جامعة مولود معمري – تيزي وزو

كلية الحقوق والعلوم السياسية

قسم الحقوق

التحقيق الجنائي في الجرائم الإلكترونية

أطروحة لنيل شهادة الدكتوراه في العلوم

تخصص: القانون

إعداد الطالب:

– برا هيمي جمال

إشراف الأستاذ:

أ.د/– إقلولي محمد

لجنة المناقشة:

أ.د–. جبالي وأعمر، أستاذ ، جامعة مولود معمري، تيزي وزو.....رئيسا

أ.د– إقلولي محمد ، أستاذ، جامعة مولود معمري، تيزي وزو .....مشرفا و مقررا

أ.د– مباركي علي، أستاذ محاضر "أ"، جامعة مولود معمري، تيزي وزو.....ممتحنا

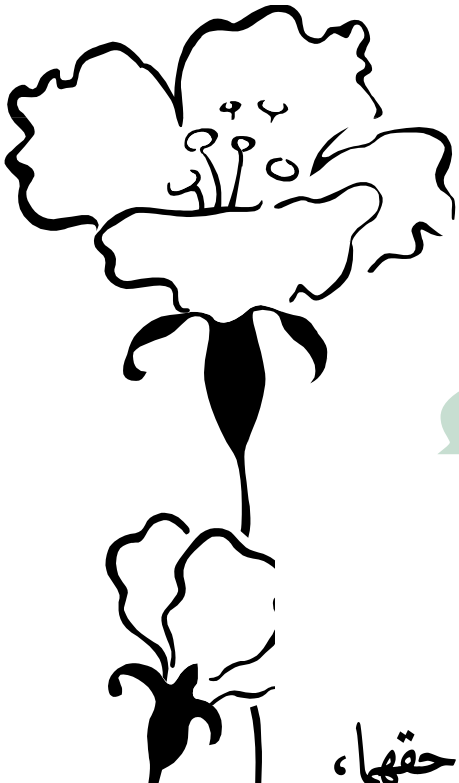
أ.د– درياد مليكة، أستاذة محاضرة "أ"، جامعة الجزائر .....ممتحنا

أ.د– علاكريمة ، أستاذة محاضرة "أ"، جامعة الجزائر.....ممتحنا

أ.د ـ حمودي ناصر، أستاذ محاضر "أ"، جامعة البويرة .....ممتحنا

تاريخ المناقشة : 2018/06/27

بسم الله الرحمن الرحيم



إهداء

إلى من لا يمكن للكلمات أن توفي حقهما،

الوالدين الكريمين

إلى من لا أستطيع الاستغناء عنهم،

زوجتي و أولادي

وإلى كل الأهل و الأقارب

و جميع الأصدقاء و الزملاء

أهدي ثمرة جهدي.

جمال.

شكر و عرفان

في البداية، أحمد الله الذي أعطانا القوة والصبر لإتمام هذا العمل العلمي المتواضع.

ثم أتوجه بجزيل الشكر و الامتنان إلى الأستاذ إقلولي محمد لقبوله الإشراف على هذه الأطروحة، إذ لم يبخل عليا بإرشاداته وتوجيهاته القيمة لإثراء هذا العمل رغم مشاغله الكثيرة .

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه الأطروحة.

ولا أنسى أن أشكر كل من قدّم لي يد العون من قريب أو بعيد في إنجاز هذا العمل.

جمال براهيمي

قائمة أهم المختصرات

أولا: باللغة العربية

–**ج.ر.ج. ج:** جريدة رسمية للجمهورية الجزائرية الديمقراطية الشعبية

ـ **د.ذ.د.ن:** دون ذكر دار النشر

ـ **د.ذ.ب.ن:** دون ذكر بلد النشر

ـ **د.ذ.س.ن:** دون ذكر سنة النشر

ـ **ص:** صفحة

ـ **ص.ص:** من صفحة إلى صفحة

ـ **ق.إ.ج** : قانون الإجراءات الجزائية

ـ **ق.ع** : قانون العقوبات

ثانيا: باللغة الأجنبية

- **C.P.P.F**: Code de Procédures Pénales Français

-Ed.: Edition.

- **JORF.:** Journal Officiel de la République Française

- **Ibid.**: Au Même Ouvrage

- **I.P** : Adresse Internet Protocole

قائمة أهم المختصرات

-**L .G.D.J** : Librairie Générale de Droit et de Jurisprudence.

-N° : Numéro.

-**O .C.D.E :** Organisation de Coopération et de Développement Économique

- **O.N.U** : Organisation des Nations Unies.

-**O.P.U** : Office des Publications Universitaires.

-**Op.cit**. : Ouvrage Précédemment Cité.

-**P**. : Page

-**P.P** : de la Page à la Page.

-**P.U.F** : Presses Universitaires de France.

-**R.I.P.C** : Revue Internationale de Police Criminelle.

- **R.I.D.P**: Revue Internationale de Droit Pénal

-**S.** : Suite.

- **T.C.P** : Trams Commission Protocol.

-**T.G.I** : Tribunal de la Grande Instance.

مقدمة:

لقد دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من التطور الفكري و المعرفي الهائل غير المعهود، وذلك بفضل الثورة العلمية التكنولوجية في مجال الاتصالات والمعلومات التي اقتحمت بقوة هذه المرحلة، و وفرت مناخا خصبا لنهضة علمية تكنولوجية شاملة غير مسبوقة في كافة مجالات الحياة، الاقتصادية، الاجتماعية، الثقافية، والعلمية، تهاوت أمامها الحدود السياسية و الحواجز بين الدول و الشعوب، وضاقت معها الأماكن وتقلصت فيها المسافات، واختزلت وطوت الأبعاد، بما تتميز به من عنصري السرعة والدقة في تجميع للمعلومات، تخزينها ومعالجتها، ومن ثم نقلها و تبادلها عن بعد بين الأطراف المختلفة داخل الدولة الواحدة أو بين عدة الدول، حتى أضحت فيه الكرة الأرضية قرية صغيرة تسبح في فضاء الكتروني. وهو ما دعا بالكثير من المفكرين إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في أواخر القرن التاسع عشر، ففي حين كان الهدف من الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان، فان هدف الثورة الثانية إحلال الآلة محل النشاط الذهني للإنسان.

ولا شك أن هذه الثورة المعلوماتية الهائلة قد انعكست بصورة إيجابية على كثير من جوانب الحياة المعاصرة، بسبب ما توفره من الوقت والجهد والتكلفة عن الإنسان تجعل حياته اليومية أكثر سهولة و يسر، الأمر الذي أدى إلى تضاعف الطلب على التقنيات التي تقوم عليها هذه الثورة والمتمثلة في الحواسيب الآلية والشبكات المعلوماتية، وتوسع ميادين استعمالها وازداد الاعتماد عليها بشكل مفرط في كل القطاعات العامة أو الخاصة، إلى حد بدا من الصعب على هذه القطاعات أداء نشاطاتها دون الاستعانة بشكل أساسي على هذه التقنيات الحديثة.

مقدمة:

وبالرغم من المزايا والفوائد الجمّة التي تحققت وتتحقق يوما بعد يوم في كل مناحي الحياة بفضل تقنيات وسائل تكنولوجيات المعلومات والاتصال، إلا أن الاستخدام المتنامي لهذه التقنيات انطوى، في الوقت ذاته، على بعض الجوانب السلبية التي تمثل تهديدا خطيرا للأمن والاستقرار في المجتمع، جراء سوء استخدام هذه التقنية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات. الشيء الذي استتبعه ظهور نمطا جديدا من الجرائم، لم يكن معهودا من قبل سمي بجرائم تقنية المعلومات أو الجرائم الإلكترونية.

ولا جدال في اعتبار الجرام الإلكترونية من أخطر و أعقد الجرائم على الإطلاق و تأتي في مقدمة الأشكال الجديدة للجريمة المنظمة، وخطورة هذه الجرائم نابعة من طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها وحداثة أساليب ارتكابها والبيئة التي ترد عليها وخصوصية مرتكبيها و وسائل كشفها. فهي جريمة تقنية سهلة الارتكاب، تنشأ في الخفاء وفي بيئة الكترونية افتراضية مكونة من إشارات وذبذبات مغناطيسية تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الاتصالات بصورة آلية دون أن تخلف أي أثار محسوسة، ويقترفها مجرمون أذكياء يمتلكون أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات ويتمتعون بمهارات و خبرات تقنية عالية، فضلا على أنها جرائم عابرة للحدود تتم عبر شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأية سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي.

وقد أدت هذه الخصائص التي تميز الجريمة الإلكترونية إلى صعوبة التعامل مع النشاطات الإجرامية المستحدثة وتكييفها على أساس النصوص الجنائية التقليدية مع ما قد يشكله ذلك من مساس بمبدأ الشرعية الجزائية والتفسير الضيق للنص الجنائي وحضر القياس، وهو ما ألقى مسؤولية كبيرة على عاتق المشرع الجزائي في اتخاذ الخطوات

التشريعية الضرورية لمواجهة الجرائم الإلكترونية الناشئة عن إساءة استخدام الأنظمة المعلوماتية. وذلك بسن نصوص جنائية جديدة تتوافق مع هذه الأنشطة الإجرامية المستحدثة، وتمكّن مرفق العدالة الجنائية من تطوير آليات ووسائل التصدي للجرائم التي أفرزتها تكنولوجية الإعلام و الاتصال، والاستفادة من معطيات هذه التكنولوجيا الحديثة في الكشف عن الجرائم و إثباتها وملاحقة مرتكبيها لتقديمهم إلى العدالة.

ولا تقتصر الصعوبات والمشكلات التي تثيرها ظاهرة الإجرام الالكتروني فقط على القانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الإجرام، بل امتدت إلى نطاق القانون الجنائي الإجرائي، حيث صيغت نصوصه لتنظم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كثيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

وتتجسد أولى المشكلات الإجرائية في مجال الجرائم الالكترونية، في التحديات القانونية والعملية التي تثيرها عملية البحث والتنقيب أمام سلطات التحقيق بجميع مستوياتها وباختلاف أدوارها. وبالتحديد فيما يخص إثبات هذه الجرائم والآلية المناسبة لمباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية وصولا الى الحقيقة. إذ أن الجهات المكلفة بالبحث والتحري متعودة على التعامل مع الجريمة التقليدية، التي ترتكب في عالم مادي و ملموس يلعب فيه السلوك المادي الدور الأكبر والأهم، ويسهل التحري والبحث فيها بالنظر إلى ما تتضمنه من عناصر مادية يمكن إدراكها بالحواس، وما يمكن أن يخلفه المجرم من أثار محسوسة في مسرح الجريمة من بصمات أو قطرات دم أو محررات مزورة...، على خلاف الجريمة الالكترونية التي ترتكب في مسرح الكتروني غير مادي يختلف تماما عن المسرح التقليدي، ولا يخلف مرتكبها أي أثار، بسبب دقة وسرعة اقترافها، وإمكانية محو أثارها، وإخفاء الأدلة

المحصلة عقب وقوعها مباشرة. وهو ما يجعل سلطات البحث والتحقيق في حيرة من أمرهم إزاء هذه الوقائع الاستثنائية غير المألوفة.

ويزداد الوضع تعقيدا بالنسبة لجهات الاستدلال حينما يتعلق التحقيق بجريمة الكترونية امتد أثارها إلى خارج الإقليم الوطني، بحيث تثير مسألة تتبعها و الدخول إليها قصد جمعها وتحويلها إلى الدولة التي يجري فيها التحقيق مشكلات تتعلق بسيادة الدولة و الولاية القضائية، والتي لا يحتاج حلها إلى تعاون دولي في هذا المجال.

ومع إدراك الصعوبة التي تطرحها المواجهة الإجرائية لأشكال الإجرام الجديدة التي أفرزتها بيئة المعالجة الآلية للمعطيات والتنبه لأثارها السلبية، بدأت مهمة معالجتها تحظى باهتمام متزايد من الحكومات وحتى العديد من الهيئات الدولية، فأخذ الفنيون وخبراء الحسابات والإعلام الآلي، يركزون جهودهم البحتة وتجاربهم العلمية على سدّ ثغرات الأنظمة الأمنية وتحسين وتطوير أساليب الحماية الفنية للنظم والبرامج المعلوماتية لتصل إلى أقصى درجة ممكنة من الفعالية تجنبا لوقوع اعتداءات عليها أو بواسطتها، وتكفّل الفقه الجنائي بإبراز أوجه القصور التي تعترى تطبيق النصوص الإجرائية للتشريعات التقليدية القائمة على النمط الإجرامي الجديد الذي أسفرت عنه المعلوماتية، وسعى المشرع إلى تدارك هذا القصور باستحداث نصوص قانونية إجرائية تحمل معها طرقا إجرائية مدعّمة من قبل التقنية ذاتها، تمكن رجال العدالة الجنائية من البحث والتحقيق واستنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم. ومن ثم تحقيق التوازن بين الضرورة الملحة في عصرنا إلى الاستفادة من إمكانات الحسابات و تقنيات التكنولوجيا الحديثة، وبين الحاجة الفردية والاجتماعية إلى الحماية الجزائية من انعكاسات هذه التقنيات.

من هنا تظهر أهمية موضوع " **التحقيق الجنائي في الجرائم الالكترونية**" وسبب اختيارنا له رغم ما يكتنفه من صعوبات ترجع في الأساس الى حداثة هذا الموضوع وما

مقدمة:

يتسم به من صبغة علمية بحتة جديدة غريبة في تصورنا على رجال القانون، إذ لم ينل حظه بعد من البحث و التمحيص على المستوى الفقه الجنائي، كما أن معظم الدراسات والأبحاث القانونية التي عنيت بالجرائم الالكترونية تركّز على الجانب الموضوعي فقط، ما نتج عنه قلة وندرة المراجع و المؤلفات التي تعرضت للجانب الإجرائي. وهو ما أثار اهتمامنا للبحث وإثراء النقاش القانوني في هذا الموضوع، من خلال تحقيق مقصدين أساسيين: فأما المقصد الأول فهو نظري، نسعى من خلاله إلى التعرف على طرق وآليات التحقيق في مثل هذه الجرائم، وما هي العقبات الإجرائية التي تصطدم بها سلطات البحث والاستدلال في التعامل معها، ثم اقتراح الحلول القانونية المناسبة و الممكنة لتجاوز هذه العقبات. للاستفادة منها في المواجهة الفعالة للجرائم الالكترونية ومواكبة تطوراتها .

وأما المقصد الثاني فهو تطبيقي، ينبع من كون هذه الدراسة تأتي في وقت تهم فيه عدة دول بما فيها الجزائر إلى إعادة النظر في قوانينها الإجراءات الجزائية، مما قد يتيح لهذا البحث المتواضع في توجيه أنظار المشرع في هذه الدول إلى ضرورة مسايرة تشريعاتها للتطورات التكنولوجية وما تطرحه من مشاكل، واستدراك وتغطية الفراغ التشريعي الملحوظ في هذا المجال، ولإفادته ببعض المقترحات التي نوردها بعد تسليط الضوء على أخر ما توصلت إليه الدول المتقدمة في علم القانون لمواجهة الإجرام الالكتروني المتطور.

وأما عن الإشكالية التي يطرحها موضوع دراستنا هذا، فتنصب أساسا حول **إبراز إلى أي مدى يمكن الاعتماد على إجراءات التحقيق التقليدية لإثبات جرائم إلكترونية ارتكبت في عالم افتراضي غير ملموس، وهل تطبيق هذه الإجراءات كافيا وفعالا لاحتواء متغيرات هذا النمط المتجدد والمتطور من الجرائم، أم أن ذلك سيؤدي إلى عدم الوفاء بمتطلبات مبدأ الشرعية الإجرائية وما ينجر عن ذلك من عقبات؟**

وللإجابة عن هذه الإشكالية اعتمدنا على المنهج الوصفي التحليلي، وصفي لأن دراستنا سترتكز على وصف المفاهيم العامة الخاصة بالإجراءات المتبعة للبحث و التحقيق في الجرائم الالكترونية لاستخلاص الدليل والعقبات التي تعتريها، وتحليلي لأننا سنستعرض أهم الإشكالات القانونية التي تطرحها المواجهة الإجرائية للجريمة الالكترونية، ثم مناقشتها وتحليلها بشكل من التفصيل والتشريح بالخوض في جزئياتها، من ثمة تقديم الحلول المناسبة على ضوء ما توصل إليه الفقه و التشريع والقضاء المقارن. ونتبع في ذلك خطة تتضمن بابين: قوام الباب الأول تحليل **آليات التحقيق في الجرائم الالكترونية**، من خلال التأكد في الفصل الأول من محدودية سريات إجراءات التحقيق المألوفة على الجرائم الالكترونية، ولما تبين لنا قصور هذه الإجراءات، عرجنا في الفصل الثاني إلى استعراض إجراءات التحقيق المستحدثة. وأما الباب الثاني فقوامه إبراز **عقبات التحقيق في الجرائم الإلكترونية و الحلول المقترحة لتجاوزها**. من خلال التركيز في الفصل الأول على تبيان عقبات التحقيق في الجرائم الإلكترونية، وتخصيص الفصل الثاني لاقتراح الحلول الممكنة لتجاوز هذه العقبات.

الباب الأول

آليات التحقيق في الجرائم الإلكترونية

لكل عصر سماته و خصائصه، وسمات العصر الحالي الدخول في عالم ثورة تكنولوجيا الإعلام والاتصالات وما ترتب عنه من تغيير في نمط الحياة سواء على مستوى الأفراد أو الحكومات، ومن الحقائق المسلم بها، أن للتقدم التكنولوجي تأثير على القانون و الواقع الذي يظهر في ظلّه، ولكي تتحقق الفائدة المرجوة من هذا التقدم، يجب ألا ينفصل القانون عن الواقع الذي يفرزه ويطبق عليه، بل يجب أن يكون متجاوبا معه ومتطورا بنفس وتيرة تطوره.

ولا ريب أن التطور الحالي الذي لحق ثورة الاتصالات عن بعد وما أفرزته هذه الثورة من وسائل الكترونية متقدمة ومتعددة، قد انعكس أثره على الجرائم التي تمخضت عن ذلك، وتميزت هذه الجرائم بطبيعة خاصة في الوسائل التي ترتكب بها، والمحل الذي تقع عليه، والجناة المقدمين على ارتكابها الذين يتمتعون بالذكاء الخارق، فهي تجمع بين الذكاء الاصطناعي والذكاء البشري، مما جعل مواجهتها جنائيا أمر في غاية الصعوبة.

فالتطور الحالي الذي انعكس أثره على قانون العقوبات، قد انعكس أثره كذلك على قانون الإجراءات الجزائية، بشكل جعل بعض أحكام هذا الأخير لا تطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الالكترونية، وهو ما ترتب عليه فراغ تشريعي في هذا المجال، وأصبح الواقع الحالي بعد ثورة المعلومات لا يستظل بالحماية القانونية الكافية التي تقيه شرّ الجرائم المتطورة التي قد لا تتقيد بنطاق المكان، وقد لا يكون محلها الأشياء المادية التقليدية التي تعارف الناس عليها، كما قد ترتكب بوسائل مستحدثة ذات تقنية عالية ولا تترك وراءها أثارا مادية ملموسة.

وأمام هذا الواقع الذي ينبئ بأن القوانين العقابية المطبقة قد ضاقت نصوصها بما رحبت عن استيعاب الأنواع الجديدة من الجرائم التي جاءت بها ثورة المعلومات،

وأن القوانين الإجرائية ليست بأحسن حالا منها، لجأ الفقه والقضاء إلى الاجتهاد في تفسير تلك النصوص التقليدية حتى تسري على هذه الجرائم المستحدثة تفاديا إفلات الجناة من المتابعة الجزائية و العقاب.

ورغم هذا الحل الذي قدمه الفقه والقضاء لمواجهة الجرائم التي أفرزتها ثورة المعلومات إلا أن القصور بقي يعتري النصوص الجزائية التقليدية، مما دفع المشرع في العديد من الدول إلى إعادة النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون. لأن كشف ستر هذا النوع من الجرائم الذي يرتكب بالوسائل الالكترونية يحتاج إلى طرق الكترونية تتناسب مع طبيعته ويمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة. وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل قادرة على القيام به، مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الالكترونية الاعتماد عليها في الوصول إلى الدليل المناسب في إثباتها.

ولا شك أن هذا الدليل سيتم استخلاصه من البيئة الالكترونية والرقمية التي تعتبر مسرح الجريمة المعلوماتية، مما يجعله يتميز بخصائصها، وهو الأمر الذي يقودنا إلى الحديث عن مسألة القيمة الثبوتية لهذا الدليل ومدى قبوله من طرف القضاء الجزائي، ومدى مشروعيته وتعبيره عن الحقيقة بالنظر الى ما يمكن أن يتعرض له من التزييف والتحريف. بل حتى مع ضمان مصداقية هذا الدليل ومشروعيته، فتثار مسألة أخرى أكثر أهمية تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي الجزائي إعمالا لمبدأ الاقتناع الشخصي للقاضي الجزائي الذي يشكل جوهر أية محاكمة.

تفصيلا لما سبق ذكره سوف، نقسم هذا الباب إلى فصلين، ندرس **في الفصل الأول إجراءات التحقيق في الجرائم الإلكترونية**، وفيه نركّز على إظهار مدى سريان إجراءات التحقيق المألوفة عليها، ثم نبيّن بعدها حاجة هذا النوع الإجرامي المستحدث إلى إجراءات تحقيق جديدة خاصة تتناسب مع طبيعته. أما **الفصل الثاني**، فنخصصه لإبراز **القيمة الثبوتية للأدلة المتحصلة من الوسائل الإلكترونية** و أثرها على تكوين اقتناع القاضي الجزائي.

الفصل الأول

إجراءات التحقيق في الجرائم الإلكترونية

إذا كانت ظاهرة الإجرام الالكتروني قد أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي، بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم واحترام مبدأ الشرعية والتفسير الضيق للنصوص الجزائية، فقد أثارت في الوقت نفسه مشكلات أكثر في نطاق القانون الجزائي الإجرائي. وتزداد المشكلات الإجرائية في مجال الجرائم الالكترونية بتعلقها في العديد من الأحيان ببيانات المعالجة الآلية وكيانات منطقية غير مادية، ومن ثم يصعب الكشف عنها وإثباتها نظرا للسرعة الفائقة والدقة غير المتناهية في تنفيذها، ناهيك عن إمكانية محوها و تمويه آثارها وإخفاء الأدلة المتحصل منها بسهولة عقب تنفيذها باستعمال تقنيات تكنولوجيا عالية.

ولقد امتد تأثير التقنية المعلوماتية إلى الجانب الإجرائي من القانون الجزائي بشكل أوسع مع مرور الوقت، لأن نصوص هذا القانون صيغت و وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية، ترتكب في عالم محسوس وملموس يؤدي فيه السلوك المادي الدور الأكبر والأهم على خلاف الجريمة الالكترونية التي ترتكب في مسرح إلكتروني افتراضي وغير مادي يختلف كليا عن المسرح التقليدي.

وأمام هذا الوضع أثير التساؤل حول مدى صلاحية تطبيق إجراءات التحقيق التقليدية على جرائم إلكترونية ارتكبت في عالم افتراضي غير ملموس، وهل هذا الأمر يجعل قانون الإجراءات الجزائية قاصرا عن الوفاء بمتطلبات الشرعية الجزائية في مواجهة هذا النمط الإجرامي الجديد؟ (المبحث الأول)، وإذا كان الوضع كذلك، فهل يقتضي تدخل المشرع لتعديل قواعد قانون الإجراءات الجزائية القائمة واستحداث قواعد إجرائية خاصة تتناسب والطبيعة المميزة للجرائم الالكترونية، والتي من خلالها يمكن لسلطات تنفيذ القانون تجاوز

المشكلات التي تواجهها أثناء عملية البحث والتحقيق في مثل هذه الجرائم ؟ (المبحث الثاني).

المبحث الأول

محدودية سريان إجراءات التحقيق المألوفة على الجرائم الإلكترونية

لم يكن لدى الدول خيار آخر للتصدي لظاهرة الإجرام الالكتروني في بداية ظهورها إلا الاعتماد على النصوص الجزائية القائمة بمختلف فروعها الموضوعية و الإجرائية، وذلك تفاديا لإفلات الجناة من العقاب من جهة، وعدم وجود قواعد قانونية أخرى تتلاءم و طبيعة هذه الجرائم المستحدثة من جهة أخرى. ولكن بعد التطور السريع الحاصل في مجال المعلوماتية وما صاحبه من انعكاسات على الجرائم في الوسائل المستعملة لارتكابها والمحل الذي تقع عليه ونوع الجناة الذين يرتكبونها، جعل هذه القوانين غير مواكبة لها، وبالتالي أضحت غير مجدية[9]. الأمر الذي دفع بالعديد من الدول خاصة المتقدمة منها إلى إعادة تقويم منهج بعض الإجراءات التقليدية والبحث عن صيغ جديدة لقوانينها العقابية و قوانين الإجراءات الجزائية بما يتناسب مع هذه الجرائم الجديدة ذات التقنية العالية، والعمل على تطوير وساءل الإثبات الجزائية بما يتوافق و الحقائق العلمية لتفادى هذا القصور.

ومما لا شك فيه، أن المشرع حينما أراد توسيع نطاق تطبيق إجراءات التحقيق التقليدية لتطال الجرائم الالكترونية، فانه يقصد بها تلك الإجراءات التي تثير إشكالات و عقبات عملية تعود إلى خصوصية هذه الجرائم، كالتفتيش، الضبط، المعاينة و الخبرة، والتي هي في

[9]– **محمد قدري حسن عبد الرحمن**، جرائم الاحتيال الالكتروني، مجلة الفكر الشرطي، عدد 79، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011، ص 159.

حاجة إلى تطوير و تحيين لكي تتناسب مع طبيعتها الخاصة و طبيعة الدليل الذي يصلح لإثباتها[10]. أما غيرها من الإجراءات كسماع المتهم أو الشهود، الاستجواب والمواجهة، فإنها مستبعدة نظرا لعدم وجود أية صعوبات في اتخاذها. استرشادا بذلك، فإننا سوف نركّز على دراسة الفئة الأولى من إجراءات التحقيق دون غيرها.

المطلب الأول

التفتيش في البيئة الإلكترونية

قد يتطلب التحقيق تفتيش شخص المتهم أو منزله أو غيره أو منزله لضبط الأشياء المتعلقة بالجريمة، والتفتيش كإجراء من إجراءات التحقيق الابتدائي هو في الأصل من اختصاص سلطة التحقيق، المتمثلة في قاضي التحقيق والنيابة العامة باختلاف التشريعات[11]،إلا أنه يخوّل استثناء لرجال الضبطية القضائية في حالات محددة قانونا[12].

---

[10]– **محمد قدري حسن عبد الرحمن**، مرجع سابق، ص 172.

[11]– تتباين تشريعات الدول في تحديد السلطة المختصة بالتحقيق الابتدائي، ففي القوانين الإجرائية اللاتينية في مقدمتها القانون الإجرائي الفرنسي، نجد قاضي التحقيق هو سلطة التحقيق الأصلية و استثناءا النيابة العامة. الشيء نفسه في القانون الإجرائي الجزائري، على عكس المشرع المصري الذي يخول تلك السلطة مبدئيا للنيابة العامة و استثناءا لقاضي التحقيق. في حين نجد في التشريعات الانجلو سكسونية جهاز الضبطية القضائية هو وحده الذي يضطلع بمهمة التحقيق الابتدائي، كما هو الحال في القانون الانجليزي و الكندي، انظر في هذا الشأن:

–**إسحاق إبراهيم منصور**، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1995، ص 105.

[12]– من بينها حالة التحقيق في جناية أو جنحة متلبس بها المنصوص عليها في المادة (41) من ق إ ج ج، وفي التحقيق الابتدائي المنصوص عليه في المواد (63) و ما يليها من ق إ ج ج. أنظر أمر رقم(66–155) مؤرخ في 08 يونيو سنة 1966، يتضمن قانون الإجراءات الجزائية الجزائري، المعدل و المتمم.

وقد أجمع الفقه الجنائي، على أن التفتيش كإجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا[13].

يتبين من هذا التعريف، أن التفتيش ما هو إلا وسيلة للإثبات المادي، غايته هي ضبط الأدلة المادية الخاص بالجريمة، مما يجعله يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي، ومعطيات شبكة الانترنت التي ليس لها أي مظهر مادي محسوس في العالم الخارجي، ومن هنا يثار التساؤل عن مدى جواز إخضاع هذه المكونات المعنوية لعملية التفتيش؟

وللإجابة عن هذا التساؤل، يقتضي الأمر منا الوقوف عند الضمانات و الضوابط التي يجب على المحقق احترامها والتقيد بها قبل وأثناء قيامه بعملية التفتيش، منها ما يتعلق بمحل التفتيش و ما هو إجرائي.

الفرع الأول: محل التفتيش الإلكتروني

يقصد بمحل التفتيش، المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره و خصوصيته، والسر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة، كالمسكن أو سيارة أو رسائل، بالتالي فمحل التفتيش قد يكون أحد المواقع المذكورة مع مراعاة الإجراءات والشروط القانونية المقررة لكل موقع على حدة[14].

---

[13]–**عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص192.

[14]–**بكري يوسف بكري**، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2010، ص.ص 76–80.

ولما كان المستودع في الجرائم الالكترونية هو الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية(Hard Ware) كوحدات المعالجة المركزية (processeur)، وحدات الإدخال والإخراج ووحدات التخزين أو ما يسمى بوحدة التحكم(Unité De Contrôle)، ومكونات أخرى منطقية(Soft Ware) كبرامج النظام الأساسية، البرامج التطبيقية، والبيانات المعالجة آليا، كما أن له شبكات اتصالات بعدية سلكية ولاسلكية متواجدة على مستوى المحلي و الدولي[15]، فان الأمر يتطلب منا البحث في مدى قابلية جميع هذه المكونات للتفتيش؟

-أولا : تفتيش المكونات المادية للحاسب

ليس هناك خلاف على أن الولوج إلى المكونات المادية للحاسوب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الالكترونية و مرتكبيها يخضع لإجراءات التفتيش المألوفة، لأن حكم تفتيش هذه الكيانات المادية يتوقف أساسا على طبيعة المكان الذي تتواجد فيه ما إذا كان عاما أو خاصا[16]. فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له حكمه، بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن و ملحقاتها وبالإجراءات والضمانات المقررة قانونا في التشريعات المختلفة لذلك[17]. ففي القانون الجزائري مثلا تشترط المواد من (44 إلى 47) من قانون الإجراءات الجزائية للقيام بإجراء تفتيش مسكن في الجرائم المتلبس بها، الحصول مسبقا على إذن مكتوب صادر

---

[15] – **على محمود على محمودة**، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، نظمته أكاديمية شرطة دبي، في الفترة من 26 الى28 أفريل 2003، ص 135.

[16] –**عادل عبد الله خميس المعمري**، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مجلد 22، عدد 86، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، 2013، ص 260.

[17]–**خالد ممدوح إبراهيم**، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، إسكندرية، 2009، ص 195.

من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار بهذا الإذن قبل الدخول إلى المسكن والشروع في التفتيش،[18] على أن يتم التفتيش نهارا في الفترة الممتدة من الخامسة صباحا إلى الثامنة مساءا وبحضور صاحب المسكن أو ممثله وإن تعذر ذلك استدعى ضابط الشرطة القضائية القائم بالتفتيش شاهدين من غير الموظفين الخاضعين لسلطته[19].

وينبغي التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة أم أنها متصلة بحواسيب أو أجهزة متواجدة في مكان آخر كمسكن الغير، ففي هذه الحالة يجب على المحقق مراعاة القيود و الضمانات التي يشترطها القانون لتفتيش هذه الأماكن[20].

أما إذ كانت المكونات المادية للحاسوب متواجدة في أماكن عامة، سواء أكانت عامة بطبيعتها كالحدائق العامة والطرق العامة، أم أماكن عامة بالتخصيص كمقاهي الانترنت ومحلات بيع وصيانة الحواسب، فإجراءات تفتيشها تكون وفقا للأصول الخاصة بتلك الأماكن. ويستوي الأمر، بالنسبة للمكونات الموجودة بحوزة شخص ما، فبغض النظر عن صفة هذا الشخص، مبرمجا كان أو عامل صيانة أو موظفا في شركة تنتج برامج الحاسب الآلي، فإن تفتيش هذه المكونات يخضع لأحكام تفتيش الأشخاص، وبالشروط والضمانات

---

[18]- تجدر الإشارة إلى انه إذا تعلق الأمر بتفتيش المساكن في إطار التحقيق الابتدائي، فتشترط المادة (64) من ق إ ج قبل البدء في التفتيش، الحصول على رضا صريح و مكتوب بخط اليد من قبل صاحب المسكن، وإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه.

[19]– ونشير في هذا الشأن، أن المشرع الجزائري بعد التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في 20 ديسمبر 2006 استغنى بموجب الفقرة الأخيرة من المادة (45) و كذا الفقرة الثانية من المادة (47) والفقرة الثالثة من المادة (64) عن تطبيق كل الضمانات المقررة لتفتيش المساكن عندما يتعلق الأمر بالتفتيش في الجرائم الالكترونية. بحيث أصبح من الممكن القيام بتفتيش مسكن المتهم في جريمة الكترونية في أي ساعة من الليل أو النهار ودون حاجة إلى رضائه ولا لحضوره أثناء التفتيش.

[20]–**أحمد بن زايد جوهر الحسن المهدي**، تفتيش الحاسب الآلي وضمانات المتهم، مذكرة لنيل درجة ماجستير في القانون، كلية الحقوق، جامعة القاهرة، 2009، ص.ص 118–119.

القانونية المحددة لذلك[21].

بناء على ما سبق، يتضح أن تفتيش المكونات المادية لجهاز الحاسب و ملحقاته مثل لوحة المفاتيح أو الشاشة أو الطباعة أو غيرها من الأشياء المادية المحسوسة، لا يثير أية مشاكل إجرائية أمام سلطات الاستدلال، إذ يسري عليه ما يسري على تفتيش الأشياء والأدوات المادية الأخرى من شروط وضمانات، كمراعاة وقت التفتيش، الإذن بالتفتيش، الأشخاص القائمين بالتفتيش، والأشخاص المطلوب حضورهم عند التفتيش، مع مراعاة الاختصاص المكاني وعدم فض الأوراق المحرزة. كما أن أجهزة القضاء المخول لها القيام بإجراء التفتيش سواء بصفة أصلية أو استثنائية يمكنها تفتيش المكونات المادية في الجريمة الالكترونية دون الحاجة إلى أن تكون متخصصة في الجوانب التقنية، مثلها مثل غيرها من المكونات المادية الأخرى[22].

-ثانيا: مدى صلاحية مكونات الحاسب المنطقية للتفتيش

تعرف الكيانات المنطقية للحاسب بأنها "**مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات**" [23].

وإذا كان الأمر قد انتهى إلى صلاحية مكونات الحاسب المادية كمحل يرد عليه التفتيش، فان امتداد ذلك إلى المكونات غير المادية أو المنطقية هو محل جدل فقهي كبير حول مدى صلاحيتها لان تكون محلا للتفتيش تمهيدا لضبط الأدلة[24].

---

[21]– **بوكر رشيدة**، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، 2012، ص 395.

[22]– **فايز محمد راجح غلاب**، الجرائم المعلوماتية في القانون الجزائري و اليمني، أطروحة لنيل شهادة الدكتوراه في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر1، الجزائر، 2011، ص 309.

[23]– **عفيفي كمال عفيفي**، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، طبعة ثانية، منشورات الحلبي القانونية، دمشق، 2007، ص 61.

فالخلاف حاصل في مسألة كون التفتيش وسيلة للبحث وضبط الآثار المتعلقة بالجريمة وتقديمها إلى المحكمة كدليل إدانة، لذلك يثور الشك والتساؤل حول إمكانية اعتبار البحث عن أدلة الجريمة الالكترونية في نظم وبرامج الحاسب نوعا من التفتيش، باعتبار أن البيانات الالكترونية أو البرامج في حدّ ذاتها تفتقر إلى مظهر مادي محسوس في المحيط الخارجي، ويستشعر الفقه صعوبة المسألة بالنظر الى غياب الطبيعة المادية للمعلومات والبيانات، بما يجعلها تتنافى مع الهدف الذي يصبو إليه التفتيش ألا وهو البحث عن الأدلة المادية[25].

وإزاء هذا التشكيك سعى جانب من الفقه إلى إزالته و تجنبه على نحو يسمح بتضمين التفتيش بمعناه التقليدي، البحث والتنقيب في نظم وبرامج الحواسب عن أدلة الجريمة الالكترونية[26]، وحجتهم في ذلك هي أنه وإن كانت هذه النظم والبرامج عبارة عن نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية إلا أنها قابلة للتسجيل والتخزين والتحميل على وسائط و دعائم مادية معينة، ولها كيان مادي محسوس من خلال استشعارها وقياسها، لذلك فمن الممكن جدا إخضاعها لقواعد التفتيش التقليدية.

وعلى النقيض من ذلك، يرى جانب آخر من الفقه بأنه من غير الممكن إخضاع مكونات الحاسب المنطقية لقواعد التفتيش التقليدية، لان هذه القواعد وضعت في وقت لم

---

[24]– **علي محمود علي حمودة**، مرجع سابق، ص 81.

[25]– يعرف الدليل المادي بأنه الدليل الذي ينبعث من عناصر مادية ناطقة بنفسها و يؤثر في اقتناع القاضي بطريقة مباشرة، أنظر :**أحمد ضياء الدين محمد خليل**، مشروعية الدليل في المواد الجنائية، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق، جامعة عين الشمس، القاهرة ، ص 374.

[26]– أبرز مثال على ذلك الفقه الكندي الذي وسّع تفسير معنى التفتيش المنصوص عليه في المادة (487) من قانون العقوبات ليشمل تفتيش المكونات المنطقية للحاسوب، و الشئ نفسه فيما يخص قانون إساءة استخدام الحاسوب الانجليزي لعام 1990 ساري المفعول الذي نص على إمكانية تفتيش المكومات المادية و المعنوية للحاسوب. راجع: **هلالي عبد الله**، تفتيش نظم الحاسب الآلي و ضمانات المتهم ألمعلوماتي" دراسة مقارنة، دار النهضة العربية، القاهرة، 2006، ص 201.

تكن نظم المعالجة الآلية والحواسيب موجودة وتطبيقاتها غير معروفة، بالتالي فطبيعة هذه المكونات تتطلب إحداث قواعد تفتيش جديدة خاصة بها، أو على الأقل تعديل قواعد التفتيش المألوفة بشكل يجعلها تتلاءم أحكامها مع متطلبات هذه التقنية الجديدة[27].

ويبدو أن غالبية تشريعات الدول المتقدمة تميل إلى هذا الاتجاه، وكان المشرع الأمريكي سباقا إلى ذلك حينما نظم بنصوص جديدة إجراء التفتيش والضبط في بيئة الحاسب الآلي في القسم 2000 من القانون الإجرائي الاتحادي الخاص بجرائم الحاسب[28]. ثم تلاه المشرع الانجليزي بنصه في قانون إساءة استخدام الحاسب الآلي لعام 1990 على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي، وتبعه المشرع الفرنسي الذي قام بتعديل نصوص التفتيش التقليدية لتواكب التكنولوجيات الحديثة، إذ أضاف بموجب المادة(42) من القانون رقم (545-2004) المتعلق بالثقة في الاقتصاد الرقمي عبارة "المعطيات المعلوماتية" مشيرا إلى المادة (94) من قانون الإجراءات الجزائية، لتصبح هذه المادة على النحـو التـالي: "يباشر التفتيش في جميع الأمـاكن التـي يمكن العثـور فيها علـى أشياء أو **معطيات معلوماتية** يكون كشفها مفيدا لإظهار الحقيقة" [29].

ولم يبق المشرع الجزائري مكتوف الأيدي تجاه المتغيرات التي تحدث في عالم التكنولوجيات الحديثة، بل قام بدوره باستحداث نصوص قانونية جديدة أجاز من خلالها تفتيش المكونات المنطقية والمعطيات المعلوماتية للحاسب، ومن بين هذه النصوص المادة (05) من القانون رقم (09-04) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة

---

[27]- **موسى مسعود أرحومة**، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول "المعلومات و القانون" المنعقد بأكاديمية الدراسات العليا، طرابلس، في 28-2009/10/29، ص8.

[28]- **نبيلة هبة هروال**، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013، ص 226.

[29] -**FOURMENT F**, procédure pénale- la perquisition du disque d'un ordinateur a chaud, CPU, Paris, 2002-2003, mise a jour de 2004, P 05.

بتكنولوجيات الإعلام والاتصال ومكافحتها التي تسمح للسلطات القضائية المختصة ولضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة (04) من هذا القانون، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعلوماتية[30].

وفي هذا الصدد، نصت الاتفاقية الأوروبية حول الجرائم الالكترونية صراحة على حق الدول الأعضاء في تفتيش النظم المعلوماتية وحثتها على تجسيد هذا الحق بكل وضوح في قوانينها الإجرائية لتفادي أي إشكال يمكن أن يثار حول الموضوع، وذلك من خلال المادة (1/19) التي نصت على أنّ " لكل طرف الحق في سنّ من القوانين ما هو ضروري لتمكين السلطات المختصة من تفتيش أو الدخول إلى:

– نظام الحاسب أو جزء منه أو المعلومات المخزنة فيه.

–الوسائط التي يتم تخزين معلومات الحاسب بها ما دامت مخزنة في إقليمها[31].

ـ <u>ثالثا: مدى قابلية شبكات المعلومات المتصلة بالحاسب الآلي للتفتيش</u>

يقصد بالشبكة المعلوماتية، اتصال جهازين أو أكثر من أجهزة الحاسب الآلي اتصالا سلكيا أو لاسلكيا أو بواسطة الأقمار الصناعية، وقد تكون هذه الأجهزة مرتبطة بعضها البعض في موقع واحد فيطلق عليها الشبكة المحلية، أو موزعة على عدة أماكن متفرقة يتم ربطهـا عن طريق خطـوط الهـاتف أو المجال المغناطيـسي فتسمى الشبكة الممتدة أو شبكة

[30]– أنظر المادة (05) من القانون رقم (4/09) المؤرخ في 14 شعبان 1430 الموافق ل 05 غشت سنة 2009 والمتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام و الاتصال و مكافحتها، ج ر عدد 47، صادر بتاريخ 25 شعبان 1430 الموافق ل 16 أوت 2009.

[31]– راجع نص المادة (1/19) من الاتفاقية الأوروبية حول الجرائم المعلوماتية، مرجع سابق.

الانترنت[32].

ومع تطور تكنولوجيات الإعلام والاتصال لم يعد نطاق الاتصالات محدودا في نطاق إقليم دولة واحدة، بل امتد ليشمل كل أرجاء العالم، خاصة بظهور الانترنت التي تمثل منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لا مركزية، ويدخل في تركيبها ملايين الحواسيب موزعة عبر مختلف دول العالم[33].

لذلك يثير إخضاع شبكات المعلومات المتصلة بالحاسب الآلي لعملية التفتيش صعوبات كبيرة، تتعلق بالدرجة الأولى بالطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، فقد يكون الموقع الفعلي لهذه المعلومات داخل اختصاص قضائي آخر في إقليم دولة واحدة أو في إقليم دولة أو عدة دول أخرى، وهو ما يزيد الأمر تعقيدا باعتبار الشبكة المعلوماتية ممتدة عبر أرجاء العالم[34]. ومن هنا يثار التساؤل حول مدى جواز إمداد التفتيش إلى الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا كانت متواجدة في

---

[32]– يتم الاتصال أو نقل المعلومات بواسطة الشبكية وفق ثلاثة أشكال هي:

–اتصال أحادي الجانب (Simplexا) وفيه يتم الاتصال بنقل المعلومات في اتجاه واحد فقط من جهاز الحاسب المستفيد إلى الجهاز المركزي.

– اتصال ثنائي النصفي للمعلومات (Half Duplex) وفيه يمكن تبادل الاتصال بين جهازين بإرسال المعلومات، شريطة أن لا يتم الإرسال من الطرفين في وقت واحد.

– اتصال ثنائي كامل المعلومات(Full Duplex) وفيه يمكن تبادل الاتصال بين جهازين بارسال و استقبال المعلومات في الوقت نفسه.

[33]– **تيطاوني الحاج**، الانترنيت عملاق العولمة، بحث مقدم إلى الملتقى الوطني الأول تحت عنوان، القانون و قضايا الساعة –النظام القانوني للمجتمع الالكتروني، المنظم من طرف المركز الجامعي لخميس مليانة، ولاية عين الدفلة، الجزائر، من 09 إلي 11 مارس 2008، ص.ص 07–08.

[34]– **عادل عبد الله خميس المعمري**، مرجع سابق، ص 262.

دوائر اختصاص مختلفة؟ ويمكن أن نتصور هنا حالتين مختلفتين هما كالتالي:

-الحالة الأولى: اتصال حاسب المتهم بحاسب آلي آخر أو منظومة معلوماتية متواجدة في موقع آخر داخل إقليم الدولة نفسها

تتحقق هذه الفرضية حينما يقوم المتهم بتحويل عبر الانترنت معلومات أو بيانات متعلقة بجريمة إلكترونية من حاسبه إلى حاسب أو منظومة معلوماتية مملوكة للغير متواجدة في مكان آخر وتخزينها فيها[35]. ففي هذه الحالة تواجه سلطات التحقيق مشكلة تجاوز الاختصاص المكاني من ناحية، والاعتداء على حرمة خصوصية الغير من ناحية أخرى، لاسيما في الدول العربية التي لم تفصل قوانينها الإجرائية في هذه المسألة بعد.

نتيجة لذلك عمدت بعض التشريعات الإجرائية إلى تنظيم هذه المسألة وإزالة الإبهام عنها، بالنص صراحة على إمكانية وجواز امتداد الحق في التفتيش عند الحاجة ليشمل أجهزة الحاسب أو أية منظومة معلوماتية مرتبط بحاسب المتهم الجاري تفتيشه، وضبط كل البيانات الضرورية لإثبات الجريمة دون التقيد بالحصول على إذن مسبق آخر من السلطات القضائية المختصة بخصوص هذا الامتداد.

ويعتبر القانون الألماني من بين هذه التشريعات إذ نص في القسم (103) من قانون الإجراءات الجزائية على إمكانية تمديد التفتيش إلى السجلات و البيانات الموجودة في مكان آخر غير المكان الجاري التفتيش فيه دون الحاجة إلى إذن يخص هذا التمديد كلما دعت ضرورة التحقيق إلى ذلك[36]، وكذلك المشرع البلجيكي الذي نص في المادة (88) من قانون تحقيق الجنايات على أنه « إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو في جزء منه، **فهذا البحث يمكن أن يمتدّ إلى نظام آخر يوجد في مكان آخر غير مكان البحث**

---

[35]– **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، 2001، ص113.

[36]– **أحمد بن زايد جوهر الحسن المهندي**، مرجع سابق، ص 150

الأصلي، بشرط أن يكون ضروريا لكشف الحقيقة بشأن الجريمة محل البحث، وتكون هناك مخاطر تتعلق بضياع الأدلة نظرا لسهولة محو أو إتلاف أو نقل البيانات محل البحث» [37].

والشيء نفسه بالنسبة لقانون الجرائم المعلوماتية الأسترالي لعام 2001، الذي سمح بعمليات التفتيش على وجه السرعة للبيانات خارج المواقع التي تمّ اختراقها عن بعد بواسطة الحواسيب الجاري تفتيشها، وذلك دون اشتراط الحصول على موافقة مسبقة من السلطات المختصة عن ذلك[38].

ولقد حسم المشرع الفرنسي بدوره هذه المسألة بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون رقم (239-2003) المتعلق بالأمن الداخلي الصادر في 2003/03/18، إذ أجاز من خلال المادة (17 /1) لسلطات الضبط القضائي الولوج من الجهاز الرئيسي إلى المعلومات التي تهمّ البحث والتحري المخزنة في أنظمة معلوماتية أخرى وضبطها بناء على أمر بالتفتيش واحد كلما كان ذلك ممكنا[39].

وفي هذا الصدد، سمحت الاتفاقية الأوروبية لجرائم الالكترونية لعام 2001 الدول الأعضاء من خلال نص المادة (19 /2) بمدّ نطاق التفتيش الذي كان محله جهاز حاسب معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال، إذا كان يتواجد بها

---

[37] – **MEUNIER. C** , La loi du 28 novembre 2000 relative à la Criminalité informatique, Formation Permanente CUP, février 2001, n°103 .

[38]– **طرشي نورة** ، مكافحة الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011، ص 110.

[39]– l'art 17/1 du L.S.I.F dispose que « les officiers de polices judicaire ou, sous leur responsabilité, les agent de police judicaire peuvent, et au cours d'une perquisition effectuée dans les condition prévues par le présent code, accéder par un système informatique implanté sur les lieux ou se déroule la perquisition a des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dés que ces données sont accessibles a partir du système initial ou disponible pour le système initial » in **QUENER Myriam**, **FERRY Joél**, cybercriminalité défi mondial , 2ème édition, Ed Economica, Paris, 2009, p 02 .

معلومات أو بيانات مهمة للتحقيق يمكن الولوج إليها من خلال الجهاز محل التفتيش دون أن يشكل ذلك تجاوزا للاختصاص الإقليمي[40].

ولم يتأخر المشرع الجزائري عن التشريعات المذكورة أعلاه، إذ نصّ في المادة (2/5) من القانون رقم (09-04) لسنة 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها بأنه "... **في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزّنة فيها، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك....**"[41].

والملاحظ هنا أن تمديد التفتيش إلى منظومة معلوماتية أخرى مشكوك فيها يكتسي طابعا خاصا، فهو يتم عن بعد وبشكل سريع تماشيا مع طابع السرعة الفائقة الذي يجري عليه نقل المعلومات، و واضح أيضا أن الولوج إلى منظومة المعلومات يتم هنا بمجرد الشك أو الاعتقاد بتواجد المعلومات محل البحث داخل هذه المنظومة أو تلك، لذلك أوجب المشرع الجزائري على عكس التشريعات سالفة الذكر لكي يكتسي هذا الإجراء طابعه الرسمي ويقع تحت طائلة القانون، أن يكون الدخول إلى النظام المعلوماتي المقصود قانونيا ومتماشيا مع مقتضيات حماية الحياة الخاصة للأفراد، وهما الأمرين التي علّق المشرع تحقيقهما على شرط إبلاغ الجهات القضائية المختصة مسبقا بذلك. ولا شك أن الجهات المختصة

---

[40]- تنص المادة(2/19) من الاتفاقية على انه "**يحق للسلطة القائمة بتفتيش جهاز الحاسب المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمدّ نطاق التفتيش إلى أي جهاز أخر إذا كانت المعلومات المحزنة فيه يتم الدخول إليها من الحاسب الأصلي محل التفتيش**"

[41]- أنظر المادة 2/05 من القانون رقم(4/09)، مرجع سابق.

المقصودة في هذه المادة هي وكيل الجهورية وقاضي التحقيق باعتبارهما الجهة المؤهلة بمنح الإذن بالتفتيش.

ومما يتعين الإشارة إليه أيضا، أن المشرع الجزائري استطاع أن يتجاوز مسألة تفتيش المنظومة المعلوماتية عن بعد بصفة نهائية، حينما وسّع في التعديل الأخير لقانون الإجراءات الجزائية اختصاصات ضباط الشرطة القضائية في مجال التحقيق عن الجرائم الالكترونية، وأجاز إمكانية قيام هذه السلطات بالتفتيش في أي وقت من الليل و النهار، وفي أي مكان على امتداد كافة التراب الوطني[42].

-الحالة الثانية: اتصال حاسب المتهم بحاسب آخر أو منظومة معلوماتية متواجدة في إقليم دولة أجنبية

يتحقق هذا الاحتمال حينما يقوم المجرم الالكتروني بتخزين بيانات أو معلومات تفيد إثبات الجريمة في حاسب أو منظومة معلوماتية متواجدة خارج إقليم الدولة التي يقيم فيها، عن طريق شبكة الانترنت بهدف عرقلة سلطات البحث و التحري من الوصول إلى الدليل.

وفي مثل هذه الحالة تواجه سلطات التحقيق مشكلة كبيرة تتمثل في مدى جواز تمديدها إجراءات البحث والتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن بالتفتيش والدخول في المجال الجغرافي لدولة أخرى، وهو ما يسمي بالتفتيش العابر للحدود[43].

اتفق الفقه الجنائي على أنه لا يجوز لسلطات التحقيق التابعة لدولة ما اللجوء إلى التفتيش الالكتروني العابر للحدود لاسترجاع بيانات مخزنة في الخارج إلا في إطار اتفاقات

---

[42]– أنظر نص المادة (2/47 و 3) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

[43]– **حسين بن سعيد بن سيف الغافري**، السياسة الجنائية في مواجهة جرائم الانترنت، رسالة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، جامعة عين الشمس، القاهرة، 2005، ص 376.

تعاون خاصة ثنائية أو جماعية تجيز و تنظم هذا الامتداد، أو في إطار الإنابة القضائية المتبادلة أو على الأقل بعد الحصول على الإذن الصريح من الدولة الأجنبية، وفي ظل غياب هذه الاتفاقات و الإذن يعد الاختراق المباشر انتهاكا فعليا لسيادة الدولة[44].

ولكن تحسبا لطابع السرعة الفائقة الذي يجري عليه نقل المعلومات الإجرامية و تهريبها للخارج قصد تخزينها وإخفائها وما يستدعيه من الاستعجال في تعقب آثارها وضبطها لاستعمالها كدليل إثبات، وسّعت بعض تشريعات الدول من صلاحيات سلطات التحقيق للقيام بتفتيش الأنظمة المتصلة حتى لو كانت متواجدة في خارج إقليمها الوطني، وقرنت ذلك بحالة الضرورة، ومن ضمنها المادة (125) من قانون جريمة الحاسب الآلي الهولندي التي نصت على انه يجوز لجهات التحقيق و الاستدلال مباشرة التفتيش داخل الأماكن وبما ينطوي عليه تفتيش نظم الحاسب المرتبطة حتى إذا كانت موجودة في إقليم دولة أخرى، بشرط أن يكون هذا التدخل ضروريا ومؤقتا ومفيدا في كشف الحقيقة[45].

كذلك هو الشأن بالنسبة للتشريع الفرنسي، إذ أجازت الفقرة الثانية من المادة (57-1) من قانون الإجراءات الجزائية المضافة بموجب المادة (2/17) من قانون الأمن الداخلي رقم (239-2003) لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المعلوماتية المتصلة المتواجدة في خارج الإقليم الوطني كلما كان ذلك ممكنا، فنصت على انه " **إذا تبيّن مسبقا أن هذه المعطيات مخزّنة في نظام معلوماتي موجود خارج الإقليم الوطني، ويمكن الدخول إليها أو أنها متاحة انطلاقا من النظام الرئيسي، فانه يمكن الحصول عليها من طرف ضابط الشرطة القضائية على وجه السرعة كلما دعت ضرورة التحقيق لذلك، على أن يتم**

---

[44]- **PADOVA.(Y)**, un aperçu de la lutte contre la cybercriminalité en France, revue de science criminelle et de droit comparé, N°04, octobre-décembre, 2002, p765.

[45]-**VERGUCHT PASCAL** , la répression des délits informatiques dans un perspective internationale , thèse pour l'obtention du doctorat en droit, soutenue a la faculté du droit de l'université de Montpellier 1, Paris, 1996, P374.

إبلاغ السلطات المختصة في الدولة التي تتواجد هذه المعطيات على إقليمها فيما بعد وفقا للضوابط المنصوص عليها في المعاهدات الدولية" [46].

اتصالا بالفكرة نفسها، أجاز المجلس الأوروبي من خلال توصيته رقم (13) لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات تمديد تفتيش الالكتروني للحاسب إلى الشبكة المتصلة به ولو كانت تلك الشبكة واقعة في إقليم دولة أخرى، وأكد على أنّه "**يجوز لسلطة التحقيق والاستدلال بمناسبة التفتيش الالكتروني بسط مجال تفتيش حاسب معين يدخل في دائرة اختصاصها إلى غيرها من الأجهزة الالكترونية المرتبطة به بواسطة شبكة الانترنت بما فيها المتواجدة خارج الاختصاص الوطني وضبط المعطيات المتواجدة فيها، كلما كان التدخل الفوري للقيام بذلك ضروريا**"[47].

وفي نفس الإطار، خوّل المشرع الجزائري على غرار التشريعات السابقة سلطات التحقيق والبحث الحق بتفتيش عن بعد الأنظمة المعلوماتية المتصلة أو جزء منها حتى ولو كانت متواجدة خارج الإقليم الوطني، وذلك بنصه في المادة (3/5) من القانون (04/09) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على انه "...**إذا تبين مسبقا أن هذه المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل**".

---

[46]- **MEIER MARSELLA Carole** , l'effectivité du processus répressif dans le traitement de la cybercriminalité- enquête sur le système juridique français , thèse pour l'obtention du doctorat en droit, soutenue a la faculté du droit de l'université Paris 2, le 13-05-2005, pp 259-260.

[47]- **DIOP Abdoulaye**, procédures pénales et TIC, p25, article publier sur le cite ;

http ;//196.1.99.9/moodle/mod/book/print.php ? id=106.

الملاحظ في هذه المادة، أن المشرع الجزائري لم يسمح للسلطات القضائية المختصة وضباط الشرطة القضائية بتوسيع نطاق التفتيش الالكتروني ليشمل المعطيات المخزنة في منظومة معلوماتية تقع خارج القطر الوطني، إلا في إطار المساعدة القضائية المتبادلة وفي نطاق الاتفاقيات الدولية المبرمة في مجال ملاحقة الإجرام المعلوماتي. كما انه وخلافا للتشريعات سالفة الذكر لم يضع أية حالة استثنائية تسمح بالخروج عن هذا الإطار. ولكن بالمقابل ونظرا للطابع الخاص لهذا النوع من الجرائم وما يتطلبه تعقبها من سرعة، أجاز المشرع لسلطات الاستدلال في حالة الاستعجال تقديم وقبول طلبات المساعدة القضـائية الدولية عن طريق وسائل الاتصالات السريعة مثـل الفاكس أو البريد الالكتروني شريطة التأكد من صحتها[48].

ومع هذا ينبغي ألاّ تفسر المادة (3/5) أعلاه على أنها تمنع و بشكل مطلق تمديد التفتيش عن بعد لتطال نظم معلوماتية متواجدة في إقليم دولة أجنبية دون إذن أو رضا هذه الأخيرة، إنما يمكن السماح لذلك بناء على اتفاقيات دولية ثنائية أو جماعية ، ولكن بالطبع في حدود ما يسمح بها التعاون الدولي ووفقا لمبدأ المعاملة بالمثل بين الأطراف المتعاقدة.

ولقد حسمت الاتفاقية الأوروبية الخاصة بالجرائم الالكترونية المبرمة ببودابست في عام 2001 هذه المسألة، بالنص صراحة في المادة (32) على إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو منظومة معلوماتية تابعة لدولة أخرى بدون الحصول على إذن مسبق

---

[48]– وهو ما تضمنته المادة (2/16) من القانون رقم (09–04) بنصها على انه " **يمكن في حالة الاستعجال...قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني، وذلك بقدر ما توفره هذه الوسائل من أمن كافية للتأكيد عن صحتها**". وتأكّد في نص المادة 36 من الأمر رقم (06–09) الصادر في 2006/7/15 المتعلق بمكافحة التهريب على انه " ... **توجه طلبات المساعدة في مجال محاربة التهريب الصادرة عن السلطات الأجنبية كتابيا أو بالطريقة الالكترونية إلى الجهات المختصة... وفي حالة الاستعجال القصوى، يوجه الطلب شفاهة مع مراعاة تأكيده بوثيقة مكتوبة أو الكترونيا في أقرب الآجال**".

من هذه الأخيرة، وذلك في حالتين حددتهما المادة (32) أعلاه[49] على سبيل الحصر هما: الأولى، إذا تعلق التفتيش بمعلومات أو بيانات متاحة للجمهور، والثانية إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش[50].

وإدراكا منها لأهمية التفتيش العابر للحدود في مواجهة الجرائم الالكترونية و ما يتطلبه من سرعة التدخل لضبط الأدلة الالكترونية و الرقمية السهلة التلف و الضياع، اقترحت لجنة دول أطراف الاتفاقية الأوروبية لجرائم الالكترونية اثر المناقشات التي أجرتها في عام 2009 إلى جانب الحالتين المشار إليهما في المادة (32) المذكورة أعلاه حالات أخرى ترى من المفيد السماح فيها بالتفتيش عن بعد في أجهزة أو شبكات تابعة لدول أخرى دون الحصول على إذن منها، وهذه الحالات هي كالتالي:

أ-**حالة التفتيش عن بعد بحسن النية:** وتتحقق هذه الحالة عندما تقوم سلطات التحقيق بالولوج في أجهزة أو شبكات تابعة لدولة أجنبية دون قصد، كأن يجد المحقق نفسه يبحث في برنامج حاسب متواجد في دولة أجنبية صدفة أو خطئا، أو عندما يصعب عليه تحديد يقينا موقع البيانات المبحوث عنها.

ب-**حالات الاستعجال القصوى أو الحالات الاستثنائية:** الملاحظ هنا أن اللجنة لم تحصر حالات الاستعجال و الاستثنائية التي يمكن لهيئات التحقيق اللجوء فيها الى التفتيش عن بعد دون الحصول على إذن من الدولة المعنية، إنما اكتفت بتقديم بعض الأمثلة عنها

---

[49] - Art (32) stipule ; « … une partie peut, sans l'autorisation d'une autre partie ; a- accéder a des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou

b- accéder a, ou recevoir au moyen d'un system informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la partie obtient le consentement légal et volontaire de la personne légalement autorisée a lui divulguer ces données au moyens de ce système informatique ».

[50]– ينبغي الإشارة إلى أن الموقف نفسه تبنته جامعة الدول العربية في نص المادة (2/40) من الاتفاقية العربية لمكافحة الجرائم المتصلة بتكنولوجية الإعلام و الاتصال.

كوجود خطر ضياع الأدلة عن طريق الإتلاف أو التلاعب فيها بالتعديل، و وجود خطر إفلات المشتبه فيه. لذلك فعدم التحديد الواضح والصريح لحالات الاستعجال والحالات الاستثنائية هنا من شأنه أن يفتح المجال لحدوث تعسف في استعمال هذا الحق من طرف سلطات التحقيق و انتهاك سيادة الدول و اختصاصها الوطني دون مبرر مشروع [51].

ج- **حالة التفتيش عن بعد وفقا لمعيار مشروعية التفتيش " سلطة الاستعمال":**

حسب هذا المعيار، فمكان تواجد البيانات المبحوث عنها ليس المعيار الوحيد لتحديد الدولة صاحبة الحق في الدخول إلى هذه البيانات، بل يتعين الأخذ بعين الاعتبار الشخص الطبيعي أو المعنوي الذي يتمتع بسلطة التصرف في هذه البيانات سواء " بتعديل أو إتلاف أو تشفير هذه البيانات أو جعلها غير قابلة للتصرف فيها من طرف الغير "، وينطبق على هذه الحالة مزود خدمات الانترنت الذي يكون موقعه في إقليم دولة ما ويتمتع بسلطة التصرف في معطيات و بيانات متواجدة في إقليم دولة أو عدة دول أخرى[52].

إذا كانت الاتفاقية الأوروبية للجرائم الالكترونية لعام 2001 قد أجازت لسلطات التحقيق الوطنية التفتيش عن بعد لأجهزة الحاسب أو المنظومات المعلوماتية المتواجدة على إقليم دولة أجنبية دون علم أو رضا هذه الأخيرة و قرنت ذلك بدافع الضرورة و الخوف من ضياع الأدلة بسبب الطبيعة الخاصة التي تتسم بها الجريمة الالكترونية، إلا أن هذا التوجه لقي معارضة شديدة من قبل الفقه و القضاء في غالبية الدول، بالنظر الى ما يحمله من انتهاك لسيادة الدول و خرق لاختصاصها الوطني، بالتالي فمن الأجدر و الأفضل أن يتم التفتيش الالكتروني العابر للحدود في إطار التعاون القضائي الدولي وفق آليات اتصال

---

[51]- **BOURGUIGNON Jonathan** « la recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat » article présenté au Colloque de Rouen sur « internet et droit international » organisé par la société française pour le droit international du 30 Mai au 01 juin 2013, édition Pedone, Paris, 2014, P368.

[52]- **Ibid.**, p 369.

ميسرة و سريعة يتم تحديدها في اتفاقات دولية ثنائية أو متعددة الأطراف.

الفرع الثاني: ضمانات التفتيش في البيئة الإلكترونية

رغم اعتبار التفتيش من الإجراءات الجوهرية في عملية التحقيق البحث عن حقيقة الجرائم إلا أن معظم القوانين الإجرائية حرصت على إحاطته بجملة من الضمانات القانونية، وذلك تفاديا لتعسف سلطات البحث والاستدلال وما يمكن أن يحدثه من اعتداء على حقوق وحريات الأفراد وحرمة مساكنهم وحياتهم الخاصة من جهة، وإحقاقا لحق الدولة ممثلة المجتمع في كشف غموض الجرائم ومتابعة مرتكبيها وتوقيع العقاب عليهم من جهة أخرى. ويمكن تقسيم هذه الضمانات إلي ضمانات موضوعية وأخرى شكلية أو إجرائية نذكرها على النحو التالي:

-أولا: الضمانات الموضوعية للتفتيش الإلكتروني: تتمثل هذه الضمانات في الشروط الواجب توفرها حتى يكون التفتيش صحيحا، وتتلخص في ثلاثة شروط أساسية هي: سبب التفتيش، محل التفتيش، والسلطة المختصة بالتفتيش.

أ ـ سبب التفتيش: يعتبر عنصر السبب ضمانة قانونية لصحة و مشروعية إجراء التفتيش، يتحقق بوقوع جريمة ما يتم بموجبها توجيه الاتهام إلى الشخص أو الأشخاص المراد تفتيشهم بناء على أدلة أو قرائن قوية تفيد تورطهم في هذه الجريمة، عملا بمبدأ الشرعية الجزائية القاضي بأن "**لا جريمة و لا عقوبة إلا بالنص**"[53]. إذ بدون وقوع جريمة، و توجيه اتهام إلى شخص أو أشخاص معينين وفقا لأدلة كافية، يكون التفتيش باطلا لانتفاء السبب الذي يبرره.

---

[53]-وهو ما أقرته محكمة النقض المصرية باعتبارها أن " **الإذن بالتفتيش لا يصح إصداره إلا لضبط جريمة واقعة بالفعل وترجحت نسبتها إلى متهم معين و هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية**". طعن نقض جنائي، جلسة 1967/10/16، مجموعة أحكام النقض، س18 رقم 165، ص 965. نقلا عن: **خالد ممدوح إبراهيم**، مرجع سابق، ص 209.

وتطبيقا لما سبق، فان سبب التفتيش في الجرائم الالكترونية لا يتحقق إلا بتحقق العناصر الثلاثة التالية:

1- وقوع جريمة الكترونية تحمل وصف جناية أو جنحة

اتفقت معظم تشريعات الدول على أنه لا يجوز لهيئات التحقيق مباشرة إجراءات التفتيش إلا بعد التأكد من الوقوع الفعلي لجريمة الكترونية نص عليها القانون في نصوص التجريم والعقاب، وأي تفتيش في جريمة محتملة الوقوع مستقبلا ولو أيقنت التحريات والدلائل الجدية على أنها ستقع بالفعل يعدّ إجراء غير مشروع مآله البطلان[54].

ولا يكفي وقوع جريمة الكترونية للقول بمشروعية إجراء التفتيش طبقا للقواعد العامة، بل لابد أن تحمل هذه الجريمة بمنظور القانون وصف جناية أو جنحة [55]، ويستثنى من ذلك المخالفات بسبب ضعف خطورتها التي لا تستحق انتهاك حرمة الحياة الخاصة للأشخاص وسرية اتصالاتهم وحرمة منازلهم من أجلها[56].

والجدير بالذكر، أن مسألة وقوع الجريمة من عدمها تثير مشكلة كبيرة عندما يتعلق الأمر بتفتيش جرائم الحاسب الآلي وشبكات المعلومات، خاصة في الدول التي لم تسّن حتى الآن قوانين تصنف فيها هذه الجرائم، وتحدد وصفها القانوني، عناصر أو أركان كل جريمة وكذا العقوبات المقررة لها، مع العلم أن إجراء التفتيش لا يكون مشروعا إلا إذا بني على سبب جدي يتمثل في الوقوع الفعلي للجريمة، وأن وقوع هذه الأخيرة من عدمه يتوقف أساسا

---

[54]- نشير إلى أن المشرع الجزائري خرج عن هذه القاعدة من خلال المادة (05) من القانون (04/09) التي تجيز إمكانية اللجوء إلى تفتيش النظم المعلوماتية للوقاية من جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة (04) من القانون نفسه.

[55]–وهذا تصديقا للمادة(66) من قانون الإجراءات الجزائية التي تنص على أنّ " **التحقيق الابتدائي وجوبي في مواد الجنايات. أما في مواد الجنح فيكون اختياريا ما لم يكن ثمة نصوص خاصة...**"

[56]– **نبيلة هبة هروال**، مرجع سابق، ص232. و**عادل عبد الله خميس المعمري**، مرجع سابق، 263.

على مدى تحقق أركانها مجتمعة[57]. فعلى سبيل المثال، ما زالت العديد من الجرائم المتعلقة بنظم المعالجة الآلية وشبكة الانترنت خارج نطاق التجريم في التشريع الجزائري مثل جرائم الاعتداء على المواقع الالكترونية و حجبها، وتدميرها، وجرائم الاستغلال الجنسي للأطفال وغيرها من الجرائم الإباحية، وتبعا لذلك فان اتخاذ أي إجراء من إجراءات التحقيق إزاء هذه الجرائم بما في ذلك التفتيش، قد يكون مصيره البطلان طالما لم يرتكز على سبب مقبول قانونا، ناهيك عمّا تتطلبه الإجراءات التقنية في حالة النص على تلك الجرائم من نصوص تتناسب مع حداثتها[58].

2- اتهام شخص أو أكثر بمساهمته في ارتكاب الجريمة الإلكترونية

يشترط لقيام سبب التفتيش إلى جانب وقوع جريمة الكترونية تحمل وصف جناية أو جنحة، أن تتوفر في حق الشخص المراد تفتيشه أو تفتيش حاسبه أو مسكنه دلائل كافية توحي إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة بوصفه فاعلا أصليا أو ثانويا، مما يستوجب اتهامه بها. ومن هنا كان عدم اكتشاف قاضي التحقيق لهوية المتهم في الشكوى ضد مجهول سببا لحفظ ملف القضية وإصداره لأمر بأن لا وجه للمتابعة [59].

وقد أجمع الفقه الجنائي على أن المقصود بالدلائل الكافية بصفة عامة هو " الشبهات المستمدة من الواقع والقرائن التي تنبئ عن اقتراف الشخص جريمة من الجرائم "[60]. أما في

---

[57]- **هلال عبد الله احمد**، تفتيش نظم الحاسب الآلي وضمانات المتهم ألمعلوماتي، دار النهضة العربية، القاهرة، 1997، ص121.

[58]- **رشاد خالد عمر**، المشاكل القانونية و الفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، 2013، ص69.

[59]- هذا ما نصت عليه المادة (163) من قانون الإجراءات الجزائية الجزائري " **إذا رأى قاضي التحقيق ...انه لا توجد دلائل كافية ضد المتهم أو كان مقترف الجريمة مايزال مجهولا، اصدر أمرا بأن لا وجه لمتابعة المتهم**".

[60]- **بوكر رشيدة** ، مرجع سابق، ص 407.

الجرائم الالكترونية فيقصد بها "مجموعة من المظاهر أو الإمارات المعينة القائمة على العقل والمنطق والخبرة الفنية والحرفية للمحقق والتي ترجح نسبة الجريمة الالكترونية إلى شخص معين باعتباره فاعلا أصليا أو شريكا".

وعلى هذا الأساس فسبب التفتيش في البيئة الالكترونية لا يتوقف على وقوع جريمة من الجـرائم الالكترونـية فقط، إنـما لابد أن يكون ذلـك الوقـوع مقترنا بنسبتها إلـى شخـص أو أشخاص معينين إما بصفتهم فاعلين أصليين أو شركاء[61].

3- توافر إمارات قوية توحي إلى وجود أدلة مادية تفيد في كشف الجريمة

لا يكفي وقوع جريمة من نوع جناية أو جنحة منصوص عليها في القانون، وتوجيه الاتهام إلى شخص أو أشخاص معينين بمساهمتهم في ارتكابها لقيام سبب التفتيش في الجرائم الالكترونية، إنما ينبغي أن تتوافر كذلك لدى المحقق أدلة قوية و قرائن كافية على وجود لدى شخص المتهم أو في الموقع المراد تفتيشه أجهزة أو أدوات استعملت في الجريمة أو أشياء متحصل منها، أو أية معلومات أو بيانات أو مستندات إلكترونية تفيد في استجلاء الحقيقة [62].

---

[61]- وهو ما يستشف من المادة 44 من قانون الإجراءات الجزائي الجزائري بنصها على أنه " **لا يجوز لضباط الشرطة القضائية الانتقال الى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا...**"

[62]- هذا ما أقرته محكمة النقض المصرية في حكمها الصادر في الطعن رقم 25380-جلسة 2002/01/20 عندما قضت بان "**كل ما يشترط لصحة التفتيش الذي تجريه النيابة او تأذن بإجرائه في مسكن المتهم او ما يتصل بشخصه، هو ان يكون رجل الضبط القضائي قد علم من تحرياته و استدلالاته ان جريمة معينة قد وقعت من شخص معين و يكون هناك من الدلائل الإمارات الكافية و الشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التفتيش لحريته او لحرمة مسكنه في سبيل كشف اتصاله بتلك الجريمة**" نقلا عن: **أحمد بن زايد جوهر الحسن المهندي** " تفتيش الحاسب الآلي و ضمانات المتهم" رسالة لنيل درجة الماجستير، كلية الحقوق، جامعة القاهرة، 2009، ص 165.

ويتم الحصول عادة على هذه القرائن والإمارات من خلال مختلف التحريات الجدية التي تجريها سلطات الضبط في مرحلة الاستدلال، بعدما يتم إخضاعها لتقدير السلطة المختصة بإصدار الإذن بالتفتيش التي تتأكد من مدى توفر هذه القرائن لمصداقية كافية تبرر اللجوء إلى إجراء التفتيش.

وينطبق على هذه الضمانة ما قيل في سابقتها بأنها لا تجدي في مجال الجرائم الالكترونية، بخلاف ما هي عليه في الجرائم التقليدية. لان التوصل إلى قرائن أو إمارات قوية كسبب لقيام التفتيش في جريمة الكترونية ليس بالأمر الهين، نظرا للصعوبات الكثيرة والعقبات الجمّة التي تواجه سلطات التحري والاستدلال في ذلك، كنقص خبرتها في تقنيات التحري في العالم الالكتروني الافتراضي، مقابل ما تتسم به تلك الأدلة من طبيعة معنوية يمكن إخفاؤها، تغيرها وإتلافها بكل سهولة وبسرعة فائقة[63]. وهو ما قد يشكل دافعا كافيا لانتفاء سبب التفتيش الذي يعتبر شرطا جوهريا لصحة إجراء التفتيش.

ب ـ محل التفتيش: يشترط كذلك لصحة و مشروعية التفتيش في الجرائم الالكترونية أن ينصب على محل، ويقصد بالمحل هنا كل المكونات المادية والمعنوية وشبكات الاتصال المتعلقة بالوسائل الالكترونية[64].

وكما أسلفنا الذكر، فالمحل في الجرائم الالكترونية لا يكون قائما بذاته، بل يكون إما مقترنا بمكان معين كمسكن المتهم أوبشخص معين (مالك أو حائز) كما هو الشأن في الحاسب المحمول أو الهاتف النقال، لذلك قبل مباشرة التفتيش يجب مراعاة طبيعة المكان الذي تتواجد فيه الوسائل الالكترونية المراد تفتيشها وكذا الضمانات القانونية المحاطة به، لان حكم تفتيش هذه الوسائل يتوقف غالبا على طبيعة المكان الذي تتواجد فيه.

---

[63]– **رشاد خالد عمر**، مرجع سابق، ص130.

[64]–**علي محمود علي حموده**، مرجع سابق، ص 94 وما يليها.

ويشترط في المحل الذي يقع عليه التفتيش، أن يكون معينا تعيينا نافيا للجهالة[65]، ويكون مما يجوز تفتيشه، فأما الشرط الأول، فهو نتيجة منطقية للمحافظة على حقوق وحرمات وحريات الأفراد، لذا لا يمكن القيام بتفتيش كل الحواسيب المتواجدة في شركة ما أو الحواسيب المحمولة أو الهواتف النقالة الخاصة بكل أفراد العائلة الواحدة[66].

وأما الشرط الثاني، فلأن القانون يستثني من التفتيش بعض الأشخاص و الأماكن مثل أشخاص ومساكن وسيارات أعضاء السلك الدبلوماسي وأعضاء المجالس النيابية[67]، وكذا مكاتب المحامين لتمتعهم بالحصانة[68]، وعليه فأي تفتيش لأجهزة الحواسيب أو الوسائل الالكترونية الأخرى الموجودة بحوزة هذه الفئة من الأشخاص أو في منازلهم أو على متن سياراتهم يعد منافيا للقانون و مآله البطلان.

كذلك الحال بالنسبة للتفتيش عن بعد عبر شبكات الاتصال أو التفتيش الالكتروني الذي لا يستلزم الاعتداء المادي لحرمة المكان أو الشخص المراد تفتيشه، فهو يخضع لقواعد الحصانة مثله مثل التفتيش المادي، لان الاعتداء المعنوي على الحياة الخاصة يرتب عادة الآثار نفسها التي يرتبها الاعتداء المادي أو اخطر منها، وذلك نظرا للكم الهائل من المعلومات والبيانات التي تحويها الوسائل الالكترونية الشخصية، والتي يسهل الولوج إليها

---

[65]– وقد أكدت محكمة النقض المصرية هذا الشرط في حكمها الصادر في 22-5-1972 تحت رقم177 ، و جاء فيه انه "**يجب ان يكون محل التفتيش محددا تحديدا نافيا للجهالة، فيجب ان يتضمن الإذن بالتفتيش تحديد المسكن الذي يأمر بتفتيشه و كذلك المتهم الذي يقيم في هذا المسكن**" مشار إليه في : **سامي جلال فقي حسين** " التفتيش في الجرائم المعلوماتية "دار الكتب القانونية، القاهرة ، 2011، ص 130

[66]– المرجع نفسه، ص129.

[67]–راجع في هذا الشأن المادتين (29 و 30)من اتفاقية فيينا للعلاقات الدبلوماسية لسنة 1961 وكذا المادة (126) من القانون رقم (16-01) مؤرخ في 6 مارس 2016، يتضمن التعديل الدستوري الجزائري، ج.ر عدد 14، صادر في 7 مارس 2016 .

[68]–راجع المادة (45) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

والإفشاء عنها والاعتداء على سريتها.

وتجدر الإشارة في هذا الشأن، إلى أن المشرع الجزائري استحدث نصوصا قانونية سمح من خلالها لسلطات التحقيق تفتيش الأنظمة المعلوماتية، أو جزء منها، والمعطيات المخزنة بتلك الأنظمة، وجعلها محلا للتفتيش الالكتروني، كما وسّع نطاق هذا المحل، بحيث لم يعد قاصرا على تفتيش الأجهزة الالكترونية تبعا لتفتيش المكان والأشخاص، بل جعله يمتدّ ليشمل التفتيش عن بعد داخل النطاق الإقليمي للدولة إلى نهاية طرفية أخرى التي يمكن الدخول إليها من المنظومة الأولى وذلك كلما استدعت ضرورة التحقيق إلى ذلك[69].

