جامعة عمار ثليجي الأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

الحماية الجنائية لجرائم الآداب المرتبطة بتقنية المعلومات

مذكرة مكملة في إطار مقتضيات نيل شهادة الماستر في الحقوق

تخصص: قانون جنائي

اعداد الطالب :

- **فضيل رابحي**

إشراف :

د. عبد الوهاب ملياني

لجنة المناقشة

الدكتورة يوسفي مباركة	**رئيســـــــا**
الدكتور ملياني عبد الوهاب	**مشرفا ومقررا**
الأستاذ محمد النذير بن عرفة	**مناقشـــــــا**

السنة الجامعية 2018/2017

شكر وعرفان

حمدا يوافي نعمه ويدفع نقمه ويكافئ الحمد لله رب العالمين مزيده.

لا ندعي أننا حققنا القصد وأشرفنا على الغاية فذاك طموح نسعى إليه نسأل الله تحقيقه وبلوغ مرتبته ولا شك أن المشروع لا يخلوا من ملاحظات وشفيعنا في ذلك سلامة القصد وحسن النية وبذل الجهد.

أتقدم بالشكر الجزيل إلى الدكتور المشرف عبد الوهاب مليا ني الذي لم يبخل علي بشيء وتحمله عناء هذه المذكرة

وإلى كل أعضاء لجنة المناقشة

الدكتورة يوسفي مباركة و الدكتور محمد نذير بن عرفة على تكرمهم بقبول مناقشة هذه المذكرة

كما لا يفوتني في هذا المقام أن أتوجه بالشكر إلى أساتذة قسم الحقوق

وإلى كل من ساهم من قريب أو من بعيد لإتمام هذا البحث

والحمد لله اولا وأخيرا على التوفيق

الجريمة ظاهرة تاريخية، ترتبط بالوجود الإنساني وتواكب تقدم الإنسان وارتقاءه في كل أطواره الحضارية ، ومع دخول القرن الواحد و العشرين اتسعت دائرة الجريمة بانتشار نوع جديد من الجرائم، يُرتكب عبر الوسائط الإلكترونية، مواكباً لنشوء نظم الحواسيب وتطورها ونشوء شبكاتها العالمية وثورة التكنولوجيا المعلوماتية؛ وقد أكدت الدراسات القانونية الحديثة أن الجرائم الإلكترونية تنطوي على مخاطر جمّة، سياسية واقتصادية واجتماعية، وتلحق بالمؤسسات والأفراد خسائر باهظة، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، وتطول المعلومات الحيوية، وبرمجيّات التشغيل الحديثة، والبيانات الرقمية، وسلامة النفوس، ورؤوس الأموال، والحياة الخاصة للأفراد، والجريمة الأخيرة هي موضوعنا. وكما يُطوّر الناس علاقات إنتاجهم ووسائله، يطور المجرمون علاقات جرائمهم ووسائلها، ويحاكون المفاهيم الحضارية السائدة في مجتمعاتهم، كونهم جزءاً أصيلاً منها يتعيّش على الجريمة، بصفتها مورداً اقتصادياً ومنهج حياة. ويستعين المجرمون بالوسائل الإلكترونية في ارتكاب جرائمهم؛ لما تتسم به تلك الوسائل من دقة بالغة في الوصول إلى النتائج الجرمّية المرجوة، ولأنها لا تخلف آثاراً خارجية ظاهرة؛ فهي تنصبّ على البيانات والمعلومات المخزنة في نظم المعلومات والبرامج، مما ينفي وجود أي أثر مادي يمكن الاستعانة به في إثباتها، إلا بفحص الدليل الرقمي، الذي يمكن إخفاؤه أو تشويهه أيضاً. وبذلك، ففي الجرائم المعلوماتية ينتفي العنف وسفك الدماء، ولا وجود لآثار اقتحام أو كسر أو سرقة للأموال المادية، وإنما تنحصر آثارها في عالم غير مرئي، يتم فيه نقل المعلومات بواسطة النبضات الإلكترونية أو الذبذبات، أو نسخ أرقامٍ ودلالات أو تغييرها أو محوها من السجلات. وتُرتكب هذه الجرائم في الخفاء، وعادة ما تتم عن بعد، فلا يظهر الفاعل على مسرح الجريمة، وتتباعد المسافات بين المجرم والضحية، وهذه المسافات لا تقف عند حدود الدولة، بل تمتد إلى النطاق العالمي، إلى دول أخرى، مما يضاعف صعوبة كشفها وإثباتها وملاحقتها قضائيا[1].

و تعد جرائم الجنسية من أكثرها انتشارا و تطورا بحيث تؤكد آخر الأخصائيات المقدمة من طرف جهاز الدرك الوطني أن ثلاثة جرائم متعلقة بالإخلال بالآداب العامة تسجل كل يوم عبر الوطن، بالإضافة إلى

[1]– عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية دراسة قانونية مقارنة دار الثقافة والنشر والتوزيع سنة2014 ص64

504 قضية متعلقة بممارسة الدعارة و192حالة اغتصاب خلال.2008 وتشير الأرقام المقدمة من طرف مصالح الدرك الوطني إلى الانتشار الكبير لجرائم الآداب العامة في المجتمع الجزائري، حيث أضحت الاعتداءات الجنسية حدثا تتناقله الألسنة وقاعات المحاكم يوميا. وتحولت هذه الممارسات إلى واقع يفرض نفسه في مجتمع محافظ، فالأرقام التي تتحدث عن الاغتصاب تدق ناقوس الخطر، حيث تمكنت مصالح الدرك الوطني في الثمانية أشهر الأخيرة من 2008 إلقاء القبض على 234 شخص ومعالجة 192 قضية من هذا النوع، وتم إحصاء 880 ضحية من بينهم 545 أنثى، والملاحظ أن المجرمين لا يفرقون بين الذكر والأنثى فالمهم بالنسبة لهم هو إشباع رغباتهم الجنسية لهذا أصبحت قضايا الاغتصاب والدعارة تملأ المحاكم .

ويبدو أن الانحلال الخلقي بدأ ينتشر في المجتمع أمام الأرقام التي سبق الإشارة إليها، حيث لم تعد الكثير من العائلات تؤمن على بناتها وحتى أبنائها في وقت لم يعد فيه المجرمون يفرقون بين الصبي والفتاة، أما الاختطافات التي تنتهي دائما بقتل الأطفال فتبين تحقيقات مصالح الأمن تعرضهم للاعتداءات الجنسية قبل أن يقوم المختطف بقتلهم، وقد ملأت صورهم صفحات العديد من الجرائد الوطنية وشغلت أخبار الاختطاف والاعتداءات الجنسية المواطنين لمدة طويلة، لدرجة أرغمت المواطنين على اصطحاب أبنائهم إلى المدرسة، وإرجاعهم إلى البيت خوفا من تكرر حالات الاعتداء على الأطفال.[1]

حيث قالت إن محاربة هذه الظاهرة هي مهمة المجتمع والسلطات ويجب أن تُجنّد لاستئصالها الوسائلُ القانونية والاجتماعية والثقافية. يأتي هذا الجدل مع تنامي ظاهرة اختطاف الأطفال في الجزائر حيث تشير الإحصائيات الرسمية إلى اختطاف أكثر من 841 طفلا جزائريا منذ عام ألفين، وقد تم الاعتداء أو قتل 367 طفلا. عمليات الخطف عادة ما تقوم بها شبكات إجرام منظمة وتقوم بطلب الفدية من عائلة الطفل مقابل تسليمه لها. فيما شهدت عمليات اختطاف أخرى نهايات مأسوية كاغتصاب الأطفال ثم قتلهم ورميهم في مناطق مهجورة. وقد شهد عام 2008 عشرين حالة اختطاف. أربعة عشر من هؤلاء الأطفال تعرضوا للاغتصاب ثم أُعيدوا إلى عائلاتهم[2] .

[1]–سهام حواس حوادث الاغتصاب والدعارة تتصدر قوائم الجرائم في الجزائر جريدة الحوار نشر يوم 11 / 01 / 2009

[2]– سليمان بصوفه – بيوت دعارة محاربة ظاهرة اغتصاب لأطفال في الجزائر اول يومية الكترونية – صدرت من لندن 21 ماي 2001

و من هنا تظهر لنا **أهمية الدراسة** التي يمكننا أن نوجزها إظهار صور جرائم الآداب العامة الواقعة في نطاق تكنولوجيا المعلومات الحديثة فكما أن جرائم الآداب العامة تتحقق صورها في الواقع المادي الملموس ، كذلك فهذه الجرائم من المتصور أن تكون تقنية المعلوماتية وسيلة من وسائل التي قد ترتكب بها من قبل فاعل يمكن أن يكون بعيدا مئات أو حتى ألاف الأميال عن الضحية في وقت وقوع الجريمة

و لهذا فإن **أسباب اختيارنا لهذا الموضوع** تكمن في:

سبب ذاتي يتمثل في رغبتنا في الخوض في غمار هذا البحث لتقوية معرفتنا القانونية المتخصصة ، بالإضافة إلى رغبتنا في دراسة هذا الموضوع نظرا لقربه من واقعنا الذي انتشرت فيه استخدامات المعلوماتية و التي ما فتئت تستخدم في الأعمال الانحلال الخلقي و التي منها مجال دراستنا.

هذا بالإضافة إلى **السبب الموضوعي** المتعلق بالرغبة في دراسة هذا الموضوع للخوض فيه من الناحية القانونية لمعرفة المعالجة التشريعية لمثل هذه الجرائم التي تستخدم فيها تقنية المعلوماتية في ارتكابها.

و عليه يمكننا أن نقترح **الإشكالية** التالية : **كيف لقانون العقوبات أن يواجه جرائم الآداب العامة إذا ما وقعت بوسائل معلوماتية ، أو بمعنى آخر هل من فعالية لنصوص قانون العقوبات مواجهته لجرائم الآداب العامة الواقعة عبر وسائل تقنية المعلوماتية ؟**

التي سنقوم بدراستها باستخدام الدراسة القانونية التحليلية التي اعتمدنا فيها المنهج الوصفي من خلال تعريف مختلف الجرائم محل الدراسة و ذكر أركانها المطلوبة قانونا.

بينما استخدمنا المنهج الاستنتاجي الذي اعتمدنا عليه من خلال دراسة النصوص القانونية لنستنتج منها موقف المشرع من الجرائم محل الدراسة.

و للإجابة على تلك الإشكالية يمكننا وضع **الخطة المنهجية** التالية التي قسمناها إلى فصلين بحيث خصصنا الفصل الأول إلى الإطار الموضوعي لجرائم الآداب العامة المرتبطة بتقنية المعلوماتية و بدوره قسمناه إلى مبحثين بحيث تطرقنا في المبحث الأول طبيعة القانونية للجريمة المعلوماتية ، في حين خصصنا المبحث الثاني منه تأطير المشرع العقابي لجريمة الآداب العامة المتصلة بالمعلوماتية ، بينما تطرقنا في الفصل الثاني من الدراسة المعنون الإطار الاجرائي لجرائم الآداب العامة المرتبطة بتقنية المعلوماتية بحيث يتضمن فكرتين فخصصنا الفكرة الأولى منا للمبحث الأول المعنون ب التحديات الأمنية ذات الصلة بمكافحة جرائم المعلوماتية ، بينما نتناول الفكرة الثانية في المبحث الثاني من هذا الفصل المعنون ب الدليل التقني بين الإشكالات الإجرائية و قبول مشروعيته و مصداقيته .

من الواضح في عصرنا هذا المعروف بعصر المعلوماتية ونظرا للتزايد المستمر في الاستخدامات كانت معروفة فقط في الواقع المادي الملموس، الا أن الأمر أصبح خطيرا لأنها أصبحت واقعة كذلك في هذا العالم الافتراضي بأشكال وصور هي نفسها التي كانت مستخدمة في الواقع العادي المعاش والمختلفة لتقنية المعلوماتية التي قد تؤدي للاستخدام المشروع لها إلى ارتكاب جرائم الآداب العامة وسنقوم من خلال هذا الفصل المعنون ب الإطار الموضوعي لجرائم الآداب العامة المرتبطة بتقنية المعلوماتية بدراسة الطبيعة القانونية للجريمة المعلوماتية كمبحث أول والذي نتطرق فيه لمفهوم الجريمة المعلوماتية كمطلب أول ، ومن ثم صور جرائم المعلوماتية بوجه عام على ضوء قانون العقوبات وهذا كمطلب ثاني من هذا المبحث.

ونتطرق في المبحث الثاني من هذا الفصل لتأطير المشرع العقابي لجرائم الآداب العامة المتصلة بالمعلوماتية بحيث نخصص المطلب الأول منه لمدى انطباق الجرائم التقليدية للآداب العامة بوجود وسيلة معلوماتية ، بينما خصصنا المطلب الثاني منه لمدى انطباق النصوص الخاصة للجريمة المعلوماتية إذا ما تعلق الأمر بالآداب العامة

المبحث الأول: الطبيعة القانونية للجريمة المعلوماتية

من المهم وعلى إثر دراستنا للجرائم الآداب العامة المرتبطة بالمعلوماتية أن نتطرق لمفهوم الجريمة المعلوماتية كخطوة أساسية لفهم هذه الجريمة من كل جوانبها، مع وجوب كشف مختلف الأساليب المستعملة في ارتكابها كمطلب أول، ومن ثم نتطرق إلى الصور التي عالج بها المشرع الجنائي الجزائري الجريمة المعلوماتية لنتبين موقفه منها وهذا وفق المطلب الثاني لهذا المبحث ، وهو ما سندرسه كما يلي:

المطلب الأول: مفهوم الجريمة المعلوماتية

سنحاول من خلال دراستنا للجريمة المعلوماتية التطرق إلى تعريف الجريمة المعلوماتية وأهم الخصائص المميزة لها في الفرع الأول ، ومن ثم نتطرق إلى الوسائل المستخدمة في إرتكاب الجريمة المعلوماتية كفرع ثاني ، وهذا وفق ما يلي :

الفرع الأول: مدلول الجريمة المعلوماتية

أولا: تعريف الجريمة المعلوماتية

يصعب الاتفاق على تعريف موحد للجريمة المعلوماتية، حيث اختلفت الاجتهادات في ذلك اختلافا كبيرا، ويرجع السبب في ذلك إلى سرعة وتيرة التطور التقني من جهة، وشكل تدخل تقنية المعلومات فيها من جهة أخرى، حيث يذهب البعض من الفقهاء إلى ترجيح عدم وضع تعريف محدد للجريمة المعلوماتية بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني .

كما أن الدراسات في مجال جرائم المعلوماتية بإعتبارها نمط جديد من الإجرام إختلفت في الوصول إلى تعريف موحد ومحدد يتلاءم مع طبيعتها ، حتى قيل عنها أنها تقاوم التعريف[1] .

ويمكن أن نعرف عامة الجريمة المعلوماتية حسب الدور الذي يلعبه النظام المعلوماتي، فيكون تارة بيئة لها، وتارة أداة لارتكابها.

أ: الجريمة المعلوماتية عندما يكون النظام المعلوماتي بيئة لها

وتتحقق هذه الحالة عندما تقع الجريمة على المكونات المعلوماتية غير المادية مثل البرامج المستخدمة والبيانات والمعطيات المخزنة داخل النظام، كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم[2].

---

[1]– هشام محمد فريد رستم ، قانون العقوبات و مخاطر تقنية المعلومات ، ب ط ، منشورات الحلبي الحقوقية ،بيروت ،2000، ص29.

[2]– فتوح الشاذلي و عقيقي كامل عقيقي ، جرائم الكمبيوتر ، ب ط ، منشورات الحلبي الحقوقية ، بيروت ، 2003 ، ص 47.

وبالتالي فالنظام المعلوماتي يكون هدفا للجريمة، ومن أوضح صوره الإجرامية عندما تكون السرية أو السلامة أو التوافر هي التي يشملها الاعتداء، بمعنى أن يوجه الهجوم من نظام معلوماتي إلى نظام معلوماتي آخر بقصد المساس بسرية أو المساس بسلامة أو محتوى النظام المعلوماتي ، أو تعطيل قدرة وكفاءة النظام في القيام بأعماله، كعرقلته أو إبطاء سرعة معالجته للمعطيات، وقد يكون الهدف هو محتويات النظام المعلوماتي وبشكل خاص المعطيات المدرجة به أو السيطرة على النظام دون موجب قانوني أو دون إذن صاحب الحق في إصداره ومراجعة معطياته[1].

ويمكن أن نتصور هذه الصورة أيضا في حالة تخزين البرامج الخبيثة فيه أو في حالة استخدامه لنشر المواد الإباحية أو استعماله كأداة للاتصال السري بين مروجي المخدرات وأنشطة شبكات الهجرة السرية وفضاء لتبييض الأموال عبر دور القمار الافتراضي أو الرهان[2].

ب: الجريمة المعلوماتية عندما يكون النظام المعلوماتي وسيلة لارتكابها

وتتحقق هذه الحالة عندما يستخدم الفاعل النظام المعلوماتي كوسيلة لتنفيذ جرائمه، سواء وقع الاعتداء على الأشخاص، كانتهاك حرمة الحياة الخاصة أو تهديد الحياة، كجرائم القتل عبر الدخول إلى البيانات الطبية والعلاجية والتلاعب بها أو عرقلة عمل الأجهزة الطبية وإحداث خلل في أنظمتها، أو عبر التحكم ببرمجيات الطائرات أو السفن بشكل يؤدي إلى تدميرها وقتل ركابها.

ويقع الاعتداء أيضا على الأموال كالسرقة والاحتيال وغيرها، وهي جرائم يصبح فيها النظام المعلوماتي أداة للجريمة لارتكاب جرائم تقليدية كما في حالة استغلاله للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عملية التزييف والتزوير، أو في الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها بشكل احتيالي، حتى أن النظام المعلوماتي يسخر في التجسس بالوسائل الالكترونية[3].

ثانيا: أهم خصائص الجريمة المعلوماتية

تمتاز الجريمة المعلوماتية بخصائص معينة تشكل علامات فارقة مع باقي الجرائم التقليدية، والتي تصعب في نفس الوقت مهمة مكافحتها، فإن كانت الدول قد طورت مع مرور الزمن آليات فعالة لمكافحة الجرائم التقليدية، فليس الأمر كذلك بالنسبة للجريمة المعلوماتية نظرا للخصائص الفريدة التي تميزها، وسنقوم بذكر أهم تلك الخصائص وفق ما يلي :

[1] – هشام محمد فريد رستم ، المرجع السابق ، ص 30 .

[2] –نعيم مغبغب ، حماية برامج الكمبيوتر، ب ط ، منشورات الحلبي الحقوقية ، بيروت ، 2009، ص 144 و ما بعدها

[3] – فتوح الشاذلي و عقيقي كامل عقيقي ، المرجع السابق ، ص 48 .

أ: الطابع الدولي للجريمة المعلوماتية

هي جريمة تتسم بالسرعة، فالاتصال بين جهازين داخل الشبكة العنكبوتية مثلا يتم خلال ثواني فقط ولو كانا يبعدان عن بعضهما بآلاف الكيلومترات، فالمسافة لا تشكل عائقا في أن يصدر الاعتداء من مجرم في دولة ويحدث أثره على ضحية أو عدة ضحايا في دولة أو دول أخرى، مما يعطي الجرائم المعلوماتية بعدا دوليا عابرا للحدود السياسية والجغرافية، الشيء الذي يعقد مسطرة المتابعة والقانون الواجب التطبيق ويحد الجهود المبذولة لمكافحتها[1].

ولهذا فإن عدد الضحايا المحتملين جد كبير، بحيث يستحيل توقع الضحية التالية لمجرم معلوماتي ينتقل بين دولة وأخرى بكل حرية ودون أن يعبر الحواجز الجمركية أو أن يخضع للتفتيش ليقصد ضحايا مختلفين، ويستعين المجرمون ببرامج معلوماتية تقوم بمسح أعداد هائلة من الأنظمة المعلوماتية التي تنتمي إلى دول مختلفة في غضون وقت قصير جدا، لتحديد الأجهزة التي تعرف ثغرات أمنية أو منافذ مفتوحة يمكن استغلالها لتنفيذ الهجمات[2].

وتطرح هذه الخاصية إشكالية كبرى عندما ينحدر المجرم المعلوماتي من دولة لا تجرم مثل هذه الأفعال مما لا يترك مجالا لمتابعته، وهنا تظهر الحاجة الملحة للممارسة ضغوط سياسية على مثل هذه الدول لكي ترقى بمستوى تعاونها الدولي في مواجهة الجريمة المعلوماتية[3].

ويختلف الطابع الدولي للجرائم المعلوماتية سهولة في التعاون على تنفيذها، بحيث لا يجد المجرمون صعوبة في الاتصال بأشخاص آخرين سواء داخل نفس البلد أو خارجه، لهم نفس التوجهات الإجرامية ويركزون على نفس الأهداف، بحيث يتم توزيع المهام بينهم ليقوم كل شخص بالدور المنوط به انطلاقا من التقنيات التي يجيدها حتى تتبدد المصاعب أمامهم، ولنكون أمام خطورة إجرامية كبرى لمجموعة منظمة، تتسم بالقوة والفعالية في اختراق نظم الحماية.

وعلى هذا الأساس فربط العلاقة بين الضحية والمجرمين تصبح دوم جدوى لتعدد المتدخلين وغياب وحدة الأسلوب في الهجمات طبقا لدور كل مجرم حسب الحالة.

وقد يتواطأ مع المجرمين أشخاص قريبون من الضحية أو يعملون لحسابها للتستر على الهجوم وتغطية الاضطرابات الظاهرة مع تقديم كل المعلومات التي تكون مفيدة في نجاح العملية[4].

---

[1]– نعيم مغبغب ، حماية برامج الكمبيوتر، ب ط ، منشورات الحلبي الحقوقية ، بيروت ، 2009، ص 218 .

[2]– يطلق على هذه البرامج بالغة الفرنسية "Scanner".

[3]– هشام محمد فريد رستم ، المرجع السابق ، ص 31 .

[4]– نائلة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية منشورات الحلبي ، ب ط ، بيروت ، 2005 ، ص 48 .

ب: الصعوبات الخاصة باكتشافها وإثباتها

تمتاز الجرائم المعلوماتية بسهولة إخفاء آثارها، ويساعد على هذه العملية العنصر المعنوي أي المجال الغير المادي الملموس لهذه الجرائم، فهنالك مثلا برامج معلوماتية متخصصة في إخفاء التغيرات التي تلحق الحاسوب خلال الإصابة بفيروس خبيث وهذا عبر محو آثار الإقتحام، أو آثار الاتصال بالشبكة ومفاتيح السجلات، وبهذا الشكل فهي تمنع أي كشف محتمل من قبل المستخدم قصد الحفاظ على وجوده لأطول فترة ممكنة.

وإن كانت الجريمة في حالات عدة لا تترك آثارا، أو من الصعب اكتشافها كما هو الحال مع سرقة المعلومات ونسخها من حاسوب الضحية، أو عمليات الاصطياد التي لا تثير شكوك المستخدم العادي، فإن ذلك يحجب إمكانية كشف درجة استفحال هذه الظاهرة ويحول جون إنجاز إحصائيات تمكن من تقييم درجة خطورتها الحقيقة وقيمة الخسائر التي تخلفها[1].

كما أن مسرح الجريمة في الجريمة المعلوماتية جد مختلف عن مسرح الجريمة في الجرائم الأخرى، فليست هنالك آثار تشير للفاعل من قبيل بصمات الأصابع والحمض النووي أو دلائل أخرى عن سلاح الجريمة، بل تحتاج عملية إثبات الجريمة الإلكترونية إلى متخصصين في البحث المعلوماتي وهم أشخاص مكونين لرفع الدليل الرقمي من الحواسيب والذي يثبت وقوع الجريمة، شكلها والأضرار التي خلفتها مع التوصل إلى مرتكبها[2].

ج: المهارات التقنية المطلوبة في إرتكابها و قلة الوعي بخطورتها

تحتاج الجرائم المعلوماتية إلى مهارات تقنية لارتكابها فهي لا تحتاج إلى قوة بدنية بل إلى الذكاء والدهاء. وما دام أن الحاسب الآلي يلعب دور أداة الجريمة، فإن الذكاء الاصطناعي يشجع على التنفيذ الآلي للهجمات دون تدخل العنصر البشري، أي أن تنفيذ الهجمات يمكن أن يكون أوتوماتيكيا من خلال برمجة الحاسوب لينفذ الأوامر المسجلة بذاكرته في وقت معين ولو عند غياب المبرمج.

وتعرف تقنية المعلوماتية تطورا كبيرا واكتشافات متوالية تجعل أسلحة المجرم المعلوماتي تتجدد وتتغير وفق مستوى التطور التكنولوجي الذي يعرفه مجال المعلوماتية، ويجعل الجريمة المعلوماتية خاضعة لحس الابتكار والإبداع التقني الذي يسبق أدوات المكافحة[3].

---

[1]– نعيم مغبغب ، المرجع السابق ، ص 149.

[2]–هشام محمد فريد رستم ، المرجع السابق ، ص 32.

[3]– هلالي عبد الإله أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، ب ط ، درا النهضة العربية ، القاهرة ، 1998 ، ص 75.

كما أن الضحية في الجرائم المعلوماتية من مستعملي هذه التقنية ، بحيث يجهل جزء كبير منهم أبسط المعارف عن مجال المعلوماتية وتقنيات الاتصال بالشبكات، ويقل وعيهم بالأخطار التي قد تنجم عن الاتصال بشبكة الانترنت وطرق الحماية منها، فنجد حواسيب بدون برامج حماية، الاتجاه نحو تحميل كل شيء بدون انتقاء أو معرفة المصدر، التلقائية في ردة الفعل وعدم توخي الحذر أثناء مراجعة رسائل البريد الإلكتروني، وغياب الجدية في التعامل مع التحذيرات من البرامج الضارة، ناهيك عن الاستهانة بما قد يستفيد منه المجرم المعلوماتي جراء مهاجمة الحاسوب على أن ذلك عند أغلب الناس لا يتجاوز العالم الافتراضي[1].

لهذا و على إثر ما سبق فإن الجريمة المعلوماتية تتميز بطبيعتها الخاصة ، فهي تنفرد بمقومات خاصة تستدعي مواجهة مختلفة عن بقية الجرائم الأخرى لأجل مكافحتها.

الفرع الثاني : الوسائل المستخدمة في ارتكاب الجريمة المعلوماتية

لا بد من الإشارة إلى أنه لا يمكن تحديد قائمة نحصر فيها جميع الوسائل التي تستخدم لارتكاب الجريمة المعلوماتية، على اعتبار أن هذا الحقل يعرف تطورا متسارعا ومتجددا بشكل كبير، ولهذا لا يسعنا إلا أن نذكر أهم التقنيات الأكثر انتشارا، ويتعلق الأمر هنا بأساليب التسلل والإصطياد ، وأساليب الحجب.

أولا: أساليب التسلل والإصطياد

يعد فيروس الحاسوب من بين البرامج الخبيثة التي تنتشر بسرعة عبر إلحاق نفسها ببرامج أو ملفات أخرى حاضنة، فتبدأ بالعمل بمجرد عمل الملف الحامل لها، وتتكاثر بطريقة ذكية سواء داخل نفس الجهاز وكذا من جهاز لآخر بتدخل من العنصر البشري، إما عبر وسائل التخزين مثل ذواكر الفلاش والأقراص المدمجة أو عن طريق شبكة الانترنت بواسطة البريد الالكتروني، البرامج المقرصنة أو عبر التحميل المباشر من المواقع الإلكترونية.[2]

هذا بالإضافة إلى دودة الحاسوب التي تعد من البرامج المضرة المنتشرة بسرعة أكبر من الفيروسات لأنها بخلاف هذه الأخيرة تعتمد على نفسها في التكاثر أي دون الحاجة إلى ملفات حاضنة، وتنتقل من جهاز لآخر دون تدخل للعنصر البشري، بإرسال نفسها إلى كل العناوين الموجودة على الحاسوب بواسطة البريد الإلكتروني، ويساعدها في ذلك الثغرات الأمنية التي تعرفها مجموعة من البرامج وأنظمة التشغيل.

[1] هشام محمد فريد رستم ، المرجع السابق ، ص 31 .

[2] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت، ط1، دار النهضة العربية، القاهرة، 1999، ص45.

إضافة إلى ما سبق نجد حصان طروادة الذي يعتمد في عمله على العلاقة بين جزأين هما العميل Client والخادم Server فصانع البرنامج يعمل على إلحاق الخادم بمجموعة من الملفات والبرامج النافعة المعروفة[1]، ويؤدي تحميلها من قبل المستخدم وتشغيلها إلى تحميل الخادم واستقراره في الجهاز دون علم الضحية، ليفتح ثغرة في الجهاز تمكنه من استقبال الأوامر من العميل.

كما يدخل في نفس الإطار برامج التجسس المجانية المتوفرة على شبكة الانترنت، التي تركز على أداة جد مهمة في التواصل مع جهاز الحاسوب ، بحيث يستعمل هذا البرنامج بشكل كبير للتجسس على الأشخاص وكل الأجهزة التي تتوفر على معلومات سرية وحساسة ، بحيث يكون ذلك من خلال الاستفادة مجانا من خدمات بعض البرامج المفيدة يجب قبول تحميل برنامج إعلاني ملحق بها، وهي طريقة غير مباشرة لفرض تنزيل برامج التجسس ، ما يعد انتهاكا لخصوصية المستخدمين واستعمالا لمعلوماتهم في سياسات تسويقية وإجراء إحصاءات دون موافقة صريحة منهم[2].

فعمل شبكة الانترنت يرتكز على الربط بين اسم النطاق والرقم العشري المخصص له من خلال خوادم معدة لهذا الغرض، فعند كتابة عنوان موقع معين على متصفح انترنت يقوم الجهاز بإرساله إلى خادم أسماء النطاقات للاستفسار عن العنوان الخاص بهذا الموقع، فيرد عليه بعنوانه إذا كان مسجلا لديه، فيقوم الجهاز بالتوجه إلى هذا العنوان لطلب الموقع ليبدأ بالظهور.

ومن أجل تسريع هذه العملية، يقوم خادم أسماء النطاقات مؤقتا ولمدة محدودة بحفظ وتخزين نتائج الاستفسارات السابقة في ملفات معينة ، وهنا ابتكرت طريقة احتيالية تتمثل في اختراق الخادم والعبث بهذه الملفات قصد تغيير وجهة المستخدم من الموقع الذي يرمي تصفحه إلى موقع آخر مزور يشبهه، عبر تغيير الرقم العشري للموقع الأصلي برقم آخر للموقع المزور[3].

---

[1] يلحق خادم حصان طروادة في أغلب الحالات بالملفات والبرامج التي تعرف إقبال كبير لمستخدمي شبكة الإنترنت كاللعب الالكترونية، برامج الدردشة المعدلة، حافظات الشاشة (Screen Saver) وكل ما قد يثير فضول المستخدمين ويشد انتباههم من صور النجوم ومقاطع الفيديو النادرة أو تلك المخلة بالآداب وكل ما يمكن توسيع نطاق الانتشار والرفع من عدد الضحايا.

[2] – نعيم مغبغب ، المرجع السابق ، ص 140 .

[3] – نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية منشورات الحلبي ، مرجع سابق ، ص 52

ثانيا: أساليب الحجب

ترتكز أساليب الحجب على المساس بسلامة الأنظمة وتوفرها العادي على شبكة الانترنت، بسلوك هجمات حجب تأثر مباشرة في الموقع وأخرى تتمثل في مهاجمة الخوادم المحتضنة للمواقع مما يؤثر سلبا عليها بطريقة غير مباشرة.

ومن بين تلك الأساليب نجد أسلوب سرقة كلمات المرور التي تتعدد طرقها فهناك مجموعة من البرامج توفر إمكانية مراقبة حركة البيانات داخل شبكة حواسيب معينة، وقد تستعمل بقصد تعقب أسماء المستخدمين وكلمات المرور خاصة تلك الغير مشفرة كبروتوكول نقل الملفات ، أما بالنسبة بكلمات المرور المشفرة فيعتمد على علم تحليل الشفرات باعتباره علم يهتم بكشف الخطوات الرياضية والمنطقية المتسلسلة التي تم بها التشفير، والبحث في الثغرات التي تشوبها من أجل فك الشفرة، ويهيأ هذا العلم قاعدة مهمة من التقنيات لبلوغ هذا الهدف.

ومثاله هجوم القوة الغاشمة الذي ينطلق من تجربة التركيبات الممكنة عشوائيا الواحدة تلوى الأخرى حتى يتوصل إلى كلمة المرور الصحيحة، ويستغرق ذلك عادة وقتا طويلا، لذا ولتسريع العملية يستعين بهجوم القاموس الذي يوفر قاموس من كلمات المرور الأكثر تداولا، وينجح هذا الهجوم عادة بالنسبة لكلمات المرور ذات عدد قليل من الأحرف وإلا فإن العملية تبوء بالفشل.[1]

ويسعى لمهاجمون في حالات معينة إلى تخمين كلمات المرور بعد تجميع معلومات عن صاحب الموقف فقد يكون تاريخ عيد ميلاده، اسم أحد أطفاله أو حيوانه الأليف، كما يمكن أن يكون رقم لوحة سيارته أو رقم هاتفه النقال.

وكيفما كانت الطريقة فإن الحصول على كلمة المرور يتيح الولوج إلى الموقع الالكتروني، ومن ثم التحكم به بشكل كامل وفتح المجال لحجبه عن المتصفحين، عبر تعديل مكوناته والعبث بملفاته أو إحداث أخطاء في لغة برمجته تؤدي إلى توقف عمله العادي.

هذا بالإضافة إلى العبث بواجهة الموقع التي توصل المهاجم إلى اختراق الحماية المفروضة على المواقع الإلكترونية فتجعله في موقع المسؤول عليه، وتتيح له القدرة على تشويه الصفحة الرئيسية للموقع عبر تعويضها بصفحة يصممها والتي تحمل مقاطع فيديو أو صورة أو رسالة أو كلمات سخرية تشير إلى عملية القرصنة واسم المهاجم المستعار ، بحيث ينتج عن تشويه الموقع حجب المعلومات والخدمة التي يقدمها الموقع. [2]

---

1 - نعيم مغبغب نفس المرجع ،ص142

[2]- ممدوح عبد الحميد عبد الطلب، زبيدة محمد جاسم وعبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، جامعة الدول العربية بجمهورية مصر العربية، ص15.

إضافة إلى ذلك نجد هجمات حجب الخدمة بحيث صمم هذا النوع ليس لتخريب المعلومات أو سرقتها من الخادم الهدف، بل ليستهدف في الأساس شل قدرت النظام المعلوماتي ومنعه من القيام بعمله الطبيعي لأطول وقت ممكن، والذي هو احتضان المواقع، إظهارها وتنظيم عملية تصفحها من خلال شبكة الانترنت.

