسم بدورها إلى عدة أقسام التي منها: الاعتراف ،الشهادة. وبالتالي فهي دليل إثبات سهل ومؤكد

2.5. الأدلة غير المباشرة : اطلق عليها اسم الأدلة غير المباشرة، لأنها لا تنصب على الواقعة المراد إثباتها بصورة مباشرة، وإنما بصورة غير مباشرة، أي بمعنى أنها تنصب على واقعة أخرى ذات صلة منطقية وثيقة بها، وعلى المحقق أن يحكم عقله فيستنبط من الواقعة التي انصب الدليل عليها الواقعة الأخرى التي يراد إثباتها، فمثلا لو أراد المحقق أن يثبت وجود الجاني في مسرح الجريمة

6) تقسيم الأدلة من حيث الأثر المترتب عليها.

تنقسم إلى ثلاثة أقسام، هي:

1.6. أدلة الاتهام : وهي الأدلة التي تحيل المتهم للمحاكمة، غير أنها لا تصلح لأن تكون أساسا للإدانة لعدم كفايتها، وهي بذلك تكون بحاجة إلي أدلة أخري[1].

2.6. أدلة النفي : وهي الأدلة التي تكون في صالح المتهم وهذا عن طريق تبرئته أو تخفيف مسؤوليته[2].

[1] د/ حسين محمود ابراهيم، الوسائل العلمية الحديثة في الإثبات، دار النهضة العربية، سنة 1981، ص45.

[2] د/ حسين محمود ابراهيم، المرجع السابق، ص 45.

3.6. أدلة الحكم : وهي الأدلة التي تكون في حد ذاتها أساسا وعمودا فقريا للحكم بالإدانة، فهي الأدلة الوحيدة التي تتوفر فيها كافة الشروط و الضوابط القانونية ولا تحتاج إلي أدلة أو قرائن أخري تعززها[1].

المطلب الثالث: المصلحة المركزية المختصة كآلية للحماية والحد من الجريمة المعلوماتية

أولا: أساليب الحماية من الجرائم الإلكترونية

إن الأنترنت إختراع بشري يحمل في طياته بدور الشر والخير معا، ولم يكن منذ الوهلة الأولى موضوع الحماية المعلوماتية مطروحا حيث كان إستعماله محتكرا من طرف فئة معينة إلا أن إنتشار إستعمال الأنترنت أظهر عيوبا، فسجل أول إختراق للشبكة سنة 1988 حيث توقف عملها لمدة ثلاث أيام ولذلك كان لابد من إيجاد برامج أمنية وقواعد قانونية للحماية من الجرائم الإلكترونية.

1) المرحلة الأولى :

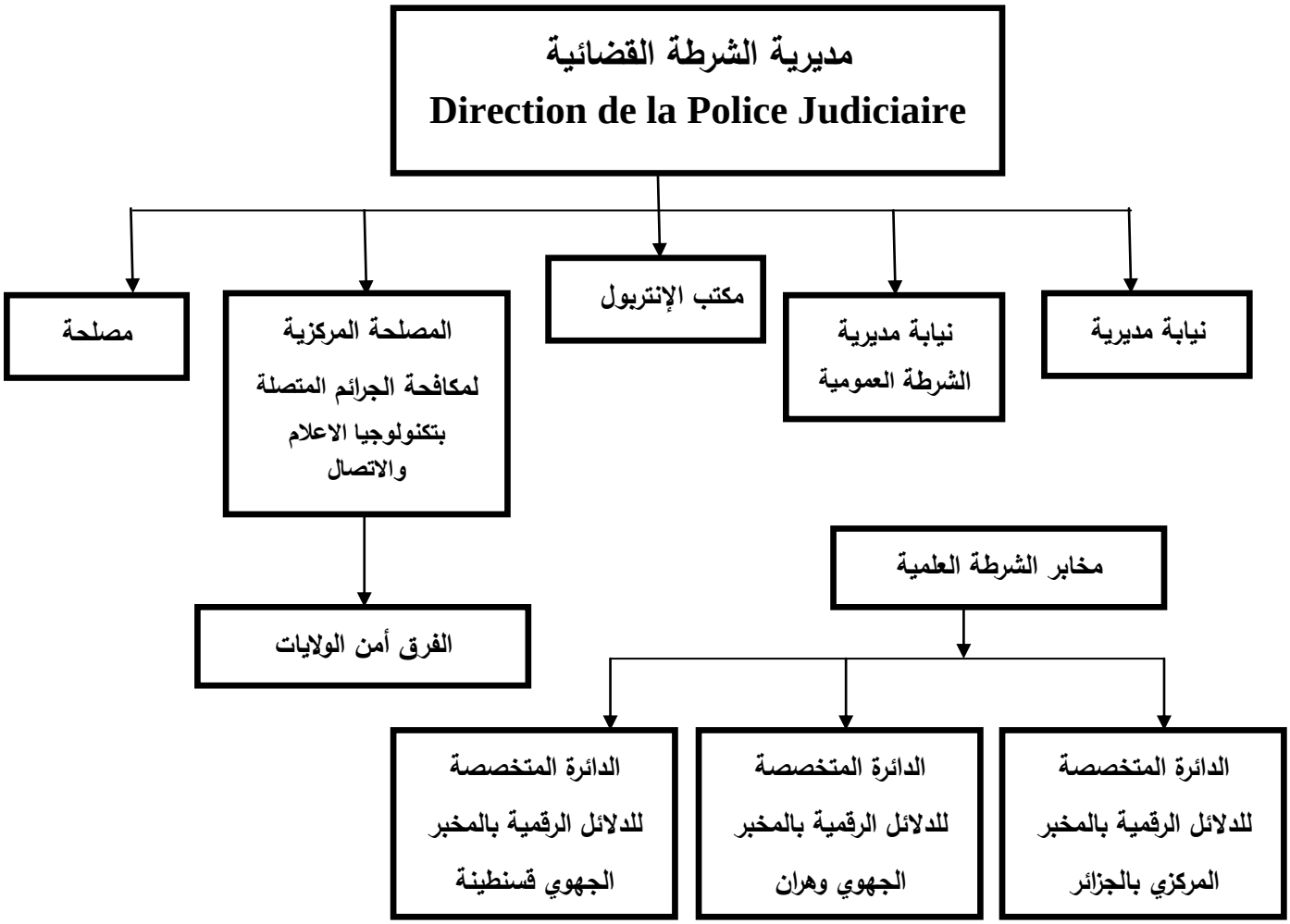
على غرار ما جاء به قانون العقوبات لسنة 2004 تم إنشاء هيئة وطنية للوقاية من جرائم تكنولوجيا الاعلام والاتصال سنة 2007 والتي أعلن عنها المرسوم الرئاسي الصادر في شهر أكتوبر 2015 والتي تعمل تحت اشراف ومراقبة لجنة مديرة يترأسها وزير العدل ، وتتضمن أعضاء من الحكومة ومسئولي مصالح الامن وقاضين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء ، كما تم عقد عدة اتفاقيات أهمها اتفاقية بودابيست التي تم ابرامها سنة 2001 صادقت عليها الدول الأوربية وهي اتفاقية لها مزايا تسمح بتبادل المعلومات بصفة فعالة ، من جهتها صادت الجزائر على اتفاقية عربية لمكافحة الجريمة المعلوماتية سنة 2014 ، كما تجدر الإشارة إلى أن المديرية العامة للأمن الوطني قدمت مقترحا لسلطات العليا في البلاد لدراسة إمكانية المصادقة على اتفاقية بودابيست ،مع ضرورة تشديدها على اقتناء أحدث الوسائل والمعدات المستعملة في التحقيقات الجنائية ، كما أشار رئيس المصلحة إلى برمجة دورات تكوينية ف مجال التكنولوجيات الحديثة وتقنيات التحقيق الالكتروني بداية من سنة 2007 إلى غاية سنة 2014 بمشاركة خبراء أجانب وجزائريين لفائدة 402 شرطي ، في حين استفادت 4 إطارات من ثلاث دورات تكوينية بالخارج .

مما أدى إلى قفزة نوعية في مجال محاربة الجريمة المعلوماتية ، حيث تم معالجة 245 قضية لسنة2014 تتعلق بالمساس بالأشخاص ، و168 قضية منها 49 قضية تتعلق بالاعتداء على سلامة الأنظمة ، كما تم معالجة 11 قضية تتعلق بما يصطلح عليه الإرهاب الالكترونية ، و9 قضايا تتعلق بإباحية الأطفال ، وبلغت نسبة معالجة هذه القضايا 65% .

[1] د/ أمال عبد الرحيم عثمان ، شرح قانون الإجراءات الجنائية ، سنة 1989، ص 400.

2) المرحلة الثانية:

تم تشكيل المصلحة المركزية المختصة لمكافحة الجريمة الالكترونية حيث تم توسيع التشكيل الأمني بتكوين فصائل على مستوى أمن الولايات 58 ويتم بعدها إنشاء المصلحة المركزية المختصة لمحاربة الجرائم المتصلة بجرائم الاعلام و الاتصال بقرار من المدير العام من الأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015 كما هو موضح في المخطط التالي:



نماذج مأخوذة من المصلحة الولائية للشرطة القضائية لفرقة مكافحة الجريمة المعلوماتيّة بأمن ولاية الوادي توضح حالة التهديدات السيبرانية

ثانيا: الجانب الأمني من الحماية

يتعلق هذا الجانب بكل ما هو فتي وتقني لحماية شبكة الأنترنت والكمبيوتر وسوف نطرحه في ثلاث نقاط، مسائل تتعلق بأمن المعلومات، مهددات أمن المعلومات وفي الأخير الإجراءات الأمنية .

مسائل تتعلق بأمن المعلومات يتعلق أمن المعلومات بالمواضيع التالية[1]

1) **المسألة الإدارية** : يوجد في كل مؤسسة كمية هائلة من المعلومات تخزن في الحاسوب، ونظرا لأهميتها تحتاج إهتمام أمني.

2) **المسألة المالية** : تتمثل في الكلفة المالية المصروفة قصد حماية النظم المعلوماتية والحاسوبية ذات القيمة الكبيرة ،

3) **المسألة الوظيفية** : يجب أن تكون المعلومات جاهزة لإستعمالها عند الحاجة وتكون صحيحة وسرية وكاملة.

4) **مسألة الخصوصية** : يجب حماية النظم الذاتية الخاصة بالأشخاص والا سوف يساء إلى الحرية الفردية بإفشائها وبها

5) **مسألة تحديد مخاطر وحوادث الكمبيوتر والشبكة** : هذه الحوادث قد تكون طبيعة أو مفتعلة وتطور تقنيات الحاسوب وإنشاء الاتصالات الحاسوبية يجعل تحديد المخاطر أكثر تعقيدا.

6) مهددات أمن المعلومات : هي الحالة أو الظرف الذي يؤدي حتما إلى تعطيل الشبكة المعلوماتية وأنواع هذه المهددات:

- مهددات طبيعية مثل الزلازل التي تؤدي إلى قطع الاتصالات بالشبكة.
- مهددات غير مقصودة من طرف الإنسان كسوء استعمال كلمة السر.
- مهددات إنسانية، وهو ما يقوم به المتسللون الذين يخترقون المواقع.

7) **الثغرات الأمنية** : يمكن كشفها من طرف الهاكرز خصوصا في الحواسب الشخصية، إما على مستوى خطوط الإتصال فهي معرضة للمراقبة بالإشعاعات، أو الاتصال والتجسس، لأنه يستخدم للإتصال بشبكة الأنترنت الألياف البصرية والأقمار الصناعية، كما يمكن إعتراض طريق وصل الأسلاك للإستراق عن طريق الشبكة. كما توجد ثغرات في بروتوكولات الإتصالات في شبكة الأنترنت وكذا الثغرات الموجودة في برامج البريد الإلكتروني E-Mail حيث لا يوجد ما يمنع من إستعمال وتغير محتوى الرسالة البرامج الخبيثة ولها عدة أنواع مثلا

[1] – سامر محمد سعيد – الانترنات و المخاير دار سعاد الصاح المطابع التعاورية الصحافية بيرو لبنان 1992 .ص74

- **الفيروسات وحصان طروادة :** هذا الأخير يمكن أن يفرغ الملفات من محتوياتها.
- **الباب السري أو الخلفي :** يسمح بالدخول دون المرور بأجهزة أو برامج الحماية.
- **الدودة :** برنامج يؤدي إلى تخريب الملفات التي يدخلها .

هذه المهددات وغيرها هي التي تعترض أمن المعلومات والتي لازالت تتطور بتطور العلم.

8) الإجراءات الأمنية : إن الوقاية هي أمثل الأساليب نقعا في هذه الجرائم ومن بينها: .

1.8. إستخدام جدار الحماية Fire Well : وهو حاجز يوضع بين الشبكة الداخلية للأنترنت وخادم الشبكة . ومن أهم مهامه فحص المعلومات الواردة والخارجة والسماح لها بالمرور في حالة مطابقتها للمواصفات، وتقديم تقارير عن التحركات المشبوهة. ولكنه يمكن أن يعطل بعض المعلومات ويحدث عطب.

2.8. التشفير : وهو تحويل المعلومة من نص واضح إلى آخر غير مفهوم وقد استحسن هذا النوع من النظام لنجاعته في عدم كشف المعلومات على شبكة الأنترنت.

3.8. التوقيع الرقمي : وهي تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية، إستخدام أنظمة كشف الإختراقات ووضع حلول للثغرات الأمنية

- وضع سياسة أمنية للشبكة وحشد كل الإمكانيات البشرية والمادية لتطبيقتها.
- الإحتفاظ بنسخ إحتياطية لكل المعلومات الحساسة في أقراص إضافية ليست مرتبطة بالشبكة
- تنصيب برامج لمنع ظهور الصور الخليعة والإتصال بالمواقع الإرهابية.
- ويرى الدكتور عبد الفتاح مراد في كتابة التحقيق الجنائي الفني ضرورة إستخدام بعض البرامج التي صممت خصيصا للكشف والوقاية من الفيروس والبعد عن إستعمال كلمة السر البسيطة.

الفصل الثاني

وسائل الاثبات والعراقيل الاجرائية في اثبات الجريمة المعلومات

بعد أن تطرقنا في الفصل الأول إلى ماهية الجرائم الالكترونية من خلال تعريفها وأنواعها والخصائص التي تمتاز بها والدوافع المؤدية إلى ارتكابها، كان علينا لزاما أن نتطرق في الفصل الثاني إلى وسائل الإثبات والتحري في الجرائم الالكترونية، على ضوء التشريع الجزائري، بحيث سنتطرق إلى أهم العراقيل الاجرائية والحلول التشريعية للحد منها، بحيث قمنا بتقسيم هذا الفصل إلى مبحثين:

المبحث الأول : وسائل الاثبات والتحري في الجرائم الإلكترونية في ظل التشريع الجزائري

المطلب الأول: التفتيش الالكتروني

المطلب الثاني: الخبرة

المطلب الثالث: اعتراض المراسلات

المبحث الثاني : الحلول القانونية للحد من العراقيل الإجرائية في اثبات الجرائم المعلوماتية

المطلب الأول: عراقيل تقنية وعراقيل بشرية

المطلب الثاني: عراقيل قضائية

المطلب الثالث: الحلول القانونية قصيرة المدى وطويلة المدى

المطلب الرابع: الحلول القانونية طويلة المدى

المبحث الأول : وسائل الاثبات والتحري في الجرائم الالكترونية في ظل التشريع الجزائري

الجريمة الإلكترونية تمتاز بخصائص وعناصر تميزها عن الجرائم التقليدية المنصوص عليها في القوانين، فأن قواعد هذه القوانين تبدو قاصرة إزاء ملاحقة مرتكب الجريمة الإلكترونية وهذا ما يبرز كأمر واقع مسألة صعوبة جمع الاستدلالات والأدلة في جريمة المعلوماتية، وأيضا تطبيق الإجراءات الجنائية التقليدية، بحيث تتوفر على أساليب خاصة للاثبات والتحري في الكشف على مرتكبيها وعلى هذا الأساس فقد قسمنا هذا المبحث إلى ثلاث مطالب، يتضمن الأول : التفتيش الالكتروني، فيما يتمحور المطلب الثاني حول الخبرة بينما في الثالث تطرقنا فيه إلى إعتراض المراسلات.