ج ـ السلطة المختصة بالتفتيش لكي يكون التفتيش في الجرائم الالكترونية أو غيرها من الجرائم صحيحا و منتجا لأثاره، لابد أن يتم من طرف سلطات التحقيق الأصلية[70] بإختلاف تشريعات الدول[71]، مـع مراعـاة الاختصـــاص المحلي الذي يتحدد عادة إما بمكان وقوع الجريمة، وإما بمكان إقامة المتهم، أو مكان القبض عليه[72].

---

[69]– راجع المادة(05) من القانون رقم(09–04) المؤرخ في 05–08–2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

[70]– يقصد بسلطات التحقيق الأصلية، السلطات القضائية التي تملك صلاحية مباشرة التحقيق بنفسها(أي بقوة القانون) ولا تحتاج إلى تفويض من غيرها.

[71]– ففي معظم الدول الأوروبية كفرنسا، ايطاليا مثلا السلطة المختصة أصلا بالتحقيق هو قاضي التحقيق، أما في مصر فهو النيابة العامة و قاضى التحقيق معا، في حين أن المملكة المتحدة تؤول هذا الاختصاص أصلا الى رجال الضبطية القضائية، أما في الجزائر فيؤول حسب المواد (1/38–2 و 1/67) من ق إ ج إلى قاضي التحقيق بناءا على طلب من وكيل الجمهورية أو المدعى المدني . راجع : **أحمد بن زايد جوهر الحسن المهدي**، مرجع سابق، ص172.

[72]– تنص المادة (40) من ق إ ج ج " **يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على احد هؤلاء الأشخاص حتى ولو كان سبب القبض قد حصل لسبب أخر** ...".

إلا أنه استثناء، يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية و ذلك وفقا للشروط و الإجراءات المنصوص عليها في القانون[73]، وفي هذه الحالة يشترط لصحة إجراء التفتيش الذي يقوم به رجال الضبطية أن يكون بناء على إذن بالتفتيش صحيح[74]، صادرا من هيئة مختصة. وفي غياب هذا الإذن، أو عدم صحته يصبح عدم مشروعية التفتيش أمرا مؤكدا[75].

وفي نطاق تفتيش الأجهزة الالكترونية يثار التساؤل حول ما إذا كان يجب تحديد محل التفتيش في الإذن بالتفتيش تحديدا دقيقا، كتحديد نوع الجهاز الالكتروني أو إحدى مكوناته (مثل الذاكرة، الوحدة المركزية، القرص الصلب ...) أو ملحقاته (كالطباعة، جهاز المسح الضوئيscanner...) الذي سوف يرد عليه التفتيش دون غيره، أم انه يكفي الحصول على الإذن بتفتيش المكان الذي تتواجد فيه تلك الأجهزة حتى يشملها جميعها؟ أو بعبارة أخرى هل يجوز لضابط الشرطة القضائية بمقتضي الإذن بتفتيش مسكن المتهم الولوج إلى الأجهزة الالكترونية التي تصادفهم فيه والتغلغل في منظومتها المعلوماتية للبحث عن أدلة إثبات يمكن أن تكون محل ضبط ؟

والجواب عن هذا السؤال هو أن غالبية التشريعات المقارنة استقرت على انه يكفي الحصول على الإذن بتفتيش مسكن المتهم حتى يكون لضباط السلطة القضائية الحق في تفتيش كل الأجهزة الالكترونية و مختلف ملحقاتها المتواجدة في هذا المسكن وكل الملفات

---

[73]– راجع المادة (6/68) و المواد من (138 إلى 142) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

[74]– كي يكون الإذن بالتفتيش صحيحا يجب آن يتوفر على الشروط التالية: أن يكون الإذن بالتفتيش مكتوبا و موقعا من طرف السلطة المختصة نوعيا و إقليما، ومسببا، ويحدد نوع الجريمة ومحل التفتيش، تاريخ القيام بالتفتيش و مدته ونطاقه. راجع: **خالد ممدوح إبراهيم**، مرجع سابق، ص.ص 220–224.

[75]–راجع نص المادة (44) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

والبيانات التي تحتويها تلك الأجهزة[76]، وحجتهم في ذلك هي، أن الأجهزة الالكترونية الرقمية بمختلف أنواعها تمثل مجالا حيويا ضخما لتخزين مئات الآلاف من الملفات ومليارات من المعلومات والبيانات، لذلك فلا يعقل مع هذه القدرة التخزينية الهائلة واللامتناهية تصور إصدار إذن بالتفتيش حسب عدد الملفات التي تحتويها.

أما عن موقف المشرع الجزائري إزاء هذه المسألة فهو غير واضح وغير حاسم، لأن بالعودة إلى القواعد الخاصة بالتفتيش المذكورة في قانون الإجراءات الجزائية فهي تتعلق بالتفتيش التقليدي الذي ينصب عادة على الفضاءات والمكونات المادية وما في حكمها كالمساكن وملحقاته[77]، أما في القواعد المتعلقة بالتفتيش الالكتروني الواردة في القانون رقم (04/09)، فالمشرع لم يحسم أمره. وإنما اكتفى فقط بالإشارة إلى ضرورة قيام جهات التحقيق بإعلام السلطة القضائية المختصة مسبقا قبل تمديد التفتيش إلى منظومة معلوماتية أخرى مرتبطة بالجهاز المأذون بتفتيشه[78].

ومن خلال هذا السكوت و طبقا لمبدأ حرمة الخصوصية التي يحميها المشرع، نفهم بأن المشرع الجزائري يميل إلى عدم جواز الولوج إلى النظام المعلوماتي وما يمكن أن يحتويه من معلومات و بيانات سرية وخصوصية الأشخاص، لتفتيشه دون إذن خاص من السلطة القضائية المؤهلة، ومؤدى ذلك أن ضابط الشرطة القضائية يحتاج في الغالب لتفتيش

---

[76]– على خلاف هذه التشريعات اتجه القضاء الأمريكي إلى أن كل ملف واحد في الحاسوب الآلي يعتبر حاوية مغلقة ويتطلب إذنا خاصا بالتفتيش، وأساسه في ذلك هو أن الحاسب يمكن أن يحتوي على ملفات تتعلق بالحياة الخاصة لصاحبه ولا علاقة لها بالجريمة ، بالتالي فتح رجال الضبطية القضائية لهذه الملفات يعد تعد على الخصوصية.انظر مجموعة أحكام القضاء الأمريكي الصادرة في هذا الشأن في: **عمر بن يونس**، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، د.د.ن ، 2008، ص.ص 60–61.

[77]– راجع المادة (44) وما يليها من القانون الإجراءات الجزائية الجزائري، مرجع سابق.

[78]– انظر نص المادة (05) من القانون رقم (09–04)، مرجع سابق.

منظومة معلوماتية إلى إذنين بالتفتيش، الأول يخص المسكن الذي يتواجد فيه الجهاز الالكتروني، والثاني يتعلق بتفتيش مكونات الجهاز أو المنظومة المعلوماتية في حد ذاتها. أو على الأقل يحتاج إلى إذن واحد يسمح بتفتيش الجهاز الالكتروني الخاص بالمتهم ومسكنه معا.

وعلى ضوء هذا الإبهام، يتعين على المشرع الجزائي الجزائري التدخل و سنّ نصوص قانونية واضحة تفصل في هذه المسالة، والحل في رأينا هو الأخذ بما ذهبت إليه معظم تشريعات الدول المتقدمة، والمتمثل في جواز تفتيش مسكن المتهم وكل الأجهزة الإلكترونية بمكوناتها وملحقاتها وملفاتها المتواجدة فيه، مع إمكانية تمديد التفتيش عن بعد على جناح السرعة إلى أية منظومة معلوماتية أخرى مرتبطة بها، كل ذلك بموجب إذن بتفتيش واحد.

ثانيا-الضمانات الشكلية للتفتيش الإلكتروني

إن الغرض من إحاطة التفتيش بضمانات شكلية إلى جانب الضمانات الموضوعية هو ليس تحقيق مصلحة القضاء في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة، وضمان مشروعية هذه الأخيرة فقط، إنما تعتبر كذلك بمثابة سياج أمني لحماية الحقوق والحريات العامة الفردية .

ومع هذا فتطبيق تلك الضمانات في مجال التفتيش الالكتروني من شأنها أن تتحول إلى عقبات تحول دون تحقيق الهدف من إجراء التفتيش بدلا من كونها ضمانات في مجال التفتيش التقليدي. وهو ما سوف نبرزه عند دراسة هذه الضمانات التي تتلخص فيما يلي:

1-احترام الميقات الزمني لإجراء التفتيش

إن فرض قيود زمنية لإجراء التفتيش يعدّ ضمانة إجرائية مهمة جدا لحماية الحريات والحقوق العامة للأفراد من أي اعتداء. ومع ذلك اختلفت التشريعات الإجرائية للدول في تنظيمها للوقت الذي يسمح فيه القيام بالتفتيش، فمنها من حددته بشكل عام على أن يتم

التفتيش في النهار فقط، مثل قانون الإجراءات الجنائية القطري[79]، ومنها من حددت وقت التفتيش بشيء من التفصيل من خلال تحديد الساعة التي يمكن البدء فيها بالتفتيش والساعة التي يجب التوقف عندها من ساعات النهار[80]، ومنها كذلك من لم يقيّد القيام بهذا الإجراء بوقت معين وترك الأمر لتقدير القائم بالتفتيش لاختيار الوقت الملائم من الليل أو النهار لتنفيذه ضمن المدة المحددة بالإذن مثل قانون الإجراءات الجنائية المصري، القانون العراقي و القانون الأردني.

وعلى خلاف ذلك كله، نجد أن المشرع الجزائري وضع قيودا زمنية على تفتيش المنازل وما في حكمها، ولم يسمح به بمقتضى المادة (47) من قانون الإجراءات الجزائية إلا في الوقت المحصور بين الساعة الخامسة صباحا و الثامنة مساء[81]، وفي الوقت نفسه أقرّ حالات استثنائية أجاز فيها الخروج عن هذا الميقات ليصح إجراء التفتيش في أية ساعة من ساعات الليل و النهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها في المواد من (342) إلى (348) من قانون العقوبات المرتكبة في أماكن معينة، وفي حالة الرضى الصريح لصاحب المسكن[82].

---

[79]– نصت المادة (53) منه على انه "**لا يجوز أن يجري تفتيش المساكن إلا نهارا...**" نقلا عن **سامي جلال فقي حسين**، مرجع سابق، ص165

[80]– حدد قانون الإجراءات الجنائي الاتحادي الأمريكي في المادة (228) وقت التفتيش بالفترة المحصورة بين الساعة السادسة صباحا و العاشرة مساءا، و حدده قانوني الإجراءات الجنائية الفرنسي في المادة (59) بالفترة الممتدة بين السادسة صباحا و التاسعة مساءا، في حين لا يسمح القانون الكرواتي بالتفتيش إلا في الفترة المحصورة بين السابعة صباحا والتاسعة مساءا. نقلا عن: **هلالي عبد الله احمد**، مرجع سابق، ص 175.

[81]– تنص المادة (47) ق اج ج على أنه "**لا يجوز البدء في تفتيش المساكن او معاينتها قبل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساءا...**"

[82]–أنظر المادتين(1/47و2) و (82) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

وقد اشتمل هذا الاستثناء التفتيش في الجرائم الالكترونية، بحيث استغنى المشرع الجزائري نهائيا عن شرط الميقات الزمني وسمح لرجال الضبطية القضائية بإجراء التفتيش في مثل هذه الجرائم في كل ساعة من ساعات الليل و النهار كما جاء في الفقرة الثالثة من نص المادة (47) ق إ ج " ...عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية أو **الجرائم الماسة بالمعالجة الآلية للمعطيات** و **...فانه يجوز إجراء التفتيش...في كل محل سكني او غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية**".

أعتقد أنّ استغناء المشرع الجزائري عن هذا الشرط بخصوص التفتيش في الجرائم الالكترونية راجع من جهة، إلى فطنته وإدراكه للطبيعة المميزة لهذه الجرائم من حيث إمكانية ارتكابها في أي وقت، وأدلة الإثبات فيها غير مرئية وسهلة المحو والإتلاف، بالتالي فتأخير التفتيش إلى الموعد القانوني وفق المبدأ العام قد يكون سببا في ضياع الأدلة ومن ثم عرقلة سير التحقيق. ومن جهة أخرى، إلى تراجع أهمية هذا الشرط أو الضمانة مع ظهور تقنية " **التفتيش عن بعد**"[83] والذي يمكن إجراؤه في أي وقت ومن أي مكان في العالم، مع العلم أن تحديد الوقت قد يختلف من دولة إلى أخرى، فالوقت الذي يكون نهارا في دولة معينة مثل كندا قد يكون ليلا في دولة أخرى مثل الجزائر.

2ـ إجراء التفتيش بحضور المتهم أو من ينوب عنه

حرصا على تضييق نطاق الاعتداء على حرمة الحياة الخاصة للأفراد وحرمة مساكنهم المحفوظة قانونا، تسهر معظم التشريعات الإجرائية على عدم جواز إجراء التفتيش إلا بحضور المتهم أو من يقوم مقامه معتبرين ذلك من القواعد الأساسية التي يترتب عن مخالفتها البطلان.

---

[83] - **PADOVA Yann** , un aperçu de lutte contre la cybercriminalité en France , R.S.C.P, N04, Dalloz, 2002, P 770.

وغني عن البيان أن الشخص الذي يستوجب القانون حضوره في الأصل هو المتهم، وهذا الشرط يكون قائما حتما في تفتيش الأشخاص على اعتبار التفتيش يقع عليه[84]، وفي هذا الإطار لم تشترط التشريعات الإجرائية حضور الشهود عند تفتيشه. أما عندما يتعلق الأمر بتفتيش المساكن وما في حكمها، فقد تباين موقف التشريعات الإجرائية بين من يشترط لصحة التفتيش حضور إما المتهم بنفسه أو من يمثله أو شاهدين من غير المعنيين بالتحقيق[85]، وبين من يستوجب إلى جانب حضور المتهم حضور شاهدي عدل[86]، كما هو الحال في قانون الإجراءات الجنائية اليمني الذي نص في المادة (134) على أن " يحصل التفتيش بحضور المتهم أو من ينوبه وبحضور شاهدين من أقاربه أو جيرانه "[87].

وعلى العكس من ذلك، فالمشرع الجزائري يقضي لإجراء التفتيش بحضور المشتبه به أو من يمثله ولم يتطلب حضور الشهود إلا في حالة تعذر حضور هؤلاء، وهو مقتضى المادة(1/45 ق إ ج) بأنه " **إذا وقع التفتيش في مسكن شخص يشتبه أنه ساهم في ارتكاب جناية فيجب أن يحصل التفتيش بحضوره، وإذا تعذر عليه الحضور وقت إجراء التفتيش، فان ضابط الشرطة القضائية ملزم بان يكلّفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته**"[88].

---

[84]– **بوكر رشيدة**، مرجع سابق، ص 414.

[85]– وهو الموقف الذي تبناه كل من المشرع الفرنسي في المادة (57) من قانون الإجراءات الجنائية، و المشرع المصري في المادة (51) قانون الإجراءات الجنائية ، مشار إليه في: **فايز محمد راجح غلاب**، مرجع سابق، ص 335.

[86]– ومن التشريعات التي أخذت بهذا الموقف نذكر قانون الإجراءات الجنائي الاتحادي الأمريكي، قانون الإجراءات الجنائية الايطالي في المادة (10/250) منه، انظر: **سامي جلال فقي حسين**، مرجع سابق،ص.ص 168–169.

[87]– المادة(134) من قانون الإجراءات الجزائية اليمني رقم 13 لسنة 1994 .

[88]–انظر المادة(45) و المادة (83) من القانون الإجراءات الجزائية الجزائري، مرجع سابق.

أما فيما يخص التفتيش في الجرائم الالكترونية، فالمشرع و إقرارا منه بخصوصية جرائم الاعتداء على نظم المعالجة الآلية للمعطيات وما يتطلبه الأمر من بسط نوع من السرية أثناء جمع الدليل التقني فيها، عاد بموجب الفقرة الأخيرة من المادة نفسها[89]، واستثنى هذه الجرائم من تطبيق أحكام المادة السابقة، وأصبح بإمكان الضبطية القضائية إجراء التفتيش في الجرائم المعالجة الآلية دون التقيد بشرط حضور المتهم أومن ينوب عنه أو حتى الشهود.

وفي رأينا، ما فعله المشرع الجزائري باستبعاد تطبيق أحكام المادة (45 ق ا ج) على الجرائم الالكترونية هو الصواب، وذلك نظرا للطبيعة التقنية المحضة التي تتميز بها هذه الجرائم و طبيعة الدليل الذي تتطلبه لإثباتها، و ما يقتضيه من السرعة في استخلاصه قبل فقدانه والذي يتطلب أحيانا عدم إعلام المتهم بعملية التفتيش.

3ـ تحرير محضر التفتيش

إضافة إلى الضمانات المتعلقة بالميقات الزمني للتفتيش والأشخاص المطلوب حضورهم، يشترط كذلك أن يحرّر محضر بالتفتيش تدون فيه كل الخطوات والإجراءات المتخذة أثناء عملية التفتيش، وما أسفر عنها من أدلة لكي يكون حجة على الجميع.

ولا يستوجب القانون شكلا أو شروطا خاصة في محضر التفتيش، بل يكفي أن يتوفر فيه ما تستوجبه القواعد العامة في المحاضر عموما، كالكتابة باللغة الرسمية، تاريخ تحريره، توقيع محرره، ويتضمن كافة إجراءات التفتيش[90].

---

[89]–تنص الفقرة الأخيرة من المادة (45 من ق إ ج ج) على أنه " **لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...باستثناء الأحكام المتعلقة بالحفاظ على السر المهني**".

[90]– **فايز محمد راجح غلاب**، مرجع سابق، ص 338.

ومن الشروط الجوهرية التي ينبغي مراعاتها في محضر التفتيش، وجوب استعانة المحقق بكاتب يتم اصطحابه لتحرير المحضر و تدوين ما تم من إجراءات و التأشير عليه تحت طائلة البطلان، وهو ما نصت عليه المادة (2/68) قانون الإجراءات الجزائية الجزائري " وتحرر نسخة من هذه الإجراءات وجميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل"، وأكدت عليه المادة (79) من القانون نفسه بنصها على " **يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بمـا يقـــوم به من إجراءات**"[91].

ولا يختلف محضر التفتيش في مجال الجرائم الالكترونية عن غيره في الجرائم التقليدية سوى انه بالإضافة إلى الشكليات السابقة لابد من إحاطة القائم بالتفتيش في الجرائم الالكتـرونية بتقنية المعلوماتية الرقمية، أو استعانته بـأهل الخبر الفنية والاختصاص في هذا المجال ليساعده في صياغة و تحرير محضر يغطي كل الجوانب الفنية للتفتيش.

وأشير إلى انه بالإضافة إلى شرط تحرير محضر التفتيش، حرصت معظم الدول على تضمين تشريعاتها الإجرائية نصوص تمنع فيها الاطلاع أثناء التفتيش على الأشياء والأوراق المختومة التي تمس الأسرار الشخصية للعائلة[92]، وتفرض على القائم بالتفتيش اتخاذ الاحتياطات الضرورية لتفادي انكشاف مثل هذه الأسرار.

---

[91]– أنظر الفقرة 2 من المادة (68) و المادة (79 من ق.ا.ج.ج)، مرجع سابق.

[92]– من بين التشريعات التي نصت على هذه الضمانة، نذكر نص الماد (52 من ق إ ج) المصري، و نص المادة (140 ق إ ج) اليمني، والمادة(1/35) من قانون أصول المحاكمات الجزائية السوري.

وقد نص القانون الجزائري على هذه الضمانة في المادة (84 من ق إ ج) على الشكل التالي: " إذا اقتضى الأمر أثناء إجراء تحقيق و جوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع عليها قبل ضبطها مع مراعاة ما تقتضيه ضرورات التحقيق و ما توجبه المادة (3/83 ق إ ج). ويجب على الفور إحصاء الأشياء و الوثائق المضبوطة ووضعها في أحراز مختومة. ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا..."[93].

وأعتقد أن هذا القيد المتعلق بعدم جواز الاطلاع على الأشياء والأوراق المختومة أثناء التفتيش يمكن تطبيقه على محتوى أنظمة المعالجة الآلية للبيانات المشفرة والمحمية فنيا ضد الاطلاع غير المرخص، لان العلة من تقرير هذا القيد بالنسبة للأوراق المختومة هي نفسها بالنسبة لبيانات أنظمة المعالجة الآلية المشفرة، ألا وهي المحافظة على الأسرار الخاصة بالشخص المراد تفتيشه[94]، فكـما يضفي الختم والتغليف والتحريز على تلك الأوراق مزيدا من السرية و الحماية فكذلك التشفير يضفي السرية على البيانات و برامج المعالجة آليا.

المطلب الثاني

ضبط الأدلة في الجرائم الإلكترونية

يعتبر الضبط من إجراءات جمع الأدلة، وهو النتيجة الطبيعية التي ينتهي إليها التفتيش والأثر المباشر الذي يسفر عنه، ويقصد به وضع اليدّ على الأشياء المتعلقة بجريمة وقعت والتي تفيد في كشف الحقيقة عنها و عن مرتكبيها، و وضعها في أحراز مختومة ولتقدم إلـى

---

[93]– أنظر المادتين (3/83 و 84) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

[94]– **محمد فريد رستم**، أصول التحقيق في جرائم الحاسوب، مرجع سابق، ص 428.

الجهة القضائية المختصة كدليل إثبات[95].

وتحصيل الأدلة في الجرائم الالكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته، الأقراص الصلبة، الأقراص والأشرطة الممغنطة، الطباعة، البرامج اللينة والمراشد، البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الانترنت مثل المودم، ففي هذه الحالة فلا يطرح ضبط هذه المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها لإجراءات الضبط والتحريز التقليدية[96]. وقد يرتبط الدليل الالكتروني بالمكونات المعنوية للحاسب، كمختلف البرامج والبيانات المعالجة آليا والمراسلات والاتصالات الالكترونية التي يجري تبادلها عبر شبكة الانترنت والبريد الالكتروني، وهنا تثير الطبيعة المجردة لهذه المكونات جدلا فقهيا واختلافا تشريعيا كبيرا حول مدى إمكانية ضبطها وفقا لقواعد الضبط المألوفة، مع العلم أن الضبط بمفهوم هذه الأخيرة لا يرد إلا على الأشياء المادية[97].

ولقد حسمت الاتفاقية الأوروبية لجرائم المعلوماتية لعام 2001 هذه المسألة، بإقرارها صراحة صلاحية المكونات المنطقية والوسائل الالكترونية لأن تكون محلا للضبط وذلك من خلال الفقرة(03) من المادة (19) التي نصت على "... 3- **يجب على كل طرف تبني الإجراءات التشريعية التي يراها ضرورية من أجل تخويل هيئاتها المختصة سلطة ضبط أو**

---

[95]- **خالد عياد الحلبي**، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر و التوزيع، عمان، 2011، ص 170.

[96]- راجع في ذلك المواد (45 و 46 و 84) من القانون الإجراءات الجزائية الجزائري.

[97]- أنقسم الفقه في هذه المسألة بين من يعترف بالطبيعة المادية للأدلة الالكترونية و بالتالي إمكانية إخضاعها إلى إجراءات الضبط التقليدية، و بين من يرى هذه الأدلة ذات طبيعة لا مادية ولها خصوصيات استثنائية تستلزم تقنيات الضبط و تحليل جديدة ومتطورة تختلف عن التقنيات المألوفة. للمزيد من التفاصيل أنظر: **عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص.ص 218 وما بعدها.

الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين (01) و (02)... ".

فبالرجوع إلى هذه الفقرة، نجدها تخول سلطات البحث والتحري طريقتين لضبط البيانات المعلوماتية والأدلة الرقمية التي كانت موضوع التفتيش أو الولوج بطريقة مشابهة عملا بالفقرتين (1 و 2) من المادة (19)، تتحقق الأولى عن طريق نسخ وتحميل البيانات والمعطيات محل البحث على دعامة تخزين مادية(كالأقراص الممغنطة، بطاقات الذاكرة، فلاش ديسك)، وتكون هذه الأخيرة قابلة للضبط والوضع في أحراز مختومة حسب ما هو مقرر في قواعد تحريز الدليل التقليدية المنصوص عليها في قوانين الإجراءات الجزائية، وهي الطريقة المقصودة في المادة أعلاه بمصطلح " **الضبط saisir**"[98]. أما الطريقة الثانية فتتضمن تدابير جديدة مستحدثة خصيصا لضبط الأدلة الجنائية الرقمية، وهي المعبر عنها في هذه المادة بمصطلح " **الحصول بطريقة مشابهة** على البيانات المعلوماتية "، والتي تكون باستعمال تقنيات وتدابير الحماية الفنية كتقنيات التشفير و الترميز، برامج منع الكتابة واستخدام خوارزميات " تجزئة" للملفات المشفرة من اجل منع الأشخاص المرخص لهم باستخدام المنظومة المعلوماتية والوصول إلى المعطيات والبيانات الأصلية التي تحتويها هذه المنظومة أو القيام بنسخها، ويكون ذلك في حالة ما إذا استحال لأسباب تقنية ضبط هذه المعطيات والبيانات وفق الطريق الأول[99]. أما إذا كانت هذه المعطيات والبيانات تتضمن خطرا على النظام العام و الآداب العامة كتحريض الأطفال على الشذوذ الجنسي أو التحريض على التمييز العنصري أو على الإرهاب، أو أنها تحتوي على برامج وقنابل

---

[98]– **هلال عبد أللاه أحمد**، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، دار النهضة العربية، القاهرة، 2011، ص 251.

[99]– أنظر: **تقرير لجنة منع الجريمة والعدالة الجناية** " دراسة شاملة عن مشكلة الجريمة السيبيرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها " الجمعية العامة لمنظمة الأمم المتحدة، من 25 إلى 28 فيفري 2013، ص 12.

فيروسات، ففي هذه الحالة يمكن لسلطات التحقيق القيام بتعطيل تشغيل هذه المعطيات (blockage des données) أو محوها بعد أخذ نسخة منها[100].

فضلا عن الإجراءات الاستثنائية التي أقرتها الاتفاقية المذكورة لضبط الأدلة الالكترونية الرقمية، فقد نصت كذلك في (المادة 3/19) على مجموعة من التدابير الخاصة لضمان تحريز هذه الأدلة ذات الطبيعة الخاصة وحمايتها فنيا وصيانتها من أي تغيير أو إتلاف أو عبث يمكن أن يصيبها والتي نلخصها فيما يلي:

ـ استخراج نسخ احتياطية من دعائم البيانات و المعطيات المضبوطة و العمل عليها لتفادي المساس بالدليل الأصلي.

ـ عدم طوي القرص لتفادي تلفه و تحطمه و فقدان المعلومات المسجلة فيه.

ـ تأمين البرامج المعلوماتية المضبوطة فنيا قبل تشغيلها.

ـ مراعاة ظروف الحرارة والرطوبة المناسبة في أماكن تخزين الأقراص والأشرطة الممغنطة المحرزة، والتي يجب أن تتراوح درجة الحرارة فيها بين (4–32 درجة) وتكون درجة الرطوبة فيها ما بين (20 – 80%)، مع تفادي تعريضها للأضواء أو لأي سائل من السوائل، مع العلم أنه في مثل هذه الظروف يمكن أن تصل مدة صلاحية تخزين هذه الأقراص إلى ثلاث سنوات دون أن يصيبها تلف أو تعديل أو تحول[101].

ـ منع الأشخاص غير المرخص لهم من الوصول إلى المعطيات والبيانات التي تم ضبطها داخل دعامة مادية للتخزين ، من خلال إحاطتها بتدابير الحماية الفنية كالترميز والتشفير او

---

[100] – **ROGGEN François et DE VALKENEEK Christian**, Actualité de droit pénal, bruyant, Bruxelles , 2005, p 128 .

[101]– **حسام محمد نبيل الشنراقي**، الجرائم المعلوماتية–دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، القاهرة، 2013، ص 525.

بأية وسيلة الكترونية أخرى تمنع الدخول إليها، و صيانتها ببرامج منع التحريف و التغيير في البيانات مثل برامج منع الكتابة[102].

وفي هذا الصدد، أضافت الهيئة الدولية لدليل الحاسب الآلي (Organisation on international computer évidence) ضوابط أخرى للتحريز الجيد والمحافظة على الدليل الرقمي، منها مراعاة عدم تسبب إجراءات التحريز في تغيير طبيعة الدليل الرقمي المضبوط، و توثيق كل المراحل المتعلقة بتحريز هاته الأدلة الرقمية و الدخول إليها و نقلها توثيقا كاملا مع المحافظة عليها وتوفيرها للمراجعة[103].

إلى جانب الإجراءات الجديدة التي تبنتها المادة (19) سالفة الذكر بخصوص ضبط الأدلة الجنائية في الجرائم الإلكترونية من خلال الفقرات (1، 2، 3)، تضمنت كذلك النص على بعض الإجراءات المسهلة والمساعدة لعملية الضبط من خلال الفقرة (4)، و لم تقتصر على وضع تلك الإجراءات فقط، بل أحاطتها بضمانات كافية تضمنتها الفقرة (5) أيضا[104].

فأما عن التدابير التي تضمنتها الفقرة (4) من المادة(19)، فتتمثل في منح السلطات المخولة بإجراء التفتيش والضبط صلاحيات الاستعانة بأي شخص لديه خبرة ومعرفة فنية في تشغيل المنظومة المعلوماتية محل البحث و الإجراءات المطبقة من أجل حماية البيانات

---

[102]– انظر الفقرة الثالثة من المادة (19) من الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001، مرجع سابق.

[103] -**FIRAL-SCHUHL Christiane**, cyber droit- le droit a l'épreuve de l'internet , 6ém édition Dalloz , Paris, 2011-2012, P 998.

[104]-تنص الفقرتين (4) و (5) من الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001 على ما يلي:

4- chaque partie adopte des mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes a ordonner a toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatique qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visée par les paragraphes 1 et 2 .

5- les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15

والمعطيات التي تتضمنها هذه المنظومة، وإلزامه بالتعاون معها بتقديم المساعدة اللازمة والضرورية لتسهيل عملية تفتيش وضبط هذه البيانات والمعطيات، وجعلهما أكثر فعالية واقل تكلفة[105]. بشرط أن تقتصر هذه المساعدة على تقديم المعلومات الضرورية فحسب دون الإخلال بحرمة الحياة الخاصة للإفراد ولا تتعارض مع قواعد السر المهني.

وأما الفقرة (5) من المادة نفسها، فقد ألزمت سلطات التحقيق أثناء قيامها بعملية التفتيش والضبط أو أي إجراء آخر مما نصت عليه الاتفاقية، مراعاة الضمانات المنصوص عليها في المادتين(14 و 15) من الاتفاقية والمتمثلة بشكل عام في احترام حقوق الإنسان والحريات الفردية، مراعاة خصوصية الأشخاص وحرمة أسرارهم والمدة القانونية المقررة لكل إجراء[106].

اقتداء بالاتفاقية الأوروبية حول الجرائم المعلوماتية، تدخلت عدة دول لتعديل قوانينها واستكمال ما بها من فراغ تشريعي في مجال ضبط الأدلة الالكترونية الرقمية وقواعد تحريزها[107]، في مقدمتها فرنسا التي قامت بتعديل قانون الإجراءات الجزائية بموجب قانون الأمن الداخلي رقم (239) لسنة 2003، واستحدثت الفقرة(03) من المادة(57-1) التي نص فيها على أنّ " **المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في هذه المادة ، يتعين نسخها على أية دعامات التخزين المعلوماتية، والتي ينبغي تحريزها في**

---

[105]- **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص 107. و**هلال عبد ألاله احمد**، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، مرجع سابق، ص 252.

[106]- أنظر نص المادتين(14 و 15) من الاتفاقية الأوروبية حول الجرائم المعلوماتية لعام 2001، مرجع سابق.

[107]- من بين هذه الدول التي استحدثت قواعد خاصة بضبط الأدلة الالكترونية، دولة بلجيكا من خلال الفقرات من (1 الى 6) من المادة(39) مكرر و المادة (88) من قانون التحقيق الجنائي البلجيكي، دولة اليونان من خلال المادة(251) من قانون الإجراءات الجنائية، ودولة كندا من خلال المادة(487) من القانون الجنائي الكندي. انظر: **أحمد سعد محمد الحسيني**، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، أطروحة لنيل درجة دكتورة في القانون، كلية الحقوق بجامعة عين الشمس، القاهرة، 2012، ص.ص 19- 20.

أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون"[108]. أما فيما يخص قواعد تحريز المضبوطات المعلوماتية وتأمينها فنيا فقد قام المشرع الفرنسي بتعزيزها من خلال المواد (41 إلى 43) من قانون الثقة في الاقتصاد الرقمي الصادر في 21 جوان 2004 وجعلها تتطابق مع تلك المذكورة في الاتفاقية الأوروبية حول الجرائم المعلوماتية[109].

وعلى غرار المشرع الفرنسي تنبه المشرع الجزائري بدوره لهذا القصور، وتبني في القانون رقم (4/09) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 2009/08/05، إجراءات مستحدثة خاصة بضبط وتحريز المعطيات والبيانات المعلوماتية وغيرها من الأدلة الرقمية بما يتناسب وطبيعتها اللامادية، تحت عنوان "**حجز المعطيات المعلوماتية** "[110] وخصص لها عددا من المواد التي نذكرها على النحو التالي:

ـ نصت المادة(06) على أنه " **عندما تكتشف السلطات التي تباشر التفتيش في منظومة معلوماتية معطيات محزنة مفيدة في الكشف عن الجرائم أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا**

---

[108] - Art (57-1-3) du C P C P dispose que « les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent êtres copiées sur tout supports. Les supports de stockage informatique peuvent etre saisis et placés sous scellés dans les conditions prévues par le présent code »

[109] -voir Arts(41-42-43)de la loi pour la confiance dans l économie numérique in : **QUEMENER Myriam - CHARPENEl Yves** « cybercriminalité droit pénal appliqué » édition Economica, Paris, 2010, p178.

[110]– تجدر الإشارة إلى أن المشرع الجزائري استعمل في هذا القانون (09–04) عبارة " **الحجز saisie**" للتعبير عن عملية الضبط كإجراء من إجراءات التحقيق بدلا من عبارة " **الضبط saisie**" التي اعتاد على استعمالها في قانون الإجراءات الجزائية، وفي اعتقادي هذا الاختيار أمر مقصود، لان عبارة " **الحجز**" لا تتعارض مع الضبط المادي التقليدي من جهة، وهي أكثر تلاؤما و تماشيا مع الطبيعة المنطقية واللامادية للأدلة الالكترونية و الرقمية من جهة أخرى.

للقواعد المقررة في قانون الإجراءات الجزائية..."

ـ أضافت المادة(07) فيما يخص الحجز عن طريق منع الوصول إلى المعطيات بأنه " **إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة(06) أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة**".

ـ أما بخصوص المعطيات المحجوزة ذات المحتوى المجرم فنصت الماد(08) على أنه " **يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك**"[111].

بالإضافة إلى هذه التدابير، وضع المشرع الجزائري على عاتق مقدمي خدمات الانترنت جملة من الالتزامات تساعد سلطات التحقيق على ممارسة مهام التفتيش والضبط على الكيانات المعنوية للحاسب الآلي عندما تستدعي ذلك ضرورة التحقيق[112]. سيتم تناولها بشيء من التفصيل في موضع آخر من هذه الأطروحة .

ويتضح من خلال النصوص السابقة، بأن المشرع الجزائري أدرك خطورة الجرائم الالكترونية وأن الجزائر ليست بمنأى عنها، فقام بتلافي القصور الموجود في قانون الإجراءات الجنائية فيما يخص ضبط الكيانات المنطقية للحاسب أسوة بالاتفاقية الأوروبية

---

[111]– أنظر المواد (6، 7، 8) من القانون (04/09) المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

[112]– أنظر في هذا الشأن، **أحمد مسعود مريم**، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال في ضوء القانون رقم 09–04، مذكرة لنيل شهادة ماجستير في القانون الجنائي، كلية قصدي مرباح بجامعة ورقلة، 2013، ص 103.

وتشريعات الدول المتقدمة، واعتقد أن موقفه هذا ليس اختيارا بل حتمية لا مفرّ منها ما دام أنه قد أجاز تفتيش هذه الكيانات كما – رأينا سابقا – وهو ما يقتضي بحكم المنطق القانوني والعقلي ضرورة إباحة ضبطها لأن الغاية من التفتيش هو ضبط كل ما يفيد في كشف الحقيقة، بالتالي لا يعقل أن ينظم المشرع مرحلة من مراحل التحقيق ويغفل عن الأخرى.

والجدير بالذكر، أنه رغم محاولة استحداث قواعد وإجراءات جديدة تواكب الطبيعة الخاصة للأدلة المستمدة من البيئة الرقمية والالكترونية وتسمح بضبطها وتحريزها بشكل سليم، إلا أن الواقع يثبت وجود صعوبات كثير ما زالت تواجه عملية ضبط هذه الأدلة ولعل أهمها مايلي:

– الحجم الهائل للمعلومات المعالجة الكترونيا التي تحتويها الشبكة المعلوماتية الواجب فحصها من طرف المحقق للوصول إلى استخلاص البيانات التي تصلح كأدلة جنائية وضبطها[113].

– قد يكون محل الأدلة الالكترونية جزء لا يمكن عزله عن المنظومة أو الشبكة المعلوماتية، مما يتعين بالضرورة ضبط النظام أو الشبكة بأكملها لتحصيل الدليل، وهو الأمر الذي يترتب عنه التوقف عن العمل لمشروعات صاحب النظام مدة زمنية قد تطول أو تقصر، ففي هذه الحالة يضطر المحقق إعمال مبدأ التناسب الذي يقضى باقتصار الضبط على الأدلة الضرورية التي تفيد كشف الحقيقة ولها علاقة بالجريمة[114].

---

[113]– **حسام محمد نبيل الشنراقي**، مرجع سابق، ص.ص 671–672.

[114]–وفي هذا الشأن قضت المحكمة الفيدرالية الألمانية بإلغاء محضر الضبط الذي ورد على 220 قرص صلب بالإضافة إلى الوحدة المركزية للحاسب الآلي بحجة مخالفة سلطة التحقيق لمبدأ التناسب. نقلا عن: **فايز محمد راجح غلاب**، مرجع سابق، ص 345.

– كما قد تكون هذه الأدلة في شبكات أو أجهزة تابعة لدولة أجنبية، مما يعيق أجهزة التحقيق الوطنية من الوصول إليها وضبطها دون تعاون ومساعدة أجهزة التحقيق التابعة لتلك الدولة[115].

– كما أن الضبط في البيئة الالكترونية، قد يشكل أحيانا اعتداء على الحقوق والحريات الفردية، ويتصادم مع حرمة الحياة الخاصة والسر المهني خاصة عند عدم مراعاة الضمانات المقررة لذلك، مما قد يعرّضه للبطلان[116].

– أضف إلى ذلك، فمن المشكلات التي يمكن أن تثار بمناسبة ضبط البيانات المخزنة في نظام جهاز الحاسب أو شبكة المعلومات مشكلة مدى قبول القاضي النسخة المأخوذة عن تلك البيانات في حالة صعوبة ضبط النسخة الأصلة كدليل إثبات، لأن القضاء في عدة دول خاصة الدول الأجلوسكسونية يشكك في حجيتها ولا يعتبرها كالنسخة الأصلية لاحتمال التلاعب[117].

– ومن الصعوبات التي تعيق الوصول إلى ضبط الدليل الرقمي كذلك، تلك الأحزمة الأمنية المفروضة من طرف مستخدم النظام للحد من الدخول والاطلاع على البيانات التي يحتويها هذا النظام. وما يزيد الأمر تأزما هو عدم معرفة المحقق الجنائي لكلمات السر أو شفرات المرور أو شفرات ترميز البيانات و ما يقابله من حق المشتبه به في الصمت و عدم

---

[115]– **أحمد بن زايد جوهر الحسن المهندي**، مرجع سابق، ص 224.

[116]- **EL CHAER Nidal** « la criminalité informatique devant la justice pénal » thèse de doctorat en droit, faculté de droit de l'université Poitiers, 2003, p 231.

[117]– أثارت محكمة النقض الفرنسية هذه المسألة في أحد قراراتها و اعتبرت ضبط نسخة من البيانات المسجلة في الحاسب الآلي دون ضبط الجهاز نفسه بما فيه الذاكرة التي تحتوي تلك المعلومات لا يعد من قبيل الضبط الصحيح بمفهوم المادتين (76 و 97) من قانون الإجراءات الجنائية. انظر: **عمر محمد أبو بكر بن يوسف**، الجرائم الناشئة عن استخدام الانترنت – الأحكام الموضوعية و الجوانب الإجرائية، دار النهضة العربية، القاهرة، 2004، ص.ص872–873.

الكشف عن هذه الشفرات تطبيقا لمبدأ عدم اتهام الشخص لنفسه.[118]

المطلب الثالث

المعاينة في العالم الإفتراضي

تعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة، ومن أهم إجراءات التحقيق على الإطلاق، نظرا لما يمكن أن توفره من أدلة إثبات، وتزداد أهميتها أكثر إذا تعلق الأمر بالجرائم الالكترونية، باعتبارها من الجرائم المستحدثة وغير مألوفة بالنظر إلى الطبيعة الخاصة للسلوك الإجرامي فيها، والذي يستوجب ابتكار تقنيات جديدة مناسبة بالمعاينة في هذا المجال. وهو ما سنبحثه في الفرعيين التاليين:

الفرع الأول : مفهوم المعاينة

تعرف المعاينة بأنها إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في كشف الحقيقة[119]. فهي بذلك تعد من إجراءات التحقيق الابتدائي التي يجوز لسلطات التحقيق اللجوء إليها من تلقاء نفسها كلما رأت في ذلك ضرورة لإجلاء الحقيقة، أو بناء على طلب من الخصوم[120]. والأصل أن تجرى المعاينة بحضور أطراف الدعوى الجزائية، غير أنه يجوز للمحقق إجراؤها في غيابهم نظرا لما تقتضيه من سرعة

---

[118]– نص المشرع الجزائري على حق المشتبه به في الصمت وعدم الإدلاء بأي إقرار أثناء التحقيق في المادة(100)من قانون الإجراءات الجزائية، انظر في هذا الشأن أيضا : **لجنة منع الجريمة والعدالة الجنائية**، مرجع سابق، ص13.

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

[120]– تنص المادة(79) من قانون الإجراءات الجزائية الجزائري على" **ويجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها** ..."

الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة[121].

وللمعاينة أهمية بارزة في مجال التحقيق الجنائي لكونها مصدرا أصيلا من مصادر الأدلة المادية والفنية الراسخة والثابتة التي تكون دائما محل ثقة سلطات التحقيق و القضاء، ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة، فهي ناطقة بما أتاه شاهد على ما فعله الجاني دون انحياز أو تعديل أو نقصان[122].

وحتى تأتي المعاينة بثمارها وتفي بأغراضها المنشودة، أحاطتها بعض التشريعات بجزاءات جنائية توقع على كل من يتجرأ ويقوم بإحداث تغييرات على حالة الأماكن التي وقعت فيها الجريمة أو ينزع شيء منها قبل الإجراءات الأولية للتحقيق القضائي، باستثناء ما إذا كانت تلك التغييرات أو نزع الأشياء للسلامة والصحة العمومية أو ستلزمها معالجة الضحية[123].

وتتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة، وإذا كانت الجريمة واقعة على المكونات المادية للأجهزة الالكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص الممغنطة ، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعدّ أدلة

---

[121]–**محمد أبو العلاء عقيدة** " التحقيق و جمع الأدلة في محال الجرائم الالكترونية" ص 07. مقال منشور في الموقع التالي: www.osamabahar.com.

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

[123]– وفي هذا الشأن تنص المادة(43) من قانون الإجراءات الجزائية الجزائري على: " **يحظر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، وإلا عوقب بغرامة 200 إلى 1000دج**".

مادية تدل على وقوع الجريمة وانتسابها لشخص معين، ثم ضبطها وضعها في أحراز مختومة تقدم للنيابة العامة[124]. أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الالكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الانترنت فيكون الانتقال للمعاينة هنا افتراضيا أو الكترونيا، ويمكن للمحقق إجراء المعاينة الافتراضية أو الالكترونية بالولوج والانتقال إلى مسرح الجريمة عبر الانترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه، أو من خلال مقهى الانترنت أو إحدى مقرات مزود خدمات الانترنت[125].

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

-الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد ومواقع الأجهزة الالكترونية وشبكاتها وسائر ملحقاتها والنهايات الطرفية المتصلة بها المتوقع مداهمتها.[126]

-توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة التي يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتامين وحفظ المعلومات.

-تأمين التيار الكهربائي بشكل لا يتم التلاعب او التخريب عن طريق قطع التيار او تعديل الطاقة الكهربائية.

-التأكد من خلو المحيط الخارجي لمسرح الجريمة الالكترونية من أية مجالات لقوى

---

[124]- **ياسر محمد الكومي محمود أبو حطب**، الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشاة المعارف، الإسكندرية، 2014، ص 243.

[125]- **وليد عاكوم**، التحقيق في جرائم الحاسوب، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية، منعقد بإمارة دبي في الفترة الممتدة من 26 إلى 28 ابريل 2003.

[126]- **ياسر محمد الكومي محمود أبو حطب**، مرجع سابق، ص 245.

مغناطيسية او ممرات اتصالات التي يمكن أن تتسبب في محو البيانات المسجلة أو إتلاف الآثار الأخرى للجريمة [127].

-التحفظ على محتويات سلة المهملات ومستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.

– إعداد فريق من المتخصصين و أهل الخبرة في مجال تكنولوجية الإعلام الآلي للاستعانة بهم عند الحاجة [128].

الفرع الثاني: نطاق إعمال المعاينة الإلكترونية

يعتمد المحقق الجنائي لإجراء المعاينة الإلكترونية بحثا عن الأدلة الرقمية على فحص مجموعة مصادر الدليل في البيئة الإلكترونية التي ارتكبت فيها الجريمة المعلوماتية، والمتمثلة عادة في مكونات أجهزة الحواسيب الخاصة بالجاني والمجني عليه وملحقاتها وكذا أنظمة الاتصال بالانترنت.

-**أولا:معاينة مكونات الحاسب:** تعتبر الحواسيب مصدرا غنيا بالأدلة الإلكترونية خاصة الحواسيب الشخصية التي تعد بمثابة أرشيف لسلوك الأفراد ونشاطاتهم ورغباتهم، لذلك فان عملية فحص هذه الحواسيب تمثل نقطة البداية في الكشف عن خفايا الجريمة الإلكترونية باعتبار هذه الأجهزة وسيلة تنفيذها أو محل وقوعها. والمعروف أن الحاسب الآلي يقوم في تركيبته على ثلاثة عناصر أساسية هي، القطع الصلبة (Hardware) والقطع المرنة او البرمجيات(Software) وكذا المعطيات المعلومات أو البيانات (données informatiques) وهو العنصر الذي يتوزع بين القطع الصلبة و البرمجيات[129]. لذلك فمعاينة

---

[127]– **سرحان حسن المعيني**، مرجع سابق، ص.ص 41–42.

[128]– **محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، مرجع سابق، ص 114.

[129] – **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 1009

هذا الحاسب يستلزم الفحص المادي والمعنوي لكل هذه العناصر نظرا للارتباط الطبيعي بين بعضها البعض.

وقد تعتمد عملية الفحص هنا على طريقتين أساسيتين، الأولى هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكوناته وتقديم تقرير كامل إلى طالب الفحص، ومثل هذه العملية تتطلب من القائم بها معرفة تقنية ومهارة فنية عالية. أما الطريقة الثانية، فهي الفحص بواسطة حاسب آلي آخر أو أجهزة تقنية عالية للبحث في جزئية او جزئيات عبر الحاسب[130]. وعادة ما تشمل عملية فحص مكونات الحاسب الآلي العناصر التالية:

1-معاينة القرص الصلب: يتم معاينة القرص الصلب للحاسب الآلي بالفحص الجزئي أو الكلي للبيانات الرقمية ذات الطابع الثنائي المتواجدة بداخله، والتي تتميز بعدم التشابه فيما بينها رغم وحدة الرقم الثنائي (0- 1) الذي يتكون منه تفصيل هذه البيانات[131]. ولتحقيق ذلك، يقوم المحقق بنزع القرص من الحاسب المراد فحصه بكل عناية وحذر من أي ارتجاج أو اصطدام بأي شيء تفاديا لإتلافه أو تعطيله أو فقد أية بيانات، ثم يقوم بفحص وتحليل النسخ التي تصدر من القرص بنفسه أو بواسطة الخبير المختص[132].

والفحص الجزئي للقرص الصلب يسمح للمحقق التعرف على محتوى البيانات ثنائية الرقم التي يؤدي التعامل معها إلى الكشف عن القيمة الاسترادادية للبيانات المخزنة فيه سواء كانت محتويات مكتوبة أو مصورة أو مسجلة. وكذا استرجاع ما تم حذفه من بيانات ومعلومات وبرامج بالاستعانة ببرمجيات مخصصة لهذا الأمر. وكمثال على ذلك، نذكر حالة البحث في ملفات النسخ الإضافية التي تحتفظ بها نظم التشغيل من كل صفحة تمّ الولوج

---

[130]- **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 1011.

[131]- **حسين بن سعيد بن يوسف الغافري**، السياسة الجنائية...، مرجع سابق، ص426.

[132]- **خالد ممدوح إبراهيم**، الجرائم المعلوماتية، مرجع سابق، ص 215.

اليها عبر الانترنت، أو الملفات الخاصة بالإنزال (Download File) المتواجدة في نظم التشغيل والتي مهمتها استقبال الملفات التي يتم تحميلها على الحاسب من خارجه عبر الانترنت[133].

فعملية فحص القرص الصلب إذا، تساعد المحقق عادة على جمع البيانات والمعطيات المخزنة فيه بشكل آلي أو إرادي التي كان يستخدمها الجاني، من معلومات أو صفحات وعناوين الانترنت أو رسائل البريد الالكتروني المرسلة والمتلقاة وكذا مجموعة البرامج الجاهزة المتخصصة التي استعملها (المشتبه فيه)، للتواصل مع أصدقائه (شركاء المشتبه فيه في الجريمة)، ثم تحليليها و تحديد تاريخها من ثم مقارنتها مع وقائع الجريمة لاستخلاص الدليل[134].

وتجدر الإشارة إلى أن عملية فحص القرص الصلب كي تكون مجدية لا بد من مراعاة مسائل عدة منها الكيفية التي يتم ضبط الحاسب و فصل القرص الصلب عنه، ومهارة الشخص القائم لاستخلاص البيانات دون العبث بمحتوياتها، وكذلك مراعاة شرط سلامة الحاسب الآلي، الذي يعني صحة حركة القطع الصلبة فيه لتجنب رفض المحكمة الاعتداد بالدليل المنبثق عنه، فشرط سلامة الحاسب مطعن رئيسي على كل دليل تم الحصول عليه، لذا يجب دائما التأكد من سلامة الحاسب في أداء وظيفته قبل أي إقرار بمشروعية الدليل من حيث التحصيل[135].

---

[133]– **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص1012.

[134]– **علي حسن الطوالبة** ، مشروعية الدليل الرقمي المستمد من التفتيش الجنائـي ـ دراسة مقارنة ـ ص 07، بحث منشور على موقع الانترنت التالي: www.policemc.gov.bh/reports/2009/...7.../633843953272369688.doc

[135]– المرجع نفسه، ص 8.

2_معاينة البرمجيات: يتّبع المحقق في هذه العملية طريقتين هما، الفحص الداخلي للبرمجيات والفحص الخارجي لها. فأما الفحص الداخلي، فيتم من خلال البحث عن البناء المنطقي للبرمجية بما يكشف عن وجود مجهودا تجديديا في إعداده للعمل حين إنزاله في جهاز الحاسب الآلي، وذلك بتتبع الخطوات المنطقية التي تعبر عن هذا الجهد. ولعل أكثر ما يسعى المحقق الوصول إليه في إطار الفحص الداخلي هو مصدر الملفات الموجودة داخل البرمجيات التي تفيد في ترتيب حدوث الجريمة الالكترونية، والتعرّف على الكيفية التي تم الإعداد لها. علما أن النسخ عبر الانترنت يختلف عن النسخ باستخدام برمجيات المعالجة (Word Processing)، فالأول نسخ عبر العالم الافتراضي أما النسخ الثاني فيتم لاستخدام مصنف متداول في العالم المادي[136].

أما الفحص الخارجي، فيتم بواسطة البحث عن البناء المنطقي للبرمجية للتأكد مما إذا كانت هذه الأخيرة منسوخة أم لا، ثم مقارنة النسخة الأصلية بالنسخة محل الاشتباه للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة[137].

والجدير بالذكر هنا، أنه ينبغي عدم التعويل كثيرا على الدليل المحصل من معاينة برمجيات الحاسب الآلي عن طريق الفحص الداخلي أو الخارجي، لأن برمجيات الحاسب ليست ذات نظرة مثالية وغالبا ما يشوبها عيب أو قصور و لو جزئي في أداء وظيفتها، وهذا القصور من شأنه أن يؤثر في الحاسب فيجعله محل شك تهتز معه قيمة الدليل، كما له أثره في عملية تقويم الدليل المستمد من البرمجية ذاتها.

3-معاينة النظام المعلوماتي: لا يحتوي النظام المعلوماتي للحاسب على معلومات مكتوبة كما يعتقد معظم الناس، إنما يتكون من بيانات ثنائية الرقمية يتم إيداعها في الحاسب

---

[136]- **حسين بن سعيد بن يوسف الغافري**، مرجع سابق، ص 427.

[137]- **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 1013.

الآلي في شكل تخزين، ثم يقوم الحاسب بمعالجتها آليا و إبرازها على هيئة معلومة موحدة كلما تم استدعاؤها من قبل مستخدم الحاسب، أما إذا لم يتم استدعاء معلومة محددة فان بياناتها تضل مخزنة على حالتها الأصلية داخل الحاسب[138]. لذلك فالمهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر الموجهة من طرف مستخدم الحاسب والاستجابة لها.

وعليه، فالمقصود بمعاينة النظام المعلوماتي للحاسب هو قيام المحقق بفحص و ضبط كافة المعلومات المخزنة في ذاكرة تخزين الحاسب على شكل ملفات والتي يمكن استردادها عبره بأية حركة استردادية ممكنة، ما دام موضوعها يشكل جريمة.[139]

وقد أكد المختصّون في مجال تكنولوجية الإعلام و الاتصال بان نظام التخزين في ذاكرة الحاسب يعد مصدرا مهما للدليل الالكتروني، لأنه يسمح للحاسب الآلي بالاحتفاظ بصفة آلية بنسخة كاملة مما اطلع عليه المشتبه فيه من مواقع و صفحات الانترنت أثناء إبحاره عبر العالم الافتراضي، كما أن هناك أنظمة وبرمجيات جديدة فور ربطها بذاكرة التخزين يمكن لها تتبع كل خطوات المشتبه فيه ومساره عبر شبكة الانترنت واسترجاع ما تم تصفحه لفترات طويلة من الزمن قد تصل إلى ستة أشهر كاملة، ولو قام المشتبه به بإغلاق الاتصال بشبكة الانترنت و حذف كل ما قام نظام التشغيل بتخزينه[140].

ومع ذلك، فلا ريب أن كثرة التعامل بالحاسب الآلي والتردد عليه من أكثر من شخص يؤدي حتما إلى تكاثر محتوى النظام المعلوماتي مما يترتب عنه صعوبة فحصه بالنظر الى

---

[138]– **حسين بن سعيد بن يوسف الغافري**، السياسة الجنائية...، مرجع سابق، ص 430.

[139]– **خالد ممدوح إبراهيم**، مرجع سابق، ص 222.

[140]– **عمر محمد أبو بكر بن يونس**، مرجع سابق، 1018

الحجم الضخم والكم الهائل من المعلومات الممكن تخزينها فيه[141]. ناهيك عن تنوع أشكال وأساليب تخزين البيانات، التي يصل مداها إلى حدّ تخزين البيانات بشكل آمن في الحاسب بواسطة نظام التشغيل او نظام إخفاء البيانات المعلوماتية، مما يتعذر الكشف عن الملفات التي تحتوي عناصر إجرامية حتى في حالة البحث الآلي للحاسب عنها، ويحول دون وصول المحقق إليها.

ثانيا ـ معاينة أنظمة الإتصال بشبكة الانترنت: أحيانا لا يكفي معاينة مكونات الحاسب وحدها لاستخلاص الدليل الالكتروني، إنما يتطلب من المحقق فحص أنظمة اتصال الحاسب بشبكة الانترنت كذلك. ويقصد بأنظمة اتصال بشبكة الانترنت بالمفهوم الإجرائي، تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة الاتصال بالانترنت، لذلك فعملية فحص أو معاينة هذه الأنظمة يشمل بالأساس فحص مسار الانترنت أو ما يعرف ببروتوكول الانترنت، والنظام الأمني للشبكات، وكذا فحص الخادم.

1ـ فحص مسار الانترنت: تتم هذه العملية من خلال تتبع الحركة التراسلية للنشاط الممارس عبر الانترنت باستخدام نظام فحص الكتروني يسمى علم البصمات المعاصر أو علم بصمات القرن الواحد والعشرين،[142] وما يتم التوصل إليه بعد ذلك، هو عنوان رقمي يطلق عليه (Internet protocole adresse) أو باختصار(IP Adresse). وهو عبارة عن بروتوكول لعنونة البيانات والمواقع في شبكة الانترنت يتم بمقتضاه التعرف على الحاسب الآلي الموصول بشبكة الانترنت من خلال عناوين عددية ، علما أن لكل حاسب آلي عنوانه (IP Adresse) الوحيد الخاص به، و كل عنوان(IP) مكون من جزأين الأول يشمل أرقام الشبكة والثاني يشمل أرقام مزود الخدمة. فالحاسب الآلـي فور اتصاله بالانترنت يقوم تلقائيا

---

[141]–**علي عدنان الفيل**، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث ، القاهرة ، 2012، ص 33.

[142]– **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 998.

باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات[143].

ويشتغل البروتوكول (IP) بشكل متزامن مع بروتوكول آخر يدعى بروتوكول التحكم بالنقل (Trams mission control protocol TCP) للاتصال بين عدة أجهزة من الحواسيب طورت أساسا لنقل البيانات الرقمية عبر شبكة الانترنت[144]، ويرتكز البروتوكولان معا(TCP/ IP)على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Pachets) بين مختلف أنظمة الاتصالات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها [145]. وحزمة المعلومات، هي جزء من ملف معلوماتي حجم مصغر ثابت تحمل رقما خاصا ومعلومات تعريفية بكل من المرسل والمرسل إليه، وعند كل اتصال تتم قراءة جهة المقصد أو المرسل إليه ثم تتم إعادة الحزمة المارة عبرهما إلى الوصلات التالية الأقرب إلى جهة المقصد النهائية[146].

تبرز أهمية الاستعانة بالمعلومات والمصادر والعناوين التي يمكن أن يحتويها نظام البروتوكول(TCP/ IP) للتحقيق عن الجريمة الالكترونية، في كونها تدّل بصفة جازمة عن مصدر الجهاز المستخدم في ارتكاب الجريمة، وتحدّد الأجهزة التي أصابها الضرر من جراء الفعل الإجرامي و نوعية النشاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة، كما

---

143 - **GRYNBAUM Vincent** « le droit de l'information de reproduction a l'heure de la société de l'information, A propos de la directive 2001 /29 /CE du parlement européen et du conseil du 22/05/2001 sur l'harmonisation de certains aspects du droit d'auteur et des droit voisins dans la société de l'information, op.cit. P 2.

144– هذا البروتوكول(TCP) مسئول عن تدقيق صحة نقل المعطيات من الحاسب إلى الخادم و ذلك من خلال الكشف عن الأخطاء والتعرف على المعطيات الضائعة أثناء عملية الإرسال و من ثم يقوم بإعادة الإرسال لحين وصول كامل المعطيات بشكل صحيح إلى وجهتها النهائية.

145– **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 382.

146– **ممدوح عبد الحميد عبد المطلب**" استخدام البروتوكول(TCP/ IP) في بحث و تحقيق الجرائم على الكمبيوتر" مقال منشور على الموقع التالي: www.arablawinfo.com

أنها تساعد بالاطلاع على جميع المراسلات و المحادثات ، وكل ما تمّ نقله أو تبادله أو معالجته من بيانات عبر شبكة الانترنت، وكذا الكشف عن مصدرها وتتبع مسارها إلى غاية نقطة وصولها، من ثم تحديد هوية المرسل والمرسل إليه اللذين قد يمثلان أول المشتبه فيهم[147].

لذلك أثبتت تقنية تتبع الحركة العكسية لمسار الانترنت جدواها للكشف عن المجرمين في أكثر من جريمة الكترونية، إذ بواسطتها تم الكشف و القبض على مبتكر فيروس ميليسا، وكذا الشخص الذي ابتكر موقع خدمات بلومبرج لأخبار المال الاحتيالي لكي يرفع أسعار الأسهم عن طريق الغش و الخداع. كما أن القضاء أقرّ في عدة قضيا بمصداقية هذه التقنية في تحديد مسار العمل الإجرامي و مشروعية الأدلة المتحصل عليها من خلالها، منها ما جـاء في الحكم الذي تبنته محكـمة بـاريس الابتدائية بتـاريخ 22 ماي 2000 في قضية ياهو (yahoo) الشهيرة [148].

2-فحص الخادم (serveur): يعتبر الخادم من أهم نظم الاتصال بالانترنت، فهو جهاز الكتروني كبير مهمته ضمان حركة الاتصال بمواقع و صفحات الانترنت، ثم استقبالها وتخزينها فيه على هيئة رقمية. من هنا فان للخادم وضيفة مزدوجة، إذ يتولى من جهة ربط مستخدمي الانترنت بالمواقع والصفحات التي يريدون الاطلاع عليها، ويقوم من جهة ثانية باستضافة هذه المواقع والصفحات وتخزينها على شكل بيانات رقمية. وهو ما يرشحه لأن يكون مصدرا غنيا جدا للأدلة الالكترونية الرقمية يطلق عليه البعض موقع تخزين المعطيات الرقمية (Lieu de stockage des données numerisées)[149].

---

[147]- **حسين بن سعيد بن سيف الغافري**، السياسة الجنائية ...، مرجع سابق، ص 421.

[148] -UEIF. Licra C. Yahoo fr./ Yahoo inc. TGI Paris. Décision du 22 Mai 2000.

[149]- **حسين بن سعيد بن سيف الغافري**، مرجع سابق، ص 424.

وللقيام بعملية فحص الخادم ينبغي على المحقق الالتزام بالضوابط المقررة لإجراء المعاينة وفق القانون المنفذ في النطاق الإقليمي الذي يوجد فيه، واتخاذ كافة التدابير التقنية والفنية اللازمة للمحافظة على مسرح الجريمة من أي عبث أو تعديل، مع ضرورة الاستعانة بأحدث وسائل وآليات الفحص الالكتروني[150]. بالإضافة إلى لزوم الأخذ بعين الاعتبار مبدأ الغاية من البحث و التفتيش وبالتالي خلق مفارقة بين الخادم العام وبين الخادم الخاص بفئة تراسلية معينة. غير أن الأمر لا يقف عند هذه النقطة لأن تقنية الانترنت تجعل من الممكن القيام بفحص الخوادم عن بعد باستخدام تقنيات حديثة في هذا المجال تجعل التوصل إلى محتوى حركة الاتصال بالخادم ذات مغزى، وربما أفضل من مجرد القيام بفحص الخادم ماديا[151].

المطلب الرابع

الخبرة التقنية في الجريمة الإلكترونية

أدى التطور التقني الهائل في عالم تكنولوجيا الإعلام والاتصال إلى احداث تغيير كبير في المفاهيم المتعلقة بالدليل الجنائي، مما أدى بدوره إلى تعاظم دور الإثبات العلمي للدليل وإعلان انضمام الخبرة التقنية إلى عالم الخبرة القضائية، وأصبحت الاستعانة بخبراء مختصين لفحص الأدلة التقنية وتقويم عملية الإثبات الرقمي وتحليل الجريمة الالكترونية أمرا ملحا لا يمكن الاستغناء عنه[152]. إذ لا يعقل أن يفصل القاضي في قضايا تقنية المعلومات

---

[150]– **أحمد مسعود مريم**، مرجع سابق، ص 75.

[151]– **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 1007.

[152]– **عبد الناصر محمد محمود فرغلي** " الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية " دراسة مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، المنظم بالرياض، في الفترة الممتدة بين 12 و14 نوفمبر 2008، ص 24.

دون أن يستند إلى الخبرة التقنية في هذا المجال تحقيقا لمبدأ معروف هو "مبدأ التخصص" وإلا كان حكمه معيبا و مطعونا فيه.

وإذا كانت الخبرة الفنية من أقوى مظاهر التعاون القضائي في مجال التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات والانترنت، خاصة إزاء نقص المعرفة الفنية لدى القانونيين بخبايا هذه الظاهرة ، فهل يعني هذا تعرض مبدأ " القاضي خبير الخبراء" لهزات عنيفة إزاء التزايد المتواصل لمبدأ التفاعل القانوني مع ظاهرة البيئة الرقمية التي تقع في اختصاص آخر غير الجوانب النظرية القانونية، ولا تسمح ثقافة القاضي المبنية على الدراسات القانونية التفاعل معها؟ والجواب عن هذا السؤال يفرض علينا تبيان دور الخبرة الفنية في إثبات الجرائم الالكترونية (الفرع الأول) ثم التطرق إلى الجوانب القانونية والفنية التي تحكمها(الفرع الثاني).

الفرع الأول: دور الخبرة التقنية في إثبات الجريمة الإلكترونية

تعرف الخبرة الفنية بأنها إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء، من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع جريمة أو نسبتها إلى المتهم[153]. فهي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها بمعرفة فنية و دراية علمية لا تتوفر لديه.

وللخبرة الفنية دور كبير في إثبات الجريمة الالكترونية، لأنها تنير الدرب لسلطات التحقيق والقضاء و سائر الجهات المختصة بالدعوى الجزائية للوصول إلى الحقيقة و تحقيق العدالة الجنائية[154]، لذلك ومنذ تفشي الجرائم الالكترونية، تستعين سلطات التحقيق

---

[153]–**عبد الناصر محمد محمود فرغلي**، مرجع سابق، ص 23.

[154]– **بوكر رشيدة**، مرجع سابق، ص 424.

والاستدلال و المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال التقنية الالكترونية من اجل كشف غموض الجريمة وتجميع أدلتها والتحفظ عنها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[155].

وقد تزايدت الحاجة إلى الخبرة الفنية للتحقيق عن الجرائم الالكتروني في الآونة الأخيرة نظرا للتحولات التكنولوجيا التي مست وسائل الإعلام والاتصال، اذ تعددت أنواع ونماذج الحواسيب وشبكات الاتصال بينها، وأصبحت العلوم والتقنيات المتعلقة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتشعبة، والتطورات في مجالها سريعة و متلاحقة لدرجة قد يصعب على المتخصص تتبعها واستيعابها. بل يمكن القول انه لا يوجد حتى الآن خبير يملك معرفة متعمقة في سائر أنواع الحاسبات و برامجها و شبكاتها، أو قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها[156]. لذلك ترك المشرع للمحقق الحرية الكاملة وفي أية مرحلة من مراحل التحقيق ندب أي خبير يأنس فيه الكفاءة الفنية اللازمة للاستعانة بخبرته[157]. كما انه لا يوجد في القانون ما يلزمه بالاستجابة للمتهم ولا غيره من الخصوم إذا طلبوا ندب خبير[158].

ومع هذا، فإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمرا واجبا على جهة التحقيق أو الحكم، فهي أوجب في مجال استخلاص الدليل الرقمي لإثبات الجرائم الالكترونية، لتعلقها بمسائل فنية آية في التعقيد لا يكشف غموضها إلا

---

[155]– **علي عدنان الفيل**، مرجع سابق، ص 27.

[156]–**سليمان احمد فضل**، مرجع سابق ، ص 341

[157]– أنظر المادة (143) من قانون الإجراءات الجزائية الجزائري.

[158]- تنص الفقرة الثانية من المادة(143) من قانون الإجراءات الجزائية الجزائري على انه " **وإذا رأى قاضي التحقيق انه لا موجب لطلب الخبرة فعليه أن يصدر في ذلك قرارا مسببا...** " تقابلها المادة 156 من قانون إجراءات الجزائية الفرنسي.

متخصص بارع في مجال تخصصه، ذلك لأن الذكاء والفن لا يكشفه ولا يفهمه إلا ذكاء وفن مماثلين[159].

وتبرز أهمية الاستعانة بالخبير الفني لإثبات الجرائم الالكترونية بشكل أكبر عند غيابه، فقد تعجز سلطات التحقيق والاستدلال عن إماطة اللثام عن الجريمة وجمع الدليل بخصوصها لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل أو محوه بسبب الجهل أو الإهمال عند التعامل معه[160].

ولعل إدراك بعض دول العالم لهذه الأهمية، جعلها لا تكتفي بالنصوص التقليدية التي تنظم الخبرة الفنية، وإنما أسرعت إلى تدعيمها بنصوص قانونية جديدة خاصة بالخبرة في مجال جرائم التقنية العالية، نذكر في مقدمتها قانون الإجرام الالكتروني البلجيكي الصادر في 2000/11/23 الذي نص في المادة(88) هـ على انه "**يجوز لقاضي التحقيق والشرطة القضائية الاستعانة بخبير مختص من أجل الحصول و بطريقة مفهومة على المعلومات اللازمة عن كيفية تشغيل نظام الحاسب الآلي والولوج إلى داخله، أو الولوج إلى البيانات المخزونة فيه أو المعالجة أو المنقولة بواسطته** ". وتضيف نفس المادة بأنه " **لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو أخذ نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق، وعلى الخبير الاستجابة لطلب هيئات التحقيق**

---

[159]– **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 640.

[160]– وفي هذا الصدد، طلبت إحدى دوائر شرطة الولايات المتحدة الأمريكية من شركة تعرضت للقرصنة ان تتوقف عن تشغيل حاسبها الآلي حتى تتمكن من وضعه تحت المراقبة بهدف كشف المجرم، فحدث نتيجة لذلك أن تسببت الشرطة بدون قصد في إتلاف الملفات والبرامج التي كانت موجودة فيه. وللمزيد من التفاصيل انظر:**هشام محمد فريد رستم**، الجوانب الإجرائية للجرائم المعلوماتية–دراسة مقارنة، مكتبة الآلات الحديثة، القاهرة، 1994، ص 29.

والقضاء و إلا تعرض لعقوبات جزائية "[161].

ولم يتخلف المشرع الجزائري عن هذه التشريعات، اذ نص في المادة (05) الفقرة الأخيرة من القانون رقم (04/09) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة تكنولوجيا الإعلام والاتصال ومكافحتها بأنه " **يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها**" [162].

واعتقد أن صياغة المشرع الجزائري لهذا النص بصيغة العموم " **كل شخص له دراية**" أمر مقصود حتى يوسّع دائرة المساعدة القضائية في مجال مكافحة الجرائم الالكترونية لتشمل إلى جانب الخبير، جميع المتخصصين والمعاملين في مجال تكنولوجيات الإعلام والاتصال، مثل مهندسي وذوي الشهادات العليا في الإعلام الآلي، ومقدمي خدمات الاتصالات الالكترونية، كمزودي خدمة العبور إلى الانترنت، مزودي خدمة الإيواء، مزودي خدمة الحوسبة و كل من له دراية في هذا المجال.

ولم يتوقف المشرع الجزائري عند هذا الحد، بل قامت بإنشاء هيئات وأجهزة متخصصة في مواجهة الجرائم الإلكترونية مزودة بوسائل متطورة وتقنيات عالية، وجعلت من مهامها الأساسية انجاز الخبرات التي تحتاج إليها السلطات القضائية، نذكر منها مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها الذي أنشأته قيادة الدرك الوطني في عام

---

[161] –**DE VILLENFAGNE Florence**, La Belgique Sort Enfin Ses Armes Contre La Cybercriminalité : A Propos De La Loi Du 28novembre 2000 Sur La Criminalité informatique, droit et nouvelles technologies , 2001. P 22, article publier sur ; **http://www.droit-technologie.org.**

[162]– أنظر نص المادة(05) من القانون(04/09) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة تكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

2009، والمعهد الوطني للبحث في علم التحقيق الجنائي الذي أنشئ بموجب المرسوم الرئاسي رقم(04-432) المؤرخ في 20 ديسمبر 2004 وتم تنظيم المصالح والأقسام والمخابر فيه بموجب قرار وزاري مشترك مؤرخ في 14-04-2007 والذي تضمن مصلحة الخبرات الخاصة بالدلائل التكنولوجية[163]. ونذكر كذلك القسم الخاص بالخبرة الرقمية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية المتواجد على مستوى المديرية العامة للأمن الوطني وتمتد مصالحها الى بعض الولايات، والذي يتولى تقديم الخبرة الفنية المتميزة في القضايا ذات الطابع الرقمي. بالإضافة إلى إنشاء مؤخرا ثلاث مخابر جنائية جهوية بشمال البلاد تابعة للأمن الوطني تضمّ عدة أقسام متخصصة بما فيها قسم الأدلة الالكترونية والرقمية، والتي ستدعّم مستقبلا على حد تعبير ممثلة المديرية العامة للأمن الوطني هودة رشيدة ملازم أول للشرطة ورئيسة فرقة مكافحة الجرائم المعلوماتية لأمن ولاية وهران في بثلاث مخابر مماثلة في الجنوب[164].

ونشير إلى أنه تم إنشاء مؤخرا بموجب المرسوم الرئاسي رقم (15-261) المؤرخ في 08 أكتوبر 2015 هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها[165]، وأسندت إليها مهمة تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في البحث والتحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام

---

[163]- أنظر القرار الوزاري المؤرخ في 14-04-2007 المتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، جريدة رسمية عدد 36، صادر بتاريخ 03 جويلية 2007.

[164]- **هودة رشيدة** " دور الشرطة الجزائرية في محاربة الجريمة الالكترونية"، مداخلة مقدمة إلى الملتقى الوطني حول " الجريمة الالكترونية وأمن المعلومات" المنظم بكلية العلوم والتكنولوجيا بجامعة وهران، يوم 06 ديسمبر 2016، بدون ترقيم. مقال منشور في الموقع التالي: www.univ-usto.dz.id=257.

[165]- مرسوم رئاسي رقم (15-261) مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015، يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، جريدة رسمية عدد 53، صادر بتاريخ 8 أكتوبر 2015.

والاتصال، بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية[166].

الفرع الثاني: الجوانب القانونية و الفنية للخبرة في الجرائم الإلكترونية

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

أولا- الجوانب القانونية للخبرة الإلكترونية : نظرا للدور البارز الذي تؤديه الخبرة الالكترونية في مجال الإثبات الجنائي، حرصت معظم التشريعات على تنظيمها و إحاطتها بمجموعة من الضوابط حتى يكون لنتائجها حجية أمام القضاء، ومن ضمن هذه الضوابط ما يتعلق بالخبير و منها ما يتعلق بالخبرة، فأما الضوابط الخاصة بالخبير، فهي كالتالي:

أ-اختياره الخبير من جدول الخبراء : الأصل أن يختار الخبراء حسب التخصص من الجداول التي تعدّها المجالس القضائية بعد استطلاع رأي النيابة العامة، ولكن استثناء في حالة عدم توفر الخبرة المطلوبة في جداول الخبراء يجوز لجهات التحقيق أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول[167].

كما ان عملية اختبار الخبير أمرا متروكا لجهات التحقيق، فبمفهوم نص المادة(147) من قانون الإجراءات الجزائية الجزائري مثلا للقاضي أن يندب خبيرا واحدا أو خبراء متعددين حسب الحاجة، ولا تهم طبيعة الخبير سواء كان شخصا طبيعيا أو شخصا معنويا كمؤسسة متخصصة تعمل في مجال الخبرة التقنية[168]. واعتقد أن مثل هذا التوجه يتجاوب مع الحالة التي عليها الخبرة التقنية اليوم، سيما أمام ما يثيره مجال تقنية المعلومات من جدل

---

[166]-أنظر الفقرة (ب) من المادة (13) من القانون رقم (09-04) المؤرخ في 05-08-2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

[167]- أنظر نص المادة (144) من قانون الإجراءات الجزائية

[168]- **بوكر رشيدة**، مرجع سابق، ص 426.

واسع حول مقدمات التعامل معه، و كذا النتائج الممكن تحقيقها فيه.

مع هذا فرغم أن القانون لا يمنع جهات التحقيق من ندب خبير أو عدة خبراء حتى من غير المقيدين بالجدول، يبقي هذا التوجه قاصرا ويحتاج إلى تطوير في مجال الجرائم الالكترونية حتى يسمح بالاستعانة بخبراء الرقمنة والإعلام الآلي من الدول الأجنبية ولو عن بعد، وهو أمر تسمح به مقومات العالم الافتراضي باعتباره بيئة اتصالية رقمية عالمية ومعمول به لدى بعض الدول المتقدمة[169]. لان هذا الإجراء من شانه أن يعود بفائدة كبيرة على الدول لا سيما التي تعاني نقص الكفاءة في مجال تكنولوجيا الإعلام والاتصال والانترنت.

ب-أداء اليمين القانونية: اتفقت كل تشريعات العالم على ضرورة أداء الخبير لليمين القانونية قبل مباشرة مهامه وإلا كان عمله باطلا. وذلك شأن المشرع الجزائري الذي أوجب في المادة (145) من قانون الإجراءات الجزائية على الخبير في كل مرة يختار فيها وقبل أداء مهامه أن يحلف اليمين القانونية، غير انه إذا كان الخبير المعين مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى ما دام قد أدى اليمين عند تقييده بالجدول أول مرة[170]. ولعل العبرة من حلف الخبير هي حمله على الصدق والأمانة في عمله، وبث الطمأنينة في نتائج خبرته التي يقدمها سواء بالنسبة لتقدير القاضي أو الثقة ببقية أطراف القضية[171].

---

[169]– من بين الدول التي اعترفت بالخبرة الأجنبية أمام القضاء في مجال الجرائم الالكترونية فرنسا، بحيث استعان القضاء الفرنسي بخبراء أجانب (من أمريكا و انجلترا) في عدة قضايا منها قضية اتحاد الطلاب اليهود، و قضية منظمة ليكراء ضد شركة ياهو لكي يقدموا رأيا فنيا بخصوص إمكانية الفوترة و التصفية عبر الانترنت . راجع **خالد ممدوح إبراهيم**، مرجع سابق، ص 292.

[170]– تنص المادة (145) من قانون الإجراءات الجزائية علي مايلي " **يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الأتي بيانها: اقسم بالله العظيم بان أؤدي مهمتي كخبير على خير وجه و بكل إخلاص و ابدي رأي بكل نزاهة و استقلال. ولا يجدد هذا القسم مادام الخبير مقيدا بالجدول**".

[171]–**عبد الناصر محمد محمود** و **عبيد سيف سعيد المسماري**، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و

أما عن الضوابط المتعلقة بالخبرة، فتتمثل في التزام الخبير بالقيام بأعمال الخبرة بنفسه دون أن يكلّف بها غيره ويتقيد بالمهام المنوطة به والمحددة في أمر التعيين[172]، على أن يتولى مهامه تحت رقابة القاضي الذي أمر بإجراء الخبرة ولا يستلزم ذلك حضوره فعلا أثناء أداء أعماله، بل يكفي أن يبقى على اتصال مستمر معه وإحاطته علما بكل المستجدات التي تطرأ بعمله، على اعتبار الخبير ليس سوى مساعد فني للقاضي[173].