وتتلخص طريقة الهجوم في إغراق الخوادم باستعلامات متوازية زائفة، تفوق بكثير قدرة المعالج لتستهلكها بالكامل وتتوقف قابليته لاستقبال الطلبات الحقيقية، ما يؤدي إلى تباطؤ كبير في أدائه ما يخلق اضطرابا في سيولة حركة البيانات، إلى حد توقف الخادم بشكل كامل وحرمان المواقع التي يحضنها من الخدمة ما يحجبها بطريقة غير مباشرة.

كانت هذه الهجمات فيما مضى تنفذ بواسطة حاسوب واحد لكن ذلك لم يعد ممكنا أمام ارتفاع القدرة الاستيعابية للخوادم الحديثة وتضاعف قوة المعالجات.[1]

هذا بالإضافة إلى هجمات حجب خدمة الموزع سواء في صيغته البسيطة أو الموزعة والذي يؤدي إلى تعطيل الخوادم، وبالتالي ليس فقط حجب الموقع المستهدف بل حجب كل المواقع التي يحتضنها الخادم خصوصا إذا علمنا أن الشركات أصبحت تنصب عدة مواقع في نفس الخادم لتقليص التكاليف.

وعليه فإن أساليب ارتكاب الجريمة المعلوماتية نجدها متعددة ومتشعبة كما أنها تزداد تعقيدا كلما ظهرت تقنيات جديدة، ولهذا تصعب عملية توفير الحماية لمستخدمي الأنظمة المعلوماتية من دون الحماية القانونية لها وبالخصوص الحماية الجنائية التي توفر اكبر قدر من الحماية لردع كل من يقوم بالإعتداء على تلك النظم .[2]

المطلب الثاني : صور جرائم المعلوماتية بوجه عام على ضوء قانون العقوبات

لا تختلف الجريمة المعلوماتية عن أية جريمة أخرى تقليدية مقررة عن طريق قانون العقوبات من حيث أنها تتطلب لتحقيقها الأركان المتفق على ضرورة تحقيقها في أية جريمة أخرى للتواجد على أرض الواقع ، فبالإضافة إلى ضرورة تواجد الشرط المبدئي في كل جريمة ونقصد هنا الركن الشرعي، فإنه لابد من وجود ركن مادي ملموس يعبر عن ارادة الفاعل بشكل جلي يمكن اثباته ، ومن ثم لابد أيضا من ركن معنوي يعبر عن ارادة مجرم تقنية المعلومات الحديثة ، فالجريمة بشكل عام ، ليست ظاهرة مادية خالصة ، قوامها الفعل وأثاره ، ولكنها كذلك كيان نفسي ، ومن ثم استقر في القانون الجنائي الحديث المبدأ الذي

[1]- عبد العزيز سعد"الجرائم الجنسية في قانون العقوبات الجزائية" – مشار اليهم على الموقع الإلكتروني الخاص بطلاب كلية الحقوق ، جامعة الزقاقين www .Law –Zag. com

[2]- عائشة بن قارة ، حجية الدليل الالكتروني في مجال الإثبات الجنائي (في القانون الجزائري و القانون المقارن)، دار الجامعة الجديدة للطباعة و النشر والتوزيع ،الإسكندرية ، سنة 2010 ص 98

يقضي بأن ماديات الجريمة تنشئ مسؤولية ولا تستوجب عقاب ، ما لم تتوافر إلى جانبها العناصر النفسية التي يتطلبها كيان.

وبالكلام عن الجريمة المعلوماتية ، فإنها تتنوع بشكل كبير على حسب التصنيف الذي يقع على الفعل المرتكب، وعليه فإن الجريمة المعلوماتية لا يمكن حصرها تحت تكييف واحد فقد تشكل هذه الجريمة المرتكبة والموصوفة بجريمة تقنية المعلومات الحديثة واقعة قتل أو قذف ، أو تهديدا ، أو تحريضا أو جريمة جنسية وغيرها العديد من الوقائع الجرمية التي قد تكون اما بشكل مطابق للجريمة التقليدية المقررة عن طريق قانون الجنائي أو قد تكون من الأفعال التي لا ينطبق عليها أي نص قانوني ، أو أنها تحتاج للتوسع في تفسير النصوص القائمة لمواجهتها.

وبناء على ما تقدم فإن الحديث عن جريمة تقنية المعلومات الحديثة ، يقودنا إلى بحث ماهية مبدأ قانون الجرائم والعقوبات ودوره في اطار ظاهرة جرائم المعلوماتية ، وتناول السياسة الجنائية في مواجهة تلك الجرائم الحديثة.

وعليه سوف نعرض في هذا المبحث لمبدأ الشرعية وجرائم المعلوماتية كفرع أول، وللوضع القانوني لجرائم المعلوماتية على ضوء قانون العقوبات الجزائري كفرع ثان.[1]

الفرع الأول: مبدأ الشرعية و جرائم المعلوماتية

لما كان ظهور تقنية المعلومات الحديثة بالشكل الراهن يرجع إلى حداثة العهد بها ، وما ان انتشرت إلا وأدى ذلك إلى انتشار الجرائم المصاحبة لها ، وبهذا الوضع أصبح المشرع أمام جرائم لم تكن لتدور بخلده أنها واقعة بأي حال من الأحوال. وازاء هذه المشكلة فقد كان الحل متمثلا حسب موقف كل مشرع في صورة من الصور الثلاثة الآتية :

الصورة الأولى : وضع نصوص تشريعية لمواجهة جرائم المعلوماتية .

الصورة الثانية : التوسع في تفسير النصوص القائمة لمواجهة مثل هذه الجرائم.

الصورة الثالثة : تطبيق النصوص القائمة على جرائم التقنية الحديثة.

وقد تعامل المعنيون مع الصورتين الثانية والثالثة بحذر شديد وذلك خوفا منهم أن تمس هذه الحلول مبدأ الشرعية الذي عانت الانسانية من أجله الكثير من الآلام وبنت عليه الكثير من الآمال ، والذي يعد من اقدس ما توارثته الإنسانية في عهدها الجديد وعلى اعتابه دانت رقاب الفساد والطغاة والاستبداد وتحكم القضاة.[2]

[1] - عائشة بن قارة، حجية الدليل الالكتروني في مجال الإثبات الجنائي (في القانون الجزائري و القانون المقارن) مرجع سابق ،ص100

[2] شيماء عبد الغني محمد عطا الله ، دار الجامعة الجديدة للطباعة و النشر ، سنة 2010 ص100

أولا : مقتضى مبدأ الشرعية

من المبادئ الأساسية في اغلب التشريعات أنه لتشريع مظهر من مظاهر النشاط فعلا كان أم امتناعا ، أي إعتبار التصرف جريمة معاقبا عليها ، لابد من تدخل المشرع بالنص مقدما على هذا التصرف أو ذلك المظهر بما يفيد النهي عن فعل ، وتقرير عقوبة لمن يخالف النهي (بالإرتكاب) أو لمن يخالف الأمر (بالإمتناع). وذلك وهو ما يعرفه بمبدأ الشرعية الذي يقضي :

- ان التجريم لا يكون إلا من قبل المشرع ، أي بنص قانوني صادر عن سلطة ممثلة للشعب ومختصة بالتشريع ، بيد أن استقلال الشارع بسلطة التجريم لا يمنعه من تفويض هذه السلطة في حدود معلومة للسلطة التنفيذية أو الإدارية ، وغالبية الدساتير تجيز هذا التفويض، ويترتب على هذا المعنى أن القاضي محروم من سلطة التجريم ، خلافا لما كانت عليه الحال في تشريعات العصور الماضية. كما أن الشخص يتمتع بحرية كاملة في تصرفاته فله أن يقوم بكل ما يشاء من تصرفات دون مساءلة أو متابعة من أي شخص إلا اذا قام بالتصرفات المحددة التي حرمها القانون ، لذلك نلاحظ أن القوانين الوضعية جرت على الزام القاضي وبصفة خاصة في المسائل الجنائية ، على ذكر النص القانوني الذي يطبقه على المسائل المطروحة أمامه ، كما لا يمكن له أن ينطق بعقوبة غير محددة بطبيعتها ومقدارها بنص القانون، الأمر الذي يلزم القاضي بالإمتثال لنص عند النطق بالعقوبة ويبعده عن خطر خلق العقوبات. [1]
- انه يتعين على المشرع – أو من يفوض من السلطات التنفيذية أو الإدارية – أن ينص مقدما على ما يعده من الأفعال أو التصرفات جرائم معاقبا عليها ، وأن يجهد في جعل ما يصوغه من هذه النصوص موضحا لخصائص أو مميزات كل جريمة ، فلا يكفي صدور نص التجريم فقط ، بل لابد من تحديد الجريمة تحديدا دقيقا وذكر عناصرها ماهية العقوبات المقررة لها ومقدارها أو كيفية تقديرها. وإذا ركان تدخل الشارع لازما على هذا الوجه ، فالمعنى الذي يستفاد من ذلك هو أن التجريم لا يكون إلا بنصوص مكتوبة ، وينبني على هذا أن النصوص المكتوبة هي المصدر الوحيد في تحديد الجرائم وتقرير العقوبات ، وبهذا يتميز القانون الجنائي في الكثير من فروع القانون الأخرى التي لا تقتصر مصادرها على القانون المكتوب بل قد تستمد من غير ذلك المعرفة مثلا. [2]
- ان التجريم لا يكون إلا للمستقبل ، أي أن القوانين التي تصدر بتجريم التصرفات لا تسري على ما وقع من هذه التصرفات سابقا على تاريخ صدورها ونفاذها. وهذا مفهوم بداهة ، إذ أن العقاب على

[1]- عبد القادر علي قهوجي ، الحماية الجنائية لبرامج الحساب الآلي ، دار الجامعة الجديدة الإسكندرية ، سنة 2010 ، ص 45

[2]- د-فاضل زايدي محمد ،سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، دار الثقافة و النشر و التوزيع ، سنة 2010، ص80

افعال أو تصرفات وقعت قبل نفاذ القانون وهو في حقيقة الأمر تجريم لها بغير قانون ، ما دام الغرض أنه وقت وقوعها لم يكن هناك قانون ينص على عقابها أي تجريمها. ذلك هو مقتضى قاعدة (عدم رجعية القوانين الجنائية) ، وهي في هذا المعنى ليست نتيجة فحسب لمبدأ الشرعية بل لأنها أصل هذا المبدأ و مقتضاه.

ثانيا : نتائج المبدأ بالنظر إلى عمل القاضي الجنائي

لا نزاع في ان مهمة القاضي الجنائي هي تطبيق القانون ، لأن هذا هو عمل القاضي بصفة عامة ولما كان مقتضى مبدأ شرعية الجرائم والعقوبات قصر سلطة التجريم على المشرع أو ما يفوضه من الهيئات التنفيذية أو الإدارية ، وحرمان القاضي الجنائي من تلك السلطة ، فإنه يجب على هذا الأخير أن يمتنع في تطبيقه للقانون الجنائي عن كل ما من شأنه أن يوصله إلى التجريم في صورة ما ، فلا ينبغي له انشاء جرائم جديدة لم ينص عليها ، أو توقيع عقوبات غير مقررة قانونا ، او الزيادة في العقوبات المقررة ، أو الحكم في جريمة لعقوبة مقررة لجريمة أخرى، وعليه فإن نتائج تطبيق مبدا الشرعية تتمثل في :

- حالة انعدام النص : اذا عرض على القاضي الجنائي أمر لا جريمة فيه ، أي لم يرد نص قانوني بتجريمه ، فإنه يتعين عليه أن يقضي بالبراءة مهما كان ذلك الأمر مستهجنا أو معيبا ، بل مهما كان فيه من اعتداء على حق فردي أو على مصلحة الجماعة.[1]

وأبرز النتائج المترتبة على ضرورة التزام التفسير الضيق تتلخص في أن القاضي الجنائي لا يملك أن يطبق القانون بطريقة القياس ، كأن يوقع العقوبة المقررة لفعل معين على متهم بفعل آخر يشابهه لا عقاب عليه بنص صريح ، قياسا لهذه الحالة الأخيرة على الحالة الأولى. وهذه القاعدة هي نتيجة مباشرة لمبدأ الشرعية ، لأن اباحة تطبيق القانون الجنائي بطريق القياس يعني تخويل القاضي الجنائي سلطة التشريع في بعض الاحوال مادام يستطيع عن طريق القياس أن يعاقب على أفعال لم يرد نص صريح بتجريمها. وفي هذا يختلف القاضي الجنائي بطبيعة الحال عن القاضي المدني الذي يستطيع أن يحكم بمقتضى قواعد العدل في حالة انعدام النص ، ويملك من باب أولى اللجوء إلى طريق القياس في تطبيقه للقانون.

[1] – وفي هذا يختلف عمل القاضي الجنائي اختلافا جوهريا من عمل القاضي المدني ، لأن هذا الاخير يملك في حالة انعدام النص أن يحكم بمقتضى (العرف) أو بمقتضى قواعد العدالة. لذا فإن غالبية القوانين المدنية تنص على أنه إذا لم يوجد نص تشريعي يمكن تطبيقه ، حكم القاضي بمقتضى العرف ، فإذا لم يوجد ، بمقتضى مبادئ القانون الطبيعي وقواعد العدالة.

- حالة وجود النص : واذا وجد النص الجنائي الذي يجرم عملا من الأعمال ، فإما أن يكون واضحا وإما أن لا يكون ، فإن كان النص واضحا ، بأن كانت عبارة مفصحة بذاتها عن غرض المشرع بغير تأويل ، التزم القاضي بتطبيقه كما هو أي وفقا لمدلوله وبغير تجاوز لما تحتمله عبارته.

وأما إذا كان النص غامضا ، فإن القاضي الجنائي مطالب بتطبيق القانون على كل حال ، ومن ثم فإنه يجب عليه أن يسعى إلى تأويل النص الغامض ، أي أن يسعى إلى استجلاء الحقيقة المنشودة من المشرع ، وله في هذا السبيل أن يستعين بكل أساليب التفسير ، منطقية أكانت أم لغوية أم تاريخية ، بما سبق النص أو صحبة من الأعمال التحضيرية والمذكرات الإيضاحية والوثائق الرسمية ، وبمقارنة النص الغامض بالنصوص الاخرى التي لها صلة[1].غير أن قاعدة التفسير الضيق تحتم عليه في كل ذلك أن لا يذهب إلى أبعد من استخلاص غرض المشرع ، أي تحديد المعنى الصحيح للألفاظ التي ورد بها النص حسبما قصده واضع القانون ، دون أن يكون في ذلك تعارض مع النص المذكور أو تحميل لعبارته أكثر مما تحتمل. على هذا فليس للقاضي أن يتوسل بالتفسير للوصول إلى التجريم في أي صورة كانت.

وتطبيقا لذلك يجب في حالة اذا بلغ النص من الغموض حدا يتعذر معه استخلاص حقيقة غرض الشارع بيقين ، أي في حالة ما اذا ثار بشأن النص شك جدي ، أن يمتنع القاضي عن تكملة ما يعتقد أنه ينقص النص المذكور أو عن اللجوء إلى طريق القياس ، بمعنى أن المتهم يستفيد من الشك في مثل هذا الغرض.

وبناء على ما تقدم لا يتصور ان يكون هناك جريمة أو عقوبة بدون نص تشريعي. وبالنسبة للجرائم التي تقع نتيجة الاستخدام غير المشروع لتقنية المعلومات الحديثة ، فالأمر جديد على مسامع المشرع في البلاد الآخذة في النمو ، مما قد يمس من قريب أو بعيد بمبدأ الشرعية الذي اصبح ملازما للإنسانية في تقدمها ورقيها. فبرغم امكانية تطبيق النصوص التقليدية القائمة على بعض من جرائم التقنية الحديثة ، إلا أنه ليس بإستطاعة القانون الجنائي بوضعه السابق مواجهة كافة صور جرائم التقنية الحديثة ، وذلك لأن النصوص التقليدية قد وضعت لتطبق وفق معايير معينة لا تتناسب مع العديد من صور جرائم التقنية الحديثة نظرا للذاتية الخاصة التي تتميز بها هذه الجرائم[2]، وبالتالي فإن تطبيق النصوص التقليدية عليها من شأنه المساس بمبدأ الشرعية الجنائية ، اذا ترك الأمر بيد القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله. لذا اختلف الفقهاء ازاء تطبيق النصوص القائمة على الجرائم الناشئة في التقنية الحديثة بين مؤيد ومعارض لتطبيق تلك النصوص على جرائم تكنولوجيا المعلومات الحديثة.

---

[1] – علي أحمد راشد – مبادئ القانون الجنائي ،منشأة المعارف – بدون تاريخ نشر – ص 232.

[2] – جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة –دار الجامعة الجديدة للطباعة و النشر و التوزيع مرجع سابق – ص 12.

فإذا أخذنا كمثال لهذا الخلاف جرائم الاعتداء على انظمة المعلومات في شبكة الانترنت ، في ظل المواد الجنائية التقليدية القائمة ، فهل ينطبق على اختلاس مثل هذه المعلومات وصف السرقة أم إن ذلك يعد توسعا في تطبيق النصوص الجزائية ، وسنتناول هذا الخلاف الفقهي تفسيرا عند حديثنا عن الأحكام الموضوعية للجرائم الواقعة على الأشخاص وضد الحكومة في اطار التقنية الحديثة ، ولكن لابد من الإشارة في هذا المقام إلى أن الخلاف الفقهي سابق الذكر يعكس لنا مدى الحاجة إلى تدخل تشريعي لمواجهة جرائم التقنية الحديثة ، اعمالا لمبدأ الشرعية ، وابتعادا عن اللجوء إلى القياس والذي يتعارض مع هذا المبدأ.

الفرع الثاني : الوضع القانوني لجرائم المعلوماتية على ضوء قانون العقوبات الجزائري

لم يكن المشرع الجزائري بمعزل عن الحركية التشريعية التي واجهت الإعتداءات على المعلوماتية ، حيث نجده قد استعد لمواجهتها ضمان لسد الثغرة التشريعية التي تمكن المجرم من الإفلات من العقاب وهذا وفق القانون رقم 04-15 المعدل والمتمم لقانون العقوبات في اطار القسم السابع مكرر الذي خصصه المشرع الجزائري لجرائم المساس بنظام المعالجة الآلية للمعطيات من المادة 394 مكرر الى المادة 394 مكرر 7 .

وبهذا فإن المشرع الجزائري قد حدّث نصوصه التجريمية بموجب القانون السالف الذكر لتتماشى مع متطلبات الواقع ، وبرجوعنا للتشريع السابق الذكر نجد أن الصور التجريمية المتعلقة بالإعتداء على النظام المعلوماتي متغيرة بتغير السلوك المرتكب والنتيجة الواقعة وهذا ما سندرسه وفق ما يلي:

أولا : جريمة الدخول أو البقاء عن طريق الغش

تعتبر الأنشطة التى تستخدم في إطار تبادل المعلومات الالكترونية[1] عن طريق النظام المعلوماتي ، وما نتج عنها من إشكالات قانونية في إطار الإعتداءات الواقعة عليها.

وهو الأمر الذي جعل المشرع يتجه لإدخال نصوص جديدة تحمي المعلومة[2] داخل النظام المعلوماتي والتي منها تجريم الدخول في نظام الحاسب الآلي فضلا عن إتلاف المعلومات المبرمجة أو الموجودة داخل هذا النظام. وهو ما نص عليه المشرع بنص المادة 394 مكرر

[1]- سليم عبد الله الخيوري، الحماية القانونية لمعلومات شبكة الانترنت، منشورات الحلبي الحقوقية، ط1،2011، ص318.

[2]- تبرز حاجة المعلومة الإلكترونية إلى الحماية بالنظر إلى أهميتها بالمقارنة مع المعلومات داخل الملفات الورقية.. كما تتميز المعلومة الإلكترونية بالضخامة والتنوع، بل منها ما يتعلق بالحياة الخاصة للأفراد ومنها ما يتعلق بالأمن القومي... ينظر، أكثر تفاصيل شيماء عبد الغني محمد عطا لله، الحماية الجنائية للتعاملات الالكترونية، دار الجمعة الجديدة، 2007، ص94.

أ : الدخول إلى نظام المعالجة الآلية للمعطيات

الدخول هو الولوج إلى المعلومات والمعطيات المخزنة داخل النظام المعلوماتي بدون رضا المسؤول عنه[1].

ويتحقق هذا السلوك المجرم عن طريق قيام الجاني الإلكتروني بإختراق أنظمة المعلوماتية الذي يمكننا أن نتصور الدخول إليها[2] بالدخول عن طريق تشغيل حاسب آلي مغلق ، حيث يقوم الجاني في هذه الحالة بفتح جهاز الكمبيوتر وتشغيله ثم يدخل إلى النظام ، غير أن العبرة ليست بتشغيل الكمبيوتر ولكن بالتمكن من الدخول إلى النظام إذ يستطيع الجاني أن يدخل إلى النظام والجهاز مغلق، وقد يتمكن من تشغيل الجهاز دون أن يصل إلى الملفات[3]، أو بالدخول بإستعمال حاسب آلي مفتوح وفي هذه الحالة يكون جهاز الحاسوب قيد الاستعمال ثم قام الجاني باستغلال ذلك ودخل إلى إحدى أنظمة المعالجة أو الملفات المتواجدة فيه..، وعليه فإن ذلك يعد دخولاً غير مشروع ويعاقب عليه أو بالدخول عن طريق الاختراق ويتم ذلك غالبا باستخدام وسائل تقنية حديثة كبرامج التجسس والاختراق ويتطلب مهارة عالية.

كما يكون بالدخول عن طريق خطوط الاتصالات وفي هذه الحالة يعمد الجاني إلى العبث بخط من خطوط الهاتف المتصل بالنظام المعنى من أجل إعطاء تعليمات إلى هذا النظام[4] لتحقيق غرض معين[5]، أو بالدخول إلى نظام الحاسب الآلي بإستعمال بطاقة الغير وفي هذه الحالة يقوم الجاني بإستعمال بطاقة الغير للدخول إلى نظام الحاسب الآلي التابع لإحدى الجهات من أجل الحصول على أمر معين أو بيانات معينة أو معلومات هي مقتصرة على أصحاب البطاقات[6].

---

[1] – هلالي عبد الإله أحمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، 2007، ص 54 وما بعدها.

[2]– خليفة محمد، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة، 2011/2010، ص 140 وما بعدها.

[3] ما تجدر الإشارة إليه أن الدخول لا يكون محققا إذا كان برضا صاحب النظام..، لذلك يعتبر البعض أن عدم الرضا ركن في هذه الجريمة فإذا توفر الرضا انتفت الجريمة حتى ولو استعمل الجاني النظام في غير الأغراض التى أرادها صاحب النظام.

[4]– شيماء عبد الغني محمد عطاالله، المرجع السابق، ص108.

[5]– نفس المرجع السابق، ص112.

[6]– محمد أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003، ص1150.

ب: البقاء بالغش داخل نظام المعالجة

يتحقق هذا السلوك المجرم بتواجد الجاني داخل النظام المعلوماتي بدون رضا من له الحق في التحكم بالنظام[1]، ويكون ذلك إما بعد الدخول غير المشروع في النظام، أو في حالة البقاء داخل النظام بعد نفاذ الوقت المحدد للبقاء داخله وكثيرا ما يحدث ذلك إذا كان استعمال النظام بمقابل محدد بمدة زمنية[2]، وقد تتحقق جريمة البقاء داخل النظام دون جريمة الدخول وذلك في الحالة التى يكون فيها الدخول إلى النظام عن طريق الخطأ أو الصدفة[3]، ومحل التجريم في هذه الحالة هو بقاء الجاني داخل النظام، إذ كان يجب عليه في هذه الحالة أن يقطع وجوده وينسحب فورا[4].

كما يعد البقاء متحققا في الحالة التى ينسخ فيه الجاني معلومات مسموح بالإطلاع عليها فقط[5]، وقد يجتمع الدخول غير المشروع وعنصر البقاء غير المشروع وذلك عندما لا يكون للجاني الحق في الدخول إلى النظام ومع ذلك يدخل إليه ويبقى داخله.

ويكفي لتحقق عنصر البقاء مجرد التواجد داخل كل أو جزء من النظام فمجرد التجول يكفي لقيام هذا السلوك المجرم[6] دونما أن يشترط لذلك المحو أو الإتلاف أو التعديل للمعلومات المتواجدة في النظام المعلوماتي حسب المادة 394 مكرر.

ثانيا: الظروف المشددة المنصوص عليها بموجب المادة 394 مكرر

تكملة لجريمة الدخول أو البقاء في النظام بحيث يمتد فيها إجرام الجاني إلى إحداث تغييرات داخل نظام عمله مما يؤدي إلى حذف أو تغيير معطيات متواجدة داخلة النظام المعلوماتي أو تخريب لسيره ، لهذا نجد أن المشرع الجزائري قد ربط بينها وبين جريمتي الدخول أو البقاء غير المشروع في النظام المعلوماتي بإعتبارها ظرف تشديد لها، وتلك الظروف المشددة تتمثل في :

أ : الحذف أو التغيير في معطيات النظام المعلوماتي

بالرجوع إلى نص المادة المذكور سلفا نجد أن المشرع لم يشترط أن ينتج عن هذا الحذف تعطيل أو ضرر للنظام وبالتالي فمجرد وقوع حذف في معطيات المنظومة كاف لتشديد العقوبة.

---

[1]- نفس المرجع السابق، ص1152.

[2]- أمال قارة، المرجع السابق، ص111 ، و شيماء عبد الغني محمد عطاالله، المرجع السابق، ص121.

[3]- نفس المرجع السابق، ص124.

[4]- أمال قارة، المرجع السابق، ص110.

[5]- يتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور كخدمة الهاتف والتى يحصل فيها الجاني على الخدمة لكن دون دفع الثمن أو يحصل على الخدمة مدة أطول من المدة الممنوحة له.

[6]-علي عبد القادر القهوجي، المرجع السابق، ص134-136.

أما التغيير فيختلف عن الحذف والذي يفترض استبدال معطيات مكان أخرى نتيجة الدخول أو البقاء في النظام، فيبقى النظام في هذه الحالة سليما لكن بوجود معطيات مغايرة، كما أن التغيير لا يشترط أيضا تعطيل النظام أو فساده إنما مجرد التعديل يجعل السلوك المجرم قائما، فمصطلح "تغيير" مجرم لذاته تجريم الدخول أو البقاء داخل نظام المعالجة هو تجريم وقائي حتى لا يحدث تعطيل لهذا النظام أو المساس بالمعطيات الموجودة فيه وهذا احتراما لمبدأ الشرعية الجنائية ، فلا يهم بعدها إن حدث معه تعطيل للنظام أو تحسين أدائه بسبب ذلك التغيير. [1]

ب : تخريب النظام المعلوماتي

المادة 394 مكرر في فقرتها الثالثة نصت على ظرف مشدد مستقل عن الظرفين السابقين و هو مجرم لذاته ،فالتخريب يقصد به هنا أن يترتب على الدخول أو البقاء داخل النظام إتلافه ، وبالتالي تعطيله عن أداء مهامه فمصطلح التخريب يشتمل على جميع الأوصاف المؤدية لعرقلة أو إفساد لوظائف النظام ، والذي يحدث من خلال العبث في معطيات النظام المتعلقة بنظام سيره ، لهذا فالتخريب أكثر ضرر من فعل التغيير غير أن المشرع ربط بينه وبين نتيجته المتمثلة في تعطيل النظام

جريمة هنا من الجرائم المادية التي يتطلب لقيامها تحقق النتيجة وإلا بغيابها سينعدم الظرف المشدد وتكون محل المتابعة فيها بموجب الدخول او البقاء عن طريق الغش للنظام المعلوماتي .

ومما لا شك فيه أن ظرف التشديد أتى هنا للعقاب على تخريب سير النظام المعلوماتي ، فإن كان النظام مخربا قبل الدخول أو البقاء فلا ظرف تشديد، غير أنه يكفي لقيام ظرف التشديد هذا أن يكون جزء من نظام تشغيل المنظومة مخرب والجزء الآخر سليم إذا وقع عليه التخريب.

ثالثا : جريمة التلاعب بالمعطيات المتواجدة داخل النظم المعلوماتي

نص المشرع على هذه الجريمة في المادة 394 مكرر 1 من قانون العقوبات ، والملاحظ هنا أن الإطار العام للنص جاء غير مميز لنوعية المعلومة بل جاء حماية لها على العموم لكل أنواع التلاعبات بمختلف الوسائل التي قد تمس بها . [2]

[1]– فتنص المادة 394 مكرر في فقرتها الثالثة".. وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة..."

[2]– تنص المادة 394 مكرر 1"...كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التى يتضمنها...".

أ: الإدخال

يعاقب المشرع كل من أدخل معطيات في النظام المعلوماتي بطريق الغش[1] ، حيث يعرف بأنه تغذية النظام بالمعلومات المراد معالجتها او بتعليمات لازمة لعملية المعالجة ، ويتحقق الإدخال عن طريق إضافة معطيات جديدة في نظام المعالجة الآلية[2]، وفعل الإدخال بيتم عن طريق إستخدام البرامج الخبيثة بغرض التعديل في البيانات الأمر الذي يؤثر على صحتها أو نسبتها أو قيمتها كما أنه يكون بغرض إتلافها او تشويهها أو تدميرها ، وهو أمر سهل القيام به خاصة في المراحل الأولى لتشغيل النظام وهي مرحلة إدخال المعلومات وبالتالي يكن من السهل تغذية النظام بمعلومات مغلوطة أو زائفة لم تكن موجودة فيه من قبل ، الأمر الذي يؤثر سلبا على المعلومات الموجودة فيه من حيث سلامتها وقيمتها
وبالتالي فإن مجرد إدخال معلومات على معطيات نظام المعالجة يشكل السلوك المجرم لهذه الجريمة، كما لا يهم صحة المعلومات المدخلة من عدمه فالعبرة بالإدخال لا بمدى صحة هذه المعلومات. [3]

ب: الإزالة

وهو السلوك الثاني المنصوص عليه في المادة 394 مكرر 1 من قانون العقوبات ويقصد بالإزالة المحو الجزئي أو الكلي للمعلومات المتواجدة داخل النظام أو النقل والتخزين لها في منطقة خاصة .
وعلى إثر ذلك تكون الإزالة عملية لاحقة عن عملية الإدخال للمعلومات المغلوطة، فهي تفترض الوجود السابق لها ، فالمسؤول عن الحفظ يمكنه تدمير إتلاف المعلومات المكلف بحفظها داخل النظام.

ج: التعديل

وهو سلوك يدخل كذلك في تكوين الركن المادي لجريمة التلاعب بالمعلومات داخل النظام المعلوماتي ويقصد بالتعديل تغيير المعلومات الموجودة داخل النظام واستبدالها بمعلومات أخرى[4]، كما أنه يدخل في إطاره كذلك التلاعب في البرنامج بإمداده بمعلومات مغايرة تؤدي لنتائج غير تلك التي صمم لأجلها .
وهو سلوك كثيرا ما يرافق جرائم الاحتيال المعلوماتي بمجالاته المختلفة بما في ذلك أنظمة التحويل الإلكتروني للأموال أو بطاقات الائتمان وأجهزة الصرافة الآلية نظرا لما تتميز به من سهولة عن طريق احتجاز الأمر بالدفع الموجه من المصرف الآلي إلى نظام الحاسب الآلي وعلى إثر ذلك يُزور الجاني

---

[1]- عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر و الأنترنت ، المرجع السابق ، ص 378، أنظر علي عبد القادر القهوجي المرجع السابق ص95.

[2]- يصنف الفقهاء هذا النوع من السلوك ضمن الغش المعلوماتي الذي يتم عن طريق التلاعب وإدخال بيانات جديدة مصطنعة بغرض تغيير الحقيقة.

[3]- عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام المرجع السابق، ص46.

[4]- شيماء عبد الغني محمد عطالله، المرجع السابق، ص135.

هذه الرسالة حتى يتم دفع المبلغ إلى حسابه الخاص، ويكفي الجاني أن يتوجه إلى شباك التوزيع بالبنك ليسحب الأموال بسرعة قبل اكتشاف الحقيقة[1].

رابعا : جريمة التعامل غير الشرعي في معطيات النظام المعلوماتي

يتمثل الركن المادي لهذه الجريمة[2] التي نص عليها المشرع بموجب المادة 394 مكرر2 في نوعين من السلوكيات المجرمة تضمن المجموعة الأولى منها الأفعال المتعلقة بالتعامل غير الشرعي في معطيات يمكن أن يرتكب بها أحد الجرائم المنصوص عليها سابقا ، وتعد المجموعة الثانية بمثابة التعامل غير الشرعي بالمعطيات المتحصل عليها من الجرائم السابقة وسنتناول كلا المجموعتين وفق ما يلي :

أ: التعامل في معطيات صالحة لارتكاب جريمة ماسة بنظام المعلومات

ويكون التعامل وفق مجموعة من الأفعال التي عددتها المادة 394 مكرر2 في فقرتها الأولى وهاته الأفعال هي:

1 : التصميم

والذي يتمثل في إعداد معلومات صالحة في ارتكاب الجريمة ، وهو عمل يقوم به المختصون في مجال البرمجيات وهم المبرمجون أو مصممي البرامج ، و من ذلك تصميم برنامج لأهداف تخريبية – البرامج الخبيثة أو البرامج المصممة من أجل الوصول للنظام المعلوماتي – .

2 : البحث

البحث في إطار الخدمات الإلكترونية المقدمة بواسطة الشبكة العنكبوتية وهو ما يسمى ب "محركات البحث" ، وهي عبارة عن برامج مساعدة للحصول على المعلومة على اساس ان الأنترنت بها كم هائل معتبر جدا من المعلومات ، فالباحث لديه هدف محدد من خلال بحثه و بالتالي فمحرك البحث يساعده لبلوغ هدفه المنشود من خلال تزويده بالمواقع المتخصصة ذات الصلة بموضوع بحثه ، ومن هنا يظهر لنا أن البحث بهذه الكيفية يتعلق بحق الأفراد في الحصول على المعلومات ، وهو لا يدخل في إطار

---

[1]– المرجع السابق، ص136.

[2]نص المشرع على هذه الجريمة في المادة 394 مكرر2 من قانون العقوبات حيث جاء فيها "يعاقب بالحبس من شهرين إلى ثلاث سنوات و بغرامة مالية من 1000.000دج إلى 5.000.000دج كل من يقوم عمداً و عن طريق الغش بما يأتي:

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

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

المعنى المقصود في المادة 394مكرر2 و بالتالي فالبحث هو البحث عن كيفية تصميم المعلومات و إعدادها .