المطلب الأول: مفهوم التفتيش الالكتروني

تعريف التفتيش والقيود والشروط التي ترد عليه.

- **التعريف اللغوي:** يعرف التفتيش على انه الاستقصاء في الطلب والبحث.
- **التعريف الاصطلاحي:** يعرف على انه البحث عن أدلة الجريمة وكل ما يفيد في كشف الحقيق من أجل إثباتها أو إسنادها للمتهم سواء كان محله شيئا أو مكانا أو شخصا، فهو اجراء من اجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق أو ترجح وقوعها فى محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبة.
- **تعريفات اخرى** :هناك عدة تعاريف للتفتيش فنجد من عرفه على انه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات و تخزين و مخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبها إلى المتهم بارتكابها»[1].

ولما يكتسيه التفيش على اهمية بالغة التحقيق في التحقيق الابتدائي، حيث يعتبر استثناء على القاعدة العامة التي تنص على حرمه الحياة الخاصة المواطن الخاصة وحرمة شرفه وحرمة مسكنه [2] . وهذا مانصت عليه المواد 300و303 من قانون العقوبات الجزائري .

1) الشروط والقيود المتعلقة بالزمن:

لقد نصت ونوهت معضم التشريعات الجنائية اجراءات التفتيش بقيود زمنية ، بحيث يجوز اتخاذ اجراءات التفتيش الا في الوقت الذي حددته تبعا لطبيعة أو خطورة الجريمة المرتكبة وهذا حسب المواد

[1] د/ هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، ط1، دار النهضة العربية، القاهرة، سنة 1997، ص 73.

[2] وهذا ما نصت عليه المادة 40 من الدستور الجزائري بنصها: « تضمن الدولة عدم انتهاك حُرمة المسكن، فلا تفتيش إلا بمقتضى القانون، وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة».

44الى47 من قانون الاجراءات الجزائية فلا يجوز التفتيش خارج الايطار الزمني الذي حدده القانون. وأن أي مخالفة لذلك، تؤدي إلي بطلان إجراءات التفتيش.

2) الشروط والقيود المتعلقة بالمكان:

اذا كان التفتيش هو استثناء علي القاعدة القائلة بحرمة المساكن، فذلك يعني أنه يجب أن يقع التفتيش على مسكن. أو على محل يحظى بالحماية القانونية، حتي تستفيد هذه الأخيرة من القيود التي فرضها القانون. وبمفهوم المخالفة، فان جميع الاماكن غير المعدة للسكن، والتي لا تحظي بحماية قانونية خاصة لا يمكن أن تستفيد من القيود التي ضربها القانون علي اجراءات التفتيش، كالأماكن العمومية و الأماكن المعدة لاستقبال الجمهور.

3) الشروط والقيود المتعلقة بالأشخاص أو الجهة المشرفة علي التفتيش:

نظرا لما تكتسيه عملية التفتيش لاهمية بالغة ونظرا لخطورتها فقد أخضعته التشريعات الجنائية لإشراف السلطة القضائية وتحت رعاية ضابط شرطة قضائية مختص اقليميا كما أناطته ببعض الضمانات المتمثلة في حضور صاحب المسكن أو من يمثله أو شخصين أخرين غير تابعين لسلطة القائم بالتفتيش.

1.3. الفرع الثاني: مدد ملائمة اتخاذ اجراءات التفتيش للبحث عن الادلة في الجرائم المعلوماتية.

إن النتيجة المستنبطة التي يمكن الخروج بها من خلال التطرق الى الشروط والقيود التي فرضها واقرها القانون في عملية التفتيش هي أنها شروط وقيود تفترض وجود مسرح مادي لجريمة تقليدية علي غرار القتل أو السرقة، الامر الذي يثير التساؤل حول مدي جدوي اجراءات التفتيش في التحقيق والبحث عن الأدلة في جريمة معلوماتية من هنا يثير هذا التساؤل مبرراته في اختلاف الطبيعة الحقيقية والخصائص التي تمتاز بها الجريمة المعلوماتية عن غيرها من الجرائم التقليدية . لقد اتجه بعض الفقهاء في تحليلهم لمسرح الجريمة المعلوماتية الي أنه يتكون من جزئين:

2.3. مسرح الجريمة التقليدي : يقع مثل هذا النوع من المسارح خارج بيئة الحاسوب، حيث يتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون الى مسرح أية جريمة تقليدية قد يترك فيها الجاني آثار عدة، كالبصمات وغيرها وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.

3.3. مسرح الجريمة الافتراضي : تكون مثل هاته الجرائم داخل البيئة المعلوماتية للحاسوب، ويتكون من البيانات الرقمية التي تتواجد وتتنقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الأقراص الصلبة

الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع[1].

لهذا يعتبر مسرح الجريمة الافتراضي مسرح خاص بحيث يخضع لنص لاجراء التفتيش الالكتروني وهذا طبقا لنص المادة 05 من القانون رقم: 09-04 المؤرخ في 14 شعبان 1430 الموفق ل 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها على أنه: « يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول، بغرض التفتيش.

أولا: مدى صلاحية الكيان المنطقي للحاسوب كمحل يرد عليه التفتيش.

إن تفتيش المكونات المنطقية للحاسوب أثار خلافا كبيرا في الفقه بشأن جواز تفتيشها فذهب رأي إلى جواز ضبط البيانات الالكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك على إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي شيء فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسوب المحسوسة و غير محسوسة[2]. والذي يشمل بيانات الحاسوب أم لا، فان الضبط يجب أن يقع عليها متي إذا اتخذت شكلا ماديا[3].ويذهب رأي فقهي[4] إلى أنه يجب عدم الخلط في تحديد مدلول الشيء بالنسبة لمكونات الحاسوب بين الحق الذهني للشخص على البرامج و الكيانات المنطقية وبين طبيعة هذه البرامج و الكيانات، و إنما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرف بأنها كل ما يشغل حيزا ماديا في فراغ معين و إن الحيز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزا ماديا في ذاكرة الحاسوب و يمكن قياسها بمقياس معين، و أنها أيضا تأخذ شكل نبضات إلكترونية، فإنها تعد طبقا لذلك ذات كيان مادي و تتشابه مع التيار الكهربائي الذي اعتبره الفقه و القضاء في فرنسا و مصر من قبيل الأشياء المادية.

نجد على ضوء هذه الآراء الفقهية، وعلى النحو الذي سنه المشرع الجزائري صراحة وجوهريا في إمكانية وقوع التفتيش على مساكن أشخاص يظهر أنهم يحوزون على أشياء لها علاقة بالأفعال الجنائية فان

[1] محمد بن نصير محمد السرحاني، مرجع سابق، ص 77.

[2] د/ حسين بن سعيد بن سيف الغفاري، التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، بحث منشور علي الرابط http://www.minshawi.com،

[3] د/ حسين بن سعيد بن سيف الغفاري، المرجع نفسه، ص20.

[4] د/ علي محمود علي حموده، مرجع سابق، ص17.

التفتيش يرد على الكيانات المعنوية في الحاسوب، بحسب أن هذه الكيانات المعنوية وإن كانت غير مادية إلا أنها تدخل في نطاق الأشياء المادية[1].

نجد انه يترتب على ذلك أنه يمكن تفتيش نظام معلومات الحاسوب ووسائط أو أوعية حفظ وتخزين البيانات المعالجة آليا كالأسطوانات والأقراص والأشرطة الممغنطة ومخرجات الحاسوب، وفقا للمادة 05 من القانون رقم: 09-04 المؤرخ في 14 شعبان 1430 الموفق ل 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها حيث يدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته[2].

ثانيا: ضوابط التفتيش الذي يقع على المكونات المنطقية للحاسوب.

إذا كان يتعبر التفتيش كإجراء جزائي يهدف الي الوقوف على دليل اثبات يساعد في الكشف عن الجريمة فان حكمه يرتبط بطبيعة المكان المراد تفتيشه، من هنا يمكننا القول هل هو من الأماكن العامة أو من الأماكن الخاصة، حيث أن لصفة المكان وطبيعته أهمية قصوى في مجال التفتيش، فإذا كانت المكونات المادية للحاسوب موجودة في مكان خاص كمسكن المتهم أو ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المسكن وبنفس الضمانات و الإجراءات المقررة قانونا. و اذا كانت تلك المكونات المادية متصلة بحواسيب أخرى موجودة في مساكن أو أماكن أخري غير مسكن المتهم، تعين مراعات القيود و الضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن3. لذلك نجد قانون سوء استخدام و التعامل بالحاسوب في انجلترا الصادر في سنة 1990 حيث نص أن إجراءات التفتيش تشمل بما في ذلك أنظمة الحاسوب[4].

إن التفتيش الوارد علي الكيان المنطقي لأجهزة الحاسوب والأنظمة المعلوماتية يخضع لبعض القيود يجب مراعاتها تحت طائلة البطلان. منها ما نصت عليه المادة 44 من قانون الإجراءات الجزائية بعد تعديله بالقانون رقم 06 – 22 ،على عدم جواز إجراء التفتيش من قبل ضابط الشرطة القضائية إلا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش.

---

[1] د. هلالي عبد الله أحمد، مرجع سابق، ص 89.

[2] د/ هشام رستم ، المرجع السابق، ص69.

3 د/ عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسوب الآلي، مرجع سابق، ص 37

[4] WASIK (MARTIN) ، Computer Crimes And Other Crimes Against Information Technology In The United Kingdom- Rev، Inter، De، Dr، Panal 1993،P:640.

ايضا نجد ان المادة 47 علي إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل دون احترام الأوقات المذكورة في الفقرة الأولى في المادة 47 من قانون الإجراءات الجزائية، إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات غير أنه يشترط أن يكون مصحوبا بإذن مسبق من وكيل الجمهورية المختص أو قاضي التحقيق.

والشيء الملاحظ هو أن المشرع الجزائري عندما تطرق في نص المادة 05 من القانون رقم: 09-04 المؤرخ في 14 شعبان 1430 الموفق ل 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها علي جواز تفتيش أي منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها أو أي منظومة تخزين معلوماتية، فإنه حسب رأيينا قصد في هذا الشيء الأنظمة المعلوماتية التي تقع داخل الدولة وحتى لوكانت متصلة ببعضها البعض وهذا من خلال طريق شبكة محلية.

لكن هنا يثار تساؤل جوهري يتمحور مضمونه في حالة ما إذا اتصلت بحواسيب أخرى خارج الدولة عن طريق الربط الشبكي بين أجزاء العالم المختلفة، ومنها شبكة الانترنت.

ففي حالة وقوع جريمة في نظم الحاسوب داخل الدولة الجزائرية فيجوز هنا لوكيل الجمهورية أو قاضي التحقيق إصدار الإذن بالتفتيش. لكن هذا الإذن بالتفتيش لا ينفذ إلا على الحاسوب الذي صدر من أجله، ويترتب على ذلك أنه إذا كان الحاسوب المراد تفتيشه يتصل بحاسوب أخر لم يصدر بالنسبة له إذن بالتفتيش لا يمكن أن يمتد إليه التفتيش حتى لو كان يحتوي على أدلة الجريمة. إلا إذا أمر قاضي التحقيق هنا في إذنه بالتفتيش أن يمتد على مستوى التراب الوطني بكامله حسب الفقرة الأخيرة من نص المادة 47. لكن في حالة الإذن بالتفتيش على حاسوب واحد معين، يتعين استصدار إذن جديد بالتفتيش للحاسوب الثاني إذا تبين أنه متصل عن طريق شبكة داخلية بالحاسوب الذي أذن التفتيش فيه.

هناك حالة أكثر تعقيدا تواجه تفتيش أجهزة الحاسوب، وذلك عندما يقوم المجرم بتخزين بياناته في أنظمة حواسيب تقع خارج الدولة الجزائرية هنا يمكننا القول باننا في صدد مواجهة معضلة كبرى ،في هذا الصدد فان تفتيش هاته الحواسيب التي تتصل بحواسيب داخل الدولة أمر قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها، وغياب أليات التعاون في هذا المجال، رغم أنه يمكن اتخاذ هذا الإجراء عن طريق اتفاقات خاصة تعقد بين الدول المعنية وهذا وفقا لقانون تعاوني بينهم .

ثالثا: مدى خضوع أجهزة الحاسوب والانظمة المعلوماتية للتفتيش عن بعد.

تطور التكنولوجيا الرقمية و اختلاف أشكال الاتصالات وتعقيداتها، وضعت الكثير من التحديات أمام التحقيقات المتعلقة بالجرائم المعلوماتية، لا سيما أمام القيام بعملية التفتيش و الضبط في مجال الجرائم المعلوماتية الوطنية العابرة للحدود. فالبيانات التي تحتوي على أدلة جنائية ، قد يكونتوزعها وتنضيمها عبر شبكة حواسيب في أماكن مجهولة بعيدة تماما عن الموقع الذي يجري فيه التفتيش. و إن كان من الممكن الوصول إلي تلك البيانات من خلال حواسيب تقع في الموقع الجاري تفتيشه، غير أن تلك البيانات قد تكون موجودة فعليا، داخل اختصاص قضائي أخر أو حتى في بلد أخر. وهو ما يثير مسألتين هامتين هما مسألة الاختصاص القضائي و مسألة التعاون الدولي.

و من هذا المنطلق يمكننا أن نميز بين ثلاثة انواع من الاحتمالات وهي التالي :

1) **الاحتمال الأول:** اتصال وارتباط حاسوب المتهم بحاسوب أخر أو نهاية طرفية موجودة في مكان أخر داخل الدولة. يثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسوب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان أخر مملوك لشخص غير المتهم ؟

يرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجزائية الألماني [1] .

2) **الاحتمال الثاني :** ارتباط و اتصال حاسوب المتهم بحاسوب أخر أو نهاية طرفية موجودة في مكان أخر خارج الدولة، فمن المشاكل التي تواجه سلطة الادعاء أو التحقيق في جمع الأدلة قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمين في ذلك شبكة اتصالات عن بعد، مستهدفين عرقلة التحقيقات المتبعة لأجل جمع الأدلة. و في هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها الإذن و دخوله في المجال الجغرافي للدولة أخرى، و هو ما يسمى بالولوج أو التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها.

3) **الاحتمال الثالث:** عملية ومهمة التصنت و المراقبة الالكترونية لشبكات الحاسوب والتي تكون تحت اشراف الجهات القضائية المختصة والجهات الامنية والعسكرية المعنية يتبين وتوضح بان التنصت و الأشكال الأخرى للمراقبة الالكترونية، رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريبا. بالذهاب الى القانون الفرنسي الصادر في 1991/08/10 يجيز اعتراض

[1] KASPERSEN(W.K.HENRIK)،Computer Crime And Other Crime Against Information Technology In Netherland،R.I.D.P.1993،P 479

الاتصالات عن بعد بما في ذلك التي تتم عن طريق شبكات تبادل المعلومات. و في هولندا أجاز المشرع، لقاضي التحقيق، حيث وضح بأهن يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة ضالع فيها المتهم و تشمل هذه الشبكة التلكس و الفاكس و نقل البيانات.[1] و تفتيش نظم الحاسوب الآلي يمكن أن يتم بعدة طرق ، فمثلا المرشد الفيدرالي الأمريكي [2] جاء بأربع طرق أساسية للتفتيش ممكنة التحقيق هي:

- طريقة تفتيش الحاسوب و طبع نسخة ورقية من ملفات معينة في نفس الوقت.
- طريقة تفتيش الحاسوب و طبع نسخة الكترونية من ملفات معينة في ذات الوقت.
- طريقة عمل نسخة إلكترونية طبق الاصل من جهاز التخزين بالكامل في الموقع، ومن بعدها إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.
- طريقة ضبط الجهاز و إزالة ملحقاته ومحوها و مراجعة محتوياته خارج الموقع.