علاوة على ذلك، يتعين على الخبير بعد تفرغه من أبحاثه وفحوصاته إعداد تقرير مفصل حول المسألة محل البحث ويبين فيه خلاصة ما توصل إليه من النتائج، وعلى الخبير إيداع تقرير خبرته لدى كتابة الجهة القضائية التي أمرت بالخبرة خلال الآجال المحددة في أمر التعيين وإلا جاز استبداله بغيره ما لم يطلب الخبير تمديد هذه الآجال[174]، وفي حالة تعدد الخبراء و لم يصلوا إلى نتائج مشتركة يقدم كل منهم تقريرا منفصلا. وتقرير الخبير لا يكون ملزما للنيابة العامة أو المحكمة، إلا أن عدم الموافقة على التقرير يجب أن يكون مسببا، وفي هذه الحالة يجوز طلب خبرة تكميلية من الخبير نفسه وتمكينه الاستعانة بفنيين من أصحاب الاختصاص إذا تطلب الأمر ذلك بموجب طلب يقدمه لقاضي التحقيق، ويعينوا بأسمائهم ويؤدون اليمين، ويرفق تقريرهم بتقرير الخبرة[175].

الفنية، دراسة تطبيقية مقارنة ، بحث مقدم للمؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، المنعقد بالرياض في الفترة الممتدة بين 12-2007/11/14. ص 24.

[172]- تنبغي الإشارة هنا إلى ان التزام الخبير هو التزام ببدل عناية، فلا يسأل إذا لم يحقق النتيجة المطلوبة بسبب ضعف خبرته أو عقبات واجهته أثناء أداء مهامه، إنما تثار مسؤوليته الجنائية اذا رفض القيام بالمهمة المكلف بها بدون عذر مشروع أو اتلف عمدا البيانات المطلوبة منه التعامل معها أو حفظها و في حالة الإفشاء بالسر المهني. انظر المادة (153) من قانون الإجراءات الجزائية الجزائري.

[173]- **QUEMENER Myriam, CHARPENEL Yves**, Cybercriminalité-Droit pénal appliqué, édition Economica, Paris, 2010. P 183.

[174]- أنظر المادة (148) من قانون الإجراءات الجزائية الجزائري.

[175]- أنظر المادة(149) من قانون الإجراءات الجزائية الجزائري.

وإذا توفرت الخبرة على الشروط المذكورة أعلاه تكون لها حجية نسبية أمام القضاء، لان نتائج الخبرة ما هي في الواقع إلا استدلالات لإنارة قاضي الموضوع، وآراء الخبير تقدّم دائما بصفة استشارية ولا تلزم المحكمة فإن شاء القاضي أخد بالخبرة وإن لم يشأ استبعدها[176]، كما له أن يفاضل بين تقارير الخبرات ويأخذ منها بما يطمئن إليه ويطرح جانبا ما عداه. فالكلمة الأخيرة تعود لقاضي الموضوع وحده عملا بمبدأ " **القاضي خبير الخبراء**".

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

ثانيا- الجوانب الفنية للخبرة الإلكترونية: نظرا للطبيعة الفنية و العلمية البحتة التي تتميز بها الجرائم الالكترونية، فان عملية تحري الحقيقة وتجميع الأدلة الرقمية فيها تعد من أصعب التحديات التي تواجه الخبير التقني، لذلك كان لزاما عليه اعتماد تقنيات ومهارات علمية مهمة والاستعانة بوسائل تكنولوجيا متطورة لرفع هذا التحدي .

أ-تقنيات انجاز الخبرة الالكترونية: لقد وضعت وزارة العدل الأمريكية إطارا عمليا نموذجيا يحدد التقنيات الأساسية التي يتعين على الخبير الالكتروني إتباعها لجمع الأدلة الرقمية، فحصها و تحليلها، ومن ثم كتابة النتائج المتوصل إليها في التقرير، والتي يمكن تلخيصها فيما يلي:

1 -**تقنيات ما قبل التشغيل والفحص:** و تتمثل في:

-التأكد من صلاحية وحدات نظام الأجهزة الالكترونية المتعلقة بالجريمة للتشغيل.

-التحقق من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها .

---

[176]- وهو ما أكدته المادة (215) من قانون الإجراءات الجزائية الجزائري كما يلي " **لا تعتبر المحاضر و التقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك**".

-تسجيل وتوثيق معطيات وحدات المكونات المضبوطة، كالنوع والطراز والرقم التسلسلي[177].

2-**تقنيات التشغيل والفحص:** وهي كالتالي:

-استكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز.

-وضع نسخة لكل دعائم التخزين المضبوطة بما فيها القرص الصلب، وإجراء الفحوصات المبدئية عليها لحماية الأصل من أي فقدان أو تلف أو تدمير يكون سببه سوء الاستخدام أو برامج القراءة المدمرة أو ما يدعى (أعراض القراءة المدمرة) فيروسات أو قنابل برمجية.

-تحديد أسماء وأنواع المجموعات البرمجية ذات دلالة بالجريمة كبرامج النظام، برامج التطبيقات وبرامج الاتصالات...الخ.

-إظهار الملفات المخبأة والنصوص المخفية داخل الصور.

-استرجاع الملفات التي تم محوها من الأصل باستعمال برامج استعادة المعلومات و إصلاح الملفات المعطلة أو التالفة، مع العلم أنه في حالة محو معطيات المجرّمة من طرف المجرم، فإنها لا تحذف ماديا و إنما "الرابط" بين هذه المعطيات هو من يمحى، فالمعطيات تبقي في ذاكرة الدعامة وبالتالي يمكن ايجاد الملفات المحذوفة عن طريق فحص الهوامش العلوية (les en-têtes) ومن ثم استعادة[178].

-تخزين هذه الملفات، أو البيانات وعمل نسخ طبق الأصل أخرى من الاسطوانة أو القرص المحتوي لها من اجل فحصها.

-إعداد قائمة يجرد فيها الخبير كل الأدلة المتحصل عليها مع إجراء مراجعة لكل نسخة أو

---

[177]- **غازي عبد الرحمن هيان الرشيد**، الحماية القانونية من جرائم المعلوماتية، رسالة لنيل درجة دكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية في لبنان، بيروت، 2004، ص.ص 530-531.

[178]- **أحمد مسعود مريم**، مرجع سابق، ص 74.

صورة محتفظ بها في جهاز أخر للتأكد من سلامة القائمة .

-تحديد الخصائص المميزة لكل جزء من الأدلة الرقمية مثل المستند الرقمي، البرامج، التطبيقات، النصوص، الصور، الأصوات، وتحويلها إلى هيئة مادية كل حسب طبيعته.[179]

ب ـ الوسائل العلمية لانجاز الخبرة الالكترونية : يعتمد الخبير في شرح ملابسات الجريمة الالكترونية واستخلاص الدليل الرقمي الذي يساعده على الكشف عن المجرم الالكتروني على جملة من الوسائل العلمية، والتي تمثل في الغالب أدوات فنية تستخدم في بنية نظام المعلومات. ونذكر منها مايلي:

ـ **برتوكول الانترنت (IP):** أو ما يسمى بعنوان الانترنت هو نظام يشبه عنوان البريد العادي يعمل على تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها، فهو موجود بكل جهاز الكتروني مرتبط بشبكة الانترنت ويتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات، ويشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الأجهزة الالكترونية المرتبطة، والجزء الرابع يحدد الجهاز الذي تم الاتصال منه[180]. وفي حالة وقوع جريمة الكترونية فيمكن للخبير إتباع المسار التراسلي للبرتوكول (IP) للبحث عن رقم الجهاز المستعمل في ارتكاب الجريمة،ومن ثم تحديد موقعه ومنه معرفة الجاني.

ـ **نظام البروكسي (PROXY):** يشتغل هذا النظام كوسيط بين شبكة الانترنت ومستخدميها يضمن توفير خدمات الذاكرة الجاهزة، ويقوم هذا النظام على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق نظام البروكسي فيما إذا

---

[179]- **خالد ممدوح إبراهيم**، مرجع سابق، ص.ص 302- 303 .

[180]- **سليمان بن مهجع العنزي**، وسائل التحقيق في جرائم نظم المعلومات، رسالة لنيل درجة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003،ص 98.

كانت هذه الصفحة قد جرى تنزيلها من قبل، ويقوم بإرسالها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشبكة العالمية مرة اخرى، أما إذا لم يتم تنزيلها من قبل، فيقوم بتحويل الطلب إلى الشبكة العالمية مستعينا في ذلك بأحد عناوين (IP)[181]. ومن أهم مزايا هذا النظام أن الذاكرة المتوفرة لديه تحتفظ وتخزّن كل عمليات التنزيل التي تمت عليه والتي يمكن أن تساعد الخبير على اقتناء أدلة إثبات مهمة، مما يجعل دور البروكسي قويا و فعالا في عملية إثبات الجريمة الالكترونية.

ـ **برنامج (Trace route):** يتم عادة ادراج هذا البرنامج ضمن نظم تشغيل الحاسب الرئيسية، ويعتبر ذا أهمية بالغة في الكشف الجنائي، إذ يحدد بدقة الأجهزة الالكترونية التي اشتركت في نقل البيانات على الانترنت بتحديد مساراتها وصولا إلى المرسل إليه، كما يمكنه أن يستدعى ويحيط بالملفات التي تم الولوج إليها وكافة عمليات الاختراق والعبور أو التجاوز خلال الإعداد للجريمة، وكافة المعلومات المتعلقة بدخول أشخاص مواقع معينة وتحديد مسارات تنقلاتهم فيها الى غاية خروجهم من هذه المواقع، وعليه فكل هذه المسارات تتضمن عادة آثار أو أدلة رقمية يمكن الاستدلال بها على الجريمة[182].

ـ **أنظمة كشف الاختراق (IDS):** يكمن دور هذه الفئة من البرامج في مراقبة العماليات التي تحدث على الأجهزة الالكترونية المرتبطة بشبكة الانترنت وتسجيلها فور وقوعها في سجلات خاصة داخل هذه الأجهزة[183]، ومن بين هذه الأنظمة برنامج (hack Tracer V 1.2) الذي يتكون من شاشة رئيسية تقدم للمستخدم بيانا شاملا بعملية الاختراق

---

[181]– **سليمان بن مهجع العنزي**، مرجع سابق، ص 99.

[182]– **ممدوح عبد الحميد عبد المطلب**، مرجع سابق، ص.ص 15–16.

[183]– **محمد بن نصير السرحاني**، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الانترنت" دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية" رسالة لنيل درجة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 84.

التي تعرض لها جهازه، يذكر فيه اسم وتاريخ الواقعة والعنوان (IP) الذي تمت من خلاله عملية الاختراق واسم مزود خدمة الانترنت المستضيف للمخترق ورقم المنفذ والبوابة الخاصة وبيانات الشبكة التي يتبعها مزود الخدمة للمخترق بما فيها أرقام هواتفها.

- **برامج مراجعة العماليات الحاسوبية واسترجاعها (Auditing Tools):** هي برامج تستعمل لمراقبة مختلف العماليات التي تجري على ملفات وأنظمة تشغيل حاسب معين وتسجيلها في ملفات تسمى (Logs)، واسترجاع هذه الملفات في حالة محوها و حذفها[184]. ومن أمثلتها برنامج (Event Viewer) لبيئة النوافذ وبرنامج(Syslogd) لبيئة يونيكس، وبرنامج(Recover). وتأتي هذه البرامج إما مضمنة في أنظمة التشغيل أو كبرامج مستقلة يتم تركيبها على أنظمة التشغيل، وفي كلتا الحالتين لا بد من تفعيلها وإعدادها للعمل مسبقا قبل وقوع الجريمة الالكترونية حتى تتمكن من تسجيل كل المعلومات المتعلقة بهذه الجريمة والتي من شانها أن تساعد الخبير في استنباط الأدلة والقرائن المفيدة لإثبات الجريمة وانتسابها إلى مرتكبها[185].

ـ **برنامج الدمج وفك الدمج (pkzip):** يستعين الخبير الالكتروني بهذا البرنامج عادة لفك البرامج التي قام المجرم الالكتروني بدمجها قصد التعرف على طبيعة البيانات التي يحتويها وتحليلها، ودمج البرامج هي تقنية عالية يستعملها المجرم الالكتروني لإخفاء معلومات معينة لا يمكن الاطلاع عليها إلا بعد فك الدمج[186].

---

[184]– **حسن بن أحمد الشهري**، نظم المعلومات وتكاملها مع النظم الخبيرة، مجلة الفكر الشرطي، عدد 82، صادر عن مركز بجوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مارس 2012، ص.ص 67ـ 68.

[185]– **حسين بن سعيد الغافري**، التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مرجع سابق، ص 16.

[186]– **حسن طاهر داود**، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص 230.

ـالذكاء الصناعي: نقصد بالذكاء الصناعي تقنيات وبرامج الحاسب الآلي التي يستعين بها الخبير الالكتروني لحصر الأسباب والفرضيات المتعلقة بالجريمة، وجمع الأدلة الجنائية وتحليلها واستخلاص الحقائق منها، عن طريق عمليات حسابية يتم حلها بواسطة برامج الحاسب الآلي صممت خصيصا لهدا الغرض[187]، كبرنامج (Xtree Progold) الذي يستخدم للعثور على الملفات المبحوث عنها في أي مكان على الشبكة أو الأقراص الصلبة أو الأقراص المرنة المضغوطة، وقراءة محتوياتها في صورتها الأصلية من اجل التحليل والتقويم[188].

المبحث الثاني

استحداث إجراءات تحقيق خاصة بالجرائم الإلكترونية

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

واعتبارا للطبيعة الخاصة للجرائم الالكترونية في عناصرها و وسائل وتقنيات ارتكابها، اضطر المشرع الجزائي في العديد من الدول إلى إعادة النظر في كثير من المسائل

---

[187]– **حسن بن أحمد الشهري**، مرجع سابق، ص 51. و **حسين بن سعيد الغافري**، مرجع سابق، ص 17.

[188]– **حسن طاهر داود**، مرجع سابق، ص 228.

الإجرائية، خاصة فيما يتعلق بمسالة التحقيق والإثبات، باعتبارها أهم موضوعات هذا القانون. لان الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية للتحقيق واستخلاص الدليل قادرة على القيام به. مما قد يؤدي في الغالب إلى إفلات العديد من المجرمين من العقاب.

وعلى ضوء ما تقدم، كان لزاما على المشرع التدخل بقواعد إجرائية جديدة أكثر فعالية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الالكترونية الاعتماد عليها في الكشف عن المجرم المعلوماتي والوصول إلى دليل الإثبات فيها بسرعة و سهولة، وهي الإجراءات التي سوف نتناولها بشيء من التفصيل في هذا المبحث من خلال خمسة مطالب.

المطلب الأول

التســرب الإلكترونـــي

يعد التسرب من إجراءات البحث والتحقيق الجديدة التي أرستها معظم تشريعات العالم الحديثة لمواجهة الجرائم الالكترونية[189]، وقد كانت اتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية سباقة الى احتواء هذا الإجراء بنصها في المادة (20) على أساليب التحري الخاصة بما فيه التسرب الذي عبّرت عنه ب" **الأعمال المستترة**". أما المشرع الجزائري فقد تبني بدوره هذا الإجراء، مباشرة عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة أعلاه بموجب المرسوم الرئاسي رقم (05/02)

[189]– نظم المشرع الفرنسي عملية التسرب "Infiltration" في المواد (7/694 ، 9/694، 81/706 و 87/706) من قانون رقم (207/2004) المؤرخ 2004/03/09 المتضمن قانون الإجراءات الجزائية، المعدل و المتمم

المؤرخ في 2002/02/02 بتحفظ واتفاقية مكافحة الفساد لسنة 2003 بتاريخ 2004/04/19.

وقد ورد النص على هذا الأسلوب لأول مرة بالجزائر بمناسبة صدور القانون رقم(01/06) المتعلق بالوقاية من الفساد ومكافحته في عام 2006، الذي نص في المادة(56) على أنه" **من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن اللجوء إلى التسليم المراقب وإتباع أساليب تحري خاصة كالترصد الإلكتروني أو الاختراق على النحو المناسب وبإذن من السلطة القضائية المختصة** "[190].

ولكن نظرا للغموض الذي انتاب هذا النص بخصوص المقصود بالاختراق أو التسرب شروطه وآليات مباشرته، بقي هذا الإجراء جامدا وبدون مفعول إلى أن تم تعديل قانون الإجراءات الجزائية بموجب قانون(06/ 22) المؤرخ في 2006/12/20، أين تم تحديد معالم إجراء التسرب من خلال تعريفه و تحديد ضوابطه والآثار المترتبة عنه، وهي النقاط التي سوف ندرسها بشيء من التفصيل من خلال الفرعين التاليين:

الفرع الأول: المقصود بالتسرب

تعرّف المادة (65 مكرر12) من القانون الإجراءات الجزائية الجزائري التسرب على انه " **قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلّف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك أو خاف** "[191].

---

[190]– أنظر نص المادة (56) من القانون رقم (06–01) مؤرخ في 2006/02/20، يتعلق بالوقاية من الفساد ومكافحته، ج رج ج عدد 14، صادر بتاريخ 08–03–2006.

[191]– هو التعريف الذي تبناه المشرع الفرنسي في المادة 706–81 من قانون الإجراءات الجزائية التي تنص:

« …un officier ou un agent de police judicaire spécialement habilité, et agissant sous la responsabilité d'un officier de police judicaire charger de cordonner l'opération

انطلاقا من هذا التعريف، يتبيّن أن التسرب عملية معقدة جدا تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية[192]، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية. لذلك اعتبار لهذه الضرورة تفطّن المشرع الجزائري وجرّد الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب[193].

ليس هذا فحسب، بل أحاط المشرع المسرّب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرّب وبعد انقضائها، منها ما ورد في المادة(65 مكرر 16) من قانون الإجراءات الجزائية بأنه "**لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراء**"[194]. وما تضمنته كذلك المادة (65 مكرر17) من القانون نفسه بأنه " **إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة(65 مكرر 14) أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائيا، على أن لا يتجاوز ذلك 4 أشهر**" .

---

peut…surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs co-auteurs, complices ou receleurs » voir la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales, JORF 16 nov 2001.

[192]– أنظر المادة (65 مكرر 14) من القانون الإجراءات الجزائية

[193]–أنظر المادة (65 مكرر 14 فقرتها الأخيرة) من القانون الإجراءات الجزائية

[194]–وقد فرض المشرع الجزائري في الفقرات (1، 2و 3 من المادة 65 مكرر 16) من قانون الإجراءات الجزائية على من يكشف هوية المتسرب عقوبات صارمة تتفاوت درجتها حسب الضرر الذي يرتبه الكشف على المتسرب أو على احد أفراد أسرته قد تصل إلى 20 سنة حبسا و غرامة مليون دينار .

وعلى هدى ذلك، لا يجوز اللجوء لعملية التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة (65 مكرر) وهي: جرائم المخدرات، الجريمة المنظمة، جرائم تبييض الأموال و الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[195].

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

الفرع الثاني: ا لضوابط التي تحكم التسرب في الجرائم الإلكترونية

نظرا للخطورة التي يشكلها إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه، فقد قيده المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي:

أولا–الضوابط الإجرائية: تتلخص الضوابط الإجرائية للتسرب الالكتروني في الإذن القضائي وكل ما يجب أن يتضمنه من أحكام، إذ لا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة والمتمثلة حسب أحكام المادة (65 مكرر 11 ق إ ج) في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه[196]. على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لتلافي حدوث

---

[195]– أنظر المادة(65 مكرر) من القانون الإجراءات الجزائية

[196]– تنص المادة(65 مكرر 11) من قانون الإجراءات الجزائية على أنه " ... **يجوز لوكيل الجمهورية او لقاضي التحقيق بعد إخطار و كيل الجمهورية ان يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب**"

تجاوزات و تعسف في استعمال هذا الحق.

ولا يكفي أن يصدر الإذن بالتسرّب من الجهة المختصة فحسب، بل لابد أن يكون مكتوبا وإلا كان هذا الإجراء باطلا، لأن الأصل في العمل الإجرائي الكتابة، وهو ما أكدته المادة (65 مكرر15 ق إ ج) بنصها " **يجب أن يكون الإذن المسلم طبقا للمادة(65 مكرر 11) مكتوبا تحت طائلة البطلان** ".

كما يشترط أن يتضمن الإذن بالتسرب جملة من البيانات التي يتوقف على تحديدها صحة الإجراء ذاته، كذكر نوع الجريمة محل عملية التسرب واسم ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وتحديد المدة المطلوبة لهذه العملية، والتي يجب ألا تتجاوز أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن الشروط نفسها. و في الوقت ذاته يجوز للقاضي الذي أذن بهذا الإجراء أن يأمر بوقفه في أي حين قبل انقضاء الآجال المحددة[197].

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

-الأول هو عنصر التسبيب، تضمنته المادة(65مكرر15 ق إ ج)، ويتمثل في المبررات والحجج التي أقنعت الجهات القضائية المختصة لمنح الإذن باجراء التسرب، وكذا الدوافع والأسباب التي جعلت ضابط الشرطة القضائية يلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكون ضمن موضوع طلبه الإذن.[198]

- أما العنصر الثاني، فيتعلق بتحديد نوع الجريمة التي ينصب عليها الإذن بالتسرب

---

[197]- أنظر المادة(65 مكر 15) من قانون الإجراءات الجزائية الجزائري.

[198]- **علاوة هوام** " التسرب كآلية للكشف عن جرائم في القانون الجزائري " مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر بباتنة، 2012 ، ص 03.

والتي يجب ألا تخرج عن نطاق الجرائم السبع التي حددتها على سبيل الحصر المادة(65 مكرر 5) المشار إليها أعلاه.

والناظر إلى هذه الطائفة من الجرائم التي خصها المشرع الجزائري بإمكانية الأمر بإجراء عمليات التسرب بخصوصها، يجدها تندرج ضمن الجرائم الخطيرة جدا لسرعة انتشارها وامتداد آثارها خارج الحدود الوطنية، كما أنها تسخر عددا كبيرا من المجرمين الأذكياء، وقائمة على التخطيط واستخدام كل الوسائل محو آثار الجريمة وطمس معالمها[199]. مما يجعل الاستعانة بإجراء التسرب للكشف عن مثل هذه الجرائم والإطاحة بمرتكبيها أمرا مبررا ومفيدا.

المطلب الثاني

اعتراض المراسلات والمراقبة الإلكترونية

إن الإقدام الهائل للأفراد والمؤسسات على وسائل الاتصال الحديثة والاستخدام المفرط لشبكات المعلوماتية في الآونة الأخيرة ، جعل المشرع في العديد من الدول يدرك الصعوبات الكثيرة التي تثيرها محاولة مدّ نطاق إجراءات الاعتراض والمراقبة وفق النصوص التقليدية لتشمل المراسلات والاتصالات عبر الشبكات المعلوماتية، لذلك عمدت العديد من هذه الدول إلى مراجعة قوانينها الإجرائية، بوضع نصوص صريحة تنظم هذه العملية.

فكان المشرع الفرنسي سباقا إلى تبني عملية اعتراض ومراقبة الاتصالات الالكترونية ضمن إجراءات التحري و التحقيق الجنائي من خلال قانون إجراءاته الجزائية لعام 1991، ثم تلاه المشرع الأمريكي في عام 2000 بمناسبة تعديل القانون الاتحادي الإجرائي

[199]– **زورو هدى**، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة و القانون، العدد الحادي عشرة، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، 2014، ص 121.

الأمريكي، أين تم توسيع مجال تطبيق إجراء الاعتراض والمراقبة ليشمل كل المراسلات السلكية واللاسلكية[200]. ونظرا لثبوت نجاعة هذا الإجراء في تعقب الدليل و إثبات الجرائم الالكترونية، فقد أوصت الاتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001 من خلال نص المادة(21) جميع الدول الأعضاء بضرورة تبني اعتراض المراسلات والمراقبة الالكترونية للاتصالات في تشريعاتها الإجرائية الداخلية ضمن إجراءات البحث والتحقيق ،[201] الأمر الذي لقي استجابة واسعة من طرف غالبية الدول الأوروبية.

ولم يتخلف المشرع الجزائري عن هاته الدول، بل تدخل بموجب قانون الإجراءات الجزائية رقم (22/06) المؤرخ في 2006/09/20 المعدل و المتمم فاستحدث لهذا الإجراء الفصل الرابع كاملا تحت عنوان " اعتراض المراسلات وتسجيل الأصوات والتقاط صور" تناول فيه المقصود بهذا الإجراء، نطاقه وضمانات استخدامه. ثم عززه بالقانون رقم (04/09) المؤرخ 5 أوت 2009 . و سنبين كل ذلك في الفرعين التاليين:

الفرع الأول: مفهوم الاعتراض و المراقبة الإلكترونية

عرّفت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد بسترسبورغ في 2006/10/06 لدراسة أساليب التحري التقنية و علاقتها بالأفعال الإرهابية عملية اعتراض المراسلات بأنها "عملية مراقبة سرية المراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكـابهم أو

---

[200]- **VERGUCHT Pascal**, op.cit., p 384.

[201] -**Article(21) ; Interception de données relatives au contenu** ;

1- chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves a définir en droit interne : a- a collecter ou enregistrer par l'application par de moyens techniques existant sur son territoire,et … ». voir ; http://convention.coe.int/Treaty/fr/Treaties/Html/185.htm

مشاركتهم في ارتكاب جريمة"[202].

وقد اقتبس المشرع الجزائري هذا التعريف بشيء من التفصيل في المادة(65 مكرر5) من قانون الإجراءات الجزائية، إذ اعتبر عملية مراقبة المراسلات بأنها " اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للانتهاج والتوزيع، التخزين، الاستقبال والعرض. مـع العلم ان هذا النص هو إعادة صياغة المادة(100) من قانون الإجراءات الجزائية الفرنسي [203].

فبالرجوع الى نص هذه المادة، نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات[204]، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، أشكال، صور) أو الدعامة التي تنصب عليها (ورقية أو رقمية)، أو الوسيلة المستعملة لإرسالها سلكية كانت (كالفكس، تليغرام) أم لاسلكية (البريد الالكتروني، الهاتف النقال)، باستثناء الكتب والمجلاّت والرسائل والحوليات التي تعد مراسلات خاصة[205].

---

[202]- مشار إليه لدى: **بوكر رشيدة**، مرجع سابق، ص 442.

[203] - l'article(100) stipule "… les autorités judiciarises peuvent intercepter, enregistrer et transcrire des correspondances émises par la voie des télécommunications … » voir la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales Français, JORF, 16 nov., 2001.

[204]- **BENNOUAR Abdelhakim**, Les techniques spéciales d'enquête et d'investigation en Algérie, article publier sur ; www.Mémoire Online 2000-2013, pp 2-3

[205]– وهو ما يستشف كذلك من خلال نص المادة (6/09) من القانون رقم (03/2000) المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد و المواصلات التي اعتبرت المراسلات بانها " **كل اتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها الى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، و لا تعتبر الكتب و الجرائد و المجلات و اليوميات كمادة مرسلات** "

وقد تأكّد هذا الأمر في المادة (02 فقرة "و") من القانون رقم(04/09) التي عرفت الاتصالات الالكترونية بأنها " **أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة الكترونية**"[206].

وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون علم أو موافقة المعنيين[207]، وذلك لغرض التصنت و التقـاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل لمواجهة المتهم[208].

ولعل من أهم المراسلات الالكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض والمراقبة والتي تمثل مصدرا غنيا لأدلة إثبات الجرائم الالكترونية، المراسلات عبر البريد الالكتروني، كون هذه التقنية من أكثر الوسائل الحديثة استخداما للاتصال عبر الانترنت و مجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون حواجز. فهو بمثابة نظام تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، كما يستخدم

---

[206]– وهو التعريف الذي كرره المشرع الجزائري في المادة(05) من المرسوم الرئاسي رقم(15–261) المؤرخ في 8 أكتوبر 2015، المحدد تشكيلة وتنظيم و كيفيات تسيير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جريدة رسمية عدد 53، صادر في 8 أكتوبر 2015 .

[207]– من أشهر تقنيات المراقبة الالكترونية تقنية برنامج كارنيفور التي طورتها إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي (FBI) من أجل تعقب و فحص رسائل البريد الالكتروني المرسلة و الواردة عبر أي حاسب خادم يستخدمه أي مزود خدمة الانترنت، و يشتبه في أن المراسلات المارة عبر خدماته تحمل معلومات مهمة عن جرائم ما. للمزيد من التفاصيل انظر : **مصطفى محمد موسى**، المراقبة الالكترونية عبر شبكة الانترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، دار الكتب و الوثائق القومية المصرية، القاهرة، 2003، ص 180.

[208]– **زيبحة زيدان**، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص157.

كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه بسهولة لأنه محاط بحماية فنية[209].

ومن هنا، فعملية اعتراض ومراقبة البريد الالكتروني التي تجري بغرض ضبط المراسلات الالكترونية تنصب على ثلاثة عناصر أساسية وهي : الأول هو الوارد (IN)، ويتم من خلاله مراقبة ومراجعة قائمة المراسلات الالكترونية التي وصلت المشتبه فيه. والثاني الصادر (OUT)، وهو عكس الوارد يفيد في الكشف عن قائمة المراسلات التي أرسلت من طرف المشتبه فيه. أما العنصر الثالث فهو الحافظ و سلة المهملات (Trash) الذي يسمح بالاطـلاع على المـراسلات المحفوظة داخل البريد الالكتروني الخاص بالمشتبه فيه و المحذوفة منه والتي تحفظ بشكل آلي في سلة المهملات[210].

وينبغي التنبيه في هذا الصدد، الى أن المراسلات التي تصلح لأن تكون محلا لإجراء الاعتراض أو المراقبة لابد أن تتسم بالسرية و الخصوصية، ولا يتحقق هذا الأمر إلا بتوفرها على عنصرين جوهرين، يتعلق الأول بموضوع وفحوى المراسلة في حد ذاتها عندما ينصب على معلومات أو أفكار شخصية وسرية فيما تخبر به. أما العنصر الثاني، فهو شخصي ويتعلق بإرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالاطلاع على مضمون المراسلة[211].

وهما العنصران اللذان تأكّدا من قبل القضاء في عدة مناسبات، منها ما قضت به المحكمة العليا بكندا بان " **الحالة الذهنية للمرسل هي الحاسمة في تحديد الصفة الخاصة**

---

[209]– **زيبحة زيدان**، مرجع سابق، ص 159.

[210]- **DOSTE AMEGEE Maximilien**; La Cyber-surveillance et le secret professionnel, paradoxes ou contradictions?, mémoire D.E.A, université Paris, Nante, P 51 sui, disponible en ligne a l'adresse suivante ; http ://mémoire online.free.fr

[211] - **FERAL-SCHUHL Christiane** « cyber droit- le droit a l'épreuve de l'internet » 06 éme édition, Dalloz, 2011-2012, p 999 . et **DOSTE AMEGEE Maximilien**, op.cit. p 50.

أو العامة للاتصال". وانتهت إليه المحكمة الأمريكية بنيويورك في قرار لها بأن " **خصوصية الرسائل الالكترونية تعتمد بشكل كبير على طبيعة تكتم الرسائل و طبيعة مرسلها**"[212]. وعليه فتحقق هذين العنصرين في المراسلة هو فقط ما يجعلها تتصف بالمراسلة الخاصة التي لها خصوصيتها وسريتها المحمية قانونا، ولا أهمية لشكل الرسالة أو طرق نقلها أو توصيلها إلى المرسل إليه.

وتجدر الإشارة إلى أن المشرع الجزائري لم يتبني في القانون رقم (09-04) مراقبة الاتصالات الالكترونية كإجراء تقتضيه التحريات والتحقيقات القضائية فقط مثلما هو في قواعد الإجراءات الجزائية، إنما أعطى تصريحا للجهات القضائية باستعمال هذا الإجراء التقني في إطار الوقاية من بعض الجرائم التي يحتمل أن تشكل خطرا على أمن الدولة وهي كما حددتها المادة (04)، الأفعال الموصوفة بجرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة، وجرائم الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة أو الدفاع الوطني[213]. والمثير للانتباه أن المشرع سمح بإجراء عمليات المراقبة للاتصالات الالكترونية لأشخاص أو مجموعات بمجرد وجود احتمال تورطهم مستقبلا في ارتكاب إحدى هذه الجرائم، لان الوقاية في اعتقاده لا تفرض القيام بأعمال تحضيرية لارتكاب هذه الأفعال وإنما مجرد تكهنات أو حتى قرائن بسيطة تنبئ بان هؤلاء الأشخاص قد يقدمون على ارتكاب تلك الجرائم.

غير أن احتمال اكتشاف جريمة بنوع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال قبل وقوعها هو احتمال ضئيل جدا إن لم نقل منعدم، لأن أكثر ما يميزها أنها جرائم متبخرة (volatile) ومجردة من أية مقدمات مادية ولا تكتشف إلا مصادفة، لذلك يثار التساؤل كيف للاحتمال الوارد في نص المادة (04 فقرة ب) من القانون رقم (04/09) الذي يبرر اللجوء

---

[212]- مشار إليه لدى: عمر بن يونس، مرجع سابق، ص 582.

[213]- أنظر نص المادة (04) من القانون رقم (09-04)، مرجع سابق.

إلى المراقبة الالكترونية لمراسلات واتصالات الأفراد و انتهاك سريتها أن يتحقق، وإن كان هذا الأمر يدخل أيضا في إطار الوقاية من هذه الجرائم ؟ واعتقد أن هذا التخوف هو الذي جعل المشرع يشدد في الفقرة الأخيرة من المادة (04) أعلاه على أن تكون الترتيبات التقنية الموضوعة لمراقبة الاتصالات الالكترونية في هذه الحالة موجهة حصرا لتجميع وتسجيل معطيات ذات صلة بالوقاية من تلك الأفعال ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

وحرصا منه على تحقيق هذا المبتغى،قام المشرع الجزائري بإنشاء هيئة وطنية خاصة بموجب مرسوم رئاسي رقم(15-261) مؤرخ في 8 أكتوبر 2015، أوكل إليها بالإضافة إلى مهام أخرى، مهمة تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مع السلطات القضائية ومصالح الشرطة القضائية، بما في ذلك جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالإعمال الإرهابية والتخريب والمساس بأمن الدولة، تحت سلطة القاضي المختص، وكذا تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية.

أضف إلى ذلك أنها تتولى تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال وتحديد مكان تواجدهم[214].

[214]– للمزيد من التفاصيل حول مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، انظر المادة (05) من المرسوم الرئاسي رقم 15-261 المؤرخ 8 أكتوبر 2015، و المادة (14) من قانون 09-04 مرجع سابق.

الفرع الثاني: القيود الواردة على عملية اعتراض ومراقبة المراسلات

إذا كان أسلوب اعتراض المراسلات السلكية واللاسلكية دون علم أصحابها قد اثبت جدارته في كشف وإثبات الكثير من الجرائم الغامضة كتلك المتعلقة بالجرائم الالكترونية، فهو في الوقت نفسه يمثل انتهاكا خطيرا لحرمة الحياة الخاصة للإفراد، واعتداء صارخا على سرية مراسلاتهم واتصالاتهم التي كفلتها معظم الدساتير والتشريعات العقابية بالحماية[215]. ولتحقيق التوازن بين ضرورة التحقيق التي تفرضها المصلحة العامة واحترام الحياة الخاصة التي تفرضها المصلحة الفردية، تمت إحاطة عملية الاعتراض بعدد من القيود القانونية التي تضمن عدم تعسف السلطات العامة وتصون الحرية الفردية. والتي نلخصها فيما يلي:

أولاـ الحصول على إذن السلطة القضائية المختصة: قيد القانون اللجوء إلى عملية اعتراض او مراقبة المراسلات بشرط الحصول المسبق على إذن مكتوب ومسبب من الجهات القضائية المختصة المتمثلة عادة في وكيل الجمهورية أثناء مرحلة التحقيق الابتدائي[216]، أو قاضي التحقيق في مرحلة التحقيق القضائي و إلا كان هذا الإجراء باطلا، فالسلطة القضائية وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمـانة لازمة لمشروعية الإجراء[217].

---

[215] – نذكر منها المادة(2/46) من الدستور الجزائري لسنة 2016 التي تنص على " **سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة**" تقابلها المادة(09) من الدستور التونسي و المادة(45) من الدستور المصري و المادة 15 من الدستور الايطالي والمادة(72) من الدستور البولندي. اما عن التشريعات العقابية نذكر المادتين(303 و 303 مكرر) من قانون العقوبات الجزائري.

[216]– غير انه استثناء لهذه القاعدة عندما يتعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بأمن الدولة يكون **النائب العام لدى مجلس قضاء الجزائر هو المختص بمنح الإذن لإجراء عملية المراقبة**، أنظر(الفقرتين 6 و 7 من المادة 04) من القانون(09-04).

[217] – ورد هذا الشرط بالنسبة لعملية الاعتراض في المادة(65 مكرر 5) من قانون الإجراءات الجزائية بالشكل التالي:" **إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم ... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق**

وحتى يكون الإذن صحيحا ومنتجا لآثاره، يجب أن يتضمن جملة من العناصر الأساسية وهي:

1- طبيعة الجريمة التي تبرر الإجراء: والتي ينبغي أن تكون من ضمن الجرائم التي يجوز فيها اللجوء إلى هذه العملية[218]، وإذا اكتشفت جرائم أخرى غير تلك الوارد ذكرها في الإذن فلا تبطل الإجراءات العارضة.

2-التعريف بالعملية: بمعنى تحديد المراسلات والاتصالات المطلوب اعتراضها وتسجيلها، تحديد الأماكن المقصودة (سكنية او غير سكانية، عامة او خاصة)، إلى جانب تحديد المدة التي تستغرقها التدابير التقنية اللازمة في عملية الاعتراض، والتي يجب أن لا تتجاوز أربعة أشهر قابلة للتجديد ضمن الشروط نفسها، حسب تقدير السلطة مصدرة الإذن لمقتضيات التحري والتحقيق[219]. وهي المدة نفسها التي حددها المشرع الفرنسي في المادة (100-1) من قانون إجراءات الجزائية الفرنسي [220].

ولا يكفي الحصول على إذن مشمول بالعناصر المذكورة لإتمام عملية اعتراض المراسلات أو المراقبة، إنما لا بد أن تنفّذ هذه العمليات تحت الرقابة المباشرة للسلطات التي أذنت بها، وذلك من خلال قيام ضابط الشرطة القضائية المأذون له بإحاطتها علما بكل

وسائل الاتصال السلكية و اللاسلكية ... و في حالة فتح تحقيق قضائي تتم العملية المذكورة بناء على إذن من قاضي التحقيق و تحت مراقبته المباشرة" . أما بالنسبة لإجراء المراقبة الالكترونية نص عليه في المادة(6/04) من القانون (04/09) على النحو التالي: "... **لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطات القضائية المختصة**"

[218]- وهي الجرائم المحددة على سبيل الحصر في المادة (65 مكرر 5) من ق إ ج و المادة (04) من قانون(09-04).

[219]- استثناء لهذه القاعدة إذا تعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بآمن الدولة تكون مدة الإذن بالمراقبة الالكترونية 06 أشهر قابلة للتجديد، انظر المادة (04/ 7) من قانون(09-04).

[220] - voir l'article (100-1) de la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales, JORF , 16 nov, p 18215.

خطوات وتطورات عملية الاعتراض والمراقبة وإخبارها بشكل دوري ومستمر عن عمليات وضع الترتيبات التقنية لهذا الغرض، ساعة بداية وانتهاء هذه العمليات، على أن يدوّن كل ذلك في محاضر مرقمة[221]. وبهذه الطريقة فقط نكون قد حققنا الغرض الحقيقي من هذه العمليات.

ثانيا- تسبيب اللجوء إلى اعتراض أو مراقبة المراسلات: يقصد به المبرر الشرعي والضرورة الملحة التي تستدعى القيام بعملية اعتراض أو مراقبة المراسلات[222]، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء إلى هذه العملية، وفي هذا الشأن يشترط على وكيل الجمهورية أو قاضي التحقيق المختص قبل منح الإذن بتنفيذ العملية المذكورة تقدير جدواها وجدية دواعيها والفائدة المنتظرة منها في إظهار الحقيقة وكشف غموض الجريمة والجناة مسبقا، ثم موازنة كل هذه العناصر للتأكد مما إذا كانت كافية لخرق مبدأ حرمة الحياة الخاصة. فإذا ارتأى بان التسبيب غير كاف رفض طلب الإذن.

والجدير بالذكر هنا هو انه إلى جانب إمكانية القيام بمراقبة الاتصالات الالكترونية في إطار التحريات والتحقيقات القضائية من اجل الوصول إلى أدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء، فقد أجاز المشرع الجزائري كذلك تطويع هذه التقنية لغرض الوقاية من احتمال وقوع جرائم خطيرة قد تهدد كيان الدولة كما قررته المادة الرابعة (4) من القانون(04/09)[223]. وهنا يصبح مفهوم الضرورة الملحة التي تستدعى القيام

---

[221]– أنظر نص المادة (65 مكرر 9) من قانون الإجراءات الجزائية، تقابلها المادة (1/100 -3) من قانون الإجراءات الجزائية الفرنسي.

[222] - **MICHEL Prud'homme**, droit criminel, écoutes et enregistrements clandestins, R.D .P, N 59, Paris, 2010, p 47.

[223]– تنص المادة(1/4و2) من القانون(04/09) على انه " **يمكن القيام بعمليات مراقبة الاتصالات الالكترونية في الحالات الآتية: 1–للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة. 2– في**

بإجراءات المراقبة الالكترونية مبهما وغير واضح، خاصة إذا تعلق الأمر بالجرائم التي تهدد النظام العام لان مصطلح النظام العام غير محدد المعالم وقد تنجر عنه إخلالات كبيرة من شأنها المساس بحرية الأفراد[224].

ثالثا- تحديد الجرائم محل الاعتراض والمراقبة: إن الاستعانة بعملية اعتراض أو مراقبة المراسلات الالكترونية لغرض التحقيق غير مسموح في كافة الجرائم إنما مجال تطبيقها يتوقف عند نوع محدد فقط وهي كالتالي:

-الجرائم المذكورة على سبيل الحصر في نص المادة(65 مكرر5) من قانون الإجراءات الجزائية، وهي جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال أو الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد والجرائم الماسة بأنظمة المعالجة الآلية[225].

- الجرائم المنصوص عليها في الفقرات أ، ب، ج، د من المادة(04) من قانون (04/09) المتمثلة في الأفعال الموصوفة بجرائم الإرهاب أو التخريب، الاعتداءات على منظومة معلوماتية الماسة بأمن الدولة بما فيها تلك التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني [226]. وتجدر الإشارة إلى أن المشرع لم يحدد نوع الجرائم التي تندرج ضمن (الفقرة ج من المادة 4 أعلاه)، والتي يصعب وصول التحريات والتحقيقات القضائية الجارية في شأنها إلى نتيجة تهم هذه الأبحاث دون اللجوء إلى المراقبة الالكترونية. وهو ما يفتح المجال أمام جميع جرائم القانون العام لكي تكون محلا للمراقبة

حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة و الاقتصاد الوطني".

[224]- **BENNOUAR Abdelhakim,** op cit, p 03.

[225]- أنظر نص المادة(65مكرر 5) من قانون الإجراءات الجزائية .

[226]- أنظر نص المادة (04) من القانون(04/09).

الإلكترونية كلما كان هذا الإجراء ضروريا.

رابعا- سرية الإجراءات وكتمان السر المهني: أي ينبغي أن تنفّذ عملية الاعتراض والمراقبة في سرية تامة و دون علم أو رضا المشتبه فيه أو صاحب الأماكن، مع مراعاة عدم المساس بالسر المهني المقرر بنص المادة(45 فقرة 4) ق إ ج ج.

وينبغي التنبيه كذلك، إلى أن المشرع الجزائري لم يشر صراحة إلى كيفية وضع الأدلة المحصل من عملية اعتراض ومراقبة المواصلات (التسجيلات السمعية البصرية، البيانات الرقمية) في أحراز مختومة، مما يطرح التساؤل حول مدى اعتبارها من قبيل الأشياء المضبوطة التي تخضع لأحكام المادة(84) من قانون الإجراءات الجزائية وحكم المادة(5/45) من القانون نفسه[227]. علما بأن هذه التسجيلات والبيانات تعتبر أدلة إثبات رقمية أصلية تقتضي الشرعية الجزائية حفظها بطريقة خاصة بوضعها في أحراز مختومة تضمن عدم التلاعب والعبث فيها بالحذف أو الإضافة، وضمّها إلى ملف الإجراءات مع المحاضر التي تصف أو تنسخ محتواها للكشف عن الحقيقة.

ومن ذلك كانت الحاجة إلى فتح المشرع المجال أمام سلطات التحقيق والاستدلال للاستعانة بذوي الاختصاص سواء عن طريق تسخير كل من لديهم دراية و مؤهلات في مجال سير تكنولوجيات الإعلام والاتصال من اجل تزويدهم بالمساعدة الفنية والتقنية الممكنة لتسهيل وإنجاح أية عملية من عمليات التحقيق بما فيها المراقبة الالكترونية للاتصالات كما هو منصوص في المادة (05) فقرة أخيرة من القانون رقم(04/09) [228]. أو عن طريق تكليف هؤلاء المختصين باستعمال الوسائل التقنية المناسبة والضرورية للحيلولة دون

---

[227]– تنص المادة(84) من قانون الإجراءات الجزائرية على "... **ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة...**"

[228]–أنظر المادة (05) من القانون رقم (04/09)، مرجع سابق.

الوصول الى المعطيات التي تشكل محل الجريمة أو تحتوي أدلة لها، الموجودة داخل المنظومة المعلوماتية و منع الاطلاع عليها أو نسخها أو تهريبها أو تدميرها وفقا لما تقتضيه المادتين (7و8) من القانون رقم(04/09).

ويجب الاعتراف بأن تكريس المشرع الجزائري لإجراءات اعتراض المراسلات والمراقبة الالكترونية يعد خطوة جريئة تحسب له، على اعتبار أنها من اخطر إجراءات التحري والتحقيق عبر العالم الافتراضي نظرا لما تحمله من انتهاكات مباشرة لخصوصيات الإنسان هذا من جهة، ومن جهة أخرى لان الفقه الجنائي لم يحسم الأمر بعد ويرى بان المراقبة الالكترونية لا تزال محل نظر في القانون لضرورة الالتزام بما هو مقرر في القوانين والدساتير من ضمانات احترام الحق في الخصوصية.

المطلب الثالث

الحفظ والإفشاء العاجلان للمعطيات الإلكترونية

يعد الحفظ والإفشاء العاجلان للمعطيات المعلوماتية بالنسبة لغالبية الدول إجراءين جديدين للبحث والتحري في مجال مكافحة الجرائم الالكترونية، وقد تمت الإشارة إليهما لأول مرة في لائحة الجمعية العامة لمنظمة الأمم المتحدة رقم (65-63) المؤرخة في 22-01-2001 المتعلقة بمكافحة إساءة استعمال تكنولوجيا المعلومات لإغراض إجرامية، إذ نصت في المادة (01 الفقرة "و") على ضرورة سماح الدول الأعضاء لجهاتها المختصة بالاستدلال أمر مزودي خدمات الاتصالات القيام بالحفظ السريع للمعطيات الالكترونية المتعلقة بالتحقيقات الجنائية[229].

[229] -**BOSSAN Jérôme** « le droit pénal confronté a la diversité des intermédiaires de l'internet » édition Dalloz, 2013, p 302.

وبعدها تضمنت اتفاقية بودابست لمكافحة الجرائم الالكترونية لعام 2001 إجراءي الحفظ والإفشاء على البيانات المخزنة في نظم المعلوماتية، وألزمت الدول الموقعة على الاتفاقية من خلال المادتين(16 و 17) باتخاذ الإجراءات التي ترى أنها ضرورية من أجل السماح للسلطات المختصة بأن تأمر بالحفظ والإفشاء العاجلين على المعطيات المعلوماتية المخزنة، بما فيها المتعلقة بالمرور، والمخزنة بواسطة نظام معلوماتي، وعلى وجه الخصوص عندما تكون هناك أسباب تدعو للاعتقاد بتعرض تلك المعطيات للفقدان أو التلف[230].

واسترشادا بذلك تضمن القانون الجزائري رقم(04/09) الخاص بالوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وبالتحديد في المادة (10) عددا من الالتزامات تفرض على مزودي خدمات الانترنت بتقديم المساعدة بخصوص العمليات التي ينجزونها للسلطات المكلفة بالبحث والاستدلال لأغراض التحقيق من بينها: حفظ المعطيات المعلوماتية المتعلقة بالسير ووضعها تحت تصرف القائمين بالتحقيق[231]. وهو ما سنحاول التفصيل فيه من خلال دراسة هاذين العنصرين في الفرعين التاليين:

---

[230]- Article (17) – conservation et divulgation rapide de données relatives au trafic :

1- afin d'assurer la conservation des données relatives au trafic, en application de l'article 16 chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires ;

1-pour veiller a la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé a la transmission de cette communication ; et

2-pour assurer la divulgation rapide a l'autorité compétente de la partie, ou a un personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la partie des fournisseurs de services et la voie par laquelle la communication a été transmise… » .

[231]– تنص المادة (10) من القانون (09-04) على ما يلي :" **في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ... و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة...**".

الفرع الأول: الحفظ العاجل لمعطيات السير

سنتناول في هذا العنصر مفهوم الحفظ العاجل لمعطيات السير (أولا) ثم ضمانات المتهم أثناء هذه العملية (ثانيا).

أولا- مفهوم الحفظ العاجل لمعطيات السير: اعتماد على ما سبق ذكره يمكن اعتبار الحفظ على المعطيات الالكترونية بأنه قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل قصد تمكين جهات الاستدلال من الاستفادة منها واستعمالها لأغراض التحقيق[232].

فعملية الحفظ إذا هي من مهام مقدمي الخدمات[233]، الغرض منها حماية المعطيات التي سبق وجودها في شكل مخزن من كل ما يمكن أن يتسبب في إتلافها أو تجريدها من صفتها أو حالتها الأصلية. ولا تهم الطريقة التي يتم من خلالها الحفظ على المعطيات الالكترونية ولا الوسيلة القانونية المقررة لذلك، فالأمر متروك لكل دولة لتقدير النماذج التي تراها ملائمة لوضع عملية الحفظ موضع التنفيذ[234].

---

[232]- **بوكر رشيدة**، مرجع سابق، ص 448.

[233]- عرفت الفقرة (د) من المادة (02) من القانون(04/09) مقدم او مزود الخدمة بأنه: " 1- **أي كيان عام او خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام الاتصال. 2- و أي كيان آخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها**". و قد عرفته اتفاقية بودابست 2001 لمكافحة الجرائم الالكترونية في المادة الأولى فقرة (ج) بأنه: " **كل من يقوم بخدمات الإيصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، و قد يكون جهة عامة أو جهة خاصة، و قد يقدم خدماته للجمهور أو مجموعة من المستخدمين الذين يشكلون مجموعة مغلقة**".

[234]- هذا ما يستشف من عبارة " **يأمر أو ...يحصل بطريقة مشابهة** " المذكورة في المادة(16) من اتفاقية بودابست 2001 والتي تفتح المجال للدول لاستعمال كل الوسائل القانونية المتاحة للتحفظ على المعطيات الالكترونية سواء كانت وسائل قضائية كالأمر القضائي، أو إدارية . فمثلا في الدول التي لم ينص قانونها على ضرورة الحصول على أمر قضائي

وينبغي التنويه في هذا الإطار إلى أن عملية الحفظ هنا لا تخص كل المعطيات الالكترونية بمختلف نماذجها[235]، إنما تخص معطيات المرور فقط أو كما يسميها البعض حركة السير، التي عرفتها المادة الأولى فقرة "د" من اتفاقية بودابست بأنها " **صنف من بيانات الحاسب التي تشكل محلا لنظام قانوني محدد، إذ يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة** ". وعرفها كذلك المشرع الجزائري في المادة(02) الفقرة الأخيرة من القانون رقم (04/09) بأنها " **أية معطيات متعلقة بالاتصالات عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات، توضّح مصدر الاتصال، الوجهة المرسلة إليها، والطريق الذي يسلكه، ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة** "[236].

إلا انه بالنظر لنص المادة (10 فقرة 1) من القانون (04/09) فان المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتوى الاتصالات بشرط أن يكون في حينه، وهو إجراء تسخير من طرف السلطات القضائية لمقدمي الخدمات المعنيين لجمع وتسجيل المعطيات المتعلق بمحتوى اتصالات أيا كانت (محادثات هاتفية أو مكالمات فيديو عبر مواقع الانترنت أو مراسلات كتابية على شكل SMS أو MMS) . ولكن لم يحدد المشرع الجزائري على عكس مثيله الفرنسي لا مدة تسجيل هذه الاتصالات ولا الأشخاص المسموح لهم بتسخير مقدمي الخدمات للقيام بهذا الإجراء الخطير وترك المجال مفتوحا للاجتهاد، بينما سمح المشرع الفرنسي بموجب المادة (2/60فقرة 2) من قانون الإجراءات الجزائية لضباط

للقيام بعملية التحفظ، فيجوز فيها القيام بهذه العملية بناء على أمر واحد مع عملية التفتيش والضبط أو بناء على أمر بإنتاج المعطيات.

[235]– نشير إلى انه توجد عدة أنواع للمعطيات المعلوماتية محل التحري و التحقيق الجزائي فمنها : معطيات متصلة بالمرور ، معطيات المحتوى، و معطيات المشترك. أنظر: **هلال عبد أللاه أحمد**، مرجع سابق، ص.ص 198–199.

[236]– أنظر المادة(02) الفقرة الأخيرة من القانون (04/09)، مرجع سابق.

الشرطة القضائية بتسخير من وكيل الجمهورية مع ترخيص مسبق من طرف قاضي الحريات والحبس، بتكليف مقدمي الاتصالات عبر الانترنت للقيام بكل الإجراءات التي تؤمن الحفظ لمدة لا تزيد عن سنة واحدة لمحتويات البيانات المتعلقة بمستعملين للخدمات [237].

ومن ضمن معطيات المرور التي يتعين على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية المختصة لأغراض التحقيق، تلك التي حددها المشرع الجزائري في المادة (11) من القانون(04/09) على النحو التالي:

ـ المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ـ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال (كرقم التسلسلي لجهاز الاتصال، و نوعه).

ـ الخصائص التقنية وكذا تاريخ و وقت و مدة الاتصال.

ـ المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

ـ المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم (كأرقام الهاتف مثلا او عناوين بروتوكول الانترنت ، تحديد مكانهم...).[238]

وإذا كان تحديد معطيات المرور قد يبدو أمرا سهلا عندما تكون تلك المعطيات مرتبطة بمقدم خدمة واحد، فالأمر غير ذلك عندما ترتبط بأكثر من مقدم خدمة، فغالبا ما يساهم عدد من مقدمي خدمات في نقل اتصال معين، ويحتفظ كل واحد منهم بجزء من معطيات المرور أو بعض أجزاء اللغز، مما يجعل تحديد مصدر هذا الاتصال ومنتهاه أمرا لا يستقيم إلا بجمع كل هذه الأجزاء و ضمها بعضها إلى البعض و اختبارها[239].

---

[237]– **أحمد مسعود مريم**، مرجع سابق، ص 101.

[238]– أنظر المادة (11) من القانون (04/09).

[239]– **فايز محمد راجح غلاب**، مرجع سابق، ص 427.

لذلك عندما ترتبط معطيات المرور بأكثر من مقدم خدمة فالحفظ العاجل لهذه المعطيات يتم من خلالهم جميعا، سواء بناء على أمر منفصل لكل مقدم خدمة على انفراد، أو أمر واحد يشملهم جميعا يتم إخطارهم به بالتعاقب، أو بناء على أمر يضمّ كل مقدمي الخدمات، ثم يطلب من كل مقدمي خدمة يصله الأمر بالحفظ، أن يقوم بإخطار من يليه بفحوى هذا الأمر وهكذا[240].

ثانيا- ضمانات المشتبه فيه أثناء عملية حفظ معطيات السير: نظرا لتعارض عملية التحفظ على المعطيات الالكترونية مع الحق في الخصوصية فقد قيّدها القانون بجملة من الشروط و الالتزامات التي وضعها على عاتق مقدمي الخدمات أو أي كيان آخر يقع عليه عبئ الحفظ و هي كالتالي:

1-احترام المدة المقررة لعملية الحفظ : تعتبر عملية الحفظ تدبيرا مؤقتا يتم اللجوء إليه بموجب أمر توجهه السلطات المختصة إلى مقدم خدمات الاتصال تلزمه بالحفظ على البيانات الالكترونية فترة معينة من الزمن و وضعها تحت تصرفها لغرض التحقيق، وتحديد مدة الحفظ يسمح بتعجيل إجراءات المتابعة الجزائية إن كان لها محل، لذلك تختلف هذه المدة من دولة إلى أخرى حسب الحاجة، فقد قدرتها اتفاقية بودابست ب(90 يوما) كحدّ أقصى تبدأ من تاريخ التسجيل وقابلة للتجديد حسب تقدير السلطات المختصة[241]، في حين حدد المشرع الجزائري مدة الحفظ بسنة واحدة وهو ما يستفاد من المادة (11) من القانون رقم (04/09) التي تنص على أن "... **تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل...**". وهي المدة ذاتها التي اقرها المشرع الفرنسي من خلال المادة (32-3- L1) من قانون البريد والاتصالات الالكترونية المعدلة بالمادة(20)

---

[240]-أنظر: **هلالي عبد أللاه أحمد**، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية...، مرجع سابق، ص 208.

[241] - Art (16 -2) stipule que ; « … cette partie adopte les masures législatives et autre qui se révèlent nécessaires pour obliger cette personne a conserver et protéger l'intégrité desdites données pondent un duré aussi longe que nécessaire, jusqu' a maximum 90 jours, … »

من القانون رقم (2003-239) المؤرخ في 18 مارس 2003 المتعلق بالأمن الداخلي[242].

ومباشرة بعد انقضاء المدة المقررة لعملية الحفظ يجب على مزود الخدمة التدخل فورا لسحب وإزالة كل المعطيات التي تم تخزينها أو على الأقل وضع ترتيبات تقنية تضمن عدم إمكانية الاطلاع على هذه المعطيات حفاظا على سريتها وخصوصيتها وإلا تعرض لعقوبات إدارية[243]، وأخرى جزائية قد تصل إلى عقوبات سالبة للحرية[244]. بل انه عندما يؤدي إخلاله بالالتزامات المذكورة إلى عرقلة حسن سير التحريات القضائية. فان ذلك يعرضه للعقوبة المقررة في نص المادة(11) فقرة الأخير من القانون(04/09) وهي الحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من50.000دج الى 500.000دج[245] .

2- الالتزام بكتمان سرية عملية التحفظ و المعلومات المتصلة بها: بالإضافة إلى ضرورة احترام المدة المقررة لعملية الحفظ العاجل لمعطيات السير، يلتزم كذلك مقدمو الخدمات بالحفاظ على سرية كل الإجراءات والتدابير التي تفرضها هذه العملية طيلة المدة المقررة لها. ولعل الغرض من فرض هذا الالتزام هو ضمان حماية الحق في الخصوصية من جهة، وتجنّب إحداث تغييرات في البيانات أو محوها من طرف أشخاص آخرين من

---

[242] - Art (L 32-3-1) Alinéa 2 du C.P.T.E.F stipule32-3-1 Alinéa 2 du C.P.T.E.F stipule que : « … et dans le seul but de permettre, en tant que de besoin, la mise a disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un ans aux opérations tendant a effacer ou a rendre anonymes certaines catégories de données techniques »

[243]- المعروف عند معظم الدول أن مقدمي خدمات الاتصالات الالكترونية والانترنت يخضعون في ممارسة نشاطهم إلى نظام الترخيص المسبق من الهيئات الإدارية المختصة، لذلك فان عدم التزامهم بمسح المعطيات المخزنة بعد انقضاء الفترة المقررة لعملية التحفظ من شانه أن يعرضهم إلى عقوبة إدارية تتمثل في سحب الرخصة . أنظر في هذا الشأن نص المادة 394مكرر6 من قانون العقوبات الجزائري، مرجع سابق.

[244] - Art (39 -3 Alinéa 1) du C.P.T.E dispose que : « Est puni d'un an d'emprisonnement et de 75000 euros d'amende le fait pour un operateur de télécommunications ou ses agent ; 1-De ne pas procéder aux opérations tendant a effacer ou a rendre anonymes des données relatives aux communications dans les cas ou ces opérations sont prescrites par la loi … ».

[245]- انظر المادة (11) من القانون رقم (04/09)

جهة أخرى. وقد تطرقت اتفاقية بودابست لهذا الالتزام في المادة (3/16) التي نصت على أنه "... **يجب على كل طرف اتخاذ الإجراءات التشريعية أو أية إجراءات ضرورية لإجبار حائز البيانات، أو أي شخص يقع عليه عبئ حفظها، أن يحافظ على السرية بالنسبة لتطبيق الإجراءات التي تتم خلال المدة المقررة...**". وعلى غرار هذا النص حرص المشرع الجزائري بدوره على ضرورة تحلي مزودي الخدمات بكتمان سرية عملية الحفظ وكذا سرية المعطـيات المخزنة طيلة فتـرة الاحتفـاظ بهـا، وعدم الإفشـاء بهـا إلا لسلطـات التحقيـق المختصة، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق[246].

واسترشادا بما سبق فتقيد مزودي الخدمات بالالتزامات المذكورة أعلاه أثناء عملية حفظ المعطيات الالكترونية يجعلهم سندا مهما لجهات التحري والتحقيق في الحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها وملزمين في الوقت نفسه بـوضعها تحت تصرف هذه الجهات إذا ما طلبتها.

الفرع الثاني: الإفشاء العاجل لمعطيات السير

يعد هذا الإجراء من الالتزامات المترتبة على مقدمي خدمات الانترنت في إطار مساعدة السلطات المكلفة بالبحث والتحقيق في الجرائم الالكترونية، فهي عملية مكملة لإجراء الحفظ العاجل لمعطيات المرور، كما أوضحت اتفاقية بودابست بنصها في المادة (17) بأنه " على كل طرف اتخاذ الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل: أ- التأكد من أن الحفظ العاجل لهذه المعطيات المتعلقة بالمرور في تطبيق المادة (16) متوافر،...

---

[246]- تنص المادة (2/10) من القانون(04/09) على ما يلي: " ... **و يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين و كذا المعلومات المتصلة بها و ذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق** ".

ب-ضمان الإفشاء السريع(divulgation rapide) للسلطة المختصة، أو الشخص المعين من قبلها، عن كمية معطيات المرور الكافية التي تسمح بتحديد هوية مقدمي الخدمات، والمسار الذي تم الاتصال من خلاله"[247].

فبالعودة إلى نص هذه، نجدها تنشئ التزامين على عاتق مقدمي خدمات الانترنت، يتعلق الالتزام الأول بالحفظ العاجل لمعطيات المرور المشار إليها في المادة (16)، ثم يلي هذا الالتزام التزاما آخر يكمله وهو الإفشاء العاجل للسلطات المختصة بالتحقيق عن بعض هذه المعطيات، التي تفيد الكشف عن هوية مقدمي الخدمات الآخرين الذين ساهموا في نقل الاتصال.

وقد تبنى المشرع الجزائري بدوره إجراء الإفشاء العاجل لمعطيات السير لغرض التحقيق وجعله التزاما على عاتق كل مقدمي الخدمات، وذلك من خلال نصه في المادة (10) من القانون (09-04) على انه: " **في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ...** و **بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) أدناه، تحت تصرف السلطات المذكورة...**"[248].

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

---

[247]- أنظر نص المادة (17) من اتفاقية بودابست حول مكافحة الجرائم المعلوماتية لعام 2001، مرجع سابق,

[248]- أنظر نص المادة (10) من القانون(09-04) المؤرخ في 05- 8- 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

الاتصال ومصبه، وهي المعلومات التي قد تقوده إلى معرفة هوية الأشخاص المتورطين في ارتكاب الجريمة الالكترونية. وتجدر الإشارة هنا إلى انه عند اللجوء لتلك الإجراءات يجب مراعـــاة الحدود والضمانـات القانونية المتعلقة بالخصوصية، وحقوق وحريات الإنسان بشكل عام، بما يحقق التوازن بين إقامة العدالة و المحافظة على تلك الحقوق[249].

ومما يحسب على هذا الإجراء رغم أهميته البالغة في عملية البحث و التحري في الجرائم الالكترونية، و رغم أن أي إخلال به من قبل مقدمي الخدمات يرتب مسؤوليتهم الجزائية،[250] هو أن مقدمي الخدمات قد لا يبدون تعاونا جديا مع السلطات المختصة بالتحقيق بسبب انعدام الثقة بين بعضهم البعض، و من ثم لا يكون هذا الإجراء فعالا ومفيدا بالشكل المطلوب.

المطلب الرابع

إنتـاج المعطيـات المعلوماتـية

إن عملية إنتاج المعطيات المعلوماتية هو إجراء يفرضه القانون على مقدم خدمات الانترنت يلتزم من خلاله بموافاة السلطات المختصة بالبحث والتحقيق بكل المعطيات أو البيانات المعلوماتية المتعلقة بالمشتركين وخدماتهم، غير بيانات المرور أو المحتوى، الموجودة بحوزته أو تحت سيطرته، من أجل استعمالها لأغراض التحقيق.

---

[249]– هذا ما نصت عليه الفقرة الأخيرة من المادة(17) من اتفاقية بودابست بالشكل التالي : " ... **ويشترط لتطبيق السلطات و الإجراءات المشار إليها أعلاه أن تكون خاضعة للمادتين (14 و 15) من الاتفاقية**".

[250] – تنص الفقرة الأخيرة من المادة (11) من القانون(04/09) على " ... **دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين و المعنويين عندما يؤدي ذلك الى عرقلة حسن سير التحريات القضائية، و يعاقب الشخص الطبيعي بالحبس من 6 أشهر إلى 5 سنوات و لغرامة من 50.000دج إلى 500.000دج. و يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات** "

وقد تناولت اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية هذا الإجراء ضمن الإجراءات المستحدثة في مجال البحث و التحقيق عن الجرائم الالكترونية في المادة(18) منها تحت عنوان " **الأمر بإنتاج معطيات معلومات L'injonction de produire**" أوجبت على كل طرف في الاتفاقية تبني الإجراءات التشريعية و إجراءات أخرى التي يراها ضرورية من اجل تأهيل سلطاته المختصة بأن تأمر:

أـ كل شخص على أرضه بإرسال معطيات معلوماتية معينة في حوزته أو تحت سيطرته، والمخزنة في نظامه ألمعلوماتي، أو في دعامة تخزين معلوماتية.

ب ـ كل مزود خدمات الذي يقدم خدماته على ارض ذلك الطرف من اجل إرسال المعطيات المتعلقة بالمشتركين و خدماتهم التي في حوزته أو تحت سيطرته [251].

بالنظر لنص هذه المادة، يتبين بأن الاتفاقية تحث الدول الأطراف على فرض من خلال قوانينها الداخلية وسائل وتجهيزات أخرى للتحقيق في الجرائم الالكترونية تكون اقل انتهاكا لحقوق الأفراد وخصوصيتهم من إجراءات التفتيش والضبط، وذلك بهدف الحصول على معلومات ضرورية تفيد التحقيق. ومن بين هذه الوسائل، الأمر بإنتاج معطيات معلوماتية باعتباره إجراء مرنا يسمح للسلطات بان تضعه موضع التنفيذ في حالات كثيرة، لا سيما تلك الحالات التي لا تستلزم بالضرورة اللجوء إلى إجراء أكثر إجبارا، أو أكثر تكلفة[252]. بالإضافة إلى أن هذا الإجراء لا ينطبق إلا على الشخص أو مقدم الخدمات الذي تكون البيانات المراد الحصول عليها بحوزته أو تحت سيطرته دون غيره.

واعتبار لما سبق، فعلى كل طرف في الاتفاقية بمقتضى البند "أ" من المادة السالفة الذكر أن يمنح سلطاته المختصة، صلاحية توجيه أمر لشخص، أو لمقدم خدمات الانترنت

---

[251]ـ أنظر نص المادة (18) من اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية، مرجع سابق.

[252]- voir : la convention sur la cybercriminalité, STE no 185, rapport explicatif, adopté le 8 novembre 2001, pp 52

على إقليمه بان يرسل معطيات أو معلومات الكترونية معينة مخزنة في نظام معلوماتي، أو دعامة تخزين الكترونية موجودة بحوزته أو تحت سيطرته لغرض البحث والتحقيق.

والمقصود هنا بعبارة " **في حيازة أو تحت السيطرة** " هو الحيازة المادية للمعطيات والبيانات المعنية داخل حدود هذا الطرف، أو البيانات التي لا تكون في الحيازة المادية للشخص ولكن بمقدوره السيطرة عليها، من خلال مرورها داخل حدوده، ومثال ذلك: الشخص الذي يتلقى أمرا بإنتاج وتقديم البيانات المخزنة لحسابه عن بعد، عن طريق الخدمة الفورية للتخزين عن بعد، فانه يتعين عليه الامتثال للأمر ويقوم بإظهار هذه البيانات [253].

ولا يندرج في سياق عبارة " **السيطرة**" الواردة في نص المادة(18) سالفة الذكر قدرة الشخص على الولوج داخل شبكة الانترنت للوصول إلى بيانات مخزنة عن بعد، دون أن تكن تحت سيطرته القانونية.

كما يلتزم كل طرف في الاتفاقية بمقتضى البند "ب" من المادة نفسها بأن يرخّص لسلطاته المختصة صلاحية توجيه أمر لأي مقدم خدمات الانترنت ينشط على إقليم ذلك الطرف من أجل إرسال البيانات والمعلومات المتعلقة بالمشترك والتي تكون في حيازته، حيازة مادية أو عن بعد بواسطة شركة أخرى تقدم مثل تلك الخدمات، أو تكون تحت سيطرته.

ويشترط في المعطيات المطلوب تقديمها، أن تكون متصلة بالمشتركين وخدماتهم، وينصرف مصطلح مشترك إلى العديد من فئات زبائن مقدمي الخدمات، فقد يكون الشخص الذي يدفع مقابل الخدمة، أو العميل الذي يدفع مقدما نظير الخدمات التي يستعملها، كما قد يكون الشخص الذي يستخدم الخدمات مجانا، الذي يستخدم حساب المشترك[254].

---

[253]– **هلالي عبد ألاه أحمد**، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية ...، مرجع سابق، ص216

[254]– **فايز محمد راجح غلاب**، مرجع سابق، ص 431.

ويقصد بالمعطيات المتعلقة بالمشتركين وخدماتهم هنا، كل البيانات المتعلقة باستخدام الخدمة و مستخدمها، فأما الصنف الأول المتعلق باستخدام الخدمة، فتتمثل في أية معلومات عدا بيانات المرور والمحتوى، التي تسمح بالتعرف على نوع خدمة الاتصال المستخدمة، والجوانب الفنية المتصلة بها، كرقم الهاتف، أو عنوان موقع الويب، اسم المجال، أو عنوان البريد الالكتروني، وكذا نوع معدات الاتصال المستخدمة من طرف المشترك، مثل أجهزة الهاتف، أو مراكز المكالمات، أو الشبكات المحلية والفترة التي من خلالها اشترك الفرد في الخدمة[255].

أما الصنف الثاني المتعلق بالمستخدمين أو المشتركين فهو كما حددتها الفقرة (03) من المادة(18) سالفة الذكر يشمل كل المعلومات باستثناء بيانات المرور أو المحتوى، التي من خلالها يتم تحديد هوية المستخدم، عنوانه البريدي أو موطنه، رقم هاتفه، رقم الولوج، والبيانات المتعلقة بدفع الفاتورة والمبلغ المدفوع، والمتوفرة على أساس عقد أو اتفاق تقديم خدمة، وكذلك أية معلومات أخرى تتعلق بموقع تجهيزات الاتصال، المتوفرة على أساس عقد او اتفاق تقديم خدمة التي تفيد في البحث والتحقيق[256].

---

[255]–**هلالي عبد أللاه احمد**، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 221

[256]-L' Art (18- 03) stipule : « aux fins de présent article, l'expression (données relatives aux abonnées) désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnées de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir ;

A- le type de service de communication utilisé, les dispositions techniques prise a cet égard et la période de service .

B- l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponible sur la base d'un contrat ou d'un arrangement de services ;

C- toute autre information relative a l'endroit ou se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

ومع ذلك، يجب عدم تفسير هذه المادة على أنها تفرض على مقدمي الخدمات الاحتفاظ بالمعطيات أو البيانات المتعلقة بالمشتركين، أو التحقق من صحة هذه المعطيات أو البيانات، فهم غير ملزمين بتسجيل معلومات عن هوية المستخدمين فيما يتعلق ببطاقة الدفع المسبق لخدمات الهاتف المحمول مثلا، كما لا يلتزمون بالتأكد من هوية المشتركين إذا ما كانت حقيقية أم مستعارة.

والجدير بالذكر انه رغم أهمية عملية إنتاج البيانات المعلوماتية في التحقيق والبحث عن الجرائم الالكترونية، باعتباره إجراءا جديد يتناسب وطبيعة الدليل المعلوماتي، وتقتضيه السرعة المطلوبة التي يفرضها الحفاظ على الأدلة الالكترونية من التلاعب، إلا أن المشرع الجزائري مثله مثل معظم دول العالم اغفل النص على هذا الإجراء ضمن إجراءات التحري المستحدثة، وعليه ينبغي التنبيه إلى هذا الفراغ والعمل لتدارك الوضع مستقبلا .

المطلب الخامس

تجميع معطيات المرور في وقتها الفعلي

يقصد بإجراء تجميع معطيات المرور المتعلقة بالاتصالات الالكترونية في وقتها الفعلي(La Collecte en temps reel des données relatives au trafic)، قيام مقدّم خدمات الانترنت بناءا على طلب سلطات البحث والتحقيق بتسجيل بيانات أو معلومات اتصال معين في فترة الإنتاج ونسخ صورة منها ثم تجميعها لحظة النقل عبر الاتصال[257]. وتتم عملية تجميع البيانات هنا بصفة غير مادية أي في شكل ذبذبات صوتية أو الكترونية دون أن يؤثر ذلك على حركتها أو تنقلها أو يعيق وصولها إلى المرسل إليه.

[257]– أنظر: **هلالي عبد ألاله احمد**، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، مرجع سابق، ص 248.

ولا مراء في أن إجراء التجميع في الوقت الفعلي يخص معطيات المرور دون سواها من المعطيات، والتي تتمثل كما أسلفت الذكر في كل البيانات المتعلقة بالاتصالات المارّة عبر نظام معلوماتي، والتي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال، كبيانات مصدر الاتصال ومقصده، خط سيره، ساعة وتاريخ الاتصال، حجم و مدة الاتصال[258].

فكما هو معلوم أن بيانات المرور تكون غالبا غير متاحة وليست صالحة للاستعمال وقت حدوث الاتصال، لأن الشخص المشتبه فيه المتدخل بطريقة غير قانونية قد يعدل مسار اتصاله في كل لحظة من اجل طمس أثاره، وهنا يظهر دور إجراء التجميع في الوقت الفعلي للبيانات المتعلقة بالمرور في الكشف عن مصدر الاتصال ومساره بين الضحية والجاني، بما يسمح بإجراء مقارنات بين ساعة وتاريخ ومصدر ومآل اتصالات المشبه به، وساعة وتاريخ التدخلات غير القانونية في منظومة الضحايا، وهوية الضحايا الآخرين، أو بيان روابط مع شركاء آخرين.

وقد تعرضت اتفاقية بودابست 2001 في المادة(20) منها لإجراء جمع معطيات المرور في وقتها الفعلي كإجراء جديد مفيد للبحث والتحري في الجرائم الالكترونية، وطلبت من الدول الأطراف الأخذ به عن طريق التقيد بالالتزامات التالية:

أولا- تبني الإجراءات التشريعية وأية إجراءات أخرى يرى كل طرف انها ضرورية من اجل تخويل سلطاته المختصة بالتحقيق سلطة:

أ-تجميع او تسجيل عن طريق وسائل فنية موجودة على أرضه.

---

[258]- أنظر في هذا الخصوص نص المادة(01) من اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية، مرجع سابق.

ب-إجبار مقدم الخدمات في إطار قدراته الفنية على :

1-أن يجمع أو يسجل عن طريق تطبيق وسائل فنية موجودة على أرضه .

2-أن يعطي السلطات المختصة عونه و مساعدته من اجل جمع أو تسجيل في الوقت الفعلي لمعطيات المتعلقة بالمرور مصحوبة باتصالات معينة منقولة على أرضه عن طريق نظام معلوماتي.

ثانيا- عندما لا يكون في مقدور أي طرف، تبني المبادئ المذكورة في الفقرة "1" بند (أ) بسبب القواعد الخاصة بنظامه القانوني الداخلي، فانه بدلا من ذلك، يتبني الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من اجل التأكد من تجميع أو تسجيل المعطيات المتعلقة بالمرور مصحوبة باتصالات معينة منقولة على أرضه عن طريق تطبيق طرق فنية موجودة على هذه الأرض[259].

وبمقتضى هذه المادة، يجب الربط بين البيانات المتعلقة بالمرور واتصالات معينة منقولة أو تتم على ارض الطرف المعني بالأمر أو صاحب الشأن، ومن اللافت للنظر ان هذه المادة تتحدث عن "**الاتصالات**" المحددة بصيغة الجمع، مما يؤكد ضرورة جمع بيانات المرور الخاصة بعدة اتصالات لكي يتم تحديد مصدر هذه الاتصالات ومنتهاها، ولا يعني ذلك التتبع أو الجمع أو التسجيل الشامل والمطلق لكميات هائلة من بيانات المرور بهدف الوصول إلى مصدر اتصالات معينة، إنما يجب أن تقتصر عملية الجمع والتسجيل على بيانات المرور المفيدة في كشف الأنشطة الإجرامية[260].

ويقع الالتزام بجمع وتسجيل بيانات المرور على عاتق السلطات المختصة في دولة الطرف، ولها أن تقوم بذلك بنفسها باستخدام وسائل فنية موجودة على أرضها، أو عن

---

[259]- أنظر نص المادة (20) من اتفاقية بودابست لمكافحة الجرائم المعلوماتية، مرجع سابق.

[260]- **فايز محمد راجح غلاب**، مرجع سابق، ص 435.

طريق إجبار مقدم الخدمات على جمع او تسجيل بيانات المرور، أو تقديم لها يد المساعدة والعون من اجل الجمع والتسجيل لتلك البيانات، بشرط أن يكون ذلك في حدود الإمكانات الفنية المتاحة لدى مقدم الخدمات[261]. مع الإشارة الى أن المادة 20 أعلاه لم تحدد الترتيبات التقنية أو التكنولوجية التي يجب استخدامها في عملية التجميع، ولا أية التزامات بالنسبة للشروط الفنية.

وفي كلتا الحالتين يجب أن يتم تنفيذ إجراءات الجمع والتسجيل لبيانات المرور في الوقت الفعلي في حدود النطاق الإقليمي للسلطة، كما يجب أن تكون البنية التحتية والتجهيزات التي يقيمها مقدم الخدمة لتطبيق تلك الإجراءات موجودة على ارض الطرف صاحب الشأن، ولا يهم بعد ذلك أن تكون هذه البنية والتجهيزات مقامة في موقع آخر غير الموقع الذي يمارس فيه مقدم الخدمات نشاطه الرئيسي.

ويكون الاتصال على أرض الطرف بمفهوم هذه المادة، إذا كان أحد المتصلين يتواجد على هذه الأرض، أو إذا كان الكيان المادي للحاسب الآلي أو معدات الاتصال عن بعد التي يتم من خلالها الاتصال تتواجد على هذه الأرض[262].

