جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم : القانون العام

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

الخبرة التقنية في مجال الإثبات للجريمة الالكترونية

ميدان الحقوق و العلوم السياسية

الشعبة: الحقوق

التخصص: القانون الجنائي والعلوم الجنائية

من إعداد الطالب :

– وناس محمد

تحت إشراف الأستاذ :

– مزيود بصيفي

أعضاء لجنة المناقشة

الأستاذة.....بن عزوز سارة .....رئيسا

الأستاذ.....**مزيود بصيفي** ..... مشرفا مقررا

الأستاذ.....بوزيد خالد .....مناقشا

السنة الجامعية: 2024/2023

نوقشت يوم:08/../06/ 2024

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
لإنجاز البحث

أنا الممضي أدناه،

السيد: وناس محمد الصفة: طالب

الحامل لبطاقة التعريف الوطنية رقم: 100460336 والصادرة بتاريخ: 07/04/2016

المسجل بكلية: العلوم السياسية قسم: القانون عام

والمكلف بإنجاز مذكرة ماستر بعنوان:

الحوكمة المحلية في مجال التنمية المحلية المستدامة

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 17/07/2024

إمضاء المعني

الد وناس محمد
ب ت 100460336
عن ب ت 2016.04.07
مستغانم
17 JUIL 2024

المجلس الشعبي البلدي

المرسوم الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

بسم الله الرحمن الرحيم

الإهداء

أهدي هذا العمل إلى أعز ما يملك الإنسان في هذه الدنيا إلى ثمرة نجاحي إلى من أوصى بهما الله سبحانه وتعالى :

" وبالوالدين إحسانا " سورة الإسراء – الآية 23

إلى الشمعة التي تحترق من أجل أن تضئ أيامي إلى من ذاقت مرارة الحياة وحلوها، إلى قرة عيني وسبب نجاحي وتوفيقي في دراستي إلى

"أمي "

أطل الله في عمرها

إلى الذي أحسن تربيتي وتعليمي وكان مصدر عوني ونور قلبي وجلاء حزني ورمز عطائي ووجهني نحو الصلاح والفلاح إلى

"أبي "

أطل الله في عمره

إلى أخواتي وجميع أفراد عائلتي

إلى أستاذي " **مزيود بصيفي** " و جميع الأساتذة الأجلاء الذين أضاءوا طريقي بالعلم

وإلى كل أصدقاء الدراسة و العمل ومن كانوا برفقتي أثناء إنجاز هذا البحث إلي كل هؤلاء وغيرهم ممن تجاوزهم قلمي ولن يتجاوزهم قلبي أهدي ثمرة جهدي المتواضع

شكر وتقدير

– الحمد لله على توفيقه وإحسانه، والحمد لله على فضله وإنعامه، والحمد لله على جوده وإكرامه، الحمد لله حمدا يوافي نعمه ويكافئ مزيده

أشكر الله عز وجل الذي أمدني بعونه ووهبني من فضله ومكنني من إنجاز هذا العمل ولا يسعني إلا أن أتقدم بشكري الجزيل إلى كل من ساهم في تكويني وأخص بالذكر أستاذي الفاضل

" **مزيود بصيفي** "

الذي تكرم بإشرافه على هذه المذكرة ولم يبخل عليا بنصائحه الموجهة لخدمتي

فكان لي نعم الموجه والمرشد

كما لا يفوتني ان أشكر أعضاء لجنة المناقشة المحترمين الذين تشرفت لمعرفتهم وتقييمهم لمجهوداتي

كما أشكر كل من قدم لي يد العون والمساعدة ماديا أو معنويا من قريب أو بعيد

إلى كل هؤلاء أتوجه بعظيم الامتنان وجزيل الشكر المشفع بأصدق الدعوات

قائمة المختصرات

ج. ر.ج. ج : الجريدة الرسمية للجمهورية الجزائرية

• ص : الصفحة

ص. ن: الصفحة نفسها

• ف: الفقرة

ع: العدد

• م: المجلد

• د.ط: دون طبعة

• د.د.ن: دون دار النشر

. د.س.ن: دون سنة النشر

• ق . إ. ج: قانون الإجراءات الجزائية

. ق. ع: قانون العقوبات

مقدمة

مقدمة

شهد العالم تقدما تكنولوجيا لم يسبق له مثيل وقد نتج عن ذلك ظهور وسائل اتصال متطورة، جعلت العالم قرية صغيرة مفتوحة تلاشت معها الحدود الجغرافية والسياسية للدول، ولقد أدى الاستخدام السيء لهذه الوسائل إلى ظهور نمطا جديدا من الجرائم لم يكن معهودا من قبل سمي بالجرائم الإلكترونية، ونظرا للطبيعة الخاصة لهذه الجرائم من حيث طابعها الفني المتعلق بأساليب ارتكابها وسهولة إخفاء أو محو الدليل بات من الضروري استعانة جهات التحقيق أو القاضي بخبير متخصص في المعلوماتية لاستخلاص الدليل الرقمي، خاصة مع ظهور الأدلة العلمية في عملية الإثبات الجنائي تنامي دور الخبراء وأصبح لهم دور إضافي يتمثل في المساهمة في تفسير الدليل الرقمي وإبداء رأيهم في التخصصات التي لا يمكن للقاضي الإحاطة بها بحكم تكوينه القانوني البحث، وهو أمر تطلبته السياسة الجنائية التي جعلت من اللجوء إلى الخبرة القضائية أمرا ضروريا ومهما في الجرائم الإلكترونية و تقوم الخبرة في العصر الراهن بدور بارز في عملية الإثبات القضائي نظرا لما شهده هذا العصر من تطور علمي وتكنولوجي لحد وصفه بعصر المعلومات.

بالرغم من الإيجابيات والمزايا التي سبق ذكرها، بفضل تقنيات وسائل تكنولوجيا المعلومات والاتصال إلا أنها لا تخلو من جوانب السلبية، حيث تمثل في بعض الحالات تهديدا خطيرا للأمن والاستقرار، ما أدى إلى بروز نوع جديد من الجرائم المستحدثة لم تكن معروفة من قبل ما اصطلح على تسميتها " الخبرة التقنية في مجال الإثبات الجريمة الالكترونية " أو "الجرائم المعلوماتية، بالتالي تعقدت معها أكثر فأكثر مهمة التحقيق الجنائي على سلطات التحقيق و الضبطية القضائية، حيث تتميز هذه الأخيرة بخصائص تختلف في مفهومها و أركانها و وسائل ارتكابها و ونوعية الجناة عن الجرائم التقليدية، ما يجعلها أكثر خطورة و تعقيد، فظلا على أنها جرائم عابرة للحدود تتم عبر شبكات اتصال لا متناهية بالإضافة إلى

السهولة والسرعة في التنفيذ و طمس الأدلة و إخفائها التي يستفيد منها المجرم الإلكتروني في هذا النوع من الجرائم.

وجمع وتثير مسألة الخبرة التقنية في مجال الإثبات للجريمة الالكترونية عوائق ومشاكل عديدة في مجال التحقيق الأدلة الجنائية، نظرا لمميزات و خصوصيات هذه الجريمة ما يشكل عقبة كبيرة أمام كشفها كما تكمن صعوبة الإثبات في هذا النوع من الجرائم، في تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر الأنترنت في سهولة محو الدليل الإلكتروني ، كما لا يترك مرتكبيها آثار مادية بسبب دقتها و سرعة القيام بها و إمكانية محو آثارها و إخفاء الأدلة عقب وقوع الجريمة مباشرة كما أن ارتكاب هذه الجرائم يتعدى الاختصاص الإقليمي للدول يثير مشكلة الاختصاص المكاني و القانون الواجب التطبيق

كل ما سبق ذكره من خصوصيات للجرائم الإلكترونية و عوائق التحقيق فيها، دفع المختصون في مجال القانون و الإعلام الآلي و تكنولوجيات الإعلام و الاتصال، يكتفون العلمية بالعمل على تطوير المنظومة القانونية وتطوير أساليب الحماية للنظم جهودهم و البرامج الإلكترونية، و سد الثغرات التي تعتري النصوص الإجرائية للتشريعات التقليدية القائمة، لمواجهة هذه الجريمة باستنباط الدليل الذي يتوافق مع الطبيعة التقنية التي يتميز بها هذا النوع من الجرائم.

أهمية الموضوع تظهر لنا أهمية هذه الدراسة باعتبار أن مرحلة التحقيق تعتبر من أهم مراحل الدعوى الجنائية، حيث تسمح هذه المرحلة بالحصول على دليل إثبات قوي و متماسك لا يمكن دحضه من أجل ضمان حماية حقوق الضحايا و محاكمة الجاني محاكمة عادلة و توقيع الجزاء المناسب مبنية على مبدأ الشرعية، كما تبرز أهمية الموضوع في التطور السريع و المستمر الذي تتميز به الخبرة التقنية في مجال الإثبات للجريمة الالكترونية ة الأمر الذي ألزم المشرع و سلطات التحقيق العمل على تطوير وسائل وأساليب التحقيق، للتصدي لهذه الجريمة التي تمتد إلى جميع القطاعات و الميادين ، فهي جريمة بلا حدود تمس الأشخاص

المعنوية و الطبيعية على حد سواء كما أن الخاصية اللامادية للدليل الإلكتروني خلقت صعوبات غير مسبوقة أمام سلطات التحقيق بالتالي كان من المنطقي أن تنصب دراستنا على الجوانب الإجرائية المتعلقة بجمع الدليل الإلكتروني و نتيجة ذلك سوف نركز في بحثنا هذا على السلطات المختصة بالتحقيق في الجريمة الإلكترونية و كذلك على الجانب الإجرائي و ما تقوم به هذه السلطات من إجراءات لجمع دليل الإلكتروني و كذلك الأجهزة المناط بها مهمة التحقيق الجنائي بالتالي بات من الضروري إعطاء هذا الموضوع الأهمية اللازمة و اتخاذ التدابير و الإجراءات اللازمة لحماية الأفراد والمجتمع و مؤسسات الدولة من هذه الجريمة.

أسباب اختيار الموضوع يرجع اختيار هذا الموضوع إلى عدة أسباب الشخصية منها و هي التعرف أكثر على هذا النوع من الجرائم نظرا لحداثتها و الخبرة التقنية في مجال الإثبات للجريمة الالكترونية الوسائل المستعملة و التزايد الهائل لعدد القضايا المطروحة في أروقة العدالة وانتشارها بمعدلات قياسية تزامنا مع التطور التكنولوجي المستمر الذي يعرفه هذا المجال و كانت حافزا قويا دفعنا لاختيار هذا الموضوع والتعمق في إجراءات التحقيق وجمع الأدلة والحصول على الدليل الإلكتروني، و طرق إثبات هذا النوع من الجرائم و ما يميزه من تعقيد و خروج عن المألوف مقارنة بالجريمة التقليدية المادية.

وتكمن أهمية الدراسة للدور التي تؤديه الخبرة في مجال الإثبات الجنائي، وتعاظم هذا الدور في ظل التطور العلمي والتقني الذي نشهده كل يوم وازدادت أهميتها في استخلاص الدليل الرقمي لإثبات الجرائم الإلكترونية، حيث تتعلق بمسائل آية في التعقيد، يصعب على المحقق جمع أدلتها و كشف حقيقتها إلا بالاستعانة بأهل الخبرة، لهذا يهدف هذا البحث بالدراسة والتحليل لدور الخبرة في إثبات الجريمة الإلكترونية،

ومن صعوبات الدراسة التي تواجه كل دراسة أو بحث من الصعوبات التي اعترضتنا أثناء إعداد هذا العمل المتواضع حيث تتمثل في حداثة هذا الموضوع و نقص المراجع و المؤلفات المتخصصة في هذا المجال و لو أن هناك مجموعة من المراجع و المقالات التي تطرقت إلى

الموضوع لكن بشكل جزئي دون تناول كل جوانبه و إنما تمت معالجته بشكل سطحي بالإضافة إلى ارتباط هذا النوع من الجرائم بالحاسب الآلي و الذكاء الاصطناعي و ما يتطلبه من إحاطة بمكونات هذا الأخير و ما بتطلبه من تقنيات تتعلق بهذا النوع من الجرائم و كل ما يحتاجه من جهد فني و قانوني ، بالتالي صعوبة الإلمام بالموضوع والحصول على المعلومات الكافية.

إشكالية الموضوع أما عن الإشكالية التي يطرحها موضوع دراستنا هذا، فتنصب أساسا حول ما

- عن القواعد والضوابط المتعلقة بأحكام الخبرة في الجريمة الإلكترونية، وبيان كيفية تعامل الخبير التقني لاستخلاص الدليل الرقمي؟

- في ما تتمثل الخبرة التقنية في مجال الإثبات للجريمة الالكترونية

منهج الدراسة كما يعتبر الاختيار الصحيح للمنهج من أهم العناصر التي تساعد على انجاز البحوث العلمية بطريقة ناجحة من خلال دراستنا هذه تم الاعتماد على المنهج الوصفي التحليلي وصفي من خلال و الخبرة التقنية في مجال الإثبات للجريمة الالكترونية وكذا وصف الجهات والسلطات المناط بها مهمة التحقيق وكذلك الإجراءات المتبعة في التحقيق في الجرائم الإلكترونية لاستخلاص الدليل الإلكتروني والصعوبات التي تعتريها أما بخصوص المنهج التحليلي تم الاعتماد عليه في تحليل ومناقشة آليات التحقيق في الجرائم الإلكترونية و مدى فعاليتها في مواجهة هذه الجريمة.

تقسيم البحث

وللإجابة على الإشكالية المطروحة من خلال دراستنا هذه، ارتأينا تقسيم البحث إلى فصلين بحيث خصصنا الفصل الأول بعنوان **الإطار القانوني للخبرة الفنية المتعلقة بالجرائم الالكترونية** بحيث تم تقسيم هذا الفصل بدوره إلى مبحثين أين تناولنا في المبحث الأول إلى القواعد القانونية التي تحكم عمل الخبير في الجرائم المعلوماتية والمبحث الثاني إلى القواعد الفنية التي تحكم عمل الخبير في مجال الجرائم المعلوماتية

أما بخصوص الفصل الثاني القواعد الاجرائية في استخلاص الدليل الالكتروني والقيمة القانونية له تم التطرق إلى بدوره إلى مبحثين أين تناولنا في المبحث الأول إلى القواعد الاجرائية في استخلاص الدليل الالكتررونيي والمبحث الثاني إلى القيمة القانونية للدليل الالكتروني في مجال الاثبات الجنائي أما وقد أنهينا البحث بإعداد خاتمة تتضمن أبرز النتائج المتوصل إليها.

الفصل الأول

الإطار القانوني للخبرة الفنية المتعلقة بالجرائم الإلكترونية

تمهيد

لقد ألقت التكنولوجيا الحديثة بتأثيرها وارتبطت بشكل قوي بمختلف مجالات النشاط الإنساني بكافة أشكاله ومضامينه، حتى أصبحت أمراً ضرورياً لا يمكن الاستغناء عنها، وأصبحت التكنولوجيا مقوماً أساسياً من مقومات دفع عجلة التقدم بالأمم والحضارات ومقياساً لتقدمها، غير أنه في المقابل أقترنت هذه التقنية بظهور أفعال غير مشروعة أصبحت تشكل ظاهرة إجرامية من نوع خاص تختلف عن الظواهر الإجرامية العادية والكلاسيكية، إذ أوضحت العديد من المفاهيم القانونية السائدة سواء على مستوى القانون الموضوعي من حيث التجريم والعقاب بفعل ازدواجية طبيعتها بين جريمة معلوماتية محضة تستهدف الأنظمة والبيانات المعلوماتية في حد ذاتها، أو كجريمة عادية مرتكبة بواسطة تقنية المعلومات كآلية من أجل التواصل والتخطيط لتنفيذ المشاريع الإجرامية، أو على مستوى القانون الإجرائي بفعل تغلبها على القواعد المسطرية المقررة كأصل عام للبحث وملاحقة مرتكبي الجرائم العادية ومحاكمتهم، مما يتعين القول بأن الإجرام المعلوماتي قد أحدث ثورة هائلة في فلسفة التجريم والعقاب والإجراءات الجنائية [1].

وقد أظهر واقع الخبرة وممارسات بعض الخبراء القضائيين تميز الخبير كمتبوع في علاقته بتابعيه عن غيره من المتبوعين الآخرين، ومن ثم تجلت خصوصية مسئوليته المدنية عن الضرر الحاصل من فعله وفعل غيره من نواح متعددة، ينبغى بيانها في سبيل الخروج بدراسة أشمل ، وأعم من الفائدة المرجوة منها [2].

[1]– هشام ملاطي، خصوصية القواعد الإجرائية للجرائم المعلوماتية – محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014 ص. 101

[2]– عبد الرحمان اللمتوني الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 20014ص 48

المبحث الأول : القواعد القانونية التي تحكم عمل الخبير في الجرائم المعلوماتية

تقوم الخبرة في العصر الراهن بدور بارز في عملية الإثبات القضائي نظرا لما شهده هذا العصر من تطور علمي وتكنولوجي لحد وصفه بعصر المعلومات ،لذا سنتناول موضوع الخبرة في مطلبين نتناول في المطلب الاول ماهية الخبرة وأهميتها وفي المطلب الثاني نتناول شروط صحة أعمال الخبرة ومدى حجيتها وعلى النحو الاتي:

المطلب الأول ماهية الخبرة وأهميتها وأنواعها

من اجل تعريف الخبرة وبيان أهميتها وأنواعها سنقسم هذا المطلب الى ثلاثة فروع نتناول في الأول ماهية الخبرة وأهميتها وفي الفرع الثاني نتناول أنواع الخبرة في المجال المعلوماتي وكالاتي :

الفرع الأول ماهية الخبرة وأهميتها

في هذا الفرع نتناول ماهية الخبرة وأهمية الاستعانة بالخبراء في مجال الجرائم المعلوماتية في نقطتين وكالاتي :

أولا:ماهية الخبرة :

الخبرة (لغة) هي العلم بالشئ واختباره[1] ،اما في الاصطلاح القانوني فهي: الاستشارة الفنية التي يستعين بها القاضي والمحقق في الاثبات لمساعدتهما في تقدير المسائل الفنية التي يحتاج تقديرها الى معرفة ودراية علمية خاصة تتعلق بالجريمة الواقعة التي لاتتوافر لدى القاضي[2] .

والخبرة أيضا هي إجراء يتعلق بموضوع يتطلب الالمام بمعلومات فنية لإمكان استخلاص الدليل منه[1].

[1]– ابن منظور ،لسان العرب ،المجلد الرابع ،بيروت ،ص227 .

[2] – جندي عبد الملك ،الموسوعة الجنائية ،دار الكتب المصرية ،القاهرة ،1931م ،ص222 .