3 : التجميع

و هو القيام بجمع قدر من المعلومات التي باجتماعها مع بعضها تؤدي لارتكاب الجريمة على النظام المعلوماتي و من هنا جاء النص عليها بصيغة الجمع ، فالتجميع يقتضي وجود الحيازة لأكبر قدر من المعلومات دون وجود نية إستخدامها فبمجرد توافرها لدى الجاني يكون قد إرتكب الجريمة المعاقب عليها بالمادة 394 مكرر 2

4 : التوفير

ومصطلح التوفير يشير إلى عرض المعلومات و إتاحتها و جعلها في متناول الغير ، بل و تحت تصرفه و حيازته ، و ذلك بالإحالة لبرنامج متصل ببرامج مصممة للاتلاف او هدم المعلومات أو للتدخل في عمل النظام المعلوماتي و الذي يكون بواسطة الفيروسات.

5 : النشر

ويقصد به إذاعة المعلومات والتي مهما كان نوعها أو طبيعتها ، و تمكين الغير من الإطلاع عليها، وهو يمتد ليشمل كل النشاط من شأنه نقل المعلومات الى الآخرين .

6 :الإتجار

الإتجار المقصود بالمادة 394 مكرر 2 يشمل كافة التصرفات التي تكون بمقابل سواء كان عينيا او نقديا ، حتى و لو لم ينص عليها القانون التجاري في اطار الاعمال التجارية المنظمة من خلاله ، و عليه فالإتجار يختلف عن التوفير على اساس ان الأخير قد يكون بدون مقابل ، لهذا فالإتجار قد يكون جزء من التوفير لأنه يشمل تقديم المعلومات بمقابل او بدون مقابل .[1]

ب: التعامل في معطيات متحصلة من جريمة ماسة بنظام المعلومات

وهي الصور الثانية لجريمة التعامل غير الشرعي في معطيات النظام المعلوماتي ، الواردة في نص المادة 394 مكرر2 الفقرة الثانية منها ، وتتم هذه الجريمة عن طريق الحيازة ، الإفشاء ، النشر ، الإستعمال ، وسنحاول شرحها وفق ما يلي :

[1] محمد محمود المكاوى ، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والإنترنت) ، المكتبة العصرية للنشر والتوزيع، القاهرة، الطبعة الأولى، 2010 ، ص101

1 :الحيازة

حيازة المعلومات تكون بالسيطرة عليها سيطرة مطلقة يستطيع معها الحائز إتلاف المعلومات او تعديلها او الإنتفاع بها أو إستعمالها أو توجيهها ، كما انها قد تكون سيطرة محدودة تمكنه فقط من الانتفاع بالمعلومات او استغلالها في وجه محدد.

2: الإفشاء

يفترض الإفشاء إنتقال المعلومات من حيازة الجاني الى الغير و هذا هو الفرق بين الإفشاء و الحيازة حيث ان الأخيرة ينحصر وجود المعلومات لدى الحائز دون تقديمها للغير في حين ان الثانية نجد ان المعلومات يتم انتقالها من يد الحائز لها الى الغير و لا يشترط في الغير ان يكون من فئة معينة .

3 : النشر

لم يحدد المشرع وسيلة للنشر و على اثر ذلك يستوي ان يتم النشر عن طريق الأقراص المضغوطة او بالكتابة او بالطريقة الورقية او اي سيلة اخرى خاصة أن الوسائل التقنية الحديثة ساهمت في النشر السريع و بكفاءة عالية للمعلومات المتحصل عليها من جرائم المعلوماتية .

4 :الإستعمال

نجد أن المشرع قد توسع في دائرة التجريم حتى يصل الى الإحاطة الكلية بهذه الجرائم و من بين مظاهر توسعه نجد تجريمه لسلوك الإستعمال لأي غرض كان للمعلومات المتحصل عليها من جرائم المعلوماتية، فالإستعمال غير المشروع للمعلومات يعد مجرما مهما كان الهدف منها ، و مهما كان نوع الإستعمال ، و بأية وسيلة كان ذلك الإستعمال ، و لو لمرة واحدة فقط[1] .

و على إثر ما سبق ذكره **يتبين لنا** أن المشرع الجنائي الجزائري قد إعتمد على وجهة نظر خاصة في تجريمه للإعتداءات الماسة بالمعلومات الإلكترونية ، و هذا واضح من النصوص القانونية السابقة الذكر ، و التي خص بها المساس بنظم المعلوماتية فكما جرم مختلف الإعتداءات المتعلقة بتلك النظم إلا أنه لم يحدد طبيعة الجهة المستهدفة من الإعتداءات ، الذي قد يكون شخصا طبيعيا أو شخصا معنويا ، و حتى بالنسبة للشخص الطبيعي أو المعنوي المستهدف من الجريمة المعلوماتية نجد ان المشرع لم يحدد لا الجنس و لا السن هذا بالنسبة للشخص الطبيعي ، أما بالنسبة للشخص الطبيعي فالمسألة تهم الشخص المعنوي العام ، و في نفس الإتجاه فهي تهم الشخص المعنوي الخاص.

و بالرجوع إلى موضوعنا محل الدراسة و المتعلق بجرائم الآداب العامة المرتبطة بتقنية المعلوماتية نجد أن المشرع لم يتطرق إلى هذا النوع من الجرائم الماسة بالآداب العامة في إطار تجريمه للمساس بأنظمة

[1] - محمد محمود المكاوى ، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والإنترنت) ،) دار الجامعة الجديدة للطباعة و النشر و االتوزيع ، مرجع سابق ص105

المعلوماتية ، إلاّ أننا نلمس من خلال ما سبق ذكره حول تلك الجرائم أنها يمكن أن تتعلق بالآداب العامة و هذا من منطلق أن السلوكات الإجرامية السابق ذكرها و التي نذكر منها على وجه الخصوص سلوك الدخول أو البقاء عن طريق الغش يمكن أن يتعلق بجريمة الآداب العامة و هذا لأجل التجسس من خلال الدخول أو البقاء في النظام المعلوماتي للحصول على معلومات شخصية متواجدة داخل النظام، و التي تتعلق بالحياة الخاصة للشخص كأن يتم التجسس على محادثاته أو صوره أو تسجيلاته المصورة المحتفظ بها داخل النظام المعلوماتي ، كما يمكن أن يتم عن طريق سلوك الإدخال لمعلومات تشوه حياته الخاصة و هذا لفضحه أو لتعكير حياته الخاصة ، كما يمكن أن يحدث ذلك من خلال تصميم برامج تتعلق بإختراق الأنظمة المعلوماتية أو تكون متعلقة بتزييف الحقيقة لقلبها رأسا على عقب كأن تقوم البرامج بحذف شخص و إستبداله بشخص آخر في صورة أو فيديو و هذا كثيرا ما يستعمل في ما يعرف بالفوتو شوب ، أو أن يقوم الجاني بالبحث أو التجميع أو التوفير أو النشر أو الإتجار أو الحيازة أو الإفشاء أو الإستعمال لمعلومات صالحة لإرتكاب جريمة معلوماتية داخل النظام المعلوماتي أو متحصل عليها منه و هذا في نفس النسق السابق ذكره أي انها تتجه لإرتكاب جريمة أخرى من جرائم الآداب العامة. [1]

و عليه يمكننا القول أن المشرع في إطار المواد من 394 مكرر إلى 394 مكرر7 لم يحدد الإتجاه الذي من خلاله تم ارتكاب الجريمة المعلوماتية و لهذا تركها مفتوحة لتحتمل الإتجاه المراد من الجاني ، و هذا إحتراما لمبدأ الشرعية الجنائية المنصوص عليه بالمادة الأولى من قانون العقوبات[2] .

و عليه فإننا سنتطرق لمختلف صور السلوكات الإجرامية المتعلقة بالآداب العامة و المرتبطة بتقنية المعلوماتية محاولين أن نلمس مدى نجاعة المشرع في التصدي لها و إحاطته بمختلف تلك الصور، و هذا من خلال المبحث الثاني من هذا الفصل.

[1] عبد القادر علي قهوجي ، الحماية الجنائية لبرامج الحساب مرجع سابق ، ص 137

[2] تنص المادة الأولى من قانون العقوبات الجزائري على ان :"لا جريمة و لا عقوبة أو تدابير أمن بغير قانون."

المبحث الثاني: تأطير المشرع العقابي لجرائم الآداب العامة المتصلة بالمعلوماتية

يعتبر تحول نطاق تقنية المعلومات الحديثة للعالمية سببا لتحولها إلى مساحة مفتوحة لممارسة جميع أنواع الإجرام الممكنة والمحتملة من جرائم جنسية وإفساد الأخلاق والتعرض للآداب العامة ،التي هي في الأساس جرائم تقليدية موجودة بالفعل إلا أن وسائط تقنية المعلومات الحديثة سهلت عملية إرتكابها وخلقت منها شكلا جديدا و متنوعا، فانتشرت الأخطار الناجمة عن نشر وعرض المواد الإباحية (من كتابات ورسومات وصور وأفلام ورموز مخلة بالآداب العامة) والتحريض على الفسق عبر المواقع والقوائم البريدية الإباحية، وارتيادها والشراء منها، والاشتراك فيها أو إنشائها. [1]

وبرغم أن هذا الإجرام المستحدث يطال ضرره المتعاملين بوسائط تقنية المعلومات الحديثة بصرف النظر عن أعمارهم أو جنسهم، إلا أن واقع هذه الظاهرة أظهر مدى الحاجة لحماية الأشخاص بوجه عام و القصر بوجه خاص ، من أن يكونوا عرضة لهذه المواد الإباحية، أو من أن يكونوا محلا لها مما يشكل أذى ماديا و معنويا لهم. فقد ظهرت جملة من الجرائم الجنسية و الأعمال الإباحية التي تستهدف القاصرين بالتحديد ، من تحريضهم على الأعمال الجنسية وإغوائهم أو محاولة إغوائهم لإرتكاب أعمال إباحية،أو تلقي أو نشر المعلومات عنهم عبر وسائط تقنية المعلومات الحديثة من أجل أعمال إباحية، او التحرش الجنسي بهم عبرها، أو نشر وتسهيل واستضافة المواد الفاحشة لهم عبر الإنترنيت، أو تصويرهم أو إظهارهم عبر أعمال إباحية، أو إستخدام الإنترنيت لترويج الدعارة أو لنشر المواد الفاحشة عنهم.

إلاّ أننا لمسنا كما وضحناه سابقا أن المشرع الجنائي الجزائري لم يقم في إطار معالجة لجرائم المعلوماتية المنصوص عليها في قانونا العقابي بالتعرض لصور العرض وإفساد الأخلاق المتعلقة بتقنية المعلومات الحديثة، وإن كان قد جرم التعرض للأخلاق و الآداب العامة بصورها التقليدية.[2]

وفي هذا الصدد سوف نستعرض في مطلب أول مدى إنطباق الجرائم التقليدية للآداب العامة في وجود وسيلة معلوماتية ، ومدى إمكانية مدى انطباق النصوص الخاصة بالجريمة المعلوماتية إذا ما تعلقت الأمر بالآداب العامة كمطلب ثان.

---

[1] والمقصود بالآداب العامة هو ما تعارف عليه الناس من خروج على الاحتشام مما تجرح رؤيته أو سماعه شعور الجمهور، كالصور والأفلام وغير ذلك.. ايا كانت درجة الفحش الذي تمثله أو تنطوي عليه ، محمد محرم محمد علي، قانون العقوبات الاتحادي ، دار الفتح للطباعة والنشر، ص930

[2] عبد العزيز سعد، المرجع السابق.

المطلب الأول: مدى إنطباق الجرائم التقليدية للآداب العامة في وجود وسيلة معلوماتية

بالرجوع إلى مختلف النصوص القانونية المنظمة للجرائم الجنسية أو الأخلاقية عامة، لا نجد تعريفا واضحا بل إن المشرع اكتفى بتحديد الجرائم التي تدخل في إطارها، وغالبية التعريفات التي تناولت الجريمة الجنسية، عرفتها بأنها كل فعل مادي ذو طبيعة جنسية يسلط على الإنسان و يمس من جسده أو أخلاقه أو كليهما. وقد يبدو هذا التعريف شاملا لكنه في الواقع لا يشمل إلا على نوعا واحدا من الجرائم الجنسية و المتمثل في الجرائم المباشرة و لا يشمل جرائم أخرى كجرائم الاستغلال مثلا .

وتجدر الإشارة في هذا المستوى إلى أن الغاية من ارتكاب الجريمة الجنسية لا يعد عنصرا جوهريا في تعريف هذا النوع من الجرائم حيث أن الجاني يهدف إلى إشباع غرائزه الجنسية عند ارتكابه للجريمة أو قد تكون غايته القيام بفعل انتقامي غير أن هذه الغاية لن تؤثر على تكييف الجريمة إذا ما توفر الركن المادي المكون لها فيكفي أن يكون هذا الفعل خارقا للقانون حتى يتوفر في شأنه الركن المعنوي للجريمة.

و حتى نتمكن من تقديم مفهوم شامل وواضح لهذا النوع من الجرائم يجب الرجوع إلى نصوص قانون العقوبات و التي من خلالها نلمس مدى تحقق المسؤولية الجنائية عن ما يتم نقله أو عرضه من مواد إباحية تؤدي إلى إفساد الأخلاق و الإخلال بالمواد العامة عبر أنظمة المعلوماتية و هذا كفرع أول ، بينما نتطرق كفرع ثان لمدى مرونة تلك النصوص بحيث تسمح بانطباقها على وسائط تقنية المعلومات الحديثة، فيما لو استخدمت كوسيلة للقيام بالأفعال المخلة بالآداب والأخلاق العامة . [1]

الفرع الأول : جريمة الإخلال بالأخلاق الحميدة

وهو الفعل المنصوص و المعاقب عليه في المادة 333 مكرر من قانون العقوبات ، بحيث تقوم الجريمة على ثلاثة اركان والمتمثلة في محل للجريمة و أفعال مجرمة و قصد جنائي ، والتي سنفصل فيها بإيجاز وفق ما يلي :

أ: محل الجريمة

يتمثل محل الجريمة في كل مطبوع او محرر او رسم او اعلان او صور او لوحات زيتية او اي شيئ مناف للحياء .

وعبارة " اي شيء" تسمح في التجريم ليمتد الى اشياء لم يرد ذكرها في النص مثل الافلام السينمائية الخليعة وافلام الفيديو من فئة "اكس " وكذلك الاشياء المنحوتة .

ويأخذ هنا تحديد مفهوم " الحياء "اهمية قصوى ، وهو المفهوم الذي يحتاج الى التوضيح نظرا لما يكتنفه من غموض يضاف اليه الطابع المتغير للحياء الذي باختلاف المكان و الزمان .

[1]– علي محمد جعفر ، قانون العقوبات القسم الخاص ، المؤسسة الجامعية للدراسة و النشر ، سنة 2006، ص95

و يمكن اعتماد التعريف التالي الذي مفاده أن منافاة الحياء يعني "مخالفة الحياء العام وهي تنطوي مبدئيا على اثارة الشهوة الجنسية و التحريض على سلوك المنحط القبيح و الانحرافات الجنسية" ، و هذا كما جاء في أحد إجتهادات محكمة النقض الفرنسية .

وتبعا لذلك تعتبر منافية للحياء الصور التي تظهر الرجل و المرأة وضع الوقاع وكذا صور للرجال او النساء وهم عراة تماما او تلك التي تبرز عوراتهم وهي عارية ، وكذلك الكتب التي تعرض او تقدم اوصافا دقيقة لمختلف اوضاع وكيفية الاتصال الجنسي ، ومع ذلك يجب التمييز بين الصور و الكتب التي تهدف الى اثارة الشهوة الجنسية وبين الصور و الكتب العلمية لاسيما في المجال الطبي التي تتضمن صورا واوصافا دقيقة لعورات الرجل و المرأة وذلك بهدف التعليم والتثقيف الطبي .

كما يتعين ايضا التمييز بين الصور العارية الفنية وبين الصورة العارية المثيرة للجنس ، وان كانت الصورة الفنية تخلو عادة من اي نية في اثارة الجنس ، فانه من الصعب القول ، في مجتمع مثل مجتمعنا العربي المسلم ، بان الصورة الفنية الخليعة غير منافية للأخلاق الحميدة ، إلا أن الامر متروك للسلطة التقديرية لقضاة الموضوع الذين يرجع اليهم وحدهم الفصل في مثل هذه الامور. [1]

ب: الافعال المجرمة

حيث حددت المادة 333 مكرر تلك الافعال و حصرتها وفق ما يلي ذكره :

- الصناعة او الحيازة او الاستيراد او السعي في الاستيراد ، وذلك من اجل التجارة او التوزيع او التاجير او اللصق او اقامة معرضا .
- العرض او الشروع في العرض للجمهور
- البيع او الشروع في البيع .
- التوزيع او الشروع في التوزيع .

و الأمر المستخلص من تلك الأفعال ان شرط العلانية مطلوب في صورتين فقط وهما : العرض او الشروع في العرض للجمهور ، اما في باقي الصور مثل البيع و التوزيع و الشروع فيهما فلا يتطلب توافر عنصر العلنية فيها .

كما أن المشرع إشترط لقيام الجريمة في صور الصناعة و الحيازة و الاستيراد ان يكون ذلك بغرض التجارة او التوزيع او التاجير او اللصق او اقامة معرض ، وتبعا لذلك لا تقوم الجريمة اذا كانت الصناعة او الحيازة او الاستيراد من اجل الاستعمال الشخصي. [2]

[1] علي محمد جعفر ، قانون العقوبات القسم الخاص ، مرجع سابق، ص96

[2] - عائشة بن قارة حجية ، الدليل الالكتروني في مجال الإثبات الجنائي مرجع سابق ص 100

ج: الركن المعنوي

تقتضي الجريمة في كل صورها توافر قصد جنائي عام ، وتتطلب ، علاوة على ذلك ، قصدا خاصا يتمثل في الاتجار او التوزيع او التأجير او اللصق او اقامة معرض عندما يتعلق الامر بصور الصناعة و الحيازة والاستيراد او السعي في الاستيراد وفي كل الاحوال فان سوء النية مفترضة في كافة الصور المذكورة .

و الملاحظ من نص المواد على النحو السالف بيانه أنه يتلاءم مع جرائم الآداب التي تقع عبر تقنية المعلوماتية كطبع لصور مخلة بالآداب أو نقلها أو عرضها بقصد الإستغلال أو التوزيع أو العرض، وسواء أكانت مجرد صور أم أفلام أم لقطات فيلمية مصورة أو رموز أو غير ذلك من الأشياء طالما كانت مخلة بالآداب العامة، والواقع يثبت بل ويؤكد أن كل تلك الطرق والجرائم أضحت تتم بالفعل عبر وسائط تقنيات المعلومات الحديثة.

و محل الجريمة حددها المشرع بأنواعها، ويدخل فيها المجلات والصحف والكتب، وكذا الرسومات سواء قام برسمها شخص بيده أو بواسطة التكنولوجيا أو الصور ويدخل فيها الصور الفوتوغرافية أو نقش صور على جسم أو الحفر عليه، أو الأفلام أو الرموز وهي كل ما يشار إليه رمزا وتجسيدا لشيء آخر. ولذلك فيشترط لقيام الجريمة أن يكون صنع أو إستيراد أو تصدير إحراز أو حيازة تلك المواد المذكورة بقصد الإستغلال أو التصدير أو التوزيع أو العرض على الغير.

حيث أن أنظمة المعلومات تتيح نقل الصوت من مستخدم لآخر في أي مكان في العالم ،فإن علانية الأعمال والحركات يمكن تصورها في نطاق تقنية المعلومات الحديثة، وذلك بانطباق المكان حال الدخول للمواقع الإلكترونية على صفحات الويب أو غرف الدردشة المفتوحة للجميع والتي يمكن أن ينطبق عليها وصف الجمع العام بالإضافة للمكان المطروق الذي يستطيع أي شخص أن يطرقه . [1]

كما تتحقق علانية الكلام أو الصورة بواسطة وسائط تقنية المعلومات الحديثة- باعتبارها من الوسائل الآلية في نقل الأصوات- ذلك أن المشرع نص على علانية الفعل إذا تم نقل الكلام والصراخ بالوسائل الآلية ،ويقصد بها الاستعانة بالأجهزة التي تجعل الكلام مسموعا في أنحاء المكان دو ن تمييز سواء تم ذلك باستخدام مكبرات الصوت أو الميكروفونات أو أية وسيلة يكشف عنها العلم وتؤدي ذات الغرض ،فلم يحصر المقصود بالوسائل الآلية ولم يقصرها على زمان ومكان .

ولا يشترط أن يتم الجهر بالكلام أو الصراخ أو نقله بالوسائل الآلية من مكان عام ،أو أن يسمع الكلام أو الصراخ جميع من يحوزون جهز استقبال ،حيث يفترض القانون استقبالهم للكلام أو الصراخ بمجرد إذاعته، كما لا يشترط تواجد من يستقبل الإرسال في مكان عام، بل يكفي أن يكون في إمكان من يحوز

[1]- جميل عبد الباقي الصغير ، قانون العقوبات (القسم الخاص) ، دار النهضة العربية ، 1998 ، ص 128.

جهاز الاستقبال سماعه ولو كان متواجدا في مكان خاص ، وحيث أن وسائط تقنية المعلومات الحديثة يمكن أن تشمل على صوت، وعادة ما ترسل من أماكن خاصة فإن الجهر بها عبر وسيط تقنية المعلومات الحديثة ، سواء تلقاها من كان في مكان عام أو خاص يتحقق به ركن العلانية[1].

ويفترض العرض وضع المكتوب أو المطبوع بصورة تسمح للجمهور برؤيته ،ويكون العرض بطريق تقنية المعلومات الحديثة من خلال شبكة الويب العالمية ومجموعات الأخبار والبريد الالكتروني وغرف الدردشة ،والتي ينشر من خلالها الجناة كتاباتهم ورسومهم ،وصورهم اليدوية والشمسية، والأفلام والشارات و التصاوير على اختلافها ، حيث يتخذون مواقعهم من خلال شبكة الأنترنت لارتكاب أفعالهم الجرمية وعرضها من خلال صفحات الويب العالمية.

أما البيع فيقصد به في مجال العالمية :تسليم الكتابة أو الرسم للغير مقابل ثمن معين ، ويشترط أن يتم البيع لعدد من الناس بغير تمييز ولو انصب ذلك على نسخة واحدة أو نسخ عديدة لشخص واحد[2].

ويمكن تصوره عبر أنظمة المعلوماتية من خلال نشر إعلان على صفحات الويب أو مجموعات الأخبار أو إرسال خطاب دعائي عبر البريد الالكتروني أو غرف المحادثة.

وبالنسبة للتوزيع إن تقنية المعلومات الحديثة تسمح بإمكانية توزيع البيانات التي يتم نشرها على المواقع الخاصة بشبكة المعلومات، على جميع المشتركين أيا كان موقعهم الجغرافي .

كما يفترض التوزيع تسليم المكتوب أو المطبوع، سواء أكان صورا يدوية أو شمسية أو رسوما استهزائية أو شارت أو أفلام أو تصاوير على مختلف أنواعها، الذي قد يكون بصورة غير مباشرة من خلال البريد الإلكتروني أو عن طريق مجموعات الأخبار أو حتى التوزيع من خلال شبكات الويب أو غرف المحادثة، ويشترط حتى تتحقق علانية التوزيع أن يكون لعدد غير محدد من الناس المتعاملين بواسطة أنظمة المعلوماتية .[3]

وعلى ذلك فان إنشاء المواقع الإلكترونية الجنسية على شبكة الانترنت بقصد استغلالها أو عرضها على الجمهور يندرج في نطاق التجريم الذي تنص عليه المواد سالفة الذكر ، وكذلك كل من يقوم بتوزيع رسالة تحتوي على صور أو عبارات مخلة بالآداب على الجمهور ، وهذا يعني أن المشرع إذا كان يعاقب على التوزيع أو الاستغلال أو العرض على الجمهور فإنه وفقا للمواد سالفة البيان لا يعاقب على إحراز مواد مخلة بالآداب طالما ليست لغرض التوزيع أو الاستغلال أو العرض ، وبالتالي فالشخص الذي يحوز مواد فاضحة في بريده الإلكتروني الخاص دون أن تتجه نيته إلى بيعها ،أو عرضها على الغير من الجمهور،

[1]– د علي جابر الحسيناوي ، جرائم الحاسوب والإنترنت ،دار اليازوري العلمية نشر سنة 2011 ، ص 110.

[2]– إبراهيم عبد الخالق ، الوجيز في جرائم الصحافة والنشر ، مرجع سابق ، ص 20.

[3]- د علي جابر الحسيناوي ، مرجع سابق ، ص 113.

فإنه وفقا لتلك المواد سالفة البيان لا يعتبر مرتكبا لجريمة وحتى يندرج فعله تحت طائلة العقاب لابد له من بيع هذه المواد أو حيازتها بقصد البيع أو التوزيع أو العرض على الغير، و ذلك باعتبار أن قصد الاستغلال أو التوزيع أو العرض على الغير شرط لقيام الجريمة ، وفي هذا الإطار يشمل التجريم الإعلان عن أية مواد مخلة بالآداب العامة ، مهما كانت كيفية الإعلان التي تتم عبر أنظمة المعلوماتية كعرض إعلان لموقع جنسي أو لتقديم خدمات جنسية

و بتحقق القصد الجنائي بإتجاه إرادة الجاني إلى إرتكاب الأفعال المنصوص عليها في المادة السالفة الذكر مع علمه بأن هذه الأشياء مخلة بالآداب العامة، وكذلك فإن القصد الخاص هنا أن يكون صنع أو إستيراد أو حيازة أو نقل تلك المواد المذكورة بقصد الإستغلال أو التوزيع أو العرض على الغير.

الفرع الثاني جريمة الحض على الفسق و الدعارة

و المقصود بالحض على الفسق أو الدعارة[1] أن يكون ذلك عن طريق التأثير في نفس المجني عليه ذكرا كان أو أنثى، بهدف إقناعه بارتكاب الدعارة أو الفسق سواء بتزيين الفكرة له أو بترغيبه فيها أو بوعده بالتحصل على العديد من المكاسب أو الأرباح من جراء ذلك، وقد يكون الحض مصحوبا بذكر أماكن مباشرة يمارس فيها الفسق والدعارة، أو بذكر أسماء من يرغبون في الممارسة و الاتصال الجنسي، وغير ذلك من الطرق المختلفة و التي تهدف إلى الترغيب و التشجيع على الممارسة، و لهذه الجريمة ركنان مادي و ركن معنوي و هو ما سنتطرق له وفق ما يلي :

أ : الركن المادي

هو فعل الإغراء أو الإستدراج أو الإغواء أو المساعدة على الفسق أو الدعارة، والركن المعنوي يتمثل في القصد الجنائي. وعلى ذلك فإن الركن المادي لجريمة الحض على الفسق وفقا لنص المادة سالفة الذكر يمكن تحققه بأن يعتاد الجاني تسهيل إغواء العامة لإرتكاب الفسق مع الغير بأي وسيلة كانت بهدف كسب المال. كما يتحقق الركن المادي لهذه الجريمة بأي فعل يقوم به الجاني بقصد تحريض الذكور أو الإناث أو استدراجهم إغوائهم أو مساعدتهم لإرتكاب الفسق ، إذا تم هذا الفعل بالكلام أو الصراخ سواء جهر بهما أو نقلا بالوسائل الآلية بحيث يسمعهما في كلا الحالين من لا دخل له بالفعل، أو بالكتابة و الرسوم اليدوية و الشمسية و الأفلام و الشارات و التصاوير على اختلافها إذا عرضت للبيع أو وزعت على شخص أو أكثر. [2]

[1]– يقصد بالدعارة عرض جسم شخص على الغير لاشباع شهواته الجنسية بمقابل ، وما يجرمه المشرع الجزائري هو فعل الوسيط بشان الدعارة دون تجريمه للمرأة الممارسة لفعل الدعارة ، و ذلك ما نلمسه بالمواد من 343 الى 345 ق.ع. ، كما يجرم المشرع كذلك فعل السماح للغير بتعاطي الدعارة ، بالمادتين 346 و 348 ق.ع.

[2]– جميل عبد الباقي الصغير، قانون العقوبات (القسم الخاص) دار النهضة العربية ، ص 172.

ب : الركن المعنوي

و الذي يتمثل في القصد الجنائي المتطلب هنا في هذه الجريمة ، و بالتحديد القصد الجنائي العام المتمثل في علم المتهم بما يقوم به من فعل بقصد إفساد المجني عليه و إتجاه إرادته لتحقيق هذه الأفعال. وهو ما قد يحدث تحديدا بالنسبة للجرائم الممكن حدوثها عبر شبكة المعلومات حيث توجد العديد من المواقع الإلكترونية المتخصصة بالحض على الفسق والتي توفر فتيات مدربات على تأدية أحاديث هاتفية مقابل الحصول على نسبة من عائد المكالمات، وكذلك تعرض إعلانات و دعوات صريحة لممارسة الفسق و الدعارة، بالإضافة إلى نشر أماكن بيوت الدعارة.[1]

الفرع الثالث : الجرائم الجنسية ضد القاصر

يعد مرتكبا لجريمة جنسية على قاصر كل من يجبر قاصرا على القيام بأفعال ذات بعد جنسي أو يرتكب فعلا ماديا ذا طبيعة جنسية مسلطا على جسد القاصر أو من يشجع على القيام بمثل هذه الأفعال أو بالتوسط فيها أو يستفيد منها أو يستغلها عن طريق النشر والتوزيع أو بأي شكل من الأشكال بغاية الحصول على منافع مادية.

فجرائم الاستغلال خلافا للجرائم الجنسية المباشرة لا تسلط مباشرة على جسد القاصر كالاغتصاب أو الفاحشة بهدف إشباع رغبة الجاني الجنسية أو إشباع رغبته في التشفي بل إنها تتمثل في استغلال جسده بغرض تحقيق نفع مادي. ولعله يمكن القول أن هذه الجرائم تعد الأخطر على الإطلاق بين الجرائم الجنسية لأنها تجعل من جسد الطفل بضاعة تباع وتشترى ووسيلة للثراء.

وفي إطار جرائم الاستغلال الجنسي للقصر يجب التمييز بين الأشكال التقليدية لهذا الاستغلال والمتمثلة أساسا في التحريض على البغاء والتوسط فيه و العيش منه، وبين الأشكال الحديثة له التي جاءت نتيجة التطور التكنولوجي في العالم، ولعل أكثر مظاهر هذا التطور سلبية، هو ما وفرته أنظمة المعلوماتية من قابلية لتسهيل إنتاج وتوزيع وانتشار المواد الإباحية المتعلقة بالقاصرين والاستغلال الجنسي لهم وإغوائهم واستدراجهم للفسق وحضهم عليه عبر المواقع الإباحية وغرف المحادثة ومجموعات الأخبار والبريد الإلكتروني .[2]

فبرغم أن هذا الإجرام المستحدث يطال ضرره المتعاملين بأنظمة المعلوماتية بصرف النظر عن أعمارهم أو جنسهم، إلا أن الواقع بين مدى الحاجة لحماية القاصرين بشكل خاص من أن يكونوا عرضة للمواد الإباحية، أو من أن يكونوا محلا لها مما يشكل أذى مادي ومعنوي لهم ، بحيث هناك جملة من الجرائم

[1]- جميل عبد الباقي الصغير، المرجع السابق، ص 174.

[2]– محمد محمود المكاوى ، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والإنترنت) ، مرجع سابق، ص 366.

الجنسية والأعمال الإباحية التي تستهدف القاصرين، من تحريضهم على الأعمال الجنسية وإغوائهم أو محاولة إغوائهم لارتكاب أعمال إباحية، أو تلقي أو نشر المعلومات عنهم عبر وسائط تقنية المعلومات الحديثة من أجل أعمال إباحية، أو التحرش الجنسي بهم عبرها، أو نشر وتسهيل واستضافة المواد الفاحشة لهم عبر الإنترنت، أو تصويرهم أو إظهارهم ضمن أعمال إباحية، أو استخدام الانترنت لترويج الدعارة أو لنشر المواد الفاحشة عنهم.

فقد أتاحت الوسائط الإلكترونية لمستخدميها من الأحداث تخطي كافة العقبات والقيود والرقابة المفروضة على المواد الضارة الواجب حجبها عنهم، ونقل الثقافة الإباحية إليهم، وتزويدهم بكل المعلومات التي تؤدي إلى إفساد أخلاقهم ودخولهم في علاقات غير مشروعة تنتهي إلى أن يكونوا مجنيا عليهم في جرائم جنسية. [1]

و حددت نصوص قانون العقوبات فكرة الآداب العامة وقصرتها على الأفعال المخلة بالآداب التي يمكن أن يطلع عليها طفل أو تلك التي يكون محلها طفل، فالمشرع اهتم بتجريم سلوكيات الذين يستغلون ضعف وعدم نضج الصغار لإرضاء رغبة أو شهوة جنسية يسعى إليها الغير، والهدف من ذلك حماية الصغير[2] ، ذلك أن المشرع جرم بعض الأفعال التي تنطوي على استغلال جنسي للأطفال أو عنيف للأطفال و ذلك بمقتضى المادة 342 من قانون العقوبات التي تتعلق بتحريض القصر على الفسق ، و هي جريمة إفساد الطفل التي يتحقق الركن المادي فيها باتخاذ الجاني سلوكا إجراميا مخلا بهدف إغواء وإفساد الأطفال، يتمثل في تنظيم أو عقد لقاءات تقوم على المعاشرة الجنسية ويشارك فيها أحداث أو قاصرون، وكذلك في شروع الجاني باتخاذ أي نشاط مادي يمكن أن يؤدي إلى ذلك[3] ، والذي قد يتحقق بصورة واقعية أو خيالية[4]، أي عن طريق أنظمة المعلوماتية بتنظيم الاجتماعات التي تنطوي على عروض أو علاقات جنسية يساهم فيها أو يحضرها الطفل[5] ، فصفحات الويب توفر معلومات عن بيوت الدعارة في العديد من بلدان العالم، كما توفر أحاديث هاتفية حية مع فتيات مدربات، مقابل الحصول على نسبة من عائد المكالمات الهاتفية[6].

---

[1]– مدحت رمضان ، جرائم الاعتداء على الأشخاص والأنترنت ، دار الجامعة الجديدة للطباعة و النشر و التوزيع ، ص139.

[2]– جميل عبد الباقي الصغير ، الانترنت والقانون الجنائي ، مرجع سابق، ص 42.

مدحت رمضان جرائم الاعتداء على الأشخاص والأنترنت، مرجع سابق، ص 14 وما بعدها .

[3]) ابراهيم عيد نايل– الحماية الجنائية لعرض الطفل من الاعتداء الجنسي – مرجع سابق – ص 141.

[4]) مدحت رمضان – جرائم الاعتداء على الأشخاص والإنترنت – مرجع سابق – ص 141 .