وغني عن البيان أن عملية جمع البيانات المتعلقة بالمرور لا تكون ذات جدوى إلا اذا تمت في غفلة عن الأشخاص الذين تنفذ العملية حيالهم، ولكن مقابل ذلك يجب على مقدمي الخدمات وموظفيهم الحفاظ على سرية البيانات محل الجمع حتى يتم تنفيذ الإجراء بفعالية، ولتحقيق ذلك ينبغي على أي طرف إدراج في قانونه الداخلي عقوبات ضد كل من يقوم بإفشاء سرية هذه العملية.

---

[261]– **هلالي عبد ألاه أحمد**، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص 248.

[262]– المرجع نفسه، ص 264.

وتجدر الإشارة في هذا الشأن إلى أن المشرع الجزائري اغفل النص على إجراء التجميع في الوقت الفعلي لمعطيات المرور ونص على الجمع في الوقت الفعلي لمعطيات الخاصة بالمحتوى ، وأتاح من خلال المادتين (03 و 10) من القانون(09-04) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها للسلطات المكلفة بالتحقيق القضائي إمكانية وضع ترتيبات تقنية لتجميع وتسجيل محتوى الاتصالات الالكترونية في حينها، وإمكانية إلزام مقدمي الخدمات الانترنت بان يوفيهم بكل المساعدات الممكنة لغرض جمع و تسجيل محتوى هذه الاتصالات في حينها[263].

وفصل الحديث، أنه رغم المخاوف الكثيرة التي أبداها الفقه حيال إجراءات التحقيق المستحدثة لما تحمله من عدوان على الحق في الخصوصية الذي يعد من أقوى الحقوق الدستورية الفردية، إلا أن الواقع يثبت بأن الاستعانة بهذه الإجراءات أصبح ضرورة ملحة للتصدي الفعال لظاهرة الإجرام ألمعلوماتي. والضرورة هنا ترجع من الناحية إلى الارتفاع المتزايد لمعدل الإجرام الالكتروني نتيجة اقتحام المعلوماتية كل مجالات الحياة، ومن ناحية أخرى إلى ثبوت عجز وقصور تقنيات التحقيق التقليدية في مواجهة الجرائم الالكترونية الحديثة نتيجة عدم ملائمتها مع الطبيعة الخاصة لهذه الجرائم.

[263]– أنظر المادتين (03) و (10) من القانون رقم (09-04) المؤرخ في 05 أوت 2009، التضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها، مرجع سابق.

الفصل الثاني

القيمة الثبوتية للدليل الإلكتروني أمام القضاء الجزائي

إن الهدف الأساسي من إتباع السلطات المختصة إجراءات التحقيق المختلفة في الدعوى الجزائية هو الوصول إلى دليل مشروع يثبت الجريمة و ينسبها إلى الجاني، لذلك فموضوع التحقيق والإثبات أمران متلازمان، فالأول يدرس وسيلة التحقيق. أما الثاني فهو غاية التحقيق وأي شيء يؤثر في احدهما ينعكس مباشرة و بصفة آلية على الآخر.

اعتبارا لذلك، فبقدر ما أثرت ثورة تقنية المعلومات وما صاحبها من جرائم جديدة غير مألوفة من قبل على إجراءات البحث والتنقيب التقليدية التي تضمنتها التشريعات الجزائية الإجرائية كما أسلفنا الذكر، إذ جعلها تفقد جدواها وفعاليتها في التصدي لمثل هذه الجرائم وملاحقة مرتكبيها، فإنها أثرت كذالك على وسائل الإثبات الجنائي، إذ أصبحت الأدلة التقليدية بدورها غير قادرة على إثبات هذا النوع من الجرائم ذات طبيعة فنية وعلمية خاصة، والذي يحتاج إلى وسائل إثبات جديدة تتناسب مع طبيعته، وتصلح لأن تتطور بتطوره ومواكبته حتى تقوى على إثباته، وهو ما يسمى بالأدلة الالكترونية أو الرقمية.

ونظرا لتزايد الجرائم المعلوماتية نتيجة الاستخدام المفرط لتقنية المعلومات في مختلف مجالات الحياة العامة، فان ذلك أدى إلى اتساع نطاق الدليل الالكتروني إذ أصبحت الأجهزة الالكترونية من حواسب، هواتف ذكية، كاميـرات، وشبكات الاتصـالات الرقمية تشكل مستودعا مهما للمعلومات والبيانات التي من شانها أن تدعم جهود تحقيق العدالة الجنائية.

ونظرا للخصائص والمميزات الاستثنائية التي تتمتع بها هذه الفئة من الأدلة من طبيعة فنية لا مادية، وسهولة إخفائها أو التلاعب بها وسرعة محوها من المسرح الجريمة، فان أجهزة القضاء الجنائية وجدت نفسها أمام تحديات قانونية وعلمية جديدة غير معهودة فيما

يخص فهم الطبيعة الخاصة لهذه الأدلة الالكترونية المنتشرة في بيئة افتراضية وأساليب البحث والتحري عنها، وكذا كيفية التعامل معها بشكل يبقي على طبيعتها الأصلية ولا يفقدها قيمتها الاستدلالية. وهو الأمر الذي دفع الفقه الجنائي إلى التدخل لرفع الإبهام عن هذه المسالة من خلال تحديد الطبيعة القانونية للأدلة الالكترونية، نطاقها وخصوصياتها كما سوف نبينه بالتفصيل في (المبحث الأول).

ولم يتوقف الأمر عند هذا الحد، بل أثارت الظاهرة الإجرامية التقنية العديد من المشكلات الأخرى في خضوعها لأحكام قانون الإجراءات الجزائية المتعلقة بالإثبات الذي وضعت نصوصه لتحكم الإجراءات الخاصة بجرائم تقليدية لا تثير صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي، منها ما يتعلق بالقيمة القانونية للأدلة الالكترونية في عملية الإثبات الجنائي أو بمعنى أخر مدى قبول هذه الأدلة كوسيلة إثبات من طرف القاضي الجزائي و ماهي حجيتها في ذلك؟ وهو الأمر الذي سوف يكون محور دراستنا في (المبحث الثاني).

المبحث الأول

الطبيعة القانونية للدليل الإلكتروني

تختلف البيئة التي ترتكب فيها الجريمة الالكترونية من وسط مادي محسوس إلى وسط معنوي أو ما يعرف بالوسط الافتراضي، وعلى هدى ذلك فالبحث عن أدلة الإثبات في إطار ما يتوافق ويتناسب مع الطبيعة التقنية لهذه الجرائم و وسائل ارتكابها لا يكون مجديا إلا إذا كان مدعّما من قبل التقنية ذاتها، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه الجريمة الالكترونية، وهي الأدلة الرقمية أو ما يسمى بالأدلة الإلكترونية.

والمعلوم أن طبيعة الدليل تتشكل وتتحدد من طبيعة الجريمة التي تولد منها، فالدليل في جريمة التزوير مثلا يستنبط من إثبات تغيير الحقيقة في المحرر الذي يقع عليه، ودليل جريمة القتل يولد من فحص الوسيلة المستعملة في القتل، أما الجريمة الالكترونية، فيمكن أن تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها.

وعليه ففي مجال التعامل مع الأدلة الجنائية فان جهات البحث والتحري مقبلة على الانتقال من مرحلة التعامل مع الأدلة المادية الملموسة المعلومة المصادر، إلى مرحلة التعامل مع الأدلة الرقمية الالكترونية المنتشرة في العالم الافتراضي المجهولة المصادر، وهو الأمر الذي يثير لا محال مشكلات عملية وأخرى قانونية ينبغي تحديد معالمها بوضوح تمهيدا لوضع الحلول المناسبة لعلاجها. ولعل أولى هذه الحلول يكمن في تحديد طبيعة الدليل الالكتروني من خلال الوقوف عند تعريفه وأهم خصائصه التي تميزه عن الأدلة التقليدية (المطلب الأول)، ثم تبيان ماهية أشكال وأصناف الدليل الالكتروني التي تصلح لان تكون وسيلة إثبات أمام القضاء الجنائي (المطلب الثاني).

المطلب الأول

مفهـوم الدليـل الإلكترونـــي

بدأ الحديث منذ شيوع استخدام الحاسب الآلي ومختلف الأجهزة الالكترونية الأخرى عن بعض الأفعال والسلوكيات المرتبطة بالاستخدام غير المشروع للبيانات المخزنة في أنظمته والتلاعب بهذه البيانات وتدميرها، وقد رافق ذلك نقاشات وتساؤلات حول كيفية التصدي لهذه السلوكيات الإجرامية المستجدة وما هي الوسائل الملائمة لإثباتها.

ولما كان الدليل الالكتروني الناشئ عن البيئة الرقمية لهذه الجرائم الحديثة مرتبطا بتكنولوجيات وسائل الاتصال وشبكات الربط الحديثة، فانه من الضروري أن يكون أي تعريف لهذا النمط من الأدلة متسما بالمرونة بما يسمح باستيعابه وتـواكبه مع سـائر الجـرائم

المرتكبة بالتقنيات المبتكرة الراهنة والمستقبلة في تكنولوجيا التعامل مع المعلومات.

ولكن التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حال دون وضع تعريف فقهي جامع وشامل لمفهوم الدليل الالكتروني، خشية حصر نطاقه داخل إطار تجريمي محدد قد يضرّ به خاصة في ظل التطور المستمر للتقنية الالكترونية(الفرع الأول).

وإذا كان التطور المتجدد والمستمر للبيئة التي يرتبط بها الدليل الالكتروني يمنع إيجاد تعريف موحد لهذا الأخير، فذلك لم يمنع الفقه الجنائي من تحديد السمات والخصائص التي يتميز بها الدليل الالكتروني عن غيره من الأدلة التقليدية، والذي قد يسهم في صياغة المشرع لنصوص قانونية حولها ويساعد القضاء من تفسير هذه النصوص وتقدير الدليل(الفرع الثاني).

الفرع الأول: مقاربة في تعريف الدليل الإلكتروني

لم يتفق الفقه الجنائي حتى الآن حول تعريف موحد للدليل الالكتروني، وذلك راجع إلى التطور المستمر الذي يطرأ على البيئة التقنية التي ينشأ فيها، وتجعله من الأدلة المتطورة بطبيعتها، لاسيما أن العالم الافتراضي لا يزال في بداية عهده ولم يبلغ بعد ذروته، وأن العالم الالكتروني أو الرقمي من غير الممكن احتوائه .

فقد عرفه البعض بأنه " **ذلك الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل ذبذبات رقمية ونبضات مغناطيسية او كهربائية يمكن جمعها او تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل علمي يمكن اعتماده أمام القضاء الجنائي**"[248]. والملاحظ على هذا التعريف أنه يلحق مفهوم الدليل الالكتروني بمفهوم البرنامج رغم وجود فرق كبير في الوظيفة التي يؤديها كل عنصر، فبرنامج الحاسب

[248]– **ممدوح عبد الحميد عبد المطلب**، البحث و التحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت، دار الفكر القانونية، القاهرة، 2006، ص 88.

الآلي له دور في القيام بمختلف العمليات التي يحتويها نظام المعالجة الآلية، أما الدليل الجزائي الالكتروني فيكمن دوره الأساسي في معرفة كيفية حدوث جرائم الاعتداء على نظم المعالجة الآلية، بهدف إثباتها و نسبتها إلى مرتكبيها.

وعرفه البعض الآخر بأنه "**معلومات يقبلها المنطق و العقل و يصدقها العلم، يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال ويمكن استخدامها في أية مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة** "[249]. أو انه " **يشمل المعطيات الرقمية المشتقة من أو بواسطة النظم و المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الإعلام الآلي أو شبكات الاتصالات وفق إجراءات قانونية و فنية لتقديمها للقضاء بعد تحليلها علميا وترجمتها الى نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة للمتهم وفقها** "[250]. غير أن ما يأخذ على هذا التعريف كذلك هو حصره الأدلة الالكترونية في تلك التي تستخرج من أجهزة الإعلام الآلي وملحقاتها، دون سواها من الوسائل التقنية الالكترونية الأخرى التي تعتمد المعالجة الآلية للمعلومات كالهواتف النقالة والبطاقات الذكية والتي يمكن أن تكون مصدرا مهما للأدلة الالكترونية، وهو ما يعد تضييقا لدائرة هذه الأخيرة.

كما عرف الدليل الالكتروني أيضا بأنه " **مجموعة البيانات والمعطيات المأخوذة من العالم الافتراضي التي يمكن إعدادها وتجميعها وتخزينها وتحليلها الكترونيا باستخدام**

---

[249]– **محمد الأمين البشري**، تأهيل المحققين في جرائم الحاسب الآلي و شبكات الانترنت، بحث مقدم في الحلقة العلمية بعنوان "الانترنت و الإرهاب"، المنظمة من طرف جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين الشمس، بدبي، في الفترة الممتدة من 15 إلى 11/19/ 2008، ص 25.

[250]– **خالد ممدوح إبراهيم** ، الدليل الالكتروني في جرائم المعلوماتية، بحث منشور في الموقع الالكتروني التالي:

http://Kenanaonline.com/users/KhaledMamdouh/posts/79345.

برامج وتطبيقات خاصة لتظهر في شكل صور او تسجيلات صوتية أو مرئية "[251]. إلا أن ما يسجل على هذا التعريف هو إضفاؤه صفة الدليل الالكتروني على تلك الأدلة المستخلصة من وسطها الافتراضي المأخوذة من الحاسب مما يعني بمفهوم المخالفة بان تلك المعطيات التي تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية التي لم تفصل عن الحاسب الآلي لا تصلح لان توصف بالدليل الالكتروني، وهذا أمر غير دقيق.

ومن التعريفات التي قدمت كذلك للدليل الالكتروني أنه "**طريقة خاصة لاظهار الحقيقة والذي يتم فيه اللجـوء إلى احـد الوسائــل الرقمية المتنوعة التي تدرس المحتويــات داخل ذاكرة القرص الصلب و الرسائل الالكترونية المخزنة او المنقولة رقميا**"[252].

استرشادا بالمقاربات السابقة فان التعريف الأكثر شمولا للدليل الالكتروني في نظرنا هو" **كل معلومات مخزنة في نظم المعالجة الآلية وملحقاتها أو متنقلة عبرها بواسطة شبكة الاتصالات في شكل مجالات الكترونية او ذبذبات كهربائية او نبضات مغناطيسية، يتم استخلاصها وجمعها وتحليلها وفق إجراءات قانونية وعلمية، وترجمتها لتظهر في شكل مخرجات يقبلها العقل والمنطق ويعتمدها العلم، ويمكن استخدامها في أية مرحلة من مراحل التحقيق والمحاكمة لإثبات الجريمة وتقرير البراءة أو الإدانة** " [253].

---

[251]– **طارق محمد الجملي**" الدليل الرقمي في مجال الإثبات الجنائي" بحث مقدم إلى المؤتمر ألمغاربي الأول حول المعلوماتية و القانون، المنظم من طرف أكاديمية الدراسات العليا بطرابلس، في الفترة الممتدة من 28-2009/10/29، ص 06.

[252] **-CLEMENT- FONTAINE Mélanie**; « définition et cadre juridique de la preuve numérique » colloque sur « la preuve numérique a l'épreuve du litige. Les acteurs de litige a la preuve numérique » organiser par la compagnie nationale des experts de justice en informatique et associées le 13-04-2010. Disponible sur le site :

www.cnejita.org/.../CNEJTA-ACTES-COLLOQUE10042010-A5-V5.1-pdf.

[253]– وهو تقريبا نفس التعريف الذي استأثرته المنظمة العالمية لدليل الكمبيوتر (IOCE) في تقريرها الصادر في أكتوبر

الفرع الثاني: مميزات الدليل الإلكترونـــي

يعتقد البعض أن الأدلة الجنائية الالكتروني ما هي إلا مرحلة متقدمة من الأدلة التقليدية المادية التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان، إلى الاستعانة بجميع ما يبتكره العلم من وسائل التقنية العالية بما فيها جهاز الحاسب[254]، ولكن الحقيقة تثبت عكس ذلك تماما، لأن الأدلة الالكترونية هي نوع آخر من الأدلة الجنائية الجديدة التي لها من الخصائص العلمية والمواصفات القانونية ما يميزها عن غيرها من وسائل الإثبات التقليدية. وهذه الموصفات والخصائص مرتبطة أساسا بطبيعة البيئة التي يتواجد فيها، وهي البيئة الافتراضية التي انعكست على طبيعة هذه الأدلة وجعلته يتصف بالمميزات التالية:

أولا: الدليل الإلكتروني دليل علمي: يتصف الدليل الالكتروني بأنه علمي لأنه مشكّل من معطيات الكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات ذات المبنى العلمي، وأن ما يسري على الدليل العلمي يسري على الدليل الالكتروني[255]، وإذا كان الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة " القانون مسعاه العدالة أما العلم فمسعاه الحقيقة "law seek justice, science seeks truth " إذ يستبعد تعارضه مع القواعد العلمية السليمة، فان الدليل الالكتروني له الطبيعة ذاتها، ويجب أن لا يخرج عما توصّل إليه العلم الالكتروني الرقمي وإلا فقد معناه[256].

2001. أنظر: **مصطفي محمد موسى**، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، 2009، ص213.

[254]ـ **عمرو حسين عباس**، أدلة الإثبات الجنائي والجرائم الالكترونية، بحث مقدم الى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، المنعقد بمقر الجامعة الدول العربية، القاهرة، خلال الفترة الممتدة من 26-27 أفريل 2008، ص.ص 06-07، و **علي محمود علي حمودة**، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي" مرجع سابق، ص 77.

[255]–**عمر محمد أبو بكر بن يونس**، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص 977.

[256]– **علي محمود علي حمودة**، مرجع سابق، ص 22.

ثانيا: الدليل الإلكتروني دليل تقني : بمعنى انه مستوحى من البيئة التقنية التي يتواجد فيها، والمتمثلة في مختلف أجهزة تكنولوجية الإعلام والاتصال من أجهزة الحاسب والخوادم والمضيفات والهواتف والشبكات. ولا يمكن تصور وجود الدليل الالكتروني خارج هذا الإطار[257].

واعتبارا للطبيعة التقنية للدليل الالكتروني فانه اكتسب جملة من مواصفات ميزته عن غيره من الأدلة التقليدية في قابليته للنسخ، إذ يمكن استخراج نسخ من الأدلة الجنائية الالكترونية مطابقة للأصل و تحمل القيمة العلمية نفسها، وهذه الخاصية لا تتوافر في الأدلة الأخرى، مما يشكل ضمانة فعالة للحفاظ على الدليل من التلف أو الفقد أو أي شكل من أشكال التلاعب والتغيير، وذلك لإمكانية مقارنة النسخ مع الأصل باستخدام برامج وتطبيقات خاصة[258]. وكذا قدرة الدليل الالكتروني على رصد معلومات عن الجاني وتحليلها في الوقت نفسه، اذ يمكنه أن يسجل تحركات الجاني، عاداته وسلوكياته ومختلف المعلومات الشخصية الخاصة به، من ثمة يكون البحث الجنائي فيه أيسر بكثير من الدليل المادي التقليدي[259]. أضف إلى ذلك قابلية الدليل الالكتروني للتطور المتواصل نظرا لارتباطه الوطيد بالطبيعة المتغيرة والمتجددة التي تتمتع بها تكنولوجية الإعلام والاتصال[260].

---

[257]– **خالد ممدوح إبراهيم** ، الدليل الإلكتروني في جرائم المعلوماتية، مرجع سابق. بدون ترقيم.

[258]– نذكر منها برنامج حساب البصمة الرقمية (Hash) و اللوغارتمية (MD5) وظيفتهما إسناد إلى ملف أو مجموعة ملفات الكترونية سلسلة أحرف أو أرقام متتالية، وأي تعديل ولو طفيف يصيب أحد هذه الملفات ، يؤدي إلى تغيير بصمته الرقمية بصفة آلية ، وبالتالي الكشف عن التغيرات المحتملة في البيانات الرقمية التي يمكن اعتبارها دليلا رقميا لجريمة ما.

[259]– **عمر محمد بن يونس،** مذكرات في الإثبات الجنائي عبر الانترنت، بحث مقدم إلى ندوة الدليل الرقمي، بمقر جامعة الدول العربية بالقاهرة، في الفترة الممتدة من 05 إلى 08 مارس 2006، ص 17..

[260]– **بوكر رشيدة،** مرجع سابق، ص 388.

ثالثا– صعوبة التخلص من الدليل الالكتروني: تعد هذه الخاصية أهم ميزة يتمتع بها الدليل الالكتروني عن غيره من الأدلة المادية، وإذا كان من اليسير جدا التخلص من الأدلة المادية نهائيا دون إمكانية استعادتها كالوثائق والأشرطة بتمزيقها وحرقها، أو بصمات الأصابع بمسحها من موضعها، أو حتى الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة، فإن الحال غير ذلك بالنسبة للأدلة الالكترونية[261]، إذ يمكن استرجاعها بعد محوها وإصلاحها بعد إتلافها وإظهارها بعد إخفائها، وذلك باستخدام أدوات وبرمجيات ذات الطبيعة الرقمية صممت خصيصا لهذا الغرض مثل برمجيات (Foremost, Recoverpeg photorec...)[262]. كما أن نشاط الجاني لمحو الدليل الالكتروني بواسطة خصائص التخلص من الملفات في الحاسب الآلي كخاصية (Delete, Rénove, Erase ...) يشكل في حد ذاته دليلا ضد الجاني، لأن هذا النشاط يتم تسجيله وتخزينه بشكل آلي في ذاكرة جهاز الحاسب و يمكن استخلاصه لاحقا كدليل إثبات ضده[263].

رابعاـ الرقمية الثنائية للدليل الإلكتروني : ومفاد هذا أن الدليل الالكتروني يتكون من تعداد غير محدود لأرقام ثنائية في هيئة الواحد والصفر (1–0) والتي تتميز بعدم التشابه فيما بينها رغم وحدة الرقم الثنائي الذي تتشكل منه، فمثلا المعلومات و البيانات الموجودة داخل الحاسب الآلي سواء كانت في شكل نصوص أو حروف أو أرقام أو صور أو تسجيلات صوتية أو فيديو ليس لها الوجود المادي الذي نعرفه في شكل ورقي، إنما هي

---

[261]– **محمد الأمين البشري**، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت، مرجع سابق، ص.ص 26– 27.

[262]– **عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 982.

[263]–**CLEMENT-FONTAINE.Mélanie,** op.cit. Article disponible sur ;

www.cnejita.org/.../CNEJTA-ACTES-COLLOQUE10042010-A5-V5.1-pdf.

مجموعة من الأرقام التي ترجع إلى أصل واحد وهو الرقم الثنائي المذكور أعلاه[264]. فما من شيء في العالم الرقمي إلا ويتكون من معادلة ثنائية قوامها الرقمان (1) و(0) وهما في تكوينهما الحقيقي عبارة عن نبضات وذبذبات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة[265]. مع العلم أن تكوين معطيات هذه المعادلة الثنائية تختلف في الحجم والموضوع، وكمية أو حجم الرقمين(1-0) في ملف يمكن أن يختلف عن كميته في ملفات أخرى.

وما يمكن استخلاصه هو أن تمتع الدليل الالكتروني بالخصائص سالفة الذكر جعلته دليلا ذا طابع خاص يختلف عن باقي الأدلة المادية المألوفة، وأصبح على حد تعبير بعض القانونيين المختصين[266] من قبيل الدليل الأحسن والأفضل لإثبات الجرائم الالكترونية لكونه مستمدا من طبيعة الوسط الذي وقعت فيه.

المطلب الثاني

تصنيفات الدليل الإلكتروني ونطاق الإثبات به

يقتضي التعريف الدقيق للدليل الإلكتروني إلى جانب إظهار خصائصه التي تجعله مختلف عن غيره من الأدلة، الوقوف كذلك عند تحديد أنواعه ومختلف تصنيفاته حتى يتسنى فهم الهيأة التي يتخذها و من ثمة الحكم على قيمته القانونية (الفرع الأول). وإذا كانت هذه القيمة القانونية أو الاستدلالية للدليل الالكتروني بتصنيفاته المختلفة تتحدد بمدى تعبيره عن حقيقة الواقعة الإجرامية وقدرته على إثبات الجريمة ونسبتها إلى الجاني، فهل هذا

---

[264]- **ممدوح عبد الحميد عبد المطلب** ، استخدام بروتوكول(TCP/IP) في بحث و تحقيق الجرائم على الكمبيوتر، بحث مقدم الى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، المنعقد بدبي، في الفترة الممتدة من 26-2003/08/28، ص 08 . منشور على الموقع الالكتروني التالي: WWW.arablaw.info.com

[265]-**عمر محمد أبو بكر بن يونس**، مرجع سابق، ص 171.

[266]- **طارق محمد الجملي**، مرجع سابق، ص 08.

يعني أن الإثبات بالدليل الالكتروني يشمل فقط الجرائم التي تتوافق مع طبيعته وهي الجرائم الالكترونية أم أن نطاقه يتعدى ذلك ليضمّ غيرها من الجرائم، وهو ما سوف نبينه في نطاق الإثبات بالأدلة الالكترونية (الفرع الثاني).

الفرع الأول: تصنيفات الدليل الإلكتروني

يمكن تقسيم الدليل الإلكتروني كأصل عام إلى صنفين هما: الدليل الإلكتروني الأصلي، ويتمثل في المحررات الإلكترونية المكونة من بيانات ومعطيات يدخلها المزود ويرسلها عن طريق وسيط الكتروني فيترجمها الوسيط وفق برنامج معين ويمررها إلى المتلقي الذي يمكنه استخراجها بالاستعانة بوسيط إلكتروني آخر وقراءتها بالبرنامج وإظهارها على شكل صورة الإدخال[267]. والدليل الإلكتروني المكرر، وهي الصورة طبق الأصل المأخوذة عن الدليل الإلكتروني الأصلي أو استنساخ رقمي دقيق لجميع المعلومات والبيانات التي يتضمنها المحرر الأصلي والمستقلة عنه[268]. ومن خلال هاذين التقسيمين الرئيسيين يتفرع الدليل الالكتروني إلى عدة تصنيفات أخرى من حيث هيئته **(أولا)** وقيمته الاستدلالية**(ثانيا)**.

أولا- تصنيف الدليل الإلكتروني من حيث هيئته

يتنوع الدليل الالكتروني من حيث هيئته وشاكلته إلى أدلة مكتوبة وأدلة العرض المرئي وأخرى صوتية أو سمعية :

1- أدلة الكترونية مكتوبة: وتشمل كل المخطوطات والنصوص التي يتم كتابتها من طرف المستخدم بواسطة الأجهزة الالكترونية الرقمية كالمراسلات عبر البريد الالكتروني أو الهاتف النقال(sms و mms)، والتي تم إدخالها أو الناتجة عن معالجة البيانات في وحدة

[267]- **محمد الأمين البشري**، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت، مرجع سابق، ص 25.

[268]- **حسام محمد نبيل الشنراقي**، مرجع سابق، ص 720.

المعالجة المركزية أو مختلف ملفات برامج معالجة الكلمات[269]. ومثل هذا النوع من الأدلة يمكن أن نجدها في مختلف وسائل التخزين الالكترونية كالأقراص الممغنطة الصلبة و المرنة والأشرطة المغناطيسية كما يمكن الحصول عليها على شكل مخرجات ذات طبيعة ورقية باستخدام الطابعات.

2- أدلة إلكترونية مرئية: وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وتظهر عادة إما في صور مرئية ثابتة على شكل ورقي أو رقمي باستخدام الشاشة المرئية، أو في شكل تسجيلات فيدو أو أفلام (مصورة)[270]. والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة وأكثر تطوراً للصورة (الفوتوغرافية) التقليدية[271].

3- أدلة إلكترونية سمعية أو صوتية: وتشمل مختلف التسجيلات الصوتية التي يتم ضبطها وتخزينها بواسطة الوسائل الالكترونية، كالمحادثات الصوتية على غرف الدردشة عبر الانترنت، أو عبر تطبيقات مواقع التواصل الاجتماعي (Skype, Vibre, twister Messenger) أو المكالمات الهاتفية[272].

وتجدر الإشارة في هذا الصدد إلى أن هناكمن اعتمد تصنيفا آخر للدليل الالكتروني[273] بما يتطابق مع نوع و طبيعة الجريمة الالكترونية المرتكبة و هو كالتالي:

- أدلة الكترونية خاصة بأجهزة الحاسب الآلي وملحقاته.

---

[269]- **_هلالي عبد أللاه أحمد**، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2003، ص27.

[270]- المرجع نفسه، ص.ص 20 ـ 23.

[271]- **ممدوح عبد الحميد عبد المطلب**" أدلة الصور الرقمية في الجرائم عبر الكمبيوتر" مركز شرطة دبي، 2005، ص 9.

[272]- **_سامي جلال فقي حسين**، الأدلة المتحصلة من الحاسب وحجيتها في الإثبات، دار كتب القانونية، القاهرة، 2011، ص 59.

[273]- نذكر منهم، **ممدوح عبد الحميد عبد المطلب**، مرجع سابق، ص.ص 88-89. و **مصطفي محمد موسى**، مرجع سابق، ص 218.

– أدلة الكترونية خاصة بالشبكة العالمية للمعلومات ومختلف نهاياتها الطرفية.

– أدلة الكترونية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات(TCP/IP).

ثانيا– تصنيف الدليل الإلكتروني من حيث قيمته الاستدلالية

يمكن تصنيف الأدلة الالكترونية من حيث قيمتها الاستدلالية إلى أدلة أعدت خصيصا لتكون وسيلة إثبات، وأخرى لم تعد لتكون وسيلة إثبات:

1– أدلة إلكترونية أعدّت لتكون وسيلة إثبات : تتضمن هذه مايلي:

أ–السجلات التي تم أنشاؤها بواسطة الجهاز الالكتروني تلقائياً، وتعتبر هذه السجلات من مخرجات الجهاز التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.

ب–السجلات التي جزء منها تم حفظه بالإدخال وجزءها الأخر تم إنشاؤه بواسطة الجهاز ومن أمثلة ذلك، البيانات التي يتم إدخالها إلى جهاز الحاسب وتتمُّ معالجتها من خلال برنامج خاص[274].

2– أدلة إلكترونية لم تعدّ لتكون وسيلة إثبات: هذا النوع من الأدلة نشأت دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده، وتسمى بالبصمة الرقمية، أو الآثار المعلوماتية الرقمية[275]، وهى تتجسد في المخلّفات التي يتركها مستعمل شبكة الانترنت كالمواقع التي تصفحها والملفات التي زارها، والتواريخ المرتبطة بهذه الزيارات، التي تسجل على الذاكرة المخفية للقرص الصلب بجهاز المستخدم داخل فهرس خاص

[274]- **أحمد يوسف الطحطاوي**، الأدلة الالكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015، ص 21.

[275]– **ممدوح عبد الحميد عبد المطلب**، مرجع سابق، ص.ص 22– 28.

للنظام. وكذا ملفات البريد الالكتروني (الإيميل) التي تحمل مختلف الرسائل المرسلة منه أو التي استقبلها الموجودة أو المحذوفة وكافة العمليات والاتصالات التي تمت من خلال النظام المعلوماتي أو شبكة المعلومات العالمية[276].

والواقع أن هذا النوع من الأدلة لم يُعد أساسا للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن ضبط هذه الأدلة ولو بعد فترة زمنية من إنشائها، فالاتصالات التي تجرى عبر الانترنت والمراسلات الصادر عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنيات التتبع و الاسترداد[277].

وتبدو أهمية التمييز بين هذين النوعين من الأدلة الالكترونية ، في كون النوع الأول قد أُعدَّ مسبقا كوسيلة إثبات لبعض الوقائع التي يتضمنها، وعادة ما يُعمد إلى حفظه للاحتجاج به لاحقاً وهو ما يقلل إمكانية فقدانه، ويجعل من السهل الحصول عليه. أما النوع الثاني فنظرا لكونه لم يُعد أصلاً ليكون أثراً لمن صدر عنه، فانه الأكثر أهمية وقيمة استدلالية من النوع الأول لأنه غالبا ما يتضمن معلومات ذات مصداقية تفيد في الكشف عن الجريمة ومرتكبيها ويكون الحصول عليه بإتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد، وهو على العكس من النوع الأول لم يعد ليحفظ مما يجعله عرضة للفقدان[278].

الفرع الثاني: نطـاق الإثبات بالدليل الإلكتروني

إن الاهتمام الذي يحظى به الدليل الالكتروني الرقمي مقارنة بغيره من الأدلة مرده انتشار استخدام وسائل تكنولوجيات الإعلام والاتصال وتقنية المعلومات الرقمية، والتي تعاظم دورها مع دخول الانترنت شتى مجالات الحياة، وأصبح هذا المجال مسرحا لطائفة

---

[276]-**TYRODE Jean François**, op.cit. PP 22- 23.

[277]– من ضمن هذه التقنيات ما يعرف ببروتوكول(IP) والذي يمكِّن من ضبط تحركات مستخدم الشبكة الانترنت عبر الجهاز الذي يستعمله من خلال بيانات الجهاز عند مزود الخدمة التي تضفي إلى كشف مرتكب الجريمة .

[278]– **أحمد يوسف الطحطاوي**، مرجع سابق، ص22.

من الجناة يطلق عليهم اسم المجرمين المعلوماتيين[279]. فالجرائم التي يرتكبها هؤلاء تقع في الوسط الافتراضي أو ما يسمي بالعالم الرقمي، لذلك كان الدليل الالكتروني الرقمي هو الأفضل لإثبات هذا النوع من الجرائم، لأنه من طبيعة الوسط الذي ارتكبت فيه.

وإذا كان فهم الدليل الالكتروني بمختلف تصنيفاته يعتمد أساسا على استخدام أجهزة الكترونية خاصة بتجميع وتحليل محتواه، وكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلا الكترونيا يعتمد عليه في إثبات الجريمة الالكترونية ونسبتها إلى الجاني، فهل هذا يعني أن الدليل الالكتروني ينحصر مجاله كدليل إثبات في الجرائم المعلوماتية فقط أم انه يمتدّ ليشمل غيرها من الجرائم التقليدية ؟

لقد اجمع الفقه الجنائي في هذه المسالة على انه لا يوجد تلازم بين نطاق العمل بالدليل الالكتروني وعملية إثبات الجرائم المعلوماتية، فمثلما يصلح الدليل الالكتروني لإثبات الجريمة المعلوماتية ويعتبر في الوقت ذاته الدليل الأفضل لإثباتها، فانه يصلح كذلك لإثبات الجرائم الأخرى التقليدية[280]. انطلاقا من هنا، يمكن أن نحدد نطاق الإثبات بالدليل الالكتروني في نوعين من الجرائم، الأول يكون فيه الحاسب الآلي والانترنت وسيلة لارتكاب الجريمة أما النوع الثاني، فيكون فيه الحاسب الآلي والمعلومات المخزنة فيه محلا للجريمة.

أولا – الجرائم المرتكبة بالحاسب: وهذا النوع من الجرائم يستخدم فيه الحاسب الآلي أو إحدى وسائل التقنية الحديثة المرتبطة به كوسيلة مساعده لارتكاب الجريمة، فهي كما عرفتها منظمة الأمم المتحدة " **كل نشاط إجرامي تستخدم فيه التقنية الالكترونية، الحاسب الآلي الرقمي وشبكة الانترنت، بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل**

---

[279]–**عادل يوسف عبد لبني شكري**، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مركز دراسات الكوفة، 2008، ص 117.

[280]– **كحلوش علي**، جرائم الحاسوب و أساليب مواجهتها" مجلة الشرطة، عدد 84، صادر عن مديرية الأمن الوطني، جويلية 2007، ص 51.

الإجرامي"[281]. ومن هذا المنطلق، فأي فعل غير مشروع يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية، أو يكون علم تكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه كاستخدام الحاسب في الغش أو الاحتيال أو غسل الأموال أو تهريب المخدرات، أو استخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان، يعد من قبيل الجرائم الالكترونية[282].

ورغم أن هذا النوع من الجرائم لا صلة له بالنظام المعلوماتي والوسط الافتراضي سوى في الوسيلة المستعملة لارتكابها، بمعنى أن الجريمة في هذه الحالة هي جريمة تقليدية استعملت في ارتكابها أداة الكترونية، إلا أن ذلك لا يمنع من أن يكون الدليل الالكتروني دليلا لإثباتها.

ثانيا- الجرائم المرتكبة على الحاسب والانترنت

ويتحقق هذا النوع من الجرائم إما عند وقوع اعتداء على الكيانات المادية للحاسب وملحقاته، كتحطيم شاشة الحاسب أو لوحة المفاتيح، أو وحدته المركزية، أو بإتيان أي فعل مادي من شأنه إخراج هذه المعدات من حيازة مالكها دون علمه وإدخالها في حيازة شخص آخر، أو إتلافها وتدميرها وغيرها من الأفعال[283]. وفي هذه الحالة نكون أمام جريمة تقليدية باعتبار أن هذه المكونات المادية محل الاعتداء تتمتع بالحماية الجزائية وفق النصوص التقليدية، بوصفها أموال منقولة تخضع سرقتها أو إتلافها للنصوص العقابية التقليدية، وفيها

---

[281] -**ONU** : Manuel pour la prévention et la répression de la criminalité informatique, Revue internationale de politique pénale, N° 43 et 44, 1995. (Publication des Nations Unies, Numéro de vente : F.94.IV.5).

[282]- **مصطفى محمد موسى**، أساليب إجرامية للتقنية الرقمية (ماهيتها و مكافحتها)، دار الكتب القانونية، القاهرة، 2005، ص 56.

[283]- **يوسف حسن يوسف**، الجرائم الدولية للانترنت، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص 76.

تكون نسبة الإثبات بالدليل الالكتروني ضئيلة إن لم نقل منعدمة[284].

أو عند وقوع الاعتداء على الكيانات المعنوية أو المنطقية للحاسب، والمتمثلة في المعلومات بكل صورها من بيانات والبرامج المخزنة في ذاكر الحاسب، أو على قاعدة البيانات أو المعلومات التي قد تكون على الشبكة العالمية للمعلومات باعتبارها حلقة الوصل بين كل الأهداف المحتملة لهذه الجرائم[285]. كأن يتم المساس بسريتها عن طريق الدخول والاعتراض غير المشروعين، أو المساس بسلامة محتواها و تكاملها[286] وتوفرها[287]، عن طريق الإتلاف أو التزوير بالتعديل أو التزييف أو التحريف. أو المساس بسلامة تشغيلها كتعطيل أو إضعاف قدرة وكفاءة الأنظمة المعلوماتية على القيام بوظائفها. وهذه الطائفة من الجرائم هي التي يقصد بها الجرائم الالكترونية، والتي يكون الدليل الالكتروني الرقمي هو الأوفر والأفضل لإثباتها إن وجد[288].

ومع ذلك، فرغم الارتباط الوطيد بين الجريمة الالكترونية والدليل الالكتروني الرقمي، إلا أن مسألة إثباتها لا يقتصر عليه، بل من الممكن استدلالها بوسائل الإثبات التقليدية،

---

[284]- **MITONGO Kalonji** , notion de cybercriminalité : praxis d'une pénalisation de la délinquance électronique en droit pénale congolais, p 10 . Article publier sur ; www.tgk.centerblog.net

[285]– **يوسف حسن يوسف**، مرجع سابق، ص.ص 29–30.

[286]– يقصد بالتكاملية في محتوى نظام المعالجة الحفاظ على سلامة و كمال و دقة المعلومات المخزنة داخل نظام المعالجة، من أي تحريف أو تعديل. أما التكامل في محتوى الاتصالات أو التخاطب عبر الانترنت فيعني التحقق من المعلومات الأصلية من خلال التحقق من هوية مرسلها و بتسجيل تاريخ الإرسال و الاستقبال و التحقق من صلاحية جهة ما لاستقبال المعلومات المرسلة.

[287]– التوفر يعني قدرة البرمجيات و الأجزاء الصلبة المحتواة في النظام على الاستمرار في أداء وظيفتها بفعالية، وقدرتها على النظام على التغطية السريعة و الكاملة في حالة حدوث أي خلل . والمفهوم المضاد للتوفر هو إنكار الخدمة أي عدم قدرة مستخدمي النظام على الوصول إلى المصادر التي يحتاجونها.

[288]– **عبد الفتاح بيومي حجازي**، الدليل الرقمي والتزوير في جرائم الكمبيوتر والانترنت، دراسة معقمة في جرائم الحاسب الآلي و الانترنت، بهجت للطباعة والتجليد، القاهرة ، 2009، ص 184.

كشهادة شهود والاعتراف. مما يستتبع القول، أنه لا تلازم بين مشكلة الدليل الالكتروني الرقمي وإثبات الجريمة المعلوماتية، إذ لهذه الأخيرة إشكاليات قانونية أخرى لا شأن لها بهذا الدليل[289]، كأن يقتصر الدليل الالكتروني على مجرد إثبات وقوع الجريمة دون تحديد مقترفها.

وعليه نستخلص أن مجال الإثبات بالدليل الالكتروني الرقمي يشمل أساسا كل الجرائم التي ترتكب بواسطة الآلة الرقمية– الحاسب الآلي، اللوحة الرقمية– الهاتف الذكي، والجرائم التي ترتكب ضد الكيان المعنوي للآلة أو ضد شبكة المعلومات العالمية. وقد يمتد كذلك، ليشمل بعض الجرائم الأخرى وإن لم تكن من ضمن النوعين المذكورين، وذلك عندما تستعمل الآلة الرقمية للتمهيد لارتكاب الجريمة، أو لإخفاء معالمها، كالمراسلات التي يبعث بها الجاني لشريكه وتتضمن معلومات عن جريمة ينويان ارتكابها أو يطلب منه إخفاء معالم هذه الجريمة[290]، فتلك المراسلة تصلح كدليل إثبات لهذه الجريمة حال وقوعها رغم أنها لم ترتكب ضد الآلة الرقمية ولا بواسطته.

المبحث الثاني

قبول القاضي الجزائي للدليل الإلكتروني

المستقر عليه في مجال الإثبات الجزائي أن القاضي لا يمكنه إصدار أحكام بالإدانة وفقا لعلمه الشخصي، فإحاطته بوقائع الدعوى يجب أن يتم من خلال ما يطرح عليه من أدلة إثبات، من هنا يبدو الدليل العنصر الأساسي الذي ينظر من خلاله القاضي الجزائي للواقعة موضوع الدعوى، ويبني على أساسه قناعته في ثبوت أو نفي التهمة عن المتهم ومن ثم إنهاء الخصومة الجزائية بحكم يكون عنوانا للحقيقة.

[289]– **أحمد يوسف الطحطاوي**، مرجع سابق، ص 30.

[290] - **MITONGO Kalonji,** op cit, p 8.

ومع ذلك فوجود دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين لا يكفي للتعويل عليه، بل ينبغي أن تكون لهذا الدليل قيمة قانونية في المشروعية والمصداقية حتى يتمتع بحجية داحضة أمام القضاء.

وفي نطاق الجرائم المتصلة بتكنولوجية الإعلام والاتصال أبدا كل من الفقه والقضاء مخاوف كبيرة حيال الدليل الالكتروني الرقمي بسبب إمكانية عدم تعبيره عن الحقيقة، نظرا لما يمكن أن تخضع له طرق الحصول عليه من التعرض والتزييف والتحريف والعبث، وهو ما يثير مسألة مشروعية الأخذ به، إذ يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا في وجوده وطريقة تحصيله[291].

كما يثير أيضا مسألة حجية الدليل الالكتروني في تعبيره عن الحقيقة التي تتطلع إليها الدعوى الجزائية لا سيما إذا أخذنا بالاعتبار الصعوبات التي تصاحب استخلاصه[292]، فضلا عن التطور المتزايد في مجال المعلوماتية الذي قد يتيح العبث بسهولة بهذا النوع من الدليل بما يجعل مضمونه مخالفا للحقيقة وهو ما قد يؤثر سلبا على مصداقيته وحجيته أمام القضاء.

تأسيسا لما سبق فقبول الدليل الالكتروني بوصفه وسيلة إثبات أمام القضاء الجزائي من عدمه إنما يتوقف على عنصرين رئيسيين، الأول هو المشروعية،(المطلب الاول) والثاني هو الحجية أو المصداقية،(المطلب الثاني) .

---

[291]– في هذا الصدد صرحت محكمة النقض المصرية بأنه " **لا يضر العدالة إفلات مجرم من العقاب بقدر ما يضرها الاعتداء على حرية الناس والقبض عليهم بدون وجه حق**" مشار إليه في: **محمد زلايجي**، مرجع سابق، ص 73.

[292]– لتفاصيل أكثر حول هذه الصعوبات أنظر: **سامي جلال فقي حسين**، مرجع سابق، ص 127 وما يليها.

المطلب الأول

مشروعية الدليل الإلكترونـــــي

يقصد بالمشروعية التقيد بأحكام القانون والعمل في إطاره، بهدف تقرير ضمانة أساسية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة بالتعدي عليها في غير الحالات المسموح فيها بذلك. واعتبارا لذلك فالدليل الجنائي لا يكون سليما ويقينيا يعوّل عليه القضاء في أحكامه إلا إذا تحلى وتغلف بالمشروعية[293].

ومع أن مسألة قبول الدليل الجنائي بشكل عام تعد الخطوة الأولى التي يتخذها القاضي تجاهه، وذلك بعد البحث عنه وقبل إخضاعه لتقديره، إلا أن سلطته في ذلك تتسع وتضيق حسب المبادئ التي تقوم عليها أنظمة الإثبات السائدة، فيما إذا كانت تجنح إلى تقييده، أم كانت تطلق حريته.

فلا ريب أن مبدأ شرعية الجرائم والعقوبات الذي يستقيم عليه بنيان القانون الجنائي الموضوعي ينعكس على قواعد الإثبات الجنائي ويفرض خضوعها هي الأخرى لمبدأ الشرعية، والتي تستلزم عدم قبول أي دليل إلا إذ كان مشروعا سواء في وجوده(الفرع الأول)، أي أن يكـون من ضمن الأدلـة التـي يجيز القـانون للقاضـي الاستناد إليهـا لتكـوين عقيدته، أو في إجراءات ووسائل البحث عنه والحصول عليه(الفرع الثاني).

الفرع الأول: مشروعية الدليل الإلكتروني في الوجود

تقتضي مشروعية وجود الدليل الالكتروني أن يعترف المشرع الجزائي بهذا الدليل بنصوص قانونية واضحة ويدرجه ضمن قائمة وسائل الإثبات التي يجوز للقاضي الاستناد

---

[293]– **هلالي عبد الله احمد**، حجية المخرجات الكومبيوترية في المواد الجنائية، مرجع سابق، ص 104.

إليها لتكوين عقيدته[294]، إذ لا يسوغ لهذا الأخير بناء حكمه على دليل لم ينص عليه القانون صراحة، كما ليس له أن يتوسّع في تفسير النصوص الجنائية أو تأويلها أو تحميلها بأكثر مما تتحمل لما قد ينجم عن ذلك من خلق أدلة إثبات أخرى لم يعرف لها وجود في القانون حتى ولو بلغت الأفعال المرتكبة درجة عالية من الخطورة.

وفي هذا الإطار، تختلف طريقة الاعتراف بالدليل الالكتروني وقبوله كدليل إثبات من دولة إلى أخرى بحسب طبيعة نظام الإثبات السائد فيها، والذي لا يمكن أن يخرج عن الفئات الثلاث التالية:

أولا – نظام الإثبات المقيد:[295] وفيه يقوم المشرع بتحديد سلفا وبشكل حصري الأدلة التي يجوز للقاضي قبولها والاستعانة بها في الإثبات، وكذا تحديد القوة الاستدلالية لكل دليل بناء على قناعته بها، في حين لا يكون للقاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، وإنما يقتصر دوره على فحص الدليل للتأكد من مدى مشروعيته وتوفره على الشروط التي حددها القانون. وفي حالة انتفاء الشروط التي يتطلبها القانون في الدليل فان القاضي لا يسع له الحكم بالإدانة حتى ولو تكونت لديه قناعة يقينية بارتكاب المتهم للجريمة المنسوبة إليه[296].

ومن هنا يتضح جليا بأن نظام الإثبات المقيد يقوم على مبدأين أساسيين، الأول يتمثل في الدور الايجابي للمشرع في عملية الإثبات لكونه الذي ينظم قبول الأدلة سواء عن طريق التعيين المسبق للأدلة المقبولة للحكم بالإدانة، أو باستبعاد أدلة أخرى، أو بإخضاع كل دليل

---

[294]– **رمزي رياض عوض**، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها ـ دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 1997، ص 85.

[295]– اقترن نظام الإثبات المقيد أو ما يسمى بنظام الإثبات القانوني بالدول الانجلو سكسونية مثل إنجلترا ، الولايات المتحدة الأمريكية، كندا، الهند، ماليزيا. لمزيد من التفاصيل انظر: **زلايجي محمد**، مرجع سابق، ص.ص 66 ـ70.

[296]– **سامي جلال فقي حسين**، الأدلة المتحصلة من الحاسوب...، مرجع سابق، ص 81.

لشروط معينة، ولكونه الذي يحدد القيمة الاقناعية لكل دليل بأن يضفي الحجية الدامغة على بعض الأدلة، والحجية النسبية على بعضها الآخر [297]. أما المبدأ الثاني، فيتمثل في الدور السلبي للقاضي الجزائي في الإثبات، إذ يلتزم التزاما صارما بما يرسمه له المشرع سلفا من أدلة إثبات على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون[298].

واعتبار لذلك، فقد انتقد الفقه الجنائي هذا النظام بشدة خاصة فيما تعلق منه بتجريد القاضي من وظيفته الطبيعية المتمثلة في فحصه للدليل المعروض أمامه بكل حرية وتقدير قيمته الاقناعية وفقا لضميره المهني، ومن ثم تكوين اقتناعه الشخصي، ومنحها للمشرع ليحل بذلك محل القاضي، بل أكثر من ذلك جعل اقتناع القاضي متوقفا على اقتناع المشرع بما يمليه عليه هذا الأخير من أدلة إدانة على سبيل الحصر.

ومن المسائل التي انتقدت في هذا النظام، قيامه بتقنين اليقين بنصوص قانونية سلفا رغم أن اليقين مسالة يطرحها الواقع ترتبط بالظروف الخاصة والمتغيرة لكل قضية وتترك لتقدير قاضي الموضوع[299].

---

[297]–**هلالي عبد أللاه أحمد**، حجية المخرجات الكومبيوترية في المواد الجنائية ، مرجع سابق، ص 91 .

[298]–**سامي جلال فقي حسين**، الأدلة المتحصلة من الحاسوب...، مرجع سابق، ص 82.

[299]– ومن النتائج الوخيمة التي تترتب عن تقيد القاضي باليقين القانوني، والالتزام بحرفية النصوص ما حدث في القضية التي حكم فيها القاضي (**Cambo**) والتي تتلخص وقائعها: بأنه في صبيحة أحد الأيام بينما كان القاضي كامبوا وهو قاضيا في إحدى محاكم مالطا يرتدي ملابسه لاحظ من نافذة غرفته شخصين يتشاجران، وأثناء ذلك قام أحدهما بطعن الأخر بخنجر فأرداه قتيلا ولاذ بالفرار، وسقط منه جراب الخنجر، الذي طعنه في جسم الضحية، وفي الوقت نفسه مرّ خباز في الجوار، وعثر على جراب الخنجر فأخذه ووضعه في جيبه، ولما شاهد الجثة خاف وهرب، وأثناء ذلك رآه رجال الشرطة والقوا القبض عليه، وعند تفتيشه وجدوا بحوزته جراب الخنجر الذي تبين فيما بعد بأنه مطابق للخنجر المطعون في جسم المجني عليه. ورغم مشاهدة القاضي كل تفاصيل القضية بأم عينيه إلا انه عند امتثال الخباز أمامه للمحاكمة لم

ونتيجة لهذه الانتقادات وغيرها، تراجع العمل بنظام الإثبات المقيد بشكل سريع في الآونة الأخيرة وتقلص نطاقه حتى في الدول التي تعتبر الأكثر اعتناقاً له، فنجد بريطانيا مثلاً وهي الدولة المؤسسة لهذا النظام قد بدأت تخفف غلواءه، وظهر فيها ما يعرف بقاعدة "**الإدانة دون أدنى شك**"، والتي مفادها أن القاضي يستطيع أن يكوِّن عقيدته من أي دليل وإن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قطعياً في دلالته[300]. وهو الاتجاه الذي سايره المشرع الأمريكي من خلال تبنيه في قانون الأدلة الاتحادي لقاعدة "**الدليل الأفضل**"[301].

ثانيا- نظام الإثبات الحر[302]: وهو نظام يسود فيه مبدأ حرية الإثبات، إذ لا يحدد فيه المشرع طرقا معينة للإثبات ولا حجيتها أمام القضاء، إنما يترك ذلك للقاضي الجزائي الذي يكون له دور ايجابي في البحث عن الأدلة المناسبة وتقدير قيمتها الثبوتية حسب اقتناعه بها[303]. فلا يلزمه القانون بالاستناد إلى أدلة معينة لتكوين قناعته فله أن يبني هذه القناعة على أي دليل يقدم في الدعوى وإن لم يكن منصوصا عليه، بل أن المشرع في

يدافع عنه، وطبق عليه القانون بكل تفاصيله، بل حمله على الاعتراف بالتعذيب، ولما اعترف الخباز مكرها حكم عليه بالإعدام. نقلا عن: **هلالي عبد ألاله أحمد**، النظرية العامة للإثبات الجنائي، المجلد الأول، دار النهضة العربية للنشر، القاهرة، بدون سنة، ص.ص 95-96، هامش رقم 1.

[300]- **STEPHEN . J et autre**, la preuve en procédure pénale comparée, rapport de synthèse pour les pays de Common Law, association internationale de droit pénal, 1992, p 33.

[301]- قاعدة الدليل الأفضل، هي القاعدة التي تعطي للقاضي سلطة تقديرية في قبول نسخ أو صور الدليل الأصلي في حالة عدم توافر هذا الأخير (أي الدليل الأصلي) أو فقدانه. أنظر: **سامي جلال فقي حسين**، التفتيش في الجرائم المعلوماتية، مرجع سابق، ص 303.

[302]- أخذت بهذا النظام التشريعات ذات الصياغة اللاتينية مثل التشريع الفرنسي، البلجيكي ، الألماني و الايطالي، ومعظم التشريعات الأوروبية.

[303]- **عفيفي كامل عفيفي**، جرائم الكمبيوتر و حقوق المؤلف والمصنفات الفنية ودور الشرطة و القانون، مرجع سابق، ص 379.

مثل هذا النظام لا يختصّ بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه من الأدلة ما يراه مفيدا للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية في قبول الدليل أو طرحه جانبا إذا لم يطمئن إليه، ودون أن يكون مطالبا بتسبيب اقتناعه[304].

ويجد هذا النظام مبرراته في كون الإثبات في المسائل الجزائية لا ينصب إلا على وقائع مادية أو نفسية خاصة بالجريمة ولا ينصب على تصرفات قانونية يتفق معها قيام المشرع سلفا بتحديد وسائل إثباتها ومدى الحجية التي تتمتع بها كل منها، كما أن الإثبات ينصرف إلى وقائع إجرامية غالبا ما يعمد الجناة بقدر المستطاع إلى إزالة ومحو آثارها، الأمر الذي يحتم تحويل القضاء كافة الوسائل المتاحة والممكنة لكشف الجريمة وتقصي الحقيقة[305].

وعلى عكس نظام الإثبات المقيد فان فلسفة هذا النظام ترتكز على مبدأين مختلفان هما: الأول يتمثل في الدور السلبي للمشرع في عملية الإثبات، ومن خلاله يمتنع المشرع عن تحديد الأدلة التي تصلح للإثبات مسبقا، وهو ما يفتح المجال لأن تكون جميع الأدلة مقبولة وفقا لتقدير القاضي وليس المشرع، كما يمتنع عن تحديد القيمة الاقناعية للدليل أو إظهار أي تسلسل بين هذه الأدلة في الحجية أو يرجّح أي دليل على الآخر، فيقتصر دور المشرع على تحديد الشروط اللازمة لصحة الدليل وطريقة تقديمه، وذلك ضمانا للحرية الفردية و كفالة حسن سير العدالة[306].

---

[304]– **ياسر محمد الكومى محمود أبو حطب**، الحماية الجنائية والأمنية للتوقيع الالكتروني، منشاة المعارف، الإسكندرية، 2014، ص 303.

[305]–**عفيفي كامل عفيفي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، مرجع سابق، ص.ص 379– 380.

[306]– **أحمد يوسف الطحطاوي**، مرجع سابق، ص 195.

أما المبدأ الثاني، فهو الدور الايجابي للقاضي الجزائي في الإثبات، ويبدو ذلك من ناحيتين : الأولى من خلال الحرية المطلقة التي يتمتع بها القاضي الجزائي في إثبات حقيقة الجريمة بكافة طرق الإثبات[307]، وسلطته الواسعة في اتخاذ جميع التدابير و الإجراءات التي يعتقد أنها مفيدة لإظهار هذه الحقيقة كسماع الشهود[308]، وندب الخبراء واستدعائهم ليقدموا إيضاحات عن التقارير المنجزة من طرفهم[309]، كما له أن يأمر باستكمال التحقيق إذا ما كانت عناصر الإثبات التي بين يديه غير كافية أو غير مقنعة.

ومن ناحية أخرى فنظام الإثبات الحرّ يمنح للقاضي الجزائي سلطة تقديرية كبيرة في قبول الأدلة، وموازنتها وتقدير قيمتها التدليلية محتكما إلى ضميره ومعتمدا على ثقافته وخبرته القانونية. فله أن يأخذ بأدلة ويستبعد أخرى، كما له أن ينسق بين الأدلة المطروحة أمامه وإزالة التعارض بينها، واستكمال نقصها، ومن ثم تكوين حكمه على أساس القناعة التي توصل إليها من مناقشة هذه الأدلة[310].

---

[307]– اقرّ المشرع الجزائري بحرية الإثبات الجزائي في نص المادة (212) من قانون الإجراءات الجزائية بالصيغة التالية "**يجوز إثبات الجرائم بأية طريقة من طرق الإثبات ... وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي**". ونص المشرع الفرنسي كذلك على هذا المبدأ في المادة (427) من قانون الإجراءات الجزائية على النحو التالي: " **ما لم يرد نص مخالف، يجوز إثبات الجرائم بكافة طرق الإثبات، و يحكم القاضي بناء على اقتناعه الذاتي**".

[308]– وفي هذا الشأن خول المشرع الفرنسي لقاضي الجنايات من خلال نص المادة (310) من قانون الإجراءات الجزائية سلطة تفويضية بمقتضاها يمكن له أن يتخذ كافة الإجراءات والتدابير الضرورية لاستجلاء حقيقة الجريمة ولا قيد عليه سوى شرفه وضميره، كسماع أقوال بعض الأشخاص دون خلف اليمين و على سبيل الاستدلال، او يأمر بتلاوة تقرير الخبير، أو تلاوة شهادة غائب وغيرها من الإجراءات.

[309]– راجع المادتين (324 و 325) من قانون الإجراءات الجزائية الفرنسي بالنسبة للجنايات، والمادتين (436 و 452) بالنسبة لمحكمة الجنح، والمادة (536) بالنسبة للمخالفات، وفي الجزائر انظر المواد(143، 147 و 155) من قانون الإجراءات الجزائية.

[310]– وفي هذا الصدد دافعت محكمة النقض المصرية في حكم لها على هذا المبدأ بشكل رائع جدا مصرحة " **إن القانون قد أمد القاضي في المسائل الجنائية بسلطة واسعة، وحرية كاملة في سبيل تقضي ثبوت الجرائم، أو عدم ثبوتها، ففتح**

ثالثا–نظام الإثبات المختلط:[311] وهو نظام وسط بين نظام الإثبات المقيد ونظام الإثبات الحر، وفيه تم التصدي للانتقادات الموجهة لنظام الإثبات الحرّ حول خشية تعسف القاضي الجزائي و خروجه عن جادة الصواب، وذلك بأن حدد له وسائل الإثبات التي يلجأ إليها لتأسيس حكمه. كما تم تلافى ما وجه من انتقادات لنظام الإثبات المقيّد، لما جعل دور القاضي سلبيا في عملية الإثبات، وذلك من خلال إعطاء القاضي الجزائي الحرية في تقدير ووزن ما يعرض عليه من أدلة ثبوتية وفقا لاقتناعه الشخصي[312].

من هنا يتبين بأن منطق هذا النظام يرتكز من جهة على تحديد قائمة أدلة الإثبات والقيمة الاثباتية لكل منها سلفا من قبل المشرع، ومن جهة أخرى منح القاضي الجزائي سلطة تقديرية واسعة في موازنة وقبول الأدلة المطروحة أمامه وفقا لاقتناعه الذاتي[313].

واعتبارا لما سبق، نستنتج بأن مسألة مشروعية الدليل الالكتروني في الوجود تثور بالدرجة الأولى في الأنظمة القانونية التي تتبنى نظام الإثبات المقيد، إذ لا يمكن في ظلّها الاعتراف للدليل الالكتروني بأية قيمة إثباتيه ما لم ينص عليه القانون صراحة ضمن قائمة أدلة الإثبات المقبولة، ومن ثم لا يجوز للقاضي الجزائي أن يستند إليه لتكوين قناعته مهما

له باب الإثبات على مصراعيه، فيختار من كل طرقه ما يراه موصلا إلى الكشف عن الحقيقة، ويزن قوة الإثبات المستند من كل عنصر بمحض وجدانه، فيأخذ ما تطمئن إليه عقيدته، و طرح ما لا يرتاح إليه، وغير ملزم بان يسترشد في قضائه بقرائن معينة، بل له مطلق الحرية في تقدير ما يعرض عليه منها، ووزن قوتها التدليلية في كل حالة، حسبما يستفاد من وقائع كل دعوى، وظروفها بغيته الحقيقة أنى وجدها ومن أي سبيل يجده مؤديا إليها، ولا رقيب عليه في ذلك غير ضميره وحده، هذا هو الأصل الذي أقام عليه القانون الجنائي قواعد الإثبات، لتكون موائمة لما تستلزمه طبيعة الأفعال الجنائية، وتقتضيه مصلحة الجماعة من وجوب معاقبة كل جاني و تبرئة كل بريء" نقلا عن: **هلال عبد أللاه أحمد**، حجية المخرجات الكومبيوترية ...، مرجع سابق، ص 33.

[311]– من التشريعات التي أخذت بالنظام المختلط، القانون الياباني، القانون الشيلي، و القانون العراقي.

[312]– **سامي جلال فقي حسين**، الأدلة المتحصلة من الحاسوب...، مرجع سابق، ص 93.

[313]–**عفيفي كامل عفيفي**، جرائم الكمبيوتر و حقوق المؤلف والمصنفات الفنية ...، مرجع سابق، ص 373.

توافرت فيه شروط اليقين.

أما بالنسبة للأنظمة القانونية التي تعتمد نظام الإثبات الحرّ كما هو الحال في القانون الجزائري[314]، فمسألة مشروعية وجود الدليل الالكتروني لا تثار إطلاقا، على اعتبار المشرع لا تعهد إليه سياسة النص على قائمة أدلة الإثبات، فالأساس هو حرية الأدلة، لذلك فمسألة قبول الدليل الالكتروني لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه لتقدير القاضي.

وفي هذا الصدد نجد المشرع الجزائري وكغيره من التشريعات المنتمية إلى نظام الإثبات الحرّ لم يفرد نصوصا خاصة تملي على القاضي الجزائي مقدما بقبول أو عدم قبول أي دليل بما في ذلك الدليل الالكتروني، إذ جاء القانون رقم (09-04) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها خاليا من أية أوضاع خاصة بالدليل الالكتروني ليترك الأمر بذلك للقواعد العامة، وعليه فالأصل في الأدلة مشروعية وجودها ومن ثم فالدليل الالكتروني سيكون مشروعا في الوجود اصطحابا للأصل.

الفرع الثاني: مشروعية الدليل الإلكتروني في التحصيل

يقصد بمشروعية التحصيل، أن تتم عملية البحث عن دليل الإدانة وتقديمه للقضاء من طرف القائمين بالتحقيق وفقا للقواعد والإجراءات التي رسمها القانون لذلك[315]، فمشروعية الدليل إذا تتطلب صدقه في مضمونه، وأن يكون هذا المضمون قد تم الحصول عليه بطرق

---

[314]– كرّس المشرع الجزائري نظام الإثبات الحر في المادة (212) من قانون الإجراءات الجزائية الجزائري التي تنص على انه " **يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه وفقا لاقتناعه الشخصي**"

[315] -**DEMARCHI Jean-Raphael** «La loyauté de la preuve en procédure pénale, outil transnational de protection du justiciable » Recueil Dalloz, 2007, p 2012 .

مشروعة تدلّ على الأمانة والنزاهة[316]. فمتى كان الأمر كذلك، كانت المشروعية حدا فاصلا بين حق الدولة في توقيع العقاب لضمان أمن واستقرار المجتمع وبين حق الأفراد في ضمان حقوقهم وحريات الأساسية[317].

لذلك لما كان الدليل المستمدّ من الوسائل الالكترونية الحديثة أكثر الأدلة اقتحاما وتعديا على حقوق وحرمات الأفراد، استوجب عدم قبوله في العملية الاثباتية إلا إذا تم الحصول عليه في إطار أحكام القانون واحترام مبادئ العدالة وأخلاقياتها. فرغم إقرار مبدأ حرية القاضي الجزائي في الإثبات إلا أن هذه الحرية يعني ألا تمتدّ الى قبول أدلة وليدة إجراء غير مشروع ليس لان ذلك يتعارض مع قيم العدالة فحسب، إنما لأنه يمس بحق المتهم في الدفاع أيضا[318].

وعلى هذا الأساس، فعملية جمع الأدلة الالكترونية إذا خالفت الأحكام والمبادئ الإجرائية التي تنظم طريقة الحصول عليها تكون باطلة، وبالتالي بطلان الدليل المستمد منها عملا بقاعدة " **ما بني على باطل فهو باطل**"[319]. وترتيبا على ذلك فلا يجوز للقاضي القبول بدليل الكتروني تم الحصول عليه من إجراء التسرب جرى القيام به دون مراعاة الشروط الشكلية والموضوعية للإذن بمباشرة هذا الإجراء، أو كان الدليل متحصلا عليه عن طريق إكراه المتهم المعلوماتي على فك شفرة أو الإفصاح عن كلمة السر اللازمة للولوج إلى الملفات المخزنة داخل النظم المعلوماتية، أو القيام بإجراء التصنت أو المراقبة الالكترونية عن بعد دون مسوغ قانوني، أو باستخدام طرق التدليس و الغش و الخداع، لأن الدليل

---

[316]- **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 394..

[317]– **رمزي رياض عوض**، سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية، القاهرة، 2004، ص 154.

[318]– المرجع نفسه، ص 154.

[319]– **علي حسن الطوالبه**، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي، مرجع سابق، ص 4.

المتحصل وفق الطرق السابقة يكون باطلا وفاقدا للمشروعية[320].

من هنا، اتخذت محكمة النقض الفرنسية موقفا صارما في حظر استخدام وسائل الغش والخداع في إجراء المراقبة، وذلك من خلال قضية ويلسون الشهيرة أو ما أطلق عليها **(بفضيحة الأوسمة)** التي تتلخص وقائعها في قيام قاضي التحقيق بتقليد صوت أحد المتهمين من أجل الحصول على معلومات وأسرار القضية، ولما حصل القاضي من خلال هذا الاتصال على اعتراف منه باشتراكه في الجريمة استعمله كدليل إدانة من قبل قاضي الموضوع، إلا أن محكمة النقض تصدت لحكم الإدانة الذي أسس على هذا الاعتراف بالإلغاء معتبرة بأن قاضي التحقيق قد لطخ كرامة القضاء وأهان سمعته باستخدامه إجراء تنبذه قواعد الأمانة والشرف، وفي الوقت نفسه ارتكب فعلا مخلا بواجبات ونزاهة القاضي[321].

والقاعدة أن لا يتوقف البطلان عند الإجراء الذي يشوبه عيب من عيوب البطلان فحسب بل يمتد إلى الإجراءات اللاحقة له مباشرة، وهو الموقف الذي تبناه المشرع الجزائري في المادة(191) من قانون الإجراءات الجزائية التي تنص على انه " **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 كلها أو بعضها** ". والموقف نفسه اتخذه المشرع الفرنسي حينما نص في الفقرة الثانية من المادة(93) على أن البطلان يلحق الإجراء المعيب والأعمال التالية له بغض النظر عن توافر رابطة معينة بينها[322].

---

[320]–**عمرو حسين عباس**، مرجع سابق، ص 08.

[321]– **بن بلاغة عقيلة**، حجية أدلة الإثبات الجنائية، مذكرة لنيل شهادة الماجستير، فرع القانون الجنائي،جامعة الجزائر، 2011، ص 117.

[322]– وقد عبر الفقه الانجلوسكسوني على هذه القاعدة بنظرية " **الشجرة المسمومة** " **(poisonous tree fruits)** والتي مفادها أن الشجرة السامة لا تطرح إلا ثمارا سامة، لان الطبيعة السامة للأصل لا بد أن تنتقل بالضرورة إلى الفرع، و

ولا ينتهي الأمر عند هذا الحد، بل أن تعمد مخالفة القانون في الحصول على الدليل قد يترتب عليه عقوبات جزائية و إدارية فضلا عن المسؤولية المدنية، فالموظف الذي يعهد إليه القانون القيام بالبحث والتحقيق فيتصرف على وجه مخالف للشروط والإجراءات المعمول بها قانونا، يعد مقصرا في عمله و مخلا بواجباته يستحق المؤاخذة[323].

وفي إطار تكريس إلزامية احترام مبدأ مشروعية الدليل الالكتروني صادقت لجنة الوزراء التابعة للمجلس الأوروبي بتاريخ 1981/01/28 على اتفاقية خاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة كاملة، صحيحة ودقيقة ومستمدة بطرق مشروعة وعدم إفشائها أو استعمالها في غير الأغراض المخصصة لها[324]. وقد تأكد هذا المعنى في الاتفاقية الأوروبية لمنع التعذيب وسائر المعاملات غير الإنسانية والمنحطة من الكرامة الإنسانية والمهينة الصادرة في 26-11-1987، وكذا في الاتفاقية الدولية لمنع التعذيب الصادرة عن منظمة الأمم المتحدة في 1-12-1994، إذ اعتبرت كل دليل تم الحصول عليه نتيجة تعذيب أو اعتراف وليد ضغط أو إكراه ترغيب أو ترهيب مهما يكن قدره بمثابة دليل باطل ومن واجب القاضي استبعاده[325]، في السياق ذاته أوصى المؤتمر

الشيء نفسه يحدث بالنسبة للأدلة الجنائية، فعدم مشروعية الدليل الأصلي تمتد إلى الدليل الفرعي أو اللاحق، وعليه يتعين استبعادهما معا، طالما أن الدليل الثاني يرتبط بالأول و يترتب عليه. أنظر: **سليمان أحمد فضل**، مرجع سابق، ص 380.

[323]- تنص المادة (107) من قانون الإجراءات الجزائية الجزائري على " **يعاقب الموظف بالسجن المؤقت من خمس الى عشر سنوات إذا أمر بعمل تحكمي أو ماس سواء بالحرية الشخصية للفرد او الحقوق الوطنية لمواطن أو أكثر** " و تضيف المادة (135)من القانون نفسه " **كل موظف في السلك الإداري أو القضائي و كل ضابط شرطة ... دخل بصفته المذكورة منزل احد المواطنين بغير رضاه، وفي غير الحالات المقررة في القانون وبغير الإجراءات المنصوص عليها فيه، يعاقب بالحبس من شهرين إلى سنة و بغرامة من 20000دج الى 100000 دج دون الإخلال بتطبيق المادة 107**".

[324]- **أحمد يوسف الطحطاوي**، مرجع سابق، ص 155.

[325]- المرجع نفسه ، ص267.

الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في البرازيل في الفترة من 04-09 سبتمبر 1994 في مجال حركة إصلاح الإجراءات الجزائية وحماية حقوق الإنسان في توصيته رقم (18) بان كل الأدلة المتحصلة عن طريق انتهاك حق من الحقوق الأساسية للمتهم تعد باطلة ولا يمكن التمسك بها أمام القضاء أو مراعاتها في أية مرحلة من مراحل الدعوى، وأكد على ضرورة احترام مبدأ المشروعية عند التحقيق والبحث عن الدليل في الجرائم الالكترونية وإلا ترتب عليه بطلان الإجراءات[326].

واقتداء بالنصوص الدولية المذكورة أعلاه، وضعت معظم الدساتير الوطنية[327]، والقوانين الإجرائية الداخلية[328]، نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بحقوق حرية الأفراد، وأي دليل تم استخلاصه بشكل مخالف لهذه النصوص يعد غير مشروع ويفقد قيمته في عملية الإثبات.

ولقد جسّدت التطبيقات القضائية المقارنة هذا التوجه عدة مرات، إذ أحكمت محكمة النقض الفرنسية قبضتها بقوة على حالات اللجوء لكل تقنيات التحري والبحث التي لا تتجاوب مع مقتضيات مبدأ قانونية أو مشروعية الدليل، وأكدت عدم التساهل في تطبيق جزاءات الإخلال بهذا المبدأ بقولها " **حيث انه لا توجد أحكام قانونية تمنع القاضي الجزائي من أن يستبعد استعمال أدلة متحصل عليها من شخص قدمه لجهاز التحقيق لسبب واحد، لأنه تم الحصول عليه (الدليل) بطريقة غير مشروعة** "[329]. وتأسيسا على هذا الموقف اصدرت المحكمة قرارا في 04 جوان 2008 انتقدت فيه حكم إدانة السلطات القضائية

---

[326]– **أحمد يوسف الطحطاوي**، مرجع سابق، ص 268.

[327]– نذكر منها المواد(32، 34، 2/35، 46، 48) من الدستور الجزائري لعام 1996، و المواد(41، 44، 45، 47) من الدستور المصري لعام 1971 المعدل والمتمم. والمادتين (10 و 18) من الدستور الأردني الحالي.

[328]– أنظر المواد (44، 45 و 47) من قانون الإجراءات الجزائية الجزائري.

[329] -**QUEMENER Myriam, CHAPRENEL Yves** «Cybercriminalité, Droit pénal applique » op.cit., P172.

الفرنسية لمواطن فرنسي بجريمة الاستغلال الجنسي للأطفال عبر الانترنت(cyber-pédopornographiques) بناءا على معلومات محصلة من طرف السلطات الأمريكية، بعدما لاحظت بأن الموقع المجرم تم إنشاءه من طرف مصالح شرطة نيويورك الخاصة بمكافحة هذا النوع من الجرائم، واعتبرت أن الأدلة المقامة ضد المتهم ليست مشروعة لأنها وقعت نتيجة تحريض، وهو إجراء غير مرخص به في القانون الفرنسي، وبما أن التحريات تمت وفقا " لخدعة من طرف السلطات الأمريكية لحث المعني لارتكاب الجريمة " فلا يمكن اعتبارها قد رعت مبدأ المشروعية، وعليه فالمتابعات يتم إلغاؤها بالرغم من تحقق إدانة المتهم بالجريمة المنسوبة إليه[330].

وينبغي الإشارة هنا إلى أن شرط مشروعية الدليل مطلوب في حالة الإدانة فقط، إذ لا يجوز أن تبنى الإدانة الصحيحة على دليل باطل، أما في حالة البراءة فالمشروعية ليست شرطا واجب التوفر في الدليل، إذ في هذه الحالة يمكن للمحكمة أن تستند إلى دليل فقد شروط صحته كشهادة قاصر غير مميز أو كان ثمرة إجراء باطل لإقرار براءة المتهم[331].

والحقيقة أن معيار قبول أية وسيلة علمية مستمدة في مجال الإثبات الجنائي لإظهار الحقيقة يرتكز أساسا على عدم إهدارها للحريات العامة للفرد وكرامته الإنسانية، وهو الأمر الذي يحرص عليه القاضي الجنائي لكي يوازن بين ما هو مشروع فيقبله وما هو غير مشروع فيتصدى له.

---

[330]- Cass.Crim, 04 juin 2008, bulletin criminel, N 141, 2008.

[331]– **أحمد يوسف الطحطاوي**، مرجع سابق، ص 267.

المطلب الثاني

حجية الدليل الإلكتروني في الإثبات الجزائي

يقصد بحجية الدليل الالكتروني ما يتمتع به من القوة الاستدلالية في كشف الحقيقة وصدق نسبة الفعل الإجرامي إلى شخص معين أو كذبه[332]، لذلك فمجرد الحصول على الدليل وتقديمه إلى القضاء لا يكفي لاعتماده كدليل إدانة، إنما ينبغي تقديره وفحص قيمته في إثبات الواقعة الإجرامية، ومسألة تقييم الدليل هي مسألة موضوعية محضة تدخل في صميم سلطة القاضي التقديرية بحثا عن الحقيقة. فالسائد في الفقه أن سلطة القاضي الجزائي في تقدير الدليل يحكمها مبدأ حرية القاضي في تكوين قناعته، مما يستتبع ذلك حتما نتيجة مهمة ألا وهي " **حرية القاضي في تقدير الأدلة** "[333]، وعملا بهذا المبدأ فالقاضي الجزائي كما يصح له أن يؤسس اقتناعه على أي دليل، له أن يهدره أيضا.

ومقابل ذلك لا ينبغي أن يفهم من حرية القاضي في الاقتناع التحكم المطلق في الأمور والقضاء كيف ما شاء وفقا لأهوائه ومزاجه الشخصي، إنما هو مطالب بتحري المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه واستلهام عقيدته، وألا يكون تفكيره هذا قد جافى الأصول المسلّم بها في الاستدلال القضائي[334].

---

[332]– **ياسر محمد الكومى محمود أبو حطب**، مرجع سابق. ص 303.

[333]– وقد أكدت هذا المبدأ المادة (307) من قانون الإجراءات الجزائية الجزائري المستوحاة مباشرة من المادة (353) من القانون الفرنسي بنصها 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 تقديم تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت و تدبر، أن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المستندة إلى المتهم و أوجه الدفاع عنها ولم يضع القانون لهم سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم : هل لديكم اقتناع شخصي؟**".

[334]– **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي والتكنولوجية الحديثة، مرجع سابق، ص 13.

ولتحقيق ذلك، أحاطه القانون بمجموعة من القيود التي تشكل في مجملها شروطا لإعمال المبدأ وتطبيقه التطبيق السليم بما يضمن بلوغ الحقيقة دون المساس بالحقوق والحريات العامة للأفراد.

ولا شك أن تطبيق ذلك على الدليل الالكتروني قد يثير عدة صعوبات، فالقاضي الجزائي بثقافته القانونية وعدم كفاءته الفنية في مجال المعلوماتية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الالكتروني، فضلا عن تمتع هذا الدليل في قوته التدليلية بقيمة اثباتية قد تصل إلى حد اليقين شأنه في ذلك شأن الأدلة العلمية عموما، ناهيك عن الطبيعة الفنية الخاصة بالدليل الالكتروني والتي تمكن من العبث بمضمونه بسهولة على نحو يحرف الحقيقة دون أن يكون بمقدور غير المتخصص إدراك ذلك[335].

وبوجود هذه الصعوبات وغيرها يطرح تساءل مهم عن مدى سلطة القاضي الجزائي في تقدير ومناقشة الدليل الالكتروني في مصداقيته وبالتالي قبوله أو رفضه لعدم اقتناعه به ؟

وعلى هدى ما سبق طرحه سوف نستعرض الشروط الواجب توفرها في الدليل الالكتروني حتى يعبّر عن حقيقة علمية محققة الحجية (الفرع الأول) ثم نبرز دور ذلك في تكوين الاقتناع الشخصي للقاضي الجزائي(الفرع الثاني).