والخبير هو كل شخص له دراية خاصة بمسألة من المسائل وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لايشعر المحقق بتوافرها في نفسه فيمكنه ان يستشير فيها خبيرا كما هو الحال في تقرير الصفة التشريحية في جرائم القتل وتحليل المادة المطعومة في جريمة تسمم او فحص لخطوط الكتابة المدعى بتزويرها[2] .

ولايشترط في الخبير الكفاءة العلمية العالية في مجال التخصص فحسب بل يجب ان تضاف إليها سنوت من الخبرة في المجال الذي تميز فيه وعلى وجه الخصوص الجرائم ذات الصلة بالحاسب الآلي فقد يتعلق الامر بتزوير المستندات او بالتلاعب في البيانات او بالغش اثناء نقل او بث البيانات او الاعتداء على حرمة الحياة الخاصة او عرض صور او افلام مخلة بالاداب العامة[3] ،ويطلق على الخبير في مجال الجرائم المعلوماتية بـ(الخبير المعلوماتي) او الخبير الالكتروني الرقمي .

ثانيا :اهمية الاستعانة بالخبراء :

تكمن أهمية الاستعانة بالخبراء في أنها تنير للقاضي الذي يهتدي به لتحقيق العدالة لذا فقد اهتم المشرع العراقي بتنظيم أعمال الخبرة فقد اجاز قانون أصول محاكات الجزائية رقم 23 لسنة 1971م للقاضي او المحقق ان يندب خبير لإبداء الرأي في حالة لها صلة بالجريمة التي يجري التحقيق فيها[4].

واذا كان للخبرة تلك الاهمية في الجرائم التقليدية فإن اهميتها تزداد وتصبح ضرورية بل وحتمية في اثبات الجرائم الالكترونية ،فالخبرة وسيلة من وسائل الاثبات التي تهدف الى كشف

---

[1]– د.مأمون محمد سلامة ،الاجراءات الجنائية في التشريع المصري ،ج1 ،دار النهضة العربية ،القاهرة ،2001م ،ص645 .

[2]) د.احمد فتحي سرور ،الوسيط في قانون الاجراءات الجنائية ،ط7 ،دار النهضة العربية ،القاهرة ،1993م ،ص457 ومابعدها .

([3]) د. محمد ابو العلا عقيدة ،التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية ، المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي ، مركز البحوث و الدراسات ، العدد 1 ، الإمارات العربية المتحدة ، دبي ،2003 م ، ص 27 .

([4]) المادة (69)من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971م .

بعض الدلائل او الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية وهي بحث لمسائل مادية او فنية يصعب على المحقق ان يشق طريقه فيها ويعجز عن جمع الادلة بالنسبة لها بالوسائل الأخرى للإثبات[1] .

وبالنسبة لمجالات الخبرة في الجرائم الرقمية نجد ان التطور الهائل في مجال تكنولوجيا المعلومات افرز العديد من الأنشطة المستحدثة التي تتم بإستخدام الوسائل الالكترونية التي قوامها نظم وبرمجيات الحاسب الآلي وشبكات الاتصال العالمي (الانترنت) كأعمال التجارة الالكترونية والمصارف والأعمال المصرفية الالكترونية مما ترتب عليه ان تتنوع الجرائم التي تقع على هذه العمليات وفقا لنوع الوسائل الالكترونية المستخدمة في ارتكابها ومن امثل هذه الجرائم :

أ. تزوير المستندات المدخلة في انظمة الحاسبات الالية .

ب. التلاعب في البيانات .

ت. التلاعب في البرامج الاساسية او برامج التطبيقات .

ث. الغش اثناء نقل وبث البيانات [2]

.

الفرع الثاني انواع الخبرة في المجال المعلوماتي

[1]– د. علي محمود حمودة ،الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي ، المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي ، مركز البحوث و الدراسات ، العدد 1 ، الإمارات العربية المتحدة ، دبي ،2003م ،ص285 .

[2]– أ. عبد الناصر محمد محمود فرغلي ؛ د.محمد عبيد سيف المسماري ،الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية ، بحث من ضمن أعمال المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي ،جامعة نايف العربية للعلوم الأمنية ، الرياض ،2007م ،ص25 .

تكون الخبرة في المجال التقني خاصة عن طريق الجهات او المؤسسات التعليمية وقد تتم عن طريق جهات الضبط القضائي وفيما يلي بيان لكل نوع منها :

اولا :الخبرة الشخصية : وهذه تعد اقوى انواع الخبرات على الاطلاق لكونها تنطلق من مفهوم السعي الى خلق فرص منافسة حقيقية بين المنظمات الخاصة وهي تظم في جنباتها الخبرة الفردية التي تعد اقوى واهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والانترنت ويكفي هنا ان نذكر ان المؤسسات الكبرى المتخصصة في مجال الكمبيوتر والانترنت تسعى بكل جهودها للاستعانة بإشخاص اثبتوا كفائتهم في مجال الكمبيوتر والانترنت حتى عصاة القانون منهم فهناك اتجاه اقتصادي يحاول جاهدا اثبات عدم جدوى التخلص من هؤلاء بمعاقبتهم وفقا للقانون وانما يلزم اللجوء للحلول الاقتصادية لكي يمكن ان يظلوا عاملين في إطار الأهداف الاقتصادية[1] ،بل ان من الدول من تسعى جاهدة الى محاولة التعرف على قراصنة تحولوا مع مرور الوقت الى رموز وطنية جراء تحركاتهم عبر الانترنت.

والى جوار الافراد توجد المنظمات الخاصة في كافة المجالات والتي سوف يكون لها السبق في مجال الخبرة وتختلف المنظمات الخاصة مابين منظمات اهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق الالكترونية وبين نوعية من المنظمات تسعى الى فك طلاسم العالم الافتراضي على اسس تجارية[2] .

ثانيا :الجهات التعليمية :

[1]– فقديكون احد خبراء المجال المعلوماتي من هؤلاء الجناة الذين تم تدريبهم داخل المؤسسات الالكترونية للاستفادة ايجابيا من قدراتهم فضلا عن تاهيلهم كمواطنين صالحين،ينظر ؛ د. عبد الفتاح بيومي حجازي ،الإثبات الجنائي في جرائم الكمبيوتر والإنترنت ،دار الكتب القانونية ، مصر ، 2007 م ،ص128 .

[2]– د. خالد ممدوح إبراهيم ،فن التحقيق الجنائي في الجرائم الإلكترونية ،دار الفكر الجامعي ،الإسكندرية ، 2009 م ،ص294 .

لما كانت شبكة الانترنت تعد احد منتجات العالم في حركته التقنية فإنه يمكن القول وبحق ان اقوى مظاهر الخبرة التي يمكن الاستعانه بها لمواجهة الجريمة في العالم الافتراضي يمكن ان تكون من خلال المؤسسات والجهات التعليمية فهذه الاخيرة تعد مصدرا داعما ومتكاملا لمؤسسات الدولة ككل ،وهذه المؤسسات تعتمد منهجا علميا غير تجاري هدفها التأكيد على تطوير العلم ليقضي على المشكلات التي تواجه البشرية كما ان التفكير العلمي لايمكن تجنبه في رصده للظاهرة الانسانية والاتجاه العالمي في رصد تطورات الجريمة عبر الانترنت يتجه إلى المؤسسات العلمية بحيث يتم دعمها مادياً ومعنوياً لتكون أفضل سبل المواجهة لاسيما وأن المعتقد السائد في مواجهة الجريمة المالية والنقدية ...إلخ. فإنه ليس هنالك أفضل من التقنيين في المعلوماتية لفك سر الجريمة عبر الإنترنت ، وقد قامت عدة مؤسسات تعليمية بتكوين قاعدة خبرة كبيرة فيها لتكون على أهبة الإستعداد لمواجهة الجريمة عبر الإنترنت ومن ذلك دراسات الكمبيوتر بشكل فائق في جامعة ستانفورد[1].

ثالثاً : جهات الضبط القضائي :

شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجراء على الإنترنت وعلى رأس تلك الدول الولايات المتحدة التي تجاوز نشاطها في هذا المجال الإطار الدولي المتمثل في منظمة الإنتربول وكان أخر نشاط في هذا الإطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية (FBI) أطلق عليه المعمل الإقليمي الشرعي للحاسوب[2] ومقره سان دييجو (San Diego) والذي تم إفتتاحه في نوفمبر 2000 م لكي يكون بيت خبرة عام متعدد النواحي القضائية غرضه مكافحة التصعيد الخطير في الجريمة عبر الإنترنت وذلك بتحليل وتصنيف الدليل الرقمي بحيث يتم إعداد محللين شرعيين للحاسب الآلي (computer

[1]– د . خالد ممدوح إبراهيم ، مصدر سابق ، ص 294 .

[2] –The Regional Computer Fervencies Laboratory .

forensics examiners) الذين سوف يكون لهم أهمية كبرى في نطاق العمل على تكثيف مواجهة الجريمة عبر الإنترنت[1].

وعلى الصعيد العربي فقد قامت المملكة العربية السعودية بإنشاء معمل علم الأدلة الرقمية بكلية الملك فهد الأمنية في الرياض والذي تم افتتاحه في 10 يناير 2012 م ذلك أن الهدف من إنشاء مشروع معمل علم الأدلة الرقمية هو تطوير المجال الأكاديمي والتدريبي في الكلية ورفع من قدرات الدارسين وليواكب تطورات العصر التقنية ليعد رجال أمن متخصصين ومؤهلين لمكافحة الجرائم الحديثة سواء كانت إلكترونية أو تقليدية والقدرة الفنية على إكتشافها عن طريق إستخدام الوسائل التقنية[2].

نعتقد إن على المشرع العراقي أن يخطو هذه الخطوة وهي إنشاء معمل علم الأدلة الرقمية وذلك لكي يعد رجال تحقيق متخصصين ومؤهلين لمكافحة الجريمة والتعرف على وسائل الإثبات بإستخدام الدليل الرقمي و الإرتقاء بمهارة رجال الأمن في التحقيق في الجرائم المعلوماتية الحديثة.

ومن التشريعات الحديثة التي نظمت أعمال الخبرة في مجال الجرائم الإلكترونية القانون البلجيكي الصادر في 23 نوفمبر 2000م فقد نصت المادة (88)من القانون المذكور على إنه[3] :" يجوز لقاضي التحقيق وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة

---

[1]– ويبرز تعدد النواحي التي يتعامل معها المعمل الشرعي الجديد كونه يتكون من إلتقاء العديد من منظمات الضبط القضائي تتعاون فيما بينها لكي تتحق الفائدة المرجوة منه مثل إدارة مكافحة المخدرات (Drug Enforcement Administration) ووحدة التحقيقات لمكافحة المجرمين (Defense Criminal Investigation Services) ووحدة تحقيقات الجريمة في البحرية(Naval Criminal Investigation Services)ووحدة الكمارك(US Customs Services)ومكتب النائب العام للمقاطعة ومكتب حاكم المقاطعة وإدارة شركة كاليفورنيا ، ينظر ؛ د.خالد ممدوح إبراهيم ، المصدر السابق ، ص 297.

[2]– متاح على الموقع الإلكتروني :

–http://forum.sh3bwah.maktoob.com/t178434.html.

، تاريخ زيارة الموقع 2024/05/25 م .

[3] – د . محمد أبو العلا عقيدة ، مصدر سابق ، ص 27 .

المعلومات اللازمة عن كيفية تشغيل النظام أو كيفية الدخول فيه أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحولة أو المنقولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق".

كذلك مشروع الجريمة المعلوماتية العراقي لسنة 2011م أجاز للقاضي المختص الإستعانة بالخبير الفني[1] ، وقد بين المشروع المذكور إنه للخبير أن يقدم مستخرجات النسخ الإلكترونية بصورة ورقية ويرفق معها تقرير تفصيلي بتاريخ إجراء عملية الإسترجاع الورقي[2].

المطلب الثاني شروط صحة اعمال الخبرة ومدى حجيتها

الخبرة رأي او استشارة يقدمها الخبير في مجال اختصاصه لقاضي التحقيق ،فكثيرا مايتطلب كشف الجرائم التحقيق فيها رأيا علميا او فنيا او مهنيا في مسألة ما ،لذلك اعطى القانون للقاضي ان يقرر ذلك من تلقاء نفسه او بناء على طلب الخصوم[3] ،في هذا المطلب سنتناول شروط صحة اعمال الخبرة ومدى حجية تقرير الخبير وذلك في فرعين مستقلين وكالاتي :

الفرع الاول : شروط صحة اعمال الخبرة وضوابطها

نظرا للاهمية البالغة للخبرة والدور الذي يلعبه الخبير في عملية الاثبات في المجال الجنائي فقد حرصت معظم التشريعات على تنظيم الخبرة ووضع شروط وضوابط لها ،وهو ما سنتناوله بالشرح في النقاط الثلاثة الاتية :

---

[1]– نصت المادة (25/رابعاً) من المشروع المذكور على إنه :" للقاضي المختص في مرحلتي التحقيق والمحاكمة الإستعانة بالخبرة الفنية من داخل العراق وخارجه ".

[2]– المادة (26/ثالثاً) من المشروع أعلاه.

[3]– فخري عبد الحسن علي ،المرشد العلمي للمحقق ،بغداد ،منشورات مديرية الشرطة ،1999م ،ص193 .

اولا: شروط صحة اعمال الخبرة :

حددت المادة الرابعة من قانون الخبراء امام القضاء رقم (163) لسنة 1964م الشروط الواجب توفرها في الخبير وهي على نوعين ؛شروط عامة وشروط خاصة .

- الشروط العامة :

1. ان يكون عراقيا.
2. ان يؤدي اليمين من اجل اداء مهمته بصدق وامانة.
3. ان يكون حسن السيرة والسلوك.
4. ان لايكون مما سبق الحكم عليه بعقوبة جنائية عن جريمة عادية او ماسة بالشرف.

- اما الشروط الخاصة فهي ان يكون حاصلا على شهادة علمية دون تحديد مستواها الا اننا نعتقد بأن الخبير يجب ان يكون حاصلا على شهادة علمية لاتقل عن البكالوريوس وان يكون متخصصا في المجال الذي يراد ابداء رأيه فيه[1] .

وبعد انتهاء الخبير من ابحاثه وفحوصاته يعد تقريرا يضمنه خلاصة ما توصل اليه من نتائج بعد تطبيق الاسس والقواعد العلمية الفنية على المسألة محل البحث ومتى قدم الخبير تقريره فإنه يعتبر جزءا من اوراق الدعوى ويكون للخصوم مناقشته .

ثانيا :اسلوب انتداب الخبير :

وفقا لقانون الخبراء امام القضاء رقم (63) لسنة 1974م يجري تسجيل الخبير في سجل خاص بعد ان يحلف اليمين امام رئيس محكمة الاستئناف الاتحادية بأن يؤدي خبرته بأمان

[1]– وتطبيقا لذلك قضت محكمة استئناف بغداد /الرصافة الاتحادية بصفتها التمييزية بإنه: (لكي يكون تقرير الخبراء سببا للحكم يجب ان يكون جميع الخبراء من المختصين بشؤن التسجيل العقاري) ،رقم القرار 233/م/2009م ،مجلة التشريع والقضاء ،العدد الرابع ،بغداد ،2009م ،ص240 .

وحياد ويمنح بعدها هوية خبير (قضائي) حيث يتم التسجيل بعد التأكد من شروط اتقانه لتخصصه بعد تقديمه ما لديه من مستمسكات تثبت اهليته لأداء الخبرة ولايشترط في الخبير ان يكون حاصلا على شهادة معينة فقد يكون ممن اكتسب خبرته بالتجربة كالخبراء في فحص المركبات وارباب الحرف كالنجارين والحدادين وغيرهم [1] ،اما اسلوب انتداب الخبير فقد ترك القانون لقاضي التحقيق اوالمحقق حرية انتدابه وفقا لضرورات التحقيق وبحسب نوع الجريمة وظروفها ووقائعها ،فبمقتضى الفقرة (أ) من المادة (69)من قانون اصول المحاكمات الجزائية فإنه: (يجوز للقاضي او المحقق من تلقاء نفسه او بناء على طلب الخصوم ان يندب خبيرا او اكثر لإبداء الرأي في ما له صلة بالجريمة التي يجري التحقيق فيها) .

وحيث ان انتداب الخبير جوازيا فللقاضي السلطة في تقدير مدى ضرورة انتداب خبير من عدمه وبالتالي له الحرية في الاستجابة لطلبات الخصوم على ندب الخبير او رفضها .

ولايشترط في الخبير ان يكون مسجلا في جدول الخبراء اذا توافرت فيه الاهلية لأداء الخبرة في مجال تخصصه ،غير ان الخبير غير المسجل لابد من تحليفه اليمين في كل مرة يستدعى فيها لأداء الخبرة بينما لايشترط ذلك في الخبير القضائي[2].

ثالثاً :استبدال الخبير ورده :

ليس في القانون مايمنع من استبدال خبير بآخر وذلك في حالة اعتذر الخبير المنتدب مثلا ،وليس للقائم بالتحقيق اجباره على ذلك ،كما ليس هناك ما يمنع من رد الخبير اذا توافرت اسبابه كما هو الشأن في رد القضاة وهذا يعني ان لذوي العلاقة في الدعوى – وكذلك للإدعاء العام – الحق في الاعتراض على الخبير على ان يكون الاعتراض مسببا ومثاله ان تكون

[1]– .محمد واصل ؛حسين بن علي الهلالي ،الخبرة الفنية امام القضاء ،المكتب الفني ،مسقط ،2004م ،ص9 .

[2]– تلاحظ المادة (129) من قانون المرافعات المدنية وبمقتضاها لاحاجة لتجديد اليمين القانونية للخبير اذا كان مسجلا في جدول الخبراء كما تلاحظ المادة (134/ثانيا) من قانون الاثبات رقم (107) لسنة 1979م ونصها : ((اذا لم يكن الخبير مقيدا في جدول الخبراء وجب ان يحلف يمينا قبل مباشرته عمله بالصدق والامانة ،واذا فات المحكمة تحليف الخبير ابتداء وكان قد انجز مهمته على الوجه المطلوب وجب تحليفه بأنه قد ادى عمله بالصدق والامانة)) .

للخبير مصلحة او صلة قربى بأحد اطراف الدعوى وعلى القاضي ان يبت في الاعتراض متى تم اختيار الخبير من قبله وذلك بالقبول او الرفض اما اذا كان الخصوم هم من اختار الخبير واتفقو عليه فلس لهم الحق في الاعتراض[1] .

من جهة اخرى فإن القاضي غير ملزم بإنتداب خبير واحد او عدد محدد فله ان يقرر انتداب خبير او اكثر في القضية الواحدة كلما اقتضت ضرورات التحقيق ذلك[2].