4) تفيش المنظومات المعلوماتية:

تفتيش المنظومات المعلوماتية هو الأمراء الذي استحدته المشرع الجزائري بموجب المادة 05 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحها، حيث أجاز للسلطات القضائية المختصة وكذا عنباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليه في المادة من من ذات القانون اسئل هذه الحالات في:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة
- حالة توفر معلومات عن احتمال اعداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني
- لمقتضيات الحريات والتحليلات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية
- في إطار تنفيذ المساعدة القضائية المتبادلة).

الدخول بغرض التفتيش ولو من بعد إلى منظمة معلوماتية أو جزء منها وكذا العمليات المعلوماتية الحرة فيها، ومنظومة خزين معلوماتية وبالرغم من أن المشرع الجزائري لم يحدد المقصود بتفتيش المنظومات

[1] KASPERSEN (W.K.HENRIK0) op-cit، p500-501

[2] تم وضع هذا المرشد عام 1994 وصدر له ملحقان في عامي 1999/1998، ولقد قام بإعداده مجموعة عمل في قسم جرائم الحاسوب الآلي والملكية الفكرية بإشراف أستاذ القانون الجنائي ORIN KERR، و لقد صدرت له تعديلات آخرها كان تعديل 2002 الذي تضمن تطبيقا للقانون الوطني الأمريكي الصادر في 2001/10/56.

أعرف المجلس الأوروبي تفتيش المنظومات المعلوماتية بأنه إجراء يسمح بجمع الأدلة المحرمة أو المسجلة بشكل قانوني)، إلا أنه عرف المنظومات المعلوماتية على أنها أي نظام منفصل أو مجموعة من الافعال التي لها الصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر معالجة آلية للمعطيات، تنفيذا لبرنامج معين (المادة 02 الفقرة (ب) من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 14 نعمان عام 1430 الموافق : 05 أوت سنة 2009). ولقد أصاب الشرع الجزائري بوضع هذا التعريف لإزالة اللبس والغموض الذي ورد في المادة 394 مكرر عندما استعمل للمشرع الجزائري مصطلح منظومة للمعالجة الالية للمعطيات، ثم استعمل في المادة 394 مكر 1 مصطلح نظام معاجلة أليه، وهو ما تم تقسوة على أن الجريمة لا تقوم في الحالة الأولى إلا إذا تم ارتكاها على منظومة كاملة للمعاينة علمية لأنظمة مترابطة إذا ما تفيدنا بنص المادة التي تعمل مصطلح نظام معالجة آلية[1].

بحيث أن المنظومة المعلوماتية تكون في شكل نظام منفصل أو في شكل مجموعة من الأنظمة المتصلة ببعضها (عرفت المادة 02 الفقرة الخامسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، النظام المعلوماتي، باله: مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات).

كما يدخل في إطار التفتيش للمعلوماتي ما عبر عنه تفتيش المنوعات المعلوماتية عن بعد، فهو يعني كحيلة طبيعية للتطور الرهيب لتكنولوجيا المعلومات مع الإمكانيات الكبيرة التي توفرها في التواصل ونقل البيانات عبر العالم، وتخزينها في مكان داخل وخارج أقاليم الدول، في شكل شبكة معلوماتية. وهو ما حدا بالمشرع الجزائري إلى تناول موضوع تفتيش المنظومات المعلوماتية من بعد من خلال نص المادة 05 من القانون 09-04 حيث يميز بين صورتين، الأول: إذا كانت هناك أسباب تدعو لاعتقاد بأن العمليات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول بها انطلاقا من المنظومة الأولى، جور تعدد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المحمية مسبقا بذلك، وهو ما من شأنه حل المشاكل القانونية والقضائية المتعلقة باتصال بين الاختصاص في تفتيش المعلومات المعلوماتية، والمتعلقة كذلك مشروعية الدليل المتحصل عليه أمام الجهات القضائية، أما الصورة الثانية فهي إذا تبين مسبقا بأن العمليات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المطبوعة الأولى، مزامنة في منظومة معلوماتية تقع جاري الإقليم عليه فإن الحصول عليها يكون بمساعدة السلطات الأحجية المحتمة طبقا للاتفاقيات الدولية ذات الصلة، ووفقا

[1] دفاتر البحوث العلمية، المجلد 9، العدد الأول، سنة 2021، ص 227 - 243

لمبدأ المعاملة بالمثل، لذلك حرمت الكثير من الدول على إبرام اتفاقيات ثنائية أو متعددة الأطراف لتسهيل التعاون الاحترازي في المتابعة، وفي نفس الإطار. ووفقا لما جاء به تقرر اخلي الأوروبي، فإن الاختراق المباشرة بعد انتهاكا لسيادة دولة أخرى، مما لم توجد اتفاقية دولية في هذا الشأن، وأن استرجاع البهارات التي تم تخزينها بالخارج دون علم الدولة الأخرى وراها، بعد انتهاكا لسيادنا وحرقا للقوانين (خالد، 2009 ص 203)، إضافة إلى ذلك فقد مكن المشرع الجزائري السلطات المكلفة بالتفتيش، تسخر كل شخص له دراية يعمل المظلومية المعلوماتية محل البحث، أو بالتدابير المتحدة لحماية المعطيات التي تتضمنها، وذلك قصد مساعدة هذه التأملات في عملها وتزويدها بكافة المعلومات الضرورية لأتاح وإنجاز المهمة المادة 05 الفقرة 4 من القانون 09 – 04، المتعلق بالوقاية من الجرائم الصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق ل: 05 اوت سنة 2009). وحرصا على تكريس الشرعية الإجرائية في حال أثمرت عملية التفتيش عن وجود معنيات عارية: استحدث المشرع الجزائري موجب نفي المادة 06 من القانون 09-04 المتعلق بالوقاية من الجرائم تكنولوجيا الإعلام والاتصال ومكافحتها وما هي تحريات العمليات، وهو إجراء من خلاه يجيز للسلطة التي تباشر التفتيش في منظومة معلوماتية، في حالة اكتشافها معطيات معينة مفيدة في الكشف عن الحرام أو عركيا أن تسخ هذه المعطيات، وكذا المعطيات اللازمة لفهمها على دعامة خرين إلكترونية تكون قابلة للحجر والموقع في أحراز، وفقا للقواعد المقررة في قانون الإجراءات الجزئية

هذا ما لم يكن من الضروري حجز كل المنظومة، أما عن القواعد المقررة في قانون الإجراءات الجزائية التي أشارت إليها المادة 06 من الفانون 09-04، فهي تلك الضوابط المنصوص عليها في نص المادة 84 من قانون الإجراءات الجزائية التي تجعل القاضي التحقيق وضابط الشرطة المنوب عنه، فقط دون غيرهما الحق الاطلاع على المستندات المبحوث عنها، مع مراعاة ما تقتضيه ضرورات التحميل التي يأتي على رأسها كان السر المهني واحترام حقوق الدفاع (المادة 83 الفقرة الثالثة من قانون الإجراءات الجزائية المعدل والمتم[1].

وتوضع الأشياء المحجوزة بعد إحصائها صورة قوية لي أحراز مختومة لا يتم فتحها إلى حضور المتهم مسحوبا بمحاميه أو بعد استدعائهما قانونا، كما يمكن استدعاء كل من ظنت لديه هذه الأشياء لحضور هذا | الإجراء (المادة 84 من قانون الإجراءات الجزائية المعدل والمتمم). وتم حجز المعطيات وفقا لما تصي عليه المشرع الجزائري بطريقتين مختلفتين تتمثل أولاهما في نسخ المعطيات المعلوماتية،

[1] دفاتر البحوث العلمية، المجلد 9، العدد الأول، سنة 2021، ص 227 – 243

والثانية في الحجز عن ضيق منع الوصول إلى العملات المعلوماتية. فيالة له العمليات فإنه وبالرجوع إلى نص المادة 06 من القانون 09 – 04، أجاز المشرع استخلاص السليل عن طريق نسخ المعلومات المضبوطة وخزنها في دعامات، مع الحرص على استعمال كافة الوسائل النقية لتنكيل أو إعادة تشكيل المعطيات محمل البحث ولحمها واستخلاصها، من أجل جعلها قابلة للاستغلال لأغراض التحقيق مع مراعاة عدم المساس محتوى المعطيات المادة 06 الفقرة 3 من القانون 04.09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المؤرخ في 14 شعبان عام 1430 الموافق 1: 05 أوت سنة 2009).

أما المحتوى من منع الوصول إلى المعلمات، فهو طريقة استثنائية، يتم اللجوء إليها في حالة عدم إمكانية إجراء الحجز عن طريق النسخ لأسباب نفسية، لذلك فإنه يتعين على السلطة التي تقوم بالتفتيش، استعمال التقنيات المناسبة، طلع الوصول أو إلى نسخ العضلات التي تحتويها المنظومة المعلوماتية الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة (المادة 07 من القانون 09 – 04، المتعلق بالوقاية من الجرائم السملة بتكنولوجيا الإعلام والاتصال ومكافحها، المؤرخ في 14 نعمان عام 1430 الموافق له 05 أوت سنة 2009). كما يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على العمليات التي بشكل متاحة جريمة (المادة 08 من القانون 09 – 04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق 1: 05 أوت سنة 2009)، وفي كل الأحوال فإنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة، إلا في الحدود الضرورية للتحريات والتحقيقات القضائية[1].

المطلب الثاني: الخبرة

ان الخبرة تعتبر من احدى وسائل البحث والتحري عن الأدلة الجنائية التي تمتاز بطابع فني بحيث تعتبر وسيلة من وسائل التحقيق القديمة لكنها في ذات الوقت فعالة في التحقيق المعمق خاصة في مجال الجرائم المعلوماتية باعتبار أن الادلة الرقمية هي أدلة علمية وتقنية وذلك ماسنتطرق اليه ونوضحه من خلال تعريف الخبرة وهذا ما وضحه قانون الاجراءات الجزائية في المواد 143//144//145//146//147 وهي كالاتي :

[1] المادة 09 من القانون 09 – 04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحها المؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت سنة 2009.

المادة 143 : (معدلة لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم.

وإذا رأى قاضي التحقيق أنه لا موجب للاستجابة لطلب الخبرة فعليه أن يصدر في ذلك أمرا مسببا في أجل ثلاثين (30) يوما من تاريخ استلامه الطلب وإذا لم يبت قاضي التحقيق في الأجل المذكور، يمكن الطرف المعنى إخطار غرفة الاتهام مباشرة خلال عشرة (10) أيام، ولهذه الأخيرة أجل ثلاثين (30) يوما للفصل في الطلب، تسري من تاريخ إخطارها. ويكون قرارها غير قابل لأي طعن.

ويقوم الخبراء بأداء مهمتهم تحت مراقبة قاضي التحقيق أو القاضي الذي تعينه الجهة القضائية التي أمرت بإجراء الخبرة[1].

المادة 144 : يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة وتحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسمائهم بقرار من وزير العدل ويجوز للجهات القضائية بصفة استثنائية أن تختار بقرار سبب خبراء ليسوا مقيدين في أي من هذه الجداول.

المادة 145 : يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الأتي بيانها :

" أقسم بالله العظيم بأن أقوم بإبداء مهمتي كخبير على خير وجه وبكل إخلاص وإن أبدي رأيي بكل نزاهة واستقلال"[2].

ولا يجدد هذا القسم ما دام الخبير مقيدا في الجدول ويؤدي الخبير الذي يختار من خارج الجدول قبل مباشرة مهمته اليمين السابق بيانها أمام القاضي التحقيق أو القاضي المعين من الجهة القضائية ويوقع على محضر أداء اليمين من القاضي المختص والخبير والكاتب ويجوز في حالة قيام مانع من حلف اليمين لأسباب يتعين ذكرها بالتحديد أداء اليمين بالكتابة ويرفق الكتاب المتضمن ذلك بملف التحقيق.

المادة 146 : يجب أن تحدد دائما في قرار ندب الخبراء مهمتهم التي لا يجوز أن تهدف إلا إلى فحص مسائل ذات طابع فقي

المادة 147 : يجوز لقاضي التحقيق ندب خبير أو خبراء[3].

---

[1] الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 الذي يتضمن ق . ا . ج ، المعدل والمتمم، سنة 2007، ص 59.

[2] المرجع نفسه، ص59.

[3] الأمر رقم 66 – 155، مرجع سابق، ص 59.

1) تعريف الخبرة.

التعريف اللغوي : جاء في القرآن الكريم في الآية 59 من سورة الفرقان (فسئل به خبيرا) من هنا تعرف لغويا على انها تعريف الشيء على حقيقته. وخبر الشيء، علمه عن تجربة، وتفسير ذلك معناه فأسأل به عارفا يخبرك بالحق في صفته.

التعريف الفقهي : تعرف على انها هي وسيلة من وسائل الإثبات يتم اللجوء إليها إذا اقتضى الأمر كشف دليل أو تعزيز أدلة قائمة ، كما أنها استشارة فنية يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى دراية علمية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته[1]، كما يمكن تعريفها على أنها المهمة الموكولة من قبل المحكمة أو الهيئة القضائية إلى شخص أو إلى عدة أشخاص أصحاب اختصاص أو مهارة أو تجربة في مهنة ما أو فن أو صنعة أو علم لتحصل منهم على معلومات أو آراء أو دلائل إثبات لا يمكن لها أن تؤمنها بنفسها وتعتبرها ضرورية لتكوين قناعتها للفصل في نزاع معين[2].

كما تعرف بأنها استبيان و استيضاح رأي أهل الخبرة في مجال استظهار بعض جوانب الوقائع المادية التي يستعصى على قاضي الموضوع إدراكها بنفسه من مجرد مطالعة الأوراق والتي لا يجوز للقاضي أن يقضي في شأنها استنادا لمعلوماته الشخصية وليس في أوراق الدعوى وأدلتها ما يعين القاضي على فهمها .

2) مدى ملائمة أعمال الخبرة في التحقيق في الجرائم المعلوماتية.

يكمن دور الخبرة في مجال التحقيقات الجنائية وهذا في الكشف عن الجرائم الاكترونية، فنجد معظم دول العالم لا يزال جهاز الحاسوب أو الشبكات المعلوماتية والأدلة المستخرجة منها من اختصاص أهل الخبرة. و قد أجاز المشرع الجزائري، للمحقق الاستعانة بخبير متخصص في المسألة موضوع الخبرة، فقد نصت المادة 143 قانون الإجراءات الجزائية في فقرتها الأولى على أنه يجوز لكل جهة قضائية تتولى التحقيق أو تجلس للحكم إذا تعرض لها مسالة ذات طابع فني أن تأمر بندب خبير إما بناءا على طلب النيابة أو التحقيق أو الخصوم أو من تلقاء نفسها.

بناءا عليه فإذا كانت الاستعانة بخبير في المسائل الفنية البحة أمر واجب على جهة التحقيق و القاضي، فهي أوجب في مجال الجرائم الالكترونية ، حيث تتعلق بمسائل فنية بالغة التعقيد و محل الجريمة فيها غير مادي و التطور في أساليب ارتكابها سريع و متلاحق، و لا يكشف غموضها إلا

[1] د/ عبد الحميد الشواربي، التزوير والتزييف مدنيا وجزائيا في ضوء الفقه والقضاء ، منشأة ، مصر1996، ص 552.

[2] د/ أميل أنطوان ديراني، الخبرة القضائية، المنشورات الحقوقية الصادرة سنة 1977، ط1، بيروت، ص 17.

متخصص و على درجة كبيرة من التميز في مجال تخصصه ، فإجرام الذكاء و الفن لا يكشفه و لا يحله إلا ذكاء و فن مماثلين.