[5])عبد الفتاح بيومي حجازي، الأحداث والأنترنت، مرجع سابق، ص134.

[6]) محمد مراد عبد الله – الانترنت وجناح الأحداث – مرجع سابق – ص5.

وبناء عليه يتحقق النشاط المادي لهذه الجريمة إذ الجاني اجتماعات تقوم على عروض أو علاقات جنسية يساهم فيها أو يحضرها طفل، دون أن يشارك الصغير في هذه اللقاءات، إذ يكفي أن يكون مجرد شاهد، فإذا قام الجاني حلقات نقاش في مجموعات الأخبار عبر الأنترنت تتعلق بعروض أو علاقات جنسية، فإن الركن المادي يتوافر، وبالتالي تتحقق الجريمة إذا ساهم في هذه الإجتماعات أطفال قاصرين. وفيما يتعلق بالرسالة التي تخل بالآداب العامة للصغير هي تلك الرسالة التي لها صفة العنف أو الإباحة أو يكون من شأنها الاعتداء بشكل جسيم على الشرف الإنساني ، وكذلك الاتجار بهذه الرسالة وينصرف النص المذكور إلى كل رسائل العنف الإباحية أو أية رسالة من شأنها الاعتداء على الكرامة الإنسانية أو الشرف الإنساني[1].

وفيما يتعلق بجريمة استغلال صورة الصغير ، فإن الباعث على تجريم هذه الأفعال هو الرغبة في مكافحة استغلال صورة الصغير أو القاصر، كما أنها وسيلة لمكافحة ظاهرة انتشرت في الوقت الحاضر وهي ظاهرة الشذوذ الجنسي والتي تلجأ إلى وسائل غير إنسانية بالنسبة للصغار مثل تسجيل أفلام إباحية و وضعها على مرأى الأطفال، حيث اتسع نشاط هذه المؤسسات بدءا من الاتجار في المجلات و الأقراص الممغنطة التي تعرض على مرأى ومسمع من الفتيات والأطفال، وهناك دعوات تحث على ممارسة أعمال البغاء مع صغار أو أطفال تم تصويرهم من قبل[2].

ولذلك فإن تجريم المشرع لإساءة استغلال صور الأطفال جنسيا يجد مبرره في أن حرية تبادل الصور الإباحية التي التقطت للصغار، سوف يدفع فئة "هواة أو عاشقي الأطفال" بوصفهم فئة من الشواذ على التفرغ لشهواتهم ورغباتهم، والبحث عن ضحايا جدد لأجل تنويع الصور وجذب أكبر عدد ممكن من الزبائن راغبي متعة الحرام والشاذة في ذات الوقت. ويخلص النشاط الإجرامي في جريمة –إساءة استغلال صورة الطفل جنسيا– في عملية الصنع أو التسجيل أو النقل بغرض عمل العرض أو القيام بالعرض ذاته[3].

ويقصد بالصنع التدخل الإرادي لالتقاط صورة للصغير أو تجميعها عن طريق –المونتاج– بحيث تكون ذات طبيعة جنسية أو تؤدي إلى إيحاء أو دلالة جنسية، وكذلك التسجيل كما لو كان بطريق –كاميرا الفيديو– أو غيرها من وسائل تسجيل الصورة الحية، أو النقل من وسيلة عرض إلى وسيلة أخرى للتسجيل، وذلك في شكل صورة مخزنة، وكل ذلك بقصد العرض، وسواء كان على عدد محدود من الناس أم غير محدد، لأن العبرة هنا هي في السلوك الإجرامي بإحدى الطرق التي نص عليها القانون وهو

[1]) إبراهيم عيد نايل – الحماية الجنائية لعرض الطفل من الاعتداء الجنسي – مرجع سابق – ص 42 .
[2]) مدحت رمضان – جرائم الاعتداء على الأشخاص والانترنت – مرجع سابق – ص 141 .
[3]) جميل عبد الباقي الصغير – الانترنت والقانون الجنائي – مرجع سابق – ص 42.

الصنع أو النقل أو التسجيل بغرض العرض، وتتوافر الجريمة متى قام الجاني بالعرض لصورة مخزنة أو مسجلة أو منقولة ولم يتدخل هو في صنعها أو تسجيلها أو نقلها، ويلحق بعرض الصور الجنسية للأطفال، توزيعها بأي طريقة كانت وبأي وسيلة طالما كان ذلك على طفل أو محل الصورة هو طفل.

وأخيرا فإن نص القانون لم يشترط لقيام الجريمة عرض الصورة بوسيلة خاصة ، و عليه فإن عرضها بطريقة إلكترونية ، يؤدي إلى قيام الجريمة المشار إليها سلفا طالما كان محل الصورة طفلا أو عرضت على طفل ، ذلك لعموم النص وإطلاقه ، فالمطلق يؤخذ على عمومه ما لم يرد ما يقيده. [1]

المطلب الثاني : مدى انطباق النصوص الخاصة بالجريمة المعلوماتية إذا ما تعلق الأمر بالآداب العامة

بعد أن عرضنا للأحكام العامة للجرائم الماسة بالأخلاق و الآداب العامة والحض على الفسق والدعارة في المطلب السابق، سنتناول مدى إمكانية ارتكاب هذه الجرائم عبر أنظمة المعلوماتية ، وما إذا كانت النصوص الخاصة من المرونة بحيث تشمل مثل هذه الأفعال، وفق الآتي توضيحه :

الفرع الأول:التعرض للآداب وإفساد الأخلاق والحض على الفسق عبر أنظمة المعلوماتية

يعد إنتشار الجرائم الماسة بالأخلاق و الآداب العامة و الحض على الفسق والدعارة عن طريق أنظمة المعلوماتية ، يؤدي إلى إعتبارها جزءا من الجريمة سواء أكانت وسيلة لارتكابها أو محلا للجريمة ذاتها، وذلك لما يشوبها من خدمات تتعرض للآداب وإفساد الأخلاق (عبر الأعمال والحركات أو بالكلام أو بالكتابة والرسوم اليدوية و الشمسية و الأفلام والشارات و التصاوير على إختلافها وغير ذلك من الأشياء المخلة بالحياء، بتوزيعها أو الإتجار بها أو الإعلان عنها أو الإعلام عن طريقة الحصول عليها) و الحض على الفسق، وجميع هذه الصور ترتكب عن طريق المعلوماتية ، من خلال المبادلات الإلكترونية الكتابية أو الصوتية أو المرئية ، وهي إما أن تكون بواسطة البريد الإلكتروني ، أو شبكة الويب العالمية أو مجموعات الأخبار أو غرف المحادثات والدردشة ، أو بلوتوث الهواتف المحمولة ، وهو ما نستعرضه وفق ما يلي :

أولا: البريد الإلكتروني

البريد الإلكتروني هو نظام للتراسل باستخدام شبكات الحاسبات يوفر إمكانية الاتصال بملايين البشر حول العالم كبديل للبريد التقليدي ويمكن من خلاله كتابة الرسائل و تضمينها الصور والفيديو و إرسال الرسائل الصوتية أو السمع بصرية، وذلك بعد معرفة عنوان البريد الإلكتروني للمرسل له، كذلك إستقبال الرسائل من أي مستخدم لشبكة الإنترنت، ويقع التعرض للآداب وإفساد الأخلاق و الحض على الفسق عبر البريد الإلكتروني بما يوزع على الناس من الكتابات أو الرسوم أو الصور أو الأفلام و الشارات و التصاوير

[1]– مدحت رمضان – جرائم الاعتداء على الأشخاص والأنترنت – مرجع سابق – ص ص 142/141 .

على إختلافها وغير ذلك من الأشياء المخلة بالحياء، بحيث يتم النشر و الإذاعة عبر البريد الإلكتروني من خلال إرسال الرسالة المتضمنة المواد المسيئة أو التي تشكل تحريضا على الفسق إلى أكثر من شخص، بأن يتم تداول الرسالة بين أكثر من مستخدم لشبكة الإنترنت سواء عن طريق الإرسال المباشر إليهم أو عن طريق الإرسال غير المباشر[1].

ثانيا: شبكة الويب العالمية

لكل مستخدم لشبكة الإنترنيت أن ينشأ له موقع (site) [2]على شبكة الويب العالمية، تتضمن معلومات يمكن إعادة تخزينها و التي يمكن لأي مستخدم آخر في جميع أنحاء العالم استقبال هذه المعلومات من خلال نظم الاستقبال، الأمر الذي جعل شبكة الويب تحفل بالمواقع التي تدعو بشكل سافر و صريح للرذيلة و البغاء، وتقدم خدماتها للجمهور بمقابل أو بدون مقابل، بل و تقوم تلك المواقع بالتعريف عن نشاطها و الدعايا لها بإرسال آلاف الرسائل الإلكترونية لمستخدمي الشبكة. وفي ظل عالمية هذه الشبكة و إنتشارها أصبح بإمكان أي فرد الولوج لتلك المواقع و الإطلاع على ما تتضمنه من مواد مخلة بالآداب (كتابية، صوتية، فيديو صوتية– سمع بصرية)، بل و التواصل عبر هذه المواقع و الإنضمام لعضويتها، حتى وإن كانت قوانين دولته قد تمنع تلك المواقع أو تجرمها.

ثالثا: مجموعات الأخبار

مجموعات الأخبار عبارة عن مناطق مناقشات عامة عبر شبكة الإنترنيت ،يمكن من خلالها التحدث حول أي موضوع ، مع إمكانية تبادل الصور والمعلومات المقروءة أو المكتوبة والمواد الصوتية والفيديوية صوتية (سمع بصرية)[3].

---

[1]- محمد محمود المكاوى ، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والإنترنت) مرجع سابق ، ص 145

[2]– كلمة site (موقع) تعني عقلا إلكترونيا ذا سعة كبيرة يرتبط مباشرة بمجموعة من شبكات الإنترنت، وذلك لتخزين واستقبال وتوزيع المعلومات، ويتطلب بناء موقع على الأنترنت أو صفحة رئيسية home page خادم ويب ومحتوى معلوماتي.

[3]–أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآالي) –دراسة مقارنة – الطبعة الأولى– دار النهضة العربية – القاهدرة –2000 –ص 327.

ونجد أن صورة التعرض للآداب و إفساد الأخلاق و الحض على الفجور تمارس من خلال مجموعات الأخبار[1] عبر ما يتبادله المتعاملين بهذه المجموعات من كتابات و صور و مواد صوتية و فيدوية صوتية وغير ذلك من الأشياء المخلة بالحياء، حيث أن كل المشتركين في مجموعات الأخبار يمكنهم أن يروا ما يرد من مواد تنشر و تذاع عبر حلقات النقاش.

رابعا: غرف المحادثات و الدردشة

غرف المحادثة عبارة عن ساحات معروفة في الفضاء الإلكتروني Cyber space تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض، بإرسال البريد الإلكتروني الذي يمكن قراءته من قبل الشخص المشترك ف غرفة المحادثة.

فالتخاطب عبر هذه الغرف يتم بكتابة المستخدم لرسالته ، حيث يمكن للآخرين رؤية ما يكتبه ، ويتم التعرض للآداب و إفساد الأخلاق و الحض على الفسق من خلال الكتابة.

خامسا: المراسلات الإلكترونية عبر طرفية إنترنت منفصلة:

هناك حالتين لإرتكاب جرائم التعرض للآداب وإفساد الأخلاق والحض على الفسق من خلال هذه الطرفية:

الحالة الأولى: تتعلق بالرسائل الإلكترونية المتضمنة مواد مخلة بالحياء من شبكة الإنترنيت (بواسطة خدماتها المتاحة) إلى الهاتف النقال، سواء كانت رسائل كتابية أو رسوم أو صور أو محادثات صوتية أو سمع بصرية.

الحالة الثانية: تتعلق بالرسائل الإلكترونية من الهاتف النقال إلى شبكة الإنترنت من خلال خدماتها المتاحة.

[1]– هناك تقرير نشرته شبكة (CNN) الإخبارية في موقعها الالكتروني، بينت فيه أن سهولة الوصول للملفات الإباحية اضحت بنفس سهولة الوصول لملفات الموسيقى، وبالتالي فإن تحميل الملفات الإباحية يتم بنفس السهولة التي تتم عند تحميل ملفات الموسيقى – نشر التقرير في 2003/3/15 تحت عنوان: سهولة الوصول للملفات الإباحية www.CNN.com

الفرع الثاني : جريمة مزود الخدمة المعلوماتية المرتبطة بالآداب العامة

يعد مزود الخدمة هو الوسيط بين مستخدمي الوسائط الالكترونية وبين موردي الخدمات ويتم عن طريقه اتصال مستخدمي تلك الوسائط بالمواقع الالكترونية التي يرغبون في الدخول عليها[1].

وقد برزت العديد من التساؤلات حول مسؤولية مزود الخدمة أو ما يطلق عليه البعض أيضا(متعهد الوصول) عما يتم بثه وتداوله عبر شبكة الأنترنت من مواد مخلة بالآداب العامة ،مما أناط بالعديد من الدول نحو إنشاء ووضع ما يسمى ب(البروكسي) (Proxy) بواسطة الشركة التي تزود المشتركين بخدمة الأنترنت ، وهي عبارة عن برامج تتلخص مهمتها في منع أي شخص من الاتصال بمثل هذه الأماكن فتعمل كجدار ناري يمنع الدخول لهذه المواقع إلا بكلمة سر معينة.

ويرى البعض قيام المسؤولية الجنائية ضد مزود الخدمة بينما يذهب البعض الآخر إلى عدم قيام المسؤولية الجنائية في أي حال من الأحوال. [2]

وبهذا الخصوص ألزم المشرع مزودي خدمات الاتصال تجاه عملائهم باقتراح وسائل تقنية معروفة باسم برامج تنقية المواقع ، للسماح بإجراء انتقاء للخدمات والمواقع التي يرغبون في الوصول إليها ،وكذلك اقتراح وسائل أخرى مشابهة على المشتركين لمنع الاتصال أو الوصول إلى عدد من المواقع أو الخدمات و التي منها برنامج أمان الذي إعتمدته شركة إتصالات الجزائر ، وهذا مسايرة لبعض الدول التي سارعت إلى سن التشريعات المناسبة لمواجهة جرائم المعلوماتية الواقعة على الأشخاص ، والمعاقبة عليها سواء بتحميل مزود الخدمة أو مقدمها المسؤولية الجنائية، إذا ما أخل بالإلتزامات المفروضة عليه ،وفي أغلب الدول الأخرى اتخذت موقفا مغايرا وذلك بوضع برامج لمنع المواقع المخلة بالآداب العامة من قبل المؤسسة المعنية بالإتصالات أو الهيئة المختصة بالإتصالات التي تزود المشتركين بخدمات الأنترنت .

وعليه في الأخير يمكننا أن نلمس أنه بالنظر إلى التطور المتنامي والمتزايد في تقنية المعلومات الحديثة والخدمات المقدمة من خلالها وتزايد أعداد المشتركين عبر شبكة الانترنت سنويا بالملايين الأمر الذي أصبح يتطلب تدخل المشرع لمنع المواد والمواقع الإباحية والمخلة بالآداب . [3]

---

[1]– محمد عبد الظاهر حسين – المسؤولية القانونية في مجال شبكة الأنترنت– دار النهضة العربية – 2002 –ص 37.

[2]– روكز رزق – ورقة عمل مقدمة إلى الندوة العلمية المتخصصة في المعلوماتية القانونية والقضائية في جرائم المعلوماتية والتجارة الالكترونية وحماية الملكية الفكرية – بيروت 28– 2009/9/30 – ص 39.

[3]– جميل عبد الباقي الصغير – الإنترنت والقانون الجنائي – دار النهضة العربية – 2002 – ص 121 .

و سنقوم من خلال هذا الفصل المعنون ب الإطار الإجرائي لجرائم الآداب العامة المرتبطة بتقنية المعلوماتية الذي قسمناه الى مبحثين بحيث خصصنا المبحث الأول منه للتحديات الأمنية ذات الصلة بمكافحة جرائم المعلوماتية ،ويتضمن المطلب أول التحديات الخاصة بالشرطة القضائية و المطلب الثاني من هذا المبحث دور الشرطة في البحث والتفتيش والضبط.

و نتطرق في المبحث الثاني من هذا الفصل للدليل التقني بين الإشكالات الإجرائية و قبول مشروعيته و مصداقيته بحيث نخصص المطلب الأول منه الإشكالات الإجرائية للدليل التقني ، بينما خصصنا المطلب الثاني منه مشروعية الدليل التقني و مصداقيته .

المبحث الأول: التحديات الأمنية ذات الصلة بمكافحة جرائم المعلوماتية

يمتد الجدل والنقاش إلى التساؤل عن مدى كفأت آليات مكافحة الجرائم الجديدة سواء من حيث التقنية العلمية المستخدمة، أو من حيث تأهيل العناصر البشرية القادرة على اكتشاف الجريمة ذات الطبيعة التقنية المعقدة، والتحقيق فيها. والقدرة على التعامل مع مختلف القرائن والأدلة الرقمية أحياناً، ناهيك عن قصور التشريعات الدولية والوطنية في معظم الدول[1].

والمشكلة التي تواجه مجتمعات اليوم (والأجهزة الأمنية تحديداً) أن الجريمة في مظهرها القديم لم تختفي بل زادت، وظهرت علاوة عليها أنماط من الجرائم المستحدثة زادت من حجم الضحايا والخسائر على كافة المستويات ، وإدراكاً لحجم خطورتها يمكن الإشارة هنا إلى أن الرئيس الأمريكي السابق "Clinton" طلب في يناير 2000م من الكونغرس تخصيص مبلغ 2 بليون دولار كميزانية لأمن الحاسبات وحدها.

وفقاً للمفهوم الحديث للأمن الذي يرى بأن هذا المدلول لا يقتصر على الجانب الجنائي الذي تقوم عليه الأجهزة الأمنية التنفيذية، يمكن أن نحدد العديد من التحديات الأمنية المصاحبة للجريمة المعلوماتية ، ولكن قبل هذا يحق لنا القول بأن النظرة التقليدية لمفهوم الأمن الذي تختزله في الأجهزة الرسمية تخل بأهمية أدوار المؤسسات الاجتماعية الأخرى التي تقوم بمهام كبيرة ضمن مفهوم أرحب، ومنظمة متكاملة تندرج كلها تحت مفهوم الأمن الشامل الذي يشمل كافة الصور المختلفة التي تسهم مجتمعة في تحقيق الأمن في صورته المتكاملة للجميع.

المطلب الأول: التحديات الخاصة بالشرطة القضائية

ظهرت شبكة الإنترنت بميزاتها الكثيرة عابرة للحدود الجغرافية، والثقافية، والسياسية، وحتى الدينية، وعلى منتديات الإنترنت، ومن خلال واقعها، وتطبيقاتها بات مفهوم السيادة الوطنية محل تساؤل. فعن طريق هذه الوسيلة بات ممكناً تنظيم الاجتماعات بين المجموعات الإجرامية لتنسيق المواقف، وتبادل المعلومات، والخدمات. كما بات ممكناً مع الإنترنت تزايد حالات الاختراق مثل قضايا التجسس المعلوماتي والاقتصادي، وبث الشائعات والأخبار المكذوبة، لإحداث البلبلة بين أفراد المجتمع.

ومع انتشار التقنيات الحديثة التي أظهرت تلك الجرائم المعقدة والتي تتطلب تعاطياً مهنياً، أمنياً، على نفس درجة التحدي.

[1]– اشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015، ص85.

وحتى يمكن وضع تصور عام للبيئة الإجرامية التي تتم فيها الجريمة المعلوماتية ومن خلال تحليل خصائص هذا النمط من الجرائم التي يتضح أنها تتم وفق ظروف موضوعية مختلفة تتمثل في الآتي:

- ضعف سبل المقاومة ضعف الإعداد الفني والبشري.
- صعوبة وضعف وسائل التحقيق الروتين، وعدم أجهزة الأمن، ويصعب عملية التدريب.
- التكلفة العالية لأساليب المكافحة الأجهزة، والتعليم والتدريب.
- التقنية، واستخداماتها السلبية أسرع من التشريعات.
- مخترعات، ووسائل المكافحة غالباً ما تأتي متأخرة الفعل ورد الفعل.
- تدني مستوى الوعي الإداري، والاجتماعي بخطورة المشكلة.
- قلة الاستثمار في مجالات البحث العلمي للمساهمة في مكافحة جرائم التقنية.

وفي ضوء ذلك كله يمكن تمييز بعض الخصائص الرئيسة للجريمة المعلوماتية منها:

- يسهل نظرياً ارتكاب الجريمة ذات الطابع التقني.
- يسهل إخفاء معالم الجريمة، وصعوبة تتبع مرتكبيها.
- الحرفية الفنية العالية التي تتطلبها سواء عند ارتكابها أو مقاومتها.
- تعدد الأطراف المرتبطة بها حيث يلعب البعد الزمني اختلاف المواقيت بين الدول، والمكاني الجريمة، وهو يعكس بطبيعة الحال اتساع نشاطها.
- أن جريمة الإنترنت تتطلب قدراً كبيراً من الذكاء والمعرفة من مرتكبها وفريق المكافحة.
- تتم الجريمة بشكل سريع، وحاسم أحياناً في دقائق معدودة.
- ترتكب الجرائم عبر الإنترنت بدقة بالغة نتيجة دقة أدوات الجريمة (برامج).
- التخفي عبر دروب الإنترنت هو أهم ما يميز مرتكبي هذه الجرائم، بحيث يمكن أن يختفون تحت قناع فني يظهرهم من دولة إلى أخرى.
- جرائم الإنترنت تتسم بالغموض حيث يصعب إثباتها، والتحقيق يها، كما هو الحال في الجرائم التقليدية.
- الصورة الذهنية لمرتكب جرائم الإنترنت غالباً هي صورة البطل، والذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يتوجب محاكمته.
- في أغلب الأحوال لا تستخدم أساليب عنيفة من قبل مرتكبي جرائم الإنترنت.

- كثير من جرائم الإنترنت لا يتم الإبلاغ عنها.[1]

لهذا كله نجد أن جرائم المعلوماتية تستدعي وجود نخبة متميزة من المحققين من ذوي التأهيل، واستعداد جيد حيث يتطلب التحقيق في الجرائم ذات الطبيعة التقنية قدراً كبيراً من التخطيط، والمهارة ، حتى يمكن أن تكتمل عناصر القضية بشكل دقيق يتفق وطبيعة هذه الجرائم. وتأسيساً على ذلك فإن بعض الخبراء يرى أن من الضروري وضع حدود فاصلة، وواضحة لإجراءات المكافحة، والتفريق بين إجراءات الوقاية، ومسائل الضبط، والمتابعة، وإجراءات مباشرة جرائم الحاسب[2].

وإجمالاً يمكن الإشارة إلى بعض النقاط الأساسية التي ربما يحسن للمحقق أخذها في الاعتبار ومنها :

- تحليل المشكلة (بمعنى تحليل الجريمة).
- ينبغي على المحقق المبادرة بالتحقيق فور تلقي التقرير بوجود نشاط إجرامي، أو جريمة ذات طابع تقني، واستغلال عامل الوقت.

كما أن المحقق يحتاج بعد تحليل العناصر الأساسية للقضية إلى النظر في الموضوع في ضوء الأسئلة التالية :

- هل هناك قضية وبالتالي عمل جنائي يتطلب التحقيق؟
- هل كان جهاز الحاسب ذاته هدفاً للدخول على المحتويات بقصد التعديل أو سرقة معلومات أو تخريبها سواء كان الجهاز شخصياً، أو متصلاً بالشبكة.
- ما مدى الأضرار على الشخص الذي كان ضحية لجريمة ذات بعد تقني، وكيف يمكن تحجيمها؟
- هل اكتملت عناصر الموضوع بصفة واضحة، وجلية ؟
- هل يمكن إشراك عنصر، أو عناصر موثوقة من منسوبي المكان الذي ارتكبت فيه المخالفة لتسرع الإجراءات، وفهم طبيعة النظام الإلكتروني بشكل سريع؟
- هل يوجد لدى المحقق ما يكفي من المهارة الفنية لمواجهة المتهم إن وجد بالحقائق ومناقشته بشيء من الندية في كافة التفاصيل.

[1] اشرف عبد القادر قنديل، المرجع السابق، ص96.

[2]–عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة والنشر والتوزيع ،سوريا ،سنة 2011 ،ص124

- هل يمكن تقديم نصيحة أمنية من خلال التحقيقات لتساعد الشخص في تجنب تكرار ما حصل.

وبشكل عام فإن أهم وسائل المكافحة تبدأ بالاستعداد الجيد سواء من حيث إعداد الكفاءات البشرية المؤهلة، أو إنشاء الوحدات المتخصصة للتحقيق في جرائم المعلوماتية ، ويترافق مع هذا ضرورة توفير الموارد المالية اللازمة لهذه الوحدات التي ترصد، وتضبط ظواهر إجرامية تتسم بالتغير، والسرعة تحتاج معه إلى مرونة في القرار الأمني، والقرار المالي.

المطلب الثاني: دور الشرطة في البحث والتفتيش والضبط.

بصدور القانون رقم 04/09 المؤرخ في 05 أوغست 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، الذي وضع قواعد خاصة للوقاية منها وحدد المفاهيم العامة لما هو متصل بتكنولوجيات الإعلام والاتصال ومجالات التطبيق ومراقبة الاتصال خاصة[1] ، وكذا القواعد الإجرائية المتعلقة بالتفتيش[2]، حجز المعطيات [3] وكذا التزام مقدمي الخدمات[4].

بحيث تختص وحدات متخصصة من أجهزة الشرطة بمكافحة جرائم الإنترنت بعد تلقي التعليم والتدريب الكافيين على استخدام شبكات المعلومات واستخدام الأجهزة الفنية الحديثة والمعرفة الكافية باللغات الأجنبية، ما يسمح لها القيام بإجراءات التفتيش والضبط والتحفظ على الأدلة التي تساعد على إثبات الجريمة. وعلى الرغم من عدم اختصاص هذه الوحدات، بملاحقة بقية الجرائم التي ترتكب بواسطة الإنترنت مثل مكافحة المخدرات وغسيل الأموال والإرهاب والدعارة واستخدام الكروت الإلكترونية وجرائم التجارة الإلكترونية، إلا أنها تلعب دوراً هاماً في معاونة الأجهزة القائمة على مكافحة هذه الجرائم باعتبارها متخصصة في مجال الحاسبات الإلكترونية. فهي تقدم لباقي الوحدات دعماً فنياً في مجال البحث والتفتيش وتحليل المعلومات التي يحصلون عليها وتحضير الوثائق الرسمية بالنسبة لما حصلوا عليه من وثائق والمثول أمام المحاكم للشهادة.

[1]– المادة 04 من القانون 04/09

[2]– المادة 05 من القانون 04/09

[3]– المادة 06 من القانون 04/09

[4]– المادة 10 من القانون 04/09

أولا :البحث الجنائي في مجال جرائم المعلوماتية

يعتقد البعض أن الإنترنت وشبكات المعلومات كمجالات فضائية يصعب فيها تطبيق القانون وذلك لمداه الدولي وغياب نقاط المراقبة على الشبكات، وتقنيات إرسال الرسائل، وعدم ذكر الأسماء أو التحقق من هويتهم، وتشفير التوقيعات الكتابة السرية وهي خصائص يتميز بها الإنترنت تجعل من الصعب تحديد شخصية وملاحقة مرتكب الأفعال المجرَّمة. مما يعقد عمل الشرطة والعدالة وربما تبقى في الكثير من الأحوال مكتوفة الأيدي.

إلا أن هذا التحليل غير صحيح للأسباب التالية :

- يجب العلم بأن الأفعال المجرَّمة التي ترتكب في داخل حدود الدولة، دون أن يمتد أثرها إلى خارجها، يستطيع المحققون أن يتصرفوا حيالها دون مصاعب أو تعقيدات.
- إن عدم معرفة شخصية الفاعل التي يتستر ورائها مرسل الرسالة غير المشروعة هو أمر نسبي إذ لا يوجد "تجهيل" بالمعنى الصحيح بالنسبة لشبكة المعلومات حيث يترك الفاعل "آثاراً" أثناء تنقله في طرقات شبكة المعلومات تسمح للمحققين الوصول إليه.

وأخيراً فإن الطابع الدولي للجريمة لا يمثل عقبة تمنع إجراء التحقيق والملاحقة وإلا ستساعد على خلق (جنات افتراضية) تمثل خطراً على الأمن العام الدولي.[1]

ثانيا : مراحل تتبع الجريمة

إذا كان تحديد هوية الفاعل بالنسبة لشبكات المعلومات لم يعد وهما، فإن الكشف عن الشخصية الحقيقية للشخص الطبيعي الذي ارتكب الجريمة ما زال يواجه الكثير من الصعاب.

لذلك من الضروري تحسين أسلوب تتبع "آثار الرسائل" وتحديد هوية المستخدمين حتى يمكن تحريك دعوى المسؤولية. وهنا يظهر أهمية دور مؤدي الخدمة كهمزة وصل ضرورية بالنسبة لنقل المعلومات. ويوجد العديد من المقترحات في هذا الصدد.

[1]- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007،ص91

أ :تحديد شخصية المشتركين بشبكات المعلومات

من الضروري تحديد هوية المشتركين بشبكات المعلومات لتسهيل عمل الشرطة في حال وقوع أي مخالفة، حيث يجب على مؤدي الخدمة أن يكون قادراً على تقديم بيانات شخصية عن زبائنه، في إطار التحقيقات التي تتم بواسطة الشرطة أو رجال النيابة عندما يطلب منه ذلك. هذا الأمر يقتضي من مؤدي الخدمة أن يطلب البيانات الشخصية لكل عميل يطلب الاشتراك عبر شبكته.[1]

وهنا تثار مشكلة جديدة بالنسبة للاشتراكات المجانية التي تتم دون تحديد هوية المشترك. هذه الاشتراكات هي التي تسهل ارتكاب الجرائم في ظل غياب أي تحديد لهوية أو مكان المستخدم وهو ما يصعب منعه أو إلغاؤه.

ب :حفظ البيانات المتعلقة بالاتصال بواسطة مزودي الخدمة

البيانات التي تتعلق بالاتصالات التي يقوم مؤدي الخدمة بتجميعها أوتوماتيكيا عند توصيل المستخدم بالشبكة، تعد ذات قيمة معلوماتية كبرى لرجال التحقيق. ويظهر فيها المستخدم، ووقت بداية ونهاية الاتصال[2] ، والرقم الكود للمتصل، والمواقع التي زارها، والمعلومات التي طلبها والبيانات التي حصل عليها هذه المعلومات وغيرها تعد بمثابة الآثار التي يتركها المستخدم.

وتحفظ هذه البيانات بواسطة مؤدي الخدمة لفترات متغيرة حسب أهمية وكثافة تردد العملاء ومن المهم الاحتفاظ بهذه المعلومات لفترة كافية، حتى يمكن تسهيل عمل رجال البحث في متابعة وإقامة الدليل على المخالفات التي ترتكب.

وتعد هذه البيانات الهدف الرئيسي والمهم لعمل رجال الشرطة، أنظر لشدة وكثافة ارتكاب هذه المخالفة. إلا أن تلك البيانات لا تحفظ إلا لمدة يومين فقط، بينما مدة حفظ المعلومات المتعلقة بالاتصالات التليفونية بواسطة Alcatel هي عام كامل.

لذلك يجب مد مدة حفظ البيانات بالنسبة لشبكات المعلومات لمدة لا تقل عن ثلاثة أشهر وتوقيع جزاء على المخالف. وبالرغم من ذلك فإن هذا الإجراء يبدو غير واقعي بالنسبة للرسائل الإلكترونية، حيث يتم مسحها بانتظام بواسطة مؤدي الخدمة نظراً لكثافة عددها والاجتماعات والمناقشات التي تتم كل لحظة.

[1] آمال قارة، المرجع السابق، ص94.

[2] بكري يوسف بكري، الجرائم الإعلامية ضد الأحداث، الطبعة الأولى، دار الفكر الجامعي،2011، ص38

وتكون بعض الأدلة قاطعة الدلالة، أحياناً، أكثر من شهادة الشهود ويلزم أن ننوه هنا بأن المحاضر الأولية في هذا الصدد تتمتع بقيمة وأهمية خاصة حيث أنه لا يمكن عملها إلا بواسطة ضباط الشرطة أو الأشخاص المحلفين أو من لهم صفة الضبطية القضائية بموجب نصوص خاصة.

والدليل القانوني هو ما يستمد من أعمال التحقيق الذي يختلف بطبيعته عن أعمال الاستدلال التي لا يتولد عنها أدلة بالمعنى القانوني، ولا يجوز أن يكون سند القاضي في الحكم أدلة وردت في محضر الاستدلال. ولكن يمد النيابة العامة بما يسمح برفع الدعوى الجنائية بناء على هذه الأدلة كأساس للتحقيق الذي يستخلص منه الدليل في معناه القانوني[1].

ج :التفتيش والضبط

يتم التفتيش في مكان معين بهدف الكشف عن أشياء أو تجميع أدلة خاصة بجريمة ما حتى يمكن استخدامها في ملاحقة المجرمين. وأما الضبط يحدث عند الحصول على تلك الأشياء أثناء التفتيش ويطلق عليها مضبوطات أشياء لغرض التحقيق أو إثبات أدلة تتعلق بالجريمة.

ويجب على ضباط الشرطة القضائية إجراء المعاينات من خلال الانتقال إلى مكان الواقعة وإثبات حالة الأشياء والتحفظ على الأدلة والقرائن المادية التي تفيد في إثبات وقوع الجريمة ونسبتها إلى مرتكبيها. الفكرة الأساسية لهذين التعريفين هو إجراء تحقيق معمق في نفس المكان وهو إجراء جنائي.

والسلطة المنوط بها البحث عن المعلومات وإجراء التحقيق والقيام بالضبط تقوم بفحص الأماكن بواسطة الضابط المختص عندما يكون لديها الأسباب المعقولة للاعتقاد بأن الجريمة قد وقعت أو ستقع لتقوم بالبحث عن الأدلة المتعلقة بهذه الجريمة وتقوم بالفحص الدقيق بهدف منع وقوع الجريمة أو معاقبة فاعلها.

ويسمح إذن التفتيش للشخص المكلف بتنفيذه سلطة تفتيش المكان للبحث عن الأشياء وأيضاً البحث في داخل النظام المعلوماتي الموجود في المكان المحدد للحصول على معلومات يمكن أن تستخدم كدليل على ارتكاب الجريمة وضبط وحفظ هذه المعلومات.

[1] – تشمل الأدلة الجنائية الإلكترونية على عملية العثور على المعلومات وفلك كلمات المرور التي تحميها، وفحص المعلومات المختزلة، وتعقب مصدر البريد الإلكتروني، وقراصنة البرمجيات، واسترجاع البيانات المحذوفة، وربط المعلومات والأقراص المرنة بالحسابات التي تم تكوينها بواسطتها ومراقبة الحاسبات الآلية عن بعد، وكذلك الاحتفاظ بالأدلة الإلكترونية من أجل تقديمها في المحكمة.