الفرع الثاني مدى حجية تقرير الخبير

الخبرة شأنها شأن باقي ادلة الاثبات تخضع حجيتها لتقدير القاضي ومدى تأثير اعمال الخبرة على الاقتناع الذاتي للقاضي ولايتقيد به القاضي واذا لم تقتنع به المحكمة جاز لها ان تعين خبيرا اخر او خبراء اخرين ولايمنع ان يكون من بينهم احد الخبراء الاولين واذا عينت المحكمة جملة خبراء واختلفوا في الرأي جاز لها ان تعين خبراء اخرين للنظر في الخلاف وتنويرها فيه وعلى العموم فإننا نعتقد إن تقرير الخبير له قيمة امام القضاء لإنه يكشف الركن المادي للجريمة (كيفية ارتكاب الجريمة) ويمكن للمحكمة أن تعتمده دليلاً في حكمها إستناداً لنص المادة (213) من قانون اصول المحاكمات الجزائية وهو ليس بحكم ولكن القيمة القضائية لتقرير الخبيرليست كالقيمة القانونية لشهادة الشهود ، ولايمنع القاضي من حقه العام في تقدير الوقائع التي تعرض عليه حق قدرها[3].

[1]– تلاحظ المادة (130) من قانون المرافعات المدنية .

[2]– د. براء منذر كمال ،شرح قانون اصول المحاكمات الجزائية ،ط1 ،دار الحامد للنشر والتوزيع ،عمان ،2009م ،ص102 .

[3]– جمال محمد مصطفى ، التحقيق والإثبات في القانون الجنائي ،مطبعة الزمان ،بغداد ،2004 م ،ص56 .

المبحث الثاني : القواعد الفنية التي تحكم عمل الخبير في مجال الجرائم المعلوماتية

للدليل الجنائي الرقمي اهمية كبرى ودور اساسي في معرفة كيفية حدوث الجريمة ولتأكيد ذلك لابد وان يحتوي التحقيق الجنائي الرقمي على هذا الدليل ويجب ان يكون الاشخاص المسؤولون عن التعامل مع هذه الامور على فهم كبير واضطلاع بالأمور التقنية والاعيبها وكيفية التعامل بها [1] وعليه سنتناول في هذا المبحث الصعوبات التي تواجه عمل الخبير المعلوماتي واساليب عمله وذلك في مطلبين مستقلين وكالاتي.

المطلب الاول : الصعوبات التي تواجه عملية الاثبات الجنائي واساليب عمل الخبير المعلوماتي

تواجه الخبير في عملية الإثبات الجنائي في الجرائم المعلوماتية بعض الصعوبات ، كما توجد هناك صعوبات في اساليب عمل الخبير وهو ما سنوضحه في الفرعين التاليين :

الفرع الاول : الصعوبات التي تواجه عملية الاثبات الجنائي في الجرائم المعلوماتية

تتسم جرائم الكمبيوتر بصعوبة اكتشافها واثباتها فالجريمة المعلوماتية تتم في بيئة او اطار لاعلاقة له بالأوراق والمستندات بل تتم بواسطة الحاسب الالي او الشبكة العالمية ويمكن للجاني عن طريق نبضات الكترونية لاترى العبث في بيانات الحاسب الالي او برامجه وذلك في وقت قياسي قد يكون جزءا من الثانية وهذه البيانات او المعلومات التي يتم العبث بها يمكن محوها كذلك في زمن قياسي قبل ان تصل يد العدالة اليه سيما وان عملية الضبط لا تتم سوى بمعرفة خبير فني او متخصص[2] .

---

[1]–عبد الناصر محمود؛ د.محمد عبيد سيف ، مصدر سابق ،ص32 .

[2]– د. عبد الفتاح بيومي حجازي ،مصدر سابق ،ص24 .

ويواجه الخبير الجنائي صعوبات متعددة في سبيل جمع الادلة الرقمية من اجهزة الحاسب الالي او الشبكات الرقمية ومن هذه الصعوبات[1] :

اولا: **فقد جزء كبير من المعلومات و الاوامر** التي تشمل الادلة الرقمية حال اغلاق الحاسب الالي بطريقة غير صحيحة أو في حالة القطع المفاجئ للتيار الكهربائي عن الجهاز ،فعند غلق او قطع التيار الكهربائي عن جهاز الكمبيوتر فإن مثل هذا الفعل قد يؤدي الى محو المعلومات من ذاكرة الجهاز او العمل على تحريف بيانات هامة وحدوث ضرر في اجهزة الكمبيوتر (hard ware) او منع نظام التشغيل من اعادة التحميل (rebooting) وبالتالي فقدان الادلة الجوهرية .

ثانيا: **قيام الجاني بتهيئة جهاز الكمبيوتر للتفجير** او التدمير بمجرد تشغيله بالضغط على زر توصيل الطاقة (power) .

ثالثا: **طبيعة مسرح الجريمة** :فالشبكات منتشرة على مستوى العالم لذا فقد لا يكون ممكنا الحصول على دليل في حالة توزيع مسرح الجريمة بين اكثر من دولة بسبب تعقيد الاجراءات او وجود مشاكل عملية او تشريعية في بعض الدول مما يحول دون الحصول على دليل رقمي ،كما ان سرعة مرور البيانات الرقمية عبر الشبكات لأقل من جزء من الثانية مع مهارة المجرمون في تدمير الادلة او تحريف او تعديل البيانات لحماية انفسهم ،وكذلك حجم البيانات الضخمة التي تمر عبر الشبكات مما يكون له التأثير العكسي عند البحث عن دليل ادانة او براءة.

رابعا :**اخفاء الهوية** :فعند تعمد المستخدم اخفاء هويته حال استخدام الانترنت سواء القيام ببعض الاجراءات او استخدام بعض البرامج والتطبيقات التي تؤدي الى طمس الهوية مما يشكل عائقا امام المحقق الجنائي او الخبير الفني .

[1] – عبد الناصر محمود؛ د.محمد عبيد سيف ، مصدر سابق ،ص32 .

خامسا :**<u>إخفاء المعلومات</u>** :وجود بعض البرامج الخاصة بإخفاء المعلومات او البيانات المخفية وذلك لخلق ما يعرف بنظام ملفات امن عبر استخدام الشبكة العالمية مما تجعل عملية استعادة الادلة او اعادة تركيبها في غاية الصعوبة امام المحقق الجنائي .

ويتضح مما تقدم فإن الحصول على الادلة الجنائية الرقمية امر صعب الوصول اليه لما تتطلبه من خبرة ومهام كبيرة في مجال الكمبيوتر .

الفرع الثاني : اساليب عمل الخبير المعلوماتي

للخبير التقني في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها وهو في إطار القيام بعمله عليه أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسبباً بشكل منطقي وإلا تعرض حكمها للطعن عليه بالنقض[1].

وهناك أسلوبان لعمل الخبير التقني:

<u>الأول</u> : القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها – كما هو الشأن في التهديد (intimidation) أو النصب(fraud) أو السب(defamation) أو جرائم النسخ (infringement of copy rights) وبث صور فاضحة بقصد الدعاية للتحريض على إرتكاب جرائم الدعارة والرقيق الأبيض ودعارة الأطفال و غيرها – ثم القيام بعملية التحليل الرقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها وكيف تم التوصل إلى معرفتها ومن ثم التوصل في النهاية إلى معرفة بروتوكول الإنترنت (IP) الذي ينسب إلى جهاز الكمبيوتر .

[1]– خالد ممدوح إبراهيم ، مرجع سابق ، ص 296 .

الثاني : القيام بتجميع وتحصيل مجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بإرتكاب جرائم كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية وذلك حسب وزن الإنسان بإدعاء إنه إذا تم تتبع العمليات الواردة فيها فلن يصاب الشخص بحالة إدمان وأيضاً كيفية زراعة المخدرات بعيداً عن أعين الغير وأيضاً كيفية إعداد القنابل وتخزينها وكيفية التعامل مع القنبلة الزمنية وتركيبها والقيام بفكها وحفظها وكذلك القيام بتحديد مسار الدخول من مكان ثابت ومثل هذا الأمر جائز الحدوث كما لو كان مرتكب الجريمة مشتركاً لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها ويقوم بالولوج إلى الإنترنت من محل إقامته.

والخبرة في جرائم الإنترنت تساعد في المسائل الآتية[1]:

1. الكشف عن الدليل الرقمي.
2. إجراء الإختبارات التكنولوجية والعلمية عليه لإختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه لجهات التحقيق و المحاكمة .
3. تحديد الخصائص الفريدة للدليل الرقمي.
4. إصلاح الدليل وإعادة تجميعه من المكونات المادية (Hard Drive) .
5. عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية إستخلاص الدليل.
6. جمع الآثار المعلوماتية الرقمية (Cyber Trial Digital) التي قد تكون تبدلت خلال الشبكة المعلوماتية.
7. إستخدام الخوارزميات (Algorithm) للتأكد من أن الدليل لم يتم العبث بهاو تعديل[1] .

[1]– خالد ممدوح إبراهيم ، مرجع سابق ، ص (296–298) .

8. تحريز الدليل الرقمي لإثبات إنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة في الدعوى.

9. تحديد الخصائص المميزة لكل جزء من الأدلة الرقمية مثل :المستند الرقمي، البرامج، التطبيقات، الإتصالات، الصور، الأصوات...وغيرها.

من كل ما تقدم فإننا نعتقد بأن الخبرة في جرائم الإنترنت تكون على قدر كبير من الأهمية ، و ذلك لأن هذه الجرائم تحتاج إلى شخص يعرف منافذ الدخول إلى النظام و الخروج منه و كيفية إستخراج الدليل من شبكة الإنترنت من دون إتلافه أو تغييره و أيضاً كيفية تقديمه على شكل تقرير مفصل و مقبول قانوناً إلى القاضي المختص .

[1]- الخوارزميات (ALOGRITHM) هي مجموعة من التعليمات التي يمكن أن تتبع لإنجاز عمل ما بعدد محدد من الخطوات وذلك عبر تجزئة المسألة البرمجية المراد حلها إلى أجزاء صغيرة بسيطة وبتجميع هذه الأجزاء يمكن التوصل إلى حل صحيح ، ينظر ؛ د . ممدوح عبد الحميد عبد المطلب ، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الإنترنت ، المؤتمر العلمي الاول حول الجوانب القانونية والامنية للعمليات الالكترونية ،مركز البحوث والدراسات العدد(4) المحور الامني والاداري للفترة (26-28)ابريل 2003م ،دبي ،الامارات العربية المتحدة ، ص 90 .

المطلب الثاني استخلاص الدليل الرقمي

تعد عملية الحصول على الادلة الجنائية الرقمية امر صعب الوصول اليه لما تتطلبه من خبرة ومهارة كبيرة في مجال الحاسب الالي[1] ،ويرجع ذلك الى تعدد صور واشكال الجرائم المعلوماتية ما بين مهاجمة المعلومات بغرض تدميرها او الاستيلاء عليها او قد يكون المقصود بالهجوم هو الاجهزة كنشر فيروس يعمل على اتلاف وحداته الرئيسية مثلا او قد يكون الامر مجرد اختراق لكلمة سر خاصة ببنك او مؤسسة كبرى بغرض الاحتيال والحصول على الاموال وقد تكون لمجرد اثبات الذات واظهار المقدرات العالية في مجال الحاسب الالي وبناء على ماتقدم فإننا سنتناول عملية استخلاص الادلة الرقمية وحجيتها امام القضاء في فرعين مستقلين وعلى النحو الاتي :

الفرع الاول عملية استخلاص الدليل الرقمي

يعرف الدليل الجنائي الرقمي بأنه : (الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها بإستخدام برامج وتطبيقات وتكنولوجيا خاصة وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور والأصوات والأشكال والرسوم وذلك من أجل الربط بين الجريمة والمجرم والمجنى عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون)[2].

والذي يلاحظ على هذا التعريف إنه يقصر مفهوم الدليل الرقمي على ذلك الدليل الذي يتم إستخراجه من الحاسب الآلي ولاشك أن ذلك فيه تضييق لدائرة الأدلة الرقمية فهي كما يمكن أن تستمد من الحاسب الآلي فمن الممكن أن يتحصل عليها من أية آلة رقمية أخرى فالهاتف

---

[1]- محمد صفوت ،استخلاص الدليل الجنائي الرقمي ،مجلة العالم الرقمي ،على الموقع الالكتروني :2024/05/20
http://www.al-jazirah.com/digimag/28032004/wr46.htm-

[2]- مصطفى محمد موسى ،التحقيق الجنائي في الجرائم الالكترونية ،ط1،مطابع الشرطة ،القاهرة ،2009م ،ص217 .

وآلات التصوير وغيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدراً للدليل الرقمي .

وعُرِفَ بأنه : (الأدلة التي تشمل جمع البيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد أُرتكِبت أو توجد علاقة بين الجريمة والمتضرر منها والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة ، الرسومات ، الخرائط ، الصوت أو الصورة) ،ويعرف كذلك بأنه : (هي معلومات يقبلها المنطق والعقل ويعتمدها العلم يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الإتصال ويمكن إستخدامها في أية مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه)[1] ولما كانت عماية تجميع الادلة العلمية الجنائية في الجرائم المعلوماتية او الرقمية تعد اهم واصعب الامور التي تواجه عملية الاثبات الجنائي ،لذا كان لزاما ان يتم اللجوء الى خبير قضائي معلوماتي او رقمي متخصص لإشتقاق الدليل العلمي الفني الجنائي ،والخبير المعلوماتي او الرقمي هو الخبير المتخصص والمدرب على معالجة جميع انواع الادلة الرقمية وفحصها وتحليلها[2].

ويرى بعض المتخصصينان عملية تجميع الأدلة الرقمية في الجرائم الرقمية التي تتم عبر الشبكة العالمية (الانترنت) تتم عبر ثلاث مراحل[3] :

المرحلة الاولى : تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة (third-party servers) حيث تتبع الحاسبات الخوادم التي دخل المجرم منها ومحاولة ايجاد اي اثر له .

[1] – محمد الامين البشري ،الادلة الجنائية الرقمية مفهومها ودورها في الاثبات ،المجلة العربية للدراسات الامنية و التدريب ،الرياض ،المجلد 17 ،العدد 33 ،2004 م ،ص109 .

[2] – محمد الأمين البشري ،التحقيق في جرائم الحاسوب والإنترنت ، المجلة العربية للدراسات الأمنية والتدريب ، الرياض ، العدد 33 ، سنة 2004 م ،ص243 .

[3] – عبد الناصر محمد محمود فرغلي ؛ د.محمد عبيد سيف المسماري ،مصدر سابق ،ص34 .

المرحلة الثانية : مرحلة المراقبة (prospective surveillance) حيث هناك فرضية بأن المجرم لابد ان يعود او يحوم حول مسرح جريمته ،وتتعدد طرق مراقبة هذه الحواسيب نذكر منها[1]:

- استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع .

- استخدام مايعرف بالحشرات او Bugs وهي اجزاء توضع في الحاسب الالي لمراقبته.

- استخدام كاميرات مراقبة لشاشة الحاسب الالي معدة للاستخدام التجاري وابسط الطرق لمراقبة الحاسب هي الدخول لمكان وجوده وزرع الكاميرات .

- وهناك وسيلة اخرى وهي اصعب قليلا وهي زرع فيروس كمبيوتر او دودة من نوع حصان طروادة وهذه الوسيلة لها ميزة انها تستطيع مراقبة اكثر من جهاز واحد ولكن يجب عدم السماح للفيروس بالانتشار والا سوف يصبح هدفا لبرامج الدفاع ضد الفيروسات .

المرحلة الثالثة : ضبط الاجهزة المشتبه فيها وفحصها فحصا فنيا شرعيا ،حيث يبدأ في هذه المرحلة عمل الخبير المعلوماتي في فحص النظام الحاسوبي المشتبه فيه بمكوناته المادية ومكوناته البرامجية سعيا لإشتقاق الدليل المادي لتقديمة لجهة التحقيق او الحكم ،لتقرير مدى وقوع الجريمة بإستخدام النظام المضبوط من عدمه ولتقرير ادانة المتهم او تاكيد براءته وذلك جميعه وفق الاسس و القواعد الفنية المتعارف عليها والمتبعة في مجال الخبرة المعلوماتية مع مراعاة القواعد القانونية اعلاءاً لمبدأ المشروعية .

كما وضعت وزارة العدل الامريكية ايضا اطارا عمليا يحدد خطوات اساسية عدة لجمع الادلة ثم فحصها ومن ثم تحليلها واخيرا كتابة النتائج في تقرير ،هذا النموذج يتميز بأنه يوضح

[1]– المرجع نفسه ،ص34 .

انواع الادلة والمعلومات المستخلصة منها واماكن وجود هذه المعلومات في الاجهزة وانظمة المعلومات المختلفة ،كما انه يربط كل مجموعة من المعلومات بنوع محدد من جرائم المعلوماتية ،فمثلا يحدد هذا النموذج قائمة بالاماكن المعتادة التي يمكن العثور فيها على الملفات المخفية والملغاة وايضا يحدد أنواع المعلومات الاخرى مثل الصور وكلمات السر وارقام بطاقات الهوية مثل رقم الضمان الاجتماعي وهي معلومات مفيدة في عملية التحري في بعض الانواع من الجرائم المعلوماتية مثل التعدي على الهويات ،ونشر الصور الفاضحة ،فالتعرف على انواع المعلومات المفيدة واماكن اخفائها يعتبر خطوة ايجابية تساعد على تقديم ادلة قانونية يعتد بها عند تقديم الجناة للمحاكمة امام القضاء[1] ،ومن الافضل ان تشكل مراكز اتصال ترتبط بشبكة الانترنت تعمل على مدار اليوم (24 ساعة في اليوم) وتحتوي على عدد كاف من الخبراء والاجهزة لغرض تقديم معلومات عن الوقائع التي تشكل جريمة واتخاذ التدابير الاولية لغرض ضبط الجناة عند طلب ذلك من قاضي التحقيق ويجب التعاون بين مراكز الاتصال في مختلف الدول لغرض اكتشاف اساءة استعمال الاجهزة الالكترونية وتعقب المجرمين وجمع الادلة ذات الصلة ،ومن الجدير بالذكر انه تم في اطار الانتربول تأسيس عدد من فرق الخبراء المعنية بجرائم الانترنت وقد اعدت هذه الفرق دليلا عن كيفية التحقيق في جرائم الانترنت وتقنيات البحث عن الادلة والحصول عليها كما تطور هذه الفرق برمجيات حاسوبية من اجل الكشف عن جرائم معينة[2] .

[1]– عبد الناصر محمد محمود فرغلي ؛ د.محمد عبيد سيف المسماري ،مصدر سابق ،ص35 .

[2]– جمال ابراهيم الحيدري ،الجرائم الالكترونية وسبل معالجتها ،ط1 ،مكتبة السنهوري ،بغداد ،2012م ،ص83 .