و بالعودة إلى نص المادة 146 نجد أن المشرع يفرض على الجهة القضائية الأمرة بندب خبير، تحديد مهمته بدقة. و هذا يعود بنا إلى ضرورة تأهيل سلطات التحقيق أو الحكم في الجرائم المعلوماتية لنجاح الهدف المتوخى من التحقيق في هذا النوع المستجد من الجرائم.

كما تجدر الإشارة الي أنه يجب على القاضي اختيار الخبراء ذوي الإمكانيات العلمية و المقدرة الفنية الحالية فلا يكفي مجرد الحصول على شهادة علمية، إذ يجب مراعاة الخبرة العلمية، فالوسائل الالكترونية متعددة وفي تطور مستمر و شبكات الاتصال بينها متنوعة فطبيعتها الفنية تجعلها موزعة على تخصصات فنية و علمية دقيقة [1].

و تقتضي فاعلية الخبرة ضرورة الجمع بين التعمق في كل من الدراسة العلمية و النظرية و الممارسة العملية للتخصص العلمي و النظري، وكذا متابعة مستمرة للتطورات التي تلحق بفروع التخصص، غير أن ذلك ليس شرطا لازما في بعض الأحيان فقد يقتصر الخبير على مجرد الخبرة العملية في فرع التخصص دون أن يكون هناك رصيد من الدراسة العلمية والنظرية وهو الأمر الذي نلاحظه في مجالات الخبرة في الفروع المهنية المختلفة2. و الخبير لا يشترط فيه فحسب كفاءة علمية عالية في مجال التخصص.

يضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه، و على وجه الخصوص الجرائم ذات الصلة بالحاسوب، فقد يتعلق الأمر بتزوير المستندات أو التلاعب في البيانات أو الغش أثناء نقل أو بث البيانات أو جريمة من الجرائم الأموال أو الاعتداء على حرمة الحياة الخاصة أو عرض صور أو أفلام مخلة بالآداب العامة.

و تستوجب طبيعة الجرائم المعلوماتية توافر شروط خاصة في الخبير الذي ينتدب لبحث مسائل فنية وعلمية متعلقة بها، وهي:

– الإلمام بتركيب الحاسوب و صناعته، طرازه، نوعه، نظم تشغيله الرئيسية و الفرعية الأجهزة الطرفية الملحقة به، و كلمات المرور أو السر و أنماط التشفير.

– طبيعة البيئة التي يعمل في ظلها الحاسوب أو الشبكة من حيث تنظيم و مدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين و الوسائل المستخدمة في ذلك.

[1] د/ هشام محمد فريد رستم، المرجع السابق، ص 140 و 141.

[2] د/ محمد فاروق عبد الحميد كامل، المرجع السابق، ص 286.

– المكان المحتمل لأدلة الإثبات و شكلها و هيئتها.

– قدرة الخبير على إتقان المهام المسندة اليه، دون أن يترتب على ذلك أعطاب أو تدمير الأدلة المحصلة من الوسائل الإلكترونية.

– التمكن من نقل أدلة الإثبات غير المرئية و تحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بدون أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على الحاسوب أو النظام أو الشبكة[1]

و أهمية الاستعانة بالخبير في مجال الجرائم الالكترونية، تظهر عند غيابه، فقد تعجز الشرطة عن كشف غموض الجريمة و قد تعجز هي أو جهة التحقيق عن تجميع الأدلة حول الجريمة وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه. و من التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم الالكترونية القانون البلجيكي الصادر في 23 نوفمبر سنة 2000.

فقد نصت المادة 88 من القانون المذكور على أنه يجوز لقاضي التحقيق و الشرطة القضائية أن تستعين بخبير ليقدم و بطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام و كيفية الدخول فيه أو الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته و يعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة لتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق[2] و وفقا للقانون المشار إليه فإن الالتزام بتشغيل النظام و استخراج البيانات المطلوبة منه

يرجع إلى قاضي التحقيق بصفة أصلية، و يجوز كذلك للنيابة العامة على سبيل الاستثناء في حالة التلبس بالجريمة، أو عند الرضا بعملية التفتيش3. فمهمة الخبير وفقا للنص السابق تتمثل من ناحية في تشغيل النظام، ومن ناحية أخرى في تقديم البيانات المطلوبة حسب الطريقة التي تريدها جهة التحقيق، كان تسجل وتسلم تلك البيانات علي الأقراص الممغنطة أو مضغوطة أو على ورق.

و التزام الخبير هو التزام ببذل عناية، فلا يسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته، أو بسبب العقبات التي واجهته أثناء مباشرته لمهمته، ويمكن أن تثور مسؤوليته الجنائية إذا رفض القيام بالمهمة المكلف بها، أو أتلف عمدا البيانات المطلوبة منه التعامل معها أو حفظها.

[1] د/ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 138.

[2] MEUMIER (C) : Art ، Prec ، P 681.

[3] - MEUMIER (c) : art ، prec ، p 682.

المطلب الثالث: اعتراض المراسلات

تطرق المشرع الجزائري في نص المادة 65 مكرر 5 من قانون الإجراءات الجزائية لاسلوب من اساليب التحري الخاصة والمتمثل في اعتراض المراسلات والاتصالات الالكترونية من الطرق الاجرائية الحديثة التي تعتمد علي التقنية والتجهيزات الالكترونية والتي تم ابتكارها لمواجهة الجرائم الخطيرة التي تهدد الأمن والسلامة العامة علي غرار الجرائم الارهابية، الجرائم المعلوماتية ، المسماس بحرمة الحياة الخاصة التشهير ،...الخ.

أولا: مفهوم اعتراض المراسلات الالكترونية.

في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

المادة 65 مكرر 5: إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي :

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية

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

يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

تنفذ العمليات المسموح بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة[1]

تنص المادة:39 من الدستور الجزائري علي أنه: « لا يجوز انتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، يحميها القانون، سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة ».

[1] الأمر رقم 66 – 155 ، مرجع سابق، ص 33.

لم ينص المشرع الجزائري تعريفا أو مفهوما محددا لاعتراض المراسلات أو الاتصالات الإلكترونية. لكنه أشار الى أنها تتم بوضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها.

ومن ثم لا يجوز التصنت عليها أو الاطلاع على الأسرار التي تحتويها إلا بذات الطرق التي ينص عليها قانون الإجراءات الجزائية، فلا يستطيع الشخص اختراق صندوق البريد الالكتروني، أو الدخول الي أنظمة الحاسوب المخزنة به الرسائل البريدية الالكترونية و ضبطها إلا عن طريق إتباع إجراءات قانونية محددة في القانون و من قبل أشخاص مخولين قانونا بذلك.

من جهة فقهاء القانون يتضح لنا جليا اختلاف ارائهم الفقهية في تكييف إجراء اعتراض المراسلات السلكية و اللاسلكية ، فمنهم من ذهب رأي إلى أنها تعد تفتيشا، و بالتالي تخضع لقيوده و استندوا في ذلك إلى أن هذه المراقبة تتفق مع التفتيش في أن الهدف منها هو البحث و ضبط ما يفيد الوصول إلى الحقيقة، و لا أهمية لان يكون الشيء المضبوط ماديا أم معنويا، و هي ذات الغاية من المراقبة و التصنت فهي البحث عن الدليل[1].

في حين ذهب رأي من جمهور الفقهاء إلى التمييز والفصل و التفرقة بين التفتيش و المراقبة، بحيث جعلوا من الاول كإجراء هدفه الوصول والعثور على الأدلة المادية و ضبطها بوضع اليد عليها لمصلحة العدالة، والثاني اعتبروه ليس له كيان مادي ملموس و القول بأن الرسائل الالكترونية، أو الحديث في التليفون يندمج في كيان مادي يمكن ضبطه، فأسلاك التليفون أو التسجيل ليس دليلا في حد ذاته و إنما هي وسيلة أو أداة لسماع الحديث و لا تتأثر طبيعته بوسيلة أو أداة للحصول عليه [2].

ومن خلال الاراء السابقة يتضح الرأي الأصح في نظرنا، هو أن طرق واساليب التحري الخاصة المتمثلة في التفتيش و اعتراض المراسلات هما إجراءان مختلفان كل الاختلاف ، ولكل منهما طبيعته وشروطه ومبرراته، فالتفتيش هو استثناء علي المبدأ الدستوري الذي يقضي بحرمة المسكن والحياة الخاصة. واعتراض المراسلات هو استثناء علي المبدأ الدستوري الذي يقضي بحرمة المراسلات والاتصالات الخاصة وسريتها. كما أن اجراءات التفتيش تتخذ بعد وقوع الجريمة، اما اجراءات اعتراض المراسلات والاتصالات فإنها تكون فورية أي خلال عملية ارسال البيانات بمعنى اخر تكون سباقة قبل وقوع الفعل المجرم .

[1] د/ رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجبل للطباعة، الطبعة السادسة عشر، 1985 ، ص 358 .

[2] حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل اجازة المدرسة العليا للقضاء، 2008، ص 55.

ثانيا: ضوابط التي ترد علي اجراء اعتراض المراسلات الالكترونية.

ان اعتراض المراسلات والاتصالات الالكترونية يعتبر استثناء على القاعدة الدستورية التي تقضي بسرية المراسلات و الاتصالات الخاصة، فقد أحاط المشرع هذه الوسيلة الاجرائية بمجموعة من القيوم والضوابط تتمثل في أن تتم في حالات معينة وتحت اشراف السلطة القضائية.

و قد تطرق المشرع الجزائري في تعديله الأخير لقانون الإجراءات الجزائية بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 في نص المادة 140 المتممة للباب الثاني من الكتاب الأول من الأمر رقم 66-155 بفصل الرابع تحت عنوان " اعتراض المراسلات و تسجيل الأصوات و التقاط الصور" و المواد 65 مكرر 5 إلى المادة 65 مكرر 10 لإجراء اعتراض المراسلات. كما تطرق في القانون رقم 09 – 04 المؤرّخ في 5 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الي الحالات التي يسمح فيها باللجوء الي المراقبة الالكترونية.

إذ اعطى صلاحيات خولت لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم محددة على سبيل الحصر في نص المادة 65 مكرر 5 و والتي تكون في نوع معين ومحدد من الجرائم مثل جرائم المساس بأنظمة المعالجة الآلية للمعطيات، الذي يسمح الإذن بالدخول إلى المحلات السكنية أو غيرها و لو خارج المواعيد المنصوص عليها في المادة 47 من قانون الإجراءات الجزائية بغير رضا أو حتى علم الأشخاص الذين لهم حق تلك الأماكن، و تنفيذ عمليات المراقبة هنا تكون تحت المراقبة المباشرة لوكيل الجمهورية أو لقاضي التحقيق.[1] والذين بدور يأذنون لضابط شرطة القضائية المختص اقليميا من القيام بهذا الاجراء والذي اوجب على ضابط الشرطة القضائية تحرير محضر عن أي عملية اعتراض أو تسجيل، أو وضع ترتيبات تقنية و عمليات الالتقاط و التثبيت و التسجيل الصوتي أو السمعي البصري، و يذكر تاريخ بداية هذه العمليات و الانتهاء منها، كما يودع أي تسجيل أو اعتراض أو نسخ تم أثناء عملية المراقبة و يودعها بالملف. بحيث حدد اجل 04 اشهر كحد اقصى قابله للتجديد وهذا مانصت المادة 65 مكرر 7 من قانون الاجراءات الجزائية.

[1] حاجب هيام، المرجع السابق، ص57.

المبحث الثاني : الحلول القانونية للحد من العراقيل الاجرائية في اثبات الجرائم المعلوماتية

إن أنشطة مكافحة جرائم المعلوماتية أظهرت تحديات و مشاكل كثيرة تختلف في جوانب كثيرة عن التحديات و المشاكل التي ترتبط بالجرائم التقليدية. حيث تتسم الجرائم التي ترتكب في نطاق الانظمة المعلوماتية وشبكة الأنترنيت، بكون أن محلها معلومات أو برامج معالجة أليا عبر الحواسيب، أو جرائم تتعلق بالأشخاص عبر عالم افتراضي غير متناهي و غير محدود، مما يعطيها طابع خاص ليس فقط في طريقة ارتكابها، بل كذلك في الوسيلة التي ترتكب بها، و رغم الجهود المبذولة للحد من الجرائم المرتكبة عبر الانترنت، سواء كانت من طرف المشرعين أو من طرف سلطات التحقيق و الضبطية القضائية دولية كانت أو داخلية، الا أن هذه الجهود تصطدم بعدة عراقيل وصعوبات.

المطلب الأول: عراقيل تقنية وعراقيل بشرية

أولا: المعوقات المرتبطة بصعوبة اكتشاف الجريمة.

نجد من بين هذه المعوقات:

عدم وجود اثار مادية للجريمة: تبقي أغلب الجرائم المعلوماتية مجهولة، ما لم يتم التبليغ عنها للجهات المعنية. وفي هذا الصدد تجدر الإشارة أن أهم الجرائم لا تصل إلى علم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية لا تخلف أثار مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة[1]. فالعديد من الجرائم الالكترونية تتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية، كجرائم التجسس التي تتم عن طريق اعتراض النبضات الالكترونية، وعن طريق زرع برامج تجسس خاصة في أجهزة الحاسوب، وجرائم اختلاس التي تتم عبر تعديل البرامج و التلاعب بالأنظمة المعلوماتية. ويرجع السبب في افتقاد الآثار التقليدية للجريمة المرتكبة عبر الانترنت إلى ما ذكره بعض الفقهاء من أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسوب دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معدا ومخزنا على جهاز الحاسوب[2] .

كما أن الوسائل التي ترتكب بها الجرائم المعلوماتية تتخذ شكل قالب غير تقليدي فهي ترتكب عادة عن طريق نقل المعلومات على شكل نبضات الكترونية غير مرئية تنساب عبر أجزاء الحاسوب،

---

[1] د/ عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دراسة متعمقة في جرائم الحاسوب الالي و الأنترنت، بهجات للطباعة و التجليد، مصر، 2009، ص41.

[2] د/ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص 83.

وشبكة الاتصالات العالمية بصورة آلية، كما تنساب الكهرباء عبر الأسلاك[1] تأتي من هنا مشكلة ضبط هذه المعطيات و إحرازها في شكل الكتروني ووضعها في قالب قانوني لاستغلالها في البحث و إذا كانت بعض التجهيزات و التقنيات تسمح للباحثين بالوصول إلى هذه المعطيات التي تبقى في ذاكرة الحاسوب المستعمل، إلا أنها تتطلب خبرة عالية وإمكانيات قد لا تتوافر عادة لدى مصالح الشرطة القضائية المكلفة بالبحث وحتى في حالة حجز المعطيات الرقمية، فان البيانات أو المعلومات التي تشتمل عليها لا تتضمن آثار أو بصمات يمكن الاستدلال من خلالها على صاحبها، بل يحتاج الوصول إلى هذا الهدف إلى عمليات بحث و تحري أخرى للوصول على نسق من القرائن المادية التي يمكن الاستدلال من خلالها على المجرم، بل يحتاج الوصول إلى هذا الهدف إلى عمليات بحث و تحري أخرى التي يمكن أن تعزز دلالتها و قيمتها في الإثبات.