وهناك اعتباران يجب أخذهما في الحسبان بخصوص إذن التفتيش :

- إن من يرخص بالتفتيش سواء القاضي أو النيابة يجب أن يلتزم بالحياد وعدم الانحياز بين الطرفين المعنيين، المصلحة العامة والمصلحة الخاصة.
- إن من يطلب الإذن بالتفتيش يجب أن يقسم بأن لديه من الأسباب المعقولة (وليس فقط وساوس أو شكوك) تحمله على الاعتقاد أن هناك جريمة قد ارتكبت وأن هناك أدلة موجودة في المكان المطلوب تفتيشه.

د :أسلوب التفتيش عن البيانات على شبكة المعلومات

يتم التفتيش عن البيانات بإحدى طرقتين :

إما معرفة رقم الاتصال الذي تم من مسرح الأحداث، أي على نفس الحاسب المستخدم في ارتكاب الجريمة.

أو نقل محتويات الاسطوانة الصلبة الخاصة بالجهاز وتفتيش المكان.

ويجب على ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة.[1]

ولكي ينجح المحققون في عملهم يجب أن يقتفوا أثر الاتصالات منذ الحاسب المصدر إلى الحاسب أو المعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل ودولة. ولكي تحدد الشرطة مكان الجريمة التي ترتكب عادة في الملفات القديمة التي تبين لحظات مختلف الاتصالات

كما يجب على رجال الشرطة، في حالات أخرى، متابعة الاتصال لحظة إجرائه الأمر الذي يستلزم دائماً تعاون ومساندة زملائهم في الدول الأخرى.

[1] آمال قارة ، مرجع سابق ص120

المبحث الثاني: الدليل التقني بين الإشكالات الإجرائية و قبول مشروعيته و مصداقيته

أثرت تقنية المعلومات على نوعية الجرائم المصاحبة لها، كما أثرت على الإثبات إذ أصبحت الأدلة التقليدية غير قادرة على إثبات هذا النوع من الجرائم، حيث أصبح الجناة يستخدمون وسائل متطورة تمكنهم من إخفاء سلوكاتهم كاستخدام كلمات السر والتشفير والتلاعب ، وتخريبها و اتلافها ،وذلك بواسطة طرق إلكترونية ، في وقت قياسي قد تكون جزء من الثانية، كل ذلك في إطار بيئة غير مادية هي بيئة النظام المعلوماتي، وهو ما يضعف بكثير من قوة الأدلة التقليدية المعروفة من حيث كفايتها في إقامة بناء الإدانة في هذه الجرائم التي تتم في عالم افتراضي كاعتراف الفاعل بارتكابه للجريمة، والحصول على أدلة مادية عن طريق التفتيش، أو الحصول على أداة الجريمة ،هذا بالإضافة إلى أن إكتشاف هذا النوع من الجرائم يحتاج لطرق إلكترونية متناسبة مع طبيعة الوسيلة المستخدمة بحيث يمكنها فك رموزها وترجمتها إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة، وهو ما يعرف بالدليل التقني .

هذا ولقد اكتنف هذا الدليل ذو النوعية الخاصة إشكالات إجرائية من حيث مضمونه و مميزاته و من ثم معوقات تطبيقه هذا بالإضافة لمشروعيته ومصداقيته للإستدال وهذا ما سنعالجه في المطلبين التاليين:

المطلب الأول: الإشكالات الإجرائية للدليل التقني

الفرع الأول: مفهوم الدليل التقني

حيث يعرف الدليل التقني بأنه "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه"[1]، أو أنه "الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون.[2]

الملاحظ على التعريفات السابقة أن منها من اعتبر الدليل التقني كل معلومات يتم إعدادها أو تخزينها بشكل رقمي كما لو كانت محملة على وسيط معين يمكن قراءته عن طريق الآلة والتي عند تنفيذها في نظام المعلومات تؤدي إلى إنجاز وظيفة ما، وهو بهذا يتلاقى مع البرنامج أي لا وجود لتفرقة بين الدليل التقني والبرنامج فبالرغم من أن كلا المكونان يتفقان في مسألة الالتصاق بتقنية المعلومات من حيث تكوينهما، فهما عبارة عن آثار معلوماتية يتركها مستخدم الانترنت، ويظهران في شكل رئيسي هو الشكل الرقمي، فالمعلومات داخل النظام المعلوماتية مهما كان شكلها فهي تتحول إلى طبيعة رقمية، من خلال تقنية الترقيم التي تتعلق

[1]– مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009،ص 50

[2]– د. خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الموقع التالي: http://kenanaonline.com/users/khaledmamdouh/posts/79345

بترجمة أو تحويل أي مستند معلوماتي مؤلف من نصوص أو صور أو أصوات أو بيانات إلى نظام ثنائي في تمثيل الأعداد قوامه الرقمان الواحد و الصفر[1] ، إلا أن الفرق بين الدليل التقني والبرنامج يكمن في الوظيفة التي يؤديها كل واحد منهما، فالأخير له دور في القيام بمختلف العمليات التي يحتويها النظام ، ذلك أنه لا يقوم بعمله إلا عن طريق مجموعة من البرامج عن طريق إعطاء أوامر بذلك، أما الدليل التقني فدوره يكمن في معرفة كيفية حدوث جرائم الاعتداء على النظام المعلوماتي، لأجل نسبتها إلى مرتكبها[2].

في حين ذهب التعريف إلى إعتبار الدليل التقني للأدلة المستخلصة من الكمبيوتر، و عليه فالمعلومات التي تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية أي التي لا زالت لم تفصل عن أجهزة الحاسب الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها... لا تصلح لأن توصف بالدليل التقني وهو قول غير دقيق في نظرنا ، هذا بالإضافة الى ان الكمبيوتر ليس وحده من يقوم بالمعالجة الآلية للمعلومات حيث أن الهواتف المحمولة و البطاقات الذكية كبطاقة الذاكرة الخارجية تقوم بالدور ذاته و لهذا فان قصر الدليل التقني في الكمبيوتر و اجهزته يعد تعريفا يشوبه النقصان .

ولما سبق نقدم تعريفنا للدليل التقني بأنه "المعلومات المخزنة في النظام المعلوماتي بجميع مكوناته ، أو المتنقلة عبره بأي طريقة إلكترونية ، و التي من ممكن تجميعها وتحليلها باستخدام تكنولوجيا خاصة لتظهر في شكل مخرجات ورقية أو إلكترونية أو معروضة على شاشة النظام أو غيره من الأشكال، لإثبات وقوع الجريمة في إطار الإجراءات المعمول بها ".

و لما كان هذا الدليل يتكون من معطيات ومعلومات في شكل إلكتروني غير ملموس و غير محسوس متواجدة في الأجهزة و المعدات ، فهو يحتاج إلى جوانب تقنية للتعامل معه، و كدليل يحتاج إلى بيئته التقنية للبحث عنه و استخراجه ، و لذلك فهو دليل يخضع للمنطق العلمي[3]،و سنتناول اهم مميزاته وفق ما يلي :

- يمتاز الدليل التقني بالسعة التخزينية العالية:

يمكن تخزين آلاف الصور، مجموعة كتب ، منشورات ، محادثات....إلخ.[4]

---

[1]- النظام الثنائي الرقمي binary اعتمد أساسا للكمبيوتر الرقمي ويمكن من هذا النظام تحويل كافة الأرقام العشرية والحروف والأشكال إلى نظام ثنائي، ويمكن من جهة أخرى الاعتماد على المكافئ له سواء كل نظام ثنائي أو نظام الست عشر، مشار إليه لدى: د. ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (tcp/ip) في بحث وتحقيق الجرائم على الكمبيوتر، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في 26-28 نيسان 2003، بدبي- الإمارات العربية المتحدة، ص 7.

[2]- أنظر في الاتفاق حول ذات المضمون: عائشة بن قارة مصطفى، المرجع السابق، ص 31.

[3]- د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 977.

[4]- د. ممدوح عبد الحميد عبد الطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في: 10-12 مايو 2003، ص 2241.

- سهولة التلاعب بالدليل التقني:

بالتعديل أو الإتلاف أو وضع المعلومات في ملفات رقمية أخرى بسرعة قصوى .

- الدليل التقني يرصد و يحلل معلومات عن الجاني:

من خلال تسجيل تحركات الفرد، عاداته ، سلوكيته، الأمور الشخصية الخاصة، لذا فهو أيسر من الدليل المادي من حيث إستخدامه في مجال البحث الجنائي.

- الدليل التقني مستوحى من بيئته التقنية:

الدليل التقني مستنبط من بيئته الافتراضية المتكونة من أجهزة الحاسوب والخوادم والمضيفات والشبكات ويتم تداوله عبرها.

- قابليته للنسخ:

حيث يستخرج منها نسخ مطابقة للأصل ، التي لها نفس القيمة العلمية، مما يشكل ضمانة فعالة للحفاظ عليه و حمايته من الفقدان و التغيير عن طريق نسخ طبق الأصل منه .[1]

-صعوبة التخلص منه:

على عكس الأدلة التقليدية[2] التي يمكن بسهولة التخلص منها ،من الأوراق والأشرطة المسجلة التي تحتوي على إقرارا بارتكاب شخص للجرائم وذلك بتمزيقها وحرقها، أو مسح بصمات الأصابع من موضعها، أو بقتل الشهود أو تهديدهم بعدم الإدلاء بالشهادة...الخ .

و بالنسبة للأدلة التقنية فإن الحال غير ذلك، حيث يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، مما يؤدي إلى صعوبة الخلاص منها، لأن هناك العديد من البرمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها مثل formes، jpeg rénover، وphotorécit المستخدمة باسترجاع الصور والملفات المحذوفة من الهارد وذاكرة USB[3].

ولا مشكلة تثار فيما إذا تم ذلك الإلغاء بالأمر délecte[4] أو عن طريق إعادة تهيئة أو تشكيل القرص الصلب hard disc باستخدام الأمر format وسواء كانت هذه المعلومات صورا أو رسومات أو كتابات أو غيرها، كل

---

[1]- د. عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الانترنت، ندوة الدليل الرقمي بمقر جامعة الدول العربية بجمهورية مصر العربية، في الفترة من 5-8 مارس 2006، ص 17. مشار إليه عند: د. عبد الناصر محمد محمود فرغلي ود. عبيد سيف سعيد المسماري، ص 15.

[2]- يتشابه كل من الدليل التقني والدليل الجيني أو ما يطلق عليه DNA وبالعربية الحمض النووي، وذلك لاتحاد كليهما في هذه الخصيصة وهي صعوبة التخلص منهما من ناحية، ومن ناحية أخرى يمكن إحداث تعديل في تكوينهما معا.

[3]- للمزيد من التفاصيل حول هذه البرامج أنظر الموقع التالي:

http://www.isecur1ty.org/articles/digital-forensics/221-photorec-recoverjpeg-foremost.html

[4]- USA, v, EDWARD m. stulock, app. 8th cir.no.02- 1401OCTOBER 25, 2002

مشار إليه لدى: د. عمر محمد بن يونس، أشهر المبادئ المتعلقة بالانترنت في القضاء الأمريكي، الطبعة الأولى، دار أكاكوس، 2004، ص 817.

ذلك يشكل صعوبة إخفاء الجاني لجريمته طالما علم رجال البحث والتحقيق بوقوع الجريمة، بل أن نشاط الجاني لمحو الدليل (فعل الجاني لمحو الدليل) يشكل دليلا، فنسخة من هذا الفعل يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقا كدليل إدانة ضده.[1]

– **الطبيعة ديناميكية للدليل التقني** : فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان.

–**عالمية مسرح الدليل التقني:** يمكن لمستغلي الدليل من تبادل المعرفة الرقمية بمناطق مختلفة من العالم، مما يساهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبيا.

–**تطور الدليل التقني بطبيعته:** التي لا تتصف بالجمود بالتبعية للتطور المتواصل في البيئة التقنية.

– الطبيعة الرقمية الثنائية (1–0) للدليل التقني:

ليس للدليل التقني هيئة واحدة، وإنما له خصيصة الالتصاق بمفهوم تكنولوجيا المعلومات من حيث تكوينه، إذ يتكون من تعداد غير محدود لأرقام ثنائية موحدة في الصفر و الواحد (1–0)، والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكون منه، فالكتابة مثلا في العالم الرقمي ليس لها الوجود المادي الذي نعرفه في شكل ورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأي شيء في العالم الرقمي يتكون من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة[2]، وأما تكوين معطياته فإنها تختلف من حيث الحجم والموضوع، إذ كمية الـ (1–0) في ملف يمكن أن تختلف عن الحجم في ملفات أخرى.

[1]– د. ممدوح عبد الحميد عبد الطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، المرجع السابق، ص 2240.

[2]– د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 971.

الفرع الثاني: معوقات الدليل التقني.

تعد المشكلات المثارة أثناء تطبيق قاعدة الدليل التقني في البيئة الافتراضية والتي حتى ولو إذا ما تدخل المشرع كما هو حال المشرع الجزائري الذي عدل أحكام تشريعه الإجرائي بل واستحدث البعض الآخر فإن ذلك لا يقدم حلا متكاملا للمعضلة العملية ما لم يقابل ذلك بحلول أخرى تعمل على القضاء أو التقليل من الصعوبات التي تواجهها أثناء مباشرتها[1] ، وهو أمر غاية في الاهمية لمواجهة هذا النوع المستحدث من الجرائم وذلك لكي نمنع ما يمكن أن يقال من ان صعوبة إثبات واكتشاف هذه الجرائم و التي نوجزها في النقاط التالية:

أولا: المعوقات الخاصة بطبيعة تكوين الدليل التقني

و يقصد بها المشاكل الداخلية فيه والمتعلقة به تحديدا، وذلك بسبب الطبيعة النابعة من تكنولوجيا المعلومات التي يتكون منها هذا الدليل ، و التي تعود على إجراءات الحصول عليه فتضعف من قيمتها إن لم يتم إيجاد حلول بشأنها، و سنفصل فيها كما يلي :

أ: طبيعته غير المرئية و المختلطة:

الشكل المجالي أو النبضات المغناطسي أو الكهربائي للمعلومات الرقمية تفقد الرجل العادي إدراكها بالحواس الطبيعية، فهي متواجدة في عالم افتراضي مبني على جانب معنوي غير ملموس في مكون رقمي مختلط، نتيجته عدم إمكانية وجود فرز، ذاتي في إطار التخزين الرقمي، فمسألة اختلاط الملف المجرم موضوع الدليل الجنائي الرقمي بالملف البريء أمر وارد في البيئة التخزينية في العالم الرقمي[2]، فعلى سبيل المثال ملفات الولوج LOG

---

[1] التحديات التي تعترض الدليل الرقمي تم التطرق لها في المؤتمرات الدولية، ولعل أهمها مؤتمر الإنتربول السادس لجرائم تقنية المعلومات الذي شهدته القاهرة في الفترة ما بين 13 إلى 15/ 4 / 2005 حيث تم تناول هذه التحدي اتمن خلال الورقة التي قدمها وفد مصر ومدير إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، فيتمثل التحدي الأول: ويتمثل في انتشار مقاهي الانترنيت التي يستطيع أي فرد من خلالها أن يتعامل مع شبكة الشبكات، بما فيه المجرم الذي يستخدمها لارتكاب جرائمه، وهو ما يؤدي إلى صعوبة التوصل لمرتكبها، نظرا إلى إمكانية تنتقل المجرم بين أكثر من مقهى خلال اليوم الواحد مما يؤدي إلى صعوبة التوصل بصورة دورية لأدلة الإثبات لقيام تلك المقاهي بإعادة تشكيل الأجهزة، أما **التحدي الثاني** فيتمثل في تكنولوجيا A.D.S.L أو ما يعرف باسم " الانترنيت فائق السرعة" والذي لم يسلم هو الأخر من يد المجرمين، إذا استخدموه لتنفيذ مخططاتهم الإجرامية وذلك عن طريق اشتراكهم إلى جانب أشخاص آخرين في جهاز واحد عن طريق موزع خطوط، مما يؤدي إلى صعوبة التوصل إليهم، أما **التحدي الثالث** فيرجع إلى ظهور الانترنيت اللاسلكي، والذي سهل لهم الانتقال إلى عدة أمكنة في اليوم الواحد[1]، أما فيما يخص **التحدي الرابع** عمليات التخفي PROXY أثناء التجوال عبر الشبكة التي تؤمنها بعض المواقع، التي استغلت من طرف القراصنة بل أن مصممي الفيروسات المدمرة من خلال تلك المواقع قاموا بإطلاق فيروساتهم المدمرة عبر العالم الأمر الذي بات يشكل ظاهرة خطيرة، ولذلك فإننا نقترح إلزام مسؤولي المواقع التي تستخدم البر وكسيات بالاحتفاظ بالمعطيات الأساسية والحقيقية لمستخدمي مواقعهم على الشبكة.

[2] د. عمر بن يونس، الإجراءات الجنائية عبر الانترنيت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصلا إلى الدليل الإلكتروني في التحقيقات الجنائية، المرجع السابق، ص 24.

FILLE تبدو مشابهة للملفات العادية، وممكن جمعها مثل أي ملف آخر وهي تحتوي على كمية هائلة من المعلومات التي قد تفيد البحث والتحقيق الجنائي، إلا أن الصعوبة في جمع هذه المعلومات الجنائية أنها عادة ما تكون مختلطة بغيرها من معلومات مستخدمي الكمبيوتر الابرياء، مما قد يشكل تهديدا لخصوصية هؤلاء[1].

وبالتالي يختلف الدليل التقني عن الأثار المادية الناتجة عن الجرائم التقليدية، فلا تنتج التقنية الشعر والدماء وبصمات الأصابع وآثار الأقدام وما إلى ذلك وإنما ما تنتجه التقنية هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة الي تشكل نظام المعالجة الآلية على أية شاكلة يكون عليها لا تفصح عن شخصية معينة، فضلا عن ذلك غالبا ما يكون الدليل التقني مرمرا أو مشفرا مع وضع عناوين مضللة لها وتخزينها في شكل ملفات غير تقليدية.

فلا مرية أن المجرمين الذين يرتكبون جرائم الاعتداء على نظم المعالجة الآلية من فئة الأذكياء الذين يضربون سياجا أمنيا على أفعالهم غير المشروعة قبل ارتكابها لكي لا يقعوا تحت طائلة العقاب، فهم قد يزيدون من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التي قد تدينهم بترميز أو تشفير المعلومات المخزنة إلكترونيا أو المنقولة عبر الشبكات الاتصال، بحيث قيد يستحيل على غيرهم الاطلاع عليها وبذلك يشكل هذا الدليل عائقا أمام سلطات البحث والتحقيق أثناء تطبيقها للقواعد الإجرائية المقررة لاستخلاصه.

ب: ديناميكية الدليل التقني:

فالأدلة التقنية أدلة ليست أقل من مادية من الأدلة المادية فحسب بل تصل إلى درجة التخيلية في حجمها وشكلها ومكان تواجدها غير المعلن فيهي ذات طبيعة ديناميكية فائقة السرعة إذا تتنقل عبر شبكات الاتصال بسرعة فائقة، بمعنى إمكانية تخزين المعلومات في الخارج ،على خادم ، بواسطة شبكة الاتصال عن بعد وهو ما قد يثير مشكلات عديدة قد تعوق اتخاذ الإجراءات اللازمة لضبط الأدلة التقنية والبحث عنها، لأنه يستلزم القيام بها خارج حدود الدولة في نطاق دولة أخرى حيث ارتكبت الجريمة أو جزء منها[2]، وهذا كله يصطدم بمشاكل الحدود والولايات القضائية، لما ينطوي عليه من مساس بسيادة هذه الدولة، وهذه المشكلة تظهر بصورة جلية حين اتخاذ اجراءات التفتيش لضبط هذه الجرائم عندما يكون نظام المعالجة الآلية متصلا بنظم أخرى خارج الدولة، ويكون تفتيش هذه النظم ضروريا لإماطة اللثام عما تشمله من جرائم.

[1] د. ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP/IP) في بحث وتحقيق الجرائم على الكمبيوتر، المرجع السابق، ص 19.

[2] Dans ce sens. Voir ;Fiche de l AWT. La criminalité informatique. Disponible en lingne à l adresse suivante ;

http;//www.awt.be/contenu/tel/sec/sec,fr,fic,140.000.pdf.

وهو ما يفرض الحاجة إلى الحصول على إذن الدولة التي يتم إجراء البحث في مجالها الإقليمي أو إبرام اتفاقية ومعاهدات دولية ثنائية أو متعددة الأطراف في مجال التعاون الدولي[1] التي تستهدف من وزراء ذلك التقريب بين القوانين الجزائية الوطنية من أجل جمع هذا النوع من الأدلة العابرة للحدود.

وتعد معاهدة المجلس الأوروبي حول جرائم تقنية المعلومات الموقعة في 2001/11/23، والتي أيدتها الولايات المتحدة بقوة هي أول خطوة رئيسية في هذا الاتجاه ويمكن اعتبارها بداية لعمل وضع القواعد والمعايير التي يتوقع من البلدان المعنية أن تتبعها في نهاية الأمر في جهودها.

خصصت اتفاقية بودابيست الباب الثالث منها لدراسة التعاون الدولي coopération international ومن خلال نصت المادة (23) على ضرورة تعاون الأطراف فيما بينها وفق لأحكام هذا الفصل، ومن خلال تطبيق الوسائل الدولية الملائمة بنسبة لتعاون الدولي في المسائل الجزائرية والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك بنسبة لقوانين المحلية، إلى أقصى مدى ممكن، بغرض التحقيقات والإجراءات الجزائية المتعلقة بالجرائم ذات الصلة بالنظم الحاسوبية، والبيانات المعلوماتية، أو لجمع الأدلة ذات الشكل الإلكتروني لمثل هذه الجرائم".

وفي هذا الصدد نجد أن المشرع الجزائري قد خصص الفصل السادس من القانون رقم (09-04) لسنة 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها " للتعاون والمساعدة القضائية الدولية " وما يستنتج ذلك من ضرورة أن تطلب الجزائر الدعم من الدول التي سبقتنا في هذا المجال على غرار اتفاق التعاون الذي وقعته الجزائر بتاريخ 25 أكتوبر 2003 مع فرنسا لمحاربة الإجراء المنظم وبالخصوص الإجرام التقني والمتضمن التعاون الأمني والدعم التقني للشرطة الجزائرية لمحاربة المجرمين الإلكترونيين إذا يجب إذا اقتضت الضرورة وضع قانون يسهل هذا التعاون بين الجزائر والدول الأخرى[2].

ج: إمكانية تعديل أو محو الدليل التقني :

تتم جرائم الاعتداء على نظم المعالجة الألية في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت ويطلق عليها " البيئة التقنية " هذه الأخيرة تعكس على طبيعة الدليل الذي تتجه مما تجعله غير مرئي، وهو ما يجعل أمر طمسه ومحوه كليا من قبل الفاعل أمرا في غاية السهولة وفي زمن قصيرا جدا. وهكذا على سبيل المثال فإن المستخدم الذي يحكم في المعلومات يمكن أن يستعمل نظاما معلوماتيا من اجل محو تلك المعلومات التي تعد موضوعا للتنقيب الجنائي، وبالتالي تدمير كل الأدلة.

---

[1] Emmanuelle L'amandé – Maga Secours , législations et dispositifs de lutte contre la cybercriminalité ; un besoin d'harmonsiation international, disponible en lingne à l'adresse suivante ;

http ;// www.mag – securscom/spip.php ?article 7842.

[2] أطلع على هذا الاتفاق في: ج-ر-م، الفترة التشريعية السادسة، الدورة العادية الرابعة، الجلسة العلنية المنعقدة يوم السبت 27 يوليو 2009، السنة الثالثة، رقم 122، ص19.

وعلى ذلك نرى أنه يمكن الحفاظ على الأدلة ومن ثم ضمان أن الإجراءات التقليدية لجمع الدليل التقني كالتفتيش والضبط لا تزال فعالة في بيئة تكنولوجية تتميز بالتلاشي أو التبخير – وذلك فظلا عن البرمجيات التي يمكن بمقتضاها استرداد كافة الملفات التي تم إلغائها أو إزالتها– إتباع نظام إلزام مزودي الخدمات بالتحفظ على المعطيات المخزنة لديهم حيث أنه إذا لم تتوافر الأدلة على الاتصال وعن عناوين الأشخاص المشتركين في الجريمة فإنها تكون عرضة للاختفاء، وهذا ما نصت عليه اتفاقية بودابيست في المادة 16 من ضرورة السماح لكل طرف لسلطاته المختصة أن تأمر أو تفرض بطريقة أخرى مزود الخدمة التحفظ على المعطيات المعلوماتية المخزنة بما في ذلك المعطيات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي.

وحتى تستوضح الصورة لنا عن هذا الإجراء نعطي المثال عليه: قد يعلم رجال الضبط القضائي بوجود فيروسات في اليوم الأول فيقومون باتخاذ إجراءات الحصول على إذن التفتيش في اليوم التالي، وفي اليوم الثالث يحصلون على الإذن ثم يصل عملهم أن المزود قام بشطب السجلات كالمعتاد في اليوم الثالث المذكور.

إذا التحفظ على المعطيات يعتبر إجراء أولي أو تمهيدي الهدف منه هو الاحتفاظ بالمعطيات قبل فقدانها، وهي المبررات التي حددتها المذكرة التفسيرية لاتفاقية بودابيست[1] والتي تدعو إلى اتخاذ مثل هذا الإجراء وذلك كما يلي:

1– قابلية المعطيات المعلوماتية للتلاشي، حيث تكون محلا للمحو أو التغيير سواء كان ذلك بدافع إجرامي – بهدف طمس معالم الجريمة أو أي عنصر إثباتي لشخصية المجرم – أو بدافع غير إجرامي وذلك في إطار الحذف الروتيني للمعطيات التي لم تعد الحاجة إليها.

2– غالبا ما يتم ارتكاب جرائم الاعتداء على نظم المعالجة الآلية عن طريق نقل الاتصالات عبر نظم الحاسوب، حيث يمكن أن تتضمن هذه الاتصالات محتويات غير مشروعة مثل الفيروسات، فتحديد مصدر هذه الاتصالات يمكن أن تساعد في تحديد هوية مرتكبي الجريمة.

3– تأمين الدليل التقني من الصياغ، حيث يتم نسخ دليل على نشاط جنائي من قبل مزودي الخدمات، مثل المراسلة الإلكترونية التي تم إرسالها أو استقبالها، ومن تم يمكن الكسف عن دليل جنائي للجرائم المرتكبة.

كما نصت عليه التشريعات الأجنبية كالتشريع الأمريكي، إذا نص على هذا الإجراء في القسم (f) 18 U.S.C 2703 من قانون خصوصية الاتصالات الإلكترونية الأمريكي ECPA[2].

يلاحظ مما سبق أن إجراء التحفيظ على المعطيات المخزنة يعد لبعض الدول العربية– كسوريا– سلطة قانونية جديدة فهو أداة تحقيق مستحدثة في إطار مكافحة جرائم تقنية المعلومات، في حين نجد المشرع الجزائري قد

[1] مشار إليها لدى: د – هلالي عبد الله أحم، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق، ص 190 وما بعدها.

[2] "A gent may direct providers to preserve existing record pending the issuance of however, compulsory legal process. Such requests have no prospective effect " .

نص في القانون رقم (09- 04) لسنة 2009 بشان الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على إجراء الحفظ وذلك في المادة (10) منه.

وباستقرائنا لنص المادة السابقة الذكر نلاحظ أنها بالرغم من أهميتها خاصة إذا تعلق الأمر بتتبع مصدر أو مكان وصول الاتصالات الإلكترونية وبالتالي تحديد هوية الجناة، إلا أن نطاق تطبيق هذه المادة لا يمتد إلى التحفظ على المعطيات، وعليه إذا كان الامر متعلقا بحفظ معطيات سبق وجودها وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها فإن السعي لدى مزود الخدمة بقصد التحفظ عليها فإن الخدمة إلى غطاء من المشروعية يبرر له قيامه بذلك، وعلى ذلك نرى أنه يتعين على المشرع الجزائري أن يتدخل لسن قاعدة قانونية إجرائية ينظم فيها الوضع القانوني للتحفظ على المعطيات المخزنة تحت السيطرة مزود الخدمات وذلك على نحو ما فعلت اتفاقية بودابيست .

ثانيا :المعوقات الخاصة بالعامل البشري

ويتعدد هذا النوع من المعوقات على النحو التالي:

أ: نقص المعرفة التقنية لدى رجال القانون:

لا شك في أن أجهزة العدالة على رأسها الشرطة تلعب دورا رئيسيا إن لم نقل يتوقف عليها أمر تطبيق القانون بصورة كلية.

وإذا كانت لهذه الأجهزة بما لها من خلفية قانونية أهمية كبيرة في التحري عن الجرائم وتحقيقها والبحث عن مرتكبيها في إطار الجرائم التقليدية إلا أن وظيفتها في مكافحة جرائم الاعتداء على نظم المعالجة الآلية لا ترقى إلى نفس الدرجة من الأهمية، ذلك أن الطبيعة الخاصة للبيئة التي تتعامل معها فضلا عن ذاتية الدليل التقني الذي يعيش فيها انعكس على عمل الجهات المكلفة بالبحث والتحري، حيث يتطلب الكشف عن هذه الجرائم إتباع استراتيجيات خاصة تتعلق باكتسابهم مهارات خاصة على نحو

يساعدهم على مواجهة التقنيات المعلوماتية وهو ما تفتقر إليه الجهات المكلفة بالتحري والتحقيق في العالم المادي.

فإذا أضفنا إلى نقطة الدراية الرقمية مسألة التعامل مع الأدلة التقنية وهي التي تشكل عقبة كبيرة أمام سلطات التحقيق، فإننا نكون أمام معضلة أكبر من مجرد الحصول على الدليل التقني، إذا أخذنا في الاعتبار أن مكمن الدليل التقني غالبا هو الحاسوب والخوادم والمضيفات والشبكات ولعل المثال التقليدي التوظيفي الملائم دائما هو قيام رجل الشرطة بوضع حقيبة كاملة تحتوي على اسطوانات الكمبيوتر المصادرة وذلك في صندوق السيارة بالقرب من جهاز الإرسال والاستقبال اللاسلكي فكانت النتيجة أن الإشارات الكهربائية القوية قد تسببت في تدميرها جميعا[1]. لذلك كان من الضروري إعداد إدارة خاصة لمواجهة هذا الاعتداء التقني تعتمد على قوة تكوين البناء العلمي والتكنولوجي لأفرادها تتلقى البلاغات وتلاحق مجرمي التقنية وتبحث عن الأدلة ضدهم وتقدمهم

[1] د- عبد الله حسين علي محمود، المرجع السابق، الهامش رقم(1)، ص 355.

للمحاكمة، وذلك كله ضمانا للنوعية لمواجهة التحديات الأمنية الناتجة عن هذا الإجرام. سيما وأن متطلبات العدالة تقتضي أن تتحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه اكتشاف كافة جرائم تقنية المعلومات، وهذا ما دعت إليه الاتفاقية الأوروبية لجرائم تقنية المعلومات[1]، وكذلك المؤتمر المنعقد في السوربون بباريس 2005/1/19 والذي كان موضوعه الشرطة والانترنيت، وكذا المؤتمر الدولي السادس بشأن الجرائم المعلوماتية المنعقد بالقاهرة في الفترة ما بين 13 إلى 2005/4/15.

وهو ما حدث فعلا، حيث بادرت مختلف الدول سواء الأجنبية أو العربية بإنشاء وحدات متخصصة لمكافحة الإجرام التقني بصفة عامة.

ولعل النموذج المعتاد والأكثر شهرة هو " الإدارة المخصصة لمتابعة جرائم تقنية المعلومات بمكتب التحقيقات الفدرالي FBI[2] في الولايات المتحدة الأمريكية والتي نالت الاعتراف بها كواحدة من أنجح هيئات مكافحة الإجرام التقني، وإلى جانبها نجد إسبانيا التي أنشأت " وحدة التحريات المركزية المعنية بمعلومات جرائم تقنية المعلومات " بصفة عامة وجرائم الاعتداء على النظم بصفة خاصة التي تعمل مع الإدارة المركزية في وزارة الداخلية الاسبانية على مراقبة مرتكبي تلك الجريمة المستحدثة والعمل على إحباط مخططهما الاجرامي، كما نجد أيضا فرنسا إذ لم تسلم هي الأخرى من مخاطر هذا الإجرام ونتيجة لذلك قرر وزير الداخلية الفرنسي السابق Dominique de Villepin بعد اطلاعه على التقرير المقدم له من قبل وزير المالية والاقتصاد Thierry Breton والذي أكد فيه تضاعف كم جرائم تقنية المعلومات بمختلف أشكالها[3]، على ضرورة اتباع مخطط محكم لتحقيق الأمن المعلوماتي، ويتضمن هذا المخطط ما يلي:

---

[1] جاء في المذكورة التفسيرية لاتفاقية بودابيست بيانا لضرورة إنشاء وحدات خاصة كما يلي: " كل طرف في الاتفاقية تكون ملزمة بتبني الإجراءات التشريعية وأية إجراءات أخرى ترى أنها ضرورية وفق قانونها الداخلي والأطر القانونية من اجل إنشاء وتأسيس سلطات .... مقررة داخل القسم الحالي بغرض التنقيبات أو الإجراءات الجنائية النوعية" مشار إليه لدى: د. هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق، ص 171.

[2] والذي يضم بداخله مجموعة اشخاص مدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتم تحصيله من أداة.

[3] كلف وزير الداخلية الفرنسي السابق Dominique de Villepin وزير الاقتصاد والماليةThierry breton في يوليو2004، بتقديم تقرير حول نوعية جرائم تقنية المعلومات الأكثر انتشارا في الوسط الفرنسي، واعطاء نسبة المتضررين منها إضافة الى الاقتراحات اللازمة والمناسبة لمكافحة ذلك الاجرام، ولقد حددت نسبة ذلك الاجرام بحوالي 600000 جريمة سنة2004 حسب الاحصائيات المقدمة من المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات، ومعظم تلك الجرائم تتعلق بالقرصنة المعلوماتية(الدخول غير المصرح به)،

Rapp. Présenté par Thierry breton et remis à monsieur le ministre de l intérieure et de des libertés locales ;Chantier sur la lutte contre la cybercriminalité ,25/02/2005 , disponible en ligne à l'adresse suivante : http : //www.lesechos.fr

– دعم قوات الشرطة والدرك المتخصصين في هذه المكافحة، وذلك عن طريق زيادة عددهم.