الفرع الثاني حجية الدليل الرقمي امام القضاء

القاعدة التي تسود التشريعات الجزائية في الاثبات ان المحكمة تحكم في الدعوى بناء على اقتناعها الذي تكون لديها من الادلة المقدمة في اي دور من ادوار التحقيق او المحاكمة[1] ،لا سلطان عليها في ذلك الا ضمير القضاة ولا تطالب الا ببيان سبب اقتناعها بدليل اخر فهي لا تلزم بإقرار صادر من المتهم او شهادة اثبات أُسندَت الجريمة اليه او شهادة دفاع نفت التهمة عنه او رأي قدمه خبير[2] الا اذا اقتنعت به .

كما أن الأدلة الجزائية التي تستقي منها المحاكمة قناعتها ليست محددة حصرا لكن القانون ذكر بعضها وهي الغالب الشائع وتتمثل في (الاقرار وشهادة الشهود ومحاضر التحقيق والمحاضر والكشوف الرسمية الاخرى وتقارير الخبراء والفنيين)ثم جاء القانون بنص عام ليشمل غيرها من الادلة بقوله :(والقرائن والادلة الاخرى المقررة قانونا)[3] ،وعلى ذلك فإنه يكون للقاضي كامل الحرية في تقدير كافة الادلة المطروحة عليه في الدعوى وله ان يفاضل بين جميع هذه الادلة سواء اكانت تقليدية ام ناتجة عن الاجهزة الالكترونية[4] فيأخذ بما يطمئن اليه من ادلة ويعرض عما لايطمئن اليه من ادلة اخرى.

وعليه فإن للقاضي الجنائي الحرية في تقدير جميع ادلة الدعوى الجزائية بغض النظر عن مصدرها الذي استمدت منه طالما كان مشروعا ويستوي في ذلك الدليل الجنائي التقليدي والدليل الجنائي الرقمي فباب الاثبات مفتوح على مصراعيه امامه وذلك بغاية الوصول الى الحقيقة

---

[1]– حيث نصت المادة (213/أ) من قانون اصول المحاكمات الجزائية على انه : " تحكم المحكمة في الدعوى بناء على اقتناعها الذي تكون لديها من الادلة المقدمة اليها في اي دور من ادوار التحقيق . . . " ؛ ينظر كذلك المواد :المادة (302) من قانون الاجراءات الجنائية المصري رقم (150) لسنة 1950م ،والمادة (275)من قانون الاجراءات الجنائية الليبي لسنة 1953م ،والمادة (212) من قانون الاجراءات الجزائري والمادة (175) من قانون الاجراءات الجنائية السوري لسنة 1954م .

[2]– براء منذر كمال عبد اللطيف ،مصدر سابق ،ص216 .

[3]– المادة (213) من قانون اصول المحاكمات الجزائية العراقي .

[4]– جمال ابراهيم الحيدري ،ضوابط اعتبار المخرجات الالكترونية ادلة إثبات في القضايا الجزائية ،ط1 ،مكتبة السنهوري ،بغداد ،2012 ،ص56 .

،كما يجب ان تكون عقيدة القاضي واقتناعه بالادلة قد استمدت من مخرجات الكترونية طرحت بالجلسة[1] لأن القاعدة هي ان لايحكم الا بناء على التحقيقات التي تحصل بالطرق والشروط القانونية وليس بناء على معلوماته الشخصية او على ما قد يكون رآه بنفسه او حقيقة في غير مجلس القضاء كما ينبغي على الا يؤسس القاضي الجزائي حكمه على دليل ناتج من الحاسب الالي لحقه سبب يبطله ويعدم اثره .

ونلاحظ ان كافة النظم القانونية في الوقت الراهن تكاد تجمع على حجية الملفات المخزنة في النظم ومستخرجات الحاسوب والبيانات المسترجعة من نظم الميكروفيلم والميكروفيش وحجية الملفات ذات المدلول التقني البحت والاقرار بصحة التوقيع الالكتروني وتساويه في الحجة مع التوقيع الفيزيائي والتخلي شيئا فشيئا عن اية قيود تحد من الاثبات في البيئة التقنية لذا اتجهت معظم التشريعات الى قبول الوسائل الالكترونية كبينة في الدعاوى المصرفية ،وتجدر الاشارة هنا الى ان المشكلة لا تزال تكمن في التعاطي الجزئي مع تدابير عصر المعلومات التشريعية وفي مجال جرائم الانترنت ونعتقد من الضروري الاستعانة بالخبرة القضائية للتأكد من سلامة الدليل الرقمي من العبث او الخطأ بالأضافة الى مراقبة القاضي صحة اجراءات جمع الدليل الرقمي .

[1]– وبذلك قضت محكمة استئناف ميسان الاتحادية بصفتها التمييزية بأنه: (للمحكمة ان تستند لتقرير الخبراء المختصين بجرائم الكمبيوتر المتضمن ان المتهم استخدم جهاز الكمبيوتر في تركيب صورة المشتكية على خلفية اختارها من الجهاز المذكور) ،رقم القرار 43/ج/ت/2012 بتاريخ 2012/6/28 ،مجلة التشريع والقضاء ،العدد الرابع ،بغداد ،2012م ،ص274 .

الفصل الثاني
القواعد الاجرائية
في استخلاص الدليل الالكتروني والقيمة القانونية له

إن طبيعة الجرائم الإلكترونية بعناصرها ووسائل ارتكابها، قد تدفع المشرع الجزائي إلى إعادة النظر في كثير من المسائل الجزائية، خاصة فيما يتعلق بمسألة الإثبات، ذلك أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لا بد أن يكون من طبيعة إلكترونية، وهو الأمر الذي يقودنا إلى الحديث عن مسألة قبول هذا الدليل أمام القضاء ومدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف والأخطاء ، وكذا مصداقيته ومشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي إعمالا لمبدأ السلطة التقديرية للقاضي الجزائي الذي يشكل جوهر أي حكم، وعليه قسمنا هذا الفصل إلى مبحثين، المبحث الأول تحت عنوان القيمة القانونية للدليل الالكتروني في مجال الإثبات الجنائي، أما المبحث الثاني فيتمثل في القواعد الإجرائية في استخلاص الدليل الإلكتروني.

المبحث الأول: القواعد الإجرائية في استخلاص الدليل الإلكتروني

إن التطور التقني الذي لحق نظام المعالجة الآلية فضلا عن الطبيعة الخاصة للدليل الرقمي سيؤدي حتما إلى تغيير كثير من المفاهيم السائدة حول إجراءات وطرق الحصول عليها، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية، فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع طبيعة البيئة التقنية، فتطور الإثبات ووسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، وهو الأمر الذي سوف نعالجه من حيث بحث القواعد الإجرائية التقليدية، وإلى أي مدى يمكن الاستناد إليها في الحصول على الدليل الرقمي في المطلب الأول، ثم نعرج إلى القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني وصعوبات التحقيق في الجريمة الإلكترونية في المطلب الثاني.

المطلب الأول : القواعد الإجرائية التقليدية في استخلاص الدليل الالكتروني

مما لاشك فيه أن المشرع لم يجز استخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معينة أهمها التفتيش وضبط الأشياء والخبرة، إن هذه القواعد عامة النطاق تنظم استخلاص الدليل في جميع الجرائم، تقليدية كانت أو مستحدثة إلا أنها في الثانية قد تكون بحاجة إلى تطوير لكي تتناسب مع خصوصيتها وطبيعة الدليل الذي يصلح لإثبات الجريمة الإلكترونية[1].

[1]– بلعليات إبراهيم ، المرجع السابق ، ص214.

الفرع الأول: التفتيش

يمكن تعريف التفتيش بصفة عامة أنه : ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي، ولا يمكن أن يقوم به سوى النيابة العامة و قاضي التحقيق، عن طريق أمر ندب أحد مأموري الضبط القضائي المختص بإجرائه، والغرض منه هو البحث عن أدلة الإثبات للجريمة المرتكبة، وكل ما يفيد للوصول إلى الحقيقة في متابعة أي شخص يشتبه أنه مرتكب الجريمة.

2.2- التفتيش التفتيش هو إجراء من إجراءات التحقيق يهدف للبحث

أدلة مادية الجناية أو جنحة تحقق وقوعها في عن محل يتمتع بحرمة، وفقا للضمانات والقيود المقررة قانونا والتفتيش في الجرائم المعلوماتية يحتاج إلى تقنيات خاصة، لسهولة إخفاء المعطيات وصعوبة تحديد مكانها و الذي من الممكن أن يكون خارج مسرح الجريمة تماما او خارج حدود الدولة كليا، لذلك يجب أن نميز بين التفتيش الذي يقع على المكونات المادية والتفتيش الذي يقع على المكونات المنطقية أو كما تسمى المعنوية. ففي الحالة الأولى التي يقع فيها التفتيش على المكونات المادية الأنظمة المعالجة الآلية للمعطيات فإن الإشكال لا يطرح، لأنه يخضع للقواعد العامة للتفتيش، إلا أنه يجب مراعاة مكان تواجد هذه المعدات، فإذا كانت في مكان خاص فإن صحة الإجراء تقتضي الالتزام بالشروط المنصوص عليها في المادتين 46 و 47 من قانون الإجراءات الجزائية وهي الحصول على الموافقة الكتابية لصاحب المسكن، فضلا عن حضوره هو أو من يمثله مع مراعاة المواعيد الخاصة بالتفتيش، في حين يخضع التفتيش إذا كان محله في مكان عام للقواعد الإجرائية الخاصة بتفتيش الأشخاص، وعليه فإنه لا يوجد أي مانع قانوني لفحص وتفتيش المكونات المادية لأنظمة المعالجة الآلية للمعطيات باعتبارها أشياء استنادا لنص المادة 44 من قانون الإجراءات الجزائية.

أما الحالة الثانية والتي تتعلق بتفتيش المكونات المنطقية لنظام المعالجة الآلية، فقد ثار خلاف حول مدى صلاحيتها لأن تكون موضوعا للتفتيش، فيرى جانب من الفقه بأن التفتيش يقع على المكونات ذات الطبيعة المادية وليس على البيانات التي ليس لها مظهر مادي محسوس في حين يرى جانب آخر أن أحكام الاجراءات الجزائية الخاصة بالتفتيش يمكن أن تتناسب مع المكونات المعنوية، باعتبارها قابلة للضبط والتخزين في وسائط مادية أو طبعها على دعائم ورقية وهو نفس اتجاه المشرع الجزائري الذي أجاز صراحة بموجب نص المادة الخامسة من القانون 09-04 للسلطات القضائية المختصة وكذا ضب باط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 منه، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، كما أجاز التفتيش عندما يتعلق الأمر بمنظومة تخزين معلوماتية. ونظرا لخطورة التفتيش باعتباره إجراء يمس بالدرجة الأولى بحقوق الأفراد وحرياتهم، وجب على المشرع إحاطته بضوابط تشكل في حقيقتها ضمانات لتكريس التوازن بين حماية المجتمع من جهة وعدم المساس بحقوق الافراد وحرياتهم من جهة أخرى، من بينها ضرورة الحصول على إذن مكتوب بالتفتيش استنادا لنصوص المواد ،44، 64 و 68 من قانون

أولا: القواعد الموضوعية لتفتيش أنظمة الحاسوب

وتلخص هذه القواعد كالآتي[1]:

- وقوع جريمة إلكترونية.

[1]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي 2006. ص .385.386.

– ارتكاب شخص أو أشخاص معينين لإحدى الجرائم الإلكترونية أو الاشتراك فيها. – توافر أدلة قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية أو إلكترونية تفيد في كشف الحقيقة.

– أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.

ثانيا: القواعد الشكلية لتفتيش نظام الحاسوب

وتتضمن عدة قواعد نذكرها كما يلي[1]:

– أن يتم بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة.

– أن يكون أمر التفتيش مسببا.

– تكوين فريق تفتيش يتضمن خبراء وفنيين متخصصين بالحاسوب والأنظمة الإلكترونية بالإضافة إلى رجال الشرطة المتخصصين بالحماية و الأمن.

الفرع الثاني: استخلاص الدليل في الجريمة الإلكترونية

الضبط والاستخلاص هو العثور على أدلة إثبات الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها، والضبط هو الغاية من التفتيش ونتيجته المباشرة، ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تطبق على التفتيش[2].

الضبط يعني أيضا وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبيها ، والهدف الذي تسعى إليه سلطة التحقيق من أجل القيام بالتفتيش، وهو

[1]– خالد عياد الحلبي، المرجع السابق، ص154،155.

[2]– مصطفى محمود موسى ، المرجع السابق ، ص208

ضبط الأدلة و الوثائق والأشياء التي تفيد في الكشف عن الجريمة، لذلك ينبغي التقيد بالقواعد الإجرائية التي تحدد الأماكن التي يجوز تفتيشها والأشخاص الذين يجري تفتيشهم[1].

أولا: مدى صلاحية الضبط في الجريمة الإلكترونية

محل الضبط يكون بطبيعته وبحسب تنظيمه القانوني وغايته، لا يرد إلا على الأشياء أما الأشخاص فلا يصلحون ليكونوا محلا للضبط بالمعنى الدقيق إلا في حدود الاستثناءات الإجرائية، وإذا كانت بعض القوانين تتحدث عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماما عن ضبط الأشياء، نظرا لكون الضبط محلا في مجال الجريمة الإلكترونية، والبيانات المعالجة الكترونيا فقد ثار التساؤل هل يصلح هذا النوع من البيانات أن يكون محلا للضبط وهو وضع اليد على شيء مادي ملموس؟[2].

انقسم الفقه إلى اتجاهين يرى البعض أن بيانات الحاسوب لا تصلح أن تكون محلا للضبط لانتفاء الكيان المادي عنها ولا سبيل لضبطها، إلا بعد نقلها على كيان مادي ملموس ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة، ويرى اتجاه ثاني أن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات الكترونية أو موجات كهرومغناطيسية قابل للتسجيل والحفظ والتخزين على وسائط مادية وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها ، فوجودها المادي لا يمكن إنكاره[3].

ثانيا: الأشياء محل الضبط في الجريمة الإلكترونية

الأشياء التي يتم ضبطها في مجال الجرائم الإلكترونية والتي لها قيمة في الإثبات هي:

- ضبط جهاز الحاسوب وملحقاته.

[1]- خالد عياد الحلبي، المرجع السابق، ص 168

[2]- عبد الفتاح بيومي حجازي، المرجع السابق، ص396

[3]- سعيداني نعيم، المرجع السابق، ص159.

أولا: القواعد الموضوعية لتفتيش أنظمة الحاسوب

وتلخص هذه القواعد كالآتي: [1]

– وقوع جريمة إلكترونية.

– ارتكاب شخص أو أشخاص معينين لإحدى الجرائم الإلكترونية أو الاشتراك فيها. – توافر أدلة قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية أو إلكترونية تفيد في كشف الحقيقة.

– أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.

ثانيا: القواعد الشكلية لتفتيش نظام الحاسوب

وتتضمن عدة قواعد نذكرها كما يلي:2

– أن يتم بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة.

– أن يكون أمر التفتيش مسببا.

– تكوين فريق تفتيش يتضمن خبراء وفنيين متخصصين بالحاسوب والأنظمة الإلكترونية بالإضافة إلى رجال الشرطة المتخصصين بالحماية و الأمن.

الفرع الثاني: استخلاص الدليل في الجريمة الإلكترونية

الضبط والاستخلاص هو العثور على أدلة إثبات الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها، والضبط هو الغاية من التفتيش ونتيجته المباشرة، ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تطبق على التفتيش[2]

[1]– عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي 2006. ص385

[2]– خالد عياد الحلبي، المرجع السابق، ص154،155.

– ضبط المعدات المستعملة في شبكة الانترنت

ضبط وسائط التخزين المتحركة كالأقراص المدمجة، والأقراص المرنة، والأشرطة المغناطيسية.

– ضبط البرمجيات

– ضبط البريد الإلكتروني والذي قد يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية.

ثالثا : الصعوبات التي تواجه عملية الضبط

عملية ضبط البيانات المعالجة إلكترونيا تواجهها عدة صعوبات منها[1] :

– حجم الشبكة التي تحتوي على المعلومات المعالجة الكترونيا والمطلوب ضبطها.

– وجود بيانات في شبكات أو أجهزة تابعة لدولة أجنبية.

– يشمل التفتيش و الضبط أحيانا اعتداء على حقوق الغير، أو على حرمة حياتهم الخاصة، فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات.

الفرع الثالث : الخبرة في إثبات الجريمة الإلكترونية

تعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجا إليه القضاء وسلطات التحقيق على حد سواء ، وذلك كل ما استعصى عليهم الأمر ، ومن بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد الجريمة الإلكترونية، حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الإلكترونيات[2].

أولا: أنواع الخبراء الإلكترونيون.

[1]– خالد عياد الحلبي، المرجع السابق، ص 172

[2]– صغير يوسف، الجريمة المرتكبة عبر الانترنت رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، كلية الحقوق والعلوم السياسية ، 2013، ص 87.

الخبير في الجريمة الإلكترونية : هو الفني المتخصص وصاحب الخبرة في التقنية الإلكترونية وشبكاتها، والذي يكون قد رأى أو سمع أو أدرك بحواسه معلومات هامة لازمة للدخول في نضام المعالجة الآلية الرقمية للبيانات، إذا كانت مصلحة التحقيق تقتضي البحث عن الدليل الرقمي الإلكتروني داخله ويتمثل الخبراء الإلكترونيون في مايلي[1]:

- المبرمجون.
- المحلل هو الشخص الذي يضع خطوات العمل ويقوم بتجميع بيانات نظام معين.
- مهندس الصيانة والاتصالات.
- مشغل الحاسوب الآلي وشبكاته.
- مدير النظام المعلوماتي.

ثانيا: أهمية الخبرة في البحث عن الدليل الإلكتروني

تكمن أهمية الخبرة في الأدلة التي تقدمها لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية، لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة في المواد 143 الى 156 من قانون الإجراءات الجزائية، واعتبرها من إجراءات البحث عن الدليل حيث نصت المادة 143 على أنه لجهات التحقيق أو الحكم عندما تعرض لها مسالة ذات طابع فنّي أن تأمر بندب خبير إما من تلقاء نفسها أو بناء على طلب من النيابة العامة وإما بطلب من الخصوم[2].

وتكمن أهمية الخبرة في مجال البحث عن الدليل الإلكتروني في أنها وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل، أو تحديد مدلولها بالاستعانة بالمعلومات العلمية

[1]– مصطفى محمود موسى، المرجع السابق، ص172

[2]– قانون رقم 155/66 مؤرخ في 08 يونيو 1966 المعدل و المتمم لقانون الإجراءات الجزائية، الجريدة الرسمية العدد 48، المعدل و المتمم للأمر رقم 2015 مؤرخ في 23 جويلية 2015، الجريدة الرسمية العدد 40 ، و المعدل و المتمم بالأمر

وهي البحث في مسائل مادية أو فنّية يصعب على المحقق أن يبحث فيها، ويعجز عن جمع الأدلة بالوسائل الأخرى للإثبات[1].