الطبيعة المتعدية للحدود الجغرافية التي تتمتع بها الجريمة المعلوماتية: اذا تطلب ارتكاب جريمة تقليدية علي غرار القيام بسرقة مصرف ما، تنقل المجرم الي موقع ذلك المصرف والدخول اليه ومن ثمة السطو علي الاموال الموجودة فيه، مع ما قد يترتب عن ذلك من نتائج وأدلة هامة، نتيجة تواجد المجرم بمسرح الجريمة فقد يتم التعرف عليه من بعض الشهود وقد يتم التقاط صور له باستعمال اجهزة المراقبة ، وقد يتم اكتشاف هويته من خلال البصمات التي يتركها خلفه،. لكن الامر يختلف بالنسبة للجرائم المعلوماتية لا سيما تلك المرتكبة عبر الانترنيت. فغالبا ما ترتكب تلك الجرائم عن بعد، أي انها جرائم لا تشترط وجود المجرم في الموقع الذي تتحقق فيه النتيجة الاجرامية، فبإمكان المجرم المعلوماتي ان يتسلل الي انظمة مصرف ما قد يقع داخل دولته او خارج حدودها الاقليمية ويقوم بعمليات تحويل مصرفية لأموال ضخمة من حسابات المصرف او من حسابات زبائنه الي حسابات سرية، دون ان يخلف دليلا واحدا ضده. وقد يتسلل المجرم المعلوماتي الي شبكة معلوماتية داخلية أو الي جهاز حاسوب مرتبط بشبكة الانترنيت ويقوم بنسخ ما يشاءا من ملفات وصور وافلام خاصة، دون ان يدرك الضحية ذلك. إن الطبيعة المتعدية للحدود الجغرافية التي تتمتع بها الجريمة المعلوماتية وامكانية ارتكابها عن بعد تشكل عائقا هاما في اكتشاف بعض الجرائم المعلوماتية التي قد لا يترتب عنها اضرار مادية.

[1] د/ محمد حماد مرهج الهيتي، جرائم الحاسوب- ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، الطبعة الاولى، دار المناهج للنشر و التوزيع، عمان، 2006، ص99.

ثانيا: معوقات تتعلق بصعوبة اثبات الجريمة.

نجد من بين تلك المعوقات:

فرض الجناة لتدابير أمنية: يعمد المجرمون عبر الانترنت عادة إلى إخفاء جرائمهم أو تمويهها علي أنها أعطال أو اخطاء في أنظمة التشغيل، أو إزالة أثار الجريمة عن طريق التلاعب بقواعد البيانات و القوائم في جهاز الحاسوب و البرامج، لا سيما أن التخزين الالكتروني غير مرئي و البيانات كثيرة وهي مكتوبة بلغة رقمية لا تفهمها إلا الآلة ما لم تستعاد على شاشة الكمبيوتر، ليتمكن الإنسان من قراءتها و فهمها، وهذا يشكل عقبة أمام إقامة الدليل على الجريمة المرتكبة عبر الانترنت و إثباتها [1]، فلا مرية أن المجرمين الذين يرتكبون جرائم بالوسائل الالكترونية الحديثة من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم الغير مشروعة قبل ارتكابها لكي لا يقعوا تحت طائلة العقاب. فهم قد يزيدون من صعوبة إجراءات التي يتوقع حدوثها للبحث عن الأدلة التي قد تدينهم باستخدام كلمات السر التي لا تمكن غيرهم من الوصول إلى البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال، و قد يلجأ هؤلاء المجرمون أيضا إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها بحيث قد يستحيل على غيرهم الاطلاع عليها و يتعذر على جهات التحري و الضبط الوصول إلى كشف أفعالهم غير مشروعة.

بالإضافة إلى ذلك يقوم المجرمون عبر الانترنت بإخفاء هويتهم أو انتحال شخصية أخرى حتى لا يمكن التعرف عليهم في حالة اكتشاف الجريمة ، وقيام المحققين بالتحري عنها، حيث توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيته، سواء أثناء إرسال البريد أو أثناء تصفح المواقع، فهم يسعون من خلالها إلى إخفاء شخصيتهم و الفرار من مسائلة نظامية[2].

و يعتبر انتحال الشخصية عبر البريد الالكتروني من بين أكثر الطرق استعمالا من طرف المجرمين عبر الانترنت، حيث يقومون بتزييف رسائل البريد الالكتروني لتبدو صادرة من شخص أخر.

الطبيعة غير المادية للأدلة المستخرجة من الوسائل الالكترونية: يكون دليل الإثبات في الجريمة التقليدية مرئيا من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب و كذلك المادة السامة التي

[1] د/ فريد منعم جبور، حماية المستهلك عبر الإنترنت و مكافحة الجرائم الالكترونية (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010،

[2] محمد بن عبد الله بن علي المنشاوي، جرائم الانترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية ، الرياض – السعودية، 2003، ص 54.

تستعمل في القتل أو المحرر ذاته الذي تم تزويره، أو النقود التي زيفت و أدوات تزييفها، وفي كل هذه الأمثلة يستطيع رجل الضبط أو التحقيق الجنائي رؤية الدليل المادي و ملامسته بإحدى حواسه[1].

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

فلا يوجد شك في إثبات الأمور المادية التي تترك أثار ملحوظة. بعكس إثبات الأمور غير المرئية، فإنه يكون في منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي أثار قد تدل عليه أو تكشف عنه بحسبان أن أغلب المعلومات و البيانات التي تتداول عبر أجهزة الحاسوب و التي من خلالها تتم العمليات الالكترونية تكون في هيئة رموز و نبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال تلك الحواسيب او اجهزة أكثر تعقيدا ، فالجرائم التي ترتكب على العمليات الالكترونية التي تعتمد في موضوعها على التشفير و الأرقام السرية و النبضات والتخزين الالكتروني يصعب أن تخلف ورائها أثار مرئية قد تكشف عنها أو يستدل من خلالها على الجناة.[2]

فالطبيعة غير المرئية للأدلة المتحصل عليها من الوسائل الالكترونية تعد أحد ابرز المشكلات التي تلقي بظلالها على الجهات التي تتعامل مع الجرائم المعلوماتية وتجعل من الكشف عن هذا النوع من الادلة وتجميعه لإثبات وقوع الجريمة و التعرف على مرتكبها عملية صعبة ومعقدة.

صعوبة الوصول إلى الدليل: لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول المواقع والتي تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها و الاطلاع عليها أو استنساخها.

سهولة محو الدليل الرقمية أو تدميرها في زمن قصير جدا: وهو ما يعبر عنه بخاصية تطاير البيانات، فالأدلة الرقمية وبحكم أنها بيانات معبر عنها بلغة الألة والارقام، يمكن التلاعب بها واخفائها بسهولة، وبالتالي يعتبر ذلك من بين الصعوبات التي يمكن أن تعترض العملية الإثباتية في مجال الجرائم المعلوماتية بحيث يقوم الجاني بمحو أو تدمير أدلة الإدانة التي تكون قائمة ضده بسهولة متناهية أي

[1] د/عبد الفتاح بيومي الحجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، مرجع سابق، ص 36

[2] غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص 539.

تدميرها في زمن قصير جدا ،فضلا عن سهولة تنصله من هذا العمل بإرجاعه حسبما تشهد على ذلك وقائع عديدة، على خطأ في نظام الحاسوب أو الشبكة أو في الأجهزة كما أن هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الانترنت و يكون أمرها حكرا عليهم كالتجسس عل الملفات المختزنة و الوقوف على ما بها من أسرار، و قد يخربون الأنظمة تخريبا منطقيا بحيث يمكن تمويهه بأنه خطأ في البرامج أو الأجهزة أو نظام التشغيل...الخ.

مما يزيد من خطورة إمكانية و سهولة إخفاء الأدلة المتحصل من الوسائل الالكترونية، أنه يمكن محو الدليل في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، و في الحالة التي قد تعلم بها فأنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده[1].

ضخامة حجم المعلومات و البيانات المتعين فحصها: تعرف قواعد البيانات بأنها عبارة عن مجموع بطاقات تشمل بيانات معدلة و منظمة تسمح باقتطاع البيانات حسب مشيئة المستعمل، تعتبر قاعدة البيانات بأنها نظام فعال يستعمل لترتيب الملفات التي تحتوي على معلومات معينة، وتعتبر قواعد البيانات كوسيط لتخزين المعلومات و معالجتها أي تنظيمها و ترتيبها.

و يشكل الكم الهائل من البيانات التي يجري تداولها عبر الانترنت أحد مظاهر الصعوبات التقنية التي تعيق التحقيق في الجرائم التي تقع عليها أو بواسطتها، وكمثال علي ذلك فإن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التي قد لا تثبت كلها تقريبا شيئا على الإطلاق[2] ، قد تكون النتيجة سلبية بحيث لا يمكنها كشف الدليل المراد ضبطه أو تحصيله، و هذا مراده في المقام الأول عدم وجود آلية للفرز الذاتي للملفات المخزنة، حتى يمكن الوقوف على الملفات غير مشروعة و ضبطها، ما يجعل القضاء لا يكترث بالدليل الرقمي، ولا يعول عليه كثيرا لافتقاره الى المصداقية التي تجعله جديرا بالثقة. لذلك وفي ظل تواضع المستوى الفني لرجال الضبط القضائي و التحقيق الجنائي فيما يتعلق بتقنيات الحاسوب و استخداماته، و إمكانية خروجها عن نطاق إقليم الدولة و البعد الجغرافي بين مرتكب الجريمة و الضحية .[3] بالإضافة إلى عدم المعرفة بمكونات الجريمة المتعلقة بالأنترنيت من قبل بعض الأطراف المعنية .

[1] د/ حسين بن سعيد بن سيف الغفاري، مرجع سابق، ص 19.

[2] هشام محمد فريد رستم، المرجع السابق، ص 430.

[3] سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض2003، ص98.

ثالثا: مظاهر تعود عراقيل بشرية.

من بين تلك المعوقات نجد:

تكتم المجني عليهم واحجامهم عن الابلاغ عن الجرائم المعلوماتية: إن تكتم المجني عليهم وإحجامهم في الابلاغ عن الجرائم المعلوماتية يؤدي الي صعوبة اكتشاف الجريمة واثباتها، ذلك لأن المجني عليه غالبا ما يكون مصرفا أو مؤسسة مالية، شركة أو مشروعا صناعيا ضخما، يلجا إلى التكتم على مثل هذه الجرائم إن تعرض لها[1]، و لا يبلغ السلطات المختصة في مكافحة هذه الجريمة لعدة أسباب. منها الحيلولة دون اكتشاف أساليب ارتكاب الجريمة لتفادي تقليد الأخرين للمجرمين، و تفادي اطلاع الأجهزة الأمنية على المعلومات ذات الطابع السري أو التي لم يتم الإبلاغ عنها، وربما يتجلى ذلك بصورة أكبر في نطاق جرائم الانترنت التي تقع على شركات التأمين أو البنوك رغبة في تجنب الخسائر التي يتوقع تحققها نتيجة هذا الإبلاغ بسبب نقص ثقة العملاء في هذه المؤسسات.

وتبقي الجريمة المعلوماتية في الخفاء ما لم يتم التبليغ عنها، وتفلت بذلك من العقاب، ففي دراسة للمعهد الوطني للعدالة التابع لوزارة العدل الأمريكية شملت 164 حالة، في مجال التحقيق في جرائم الحاسوب و الانترنيت يمثلون 114 وكالة رسمية ، كان غالبية المشاركين في الدراسة يعتقدون أن معظم جرائم الحاسوب و الانترنيت التي يتم اكتشافها لا يبلغ عنها للشرطة. كما توصلت دراسة أخرى أجراها معهد أمن الحاسوب CSI بالاشتراك مع مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية إلى أن حوالي 80% من الجرائم التي يتم اكتشافها لا يتم البلاغ عنها للسلطات المختصة.

إن أسباب الاحجام عن الابلاغ عن الجرائم المعلوماتية متعددة، منها:

- جهل الأفراد العاديين أو المسؤولين أن مثل هذه الأفعال و الهجمات تعتبر جرائم تقع تحت طائلة العقاب.

- خوف المجني عليهم، خاصة المؤسسات و الشركات المالية أو الامنية من أن يؤدي انتشار خبر الحادث على سمعتها و مصداقيتها و ظهورها بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعا بإهمالها أو قلة خبرتها أو عدم وعيها الأمني، و لم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها ، الأمر الذي ينعكس سلبا على أرباحها و قيمة أسهمها.

[1] د/ محمد حماد مرهج الهيتي، مرجع سابق ، ص 217.

– رغبة المؤسسات و الشركات التجارية في تفادي أعمال التحقيق التي قد تؤدي إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق، اضافة الي الاضرار التي طالتها من جراء الجريمة في حد ذاتها.

– انعدام ثقة المجني عليهم في قدرة الجهات المكلفة بالبحث والتقصي عن الجرائم المعلوماتية والتحقيق الجنائي عن توقيف المجرمين وتقديمهم للمحاكمة.

المطلب الثاني: عراقيل قضائية

أولا: قصور التعاون الدولي في مكافحة الجرائم المعلوماتية.

باعتبار أن الجرائم المعلوماتية، جرائم لا تعترف بالحدود الاقليمية لكل دولة، يمكن ارتكابها عن بعد، ويمكن بذلك أن تقع تحت طائلة عدة انظمة قانونية، فإن مسالة التعاون الدولي في مكافحة هذا النوع من الجرائم واثباتها، تعد مسالة هامة وحاسمة. ولكنها في نفس الوقت مسالة معقدة، لأسباب عدة منها:

1) صعوبة توحيد المفاهيم:

لا شك أن أي اتفاق دولي في أي مسالة من مسائل التعاون لا بد أن يؤسس علي مفاهيم موحدة غير مختلف عليها. في المقابل نجد ان مفهوم الجريمة المعلوماتية في حد ذاته محل اختلاف بين مختلف الانظمة القانونية، كما أن عالم الاجرام المعلوماتي ينطوي علي الكثير من المصطلحات التقنية غير المستقرة بسبب تغير مفاهيمها وتجددها مع التطور التكنولوجي، وبذلك فانه من الصعوبة علي تلك الانظمة القانونية أن تستوعب معا تلك التغيرات وتضع مفاهيم موحدة لتلك المصطلحات خاصة مع التباين الكبير الموجود بين الدول التي تنتمي اليها تلك الأنظمة القانونية فيما يخص مدي تقدمها العلمي و استيعابها للتكنلوجيا.

إن اختلاف المفاهيم المرتبطة بالجرائم المعلوماتية بين نظام قانوني واخر يضعف من منظومة القانون الدولي في ضبط تلك الجرائم، وبالتالي يسهل علي الجناة الافلات من المسائلة الجنائية[1]. لأن عدم الاتفاق علي ماهية النمط او السلوك الاجرامي المحدد للجرائم المعلوماتية من شانه أن يؤدي الي افلات الكثير من الانشطة الاجرامية من مسالة التعاون الدولي، فالتباين والاختلاف الموجود بين مفهوم الجريمة المعلوماتية بين الدول يؤدي ببعضها الي تجريم افعال وسلوكات لا تعبرها دول اخري جرائم وبالتالي فإنها لا تعتبرها من مسائل التعاون الدولي[2].

[1] ايهاب ماهر السنباطي، «الجرائم الالكترونية (الجرائم السيبرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد»، االندوة الاقليمية حول الجرائم المتصلة بالكومبيوتر، المملكة المغربية، جويلية 2007، ص15- 36.

[2] فريد منعم جبور، مرجع سابق، ص 215.

وتعتبر قضية الدودة الحاسوبية: "لوف باغ LOVE BUG " التي أدت في الفلبين سنة 2000، وتسببت في تعطيل ملايين الحواسيب في انحاء العالم، احسن مثال علي اختلاف الانظمة القانونية، بين الدول، حيث وجدت أعمال التحقيق المتخذة للكشف عن القضية صعوبات كثيرة، بسبب أن الفلبين لم تكن تجرم ذلك العمل الضار والمؤذي بشكل كاف.

2) تنوع واختلاف الانظمة الاجرائية.

لا يقتصر التعاون الدولي علي المسائل الموضوعية فقط، لا سيما في المجال الجنائي، بل إن التعاون في المسائل الاجرائية لا يقل عنه أهمية عنه في المسائل الموضوعية. ذلك أن التعاون في حد ذاته يتطلب ايجاد وسائل اجرائية واليات يتم من خلالها، وأنه من شأن الاختلاف الموجود بين الانظمة الاجرائية للدول أن تصعب من مسالة التعاون.