–تكوين شبكة خبراء من الشرطة والدرك

والى جانب الاقتراحات لسابقة، يضيف الوزير السابق ضرورة تطوير التعاون مع مراكز البحوث المتواجدة في الجامعات والمؤسسات الكبيرة بغرض تسهيل مسايرهم للتطورات التكنولوجية، أضف الى ذلك ضرورة وضع شهادة مواطن[1]مسندة الى مزودي الخدمات أو الدخول الى الأنترنيت.

كما قامت فرنسا وسعيا الى مكافحتها هذا الاجرام المستحدث بجميع صوره بإنشاء عدة وحدات ومراكز متخصصة وغير متخصصة ضمن الشرطة والدرك لمكافحة هذا الاجرام، وهذا ما اشارت اليه الاتفاقية الاوربية لمكافحة جرائم تقنية المعلومات والتي وقعت وانضمت اليها فرنسا وصادقت على سريانها على ارضها، ومن ذلك المكتب المركزي لمكافحة الاجرام المرتبط بتكنولوجيا المعلومات والاتصالات المعروف اختصارا ب: (OCLCTIC)[2]، قسم الانترنيت التابع للمصلحة التقنية للبحوث القانونية والوثائقية المعروف اختصارا ب:(

–la gendarmerie et la lutte contre lacybercriminalité .disponible en ligne à l adresse suivante http://www.libertysecurity.org/article226.html.

[1]شهادة مواطن: وضعت هذه الشهادة من أجل معرفة الجهود المبذولة من قبل مزودي الخدمات والدخول إلى الإنترنت لمكافحة الإجرام عبر تلك الشبكة لمزيد من التفاصيل أنظر: ’ (Rapp. Présenté par Thierry ,diponible en ligne à adresse précédent)

[2] يعتبر هذا المكتب سلاح الدولة الفرنسية في مكافحة جرائم تقنية المعلومات بصفة عامة بما فيها جرائم الاعتداء على نظم المعالجة الآلية، إلى جانب وحدات أخرى، ولقد تم إنشاءه بموجب مرسوم وزاري رقم (2000– 405) المؤرخ في 15– 5 – 2000 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية.

Décri. n° 2000 – 405 du 15 mai 2000 portant création d’un office central de lutte contre la criminalité liée aux technologies de l’information et de la communication.

وتجدر الاشارة في هذا المقام أن المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال يمثل لفرنسا نقطة الاتصال المركزية التبادلية le point de contact international dans le domaine de la cyber– criminalité الدولية، فهو من جهة يشارك على المستوى الوطني، في تحريك وتنسيق الأعمال التحضيرية اللازمة ومن جهة أخرى، فهو يشارك في نشاطات المنظمات الدولية، كما أنه يحافظ على الروابط العلمية بين المصالح المختصة في البلدان الأخرى ومع المنظمات الدولية (ومن بين تلك المنظمات الدولية التي تسهر على مكافحة جرائم تقنية المعلومات بصفة عامة والجرائم التي تستهدف نظم المعالجة الآلية بصفة خاصة: مجموعة الثمانية G8وأربولEuropol والانتربول Interpol والجنة الأوروبية commotion Europeéne)، وذلك مع مراعات الاتفاقية الدولية – في بحثها – على المعلومات المرتبطة بتلك الجرائم المميزة وكذا المتعلقة بالتعرف وتحديد مرتكبيها، أنظر المادة (7) من نفس المرسوم، وأنظر كذلك:

la police nationale ; la lutte contre la cybercriminalité et les fraudes aux cartes bancaires, disponible en ligné à l’ adresse suivante ; http //www. intérieur. goun. Fr.

STRJD)، القسم المعلوماتي الالكتروني التابع لمعهد البحوث الجزائية للدرك الوطني المعروف اختصارا ب: (IRCGN)، وحدات أقسام الاستعلامات والتحقيقات القضائية المعروفة اختصارا ب: (BDRIJ)[1].

وهذا ما قامت به مصر أيضا حيث أنشأت إدارة مكافحة جرائم الحاسبات وشيكات المعلومات وذلك بموجب القرار رقم 13507 الصادر عن وزرارة الداخلية المصرية[2]أيضا الأردن التي نشأت مديرية الأمن العام قسم خاص يعني بجرائم تقنية المعلومات بصفة عامة ويتولى إجراءات المكافحة والاستدلال والتحقيق في الجرائم التي ترتكب بواسطة النظم هدفا أو بيئة لها وذلك عام 1998[3]، أما والحال بالجزائر فقد تم إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته تتولى تنشيط وتنسيق عملية الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم[4].

ونذكر على سبيل المثال الدرك الوطني الذي كان السباق في إنشاء مركز لمكافحة جرائم تقنية المعلومات ببئر مراد رايس، وأوضح العقيد بالدرك الوطني – معمري – أن هذا المركز الذي سيباشر عمله بعد أشهر قليلة يعنى بتطوير أساليب التعامل مع هذا النوع من الجرائم[5].

---

[1] للمزيد من التفاصيل حول هذه الأقسام، مهامها، أنظر ما يلي:

- Rapp. présenté par Thierry Bereton .disponible en ligne à l'adresse précédente.
- La gendarmerie et la lutte contre la cybercriminalité disponible en ligne à l'adresse suivante http ; //www. libertysecurity.org/ article 226. html.

[2] وهذه الإدارة جديدة في تكوينها ونوعيتها تختص بمكافحة مثل تلك الجرائم، وهي في الأصل تابعة للإدارة العامة للمعلومات والتوثيق، وتخضع للإشراف المباشر لمدير الإدارة، وتشرف عليها فنيا مصلحة الأمن العام، ويشمل البناء التنظيمي لهذه الإدارة على ثلاث أقسام وهي: قسم العمليات، وقسم التأمين وقسم البحوث والمساعدات الفنية وتجدر الإشارة إلى أن إدارة مكافحة جرائم الحسابات و شبكات المعلومات ليست الإدارة الوحيدة المختصة بمكافحة هذه الجرائم بل هناك عدة جهات تسعى إلى تحقيق هذا الهدف، ومن قبيل ذلك الإدارة العامة لمباحث الأموال العامة/ الإدارة العامة للمعلومات والتوثيق، وتعد هذه الأخير من اكثر الإدارات بوزارة الداخلية تعاملا مع الجرائم المعلوماتية، وهي تختص بعملية المتابعة الفنية من خلال التحري عن الجرائم المبلغ عنها من الإدارات الأخرى، كما تقوم بتحديد شخص المتهم من خلال عملية التتبع باستخدام عنوان الانترنيت IP الذي يتعامل من خلاله الشخص مع شبكة الانترنت انظر: د. ايمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، أكاديمية الشرطة، 2003.ص398 وما بعدها.

[3] وقد تم تزويد هذا القسم بمختصين في مجال علوم وهندسة الكمبيوتر وكما تم تزويده بما يلزم من اجهزة ومعدات وبرمجيات تساعده في عمليات التحقيق في جرائم الكمبيوتر وفي فحص الأجهزة المضبوطة في الجريمة والمحافظة على الادلة فيها، وضاح محمود الوضاح، نشأت مفضي المجالي، المرجع السابق، ص 113.

[4] أنظر المادة (13) و (14) من لقانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[5] أطلع عليه على الموقع الإلكتروني التالي:

http ; //www. sawt – alahrar. net/ online/ modules. PHP? Name= News & file= article & Sid= 858.

أما من حيث التكوين والتأهيل فقد قامت الجزائر يبعث إطارات من الدرك الوطني للتكوين والتخصص في البحث والتنقيب، وفي ملاحقة مجرمي المعلوماتية إلى بلدان أجنبية مثل فرنسا والولايات المتحدة الأمريكية وفق اتفاقيات ثنائية للتعاون بين البلدتين[1] كما قامت وزارة العدل الجزائرية وفي تاريخ 2008/12/13 وبالتعاون مع المدرسة الوطنية للقضاء الفرنسية بمقر المدرسة العليا للقضاء بالعاصمة بتنظيم دورة تكوينية لضباط الشرطة القضائية التابعين للمديرية العامة للأمن الوطني وقيادة الدرك الوطني والأمن العسكري والتي كانت بحضور الخبير الفرنسي برنارد سيسمي، نائب الرئيس المكلف بالتحقيق القضائي الجهوي المتخصص بران بفرنسا، وقد نظمت هذه الدورة وعلى حد قول مدير التكوين بوزارة العدل[2] بهدف تعزيز قدرات ضباط الشرطة القضائية خلال التحقيقات الامنية والقضائية في هذا النوع من الجرائم وتكثيف معارفهم القانونية مع عرض تجربة فرنسا في هذا المجال، خاصة وأن الجريمة ظاهرة جديدة في الجزائر[3].

يتضح لنا من خلال ما سبق ذكره أنه مهما نجح المشرع في وضح النصوص القانونية ومجاراته للتطورات التي تشهدها التقنية المعلوماتية يوما بعد يوما إلا أن ذلك يعدو غير كافي ما لم يتبع بإنشاء أجهزة فنية متخصصة يناط بها عملية تطبيق هذه القوانين، وما يطلبه الأمر من إتباع تكوين متعمق في ميدان تكنولوجيات الإعلام والاتصال، ذلك أن توفر استراتيجية تدريبية تعد أفضل وسيلة لتنمية وعي الثقافة المعلوماتية للعاملين يسيرون في خطوات متناسقة مع التطورات السريعة التي صاحبت هذه التكنولوجيا ومواجهتها، لذلك يجب على الجهات المعنية أن تولي التأهيل والتدريب اهتمام خاصا، وذلك بالاعتماد على الكوادر الوطنية داخل وخارج الوطن ومتابعة ذلك بالبحث عن كل جديد حول هذه التقنية وأخذ ما يلزم من الدورات المتعلقة بهذا المجال، فضلا عن الاحتكاك بالكوادر العربية والاجنبية والإفادة من خبرات الدول التي لها تجارب ناجحة في المجال التقني [4] لاسيما أمام الفجوة الرقمية[1] التي يعيشها سكان العالم.

---

[1]la gendarmerie étudie les expériences étrangères afin de combattre la cybercriminalité. disponible en ligne à l'adresse suivante

http ; // www. Alegria. Com/ forums / computer – internet / 21325 – cybercriminalité –en – alg – rie– 4. html.

[2] السيد الحاج محمد أزرقي. مدير التكوين بوزارة العدل الجزائر

[3] كما يضيف مدير التكوين أنه " تم تنظيم دورة من تأطير خبراء أجانب لحداثة الجريمة على اعتبار أن المجتمع الجزائري حيث الإدراك بالتكنولوجيا " والجريمة تفرض تكوين ضباط الشرطة القضائية وتمكينهم من اكتساب تجربة معالجة القضايا باحترافية مستقبلا، واعتبر مدير التكوين أن مثل هذه الملتقيات هي بمثابة تمرين ميداني للمحققين، أنظر أكثر تفاصيل حول هذه الدورة على الموقع التالي:

http ; // www. echoroukonline . com/ara/national/30039.html.

[4]هذا ما أكد عليه الدكتور بشار حافظ الأسد – رئيس الجمهورية العربية السورية – بقوله: " علينا أن نول التأهيل والتدريب اهتماما خاصا في كل المجالات وعلى كل المستويات... وذلك بالاعتماد على الكوادر الوطنية في سورية وخارجها إضافة إلى الاحتكاك بالكودار العربية والأجنبية والإفادة من خبرات الدول التي لها تجارب ناجحة في مجالات محددة ..." أنظر نص الكلمة القومية

ب: إحجام المتضررين عن التبليغ:

إن الطبيعة الخاصة التي تتميز بها الجرائم الاعتداء على نظم المعالجة الآلية، جعلتها تثير العديد من المشكلات، أهمها صعوبة اكتشاف هذه الجرائم وإن اكتشفت فإن ذلك يكون بمحض الصدفة ولا نتحدث من واقع التقنية بالجزائر إذا المتتبع لها يلاحظ ندرة إن لم نقل انعدام القضايا الأمنية والقضائية المنشورة والموثقة المتعلقة بها، إلا أن هذا الواقع من وجهة نظرنا لا يعكس حقيقة الأمور فقلة هذه الجرائم يعود– فيما نرى – إلى عدم اكتشافها والسبب في ذلك هو ذاتية هذه الجرائم من حيث كونها مجهولة ومستترة تتم في بيئة تقنية لا تترك وراءها أي أثر خارجي وذلك عن طريق تلاعب الفاعل غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل المعلومات عن طريقها لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها[2]

والأسوأ من ذلك أنه إذا ما تصادف واكتشفها فإنه يعمد في أغلب الأحوال إلى التستر عليها والصمت بدل استدعاء الشرطة والاعتراف بأنه من ضحايا جرائم الهاكرز.

فقد دلت دراسة أجريت في فرنسا على أن جرائم تقنية المعلومات التي تم اكتشافها لم تمثل إلا (1%) فقط من الجرائم المرتكبة، أما التي تم الإبلاغ عنها فلم تتعد (15%) من النسبة الثانية[3] مما يزيد من الصعوبة لا في مجال اكتشاف وإثبات جرائم الاعتداء على نظم المعالجة الآلية فحسب، بل وفي دراسة الظاهرة برمتها، وهو ما يعبر عنه العلماء الإجرام بالرقم الأسود chiffre noire[4] حيث يعوق رسم السياسة الجزائرية السليمة لمواجهة الظاهرة الإجرامية المستجدة واختيار أفضل الوسائل لمواجهتها.

فكثيرا من الجهات التي تتعرض أنظمتها للانتهاك تعمد إلى عدم الكشف عنها حتى تبين موظفيها لما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة، تجنبا للإضرار بسمعتها وماكنتها واهتزاز ثقة عملائها فيها [5]، لاسيما أن هذه الجرائم تقع بصفة كبيرة على المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة.

الشاملة للرئيس بشار الأسد لدى أدائه القسم الدستوري في مجلس الشعب، مؤسسة تشرين للصحافة والنشر، بتاريخ 2000/07/17، ص 20.

[1] " الفجوة الرقمية " هو تعبير أصبح شائعا خلال السنوات القليلة الماضية، يستخدم للدلالة على الهوة التي تفصل بين من يمتلكون المعرفة والقدرة على استخدام تقنيات المعلومات والكمبيوتر والإنترنيت، وبين من لا يمتلكون مثل هذه المعرفة أو هذه القدرة ذلك أن المجتمع أصبح ينقسم على هذا النحو، بالإضافة إلى اقتساماته التقليدية الأخرى، رأفت نبيل علوه، المرجع السابق، ص171.

[2] ومن أمثلة ذلك إدخال فيروس إلى الجهاز عن طريق الاتصال بشبكة الانترنت ويظل الفيروس كامنا حتى لحظة معينة ثم يقوم بتدمير المعلومات.

[3] د– سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الطبعة الاولى، دار النهضة العربية، القاهرة، 1999، ص95.

[4] أنظر في هذا المعنى: د محمود صالح العادلي، الجرائم المعلوماتية ماهيتها وصورها، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية بتاريخ 2– 4 أبريل 2006، مسقط، عمان، ص8.

[5] محمد عبد الله ابو بكر سلامة ، المرجع السابق، ص97.

إلى جانب ذلك فإن المجني عليه يتردد احيانا في الابلاغ عن هذه الجرائم خوفا من أن الكشف عن أسلوب ارتكاب هذه الأخيرة قد يؤدي الى تكرار وقوعها بناء على تقليدها من قبل الخرين، كما أنّ الاعلام عنها يؤدي أحيانا الى الكشف عن مواطن الضعف في نظام المجني عليه مما يسهل عملية اختراقه[1].

وفي هذا الصدد أوصى المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات والذي عقد في ريودي جانيرو بالبرازيل في الفترة من 4-9سبتمبر 1994 على ضرورة تشجيع المجني غليهم غلى الابلاغ عن الجرائم والشهود، وغيرهم من مستخدمي تكنولوجيا المعلومات، كذلك القرار الصادر عن الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء من ضرورة اتباع تدابير لتشجيع الضحايا على ابلاغ السلطات المختصة بهذه الجرائم. من الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم تقنية المعلومات التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصلهم من أخبار عن وقوع تلك الجرائم على الجهة مع تقدير جزاء عن الاخلال بهذا الالتزام[2].

ويثير مسألة الابلاغ عن الجرائم الاعتداء على نظم المعالجة الآلية مسائل تتعلق بمدى ما هو متاح من نصوص في التشريعيات الجزائية التي توجب الإبلاغ وترتب عقوبة على ذلك، وبالرجوع الى قانون العقوبات الجزائري وفيما يتعلق بالجرائم التي يعلق القانون تحريك الدعوى فيها على شكوى أو طلب من المجني عليه يكون التبليغ عن الجريمة حقا لكل شخص، وهذه هي القاعدة العامة في حق كل مواطن في الابلاغ طالما أن الجريمة ليست ممن يلزم لتحريك الدعوى عنها شكوى أو طلب من الجهة التي حددها القانون.

ولكن هناك حالات يكون فيها الإبلاغ عن الجريمة واجبا على كل من علم بوقوعها ويترتب على الإخلال بهذا الواجب جزاء جزائيا، كالجريمة المنصوص عليها في المادة (91) من قانون العقوبات الجزائري التي تنص على" مع عدم الاخلال بالواجبات التي يفرضها سر المهنة، يعاقب بالسجن المؤقت لمدة لا تقل عن عشر سنوات ولا تتجاوز عشرين سنة في وقت الحرب وبالحبس من سنة الى خمس سنوات وبغرامة من 3000الى 30000دج في وقت السلم، كل شخص علم بوجود خطط أو أفعال لارتكاب جرائم الخيانة أو التجسس أو غيرها من النشاطات التي يكون من طبيعتها الاضرار بالدفاع الوطني ولم يبلغ عنها السلطات العسكرية او الإدارية أو القضائية فور علمه بها..." والجريمة المنصوص عليها في المادة (32) من قانون الإجراءات الجزائية الي تنص على ما يلي "يتعين على كل سلطة نظامية وكل ضابط أو موظف عمومي يصل إلى علمه أثناء مباشرته مهام وظيفته خبر جناية او جنحة إبلاغ النيابة العامة بغير ثوان، وأن يوافيها بكافة المعلومات ويرسل إليها المحاضر والمستندات المتعلقة بها".

[1] د- احمد خليفة الملط، المرجع السابق، ص95. د – خالد ممدوح ابراهيم، المرجع السابق، ص325.

[2] .د-هشام محمد فريد رستم، المرجع السابق، ص25-27.

من هذه الزاوية يجب على أي سلطة عامة وكل ضابط أو موظف عمومي، وذلك حسب النص أن يبلغ بأي جريمة من الجرائم محل الدراسة وصل علمها إليه، إلا تعرض للمساءلة التأديبية، لكن ذلك مرتبط برفع ثقافة رجل الأمن أو الموظف فيما يتعلق بهذه الجريمة نظرا لخصوصيتها وطبيعتها الخاصة التي تختلف تماما عن الجريمة التقليدية، ذلك أن أثار الجريمة ودليلها لا يظهران غالبا، وإن ظهرت فلا يستوضحها إلا خبير أو متخصص في المعالجة الآلية وعلى معرفة بنظم الاتصالات وشبكة المعلومات الدولية، فضلا عن ذلك فإن واجب الإبلاغ المقرر بنص المادة (32) لا يمتد إلى اولئك العاملين في القطاع الخاص وشركاته ومؤسساته وهي الكثرة الغلبة من الجهات التي تستخدم نظم المعالجة الآلية مثل المؤسسات المالية والشركات والمصانع الكبرى التي ليست مملوكة للحكومة[1].

لخذا يجب على المشرع الجزائري أن يسارع إلى تكريس قاعدة قانونية موضوعية يعاقب من خلالها على كل من يعلم بوقوع الجريمة ولا يبلغ عنها ولو لم يكن متضررا منها أو ذا مصلحة، ولا شك أن ذلك كله يصب في مصلحة الدعوى الجزائية وإمكانية استجماع الأدلة التقنية في شأن جرائم الاعتداء على نظم المعالجة الألية وبالتالي مساعدة السلطات العامة على كشف ستر هذا النوع من الجرائم والوصول غلى الحقيقة تحقيقا لصالح المجتمع وأفراده، ولصالح المتهمين أنفسهم لكي لا يدان إلا المسيء ويبرأ البريء، مع ضرورة تفادي البلاغات الكيدية.

إلا أن ما يسجل في هذا الإطار أنه في معظم البلاغات عن جرائم الاعتداء على نظم المعالجة الالية خاصة الرقمية منها فإن إمكانيات توافر الجهالة عبرها أكثر حدة مما هي عليه الحال في العالم المادي، أو بمعنى أخر فإن البلاغات التي تصل إلى الجهات المختصة بالتحقيق كثيرا ما تكون مقيدة ضد مجهول وإذا كان الامر على ما سلف، فهل يمكن التعرف على هوية الجاني الحقيقي؟

- صعوبة تحديد شخصية مرتكب الجريمة:

ويعد هذا التحدي على حد ما في المذكرة التفسيرية لاتفاقية بودابست من إحدى المشاكل التي تطرح للكفاح ضد الإجرام في عالم الشبكات إن لم يكن في نظرنا أهمها وإن كان يمكن معرفة النظام – أي هوية الحاسوب والخادم والمضيف والشبكات – الذي ارتكبت من خلاله ومثل هذا الأمر أوجد اتجاهات في الفقه المقارن تقضي باعتبار مزود الدخول أو خدمات الأنترنت – حسب الأحوال – مسؤولا عن الجريمة حال عدم معرفة شخصية الجاني الأصلي على أساس مبدأ افتراض مسؤولية الغير[2]

فقد أثير في المؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلوا / النرويج في الفقرة ما بين 29 – 31 /5/ 2000 موضوع عدم إمكانية البنية التحتية للإنترنت من التوصيل إلى تحديد شخصية مرتكبة الجريمة، أو المصدر الحقيقي لها، وموقعه على وجه التحديد، وإن كانت توفر إمكانية التعرف على عنوان ورقم الحاسوب

[1] د- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 77 – ص 78.

[2] د- عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 835.

فقط المرتبط بالأنترنت والمستعمل كوسيلة لارتكاب الجريمة أي ما يعرف اختصارا في النظام التقني (IP) الذي يشير إلى رقم يعين الحاسوب الموصل على الانترنت مثل هذا الرقم الذي يحدد هوية الحاسوب الذي استخدم في ارتكاب جرائم الاعتداء على نظم المعالجة الآلية إنما يفيد حال التوصيل إليه اتخاذ اجراءات التحفظ بقصد ضبط، ولكن في مقابل ذلك، فإن هذا الرقم ليس موحدا على المستوى العالمي، إذا أن هناك أقلية من الدول التي تتبعه دون غيرها وخاصة الدول العربية، ففي الولايات المتحدة أو كندا وبعض الدول الأخرى يمكن للشخص فيها اقتناء (IP) خاص به يشير إلى كونه أحد أعضاء الانترنيت ومن ثم يمكن تحديد هذا الشخص بكل سهولة لتبدأ بعد ذلك سلسلة إثبات ارتكابه للجريمة من عدمه.

إلا أنه في دول الاخرى مثل أغلب الدول العربية فإن مصداقية الهوية عبر الانترنت (IP) تتقلص كثيرا إذا علمنا أن كل خط هوية على الانترنت يصادفه عدد من الهويات التي يمكن أن تكون محل للتغاير بين أعضاء الانترنت المشتركين في مزود انترنت واحد وهنا يمكن القول أن مجرد وجود شخص في الجزائر أو في سوريا فإنه يملك فورا هوية رقمية محددة حقا حال وجوده على الانترنت، إلا أنه إذا حدث وانقطع الإرسال فإن الشخص إذا عاد من جديد إلى الانترنت فإن الهوية السابقة لن تكون له وإنما لغيره، إذا من الممكن جدا – بل وهو الامر المعتاد هنا– أن يتواجد بهوية (IP) أخرى.

ونتفق فيما يذهب إليه البعضمن ان الأمر هنا يترك بعد ذلك لفطنة عضو الضابطة العدلية وكيفية تعامله مع الحدث، وهو هنا يستند إلى مسالة الدلائل الكافية وما ينبثق عنها من شبهات كما لو كان الحاسوب الذي تم عبره ارتكاب جريمة الاختراق هو حاسوب شخصي يخص شخص بعينه، وفي هذه الحالة فإن ضبط الحاسوب ذاته يستدعي بالضرورة سؤال صاحبه فيما إذا كان قد استخدم احد غيره الحاسوب المذكور أو يكون الحاسوب المذكور موضوعا في الغرفة الشخصية سيما وأن العادة قد جرت على أن يحتفظ الأشخاص صغار السن بمقتنياتهم الشخصية في غرفهم ولا يسمحون لأحد غيرهم باستعمالها، ومن ثن فإنه ما يتم تحديد هوية الحاسوب (IP) حتى يتمكن في الغالب من الأحوال تعيين المتهم طالما أن الأمر يتعلق بحاسوب موضوع في منزل أو في شركة أو مكتب أو هيئة، إلا أن الامر يزداد صعوبة حين يكون الحاسوب في مكان شبه عام معد لتقديم خدمة للجمهور كما هو الشأن في مقاهي وإن كانت تقوم في العادة بالاستعلام عن اسم عضو الانترنت الذي استخدم الحاسوب فيها فقط كل ما يمكن الحصول عليها معطيات حول هيئته وزمن استعماله للحاسوب ... ومطابقة ذلك مع زمن حدوث الواقعة. [1]

لكن ماذا او كانت المعلومات المحملة في عناوين IP غير حقيقة أو زائفة؟ وهذا ممكن حينما تحث حزم معلوماتية Pocket باستخدام مصدر زائف لمصدر عنوان (IP) بحيث يظهر أن المعلومات جاءت من نظام معالجة محدد بينما في الحقيقة جاءت من كمبيوتر آخر، ومثال ذلك حينما يقوم برنامج خبيث بإدخال معلومات كاذبة أو غير حقيقية عن حقيقية عنوان (IP) في Pocket الإرسال وقبل الولوج في الشبكة المعلوماتية ويحدث

[1] د– عمر أبو بكر بن يونس، المرجع السابق، ص 833.

ذلك حينما يقوم البرنامج الخبيث بإغراق الشبكة بالمعلومات أو إرسال العديد من الرسائل أو حث الماكينة الرئيسية في مزود الخدمة أو الشبكة على الإسراع أو التعجيل في العمل، إلا أنه لحسن الحظ معظم المجرمين لا يعلمون كيف يزيفون عناوين (IP) ولا يعرفون أي من عناوين (IP) يمكن أن تكون دالة على شخص المجرم في الجريمة المحددة[1].

وبعد دراستنا للقواعد المنظمة لاستخلاص الدليل التقني، توضح لدينا مدى الصعوبات والتعقيد التي تكتنف الحصول عليه، وهو ما يفتح الباب لمناقشة مسألة مشروعية الأخذ بهذا النوع من الأدلة ومصداقيتها في إطار نظرية الإثبات الجزائي، وهو ما سنتناوله في المطلب التالي.

المطلب الثاني :مشروعية الدليل التقني و مصداقيته

يعتبر الدليل التقني من الأدلة الحديثة التي أفرزها التطور التقني، وهو ايضا ذو طبيعة خاصة من حيث الوسط الذي ينشأ فيه والطبيعة التي يبدو عليها وهذا يثر التساؤل حول مشروعية الأخذ به، إذا أنه يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا من حيث وجوده والحصول عليه، فمشروعية الوجود تقتضي أن يكون الدليل قد قبله المشرع ضمن أدلة الإثبات الجنائي المعمول بها في قانونا الإجرائي.

كما أن الدليل التقني في تعبيره عن الحقيقة التي تهدف إليها الدعوى العمومية ، لا سيما من خلال الصعوبات المصاحبة لاستخلاصه اضافة للتطور في مجال التقنية مما يتيح العبث بمهامها يؤثر في مضمونها مما يجعلها مخالفة للحقيقة ، و هو ما سنحاول تحديده على النحو التالي:

الفرع الأول : مشروعية الدليل التقني

إن قبول الدليل يتسع ويضيق تبعا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة، فيما إذا كانت تجنح إلى تقييده ، أم كانت تطلق حريته.

ويتيقن القاضي الجزائي في هذه المرحلة أساسا من مدى مراعاة الدليل الجنائي أساسا لقاعدة مشروعية إن منطق الحديث لدراسة مشروعية الدليل التقني يقتضي منا تناول مشروعية وجوده ومن ثم مشروعية الحصول عليه.

أولا :مشروعيته من حيث الوجود

يقصد بمشروعية الوجود أن يكون الدليل معترف به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة[2]، ويمكن القول أن طبيعة نظام الإثبات السائد في الدولة هو المعيار الذي يتحدد على أساسه موقف القوانين المقارنة فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل التقني.

وفي هذا الإطار نجد أن نظم الإثبات لا تخرج عن ثلاث فئات:

الفئة الأولى:

وتأخذ بنظام الأدلة القانونية، حيث تحدد الأدلة التي يجوز للقاضي الجنائي قبولها.

---

[1] د – ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (tcp/IP) في بحث وتحقيق الجرائم على الكمبيوتر، المرجع السابق، ص 18.

[2] طارق محمد الجملي، المرجع السابق، ص 11.

الفئة الثانية: وهي القوانين الأنجلوساكسونية حيث تقيد من حرية الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة، أما في مرحلة تحديد العقوبة فسيود مبدأ حرية الإثبات.

الفئة الثالثة: وهي القوانين ذات الصياغة اللاتينية، حيث تبنى مبدأ حرية الإثبات، ومنها سلطة القاضي في قبول جميع الأدلة وهنا تكون جميع طرق الإثبات مقبولة، ما لم يستبعد المشرع بعضها صراحة وينتمي إلى هذه الفئة القانون الفرنسي (المادة 427 من قانون الإجراءات الجزائية) والقوانين الاخرى التي تأثرت به كالقانون الجزائري (المادة212 من قانون الإجراءات الجزائية) وهو النظام الذي سيكون محل دراستنا على اعتبار اعتناقه من قبل المشرع الجزائري .[1]

وفي هذا الصدد لم نجد المشرع الجزائري وكغيره من التشريعات المنتمية إلى العائلة ذات الأصل اللاتيني أنه قد أفرد نصوصا خاصة تحظر على القاضي مقدما قبول أو عدم قبول أية دليل بما في ذلك الدليل التقني، وهذا أمر منطقي على اعتبار أن الجزائر تستند لمبدأ حرية الإثبات الحر، حيث أصبح هذا الأخير القانون العام في الإجراءات الجزائية في التشريعات اللاتينية، وتتمثل خصائص هذا النظام في أنه لا يرسم للقاضي طرقا محددة للإثبات يقيده بها، بل يترك الخصوم أحرار يقدمون الادلة التي يستطيعون إقناع القاضي بها، ويترك القاضي حرا في تكوين اعتقاده من أي دليل يقدم إليه وهو حر في وزن وتقدير كل دليل، وفي التنسيق بيم الأدلة التي تتمثل في الحكم بالإدانة أو البراءة، دون أن يقيده في هذا الإطار بأي نوع من الشروط سوى تلك التي يتعين عليه تطلبها فيه – أي في الدليل –.

وعليه فإنه في مثل هذا النظام لا تثور مشكلة مشروعية الدليل التقني من حيث الوجود، على ، فالأساس هو حرية الأدلة ولذلك فمسألة قبول الدليل التقني لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه للتقدير القضائي، إلا أن الطبيعة الخاصة للدليل التقني قد اقتضت منا توسيع نطاق بحث مشروعية الوجود إلى مسالة هامة تتعلق بأصالة الدليل التقني.

أ: قبول الدليل التقني في التشريع على أساس مبدأ حرية الإثبات الجزائي:

تعتبر حرية الإثبات في المسائل الجزائرية من المبادئ المستقرة في نظرية الإثبات الجزائي، ويقصد بهذا المبدأ أنه لجميع الأطراف لحرية في اللجوء إلى كافة وسائل الإثبات للتدليل على صحة ما يدعونه، فلسلطة الاتهام أن تلجأ إلى أية وسيلة لإثبات وقوع الجريمة على المتهم، ويستظهر القاضي الحقيقة بكل ذلك أو بغيره من طرق الإثبات[2].

---

[1] أنظر في نظم الإثبات الجزئي بالتفصيل لدى: د– موسى مسعود رحومة عبد الل، حرية القاضي الجنائي في تكوين عقيدته، دراسة مقارنة، الطبعة الأولى، الدار الجماهيرية للنشر والتوزيع والإعلان، 1988، ص19 وما بعدها، د. فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، دراسة مقارنة، دار الثقافة، عمان، 2006، ص 48 وما بعدها.

[2] د– أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجزائية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 1982، ص240.

وقد أقر المشرع الجزائري مبدأ حرية الإثبات الجزائي في المادة (212) من قانون الإجراءات الجزائية حيث نصت على أنه " **يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي**" .

بينما نص عليه المشرع الإجرائي الفرنسي بالمادة (427) من قانون الإجراءات الجزائية الحالي والتي جاء فيها " **ما لم يرد نص مخالف، إثبات الجرائم بجميع طرق الإثبات، بحكم القاضي بناء على اقتناعه الشخصي**"[1] وهذا النص وإن كل مخصصا لمحاكم الجنح، إلا أن مبدأ حرية الإثبات يطبق أمام جميع أنواع المحاكم الجزائية، إلا إذا نص القانون على خلاف ذلك. وهناك العديد من الاسباب التي تبرز الأخذ بمبدأ حرية الإثبات في نطاق نظرية الإثبات الجزائي منها أن حرية الإثبات تعد نتيجة منطقية لمبدأ قضاء القاضي بمحض اقتناعه الذاتي والتي تستلزم بالضرورة منح الحرية للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها حتى يتسنى له أداء رسالته في إرساله العدالة بين المتقاضين.

كما أنه ومن العلم أن الإثبات في الدعوى الجزائية يرد على وقائع قانونية مادية كانت أو نفسية ، التي يصعب الحصول على دليل مسبق لها وذلك بعكس الدعوى المدنية التي يرد الإثبات فيها على تصرفات وأعمال يسهل إعداد دليل مسبق بشأنها[2].

و من بين المبررات الداعية للإخذ بحرية الإثبات ظهور الادلة العلمية الحديثة التي كشف عنها العلم الحديث في إتيان الجريمة ونسبتها إلى المتهم كبصمة الصوت، والبصمة الوراثية D.N.A .

ولا يختلف الأمر في الجزائر بالنسبة للدليل التقني حيث لم يتضمن قانون (09 – 04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها أية وأوضاع خاصة بهذا الصدد، ومن ثم فإن الدليل التقني سيكون مشروعا من حيث الوجود استصحابا للأصل – أي الاصل في الأدلة مشروعية وجودها – وذلك باعتباره من الاساليب العلمية الحديثة في الإثبات الجزائي.