تبرز أهمية الاستعانة بالخبرة في مجال الجرائم الإلكترونية، في أنه عند غيبها تعجز الضبطية القضائية في كشف غموض الجريمة لنقص الكفاءة و التخصص اللازمين للتعامل مع الجوانب التقنية و التكنولوجية التي ارتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل والإهمال عند التعامل معه[2].

ولعل هذه الأهمية للخبرة في مجال التحقيق في الجريمة الإلكترونية جعل بعض التشريعات لا تكتف بالنصوص التقليدية التي تنظم الخبرة، وعمدت إلى إدراج نصوص قانونية خاصة تنظم الخبرة في هذا المجال، ونجد أن المشرع الجزائري أشار في المادة 05 الفقرة الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه : "يمكن للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

[1]- صغير يوسف، المرجع السابق، ص 89

[2]- مصطفى محمود موسى، المرجع السابق، ص222

المطلب الثاني: القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني وصعوبات التحقيق في الجريمة الإلكترونية

كان لتطور أساليب ارتكاب الجريمة الإلكترونية منحى تصاعدي بين الجرائم المرتكبة في الجزائر، أي فرض على المشرع الاعتماد على قواعد إجرائية خاصة في سبيل مكافحة الجريمة الإلكترونية وهو ما جاء به القانون 06-22 المؤرخ في ديسمبر 2006 المعدل والمتمم للأمر رقم 155/66 المؤرخ في 08 يوليو 1966 والمتضمن لقانون الإجراءات الجزائية.

الفرع الأول: القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني

نص المشرع الجزئري على إجراءات خاصة تهدف إلى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم الأخرى، وتتمثل هذه الإجراءات في التسرب واعتراض المراسلات وكذلك من خلال القانون 09-2004 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها استحداث إجراءين آخرين هما المراقبة الإلكترونية وحفظ المعطيات [1].

أولا: التسرب (الاختراق) واعتراض المراسلات.

تعتبر الجريمة الإلكترونية من بين الجرائم التي يمكن اللجوء فيها إلى إجراء التسرب واعتراض المراسلات إذا اقتضت ذلك ضرورات التحري والتحقيق بشأنها.

1- التسرب (الاختراق)

نضم المشرع الجزائري أحكام التسرب في الفصل الخامس من قانون الإجراءات الجزائية من المادة 65 مكرر 11 إلى مكرر 18 ، حيث بين كيفية القيام بعملية التسرب وكذا شروط

[1]- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر ، باتنة، كلية الحقوق والعلوم السياسية قسم الحقوق ، 2011-2012، ص 106.

القيام بهذا الإجراء، وكذلك الأحكام الجزائية لمن تسبب في الكشف عن هوية الضابط أو العون المتسرب، ويتم الاستماع إلى الضابط المتسرب بوصفه شاهدا عن الجرائم المرتكبة بعد انتهاء المهلة المحددة في رخصة التسرب.

أ – مفهوم التسرب :

المقصود بالتسرب هو قيام ضابط أو عون الشرطة القضائية بمراقبة الاشخاص المشتبه في أنهم ارتكبوا الجريمة بإظهار أنه مساهم معهم أو شريك، بحيث يستعمل الضابط أو العون هوية مستعارة وذلك إذا ما ارتبط البحث والتحري واحدة من الجرائم التالية:

- جرائم المخدرات.
- الجريمة المنظمة العابرة للحدود الوطنية.
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- جرائم تبييض الأموال.

القواعد الإجرائية في استخلاص الدليل الالكتروني و القيمة القانونية له

الجرائم الموصوفة بأفعال إرهابية أو تخريبية.

الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد[1].

ب– طرق التسرب في مجال الجريمة المعلوماتية:

يمكن تصور عملية التسرب في نطاق الجرائم الإلكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي، وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها أو اشتراكه في محادثات في غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم،

[1]– المادة 65 مكرر 12 من قانون الإجراءات الجزائية، المرجع السابق.

والظهور بمظهر كما لو كان فاعلا مثلهم ، مستخدما في ذلك أسماء أو صفات هيئات مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام المخترق للمواقع ، أو كيفية ارتكاب الجرائم وحتى المشاركة معهم في ارتكابها لتجميع كل ما يمكن جمعه من الأدلة[1].

2- اعتراض المراسلات السلكية واللاسلكية

أ - مفهوم اعتراض المراسلات

استحدث بموجب المادة 65 مكرر إلى 65 مكرر 10 من قانون الإجراءات الجزائية، إمكانية قاضي التحقيق أن يأمر ضابط الشرطة القضائية بترخيص كتابي وتحت إشرافه مباشرة للقيام باعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية ، ووضع الترتيبات التقنية دون موافقة الشخص المعني من اجل القيام بالتقاط وتثبيت وتسجيل وبحث فيسرية وفي أي مكان عام أو خاص والتقاط الصور لأي شخص.

إن مقتضيات المادة ليست مطلقة بل ترد عليها بعض الاستثناءات عن طريق تشريع قواعد إجرائية، تنص على تقييد هذه الحرية من أجل الحفاظ على المصلحة العامة للمجتمع وأمنه وسلامته، وهذا لحسن سير التحريات والتحقيقات القضائية، بحيث منح حق اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع ترتيبات تقنية دون مراقبة المعنيين من أجل التقاط الصور وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن عامة أو خاصة[2].

في المادة 619 من القانون 00-03 المؤرخ في 05 سبتمبر 2000 المحدد للقواعد شكل العامة المتعلقة بالبريد والمواصلات، اعتبر أن مادة المواصلات هي كل اتصال مجسد في

[1]- سعيداني نعيم، المرجع السابق، ص177,

[2]- قادري ، سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماجستير ، جامعة قاصدي مرباح ، ورقلة ، كلية الحقوق والعلوم السياسية ، قسم الحقوق، 2013 - 2014، ص .27

كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، ولا تعتبر الكتب والجرائد والمجلات واليوميات كمادة مراسلات[1].

إلا أنه بالرجوع إلى نص المادة 39 من الدستور الجزائري التي تنص على أن سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، ولذلك نصت المدة 303 [2] من قانون العقوبات التي تعاقب كل من يفضح أو يتلف رسائل أو مراسلات موجهة للغير، إذا يمكن التوصل للقول بان المراسلات الخاصة تعني كل رسالة مكتوبة بأي شكل من الأشكال سواء مادية أو إلكترونية وسواء كانت على دعامة ورقية أو رقمية مرسلة بأي وسيلة لعدد معين ومحدد من المرسل إلى المرسل إليهم، باستثناء الكتب والمجلات والجرائد والدوريات التي لا تعتبر مراسلات خاصة.

وهذا ما جاء به القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في المادة 2 الفقرة "و" في تعريفه للاتصالات الإلكترونية: على أنها تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور او أصوات أو معلومات مختلفة بأي وسيلة كانت.

وتجدر الإشارة في هذا الصدد إلى أن المراسلات التي يمكن اعتراضها يجب أن تتسم بالخصوصية ولكي تكون كذلك يلزم أن يتوافر فيها عنصران أساسيان هما[3]:

عنصر موضوعي يتعلق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسري.

---

[1]- قانون رقم 00-03 مؤرخ في 5 غشت 2000 المحدد للقواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، الجريدة الرسمية العدد 48 ، بتاريخ 6 غشت 2000.

[2]- القانون رقم 16-01 ، مؤرخ في 6 مارس 2016 المتضمن الدستور الجزائري، الجريدة الرسمية العدد 63، بتاريخ مارس.2016

[3]- سعيداني نعيم ، المرجع السابق، ص179

– عنصر شخصي والمراد به إرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون الرسالة.

وعند توفر هذان العنصران في الرسالة فإنها تتصف بالمراسلة الخاصة التي لها خصوصيتها وسريتها المحمية قانونا ولا أهمية لشكل الرسالة أو طريق نقلها وتوصيلها إلى المرسل إليه.

لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي

ب – طرق اعتراض المراسلات الإلكترونية

يعتبر البريد الإلكتروني أهم وسيلة تقنية في مجال التراسل الالكتروني ومن ثمة فعملية الاعتراض تنصب عليه، ومن المعلوم أن كل رسالة إلكترونية تظهر فيها معلومات عامة مثل تاريخ إنشاء الرسالة وتاريخ تلقيها وكذا عنوان المرسل وعنوان المرسل إليه، وهذه المعلومات ليست كافية لمعرفة المرسل إذ بإمكان هذا الأخير إرسال رسائله من صناديق بريد مسجلة بأسماء وهمية، كما أن هناك وسائل تتيح للمرسل أن يرسل رسائله دون أن يظهر فيها عنوان

بريده الإلكتروني الصحيح، لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية رسائل البريد الالكتروني والتي يطلق عليها مصطلح Email Heade والمعلومات التي تحتويها الحاشية هي عبارة عن معلومات تراكمية لمختلف الأجهزة الخادمة للبريد الإلكتروني التي مرت من خلالها الرسالة، ونجد أن حاشية المعلومات تتضمن أرقام IP[1]

[1]– IP Imail Header: صفحة تحتوي على عنوان IP لشركة البريد الالكتروني وعنوان IP الخاص ببريد الشخص مرسل الرسالة.

مختلفة تمثل أرقام خاصة بكل الأجهزة التي مرت بها الرسالة وعادة ما يظهر[1] رقم IP الخاص بمرسل الرسالة أمام عبارة x originating IP ، وفي حالة عدم ظهور هذه العبارة فإن رقم[2].

الخاص لمرسل الرسالة يكون أمام آخر كلمة received [3].، وتعد هذه المعلومات أساسية يمكن من خلالها الاستدلال على صاحب الرسالة ويصبح بعد ذلك من السهل الحصول على المزيد من المعلومات عن المرسل، وذلك بإدخال رقم IP في بعض المواقع أو البرامج التي تقوم بالكشف عن مصدر الرسالة والمكان الجغرافي التي أرسلت منه ، وكذلك مزود الخدمة الذي يتعامل معه المرسل وبذلك يكون من السهل اعتراض المراسلات والإطلاع على محتواها دون علم مرسلها[4].

ثانيا : المراقبة الإلكترونية وحفظ المعطيات

سوف نتناول بالشرح إجراءات المراقبة الإلكترونية فقط على اعتبار انه سبق الحديث عن حفظ المعطيات.

1- مفهوم الرقابة الإلكترونية للاتصالات

استحدث المشرع الجزائري إجراءات المراقبة الإلكترونية بموجب المادة 03 من القانون 04-09 الصادر بتاريخ 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حينما أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إظهار هذا النوع من الجرائم اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها، غير أن المشرع الجزائري لم يتطرق

---

[1]- IP هو عبارة عن رقم يمثل عنوان جهاز الحاسوب على الانترنت ويكون بهذا الشكل 192.168.1.1. وهو اختصار لكلمة

Protocol Internet

[2]- x originating IP صحة تحتوي على عناوين IP شركة البريد و IP الشخص مرسل الرسالة في شركة هوتمايل

[3]- Received صحة تحتوي على عناوين IP شركة البريد و IP الشخص مرسل الرسالة في شركة ياهو

[4]- سعيداني نعيم، المرجع السابق، ص 181 ، 182.

إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية واكتفى بتحديد مفهوم الاتصالات الإلكترونية وذلك في الفقرة "و "من المادة الأولى من نفس القانون[1].

من الواضح أن المشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الإلكتروني فقط بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية، فإلى جانب القيام بإجراءات مراقبة الاتصالات الإلكترونية فإنه يمكن كذلك تطوير هذه التقنية، لكي تعمل في بيئة الرقابة لغرض الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة وهو ما أقرته المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

2- شروط المراقبة التقنية للاتصالات

اعتبر المشرع الجزائري المراقبة التقنية للاتصالات وسيلة إجرائية للحصول على الدليل في مجال الجريمة الإلكترونية بمجموعة من الشروط أهمها[2] :

- أن يتم تنفيذ هذا الإجراء تحت سلطة القضاء وبإذن منه، وهو ما أكدته المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بنصها على أنه : " لا يجوز إجراء عملية المراقبة إلا بإذن من السلطة القضائية المختصة".

- أن تكون هناك ضرورة تتطلب هذا الإجراء، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء الى المراقبة الإلكترونية، وهو ما

[1]- المادة 03 من القانون 09-04 : " مع مراعات الاحكام القانونية التي تضمن سرية المراسلات والاتصالات. يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات او التحقيقات القضائية الجارية ، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون ، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية

[2]- سعيداني نعيم ، المرجع السابق ، ص.185

أكد عليه المشرع في المادة 4 الفقرة "ج" من القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الفرع الثاني: معوقات و صعوبات التحقيق في الجريمة الإلكترونية

يتسم التحقيق في الجريمة الإلكترونية بالعديد من المعوقات والصعوبات التي تؤثر على عملية التحقيق التي تؤدي بها إلى الخروج بنتائج تنعكس على نفسية المحقق، بفقدانه الثقة في نفسه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضا على المجرم نفسه، حيث يشعر أن الجهات القضائية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق، لا تجاري خبرته وعلمه الأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من الجرائم التي قد تكون أكثر فداحة وأشد ضررا على المجتمع.

أولا: المعوقات المتعلقة بجهات التحقيق

توجد معوقات للتحقيق في الجريمة الإلكترونية تتعلق بالسلطة القائمة بالتحقيق وتجمع لعدة أسباب نذكرها كالآتي:

1- قلة خبرة القائمين بالتحقيق في هذه الجرائم

لقلة المهارات الفنية المطلوبة للتحقيق في هذا النوع من الجرائم ونقص المهارات في استخدام جهاز الحاسوب والانترنت، وعدم توافر المعرفة بأساليب ارتكاب الجرائم الإلكترونية، وقلة الخبرة في مجال التحقيق في جرائم الحاسوب والانترنت وقلة المعرفة باللغة الأجنبية لا سيما أن للعاملين في مجال الحاسوب مصطلحات عملية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم بينهم، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات [1].

[1]- خالد ممدوح ابراهيم، المرجع السابق، ص 69.

2 – الصعوبات التقنية لاستخدام بروتوكول TCP/IP في الإثبات وهي [1]:

هناك تحديات عند استخدام المحقق بروتوكول TCP/IP 2 كدليل الكتروني للإثبات ذلك بروتوكول IP وحدة معلوماتية تحتوي على معلومات عن الحاسوب وليس عن الأشخاص، لذلك فمن الصعوبة إثبات أن شخصا محددا أحدث الفعل غير المشروع، ومع يمكن أن يستخدم كقرينة قضائية ضد مالك الجهاز إلى أن يثبت العكس.

– الجاني يعمد إلى استخدام عناوين ومعلومات غير صحيحة أو غير قانونية باستخدام حاسوبه الشخصي في ملف خدمات عامة لتجنب التعرف عليه، ويستخدم عنوان IP له مستخدمين كثر ويمكنهم استخدام نفس العنوان، وبعد مرور فترة زمنية يقوم بغلق الاتصال، وبعد فترة يعاود الاتصال مما يجعل النشاط الإجرامي غالبا مزعا على عدة عناوين[2].

تكون المعلومات المحملة لمصدر عنوان IP غير حقيقية أو زائفة وهذا ممكن باستخدام مصدر زائف لمصدر عنوان IP بحيث يظهر بأن المعلومات جاءت من حاسوب محدد وفي الحقيقة جاءت من حاسوب آخر.

3– ارتفاع تكاليف جمع الأدلة

إن التحقيق في هذه الجرائم يحتاج إلى خبراء متخصصين وهؤلاء يحتاجون إلى دورات مستمرة متزامنة مع تطور التقنية الإلكترونية، وهذا الأمر مرتبط بتكاليف باهظة، وكذلك التفتيش الأدلة يحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات شيئا.

[1]– هو اختصار لكلمة Transmission Control Protocol بروتوكول التحكم في نقل البيلنات وكلمة Internet protocol بروتوكول TCP/IP هو العصب المحرك للانترنت يضم مجموعة بروتوكولات مطورة كطريق للتواصل بين مختلف أنواع الحواسيب.

[2]– خالد عياد الحلبي ، المرجع السابق، ص 226.

ثانيا: عوائق تتعلق بالجريمة والجهة المتضررة منها

المعوقات المتعلقة بالجريمة الإلكترونية تتمثل في[1]:

- خفاء الجريمة وغياب الدليل المرئي وصعوبة التعرف عليه.
- الإعاقات المتعلق بالوصول إلى الدليل الإحاطته بوسائل الحماية الفنية.
- سهولة محو الدليل أو تدميره في زمن قصير جدا.

الجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها ، وفي هذه الحالة التي قد تعمل بها فإنه يستهدف بالمحو السريع عدم استطاعة السلطات إقامة الدليل ضده، وبالتالي تملصه من مسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسوب الآلي أو الشبكة أو في الأجهزة. أما المعوقات المتعلقة بالجهات المتضررة من جرائم الحاسوب والانترنت، وهي عدم إدراك خطورة جرائم الحاسوب والانترنت من قبل المسئولين بالمؤسسات المجني عليها التي تعد من معوقات التحقيق، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالانترنت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، وهذا يؤدي إلى الإحجام عن الإبلاغ عن الجريمة، التي تعتبر من أهم وأخطر الإشكالات التي تتعلق بعملية الإبلاغ عن الجريمة الإلكترونية، حيث يحـ البعض عن إبلاغ السلطات المختصة بالجرائم التي ارتكبت بحقهم خاصة إذا تعلق الأمر بالمؤسسات المالية أو ما شابهها[2].

[1]– خالد ممنوح ابراهيم ، المرجع السابق ،ص65

[2]– خالد عياد الحلبي، المرجع السابق، ص223، 224.

المبحث الثاني : القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي

لقد أثارت مسألة الدليل الرقمي الكثير من التساؤلات حول تعبيره أو عدم تعبيره عن الحقيقة، نظرا لما يمكن أن تخضع له طرق الحصول عليه من التزييف والتحريف والعبث، وهو ما يثير مسألة مشروعية الأخذ به، إذ يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا من حيث وجوده ومن حيث الحصول عليه.

إن مجرد وجود دليل يثبت وقوع الجريمة ونسبيتها إلى شخص معين لا يكفي أن يكون دليل إثبات، إذ يجب أن تكون لهذه الأدلة قيمة قانونية وقيمة الدليل الجنائي تتوقف على مسألتين رئيسيتين الأولى مشروعية الدليل والثانية هي حجية الدليل على المراد إثباته.