إن التعاون في المسائل الاجرائية من المسائل الهامة في مكافحة الجرائم المعلوماتية خاصة وأن هذه الجرائم وبسبب طبيعتها وسرعة ارتكابها أو سهولة اخفاء الادلة الناتجة عنها، تتطلب من مختلف الانظمة القانونية الاجرائية أن تكييف الاجراءات التقليدية المتبعة من طرفها في التحقيق والمحاكمة بما يتوافق مع تلك الطبيعة والسرعة. كما أن مسالة التعاون الاجرائي، تتطلب ازاحة الكثير من العراقيل المتعلقة بتحديد طرق واليات التفتيش والضبط والحفظ والمصادرة وكيفياتها، خاصة مع امكانية اجراء التفتيش لأي منظومة معلوماتية عن بعد.

فعادة ما تختلف طرق واجراءات التحري والتحقيق في دولة ما عنها في دولة اخري وهي إجراءات وإن كانت تثبت فاعليتها في دولة ما، قد لا تكون كذلك في دولة أخري، وهي إن كانت مشروعة في دولة ما، قد لا تكون كذلك في دولة اخري، وقد لا تكون مرخص بها أصلا، كما هو الحال بالنسبة للمراقبة الالكترونية، والتسليم المراقب، والعمليات المستترة، وبالتالي فان التعاون في هذه المسائل لديه اهمية كبيرة خاصة في تقدير مشروعية وحجية الأدلة التي تستنبط في ظلها[1].

كما تتعلق مسائل التعاون الاجرائي بالقانون الواجب التطبيق و امتداد الاختصاص القضائي، وتسليم المجرمين، وهي عادة مسائل مستعصية، غالبا ما تصطدم بمسائل اخري تحول دون الاتفاق عليها، علي غرار مسالة السيادة، ومسالة المعاملة بالمثل.

[1] براء منذر كمال عبد اللطيف، ناظر احمد منديل، « القانون القضائي الدولي في مواجهة جرائم الانترنيت » المؤتمر العلمي لتحولات القانون العام في مطلع الالفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009، ص11.

ثانيا: اشكالية الاختصاص القضائي و القانون الواجب التطبيق.

قد يكون الأثار المترتبة عن بعض الجرائم المعلوماتية ذو طابع عالمي، أي أن تلك الاثار قد تمتد الي أكثر من دولتين، وهي بذلك تشمل أكثر من نظامين قانونيين. وهذا يطرح مسالة هامة في مكافحة الجرائم المعلوماتية تتعلق بإشكالية الاختصاص القضائي والقانون الواجب التطبيق، ومدي فاعلية المبادئ القانونية المعتمدة في هذا المجال، كمبدأ الإقليمية ومبدأ الشخصية ومبدأ العينية، وكذا المعايير والضوابط المحددة للاختصاص، كمعيار الاختصاص المكاني، معيار القانون الاكثر ملائمة، ومعيار الضرر المرتقب، في حل مشكلة القانون الواجب التطبيق و مشكلة تنازع الاختصاص بنوعيه الايجابي والسلبي.

1) اشكالية القانون الواجب التطبيق.

إن المبادئ التقليدية السالفة الذكر وإن كانت تتفق مع طبيعة الجرائم التقليدية، غير أنها لا قد لا تجد مكان لتطبيقها في الجرائم المعلوماتية، التي تتسم بكونها جرائم لا موطن لها فغالبية تلك الجرائم ترتكب عبر شبكة الانترنيت التي تتميز بانها شبكة عالمية لا مقر لها في دولة معينة، تخضع لرقابتها او سيطرتها، ونظرا لعدم وجود قانون جنائي موحد يحكم هذه الشبكة، فان القوانين الجنائية التي تطبق عليها تتعدد بتعدد الدول المرتبطة بها باعتبار أن القانون الجنائي يتعلق بسيادة الدولة. فالأصل في القوانين هو اقليمية القانون الجنائي، وبذلك فان الدول عادة لا تهتم الا بالجرائم المعلوماتية التي ارتكبت في اراضيها أو تحققت النتائج الاجرامية بها. غير أن ذلك قد لا يتفق مع حماية مصالح الدولة، بالنظر الي البعد الدولي للجرائم المعلوماتية المرتكبة بواسطة شبكة الانترنيت، حيث تضع هذه الشبكة دول مختلفة في حالة اتصال دائم، كما أن المعلومات والبيانات التي يتم ادخالها وتحميلها علي الشبكة تنتشر في ثوان معدودة في كل الدول المرتبطة بها، بحيث تكون متاحة لأي مستخدم بها [1].

إن الاخذ بمبدأ الشخصية أو مبدأ العينية كمبدأين مكملين لمبدأ اقليمة النص الجنائي، في تحديد القانون الواجب التطبيق علي الجرائم المعلوماتية لا سيما تلك المرتكبة عبر الانترنيت، محل انتقاد باعتبار أن تحديد جنسية المجرم في الجرائم المعلوماتية، عادة ما لا يتأتى الا بعد القيام بالتحقيقات اللازمة. وأن هذه التحقيقات لا بد أن تقع في ظل نظام قانوني اجرائي معين، أي أن مسالة تحديد القانون الاجرائي الواجب التطبيق تكون سابقة لمعرفة جنسية المجرم وليست لاحقة. مما يتعذر معه الأخذ بمبد الشخصية.

[1] محمد عبد الكريم سلامة، جرائم غسيل الأموال الكترونيا في ظل النظام العالمي الجديد، مؤتمر الاعمال المصرفية الالكترونية بين الشريعة والقانون، المنعقد بجامعة الامارات العربية المتحدة، كلية الشريعة والقانون، 10 الي 12 ماي 2003، المجلد الرابع، ص28.

شأنه في ذلك شان مبدأ العينية الذي يصطدم بمبدأ السيادة خاصة إذا وقعت الجريمة في دولة غير دولة المجني عليه.

2) اشكالية الاختصاص القضائي.

تثور اشكالية الاختصاص القضائي، لأن الاثار المترتبة عن الجرائم المعلوماتية المرتكبة عبر شبكة الأنترنيت لها امتداد واسع النطاق تشمل أكثر من نظام قانوني واحد وبذلك يحتمل أن تتنازع تلك الانظمة إيجابيا وسليبا في بسط اختصاصها القضائي للتحقيق في تلك الجرائم ومحاكمة مرتكبيها.

وإن كانت هناك معايير أو ضوابط علي الصعيد الوطني لكل دولة تحكم مسألة تنازع الاختصاص هذه، غير أن الامر يختلف علي المستوي الدولي لعدم وجود نظرة موحدة أو اتفاقية دولية تحكم تنازع الاختصاص أو تنظمه. فقد تثور مسائل التنازع الايجابي للاختصاص القضائي في حالة ما اذا تمسكت كل دولة تضررت من الجريمة المعلوماتية المرتكبة عبر الانترنيت. كما قد تثور مسألة تنازع الاختصاص السلبي في حالة ما اذا كانت الانظمة القانونية التي

تم ارتكاب السلوك الإجرامي أو تحققت النتيجة الإجرامية في ظلها غير مختصة بالتحقيق في الجريمة أو محاكمة مرتكبها، بسبب عدم اعترافها بأن ذلك السلوك يشكل جريمة. وبذلك يفلت المجرم من العقاب رغم أن نفس السلوك الضار الذي أتي به قد يشكل جريمة في ظل انظمة قانونية اخري، وهو الأمر الذي دفع ببعض مجرمي الانترنيت علي غرار من يقومون بأنشاء مواقع خلاعية وإباحية عبر شبكات الانترنيت الي انشاء تلك المواقع وادراتها في دول لا تجرم او تعاقب علي مثل تلك الافعال.

إن الاختصاص القضائي أو المحكمة المختصة بالبث في الجرائم المعلوماتية ، تحكمه ثلاث معايير تتمثل في معيار الاختصاص المكاني، معيار القانون الاكثر ملائمة، ومعيار الضرر المرتقب.

فمعيار الاختصاص المكاني يقوم علي ثلاث ضوابط تتمثل في:

مكان ووقوع الجريمة محل إقامة المتهم أو مكان القاء القبض عليه، وفي حالة اجتماع اكثر من ضابط، تكون المحكمة المختصة هي المحكمة التي ترفع اليها الدعوي اولا[1]. غير ان ذلك قد لا يتفق مع حسن سير اعمال الاستدلال و التحقيقات القضائية اذا ما تم استناد الاختصاص علي اساس محكمة مكان القاء القبض علي المتهم أو مكان اقامته. فالضابط الأصلح لحسن سير التحقيقات واتخاذ الاجراءات لا سيما اعمال المعاينة و التفتيش والضبط هو ضابط مكان ارتكاب الوقائع ومكان وجود مسرح الجريمة.

[1] غازي عبد الرحمان هينان الرشيد، مرجع سابق، ص 518.

ويري أصحاب معيار القانون الاكثر ملائمة أن الاستناد الي المعيار المكاني في اسناد الاختصاص القضائي فيه اجحاف في حق الدول التي تضررت من الجريمة، ذلك ان نسبة الضرر الناتج عن الجرائم المعلوماتية المرتكبة عبر الانترنيت قد تتفاوت بين دولة واخري، ومن العدل والانصاف أن ينعقد الاختصاص القضائي للدولة التي تضررت اكثر من الجريمة[1].

أما معيار الضرر المرتقب فهو يقوم علي أساس أن الضرر الذي قد تسببه الجرائم المعلوماتية المرتكبة عبر شبكة الانترنيت، يمكن أن يحدث في أي دولة متصلة بهذه الشبكة. وقد قدم المجلس الاوروبي العدلي تفسيرا بشان مفهوم قاعدة اختصاص محل وقوع أو حدوث الفعل الضار، وذلك بالتأكيد علي حق المتضرر، باللجوء حسب خياره الي محكمة محل ارتكاب الفعل، أو الي محل وقوع الضرر، ولكن مع إضافة قيد هام في حالة لجوء المتضرر الي محكمة وقوع الضرر، يقضي بحجب اختصاص هذه المحكمة إذا اثبت المدعي عليه، أنه لم يكن قادرا علي ارتقاب بصورة معقولة، أن الفعل أو الامتناع كان من شأنه احداث أو انتاج ضرر مماثل في دولته [2].

وقد ورد في حيثيات هذا القرار أن المعلومات المنشورة عبر شبكة الانترنيت يمكن معاينتها من قبل جميع الدول الموصولة بها، ومن دون أن تكون موجهة بالضرورة ، لكن طبيعة هذه الوسيلة الاعلامية الجديدة لا يجب أن ينتج عنها تطبيق لجميع القوانين الموجودة بل يجب أن نطبق معيار(الارتقاب)، علي المسؤول عن المعلومات الضارة فيها وهذا المعيار لا يمكن إيجاده إلا من خلال إيجاد صلة أو علاقة للقانون المختص مع مبدأ موضوعي، وذلك بمعزل عن تذرع كل دولة باختصاصها المحتمل.

وأن المعالم الموضوعية في الاختصاص هي محل تمركز الموقع الذي نشر الأقوال أو المعلومات، وهو أكيد وثابت، ويمكن التحكم فيه، بخلاف مكان تلقي تلك المعلومات الذي يبقي احتماليا.

وقد وجد هذا المعيار طريقه الي التطبيق في بعض الدول، ومنها فرنسا حيث اصدرت محكمة استئناف باريس في عام 1999، قرارا اعتبر صراحة أن الطبيعة الكونية الخاصة لشبكة الانترنيت، لا يجب أن تؤدي الي تطبيق محتمل لجميع القوانين الموجودة، بل الي تطبيق القانون ذي الصلة مع مبدا موضوعي. هو ارتقاب المسؤول للمحتوي الضار الذي ينشره [3].

---

[1] فريد منعم جبور، مرجع سابق، ص 207.

[2] غازي عبد الرحمان هينان الرشيد، المرجع السابق، ص 254.

[3] د/ عبد الفتاح بيومي حجازي، مبادي الإجراءات الجنائية في جرائم الكومبيوتر والانترنيت، مرجع سابق، ص 52.

فقد يقوم المجرم بارتكاب الأفعال المكونة للجريمة المعلوماتية في دولة ما، غير أنه يستهدف ضحاياه في دول اخري، كان يقوم المجرم ببث صور أو افلام ذات طابع اباحي في اقليم دولة ما ويتم الاطلاع عليها في دول اخري، فهما نكون أمام اختصاص قضائي ايجابي متعدد لكل الدول التي تضررت من الجريمة[1] .

ثالثا: اهم العقبات التي واجهت ظبطية القضائية في اثبات جريمة معلوماتية:

- عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي ذلك أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب اتباعها وربما يتجلى سبب غياب هذا النموذج في كثرة التعاريف والمفاهيم القانونية التي تؤطر هذا الجانب فكل دولة تضع تعريفات ومصطلحات حسب أنظمتها القانونية الجنائية بالخصوص هذه الكثرة الناتجة أساسا عن التطور الذي يعرفه المجال المعلوماتي وبالتالي تطور تقنيات وسائل ارتكاب الجرائم المعلوماتية او جرائم الانترنيت.

- مسألة الطبيعة القانونية للمال المعلوماتي ومدى اعتباره مالا ماديا او معنويا ومنقولا باعتبارها هذا الأخير محلا لمعظم جرائم الأموال

- عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة بخصوص الجريمة المعلوماتية بين الدول المختلفة خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق.

- فجرائم الحاسب الآلي آثار خارجية ظاهرة ، وإنما تنصب على البيانات والمعلومات والمستندات المخزنة في نظم المعلومات والبرامج وبالتالي عدم الحصول على آثار مادية تشكل دليلا لإثبات الجريمة المعلوماتية الواقعة وفي غياب أعمال العنف والاقتحام والتكسير على خلاف الجرائم العادية يصعب إثبات الجريمة .

- بالإضافة إلى ارتكاب الجريمة المعلوماتية في الخفاء وتعمد الجاني عدم ترك أي دليل إدانة بعد ارتكابه للجريمة .

- عدم وجود معاهدات ثنائية أو جماعية بين الدول نحو يسمح بالتعاون المثمر في هذا المجال وحتى في حال وجودها فإنها لا تستطيع مواكبة التطور السريع لنظم وبرامج الحاسب وشبكة الانترنت.

- وتبرز أهمية وضرورة وجود مثل هذه المعاهدات عندما نستحضر الطابع العابر للحدود والقارات الذي تتميز به الجريمة المعلوماتية بحيث تتباعد المسافة بين الجاني ونتيجة فعله مما يؤثر سلبيا على أعمال البحث والتحري والتحقيق

[1] عبد الله عبد الكريم عبد الله، كتاب عن جرائم المعلوماتية والانترنيت (الجرائم الالكترونية)، ط الاولي، منشورات الحلبي الحقوقية، بيروت، 2007،

– ونتيجة الطابع العابر للحدود لهذه الجريمة تظهر مشكلة الاختصاص على المستوى الوطني والدولي والقانون الواجب تطبيقه.

– ضخامة كم البيانات المعلوماتية التي تقف عائقا أمام إجراءات التحقيق الجنائي والبحث عن دليل الإدانة والأكثر من ذلك تتجلى الصعوبة عندما يقوم الجاني بتشتيت المعلومات والمستندات رغبة منه في عدم الابقاء على أي دليل إثبات إضافة إلى أن طباعة كل ما هو موجود على الدعامة الممغنطة لحاسب متوسط العمر، يتطلب مئات ألاف الصفحات في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئا مفيدا للتحقيق.

المطلب الثالث: الحلول القانونية قصيرة المدى

تمثل هذه الحلول التشريعية في تدابير وقائية تخذها الدولة وقوانين نصتها من أجل مكافحة هذه الجريمة وحماية المجتمع ولكن لصعوبة التعامل مع هذه الجرائم الجديدة في الوقت الراهن يتطلب الأمر بداية اللجوء إلى حلول قصيرة المدى ثم حلول طويلة المدى وهو إعادة النظر في معظم التشريعات لأن معظم جرائم الانترنت أصبحت ظاهرة تمس جميع مجالات الحياة.