إن أعمال مبدا حرية الإثبات على النحو السابق ذكره يجعل من دور القاضي الجزائي دور إيجابي في كشف الحقيقة الفعلية في الجرائم التقليدية منها والمستحدثة كالجرائم محل الدراسة، ويبدو هذا الدور من ثلاث جوانب:

الأول: له الحرية في توفير الدليل المناسب والضروري للفصل في الدعوى بما في ذلك الدليل التقني.

الثاني : له الحرية في قبول اي دليل ، يمكن ان تتولد منه قناعته بما في ذلك الدليل التقني .

الثالث : انه يتمتع بالحرية نفسها في تقدير قيمتها الاقناعية حسبما تتكشف لوجدانه .

و بالرغم من ان النيابة العامة عليها اقامة الدليل على الادانة والمتهم عليه نفيه بكل الإمكانيات ، إلا أن ذلك ليس معناه عدم تدخل القاضي ،فدوره سلبيا يقتصر على موازنة الأدلة مع بعضها البعض و ترجيح الأقوى منها

---

[1] ART 427 du C.P.PF dispoose que « hors les cas ou la loi en dispose autrement, les infractions peuvent etre établies par tout mode de preuve rt le juge décide d/ après son intime convicition »

[2] د– محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988، ص 409 وما بعدها.

كدور القاضي المدني بل دوره ايجابي ، فمن حقه و واجبه ان يتحرى وينقب عن الحقيقة باتخاذ الاجراء الذي يراه مناسبا ، ويقتنع بمنتهى الحرية ، ذلك في إطاره مسعاه لاكتشاف الحقيقة .

وهكذا فان القاضي الجزائي سواء بناء على طلبات الاطراف او بموجب مقتضيات سلطته ، ان يأمر باتخاذ الاجراء الذي يراه مناسبا وضروريا للفصل في الدعوى[1] ،فيمكنه سماع الشهود او استدعاء الخبراء اذ واجهتها مسالة فنية ، كما لها ان تسال او تستجوب المتهم حول اساس الاتهام الموجه اليه (المادتان (442) و (536) من قانون الاجراءات الجزائية .

اما في مواد الجنايات فقد خول القانون الاجرائي الفرنسي لرئيس محكمة الجنايات بموجب نص خاص وهو المادة (310) من قانون الاجراءات الجزائية سلطة تفويضية بمقتضاها يمكن ان يتخذ كافة الاجراءات التي يعتقد انها مفيدة في الكشف عن الحقيقة حيث لا قيد عليه سوى شرفة وضميره .

وتطبيقا على جرائم الاعتداء على نظم المعالجة الالية ، فان للقاضي الجزائي وفي سبيل الوصول الى الحقيقة له ان يوجه امرا الى مزود الخدمة بتقديم المعطيات التي تسمح بالتعرف على المرسل اليهم الاتصال وكذا عناوين المواقع المطلع عليها ... الخ .

ومن ابرز مؤشرات او دلائل الدور الايجابي للقاضي الجزائي في البحث عن الدليل التقني ايضا ، ان للقاضي الجزائي سلطة الامر باعتراض الاتصالات السلكية و اللاسلكية متى ما قدر فائدة الاجراء وجديته وملائمته لسير الدعوى .

كما للقاضي الجزائي ندب الخبراء وكذا اعلانهم ليقدموا ايضاحات عن التقارير المقدمة منهم ، لما للخبرة في مجال المساعدة القضائية من الدور الكبير ، فهي تعد من اقوى مظاهر تعامل قاضي الموضوع من الواقعة الاجرامية الموضوعة وهذا الاخير يملك تعيين الخبراء سيما ان الاصل يظل للتحقيق التي تجريه المحكمة في الجلسة ، وهذا ما اكدته المادة (143) من قانون الاجراءات الجزائية الجزائري حينما نصت " **لجهات التحقيق او الحكم عندما تعرض لها مسالة ذات طابع فني ان تامر بندب خبير اما بناء على طلب النيابة العامة واما من تلقاه نفسها او من الخصوم .....**"[2]

وفي مجال البحث عن الدليل التقني نجد ان الخبرة التقنية في مجال المساعدة القضائية تعد اقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات ازاء نقص المعرفة القضائية الشخصية لها ، فمما لا شك فيه ان عملية الحصول على الادلة الجنائية التقنية امر صعب الوصول اليه لما تتطلب من خبرة ومهارة كبيرة في مجال تقنية المعلومات ، ويرجع ذلك لتعدد صور و اشكال الإجرام الواقع على نظم المعلوماتية ، مابين مهاجمة المعلومات بغرض تدميرها او الاستيلاء عليها او قد يكون المقصود بالهجوم هو الاجهزة كنشر الفيروس يعمل على اتلاف وحداته الرئيسية مثلا ، او قد يكون الامر مجرد اختراق لكلمة سر خاصة ببنك او مؤسسة

[1]– أحسن بوسقيعة، الوجيز في القانون الخاص، الجزء الأول، ط15، دار هومة للنشر والطباعة والتوزيع، الجزائر، ص98.

[2]– أنظر للمادة 143 من قانون الاجراءات الجزائري.

كبرى بغرض الاحتيال والحصول على الاموال ، وقد تكون بمجرد اثبات الذات واظهار المقدرة العالية في مجال نظم المعلوماتية .

ولما كانت عملية تجميع الادلة التقنية الجزائية في الجرائم محل الدراسة ، تعد من اهم واصعب الامور التي تواجه عملية الاثبات الجزائي لذا كان لزاما ان يتم اللجوء الى خبير قضائي تقني او رقمي ، متخصص ، لاستخلاص الدليل التقني .

تعد مرحلة قبول الدليل التقني المرحلة او الخطوة الثانية التي تلي البحث عن الدليل وتقديمه من قبيل جميع الاطراف (سلطة الادعاء، المتهم ، القاضي).

و في هذا الصدد طبقا لمبدأ الشرعية الاجرائية التي يتحصل من خلالها الدليل الجزائي بما يتضمنه من ادلة مستخرجة من وسائل الكترونية كالكمبيوتر المحمول مثلا ، لا يكون الدليل مقبولا في عملية الإثبات والتي يتم من خلالها إخضاعها للتقدير ، إلا إذا كان مشروعا بأن تم البحث عنه والحصول عليه وفقا لطرق مشروعة[1].

ب- مدى تأثير الأصالة الرقمية في الدليل التقني على مبدأ قبوله:

وهذه المسألة لا يمكن المرور دون بحثها ، فهناك تميز حقيق بين الأصالة في طابعها المادي وبين الأصالة في طابعها الرقمي ، من حيث أن الأولى إن هي سوى تعبير عن وضعية مادية ملموسة ، كما هو الشأن في الورق المكتوب أو بصمة الأصبع أو الحدوث العيني للواقعة ، فهذه كلها لها طابعها المادي المتميز ، في حين أن الثانية ليست سوى تعداد غير محدود لأرقام ثنائية موحدة في الصفر والواحد ، فطبيعة الدليل التقني لا تعبر عن قيمة أصلية بمجرد رفع محتواه على الأنترنت حيث يتواجد في كل مكان يتم استدعاءه منه.

وتبرز هذه المشكلة بصورة جلية عندما يقوم المتهم بإزالة الدليل التقني عن بعد ، فكما هو معلوم يكون ما تبقى منه هو نسخة فقط قد تم التوصل إليها عن بعد أيضا بطريق المراقبة الإلكترونية مثلا ، ومن ثم فهل يكفي ناتج المراقبة الإلكترونية وحده للقول بأن الدليل هنا هو دليل أصلي وبالتالي يقبل طرحه على القضاء؟ وذات السؤال ينطبق على حالة الدليل المسترد بعدما تم حذفه باستخدام خاصية الإلغاء؟

والواقع من الأمر أن بحث موضوع الأصالة على المستوى القانوني جعل المشرع المقارن يعتمد على منطق افتراض أصالة الدليل التقني[2]، حيث نص قانون.

الإثبات الأمريكي في المادة (3/1003) على أنه ، « إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة فإن أية مخرجات طابعة مشا أو مخرجات مقروءة برؤية العين تبرز انعكاسا دقيقا للبيانات تعد بيانات أصلية».

وإن كان ذلك كذلك، فإنها دعوة إلى المشرع الجزائري لكي يأخذ حظه في تقنين هذا النوع من المسائل وأهميته، وتبرز أهمية التسليم بمنطق افتراض الأصالة في الدليل التقني على المستوى القانوني هو في حالة

[1] أنظر في هذا المعنى: عائشة بن قارة مصطفى ، المرجع السابق ، ص125.

[2] د.عمر محمد أبو بكر بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، المرجع السابق ، ص973.

رفضها، إذ لا نكون أمام دليل إدانة، وهو ما يؤدي في النهاية إلى رفض منطق التعامل مع هذه النوعية من الأدلة حال كونها لازمة.

إذا كان مبدأ حرية الإثبات يجيز للقاضي حرية الاستعانة بكافة وسائل الإثبات اللازمة بما في ذلك الدليل التقني لتكوين عقيدته، إلا أن هذا الإطلاق ليس بلا قيد وبلا حدود، وإلا لوصل الأمر إلى درجة الفوضى، بل لكان الأمر قد وصل إلى درجة التساهل بارتكاب جرائم تحت ستار البحث عن الأدلة والتحقيق فيها، لذا كان من الضروري رسم ضوابط وأطر معينة يتعين أن تمارس في نطاقها بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من وراءها، وهو الوصول إلى الحقيقة الفعلية في الدعوى، وإذا كانت هذه الحقيقة تمثل الهدف الأسمى لقانون الإجراءات الجزائية.

ونتيجة لذلك جنحت أغلب التشريعات إلى تحديد الأدلة التي تقبل في إثبات عينة من الجرائم إذ لا يجوز الإثبات بغيرها كأدلة إثبات جريمة الزنا[1].

كما يلزم المشرع أحيانا القاضي الجزائي بإتباع طرق الإثبات الخاصة في بعض المسائل غير الجزائية التي يتوقف على الفصل فيها الفصل في الدعوى الجزائية – أي إثبات المسائل الأولية خاصة المدنية والتجارية منها مثل إثبات عقد الأمانة في جريمة خيانة الأمانة[2]، إلا أن هناك قيدا عاما يحد من حرية القاضي في قبول الدليل بما في ذلك الدليل التقني وهو قيد المشروعية، حيث يشترط في الدليل الذي يبني عليه حكمه أن يكون قد تم الحصول عليه بطريقة مشروعة والقول بغير ذلك يهدر قيمة الدليل وتشوب قضاءه بالبطلان انطلاقا من القاعدة التي تقول: « ما بني على باطل فهو باطل ».

ثانيا : مشروعيته من حيث طريقة الحصول عليه

طبقا لمبدأ المشروعية الذي تخضع له قواعد الإثبات الجزائي فإن الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية، لا يكون مشروعا إلا إذا تم الحصول عليه و تقديمه إقامته أمام القضاء، بالطرق المطلوبة قانونا ، ومتى ما تم الحصول على الدليل خارجها فلا يعتد بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته، ومن قبيل ذلك حصوله من تفتيش لنظام معلوماتي باطل، كما لو لم تكن جريمة من جرائم الاعتداء على النظم محل الإذن قد وقعت بعد .

[1] حيث اقتصر المشرع الجزائري على ثلاثة أنواع من الأدلة فحسب لإثبات جريمة الزنا وذلك ما نصت عليه صراحة المادة (341) من قانون العقوبات الجزائري، على أن الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة (339) يقوم إما على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة التلبس، وإما بإقرار وارد في رسائل أو مستندات صادرة من المتهم وإما بإقرار قضائي.

[2] و في ذلك نصت المادة (177) من قانون أصول المحاكمات الجزائية السوري صراحة، إذا كان وجود الجريمة مرتبطا بوجود حق شخصي وجب على القاضي إتباع قواعد الإثبات الخاصة به.

ولقد وضعت الدساتير الوطنية[1]، والقوانين الإجرائية المختلفة[2]، نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية ومن تم مخالفة هذه النصوص في استخلاص الدليل الجزائي يصبغ هذا الدليل بالا مشروعية.

ومشروعية طريقة الحصول على الدليل بصفة عامة لا تعني بالضرورة اتفاق الإجراء مع القواعد القانونية المكتوبة أو التي ينص عليها المشرع فحسب، بل يجب أن تتعدى ذلك إلى مراعاة إعلانات حقوق الإنسان والمواثيق والاتفاقيات الدولية وقواعد النظام العام وحسن الآداب السائدة في المجتمع وبالإضافة إلى المبادئ التي استقرت عليها محكمة النقض وبصفة عامة مع الأنظمة الثابتة في وجدان المجتمع المتحضر[3].

ويترتب على ذلك أن إجراءات جمع الأدلة المتحصلة من الوسائل الإلكترونية إذا خالفت تلك القواعد والمبادئ التي تنظم كيفية الحصول عليها، فإنها تكون باطلة وبالتالي بطلان الدليل المستمد منها لأنه ما بني على باطل يكون باطل، ولهذا الموضوع أهمية بالغة لما يترتب على بطلان الدليل آثار فإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الاستناد عليه في إدانة المتهم.

فمشروعية الدليل تتطلب صدقه في مضمونه، وان يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة وتدل على الأمانة والنزاهة من حيث طرق الحصول عليه.

والحقيقة أن هذا القيد يحظى أهمية كبرى نتيجة التطور الكبير الذي تحقق مؤخرا في شأن تطويع التقنية لكي تعمل في بيئة الرقابة والبحث والتحقيق كالمراقبة الإلكترونية مثلا التي استحدثها المشرع الجزائري بموجب القانون رقم (04-09) المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإذا كانت هذه الأخيرة تفيد في الكشف عن الجريمة وإقامة الدليل على الجاني، فإنها قد تعصف أكثر فأكثر بحقوق الأفراد وحرياتهم إذا لم يحسن استخدامها، وهو ما قد ينجر عنه الإضرار بالعدالة .

والقاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراء والإجراءات اللاحقة له مباشرة، غير أن هذه القاعدة تثير مسألة في غاية الأهمية تتعلق بماهية المعيار الذي يبين مدى العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له حتى يمتد إليها البطلان، وقد تعددت المعايير التي قال بها الفقه المقارن والمعيار الراجح والسائد في الجزائر هو أن العمل اللاحق يعتبر مرتبطا بالإجراء السابق إذا كان هذا الأخير مقدمة ضرورية لصحة العمل

---

[1] راجع المواد (46)،(48) ،(32) ، (34) فقرة (2 – 35) من الدستور الجزائري لسنة 1996، والمواد (28)،(29)،(31)،من الدستور السوري لسنة 1973 المعدل بالقانون رقم 6 لعام 2000 .

[2] راجع المواد (41) و (44) من قانون الإجراءات الجزائية الجزائري.

[3] انظر في هذا الشأن: د. هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، 2008 ، ص 118-120.عبدالكريم بن غطاي العنزي، الاقتناع الذاتي للقاضي الجنائي بين الشريعة والقانون مع التطبيق في المملكة العربية السعودية، رسالة ماجستير الجامعة العربية للعلوم الأمنية، الرياض، 1428هـ،2003م، ص190

اللاحق، فإذا أوجب القانون مباشرة إجراء معين قبل آخر بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه كان الإجراء، الأول شرطا لصحة الإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه[1].

أما موقف القاضي من الدليل التقني غير المشروع ومدى الأخذ به سواء كان ذلك في إدانة المتهم أو براءته سوف نتعرض له فيما يلي .

أ- الدليل التقني غير المشروع :

في إطار بحث مشروعية الدليل التقني أثيرت مسألة قيمة الدليل التقني غير المشروع في الإثبات الجنائي؟

ومثل هذا التساؤل سوف يقود حتما إلى بحث قيمة كل من دليل الإدانة ودليل البراءة للوقوف على ما إذا كان هناك فرق بين الحالتين أم لا، وذلك كل في فقرة مستقلة على التوالي:

- بالنسبة لدليل الإدانة :

انطلاقا من قاعدة أن الأصل في الإنسان البراءة فإن المتهم يجب أن يعامل على أساس أنه بريء في مختلف مراحل الدعوى إلى أن يصدر بحقه حكم بات (نهائي)، وهذا يقتضي أن تكون الأدلة التي تؤسس عليها حكم الإدانة مشروعة ولا يهم في ذلك إن كانت أدلة تقليدية أو مستخلصة من الوسائل الإلكترونية.

وأي دليل إدانة يتم الحصول عليه بطريقة غير مشروعة أو بوسيلة مخالفة للقانون يعتبر غير مشروع ومن ثم غير مقبول في عملية الإثبات، لأنه إذا ما سمح بقبول الأدلة التي تكون وليدة إجراءات باطلة، فإن الضمانات التي كفلها القانون لحماية حقوق المواطن أو كرامته لا قيمة لها، كما أن القواعد التي يسنها المشرع لا أهمية لها متى ما أمكن إهدارها وعدم الالتزام بها [2].

وبناء على ذلك لا يجوز القبول بدليل تقني جرى الحصول عليه من تسرب، جرى القيام به دون مراعاة الشروط الشكلية والموضوعية للإذن بمباشرة التسرب، أو عن طريق إكراه المتهم المعلوماتي من أجل فك شفرة الدخول إلى النظم المعلوماتية، أو كلمة السر اللازمة للدخول إلى ملفات المعلومات المختزنة، وتتسم بعدم المشروعية أيضا أعمال التحريض على ارتكاب الجريمة من قبل أعضاء الضابطة العدلية، التنصت والمراقبة الإلكترونية عن بعد دون مسوغ قانوني .

---

[1] د. أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجزائية، رسالة دكتوراه كلية الحقوق، جامعة القاهرة، 1959، ص382، مشار إليه لدى: د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الجديدة، دار النهضة العربية، القاهرة، 2002،ص114 .

[2] د. محمد راغب، النظرية العامة للإثبات في التشريع العربي المقارن، الطبعة الأولى، مطبعة المعرفة،القاهرة،1960،ص177، مشار إليه لدى : عبد الله بن صائح بن الرشيد الربيش، سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المملكة العربية السعودية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 1423 -1934هـ، ص146.

فإذا ما حصل دليل تقني وفق الطرق السابقة يتم إبطاله، وعدم إنتاج الإجراء الباطل الآثار التي تترتب عليه مباشرة، حيث نصت المادة (191) منقانون الإجراءات الجزائية الجزائري على أنه: «تنظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها..» .[1]

ب – بالنسبة لدليل البراءة:

بينا في الفقرة السابقة أن حكم الإدانة يجب أن يكون مستندا على دليل تقني مشروع، ولا يجوز أن تبنى الإدانة على دليل باطل، إلا أنه في دليل البراءة نلمس اختلافا حول مدى اشتراط المشروعية بوجه عام في دليل البراءة ويمكن رد هذا الخلاف إلى ثلاثة اتجاهات كما يلي :

الاتجاه الأول[2]: يرى أن المشروعية لازمة في كل دليل سواء أكان إدانة أو براءة، على سند من القول أن القضاء ليس له أن يقر قاعدة أن الغاية تبرر الوسيلة كمبدأ قانوني صحيح، فالمفروض أن تكون السبل القانونية المشروعة كفيلة وحدها بإثبات براءة البريء في أي تشريع إجرائي قويم وإلا فإن البنيان الإجرائي كله يكون مختلا متداعيا، إذا كان يسمح بإدانة البريء، أو بالأدق إذا كان لا يسمح ببراءة البريء إلا بإهدار مبدأ الشرعية من أساسه. وينتهي هذا الاتجاه إلى إثبات البراءة – كالإدانة – لا يون إلا من خلال سبل مشروعة ولا يصح أن يفلت إثبات البراءة من قيد المشروعية الذي هو شرط أساسي في أي تشريع لكل اقتناع سليم.

الاتجاه الثاني[3] : يرو أن المشروعية لازمة في دليل الإدانة دون البراءة على سند من القول أن الأصل في الإنسان البراءة ولا حاجة للمحكمة بأن تثبت براءته، وكل ما تحتاج إليه هو أن تشكك في إدانته، ويضيف هذا الاتجاه إلى أن بطلان دليل الإدانة الذي تولد من إجراء غير مشروع لم نما شرع لضمان حرية المتهم، فلا يجوز أن ينقلب هذا الضمان وبالا عليه .

---

[1] وفي ذلك أوصى المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، والذي عقد في ريو دي جاني رو بالبرازيل في الفترة من 4–9 سبتمبر سنة 1994 في مجال حركة إصلاح الإجراءات الجنائية وحماية حقوق الإنسان بمجموعة من التوصيات، منها التوصية رقم (18) التي تنص على أن «كل الأدلة التي تم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة، ولا يمكن التمسك بها أو مراعاتها، في أي مرحله من مراحل الإجراءات، وقد أشار هذا المؤتمر إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الآلي والجرائم التقليدية في بيئة تكنولوجيا المعلومات، وإلا ترتب عليه بطلان الإجراء فضلا عن تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون». مشار إليه لدى: د. غازي عبد الرحمن هيان الرشيد، المرجع السابق، ص 624.

[2] انظر في هذا الاتجاه : د.رؤوف عبيد ، مبادئ الإجراءات الجنائية في القانون المصري ، دار الفكر العربي ، القاهرة ، ص747–741. د.محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، المرجع السابق ، ص426 هامش رقم (2).

[3] أنظر في هذا الاتجاه: د. محمود محمود مصطفى، شر قانون الإجراءات الجنائية، الطبعة الثانية، مطبعة دار النشر الثقافة، القاهرة، 1974، ص174. د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الجزء الثالث، دار النهضة العربية، القاهرة، 1980 ص388، مشار إليه لدى: عبد الكريم بن غطاي العنزي في رسالته، المرجع السابق، ص 348. ومن هذا الاتجاه أيضا: عبد الكريم بن غطاي العنزي في رسالته، المرجع السابق، ص96 .

بينما يبرز اتجاه ثالث وسط، مفاده أن أداة البراءة غير المشروعة تقبل في حالات دون أخرى، فإذا كان الدليل قد تم التوصل إليه بوسيلة تعد جريمة جنائية، فإن هذا الدليل لا يعول عليه ويجب استبعاده.
أما إذا كانت الوسيلة لا تصل إلى حد الجريمة وإنما تتضمن مخالفة قاعدة إجرائية، ففي هذه الحالة لا يهدر الدليل المتحصل عليه بل يمكن الاستناد إليه. [1]

وفي إطار الترجيح بين هذه الاتجاهات نجد أنفسنا نؤيد الاتجاه الثاني والذي يقصر المشروعية على دليل الإدانة دون البراءة، وذلك لأننا لو تمسكنا بعدم قبول دليل البراءة بحجة أنه غير مشروع، فإننا سوف نصل إلى نتيجة خطيرة للغاية وهي إدانة بريء، وفي هذه الحالة يتحمل المجتمع ضررين: الضرر الأول عقاب بريء قام الدليل على براءته، أما الضرر الثاني هو إفلات مجرم يستحق العقاب من العقاب.

أما التعليل بأن التشريع القانوني كفيل وحده بإثبات براءة البريء، فليس على إطلاقه، لأنه وعلى حد قول البعض من الفقه وبحق– ما من تشريع في العالم من منع البشر إلا وتعتريه فجوات وعيوب كثيرة، تجد س الناس من يستطيع خرق هذه القوانين، بحجة إتباع القانون نفسه وذلك بطرق غير مباشرة، ولذلك فالقوانين الوضعية مرشحة للتعديل والتجديد في أي وقت .

وإذا كان الأمر على ما سلف، فإنه لا يكفي لاعتماد هذا الدليل كدليلا للإدانة، إذ الطبيعة الفنية الخاصة للدليل التقني تمكن من العبث بمضمونه على نحو يحرف الحقيقة أو لوجود خطأ في الحصول عليه، وهو ما يفتح الباب لمناقشة مسألة مصداقيته في إطار نظرية الإثبات الجزائي. [2]

الفرع الثاني : مصداقية الدليل التقني

السائد فقهيا أن سلطة القاضي الجزائي في تقدير الدليل يحكمها مبدأ حرية القاضي الجزائي في تكوين قناعته مما يستتبع ذلك حتميا نتيجة هامة ألا وهي « حرية القاضي في تقدير الأدلة» ، ذلك أن مسألة قيمة الدليل لإثبات الحقيقة هي مسألة موضوعية محضة للقاضي أن يمارس سلطته التقديرية فيها، بل هي المجال الطبيعي لهذه السلطة حيث أنها تتعلق بقيمة الدليل في الإثبات وصولا للحقيقة[3].

إلا أنه في الوقت الذي منح القانون للقاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لاقتناعه الشخصي، فإنه في المقابل لم يطلق حريته ليقضي كيفما شاء وفقا لهواه الشخصي، بل قد أحاطه بقيود وضوابط تشكل في مجموعها شروطا لضمان الوصول إلى الحقيقة الفعلية في الدعوى من دون الانتقاصمن الحقوق والحريات .

---

[1] د. سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، القاهرة، دار النهضة العربية 1972، ص471–473، مشار إليه لدى: د. موسى مسعود رحومة عبد الله، حرية القاضي الجنائي في تكوين عقيدته، المرجع السابق. ص96.

[2] عبد الكريم بن غطاي العنزي، المرجع السابق،ص 54

[3] د.فاضل زيدان محمد، المرجع السابق ،ص ص 92 – 94 .

وهو ما كرسه المشرع الجزائري صراحة بموجب المادة (212) من قانون الإجراءات الجزئية حيث نصت " **يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي....**" و هذا يعني أن الأدلة الجزائية لا تحضى أمام القاضي الجزائي بقوة ثبوتية ، مما ينتج عنه أن القاضي يؤسس اقتناعه على أي دليل كما يصح أن يهدمه تبعا لقناعته الشخصية ، فلا يجوز مطالبة أو إلزام القاضي بالاقتناع بأي دليل ولو لم تكن في الدعوى أدلة سواه .

و في إطار الجرائم محل الدراسة خاصة فيما تعلق بالطبيعة الخاصة للدليل التقني التي تمكن من العبث بمضمونه على نحو يؤدي لتحريف الحقيقة أو التغيير في مضمونها ، ومع نقص المعرفة المعلوماتية للقاضي الجزائي فإن الأمر على القاضي الإستعانة بالخبرة الإستخراج الدليل ويبحث مصداقيته في مجال المعلومات، مما قد يقوي من قيمته على نحو لا يقبل العكس، الذي من شأنه إضفاء حجية قاطعة وقوة على الدليل التقني بما لا يمكن للقاضي الجزائي أن يعمل سلطته التقديرية لقبوله .

أولا : مصداقية الدليل التقني بوصفه يعبر عن حقيقة علمية

يعتبر الدليل التقني تطبيق من تطبيقات الدليل العلمي، بل أكثر منه حجية في الإثبات وذلك بما يتميز به من موضوعية وحياد وكفاءة، محكم وفق قواعد علمية حسابية قاطعة لا تقبل التأويل يقوي يقينيته، ويساعد القاضي من التقليل من الأخطاء القضائية، والاقتراب إلى العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة.

فالفقه الفرنسي يتناول حجية الدليل التقني في المواد الجزائية ضمن مسألة قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل الرادارات الأجهزة السينمائية، أجهزة التصوير، أشرطة التسجيل، أجهزة التنصت[1]، وتطبيقا لذلك قضي في فرنسا بخصوص قوة المحررات الصادرة عن الآلات الحديثة في الإثبات بأنه إذا كانت التسجيلات الممغنطة لها قيمة الدلائل يمكن الاطمئنان إليها، ويمكن أن تكون صالحة في الإثبات أمام القضاء الجزائي[2]، وفي حكم آخر قررت محكمة النقض الفرنسية بأنه إذا اطمأنت محكمة الموضوع وفقا لاقتناعها الذاتي والقواعد العامة إلى ما استندت إليه النيابة العامة من قرائن بشأن خطأ سائق سيارة منسوب إليه تجاوز السرعة، وقد ثبت ذلك من خلال جهاز آلي التقط صورة السيارة المتجاوزة للسرعة، ودون أن يكون السائق قد سئل فإنها لا تكون ملزمة بتحديد من استندت إليه من عناصر الواقعة في تبرير اقتناعها[3].

ومما سبق يتبين لنا أن ظهور الدليل التقني قد زاد من دور الإثبات العلمي واستتبعه ذلك تعاظم دور الخبراء في القيام بدور فعال في إبداء خبرتهم الفنية، بالنضر إلى أن الكثير من الجرائم التي ترتكب ستقع على مسائل إلكترونية آية في التعقيد. وبالنظر إلى تطور مجالات الخبرة فإنه سوف تتسع مجالات اللجوء إليها. كذلك فقد

---

[1] د.هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية ، المرجع السابق، ص ص42-43.

[2] Crim 24 avril 1987, Bull. n" 173. Cité par: Francillon (Jacques), les crimes informatiques et d'autres crime dans le domaine de la technologie informatique en France. r.i.d.p, 1993. p.308.

[3] Crim 3janvier 1978,bull,n°1,D.c.p.p.1991-1992,p413.Crime.20janvier 1977,J.C.P.1977,n° 11.

توفر التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في صنع الدليل، بحيث أن هذا الدليل قد يتمتع بقوة علمية قد يصعب إثبات عكسها.

وإذا كان للخبرة التقنية أهمية كبرى في استخلاص الدليل التقني فإن دورها في بحث مصداقيته في مجال المعالجة الآلية للمعلومات تغدو أعظم، فالدليل التقني وبحكم طبيعته العلمية يمثل إخبارا صادقا عن الواقع من منظور علمي ذو كفاءة بيّنة ، إلا أن هذا لا ينفي استبعاده للشك في سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى، ولا شك أن الخبرة تحتل في هذه الحالة دورا مهما في التثبت من سلامة هذا الدليل.

التقنية الحديثة تمكن من العبث بالدليل التقني بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة. أما الثانية وان كانت نسبة الخطأ الفني في الحصول على الدليل التقني نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ في الحصول على الدليل التقني لسببين[1]: الخطأ في استخدام الأداة المناسبة في الحصول على الدليل التقني، ويرجع ذلك للخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة أما الثانية تكمن في الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن 100 % ويحدث هذا غالبا بسبب وسائل اختزال المعطيات أو بسبب معالجة المعطيات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها .

فمثلما يخضع الدليل التقني لقواعد معينة تحكم طرق الحصول عليه، فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية من الناحية العلمية، وذلك يرجع للطبيعة الفنية لهذا الدليل، فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه[2]، وسوف نحاول فيما يلي تناول بعض هذه الوسائل من حيث سلامته من العبث، ثم وسائل تقييمه من حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو التالي :

يمكن التأكد من سلامة الدليل التقني من العبث بعدة طرق نذكر منها:

- يلعب علم الكمبيوتر دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون وكينونة الدليل التقني[3]، وهذا العلم يستعان به في كشف مدى التلاعب بمضمون هذا الدليل، وتبدو فكرة التحليل التناظري الرقمي من الوسائل المهمة للكشف عن مصداقية الدليل التقني، ومن خلالنا تتم مقارنة الدليل التقني المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا[4].

[1] راجع في ذالك : د.ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، مرجع سابق،ص2253.

[2] طارق محمد الجملي، المرجع السابق،ص 26.

[3] د. ممدوح عبد الحميد عبد المطلب، زبيده محمد قاسم، عبد الله عبد العزيز، المرجع السابق، ص2241.

[4] المرجع السابق، ص 2246-2247.

- حتى في حالة عدم الحصول على النسخة الأصلية للدليل التقني أو في حالة أن العبث قد وقع على النسخة الأصلية، ففي الإمكان التأكد من سلامة الدليل التقني من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات.
- هناك نوع من الأدلة التقنية يسمى بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم في التأكد من مدى سلامة الدليل التقني المقصود من حيث عدم حصول تعديل أو تغيير في النظام لمعلوماتي[1].

فمن خلال هذه الطرق يمكن التأكد من سلامة الدليل التقني ومطابقته للواقع .

عادة تتبع جملة من الإجراءات الفنية للحصول على الدليل التقني وقد قدمنا أن هذه الإجراءات من الممكن أن يعتريها خطأ قد يشك في سلامة نتائجها، ولذا فإنه يمكن في هذا الشأن اعتماد ما يعرف باختبارات (داو بورت)[2] كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل التقني من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات، ولذا فإننا سنعرض باختصار للخطوات التي تتبع للتأكد من سلامة هذه الإجراءات من الناحية الفنية[3]، وذلك بإتباع اختبارين رئيسين هما :

***اختبار السلبيات الزائفة:** ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل التقني، وأنه لا يتم إغفال معطيات مهمة عنه .

* **اختبار الايجابيات الزائفة:** ومفاد ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل التقني لاختبار فني يمكن من التأكد من أن هذه الأداة لا تعرض معطيات إضافية جديدة .

وبذلك يتم من خلال هذين الاختبارين التأكد من أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل التقني وفى ذات الوقت لم تضف إليها أي بيان جديد، وهذا يعطي للنتائج المقدمة عن طريق تلك الآلة مصداقية في التدليل على الواقع.

حيث تدل البحوث المنشورة في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل التقني، وفى المقابل أثبتت تلك الدراسات الأدوات المشكوك في كفاءتها، وهذا يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات[4].

ومن خلال ما تقدم نخلص إلى أنه يمكن التغلب على مشكلة الشك في مصداقية الدليل التقني من الناحية العلمية من خلال إخضاعه لاختبارات تمكن من التأكد من صحتها، لكن ما موقف القاضي الجزائي من هذا الدليل إذا ما خضع لمثل ذلك التقييم ؟

---

[1] نفس المرجع، ص2247

[2] ترجع أصول هذا الاختبار (اختبارات داو برت) للحكم الذي أصدرته المحكمة العليا الامريكية في قضية داو بورت ضد ميريل دو للصناعات الدوائية 1993 ، ص 2248.

[3] المرجع السابق، ص2294ومابعدها.

[4] طارق محمد الجملي، المرجع السابق، ص 26 .

يخضع الدليل التقني شأنه شأن الدليل الجزائي بشكل عام للمبدأ العام في الإثبات الجزائي وهو حرية القاضي الجزائي في الاقتناع، والقاضي في ظل هذا المبدأ يملك حرية واسعة في تقييم عناصر الإثبات، ووزن الأدلة وتقديرها بالكيفية التي تمكنه من تكوين عقيدته في الدعوى المطروحة عليه، ولا يخضع في ذلك إلا إلى صوت ضميره وما يقتنع به شخصيا، ولا يستشير في ذلك سوى وجدانه، فهو وحده الذي يملي عليه الحكم الذي يصدره والرأي الذي يتوصل إليه.