المطلب الأول : مشروعية الدليل الإلكتروني

تعرف المشروعية بأنها التوافق والتقيد بأحكام القانون في إطاره ومضمونها العام، فهي تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حريتهم وحقوقهم الشخصية ضد تعسف السلطة ومن التطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته[1].

لذلك فإنه لصحة الإجراءات التي تقوم بها جهة التحقيق أن لا تخل بمبدأ المشروعية من أجل أن الحصول على دليل صحيح وسليم يستند عليه القضاء في أحكامه والحقيقة أن مشروعية الدليل الإلكتروني هي مشروعية الوجود ومشروعية الحصول.

مشروعية الدليل الالكتروني ان مبدأ الاقتناع الشخصي للقاضي الجزائي مفاده ان القاضي لا يقيد بأدلة معينة ، لكن إذا كان القانون يترك للقاضي الجزائي الحرية في أن يستمد اقتناعه من أي دليل وبأية وسيلة يراها موصلة للحقيقة، فهذا لا يعني انه يمكن للقاضي أن يبني عقيدته على أي دليل يقدم له مهما كان مصدره ووسيلة البحث عنه، لأن الخصومة الجزائية تقوم على ضمان حرية المتهم لا على مجرد إثبات سلطة الدولة في العقاب، ومن ثم يتعين على القاضي ألا يثبت توافر هذه السلطة اتجاه المتهم إلا من خلال دليل مستمد من إجراءات مشروعة احترمت فيها الحريات وأمنت فيها الضمانات التي رسمها القانون وهذا ما يسمى بمشروعية الدليل.

تتمثل مشروعية الدليل الالكتروني في نقطتين قانونيتين هما مشروعية وجود الدليل أي ان يكون الدليل معترفا به ، بمعنى أن يجيز القانون للقاضي الاستناد اليه لتكوين عقيدته للحكم

[1]– هلال عبد الله محمد حجية مخرجات الكمبيوتر في المواد الجنائية، الطبعة الثانية، دار النهضة العربية ، مصر، 2008 ص 104.

بالادانة . ويمكن القول ان النظم القانونية تختلف في موقفها من الادلة التي تقبل كأساس للحكم بالادانة بحسب الاتجاه الذي تتبناه

فالنظم التي تتبنى نظام الاثبات القانوني أي النظام الذي حدد المشرع فيه حصرا الادلة التي يجوز للقاضي اللجوء اليها في الاثبات كما حدد القيمة الاقناعية لكل دليل بحيث يقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون ، فلا سبيل للاستناد الى اي دليل اذا لم ينص القانون عليه صراحة ضمن ادلة الاثبات كما انه لا دور للقاضي في تقدير القيمة الاقناعية للدليل، وهذا النظام ينتمي للنظم الانجلوسكسونية كالمملكة المتحدة والولايات المتحدة الامريكية فالنظم التي تتبنى هذا النظام لا يمكن في ظلها الاعتراف للدليل الالكتروني بأية قيمة اثباتية مالم ينص عليه القانون صراحة ضمن ادلة الاثبات، ومن ثم فأن خلو القانون من النص عليه سيهدر قيمته الاثباتية مهما توافرت فيه شروط اليقين لانه لا يجوز للقاضي أن يستند اليه لتكوين عقيدته، وتطبيقا لهذا فقد نص قانون الاثبات في المواد الجنائية البريطانية على قبول الدليل الرقمي وحدد قيمته الاثباتية اتفاقا . يعاب على نظام الاثبات القانوني أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع ، فيحكم في كثير من الاحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في اطاعته لنصوص القانون ، ولذلك فان هذا النظام بدأ ينحسر

الفرع الأول: مشروعية وجود الدليل الإلكتروني

تقتضي مشروعية وجود الدليل الإلكتروني أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثبات الجنائي.

يقصد بمشروعية الوجود أن يكون الدليل معترفا به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه والاستدلال به لتكوين عقيدته وقناعته للحكم بالإدانة أو البراءة، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الإلكترونية، تتمثل في طبيعة نظام الإثبات السائد في الدولة إذ يختلف النظام القانوني في

موقفها من حيث الأدلة التي يمكن قبولها في الإثبات، وهناك اتجاهان رئيسيان الاتجاه الأول هو نظام الأدلة القانونية، أما الاتجاه الثاني فهو نظام الإثبات الحر.

أولا: أنظمة الإثبات المقيد

في ظل نظام الإثبات المقيد فإن الدليل الرقمي لا يكون مقبولا أمام القضاء ما لم ينص عليه القانون حيث يتوجب عليه تحديد هذا النوع من الأدلة سلفا وبدقة، ويتوجب على القاضي الجنائي أن يأخذ بهذه الأدلة متى توفرت فيها شروط الدليل الصحيح، وقد نظمت العديد من التشريعات التي تأخذ بها النظام هذه الأدلة " الأدلة الالكتروني " وحددتها بدقة

ولقد حدد المشرع الانجليزي بالدليل الرقمي كدليل في الإثبات الجنائي و ذلك خروجا عن الأصل العام في عدم قبول الشهادة السماعية و ضرورة تقديم الأصل لإثبات المحتوى حيث تعاقبت القوانين التي سمحت بذلك منذ قانون الإثبات الجنائي لسنة 1968 و حتى القانون الصادر في 1988 الخاص بالعدالة الجنائية و قانون الشرطة و الإثبات الجنائي سنة 1984 ، إلا أن هذا القبول مقيد بشروط نصت عليها المادة (69) من قانون الشرطة و الإثبات الجنائي لسنة 1984 تمثلت في[1]:

1-أن جهاز الكمبيوتر يعمل بصورة سليمة في جميع الأحوال.

2- غياب أية أسباب معقولة للاعتقاد بأن الدليل يفتقر إلى الدقة بسبب الاستخدام غير المناسب أو الخاطئ لجهاز الكمبيوتر.

3-الوفاء بأية شروط متعلقة بالمستند محددة طبقا لقواعد المحاكمة.

و يتضح جليا أن صحة الدليل الرقمي تتوقف على صحة برنامج التشغيل الذي وعمل الكمبيوتر بحسب تعليماته، كما لا يشترط إثبات الدليل الرقمي من طرف خبير. أولا: قبول الأدلة الرقمية استثناءا من قاعدة استبعاد شهادة السماع

[1]- عائشة بن قارة مصطفى ، المرجع السابق ص197

لقد اعتبرت التشريعات في ظل هذا النظام المقيد الدليل الرقمي شهادة سماع فيعتبر من أول وهلة دليلا غير مقبول ، إلا أن المشرع في هذا النظام وضع استثناءات على قاعدة شهادة السماع و من بينها البيانات و المعلومات التي يتم الحصول عليها من الكمبيوتر.

و بالتالي فإن الدليل الرقمي يدخل في طائفة الحالات الاستثنائية عن قاعدة شهادة السماع، ليصبح الدليل الرقمي دليلا مقبولا في الإثبات الجنائي

وقد اعتبر القضاء الانجليزي الدليل الرقمي شهادة مباشرة، و ظهر ذلك في العديد من القضايا المعروضة أمامها ففي قضية (R. Wood . v) تم العثور في حيازة المتهم على بعض المعادن المسروقة و كانت تركيبة المادة الكيميائية لهذه المعادن مسجلة في كمبيوتر المجني عليه، و قد قدمت ورقة مخرجة من الكمبيوتر كدليل، وقد اعتبرت المحكمة هذه الورقة مقبولة و صالحة للإثبات.

و في نفس السياق قبلت محكمة الاستئناف في انجلترا دليلا مستخرجا من الكمبيوتر في قضية (R . V Pettigrew) بوصفه شهادة مباشرة و ليست سماعية و التي تمثلت وقائعها في القبض على متهم يحوز نقودا مسروقة و قد كانت أرقام هذه النقود مسجلة في كمبيوتر البنك في انجلترا، و قبلت مخرجات الكمبيوتر الورقية باعتبارها دليلا مباشرا.

فيه يقوم المشرع بتحديد أدلة الإثبات حصرا، وكذا القوة الثبوتية لكل دليل من أدلة الإثبات بناء على قناعته، وهو ما يعرف بنظام الأدلة القانونية، إذ لا يكون لقناعة القاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، إذ تحدد للقاضي الأدلة التي يجوز له قبولها واللجوء اليها في الإثبات ولا سبيل لإنشاء أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات[1].

[1]– خالد عياد الحلبي، المرجع السابق، ص 235، 236

قبول الدليل الرقمي استثناءا من قاعدة الدليل الأفضل

تعتمد التشريعات في ظل النظام المقيد في قواعد الإثبات على قاعدة الدليل الأفضل و التي فحواها أنه من أجل إثبات محتويات كتابة أو صورة أو غيرها فإنه لابد من تقديم الأصل لإثبات المحتوى، فلابد من تقديم أفضل نموذج و أن يكون الدليل المقدم أوليا أو أصليا.

و على إثر ظهور المستندات الإلكترونية كان لابد من تغيير هذه القاعدة لتتلاءم مع عصر المعلومات و الأدلة الرقمية

و بالتالي اعتبرت الكتابة الموجودة داخل الأجهزة في صورة كهرومغناطيسية نسخة أصلية و بالتالي لا اصطدام بقاعدة الدليل الأفضل[1].

ثانيا: نظام الإثبات الحر

وفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته، فله أن يبني هذه القناعة على أي دليل وإن لم يكن منصوصا عليه ، وكل الأدلة تتساوى قيمتها في الإثبات في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه ما يراه صالحا للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يقتنع به، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توفر شرط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع، ولذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في هذا النظام[2].

[1]– عائشة بن قارة مصطفى المرجع السابق ص 204

[2]– شيماء عبد الغني، محمد عطا الله الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 435 436

ثالثا : الدليل الإلكتروني في نظام الإثبات المختلط

كما يبدو من خلال تسميته فإن هذا النظام المختلط بين نظام الإثبات الحر و نظام الإثبات المقيد ، و يتميز النظام بأنه يجمع بين استقرار المعاملات ، بما يفرضه من قيود على الإثبات ، و يحد في ذات الوقت من تحكم القضاء ، و بين اقتراب الحقيقة القضائية من الحقيقة الواقعية ، لما يمنحه للقاضي من حرية في التقدير [1].

فهو يحاول التوفيق بين يقين القاضي ويقين المشرع، وبمقتضاه يكون بمقدور القاضي أن يصدر حكما استنادا إلى دليل وفقا لقناعته، ولكن مع توافر الشروط التي يستلزمها المشرع لقبول هذا الدليل.

إن نظام الإثبات المختلط يتجنب ما وجه من انتقادات إلى نظام الإثبات الحر من خشية تعسف القاضي الجنائي، و خروجه عن الصواب، و هذا عن طريق تحديد طرق الإثبات التي يعتمد عليها ، و كذلك تجنب الانتقادات التي وجهت لنظام الإثبات المقيد الذي يجعل دور القاضي سلبيا في عملية الإثبات، و هذا عن طريق إعطاء القاضي الجنائي الحرية في تقدير ما يعرض عليه من أدلة ثبوتية في الدعوى المعروضة عليه، و أبرز نموذج لنظام الإثبات المختلط هو الذي اقترحه " روبسبير " في إجتماع الجمعية التأسيسية الفرنسية عام 1791،[2] الذي كان يحتوي على جزأين، حيث تمثل الجزء الأول في عدم الحكم بالإدانة على المتهم إذا لم تتوفر ضده أدلة حددها القانون، أما الجزء الثاني فهو عدم الحكم بالإدانة على المتهم حتى و إن توافرت الأدلة القانونية ما لم تحقق قناعة القاضي.

و من التشريعات الغني أخذت بنظام الإثبات المختلط القانون الإجرائي الياباني الذي حدد سلفا أدلة و وسائل الإثبات، و أيضا أخذ بقاعدة الاقتناع الذاتي للقاضي [3].

و بالنسبة لموقع و حجية الأدلة الرقمية في ظل هذا النظام تتعرض إليه الفروع الآتية:

---

[1]– عصمت عبد المجيد بكر، المرجع السابق، ص 43

[2]– عباسي خولة، المرجع السابق ص 60

[3]– رمزي رياض عوض سلطة القاضي الجنائي في تقدير الأدلة، د ط دار النهضة العربية، ، القاهرة ،2010 ص ، 16

1- مبادئ نظام الإثبات المختلط بالنسبة للدليل الرقمي

الم تنص التشريعات على الدليل الرقمي باعتباره دليلا مستحدثا لجريمة مستحدثة و لكن تماشيا مع هذا النوع المستحدث من الأدلة و في إطار مواكبة التكنولوجيا فقد قامت بوضع استثناءات حتى تشمل هذا الدليل في تشريعاتها . و بالنسبة لمبدأ حرية القاضي الجنائي فإنه لا يمثل إشكالا باعتبار أن كل الأدلة الجنائية خاضعة لحرية و تقدير القاضي الجنائي، و الدليل الرقمي دليل من أدلة الإثبات الجنائي، و بالتالي فهو خاضع لحرية القاضي و تقديره و اقتناعه كغيره من الأدلة . و نظام الإثبات المختلط في إطار التوفيق بين نظامي الإثبات المقيد و الحر، أخذ صورتين وتتمثل الصورة الأولى في الجمع بين الحقيقتين في كل الحالات سواء كان ذلك في الإدانة أو البراءة و لكن في هذه الحالة تطرح مشكلة تطابق قناعة القانون مع قناعة القاضي، و في هذه الحالة فإن القاضي لا يمكنه الفصل في القضية لا بالإدانة و لا بالبراءة، و لذلك اقترح النظام المختلط حلا وسطا و مؤقتا مفاده أن القاضي في هذه الحالة ما عليه إلا أن يحكم بعدم ثبوت التهمة، حتى تتوقف المحاكمة و يستعيد المتهم حريته، و ألا يحكم في نفس الوقت بالبراءة، و لكن يؤجل الحكم مع بقاء الدعوى معلقة أمام القضاء أما الصورة الثانية فهي ضرورة الجمع بين القناعة القانونية و قناعة القاضي في حالة الإدانة فقط[1].

2- حجية الدليل الرقمي في نظام الإثبات المختلط

في ظل نظام الإثبات المختلط يحدد المشرع الأدلة الالكترونية سلفا عن طريق اصدار تشريع بهذه الأدلة يحدد فيه الأدلة المقبولة ومن ثم فإنه يمنح القاضي الحق في تقدير هذه الأدلة المعروضة أمامه في القضية التي ينظرها ، له الحق في استبعاد أي دليل لا يقتنع به والأخذ بدليل آخر يقتنع به، فعلى سبيل المثال لو حدد التشريع المنظم للأدلة الالكترونية أن الأدلة المقبولة هي الأقراص المغناطيسية والمخرجات الورقية، وكان هذان الدليلان معروضين

[1]- هلال أمنة، المرجع السابق، ص 86

أمام القاضي الجنائي في قضية ما فيحق له الأخذ بأحدهما، والذي يقتنع به ويطمأن له، ويستبعد دليل آخر .

فالقانون الإجرائي الياباني مثلا حصر طرق الإثبات المقبولة في أقوال متهم وأقوال الشهود والقرائن والخبرة، أما بالنسبة للأدلة الالكترونية، فقد قرر الفقه الياباني أن السجلات الالكترومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة إلا إذا تم تحويلها إلى صور مرئية ومقروءة عن طريق مخرجات الطابعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة، وهي الأدلة الالكترونية سواء هي الأصل أو كانت نسخة من هذا الأصل[1].

كما نص قانون الإجراءات الجنائية التشيلي من خلال نص المادة 113، على امكاني استخدام الأفلام السينمائية والفوتوغراف والنظم الأخرى بإنتاج الصور والصوت والاختزال وبصفة عامة أي وسيلة أخرى قد تكون ملائمة وثيقة الصلة، تؤدي إلى استخلاص المصداقية، يمكن أن تكون مقبولة كدليل إثبات، ويرى الفقه التشيلي أن الدليل الناتج عن الحاسوب والأنترنت أو الدليل الالكتروني يمكن أن يكون مقبولا في المحكمة كدليل كتابي أو مستندي كالنظم الحديثة الأخرى لجمع وتسجيل المعلومات، وحجية الفقه التشيلي تستهدف توسيع نطاق الوسائل العلمية الحديثة في الاثبات لتغطي العناصر الاثباتية الناتجة عن الجرائم المعلوماتية. ومنه نقول أن الدليل الالكتروني في ظل نظام الاثبات المختلط يعمل على تحديد نظام أدلة الإثبات الجنائية من جهة، والدليل الالكتروني حدد كاستثناء على هذه القاعدة، كما أنه يولي أهمية كبيرة في سلطة القاضي الجنائي في الأخذ بالأدلة وتقديرها، الأمر الذي يسهل الأخذ بالدليل الإلكتروني على أساس حرية القاضي الجنائي في قبول أي دليل يراه مناسبا استبعاد الدليل الذي لا يراه مناسبا.

[1]– مبروك نصر الدين، محاضرات في الاثبات الجنائي، الجزء الأول، الطبعة الثالثة، دار هومة للطباعة النشر والتوزيع، الجزائر، 2009، ص 97

ثالثا: نطاق تطبيق الدليل الرقمي

تنقسم أدلة الإثبات الجزائية إلى أدلة إثبات تقليدية مثل (الاعتراف، الاستجواب، الخبرة الجزائية والقرائن القضائية... الخ)، وأدلة الإثبات المستحدثة ومنها: الأدلة البيولوجية (كالبصمة الوراثية وتحليل الدم، والأدلة التقنية (كالدليل الالكتروني والتسجيل الصوتي والتنصت الهاتفي). وبالحديث عن الدليل الرقمي كدليل من الأدلة الجنائية لا بد من التطرق إلى نطاق العمل بهذا النوع من الأدلة، حيث تختلف الجريمة التقليدية عن الجريمة المعلوماتية في كون الأخيرة تتم في بيئة غير مادية عبر نظام الحاسب الآلي أو شبكة المعلومات الدولية (الإنترنت)، فيمكن للجاني عن طريق نبضات رقمية إلكترونية لا ترى أن يبعث بيانات الحاسب أو برامجه وذلك في وقت قياسي قد يكون جزء من الثانية، كما يمكن محوها في زمن قياسي كذلك قبل أن تصل العدالة إليه مما يصعب الحصول على دليل مادي في مثل هذه الجرائم [1].

1- الدليل الرقمي في الجرائم التقليدية

مع التطور السريع في التقنيات أضحي المجرمون يستخدمون الوسائل التقنية المتطورة لتنفيذ أعمالهم الاجرامية، مما يؤكد ضرورة التعرف على الأدلة المنبثقة عن هذه الوسائل[2].

ويلاحظ أن الدليل الرقمي لا يتعلق فقط بجرائم تقنية المعلومات، فقد تكون هناك جريمة عادية، مثل القتل أو التهريب أو غيرها، لكن الدليل الذي يدين المجرمين هو دليل رقمي.