الفرع الأول: شروط إ كتساب الدليل الإلكتروني حجية في الإثبات

الدليل الالكتروني ما هو إلا تطبيق من تطبيقات الدليل العلمي الذي يعبر عن حقيقة علمية ثابتة، فهو يتمتع بحجية قوية في الإثبات، وذلك بما يتميّز به من موضوعية وحياد، ولكونه محكما بقواعد علمية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته[336]، ويساعد

---

[335]– **أحمد يوسف الطحطاوي**، مرجع سابق، ص 233.

[336]– لقد اعترف المشرع الفرنسي بحجية قوية للأدلة الناشئة عن الوسائل الالكترونية مثل الحواسب، الرادارات و أجهزة التصوير والتسجيل والتصنت، كما نص المشرع البريطاني في قانون البوليس والإثبات لعام 1984 المعدل و المتمم على

القاضي في التقليل من الأخطاء القضائية، والاقتراب أكثر إلى تحقيق العدالة، والتوصل بدرجة أكبر من الحقيقة. لأن التقنية العلمية قد توفر طرقا دقيقة لجمع الأدلة ذات قوة علمية يصعب إثبات عكسها[337].

ومع هذا فرغم أن الدليل الالكتروني بحكم طبيعته العلمية وموضوعيته وحياده يمثل إخبارا صادقا عن الواقع، إلا أن ذلك لا يستبعد أن يكون موضع شك في سلامته من العبث عن طريق التحريف أو التغيير من ناحية، وفي صحة الإجراءات المتبعة للحصول عليه من ناحية أخرى.

وإذا كان الشك في مصداقية الدليل الالكتروني مرتبطا أساسا بعوامل خارجية مستقلة عنه لا بمضمونه، فاكتسابه حجية داحضة في الإثبات وكذا قبوله كدليل تبنى عليه الحقيقة في الدعوى الجزائية يتطلب توافر الشروط التالية:

-أولا- يقينية الدليل الإلكتروني

يشترط في الأدلة الالكترونية أن تكون غير قابلة للظن أو الترجيح حتى يشيّد عليها الحكم بالإدانة، لأنه لا مجال لدحض قرينة البراءة أو افتراض عكسها إلا عند بلوغ اقتناع القاضي حد الجزم و اليقين[338].

أن الأدلة الالكترونية الناتجة عن الحاسب بصفة سليمة تكون ذات دلالة يقينية في الإثبات، وفي كندا فالرأي السائد في الفقه هو اعتبار مخرجات الحاسب من أفضل الأدلة يحقق اليقين المنشود في الأحكام الجزائية، وفي السياق نفسه نصت بعض القوانين في الولايات المتحدة الأمريكية كقانون الحاسب الآلي لولاية (ايوا) الصادر في عام 1984 وقانون الإثبات لولاية (كاليفورنيا) المؤرخ في 1983 على أن النسخ المستخرجة من البيانات التي يحتويها الحاسب تعد من أفضل الأدلة المتاحة للإثبات مما يحقق اليقين لهذه الأدلة. للمزيد من التفاصيل انظر: **ياسر محمد الكومى محمود أبو حطب** ، مرجع سابق، ص.ص 305-308.

[337]- **بوكر رشيدة**، مرجع سابق، ص 497.

[338]- **علي حسين محمد طوابلة**، مرجع سابق، ص 190.

ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال التمعّن والتدقيق فيما يعرض عليه من وقائع الدعوى وأدلة الكترونية على اختلاف أشكالها، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التأكيد بالنسبة لها، وهكذا يستطيع القاضي أن يحدد قوتها الاستدلالية على صدق نسبة جريمة من الجرائم الالكترونية إلى شخص معين من عدمه[339].

ويعتمد القاضي الجزائي عادة لبلوغ اليقين والجزم في اقتناعه بالأدلة على نوعين من المعرفة، الأولى هي المعرفة الحسية التي تستنبط من الحواس بعد معاينته لهذه المخرجات وفحصها، أما الثانية فهي المعرفة العقلية التي يدركها القاضي عن طريق التحليلات، والاستقراءات والاستنتاجات التي يجريها على المخرجات الالكترونية وربطها بالملابسات التي أحاطت بها[340]. فإن لم ينته القاضي إلى الجزم بنسبة الجريمة الالكتروني إلى المتهم تعين عليه القضاء بالبراءة، لأن الشك يفسر لصالح المتهم[341].

وحتى يتحقق اليقين للأدلة الالكترونية أكثر ينبغي إخضاعها للتقييم الفني بوسائل فنية من طبيعة هذا الدليل تمكّن من فحصه للتأكد من سلامته من العبث، وكذا صحة الإجراءات المتبعة في الحصول عليه، فمثلما يخضع الدليل الالكتروني لقواعد وإجراءات معينة تحكم طرق الحصول عليه، فإنه يخضع كذلك لقواعد أخرى تحكم على قيمته التدليلية من الناحية العلمية، ولعل من أهم هذه الوسائل مايلي:

1ـــ تقييم الدليل الإلكتروني في سلامته من العبث: إن الطبيعة التقنية للدليل الالكتروني تجعله في الغالب عرضة للشك والظنون في سلامته، وذلك راجع إلى إمكانية

---

[339] – **إيمان محمد علي الجابري**، يقين القاضي الجنائي، منشأة المعارف، الإسكندرية، 2005، ص 131.

[340]– **علاء عبد الباسط خلاف**، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 2002، ص 463.

[341]– **سليمان أحمد فضل**، مرجع سابق، ص 373.

تعرضه للعبث والخروج به على نحو يخالف الحقيقة، فقد يقدم هذا الدليل ليعبر عن واقعة معينة صنع خصيصا من أجل التعبير عنها خلافا للحقيقة، وذلك دون أن يكون بمقدور غير المتخصص إدراك ذلك العبث، على نحو يمكن القول معه أن ذلك قد أصبح هو الشأن في النظر لسائر الأدلة التقنية التي تقدم للقضاء، فالتقنية الحديثة تمكّن من العبث بالدليل الالكتروني التقني بسهولة و يسر ليظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة[342].

ولأجل التأكد من سلامة الدليل الالكتروني من التغيير أو العبث تتم الاستعانة عادة بمجموعة من الآليات التالية:

أ ــ تقنية التحليل التناظري الرقمي: وهي تقنية يتم من خلالها مقارنة الدليل الرقمي المقدّم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثمة يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا[343]، ويستعان في ذلك بتكنولوجية الإعلام الآلي التي أثبتت دورها الفعّال في تقديم المعلومات الفنية التي تساهم في فهم مضمون وكينونة الدليل التقني، وكشف مدى التلاعب بمضمون هذا الدليل.

ب ــ استخدام عمليات حسابية خاصة تسمى بالخوارزميات: ويتم اللجوء إلى هذه العملية عادة في حالة عدم الحصول على النسخة الأصلية للدليل الالكتروني أو في حالة ما إذا كان هناك شك في أن العبث قد مسّ النسخة الأصلية، فهنا تسمح هذه التقنية بالتأكد من مصداقية الدليل الالكتروني وسلامته من العبث بالتبديل أو التحريف.

ج ـ استخدام الدليل المحايد: وهو نوع من الأدلة الالكترونية الرقمية المخزنة في البيئة الافتراضية ولا علاقة له بموضوع الجريمة، ولكنه يساهم في التحقق من مدى سلامة الدليل

---

[342]– **Ammar.(D)** « preuve et vraisemblance, contribution a l'étude de la preuve technologique » RTD Civ, juillet-septembre, 1993, p 499.

[343]– **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي والتكنولوجية الحديثة، مرجع سابق، ص 27.

الالكتروني المقصود في عدم وقوع تعديل أو تغيير في نظام الحاسوب[344].

2 ــ تقييم الدليل الإلكتروني في السلامة الفنية لإجراءات تحصيله

إذا كانت نسبة الخطأ الفني في الحصول على الدليل الالكتروني ضئيلة جدا باعتباره تطبيقا من تطبيقات الدليل العلمي الدقيقة كما أسلفنا الذكر، فذلك لا يعني أنها منعدمة تماما، إنما يظل الوقوع في الخطأ ممكنا أثناء استخلاصه[345]، ويكون ذلك إما بسبب الخطأ في استخدام الأداة المناسبة لاستخلاص الدليل، كالخلل في الشفرة المستخدمة، أو استعمال معلومات ومواصفات خاطئة. وإما بسبب الخطأ في استخدام أداة تقل نسبة صوابها مائة بالمائة (100%)، مثل ما يحدث غالبا في وسائل اختزال المعطيات أو معالجتها بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.

ومن أجل تجنب مثل هذه الأخطاء يمكن إتباع بعض الاختبارات والتطبيقات للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الالكتروني من حيث إنتاجها لدليل

---

[344]– **ممدوح عبد الحميد عبد المطلب**، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد بدبي في الفترة من 10–12 ماي 2003 ، ص.ص 2246–2247.

[345]– لقد تضمنت المادة (69) من قانون الشرطة والإثبات الجنائي البريطاني تحذيرا من هذه الأخطاء الفنية التي يمكن أن تنال من مصداقية الدليل الالكتروني بنصها على انه " **لا يكون البيان المتضمن في مستند صادر عن طريق الحاسب مقبولا كدليل على أية واقعة واردة فيه إلا إذا تبين : 1– عدم وجود أسس معقولة لاعتقاد بان البيان يفتقد الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسب. 2– أن الحاسب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فأي جزء لم يكن يعمل فيه بصورة سليمة أو كان معطلا عن العمل، لم يكن ليؤثر في أخراج المستند أو دقة محتوياته. 3– الوفاء بالشروط المتعلقة بالمستند المحددة طبقا لقواعد المحاكمة (المتعلقة بالطريقة او الكيفية التي يجب أن تقوم بها المعلومات الخاصة بالبيان المستخرج عن طريق الحاسب)**. أنظر :

-CASILE Jean François « plaidoyer en faveur d'aménagement de la preuve de l'infraction informatique » Revue des sciences criminelles et de droit pénal comparé (R.S.C.D.P.C) , N 01, Paris, 2004, PP 76-78. et **Ammar (D)**, op.cit., p 500.

تتوافر فيه المصداقية لقبوله كدليل إثبات، والتي نلخصها فيما يلي:

أ ــ إخضاع الأداة المستخدمة في الحصول على الدليل لعدة تجارب بغية التأكد من دقتها في إعطاء النتائج المبتغاة: ويكون ذلك بإتباع اختبارين أساسيين يتم من خلالهما التأكد من أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الالكتروني، وفي الوقت نفسه لم تضف إليها أي بيان جديد، وهو ما قد يعطي للنتائج المقدمة عن طريق هذه الأداة مصداقية في التدليل على الوقائع. ويتمثل هذان الاختباران فيما يلي :

1-اختبار السلبيات الزائفة: وفيه يتم إخضاع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الالكتروني دون إغفال أية بيانات مهمة عنه.

2-إختبار الإيجابيات الزائفة: ومفاده إخضاع الأداة المستخدمة في الحصول على الدليل الالكتروني لاختبار فني يمكّن من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة[346].

ب ــ الاستعانة بأدوات ذات تقنية عالية أثبتت التجارب العلمية مجاعتها في تقديم نتائج أفضل: هناك دراسات وبحوث علمية متخصصة في مجال تقنية المعلومات حددت الأدوات السليمة التي يجب إتباعها في سبيل الحصول على الدليل الالكتروني، وفي المقابل بينت كذلك الأدوات المشكوك في كفاءتها وحثت على اجتنابها، وعليه فاختيار أية أداة من هذه الأدوات من شأنه أن يؤثر على مصداقية المخرجات المستمدة منها[347].

ومن هنا، يمكن القول بأنه إذا سلمنا سابقاً بإمكانية التشكيك في سلامة الدليل الالكتروني بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية

---

[346]- **بوكر رشيدة**، مرجع سابق، ص501. و**أحمد يوسف الطحطاوي**، مرجع سابق، ص 238.

[347]- **طارق محمد الجملي**، مرجع سابق، ص 28.

لا يمكن للقاضي أن يقطع في شأنهما برأي حاسم إن لم يقطع به أهل الاختصاص، لذلك فإذا توافرت في الدليل الالكتروني الشروط المذكورة سابقاً بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استناداً لسلطة القاضي التقديرية[348]. لأن سلطة القاضي في ردّ الدليل استناداً لفكرة الشك يستلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، وهو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة، فيقتصر دوره على بحث صلة الدليل بالجريمة فقط. ولا شك أن الخبرة الفنية تحتل في هذه الحالة دروا مهما في التثبت من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، بل البحث في مصداقية هذا الدليل هو من صميم فن الخبير لا القاضي.

ـ ثانيا: وجوب مناقشة الدليل الإلكتروني

إن تحقق شرط سلامة الدليل الالكتروني من العبث وسلامته من الخطأ في إجراءات التحصيل وحده لا يكفي لاكتسابه حجية دامغة في الإثبات، بل لابد أيضا من مناقشة هذا الدليل بصفة علانية في جلسة المحاكمة وفقا لمبدأ أساسي في الإجراءات الجزائية هو مبدأ الشفوية والمواجهة[349]. فلا يجوز للقاضي الجزائي أن يأخذ بدليل قدمه أحد أطراف الدعوى أو يبني حكمه على أساسه إلا إذا عرضه شفويا في جلسة المحاكمة ليعلم به سائر أطراف الدعوى، فتتاح لهم مناقشته والرد عليه وإبداء أرائهم في قيمته القانونية.

ويترتب عن ذلك عدم جواز اقتناع القاضي من معلومات شخصية حصل عليها خارج الجلسة أو في غير نطاق المرافعات والمناقشات التي جرت فيها، وإلاّ يكون بذلك قد جمع

---

[348]– هذا ما أكدته المحكمة الاتحادية الأمريكية في القضية المعروفة ب (**United States v. Russo**) لعام 1974 حينما قررت المحكمة انه " **مع افتراض استخدام حاسب يؤدي وظائفه بشكل سليم، ومع توافر الثقة فيه وإمكانية التعويل عليه، فان مخرجاته يجب أن تكون مقبولة كدليل على المعاملات التي أدخلت فيه**" نقلا عن: **هشام محمد فريد رستم**، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 182.

[349]– **سليمان أحمد فضل**، مرجع سابق، ص 375.

في شخصه صفتين متعارضتين هما صفة الشاهد وصفة القاضي، مما يبعث الحرج في نفسية الخصوم ويعيقهم عن مناقشة شهادته والرد عليها بحرية، لان اعتماده على علمه الشخصي يجعله عرضة للتهم والشبهات وهو الأمر الذي يجب أن يتنزه القضاء عنه عموما[350].

كما لا يجوز للقاضي الجزائي أن يبني اقتناعه على رأي الغير، إلا إذا كان من الخبراء والفنيين الذين استشارهم وفقا للقانون و ارتاح ضميره لرأيهم فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه[351].

وعليه فإذا كان القاضي لا يمكنه أن يحكم في الجرائم الالكترونية استنادا إلى علمه الشخصي، أو استنادا إلى رأي الغير كما أسلفنا الذكر، فذلك يحتّم عليه أن يعيد تحقيق و مناقشة كافة الأدلة المتولدة من الحاسبات الالكترونية القائمة في ملف الدعوى لكي يتمكّن من تكوين اقتناع يقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاض عادل، فمثلا بالنسبة لشهود الجرائم المعلوماتية[352] الذين تم سماعهم من قبل في التحقيق الابتدائي فانه يجب إعادة سماعهم مرة أخرى أمام محكمة الموضوع، كذلك بالنسبة لخبراء المعلوماتية على اختلاف تخصصاتهم ينبغي أن يمتثلوا أمام المحكمة لمناقشة تقاريرهم التي خلصوا إليها[353].

---

[350]– **نبيل إسماعيل عمر** " قاعدة عدم قضاء القاضي بعلمه الشخصي" المجلة العربية للدراسات الأمنية، المجلد الأول، العدد الأول، الرياض، 1989، ص 24.

[351]– **علي محمود علي حمودة**، مرجع سابق، ص 120.

[352]– يقصد بالشاهد المعلوماتي، الفني المتخصص في تقنية الإعلام الآلي والذي لديه معلومات جوهرية لولوج نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي البحث عن أدلة الجريمة داخله. للمزيد من التفاصيل أنظر:

-**AMORY (B) et POULLET (Y)**, le droit de la preuve face a l'informatique et la télématique, revue international de droit comparé, N 2, Paris, Avril 1985, p335 .

[353]- **علي حسن الطوالبه**، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي، مرجع سابق، ص 13. و**أحمد يوسف الطحطاوي**، مرجع سابق، ص157.

لأن بهذا التصرف يكون القاضي قد حقق رقابة فعالة على جدية الأدلة التي تكون قد حصلت في مرحلة التحقيق فتعرض عليه مجددا، وهو ما يتيح له مراقبة التقدير الذي كانت سلطة التحقيق قد خلصت إليه بخصوص وقائع الجريمة الالكترونية.

اعتبار لذلك، أرست معظم تشريعات العالم هذه القاعدة وجعلتها عنصرا جوهريا لقبول أي دليل، فنجد الفقرة الثانية من المادة(427) من قانون الإجراءات الجنائية الفرنسي تنص على أنه " **لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة و نوقشت أمامه في مواجهة الأطراف**" وفي السياق نفسه نصت المادة (302) من قانون الإجراءات الجنائية المصري انه " **لا يجوز للقاضي أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة**" أما المشرع الجزائري فقد تبنى شرط مناقشة الأدلة ضمن الفقرة الثانية من المادة (212) من قانون الإجراءات الجزائية بالصيغة التالية " **لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه**" [354].

وتبدو المشكلة بالنسبة لمناقشة الأدلة الالكترونية في كون معظم هذه الأخيرة تعتبر أدلة غير مرئية بالعين المجردة وتسجّل على وسائل الكترونية لا يمكن قراءتها أو استخراجها إلا باستعمال أجهزة الكترونية، فضلا عن إمكانية التلاعب في المعلومات المسجلة بمسحها أو استبدال غيرها دون علم احد، وهو ما يثير التساؤل عن إمكانية المناقشة العلانية لهذه الأدلة في أصالتها[355]، ومدى تأثير ذلك على مبدأ قبوله من طرف القضاء. خاصة إذا تعلق

---

[354]– وهو الأمر الذي تمسكت به المحكمة العليا الجزائرية في عدة قراراتها نذكر منها، قرارها الصادر بتاريخ 21-01-1981 القاضي ب " **لا يمكن لقضاة الموضوع أن يؤسسوا قرارهم إلا على الأدلة المقدمة لهم أثناء المرافعات و التي تتم مناقشتها حضوريا**"

[355]– تجدر الإشارة إلى أن هناك اختلافا بين الأصالة للدليل في طابعها المادي وبين طابعها الرقمي لان الأولى ما هي إلا تعبير عن وضعية مادية ملموسة كما هو الحال في الورق المكتوب أو بصمة الأصبع، أو البصمة الوراثية، في حين أن الثانية تمثل تعداد غير محدود لأرقام ثنائية مكونة من صفر و واحد.

الأمر بالدليل المستخرج بواسطة الطابعات، أو المسترجع بعدما تم حذفه باستخدام خاصية الإلغاء، أو عندما يقوم المتهم بإزالة الدليل الرقمي عن بعد، فيكون ما تبقى منه مجرد نسخة يتم التوصل إليها عن بعد بطرق المراقبة الالكترونية، وفي هذه الحالة هل يمكن اعتبار الدليل المسترجع أو الناتج عن المراقبة الالكترونية دليلا أصليا وبالتالي يقبل طرحه على القضاء و مناقشته ضمن أدلة الدعوى ؟

ومن أجل الفصل في هذه المسالة من الناحية القانونية، عمدت بعض التشريعات المقارنة إلى اعتماد منطق افتراض أصالة الدليل الالكتروني الرقمي، اذ نص قانون الإثبات الأمريكي في المادة (3/1001) على انه " **إذا كانت البيانات مخزنة في حاسب أو آلة مشابهة فان أية مخرجات طابعة منها أو مخرجات مقروءة برؤية العين تبرز انعكاسا دقيقا للبيانات تعد بيانات أصلية** " وتضيف المادة (5/1500) من قانون الإثبات لولاية كاليفورنيا لعام 1983 بان " **المعلومات المسجلة بواسطة الحاسب أو برامج الحاسب ، او نسخ أيهما، يجب ألا توصف أو تعامل على أنها غير مقبولة بمقتضى قاعدة –أفضل دليل–** "[356]. وقد ذهب المشرع الأمريكي إلى أبعد من ذلك، فاعترف للنسخة طبق الأصل بنفس القيمة الثبوتية للنسخة الأصلية[357]، وكذلك فعل المشرع الانجليزي والياباني بقبوله ضمن أدلة الإثبات مخرجات الحاسب الآلي التي تم تحويلها إلى صور مرئية، سواء كانت هي الأصل أم كانت نسخا مستخرجة عن هذا الأصل[358]. أما المشرع الألماني فقد جعل من خلال المادة (224) فقرة ثانية من قانون الإجراءات الجزائية مخرجات الحاسب الآلي

---

[356]– **سعيد عبد اللطيف حسن**، إثبات جرائم الكمبيوتر و الجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999، ص 165.

[357]– تنص المادة (1003) من القانون الإثبات الأمريكي على أن " **النسخة المطابقة للأصل تقبل كالأصل إلا أذا أثير حولها تساؤل جدي يتعلق بسلامتها ومصداقيتها، أو إذا كانت الظروف لا تسمح بقبول النسخة المطابقة للأصل محل النسخة الأصلية** ". نقلا عن: **عمر محمد ابو بكر بن يونس**، مرجع سابق، ص 989.

[358] – **AMORY (B) et POULLET (Y),** op cit, p 339.

بأنواعها المختلفة من بيانات أو مطبوعات أو نسخ من قبيل المصادر التي يجب على المحكمة تقبلها في الإثبات. وهو الشيء نفسه الذي تبناه المشرع اليوناني في المادة (364) من قانون الإجراءات الجزائية[359].

ولعل ما دفع هذه الدول إلى التسليم بمنطق افتراض الأصالة في الدليل الالكتروني الرقمي على مستوى القانوني هو الطبيعة التقنية لهذا الدليل التي لا تعبر عن قيمة أصلية بمجرد رفع محتواه من النظام المعلوماتي إذ يظل متواجدا في المكان الذي تم استخلاصه واستدعاؤه منه.

ونخلص إلى أنه إذا كان القانون يشترط لاكتساب الدليل الالكتروني حجية في الإثبات أن يخضع لمناقشة علانية في جلسة المحاكمة، فان دور القاضي في ذلك يبقى محدودا جدا بسبب النقص الفادح في ثقافته المعلوماتية، وهو ما جعل البعض يعتقد انه بمقدار اتساع مساحة الأدلة الالكترونية يكون انكماش وتضاءل دور القاضي الجزائي في التقدير، مما يستتبع بالقول أن التطور العلمي من شانه أن يطغى على نظام الاقتناع القضائي ولا يبقي للقاضي إلا الإذعان للخبراء المختصين دون أي تقدير من جانبه. ومثل هذا الأمر يدفعنا إلى البحث في دور الطابع العلمي للدليل الالكتروني في تكوين الاقتناع الشخصي للقاضي الجزائي.

الفرع الثاني: دور القيمة العلمية للدليل الإلكتروني في تكوين اقتناع القاضي الجزائي

أدى ارتفاع نسبة الجرائم الالكترونية وتعاظم أساليب وتقنيات ارتكابها إلى انضمام الدليل الالكتروني الرقمي إلى حقل الأدلة العلمية الجنائية الموثوقة واحتلاله مرتبة أفضل دليل لإثبات هذا النوع من الجرائم، وهو ما فرض على القاضي الجزائي التعامل معه رغم

[359]– نقلا عن: **أحمد يوسف الطحطاوي**، مرجع سابق، ص.ص 202–203.

نقص ثقافته المعلوماتية من جهة والقيمة العلمية التي يتمتع بها الدليل من جهة أخرى.

وأمام هاتين المعادلتين يثار التساؤل التالي: هل يبني القاضي الجزائي اقتناعه بالدليل الالكتروني على أساس أن أمره محسوم علميا ؟ أو بتعبير أخر، هل يسلم القاضي الجزائي بيقينية الدليل الالكتروني باعتباره دليل علمي وبالتالي الاطمئنان إليه بمجرد عرضه عليه، أم أن ذلك يدخل في محض تقديره الشخصي مثله مثل باقي الأدلة ؟

لقد انقسم الفقهاء في هذه المسالة إلى من يرى بأن الدليل الالكتروني بحكم أصالته العلمية ودقته الفنية التي يبلغ معها إلى درجة اليقين له قوته الثبوتية الملزمة للقاضي[360]، وحجتهم في ذلك أن الدليل العلمي هو النتيجة التي تسفر عنها التجارب العلمية لإثبات أو نفي الواقعة التي يثار الشك حولها، والتي غالبا ما يتطلب فهمها معرفة ودراية خاصة قد لا يملكها القاضي بحكم تكونه القانوني المحض. وما دام الدليل الالكتروني تطبيقا من تطبيقات الدليل العلمي فالقاضي لا يمكنه أن ينازع في قيمة ما يتمتع بها من قوة استدلالية قد تأكدت له من الناحية العلمية[361].

ويذهب أنصار هذا الاتجاه إلى ابعد من ذلك، إذ يعتقدون بأنه ليس بشرط أن يكون اقتناع القاضي بالدليل الالكتروني يقينيا، وأسسهم في ذلك أن القاضي الجزائي لا يملك وسائل إدراك اليقين كحالة ذهنية تلتصق بالحقيقة دون أن تختلط بأي شك على المستوى الشخصي أو جهل أو غلط على المستوى الموضوعي، كما أن الاقتناع ليس اعتقادا، لان القاضي لا يجوز له أن يحكم بناء على أسباب شخصية صلحت لحمله هو على نفسه على التسليم بثبوت الواقع، لكنها تصلح إذا نظر إليها من الناحية الموضوعية من طرف

---

[360]– ينتمي أنصار هذا الاتجاه إلى الدول التي تبنت نظام الإثبات المقيد أو القانوني مثل بريطانيا، أمريكا، كندا وغيرها راجع : **هلالي عبد الإله أحمد** ، حجية المخرجات...، مرجع سابق، ص 95 .

[361]– **بوكر رشيدة**، مرجع سابق، ص 507.

الآخرين[362].

وحسب هذا الاتجاه، فان الاقتناع يقف موقفا وسطا بين اليقين والاعتقاد، لا هو يقينا بالمعنى العلمي لليقين ولا جزما كحالة موضوعية لا تبعث شكا لدى من تيقن أو جزم ولا تورث جهلا أو غلطا لدى الآخرين، إنما الاقتناع هو اعتقاد قائم على أدلة موضوعية ومبني على استقراء واستيحاء الذي يتوجه به أطراف الخصومة لنيل اقتناع القاضي[363].

انطلاقا من هنا، يرى أصحاب هذا الاتجاه بأنه إذا كانت للقاضي في الدليل سلطة تقديرية واسعة في اللجوء إلى الخبرة الفنية وتقدير قيمتها الاستدلالية انطلاقا من مبدأ حرية الإثبات في المواد الجزائية والذي تولد عنه مبدأ القاضي خبير الخبراء، فذلك مقتصر على ما يمكن للقاضي أن يبت فيه لوحده، أما المسائل ذات الصبغة الفنية البحتة، فلا يجوز للقاضي أن ينصّب نفسه فيها مكان الخبير ولا يمكنه طرح رأيه إلا لأسباب سائغة ومقبولة[364].

ويخلص هذا الاتجاه، إلى القول بأن الأدلة الالكترونية تتمتع بحجية قاطعة في الدلالة على الوقائع التي تتضمنها، ويمكن التغلب على مشكلة التشكيك في مصداقيتها من خلال إخضاعها لاختبارات تسمح بالتأكد من صحتها وسلامتها، ويجب عدم الخلط بين الشك الذي يشوب الدليل الالكتروني بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه، والقيمة الاقناعية لهذا الدليل. ففي الحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية بحتة والقول فيها هو قول أهل الاختصاص[365]، وإن سلم الدليل الالكتروني من العبث والخطأ وتوافرت فيه الشروط المذكورة من قبل، فلن يكون للقاضي سوى قبول هذا الدليل والاقتناع

---

[362]– **عفيفي محمد عفيفي**، جرائم الكمبيوتر و حقوق المؤلف...، مرجع سابق، ص 364.

[363]– **طاهري شريفة**، تأثير أدلة الإثبات على الاقتناع الشخصي للقاضي الجنائي، مذكرة لنيل شهادة الماجستير، كلية الحقوق بجامعة الجزائر، 2003، ص 23.

[364]– **بن بلاغة عقيلة**، مرجع سابق، ص 59.

[365]– **طارق محمد الجبلي**، مرجع سابق، ص 29.

به، ولا يمكنه رده أو التشكيك في قيمته الثبوتية لكونه وبحكم طبيعته الفنية يمثل إخبارا صادقا عن الوقائع وحقيقة علمية ثابتة، ما لم يثبت عدم صلة هذا الدليل بالجريمة المراد إثباتها.

واسترشادا بذلك، يمكن القول بأن أصحاب هذا الاتجاه قد جعلوا الطبيعة العلمية للدليل الالكتروني قيدا حقيقيا لحرية القاضي الجزائي في تقدير الدليل يجبره على الاقتناع به والحكم بمقتضاه ولو لم يكن مقتنعا بصحة الواقعة المطروحة أمامه، إذ لم يعد القاضي وفقا لهدا الاتجاه حرا في مناقشة و وزن وتقدير الدليل العلمي الذي أصبح يؤدي دور الصدارة في الإثبات الجنائي سيما بعد ظهور الأدلة الالكترونية الرقمية وإنشاء معامل ومخابر جنائية لفحص هذه الأدلة وتقييمها.

وخلافا لما ذهب إليه الاتجاه الفقهي الأول، هناك من يرى بأن مبدأ حرية القاضي في الاقتناع يجب أن يبسط سلطانه على كل الأدلة دون استثناء بما فيها الدليل الالكتروني[366]، معبرين بأن إعطاء الدليل الالكتروني قوة ثبوتية مطلقة لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى الوراء إلى نظام الإثبات المقيد[367].

زيادة عن ذلك، يرى أنصار هذا المذهب بأن الوسائل العلمية في اغلب حالتها ليست دليلا في ذاته إنما هي قرائن تتم دراستها و تحليلها لاستخلاص دلالتها، ومؤدى ذلك أنها لا تصلح في ذاتها كدليل وحيد في الإثبات الجنائي. وإذا كان لابدّ على القاضي الاستعانة بأهل الخبرة في المسائل الفنية البحتة واستطلاع رأيهم فيما يتعلق هذه المسائل[368]، فان ذلك

---

[366]– ينتمي أنصار هذا الاتجاه إلى الدول التي تبنت نظام الإثبات الحر، مثل فرنسا، ايطاليا، مصر، سورية، الجزائر. انظر: **علي حسن طوالبة**، مشروعية الدليل المستمد من التفتيش الجنائي، مرجع سابق، ص.ص 13-14

[367]– **محمد عبد الشافي إسماعيل**، مبدأ حرية القاضي الجنائي في الاقتناع ـ دراسة مقارنة، دار المنار، القاهرة، 1992، ص 165.

[368]– **بن بلاغة عقيلة**، مرجع سابق، ص 59-60.

لا يعني التخلي عن حقه في مناقشة وموازنة نتائج الخبرة واستبعادها إن رأى في ذلك تحقيق العدالة، لان هذا يدخل في نطاق تقديره الذاتي ومن صميم وظيفته القضائية[369].

ويضيف هذا المذهب بأن توفر الدليل العلمي الالكتروني لا يعني التزام القاضي بالحكم بموجبه مباشرة بالإدانة أو البراءة، لان الدليل الالكتروني ليس آلية معدة لتقرير القاضي بخصوص مسألة غير مؤكدة [370]. خاصة إذا أخذنا في الحسبان أن مثل هذا الدليل كثيرا ما يتضارب مع باقي أدلة الدعوى الجزائية، فضلا عن احتمال تباين واختلاف آراء الفنيين المختصين في شأنه.

وحسب هذا الاتجاه، فانه مهما يعل شأن الأدلة العلمية الالكترونية في مسألة الإثبات الجنائي، فانه يجب الإبقاء على سلطة القاضي في تقدير هذه الأدلة وتكوين اقتناعه منها بكل حرية، وذلك من أجل ضمان تنقية هذه الأدلة من شوائب الحقيقة العلمية، ويظل القاضي هو المسيطر على هذه الحقيقة لأنه من خلال سلطته التقديرية يستطيع أن يفسر الشك لصالح المتهم، ويستبعد الأدلة التي يتم الحصول عليها بطرق غير مشروعة، ويجعل من الحقيقة العلمية حقيقة قضائية[371].

والرأي عندنا في هذا الشأن هو ما ذهب إليه الاتجاه الثاني، إذ يجب على القاضي الجزائي ألا يتقيد بالدليل العلمي ومنه الدليل الالكتروني المطروح أمامه في تكوين اقتناعه

---

[369]– **أحمد يوسف الطحطاوي**، مرجع سابق، ص.ص 204–205. و **بوكر رشيدة**، مرجع سابق، ص.ص 507–508.

[370]– هذا ما أكدته محكمة النقض الفرنسية في حكم لها بقولها " **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 و قد ثبت ذلك من خلال جهاز آلي إلتقط صورة السيارة المتجاوزة للسرعة و دون أن يكون السائق قد سؤل فإنها لا تكون ملزمة بتحديد ما استندت إليه من عناصر الواقعة في تبرير اقتناعها** " أنظر: **محمد عبد الشافي إسماعيل**، مرجع سابق، ص 166.

[371]– **علي محمود علي حمودة**، مرجع سابق، ص 15.

والحكم وجوبا بما يتطابق مع النتائج التي أسفرت عليها هذه الأدلة، بل لابد أن يستمد هذا الاقتناع مما له من سلطة في تقدير الأدلة مهما بلغت درجتها اليقينية والعلمية وموازنتها وفقا لما يمليه عليه وجدانه. ولكي نضمن نجاح مهمة القاضي الذي تناط به المناقشة العلمية لأدلة التقنية إلى جانب مناقشتها القانونية يتطلب منه أن يكون مؤهلا التأهيل الفني والتقني على كيفية التعامل مع هذه الأدلة عند الأخذ بها كأدلة إثبات، وهو الأمر الذي لا يتأتى إلا بعقد دورات تدريبية مكثفة لهؤلاء القضاة على كافة مستوياتهم حول تقنية المعلومات.

المطلب الثالث

موقف المشرع الجزائري من الإثبات بالأدلة الإلكترونية

الإثبات الجنائي هو إقامة الدليل لدى السلطات المختصة على حقيقة وقوع الجريمة أو عدم وقوعها، باستعمال طرق و وسائل مشروعة وبيان حقيقة نسبتها إلى المتهم لإعمال حكم القانون عليه. ويعني ذلك أن موضوع الإثبات هو الوقائع وليس القانون[372].

وعليه فالدليل هي الوسيلة القانونية التي يستعين بها القاضي الجزائي للوصول إلى كشف غموض الجريمة والتأكد من أن المتهم هو من قام بارتكابها بالفعل، بل يعتبر الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه، وذلك إما بتحقيق حالة اليقين لدى القاضي فيحكم بالإدانة، أو ترجيح موقف الشك لديه فيحكم بالبراءة.

ولقد ذكرنا فيما سبق أن حجية أي دليل أمام القضاء الجنائي إنما تحدد حسب طبيعة نظام الإثبات المعتمد، وسبق البيان كذلك بأن الفقه الجنائي أرسى نظامين رائدين في مجال الإثبات وهما مختلفان من حيث الأسس التي يقوم عليها كل واحد منها، فالأول هو نظام الإثبات القانوني أو المقيد وفيه يحدد القانون الأدلة التي يجوز للقاضي الأخذ بها والاستناد

---

[372]– **نجيمي جمال**، إثبات الجريمة على ضوء الاجتهاد القضائي، دار هومة، الجزائر، 2011، ص 21.

عليها، والثاني هو نظام الإثبات الحر أو المطلق وفيه لا يقيد القانون القاضي بأدلة معينة في الإثبات وله أن يقتنع بأي دليل يعرض عليه.

ومن هنا يثار الفضول حول أي من هذين النظامين أخذ المشرع الجزائري(الفرع الأول). وما أثر ذلك الاختيار على مسألة الإثبات بالدليل الالكتروني بشكل عام وبالخصوص على سلطة القاضي الجزائي الجزائري في تقدير الدليل الالكتروني (الفرع الثاني) ؟

الفرع الأول: موقف المشرع الجزائري من أنظمة الإثبات الجنائي

لقد حسم المشرع الجزائري موقفه من أنظمة الإثبات الجنائي بشكل واضح في نصي المادتين(212 و307) من قانون الإجراءات الجزائية، وذلك حينما نص في المادة(212) على انه " **يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الاحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي**" ونص في المادة(307) بأن " **القانون لا يطلب من القضاة أن يقدموا حسابا عن 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 وتدبر، ويبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة الى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي**".

فبالنظر إلى نصي هاتين المادتين يتضح جليا أن المشرع الجزائري تبنى كأصل عام نظام الإثبات الحر أو الاقتناع الشخصي للقاضي الجزائي، والذي منح من خلاله للقاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لقناعته الذاتية، وفتح أمامه باب الإثبات

على مصراعيه كي يستلهم عقيدته من أي موطن يراه[373]، دون أن يطالبه بتقديم مبرر لذلك. وفي الوقت نفسه وعلى سبيل الاستثناء نجده أخذ بنظام الإثبات المقيد أو ما يسمى كذلك بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محددة مسبقا على سبيل الحصر كما هو الشأن بخصوص جريمة الزنا المنصوص عليها في المادة (339) من قانون العقوبات[374]. كما منع الأخذ ببعض وسائل الإثبات كالمراسلة المتبادلة بين المتهم ومحاميه وإن تضمنت اعتراف المتهم بأنه ارتكب الجريمة[375].

وقد تأكد الأخذ بمبدأ الإثبات الحر كذلك بطريقة غير مباشرة في عدة نصوص قانون الإجراءات الجزائية، فيما يخص جهات الحكم، نذكر منها الفقرة الأولى من المادة(235) التي تنص على أنه " **يجوز للجهة القضائية إما من تلقاء نفسها أو بناء على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة** ". وكذلك الفقرة الأولى من المادة (286) " **... له (اي لرئيس الجلسة) سلطة كاملة في ضبط حسن سير الجلسة وفرض الاحترام الكامل واتخاذ أي إجراء يراه مناسبا لإظهار الحقيقة ...**".

ولعل ما يعزز توجه المشرع الجزائري هذا الاتجاه هو عدم سنّه نصوصا تملي على القاضي الجزائي مقدما بقبول أو عدم قبول أي دليل من الأدلة المطروحة عليه في الدعوى أو ترسم له طرقا محددة للإثبات يتقيد بها ، إنما فسح له المجال لكي يختار بحرية من كل

---

[373]– جاء في إحدى قرارات المحكمة العليا الصادر عن الغرفة الجزائية انه " **يمكن لقاضي الموضوع تأسيس اقتناعه على أية حجة حصلت مناقشتها حضوريا أمامه**" نقلا عن: **أحسن بوسقيعة**، مرجع سابق، ص 79.

[374]– تنص المادة(341) من قانون العقوبات على أن " **الدليل الذي يقبل في ارتكاب الجريمة المعاقب عليها في المادة 339 يقوم إما على محضر قضائي يحرره احد رجال الضبط القضائي عن حالة التلبس، و إما بإقرار وارد في رسائل أو مستندات صادرة عن المتهم و إما بإقرار قضائي** ".

[375]– تنص المادة(217) من القانون الإجراءات الجزائية على انه " **لا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم و محاميه**"

طرقه ما يراه مفيدا وموصلا إلى الكشف عن الحقيقة ويستلهم عقيدته من أية وسيلة أو دليل يطمئن إليه وجدانه ويرتاح إليه ضميره[376]، ولو تعلق الأمر بالأدلة الالكترونية، خاصة أنه لم يتضمن قانون رقم (09-04) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أية استثناءات أو أوضاع خاصة بهذا الصدد، مما يوحي بأن الدليل الالكتروني مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والإثبات في مجال جرائم الاعتداء على النظم المعالجة الآلية بصفة خاصة، و يمثل مظهرا من مظاهر اعتناق المشرع لمبدأ حرية الإثبات والاقتناع .

ولم يكتف المشرع الجزائري بالنصوص المذكورة التي أطلقت حرية قاضي الموضوع في إثبات الجريمة بكافة طرق الإثبات وأعطته سلطة تقديرية واسعة في موازنة الدليل، بل خول كذلك لسلطات تنفيذ القانون الأخرى (الاتهام و التحقيق) الحق في البحث عن الأدلة بكل حرية بما فيها الالكترونية، وتجميعها عن طريق وضع الترتيبات التقنية اللازمة لذلك[377]، وكذا تمحيصها وصولا إلى الحقيقة التي سوف تبرر وفقها الاتهام وتؤسس عليها الأوامر التي يصدرها أثناء التحقيق، منها ما تضمنته المادة(162) الفقرة الثانية من قانون الإجراءات الجزائية " **يمحص قاضي التحقيق الأدلة وما إذا كان توجد ضد المتهم دلائل مكونة لجريمة من جرائم قانون العقوبات**". إضافة إلى إمكانية الاستعانة بكل شخص مؤهل أو لديه علم وخبرة في الواقعة المراد اتخاذ الإجراء بشأنها[378].

---

[376]– **خنفوسي عبد العزيز** " تجسيد مبدأ حرية الإثبات الجزائي في القانون الجنائي الجزائري" ص.ص 01-02، مقال منشور في الموقع الالكتروني : http://ifttt.com/images/no_image_card.pn

[377]– نذكر منها المادة (68 الفقرة 1) من القانون الإجراءات الجزائية التي تنص على أن: " **يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة، بالتحري عن أدلة الاتهام أو النفي** ". والمادة(69) من القانون نفسه تنص " **يجوز لوكيل الجمهورية سواء في طلبه الافتتاحي لإجراء التحقيق او بطلب اضافي في اية مرحلة من مراحل التحقيق أن يطلب من القاضي المحقق كل إجراء يراه لازما لإظهار الحقيقة**".

[378]– وهذا ما أكدته المادة(143) من قانون الإجراءات الجزائية الجزائري في نصها " **لجهات التحقيق أو الحكم عندما**

وفي مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وضع المشرع الجزائري على عاتق مقدمي خدمات الانترنت عددا من الالتزامات لمساعدة السلطات المختصة بالتحري والتحقيق[379]، بما من شأنه تسجيل وحفظ المعطيات المتعلقة بمحتوى الاتصال أو المراسلة في حينها، كالمعطيات التي تسمح بالتعرف على مستعملي الخدمة، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، خصائصها التقنية، وكذا تاريخ و وقت ومدة الاتصال، والمعطيات التي تسمح بالتعرف على مرسل الاتصال والمرسل إليه، وكذا عناوين المواقع المطلع عليها[380]. وكل ذلك يعد إخبارا صريحا على أن المشرع الجزائري قد سار على نهج نظام الإثبات الحر.

وهناك أسباب أخرى عديدة تبرر أخذ المشرع الجزائري بنظام الإثبات والاقتناع الحر، ولعل أهمها ظهور وتفشي الأدلة العلمية بمختلف أنواعها، كتلك المستمدة من الطب الشرعي والتحاليل العلمية الدقيقة (كالبصمات الشخصية والبصمة الوراثية) ومضاهاة الخطوط والأدلة الالكترونية الرقمية، والتي لا تقبل بطبيعتها إخضاع القاضي لأية قيود بشأنها، بل بالعكس فهي تفرض أن يترك أمر تقديرها وتمحيصها لمحض إرادة واقتناع القاضي الجزائي.

تعرض لها مسالة ذات طابع فني أو تأمر بندب خبير إما بناء على طلب النيابة العامة و إما من تلقاء نفسها أو من الخصوم ..."

[379]–أورد المشرع الجزائري في المادة(10) من القانون رقم(04/09) أنه في إطار تطبيق أحكام هذا القانون يتعين على مزود الخدمة تقديم المساعدات للسلطات المكلفة بالتحريات القضائية ...بوضع المعطيات التي يتعين عليهم حفظها وفقا لأحكام المادة(11) أدناه تحت تصرف هذه السلطات.

[380]– أنظر المادة (11/3) من القانون رقم (09-04) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

الفرع الثاني: أثر تبني نظام الإثبات الحر على سلطة القاضي الجزائي الجزائري في قبول الدليل الإلكتروني

بالرجوع إلى نص المادة (212) من قانون الإجراءات الجزائية التي تجسدت فيها إرادة المشرع الجزائري في تبني نظام الإثبات الحر، نجدها تكرس قاعدتين تكمل إحداهما الأخرى، ومهمتان لإعمال هذا النظام وتحديد سلطة القاضي الجزائي في قبول أدلة الإثبات، وهاتان القاعدتان هما: قاعدة الاقتناع الحر للقاضي الجزائي، وقاعدة حرية اختيار وسائل الإثبات الجزائي.

وإذا كان الدليل الالكتروني ذو الأصالة العلمية، هو الأوفر والأنسب في إثبات الجريمة المعلوماتية فالسؤال المطروح هنا هو ما مدى إمكانية إعمال القاضي الجزائي الجزائري لمبدأ الاقتناع الشخصي حيال هذا الدليل؟ وما مدى حريته في الأخذ أو عدم الأخذ به بوصفه دليلا علميا دقيقا طبقا لأحكام المادة(212) أعلاه؟

أولا: مفهوم الاقتناع الشخصي للقاضي الجزائي

إن الهدف الأسمى الذي تصبو إليه التشريعات الإجرائية هو أن يصيب القاضي الحقيقة في حكمه سواء بالبراءة أو الإدانة، لذا يجب على القاضي الجزائي قبل أن يصدر حكمه أن يكون قد وصل إلى الحقيقة وهو الأمر الذي لا يبلغه إلا إذا اقتنع بحدوثها و كوّن يقينا حول الوقائع والملابسات المحيطة بها.

والاقتناع الشخصي هو نشاط عقلي لا يتدخّل المشرع ليبين للقاضي كيفية ممارسته وترجمته إلى واقع منتج ولا يرسم له كيف يشكل معادلاته الذهنية في مجال تقدير الأدلة ليصل من خلالها إلى الحقيقة. ويجد الاقتناع الشخصي مناخه الطبيعي الملائم في ظل مذهب الإثبات الحر الذي لا يضع تقديرا مسبقا لأدلة معينة لا يمكن الوصول بغيرها إلى اليقين.

1-تعريف الاقتناع الذاتي للقاضي:

لقد اختلف فقهاء القانون الجنائي في تعريف الاقتناع، فمنهم من عرفه بأنه الإيمان العميق والركون إلى صحة الوقائع التي تقدمها الأطراف المتنازعة الذي يخلف في نفس القاضي الجزائي أثرا عميقا يجعله يصدر حكمه عن قناعة وجدانية وإحساس كبير بإصابته الحقيقة في حكمه[381]. ومنهم من عرفه بأنه حالة ذهنية ذاتية تستنتج من تفاعل ضمير القاضي مع أدلة الإثبات المطروحة على بساط البحث والتي يثيرها الخصوم لإثبات أو إنكار اتهام[382]. وذهب اتجاه فقهي عريض إلى أن الاقتناع الشخصي هي حالة ذهنية ذاتية نابعة عن إمعان فكر القاضي في الوقائع المعروضة عليه من أجل بحثها والوصول بعد ذلك إلى حالة ذات درجة عالية من التأكد والجزم تزيل الشك والاحتمال[383].

وبتحليل هذه التعريفات نجد الاقتناع الشخصي للقاضي الجزائي يتكون من عنصرين أساسيين هما:

أ- التقدير الحر والمسبب لعناصر الإثبات، والذي يكوّن من خلاله القاضي حالة ذهنية مبنية على الاحتمال، لأن العبرة ليست بكثرة الأدلة وإنما بما تتركه من أثر في نفسية القاضي، وهذا التأثير وحده الذي يحدد مصير الدعوى الجزائية بالإدانة أو البراءة.

ب- حرية أخذ القاضي الجزائي قناعته وعقيدته من أي دليل، وهو ما يسمح للقاضي بان يصل إلى الحقيقة بكافة الطرق التي تؤدي إليها في نظره، ويستنتجها من كل ما يمكن أن يدلّ عليها في اعتقاده، وإليه المرجع في تقدير صحة الدليل من هذه الوسائل وما بها من قوة

---

[381]- **سيد محمد حسن الشريف**، النظرية العامة للإثبات الجنائي، دار النهضة العربية، القاهرة ، 2002، ص 28.

[382]- **زبده مسعود**، الاقتناع الشخصي للقاضي الجزائي، المؤسسة الوطنية للكتاب، الجزائر، 1989، ص 36.

[383]- **محمد عبد الكريم عبادي**، القناعة الوجدانية للقاضي الجزائي و رقابة القضاء عليها، عمان، 2002، ص 12.

الدلالة[384].

وبناء على هذين العنصرين يصبح مدلول القناعة الوجدانية للقاضي الجزائي لا يقتصر على تقدير الأدلة المقدّمة في الدعوى وإنما يتسع ليشمل، فضلا عن ذلك حرية القاضي الجنائي في الاستعانة بأي دليل يراه مناسبا لإثبات الجريمة وتكوين قناعته.

2ـ سبل تكوين الاقتناع الشخصي للقاضي الجزائي:

إن الجهد الاستنباطي الذي يبذله القاضي من خلال نشاطه العقلي المكوّن لقناعته والذي ينصرف إلى فرز الحقيقة من الدليل محل تقديره يتبع فيه القاضي ثلاث طرق هي:

ـ قبول جميع الأدلة المطروحة أمامه في جلسة المحاكمة، إذ لا يُمنع على القاضي قبول دليل أو يُفرض عليه دليلا كما أنه لا يتقيّد في ذلك إلا بقيد مشروعية إجراءات تحصيل الدليل وطرحه للمناقشة العلنية في الجلسة.

ـ أن يقوم القاضي بموازنة كل دليل على حدا بمعزل عن باقي الأدلة المطروحة أمامه ويقدر قيمته التدليلية وقوته الثبوتية بالنظر إلى ما يعبر عنه من حقيقة، وله أن يهدر أي دليل مهما تبلغ قيمته كليا أو جزئيا طالما أنه لم يطمئن إليه [385].

ـ أن يقوم القاضي بتنسيق كافة الأدلة المعروضة عليه من خلال التحقيق والتمحيص والتأكد من أنها متساندة تشدّ بعضها البعض و ليست متعارضة.

3ـ الشروط التي تردّ على القاضي الجزائي في تكوين اقتناعه

إن الهدف من العملية القضائية التي يجريها القاضي الجزائي هو بلوغ الحقيقة الواقعية للجريمة، فكل نشاط أو جهد ذهني يبذله القاضي من خلال هذه العملية ينبغي من ورائه

---

[384]– **طاهري شريفة**، تأثير أدلة الإثبات على الاقتناع الشخصي للقاضي الجنائي، مذكرة لنيل شهادة ماجستير، جامعة الجزائر، 2003، ص 23.

[385]– **علي محمود علي حموده**، الأدلة المتحصلة من الوسائل الالكترونية ...، مرجع سابق، ص.ص 119ـ120.

الوقوف على وقائع وملابسات الجريمة كما حدثت، وإذا استقرت لديه تلك الحقيقة و ارتاح ضميره للصورة الذهنية التي تكوّنت له يكون قد وصل إلى حالة الاقتناع[386]. ولكي يكون هذا الاقتناع منتجا لآثاره يجب أن يراعى فيه الشروط التالية:

أ-بناء اقتناع القاضي على الجزم واليقين: لكي تكون قناعة القاضي سليمة في تقديرها للأدلة، يجب أن تكون النتيجة التي توصل إليها تتفق مع العقل والمنطق، ومطابقة للنموذج المنصوص عليه في القانون وهو ما يطلق عليه الحقيقة القضائية، والتي يشترط أن تتفق مع الحقيقة الواقعية.

فحرية القاضي في الاقتناع هي أن لا يبني حكمه على الظن والتخمين، أو على قرائن لأن حجية القرائن في الإثبات بسيطة ولا تصل إلى درجة الجزم، فهي كافية للاتهام ولكنها لا تعبّر على صدق التهمة ولا توّلد في الاقتناع أكثر من احتمال غير قاطع. كما يجب عليه (أي القاضي) أن يتأكد وبشكل جازم مبني على اليقين بأن المتهم الماثل أمامه هو من قام بارتكاب الفعل المجرم، لان الحقيقة لا يمكن توفرها إلا باليقين لا بالشك والاحتمال[387].

وباعتبار هذا الشرط ما هو إلا نتيجة منطقية لقاعدة جنائية جوهرية هي قاعدة الأصل في الإنسان البراءة وأن المتهم بريء حتى تثبت إدانته، فان الأحكام التي تقضي بالإدانة يجب أن تُأسس على حجج قطعية الدلالة تفيد الجزم واليقين.

ب – تفسير الشك لصالح المتهم: يجد هذا الشرط مكانه عادة عندما لا يتحقق الشرط الأول أي في الحالة التي لا يبلغ فيها القاضي درجة اليقين والجزم في تقديره لوقائع الجريمة أو انتسابها للمتهم، الأمر الذي يسمح بحلول الشك محل اليقين والظن محل الجزم.

---

[386]– **خنفوسي عبد العزيز** ، مرجع سابق، ص 02.

[387]– **العربي شحط عبد القادر و نبيل صقر**، الإثبات في المواد الجزائية، دار الهدى، الجزائر، 2006، ص 34.

ورغم المكانة العالية التي يتمتع بها الدليل العلمي ومنه الدليل الالكتروني في مجال الإثبات الجنائي تجعله مقبولا أمام المحكمة، إلا انه قد يوجد في الدعوى الجزائية ما يجعل القاضي يقتنع ولو احتمالا يدعو إلى الشك، بأن الدليل لا يمدّ بأية صلة إلى الجريمة، أو أن شخصا آخر قد ارتكب الجريمة، ففي هذه الحالة يجب على القاضي أن يفسر هذا الشك لمصلحة المتهم و يحكم له بالبراءة[388].

ثانيا- سلطة القاضي الجزائي الجزائري في تقدير الدليل الإلكتروني

أجمعت تشريعات العالم على أن تقدير الدليل بعد قبوله يعد جوهر عمل القاضي الجزائي الذي يختص به وحده دون منازع، فهي عملية ذهنية يعتمد فيها قاضي الموضوع على المنطق، وعلى وعيه وإدراكه بكافة أدلة الدعوى الجزائية، وتمحيصها ثم استنتاج ما تحتويه من قرائن قادرة على خلق اليقين لديه[389]، فالقاضي الجزائي في نهاية المطاف هو الذي يقوم بالتنسيق بين الأدلة المختلفة إثباتا ونفيا، ليستخلص منها بعد ذلك مجتمعة عقيدته سواء بالبراءة أو الإدانة.

ويصدق هذا القول على الأدلة المادية التقليدية. أما بالنسبة للدليل الالكتروني كما سبق البيان، فإن الأصالة العلمية التي يتميّز بها جعلت سلطة القاضي الجزائي في تقديره محل جدل فقهي عريض، بين من يرى أن الدليل الالكتروني وما يتسم به من مصداقية ودقة علمية عالية يبلغ معها درجة اليقين تجعله يكتسب قوة ثبوتية قاطعة وملزمة للقاضي، وبين من يرى بأنه من الضروري بسط سلطان مبدأ حرية القاضي في الاقتناع على كل الأدلة دون استثناء بما فيه الدليل الالكتروني الرقمي، معتبرين إعطاء الدليل الالكتروني قوة ثبوتية قـاطعة لا يستطيع القاضـي مناقشتها أو تقديرها يعدّ بمثابة خرق لقاعدة تكافئ الأدلة،

---

[388]- **العربي شحط عبد القادر و نبيل صقر**، مرجع سابق، ص.ص 34- 35.

[389]- **بن بلاغة عقيلة**، مرجع سابق، ص59 .

بل هو تجريد القاضي من وظيفته الأصلية التي هي تحقيق الحقيقة القضائية.

أما بالنسبة للمشرع الجزائري فقد بينا فيما سبق بأنه أجاز إثبات الجرائم بأية طريقة من طرق الإثبات ماعدا الجرائم التي قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن إليه. و لكن السؤال الذي يثار هنا هو هل تتصرف هذه السلطة التقديرية التي يتمتع بها القاضي الجزائي الجزائري إلى الأدلة المستخرجة من الوسائل الالكترونية أو ما يسمي بالأدلة الالكترونية والرقمية؟

بالرجوع إلى القانون رقم(04/09) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجده خاليا من أية أحكام خاصة تتعلق بحجية مخرجات الالكترونية في الإثبات[390]، ومن هنا فسكوت المشرع عن هذا الأمر هو تفسير لنيته في إخضاع هذه الأدلة مثلها مثل باقي الأدلة الأخرى للقواعد العامة.

وإذا أخذنا في الحسبان بأن الجرائم الالكترونية تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكل الأفعال الإجرامية الأخرى التي ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام الاتصالات الالكترونية كما صرحت المادة (02) من القانون رقم (04/09)[391]، فان ذلك يعني أن الإجرام المعلوماتي قد يأخذ وصف المخالفة أو الجنحة أو الجناية بحسب طبيعة الجرم المرتكب.

اعتبارا لذلك، فإن كان مبدأ الاقتناع القضائي عام النطاق لدى كافة أنواع المحاكم الجزائية سواء كانت محاكم الجنايات أم الجنح أم المخالفات[392]، وبدون تفرقة بين القضاة

---

[390]– أنظر القانون رقم (04/09) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

[391]– أنظر نص المادة(02) من القانون رقم(09-04) مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[392]– تجدر الإشارة هنا إلى أن المشرع الجزائري لم ينص صراحة على هذا المبدأ إنما يستنبط من أحكام المادتين (212

والمحلفين،[393] وأنه يمتد كذلك ليشمل إلى جانب جهات الحكم جهات التحقيق والإحالة،[394] إلا أن قواعد بيان عناصر تقدير القاضي للدليل تختلف حسب اختلاف وصف الفعل المجرم.

فإذا كان الفعل الإجرامي يحمل وصف جناية فان محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها وتصدر أحكامها وفقا لمحض قناعتها دون أن يكون قضاتها مطالبين بتسبيب أو تعليل أحكامهم[395] ودون أن تكون لجهات الطعن في ذلك رقابة عليهم[396]. أما إذا أخذ الفعل المجرم وصف جنحة، فان القاضي في هذه

و307) من قانون الإجراءات الجزائية، و هذا خلافا لما ذهب إليه معظم التشريعات ، فنجد المشرع الفرنسي خصص المادة (353-1) من قانون الإجراءات الجزائية لتطبيق مبدأ الاقتناع القضائي أمام المحاكم الجنائية، وخصص الى جانب ذلك نص المادة(427) من القانون ذاته لتطبيق هذا المبدأ كذلك أمام محاكم الجنح. أما المشرع السوري نجده نص صراحة على تطبيق هذا المبدأ أمام كل من محاكم الجنايات والجنح والمخالفات في المادة (175) من قانون الإجراءات الجنائية. انظر: **أحمد يوسف الطحاوي**، مرجع سابق، ص 199.

[393]– لقد سوى المشرع الفرنسي بين المحلفين و القضاة فيما يتعلق بالاقتناع بحيث نص في المادة(303) من قانون الإجراءات الجزائية على أن " **يقسم المحلفون على أن يصدروا قراراتهم طبقا لضمائرهم و اقتناعهم الشخصي**".

[394]– بمعنى أن مبدأ الاقتناع القضائي يطبق حتى على أعضاء النيابة و قضاة التحقيق و مستشاري الإحالة حينما يقدرون ما اذا كانت الأدلة المتوفرة لديهم كفاية لتوجيه الاتهام أم لا، إذ لا يخضعون في ذلك إلا لرقابة ضمائرهم واقتناعهم الذاتي، ولعل السبب في توسيع نطاق هذا المبدأ ليشمل جهات التحقيق الابتدائي هو كون الغاية من مرحلتي التحقيق الابتدائي و النهائي هي ضمان لتأكيد أساس العدالة في الأحكام، بتأسيس المبادئ التي يجب أن ترشد القضاة عند تقرير عناصر الإثبات و البحث عن الحقيقة .

[395]– إلا أن بعد التعديل الأخير لقانون الإجراءات الجزائية بموجب القانون رقم(6/17) ألزم المشرع في المادة 309 قضاة المحاكم الجنائية الابتدائية منها والإستئنافية بتسبيب جميع أحكامهم القاضية بالإدانة أو بالبراءة أو حتى بالإعفاء من المسؤولية.

[396]– وهذا ما عبرت عنه المحكمة العليا الجزائرية في إحد قراراتها بقولها " **ان العبرة في الإثبات في مواد الجنايات بالاقتناع الشخصي، وهو لا يخضع لرقابة المحكمة العليا**" نقلا عن: **بوسقيعة أحسن** ، قانون الإجراءات الجزائية على ضوء الممارسات القضائية، برتي للنشر، الجزائر،2014، ص 102 .

الحالة يكون مطالبا ببيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه[397]، والذي يكون محل رقابة من قبل جهات الطعن[398]. وليس المراد بالتزام القاضي بالتسبيب هنا أن يبيّن في حكمه لماذا اقتنع والكيفية التي استمدّ بها اقتناعه، والعلّة في اقتناعه بها، لأن ذلك يدخل في نطاق السلطة التقديرية المعترفة له قانونا، إنما المراد هو حمله على الإفصاح عن مصادر اقتناعه توطئة للنظر فيما إذا كان من شأنها أن تؤدي منطقيا لما انتهى إليه[399].

وعليه فقاضي الموضوع في مواد الجنح مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات بما فيها وسائل الإثبات الالكترونية الرقمية، والتي قد تأخذ شكل محاضر معدة بمناسبة استجواب أو تفتيش، مراقبة الكترونية أو اعتراض مراسلات، أو شكل تقرير خبرة محرر بمناسبة معاينة وفحص الأدلة المضبوطة من أجهزة أو دعامات الكترونية. فأما ما يتعلق بالمحاضر، فالمشرع الجزائري اعتبرها كقاعدة عامة مجرد استدلالات ما لم ينص القانون على خلاف ذلك[400]، ولا تكون للمحضر أية قوة إثبات إلا إذا كان صحيحا من حيث الشكل، وتم إعداده من طرف واضعه أثناء مباشرة أعمال

---

[397]– تنص المادة (379) من قانون الإجراءات الجزائية الجزائري على أن " **كل حكم ...يجب أن يشمل على أسباب و منطوق. و تكون الأسباب أساس الحكم...**" تقابلها المادتين (485 و 593) من قانون الإجراءات الجزائية الفرنسي.

[398]– لقد أصدرت المحكمة العليا الجزائرية عدة قرارات أكدت فيها ضرورة التزام قضاة الجنح بتسبيب أحكامهم بشكل يسمح لقضاة الطعن ممارسة رقابتهم عليها نذكر منها: القرار رقم(23946) المؤرخ في 19-2-1981 القاضي بأنه " **رغم السلطة التقديرية الممنوحة لقضاة الموضوع فهم ملزمون بتسبيب قراراتهم بكيفية واضحة وليست غامضة حتى يتمكّن المجلس الأعلى من ممارسة رقابته** " والقرار رقم (19090) المؤرخ في 05-03-1981 القاضي بأن " **السلطة التقديرية لقضاة الموضوع محدودة بإلزام هؤلاء بتسبيب قراراتهم**". والقرار المؤرخ في 26-06-1984 القاضي ب " **يتعرض للنقض القرار الذي جاء خاليا من الأسباب...**" مشار إليها في: **بوسقيعة أحسن**، مرجع سابق، ص.ص 127-128.

[399]– **أحمد يوسف الطحطاوي**، مرجع سابق، ص 270.

[400]– تنص المادة(215) من قانون الإجراءات الجزائية الجزائري

وظيفته وأورد فيه موضوعا داخلا في نطاق اختصاصه[401]. غير أن المحاضر التي يخول القانون إعدادها بموجب نص خاص لإثبات جنح معينة كمحاضر الجلسات في الحاكمة ومحاضر التحقيق الصادرة عن قاضي التحقيق فإنها تتمتع بحجية ما لم يدحضها دليل عكسي[402]. وقد سوّى المشرع من خلال هذه الأحكام بين المحاضر المعدة حول الجرائم الالكترونية وتلك المتعلقة بأية جريمة تقليدية أخرى، وترك تقدير قيمتها الاستدلالية للقاضي الجزائي .

وأما بالنسبة لتقارير الخبرة فشأنها شأن باقي أدلة الإثبات تخضع لمناقشة و تقدير قاضي الموضوع ، كما يستشف من نص المادة (215) من قانون الإجراءات الجزائية التي تنص على أنه " **لا تعتبر ,,,والتقارير المثبتة للجنايات أو الجنح إلا مجرد الاستدلالات...**"، وهو المعنى الذي أكدته المحكمة العليا في عدة قراراتها ومنه ما تضمنه القرار المؤرخ في 14 نوفمبر 1981 بأن " **تقرير الخبرة ليس إلا عنصرا من عناصر الاقتناع يخضع لمناقشة الأطراف و تقدير قضاة الموضوع** "[403].

ومع هذا فالطبيعة العلمية والفنية التي تتميز بها الجرائم الالكترونية، بالإضافة إلى نقص ثقافته الفنية في هذا المجال غالبا ما تفرض على القاضي الجزائي الجزائري الاستناد في تكوين اقتناعه وبدون تردد على الخبرة الفنية والتقيد بالنتائج المفضي إليها في تقرير الخبرة، ولا يمكنه طرحها واستبعادها إلا إذا قدّر أن ما تحتويه من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة والمنطق العلمي، إذ حدث وأن اكتفى القاضي

---

[401]– أنظر نص المادة (214) من قانون الإجراءات الجزائية الجزائري

[402]– أنظر المادتين(216 و 218) من قانون الإجراءات الجزائية الجزائري

[403]– أنظر قرار محكمة العليا الصادر عن الغرفة الجزائية في 21 نوفمبر 1981، مشار إليه في: **أحسن بوسقيعة**، مرجع سابق، ص 79.

الجزائي في عدة قضايا بالخبرة وحدها للفصل في وقائع ذات طابع تقني بحت دون أن يتعرض لمناقشة نتائجها.

خلاصة الأمر، أن موقف المشرع الجزائري من الإثبات بالأدلة الالكترونية هو على العموم موقف التشريعات التي أخذت بنظام الإثبات الحر، إذ أجاز الإثبات في المسائل الجزائية بكافة وسائل الإثبات، أيا كان نوعها أو طبيعتها، على نحو تكون فيه جميع الأدلة متساوية ومتساندة في قيمتها التدليلية، ومقبولة أمام القضاء الجزائي من حيث المبدأ، خاضعة لتقدير وموازنة قاضي الموضوع الذي يكون له مطلق الحرية في أن يأخذ عقيدته من أية بينة أو قرينة يرتاح إليها، وله أن يبني اقتناعه من أدلة ويطرح غيرها.

فلا وجود في ظل التشريع الجزائري، لأدلة يحظر مقدما على القاضي الجزائي قبولها أو رفضها، بل كل دليل يمكن أن يتولّد معه اقتناعه يكون مبدئيا مقبولا، وبالتالي فليس ثمة ما يمنع القاضي من قبول الأدلة الالكترونية من تسجيلات وبيانات ومخرجات الحاسب الآلي، كأدلة يدخل تقدير قيمتها الإثباتية في دائرة اقتناعه ما دام أنها تتوافر على شروط المشروعية والسلامة من العبث والخطأ.

البـــاب الثانـي

عقبات التحقيق الجنائي في الجرائم الإلكترونية والحلول المقترحة لتجاوزها

الباب الثاني:عقبات التحقيق الجنائي في الجرائم الإلكترونية و الحلول المقترحة لتجاوزها

تثير ظاهرة الإجرام الالكتروني العديد من المشكلات في نطاق القانون الجنائي الإجرائي، لأن نصوصه وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كثيرة في إثباتها أو التحقيق و جمع الأدلة فيها، مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشان الجريمة المرتكبة و المجرم.

وتبدأ هذه المشكلات الإجرائية من تعلق الجريمة الالكترونية في كثير من الأحيان ببيانات معالجة آليا و كيانات منطقية غير محسوسة، مما يصعب اكتشافها من جهة، ويستحيل من جهة أخرى في بعض الأحيان البحث وجمع الأدلة بشأنها. وما يزيد المشكلات الإجراءات تعقيدا، سهولة وسرعة ودقة تنفيذ الجرائم الالكترونية مع إمكانية محو أثارها وإتلاف الأدلة التي تخلفها عقب التنفيذ مباشرة، فضلا عن إمكانية لجوء مرتكبي هذه الجرائم إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية محمية بشفرات أو رموز سرية قصد إخفائها عن أعين سلطات التحقيق والعدالة .

وقد تواجه عملية التحقيق و جمع الأدلة عقبات أكثر تعقيدا في هذا المجال حينما يتعلق الأمر بالجريمة الالكترونية عبر الوطنية التي تتشتت أركانها بين أكثر من دولة ، وتخزّن أثارها وبياناتها في أنظمة أو شبكات الكترونية موجودة فوق أقاليم دول مختلفة، بحيث تصطدم مسألة الولوج إليها و محاولة جمعها وتحويلها إلى الدولة التي يجري التحقيق فيها بمشكلات تتعلق بسيادة الدولة التي توجد عندها هذه البيانات، ومع اقتران هذه المشكلة بتباين نظرة التشريعات الإجرائية للدول إلى الجريمة الالكترونية، بالإضافة إلى ضعف وهشاشة وسائل التعاون الدولي لمـواجهة هذا النمط المستحدث من الإجـرام، يصبـح البحث والتحقيق أمرا شبه مستحيل.

الباب الثاني:عقبات التحقيق الجنائي في الجرائم الإلكترونية و الحلول المقترحة لتجاوزها

تفاديا للعقبات والمشكلات المذكورة أعلاه، والتي تصد فعالية التحقيق الجنائي في الجرائم الالكترونية، سارعت الدول إلى مراجعة الكثير من المسائل الإجرائية المتعلقة بهذا المجال بما يضمن تطوير أساليب التحقيق وإجراءاته بصورة تتلاءم مع خصوصية هذه الجرائم، و تقديم جملة من الحلول الوطنية والدولية التي من شأنها أن تستدرك هذه العقبات والحدّ من تأثيراتها السلبية على عملية التحقيق، وإضفاء الفعالية المطلوبة للأجهزة الأمنية وسلطات البحث والتحري في كشف غموض الجريمة وضبط فاعليها و التحقيق معهم وتقديمهم للعدالة. وهي الحلول التي سوف نتعرض لها في (الفصل الثاني من هذا الباب)، بعد دراسة أهم العقبات التي تعترض التحقيق في الجرائم الالكترونية في (الفصل الأول).

الفصل الأول

عقبات التحقيق الجنائي في الجرائم الإلكترونية

يتسم التحقيق في الجرائم الالكترونية و ملاحقة مرتكبيها جنائيا بالعديد من المعوقات والعقبات التي من شانها أن تعرقل الوصول إلى الكشف عن الجريمة و إثباتها، بل قد تؤدي إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في نفسه و في أدائه، وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون لعجزها عن حمايته من هذه الجرائم وملاحقة مرتكبيها، وتنعكس أيضا على المجرم نفسه، فيشعر بأن الجهات الأمنية غير قادرة على كشف أمره و التصدي له وخبرة القائمين بالمكافحة والتحقيق لا تجاري خبرته ومعرفته، الأمر الذي يبعث ثقة كبيرة في نفسه و يرفع من عزيمته في ارتكاب المزيد من هذه الجرائم التي قد تكون أكثر بشاعة و اشد ضرر للفرد و المجتمع.

ولعل من أهم هذه العقبات والمعوقات التي تواجه سلطات التحقيق و الاستدلال، العقبات الناتجة عن الطبيعة الخاصة للجرائم الالكترونية التي تجعلها متميزة و مختلفة عن الجرائم التقليدية (المبحث الأول). وعقبات أخرى سببها عدم ملائمة القوانين العقابية التقليدية بنصوصها و نظرياتها مع هذه الجرائم المستحدثة، وعدم كفايتها بالشكل المطلوب لمواجهتها(المبحث الثاني).

المبحث الأول

عقبات ناتجة عن الطبيعة الخاصة للجرائم الإلكترونية

تعتبر الجرائم الالكترونية من بين الجرائم المستحدثة التي ظهرت في ظل التطور التكنولوجي الهائل الذي عرفه مجال الإعلام و الاتصالات، فهي تختلف عن الجرائم التقليدية التي ترتكب في العالم المادي، وتتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يألفها العالم من قبل.

فالجرائم الالكترونية في أغلب صورها تكون خفية و مستتيرة لا يلاحظها المجني عليه ولا يدري بوقوعها، كونها تقع في بيئة افتراضية غير محسوسة و لا يتطلب ارتكابها استعمال العنف أو بذل مجهودا كبيرا كما في الجرائم التقليدية، فكل ما تحتاجه هو القدرة على التعامل مع حاسوب مرتبط بشبكة المعلومات الدولية بمستوى تقني يوظف لارتكاب أفعال غير مشروعة، مما يجعلها في الغالب لا تترك أية آثار مادية.

أضف إلى ذلك فهده الجرائم المستحدثة لا تعترف بالحدود الجغرافية لارتباطها بشبكة الانترنيت، ولا توجد حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحواسيب و شبكاتها في نقل كميات كبير من المعلومات و تبادلها بين أنظمة يفصل بينها ألاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دولة مختلفة قد تتأثر بالجريمة الالكترونية الواحدة .

وقد نتج عن الطبيعة الخاصة التي تتميز بها الجرائم المرتكبة عبر الوسائل الالكترونية العديد من المشاكل و الصعوبات أمام سلطات التحقيق والاستدلال، يتعلق بعضها بالمشاكل التي يثيرها الطابع العابر للحدود الذي تتصف به الجرائم الالكترونية (المطلب الاول). وبعضها الأخر يتعلق بصعوبات اكتشاف الجريمة الالكترونية وصعوبات إثباتها(المطلب الثاني).

المطلب الأول

انعكاسات الطابع العابر للحدود للجرائم الإلكترونية على التحقيق

يعد الطابع عبر الوطني أهم السمات التي تميز الجريمة الالكترونية عن غيرها من الجرائم التقليدية ، ويقصد به أن أثار هذه الجرائم قد تتجاوز الحدود الوطنية للدولة إلى غيرها من الدول ، لارتباطها بالشبكة العالمية للمعلومات – الانترنت– وما طرأ عليها من تطورات هائلة في الآونة الأخيرة، تلاشت أمامها كل الحواجز و الحدود الجغرافية للدول.

فالطابع العابر للحدود الذي تتسم به الجريمة الالكترونية يثير العديد من المشاكل القانونية التي تشكل عقبات حقيقية أمام مكافحة هذا النوع من الجرائم، ولعل من هذه المشاكل القانونية، تنازع الاختصاص بين الدول، وصعوبة تحديد الدولة التي يختص قضائها بالتحقيق في الجريمة الالكترونية و متابعة مرتكبيها (الفرع الأول). ومشكلة احترام سيادة الدولة، والتي تقف حاجزا أمام رجال التحقيق عندما يستوجب البحث و التنقيب عن أدلة إثبات جريمة الكترونية خارج الإقليم الوطني و في أقاليم عدة دول أجنبية (الفرع الثاني).

الفرع الأول: تنـــازع الاختصاص بالتحقيق في الجرائم الإلكترونية

تعد مسألة تنازع الاختصاص أكبر التحديات التي تواجهها عملية التحقيق في الجرائم الالكترونية، إذ أن ما تتميز به هذه الجرائم من طابعها المتخطى لحدود الدولة الواحدة واتسامها بالبعد الدولي، بالإضافة إلى تجرّد السلوك الإجرامي فيها من الطابع المادي لارتباطه بالعالم الافتراضي والرقمي، يجعلها ترتبط بأكثر من ولاية قضائية ويجتمع فيها أكثر من معيار واحد من معايير إسناد الاختصاص، مما يؤدي إلى تنازع ايجابي في الاختصاص بين جهات قضائية عدة[404].

[404]-**CHAWKI Mohamed**, combattre la cybercriminalité, Edition de saint-amans, Paris, 2008, p318. voir aussi Rapport explicatif sur la convention du conseil de l'Europe : www.Coe.int.

وقد يحدث أن ترتكب جريمة من الجرائم الالكترونية من طرف أجنبي على إقليم دولة معينة، فيؤول الاختصاص في هذه الحالة إلى الدولة التي ارتكبت الجريمة على إقليمها استنادا إلى مبدأ الإقليمية، وإلى الدولة التي يحمل الجاني جنسيتها استنادا إلى مبدأ الشخصية، وقد تشكل هذه الجريمة تهديدا لأمن و سلامة دولة أخرى أو تمس بمصالحها الأساسية، فتدخل في اختصاصها استنادا إلى مبدأ العينية، وهو ما يترتب عليه تنازع الاختصاص بين هذه الدول كل واحدة حسب المعيار الذي تربطها بالجريمة[405].

إلى جانب هذا، فمعظم الجرائم الالكترونية يتجزأ ركنها المادي و يتوزع على أكثر من إقليم، ويتحقق ذلك عندما يرتكب السلوك الإجرامي في إقليم دولة معينة وتتحقق النتيجة الإجرامية في دولة أو عدة دول أخرى، كأن يرسل المتهم برنامج من برامج الفيروسات من جهاز الكتروني متواجد في دولة معينة إلى جهاز آخر يقع في دولة ثانية مرورا بجهاز ثالث ورابع في دول أخرى، ففي هذه الحالة تثار مشكلة الاختصاص بحدة لان تحديد الجهة القضائية المختصة للتحقيق و البحث في مثل هذه الجريمة، وكذا القانون الواجب التطبيق عليها يتوقف مبدئيا على تحديد مكان وقوع الجريمة. مع العلم أن ضوابط تحديد هذا الأخير (مكان وقوع الجريمة) هي محل اختلاف و تباين بين الدول[406].

إذ ترى بعض الدول، بأن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه النشاط الإجرامي بغض النظر عن المكان الذي تحققت فيه نتيجته أو من المفترض تحققها فيه[407]. في حين يرى البعض الأخر بان مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه

---

[405]–**عبد محمد بحر**، معوقات التحقيق في جرائم الانترنت، مذكرة لنيل شهادة الماجستير في العلوم الشرطية، قسم العلوم الشرطية، معهد الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، دبي، 1999، ص 26.

[406] -**DIOP. Abdoulaye**, Cour procédure Pénale et TIC , article publier sur le site suivant ;

http:// 196.1.99.9/moodle/mod/book/print.php?id=106. 2011. P 14

[407]– أقر بهذا الرأي كل من المشرع الفرنسي والمشرع المصري.

النتيجة الإجرامية أو كان من المفترض تحققها فيه[408]، وبين هذا و ذاك انبرى فريق ثالث من الدول يرى بان العبرة في تحديد مكان وقوع الجريمة تكون بحصول أي من هذين الضابطين[409].

ولم يتوقف الأمر عند هذا الحد، بل أصبح لمبدأ الإقليمية مفهوما واسعا جدا فيما يتعلق بتحديد مكان وقوع الجريمة الالكترونية و لم يعد يلازم وقوع الفعل المادي أو أحد العناصر المكونة له مثلما هو معروف في السابق ، بل بلغ الأمر حد نزع الصفة المادية كلية من هذا الفعل، نظرا لارتباط هذه الجرائم بالعالم الافتراضي وكون تقنيات ارتكابها لا تترك أي أثار محسوسة[410].

تطبيقا لهذا المفهوم الجديد لمبدأ الإقليمية، أقرّ القضاء الفرنسي اختصاصه بالنظر في قضية " Yahoo " وفقا للقانون الفرنسي مؤسسا موقفه على انه رغم تواجد مركز البث أو جهاز الخادم خارج الإقليم الفرنسي، إلا أن الرسائل التي يقوم ببثها هذا الجهاز تظهر في فرنسا و يمكن للجمهور الفرنسي الاطلاع عليها، لذلك اعتبر أن الجريمة مرتكبة في كل مكان تظهر فيه هذه الرسائل غير المشروعة محل البث[411].