ولقد تعاظم دور الإثبات العلمي مع بروز الدليل التقني إلى حقل الأدلة الجنائية كأفضل دليل لإثبات الجرائم محل الدراسة إن وجد، مما ألزم القاضي أن يتعامل معه في مقابل نقص الثقافة المعلوماتية من جهة، وشروط السلامة التي يتمتع بها من العبث والخطأ من جهة أخرى فهل من شأن ذلك أن القاضي يسلم ويبني اقتناعه بالدليل التقني على أساس أن أمره محسوم علميا.

حيث يعد مبدأ الاقتناع القضائي أحد أهم المبادئ التي تقوم عليها نظرية الإثبات في المواد الجزائية، وعنه تتفرع معظم القواعد التي تحكم هذا الإثبات[1]، وقد تعددت الآراء فيما يتعلق ببيان مدلوله[2]، وأيا كان التعريفات الموضوعة له إلا أنها تصبو إلى معنى واحد وهي: أن للقاضي أن يستمد من أي دليل تطمئن إليه نفسه، ويسكن إليه وجدانه، دون أي قيد يقيده في ذلك إلا ما تقتضيه العدالة ذاتها من قيود، ويتصل بذلك سلطته في استبعاد أي دليل لا يقتنع به إذ لا وجود لدليل يفرض عليه أن يستمد منه اقتناعه سواء تلك الأدلة التي طرحت عليه من قبل الخصوم أو النيابة العامة، بل حتى التي يرى بنفسه تقديمها، والحرية هذه التي يتمتع بها القاضي الجزائي في هذا المجال ليست مقررة بهدف توسيع الإدانة أو البراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجزائية.

ومبدأ الاقتناع القضائي وفق هذا المعنى يتيح للقاضي حرية واسعة في تقدير القيمة الدامغة للأدلة المقامة أمامه على حسب اقتناعه، بل لعله أهم نتيجة تترتب على هذا المبدأ .

ويعد التشريع الجزائري في طليعة التشريعات التي أكدت هذا المبدأ وذلك من خلال المادة (307) من قانون الإجراءات، و التي تقابلها المادة(353) من قانون الإجراءات الفرنسي حيث تنص على" ... **إن القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت أن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي**". كما أن الاقتناع القضائي كرسته أيضا صراحة المادة 212 من قانون الإجراءات الجزائية الجزائري .

[1] د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، المرجع السابق، 2241

[2] حيث عرفه د. محمود مصطفى بأنه «التقدير الحر المسبب لعناصر الإثبات في الدعوى وهو البديل عن نظام الأدلة القانونية» وفي رأي د. علي راشد بأنه «تلك الحالة الذهبية والنفسية أو ذلك المظهر الذي يوضح وصول القاضي باقتناعه لدرجة اليقين بحقيقة واقعة أم تحدث تحت بصره بصورة عامة». مشار إليه لدى: عبد الله بن صالح بن الرشيد الربيش، المرجع السابق، ص 75

وما تجدر الإشارة إليه هنا أن مبدأ إقتناع القاضي هو عام يسري في كافة أنواع المحاكمات الجزائية بإختلاف التصنيفات للجرائم محل المتابعة الجزائية ، سواء كانت محاكم الجنايات أو أقسام للجنح أو للمخالفات[1]،

و هذا لا يعني أن نطاقه محدد فقط على مرحلة المحاكمة، بل يمتد كذلك ليشمل مرحلة التحقيق الابتدائي حيث يطبقه قضاة التحقيق[2].

و مما سبق نجد أن مبدأ الاقتناع الشخصي للقاضي الجزائي يعد أساسا في العمل القضائي لإصدار الأحكام الجزائية ، وعليه فإن ظهور الدليل التقني بكل مميزاته يجب أن لا يغير شيئا من هذا المبدأ . ومن ثم فإن الدليل التقني لا يحظى بقوة حاسمة في الإثبات تماشيا مع الأصل. فهو مجرد دليل لا تختلف قيمته و حجته الثبوتية عن بقية الأدلة ، فيصح للقاضي أن يبني قناعته عليه كما يصح أن يطرحه إذا تطرق الشك إليه بخصوصه .

فالدليل التقني بوصفه تطبيقا من تطبيقات الدليل العلمي لا يمكن أن ينازع القاضي في قيمة ما يتمتع به من قوة استدلالية قد استقرت بالنسبة له وتأكدت من الناحية العلمية، فإذا سلمنا سابقاً بإمكانية التشكيك في سلامة الدليل التقني بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنهما برأي حاسم وإن لم يقطع به أهل الاختصاص، ولذلك فإذا توافرت في الدليل التقني الشروط المذكورة سابقاً بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية وفقاً للمادة لـ(212) والمادة (307) من قانون الإجراءات الجزائية الجزائري، ولكن يقتصر دور القاضي على الظروف والملابسات التي وجد فيها الدليل فهي من يدخل في نطاق تقديره الذاتي، فهي من صميم وظيفته

---

[1]:وان كان المشرع الجزائري لم يحد ذلك صراحة في المواد المقررة لهذا المبدأ (راجع المواد 307و212 من قانون الإجراءات الجزائية) بخلاف المشرع الفرنسي، فقد صرح ذلك صراحة، حيث خصص المادة (353-1) من قانون الإجراءات لتطبيق المبدأ أمام محكمة الجنايات، كما نصت المادة (427) من ذات القانون على تطبيق هذا المبدأ بالنسبة لمحاكم الجنح، أما المادة (ط 55) من نفس القانون فهي مخصصة بالنسبة لمحاكم المخالفات. وما يقيل بخصوص المشرع الفرنسي يقال بالنسبة للمشرع السوري، حيث نجد هذا الأخير قد أدرج نص المادة (75 – 1) السابقة ضمن الكتاب الثاني تحت عنوان – المحاكمات –، فضلا عن ذلك فإن هذه المادة قد أقرت للقاضي حرية الاستعانة بكافة وسائل الإثبات لتكوين قناعته حول حقيقة الوقائع المرفوعة عنها الدعوى، وأعمتها في ذلك على الجنايات والجنح والمخالفات بصريح العبارة.

[2]:فقضاء التحقيق يملك حرية التصرف في الدعوى وتحديد مصيرها حسب تقديره غير أن مهمة هذا الأخير لا تعدو أن تكون مقصورة فقط على تقدير مدى كفاية الأدلة أو عدم كفايتها للاتهام، وهي بذلك تختلف عن وظيفة قضاة الحكم الذين عليهم تقدير الأدلة القائمة من حيث كفايتها أو عدم كفايتها للحكم بالإدانة. وإذا صح التعبير يمكن القول بأن الأولى تسعى إلى ترجيح الظن بينما الثانية تسمى إلى توكيد اليقين، وشتان بين الاثنان. يترتب على ذلك نتيجة هامة وهي إن الشك في مرحلة الاتهام يفسر ضد مصلحة المتهم، مما يستوجب إحالة الدعوى إلى المحكمة المختصة، بخلاف الشك في مرحلة الحكم فهو كما هو معلوم – يفسر لمصلحة المتهم.

وبالتالي يظهر لنا أن نطاق تطبيق مبدأ حرية القاضي في مرحلة التحقيق محدود، إذ يكاد يقتصر على مجرد الموازنة بين الأدلة المثبتة للتهمة وتلك النافية لها، لترجيح مدى كفايتها أو عدم كفايتها للاتهام. بينما في المقابل نجد أن نطاق تطبيق المبدأ المذكور أمام قضاء الحكم يتسع الى حد كبير باعتباره يتصل بوقائع كل دعوى على حدة بحس نظر: عبد الله بن صالح بن الرشيد الربيش، المرجع السابق، ص 80.

القضائية، بعيث يكون في مقدوره أن يطرح مثل هذا الدليل – رغم قطيعته من الناحية العلمية – إذا تبين بأنه لا يتفق مع ظروف الواقعة وملابستها، حيث تولد الشك لدى القاضي، ومن تم يقضي في إطار تفسير الشك لصالح المتهم .

ذلك أن مجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أم بالبراءة، دون بحث الظروف والملابسات، فالدليل العلمي ليس آلية معدة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة[1]

و عليه فإنه يجب الإبقاء على السلطة التقديرية للقاضي التقديرية في تقديره للأدلة التقنية ، لضمان تنقيتها من الشوائب العلمية لأن الحقيقة العلمية لابد ان تتشكل وفق حقيقة قضائية ، فهو المسيطر على هذه الحقيقة لأنه من خلال سلطته التقديرية يستطيع تفعيل الشك لصالح المتهم، بأن يستبعد الأدلة التي يتم الحصول عليها بطرق غير مشروعة[2].

ثانيا :مصداقية الدليل التقني بوصفه يعبر عن الحقيقة التي تهدف إليها الدعوى العمومية

إن تأثير التطور العلمي لا يقف عند مضمون الدليل بل يجب أن يمتد إلى الإجراءات المعمول بها للحصول عليه ، لذلك لابد أن تكون تلك الإجراءات متطورة تماشيا مع طبيعة الدليل و ان تكون مشروعة للحفاظ على شرعية الدليل المتولد منها ، وأن تكون مطروحة أمام القاضي في الجلسة ضمن أوراق الدعوى لأتاحا للخصوم بشكل يمكن من مناقشته والرد عليه، كما يجب أن تكون يقينية .

فالقانون و إن ترك للقاضي الجزائي الحرية في أن يستمد اقتناعه من أي دليل وبأية وسيلة يراها موصلة إلى الحقيقة[3] ، إلا أن هذه الحرية لا تعني أن القاضي الجزائي يستطيع بناء عقيدته على أي دليل يحصل عليهمهما كان مصدره ووسيلة البحث عنه، فهو ملزم بضرورة أن يكون الدليل المستند عليه في الحكم مقبولا في الدعوى بمراعاة قاعدة مشروعية الحصول عليه وفق النظام الإجرائي المعمول به ، بل إن مخالفة هذا الشرط قد يهدر قيمة الدليل و يقضى في النهاية الى بطلان، فالخصومة الجزائية قائمة على ضمان حرية المتهم لا على سلطة الدولة في العقاب، وبالتالي يتعين على القاضي ألا يثبت توافر هذه السلطة تجاه المتهم إلا من خلال دليل يتم الحصول عليه من إجراءات مشروعة احترمت فيها الحريات و الضمانات المعمول به قانونا، و لهذا لا يجوز الإعتماد على دليل يتصف بالبطلان و لابد أن يكون مطابقاً للنصوص المقررة لضمانات الحرية الفردية وكذا القواعد العامة للإجراءات الجزائية والمبادئ القانونية العامة كالقواعد والمبادئ التي توجب احترام قيم العدالة وأخلاقياتها والنزاهة في الحصول على الأدلة واحترام حقوق الدفاع. [4]

---

[1]– د.جميل عبد الباقي الصفير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص 22.

[2]– د.علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إحلال نظرية الإثبات الجنائي، بحث مقدم ضمنأعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، أكاديمية شرطة دبي، الفترة من 26إلى 48-4-2003، دبي ، ص15.

[3]– د. موسى مسعود رحومة عبد الله، حرية القاضي الجنائي في تكوين عقيدته ،جامعة قاز يونس كلية الحقوق ، ص86.

[4]– د. فتحي محمد أنور عزت، المريع السابق، ص 44

و الأمر نفسه ينطبق على الدليل التقني الذي يشترط فيه هو الآخر أن يكون مشروعا في ذاته وغير مخالف للقواعد القانونية وللمبادئ القانونية العامة.

و متى تأكد القاضي من الأدلة أنها مقبولة قانونا، حينئذ يستكمل عمله بمناقشته و هذا بحضور الخصوم،فمن القواعد الأساسية في الإجراءات الجزائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعرف"بوضعية الدليل" بما يعني أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الإطلاع عليه ومناقشته وذلك احتراماً لحقوق الدفاع .

وبمقتضى هذا فإن القاضي لا يجوز له أن يبني حكمه على دليل لا صلة له في الأوراق، فالدليل الذي لا يتحقق فيه هذا الشرط يكون منعدما في نظر القانون وذلك استناداً إلى قاعدة وجوب تدوين كافة الإجراءات الاستدلال والتحقيق. وغاية ذلك حتى يكون الخصوم على بينة مما يقدم ضدهم من أدلة، وأن تتاح لهم إمكانية مناقشتها والرد عليها[1]

و هو ما كرسته الفقرة الثانية (2) من المادّة (212) من قانون الإجراءات الجزائية الجزائري إذا تنص " **ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه**"و التي تقابلها المادة (427) في فقرتها الثانية من قانون الإجراءات الجزائية الفرنسي التي نصت على أنه "**لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه فيمواجهة الخصوم**"[2].

و بمقتضى هذا فإن القاضي في تقديره للأدلة سواء كانت تقليدية أو مستخرجة من الوسائل الإلكترونية لا يكتفي بالمحاضر التحقيق و ما دوّن فيها ، بل عليه إعادة الإستماع للشهود الذين قد سبق سماعهم شهاداتهم أثناء التحقيق الابتدائي، فضلا عن اعتراف المتهم نفسه وكذا تقارير الخبراء وذلك بمناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة ، ويطرح جميع الأدلة الأخرى للمناقشة الشفوية، فلا يكون بين الدليل والقاضي وسيط، والغرض من ذلك أن يتاح لكل طرف في الدعوى أن يواجه خصمه بما يحوزه من أدلة ضده، مما يفيد القاضي في تكوين قناعته من نتيجة هذه المناقشات التي تجري أمامه في الجلسة[3].

فضلا عن ذلك فإن هذا من شأنه أن يحقق رقابة فعالة على جدية الأدلة التي تكون قد حصلت في مرحلة التحقيق فتعرض مجدداً، وهو ما يتيح في المقابل مراقبة التقدير الذي كانت سلطة التحقيق قد خلصت إليه.

---

[1]– إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية – دراسة قانونية نفسية – الطبعة الأولى رسالة دكتوراة ،عالم الكتاب، القاهرة،1980، ص 646.

[2]Art 427 alinéa 2 du C.P.P.F dispose que : «Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui».

[3]– د. فاضل زيدان محمد، المرجع السابق، ص 259 .

و هو ما عبرت عنه المحكمة العليا الجزائرية في قضاء لها بقولها "**لا يمكن لقضاة الموضوع أن يؤسسوا قرارهم إلا على الأدلة المقدمة لهم أثناء المرافعات والتي تتم مناقشتها حضورياً**"[1]

لا يختلف الأمر بالنسبة للدّليل التقني بوصفه دليل من أدلّة الإثبات، مهما كانت الحالة التي يكون عليها سواء كان على شكل مخرجات ورقية أو إلكترونية أو معروضة بواسطة الكمبيوتر على الشاشة الخاصة به. كل أولئك سيكون محلاً للمناقشة عند الأخذ بها كأدّلة إثبات أمام المحكمة[2].

و عليه فإن القاضي الجزائي له الحرية الكاملة في أن يستمد اقتناعه من الدليل التقني طالما اطمئن إليه وكان متضمنا في أوراق ملف الدعوى ، وعرض عليه أثناء المرافعات وناقشها أطراف الدعوى ، فلا يجوز للقاضي أن يبني اقتناعه على هذه المعلومات الشخصية، وذلك حماية للخصوم من أي تأثير خاطئ على القاضي، يكون ناتجاً عما وصله من معلومات خارج إطار الدعوى، وإلا يكون قد جمع في شخصه صفتين متعارضتين صفة الشاهد وصفة القاضي، وهذا ما لا يجيزه القانون ويرتب عليه بطلان الحكم. لأن الخصوم ليس بإمكانهم مناقشة شهادته، والرد عليها بحرية، مما يشكل مساساً بحق الدفاع.بل باعتماده على معلوماته الشخصية يكون عرضة للتهمة، وسوء الظن به وهو الشيء الذي يجب أن ينزه عنه القضاء عموماً.[3]

وإن كان ذلك كذلك، فإن المعلومات العامة المستقاة من خبرة القاضي بالشؤون العامة المفروض إلمام الكافة بها لا تعد من قبيل المعلومات الشخصية المحذورة على القاضي أن يبني حكمه عليها، ومن قبيل ذلك الثقافة المعلوماتية فيما يتعلق بأساسيات الكمبيوتر .

لكن يلاحظ أنه وإن كان يجب أن يصدر الحكم من عقيدة للقاضي يستقيها هو مما يجريه من التحقيقات مستقلاً في تحصيل هذه العقيدة بنفسه لا يشاركه فيها غيره إلا أن ذلك لا يعني حرمان القاضي بصفة مطت من الأخذ برأي الغير، لم في يجوز له ذلك متى كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناء عليه يكون متولدا من عقيدته هو وليس من تقرير الخبير.

و في نطاق الأدلة التقنية يتطلب من القاضي الجزائي أن يكون مؤهلا التأهيل الفني والتقني على كيفية التعامل مع الدليل التقني، لأنه سيكون محلاً للمناقشة الحضورية بين الأطراف عند الأخذ بها كأدلة إثبات في الدعوى الجزائية، فهذا التأهيل يضمن نجاح مهمة القاضي الذي تناط به مهمة المناقشة العلمية لهذه الأدلة والهيمنة على الدعوى الجزائية ولن يتحقق ذلك إلا بعقد دورات تدريبية مكثفة لهؤلاء القضاة على كافة مستوياتهم ودرجاتهم في تقنية المعلومات، وإذا كان قد تم وضع حذا المفهوم وتطويره من قبل المجلس الأدبي

---

[1]– جنائي 21 جانفي 1982 ، الاجتهاد القضائي، ص 66 ، غير منشور اطلع عليه لدى تقنين الإجراءات الجزائية، تحت إشراف د. أحسن بوسقيعة، ص 73 .

[2]د. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية ،2010.

[3]– د. موسى مسعود رحومة عبد اءله، حرية القاضي الجنائي في تكوين عقيدته، المريع السابق، ص 114

بشأن جرائم تقنية المعلومات، وصدقت عليه شبكة لشبونة للمجلس الأوروبي في سبتمبر 2009[1]، فإنه برأينا لا حرج لو كان هناك دور عربي يعمل على مساعدة مؤسسات التدريب القضائي لوضع برامج تدريب على الأدلة التقنية للقضاة، وإدماج هذا النوع من التدريب ضمن أساس التدريب الأولي والتدريب أثناء الخدمة .

ثالثا: يقينية الأدلة التقنية

لما كان هدف التشريعات الإجرائية هو إصابة القاضي الحقيقة الواقعية في حكمه، لذا وجب على القاضي قبل تحريره لحكمه أن يصل إلى الحقيقة مؤكدة بأن تكون لديه يقينا مؤكدا بحدوثها، لا بمجرد الظن والاحتمال، إذ أن الشك يفسر لصالح المتهم بحسبان أن الأصل في الإنسان البراءة .

وشرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستخلص منها هذا اليقين أدلة تقليدية أو مستحدثة كالدليل التقني.

و يقصد باليقين **لغة** : بأنه **العلم وإزاحة الشك، وتحقيق الأمر، وقد أيقن يوقن إيقانا فهو موقن، أو يقن ييقن يقنا، فهو يقن، واليقين نقيض الشك، والعلم نقيض الجهل**[2].

أما اصطلاحا :فاليقين هو **كل معرفة لا تقبل الشك، ومنه حدسي كاليقين ببعض الأوليات أو استدلالي غير مباشر يتنبأ إليه المرء بعد البرهنة، ومنه ذاتي يسلم به المرء ولا يستطيع نقله إلى غيره، أو موضوعي يفرض نفسه على العقول كاليقين العلمي، وقد يسمى التسليم بأمر ظاهر أو راجح يقينا اقتناعا، أو شبه يقين .**

والعلم اليقيني هو الذي ينكشف فيه المعلوم انكشاف لا يبقى معه ريب ولا يقاربه إمكان الغلط أو الوهم[3].

أما **اليقين في الاصطلاح القانوني فقد عرفه البعض من الفقهاء[4] على أنه «عبارة عن اقتناع مستمد إلى حجج ثابتة وقطعية»** أو أنه عبارة عن «**حالة ذهنية أو عقلانية تؤكد وجود الحقيقة»**[5]**، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة ثقة عالية من التوكيد.** "

ومتى ما تكامل اليقين بأن وصل القاضي إلى درجة القطع ينشأ ما يسمى بالاقتناع اليقيني وهو أساس الحقيقة القضائية التي ينشدها القاضي في حكمه .

---

[1] أنظر في ذلك: الفريق العامل للأصحاب المصلحة المتعددين في إطار المشروع المعني بالجريمة المعلوماتية ومن قبل شبكة لشبونة، التدريب على الجريمة المعلوماتية للقضاة وأعضاء النيابة العامة، ورقة عمل معدة لمؤسسات التدريب القضائي التابعة للمجلس القضائي، قسم مجتمع المعلومات والعمل على مكافحة الجريمة، المديرية العامة لحقوق الإنسان والشؤون القانونية، المجلس الأوروبي، ستراسبورغ، فرنسا، 8 أكتوبر 2009.

[2] ابن منظون، لسان العرب، المرجع السابق، ص 4934

[3] د. إبراهيم مدكور، المعجم الفلسفي، دار الكتاب، القاهرة، 1983 ، ص216.

[4] موسى مسعود رحومة عبد الله، حرية القاضي الجنائي في تكوين عقيدته، المرجع السابق، ص131.

[5] RACHED (a-a) de l'intime conviction du juge , thèse paris ;1942, p3.

مشار إليه لدى: د. هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 78.

في الوقت الذي يعود فيه لقاضي الموضوع تقدير الأدلة وموازنتها وفقاً لما يمليه عليه وجدانه، ودون أن يخضع في ذلك لرقابة لمحكمة العليا، إلا أنه مع ذلك مقيد في ذلك بضرورة تأسيس قناعته على الجزم واليقين لا على الظن والترجيح وذلك لاستبعاد قرينة البراءة اللاصقة بكل إنسان استنادا إلى أن الأصل في الإنسان البراءة .

وإذا كانت هذه هي الأحكام العامة التي تحكم اليقين في الأدلة الجزائية في الجزائر وفي الدول ذات الصياغة اللاتينية، فإن الأمر لا يختلف بالنسبة للدليل التقني، إذ يشترط أن يكون هو الآخر يقيني حتى يمكن الحكم بالإدانة[1]

ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من أدلة تقنية، وهكذا يستطيع القاضي من خلال ذلك وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، أن يحدد قوتها الاستدلالية على صدق نسبة جريمة من جرائم الاعتداء على نظم المعالجة الآلية إلى شخص معين من عدمه .

فكأن اقتناع القاضي يصل إلى الجزم واليقين عن طريق نوعين من المعرفة: أولهما المعرفة الحسية التي تدركها الحواس، والآخر المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها[2]

إلا أنه في نطاق الجزم بوقوع جرائم الاعتداء على نظم المعلوماتية ونسبتها إلى المتهم يستدعي نوعا آخر من المعرفة ألا وهي المعرفة العلمية في مجال المعلوماتية[3]، وهو ما يلقي المزيد من الأهمية على تدريب القضاة، وتكمن خطورة هذه الأخيرة في كون الجهل بها قد يؤدي في بعض الأحيان إلى التشكيك في قيمة الدليل التقني وما يستتبعه ذلك من القضاء بالبراءة، على اعتبار أن الشك يجب أن يستفيد منه المتهم في مرحلة المحاكمة، بل حتى لإعمال هذه الأخيرة يلزم أن يكون هناك ما يرقى لمستوى التشكيك في الدليل وهو ما قد لا يتوافر لدى القاضي .

تحدثنا فيما سبق عن كيفية الوصول إلى درجة اليقين والقطع وتبين كيف أن القاضي يصل إليها إلا من خلال ثلاث أنواع من المعارف حسية عقلية ومعلوماتية، حتى يبنى عليها حكمه بالإدانة في نطاق جرائم الاعتداء على نظم المعلوماتية، وذلك لاستبعاد قرينة البراءة اللاصقة بكل إنسان استنادا إلى أن الأصل في الإنسان البراءة .

أما إذا لم تقدر الأدلة التقنية على إحداث القطع أو اليقين بوقوع الجريمة ونسبتها إلى المتهم يلزم حينئذ استمرار حالة البراءة التي يكفي لتأكيد وجودها مجرد الشك في ثبوت تلك الإدانة استنادا إلى القاعدة التي تقول بأن الشك يفسر في مصلحة المتهم[4].

---

[1] د. هلالي عبد الله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 90.

[2] المرجع السابق، ص ص 90 – 91 .

[3] أنظر في الاتفاق حول ذات المضمون، عائشة بن قارة مصطفى، المرجع السابق، ص181.

[4] د. هلالي عبد الله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص 87.

ويبنى على ذلك، أن حكم الإدانة يكون معيبا إذا ما تأسس على ترجيح ثبوت التهمة أو إذا كان قد بني على مجرد افتراضات أو استنتاجات لا يؤيدها الواقع .

ومن خلال هذا العمل البسيط خلصنا إلى ان القوانين الردعية ليست فقط التي يجب الاعتماد عليها في محاربة هذه الجرائم ، بل يجب إدخال سياسة التوعية بالمسؤولية لا سيما في أوساط الشباب داخل المدارس، مراكز تنشيط الشباب، عن طريق وسائل الإعلام ، وكذا وزارة الشؤون الدينية، لأن هذه الظاهرة عمت مجتمعنا، وتفشي الفسق والدعارة والفاحشة ، وتطورت عن طريق التقنية المعلوماتية كوسيلة

إلى أن الجريمة المعلوماتية قد تكون متعلقة بالبيئة المعلوماتية أي أن محل الجريمة هو تلك البيئة المعلوماتية بمختلف محتوياتها أو بما يعرف بالكيان المعنوي وهذا هو الشائع و المتعارف عليه لكن قد تكون الجريمة المعلوماتية متعلقة بالوسيلة المعلوماتية المستخدمة لارتكاب جريمة تقليدية وهي جرائم متفشية ومعروفة لدى الكثير من الناس حيث أنهم لا يتصورون وقوع جرائم معروفة وتقليدية في شكل معلوماتي وهذا ما وضحنها خلال بحثنا هذا.

حيث ظهر لنا جليا الدور الذي تلعبه الوسيلة المعلوماتية في وقوع جرائم الآداب، وتطرقنا إلى الإطار الموضوعي وكذا الإطار الإجرائي لجرائم الآداب العامة المرتبطة بتقنية المعلوماتية كما تطرقنا في موضوعنا هذا لجريمة ذات طبيعة خاصة والمتمثلة في المضايقة باستخدام تقنية المعلوماتية حيث وضحنا طبيعة الجريمة بموجب عام وصورها المختلفة التي يمكن ان تقع من خلالها هذه الجريمة كما وضحنا الموقف التشريعي من هذه الجرائم معتمدين على الرؤية الغربية و العربية وصولا إلى موقف المشرع الجنائي الجزائري لها حيث آن المشرع لم ينص على هذه الجريمة كما أطلقنا عليها هذه التسمية

وفي الأخير يمكننا ان نتوجه بحل نراه بالإمكان آن يطبق على إشكالية الدراسة و المتمثل في ان يدرج نصوص قانون العقوبات مواجهته لجرائم الآداب العامة الواقعة عبر وسائل تقنية المعلوماتية ولتي من بينها الجرائم محل الدراسة هذا من جهة ومن جهة أخرى على المشرع مراعاة الوسيلة المعلوماتية التي قد تتداخل مع الجريمة التقليدية كوسيلة لارتكابها وبهذا لا يفلت المجرم من العقاب لغياب النص على ما قام به أو لوجود ثغرة في النص القانوني يجعله لا يدخل في دائرة التجريم وبالتالي يفلت من العقاب ، ولهذا نناشد المشرع الجزائري في وضع القوانين خاصة لهذه الجريمة نضرا لانتشارها الواسع فهي جريمة عابرة للحدود وفي تطور مستمر وسريع

الكتب:

1. إبراهيم مدكور، المعجم الفلسفي، دار الكتاب، القاهرة، 1983 .
2. أحسن بوسقيعة، الوجيز في القانون الخاص، الجزء الأول، الطبعة 15، دار هومة للنشر و الطباعة والتوزيع، الجزائر.
3. أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآالي) –دراسة مقارنة – الطبعة الأولى– دار النهضة العربية – القاهدرة –2000
4. أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ّ2015.
5. آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007.
6. بكري يوسف بكري، الجرائم الإعلامية ضد الأحداث، الطبعة الأولى، دار الفكر الجامعي،2011.
7. جميل عبد الباقي الصغير – الإنترنت والقانون الجنائي – دار النهضة العربية – 2002 .
8. جميل عبد الباقي الصغير ، قانون العقوبات (القسم الخاص) ، دار النهضة العربية ، 1998 .
9. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الجديدة، دار النهضة العربية، القاهرة، 2002.
10. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية ،2010.
11. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الطبعة الاولى، دار النهضة العربية، القاهرة، 1999.
12. شيماء عبد الغني محمد عطا لله ، دار الجامعة الجديدة للطباعة و النشر ، سنة 2010 .
13. عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الكترونية دراسة قانونية مقارنة دار الثقافة والنشر والتوزيع سنة2014 .

14. عائشة بن قارة ، حجية الدليل الالكتروني في مجال الإثبات الجنائي (في القانون الجزائري و القانون المقارن)، دار الجامعة الجديدة للطباعة و النشر والتوزيع ،الإسكندرية ، سنة 2010 .

15. عبد القادر علي قهوجي ، الحماية الجنائية لبرامج الحساب الآلي ، دار الجامعة الجديدة الإسكندرية ، سنة 2010 .

16. علي أحمد راشد – مبادئ القانون الجنائي ،منشأة المعارف، بدون تاريخ نشر .

17. علي جابر الحسيناوي ، جرائم الحاسوب والإنترنت ،دار اليازوري العلمية نشر سنة 2011.

18. علي محمد جعفر ، قانون العقوبات القسم الخاص ، المؤسسة الجامعية للدراسة و النشر ، سنة 2006.

19. عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة والنشر والتوزيع ،سوريا ،سنة 2011 .

20. فاضل زايدي محمد ،سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، دار الثقافة و النشر و التوزيع ، سنة 2010.

21. فتوح الشاذلي و عقيقي كامل عقيقي ، جرائم الكمبيوتر ، ب ط ، منشورات الحلبي الحقوقية ، بيروت ، 2003 .

22. محمد راغب، النظرية العامة للإثبات في التشريع العربي المقارن، الطبعة الأولى، مطبعة المعرفة،القاهرة،1960.

23. محمد عبد الظاهر حسين – المسؤولية القانونية في مجال شبكة الأنترنت– دار النهضة العربية – 2002 .

24. محمد محمود المكاوى ، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والإنترنت) ، المكتبة العصرية للنشر والتوزيع، القاهرة، الطبعة الأولى، 2010 .

25. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988.

26. مدحت رمضان ، جرائم الاعتداء على الأشخاص والأنترنت ، دار الجامعة الجديدة للطباعة و النشر و التوزيع .
27. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009.
28. نائلة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية منشورات الحلبي ، ب ط ، بيروت ، 2005 .
29. نعيم مغبغب ، حماية برامج الكمبيوتر، ب ط ، منشورات الحلبي الحقوقية ، بيروت ، 2009.
30. هشام محمد فريد رستم ، قانون العقوبات و مخاطر تقنية المعلومات ، ب ط ، منشورات الحلبي الحقوقية ،بيروت ،2000.
31. هلالي عبد الإله أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، ب ط ، دار النهضة العربية ، القاهرة ، 1998 .
32. هلالي عبد الإله أحمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، 2007.
33. هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، 2008 .
34. إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية – دراسة قانونية نفسية – الطبعة الأولى رسالة دكتوراة ،عالم الكتاب، القاهرة،1980.

المذكرات الرسائل الجمعية:

1. خليفة محمد، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة، 2011/2010.
2. عبد الله بن صائح بن الرشيد الربيش، سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المملكة العربية السعودية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 1423 –1934هـ.

3. عبدالكريم بن غطاي العنزي، الاقتناع الذاتي للقاضي الجنائي بين الشريعة والقانون مع التطبيق في المملكة العربية السعودية، رسالة ماجستير الجامعة العربية للعلوم الأمنية، الرياض، 1428هـ،2003م.

المؤتمرات والندوات:

1. عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الانترنت، ندوة الدليل الرقمي بمقر جامعة الدول العربية بجمهورية مصر العربية، في الفترة من 5-8 مارس 2006.
2. محمد أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003.
3. ممدوح عبد الحميد عبد الطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في: 10-12 مايو 2003.

المنشورات:

1. جريدة الحوار يوم 11 / 01 / 2009 نشر سهام حواس حوادث الاغتصاب والدعارة تتصدر قوائم الجرائم في الجزائر.
2. سليم عبد الله الخيوري، الحماية القانونية لمعلومات شبكة الانترنت، منشورات الحلبي الحقوقية، ط1، 2011.
3. سليمان بصوفه – بيوت دعارة محاربة ظاهرة اغتصاب لأطفال في الجزائر اول يومية الكترونية – صدرت من لندن 21 ماي 2001.

المواقع الالكترونية:

1. http : //www.lesechos.fr
2. http ; // www. Alegria. Com/ forums / computer – internet / 21325 – cybercriminalité –en – alg – rie- 4. html.
3. http ; // www. echoroukonline . com/ara/national/30039.html.
4. http ; //www. libertysecurity.org/ article 226. html.

5. http ; //www. sawt – alahrar. net/ online/ modules. PHP? Name= News & file= article & Sid= 858.
6. http ;// www.mag – securscom/spip.php ?article 7842.
7. http://kenanaonline.com/users/khaledmamdouh/posts/7934
8. http://www.isecur1ty.org/articles/digital-forensics/221-photorec-recoverjpeg-foremost.html
9. http://www.libertysecurity.org/article226.html.
10. http;//www.awt.be/contenu/tel/sec/sec,fr,fic,140.000.pdf.
11. www .Law –Zag. com

الدساتير:

1. مرسوم رئاسي رقم 96-438 مؤرخ في 07 ديسمبر 1996 متعلق بإصدار نص تعديل الدستور المصادق عليه في استفتاء صادر في 28 نوفمبر 1996، ج ر، ع 76، صادر في 08 ديسمبر 1996
2. الدستور السوري 1973 المعدل بقانون رقم 6 لعام 2000.

القوانين:

1. أمر رقم 66-156 مؤرخ في 08 جوان 1966، ج ر، ع 49، صادر في 11 جوان 1966 متضمن قانون العقوبات، المعدل والمتمم.
2. القانون رقم 17-07 المؤرخ في : 28 جمادى الثانية عام 1438 هجري الموافق لـ: 27 مارس 2017 المعدل و المتمم للأمر رقم: 66 – 155 المؤرخ في 18 صفر عام 1386 هجري الموافق لـ: 08 يونيو سنة 1966 المتضمن قانون الاجراءات الجزائية
3. قانون 04/09 المؤرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47 المؤرخة في 16 /2009/08.

فهرس المحتويات

فهرس المحتويات