إن الدليل الرقمي مثلما يصلح لإثبات الجريمة المعلوماتية، يعتبر في ذات الوقت دليلا لإثبات الجريمة التقليدية، كما لو أرسل شخص لشخص آخر رسالة إلكترونية تحتوي فيروسات الإتلاف الموقع الإلكتروني الخاص بذلك الشخص والتي تتضمن معلومات لتمهيد ارتكاب جريمة سطو أو قتل، فإن هذه الرسالة تعد دليلا في نسبة الفعل المرتكب، وهو ما يجعل الدليل

[1]- طاهري عبد المطلب، المرجع السابق، ص 70-71

[2]- عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص 13

الرقمي ذو قرينة قوية في نسبة الدليل لصاحبه الحقيقي خاصة الدليل البيولوجي، لاسيما وإن كانت الرسالة المرسلة إلكترونيا تحتوي على بيانات تثبت هوية الجاني، والذي يتصف كونه شخص عادي أمام جهاز الحاسوب ليتحول إلى جاني في مسرح الجريمة يدلل عليه أثره البيولوجي بعد تمام فعله الاجرامي.

والجريمة التقليدية هي تلك الجريمة التي عرفها الناس منذ آلاف السنين وتعرف بالجرائم الطبيعية وهي توجد في كل مجتمع مثل جريمة السرقة وجريمة القتل، بخلاف الجريمة الإلكترونية – مثلاً – التي تستخدم في ارتكابها أجهزة الكمبيوتر والإنترنت ووسائل الاتصال الحديثة.[1]

وفي الجرائم التقليدية تخضع لأدلة إثبات عادية، فقد أعطى القانون للقاضي الجنائي كامل الحرية في تقدير الأدلة المقدمة إليه في الدعوى الجنائية ووزنها وترجيح بعضها على الآخر وذلك تطبيقا لمبدأ حرية الإثبات المقرر في المسائل الجنائية باستثناء بعض الحالات المحددة في الإثبات حصرا، إذن لا يتقيد الإثبات الجنائي بوجه عام بأدلة معين وللقاضي أن يكون اقتناعه من أي دليل يقدم إليه وهذا بخلاف الحال في الإثبات المدني.

[1]- سميرة بيطام، حجية الدليل البيولوجي أمام القاضي الجنائي، مذكرة ماجستير في تخصص: القانون كلية الحقوق، جامعة الجزائر 1، 2013 – 2014، ص 156

الفرع الثاني : مشروعية الحصول على الدليل الالكتروني

ان الدليل العلمي لا يكون مشروعا أو مقبولا إلا إذا تمت عملية البحث والحصول عليه وتقديمه أمام القضاء بإجراءات صحيحة وسليمة من الناحية القانونية ، مع استعمال وسائل وطرق مشروعة يقرها العلم والقانون بشكل يحقق التوازن بين مصلحتين متعارضتين، مصلحة المجتمع في الحفاظ على أمنه بتوقيعه

الجزاء على مرتكب الجريمة، ومصلحة المتهم في احترام حقوقه وكرامته الإنسانية و هذا ما يسمى بالشرعية الإجرائية. في مجال الدليل الالكتروني تتمثل في ضرورة اتفاق الإجراء – الذي تم الحصول على الدليل بواسطته – مع القواعد القانونية و الأنظمة الثابتة ، فالقاضي لا يمكنه أن يعتمد على أدلة لم تراع فيها القواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية المتعلقة بالتفتيش والاستجواب ونتب الخبراء لانه لا يمكنه تكوين قناعته وعقيدته من الأدلة غير المشروعة حتى في حالة كون الدليل صادق ، كما لا يمكنه أن يعتمد على أي دليل مخالف للنظام العام والآداب العامة لانه يعتبر دليل معيب و القاضي لا يجوز له الاعتماد على دليل معرب لبناء حكمه وقاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا ان تراعى فيه المواثيق والاتفاقات و المعاهدات الدولية و خاصة في مجال الجرائم الالكترونية .

ان سلطة القاضي في تقدير مشروعية الدليل الالكتروني يجب ان تراعي خصوصية هذا الدليل باعتباره يدخل ضمن المسائل العلمية الدقيقة ، فتقدير القاضي لا يجد مجاله في تقدير القيمة العلمية للدليل و انما في الظروف و الملابسات التي وجد فيها ، ذلك أنه لا حرية للقاضي في مناقشة الحقائق العلمية الثابتة ، لانها أمور دقيقة لا اعتراض عليها عكس الظروف التي وجد فيها الدليل فان تقديرها يدخل ضمن نطاق تقديره الذاتي ، لذا فان رقابة القاضي على الدليل الالكتروني تتمثل في رقابته على طرق و أساليب استخلاصه وذلك من

خلال نقطتين اثنتين هما سلامته من العبث به من ناحية وصحة الاجراءات المتبعة في الحصول عليه من ناحية اخرى ، فالدليل الالكتروني يشكك في سلامته من ناحيتين

أ- يمكن ان يخضع الدليل الرقمي للعبث به مما يجعله يقدم على نحو يخالف الحقيقة ، فقد يقدم هذا الدليل معبرا عن واقعة معينة صنع أساسا لاجل التعبير عنها خلافا للحقيقة ، وذلك دون أن يكون في استطاعة غير المتخصص ادراك ذلك العبث ، فالتقنية الحديثة تمكن من العبث بالدليل الرقمي بسهولة و يسر بحيث يطهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة .

ب – الخطأ في استخلاص الدليل : ان نسبة الخطأ التقني في الحصول على الدليل الرقمي نادرة للغاية الا انها تظل ممكنة ، و يرجع الخطأ في الحصول على الدليل الرقمي إلى سببين اثنين :

من الضروري أن يتم رسم ضوابط و أطر معينة يتعين أن تمارس في نطاقها عملية البحث عن الأدلة وتحصيلها والتحقيق فيها، بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من ورائه، وهو الوصول الى الحقيقة الفعلية في الدعوى وهي الهدف الاسمى لقانون الإجراءات الجزائية.

الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي بسبب خلل في الشيفرة المستخدمة أو بسبب استخدام مواصفات خاطئة

– الخطأ في استخلاص الدليل بسبب وسائل اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الاصلية التي يتم تقييمها

ومن خلال ذلك يتبين لنا ان الشك الذي يمكن ان يثور حول الدليل الالكتروني لا يتعلق بمضمونه كدليل

– لانه من هذه الناحية كدليل علمي يكاد يصل الى درجة اليقين و انما بعوامل مستقلة عنه ولكنها تؤثر في حجيتة الاثباتية بسبب الطبيعة الفنية لهذا الدليل وهذه الناحية من الدليل هي التي تخضع لحرية القاضي في قبوله او اهداره تبعا لكون المحققين احترموا الإجرائية الشرعية في استخلاصه ام خالفوها. يتم تقييم الدليل الالكتروني بعدة وسائل للتأكد من سلامته وصحة الاجراءات المتبعة للحصول عليه، منها فكرة التحليل التناظري الالكتروني التي يتم من خلالها مقارنة الدليل الالكتروني المقدم للقضاء للتأكد من مدى حصول عبث في النسخة المستخرجة من عدمه ، كذلك استخدام عمليات حسابية تسمى بالخوارزميات للتأكد من سلامة الدليل الالكتروني من التبديل أو العبث

نجد أنه ثار خلاف كبير بين الفقهاء حول مبدأ اليقينية بالنسبة للدليل الالكتروني ، فجانب منهم يرى أن الدليل العلمي يخضع كغيره من الأدلة الأخرى إلى مبدأ لاقتناع الشخصي للقاضي، وهو الرأي الذي أخذ به أنصار المذهب الشخصي، وجانب منهم يرى أن الدليل العلمي له قوة ملزمة وثبوتية حتى للقاضي، وهو الرأي الذي أخذ به أنصار المدرسة الوضعية، ويتجلى ذلك من خلال ما يلي:

ا – أنصار مبدأ الاقتناع الشخصي:

يقال في الفقه عادة أن سلطة القاضي الجزائي في تقدير الأدلة العلمية محكومة بمبدأ حريته في الاقتناع وأن هذا المبدأ يؤدي بطريقة مباشرة أو غير مباشرة إلى نتيجتين: الأولى هي حرية القاضي الجزائي في قبول الدليل على نحو تكون أدلة الإثبات مقبولة ، أما الثانية فهي أن

الدليل الجزائي يخضع لمنطق تقدير القاضي وهو المبدأ الذي أخذ به غالبية الفقه، والذي مقتضاه حرية قبول الدليل بما فيه الدليل العلمي وتقدير قيمته القانونية من طرف القاضي مدعمين رأيهم على مجموعة من الأسانيد والحجج، وهو ما ستشير إليه من خلال نقطتين:

ويعني مبدأ مشروعية الحصول على الدليل الإلكتروني بما يتضمنه من مفاهيم الكترونية، ضرورة اتفاق الإجراءات مع القواعد القانونية والأنظمة المتبعة في وحدات المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القواعد القانونية، بل يجب أن تراعي المبادئ السامية لحقوق الانسان وقواعد النظام وحسن الآداب في المجتمع ويشترط في الدليل الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة، وذلك يقضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن ونحن هنا نبحث عن مشروعية الدليل الإلكتروني، فإننا نقتصر على ما هذا الدليل من إشكالات قانونية بالنظر إلى طبيعته الخاصة، ولذا يمكننا القول ان ما يثيره الدليل الالكتروني من حيث مشروعية الحصول عليه يتركز بشكل اساسي في اجراءات التفتيش للبحث عن هذا الدليل وذلك يتم بنقطتين رئيستين [1] :

– صفة القائم بالتفتيش

– مدى مشروعية التفتيش عن الدليل الالكتروني وفي ضبطه في الوسط الافتراضي.

من المقرر أن الإدانة في أي جريمة لا بد ان تكون مبنية على أدلة مشروعية في الحصول عليها وفق قواعد الأخلاق والنزاهة، واحترام القانون من طرف الجهة المتخصصة بجمع الدليل الجزائي بما يتضمنه من لأدلة مستخرجة من وسائل الكترونية.

ولا يكون إلا إذا أجرى التفتيش عنه أو الحصول عليه أو كانت عملية تقديمه إلى و إقامته أمامه بالطرق التي رسمها القانون، فمتى ما تم الحصول على الدليل خارج هذه القواعد

[1]– حسين ربيعي ، المرجع السابق ، ص 265.

القانونية فلا يعتد بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته، وعلى هذا الأساس فإن إجراءات جمع الأدلة الإلكترونية المتحصلة من الوسائل الإلكترونية إذا خالفت[1].
القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح لان تكون أدلة تبنى عليها الإدانة في المواد الجنائية[2].

المطلب الثاني : حجية الدليل الإلكتروني في الإثبات الجنائي وموقف المشرع الجزائري منه

إن مجرد الحصول على الدليل الإلكتروني وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ أن الطبيعة الفنية الخاصة بالدليل الالكتروني تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة الشخص غير المتخصص إدراك ذلك العبث، فضلا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإبلاغ عن الحقيقة فتبدو عادية في مثل هذا النوع من الأدلة، لذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي[3].

الفرع الأول: حجية الدليل الإلكتروني في الإثبات الجنائي

تشمل جرائم الكمبيوتر في القانون الجزائري الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكذا كل جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة حاسوبية أو نظام للاتصالات الإلكترونية، وهذه الأخيرة قد تنقسم إلى جرائم تقليدية منصوص عليها في قانون العقوبات يمكن حسب طبيعتها أن ترتكب بواسطة منظومة حاسوبية رقمية
، وهذا يعني أن الإجرام المعلوماتي قد يأخذ وصف الجناية أو الجنحة أو المخالفة حسب وصف الجرم المرتكب بواسطة المنظومة الحاسوبية، والمشرع الجزائري أجاز إثبات الجرائم بأي

[1]– خالد عياد الحلبي ، المرجع السابق ، ص 239.
[2]– سعيداني نعيم ، المرجع السابق ، ص 210
[3]– خالد عياد الحلبي ، المرجع السابق ، ص 246.

طريق من طرق الإثبات ما عدا الجرائم التي قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن إليه.

إن كان مبدأ الاقتناع القضائي عام النطاق لدى كافة أنواع المحاكم الجزائية سواء كانت محاكم الجنايات أم الجنح أم المخالفات، فإن قواعد بيان عناصر تقدير الدليل تختلف حسب اختلاف وصف الفعل المجرم[1].

فإذا كان الفعل من طبيعة جنائية فإن محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها وتصدر أحكامها دون أن يكون قضاتها
مطالبين بتسبيب أحكامهم ولا رقابة لجهات الطعن عليهم. أما إذا أخذ الفعل المجرم وصف الجنحة فإن قاضي الجنح مطالب بعرض وبيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه، والذي يكون محل رقابة من جهات الطعن[2].

لهذا فهو مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات والتي قد تأخذ شكل محاضر معدة بمناسبة تفت أو اعتراض مراسلات أو شكل تقرير خبرة محرر بمناسبة معاينة وفحص الأدلة المضبوطة من جهاز الإعلام الآلي أو دعامات إلكترونية.

أما بالنسبة لتقارير الخبرة فإن المحكمة العليا ذهبت للقول أن الخبرة شأنها باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع، وهذا ما نصت عليها المادة 215 من قانون الإجراءات الجزائية بنصها: " لا تعتبر التقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات[3].

[1]– جواحي عبد الستار، المرجع سابق، ص 59

[2]– عبد الله بن صالح بن رشيد الربيش، سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون و تطبيقاتها في المملكة العربية السعودية مذكرة ماجستير ، أكادمية نايف العربية للعلوم الأمنية قسم العدالة الجنائية، الرياض 1424 هجري ص 74

[3]– جواحي عبد الستار ، المرجع السابق، ص 56

والواضح أن المشرع الجزائري قد تبنى نظام الاقتناع الشخصي للقاضي الجزائي، من خلال نص المادة 212 من قانون الإجراءات الجزائية: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص[1].

وكذلك نص المادة 307 من نفس القانون: "أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم .."

واستثناء نجده أخذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط الإثباتها أدلة قانونية محددة مسبقا وعلى سبيل الحصر.

إن مسألة تقييم الدليل الجنائي في إثبات الوقائع الجرمية مسألة موضوعية محضة للقاضي أن يمارس سلطته التقديرية فيها[2].

أولا: تقييم الدليل الإلكتروني من حيث سلامته من التزوير يمكن التأكد من سلامة الدليل الالكتروني من العبث به بعدة طرق نذكر منها:

– فكرة التحليل التناظري الرقمي والتي من خلالها يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثم يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا، ويستعان في ذلك استخدام جهاز الحاسوب الذي يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون الدليل الرقمي، وهذا العلم يستعان به أيضا في كشف مدى تلاعب بمضمون هذا الدليل.

– استخدام عمليات حسابية خاصة تسمى الخوارزميات ويلحق إلى هذه التقنية في حالة عدم الحصول النسخة الأصلية للدليل الرقمي، وفي حالة العبث قد وقع على النسخة الأصلية

[1]– أنظر المادة (215) ق ج ج) ق ا ج ج

[2]– سعيداني نعيم ، المرجع السابق ، ص217.

بالإمكان التأكد من سلامة الدليل الرقمي من التحريف والتغيير باستعمال هذه العمليات الحسابية .

استعمال الدليل المحايد وهو نوع من الأدلة الرقمية المخزون في البيئة الافتراضية لا علاقة له بموضوع الجريمة، ولكنه يساعد في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول أي تعديل عليه في نظام الحاسوب[1].

ولا شك أن الخبرة التقنية تمثل في هذه الحالة دورا مهما في التثبت من سلامة الدليل الرقمي، فإذا كان للخبرة التقنية أهمية كبرى في مجال استخلاص الدليل الرقمي، فإن لها ذات الدور في بحث مصداقية وتقييمه من حيث عدم حصول أي عبث عليه، فنقص الثقافة المعلوماتية للقاضي الجزائي قد يحتم عليه كواجب قضائي أن يستعين في هذه المسائل بوسائل الخبرة كنهج، ليس من اجل استيفاء الدليل فحسب بل لبحث مصداقيته في مجال معالجة الآلية للمعلومات وتحقيق اليقينية لهذا الدليل.

ثانيا : تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول عليه

سبق الحديث على أن الدليل الرقمي يتم الحصول عليه بإتباع جملة من الإجراءات الفنية، والتي من الممكن أن يعتريها خطأ قد يشكك في سلامه نتائجها، الأمر الذي يحتم إخضاعها إلى اختبارات كوسيلة للتأكد من سلامة هذا الإجراءات من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات ويتبع في ذلك مجموعة من الخطوات [2]:

– إخضاع الأدلة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج ويكون ذلك بإتباع اختبارين أساسيين يتم التأكد من خلالهما أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الرقمي، وفي ذات الوقت لن تضف إليها أي بيانات جديدة وهو ما قد يعطي النتائج

[1]– خالد عياد الحلبي ، المرجع السابق ، ص 249.

[2]– سعيداني نعيم ، المرجع السابق ، ص 218.

المقدمة مصداقية في التدليل على الوقائع، أو يمثل هذان الاختباران في:2 اختبار السلبيات الزائفة ومفاده أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي، وأنه لم يتم إغفال معطيات مهمة عنه، أما الاختبار الثاني والذي يجري باختبار الايجابيات الزائفة مفاده إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي للاختبار يمكن من التأكد من أن هذه الأداة لاتعرض معطيات إضافية جديدة[1].

– الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل، إذ تبين الدراسات العلمية والبحوث المنشورة في مجال تقنية المعلومات بالطرق السليمة التي يجب إتباعها في الحصول على الدليل الرقمي، وفي المقابل بينت تلك الدراسات أيضا الأدوات المشكوك في كفائتها وهو ما يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات[2].

من خلال ما تقدم يمكن الوقوف على سلامة الدليل الإلكتروني، فإذا توافرت في الدليل الالكتروني الشروط العامة لما يمكن أن يمثل أساسا لتأكيد الثقة فيه، فإنه يبدو ومن غير المعقول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على البحث، فإن الدليل الإلكتروني بوصفه دليلا علميا فإن دلالته قاطعة شأن الواقعة المستشهد به منها، فإذا سلمنا سابقا بإمكانية التشكيك في سلامة الدليل الالكتروني بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم وإن لم يقطع به أهل الاختصاص.

[1]– خالد عياد الحلبي، المرجع السابق ، ص 251

[2]– سعيداني نعيم ، المرجع السابق ، ص.218

إذا توافرت في الدليل الالكتروني الشروط السابقة بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استنادا لسلطة القاضي التقديرية إذا سلطة القاضي في رد الدليل استنادا لفكرة الشك، يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، وهو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة، بحيث يقتصر دور القاضي على بحث صلة الدليل بالجريمة، ولا شك أن الخبرة تحتل في هذه الحالة دورا مهما في التأكد من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث مصداقية الدليل هي من صميم فن الخبرة لا القاضي[1].