لقد ذهب القضاء الأمريكي إلى أبعد من ذلك، حينما وسّع اختصاصه ليشمل كل الجرائم التي يمتد أثارها إلى إقليمه، وقضى بأنه إذا تم إدخال بيانات من إقليم دولة معينة

---

[408]– تم تبني هذا الرأي من طرف المشرع الألماني في عام 1975 و المشرع البلجيكي في عام 1982

[409]– أخذ بهذا الرأي المشرع الدانمركي، المشرع الايطالي والمشرع النرويجي، وكرس المشرع الجزائري هذا الرأي صراحة في المادة (586) من قانون الإجراءات الجزائية بنصها على " **تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها قد تم في الجزائر**".

[410]– **VERGUCHT Pascal**, la répression des délits informatiques dans une perspective internationale, thèse de doctorat soutenue a L'université Montpellier 1, le 11 avril 1996, pp. 347-348.

[411]- **DIOP Abdoulaye**, op.cit., p15. voir aussi **MIGNARD Jean-Pierre** , cybercriminalité et cyber-répression entre désordre et harmonisation mondiale, thèse de doctorat, université paris 1 panthéon-Sorbonne, 2004, pp 603-604.

تتضمن جريمة معلوماتية، و كانت هذه البيانات مقروءة في دولة أخرى و تمس بمصالحها أو تعرضها للخطر أو يمكن أن تمتد أثارها إلى إقليمها، فان محاكم هذه الدولة تكون مختص للتصدي لتلك البيانات الإجرامية ما دام يمكن الاطلاع عليها في إقليمها[412]. فمثلا إذا وضع الجاني صورا مؤثرة على جهاز الخادم متواجد في بريطانيا وكانت هذه الصور متاح الاطلاع عليها في الولايات المتحدة الأمريكية، ففي هذه الحالة يكون القضاء الأمريكي مختصا في التحقيق و الفصل في هذه الوقائع لا لأن أحد عناصر هذه الجريمة وقع في الإقليم الأمريكي، ولكن بمجرد أن هذه الصور الإجرامية متاحة للشعب الأمريكي[413].

ونظرا لتفاقم مسألة تنازع الاختصاص وتحولها إلى عائق حقيقي أمام مكافحة الجريمة الالكترونية، تدخل الفقه الجنائي وقدم حلا لهذه المشكلة يتمثل في إعطاء أولوية النظر في الجريمة الالكترونية للدولة التي تتوفر على أحد معايير تحديد الاختصاص الذي يكون الأكثر جدوى وفعالية لضمان سرعة ملاحقة المجرم الالكتروني. وقد يكون مبدأ الإقليمية الأكثر قبولا، لأن الدولة التي ترتكب علي إقليمها الجريمة أو أحد العناصر المكونة لركنها المادي تكون الأقرب إلى مسرح الجريمة وملابساتها و الأوفر حظا للوصل إلى أدلة إثبات، بالتالي فهي الأولى بالتحقيق في الجريمة وملاحقة فاعليها من غيرها من الدول. ولا يجد هذا الحل مبرره الحقيقي في اعتبارات السيادة الوطنية إنما في جدواه العملية، اذ حيث ترتكب

412– وهذا ما قضت به المحكمة العليا لولاية نيويورك بصدد جريمة انتهاك قانون المستهلك والدعاية الخادعة، وقضت به كذلك محكمة مينيسوتا في قضية (جرانتي جات ريسورت) بشأن بث موقع لألعاب القمار عبر الإنترنت من لاس فيغاس بولاية نيفادا ، الذي وصل إلى ولاية (مينيسوتا) التي يحظر قانونها مثل هذه الألعاب. وتكرس هذا الاتجاه القضائي أيضا فيما انتهت إليه الدائرة الخامسة الاستئنافية في قضية قمار ومراهنات عبر الإنترنت. وقد اعتبر القضاء المذكور مجرد وضع برمجية فك التشفير (PGP) على الإنترنت بمثابة تصدير لها، وهو ما يخول المحاكم الأمريكية التصدي لها باعتبارها صاحبة الاختصاص، بصرف النظر عن مكان وضع البرمجية. أنظر تفاصيل هذه القضايا في: **عمر محمد بن يونس**، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004، ص.ص908-910.

413 – **CHAWKI Mohamed** , op cit, pp 323-324

الجريمة الالكترونية تكون أدلة الإثبات أكثر وفرة ويكون إجراء التحقيقات الكفيلة لإظهار الحقيقة أكثر يسرا[414].

وأمام عدم نجاعة الحلول الفقهية المقترحة لتجاوز مشكلة تنازع الاختصاص التي تثيرها عملية التحقيق في الجرائم الالكترونية، لجأت الدول إلى تنظيم مسألة الاختصاص بنصوص واضحة في اتفاقيات دولية ثنائية ومتعددة الأطراف، يتم من خلالها تحديد الضوابط التي بموجبها توزع الولاية القضائية بين الأطراف المتعاقدة لتفادي التنازع، فقد نصت المادة (15) من اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة على انه يتعين على كل دولة طرف أن تعتمد ما يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقررة في الحالات الآتية:

ـــ حينما ترتكب الجريمة في إقليم تلك الدولة.

ـــ حينما ترتكب الجريمة ضد احد مواطني تلك الدولة.

ـ حينما ترتكب الجريمة من طرف احد مواطني تلك الدولة أو من طرف شخص عديم الجنسية اتخذ مكان إقامته المعتاد في إقليمها.

وأضافت هذه المادة، أنه إذا بلغت الدولة التي تمارس ولايتها القضائية عن سلوك إجرامي ما بموجب المعايير السالفة الذكر او علمت بطريقة أخرى أن دولة واحدة أو أكثر باشرت إجراءات التحقيق والمتابعة القضائية في السلوك ذاته، فعلى السلطات المختصة في هذه الدول أن تتشاور فيما بينها لغرض تنسيق ما تتخذه من التدابير.

أما عن اتفاقية مجلس أوروبا لمكافحة الجريمة الالكترونية فنظمت بدورها مسالة الاختصاص من خلال المادة (22) التي نصت على أنه يلتزم كل طرف بوضع مـا يلزم من

414 -**CONSEIL DE L'EUROPE** « la criminalité informatique, recommandation n° R (89) sur la criminalité en relation avec l'ordinateur et rapport final du comité Européen pour les problèmes criminels » Strasbourg, conseil de l'Europe, 1990, pp94-96.

تدابير تشريعية لإقرار الاختصاص بشان أي جريمة الكترونية وذلك:

ـ عندما ترتكب الجريمة علي إقليمه.

ـ عندما ترتكب الجريمة من طرف أحد مواطنيه إذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي لمكان ارتكابها. أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأي دولة[415].

وحثت هذه الاتفاقية الأطراف المتعاقدة في حالة وجود تنازع الاختصاص بين أكثر من طرف بشأن أي جريمة الكترونية تقررها هذه الاتفاقية، باللجوء متى كان ذلك ممكنا إلى التشاور فيما بينها لغرض تحديد الاختصاص القضائي الأكثر ملائمة لمتابعة هذه الجريمة[416].

اقتداء بهذه التشريعات، حاول المشرع الجزائري بدوره تقديم حلا لمشكلة تنازع الاختصاص، بنصه في المادة (15) من القانون رقم(04/09) المتضمن القواعد الخاص بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال وكافحتها، على أنه "**بالإضافة إلى قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، فان المحاكم الجزائرية تكون مختصة أيضا بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني**".

ولكن بالتمعن في هذا النص، يتبين أنه إعادة صياغة للمادة (588) من قانون الإجراءات الجزائية التي نصت على مبدأ الاختصاص العيني، ولم يأتي بأية إضافة جديدة

---

[415]- راجع نص المادة (22) من اتفاقية مجلس أوروبا لمكافحة الجريمة الالكترونية في الموقع التالي:

http://convention.coe.int/Treaty/FR/Treaties/Htm/185.htm.

[416]– أنظر الفقرة (05) من المادة (22) من الاتفاقية نفسها.

إلى قواعد الاختصاص مثلما استهل به نص المادة(15) من القانون (04/09).

الفرع الثاني: مشكلة احترام سيادة الدولة

تثار مسالة احترام السيادة عادة بمناسبة التفتيش الالكتروني العابر للحدود أو ما يسمي بالتفتيش عن بعد، وذلك حينما تكتشف سلطات التحقيق بان المعلومات أو البيانات التي يجري التفتيش عنها مخزونة في حاسوب أو أي جهاز الكتروني آخر متواجدة خارج إقليم الدولة التي يتواجد فيها حاسوب المتهم محل التفتيش والمرتبط به عن طريق شبكة الاتصالات البعيدة، وأن هذه المعلومات أو البيانات مهمة ومفيدة جدا لإثبات الجريمة الالكترونية، ففي هذه الحالة يطرح التساؤل حول مدى إمكانية إمداد التفتيش ليشمل الحاسب أو الجهاز الالكتروني المتواجد داخل إقليم دولة أجنبية ؟

أجمع الفقه على أنه لا يجوز أبدا لأجهزة التحقيق التابعة لدولة ما اللجوء إلى التفتيش العابر للحدود من أجل البحث عن معلومات أو بيانات مخزنة داخل حاسوب متواجد في إقليم دولة أخرى، واعتبر ذلك انتهاكا لسيادة هذه الدولة و خرقا لقواعد الاختصاص المكاني المتعارف عليها[417]. فحسب تقرير منظمة الأمم المتحدة حول الإجرام المعلوماتي، فان أي اختراق مباشر لقاعدة بيانات حاسوب متواجد في إقليم دولة أجنبية قصد استرجاع معلومات أو بيانات تم تخزينها فيه دون علم هذه الدولة أو رضاها المسبق، يعد خرقا لسيادة هذه الأخيرة وانتهاكا لمبدأ القانون الدولي القاضي بعدم التدخل في شؤون الداخلية للدول[418].

تأكيدا لهذا الموقف، أصدرت اللجنة الأوروبية الخاصة بالمشكلات التي يطرحها الإجرام المعلوماتي توصية اعتبرت فيها كل اختراق مباشر لغرض التفتيش أو الضبط أو أي إجراء من إجراءات التحقيق الأخرى يتم على إقليم دولة أجنبية يعد مساسا بسيادة هذه الدولة

417– **VERGUCHT Pascal**, op.cit, p 406 .

418 - **O.N.U**. Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique, New York, Nations Unies, 1994.

وتدخلا في اختصاص سلطات التحقيق التابعة لها، ويترتب عنه بطلان هذا الإجراء وعدم مشروعية الأدلة المتحصل عليها من خلاله[419]. وقد أكد القضاء هذا الموقف في عدة قضايا، أشهرها قضية الغش المعلوماتي المطروحة أمام القضاء الألماني، أين رفضت محكمة التحقيق الألمانية منح الإذن بالولوج عن بعد إلى بيانات مخزنة في حاسوب موجود في سويسرا قصد تفتيشها قبل موافقة أو مساعدة السلطات القضائية السويسرية، معتبرة ذلك مظهر من مظاهر احترام السيادة [420].

وهو الموقف ذاته الذي تبناه المجلس الأوروبي من خلال توصيته رقم(13) الصادرة في سنة 1995 المتعلقة بمشكلات قانون الإجراءات الجزائية المتصلة بتقنية المعلوماتية، إذ أوصى بعدم جواز اللجوء إلى التفتيش الالكتروني عن بعد أو العابر للحدود إلا في حالة وجود اتفاقيات تعاون قضائي ثنائية أو جماعية بين الدول تسمح بذلك، وأكدت بان أي تفتيش الكتروني عابر للحدود يتم دون اتفاق مسبق بين الدولتين المعنيتين يسمح بدلك يعد عملا منافيا لمبدأ احترام سيادة الدول، و مآله البطلان المطلق[421].

ومن أجل التوفيق بين ضرورة اللجوء السريع في بعض الأحيان إلى التفتيش الالكتروني العابر للحدود الذي تفرضه طبيعة الجريمة الالكترونية من جهة، وضرورة احترام سيادة الدول وعدم التدخل في شؤونها الداخلية من جهة أخرى، أوصت الاتفاقية الأوروبية الخاصة بالجرائم المعلوماتية المبرمة في بودبست عام 2001 من خلال مادتها (25) جميع دول الأطراف بضرورة توفير لبعضها البعض أقصى حد ممكن من المساعدة القضائية

---

[419]–**COMITE EUROPEEN** ; la Recommandation N°(89)-9 sur la criminalité en relation avec l'ordinateur et le Rapport final du comité européen pour les problèmes criminels, Strasbourg, 1990, p98.

[420]– **هلالي عبد ألاه أحمد** " تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي " مرجع سابق، ص 79.

[421]–**CONSEIL DE L'EUROPE** ; la Recommandation N°(95) 13 sur les problèmes de procédures pénales liées a la technologie de l'information et exposé des motifs, Strasbourg, 1996, p 188.

المتبادلة في مجال التحقيق وجمع الأدلة الالكترونية المتعلقة بالجرائم المعلوماتية. كما أقرت الاتفاقية في المادة (32) بحالتين يمكن فيها الدخول بغرض التفتيش عن بعد إلى أجهزة وشبكات تابعة لدولة أخرى بدون إذنها، الحالة الأولى هي حينما يتعلق التفتيش بمعلومات أو بيانات متاحة للجمهور، والحالة الثانية حينما يسمح ويرضى صاحب أو حائز هذه المعلومات بالتفتيش[422].

إقتداء بالقوانين سالفة الذكر، لم يسمح المشرع الجزائري بدوره بالتفتيش عن بعد لأنظمة الحاسب المتواجدة خارج الإقليم الوطني إلا في إطار المساعدة المتبادلة مع السلطات المختصة الأجنبية طبقا للاتفاقيات الدولية ذات الصلة، و في إطار مبدأ المعاملة بالمثل. وهو الموقف الذي عبّر عنه من خلال نص المادة (2/5) من القانون رقم(04/09) على النحو التالي :"...**إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظمة معلوماتية تقع خارج الإقليم الوطني، فالحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات صلة و وفقا لمبدأ المعاملة بالمثل**"[423].

اعتبار لما سبق، فان حضر معظم التشريعات استعمال تقنية التفتيش الالكتروني العابر للحدود بحجة تصادم هذا الإجراء مع مبدأ احترام سيادة الدول، شكل عائقا كبيرا أمام مكافحة سلطات البحث والتحري للجريمة الالكترونية، ويدفعها إلى اتخاذ إحدى المواقف التالية:

ـ إما أن يلجأ المحقق إلى التفتيش الالكتروني عن بعد والولوج في الحاسوب الآلي المتواجد في إقليم دولة أجنبية دون علم هذه الأخيرة، ففي هذه الحالة يكون إجراء التفتيش

---

[422] - **CHAWKI Mohammed** « combattre la cybercriminalité » op.cit., p 333.

[423]ـ أنظر المادة (2/05) من القانون رقم(4/09) المؤرخ في 14 شعبان 1430 الموافق ل 05 غشت سنة 2009 والمتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام و الاتصال ومكافحتها.

باطلا لتعارضه مع مبدأ احترام سيادة الدول، وبالتالي تكون الأدلة المتحصل عليها من هذا التفتيش غير مشروعة وفقا لقاعدة قانونية معروفة وهي **(ما بني على باطل فهو باطل)**، ناهيك عن إمكانية إثارة المسؤولية الجزائية للمحقق عن هذا التصرف.

ــ وإما أن يستغني المحقق عن التفتيش الالكتروني العابر للحدود ويطلب المساعدة عن طريق الإنابة القضائية من سلطات التحقيق التابعة للدولة الأجنبية التي يتواجد فيها الحاسوب أو الأجهزة المراد تفتيشها، وفي هذه الحالة لا يتم عادة التوصل إلى النتائج المنتظرة، نظرا للوقت الكبير الذي تستغرقه إجراءات المساعدة القضائية مقارنة بالسرعة الفائقة التي يتميز بها المجرم الالكتروني في إخفاء ومحو أثار الجريمة والدليل. أضف إلى ذلك، فان معظم الدول لا تقبل في الوقت الراهن طلبات إجراء التفتيش الالكتروني العابر بالحدود وتعتبرها مساسا بسيادتها الوطنية.

المطلب الثاني

صعوبات الاستدلال و الإثبات في الجرائم الإلكترونية

تتميز الجريمة الالكترونية عن الجريمة التقليدية بكونها ترتكب في بيئة افتراضية غير مادية عبر نبضات وذبذبات إلكترونية رقمية غير محسوسة، وتمحى آثارها بمجرد نقرة بسيطة على لوحة مفاتيح الحاسب، و في وقت قياسي قد يكون جزءًا من الثانية. مما يعطيها طابع خاص ليس فقط في طريقة ارتكابها، وإنما حتى في الوسيلة التي ترتكب بها، وهو ما قد يشكل صعوبات في اكتشاف الجريمة الالكترونية (الفرع الأول).

وتقودنا صعوبة اكتشاف الجريمة الالكترونية حتما إلى صعوبة إثباتها، إذ أن المجرم الالكتروني بما له من ذكاء ومعرفة فنية عالية يسعى دائما إلى عدم ترك وراءه أية آثار مادية تدّل على ارتكابه للجريمة أو تكشف عن هويته، مستعينا في ذلك بأساليب أمنية معقدة وتدابير الحماية الفنية ذات تقنية عالية (الفرع الثاني). ولعل من الأسباب الجوهرية التي

تحول دون إثبات الجريمة الالكترونية، ضعف معرفة أجهزة التحقيق والاستدلال و نقص خبرتهم في أساليب التصدي لهذه الجريمة (الفرع الثالث). ناهيك عن تعارض إجراءات التحقيق في مثل هذه الجرائم المستحدثة مع حرمة الحياة الخاصة للأشخاص (الفرع الرابع). بالإضافة إلى ضخامة كم البيانات التي يجب فحصها في ظرف وجيز من طرف سلطات التحقيق(الفرع الخامس). كل هذه العوامل من شأنها إعاقة مهمة الوصول إلى دليل الإثبات.

الفرع الأول: صعوبة اكتشاف الجريمة

يعد اكتشاف الجريمة الالكترونية من التحديات الحقيقية التي تعيق رجال الضبطية القضائية عن المواجهة الفعالة لها، والتي يرجع سببها إلى عدة اعتبارات، منها ما يتعلق بغياب الآثار المادية للجريمة، لأن الجريمة الالكترونية ترتكب عادة في بيئة افتراضية تقنية لا تترك أية آثار مادية محسوسة تدّل على الجريمة أو مرتكبها، ومنها ما هو راجع إلى سهولة إخفاء ومحو الدليل، إذ يكفي الضغط على زر في لوحة الاستخدام لزوال ملفات أو حتى قواعد بيانات وأنظمة بأكملها(أولا). كما أن الامتناع عن التبليغ بوقوع الجريمة الالكترونية، ونقص الخبرة و المعرفة الفنية لدى سلطات الاستدلال والإثبات تحول بدورها دون اكتشاف هذا النوع المستحدث من الجريمة(ثانيا).

-أولا:غياب الآثار المادية للجريمة و سهولة محو الدليل

توصف الجريمة الالكترونية بالهادئة، لان ارتكابها لا يحتاج إلى استعمال العنف أو القوة ولا إلى سفك دماء أو وقوع جثث، وإنما يتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح لحدوث اختراق معلومات و سجلات مخزنة في الحاسب الآلي و هتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها دون أن تخلف أية آثــار خارجية مرئية

أو ملموسة[424].

فالجريمة الالكترونية من الجرائم المستحدثة التي لا تترك شهودا يمكن الاستدلال بأقوالهم ولا بصمات يمكن تحليلها أو أدلة مادية يمكن فحصها، إنما تقع في بيئة الكترونية افتراضية عن طريق نقل معلومات رقمية و تداولها بواسطة ذبذبات الكترونية غير مرئية.

ولعل ما يزيد اكتشاف الجريمة الالكترونية وإثباتها أكثر صعوبة هو الوسيلة المستعملة في ارتكابها، والتي تتسم في معظم الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، إذ عادة ما ترتكب الجريمة الالكترونية بواسطة وسائل الكترونية ذات تقنية وتكنولوجيا عالية عن طريق نقل معلومات على شكل نبضات رقمية تنساب عبر أجزاء الحاسب الآلي وشبكة الاتصالات العالمية (الانترنيت) بصورة آلية ومجردة مثلما تنساب الكهرباء عبر الأسلاك. الأمر الذي يؤدي إلى تجريد الكيانات الإجرامية من الآثار والمعالم المادية التي يمكن الاستدلال من خلالها على وقوع الجريمة وإسنادها إلى شخص معين[425].

ومن الأسباب التي تصدّ عن اكتشاف الجرائم الالكترونية، القدرات الفنية العالية والمعرفة الواسعة التي يتمتع بها المجرم الالكتروني في مجال الإعلام الآلي والتكنولوجيات الحديثة، والتي تسمح له بالتحكم في جريمته بدقة كبيرة من خلال اختيار الفترة والطريقة المناسبتين لارتكابها تجعل المجني عليه لا يشعر بها ولا يدري حتى بوقوعها رغم حدوثها على مرأى أعينه. وهذه القدرات الفنية العالية جدا، كثيرا ما يكتسبها المجرمين من خلال مختلف المواقع الالكترونية ومنتديات القراصنة التي تضمن لهم الاتصال باستمرار فيما بينهم

---

[424]–**حسين بن سعدي الغافري** " التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت" ص 19. مقال متوفر في الموقع التالي: www.eastlaws.com.

[425]– **عمرو حسين عباس** "أدلة الإثبات الجنائي والجرائم الإلكترونية" بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكية في الوطن العربي،المنظم من طرف دولة مصر بمقر جامعة الدول العربية خلال الفترة الممتدة من 26-27 /2008/04، ص 08.

من وتبادل المعارف والخبرات في مجال الإجرام الالكتروني[426].

وتعتبر سهولة إخفاء الدليل الذي تخلفه الجريمة الالكترونية و سرعة محوه من الأسباب الجوهرية التي تقف دون اكتشاف الجريمة الالكترونية وإثباتها. إذ يستعمل المجرم الالكتروني عدة أساليب وتقنيات تسمح له بإخفاء كل آثار الجريمة والتستر عنها بسهولة كبيرة من أهمها، أسلوب التغليط والتضليل الذي يتم إما عن طريق التلاعب بقواعد البيانات والبرامج أو إدخال بيانات مختلقة مزيفة أو محرفة في نظام معلومات الحاسب، أو تغيير مسار البيانات الصحيحة المدخلة دون أن يحس المجني عليه بذلك. أو نتيجة تردد عدد كبير من الأشخاص على المكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط بين زمن ارتكابها وبين حدوث النتيجة الإجرامية (كما هو الحال بالنسبة لمقاهي الانترنت) مما يفسح المجال لحدوث تغيرات أو عبث في الآثار المادية للجريمة أو زوال بعضها، وهو ما يلقي ظلالا من الغموض على الدليل[427].

بالإضافة إلى ذلك، فان الدليل في الجريمة الالكترونية يتمثل عادة في بيانات أو معطيات الالكترونية على شكل كتابة أو تسجيلات صوتية أو صورية أو فيلمية، تخزن بذاكرة الحاسب بلغة رقمية في صورة برامج أو أنظمة تشغيل تتجسد في وحدات حسابية لا يمكن لأي شخص قراءتها و فهمها إلا باستعادتها في شاشة الحاسب، لذا يسهل محوها والتخلص منها بسرعة فائقة بمجرد الضغط على زرّ واحد في لوحة المفاتيح. ومن أمثلة ذلك، قيام أحد مهربي الأسلحة بالنمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه في تخزين عناوين عملائه و المتعاملين معه، على نحو يجعل

---

[426]– **حقاص صونية**، حماية الملكية الفكرية الأدبية و الفنية في البيئة الرقمية في التشريع الجزائري، مذكرة لنيل درجة الماجستير في علم المكتبات، تخصص المعلومات الالكترونية، الافتراضية والإستراتيجية البحث عن المعلومات، كلية العلوم الإنسانية والاجتماعية، جامعة قسنطينة، 2012، ص.ص 64-65.

[427]– **حسين بن سعدي الغافري**" التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت"، مرجع سابق، ص 09.

أية محاولة دخول إلى هذا الحاسب أو نسخ و طبع هذه العناوين قد تؤدي إلى المحو الفوري لكل البيانات[428].

-ثانيا: العزوف عن التبليغ بوقوع الجريمة الإلكترونية

من بين الأسباب الرئيسة التي تحول دون اكتشاف الجريمة الالكترونية، تكتم المجني عليه عنها و عدم تبليغ السلطات المختصة عن وقوعها بعد اكتشافها. إذ أثبتت التجارب أن معظم الجهات المجني عليها، لاسيما المؤسسات التجارية والمالية الخاصة أو العمومية تمتنع عن الكشف حتى بين موظفيها عما تعرضت لها من اعتداءات إلكترونية، وتكتفي فقط باتخاذ إجراءات إدارية وأمنية داخلية دون أن تبلغ السلطات المختصة عنها. ويجد هذا الموقف مبرره في أمرين، الأمر الأول يتمثل في حرص هذه المؤسسات على عدم المساس بسمعتها وفقدان زبائنها والمتعاملين معها الثقة في كفاءتها وقدرتها على حماية مصالحهم[429]. والأمر الثاني هو تشكيكها في قدرة و كفاءة سلطات الأمن على التصدي لهذا النمط الإجرامي الجديد، وتخوفها من أن تؤدي أعمال البحث والتحري إلى حجز حواسبها أو تعطيل شبكتها و نشاطها لفترة طويلة، ما قد يتسبب في زيادة خسائرها بالمقارنة مع الخسائر التي سببتها الجريمة أصلا [430].

إثباتا لهذا الواقع، كشفت إحدى الدراسات الإحصائية التي أجراها المعهد الوطني للقضاء التابع لوزارة العدل الأمريكية مؤخرا بأنه أكثر من 70% من الجرائم الالكترونية التي يتم اكتشافها لا تبلغ عنها إلى سلطات الأمن. وهي النتيجة نفسها التي أكدتها الدراسة

---

[428]– **سليمان أحمد فضل**، مرجع سابق، ص.ص 345–346.

[429]–**هشام محمد فريد رستم** " الجرائم المعلوماتية – أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي" بحوث مؤتمر القانون والكمبيوتر والانترنيت، جامعة الإمارات المتحدة ، كلية الشريعة والقانون، المجلد الثاني، ط 3، من 1 –3 ماي 2000، ص.ص 435–436.

[430] - **VERGUCHT Pascal**, op.cit., pp 323-326.

المنجزة من طرف معهد أمن الحاسوب بمشاركة مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية [431].

ومن أجل التقليل من ظاهرة التكتم عن الجرائم الالكترونية، عمدت بعض الدول إلى فرض التزاما على عاتق جهات المجني عليها بالإبلاغ عن هذه الجرائم بمجرد علمهم بوقوعها، و جعلت أي تقصير أو إخلال بهذا الالتزام يعرض صاحبه إلى عقوبات جزائية. إلا أن هذا الحل تعرض لانتقادات شديد من طرف الفقه والقضاء الدوليين، مفادها أنه من غير المقبول أبدا تحويل المجني عليه إلى مجرم يتم معاقبته بمجرد عدم تبليغه عن الجريمة التي وقع ضحية فيها، في حين يبقي المجرم الحقيقي دون عقاب [432].

أمام هذا الرفض، اتجهت بعض الدول إلى تبني حلول أخرى توافقية للوقوف ضد تفاقم ظاهرة التكتم عن الجريمة نذكر منها:

– فرض على المجني عليه التزاما بالتبليغ عن وقوع الجريمة الالكترونية إلى جهة خاصة أو سلطات إشرافية وليس إلى سلطات الأمن، فقد نص المشرع الأمريكي مثلا في القانون الخاص بحماية البنوك على أنه " يلتزم كل موظفي البنوك تحت طائلة عقوبات جزائية، بالتصريح و التبليغ عن كل ضياع أو نقص غير مبرر لمبلغ يفوق ألف دولار إلى جهاز المراقبة المالية، الذي يقوم بمراجعة هذه البلاغات و التدقيق فيها ثم يقرر من بين هذه البلاغات ما يستوجب تحويله إلى جهات الأمن[433].

– التحريض على التبليغ بالجريمة، عن طريق اتخاذ الدولة جملة من التدابير تشجع وتحفّز من خلالها الأشخاص على التبليغ عن وقوع الجرائم الالكترونية بعد اكتشافها. وقد

---

[431] – **حسين بن سعدي الغافري**، مرجع سابق، ص.ص 19–20.

[432] – **هشام محمد فريد رستم**، الجرائم المعلوماتية – أصول التحقيق الجنائي الفني...، مرجع سابق، ص 438.

[433] - **VERGUCHT Pascal**, op.cit. pp. 327-328.

تأخذ هذه التدابير شكل تنظيم حمالات تحسيسية وتوعية لبعث روح المسؤولية في ضمائر جهات المجني عليها، وقد تكون في شكل تدابير إدارية تشترط من خلالها على جهات المجني عليها التبليغ عن الجريمة لكي يستفيد من بعض الحقوق و الامتيازات. ففي كندا مثلا تشترط معظم شركات التامين على المؤمنين عندها، التبليغ المسبق لدى سلطات الأمن عن وقوع الجريمة الالكترونية، تحت طائلة عدم استفادتهم من التعويض عن الأضرار اللاحقة بهم جراء هذه الجريمة ، وعادة ما ينص على هذا الشرط في عقود التامين حتى لا يجهل به الزبائن و يكون حجة عليهم[434].

الفرع الثاني: صعوبة اكتشاف هوية الجناة

تعود صعوبة اكتشاف هوية المجرم الالكتروني إلى عدة عوامل نذكرها كالتالي:

أولاـ تعذر تحديد عنوان المجرم الإلكتروني

من بين المسائلة الشائكة التي تعرقل عملية التحقيق في الجرائم الالكترونية صعوبة تحديد مكان تواجد جهاز الحاسب الآلي مصدر النشاط الإجرامي، والذي يسمح من خلاله الكشف عن المجرم.

لذلك تستعين سلطات التحقيق عادة لتحديد مكان الحاسب الآلي أو الجهاز مصدر الفعل الإجرامي بنظام فحص الكتروني يسمي بعلم البصمات المعاصر[435]، الذي يتم من خلاله تتبع الحركة العكسية لمسار الانترنت، أو الحركة التراسلية للنشاط الممارس عبر الانترنت إلى غاية الوصول إلى عنوان رقمي للجهاز يسمي(adresse internet protocole IP). وهذا العنوان هو عبارة عن بروتوكول لعنونة البيانات و المواقع في شبكة

---

[434]- **LINGLET Monique_** « délinquance informatique, sur le front de la nouvelle criminalité, une parade concerné » R. I.P.C, mai 1995, P 182.

[435]– بفضل هذا النظام تم الكشف عن العديد من المجرمين مثل مبتكر فيروس ميليسا و مبتكر موقع خدمات بولمبروج لأخبار المال الاحتيالي الذي يرفع الأسهم عن طريق الخداع.

الانترنت، والذي يتم التعرف بمقتضاه على الجهاز الموصول بشبكة الانترنت من خلال عناوين عددية. مع العلم أن لكل جهاز الكتروني عنوانه الوحيد و الخاص به يسمي (IP adresse)، وكل عنوان (IP) مكون من جزأين، الجزء الأول يشمل أرقام الشبكة، والثاني يشمل أرقام مقدم الخدمة[436].

ويعمل برتوكول(IP) بشكل متزامن مع برتوكول آخر يدعى برتوكول التحكم بالنقل (Trams Commission Protocol TCP)، وهذان البرتوكولان (TCP/ IP) هما من عائلة بروتوكولات الاتصال بين عدة حواسيب طورت أساسا لنقل البيانات بين أنظمة (UNIX)[437]، ثم أصبحت المقياس المستخدم لنل البيانات الرقمية عبر شبكة الانترنت. ويرتكز البروتوكولان معا(TCP/ IP) على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Pachet) بين مختلف الوصلات السلكية و اللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها. وحزمة المعلومات تمثل جزء من ملف معلوماتي ذات حجم مصغر ثابت تحمل كل منها رقما خاصا ومعلومات تعريفية بكل من الحاسب المرسل و المرسل إليه، وعند كل وصلة تتم قراءة جهة المرسل إليه ثم تتم إعادة إرسال الحزمة المارة عبرهما نحو الوصلات التالية الأقرب إلى جهة المقصد أو المرسل إليها النهائية [438].

---

[436]– **عبد الحميد عبد المطلب** " استخدام برتوكول(TCP/ IP) في بحث و تحقيق الجرائم على الكمبيوتر" ص 05. بحث منشور على الموقع الالكتروني www.arablaw.info.com.

[437]–(UNIX) :هو نظام تشغيل متعدد المهام صمم لاستخدامه في الحاسب المنزلي أو المكتبي باعتباره مكتوب باللغة (C) ، وهي لغة برمجة عالية المستوى صممت خصيصا لتعمل وفق نظام(UNIX) ، و تستخدم في كتابة كافة التطبيقات بعد أن وضع مقاييسها من طرف المعهد القومي الأمريكي للمقاييس، لذلك يعد نظام (UNIX) الأكثر قابلية للنقل ألمعلوماتي من الأنظمة الأخرى.

[438]– **عبد الحميد عبد المطلب**، مرجع سابق، ص 01.

وإذا كانت الاستعانة بالمعلومات والعناوين والمصادر التي يحتويها نظام(TCP/ IP) يساعد حقيقة على الكشف عن مصدر الجهاز المستخدم في ارتكاب جريمة الكترونية ما و موقعه، وبالتالي الكشف عن المجرم الذي يفترض أن يكون صاحب هذا الجهاز، إلا أن هذه النتيجة ليست دائما صحيحة و موثوقة، لأن ما يتم التوصل إليه من خلال التقنية السابقة هو عنوان رقمي للحاسب فقط (adresse IP)، وهذا لا يكفي وحده لإسناد الفعل الإجرامي إلى صاحب الحاسب المذكور[439]. إذ من المحتمل جدا أن لا يكون هذا الأخير هو مرتكب الجريمة، كما لو كان حاسوبه مسروقا أو مؤجرا في الأماكن العامة كمقهى الانترنت، أو أن يكون عنوانه الرقمي مسروقا أو تم استخدامه من طرف شخصا أخر احتيالا. أو كأن يتبين في الأخير أن المتهم صاحب الحاسب لا يعرف استعمال الانترنت ولا استخدام الحاسب.

وقد أكدت المحكمة الفرنسية هذه الاحتمالات في قضية شهيرة تدعى فوريسيوا (Faurission)، حين نشرت رسالة الكترونية عنصرية ضد الصهيونية تحمل اسم الفرنسي(Robert Faurission) ، ولما اكتشفت على الموقع (Aaargh) الذي تم إيوائه في الولايات المتحدة الأمريكية حركت دعوى قضائية ضد هذا الشخص، إلا أن المحكمة لم تستطيع إقامة الدليل على أن المتهم هو الناشر الحقيقي للرسالة المجرّمة. وبالتالي قضت بأن وجود اسم المتهم في ذيل الرسالة لا يثبت بأنه مصدرها الحقيقي ولا يكفي أن يكون دليل إدانة، لان هدا الاسم يمكن لأي شخص أن يكتبه إمعانا في التمويه، الأمر الذي يقتضى إلزام متعهد الوصول بتحديد شخصية المشترك و عدم توصيل الأسماء المجهولة[440].

أضف إلى ذلك، فبرتوكول الانترنت (TCP/ IP) الذي يكشف عن الحاسب المرتكب بواسطته الجريمة الالكترونية ليس موحدا على المستوى العالمي وليس لصيقا به بصفة

---

[439]– **راسل تاينر** " أهمية التعاون الدولي في منع جرائم الانترنت" بحث مقدم إلى الندوة الإقليمية حول: الجرائم المتصلة بالكمبيوتر، الجارية بالمملكة المغربية في الفترة 19 و 20 جوان 2007، ص.ص 113–114.

[440]- **T.G.I**. novembre, 1998, disponible a l'adresse suivant ; http://www.legalis.jnet.decision/illicite - divers/correct-Paris-1998-htm.

دائمة، بل هو قابل للتغير مع كل اتصال بشكة الانترنت. لان كل خط هوية على الانترنت (IP) يصادفه عدد من الهويات التي يمكن أن تكون محلا للتغير بين أعضاء الانترنت المشتركين في مزود انترنت واحد، فمثلا عندما يتصل شخص من الجزائر بالانترنت تمنح له فورا هوية رقمية خاصة به، ولكن إذا حدث انقطاع في الإرسال و قام بعدها هذا الشخص بإعادة الاتصال بالانترنت مرة ثانية، فان ذلك يفقده هويته السابقة ليجد نفسه بهوية(IP) أخرى[441] .

ويزداد الأمر صعوبة، حينما تكون المعلومات المحملة في عناوين (IP) غير حقيقية أو مزيفة و هذا ممكن عند استخدام الحزم المعلوماتية (Packet) عنوان (IP) زائف، بحيث يظهر كأنما أرسلت هذه المعلومات من نظام معالجة محدد، في حين أنها أرسلت من حاسب آخر، ومثال ذلك عندما يقوم برنامج خبيث بإدخال معلومات كاذبة عن عنوان (IP) في حزم الإرسال قبل الولوج في الشبكة المعلوماتية[442]. ويتعقد الأمر أكثر، في حالة قرصنة عنوان أو صندوق البريد الالكتروني(boite e-mail) الخاص بشخص معين واستعماله من طرف شخص ثاني لارتكاب جريمة منتحلا هوية صاحب العنوان، بحيث يستعمل المجرم الالكتروني عادة في ذلك تقنية تسمي الصيد (Phishin) ، يتم من خلالها تقديم عروض مغرية للجمهور عبر الانترنت باستعمال صفحات ويب مزيفة خاصة بمؤسسات كبرى مشهورة تظهر وكأنها حقيقية و رسمية، ثم يشترط للاطلاع على هذه العروض والاستفادة منها ملئ صفحة البيانات الشخصية (اسم و لقب، عنوان البريد الالكتروني، رقم السر)، وبمجرد ملئ هذه الصفحة يتم سرقتها لتستعمل بعد ذلك لارتكاب جرائم باسم صاحب

---

[441]– **عمر محمد أبو بكر بن يوسف**، مرجع سابق، ص 811.

[442]–**غنام محمد غنام**، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت و جرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، القاهرة، 2013، ص220.

البيانات[443]. ففي هذه الحالة يستحيل على رجال التحقيق الكشف عن هوية المجرم الحقيقي.

ولقد طرح بشدة في مؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلو في الفترة الممتدة بين 29 و 31 ماي 2000، مشكل عدم إمكانية البنية التحتية للانترنت من التوصل إلى تحديد هوية مرتكب الجريمة أو المصدر الحقيقي لها، رغم توفر إمكانية التعرف على مكان ورقم الحاسوب أو الجهاز المرتبط بالانترنت والمستعمل كوسيلة لارتكاب الجريمة عن طريق عنوان (IP). ولكن مقابل ذلك، اعتبر بعض المشاركين في المؤتمر مسألة عدم الكشف عن شخصية و هوية الفاعل الذي يتستر وراءها مرسل الرسالة غير المشروعة هي أمر نسبي، إذ لا يوجد تجهيل بالمعني الكلي لشبكة المعلومات، حيث يترك الفاعل في كل الأحوال آثار أثناء تنقله في شبكة المعلومات تسمح للمحقق الوصول اليه. بالتالي فان هذا الأمر يتوقف بالدرجة الأولى على فطنة رجال الضبطية القضائية من خلال الإسناد الى فكرة الدلائل الكافية وما ينبثق منها من الشبهات، كما لو كان الحاسب الذي تم بواسطته ارتكاب الجريمة هو حاسب شخصي، ففي هذه الحالة يمكن للمحقق استجواب صاحب هذا الحاسب المشتبه فيها عما إذ سمح لشخص آخر استعمال جهازه، تاريخ و مدة استعماله، ثم يقارن كل هذه المعلومات مع معلومات الجريمة. كما يتوقف الأمر كذلك على مدى فعالية ونجاعة أساليب تتبع الآثار عبر الانترنت (la traçabilité) وتحديد هوية المستخدمين حتى يتسنى تحديد هوية الشخص المسئول جنائيا [444].

---

443 –**HABHAB Mohamad Ahmad ,** le droit pénal libanais a l Epreuve de la cybercriminalité, thèse de doctorat, soutenu a la Faculté de droit de Université Montpellier, le 10 juillet 2009, p.p 115-116.

444 –**أرحومة موسى مسعود** " الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" بحث مقدم الى المؤتمر المغاربي الأول حول المعلومات و القانون، المنظم من طرف أكاديمية الدراسات العليا طرابلس الفترة الممتدة من 28-2009/10/29، دون ترقيم الصفحات.

وفي هذا الإطار، وضعت بعض الدول المتقدمة في صدارتها فرنسا التزاما على مزودي خدمات الاتصال و الانترنت، بتحديد على مواقعهم هوية ناشر مضمون الرسالة وبياناته، وهوية المشتركين بشبكات المعلومات، لان مثل هذه التدابير من شأنها أن تجسد الشفافية بالنسبة للخدمات الموضوعة تحت تصرف الجمهور وتساعد عمل الضبطية القضائية في الكشف عن هوية المجرمين و الوصول إلى الأدلة [445].

ثانيا – فرض الجناة لتدابير أمنية

يتميز المجرم الالكتروني عن المجرم العادي بالذكاء و المعرفة الفنية الواسعة ، وهذه الخصلة تمكنه من التخطيط جيدا لجريمته قبل أن يقدم على ارتكابها، وإحاطتها بأساليب أمنية وتدابير الحماية الفنية التي تحول دون كشف أمره وتعيق مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل. فالمجرم الالكتروني غالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل ارتكابها، وذلك باستخدام كلمات المرور السرية وترميز البيانات المخزنة إلكترونيا والمنقولة عبر شبكات الاتصال، وتشفيرها بشكل يستحيل على سلطات البحث والتحري تعقب آثار الجريمة واستخلاص الدليل حولها دون الحصول على هذه الرموز والشفرات [446].

وقد يعمد المتهم إلى حماية حاسوبه الذي ارتكب بواسطته الجريمة الالكترونية بكلمة السر لمنع الغير من الدخول إليه والاطلاع على محتواه. ففي هذه الحالة يكون القائم بالتفتيش أمام خيارين هما، إما أن يطلب من المتهم الإفصاح عن كلمة السر التي تسمح له بالولوج إلى داخل الحاسب و تفتيشه، وهنا غالبا ما يتحفظ المتهم عن تقديم كلمة السر لان

---

[445]– **صالح أحمد البربري**" دور الشرطة في مكافحة جرائم الانترنت في إطار اتفاقية بودابست" مقال متاح في الموقع التالي: www.Arablaw.Com.

[446]- **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، القاهرة، 2002، ص 115.

القانون لا يجيز إجبار المتهم على تقديم أدلة أو الإجابة عن الأسئلة التي من شأنها أن تفضي إلى إدانته؛ إذ من حقه الاعتصام بالصمت دون أن يُفسَّر ذلك ضد مصلحته. وإما أن يسعى القائم بالتفتيش بنفسه إلى الكشف عن كلمة السر وفكّ رمز الدخول إلى الحاسوب، وفي هذه الحالة أيضا تصطدم سلطات البحث بجملة من الصعوبات، لان فكّ رموز الدخول ليس بالأمر الهين إذ يحتاج في أغلب الأحيان إلى جهد و وقت كبيرين بالإضافة إلى خبرة ومعرفة عالية في الميدان وهو الأمر الذي لا يتوفر عادة لدى معظم رجال التحقيق خاصة في الدول المتخلفة[447].

وقد يلجأ كذلك المتهم إلى تشفير البيانات المخزنة داخل حاسوبه للحيلولة دون وصول المحقق إلى الأدلة التي تدينه، ويقصد بتشفير البيانات استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها البيانات أو المعلومات المراد تمريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات المخزنة في الحاسوب بدونها[448]. مع العلم أن عملية التشفير تتم وفق معادلات رياضية معقدة تسمى الخوارزميات. وهنا أيضا يجد المحقق نفسه أمام خيارين لحل مشكلة التشفير وهما، إما أن يحصل على مفاتيح الشفرات من المتهم مشغل الحاسوب، وإما أن يحاول فكّ الشفرات بنفسه. إلا أن في الخيار الثاني يجب أن يكون المحقق ملمّ بعلم تحليل الشفرات أو ما يعرف بعلم استرجاع النص الواضح بعبارة معينة بدون معرفة المفاتيح، ويرتكز هذا العلم على الرياضيات التطبيقية وفروعها المختلفة مثل نظرية الاحتمالية و نظرية الإعداد والإحصاء والجبر، وهو الأمر المفقود لدى المحقق.

---

[447]– **ممدوح عبد الحميد عبد المطلب**" جرائم استخدام شبكة المعلومات العالمية" بحث مقدم الى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة ، 2000، ص.ص 24 وما بعدها.

[448]– **إسماعيل عبد النبي شاهين**" أمن المعلومات في الانترنت" بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، 2000، ص11.

ومن ضمن الأساليب الأمنية والتدابير الحماية الفنية المهمة التي يستعين بها المجرم الالكتروني لإعاقة مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل، إعداد الفيروسات داخل حاسبه على شكل برامج غير مرئية، كفيروس حصان طروادة والدودة أو برامج القنابل المنطقية أو الزمنية، وجعل وظيفة هذه الفيروسات هي حماية الحاسوب وما يحتويه من بيانات وبرامج و ملفات من خطر الدخول والنسخ غير المرخص. ففي الغالب يبرمج المجرم بداية نشاط هذه الفيروسات بمجرد محاولة اختراق الحاسب أو النسخ لتقوم مباشرة بتخريب نظام تشغيل الجهاز محل التفتيش وإتلاف كلي للبيانات والملفات المخزنة داخل ذاكرته، مما يجعلها غير قابلة الاسترجاع وبالتالي استحالة وصول المحقق إلى الملفات المفقودة والاطلاع على محتواها[449].

علاوة على ذلك، هناك تقنية حديثة يستعين بها المجرم الالكتروني لإخفاء آثار جريمته تسمي بتقنية إخفاء المعلومات (Steganography)[450]، يقوم المتهم من خلالها بإخفاء بيانات مهمة داخل بيانات أخرى قد تكون على شكل ملفات مصورة أو صوتية أو فيلمية أو على شكل بيانات تنفيذية لبرامج الحاسب، أو يقوم بإخفاء هذه المعلومات في مساحة معينة من القرص الصلب مخصصة فقط لتخزين ملفات أنظمة التشغيل دون غيرها تسمى بالمساحة الهادئة (Slack). وهذه التقنية من شأنها تغليط مسار رجال التحقيق و تعيقهم من الوصول إلى أدلة مادية ضد المتهم، مع العلم أن اكتشاف البيانات المخفية و تحليلها في هذه الحالة لا تتم إلا بطريقة علمية و رياضية معقدة جدا تسمى بتقنية تحليل البيانات

---

[449]– **محمد حسام محمود لطفي** " الجرائم التي تقع على الحاسبات او بواسطتها" بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص 496.

[450]– للمزيد من التفاصيل في هذا الموضوع راجع : **مراد عبد الرحمان مكاوي** " الستيغانوغرافي " مجلة المعرفة، العدد 147، نيسان، 2009، ص 41. منشور على الموقع التالي:

http://www.almarefh.org/news.php?action=shawgid=6,4

المخفية (Steganalysis) لا يفهمها إلا ذوي الاختصاص[451].

ونظرا للإفراط الكبير في استعمال تدابير الحماية الفنية في الدول المتقدمة وما نتج عنه من آثار سلبية، قامت بعض الدول باستحداث تشريعات تمنع بموجبها اللجوء إلى هذه التدابير والتقنيات (التشفير والترميز) بدون ترخيص، في مقدمة هذه الدول، فرنسا التي وضعت ضوابط صارمة لعملية التشفير منها ما يتعلق بإلزام كل من المقدم على التشفير أو مبتكر برنامج التشفير بالحصول على ترخيص مسبق من الهيئات المعنية، مع ضرورة إيداع مفاتيح التشفير لدى هذه الهيئات، واعتبرت أي إخلال بهذه الالتزامات جريمة يعاقب عليها القانون [452].

الفرع الثالث: نقص خبرة و كفـاءة سلطات الاستدلال

إذا كانت السلطات القائمة بالتحقيق من رجال الضبطية و قضاة تلعب دورا كبيرا في التحري عن الجرائم و البحث عن مرتكبيها في إطار الجرائم التقليدية، فان دورها في مكافحة الجرائم الالكترونية محدود ولا يرقى إلى الدرجة نفسها، وذلك راجع إلى عدة أسباب بعضها مرتبط بشخصية المحقق، كالتهيب من استخدام وسائل تكنولوجيا الإعلام والاتصال الحديثة والانترنت، وعدم الاهتمام بمتابعة المستجدات الحاصلة في مجال الإجرام الالكتروني[453]. والبعض الأخر يتعلق بنقص مهاراتهم الفنية في استخدام الوسائل الالكترونية الحديثة والانترنت، وقلة خبرتهم في تقنيات البحث والتحقيق بخصوص الجرائم المتصلة بهذه الوسائل، الناتج عن عدم إلمامهم بأساليب ارتكاب الجرائم الالكترونية وعدم معرفتهم باللغة العلمية الرقمية. إذ يملك العاملين في مجال الإعلام الآلي مصطلحات علمية خاصة

---

[451]– **مراد عبد الرحمان مكاوي**، مرجع سابق، ص43.

[452] - **HABHAB Mohamed Ahmad**, op.cit. p 120

[453]– **عبد الرحمان محمد بحر**، مرجع سابق، ص.ص 95–96.

أصبحت تشكل الطابع المميز لمحادثاتهم و أساليب التفاهم فيما بينهم، وليس هذا فحسب بل قاموا باختصار هذه المصطلحات بالحروف اللاتينية الأولى و جعلوا منها لغة جديدة غريبة تسمي بلغة المختصرات لا يفهمها إلا من كان منهم أو كان مختصا في الإعلام الآلي[454].

على غرار ذلك، فان الطبيعة الخاصة للبيئة الالكترونية والخصوصية اللامادية للدليل الالكتروني الرقمي الذي يتطلبه إثبات الجريمة الالكترونية ينعكس سلبا على عمل الجهات المكلفة بالبحث والتحري، إذ يتطلب الكشف عن هذه الجرائم اكتساب جهات التحقيق مهارات خاصة على نحو يساعدهم على مواجهة التقنيات المعلوماتية العالية[455]. فنقص الخبرة لدى هؤلاء قد يفضي إلى تدمير الدليل وإتلافه، على اعتبار أن جهلهم بأساليب ارتكاب الجرائم المعلوماتية يجعلهم في كثير من الأحيان يقعون في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها، مثل إتلاف محتويات الأقراص الممغنطة و أوعية المعلومات التي تُخزَّن بها البيانات[456]. وقد ترتكب جرائم إلكترونية على مرأى و مسمع من سلطات الضبط، بل قد يقدمون على تقديم يد العون لمرتكبي هذه الجرائم عن جهالة دون أن يشعروا بذلك. من هنا يرى المتخصصون في مكافحة الجرائم الالكترونية أن الأنظمة المعلوماتية و ما يقع عليها من جرائم تعد تحديا حقيقيا لأجهزة العدالة الجنائية، ذلك لأن رجل الأمن غير المتخصص والذي انحصرت معلوماته و خبراته في الجرائم التقليدية من قتل وضرب وسرقة لن يكون قادرا على التعامل مع الجريمة الالكترونية الحديثة التي ترتكب بواسطة تقنيات عالية[457].

---

[454]– **خالد ممدوح إبراهيم**، مرجع سابق، ص 69.

[455]– **محمد الأمين البشري**" التحقيق في جرائم الحاسب الآلي" بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، ط الثالثة، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من 1 إلى 3 ماي 2004، ص 1070.

[456]– **جميل عبد الباقي الصغير**، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص115.

[457]– **حسين بن سعيد بن سيف الغافري**، مرجع سابق، ص 410.

ولقد دفع هذا العجز والهون الذي أصاب سلطات تنفيذ القانون بعض الدول إلى استقطاب المختصين وذوي الكفاءات العالية في مجال تكنولوجية الإعلام والاتصال ضمن أجهزتها الأمنية والقضائية، وتنظيم دورات تدريبية تخصصية وندوات تبادل المعارف والخبرات قصد الرفع من قدرات هذه الأخيرة في مكافحة الإجرام الالكتروني[458].

ولكن رغم هذه الجهود إلا أن أجهزة الأمن القضاء ما تزال غير قادرة على مواكبة التطورات والمتغيرات السريعة التي تطرأ يوما بعد يوم على ظاهرة الإجرام الالكتروني، وذلك راجع إلى عوامل عدة أهمها، اتساع مهامها ليشمل مجالات متنوعة و عدم تفرغها تماما للجرائم الالكترونية، ومن هنا كانت المناداة إلى إنشاء وحدات تحقيق خاصة بالجرائم الالكترونية متفرغة لهذا النوع من الجرائم. وقد يكون لحداثة هذا النوع من الجرائم وقلّة المستكشف عنها عامل آخر لعدم اكتساب تلك الأجهزة خبرة التعامل معها، ناهيك عن ضخامة المعلومات الموجودة على شبكة الانترنت، و التي يستلزم الاطلاع عليها والبحث فيها وقتا وجهدا كبيرين. إلى جانب انتشار أجهزة الإعلام والاتصال الحديثة وتنوع برامجها وأنظمتها وتطبيقاتها بشكل يجعل مهمة حصر أساليب الجريمة الالكترونية وصورها وأنماطها أمرا صعب يتعذر معه تدريب المحققين.

علاوة على ما سبق، فان الميزانية المالية المرصودة لتدريب رجال الضبطية القضائية لا تكفي في أغلب الأحيان لاستقطاب النخبة المتميزة والمتفوقة في مجال تكنولوجية الإعلام ضمن الأجهزة الحكومية، خاصة أمام المنافسة الشرسة من طرف شركات ومؤسسات القطاع الخاص التي تبذل المستحيل من أجل ضم هذه النخبة إليها[459]. وكل هذه العوامل ساهمت في ركود القدرات المعرفية في مواجهة الجرائم المعلوماتية لدى رجال الضبطية القضائية.

---

[458]– **محمد الأمين البشري**" تأهيل المحققين في جرائم الحاسب الآلي والانترنت" ، مرجع سابق، ص.ص 32–33.

[459]– **حسين بن سعيد بن سيف الغافري**، مرجع سابق، ص 411.

الفرع الرابع: تعارض إجراءات التحقيق مع مبدأ احترام الحياة الخاصة

يعتبر الحق في الخصوصية أو الحياة الشخصية أحد الحقوق الفردية الأساسية التي تكفّلت معظم تشريعات العالم بحمايتها من أي خرق أو انتهاك[460]، وهذه الحماية ذاتها قد تشكل أحيانا عقبة أمام سلطات التحقيق في مكافحة الجرائم الالكترونية. لأن المحقق الذي يقوم بالتفتيش على نظم الحاسب الآلي وقواعد بياناته أو على شبكات الانترنت غالبا ما يتجاوز النظام المعلوماتي للمشتبه فيه إلى أنظمة أخرى مرتبطة به، بسبب شيوع التشبيك بين أجهزة الحواسيب و انتشار الشبكات الداخلية على مستوى المنشآت، والشبكات الجهوية والدولية على مستوى الدول. وهذا الامتداد في التفتيش إلى نظم معلوماتية غير النظام محل الاشتباه، قد يؤدي إلى الاطلاع على ملفات سرية و بيانات خاصة بأشخاص لا علاقة لهم بالجريمة، مما يشكل انتهاكا للخصوصية المعلوماتية لهؤلاء ومساسا بحرمة إسرارهم الشخصية.

ولعل من أكثر إجراءات التحقيق تعارضا مع الحق في الخصوصية و أكثرهم انتهاكا لحق السرية باعتباره جوهر هذه الأخيرة (أي لحق الخصوصية)، إجراء اعتراض المراسلات وتسجيل الأصوات والمراقبة الالكترونية للاتصالات، الذي يقوم أساسا على تصنّت وتسمّع سلطات الضبط القضائي خفية على كل المكالمات والمحادثات التي يجريها المشتبه به عبر وسائل الاتصال السلكية و اللاسلكية، والاطلاع على ما تتضمنه مراسلاته من أسرار وأفكار شخصية وتسجيلها دون علمه.

---

[460]–نذكر منها المواد (1 و 5 و 12) من الإعلان العالمي لحقوق الإنسان لعام 1948، والمادة (17/ف1و2) من العهد الدولي للحقوق المدنية والسياسية لعام 1966، والمادة (8) من الاتفاقية الأوربية لحقوق الإنسان والحريات الأساسية لعام 1950، و المادة (11) من الاتفاقية الأمريكية لحماية حقوق الإنسان لعام 1969، والمادة (17) من الميثاق العربي لحقوق الإنسان لعام 2004.

وهذا الإجراء، إن كان قد أجازه القانون في حالات خاصة استثنائية تقتضيها ضرورات البحث والتحري عن حقيقة بعض الجرائم[461]، وأحاطه بضمانات وضوابط إجرائية وموضوعية صارمة[462]، إلا أن ذلك لا يمنع من حدوث تجاوزات مقصودة وغير مقصودة من طرف سلطات الاستدلال ضد حرمة سرية مراسلات واتصالات الأفراد. فكم من دعاوى جزائية انقضت بسبب بطلان إجراءات التحقيق لخروجها عن حدود المشروعية، وأدلة إثبات استبعدت من طرف القضاء لعدم التزام سلطات الاستدلال بشروط بحثها وتحصيلها، وكم من محادثات خاصة أو شخصية تعرضت لانتهاكات متكررة من قبل السلطات العامة للدولة لا لشيء إلا لهاجس أمني[463] أو بدافع الضغط على الأفراد لتحقيق أغراض سياسية أو مصالح شخصية[464]. وقد عبّر القاضي الأمريكي دوجلاس (Douglas) عن عدم ارتياحه لهذه التجاوزات وصرح بلهجة شديد بأن " **المراقبة الالكترونية أصبحت أكبر سالب لخصوصية الإنسان، وامتدادها شيء لا يطاق في مجتمع يتمتع بحرية التعبير وحرمة الحياة الشخصية، لذا ينبغي إلغاءها، أو على الأقل قصرها على الحالات شديدة الاضطرار**" [465].

---

[461]- أنظر نص المادة(65 مكرر 5) من الأمر (02/15) يتضمن قانون الإجراءات الجزائية الجزائري، مرجع سابق.

[462]–أنظر هذه الضمانات في نص المادة (46) الدستور الجزائري، و المواد (65 مكرر5 إلى 65 مكرر 10) من قانون الإجراءات الجزائية الجزائري، المرجع نفسه.

[463]– في هذا الصدد أصدرت مفوضة منظمة الأمم المتحدة بيانا في 11 أكتوبر 2001 بعنوان "حقوق الإنسان والإرهاب" أكدت فيه "**أن مكافحة الإرهاب لابد ان تكون مقيدة بمتطلبات العدالة وسيادة القانون واحترام حقوق الإنسان، ولا يجوز أن يتخذ الهاجس الأمني ذريعة على انتهاك حقوق الإنسان**" .

[464]– **جلاد سليم**، الحق في الخصوصية بين الضمانات و الضوابط في التشريع الجزائري و الفقه الإسلامي، مذكرة لنيل شهادة الماجستير في الشريعة و القانون، تخصص حقوق الإنسان، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، 2013، ص 91.

[465]–نقلا عن، **جلاد سليم**، المرجع نفسه، ص 92.

وفي هذا الصدد، أثيرت عدة تعليقات حول استحداث المشرع الجزائري للمادة (65 مكرر 5 من ق إ ج) التي تسمح باعتراض المراسلات و تسجيل الأصوات والتقاط الصور، بأنها تخالف ما جاء في المادتين(303 و 303) مكرر من قانون العقوبات اللّتان تنصّان على تجريم إتلاف الرسائل، والمراسلات والتقاط وتسجيل ونقل المكالمات والأحاديث الخاصة أو السرية، والتقاط وتسجيل أو نقل في مكان خاص بغير **إذن صاحبها أو رضاه**. مع العلم أن عمليات الاعتراض و التسجيل التي تجيزها المادة (65 مكرر 5) أعلاه تتم خفية وبدون علم أو رضا المشتبه فيه صاحب المراسلات و المكالمات. وعليه فإذا كان قانون الإجراءات الجزائية هو الدرب الذي يبين كيفية وضع ما ورد في قانون العقوبات حيز التطبيق، فيفترض ألا تكون أحكامه مخالفة لهذا الأخير، أو يكون هناك تناقض بين القانونين مثلما هو الوضع بالنسبة لهذه المواد، لان ذلك قد يشكل ثغرة يمكن أن يستغلها البعض لضرب حقوق وحرمات أشخاص أبرياء[466].

كما قد، يضع سلطات التحقيق في موقف صعب يفرض عليها تحقيق التوازن بين مصلحتين متعارضتين هما، مصلحة الدولة التي تهدف إلى تحقيق المصلحة العامة من خلال الكشف عن الجرائم الالكترونية والبحث و التحري فيها للوصول إلى الحقيقة بغرض اقتضاء الدولة لحقها في العقاب، ومصلحة الفرد بضمان عدم المساس بحقوقه و حرياته وحرمة حياته الخاصة[467]. وفي حالة عدم توفيقه في تجسيد هذا التوازن و صدرت عنه تصرفات غير فعالة أو منتجة لأضرار زائدة أو متجاوز فيها في حق هاته المصلحة أو تلك، يكون المحقق عرضة لمتابعات جزائية وعقوبات سالبة للحرية[468].

---

[466]–**وهاب حمزة**، الحماية الدستورية للحرية الشخصية خلال مرحلة الاستدلال و التحقيق في التشريع الجزائري، دار الخلدونية، الجزائر، 2011، ص123.

[467] – **DIOP Abdoulay**, procédures pénales et TIC, op.cit., p 125

[468]– تنص المادة 137 من قانون العقوبات الجزائري على " **كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة للبريد يقوم بفض أو اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو**

نتيجة لهذا الوضع، لم تستطع معظم التشريعات والمواثيق الدولية التكتم عن مخاوفها الكبيرة حول الانتهاكات التي يمكن أن يرتكبها رجال الضبطية القضائية ضد خصوصية الأفراد وحرمة إسرارهم بمناسبة التحقيق في الجرائم الالكترونية، فقد أوصت اتفاقية بودابست في ديباجتها ومادتها (15) على ضرورة الأخذ بعين الاعتبار الحاجة إلى ضمان وجود توازن مناسب بين مصلحة المجتمع الدولي في مكافحة وقمع الإجرام الالكتروني واحترام حقوق الإنسان الأساسية، وفي الشأن نفسه أشارت أجندة تونس التي وضعت خلال القمة العالمية حول مجتمع المعلومات، تحت رعاية الأمم المتحدة إلى أهمية احترام الحريات الأساسية من طرف سلطات الضبطية القضائية وصرحت بأنه " يجب على الدول عند اتخاذها التدابير والإجراءات الضرورية لضمان استقرار وأمن شبكة الانترنت ومكافحة الجرائم الناشئة عنها، أن تراعي الحق في الخصوصية وغيرها من الحقوق و الحريات العامة للأفراد تطبيقا للأحكام الواردة في الإعلان العالمي لحقوق الإنسان و إعلان جنيف للمبادئ "[469].

تجسيدا لهذا المبتغى، فقد سعى المشرع الأوروبي إلى التوفيق بين فعالية عمل الشرطة القضائية واحترام الحقوق الأساسية للإفراد من خلال استحداث نظام شنجين للمعلومات (système d'information Schengen SIS)، يتكون من قسم مركزي مقره في مدينة ستراسبورج و أقسام فرعية في كل دولة من دول المنظمة، يحتوى على بنك معلومات كبير تسجل فيه كل المعلومات التي ترسلها إليه قوات الشرطة و السلطات القضائية في كل دولة عضو، بما فيها عناوين الأشخاص المطلوب تسليمهم من قبل دولة أخرى، أو الممنوعين من دخول إقليم دولة ما، أو المعلن اختفائهم أو المطلوب تقديمهم للعدالة بموجب أمر قضائي.

إتلافها بالحبس من ثلاثة أشهر إلى خمسة سنوات و بغرامة من 3000دج إلى 500000دج...، ويعاقب الجاني فضلا على ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات".

[469]– أنظر أجندة تونس، المتبني في 15 نوفمبر 2005، متوفرة على الموقع:
http://portal.unesco.org/ci/fr/files/20687/11327544873tunis_agenda_fr.pdf/tunis_agenda_fr.pdf.

ولا يجوز الرجوع إلى نظام المعلومات (SIS) إلا في حالة القيام بإجراءات المراقبة على الحدود من طرف الشرطة أو الجمارك، أو عند تسليم تأشيرة الدخول و كذا الإقامة[470].

رغبة في تعزيز نظام تشنجين للمعلومات (SIS)، وضمان احترام أوسع للحقوق الأساسية للإفراد، قام المجلس الأوروبي في عام 1981 بإبرام اتفاقية خاصة بحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات ذات الطابع الشخصي، وفرض فيها على كل دولة انضمت إلى الاتفاقية ضمان حدّ أدنى من الحماية للبيانات الشخصية في قانونها الوطني. ولم يتوقف الأمر عند هذا الحد، بل قام المجلس الأوروبي كذلك بتكليف هيئة رقابة مشتركة بمهمة دعم العمل الآلي لنظام معلومات شنجين قصد توفير وضمان حماية أفضل لخصوصية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات ذات طابع شخصي، على أن تتم عملية الرقابة طبقا للإجراءات التي حددتها هذه الاتفاقية واتفاقية المجلس الأوروبي. وفي السياق نفسه، أوصت لجنة وزراء المجلس الأوروبي من خلال توصيتها رقم (R15ـ85) الدول الأطراف في اتفاقية المجلس بضرورة تقنين عملية استخدام البيانات ذات الطابع الشخصي من قبل سلطات الأمن وطبقا للقانون الوطني للجهة المتعاقدة والمسئولة عن وظيفة الدعم الآلي[471].

نخلص إلى، أن هذه الالتزامات التي وضعتها مختلف التشريعات الوطنية و الدولية على عاتق رجال الضبطية القضائية لتفادي أي خرق لخصوصية و أسرار الأفراد بمناسبة البحث والتحري في الجرائم الالكترونية قد تمثل عقبة تصعب من مهمة التحقيق. لأنها من جهة تبعث التردد و الخوف في نفس المحقق من وقوعه في خطأ عدم احترام هذه الالتزامات

---

[470]– **جان فرنسوا هنروت**" أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي" بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنظمة من طرف المملكة المغربية خلال الفترة الممتدة من 19-2008/06/20، ص 109.

[471]– المرجع نفسه، ص 110.

وبالتالي إثارة مسؤوليته الجزائية، وهذا التردد و الخوف من شأنهما أن يصدا المحقق من أداء وظائفه في أكمل وجه، إن لم يدفعا به إلى التخلي نهائيا عن التحقيق. ومن جهة أخرى، قد يبذل المحقق قصار جهده للوصول إلى أدلة مادية تثبت الجريمة الالكترونية المرتكبة، ولكن في النهاية تستبعد من قبل القضاء لعدم مشروعيتها بسبب انتهاك المحقق حرمة الخصوصية أثناء جمعه هذه الأدلة.

الفرع الخامس: ضخامة كم البيانات الواجب التحقيق فيها

تعرف قواعد البيانات بأنها مجموعة من بطاقات تشمل بيانات معدلة ومنظمة تسمح باقتطاع البيانات حسب رغبة المستعمل، ومصطلح قاعدة أو بنك البيانات شاع استعماله وربما يعني لمعظم الناس بأنه نوع من الحاسب تجمع فيه كل أنواع المعطيات الخاصة يتم الرجوع إليها عند الحاجة[472].

وتعتبر قاعدة البيانات نظام فعال يستخدم لترتيب الملفات التي تحتوي على معلومات محددة في بطاقات خاصة، وقاعدة بيانات واحدة يمكنها أن تشمل على عدد لا يحصى من الملفات، ويمكن استخراج هذه البطاقات بنظام أبجدي باختيار عناصر معينة وترتيبها للاستفادة منها لاحقا، كما تستعمل قواعد البيانات كوسيلة لتخزين المعلومات ومعالجتها وتجميعها في حقل خاص[473].

لذلك، يشكل الكم الهائل للبيانات التي يجري تداولها في الأنظمة المعلوماتية إحدى الصعوبات البارزة التي تعيق التحقيق في الجرائم التي تقع عليها أو بواسطتها، إذ عادة ما يتطلب البحث عن الأدلة في حاسب واحد، الاطلاع والفحص الدقيق لكل المعطيات التي

---

[472]– **صغير يوسف**، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري بتيزي وزو، 2013، ص 128.

[473]– **بوعمرة آسيا**، النظام القانوني لقواعد البيانات، مذكر لنيل شهادة الماجستير في القانون، فرع الملكية الفكرية، كلية الحقوق، جامعة الجزائر، 2005، ص.ص 11–12.

تتضمنها آلاف الملفات المخزنة في ذاكرته، ويكلّف المحقق وقتاً و جهدا كبيرين [474]. وهو ما قد ينعكس سلبا على مردود سلطات البحث والتحقيق بسبب الضجر و الملل ويؤدي بهم إلى التخلي عن مواصلة البحث والتحقيق.

وتزداد المسألة تعقيداً، حينما يكون محل البحث هو الشبكة المعلوماتية (الإنترنت)؛ إذ يصبح ضبط الدليل والبحث عنه أمراً في غاية الصعوبة، إن لم يكن مستحيلاً، على اعتبار أن التفتيش والضبط في هذا الفضاء الافتراضي اللامتناهي يستدعى من المحقق تصفح عدد هائل من مواقع وصفحات الانترنت وفحص كم ضخم من البيانات لا قبل له بها. ما قد يسبب له إرهاقا شديد قد يدفعه إلى الخروج عن الضوابط القانونية للبحث و تحصيل الدليل، ما يجعل القضاء لا يكترث بالدليل الرقمي المستخلص من هذه العملية، لافتقاده لشروط المشروعية والمصداقية التي تجعله جدير بالثقة[475].

وقد لا تضفي عملية البحث والتحري إلى نتيجة رغم الجهد والوقت الكبيرين المبذولين من طرف المحقق، بسبب تواضع مستواه الفني و التقني في فنون وتقنيات استخدام وسائل الإعلام والاتصال الحديثة من ناحية، وعدم وجود آلية للفرز الذاتي للملفات المخزنة، حتى يتسن الوقوف على البيانات غير المشروعة و ضبطها من جهة أخرى، مما يؤثر سلبا على معنويات المحقق، ويفقده الثقة في مؤهلاته وقدراته[476].

---

[474]– **هشام محمد فريد رستم** " الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي" مرجع سابق، ص430.

[475]– **موسى مسعود أرحومة**، مرجع سابق، ص05.

[476]– **صغير يوسف**، مرجع سابق، ص.ص 129–130.

المبحث الثاني

عقبات ناتجة عن ضعف قوانين مكافحة الجرائم الإلكترونية

تتسم القوانين الجنائية الموضوعية منها و الإجرائية بطابع تقليدي مفرط يميل إلى الثبات والاستقرار، وقد ترتب على ذلك قصور هذه القواعد عن مواكبة التطور العلمي والتكنولوجي الذي طرأ على كافة مناحي الحياة المعاصرة بصفة عامة، وملاحقة الجرائم الناشئة عنها بصورها المختلفة، ويقف حجر عثرة في سبيل الاستفادة من معطيات التكنولوجيا الحديثة في الكشف عن الجرائم الالكترونية و ملاحقة مرتكبيها.

ويبدو جوهر هذه الإشكالية في حداثة العهد بهذا النوع من الجرائم و سرعة تطورها، وما يثور من شك حول مدى كفاية النصوص التقليدية في مواجهتها، مع العلم ان هذه النصوص قد وضعت لتطبق وفق مفاهيم تقليدية لا تتفق مع طبيعة وذاتية الجرائم الالكترونية (المطلب الأول). ولا يسري هذا الأمر على التشريعات الوطنية فحسب، بل يمتد أيضا إلى القانون الجنائي الدولي ليصيبه بالهوان و بعدم الفعالية، خاصة ما تعلق منه بالتعاون الدولي بكافة صوره في مجال مكافحة الجرائم الالكترونية (المطلب الثاني).

المطلب الأول

قصور التشريعات الجنائية القائمة

المؤكد أن القوانين الجنائية لا تتطور دائما بالوتيرة نفسها التي تتطور بها التكنولوجيات الحديثة أو مهارات الذهن البشري في تسخير المبتكرات التكنولوجية للاستخدام السيئ، وعليه فان القوانين القائمة لا تكفي من حيث المبدأ لمجابهة هذا الشكل الجديد من الإجرام، بشتى أنواعه و أساليبه، لأنها وضعت لتطبق وفقا لمعايير ومعطيات معينة (الفرع الأول). ولا يقتصر هذا الأمر على القوانين العقابية الموضوعية فحسب، بل يشمل كذلك التشريعات

الإجرائية، لأن معظم إجراءات التحقيق والمتابعة الجزائية التي تتضمنها التشريعات التقليدية لا تتلاءم لا مع طبيعة هذه الجرائم ولا مع تقنيات و وسائل ارتكابها (الفرع الثاني). وإذا اضطرت سلطات التحقيق إلى تطبيق هذه النصوص التقليدية على الجرائم الالكترونية لتفادي إفلات الجناة من العقاب، فإن ذلك قد ينعكس سلبا على حجية أدلة الإثبات المتحصل عليها، مما قد يودي إلى استبعادها من طرف القاضي الجزائي لضعف قيمتها الثبوتية (الفرع الثالث).

الفرع الأول: عدم كفاية النصوص العقابية التقليدية

على الرغم من أن إرهاصات الثورة التكنولوجية في مجال الاتصال عن بعد قد أفرزت العديد من الجرائم المستحدثة ذات الطبيعة الخاصة،إلا أن مكافحة هذه الجرائم مازال يتم في إطار النصوص العقابية المألوفة التي وضعت لكي تطبق على الجرائم التقليدية[477]، وهذا الأمر ترتب عليه الكثير من المشكلات بالنسبة لملاحقة هذه الجرائم الالكترونية ذات الطابع المعنوي و التي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الانترنت، فيتعذر تبعا لذلك اتخاذ إجراءات جمع الدليل بالنسبة لها، أو قد تلحق عدم المشروعية بهذه الإجراءات.

إن عدم تطور القوانين بنفس السرعة والوتيرة التي تتطور بها وسائل الإعلام والتكنولوجيا و مهارات الذهن البشري في تسخير مبتكرات التكنولوجية، جعل القوانين التقليدية تقف عاجزة عن مواجهة العديد من الجرائم الجديد التي ارتبطت بظهور و انتشار الوسائل والأجهزة الالكترونية، خاصة إذا علمنا أن القوانين الوضعية السائدة في اغلب دول العالم يحكمها مبدأ الشرعية الجزائية الذي ينص على انه" **لا جريمة و لا عقوبة إلا بالنص**"، وأن

---

[477]– **سرحان حسن ألمعيني**، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، مجلد 20، عدد 79، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011، ص 19.

نطاق التجريم بالقياس في ظل هذا المبدأ يكون ضيقا جدا[478].

فثمة أفعالا جديدة كثيرة خاصة في الدول المتخلفة، مرتبطة باستعمال الحاسب الآلي غير مجرّمة بمنظور القوانين العقابية التقليدية، ولا تمتد إليها لمكافحتها رغم تهديدها للمصالح العامة و تشكل خطورة بالغة على النظام العام، ومن الأمثلة على هذه الأفعال الاعتداء على حرمة الحياة الخاصة المعلوماتية، هذا النوع من الاعتداء لا يعاقب عليه قانون العقوبات إلا إذا كان مرتبطا بمكان خاص، أما التسلل والنفاذ إلى أسرار الفرد وخصوصياته الشخصية أو المهنية من خلال الوصول إلى المعلومات المخزنة لديه في أنظمته المعلوماتية داخل الحاسب، فان هذا التصرف لا يخضع للتجريم وفقا للقواعد العامة[479].

كما أن الدخول في نظام حاسب مملوك للغير وسرقة المعلومات منه ، لا يعد جريمة بمفهوم القوانين التقليدية لان السرقة حسب هذه الأخيرة لا ترد إلا على المال المنقول، وهذه الصفة لم تثبت بعد للمعلومات كونها تعتبر سوى أفكار معنوية بحتة ، زيادة على ذلك فان فعل السرقة أو الاختلاس بالمفهوم الكلاسيكي يعني تجريد الغير من ماله في حين أن اختلاس المعلومات يتمثل في أخذ نسخة منها مع الإبقاء بأصلها عند صاحبها، لذا فإنها لا يحميها التجريم المقرر في جرائم الأموال[480]. والشيء نفسه قيل بعدم وقوع جريمة الإتلاف على الكيانات غير المادية للوسائل الالكترونية كالبيانات و البرامج [481]، وعدم وقوع جريمة

---

[478]– **سرحان حسن ألمعيني** ، مرجع سابق، ص21.

[479]– **غنام محمد غمام**" عدم ملائمة القواعد التقليدية في القانون العقوبات لمكافحة جرائم الكمبيوتر" بحث مقدم إلى مؤتمر القانون و الكمبيوتر والانترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة الممتدة من 01 إلى 03 ماي 2003، ص 625.

[480]– المرجع نفسه، ص646.

[481]– **بكرى يوسف بكرى**، مرجع سابق، ص22.

التزوير على المعلومات المبرمجة في الحاسب أو في أية دعامة مادية كالاسطوانات أو أقراص ممغنطة أو أشرطة لعدم انطباق وصف المحرر عليها[482].

ففي مثل هذه الحالات، تثور العديد من الصعوبات أمام تطبيق نصوص التجريم التقليدية، مردها أن هذه النصوص وضعت أساسا لحماية الأشياء المادية في مواجهة صور الاعتداء المألوفة والتقليدية مما يتعذر معه أو يستحيل أن يقع تحت طائلة العقاب الاعتداء على عناصر ومكونات الأنظمة المعلوماتية المتمثلة في صور غير مادية، فضلا عن أن تطبيق مثل هذه النصوص قد يتعارض أحيانا مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها البيانات أو المعلومات بشتى أنواعها المرئية أو المصورة أو المكتوبة[483].

لذلك، دفع عدم مواكبة القوانين العقابية للتطورات السريعة والمستمرة المصاحبة للجرائم الالكترونية، معظم دول العالم، لا سيما التي لم تسن بعد قوانين خاصة لتجريم مختلف أنماط الجرائم المستحدثة إلى اتخاذ سبيل التفسير الموسع للنصوص الجنائية التقليدية ليطال تطبيقها هذه الجرائم التي أوجدتها ثورة الاتصالات عن بعد. وذلك بمنح سلطاتها القضائية حرية تفسير هذه النصوص بشكل أكثر مرونة يسمح من وضع هذه الجرائم تحت طائلة التجريم و المتابعة، تفاديا من إفلات الجنات من قبضة العدالة.

ولكن تطبيق النصوص التقليدية بمفهومها الموسع لتشمل الجرائم الالكترونية قد يشكل خرقا صارخا لمبدأ جوهري من مبادئ القانون الجنائي وهو مبدأ التفسير الضيق للنصوص العقابية وحضر القياس، ومن شأنه أن يمس بمبدأ الشرعية الجزائية إذا ترك الأمر بيد القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله[484]. الأمر الذي

---

[482]– **JRANDIDIER Wilfrid** « interprétation de la loi pénale » Juris- Class Pénal ,art 111- 2 a 111- 5, N 38.

[483]– **بكرى يوسف بكرى**، مرجع سابق، ص 23.

[484]–**عبد الفتاح بيومي حجازي**، مرجع سابق، ص 115.

قد يؤدي إلى ارتكاب خروقات واعتداءات على الحريات والحقوق الفردية بدون مبرر أو أساس قانوني مشروع.