أولا: الحلول التشريعية قصيرة المدى

إن هذه الحلول تتمثل في إصدار السلطة المختصة بعض المراسيم التنظيمية لمقاهي الأنترنت دون إحتكار المعلومة فيمكن في إجراءات إستعجالية فرض بعض الأمور على أصحاب مقاهي الأنترنت: وضع البرامج اللازمة لمنع الدخول إلى المواقع المخلة بالحياء، وهذا من أهم الظواهر التي برزت في مجتمعنا في ظل غياب التربية السليمة مما يؤدي للإنحلال الخلقي لشبابنا وحتى المراهقين الذي أصبح من السهل عليهم دخول أي موقع يشاءون بالإضافة إلى المواقع الإباحية هناك المواقع الإرهابية ومواقع العنف كتعليم القتل فلا بد من تدبير عاجل لإن الحرية في المعلومة لا تكمن في دخول هذه المواقع[1].

– وضع برامج للحماية من الفيروسات . وهذا كله بمراسيم تنظيمية ويمكن للدولة أن تدعم هذه العملية بتخفيض أسعار هذه البرامج

– القانونية والتعريف بمدى خطورة الجرائم الإلكترونية

– إصدار مراسيم من أجل تنظيم تكوين محققين ورجال شرطة وقضاة على التقنية | المعلوماتية والمعرفة الكافية لجرائم الانترنت

[1] – سامر محمد سعيد، المر ل السابق، ص .199

- تعريض أصحاب مفاهي الأنترنت لغرامة مالية أو حتى إغلاق المقهى إذ ثبت بأنه سمح للمراهقين أو حتى الشباب بالدخول للمواقع السابقة، ففي المواد الجنائية لا يمكننا ذكر أكثر من هذا إحتراما لمبدأ لا عقوبة إلا بنص قانوني .

ثانيا: أما من ناحية المواد المدنية والتجارية فإنه :

- يمكن للمحاماة لعب دور مهم لتكييف بعض السلوكيات والمعلومات، مع محاولة الفضاء تكييف بعض المنازعات التجارية الإلكترونية قياسا على التجارة العادية لحين صدور التشريع المنظم للتجارة الإلكترونية،
- إعتماد حرية الإثبات في المجال التجاري.
- يجب على المشرع أن يوقع بعض المعاهدات لمكافحة الجريمة الإلكترونية
- يجب على المشرع أن يوقع بعض الإتفاقيات التي تتبنى تعريف التوقيع الإلكتروني والعقد الإلكتروني ومسايرتها بسن قوانينها التنظيمية.[1]

المطلب الرابع: الحلول القانونية طويلة المدى

إن الطابع اللامادي والإفتراضي لشبكة الأنترنت يستلزم تعديل العديد من التشريعات الحالية بالإضافة إلى استحداث أخرى، وهذا لا يضطرنا بالضرورة إلى خلق شيء جديد بل يمكننا الإستفادة من الدول الأخرى التي سبقتنا في مجال التشريع لتجريم هذه السلوكيات ما دامت هذه التشريعات لا تخالف النظام العام والآداب العام وبما أنه لا يمكن معافية شخص من دون نص قانوني – الركن الشرعي – إذن لابد من سن نصوص قانونية تتناسب والتطور الحالي.

ولكن الملاحظ أنه رغم زيادة إنتشار الجرائم الإلكترونية وفعاليتها إلا أن المشرع لم يضع الحد الآن الإطار القانوني لأي من هذه الظواهر. لذا على المشرع أن يعدل أو بصدر قوانين جديدة، ففي نطاق الحماية الجنائية يتعين الإقرار بصلا حية المعلومات كمحل للحماية من أنشطة الإعتداء كافة فبدا بالتشريعة العامة وهي القانون المدني، فعلى المشرع أن يعدل فيه بسن تشريع جديد يتضمن المحررات الإلكترونية ومن بينها العقد الإلكتروني والتوقيع الإلكتروني، وغيرها من المفاهيم في العالم الإفتراضي الجديد

1) **القانون التجاري** : لقد ظهر في عالمنا اليوم مفهوم جديد هو التجارة الإلكترونية والتسويق الإلكتروني، والدفع فيه يكون عن طريق بطاقة الإئتمان وهي مجالات خصبة للإحتيال فلا بد على

[1] –محمد عادت ريان، المر ل السابق، ص .124

المشرع أن ينظمهاء – الإثبات : وهذا في إعتقادنا من أهم الخطوات التي يجب أن يقوم بها المشرع وهذا بتبني الخبرة والمعاينة كأساليب للتحقيق واثبات الجريمة الإلكترونية. – تعديل قانون الإجراءات الجزائية وتعديل قانون حقوق المؤلف والحقوق المجاورة [1].

– تعديل قانون الإجراءات المدنية وتحديد الاختصاص النوعي والمحلي لهذه الجرائم والمعاملات.

– تحديد مسؤولية مزودي الأنترنت.

– تكليف النظام القضائي لمعالجة هذه الجرائم وتأهيل القضاة وأهم قانون يجب تعديله هو قانون العقوبات الجزائري الذي يعتبر أهم حل في الحلول التشريعية طويلة المدى.

[1] – محمد أمين الرومي المر ل السابق ص .122


الخاتمة

بعد ان اصبح المجتمع المعلوماتي ومنذ اواخر القرن الماضي ومطلع هذا القرن حقيقة واقعة لا تجريد، وبعد ان تم استعراض موقف التشريعات المقارنة في معظم الانظمة القانونية لمواجهة او التصدي لهذه الظاهرة الاجرامية الخطيرة المتمثلة بالجرائم المعلوماتية بات واضحاً لنا مدى قصور التشريعات الجزائية العربية ومنها قانون العقوبات العراقي في التصدي لهذا النمط من الجرائم .

واذا سلمنا بأن قانون العقوبات بوضعه الحالي لا يكفي لمواجهة هذا النوع الجديد والخطير من الجرائم فهل يعني ذلك ان نقف مكتوفي الايدي ازاء هذا الفراغ او النقص التشريعي ونترك بدون عقاب افعال اجرامية رغم خطورتها ام نخالف مبدأ الشرعية الجزائية والذي يقضي بأن (لا جريمة ولا عقوبة الا بنص (ومن ثم نسمح للقضاء ان يتدخل لملئ هذا الفراغ التشريعي او سد ذلك النقص القائم ، ام يسارع المشرع لسن تشريعات جديدة او تعديل التشريعات القائمة حتى تلائم في تطبيقها ثورة الاتصالات المعلوماتية التي تحياها البشرية بالشكل الذي يجعلها كفيلة بحماية النظام المعلوماتي ومكافحة الاجرام الناشئ عن استخدامه او الواقع عليه ولتحقيق هذه الاهداف نقترح ما يلي :

– اصدار تشريعات جديدة او تعديل التشريعات الجزائية القائمة لمواجهة الجرائم المعلوماتية وذلك بتقرير الجرائم وتحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي .

– ايجاد ادلة اثبات جديدة تتلائم مع طبيعة هذه الجرائم وذلك لعدم ملائمة ادلة الاثبات التقليدية في القانون الجنائي لاثباتها .

– اعتماد الدقة والوضوح والحبكة القانونية عند تحديد انماط السلوك الاجرامي والابتعاد عن التعبيرات الغامضة او المطاطية التي تحمل اكثر من معنى او دلالة .

– عدم الاقتصار عند التجريم والعقاب على انماط السلوك المحظور المرتكبة حالياً بل يجب مراعاة الابعاد المستقبلية لان تكنولوجيا المعلومات والحواسيب في تطور سريع بل يكاد يكون مذهل .

ويمكن تقديم نتائج دراستنا في ما يلي:

– أن الترسانة القانونية المحمية التي استحدثها الشرع الجزائري، وبالرغم من تأخرها، فإنها تعني تدعيما نوعها للمنظومة التشريعية في الجزائر، ساهمت بالقدر الكبير في توفير الإطار الإجرائي لمكافحة الجريمة المعلوماتية من طريق استخلاصي الدليل باعتباره حالة قانونية بواسع لها يتم إستاد المسؤولية الجزائية للحان، وتأتي قبل العملية القضائية بما أنها تتمتع بإتسام نوعي عام، تحيز لها اتخاذ أي إجراء ضمن حدود اجتماعها الإقليمي الذي يتحدد بالدائرة الإقليمية التي تمارس فيها وطالعها العادية أو كامل التراب الوطني إذا تعلق الأمر بالجرائم المنصوص عليها في المادة 16 من قانون الإجراءات الجزائية

– من خلال تحليلنا للنصوص القانونية فإن تنمية الإجراءات البحث والتحري المستحدثة يعد بأن المشرع الجزائري وبالرغم من خطورة هذه الإجراءات وسياستها بالحياة الشخصية للمشتبه فيهم، فإنه كرس كافة الضمانات الكفيلة بتحقيق التوازن بين حماية المجتمع من جهة والخافقة على حقوق وحريات الأشخاص من جهة أخرى، من خلال الإشراف القضائي، لاسيما إلزامية الحصول على الإذن المسبق من السلطة القضائية المحتملة قبل أي إحراء.

– الطبيعة الخاصة للجريمة المعلوماتية فرضت على المشرع الجزائري مطا جديدا من الأدلة وهو الأدلة الرقمية، ويبقى استحداث المشرع الجزائري لقواعد إجرائية جديدة في البحث والتحري في هذا النوع من الجرائم اعترافا صريحا منه بأن الدليل الرقمي هو الأنسب في إثباتها.

قائمة المصادر والمراجع

أولا: الكتب

1. أبو العلاء علي النمر، دراسة تحليلية، الاثبات الجنائي، دار النهضة العربية، ط الثانية.
2. احمد خليفة الملط ـ الجرائم المعلوماتية ـ دار الفكر العربي ـ الاسكندرية.
3. أمال عبد الرحيم عثمان ، شرح قانون الإجراءات الجنائية ، سنة 1989.
4. أميل أنطوان ديراني، الخبرة القضائية، المنشورات الحقوقية الصادرة سنة 1977، ط1، بيروت.
5. ايهاب ماهر السنباطي، «الجرائم الالكترونية (الجرائم السيبرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد»، الندوة الاقليمية حول الجرائم المتصلة بالكومبيوتر، المملكة المغربية، جويلية 2007.
6. براء منذر كمال عبد اللطيف، ناظر احمد منديل، « القانون القضائي الدولي في مواجهة جرائم الانترنيت » المؤتمر العلمي لتحولات القانون العام في مطلع الالفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009.
7. حاتم عبد الرحمن منصور الشحات ـ الاجرام المعلوماتي ـ دار النهضة العربية ـ القاهرة ط ١ـ 2003.
8. حسين محمود ابراهيم، الوسائل العلمية الحديثة في الإثبات، دار النهضة العربية، سنة 1981.
9. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجبل للطباعة، الطبعة السادسة عشر، 1985.
10. سامر محمد سعيد – الانترنات و المخاير دار سعاد الصاح المطابع التعاورية الصحافية بيرو لبنان . 1992
11. عبد الحميد الشواربي، التزوير والتزييف مدنيا وجزائيا في ضوء الفقه والقضاء ، منشأة ، مصر 1996.
12. عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دراسة متعمقة في جرائم الحاسوب الالي و الأنترنت، بهجات للطباعة و التجليد، مصر، 2009.
13. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.
14. عبد الله عبد الكريم عبد الله، كتاب عن جرائم المعلوماتية والانترنيت (الجرائم الالكترونية)، ط الاولي، منشورات الحلبي الحقوقية، بيروت، 2007،
15. علي عبد القادر القهوجي ـ الحماية الجنائية لبرامج الحاسب ـ دار الجامعة الجديدة ـ 1998.
16. علي عبد القادر القهوجي ـ قانون العقوبات ـ القسم العام ـ الدار الجامعية .

17. عمر بن محمد يونس، الجرائم الناشئة عن استخدام الانترنت، ط الاولى، دار النهضة العربية القاهرة، سنة 2004. .

18. فرعون محمد الصديق، بوعلي العربي، إثبات الجريمة المعلوماتية، ملازمي الأوائل للشرطة، الدفعة 2018 – 2020.

19. فريد منعم جبور، حماية المستهلك عبر الإنترنت و مكافحة الجرائم الالكترونية (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010،

20. كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية، دار ريم للنشر والتوزيع، سنة 2011.

21. مأمون سلامة، قانون الاجراءات الجنائية، ط الاولي، دار الفكر، سنة: 1980.

22. محمد حماد مرهج الهيتي، جرائم الحاسوب– ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، الطبعة الاولى، دار المناهج للنشر و التوزيع، عمان، 2006.

23. محمد عبد الكريم سلامة، جرائم غسيل الأموال الكترونيا في ظل النظام العالمي الجديد، مؤتمر الاعمال المصرفية الالكترونية بين الشريعة والقانون، المنعقد بجامعة الامارات العربية المتحدة، كلية الشريعة والقانون، 10 الي 12 ماي 2003، المجلد الرابع.

24. محمد كمال عواد، الضوابط الشرعية والقانونية للأدلة الجنائية، سنة 2011، دار ريم للنشر والتوزيع.

25. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، ط الثالثة، سنة 1997.

26. هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، ط1، دار النهضة العربية، القاهرة، سنة 1997.

ثانيا: الرسائل والمذكرات:

1. أحمد ضياء الدين محمد خليل، رسالة دكتوراه: مشروعية الدليل في المواد الجنائية، جامعة عين شمس، سنة 1982.

2. حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل اجازة المدرسة العليا للقضاء، 2008.

3. سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض2003.

4. غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.

5. محمد بن عبد الله بن علي المنشاوي، جرائم الانترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية ، الرياض – السعودية، 2003.

ثالثا: المتلقيات والمنشورات:

1. دفاتر البحوث العلمية، المجلد 9، العدد الأول، سنة 2021.

رابعا: الأوامر والقوانين:

1. قانون رقم 04-05 مؤرخ في 14 أغسطس 2004، يعدل و يتمم القانون رقم 90-29 المؤرخ في أول ديسمبر سنة 1990 و المتعلق بالتهيئة و التعمير.

2. الأمر رقم 66-156 المؤرخ في مؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة يونيو سنة 1966 ،الذي يتضمن قانون العقوبات، المعدل والمتمم قانون العقوبات، المعدل والمتمم، طبعة 2012.

3. المادة 09 من القانون 09 – 04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحها المؤرخ في 14 شعبان عام 1430 الموافق ل 05 أوت سنة 2009.

4. الأمر رقم 66 – 155 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 الذي يتضمن ق . ا . ج ، المعدل والمتمم، سنة 2007.

خامسا: المواقع الإلكترونية:

1. خالد ممدوح إبراهيم، الدليل الالكتروني في جرائم المعلوماتية، بحث منشور على الانترنت الرابط: http://www.f-law.net.

2. طارق محمد الجملي، الدليل الرقمي في مجال الاثبات الجنائي، بحث منشور علي الانترنيت.

3. محمد عبد الرحيم سلطان العلماء ـ جرائم الانترنيت والاحتساب عليها ـ بحث مقدم لمؤتمر القانون والكمبيوتر والانترنيت ـ مايو 2005..

4. حسين بن سعيد بن سيف الغفاري، التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، بحث منشور علي الرابط http://www.minshawi.com،

سادسا: المراجع باللغة الفرنسية

1. WASIK (MARTIN) ، Computer Crimes And Other Crimes Against Information Technology In The United Kingdom- Rev، Inter، De، Dr، Panal 1993.

2. KASPERSEN(W.K.HENRIK)،Computer Crime And Other Crime Against Information Technology In Netherland،R.I.D.P.1993.

3. KASPERSEN (W.K.HENRIK0) op-cit.

الملاحق

إستبيان من الضبطية القضائية

على أهم العراقيل التي واجهتهم ميدانيا في الكشف أثناء التحقيق في الجريمة المعلوماتية

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة حمه لخضر بالوادي

كلية الحقوق والعلوم السياسية

قسم: الحقوق

التخصص: جريمة وأمن

إستمارة استبيان

السلام عليكم ورحمة الله تعالى وبركاته

في إطار استكمال مذكرة تخرج لنيل شهادة الماستر تخصص جريمة وأمن تحت عنوان العقبات الإجرائية في إثبات الجريمة المعلوماتية ، يقوم الباحثون بإجراء دراسة ميدانية تهدف الى معرفة العقبات الإجرائية في الجزائر عند إثبات الجريمة المعلوماتية لذا نأمل من سيادتكم التعاون معنا في استفتاء البيانات التي تتضمنها استمارة الاستقصاء (الاستبيان) المرفقة بدقة وبصراحة تامة وبدون أي إحراج، حيث لا توجد إجابات صائبة وأخرى خاطئة، وأن أفضل إجابة هي الرأي الشخصي للمستقصى منه والذي يمثل الواقع الفعلي.