الفرع الثاني: موقف المشرع الجزائري من الدليل الالكتروني في مجال الإثبات الجنائي

إن من واجب القاضي الجنائي سواء كان قاضي التحقيق أو غرفة الاتهام أو المحكمة الجزائية، أن تقيم الدليل على المتهم، ولا يجوز أن يحاكم المتهم و يدان بمجرد وجود قرائن بل لا بد أن تكون هذه الدلائل مكملة لبقية الأدلة المادية الأخرى كما يجب أن تتسم إجراءات جمع الأدلة بالمشروعية وذلك احتراما للحرية الشخصية للمتهم باعتباره بريئا إلى أن تثبت إدانته بحكم بات[2].

إن الإثبات الجنائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف الجريمة ونسبتها إلى المتهم، وقد ذهب الفقه الإجرائي إلى وضع نظامين إجرائيين في مجال الإثبات الجنائي يختلفان فيما بينهما من حيث الأسس التي يقوم عليها كل واحد منها وقد سبق الإشارة إليهما.

[1]- هلالي عبد الله احمد ، المرجع السابق ، ص 95

[2]- بلعليات ابراهيم . المرجع السابق ، ص 139.

تنتمي الجزائر إلى مجموعة الدول التي تتبنى نظام الإثبات الحر في مجال الإثبات الجنائي، فهي تساير النظم اللاتينية كفرنسا وبلجيكا والأردن وسوريا، وهو الأمر الذي كرسته المادة 212 من قانون الإجراءات الجزائية التي جاء في نصها على أن: "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص بها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ، ولا يجوز للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه."

إن إقرار المشرع الجزائري للحرية في تقديم الأدلة وتركها للقانعة الشخصية لقاضي الموضوع هو لتعزيز إثبات قرينة البراءة، وتعزيز لممارسة حقوق الدفاع الفردية ، غير أن هذا الإطلاق بدون تحديد وتخصيص يعد قصورا تشريعيا واضحا فلا نجد ضمن قانون الإجراءات الجزائية ما يدل على أن الدليل الالكتروني، هو دليل من نوع خاص شانه شان الجرائم الإلكترونية ، فغياب أدنى نص قانوني في هذا الشأن يؤدي إلى ظهور إشكالات متعلقة بطبيعة الأدلة المقدمة أمام الجهات القضائية، بحيث يمكن لهذه الأخيرة وفي حال عدم إلمامها بتقنية المعلوماتية دحض هذا الدليل وعدم الاعتداد به ، ولو كان حائزا على القوة الثبوتية، وتتوفر فيه كافه شروط الصحة وكذلك العكس صحيح.

أما بالنسبة لسلطة القاضي الجزائري في تقدير الدليل الالكتروني، فإن المادة العلمية للدليل الالكتروني جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، إن هناك من يرى أن الدليل العلمي ومنه الدليل الالكتروني له قوته الثبوتية الملزمة حتى للقاضي، مستندين في رائيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين، وهناك من يرى بأن مبدأ حرية القاضي في الاقتناع، يجب أن يبسط سلطاته على كل الأدلة دون استثناء حتى على الدليل الرقمي، معتبرين أن إعطاء الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني المقيد، والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأية طريقة من طرق الإثبات ما عدا الجرائم التي

قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن عليه[1].

[1]– سعيداني نعيم ، المرجع السابق ، ص229.

خاتمة

توصلنا من خلال دراستنا أن الخبرة تعد من أهم وسائل الإثبات التي يلجأ إليها القضاة في الكشف عن الجريمة، وإثبات وقوعها ونسبتها إلى شخص معين، وتشمل الخبرة حيزا كبيرا في الجرائم ذات الطبيعة العلمية والفنية، لذلك يتم اللجوء إليها بنسبة كبيرة في الجرائم الالكترونية لطبيعتها الخاصة، ووقوعها في بيئة افتراضية يصعب اكتشافها واثباتها، ومن خلال هذه الدراسة توصلنا إلى النتائج التالية:

– إن التحقيق في الجرائم الإلكترونية يقتضي ضرورة ندب خبراء تقنيين لهم دراية في التعامل مع الأنظمة المعلوماتية، ومرجع ذلك هو الطبيعة الفنية و التقنية التي ترتكب بها هذه الجريمة فضلا عن طبيعتها الخاصة. – تخضع الخبرة في الجرائم الإلكترونية إلى نفس أحكام الخبرة القضائية من حيث القواعد القانونية التي تحكم عمل الخبير وإجراءاته.

– يعتمد الخبير التقني في سبيل تحري الحقيقة أساليب فنية

لا غنى عن الخبرة التقنية لدورها الفعال في اثبات الجرائم الالكترونية، لاستعانة الخبير الالكتروني بأساليب ووسائل تقنية بحثة في استخلاص الدليل الرقمي. 4– عدم الزامية تقرير الخبرة بالنسبة للقاضي كمبدأ عام الا انه استثناء يمكن اعتبار الخبرة التقنية السبيل الوحيد لإثبات الجرائم الالكترونية، فالقاضي مجبرا على انجازها والأخذ بنتيجتها، ولا حجة في استبعادها.

أما ما يمكن تسجيله من توصيات من خلال ما تقدم من البحث فهي على النحو التالي :

1–تأهيل وتدريب سلطات التحقيق في مجال التحقيق في الجرائم الالكترونية، من أجل تحديد للخبير دوره في المسالة المنتدب فيها بدقة وليس للخبير أن يحدد إطار مهمته.

2– ضرورة التعاون الدولي في مجال الخبرة التقنية من خلال عقد مؤتمرات والاستفادة من تجارب الدول الاخرى ولو عن بعد، لأنه يعود بالفائدة على الدول التي تعاني من نقص الكفاءة في مجال تكنولوجيا الاعلام والاتصال .

3- ضرورة أن تتبنى كل دولة جهازا خاصا يتكون أعضاؤه من فريق متخصص فنيا في التقنية المعلوماتية، على أن يتم إعادة النظر في القواعد التقليدية للخبرة لأن إثبات الجريمة الإلكترونية يتطلب قواعد خاصة للتعامل مع الأدلة في هذه الجرائم.

4- على المجتمع الدولي تكثيف الجهود و التعاون والتنسيق بين الدول بتوحيد القوانين لمكافحة الجرائم الإلكترونية، ذلك بالعمل على إبرام اتفاقيات دولية على غرار إتفاقية بودابست لسنة 2001 لمكافحة الجريمة المعلوماتية، والإعتماد على سياسة فعالة و موحدة في مجال التعاون الدولي المتبادل و تكريس إجراءات تحقيق و المتابعة بشكل يسمح بالتدخل و التحقيق بشكل متكامل في إقليم دولة أجنبية دون المساس بسيادة هذه الدولة .

5- الإسراع في الإنضمام إلى مختلف الإتفاقيات الدولية الخاصة بمكافحة الجريمة الإلكترونية، وكل ما من شانه تكثيف الجهود على المستوى الدولي و الإقليمي، كإنشاء الدول الإفريقية أو العربية، الأجهزة و هيئات و منظمات تهتم بالتنسيق الأمني في مجال مكافحة الجريمة الإلكترونية و العمل على تطوير كفاءاتها و خبراتها في هذا المجال . 3- بطئ الإجراءات على المستوى الدولي بسبب الأعراف و الطرق الدبلوماسية المعقدة و الطويلة، خاصة في مجال الإنابات القضائية الدولية و تسليم المجرمين، المقيدين بجملة من الشروط ما يعرقل من جهود سلطات التحقيق و يستفيد منه المجرم الإلكتروني الذي يتميز بالسرعة في تنفيذ جرائمه في العالم الإفتراضي اللامتناهي الحدود.

6- الإستفادة من تجارب الدول المتقدمة في مجال مكافحة الجرائم الإلكترونية و التي تملك تقنيات و خبرات علمية جد متقدمة في هذا المجال، ذلك بتفعيل عمل الإستباقي و إستحداث آليات إجرائية وقائية للوقاية من هذه الظاهرة الإجرامية المستحدثة المخلفات الذي تتركها على جميع الأصعدة، بحيث تعتبر في بعض الحالات تهديدا مباشرا لأمن الدولة كالجرائم المتعلقة بالإرهاب الإلكتروني و التجمس الإلكتروني.

قائمة المراجع

قائمة المراجع

الكتب

1. عبد الفتاح بيومي حجازي ،الإثبات الجنائي في جرائم الكمبيوتر والإنترنت ،دار الكتب القانونية ، مصر ، 2007

2. خالد ممدوح إبراهيم ،فن التحقيق الجنائي في الجرائم الإلكترونية ،دار الفكر الجامعي ،الإسكندرية ، 2009

3. عبد الناصر محمد محمود فرغلي ؛ د.محمد عبيد سيف المسماري ،الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية ، بحث من ضمن أعمال المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي ،جامعة نايف العربية للعلوم الأمنية ، الرياض ،2007

4. فخري عبد الحسن علي ،المرشد العلمي للمحقق ،بغداد ،منشورات مديرية الشرطة ،1999م

5. محمد واصل ؛حسين بن علي الهلالي ،الخبرة الفنية امام القضاء ،المكتب الفني ،مسقط ،2004

6. محمد الامين البشري ،الادلة الجنائية الرقمية مفهومها ودورها في الاثبات ،المجلة العربية للدراسات الامنية و التدريب ،الرياض ،المجلد 17 ،العدد 33 ،2004

7. مصطفى محمد موسى ،التحقيق الجنائي في الجرائم الالكترونية ،ط1،مطابع الشرطة ،القاهرة ،2009م

8. مأمون محمد سلامة ،الاجراءات الجنائية في التشريع المصري ،ج1 ،دار النهضة العربية ،القاهرة ،2001

9. .احمد فتحي سرور ،الوسيط في قانون الاجراءات الجنائية ،ط7 ،دار النهضة العربية ،القاهرة ،1993

10. براء منذر كمال ،شرح قانون اصول المحاكمات الجزائية ،ط1 ،دار الحامد للنشر والتوزيع ،عمان ،2009.
11. . محمد الأمين البشري ،التحقيق في جرائم الحاسوب والإنترنت ، المجلة العربية للدراسات الأمنية والتدريب ، الرياض ، العدد 33 ، سنة 2004
12. د. جمال ابراهيم الحيدري ،الجرائم الالكترونية وسبل معالجتها ،ط1 ،مكتبة السنهوري ،بغداد ،2012.
13. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي .2006
14. هلال عبد الله محمد حجية مخرجات الكمبيوتر في المواد الجنائية، الطبعة الثانية، دار النهضة العربية ، مصر، 2008
15. شيماء عبد الغني، محمد عطا الله الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007
16. جمال ابراهيم الحيدري ،ضوابط اعتبار المخرجات الالكترونية ادلة إثبات في القضايا الجزائية ،ط1 ،مكتبة السنهوري ،بغداد ،2012
17. جمال محمد مصطفى ، التحقيق والإثبات في القانون الجنائي ،مطبعة الزمان ،بغداد ،2004
18. جندي عبد الملك ،الموسوعة الجنائية ،دار الكتب المصرية ،القاهرة ،1931م

المذكرات

1. قادري ، سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماجستير ، جامعة قاصدي مرباح ، ورقلة ، كلية الحقوق والعلوم السياسية ، قسم الحقوق، 2013 – 2014،

2. صغير يوسف، الجريمة المرتكبة عبر الانترنت رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، كلية الحقوق والعلوم السياسية ، 2013

3. عبد الله بن صالح بن رشيد الربيش، سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون و تطبيقاتها في المملكة العربية السعودية مذكرة ماجستير ، أكادمية نايف العربية للعلوم الأمنية قسم العدالة الجنائية، الرياض 1424 هجري

4. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر ، باتنة، كلية الحقوق والعلوم السياسية قسم الحقوق ، 2011-2012

5. محمد ابو العلا عقيدة ،التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية ، المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي ، مركز البحوث و الدراسات ، العدد 1 ، الإمارات العربية المتحدة ، دبي ،2003

6. ممدوح عبد الحميد عبد المطلب ، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الإنترنت ، المؤتمر العلمي الاول حول الجوانب القانونية والامنية للعمليات الالكترونية ،مركز البحوث والدراسات العدد(4) المحور الامني والاداري للفترة (26-28)ابريل 2003م ،دبي ،الامارات العربية المتحدة

7. صغير يوسف، الجريمة المرتكبة عبر الانترنت رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، كلية الحقوق والعلوم السياسية ، 2013،

8. سميرة بيطام، حجية الدليل البيولوجي أمام القاضي الجنائي، مذكرة ماجستير في تخصص: القانون كلية الحقوق، جامعة الجزائر 1، 2013 – 2014، ص 156

النصوص القانونية

1. قانون رقم 155/66 مؤرخ في 08 يونيو 1966 المعدل و المتمم لقانون الإجراءات الجزائية، الجريدة الرسمية العدد 48، المعدل و المتمم للأمر رقم 2015 مؤرخ في 23 جويلية 2015، الجريدة الرسمية العدد 40 ، و المعدل و المتمم بالأمر
2. القانون 04-09 الصادر بتاريخ 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها
3. القانون رقم 16-01 ، مؤرخ في 6 مارس 2016 المتضمن الدستور الجزائري، الجريدة الرسمية العدد 63، بتاريخ مارس.2016
4. قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971.
5. قانون الاجراءات الجنائية المصري رقم (150) لسنة 1950
6. قانون الاجراءات الجنائية الليبي لسنة 1953
7. قانون الاجراءات الجزائري والمادة (175)
8. قانون الاجراءات الجنائية السوري لسنة 1954.

المواقع الالكترونية

خالد ممدوح إبراهيم، الدليل الرقمي الانترنت، في جرائم المعلوماتية، مقال منشور على http://www.f-law.net

محمد صفوت ،استخلاص الدليل الجنائي الرقمي ،مجلة العالم الرقمي ،على الموقع الالكتروني : http://www.al-jazirah.com/digimag/28032004/wr46.htm

متاح على الموقع الإلكتروني :

-http://forum.sh3bwah.maktoob.com/t178434.html.

، تاريخ زيارة الموقع 2017/1/25 م

originating IP x صحة تحتوي على عناوين IP شركة البريد و IP الشخص مرسل الرسالة في شركة هوتمايل

– Received صحة تحتوي على عناوين IP شركة البريد و IP الشخص مرسل الرسالة في شركة ياهو

الفهرس

إهداء

الشكر

قائمة المختصرات

مقدمة 01

الفصل الأول : الإطار القانوني للخبرة الفنية المتعلقة بالجرائم الالكترونية 07

المبحث الاول : القواعد القانونية التي تحكم عمل الخبير في الجرائم المعلوماتية 08

المطلب الأول ماهية الخبرة واهميتها وانواعها 08

الفرع الاول ماهية الخبرة واهميتها.....08

الفرع الثاني انواع الخبرة في المجال المعلوماتي 11

المطلب الثاني شروط صحة اعمال الخبرة ومدى حجيتها 14

الفرع الاول : شروط صحة اعمال الخبرة وضوابطها.....14

الفرع الثاني مدى حجية تقرير الخبير 17

المبحث الثاني : القواعد الفنية التي تحكم عمل الخبير في مجال الجرائم المعلوماتية ..18

المطلب الاول الصعوبات التي تواجه عملية الاثبات الجنائي واساليب عمل الخبير المعلوماتي 18

الفرع الاول : الصعوبات التي تواجه عملية الاثبات الجنائي في الجرائم المعلوماتية 18

الفرع الثاني : اساليب عمل الخبير المعلوماتي 20

المطلب الثاني استخلاص الدليل الرقمي 23

الفرع الاول عملية استخلاص الدليل الرقمي 23

الفرع الثاني حجية الدليل الرقمي امام القضاء 27

الفصل الثاني: القواعد الاجرائية في استخلاص الدليل الالكتروني والقيمة القانونية له 30

المبحث الأول: القواعد الاجرائية في استخلاص الدليل الالكتررونيي.....31

المطلب الأول: القواعد الاجرائية التقليدية في استخلاص الدليل الالكتررونيي.....31

الفرع الأول: التفتيش.....31

الفرع الثاني: استخلاص الدليل في الجريمة الإلكترونية.....33

الفرع الثالث : الخبرة في إثبات الجريمة الإلكترونية.. 36

المطلب الثاني: القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني وصعوبات .

التحقيق في الجريمة الإلكترونية... 40

الفرع الأول: القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني .....40.

الفرع الثاني: معوقات وصعوبات التحقيق في الجريمة الإلكترونية.....47

المبحث الثاني : القيمة القانونية للدليل الالكتروني في مجال الاثبات الجنائي 50

المطلب الأول: مشروعية الدليل الالكتروني.....51

الفرع الأول: مشروعية الدليل الإلكتروني.....52

الفرع الثاني : مشروعية الحصول على الدليل الالكتروني.....59

المطلب الثاني : حجية الدليل الإلكتروني في الإثبات الجنائي 63

الفرع الأول: حجية الدليل الإلكتروني في الإثبات الجنائي 63

الفرع الثاني: موقف المشرع الجزائري من الدليل الالكتروني في مجال الإثبات الجنائي. 68

الخاتمة. **74**

قائمة المراجع **77**

الفهرس.....**83**

مـلخص مذكرة الماستر

يكتسي الخبرة التقنية في مجال إثبات الجريمة الالكترونية ية من الجرائم المستحدثة التي شغلت أجهزة العدالة ، حيث يعتبر إثبات هذه الجرائم من أهم المشاكل التي تواجه سلطات التحقيق نظرا لتكوينهم القانوني البحث من جهة ،ونقص خبرتهم و كفاءتهم الفنية من جهة أخرى ، مما يتطلب الاستعانة بالخبراء متخصصين في مجال الحاسب الالي و الأنترنت مما يساعدهم على كشف الأدلة و الحفاظ عليها ن للطبيعة الخاصة و المتميزة لهذه الجرائم.

الكلمات المفتاحية :

1/ الجريمة الإلكترونية 2 / أجهزة العدالة 3/ 4 الخبير / 5 التقني6/ الخبرة التقنية

Abstract of The master thesis

He acquires technical expertise in the field of proving cybercrime, one of the new crimes that has preoccupied the justice system, as proving these crimes is considered one of the most important problems facing the investigation authorities due to their legal research training on the one hand, and their lack of experience and technical competence on the other hand, which requires the assistance of specialized experts. In the field of computers and the Internet, which helps them uncover and preserve evidence of the special and distinct nature of these crimes.

key words :

1/ Cybercrime 2/ Justice agencies 3/ 4 The expert / 5 The technician 6/ Technical expertise