ونظرا للعجز الكبير الذي أثبتته القوانين العقابية التقليدية في مواجهة الجرائم الالكترونية، حاولت بعض الدول خاصة المتقدمة منها إلى استدراك الوضع بسن تشريعات جديدة تتجاوب مع الطبيعة الخاصة لهذه الجرائم الحديثة، فمنها التي اختارت تعديل قوانينها العقابية وإضافة نصوص جديدة إليها تتجاوب مع الظاهرة الإجرامية الحديثة لسدّ الفراغ التشريعي القائم في هذا المجال، ومنها التي فضلت استحداث نصوص جديدة خاصة بهذا النوع المستجد من الإجرام. غير أن الملاحظ في هذه القوانين، أنها لا تشمل كافة الأفعال غير المشروعة الناتجة عن استعمال التكنولوجيا الحديثة، بسبب عدم تطورها بالوتيرة نفسها التي تتطور بها الجرائم الالكترونية، كما أن معظم دول العالم خاصة المتخلفة منها لم تسن بعد قوانين تجرم مثل هذه الأفعال غير المشروعة، واكتفت فقط بتطبيق القواعد القانونية القائمة رغم ثبوت قصورها. ولعل السبب في ذلك هو افتقارها إلى الخبرة والتخصص والمعرفة الكافية للبيئة الالكترونية العالية التقنية والمعقدة.

الفرع الثاني:عدم ملائمة إجراءات التحقيق المألوفة مع الجرائم الإلكترونية

لم يتوقف الأمر عند قصور النصوص العقابية في مواجهة الجرائم الالكترونية، بل تعدّ إلى القوانين الإجرائية، إذ أن معظم إجراءات التحقيق والمتابعة الجزائية التي تتضمنها التشريعات التقليدية لا تتلاءم مع طبيعة هذه الجرائم وأحيانا تتعارض حتى مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها المعلومات أو البيانات بشتى أنواعها، وهذا الأمر يشكل عقبة كبيرة أمام رجال الضبطية القضائية من عدة نواحي نلخصها كمايلي:

أولا–صعوبة إخضاع المكونات المنطقية للحاسوب الآلي للتفتيش و الضبط

إذا كان الهدف الأساسي من التفتيش كوسيلة إجرائية هو الحصول على دليل مادي يثبت الجريمة وينسبها إلى مرتكبيها، فانه بذلك يتنافى مع الطبيعة غير المادية للمكونات المنطقية للحاسب الآلي، كونها مجرد برامج و بيانات الكترونية ليس لها أي مظهر محسوس في العالم الخارجي. ويرجع هذا التناقض أساسا إلى غياب مفهوم واضح ومتفق عليه لمصطلح (شيء) الذي يفترض أن يكون محلاً للتفتيش والضبط، فإذا كان التفتيش كما هو متعارف عليه ينصب على" شيء مادي " فقد أثير تساؤل حول مدى انطباق لفظ (الشيء) على الكيانات المعنوية أو الوسط الافتراضي للحاسوب ؟ أو بالأحرى على مدى جواز تفتيش الوسط الافتراضي والمنطقي للحاسوب وضبط ما به من محتويات؟ وهي المسألة التي انقسم رأي الفقه الجنائي فيها إلى ثلاثة اتجاهاه مختلفة[485].

فذهب الاتجاه الأول إلى جواز تفتيش وضبط المكونات المعنوية للحاسوب بمختلف إشكالها، وحجته في ذلك هي أن القوانين الإجرائية عندما تنص على جواز تفتيش وضبط "**أي شيء**" يتعلق بالجريمة أو يساعد على كشف حقيقة وقوعها، فـــان ذلك يجب أن يفسـر بالمعني الواسع ليشمل كل من المكونات المادية والمعنوية للحاسوب معا[486].

وقد أخذ القضاء اليوناني بهذا التوجه الفقهي، وفسّر عبارة " **أي شيء**" الواردة في المادة (251) من القانون الإجراءات الجزائية التي تنص على انه " يجوز لسلطات التحقيق القيام بأي شيء يكون ضروريا لجمع الدليل". بأنها تشمل البحث وضبط البيانات والمعطيات المعالجة إلكترونيا والمخزّنة داخل الأوعية الالكترونية الرقمية أو حاملات البيانات المادية أو في الذاكرة الداخلية للحواسيب، وهو ما ساعد على رفع اللبس عند سلطـات البحث والتحقيق

---

[485]– **نبيلة هبة هروال**، مرجع سابق، ص 225.

[486]– **خالد ممدوح إبراهيم**، مرجع سابق، ص 197.

بخصوص مدى سريان نص المادة(251) أعلاه على الكيانات المنطقية الحاسب الآلي[487].

وهو الموقف ذاته الذي اتخذه الفقه و القضاء بدولة كندا، حينما فسّرا المادة(487) من القانون الجنائي الكندي التي تعطي للسلطة المختصة الحق في إصدار الإذن بتفتيش وضبط " **أي شيء**" تتوفر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأن جريمة قد وقعت أو يشتبه في وقوعها، أو أن هناك نية لاستخدامه في ارتكاب جريمة، أو انه سيتيح دليلا على وقوع الجريمة. بأن عبارة " **أي شيء**" تضم المكونات المادية و المعنوية للحاسوب الآلي على حد سواء ، ولا يوجد أي مانع في أن يرد التفتيش و الضبط على مثل هده المكونات اللامادية[488].

وبالمقابل ذهب اتجاه فقهي آخر وهو الغالب، إلى عدم إمكانية إخضاع المكونات المعنوية للحاسوب من برامج و بيانات لعملية التفتيش و الضبط، لأن الغرض الأساسي من التفتيش هو ضبط الأدلة المادية، ولما كانت هذه المكونات الالكترونية المنطقية تفتقر إلى مظهر مادي ملموس كالأشياء المادية (كالمركبة مثلا أو المسدس أو السكين) فلا يمكن تفتيشها ولا ضبطها، إلا إذا تم تعديل غاية التفتيش تلك بجعلها تشمل ضبط الأدلة المادية وغير المادية على حد سواء[489].

وقد تأثّر بهذا الاتجاه المشرع الألماني، إذ نص في المادة(94) من قانون الإجراءات الجنائية صراحة على أن التفتيش والضبط يرد فقط على الأشياء المادية المحسوسة المتعلقة بالجريمة دون غيرها. ومن هنا، يرى الفقه الألماني أن البيانات و المعلومات الالكترونية لا

---

[487]–**أحمد بن زايد جوهر الحسن المهندي**" تفتيش الحاسب الآلي و ضمانات المتهم" رسالة لنيل شهادة الماجستير في القانون، كلية الحقوق، جامعة القاهرة، 2009، ص145.

[488]– **على محمود على محمود** "الأدلة المحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي" بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعماليات الالكترونية، الإمارات العربية المتحدة، 2003، ص 14.

[489]– **هلالي عبد اللاه احمد**، مرجع سابق، ص89.

يمكن ضبطها إلا بعد تفريغها في كيان مادي محسوس مثل طبع هذه البيانات على الورق، أو تخزينها في دعامة مادية مثل الأقراص المغناطيسية، أو تصويرها على الشاشة أو نقلها على حافظة بيانات، فالمهم هو نقل هذه البيانات إلى وسط مادي محسوس لكي يتم إخضاعها للتفتيش و الضبط .

ويرى الفقه في معظم دول أمريكا الجنونية كالبرازيل و التشيلي بدوره، أن عملية الضبط لا تنصب إلا على الدعامة المادية التي تحتوي المعلومات و البيانات كالأشرطة والأقراص المغناطيسية و غيرها من وسائل التخزين الأخرى[490]. وهو الموقف ذاته الذي تبناه كل من الفقه الياباني و الروماني حين اعتبر البيانات والبرامج والسجلات المغناطيسية مجرد مكونات غير مرئية في حدّ ذاتها، كونها نبضات أو ذبذبات الكترونية أو موجات كهرومغناطيسية غير محسوسة ماديا، بالتالي لا يمكن ضبطها إلا إذا كانت قابلة للتحويل إلى صورة مرئية مقروءة عن طريق مخرجات الطباعة، وإفراغها في قالب مادي محسوس[491].

وعكس ما ذهب إليه الاتجاهين الفقهيين الأول و الثاني، يرى اتجاه فقهي ثالث بأنه لا يجب الخلط عند تحديد مدلول (الشيء) بالنسبة لمكونات الحاسب بين الحق الذهني للشخص على البرامج والبيانات والكيانات المنطقية الأخرى، وبين طبيعة هذه البرامج والكيانات، إنما ينبغي الرجوع في ذلك إلى تحديد مدلول كلمة (المادة) في العلوم الطبيعية. فلما كانت (المادة) تعرف بأنها " **كل ما يشغل حيزا ماديا في فراغ معين**" ، وكان الحيز مما يجوز قياسه و التحكم فيه، فان البرامج و الكيانات المنطقية باعتبارها تشغل حيزا ماديا

---

[490]– **GEORGO Antoniu** « les crimes informatique et d'autres crimes dans le domaine de la technologie informatique en Roumanie » Revue internationale de droit pénal, 1993, p 551 .

[491]– **رشاد خالد عمر**، المشاكل القانونية الفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، القاهرة، 2013، ص146

في ذاكرة الحاسب الآلي ويمكن قياس حيزها بوحدات قياس خاصة هي، البايت (bite) والكيلوبايت (kilobit) والميجابايت(Mégabit) والجيجابايت(Gigabit)، وتأخذ شكل نبضات الكترونية، تتوفر على خصائص المادة و تتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء من قبيل الأشياء المادية[492].

ويبدو في تقديرنا، أن الاتجاه الثاني هو الأكثر منطقي، لأن القواعد التقليدية التي تحكم التفتيش والضبط إنما وُضِعت قبل ظهور الوسائل الالكترونية الحديثة بما فيها الحاسب وملحقاته، لذلك فمهما كانت المبررات التي ساقها معتنقو المساواة بين الكيان المادي والمنطقي، تبقي طبيعة البيانات المعالجة إلكترونيا بحاجة لإجراءات تحقيق خاصة بها، وهذا الأمر لا يتأتّى إلا بتعديل النصوص الإجرائية بما يوسع نطاق الأشياء التي تكون مشمولة بالتفتيش والضبط، وتضمينها من الأحكام بما يتلاءم ومتطلبات هذه التقنية الجديدة. فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا ينبغي إعمالها بحالتها تلك على المكونات المنطقية قياسا على الأشياء المادية كما فعلت بعض التشريعات المشار إليها أعلاه، لأن ذلك يتنافى مع مبدأ الشرعية الإجرائية وحضر القياس.

وباستقراء موقف غالبية التشريعات الحديثة، نجدها حذت حذو الاتجاه الفقهي الأخير لتجاوز التباين القائم حول مدى خضوع المكونات المعنوية للحاسوب الآلي للتفتيش والضبط، ورفع الإبهام عن عبارة " الشيء " التي كانت محور الجدل. إذ لجأت بعض الدول إلى تعديل تشريعاتها الجزائية التقليدية والنص صراحة على أن تفتيش الحاسب الآلي يشمل البرامج و البيانات المعالجة الكترونيا، وذلك استجابة لتطلعات الاتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001 التي نصت على ضرورة اتخاذ كافة الدول الأطراف لكل ما يلزم من تدابر تشريعية وغيرها لتمكين سلطاتها من تفتيش وضبط المكونات الالكترونية[493].

---

[492]– **رشاد خالد عمر**، مرجع سابق، ص147.

[493]– انظر المادة(19) من الاتفاقية الأوروبية حول الجرائم الالكترونية المبرمة ببودبست عام 2001، مرجع سابق.

ونذكر من بين هذه الدول، فرنسا التي قامت بتعديل المادة(94) من قانون الإجراءات الجنائية وأضافت إليها عبارة "**البيانات الالكترونية**"[494]، و الولايات المتحدة الأمريكية بتعديلها القاعدة(34) من القواعد الخاصة بالإجراءات الجنائية الاتحادي لعام 1980، والنص على جواز تفتيش أجهزة الحاسب و الكشف عن الوسائط الالكترونية بما في ذلك البريد الالكتروني والبريد الصوتي والبريد المنقول. لتصبح الغاية الجديدة من التفتيش بعد التعديل هي، البحث وضبط الأدلة المادية أو أي مادة معالجة آليا بواسطة الحاسب. استمرار في هذا المسار تدخل المشرع الإسرائيلي وعدّل قانون الحاسب الآلي المندرج في زمرة أسبابه عدم توائم التفتيش والضبط في قانون الإجراءات الجزائية الإسرائيلي لعام 1969، بحيث أعاد صياغة التحديد الوارد بقانون الإجراءات لعبارة " الشيء" الذي يمكن أن يكون محلا للتفتيش و الضبط على نحو أدرج فيه، إلى جانب الأشياء المادية المعروفة، أية " **مادة معالجة بالحاسب**" وهو ما يشمل مكونات الحاسب المنطقية[495].

الخلاصة أنه صحيح هناك بعض الدول التي تدخلت مؤخرا لحل هذا المشكل، عن طريق إحداث تعديلات في تشريعاتها الإجرائية التقليدية بما يضمن سريان إجراء التفتيش والضبط على المكونات المادية والمنطقية للحاسوب على حد سواء، إلا أن هذا المشكل مازال قائما في معظم دول العالم خاصة المتخلفة منها، بسبب احتفاظها بالقوانين الإجرائية التقليدية لمواجهة الجرائم الالكترونية رغم عدم ملائمتها مع طبيعة هذه الأخيرة. وهذا الأمر من شأنه أن يشكل عقبة كبيرة أمام هيئات التحقيق بحيث يجدون أنفسهم في موقف حرج مذبذبين بين جواز وعدم جواز امتداد التفتيش و الضبط ليضمّ المكونات المعنوية. مما قد يدفعهم في نهاية المطاف إلى وقف التحقيق ومن ثمة إفلات المجرم الالكتروني.

---

[494] –Art (94) du C.P.P.F stipule que « **les perquisitions sont effectuées dans tout les lieux ou peuvent se trouver des objets ou des données informatiques dont tous découverte serait utile a la manifestation de vérité** ».

[495]– **LEDERMAN Eli And RON Shapira** « computer crimes and other crimes against information technology in Israël » R.I.D.P,1er et 2e trimestres, 1992, P 420 .

ثانيا: صعوبة معاينة الجرائم الإلكترونية

لا تتمتع المعاينة في مجال كشف غموض و ملابسات جرائم الالكترونية و إثباتها بالدرجة نفسها من الأهمية التي تتمتع بها في ومجال الجرائم التقليدية، وذلك راجع إلى عدة أسباب أولها أن هذه الأخيرة لها مسرح تجري عليها الوقائع و الأحداث، وتخلف أثارا مادية تقوم عليها الأدلة كالبصمات أو قطرات دم. وهذا المسرح يعطي المجال أمام سلطات التحقيق والاستدلال الجنائي في كشف الجريمة عن طريق المعاينة الميدانية و التحفظ عن الآثار المادية التي خلفتها هذه الجريمة. في حين أن فكرة معاينة مسرح الجريمة الالكترونية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة، لأن معظم الجرائم التي تقع على نظم المعلومات وشبكات الانترنت قلما تخلف ورائها أثارا مادية [496].

كما أنه من الممكن أن يتردد عددا كبيرا من الأشخاص على مكان أو مسرح الجريمة خلال الفترة الزمنية الممتدة من لحظة وقوع الجريمة حتى اكتشافها والتي تكون عادة طويلة نسبيا، مما يفسح المجال لحدوث تغيير أو تلف أو عبث بالآثار المادية أو زوال بعضها، وهو ما يلقي ظلالا من الشك على الدليل المتحصل من المعاينة. ناهيك عن إمكانية تلاعب الجاني في البيانات أو المعطيات محل المعاينة عن بعد أو محوها عقب الولوج إليها عبر الانترنت بواسطة جهاز أخرى مرتبط بها [497].

أضف إلى ذالك، فان عدم دراية وتحكم المحقق بالجوانب الفنية والتقنية للاستخدام شبكة الانترنت، ونقص كفاءتهم العلمية في مجال الحاسبات واسترجاع المعلومات، وأساليب التعامل مع نوعية الآثار والأدلة التي يمكن أن يحويها مسرح الجرائم الالكترونية، قد يؤثر سلبا على جدوى المعاينة في هذه الجرائم، الأمر الذي يعطي الفرصة للمحكمة بالتشكيك في صحة ومشروعية الدليل الموجه ضد المتهم، وبالتالي استبعاده.

---

[496]– **هشام محمد فريد رسم**، مرجع سابق، ص 59.

[497]– **صغير يوسف**، مرجع سابق، ص 131.

الفرع الثالث: ضعف الحجية الثبوتية للأدلة الإلكترونية

إذا كان المبدأ هو حرية القاضي الجنائي في تكوين اقتناعه من أي دليل يطرح أمامه، فان هذه الحرية ليست مطلقة حينما يتعلق الأمر بالأدلة المستمدة من الوسائل الالكترونية، نظرا للصعوبات الكثيرة التي تثيريها عملية تحصيل وجمع هذه الأدلة والتي تنعكس سلبا على قوتها الثبوتية أمام القضاء الجنائي.

ولقد أوجس كل من الفقه و القضاء خيفة من الأدلة المحصلة من الوسائل الالكترونية بسبب طبيعتها الفنية التي تُمكِّن من العبث بمضمونها بالمحو أو التعديل أو التزييف بكل سهولة و في فترة وجيزة، على نحو يحرِّف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث. فضلاً عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة عادة ما تكون عالية في مثل هذا النوع من الأدلة، مما يثير الشك في مصداقيتها كأدلة للإثبات الجنائي[498].

وتثار مشكلة أخرى بالنسبة للإثبات بالأدلة الالكترونية في كون المعلومات والبيانات التي تسجل على الوسائل الإلكترونية لا يمكن قراءتها بالعين المجرة، وهي بذلك تعتبر أدلة غير مرئية ولا يمكن استخراجها إلا عن طريق أجهزة تدوير خاصة بمساعدة الحاسب تسمى بأجهزة التدوير لوسائط تخزين المعلومات(baking storage devices)، كما أن هذه الوسائط كالأشرطة والأقراص الممغنطة والدعامات المادية الأخرى التي تستعمل لتخزين المعلومات والبيانات لا يمكن قراءتها أيضا إلا باستعمال الحاسب، مما يتعذر على القاضي مناقشة هذه الأدلة أمام المحكمة وأمام الخصوم كما يقتضيه مبدأ المناقشة الشفوية والمرافعة[499]. علما أن مناقشة الدليل في جلسة المحاكمة من الشروط الجوهرية لقبوله والأخذ به.

---

[498]– **عمرو حسين عباس**، مرجع سابق، ص 08.

[499]–**سعيد عبد اللطيف حسين**، مرجع سابق، ص.ص 238– 239.

ولقد أثيرت مشكلة قبول الأدلة المتحصلة من الوسائل الالكترونية بشدة في ظل قواعد الإثبات الجنائي الانجلوسكسوني القائمة على نظام الإثبات المقيد، أين يتولى المشرع تحديد مسبقا وبصفة حصرية الأدلة التي يجوز للقاضي الاستعانة بها في الإثبات، وضوابط كل دليل وقيمته الاقناعية. في حين يختص القاضي فقط بفحص الدليل للتأكد من توافر الشروط التي حددها القانون من عدمها. إذ لا سبيل للاستناد في هذا النظام على دليل أو الاعتراف له بأية حجية إن لم ينص عليه القانون صراحة ضمن قائمة أدلة الإثبات. لذلك فإن عدم إدراج معظم تشريعات الدول التي تبنت نظام الإثبات المقيد الدليل الالكتروني ضمن الأدلة المقبولة في الإثبات، يؤدي إلى هدر قيمته الاثباتية أمام القضاء الجزائي مهما توافرت فيه شروط اليقين، وبالتالي لا يجوز للقاضي أن يستند إليه لتكوين عقيدته[500].

الجدير بالذكر، أن مسألة القيمة الثبوتية للأدلة الالكترونية متوقفة بالدرجة الأولى على مصداقية الوسائل و الآليات الالكترونية المستعملة لتحصيلها، والتي لا يزال القاضي الجزائي يتردد في قبولها بسبب اختلاف تلك الوسائل عما نظمه القانون من وسائل تقليدية في الإثبات. لذا لا تزال المحاكم في كثير من الدول تتردد في قبول المستندات المطبوعة والمصورة لمخرجات الوسائل الالكترونية كدليل إثبات، بدافع أن عملية التصوير والطباعة تغير هذه المخرجات من طبيعتها الأصلية كإشارات وذبذبات الكترونية ونبضات ممغنطة إلى بيانات مدونة على الورق قد تكون غير مطابقة للأصل ولا تعبر عن كامل حقيقته، وهو ما يبعث في نفس القاضي الريبة والشكوك بخصوص مصداقيتها.

كما أنه قد يحدث ألا تؤدي الأجهزة الالكترونية المستعملة للبحث وتحصيل الدليل وظيفتها بشكل سليم أو تتعرض أثناء تشغيلها لعطل معين فتفقدها القدرة على تقديم نتائج

---

[500]–**محمد زلايجي** "حجية دليل الحاسوب الآلي في النطاق الجنائي" مجلة مخبر القانون الخاص الأساسي، العدد 07، كلية الحقوق، جامعة تلمسان، 2010، ص.ص 66-67.

صحيحة مائة بالمائة بالنسبة للدليل[501]. لذلك حتى المحاكم في بعض الدول القليلة التي تعترف بحجية المخرجات الالكترونية في الإثبات الجنائي، تشترط لقبول الدليل الالكتروني أن يعمل نظام الجهاز الالكتروني المستخرج بواسطته الدليل بصفة سليمة وأن يستخدم بشكل صحيح [502]، وتشترط كذلك توفر في السند الالكتروني الشروط الأخرى المتطلب توفرها في المحررات التقليدية كالتوقيع و التبصيم، بل أن بعضها تطلب للاعتداد بها أن تعزز بشهادة الشهود[503]. والحق أن اشتراط وجود التوقيع على المستندات الالكترونية حتى تكون له حجية عند القاضي الجزائي من شانه التضييق من نطاق قبول القضاء للدليل الالكتروني و يفتح مجال واسع أمام هذا الأخير في استبعاد الأدلة الالكترونية، كما أن اشتراط تعزيز هذه الأدلة بشهادة أحد الشهود حتى تكون مقبولة لدليل قاطع على ضعف قيمة المخرجات الالكترونية في الإثبات إذا لم يتوفر معها دليل أخر[504].

---

[501]– **CASILE Jean-François** « plaidoyer en faveur d'aménagements de la preuve de l'infraction informatique » op.cit., pp 77-78.

[502]–نصت المادة (69) من القانون الانجليزي للإثبات الجنائي الصادر في سنة 1984 على أن " المخرج **الناتج من الوسائل الالكترونية لا يقبل كدليل إذا تبين وجود سبب معقول يدعو إلى الاعتقاد بان هذا المخرج الالكتروني غير دقيقا وأن بياناته غير سليمة ، ويجب كذلك أن يكون الحاسب الناتج منه المخرج الالكتروني يعمل بكفاءة و بصورة سليمة**" نقلا عن :**هلالي عبد ألاله احمد** " حجية المخرجات الكمبيوترية في المواد الجنائية" دار النهضة العربية، القاهرة، 1998، ص 53.

[503]– ورد هذا الشرط في المادة(195) من قانون الإجراءات الجزائية الايطالي، و في نص المادة (1/129) من قانون الإجراءات الجزائية البرتغالي. راجع نص المادتين في :

- **VERGUCHT Pascal**, op.cit., p 432

[504] - **ROBILLARD Yves** " la preuve des communications a l'ère économique" article disponible sur ; www.Avocat.qc.ca/affaires/iitechno.htm.

المطلب الثاني

عدم فعالية التعاون الدولي في مجال مكافحة الجرائم الإلكترونية

يعتبر التعاون الدولي بمختلف صوره في مجال مكافحة الجرائم الالكترونية مطلبا أساسيا تسعى إلى تحقيقه أغلب الدول، إلا أنه في الوقت نفسه من بين أصعب المواضيع المطروحة في الوقت الراهن، بالنظر إلى الصعوبات المختلفة والمعوقات الكثيرة التي تقف دون تحقيقه.

ولعل من بين هذه الصعوبات الاختلافات الموجودة في التشريعات العقابية بين الدول سواء ما تعلق بالجوانب الموضوعية منها كغياب اتفاق مشترك حول نماذج النشاط الإجرامي المتعلق بالجرائم الالكترونية ومعايير تصنيف هذه الجرائم ، أو ما تعلق بالجوانب الإجرائية كتباين القوانين الإجرائية الخاصة بمكافحة الجرائم الالكترونية من دولة إلى أخرى (الفرع الأول)

أضف إلى ذلك، الصعوبات الكثيرة التي تثيرها المساعدة القضائية الدولية، و التي تعود تارة إلى العدد المحدود من المعاهدات و الاتفاقيات المتاحة للدول بهذا الشأن ، وتارة أخر إلى تباطؤ إجراءات المساعدة القضائية بالمقارنة للطابع السريع للجرائم الالكترونية (الفرع الثاني).

الفرع الأول: تباين التشريعات العقابية للدول

يعتبر التباين والاختلاف الموجود بين التشريعات العقابية الوطنية للدول في معالجتها للجريمة الالكترونية مشكلة حقيقية و حجر عثرة أمام سلطات إنفاذ القانون، ويظهر هذا الاختلاف أساسا في العناصر التالية :

-أولا-غياب نموذج موحد للنشاط الإجرامي

لو تأملنا جيد في الأنظمة القانونية القائمة في كثير من الدول يتبين لنا عدم وجود اتفاق عام مشترك بينها حول نماذج النشاط الإجرامي المتعلق بالجرائم الالكترونية و معايير تصنيف هذه الجرائم ، بحيث ما يكون مباحا في أحد الأنظمة قد يكون مجرما و غير مباحا في نظام أخر، والنشاط الذي يشكل جنحة يعاقب عليها بالحبس في تشريع معين قد يشكل مخالفة يعاقب عليها بغرامة في تشريع أخر. ولعل السبب في هذا التباين يعود إلى قصور التشريع ذاته في بلدان العالم وعدم مسايرته لسرعة التقدم التكنولوجي، ومن ثم الجريمة الالكترونية، فلنا أن نتصور مثلا انه حتى الآن لم يصدر قانون في دولة عربية خاص بالجوانب الموضوعية والإجرائية للجريمة الالكترونية، بل لازال الخلاف دائر حول ما إذا كان من الأفضل تعديل التشريعات العقابية القائمة كي تستوعب نماذج الجريمة الالكترونية، أم إدراج هذه الأخيرة في قوانين فرعية متخصصة كقانون حماية الملكية الفكرية ، أم يكون من الملائم استحداث تشريعات جديدة خاصة بالجرائم الالكترونية [505].

وعليه فان عدم توفر تعريف موحد للجريمة الالكترونية يضفي عادة إلى إحداث ثغرات في منظومة القانون الدولي في مجال مكافحة تلك الجرائم و إضعاف فعاليته، وإبقاء أفعالا إجرامية خطيرة دون تجريم ولا عقاب، مما يسهل إفلات الجناة من المسؤولية الجزائية لان نص التجريم هو بمثابة الركن الشرعي لقيام الجريمة و انتفاءه يؤدي بالضرورة إلى انتفاء المسؤولية الجنائية[506] .

تثار مسالة عدم الاتفاق على نموذج موحد للنشاط الإجرامي بقوة، حينما يتعلق الأمر بتسليم المجرمين، الذي هو إجراء دولي تتخلى الدولة بموجبه عن شخص متواجد عندها

---

[505]–**عبد الفتاح بيومي حجازي**، مرجع سابق، ص 103

[506] -**UNODC** « Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face » Commission pour la prévention du crime et la justice pénale EG.4, 2013 p 06 .

لسلطات دولة أخرى تطالب بتسليمه بغرض محاكمته عن جريمة ارتكبها أو لتنفيذ حكم صادر ضده. إذ يخضع التسليم كما هو معلوم لشرط جوهري يتمثل في التجريم المزدوج، بمعني أن يكون الفعل المطلوب التسليم من أجله مجرّم في قانون الدولة المطلوب منها التسليم و الدولة الطالبة للتسليم، أما إذا كان هذا الفعل غير مجرم في نظر قانون إحدى الدولتين فانه لا يجوز المطالبة بتسليم الفاعل قصد محاكمته او معاقبته على سلوك مباح وفقا لقانون هذه الدولة[507].

ولا يتوقف تسليم المجرمين على توفر شرط التجريم المزدوج فقط، بل لا بد أن تكون الجرائم المراد التسليم من أجلها تحمل وصف قانوني نفسه و تشترك في الحد الأدنى من العقوبة بمنظور قانون كل من الدولة طالبة التسليم و الدولة المطلوب منها التسليم، فبالرجوع الى المادة الثانية من الاتفاقية الأوروبية الخاصة بتسليم المجرمين المبرمة في 13 ديسمبر 1957 فإنها تشترط بالإضافة إلى شرط التجريم المزدوج أن تكون العقوبة المقررة للجريمة المطلوب التسليم من أجلها تساوي على الأقل عامين حبس في قانون الدولتين المعنيتين بالتسليم[508]. وهذا الشرط غلبا ما يتحقق بسبب الاختلاف الشاسع بين تشريعات دول العالم فيما يخص الوصف القانوني للجرائم الالكترونية والعقوبة المقررة للجريمة الالكترونية الواحدة، فما يشكل جنحة في قانون دولة ما يمكن أن يشكل مخالفة في قانون دولة أخرى بالتالي لا يتم التسليم.

-ثانيا- تباين النظم القانونية الإجرائية

يشكل اختلاف القوانين الإجرائية من دولة إلى أخرى عقبة أخرى أمام المواجهة الدولية للجرائم الالكترونية، لاسيما أن هذه الجرائم تتميز بالطابع الدولي و العابر للحدود، بحيث نجد إجراءات التحقيق والاستدلال والمحاكمة التي تثبت فائدتها وفعاليتها في دولة ما قد

---

[507]- **FERAL-SCHUHL - Christiane** « cyber droit- le droit a l'épreuve de l'internet » 06éme édition, Dalloz, 2011-2012, pp 1016-1017

[508] - **AL CHAER Nidal** « la criminalité informatique devant la justice pénale » op.cit.pp 264-265

تكون عديمة الجدوى والفائدة في دولة أخرى، كما هو الحال بالنسبة للمراقبة الالكترونية واعتراض المراسلات، التصنت وتسجيل المكالمات والمحادثات الهاتفية وغيرها من العمليات المستترة[509]. فإذا ما اعتبر إجراء ما من إجراءات جمع الأدلة أو التحقيق أنه مشروع ومقبول بمنظور قانون دولة معينة، فانه قد يكون ذات الإجراء غير مشروعة في قانون دولة أخرى. وبالتالي فان الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الثانية على استخدام ما تعتبره هي أنه أداة فعالة لإثبات الجريمة، بالإضافة إلى أن السلطات القضائية لدى الثانية قد لا تسمح باستخدام أي دليل إثبات تم الحصول عليه بطرق ترى هذه الدولة أنها طرق غير مشروعة[510].

ولعل أحسن مثال على ذلك، التباين التشريعي القائم بين القوانين اللاتينية و الانجلوسكسونية حول مدى حجية الدليل الرقمي المستمد من الحاسوب الآلي في الإثبات الجنائي، ففي القوانين ذات الصياغة اللاتينية القائمة على نظام الإثبات الجنائي الحر، ومنها القانون الفرنسي والجزائري والسوري واللبناني، فإن القاضي الجزائي يتمتع بحرية مطلقة في تقدير الأدلة المطروحة أمامه والأخذ منها ما يراه مناسبا لتكوين قناعته ولو كان هذا الدليل من الأدلة الرقمية أو الالكترونية[511]، في حين أن النظم الإنجلو سكسونية مثل بريطانيا و الولايات المتحدة الأمريكية لا تعترف للدليل الرقمي بحجية الإثبات الجنائي إلا إذا أخذ احد الأشكال التي حددها المشرع مسبقا في وسائل الإثبات وقدر قيمتها الإقناعية، وتم الحصول عليه وفق شروط محددة سلفا[512].

---

[509]– **عبد الفتاح بيومي حجازي**، مرجع سابق، ص 104

[510] – **AL CHAER Nidal**, « la criminalité informatique devant la justice pénale » op.cit. pp 259-260.

[511]– **محمد زلايجي** ، مرجع سابق، ص.ص 62-66.

[512]- **VERGUCHT Pascal**, op.cit. pp 433-434.

ويضاف إلى ما سبق ذكره، اختلاف دور سلطات انفاد القانون من دولة إلى أخرى، إذ نجد سلطات الضبطية القضائية في بعض الدول الأوروبية مثل فرنسا وسويسرا تتمتع باستقلالية كبيرة وصلاحيات واسعة في مجال مكافحة الجرائم الالكترونية، في حين السلطات نفسها في دول أخرى مثل ألمانيا وهولندا وبلجيكا تخضع خضوعا تاما إلى النيابة وتمارس مهامها تحت الرقابة الشديدة لهذه الهيئة، وهذا الوضع من شانه أيضا أن يعرقل فعالية التعاون الدولي في مجال مكافحة الجرائم الالكترونية[513].

الفرع الثاني: صعوبات متعلقة بالمساعدات القضائية الدولية

تفرض الطبيعة العالمية للجرائم الالكترونية أحيانا على رجال الضبطية القضائية التابعة لدولة ما تمديد إجراءات التحقيق إلى خارج الإقليم الوطني قصد ضبط أدلة مخزنة في حاسب أو إحدى ملحقاته المتواجد في إقليم دولة أجنبية، ولكي تكون هذه الإجراءات مشروعة وقانونية لا بد أن تتم في إطار المساعدة القضائية عن طريق الإنابة القضائية الدولية، بحيث تعهد بموجبها للسلطات القضائية المطلوب منها اتخاذ إجراء أو عدة إجراءات التحقيق لمصلحة السلطة القضائية في الدولة الطالبة، مع مراعاة احترام حقوق و حريات الإنسان المعترف بها علميا، ومقابل ذلـك تتعهد الدولة الطالبة للمساعدة القضائية بالمعاملة بالمثل مع احترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة[514].

والمعروف أن طلب الإنابة القضائية الدولية يتم أصلا بالطرق الرسمية الدبلوماسية، فمثلا يرسل طلب الحصول على دليل إثبات من طرف النيابة العامة بعد توثيقه من المحكمة الوطنية المختصة في الدولة الطالبة، ثم يمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب، لتقوم هذه الأخيرة بدورها بإرساله إلى السلطات القضائية المختصة في

---

513 - **AL CHAER Nidal**, op.cit. pp 299-300.

514 –**راسل تينر**" أهمية التعاون الدولي في منع جرائم الانترنت" بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنظمة من طرف المملكة المغربية في الفترة الممتدة من 19–2008/06/20، ص 112.

الدولة المطلوب منها الإنابة القضائية. وما يعاب على هذه الطرق الدبلوماسية هو اتسامها بالبطء الشديد والتعقيد بالمقارنة مع طبيعة الجرائم الالكترونية وما تتميز به من السرعة الفائقة، مما ينعكس سلبا على عملية التحقيق في مثل هذه الجرائم[515].

ومن المشكلات الكبيرة كذلك التي تثيرها المساعدة القضائية الدولية المتبادلة، التباطؤ في فحص طلب المساعدة والرد عليه، إذ غالبا ما تكون الدولة متلقية الطلب متباطئة ومماطلة في فحص والرد على الطلب، سواء بسبب عدم تحديد الهيئة المختصة المؤهلة بالرد على طلبات المساعدة القضائية، أو تخوف هذه الهيئة من موضوع طلب المساعدة الذي يستوجب عليها فحصه و مراجعته بدقة، أو نتيجة الانشغالات الكثيرة للسلطات مكلفة بتنفيذ طلب المساعدة، أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب. فكم من طلب مساعدة قضائية لم يستجاب له إلا بعد فوات الأوان و كم من قضية شطبت لعدم تلبية طلب مساعدة بسيط في الوقت المناسب[516].

وما يزيد الأمور أكثر تعقيدا فيما يخص المساعدة القضائية الدولية، هو فتح غالبة الاتفاقات و المعاهدات الدولية الثنائية والجماعية المجال واسعا جدا لإمكانية رفض واستبعاد تنفيذ الإنابة القضائية الدولة في مجال الجرائم السياسية و الجرائم التي تمس بسادة الدولة و تلك التي تمس بمصالحها الأساسية، كما هو الحال بالنسبة للمادة (27 فقرة 4) من اتفاقية بودابست التي تنص على انه " بالإضافة إلى الشروط أو أسباب الرفض المنصوص عليها في الفقرة الرابعة من المادة (25) فانه يمكن رفض طلب المساعدة من قبل الطرف الموجه إليه إذا:

أ-كان موضوع طلب المساعدة ينصب على جريمة يعتبرها الطرف المطلوب منه جريمة سياسية أو جريمة تمرتبطة بجريمة سياسية.

---

[515]- **حسين بن سعيد بن سيف الغافري**" الجهود الدولية في مواجهة جرائم الانترنت" مرجع سابق، ص 54.

[516]- **صغير يوسف**، مرجع سابق، ص 139.

ب-إذا كان الطرف الموجه إليه طلب المساعدة يعتقد بأن تنفيذ هذا الطلب من شأنه المساس بسيادة دولته أو نظامها العام الداخلي، أو مصالحه الأساسية الأخرى"[517]. والجدير بالذكر هنا، هو أن مفهوم النظام العام يختلف من دولة إلى أخرى، كما أن المصالح الأساسية للدولة مثلما صرحت اللجنة الأوروبية للمشكلات الجنائية في تقرير لها أعدته في عام 1990 هي غير معروفة وغير محددة بمفهوم القانون الدولي[518]، مما يسمح للدول استغلال هذه الثغرات في القانون لرفض الإنابة القضائية كلما سنحت لها الفرصة.

ومن أجل التصدي لهذه المعضلة التي باتت تأثر سلبا على فعالية المواجهة الدولة للجرائم الالكترونية، أبرمت العديد من الاتفاقيات الدولية التي ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين سلطات التحقيق المعنية، في مقدمتها اتفاقية الأمم المتحدة لمكافحة الفساد، التي نصت على إمكانية تبادل المعلومات بين دول الأعضاء شفويا في حالة الاستعجال، و نصت كذلك المادة(53) من اتفاقية تشنجين الأوروبية لعام 1990 الخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف، على إمكانية الاتصال المباشر بين السلطات القضائية للدول الأطراف لنقل الإجراءات و تبادل المعلومات المفيدة للتحقيق عن طريق البريد[519]. وقد تم النص على هذا الإجراء في كل من البند الثاني من المادة (30) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لعام 1999، و المادة (15) من اتفاقية الرياض العربية للتعاون القضائي لعام 1983[520]، غير أن غالبية هذه الاتفاقيات لا تسمح بالتعاون المثمر في مجال

---

[517]-**أحمد سعد محمد الحسيني**، مرجع سابق، ص 300.

[518] -**CONSEIL DE L'EUROPE** « la criminalité informatique » recommandation N° R(89)9 sur la criminalité en relation avec l'ordinateur et rapport final du comité européen pour les problèmes criminels, Strasbourg, 1990, p 101.

[519]- **سامي جلال فقي حسين**، الأدلة المتحصلة من الحاسوب و حجيتها في الإثبات الجنائي، دار الكتب القانونية، القاهرة، 2011، ص131.

[520]- **جميل عبد الباقي الصغير**" الجوانب الإجرائية للجرائم المتعلقة بالانترنت" مرجع سابق، ص 86.

الجرائم الالكترونية وعجزت عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب و شبكة الانترنت، لاسيما أن معظم هذه الاتفاقيات تجاوزها الزمن صدرت في وقت لم تكن شبكة الانترنت قد ظهرت، أو كانت موجودة ولكنها محدودة، بالتالي فان تعديل هذه الاتفاقيات التقليدية للتعاون القضائي الدولي أصبح ضرورة ملحة حتى تتماشى مع التطورات الكبيرة في تكنولوجيا المعلومات و الاتصالات .

الفصل الثاني

الحلول المقترحة لتجاوز عقبات التحقيق في الجرائم الإلكترونية

لقد رأينا كيف أن عملية البحث والتحقيق في الجرائم الالكترونية وملاحقة مرتكبيها يتخللها العديد من المعوقات والعقبات الإجرائية، فمنها ما يتعلق بالطبيعة المتميزة للجريمة الالكترونية، أو بالجهات المتضررة، ومنها ما يتعلق بجهات التحقيق، وأخرى تتعلق بإجراءات الحصول على الدليل الالكتروني لارتباطها ببيانات معالجة الكترونيا وكيانات منطقية غير مادية. وأن كثرة وتشعب هذه العقبات قد انعكس سلبا على مردود سلطات التحقيق والعدالة الجنائية في ملاحقة مرتكب الجريمة، بل وشجع ارتفاع معدّل الجريمة في العالم بسبب إدراك المجرم الالكتروني أن وجود كل تلك العقبات سيعيق حتما الجهات الأمنية من اكتشاف أمره أو ملاحقته، ما يعطيه ثقة اكبر في ارتكابه المزيد من هذه الجرائم.

ولتدارك هذا الخطر باتت عملية البحث عن الحلول المناسبة للقضاء على ما تثيره مكافحة الجريمة الالكترونية من مصاعب ضرورة حتمية، خاصة وقد وجدت الدول نفسها عاجزة عن أداء واجبها الدستوري والقانوني لحماية الأفراد وتحقيق الأمن والاستقرار الاجتماعي المنوط بها إزاء الفراغ التشريعي لمكافحة هذه الظاهرة. فما كان منها سوى الإسراع إلى احتواء هذا النوع الجديد من الإجرام بسد الفراغ التشريعي المذكور، وذلك بتفعيل قوانينها العقابية الموضوعية والإجرائية القائمة بالرغم عما تتضمنه من نقائص وجعلها تسري على الإجرام الالكتروني، ثم تدعيمها بنصوص أخرى جديدة تكون أكثر تلاءم مع طبيعة هذه الجرائم. ثم القيام بعدها بمراجعة تشريعاتها الجنائية الوطنية بما يكفل التنسيق والموائمة بينها وبين تشريعات الدول الأخرى الراغبة في التعاون معها، والسعي إلى تكوين

أرضية قانونية تعمل على الكفاح الدولي المشترك ضد هذا الإجرام، وطرح المشاكل والحلول وإعداد مشروعات القوانين تسير على هديها الدول المشتركة (المبحث الاول).

ولما كانت أكثر العقبات تعقيدا التي تواجه عملية التحقيق في الجرائم الالكترونية مرتبطة أساسا بالبعد العابر للحدود الذي تتميز به هذه الجرائم ، كمشكلة احترام السيادة ومشاكل الحدود والولايات القضائية والاختصاص، فان من الحلول الناجعة التي وجدتها الدول لتجاوز هذه العقبات، بسط التعاون القضائي الدولي بصوره المختلفة، نظرا لما يحدثه من تنسيق وتبادل المساعدات بين سلطات إنفاذ القانون للدول في سبيل منع الجريمة وتعقب مرتكبيها على الصعيد الدولة والقبض عليهم ومحاكمتهم وإنزال العقاب عليهم (المبحث الثاني).

المبحث الأول

الحلول القانونية المقترحة لتدارك عقبات التحقيق في الجرائم الإلكترونية

المتأمل جيدا في المشاكل الإجرائية التي تصادفها سلطات التحقيق والبحث في الجرائم الالكترونية يجد أن معظمها مرتبط بطبيعة القوانين الإجرائية المتعارف عليها، وما تتسم به من قصور في استيعاب أهم التحديات التي تفرضها مواجهة هذا النمط المستحدث من الجريمة، والأساليب والإجراءات التي يتم التعامل بها معها، وكذا المناخ المناسب الذي يسمح بتنفيذ هذه الإجراءات، والسرعة والدقة والمهارة الفائقة المطلوبة لاتخاذها. لذلك يتعين لعلاج هذا القصور الذي تعاني منه عديد الدول، وضمان مواجهة فعالة للجريمة الالكترونية الإسراع من جهة إلى ترشيد تشريعاتها الوطنية الإجرائية بجعل أحكامها التقليدية تسري وتطبق على الجرائم الحديثة حتى لا يفلت من يقدم على ارتكاب هذه الجرائم من العقاب.

ومن جهة أخرى الإسراع في مراجعة هذه التشريعات حتى تتلاءم وطبيعة هذه الجرائم الحديثة وتتواكب مع التطورات الهائلة والمتلاحقة في مجال تقنية المعلومات وما تفرزه من جرائم معلوماتية جديدة (المطلب الأول).

أما عن المشكلات الأخرى التي لها علاقة بالبعد الدولي للفضاء الالكتروني الذي ترتكب فيه الجرائم الالكترونية، وبعدم كفاية التعاون الدولي وفقا للنصوص التقليدية في مكافحة هذه الجرائم بسبب انعدام نموذج موحد للنشاط الإجرامي المكون للجريمة الالكترونية، بالإضافة إلى تنوع واختلاف النظم القانونية والإجرائية للدول، فان حلّها يتطلب تبني تشريعات مشتركة وموحدة لمكافحة الجرائم الالكترونية عبر الوطنية، أو على الأقل خلق نوع من التقارب والاتساق بين الأحكام الإجرائية الوطنية للدول التي يتم وفقها ملاحقة مرتكبي هذه الجرائم ومحاكمتهم وتوقيع العقاب عليهم وتسليمهم، وهو الأمر الذي لا يتأتى إلا عن طريق إبرام اتفاقيات تعاون دولي في مجال التشريع (المطلب الثاني).

المطلب الأول

حوكمة المنظومة التشريعية الوطنية لمواجهة الجريمة الالكترونية

إذا كان التطور المتجدد والمستمر للمعلوماتية يمنع القوانين الجزائية الحالية من مواكبة ما يطرأ من صور وسلوكيات إجرامية مستحدثة في مجال المعلوماتية، فان تطبيق القواعد القانونية الموجودة التي تنظم الحماية الجنائية بما لها من نقص أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية. انطلاقا مما تقدم يرى البعض أن المواجهة الفعالة للتحديات الإجرائية التي تثيرها الجرائم الالكترونية يقتضي التصرف بحكمة و بدون تسرع أو طيش معها[513]، وذلك بداية بترشيد النصوص الجنائية التقليدية بالشكل الذي يجعلها تسري

[513] -**FALQUE Pierrotin,** la gouvernance du monde en réseau, in gouvernance de la société de l'information, cahier du C.R.I.D. n 22, Bruxelles, Bruylant, 2002, P 109 et s.

وتطبق على الجرائم الالكترونية، لا سيما تلك الجرائم التقليدية التي ترتكب عبر شبكة الانترنت، والتي لا تعدو هذه الشبكة أن تكون سوى مجرد وسيلة حديثة لارتكابها. على أن يتم ذلك في حدود ما يفرضه مبدأ الشرعية الجزائية من الالتزام بالتفسير الضيق للنصوص الجزائية، وحظر القياس (الفرع الاول)، وهذا الخيار يعد ضرورة لا مناص منها بالنسبة للدول التي لم تسن بعد تشريعات جنائية خاصة لمواجهة هذا النوع الجديد من الإجرام.

ويرى البعض الأخر أنه لا ينبغي التعويل كثيرا على القواعد التقليدية لمواجهة هذه التحديات، إنما لابد من التوجه إلى مراجعة هذه النصوص بصفة دورية و مستمرة بما يضمن مواكبة متغيرات وتطورات الجريمة الالكترونية. وإلى إرساء قواعد قانونية جديدة خاصة تواجه المشكلات المعاصرة التي أسفرت عن هذه الجريمة المستحدثة وتطوراتها اللامتناهية (الفرع الثاني).

الفرع الأول: تطبيق النصوص الجنائية التقليدية على الجرائم الإلكترونية

يمثل تطبيق النصوص الجنائية التقليدية الإجرائية منها والموضوعية على الجرائم الالكترونية إحدى الحلول الناجعة التي يمكن الاستعانة بها للتصدي لهذا النمط الإجرامي الجديد ومنع إفلات المجرمين من المسؤولية الجزائية، ويتأسس هذا الخيار على أنه في ظل عدم تدخل المشرع الجنائي بإصدار تشريعات جنائية جديدة خاصة بالإجرام الالكتروني، أو مراجعة النصوص الجنائية الموجودة حتى تصبح كفيلة بمواجهة هذا الإجرام، فانه لا مناص من استعانة القضاء بالنصوص الجنائية التقليدية في القواعد العامة أو أية قوانين جنائية خاصة أخرى، حتى لا تترك الأفعال التي تقع بها هذه الجرائم دون متابعة أو عقاب[514].

[514]–**عادل يحي**، مرجع سابق، ص 62.

ويتجسد هذا الحل من خلال الاجتهاد في تفسير النصوص العقابية التقليدية التي تعاقب على مختلف صور الاعتداءات، حتى يمكن تطبيقها على الجرائم المستحدثة التي أوجدتها ثورة الاتصالات عن بعد، فلا محالة أن التطور قد يوسع من دائرة المجالات التي تحميها نصوص التجريم والعقاب بحيث يمكن أن ندخل في إطارها عناصر أخرى طالما أمكن اعتبارها من جنسها وأن المشرع يحميها بذات النصوص[515].

ويكون اتخاذ سبيل التفسير الموسع للنصوص القائمة من أجل تطبيقها على الجرائم الالكترونية، بمنح القاضي الجزائي حرية تفسير هذه النصوص تفسيرا أكثر مرونة يسمح من وضع هذه الجرائم تحت طائلة التجريم و المتابعة الجزائية، وذلك في ظل السلطة التقديرية التي يتمتع بها القاضي[516].

فعندما تعرض قضية جزائية على القاضي، فان أول شيء يقوم به هو تكييف الواقعة لمعرفة مدى تطابقها مع النص القانوني الذي يجرّمها، وللوصول إلى هذه الغاية يقوم القاضي باستخلاص عناصر هذه الواقعة من النص، وقد يصادفه أثناء ذلك صعوبة أو غموض فيلجأ عندئذ إلى تفسير النص الجنائي[517].

وفي هذا الصدد نجد القضاء في العديد من الدول، قام بتفسير النصوص الجنائية التي تجرّم استخدام مال الغير دون وجه حق، مثل القانون البلجيكي المادة (2/261) والدانمركي المادة (293)، بشكل يسمح بمدّ نطاقها لتجريم سرقة وقت وجهد وخدمات الأجهزة والأنظمة

---

[515]– **هدى حامد قشقوش**، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012، ص 72.

[516]– **يوسف حسن يوسف**، الجرائم الدولية للانترنت، مرجع سابق، ص 126 و ما يليها.

[517]– **صغير يوسف**، مرجع سابق، ص 64.

المعلوماتية في حالة ما استخدمت من قبل الغير بدون الحصول على موافقة حائزها أو مالكها. وذلك نظرا لعدم توفر قوانينها الجنائية لنص صريح يجرّم هذه الأفعال[518].

كما نجد القضاء الفرنسي قد وسّع من تفسير نص المادة (145) من قانون العقوبات المتعلقة بجريمة تزوير المحررات التقليدية قبل تعديلها بالمادة(462) من قانون الغش المعلوماتي لعام 1988، لتشمل كل أشكال التلاعب في البيانات و الأنظمة المعلوماتية. وكذلك فعل القضاء الياباني، إذ لجأ في ملاحقة جرائم التزوير المعلوماتي، إلى تبني المفهوم الموسع لجريمة التزوير، واعتبر تغيير الحقيقة في الجزء الممغنط من بطاقات البيانات يقع تحت طائلة العقاب على التزوير في المحررات التقليدية[519].

كذلك هو الشأن بالنسبة للنصوص الجنائية المتعلقة بجريمة السرقة، فقد أصدرت محكمة النقض الفرنسية أكثر من قرار، وضحت فيها بشكل قطعي بأن الأشياء المعنوية والمعلومات على وجه الخصوص، تشملها الحماية التي يكفلها النصوص التقليدية للسرقة. ومن بين هذه القرارات، قرار إدانة عاملين بورشة التأليف الضوئي بجريمة السرقة، لقيامهما داخل المطبعة وباستخدام معداتها، بنسخ (47) أسطوانة معلوماتية تحتوي ملفا للعملاء ذات أهمية وقيمة تجارية كبيرة، ونسخ(70) أسطوانة ممغنطة أخرى مسجل عليها عمليات التأليف الضوئي التي باشرتها المطبعة دون علم رب العمل، بهدف تأسيس مشروع منافس للمطبعة التي يعملاني فيها. وقد أسست المحكمة قرارها، على أن واقعة النسخ هنا تتوفر على سائر العناصر المكونة لجريمة السرقة المنصوص عليها في قانون العقوبات وهي ثابتة في حق المتهمين، لذا يتعين إدانتهما و معاقبتها وفقا لأحكام هذا القانون[520].

---

[518]– **غازي عبد الرحمان هيان الرشيد**، مرجع سابق، ص 222.

[519]– المرجع نفسه، ص.ص 252– 258.

[520]– مشار إليه في: **هشام محمد رستم**، مرجع سابق، ص 246.

ولا يختلف الأمر بالنسبة لقابلية بسط نطاق النصوص التقليدية المتعلقة بجريمة الاحتيال، لتسري على الاحتيال الذي يباشر بواسطة التلاعب في الأنظمة المعلوماتية، إذ سمح الفقه والقضاء في العديد من الدول، بالتوسع في تفسير الركن الشرعي المكون لجريمة الاحتيال إلى المدى الذي يتيح إدخال الاحتيال المعلوماتي في نطاقه، منه الفقه الكندي الذي يرى بأنه في ظل عدم وجود نصوص جديدة تجرّم الاحتيال عبر الوسائل الإلكترونية، فلا مانع من مد نطاق المادتين(387 و 388) من قانون العقوبات الكندي إلى جرائم الاحتيال الالكتروني[521]. ويرى الفقه الفرنسي أن خداع الحاسب الآلي بهدف سلب مال الغير تتحقق فيه الطرق الاحتيالية بمفهومها المشار إليه في المادة (405) من قانون العقوبات باعتباره كذب تدعمه أفعال مادية أو وقائع خارجية. وعملا بهذا الرأي قضت محكمة النقض الفرنسية، بتطبيق العقوبة المقررة لجريمة النصب على شخص أدخل سيارته إلى موقف للسيارات، وقام بوضع قطعة معدنية في عداد الموقف لدفع مقابل التوقيف بدلا من النقود، ما ترتب عليه تشغيل الماكينة وتحريك العقارب، واعتبرت المحكمة هذا التصرف من قبيل الطرق الاحتيالية[522] .

وينبغي ألا يقتصر هذا الحل على تمديد سلطان النصوص الجنائية التقليدية الموضوعية إلى الجرائم الالكترونية فقط، بل لابد أن يشمل كذلك النصوص الإجرائية، لا سيما المتعلقة بالتحقيق والإثبات، وهو ما أوصت به اللجنة الأوروبية الخاصة بمشكلات الإجرائية الجزائية المرتبطة بتكنولوجيات الإعلام الدول الأعضاء في المجلس الأوروبي من خلال توصيتها رقم (ر 89) 9 الصادرة في عام 1990 وأكدته في توصيتها رقم (ر95) 13 المؤرخة في 11 سبتمبر 1995 بتصريحها أنه " إلى حين وضع نصوص إجرائية

---

[521]- **BRIAT Martin**. La Fraude Informatique: Une approche de droit compare, Revue D.P.C, N04 Paris, Avril 1985, p 191.

[522] -**Ibid**., p 192.

جديدة تخص التفتيش و الضبط واعتراض المراسلات في البيئة الالكترونية، يمكن للسلطات القضائية المختصة في الدول الأعضاء الاستعانة بالنصوص الإجرائية القائمة في هذا الخصوص، حتى لا تبقى الجرائم المتصلة بتكنولوجيات الإعلام بلا متابعة أو عقاب"[523].

وتجدر الإشارة إلى أن تطبيق النصوص الجنائية التقليدية على الجرائم التي تقع في البيئة الالكترونية، وإن كان يشكل ضرورة لا مفرّ منها في الدول التي لم تسنّ بعد تشريعات حديثة مواكب لهذا النوع من الجرائم، إلا أنه لابد من توخي الحذر في ذلك. إذ أن الآلية الوحيدة لإعمال هذا الخيار هو توسع القضاء في تفسير النصوص الجناية التقليدية بما يضمن سريانها على الجرائم الالكترونية، وهو ما قد يشكل إنتهاكا خطيرا لمبدأ الشرعية الجزائية الذي طالما كان درعا حاميا للحقوق والحريات الفردية من تعسف القضاء [524].

مع هذا تعتمد غالبية الدول العربية على هذا الحل، بحيث لم تفرد تشريعات عقابية خاصة لمواجهة الجرائم الالكترونية مواجهة شاملة، إنما تعتمد في ذلك على نصوص قانونية متفرقة في بعض التشريعات الخاصة، كقوانين حماية الملكية الفكرية، قوانين حماية حقوق المؤلف، قوانين التوقيع الالكتروني، وقوانين المتعلق بتكنولوجيا الإعلام والاتصال، أما غالبية الجرائم الالكترونية فتواجهها هذه الدول من خلال تطويع نصوص قوانين العقوبات والإجراءات الجزائية التقليدية [525].

---

[523] - voir : la recommandation n R (89) 9 sur la criminalité informatique, comité européen pour les problèmes de droit procédural liés a la criminalité informatique, conseil de l'Europe, Strasbourg, 1990, p 80. Et sa recommandation n R (95) 13, op.cit., p19.

[524] -**CHAWKI Mohamed**, combattre la cybercriminalité, op.cit. , p 399.

[525]– **لجنة منع الجريمة والعدالة الجنائية**، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، مرجع سابق، ص 05.

الفرع الثاني: ضمان مواكبة التشريعات الجزائية الوطنية لمتغيرات الجريمة الالكترونية (التحيين و التحديث)

لا يكفي الاعتماد على التشريعات الجنائية القائمة كحل لمواجهة الجريمة الالكترونية، بل لا بد من العمل على مواكبة هذه التشريعات لمتغيرات وتطورات الجريمة الالكترونية، وذلك إما عن طريق تعديل النصوص الجزائية التقليدية بحيث تتواءم مع هذه الصورة الجديدة من الإجرام، أو بخلق نصوص قانونية جنائية جديدة يضاف إليها البعد الخاص بالبيئة الالكترونية[526].

تأسيسا على ذلك، فقد استدركت اغلب الدول بمختلف أنظمتها القانونية العجز في ملائمة القوانين النافذة للاعتداءات الحاصلة على النظم المعلوماتية، وسوف نأخذ في هذا الصدد عينة من النماذج الناجحة من التشريع المقارن (أولا)، ثم نركز على دور المشرع الجزائري في هذا المجال (ثانيا).

أولا – التشريعات المقارنة

يعد المشرع الفرنسي من أوائل المشرعين الذين تيقنوا بأن التصدي الفعال للجرائم الالكترونية لن يكون إلا من خلال سنّ نصوص عقابية و إجرائية خاصة بهذه الجرائم. وقد كانت أولى محاولاته لمد سلطان قانون العقوبات ليشمل المجال المعلوماتي في 06 جانفي 1978 حينما أصدر قانون " المعلوماتية والحقوق الشخصية"، وأعقبه بإصدار مرسوم مؤرخ في 23 ديسمبر 1981 حدد فيه بعض المخالفات المرتبطة بالمعلوماتية[527].

---

[526]– **هشام محمد فريد رستم**، الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مرجع سابق، ص 418.

[527]-**CHOPIN- Frédérique**, Les politiques publiques de lutte contre la cybercriminalité, AJ Pénal, Paris, 2009 p. 102.

وفي سنة 1988 أصدر المشرع الفرنسي قانون خاص " بحماية نظم المعالجة الآلية للبيانات"، والذي تم إدماجه في عام 1992 ضمن قانون العقوبات الفرنسي في الباب الثالث من الكتاب الثاني من القسم الثاني، المعدل بموجب القانون المؤرخ في 1 مارس 1994[528]، وقد نص هذا القانون في المواد من(2/462 إلى 9/462)على مجموعة من الجرائم التالية:

ـ الدخول غير المشروع في نظام معالجة آلية للمعطيات او البقاء فيه.

ـ إدخال معطيات في نظام معلوماتي ملك للغير أو محو أو تعديل المعطيات الموجودة فيه أو طرق معالجتها أو نقلها.

ـ كل فعل عمدي من شانه أن يعرقل أو يفسد أداء النظام المعلوماتي لوظيفته.

ـ تزوير المستندات المعالجة آليا مهما كان شكلها و كذا استعمال هذه المستندات المزورة.

وقد تواصلت جهود المشرع الفرنسي في هذا المجال بشكل مكثّف بعد تصديق فرنسا في 23 نوفمبر 2001 على الاتفاقية الأوروبية الخاصة بالجرائم الالكترونية 2001، فقام من جهة بتعديل تشريعاتها العقابية لتتجاوب مع أحكام هذه الاتفاقية، ومن جهة أخرى استحدث ترسانة من نصوص أخرى خاصة لمواجهة الجريمة الالكترونية أهمها، القانون رقم (1062/01) المتعلق بالأمن اليومي المؤرخ في 2001/11/15[529]، والقانون رقم (239/03) المتضمن التوجيه والتخطيط للأمن الداخلي المؤرخ في 18 مارس 2003[530]، القانون رقم(204/04) المتضمن مواكبة العدالة لتطورات الإجرام[531]، القانون رقم

---

[528]– **محمد أمين الرومي**، جرائم الكمبيوتر و الانترنت، دار المطبوعات الجامعية، القاهرة، 2004، ص 101.

[529]- Loi n° 2001-1062, 15 nov. 2001 relative à la sécurité quotidienne, JORF 16 nov. 2001, p. 18215

[530] - Loi n° 2003-239, 18 mars 2003 pour la sécurité intérieure, JORF 19 mars 2003, p. 4761.

[531] - Loi n° 2004-204, 9 mars 2004, portant adaptation de la justice aux évolutions de la criminalité, JORF 10 mars 2004, p. 4567.

(575/04) المتعلق بالثقة في الاقتصاد الرقمي مؤرخ في 2004/07/22 ،[532] القانون رقم (669/04) المتعلق بالاتصالات الالكترونية و خدمات الاتصال لعام 2004،[533] قانون رقم (297/07) المؤرخ في 2007/03/05 المتعلق بالوقاية من الإجرام[534]. قانون البث وحماية الإبـداع عبـر الانتـرنت(Hadopi1) لعام 2009 [535]، وقـانـون الحمـاية الجنـائية للملكية الأدبية والفنية عبر الانترنت (Hadopi2) لعام 2009[536].

ومن أجل محاصرة ظاهرة الإجرام الالكتروني أدخل المشرع الفرنسي كذلك عدة تعديلات على إجراءات المتابعة الجزائية و التحقيق و الإثبات التقليدية (كإجراءات التحري والتفتيش وضبط والمعاينة و إجراءات جمع الأدلة، تحريزها و حجيتها) بما يجعلها تتناسب وطبيعة الجرائم الالكترونية، كما استحدث إجراءات أخرى خاصة التي يمكن لرجال إنفاذ القانون الاستعانة بها للكشف عن الجريمة مثل اعتراض المراسلات، التسرب الالكتروني، المراقبة الالكترونية، الكشف عن المعطيات المشفرة، التحفظ العاجل للمعطيات، نقل الإجراءات[537].

أما في الولايات المتحدة الأمريكية، فيعد قانون ولاية فلوريدا لجرائم الحاسب الصادر عام 1978 أول قانون يخص الجريمة الالكترونية، إذ اعتبر هذا القانون أن كل ولوج غير

---

[532]- Loi n° 2004-575, 21 juin 2004 pour la confiance dans l'économie numérique, JORF 22 juin 2004, p. 11568.

[533] - Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication, JORF du 10 juillet. 2004, p. 12483.

[534] - Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, JORF du 7 mars 2007, p 4297

[535] - Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet dite Hadopi1, JORF du 13 juin 2009, p 966.

[536]- Loi n° 2009-1311 du 28 octobre 2009 favorisant relative a la protection pénale de la propriété littéraire et artistique sur internet dite Hadopi2, JORF du 31 décembre 2009.

[537]- **CHOPIN Frédérique**, op.cit. p110.

مصرح به إلى جهاز الحاسب هو بمثابة جريمة، ولو كان هذا الدخول بحسن نية. أما على الصعيد المركزي، فقد صدر عام 1984 قانون الاحتيال وإساءة استخدام الحاسب الآلي المعدل عدة مرات أخرها في عام 2001، والذي تناول الجرائم التي تقع على أنظمة الحاسبات الآلية التابعة الحكومة المركزية من جهة، والجرائم التي يتطلب ارتكابها استخدام أجهزة الحاسب تتواجد في أكثر من ولاية أمريكية من جهة أخرى، وقد نصت المادة (1030) منها على معاقبة كل من يدخل عمدا وبدون ترخيص إلى نظام حاسب مشمول بالحماية، أو يتجاوز عمدا الترخيص الممنوح له إذا أدى هذا السلوك إلى استخدام أو تعديل أو تدمير أو كشف المعلومات المخزنة داخله أو إعاقة أداء النظام الحاسب الآلي بوظائفه المعتادة[538].

وبصدور قانون حماية بنية المعلومات القومية لعام 1996، تم توسيع نطاق حماية أنظمة الحاسبات الآلية، فبعدما كانت الحماية مقتصرة على الحاسبات الآلية التابعة للحكومة وإدارتها أو التي يتم استعمالها من قبلها، توسعت لتشمل جميع الحاسبات التي يتم استخدامها من قبل المؤسسات الاقتصادية والتي تستخدم في العمليات التجارية والاتصالات. وعلى اثر هذا القانون، حدد معهد العدالة القومي الأمريكي خمسة أنواع رئيسية للجرائم المعلوماتية هي كالتوالي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية وسرقة البرامج والمكونات المادية للحاسب[539].

---

[538]-**KARY (T)** « Etats Unis ; projet de loi prend a nouveau pour cible le crime informatique » 04 février 2002. Disponible a l adresse suivante ; http://news.zdnet.fr/story/ot118-s20104405.00.hunl

[539]- **يوسف حسن يوسف**، مرجع سابق، ص79.

وفي سنة 1986 تم إصدار قانون رقم (1213) عرّف فيه جميع المصطلحات الضرورية لتطبيق القوانين العقابية على الجرائم المعلوماتية، وإحاطتها بالمتطلبات الدستورية اللازمة لذلك، ثم استتبعته في عام 1988 بقانون " سرية المعلومات الالكترونية" الذي جرّم أي اعتراض للاتصالات الالكترونية الخاصة أو التصنت عليها بشكل غير مرخص به، وهو القانون الذي خولت على أساسه وزارة العدل الأمريكية خمسة جهات التحقيق بما فيها مكتب التحقيقات الفيدرالي صلاحية التعامل مع الجرائم الالكترونية[540].

بالموازاة مع هذا القانون، أصدر المشرع الأمريكي في الثامن من فيفري 1996 قانون الاتصالات استهدف من خلاله حماية القصر من جرائم الاستغلال الجنسي أو المخلة بالحياء عبر وسائل الاتصال والانترنت، إذ نصت المادة (223) منه على معاقبة كل من يقوم عمدا بواسطة أية وسيلة من وسائل الاتصالات بخلق أو تشجيع أو صناعة أو بثّ أو تعليق أو طلب أو اقتراح صورة أو أي اتصال أخر يكون خليع أو غير أخلاقي وهو يعلم أن المتلقي قاصرا لم يبلغ الثماني عشر عاما[541].

إلى جانب التشريعات المركزية، فقد أصدرت معظم الولايات الأمريكية تشريعات خاصة بمكافحة الإجرام الالكتروني، منها ما تضمنه قانون ولاية " كاليفورنيا" من نصوص تجرم إتلاف القيم المعلوماتية المادية وغير المادية، وقانون و تعطيل الخدمة، وكذا قانون ولاية "ألاسكا" الذي أدرج الإتلاف ألمعلوماتي ضمن فئة الجرائم الواقعة على الأموال [542]. الشيء نفسه فيما يخص قانون جرائم الحاسبات الآلية في ولاية " مين" الصادر عام 1998 والذي

---

[540]– **يوسف حسن يوسف**، مرجع سابق، ص80.

[541]– **محمود أحمد عبابنة**، جرائم الحاسب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص 143.

[542]– المرجع نفسه، ص 146.

جرّم كل سلوك يسبب إتلاف النظم المعلوماتية للحاسب، وكل إدخال أو خلق الظروف الملائمة لدخول فيروس إلى أي مكونات نظام الحاسب الآلي [543].

ولم يكتفي المشرع الأمريكي بتكريس تشريعات جنائية خاصة بالإجرام الالكتروني، بل اهتم كذلك بتدريب رجال الضبطية القضائية والعاملين في إدارات العدالة الجنائية على مكافحة هذا النوع من الإجرام والتحقيق فيها، من خلال تنظيم دورات تدريب متخصصة تنظمها أكاديمية التحقيقات الفيدرالية في مختلف الولايات بشكل دوري، بغية رفع كفاءتهم في مجال كشف هذه الجرائم وملاحقة مرتكبيها وتوقيع العقاب عليهم، وموافاتهم باستمرار بأخر التطورات والمستجدات في هذا الميدان.

ثانيا- سياسة المشرع الجزائري في مواكبة تطورات الإجرام الإلكتروني

اعتمد المشرع الجزائري منذ الألفية الثانية على إستراتيجية مزدوجة لمواكبة الجريمة الالكترونية، بحيث قام من جهة بتعديل العديد من القوانين الوطنية بما فيها التشريعات الجزائية (العقوبات و الإجراءات) وجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجي الإعلام والاتصال. وقام من جهة ثانية باستحداث قوانين أخرى خاصة أكثر انسجاما مع الطبيعة المميزة للجريمة الالكترونية .

1ـ تعديل التشريعات الجزائية : اقتداء بالمشرعين الذين سبقوه، سارع المشرع الجزائري إلى تدارك الفراغ القانوني الحاصل في مجال الإجرام الالكتروني، فقام بتعديل قانون العقوبات بموجب القانون رقم (04-15)[544] مستحدثا فيه جملة من النصوص جرّم

---

[543]– **طرشي نورة**، مكافحة الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق بجامعة الجزائر 1، 2012، ص 29.

[544]– قانون رقم(04-15) مؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم (66-156)، يتضمن قانون العقوبات، ج.ر عدد 71، صادر بتاريخ 2004/11/10، معدل ومتمم.

من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها ما يقابله من الجزاء. وقام إلى جانب ذلك بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماش مع الطبيعة المميزة للجرائم الالكترونية، وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم (06-22)[545].

أ-التعديلات المقررة في قانون العقوبات

عمد المشرع الجزائري في تعديله لقانون العقوبات بمقتضى القانون رقم (04-15) المؤرخ في 10 نوفمبر 2004 الى استحداث القسم السابع مكرر تحت عنوان " **المساس بأنظمة المعالجة الآلية للمعطيات**"، وقد تضمن هذا القسم ثمانية مواد (من 394 مكرر إلى 394 مكرر 7) حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات و ما يقابلها من جزاء أو عقوبة.

وباستقراء نصوص هذه المواد يتبين أن المشرع الجزائري حصر هذه الأفعال في ثلاث فئات هي:

1- جرائم الاعتداء على نظام المعالجة الآلية: وهي الجرائم التي تتحقق في صورتين، الصورة البسيطة التي تشمل جريمتي الدخول والبقاء غير المرخص بهما في نظام المعالجة الآلية، وحدد لهما العقوبة نفسها هي الحبس من 03 أشهر الى سنة وغرامة مالية من 50000دج الى 100000دج[546]. والصورة المشددة هي التي تتحقق عندما يقترن فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية بإحدى ظروف التشديد المنصوص عليها في المادة (394مكرر)، كمحو أو تعديل بيانات النظام، أو تخريب نظام تشغيل

---

[545]- قانون رقم (06-22) مؤرخ في 2006/12/20، يعدل ويتمم الأمر رقم(66-155)، يتضمن قانون الإجراءات الجزائية، ج.ر عدد 84، صادر بتاريخ 2006/12/24.

[546]- أنظر نص المادة (394 مكرر) من القانون رقم(15/04)، مرجع سابق.

المنظومة وإعاقته عن أداء وظيفته[547]. فمتى تحققت هذه الجريمة في صورتها المشددة عوقب الجاني بالحبس من (6) أشهر الى سنتين وبالغرامة من 50000دج إلى 150000دج[548].

2- جرائم الاعتداء على معطيات نظام المعالجة الآلية[549]: وتشمل الاعتداءات التي تهدف إلى الإضرار بمعلومات الحاسب الآلي أو وظائفه سواء بالمساس بسريتها أو المساس بسلامتها محتوياتها، تكاملها أو بتعطيل قدرة وكفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بصورة سليم. وهي لا تخرج في مجملها عن أحد الشكلين التاليين:

- **الشكل الأول / الاعتداء على المعطيات الداخلية للنظام:** وقد حددت المادة (394 مكرر 1) من قانون العقوبات صور هذه الجريمة على سبيل الحصر كالتالي:

ـ الإدخال: يقصد به إضافة معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام و التي تمت معالجتها أليا.

ـ المحو : يعني إزالة من معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الآلية أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة.

. التعديل :يعني تغيير المعطيات الموجودة داخل نظام المعالجة واستبدالها بمعطيات أخرى.

ولا تشترط المادة المذكورة اجتماع هذه الصور الثلاثة، بل يكفي أن يصدر عن الجاني

---

[547]- للمزيد من التفاصيل أنظر : **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط ثانية ، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص 102 و بعدها.

[548]- أنظر الفقرة الثانية من المادة (394 مكرر) من القانون رقم (04-15)، مرجع سابق.

[549]- يقصد بالمعطيات محل جريمة الاعتداء بمفهوم هذه المادة (394 مكرر 1) من قانون (04-15) ، تلك المعطيات والمعلومات التي يحتويها النظام وتشكل جزء منه و التي تمت معالجتها آليا وأصبحت عبارة عن رموز و إشارات تمثل تلك المعلومات، وليس المعلومات ذاتها باعتبارها أحد عناصر المعرفة.

إحداها لكي يكتمل الركن المادي لجريمة الاعتداء على معطيات نظام المعالجة[550].

الشكل الثاني/ الاعتداء على المعطيات الخارجية للنظام: يقصد بالمعطيات الخارجية لنظام المعالجة، تلك المعطيات التي لها دور في تحقيق نتيجة معينة تمثل في المعالجة الآلية للمعطيات، وقد نص عليها المشرع الجزائري في المادة (394 مكرر 2) من قانون العقوبات على النحو التالي:"**يعاقب بالحبس من شهرين إلى 3سنوات و بغرامة من 1000000دج الى 5000000دج كل من يقوم عمدا أو عن طريق الغش بـ**

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

ـ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيـــات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"[551].

يتبين لنا من نص هذه المادة أنها جاءت عامة و مطلقة، فهي تقرر الحماية الجنائية لكل من المعطيات الداخلية و الخارجية للنظام معا.

فيقصد المشرع بالمعطيات المخزنة إما تلك المفرغة في دعامة مادية خارج النظام كالأقراص الممغنطة أو تلك المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب[552].

---

[550] -**BOUDER Hadjira** « protection des systèmes d'informations : aspects juridiques » centre de recherche sur l'information scientifique et technique, Alger, 2012, p 32.

[551]– أنظر نص المادة(394 مكرر 2) من القانون رقم (04–15)، مرجع سابق.

[552]– **فايز محمد راجح غلاب**، مرجع سابق، ص 183.

ويقصد بالمعطيات المعالجة، إما تلك التي أصبحت جزءا من النظام بعد أن تحولت إلى إشارات أو رموز تمثل المعطيات المعالجة، وإما تلك المعطيات المرسلة عن طريق منظومة معلوماتية مثل تبادل إرسال المعلومات بين أجهزة المنظـومة المعلومـاتية. فـالأولـى تعتبر معطيات داخلية للنظام والثانية هي معطيات النظام الخارجية[553].

وعليه فأي تلاعب بالمعطيات المذكورة أعلاه، واستعمالها عمدا أو عن طريق الغش بإحدى الطرق المحددة في المادة (394مكرر 2) (أي تصميمها أو بحثها أو تجميعها أو توفيرها أو نشرها أو الاتجار بها أو حيازتها أو إفشاءها أو نشرها) يعد جريمة اعتداء على المعطيات الخارجية لنظام المعالجة والتالي يعاقب الجاني بالحبس من شهرين إلى 3سنوات وبغرامة من 1000000دج إلى 5000000دج.

3- جرائم الاعتداء على سير نظام المعالجة الآلية: لم ينص المشرع الجزائري على هذه الفئة من الجرائم الالكترونية بشكل صريح، إلا انه يمكن استخلاصها من خلال مختلف النصوص التي تجرّم أفعال الاعتداء على أنظمة المعالجة، اعتبارا أن وقوع هذه الأخيرة تؤثر حتما على سير أو وظيفة نظام المعالجة الآلية.

فالاعتداء على النظام بتخريبه كما نصت عليه المادة(394مكرر) من شأنه أن يعيب عملية سير النظام، والاعتداء على معطيات الداخلية للنظام باستعمال برامج الفيروسات وبرامج القنابل المعلوماتية من شأنه كذالك التأثير في سير أو حسن سير النظام المعلوماتي[554]. وعليه يمكن أن تتخذ الأفعال الماسة بسير النظام عدة صور نذكر منها:

---

[553]ـــ **فشار عطاء الله** "مواجهة الجريمة المعلوماتية في التشريع الجزائري " بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية المنعقد بأكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص 31.

[554] - **BOUDER Hadjira** « protection des systèmes d'informations : aspects juridiques » op.cit., p 22 .

ـ **التعطيل:** وقد يصيب الأجهزة المادية لنظام المعالجة كتحطيم الاسطوانات أو قطع شبكة الاتصال، أو يصيب كياناته المنطقية كالبرامج أو المعطيات باستخدام برنامج فيروسي أو قنبلة منطقية مما يؤدي إلى عرقلة سير النظام.

ـ **الإفساد:** وهو جعل نظام المعالجة الآلية غير صالح للاستعمال بإحداث خلل في نظام سيره وإفقاده التوازن في أداء وظائفه، كأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، ومثل هذا الفعل إن لم يؤدي إلى تعطيل نظام المعالجة كلية فانه يحول دون تحقيقه لوظائفه بشكل صحيح[555].

وتجدر الإشارة إلى أن المشرع الجزائري جرّم كل من الاشتراك والشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية المذكورة، وجعل العقوبة عليهما تساوي العقوبة المقررة للجريمة ذاتها[556]. وقد تأخذ هذه العقوبات إما شكل عقوبات أصلية كالحبس والغرامة، أو عقوبات تكميلية كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع وأماكن الاستغلال إذا ارتكبت الجريمة بعلم مالكها[557]. كما أن المشرع ضاعف عقوبة الغرامة المقررة للشخص المعنوي الذي يرتكب إحدى الجرائم الالكترونية المذكورة إلى (05) مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي، مع إقراره المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أصليين أو شركاء في الجريمة نفسها التي ارتكبها الشخص المعنوي[558].

---

[555]– **فشار عطاء الله**، مرجع سابق، ص 28.

[556]– راجع المادتين (394 مكرر5 و 394مكرر7) من قانون العقوبات الجزائري، مرجع سابق.

[557]– راجع العقوبات التكميلية في نص المادة(394مكرر6) من قانون العقوبات الجزائري، المرجع نفسه .

[558]–راجع المادة(394مكرر4) من قانون العقوبات الجزائري،.

ب ـ التعديلات المقررة في قانون الإجراءات الجزائية:

أدرك المشرع الجزائري جيدا بان المواجهة الفعالة للإجرام الالكتروني لا تكون بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية فقط، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية و تحفظية، وهو ما استدركه بتضمين القانون رقم (06-22) المعدل لقانون الإجراءات الجزائية تدابير إجرائية جديدة تتعلق بالتحقيق في الجـرائم الالكترونـية تتمثل فيما يلي:

- **اعتراض المراسلات و تسجيل الأصوات و التقاط الصور:** بالرجوع إلى المادة (65مكرر5) من قانون الإجراءات الجزائية، فان المشرع الجزائري سمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري أو التحقيق في الجريمة الالكترونية، باللجوء إلى إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور، والاستعانة بكل الترتيبات التقنية اللازمة لذلك من اجل الوصول إلى الكشف عن ملابسات الجريمة و إثباتها دون أن يتقيدوا بقواعد التفتيش و الضبط المألوفة[559].