ونود أن نؤكد لكم أن هذه الدراسة تتم لأعراض البحث العلمي فقط، وأن كافة البيانات ستعامل بسرية تامة وحرص شديد. والباحثون يشكرونكم مقدما على تعاونكم معهم.

س1	ماهي أهم العراقيل التي واجهتكم أمام وكالات الاتصال وماهو تأثير شريحة الاتصال؟
ج1	من أهم العقبات هي استخدام الشرائح الهاتفية بهويات مزورة أو بدون ملفات قاعدية لدى مزودي الخدمات لوكالات الاتصال (موبيليس، جيزي، نجمة) في قضايا مثل النصب والاحتيال للتهرب من المسؤولية والمتابعة الجزائية
س2	هل الوقت مهم جدا للكشف عن الحسابات الخاصة في الجرائم الفيسبوكية؟
ج2	بالنسبة للجرائم الفيسبوكية تمتاز بسرعة تنفيذ الجريمة وسرعة إخضاعها وذلك عن طريق حذف الحساب أو التخلي عنه بإستخدام بعض التطبيقات لإخفاء عنوان البروتوكول مثل VPN، TOR، BROKSI
س3	مامدى وعي الشاكي في مساعدة الكشف عن الجريمة؟
ج3	عدم التقدم الشاكي لضبطية القضائية ومصالح الأمن في وقت تعرضه للجريمة المعلوماتية مما يسهل على الجاني إخفاء الجريمة مما يتعذر على رجال الضبطية القضائية لتحديد هوية الجاني
س4	ماهي أهم أدوات الجريمة التي تجدون صعوبات في مواجهتها؟
ج4	من أهم أدوات الجريمة المعلوماتية التي عادت وغالبا ما تواجه صعوبات في التعامل معها هي جهاز الكمبويتر والهاتف النقال .... الخ، والتي عادة ماتكون سهلة الإخفاء والإتلاف
س5	هل عامل الوقت يأدي دورا هاما وله مكانة خاصة في الجريمة المعلوماتية وإثباتها؟ وهل هي غير شرعية؟ وماهي الجهات التي تتأثر في تقديم
ج5	عامل الوقت مهم جدا خاصة في الجرائم السيبيرالية وعادة مانواجه صعوبات في الاخلال بالإلتزامات لمزودي الخدمة وذلك من خلال عدم تقديم المساعدة في الوقت المحدد والمدة الزمنية للإحتفاظ بقاعدة البيانات والمحددة بعامين
س6	هل عدم وجود دليل مادي يعتبر عقبة بالنسبة لرجال الضبط القضائي؟
ج6	ان جرائم الحاسب الآلي لها آثار خارجية لكن تنصب على البيانات والمعلومات وبالتالي صعوبة الحصول على آثار مادية تشكل دليلا لإثبات الجريمة المعلوماتية مثل جرائم العنف، الاقتحام، إلا أنها تقع في الخفاء وتعمد الجاني عدم ترك أي دليل إدانة ضده بعد ارتكابه الجريمة
س7	هل ضخامة البيانات تعتبر عائقا حقيقيا خاصة في إطار التحقيق والكشف على الجريمة؟
ج7	نعم ضخامة البيانات المعلوماتية تقف عائقا أمام إجراءات التحقيق الجنائي والبحث على دليل الإدانة بل الأكثر من ذلك تتجلى الصعوبة عندما يقوم الجاني بتشتيت المعلومات والمستندات رغبة منه في عدم الإبقاء على أي دليل إثبات بالإضافة إلى أن طباعه عموما هو موجود على الدعامة الممغنطة

	الموجودة في الجريمة يتطلب مئات الصفحات في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئا مفيدا للتحقيق

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة حمه لخضر بالوادي

كلية الحقوق و العلوم السياسية

قسم: الحقوق

تقرير تربص ميداني

تخصص سنة ثانية ماستر جريمة وأمن

إعداد الطالبين:

- محمد تومي
- وحيد عبد الليلة

إشراف الدكتور:

- صادق جراية

السنة الجامعية: 2024/2023

تقرير التريص الميداني

في إطار إنجاز مذكرة الماستر المعنونة تحت إسم " العقبات الإجرائية في إثبات الجريمة المعلوماتية"، المؤرخ في 2023/04/25 صادر عن السيد / رئيس قسم الحقوق، بكلية الحقوق والعلوم السياسية بجامعة الوادي، من أجل تدعيم هذه الدراسة بتقرير تطبيقي ، يتم إدراجه كملحق بالمذكرة ، حيث قمنا بتاريخ: 2024/05/27 بزيارة ميدانية لمكتب المحامي " عماد ميده "، للاطلاع على مختلف لها علاقة بموضوع الدراسة محيث صادفتنا عدة صعوبات في الحصول على المعلومات المتعلقة بموضوع الطفولة الجائحة ، و إجراءات متابعتها، نظرا لاعتبارات متعلقة بحساسية الموضوع .

ان مهنة المحاماة مهنة منظمة وفق التشريع الجزائري، بموجب القانون رقم : 07/13 المؤرخ في 2013/10/19، منشور بالجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، بالعدد رقم : 55 المؤرخة في 2013/10/30

وانطلاقا مما سبق اكتفينا في هذا التقرير بزيارة ميدانية لمكت الأستاذ عماد ميده

وتعد مهنة المحاماة ، مهنة مهمة وضرورية، فحق الدفاع، هو أحد المبادئ التي ترتكز عليها النظم القضائية الحديثة، إذ يعتبر المحامي أحد المكونات الأساسية للنظام القضائي بل أحيانا يكون ضروريا لصحة الإجراءات، تحت طائلة البطلان ، و هذا لاحظنا في قضايا الجرائم الإلكترونية مما تكسيه هذا النوع من الجرائم من دقة وحداثة.

وبالرجوع لقضايا الجرائم الإلكترونية، فقد اتضح أن حضور المحامي أمر ضروري لصحة الإجراءات، كي لا تقع تحت طائلة البطلان وهذا وفقا للمادة 11 من قانون الإجراءات الجزائية، لأن معظم الجرائم الإلكترونية لها قانون خاص وهو القانون رقم 04/09 المتعلق بالجرائم الماسة بتكنولوجيا الاعلام والاتصال، من هذا المنطلق يعتبر حضور المحامي ضروري وإلزامي في هذا النوع من الجرائم، سواء على مستوى مرحلتي التحقيق الابتدائي ، وعلى مستوى المحاكم.

بالحديث عن دور المحامي في قضايا الجرائم الإلكترونية ودوره في إثبات العقبات الإجرائية، فإنه يتم الاتصال بالمحامي غالبا من طرف الضحية، أو عن طريق نقيب المحامين وفق إجراءات تنظيمية.

تكتسي قضايا الجرائم الإلكترونية، طابعا خاصا وأهمية كبرى لكل الأطراف بالنسبة للنيابة أو للدفاع، نظراً لتطور مثل هذا النوع من جرائم وما تكتسيه من خطورة وأهمية بالغة، هذه الخصوصية وضحها المشرع الجزائري بالقانون 09-04 المؤرخ في 2009/08/06 وهو القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة لتكنولوجيا الإعلام والاتصال ومكافحتها، لأن الغاية من كل هذه الإجراءات في مثل هذا النوع من القضايا هو حماية الدليل الإلكتروني باعتباره سهل الإتلاف، ومثل هاته القواعد الصارمة تساعد المحقق في محاولة إثبات العقبات الإجرائية التي تواجهه في الكشف على مرتكبي هذه الجرائم.

فإن معظم جلسات التحقيق أو المحاكم الخاصة في الجرائم المعلوماتية وإثباتها تأخذ طابعا اجتماعا وقضائيا وعالميا بإعتبارها تكون في الفضاء السيبيراني ، و هذا تماشيا مع المبادئ والقواعد العالمية التي تبناها المشرع الجزائري، و كرسها في نصوص القانون، من هذا المنطلق نجد قانون الخاصة للوقاية من الجرائم المتصلة لتكنولوجيا الإعلام والاتصال ومكافحتها الذي جعل من إثبات الجرائم الإلكترونية غاية وهدف لحماية حقوق المتضررين، وهذا من خلال المحافظة على الدليل الإلكتروني ومحاولة إيجاد الحلول في المشاكل التي تواجه الضبطية القضائية وجهات التحقيق أثناء سير عملية التحري والتي تتمحور في العقبات الإجرائية من خلال سن قوانين مرنة.

حالة عملية:

خلال فترة التربص، تم متابعة عدة حالات في الجرائم الإلكترونية، ومن أبرزها:

- ✓ حالة الطفل القاصر (س، ف)
- ✓ التهمة جنحة صناعة وحيازة وعرض وتوزيع صور مخلة بالحياء/ المساس بحرمة الحياة الخاصة / تحريض قاصر على الفسق وفساد الأخلاق.
- ✓ التاريخ: 14 فيفري 2024

✓ المكان: مدينة الوادي

تفاصيل الواقعة

في يوم 14 فيفري 2024، في حدود الساعة 10:00 صباحا تم تحديد هوية المشتبه فيهم الخمسة ويتعلق الأمر بكل من (ف، ن)، (ب، ي)، (ع، خ)، (ك، ن)، (م، ب)، بطبيعة الجرم المنسوب إليهم أين تم توقيفهم من قبل رجال الضبطية القضائية بعد الإشتباه في تورطهم و هذا بوجود قرائن تثبت إدانتهم، بعد توقيفهم تم العثور بحوزتهم على هواتف نقالة تحتوي علة فيديوهات خاصة بالضحية تثبت الجرم المنسوب إليهم.

إجراءات التوقيف وإبلاغ ولي الأمر:

✓ تم توقيف المشتبه فيهم الخمسة من بينهم ثلاث "قصر"

✓ فور توقيف القصر سالفي الذكر قامت رجال الضبطية القضائية بإتصال بأوليائهم الشرعيين وبإبلاغهم تهم موجهة لأبنائهم ولمكان احتجازهم أين قاموا بالإلتحاق بمركز الأمن ساعة إبلاغهم

تعيين محام

تم تعيين محام متخصص ومتمرس في قضايا الجنح للدفاع عن القاصر الضحية (س، ف).

توقيف الطفل للنظر :

تم نقل المشتبه فيهم الخمسة إلى غرفة التوقيف للنظر أين تم وضع القصر منهم بغرفة توقيف النظر الخاصة بالأحداث ، حيث تتوفر ظروف إنسانية تراعي سنه. وهذا بعد فحصهم عند الطبيب للتأكد من توفير ظروف احتجاز ملائمة.

الاستجواب والتحقيق

بدأ التحقيق في الساعة 10:00 صباحا بحضور أوليائهم الشرعيين

الإجراءات القانونية اللاحقة:

✓ تم تحديد جلسة محكمة خاصة بالأحداث بعد يومين من توقيفهم بالنسبة للقصر والمشتبه فيهم.

✓ إحالة باقي المتهمين البالغين على قسم جنح المثول الفوري

الخلاصة:

تم التعامل مع حالة الضحية (س، ف) بمهنية عالية، مع التركيز على حقوقه كقاصر وضمان توفير بيئة احتجاز مناسبة شملت الإجراءات القانونية توفير محام والدعم النفسي والاجتماعي.

أهم العراقيل:

✓ قيام المشتبه فيهم بإخفاء القرائن والأدلة وطمسها، وذلك عن طريق مسح الشرائح التي تخص الفيديوهات المضرة بالضحية

✓ تعاون فرقة مكافحة الجرائم السيبيرانية بحيث استطاعت استرجاع نصف الفيديوهات لكن الباقي تم إتلافه، مما يؤكد صعوبة إثبات مثل هذا النوع من الجرائم، بحيث تعتبر من أهم العراقيل التي تواجه المحققين في إثبات الجرائم الإلكترونية

✓ من خلال التربص، تبين أن النظام القانوني يولي أهمية كبيرة لمكافحة الجرائم الالكترونية وطريقة إثباتها وذلك من خلال ضمان وجود إجراءات خاصة تتناسب مع نوع الجرم وطبيعته، كما يمتاز هذا النوع من الجرائم بأساليب تحري خاصة.

التوصيات:

✓ تطوير برامج لحماية حرمة الحياة الخاصة.

✓ من خلال التربص الميداني الذي قمنا به اتضح لنا ميدانيا ومن خلال النصوص القانونية فإن تنمية الإجراءات البحث والتحري المستحدثة يعد بأن المشرع الجزائري وبالرغم من خطورة هذه الإجراءات وسياستها بالحياة الشخصية للمشتبه فيهم، فإنه كرس كافة الضمانات الكفيلة بتحقيق التوازن بين حماية المجتمع من جهة والخافقة على حقوق وحريات الأشخاص من جهة أخرى.

✓ الطبيعة الخاصة للجريمة المعلوماتية فرضت على المشرع الجزائري مطا جديدا من الأدلة وهو الأدلة الرقمية، ويبقى استحداث المشرع الجزائري لقواعد إجرائية جديدة في البحث والتحري في هذا النوع من الجرائم اعترافا صريحا منه بأن الدليل الرقمي هو الأنسب في إثباتها.

فهرس المحتويات

ملخص الدراسة:

تواجه الجهات المختصة صعوبات جمة في إثبات الجرائم المعلوماتية لعدة أسباب، أهمها صعوبة تحديد مكان الجريمة بحيث قد تحدث الجريمة المعلوماتية في أي مكان في العالم، مما يجعل تحديد مكان وقوعها أمرًا صعبًا، وكذا تترك الجريمة المعلوماتية آثارًا رقمية في العديد من البلدان، مما يتطلب تعاونًا دوليًا لجمع الأدلة ومن جهة أخرى سهولة إخفاء الأدلة الرقمية والتي يمكن للمجرمين فيها بسهولة إخفاء أو تدمير الأدلة الرقمية، مثل حذف الملفات أو مسح سجلات الكمبيوتر، و قد تتواجد الأدلة الرقمية على أجهزة متعددة، مما يجعل جمعها وتحليلها أمرًا صعبًا، كما أن افتقار المحققين والقضاة إلى الخبرة والمهارات اللازمة للتحقيق في الجرائم المعلوماتية وفهم الأدلة الرقمية وقد لا يكون لدى الجهات المختصة الأدوات والتقنيات اللازمة لجمع وتحليل الأدلة الرقمية، بإعتبار أن المجرم الإلكتروني متخصص في مثل هذا النوع من الجرائم.

الكلمات المفتاحية: العقبات الإجرائية، الجريمة المعلوماتية، الدليل الإلكتروني، التفتيش، إعتراض المراسلات، الخبرة

Study summary:

Competent authorities face great difficulties in proving cybercrimes for several reasons, the most important of which is the difficulty of determining the location of the crime, as cybercrime may occur anywhere in the world, which makes determining the location of its occurrence difficult. Cybercrime also leaves digital traces in many countries, which requires cooperation. On the other hand, it is easy to hide digital evidence, in which criminals can easily hide or destroy digital evidence, such as deleting files or erasing computer records. Digital evidence may exist on multiple devices, which makes collecting and analyzing it difficult, and investigators and judges lack The experience and skills necessary to investigate cybercrimes and understand digital evidence, and the competent authorities may not have the tools and techniques necessary to collect and analyze digital evidence, given that the cybercriminal specializes in this type of crime.

Keywords: procedural obstacles, information crime, electronic evidence, inspection, interception of correspondence, experience