ونظرا لخطورة هذه الإجراءات على الحقوق والحريات العامة والحياة الخاصة للأفراد، فان المشرع لم يطلق حق اللجوء إليها، إنما قيده بتوفر مجموعة من الشروط القانونية التي تتلخص في، الحصول على الإذن المسبق من السلطات القضائية المختصة للقيام بالإجراء ومراقبتها له، الضرورة الملحة إلى الإجراء لإظهار الحقيقة، مراعاة الجرائم التي يجوز فيها الإجراء، مراعاة مدة الاعتراض، مراعاة السر المهني أثناء الاعتراض[560].

---

[559]- أنظر هذه القواعد في المادتين(45 و 47) من ق إ ج رقم(06-22) ، مرجع سابق.

[560]- للمزيد من التفاصيل انظر المواد من (65مكرر 5 الى 65 مكرر) من ق إ ج رقم(06-22) المرجع نفسه.

ـ **التسرب** : بناء على المادة(65 مكرر 11 ق إ ج ج) فقد أجاز المشرع لمتطلبات التحري و التحقيق في الجرائم الالكترونية، اللجوء إلى عملية التسرب للكشف عن الحقيقة، وتقتضي عملية التسرب حسب المادة (65 مكرر 12) من القانون نفسه " **قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك أو خاف**".

ولضمان إنجاح العملية سمحت المادة(65 مكرر 14) من قانون الإجراءات الجزائية لضابط أو العون المتسرب، استعمال الوسائل المادية كالأموال أو المنتجات أو الوثائق المتحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها. كما يجوز له تسخير وضع تحت تصرف مرتكبي هذه الجرائم كل الوسائل المادية المتاحة لتنفيذ الجريمة كوسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال، وكذا الوسائل القانونية كتوفير الوثائق الرسمية إن كان هناك ضرورة لذلك كاستخراج بطاقة التعريف الوطنية أو بطاقة رمادية أو جواز السفر و لو استدعى الأمر تزويرها، دون أن يكون الضابط أو العون المتسرب مسئولا جزائيا عن هذه الأعمال.

مع هذا واعتبارا أن التسرب إجراء غير مألوف عند سلطات الضبط القضائي، ومن أخطر إجراءات التحقيق انتهاكا لحرمة الحياة الخاصة للمتهم، كان لزاما على المشرع إحاطته بجملة من الضمانات والضوابط التي يتعين مراعاتها عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة اللجوء إليه، وهي الضمانات المنصوص عليها في المادتين (65 مكرر11) و (65 مكرر 15)، والتي لا تختلف كثيرا عن تلك المفروضة على عملية اعتراض المراسلات.

ـ **تمديد الاختصاص** : من أجل تحقيق المواجهة الفعالة لظاهرة الإجرام الالكتروني، فقد قام المشرع الجزائري بموجب المادة (16 الفقرتين 7 و8) والمادة (16 مكرر) من قانون

الإجراءات الجزائية رقم (06-22) بتمديد الاختصاص المحلي لضباط الشرطة القضائية إلى كامل الإقليم الوطني، فبناء على هذا النص أصبح بمقدور الضبطية القضائية ممارسة جميع إجراءات البحث والتحري التي تدخل ضمن صلاحياتها، عبر كافة الإقليم الوطني إذا تعلق الأمر بالجرائم الماسة بالمعالجة الآلية للمعطيات. ومثل هذا التدبير لم يكن مسموحا به في السابق إلا في حالات استثنائية ضيقة جدا، وبشروط صارمة[561] .

بالموازاة مع ذلك، فقد تم أيضا توسيع مجال الاختصاص المحلي لنيابة الجمهورية في متابعة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ليشمل نطاق اختصاص مثيلتها في محاكم أخرى دون أن يشكل ذلك حالة تدخل أو تنازع في الاختصاص[562]. وكذلك فعل بالنسبة لقضاة التحقيق بموجب المادة (2/40) من قانون الإجراءات الجزائية التي تنص بأنه " **يجوز تمديد الاختصاص المحلي لقاضي التحقيق الى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخذرات و الجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...**".

ليس هذا فحسب، بل أجاز المشرع الجزائري كذلك في المادة (329) فقرتها الأخيرة من نفس القانون تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، للنظر و البث في الجرائم الماسة بالمعالجة الآلية للمعطيات[563].

---

[561]- أنظر نص المادة(16)من قانون الإجراءات الجزائية قبل التعديل الحاصل في 2006 .

[562]- تنص المادة(2/37) من ق إ ج بأنه " **يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في ...الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...**"

[563]- أنظر نص المادة(339 /5) من قانون الإجراءات الجزائية رقم (06-22)، مرجع سابق.

2- إرساء قوانين إجرائية جديدة خاصة بالجرائم الالكترونية:

يعتبر القانون رقم (09-04) [564] أهم النصوص الجديدة التي سنّها المشرع الجزائري لمواجهة الجرائم الناشئة عن الاستخدام غير المشروع لوسائل الإعلام والاتصال الالكترونية وشبكة الانترنيت، والذي تضمّن جملة من تدابير مستحدثة غير مألوفة في القوانين السابقة، وأكثر ملائمة مع خصوصيات هذه الإجرام، تتنوع بين تدابير وقائية، وأخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائية، والتي سنفصل فيها بالشكل التالي:

أـ التدابيـر الوقائية: وهي التي يتم اتخاذها مسبقا من طرف مصالح معينة مختصة لتفادي وقوع جرائم معلوماتية أو الكشف عنها و رصد مرتكبيها في وقت مبكر[565]، وتتلخص فيمايلي:

1-**مراقبة الاتصالات الالكترونية:** لقد نصت المادة(04) من القانون رقم (09-04) على أربع حالات التي يجوز فيها لسلطات الأمن والتحقيق القيام بمراقبة المراسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي:

ـ للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب و التخريب و جرائم ضد أمن الدولة.

ـ في حالة توفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.

---

[564]- قانون رقم (09-04) مؤرخ في 2009/08/5، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، جريدة رسمية عدد 47، صادر بتاريخ 16 أوت 2009.

[565]-تجدر الإشارة إلى أن هذه التدابير هي نفسها المنصوص عليها في المادة(20 الفقرة (ب) و المادة (21) من الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية لعام 2001، مرجع سابق.

ــ لضرورة التحقيقات و المعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية .

ــ في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة[566].

2-إقحام مزودي خدمات الاتصالات الالكترونية [567] في مسار الوقاية من الجرائم المعلوماتية: وذلك من خلال فرض عليهم مجموعة من الالتزامات المذكورة في المواد(10، 11 و 12) بالشكل التالي:

-الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات والتحقيق.

-الالتـزام بحفظ المعطـيات المتعلقـة بحركة السير وكل المعلومات التي من شأنـها أن تساهم في الكشف عن الجرائم ومرتكبيها، وهذين الالتزامين موجهين لكل مقدمي خدمات الاتصالات الالكترونية (Fournisseurs de services) دون استثناء[568].

- الالتــزام بالتدخل الفــوري لسحب المحتويات التي يسمح لهـم الاطـلاع عليها بمجر

---

[566]-أنظر نص المادة(04) من القانون رقم (09-04)، مرجع سابق.

[567]- عرفت المادة(2 الفقرة (د) من القانون رقم (09-04) مزودي الخدمات بأنه: 1-**أي كيان عام او خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام الاتصالات.** 2- **أي كيان آخر يقوم بمعالجة أو تخزين معطيان معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.**

[568]- **BOUDER Hadjira** « Quel cadre juridique pour la lutte contre la criminalité liée aux TIC en Algérie » séminaire national sur le cadre juridique des TIC en Algérie ; entre opportunité et contraintes, CERIST, Alger, du 16 au 17 mai 2012, p04.

علمهم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الوصول إليها غير ممكن.

–الالتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم بوجودها. ونشير هنا إلى أن هذين الالتزامين يخصان فقط مقدمي الدخول إلى الانترنيت (Fournisseurs D'accès a l'internet) دون غيرهم[569].

ب ـ **التدابير الإجرائية** : إضافة إلى التدابير الوقائية سالفة الذكر، تبنى المشرع في القانون رقم(09–4) إجراءات تحقيق جديدة يكمّل بها تلك المنصوص عليها في قانون الإجراءات الجزائية بخصوص مكافحة جرائم تكنولوجية الإعلام و الاتصال، و التي نلخصها فيما يلي:

– السماح للجهات القضائية المختصة وضباط الشرطة بالولوج لغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها واستنساخها، مع إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى التي يمكن الدخول إليها بواسطة المنظومة الأصلية، بشرط إخطار السلطات المختصة مسبقا.

– إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقـيات

[569]- **بوكر رشيدة**، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، بيروت، 2012، ص 450.

الدولية ومبدأ المعاملة بالمثل[570].

-توسيع دائرة اختصاص الهيئات القضائية الجزائرية لتشمل النظر في الجرائم المتصلة بتكنولوجية الإعلام والاتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية والدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة.

-السماح للسلطات الجزائرية المختصة اللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام والاتصال عبر الوطنية ومرتكبيها، وذلك عن طريق تبـــادل المعلومات أو اتخـاذ تدابير احترازية في إطـار الاتفاقيـات الدولية ومبدأ المعاملة بالمثل[571].

وتجدر الإشارة إلى أن أحكام القانون رقم (09-4) جاءت عامة و مطلقة في مجال مكافحة الجرائم المتصلة بتكنولوجية الإعلام والاتصال، إذ تجرّم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال، وتطبّق على كافة التكنولوجيات القديمة والجديدة، بما فيها شبكة الانترنيت وعلى أي تقنية يمكن أن تظهر مستقبلا. وهو الأمر الذي يجعله قانونا فعالا ويساير حقا التطور التكنولوجي السريع.

ومع هذا ينبغي الاعتراف بحقيقة وهي انه رغم الجهود الجبارة التي بذلها المشرع الجزائري في سبيل التصدي لظاهرة الإجرام الالكتروني، إلا أنها تبقى غير كافية لبلوغ الهدف المنشود، نظرا للتطورات السريعة والمستمرة التي تعرفها ظاهرة الإجرام الالكتروني من جهة، ونظرا للطابع العالمي والعابر للحدود الذي تتميز بها هذه الظاهر من جهة أخرى،

---

[570]- راجع المادة (05) من القانون (09-04) المؤرخ في 05-02-2009، مرجع سابق.

[571]-راجع المادتين (16 و 17) من القانون(09-04)، المرجع نفسه.

لذلك لابد من التوجه إلى التنسيق التشريعي والقضائي والأمني مع الدول العربية و لما لا مع الدول الغربية الأكثر دراية بالجرائم الالكترونية والاستفادة من خبراتها في مجال مكافحة هذه الجرائم.

المطلب الثاني

تكثيف التعاون الدولي في مجال التشريع

إن قصور التشريعات الداخلية في مواجهة الجريمة الالكترونية وعجز الدول فرادى التصدي لها بسبب طبيعتها عبر الوطنية، جعل المجتمع الدولي يقتنع بأن توحيد جهوده وحشد قواه هو الحل الأمثل لمكافحة هذا الإجرام[572].

ويعتبر التعاون بين الدول في مجال التشريع أنجع الحلول لمعالجة و تجاوز العقبات التي تعيق عملية مكـافحة الجرائـم الالكترونية، وأكثرهـا فعالـية في مجـال تعقب مرتكبي هذه الجرائم وملاحقتهم والقبض عليهم ومحاكمتهم وكذا إنزال العقاب عليهم[573].

وتتجلى أهمية هذا النوع من التعاون الدولي، فيما يحدثه من تقارب وتوافق بين التشريعات الجنائية الوطنية للدول بشقيها الموضوعي والإجرائي، وما يترتب عنه من خلق منظومة قانونية مشتركة لمكافحة ظاهرة الإجرام المعلوماتي ذات الطابع عبر الوطني، تتوحد فيها الرؤية من خلال وضع تعريف موحد للجريمة الالكترونية، تحديد الأفعال وصور النشاط

---

[572]– أنظر: قرار الجمعية الدولية لقانون العقوبات الصادر عن مؤتمرها الدولي الخامس عشر حول القواعد الإجرائية في بيئة جرائم الكمبيوتر، مشار إليه في: **زيبحة زيدان**، مرجع سابق، ص 144.

[573]–**إيهاب ماهر السنباطي**، الجرائم الإلكترونية(الجرائم السيبيرية :) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد!، بحث مقدم إلى الندوة الإقليمية حول " الجرائم المتصلة بالكمبيوتر"، المنعقدة بالرباط في 19 و 20 جويلية 2007، ص 28.

محل التجريم، والتكييف القانوني لكل فعل إجرامي والعقوبات التي تقابله، وكذا توحيد الأحكام الإجرائية التي يتم وفقها ملاحقة مرتكبي هذه الجرائم و معاقبتهم، وهو ما قد يشكل سدا منيعا لاستغلال المجرمين أوجه النقص التي تنطوي عليها تشريعات بعض الدول[574].

بغية بلوغ الهدف المنشود، سارعت بعض الدول إلى لمّ شملها وتوحيد جهودها في مواجهة الإجرام الالكتروني، وذلك من خلال مراجعة تشريعاتها الجنائية الوطنية بما يكفل التنسيق والموائمة بينها وبين تشريعات الدول الأخرى الراغبة في التعاون معها، والسعي إلى تكوين أرضية قانونية تعمل على الكفاح الدولي المشترك ضد هذا الإجرام وطرح المشاكل والحلول وإعداد مشروعات القوانين تسير على هديها الدول المشتركة، وهذه الجهود أخذت بعدا دوليا (الفرع الأول) وبعدا إقليميا (الفرع الثاني).

الفرع الأول:الجهود المبذولة على المستوى الدولي

سنركز في هذا العنصر على دراسة تجربتين ناجحتين هما، التنسيق التشريعي في إطار منظمة الأمم المتحدة (أولا)، ومنظمة التعاون والتنمية الاقتصادية(ثانيا) كمايلي:

أولا –التنسيق التشريعي في إطار منظمة الأمم المتحدة : إمانا منها بأن منع الجريمة الالكترونية و مكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم التي يخلفها، فقد كانت منظمة الأمم المتحدة من الهيئات الدولية السباقة إلى وضع خريطة طريق للتصدي للجريمة الالكترونية، والحث على تعزيز العمل المشترك والتعاون بين الدول الأعضاء من أجل الحد من انتشارها وتعاظم أثارها[575]،

[574] -**CHAWKI Mohamed**, combattre la cybercriminalité, op.cit., p 401.

[575]– **إيهاب ماهر السنباطي**، مرجع سابق، ص 29.

وذلك من خلال تنظيمها ورشات عمل دولية خاصة بمنع الجريمة ومعاملة المجرمين، وإشرافها على عقد مؤتمرات دولية في هذا المجال.

فقد كانت الجريمة الالكترونية موضع اهتمام منظمة الأمم المتحدة منذ مؤتمرها السابع الخاص بمنع الجريمة و معاملة المجرمين المنعقد بمدينة ميلانو الايطالية في 1985، أين كلّفت لجنة الخبراء العشرين بدراسة موضـــوع حماية نظم المعـالجة الآلية و الاعتـداء علـى الحاسب الآلي، وإعداد تقرير مفصل يعرض على المؤتمر الثامن الذي سيعقد فيما بعد[576].

وبالفعل عرضت نتائج هذا التقرير على المؤتمر الثامن للأمم المتحدة المنعقد بهافانا في عام 1990، وتمت الموافقة عليها ثم أصدرتها منظمة الأمم المتحدة على شكل جملة من التوصيات بخصوص الجريمة الالكترونية، أكدت فيها بأن مواجهة هذا النوع الجديد من الإجرام يتطلب من الدول الأعضاء اعتماد عدة تدابير أهمها :

ـــ ضرورة تحين وتحديث القوانين الموضوعية والإجرائية التي تتناول هذا النمط الجديد من الإجرام والعمل على تحسين أمن المعلومات والوقاية المتعلقة بالحسابات الآلية وشبكات الانترنت المتصلة بها.

ـــ وضع التدابير الوقائية والأمنية لمنع الجريمة مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.

ـــ توعية الجماهير بخطورة الجريمة الالكترونية و أهمية مكافحتها.

ـــ تنظيم دورات تدريب مكثفة لرجال القضاة و الأمن حول تقنيات و فنيات التصدي لمثل هذه الجرائم.

---

[576]– **محمد الأمني البشري** و **محسن عبد الحميد محسن**، معايير الأمم المتحدة في مجال العدالة الجنائية و منع الجريمة، أكاديمية نايف للعلوم الأمنية، رياض، 1998، ص 19.

ـ التعاون مع المنظمات المهتمة بهذا الموضوع، و إدراج أبجديات الإعلام الآلي واستخدام الحواسب ضمن المناهج المدرسية[577].

أما في عام 1994، فقد أصدرت منظمة الأمم المتحدة قانون نموذجي حول الوقاية من الجرائم الالكترونية ومكافحتها، موجه إلى مساعدة حكومات الدول في إحداث نصوص قانونية داخلية خاصة بالإجرام الالكتروني، وكذا تحين وتحديث قوانينها الموجودة حتى تواكب تطورات هذا النمط من الإجرام. وقد تضمن هذا القانون على وجه الخصوص تحديد المفاهيم الأساسية للجرائم الالكترونية، والتي قسمها إلى صنفين، الأول يتعلق بالجرائم التي تكون الوسائل الالكترونية محلا لها، أما الصنف الثاني، فيتعلق بالجرائم المرتكبة بواسطة وسائل تكنولوجية الإعلام و الاتصال أو الوسائل الالكترونية بصفة عامة[578].

وفي نفس السياق، عقد مؤتمر آخر لمنظمة الأمم المتحدة بالقاهرة في عام 1995 أهم ما خرج به هو وجوب حماية الإنسان في حياته الخاصة وملكيته الفكرية من تزايد مخاطر التكنولوجيا، وضرورة التنسيق والتعاون بين أشخاص المجتمع الدولي لاتخاذ الإجراءات المناسبة لتحقيق ذلك.

وبعد سنة تقريبا، اعتمدت لجنة الأمم المتحدة في عام 1996 قانون الانسيترال النموذجي بشأن التجارة الالكترونية، الذي يعتبر مرجعا مهما للدول في مواجهة جرائم الانترنت في مجال التجارة الالكترونية، وقد كان الهدف الرئيسي من وضع هذا القانون هو تعزيز تنسيق وتوحيد القانون التجاري الدولي بغية إزالة أية عقبات لا لزوم لها أمام التجارة الدولية تنتج عن أوجه القصور والاختلاف في القانون المتعلق بالتبادل التجاري، وأن يكون

---

[577]– **محمد طارق عبد الرءوف الحن**، جريمة الاحتيال عبر الانترانت(الأحكام الموضوعية و الأحكام الإجرائية)، منشورات الحلبي الحقوقية، دمشق، 2011، ص 118.

[578] - **KALINA (L)**, lutte contre la cybercriminalité, vers la construction d'un modèle juridique normalise, article disponible sur ; http://www.adie.sn.

نموذجاً تهتدي به البلدان فيما يتعلق بتقييم وتحديث جوانب معينة من قوانينها وممارساتها في ميدان العلاقات التجارية، ومساعدة جميع الدول على تحسين تشريعاتها وتدارك المساوئ الناجمة عن قصور التشريعات على الصعيد الوطني مع تقديمه للمشرعين الوطنيين كمجموعة من القواعد المقبولة دولياً في هذا المجال[579]. استمـرارا في هذا المسار أصدرت اللجنة ذاتها القانون النموذجي بشأن التوقيعات الالكترونية في عام 2001 باعتباره صكا قانونيا جديدا مستمد من القانون الانسيترال النموذجي بشأن التجارة الالكترونية، ومتسقاَ مع أحكامه وبشكل مفصل[580].

وتزامنا مع اتساع دائرة جرائم تكنولوجية الإعلام و الاتصال و ما صاحبها من مخاطر وأضرار، عقدت منظمة الأمم المتحدة مؤتمرها العاشر في بودابست عام 2000 [581] أسفر إلى إبرام الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية، التي ناشدت بموجبها الدول الأعضاء بوجوب تعزيز التنسيق و التعاون بين الدول من أجل الحد من جرائم تقنية المعلومات المتزايدة الناتجة عن إساءة استعمال التكنولوجيا لأغراض إجرامية، والعمل الجاد على اتخاذ التدابير المناسبة للحد من هذا النمط الإجرامي المستحدث، بالإضافة إلى إشادتها بالدور الفعال الذي يمكن أن تؤديه كل من منظمة الأمم المتحدة المنظمات الإقليمية في هذا الشأن[582].

---

[579]– **سيناء عبد الله محسن**، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، بحث مقدم إلى الندوة الإقليمية حول " الجرائم المتصلة بالكمبيوتر"، المنعقدة بالرباط في 19 و 20 جويلية 2007، ص 54.

[580]–المرجع نفسه، ص 55.

[581]- Disponible sur : http//www.un.org/News/fr-press/docs/2000/20001208.12954.doc.html.

[582]– اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم 55/63، صادرة عن هيئة الأمم المتحدة، بالجمعية العامة 81، 19 ديسمبر 2000. متاحة على الموقع الالكتروني:

http://www.unodc.org/pdf/crime/a_res_56/121f.pdf.

وفي السنة نفسها و بالتحديد في الفترة من 12 الى 15 ديسمبر 2000، عقدت منظمة الأمم المتحدة مؤتمر دولي يضم الشخصيات السياسية للحكومات المصادقة على اتفاقية الأمم المتحدة الخاصة بالجريمة عبر الوطنية، بعنوان تحديات الجريمة السيبيرانية العابرة للحدود، ومن أهم المسائل التي تمت مناقشتها في هذا المؤتمر هي، ضرورة حصر وإحصاء كل الأفعال المجرّمة التي تعد من قبيل الجرائم العابرة للحدود و إعدادها في قائمة تضع في متناول علم جميع الأعضاء حتى يتم إدراجها في نصوصها الداخلية[583].

مواصلة للجهود السابقة، عقدت منظمة الأمم المتحدة بالبرازيل في الفترة الممتدة من 12 إلى 19 أفريل 2010 مؤتمرها الثاني عشر حول منع الجريمة والعدالة الجنائية، أين دارت مناقشات عميقة بخصوص حصيلة تطورات استخدام العلم والتكنولوجيا من جانب المجرمين بالمقارنة مع المجهودات المبذولة من طرف السلطات المختصة في مكافحة الجريمة الحديثة بما فيها الجريمة الالكترونية، أضفت إلى تشكيل لجنة سميت بلجنة منع الجريمة والعدالة الجنائية، كلفت بإعداد دراسة تحليلية شاملة حول مشكلة الجريمة الالكترونية والتدابير الممكنة للتصدي لها.

وتنفيذا لهذه المهمة، دعت لجنة منع الجريمة و العدالة الجنائية إلى عقد اجتماع دولي لفريق من خبراء حكوميين مفتوح العضوية في الفترة الممتدة من 17 إلى 21 جانفي 2011، أين تولى الفريق بإجراء دراسة مفصلة لظاهرة الجريمة الالكترونية، بداية من تحليل هذه الظاهرة، جمع المعلومات والإحصائيات المتعلقة بها وتحدياتها، ثم عرج إلى إبراز مدى مواكبة التشريعات الوطنية خاصة المتعلقة بإجراءات التحقيق وجمع الأدلة الالكترونية،

---

[583]- **جان فرانسوا هنروت**، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، بحث مقدم إلى الندوة الإقليمية حول " الجرائم المتصلة بالكمبيوتر"، المنعقدة بالرباط في 19 و 20 جوان 2007، ص 102.

مسؤولية مزودي خدمات الانترنت لظاهرة الإجرام الالكتروني، ومكانة التدابير الوقائية، والتعاون الدولي والمساعدة التقنية الدولية في مواجهة هذه الجرائم، وكذا دور القطاع الخاص في الحد منها، وخلصت الدراسة بتقديم حلول مناسبة للمشكلات التي تعيق المواجهة الفعالة للجريمة الالكترونية. وقد دونت نتائج هذه الدراسة في تقرير مفصل قدم إلى أمانة منظمة الأمم المتحدة التي وضعته تحت تصرف جميع الدول الأعضاء لتستفيد منه كمرجع في التصدي للإجرام الالكتروني[584].

وفي 15 نوفمبر 2005 بمناسبة القمة العالمية لمجتمع المعلومات المنظمة تحت رعاية الأمم المتحدة، وضعت أجندة لمكافحة جرائم تقنية المعلومات سميت " **أجندة تونس**"، أكدت فيها على مسؤولية كل دولة في ملاحقة مرتكبي جرائم الانترنت، بما في ذلك العابرة للحدود، وضرورة التزامها بتوفير الوسائل القانونية والفنية الفعالة على المستوى الوطني والدولي من اجل تعزيز التعاون في ذات المجال، كما حثت الدول المشاركة على بحث صياغة تشريع توافقي الذي يسمح بإجراء تحقيقات عبر الوطنية في جرائم الانترنت والملاحقة القضائية الفعالة لمرتكبيها[585].

زيادة على جهود منظمة الأمم المتحدة من خلال مؤتمراتها التي تعنى بخلق تقارب وتواءم بين تشريعات العقابية للدول الأعضاء، من خلال إيجاد البرامج و وضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة بصفة عامة والجريمة الالكترونية بصفة خاصة، تبذل الوكالات والمنظمات العالمية العاملة تحت لواء الأمم المتحدة مجهودات لا

---

[584]– اجتماع فريق خبراء حول الجريمة الالكترونية (السيبرانية)، مشروع المواضيع المطروحة للنظر في إطار دراسة شاملة بخصوص الجريمة الالكترونية (السيبرانية) و تدابير التصدي لها، المنعقد بفينا، في الفترة الممتدة من 17 إلى 21 جانفي 2011. رقم UNOD/CCPCJ/EG4/2011/2

[585]– لمزيد من التفاصيل انظر "أجندة تونس" في الموقع الالكتروني :

http://portal.unesco.org/ci/fr/files/20687/11327544873tunis_agenda_fr.pdf/tunis_agenda_fr.pdf.

يتسهان بها في هذا المجال، نذكر منها المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في ريو دي جانيرو عام 1994، والذي خرج بالعديد من التوصيات في مجال القانون الجنائي الموضوعي، منها ما يتعلق بضرورة وضع قائمة بالحد الأدنى للأفعال المعتبرة من قبيل الجرائم الالكترونية[586]، ووجوب تحديد الجهات التي تتولى التفتيش والضبط فيها، مع ضرورة وضع القواعد المتعلقة بالإثبات الالكترونية، حجية ومصداقية الأدلة الالكترونية أمام القضاء[587].

وفي السياق ذاته، عقدت اللجنة الاقتصادية والاجتماعية لغربي أسيا التابعة للمجلس الاقتصادي و الاجتماعي تحت إشراف منظمة الأمم المتحدة ورشة عمل حول التشريعات الدولية الخاصة بالإجرام الالكتروني ومدى تبنيها وتطبيقها من طرف دول منطقة الإسكوا عام 2008، أين رصدت نتائج غير مرضية في هذا الشأن، وأوصت من خلالها هذه الدول بضرورة الإسراع إلى إدراج أحكام النماذج الناجحة من التشريعات العقابية الدولية في القوانين الداخلية، وكذا الاتجاه نحو تعزيز التعاون الدولي الثنائي والمتعدد الأطراف في مجال التشريع من أجل مواجهة أفضل لمخاطر الجريمة الالكتروني[588].

---

[586]– ومن ضمن الأفعال المقترح تجريمها، الاحتيال أو الغش المرتبط بالحاسب، التزوير المعلوماتي، أعمال التخريب والإتلاف الواقعة على الحاسب الآلي، الدخول غير المرخص إلى الحاسوب، الاعتراض غير المرخص لاتصالات الالكترونية

[587]– مشار إليه في: **محمد طارق عبد الرءوف الحن**، مرجع سابق، ص 188.

[588]– **اللجنة الاقتصادية و الاجتماعية لدول غرب أسيا (ESCWA)** ، ورشة عمل حول التشريعات المتعلقة بالجريمة الالكترونية (السبيرانية) و تطبيقها في منطقة الاسكوا، بيروت، يومي 15 و 16 ديسمبر 2008، المجلس الاقتصادي والاجتماعي التابع لمنظمة لأمم المتحدة، رقم E/ESCWA/ICTD/2009/1.

أما الاتحاد الدولي للاتصالات الذي يضم أكثر من(192) دولة و(700) شركة من القطاع الخاص والمؤسسات الأكاديمية، فانه يوفّر منبرا استراتيجيا للتعاون التشريعي والفني بين أعضائه باعتباره وكالة متخصصة داخل منظمة الأمم المتحدة، إذ سطّر الاتحاد مؤخرا مخططا دوليا لتعزيز الأمن السيبراني العالمي، وناد كل الفاعلين إلى تجسيده والعمل بمقتضاه حتى يكون لهم سندا في منع هذا النمط الجديد من الإجرام، وقد تضمن هذا المخطط سبعة أهداف رئيسية هي :

– وضع إستراتيجية لتطوير نموذج مشترك للتشريعات السيبرانية يكون قابلا للتطبيق وطنيا وعالميا.

– تهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهياكل التنظيمية والسياسات المتعلقة بالجرائم الالكترونية.

– وضع آلية عالمية للمراقبة الالكترونية والإنذار والرّد المبكر مع ضمان التنسيق عبر الحدود.

– إنشاء نظام هوية رقمي عالمي وتطبيقه، مع تحديد الهياكل التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

– تطوير إستراتيجية عالمية للإسراع في رفع المؤهلات البشرية والمؤسساتية وتعزيز المعرفة والدراية والتحسيس في مجال الإجرام المعلوماتي.

– اعتماد إطار استراتيجي عالمي لجميع الفاعلين و المهتمين بالإجرام الالكتروني من أجل التعـاون و الحوار، تبـادل المعـارف و الخبرات، والتنسيق على كـل المستويـات فـــي هذا

المجال[589].

إضافة إلى ذلك، فقد شكلت المنظمة العالمية للملكية الفكرية فريق عمل يضم عدد كبير في ميدان الإعلام الآلي والتكنولوجيات الحديثة بهدف دراسة الأساليب المناسبة لحماية برامج الحاسب الآلي من خلال إخضاعها لقوانين حماية الملكية الفكرية حق المؤلف، ولا يمكننا تجاهل مجهودات لجنة حقوق الطفل التابعة لمنظمة الأمم المتحدة التي أبرمت اتفاقية حـول حقـوق الطفـل والوقـاية مـن الجرائـم الالكترونـية التـي ترتكـب فـي حـق الطفولة، كاستغلالهم في المواد الإباحية عبر الانترنت[590].

ثانيا: التنسيق التشريعي في إطار منظمة التعاون و التنمية الاقتصادية (OCDE)

تعود أولى اهتمامات المنظمة بالجرائم الالكترونية إلى عام 1980، حينما وضعت دليل تشريعي يتضمن مجموعة من قواعد إرشادية لحماية الخصوصية و نقل البيانات عبر وسائل الاتصال الالكترونية وأوصت الدول الأعضاء إدراجها ضمن تشريعاتها الداخلية والالتزام بها، ومن بين هذه القواعد:

ـ الحق في الخصوصية مضمون، ولا يجوز الاطلاع على المعلومات الخاصة للأفراد أو إفشائها إلا في إطار القانون بعد علمهم و موافقتهم على ذلك.

ــ لا يجوز استعمال المعلومات الخاصة للأفراد لأغراض أخرى غير تلك التي تم الحصول عليها من اجلها.

---

[589]– **جورج لبكي**، المعاهدات الدولية للانترنت حقائق وتحديات، مجلة الدفاع الوطني اللبناني، عدد 83، بيروت، 2014، ص.ص 12-13.

[590]– اتفاقية حقوق الطفل، النظر في التقارير المقدمة من الدول بموجب المادة (1/12) من البرتوكول الاختياري لاتفاقية حقوق الطفل حول بيع وبغاء الأطفال في المواد الإباحية، لجنة حقوق الطفل، الدورة 57، المنعقدة من 30 ماي إلى 17 جويلية 2011، الأمم المتحدة، رقم : CRC/c/opsc/egy/co/1

ـــ ضمان أمن وحماية المعلومات الخاصة للأفراد ضد كل اختراق، ضياع، إتلاف أو تعديل، دون ترخيص[591].

وفي عام 1986 أصدر مجلس المنظمة تقريرا حول الغش الالكتروني، تم من خلاله تشخيص وضع السياسة التشريعية الجنائية القائمة لدى عدد من الدول الأعضاء في هذا المجال، واقترح قائمة تتضمن الحد الأدنى لأفعال سوء استخدام الحاسب الآلي التي يجب على الدول الأعضاء أن تجرّمها وتفرض عليها عقوبات في قوانينها الداخلية، من أهمها الاستخدام أو الولوج غير المصرح به إلى نظام الحاسب والمعلومات المخزنة داخله، الإفشاء غير المرخص به للمعلومات المعالجة آليا و نسخ أو تعديل أو إتلاف أو تخريب ما تحتويه من بيانات، الإعاقة غير المشروعة للوصول إلى مصادر الحاسب كمنع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة فيه[592].

استمرار في نفس المسار، أصدرت منظمة التعاون والتنمية الاقتصادية في عام 1992 توصية إرشادية تتضمن جملة من التدابير الفعالة لمواجهة الجرائم المرتكبة عبر الانترنت، والتي أوصت الدول الأعضاء بضرورة إدراجها ضمن قوانينها العقابية الوطنية وهي كالتالي:

ـــ تجريم التلاعب في البيانات المعالجة آليا و محوها.

ـــ منع التجسس المعلوماتي و يندرج تحته جمع، أو اقتناء، أو استعمال الغير المشروع للمعطيات الالكترونية.

ـــ حضر التخريب المعلوماتي بما فيه الاستعمال غير المشروع للحاسب الآلي، إتلافه ومكوناته المادية و المنطقية، وسرقة وقت الحاسب.

---

591 -**CHAWKI Mohamed**, combattre la cybercriminalité, op.cit., p 308.

592 -**OCDE**, la fraude liée a l'informatique :Analyse des politiques juridiques, PIIC, n 10, 1986, p 72.

ـــ تجريم الولوج و البقاء غير المرخص داخل برامج الحاسب، واعتراض استخدام المعطيات أو نقلها.

ـــ تجريم قرصنة البرامج.

زيادة على هذه الجهود، تعقد منظمة التعاون والتنمية الاقتصادية سنويا عددا من الملتقيات و ورشات عمل معمقة تعنى بمنع الجريمة الالكترونية تبحث فيها السبل الجديدة للأمن والوقاية المعلوماتية، إضافة إلى المعايير القانونية المشتركة لمواكبة تطورات هذا النوع من الإجرام[593].

الفرع الثاني:الجهود المبذولة على المستوى الجهوي

سنركز هنا على إبراز الجهود المبذولة أوروبيا في إرساء سبل التعاون التشريعي بين الدول(أولا)، ثم على مستوى الدول العربية(ثانيا)، بعدها نتوقف عند جهود مجموعة الدول الثمانية (ثالثا).

-أولا:على المستوى الأوروبي: أدى المجلس الأوروبي دورا مهما في تحقيق الانسجام بين التشريعات الوطنية للدول الأطراف في مجال مكافحة جرائم تقنية المعلوماتية، وقد تجسدت أولى جهوده في توقيع دول الاتحاد في 28-01-1981 اتفاقية رقم(108) تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية، والتي شكّلت الإطـار القانونـي المشترك لضمـان حرية تنقل البيـانـات الشخصية المعـالـجة إلكترونا و حمايتها من أي شكل من أشكال التعدي[594].

---

[593]– **صغير يوسف**، مرجع سابق، ص 97.

[594] - **QUEMENER Myriam**, conseil de l'Europe et lutte contre la cybercriminalité, Revue Expertises des systèmes d'information, Paris, Mai 2010, P 174 .

ثم في عام 1985 قام المجلس بوضع قواعد إرشادية خاصة بتحديد أنماط جرائم الحاسب ونبّه من خلالها المشرع في الدول الأعضاء إلى ضرورة حصر الأنشطة غير المشروعة المرتبطة باستخدام الحاسب الآلي، على أن تراعي في ذلك التوازن بين مواجهة الحاجة للحماية الجنائية ضد هذه الأنشطة من ناحية، و حماية الحق في المعلومات، وحقوق وحريات الأفراد المدنية من ناحية أخرى[595].

استمرار في المسار ذاته، أصدر المجلس الأوروبي في عام 1989 توصية هامة ناد من خلالها دول الأطراف إلى ضرورة تفعيل دور القانون لمواجهة مخاطر الأفعال غير المشروعة عبر الحاسب[596]، وهي التوصية التي ألحقها في عام 1995 بتوصية أخرى حول مشاكل الإجراءات الجنائية المتعلقة بالجرائم الالكترونية[597]. حث فيها الدول الأعضاء بمراجعة قوانين الإجراءات الجنائية الوطنية لتتلاءم مع التطور الحاصل في هذا المجال، آخذتا بعين الاعتبار النقاط التالية:

ـ توضيح إجراءات تفتيش أجهزة الحاسب الآلي وضبط المعلومات التي تحتويها ومراقبة انتقال المعلومات عبر وسائل الاتصال الالكترونية، والسماح بممارستها وفقا لذات الشروط و الضمانات الخاصة بإجراءات التفتيش العادية.

ـ الاعتراف للجهات المختصة بالتفتيش إذا دعت الضرورة، بمدّ عملية التفتيش إلى أنظمة الحاسب الآلي الأخرى المتصلة بالنظام محل التفتيش داخل دائرة اختصاصهم، وضبط ما بها من معلومات و بيانات.

---

595 - **EL CHAER NIDAL**, op cit, p 312 .

596 -http://europa.eu.int/abc-en.htm – Recommandation-(1989/9) on computer-related crime.

597 -**Recommandation N (95) 13** relative aux problèmes de la procédure pénale lies a la technologie de l'information, adoptée par le comité des ministres du conseil de l'Europ le 11 septembre 1995, Edition du conseil de l'Europ, 1995.

ـ الموازنة بين المعلـومـات والبيانـات الالكترونية الـواردة علـى أجهزة الحـاسب الآلـي والوثائق التقليدية من حيث إجراءات التحقيق المطبق عليها.

ـ السماح بتطبيق إجراءات المراقبة والتسجيل لأغراض التحقيق الجنائي على تقنية المعلومات كلما دعت الضرورة لذلك. وفي حالة جمع المعلومات بطريق المراقبة والتسجيل، يجب مراعاة معايير احترام الخصوصية و سرية المعلومات، والحصانات المقررة لذلك.

ـ إعطاء جهات التحقيق سلطة توجيه أوامر، لكل من يحوز أشياء أو معلومات تخص نظام أجهزة الحاسب الآلي(دخول، تشغيل برامج أو قواعد بيانات) تفيد الكشف عن الحقيقة بتسليمها لها.

ـ إلزام متعاملين خدمات الاتصال الحكومية و الخاصة بالتعاون مع سلطات التحقيق وتقديم لهم يدّ المساعدة بخصوص التحقيق.

ـ تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية(جمع الأدلة، المحافظة عليها، تقديمها، حجيتها) على الأدلة الالكترونية، والسعي إلى تطوير وتوحيد أنظمة التعامل مع الأدلة الالكترونية حتى يتم الاعتراف بها بين كل دول الأعضاء.

ـ ضرورة تشكيل وحدات أمن خاصة لمكافحة الجرائم الالكترونية، وإعداد برامج تدريبية خاصة، لتأهيل العاملين في العدالة الجنائية وتطوير معارفهم وخبراتهم في مجال التقنية المعلوماتية.

ـ اعتماد سياسة واضحة و فعالة حول التعاون المتبادل والمساعدة القضائية والفنية بين الدول في مجال مكافحة الجريمة الالكترونية، من خلال تبني إجراءات التحقيق والمتابعة الجزائية سريعة ومناسبة، وخلق قنوات اتصال ثنائية أو متعددة الأطراف تسمح للسلطات القائمة على التحقيق، الاتصـال بسهـولة بمثيلتها الأجنبية والتنسيق معها. أو التدخل السريـع

للتحقيق في إقليم دولة أجنبية دون أن يشكل ذلك مساسا بسيادة هذه الدولة.

تجسيدا للمبادئ التي تضمنتها هاته التوصيات، كلّف المجلس في فيفري عام 1997 لجنة خبراء بإجراء دراسة معمقة حول الجريمة الالكترونية وإعداد مشروع اتفاقية عامة ملزمة حول ذلك[598]، توجت بوضع اتفاقية أوروبية لمكافحة الجرائم الالكترونية بالتعاون مع الولايات المتحدة الأمريكية، كندا، اليابان، وجنوب إفريقيا، عرضت للتوقيع في بودابست في عام 2001 بمناسبة المؤتمر الدولي حول الإجرام الالكتروني، ودخلت حيز التنفيذ في عام 2004. وهي متاحة الانضمام لجميع دول العالم.

وتمثل هذه الاتفاقية دليلا إرشاديا لتطوير التشريع الجزائي في مجال الجرائم الالكترونية، الهدف منها توحيد التدابير التشريعية بين الدول الأطراف و التأكيد على أهمية التنسيق والتعاون الإقليمي والدولي في ميدان مكافحة الإجرام الالكتروني، وكذا تحقيق التوازن بين حقوق الإنسان والإجراءات المتخذة لمواجهة هذا النوع من الإجرام[599]. وقد تضمنت هذه الاتفاقية 48 مادة غطت في مضمونها ثلاث أقسام كبرى هي:

ـ **القسم الأول:** تناول قائمة الجرائم الالكترونية التي حددت في أربعة طوائف رئيسية هي كالتالي:

1- الطائفة الأولى: تتضمن الجرائم التي تستهدف عناصر أمن المعلومات وهي، الجرائم ضد السرية والسلامة وإتاحة البيانان ونظم الحاسب وتشمل جريمة الولوج غير

---

[598]- **حسين بن أحمد الشهري**، قانون دولي موحد لمكافحة الجرائم الالكترونية، المجلة العربية للدراسات الأمنية والتدريب، مجلد 27، عدد 53، صادر في 2010، ص 41.

[599]- **كريستينا سكولمان**، المعايير الدولية المتعلقة بجرائم الانترنت (مجلس أوروبا)، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، في الفترة من 19-20 جوان 2007، ص 62.

المشروع، جريمة الإتلاف غير المشروع للنظم أو البرامج أو بيانات الحاسب، جريمة المراقبة أو الاعتراض غير المشروع.

2- الطائفة الثانية: تضّم جريمة الغش المعلوماتي و جريمة التزوير المعلوماتي.

3- الطائفة الثالثة: تتعلق بالجرائم المرتبطة بالمحتوى وهي، جريمة الإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية.

4- الطائفة الرابعة: تتضمن جرائم الاعتداء على الملكية الفكرية و الحقوق المجاورة[600].

ـــ **القسم الثاني:** تضمن القواعد الإجرائية المناسبة لمواجهة الجرائم الالكترونية، عبر مختلف مراحل المتابعة الجزائية، خاصة مرحلة التحري والاستدلال، من ثمة التحقيق، بحيث تتصل هذه القواعد بتنظيم عملية جمع الأدلة الالكترونية، تدابير الحماية الوقائية للنظم المعلوماتية، وتسليم معطياته المخزنة وإجراءات حفظها، والقواعد المتعين اتخاذها بشأن تفتيش وضبط وجمع المعطيات الالكترونية واعتراض المعلومات، وإصدار الأوامر بتسليمها أو إنتاجها أو إتلافها.

وفي القسم نفسه، أوجبت الاتفاقية على الدول الأعضاء، اتخاذ التدابير التشريعية الملائمة التي تمكّن السلطات المختصة بالتحقيق القيام بالمهام التالية:

ـ إصدار أوامر، أو الحصول على أوامر مستعجلة من الجهات المختصة، للقيام بحفظ بيانات معينة من الحاسب الآلي، بما فيها بيانات المرور، أو المتناقلة التي تحفظ داخل نظم الحاسب الآلي، خاصة المعرّضة منها للفقد أو الإتلاف أو التعديل[601].

---

[600]- **هلالى عبد الله أحمد**، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، مرجع سابق، ص.ص 24-37.

[601]- أنظر المادتين (16 و 17)من اتفاقية بودابست 2001 .

ـ توجيه أوامر للجهات المهنية بحفظ البيانات المخزنة في أنظمة الحاسب الآلي، وقواعد البيانات المتواجد ضمن إقليمها، ولجهات تزويد خدمات الانترنت، التي تمارس نشاطها على إقليم الدولة العضو، لتقديم المعلومات التي في حوزته أو تحت سيطرته المتعلقة بالمشترك، وأية معلومات تخص حركة البيانات التي من شانها، أن تبيّن نوع خدمة الاتصال، مصدرها، وقت و مدة الخدمة، هوية الاشتراك، موقع تجهيزات الاتصـال، المتوفرة على أساس عقد أو اتفاق تقديم خدمة[602].

ـ الدخول لغرض التفتيش إلى أي نظام حاسب آلي، أو أي جزء منه، و إلى البيانات المحزنة فيه، وكذلك إلى أية واسطة أو وسيلة تخزن فيها البيانات، الموجود ضمن النطاق الإقليمي للدولة[603].

ـ الوصول إلى المعلومات للتثبت من مشروعيتها، بها في ذلك تتبع المعلومات إلى الأنظمة الأخرى و الدخول إليها عن بعد[604].

ـ ضبط البيانات محل التفتيش، أو ضبط نظام الحاسب الآلي كله، أو جزء منه، أو الواسطة التي خزنت فيها البيانات، وعمل نسخة من هذه البيانات، ضمان سلامة البيانات المخزنة، وإزالة البيانات المانعة من دخول نظام الحاسب الآلي.

ـ الاستعانة بذوي الخبرة و المعرفة في مجال الإعلام الآلي، من أجل الحصول على المعلومات الضرورية الخاصة بتقنيات تشغيل وتأمين نظم الحاسب الآلي محل التفتيش، والتي تمكنها من القيام بمهامها على أحسن وجه[605].

---

[602]– أنظر المادة(18) من الاتفاقية نفسها.

[603]– أنظر المادة(1/19) فقراتها (أ، ب) من الاتفاقية نفسها

[604]– أنظر المادة (2/19) من الاتفاقية نفسها.

ـ جمع أو تسجيل البيانات المارة بوسائل اتصال الكترونية موجودة على إقليم دولتها، وإجبار مقدمي الخدمات بتجميع و تسجيل البيانات المارة عبر وسائل الاتصال الالكترونية الموجودة في أراضيهم، والتي أرسلت بواسطة نظام معلوماتي[606].

–**القسم الثالث:** تناول موضوع التعاون الدولي بين الأعضاء الموقعة على الاتفاقية لمواجهة جرائم المعلوماتية عابرة الحدود والذي قسّم إلى فصلين هما:

– الفصل الأول : خصص للتعاون القضائي بين الدول الأطراف في تطبيق الأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية، الاتفاقيات المعتمدة على التشريعات المماثلة أو النظيرة و القوانين المحلية، وهذا التعاون يشمل ثلاثة محاور هي تدابير تسليم المجرمين[607]، والمبادئ العامة التي تحكم الالتزام بالمساعدة القضائية المتبادلة، وكذا إجراءات طلب المساعدة القضائية المتبادلة في ظل غياب اتفاقيات دولية مطبقة، و وجود قيود متعلقة بسرية و تحديد الاستخدام[608].

–أما الفصل الثاني: فخصص للتعاون الأمني الفني المتبادل بين سلطات إنفاذ القانون التابعة للدول الأطراف، وتضمّن ثلاث محاور هي على التوالي، محور المساعدة المتبادلة في مجال الإجراءات الوقتية العاجلة، كتلك المتعلقة بالتحفظ العاجل على بيانات معلوماتية مخزنة في نظام معلوماتي متواجد داخل إقليم طرف آخر، وبالإفشاء العاجل لسرية بيانات المرور المتحفظ عليها في إقليم دولة أخرى[609]. ومحور المساعدة الفنية المتبادلة في مجال

---

[605]– أنظر المادة(3/19و4) من اتفاقية بودابست 2001.

[606]– أنظر المادة(20) من الاتفاقية نفسها.

[607]–أنظر المادة (24) من الاتفاقية نفسها.

[608]– أنظر المادتين (25 و 26) من الاتفاقية نفسها.

[609]– أنظر المادتين (29 و 30) من اتفاقية بودابست 2001.

إجراءات التحقيق، كالمساعدة المتبادلة الخاصة بالوصول أو الولوج إلى البيانات المعلوماتية المخزنة في الخارج، والمساعدة الخاصة بالتجميع في الوقت الفعلي لبيانات المرور واعتراض بيانات المحتوى في الخارج[610]. ومحور ثالث يخص إنشاء شبكة طوارئ دائمة لتفعيل المساعدة الأمنية المتبادلة، يطلق عليها الشبكة (7/24) وهي، شبكة اتصال تعمل علـى مدار (24) ساعة يوميا وبمعدل (7) أيام في الأسبـوع بغرض توفير المسـاعدة الفورية لإجراءات التحقيق المتعلقة بالجرائم الالكترونية[611].

ولا تعتبر اتفاقية بودابست المجهود الوحيد الذي بذله المجلس الأوروبي في هذا المجال، بل بذل جهود عديدة أخرى أهمها اتفاقية التعاون المتبادل في مجال قانون العقوبات بين الدول الأعضاء في الاتحاد الأوروبي، التي سعت من خلالها هذه الدول إلى توحيد تشريعاتها العقابية الوطنية أو على الأقل تقريب بعضها البعض[612]. وكذا قرار إطار (decision cadre) رقم JAI /68/2004 المتعلق بمكافحة الاستغلال الجنسي للأطفال وإقحامهم في النشاطات الإباحية عبر الانترنت، المدعم في 22 ماي 2007 بتوصية تحت عنوان " **نحو اعتماد سياسة عامة في مجال مكافحة الجريمة الالكترونية**"، التي حدد فيها ثلاث أولويات هي كالتوالي، تحقيق أكبر قدر ممكن من التناسق بين التشريعات الوطنية للدول الأعضاء في هذا المجال، ضمان التعاون العابر للحدود بين أجهزة إنفاذ القانون، والتعاون بين القطاع العام و الخاص. وقد التزمت اللجنة الأوروبية بتحقيق هذه الأولويات

---

[610]– أنظر المواد من(31 و 34) من الاتفاقية نفسها.

[611]– أنظر المادة(35) من الاتفاقية نفسها.

[612]– مشار إليها في جان فرانسوا هنروت، مرجع سابق، ص 107.

في أقرب الآجال وذلك بالتنسيق مع الدول الأعضاء من جهة، وبالتعاون مع الهيئات الدولية التي تبدي استعداد في هذا الشأن من جهة أخرى[613].

ولا يعد القرار الإطار رقم JAI /222/2005 حول الاعتداءات التي تشن على نظم المعلومات الصادر عن المجلس الأوروبي بتاريخ 17 جانفي 2005 أقل أهمية من الأول[614]، إذ بمقتضاه ألزم المجلس الدول الأعضاء بتوحيد نصوصها الجنائية التي تجرّم وتعاقب على أفعال الاعتداء التي تمس الأنظمة المعلوماتية، كأفعال القرصنة، كسر كلمة السر، كشف كلمات المرور، والهجمات بواسطة الفيروسات الالكترونية ...الخ. وأوصاها بضرورة تأسيس حيز للتعاون الدولي في مجال مكافحة هذه الجرائم على مستوى الأوروبي، و وضع أرضية أوروبية للتكوين و التدريب الجيد لرجال العدالة الجنائية و إنفاذ القانون في هذا المجال.

وفي الفترة ما بين 2010 و 2014 وضع المجلس الأوروبي مخطط عمل شامل مشترك، حدد الإستراتجية التشريعية والأمنية التي يجب على جميع الدول الأعضاء إتباعها سواء على المستوى الوطني أو على المستوى الأوروبي للتصدي لظاهرة الإجرام الالكتروني المعلوماتي[615]. وقد ساهم هذا المخطط بشكل كبير في توحيد السياسة الجنائية التشريعية بين دول الاتحاد الأوروبي في مواجهة تحديات الجرائم الالكترونية، وخلق مناخ للتعاون المشترك فيما بينها في هذا الشأن.

---

[613] -**QUEMENER Myriam. et CHARPENEL Yves**, cybercriminalité droit pénal applique, op.cit. p 230.

[614]– قرار المجلس رقم (JAI/222 / 2005)، مؤرخ في 24 فبراير2005، يتعلق بالهجمات التي تُشَنُّ على نظم المعلومات، الجريدة الرسمية للاتحاد الأوروبي، 16 مارس2005 .

[615] - **QUEMENER. Myriam et CHARPENEL Yves**, cybercriminalité droit pénal applique, op.cit.p 231.

-ثانيا- على مستوى الدول العربية: إن أبرز ما يمكن ذكره بخصوص الجهود العربية المبذولة في سبيل تحقيق التقارب والتوافق بين النصوص العقابية و الإجرائية الوطنية التي تعنى بالإجرام الالكتروني، القرار رقم (495) المتضمن القانون العربي النموذجي لمكافحة الجريمة الالكترونية، الذي اعتمدته جامعة الدول العربية عبر مجلس وزراء العدل العرب في دورته التاسعة عشر المنعقدة بتاريخ 08-10-2003[616]. بحيث يمثل هذا القانون القواعد الأساسية الإرشادية التي يمكن أن يستعين بها المشرع في الدول العربية عندما يريد سنّ نصوص وطنية بخصوص الجرائم الالكترونية، سواء باستحداث قوانين خاصة بذلك أو تحيين قوانينه القائمة. وقد تضمن هذا القانون (27) مادة موزعة على أربعة أبواب، عالج الباب الأول الجرائم الالكترونية و العقوبات المقررة لها، تم النص عليها في المواد من(3 إلى 22) و يمكن تلخيصها فيما يلي:

ـ جريمة الولوج غير المشروع إلى موقع أو نظام معلوماتي، والتلاعب في بياناته

ـ جريمة تزوير المستندات المعالجة في نظام معلوماتي و استعمالها.

ـ جريمة الإدخال المؤدي إلى إيقاف أو تعطيل نشاط الشبكة المعلوماتية، أو إتلاف البرامج أو البيانات فيها.

ـ جريمة التصنت واعتراض المراسلات عبر الشبكة المعلوماتية.

ـالجرائم المخلة بالآداب العامة والنظام العام وأمن الدولة عبر الشبكة المعلوماتية[617].

---

[616]- متاح في الموقع الالكتروني: http//Arabic.justice.dz/liguearabe/loi.emir ar crimtech info.pdf.

[617]- **عبد الفتاح بيومي حجازي**، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006، ص 10.

وتناول الباب الثاني، التجارة و المعاملات الالكترونية. أما الباب الثالث فقد تناول تدابير حماية حقوق الملكية الفكرية عبر الوسائل الالكترونية، في حين عالـج البــاب الرابــع الجوانب الإجرائية المتعلقة بالجرائم الالكترونية[618].

ونظرا لأهمية القانون العربي لمكافحة جرائم الإنترنت، فقد حث المؤتمر الإقليمي للدول العربية حول جرائم الإنترنت من خلال عدة توصياته[619]، الدول العربية على استخدام هذا القانون كنموذج يمكن أن يساعدهم في وضع قانون وطني فيما يتعلق بجرائم الإنترنت، ويساعدهم في الوقت نفسه على تجسيد تقارب وتلاؤم بين هذه القوانين الوطنية بعضها البعض.

ومع ذلك ، لم يلقى هذا القانون أي اهتمام من قبل معظم الدول العربية بسبب تركيزه على الجوانب الموضوعية للجريمة الالكترونية فقط، من خلال رسم أطر عامة حول ضوابط استخدام وأمن تقنية المعلومات عن طريق تحديد أهم النشاطات الإجرامية التي يمكن أن توظّف شبكة المعلوماتية والحاسبات عموما فيها، مقابل إهماله للأحكام الإجرائية الضرورية لملاحقة مثل هذه الجرائم، إذ لم يتعرض مثلا لمسالة الاختصاص القضائي بشكل واضح، ولم يشير إلى إخضــاع البيانات والمعلومات لإجـراءات التحقيق، ولـم يتعرض كذلـك للدليل

---

[618]– للمزيد من التفاصيل انظر: **سليمان أحمد فضل**، مرجع سابق، ص 437.

[619]– نذكر منها التوصية رقم (1) الصادرة عن المؤتمر الإقليمي للدول العربية حول جرائم الإنترنت المنعقد في الدار البيضاء بتاريخ 19و 20 جوان 2007، متاحة باللغة العربية على الموقع:

http://www.arab-niaba.org/publications/crime/casablanca/recommendations-a.pdf.

والتوصية رقم (2) الصادرة عن المؤتمر الإقليمي للدول العربية حول جرائم الإنترنت المنعقد في القاهرة بتاريخ 26 و 27 نوفمبر 2007 متاحة باللغة العربية على الموقع:

http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_Arabic.pdf.

الالكتروني و ضوابط قبوله و حجيته.

ومن أجل تعزيز ما جاء في القانون العربي النموذجي لمكافحة الجريمة الالكترونية من أحكام موضوعية من جهة، وتدارك الفراغ الذي تخلله في الجانب الإجرائي من جهة أخرى، أبرمت جامعة الدول العربية بتاريخ 21 ديسمبر 2010 الاتفاقية العربية لمكافحة جرائم التقنية المعلوماتية[620]، أكدت في ديباجتها على الحاجة الملحة إلى تبني اتفاقية إقليمية ملزمة تأسس لسياسة جنائية مشتركة بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وتعزيز التعاون و تدعيمه فيما بينها لدرء أخطار هذه الجرائم حفاظا على أمنها ومصالحها وسلامة مجتمعاتها وأفرادها.

وقد تضمنت هذه الاتفاقية خمسة فصول، خصص الفصل الأول لتعريف بعض المصطلحات، وتحديد نطاق تطبيق أحكام الاتفاقية، وكذا موقفها اتجاه سيادة دول الأطراف[621]. في حين خصص الفصل الثاني لحصر الأفعال أو السلوكيات التي تعد من قبيل الجرائم الالكترونية، وهي عموما نفسها الأفعال المنصوص عليها في القانون العربي النموذجي المذكور آنفا[622]. أما الفصل الثالث فقد تضمن أهم إجراءات التحقيق و الإثبات الجنائي في جرائم تقنية المعلومات، كإجراءات التفتيش عن بعد في البيئة المعلوماتية، إجراءات ضبط وتأمين بيانات تقنية المعلومات، إجراءات اعتراض و مراقبة المراسلات

---

[620]– أنظر الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 في الموقع الالكتروني التالي:

Www.arablegalnet.org.

[621]– أنظر المواد من(01 الى 04) من اتفاقية جرائم تقنية المعلومات لعام 2010، مرجع سابق.

[622]– أنظر المواد من (05 إلى 21) من الاتفاقية نفسها.

الالكترونية، الجمع و التسجيل الفوري لبيانات المحتوى وبيانات المرور المتعلقة بالاتصالات عبر وسائل تقنية المعلومات[623].

بينما تناول الفصل الرابع، أحكام التعاون القانوني والقضائي بين الدول الأطراف لمواجهة جرائم تقنية المعلومات، وقد اشتمل عدة صور للتعاون أبرزها تمديد الاختصاص، إذ من خلالها يجوز لأية دولة طرف في الاتفاقية مدّ اختصاصها القضائي في الجرائم المنصوص عليها في هذه الاتفاقية إلى أقاليم دول الأطراف أخرى، والتعاون في تسليم وتبادل المجرمين المعلومتيين بين الدول الأطراف، سواء في إطار معاهدات التبادل أو خارجها، المساعدة الفنية المتبادلة لأغراض التحقيق وجمع الأدلة في الجرائم المعلوماتية، كالمساعدات المتبادلة بين دول الأطراف في مجال البحث أو ضبط أو تأمين أو كشف أو الحفظ العاجل أو الجمع الفوري لبيانات مخزنة في أنظمة معلوماتية تقع خارج الإقليم الوطني، أو المساعدات المتبادلة المتعلقة بالوصول عن بعد إلى معلومات الكترونية مخزنة في نظم معلوماتية متواجدة خارج الإقليم الوطني.

وفي ختام الفصل الرابع ألزمت الاتفاقية الدول الأطراف بإنشاء على إقليمها جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية والمشورة المتبادلة فيما بينها لأغراض التحقيق أو نقل الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الالكتروني فيها[624]. أما الفصل الخامس و الأخير فتناول الأحكام الختامية.

الجدير بالذكر، أنه إذ كانت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تشكل نموذجا موفقا، يمكن للدول الأطراف الاعتماد عليه لتوحيد تشريعاتها الجزائية الوطنية في مجال الجرائم الالكترونية، أو على الأقل لتحقيق التقارب فيما بين هذه التشريعات، إلا أنها

---

[623]– أنظر المواد من (22 إلى 29) من الاتفاقية نفسها.

[624]– أنظر المواد من (30 إلى 43) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

وللأسف الشديد بقيت حبر على ورق ولم تدخل حيز التنفيذ إلى يومنا هذا بسبب عدم بلـوغها النصاب القانونـي المقرر لذلك، والمتمثل في التصديق عليـها من طـرف سبع دول عربية على الأقل[625].

ثالثا ـ على مستوى مجموعة دول الثمانية(G8)

تعتبر هذه المجموعة حيزا خصبا للدراسات العلمية والتطبيقية الناجحة في شتى الموضوعات التي تهم الدول الأطراف، فهي تقوم على فكرة تبادل قادة هذه الدول وجهات النظر والمعارف في المسائل ذات الاهتمام المشترك لبلورة إستراتيجية أو خطة عملية موحدة لمواجهة كل ما من شانه التهديد أو التأثير بالمصلحة الخاصة أو المشتركة لدول المجموعة.

وفي موضوع مكافحة الجرائم الالكترونية، أجرى وزراء العدل و الداخلية التابعين لدول مجموعة الثمانية عدة دراسات متخصصة في الموضوع انتهت كلها إلى وضع خطط عمل مشتركة تعتمد عليها الدول الأطراف للتصدي لظاهرة الإجرام الالكتروني، نذكر منها خطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الحاسب الآلي لعام 1997، والتي تضمنت المبادئ التي يمكن على أساسها إنشاء شبكة نقاط اتصال وتبادل معلومات وطنية تعمل على مدار (24سا/ 24سا)، وآليات إنشاء شبكة متابعة لتقديم تقارير دورية حول مدى

---

[625]– تنص الفقرة (03) من الفصل الخامس من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 على انه " **تسري هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية**" غير أنها لم تحض إلى يومنا هذا إلا بتصديق ستة (06) دول هي: دولة الإمارات العربية المتحدة في 21-09-2011، دولة قطر في 24-05-2012، المملكة الأردنية في 08-01-2013، دولة فلسطين في 21-05-2013، دولة قطر في 24-05-2013، جمهورية السودان في 15-07-2013، و دولة الكويت في 05-09-2013.

التزام الدول الأعضاء في الشبكة. وقد أنشئت بالفعل هذه الشبكة على غرار نموذج منظمة الأنتربول في عام 1999 [626].

وفي عام 2000 اثر المؤتمر الذي عقدته بباريس، اعتمدت مجموعة دول الثمانية خطة عمل لحضر إتاحة ملذات آمنة للمعتدين على تكنولوجية الإعلام والاتصال، وتعقب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية، وقد سايرت في ذالك محاولات وجهود المجلس الأوروبي في مجال الجريمة المعلوماتية[627].

وقد تواصلت جهود المجموعة في هذا الشأن، إذ سطّرت خطة عمل أخرى في عام 2001 تناولت فيها الأدوات الإجرائية الضرورية للحد من الجريمة الالكترونية، خاصة السريعة منها كالحفظ العاجل للبيانات الالكترونية، تسجيل البيانات في وقتها الفعلي، الحصول على البيانات الالكترونية المخزنة خارج حدود الدولة. وفي عام 2002 وضعت مبادئ توافر البيانات المعلوماتية الأساسية لحماية السلامة العامة، وفي السنة نفسها أصدرت بيان تؤكد فيه أن الحماية الفعالة ضد الجرائم ذات التقنية العالية تتطلب الاتصال والتنسيق والتعاون داخليا ودوليا بين جميع المعنيين في القطاع الخاص والأوساط الأكاديمية والمؤسسات العمومية[628].

بالإضافة إلى ما سبق، فقد صدرت مجموعة دول الثمانية عدة توصيات بخصوص الجريمة الالكترونية[629]، تحثّ في مجملها الدول الأعضاء على مايلي:

---

[626] - **QUEMENER Myriam et Yves CHARPENEL**, cybercriminalité droit pénal applique, op.cit.p 237.

[627]– **جورج لبكي**، مرجع سابق، ص 08.

[628]– المرجع نفسه، ص 09.

[629]– أنظر هذه التوصيات في الموقع الالكتروني التالي:

www.canadainternationalgc.ca/G8/.

ــ السهر على توحيد تشريعاتها العقابية والإجرائية الوطنية فيما يتعلق بجرائم التكنولوجيا الحديثة والجرائم ذات الصلة بالحاسب الآلي.

ــ تكثيف سبل التعاون الدولي لمكافحة الجرائم الالكترونية والتنسيق بين الدول لتجاوز العقبات و معالجة المشاكل المتعلقة بالتحقيقات القضائية في هذه الجرائم.

ــ اتخاذ تدابير وقائية وأخرى رادعة لمنع الجريمة الالكترونية.

ــ العمل الدءوب على اقتناء التكنولوجيات الملائمة والتطوير المستمر للخبرات والقدرات الفنية في مجال التحقيق والادعاء العام، وتشجيع البحث العلمي والتطبيقي في هذا المجال من أجل زيادة فعالية تقنيات تطبيق القانون.

ــ تشجيع التعاون في مجال تطوير الاستراتيجيات المناسبة لرفع الوعي العام في هذا الشأن، مع التقييم المستمر لبرامج المكافحة والوسائل القانونية المتبعة.

تجدر الإشارة إلى، أن جهود مجموعة دول الثمانية وإن كانت لا تشكل في مجملها إطارا تشريعيا ملزما للدول الأعضاء، إلا أنها قد تمثل أرضية مناسبة لبعث التعاون والتنسيق بين الدول الأطراف في مجال مكافحة الجريمة الالكترونية، ومساعدة حكوماتها على تطوير نموذج مشترك للتشريع الالكتروني يكون قابلا للتطبيق محليا ودوليا بالتوازي مع التدابير القانونية الوطنية و الدولية المعتمدة.

المبحث الثاني

الحلول القضائية المقترحة لتدارك عقبات التحقيق في الجرائم الإلكترونية

إذا كان للحلول التشريعية أهمية قصوى في رفع العقبات التي يثيرها البحث والتحقيق في الجرائم الالكترونية، بالنظر لما توفره من مشروعية وفعالية للسلطات القائمة على التحري والضبط والمحاكمة في نشاطاتها ذات الصلة بالسلوك الاجرامي الالكتروني، فان الحلول القضائية بدورها لا تقل أهمية، لأنها تهتم بتجسيد الحلول القانونية في أرض الواقع ونقلها من دائرة التجريد القانوني إلى التطبيق العملي ومن حالة السكون إلى حالة الحركة الفعالة.

وإذا كانت الحلول التشريعية قد ارتبطت بشكل عام بالعقبات التي تثيرها عملية التحقيق في الجريمة الالكترونية الوطنية، التي تكتمل كافة أركانها على إقليم دولة معينة، فان الحلول القضائية التي نقترحها ترتبط أكثر بالمشكلات الإجرائية والعملية التي تطرحها الجريمة الالكترونية عبر الوطنية التي تمتد أركانها وأثارها إلى خارج حدود الإقليم الوطني، ما يجعل هذه الحلول إحدى الضروريات اللازمة لمواجهة هذا النمط من الإجرام.

وتتجلى هذه الحلول، في تعزيز التعاون الدولي القضائي بصوره المختلفة، باعتباره أحد التدابير التي تضمن المساعدة المتبادلة والتنسيق المشترك بين سلطات العدالة الجنائية التابعة لدول مختلفة في مواجهة الجريمة الالكترونية(المطلب الاول). وفي الاستعانة بالتدابير الوقاية والحماية الأمنية، باعتبارها إحدى التدابير المانعة من ارتكاب الجرائم الالكترونية أو التي تحدّ من الآثار الضارة المترتبة عنها (المطلب الثاني).

المطلب الأول

تعزيز التعاون القضائي الدولي

من العقبات الشائعة التي تواجه عملية التحقيق في الجرائم الالكترونية، احترام سيادة الدول ومشاكل الحدود والولايات القضائية، وذلك راجع إلى الطابع العابر للحدود الذي تتميز به هذه الجرائم. ولعل من الحلول الناجعة التي وجدتها الدول لتجاوز هذه العقبات وتحقيق التوافق بين حرية كل دولة في ممارسة اختصاصها الجنائي على كافة حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب، تعزيز التعاون والمساعدة القضائية المتبادلة فيما بينها.

فالتعاون القضائي ينبع من الضرورة ذاتها التي ينبع فيها التعاون التشريعي، وفعالية التحقيق والملاحقة القضائية في الجرائم المعلوماتية غالبا ما تقتضي الحاجة إلى مساعدة من سلطات دولة منشأ الجريمة، أو من سلطات الدولة التي عبر من خلالها السلوك الإجرامي للوصول إلى الهدف أو النتيجة، أو حيث توجد أدلة الجريمة. كما أن الأحكام والقرارات التي تصدر من الهيئات القضائية بالنسبة لهذه الجرائم لا تسري على إقليم دولة أخرى ولا ترتّب أي أثر قانوني ما لم تعترف بها هذه الأخيرة، وعليه فلا تتأتي هذه الأمور إلا في إطار التعاون القضائي الدولي المتبادل.

وقد يأخذ التعاون القضائي الدولي في مجال مكافحة الجرائم الالكترونية مظهرين، الأول يتعلق باتخاذ جملة من التدابير والآليات المشتركة ذات الطبيعة الأمنية والفنية التي تضمن منع الجريمة أو الكشف عنها في مرحلة التنفيذ أو ما يسمي بالمساعدة الأمنية والفنية (الفرع الأول). أما الثاني فيتعلق بإجراءات إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة وهو يدعى بالمساعدة القضائية الدولية (الفرع الثاني).

الفرع الأول: تدعيم المساعدة الأمنية والفنية المتبادلة بين الدول

اثبت الواقع بأن أية دولة مهما بلغت قوتها ودرجة تطورها لا تستطيع بمفردها القضاء على الجرائم المعلوماتية العابرة للحدود، لأن سلطاتها الأمنية عادة ما تصطدم بمبدأ احترام سيادة الدولة و اختصاصها القضائي الذي يقف حجر عثرة أمام اكتشاف هذه الجرائم وتعقب المجرمين وكذا متابعتهم خارج حدود الإقليم الوطني. لذا فالسبيل في ذلك هو خلق فظاءات تعاون وقنوات اتصال أجهزة الشرطة فيما بين الدول و تنسيق العمل الأمني بعضها مع البعض عن طريق إنشاء هيئات أمنية إقليمية ودولية مشتركة (أولا)، وخلق فظاءات أخرى لتبادل الخبرات والمهارات الفنية في هذا المجال عن طريق عقد دورات تدريبية لمواكبة التطور السريع الحاصل في ميدان الجرائم المستحدث ذات البعد الدولي(ثاني).

أولا ــ تفعيل التعاون الأمني أو الشرطي الدولي: يعتبر التعاون الشرطي مظهر من مظاهر التعاون الدولي الذي تسعى من خلاله الدول إلى تجاوز الصعوبات التي تطرحها عملية البحث والتحري وجمع الأدلة خارج الإقليم الوطني بخصوص الجرائم الالكترونية العابرة للحدود، ويتجسد هذا التعاون في إنشاء هيئات أمنية دولية وإقليمية مشتركة تضمن الاتصال المباشر بين سلطات الأمن في الدول والتبادل السريع للمعلومات بخصوص الجرائم المرتكبة والمجرمين، وتوفر المساعدة و التنسيق فيما بينها من اجل تحقيق أهداف لا قبل للشرطة الإقليمية بتحقيقها[630]. ومن أبرز هذه الهيئات على هذا الصعيد نذكر مايلي:

[630] -**HABHAB Mohamed Ahmed,** op cit., p 274 .

1ـ دور المنظمة الدولية للشرطة الجنائية(INTERPOL)في دعم التعاون الأمني

تعتبر المنظمة الدولية للشرطة الجنائية أحسن نموذج للتعاون الشرطي[631]، فهي تمثل أكبر شبكة اتصالات لتبادل المعلومات الأمنية على المستوى العالمي، الهدف منها تعزيز وتشجيع المساعدة المتبادلة بين أجهزة الشرطة الجنائية في الدول الأطراف من أجل التصدي الفعال للجرائم ذات الطابع العالمي بما في ذالك الجرائم المرتبطة بالمعلوماتية، وتجاوز العقبات التي يثيرها الطابع العالمي و الخاص لهذا النوع من الجرائم. بالإضافة إلى إنشاء وتطوير كل النظم القادرة على المساهمة بفعالية في الوقاية من هذه الجرائم و مكافحتها، [632] وتعتمد المنظمة لتحقيق أهدافها على طريقتين:

ـ **الطريقة الأولى:** تتمثل في تجميع كافة البيانات و المعلومات المتعلقة بالجريمة والمجرمين عن طريق المكاتب المركزية للمنظمة الموجودة على أقاليم الدول الأطراف، وتخزينها على شكل أرشيف يتم الرجوع إليها و تبادلها بشكل سريع فيما بين هذه المكاتب كلما دعت ضرورة التحقيق و البحث إلى ذلك[633]. ومن أجل تسهيل هذه المهمة أنشئت

---

[631]–أنشئت هذه الهيئة في عام 1923 تحت اسم " اللجنة الدولية للشرطة الجنائية" بمناسبة المؤتمر الدولي للشرطة القضائية المنعقد بمدينة فينا، ثم تحولت في عام 1956 إلى " المنظمة الدولية للشرطة الجنائية" بعد إصدار الجمعية العامة لمنظمة الأمم المتحدة في دورتها الخامسة والعشرون قرار اعتماد نظامها الأساسي و جعلت مقرها في مدينة ليبو(Lyon) الفرنسية، وتظم حاليا أكثر من 189 دولة عضو. للمزيد من التفاصيل حول نشأة الأنتربول انظر الموقع الالكتروني التالي:

http://www.interpol.int/public/icpo/default.asp.

[632]– أنظر هذه الأهداف في المادة 02 من ميثاق المنظمة الدولية للشرطة الجنائية على الموقع الالكتروني التالي

http://adamrights.org/001.htm.

[633]– نشير إلى أن الانتربول في 1998 فقط كون بنك معلومات بخصوص ما يقارب 166000 مجرم من مختلف الأصناف، وفي نفس السنة تم تسجيل حوالي 162 طلب الحصول على معلومات موجه إلى هذا البنك. كما انشأ في

المنظمة في جوان 2006 نظام عالمي للإنذار العاجل متصل مباشرة مع المكاتب المركزية المتواجدة في الدول الأطراف يعمل 24سا على 24سا على مدار أيام الأسبوع[634].

ـ **الطريقة الثانية:** تتجسد في التنسيق والتعاون بين الدول الأعضاء في ملاحقة المجرمين الفارين والقبض عليهم وتسليمهم للدولة طالبة التسليم، عن طريق المكاتب المركزية المتواجدة على أقاليمها. ومن خلال إذاعة مذكرات التوقيف دوليا ومنحها قوة نفاذ عالمية.

ونظرا لتنوع أنظمة الدول الأطراف، فقد وضع خيارين لأنظمة الاتصال داخل هذه الشبكة، الأول مخصص للدول المركزية، تجري الاتصالات العالمية للشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بواسطة الأمانة العامة للمنظمة. أما الثاني للدول اللامركزية وفيه تجري الاتصالات مباشرة بين أجهزة الشرطة في الدول المختلفة عن طريق المكاتب المركزية الوطنية[635].

إلى جانب ذلك، تلعب الأمانة العامة للأنتربول دورا كبيرا في تعزيز التعاون الدولي الأمني في مجال مكافحة الجريمة، من خلال إصدارها نشرات إخبارية إعلامية من تلقاء نفسها[636]، أو بناء على طلب من المكاتب الوطنية المركزية للشرطة الجنائية في الدول

2008 قاعدة بيانات خاصة بجرائم الشذوذ الجنسي و الصور الإباحية للأطفال، يتم من خلالها تسجيل وحفظ معلومات حول هذه الجرائم والأشخاص المتورطين فيها بعد اكتشافها بواسطة برنامج خاص يسمى برنامج التحليل والمقارنة الالية (**Excalibur**)، وبفضل هذا النظام فقد تم الكشف و توقيف عدة مجرمين عبر العالم انظر:

LEBRUN. M, Interpol, PUF, que sais-je ? 1997, p 46.

[634] **-Ibid.**, p 47 et s.

[635]– **حسين بن سعيد بن سيف الغافري**، مرجع سابق، ص 506.

[636]– تتمثل هذه النشرات في النشرة الخضراء الغرض منها التزيد بتحذيرات و معلومات جنائية عن أشخاص ارتكبوا جرائم، و يرجح ارتكابهم جرائم مماثلة في بلدان أخرى. والنشرة البرتقالية تصدر لغرض التحذير والاستخبار الجنائي.

الأطراف، أو من أية منظمة دولية تربطها بالأنتربول اتفاقية تعاون[637]. وتتضمن هذه النشرات الإخبارية عادة نوعين من المعلومات، معلومات حول تفاصيل هوية الأشخاص، كالأوصاف البدنية، بصمات الأصابع، المهنة وأرقام وثائق الهوية، السنّ العنوان والجنسية. ومعلومات أخرى قضائية، كنوع و طبيعة التهمة الموجهة للشخص، القانون الواجب التطبيق، العقوبة المقررة لها، حكم الإدانة، تفاصيل الدولة المطلوب منها التسليم.

ومن أجل توسيع المساعدة الأمنية أو الشرطية في مجال مكافحة الجريمة الالكترونية إلى أكبر نطاق ممكن، قام الانتربول بإنشاء عدة مراكز اتصالات إقليمية في كل من طوكيو، نيوزيلندا، نيروبي، أذربيجان، وبيونس أيرس(الأرجنتين) ومكتب إقليمي فرعي في بنكوك لتسهيل عملية تنقل وتبادل المعلومات فيما بينها. كما قام مؤخرا بخلق ثلاث هياكل خاصة وهي، الندوة الإقليمية الأوروبية، اللجنة التقنية الأوربية والأمانة الإقليمية الأوروبية، استطاع من خلالها مدّ جسور التعاون الشرطي إلى أوروبا وجعلها شريكا مهما لمختلف الأجهزة الأمنية الناشطة على الإقليم الأوروبي في هذا المجال[638].

ليس هذا فحسب، بل تقوم الانتربول في مجال الجرائم الالكترونية بوضع قائمة اسمية لضباط متخصصين تحت تصرف الدول الأعضاء للاستعانة بهم في عملية البحث والتحري

---

[637]– وتأخذ هذه النشرات خمسة أنواع هي كالتالي: النشرة الحمراء تصدر لتوقيف متهم يجري البحث عنه أو تم احتجازه مؤقتا تمهيدا لتسليمه استنادا إلى مذكرة توقيف. النشرة الزرقاء و تصدر لجمع معلومات إضافية عن هوية شخص أو نشاطاته غير المشروعة في سياق متابعة جنائية. النشرة الصفراء تصدر للمساعدة على تحديد مكان مفقودين، لا سيما القصّر، على تحديد هوية أشخاص عاجزين عن التعريف بأنفسهم. النشرة السوداء غرضها تحذير سلطات الأمن والهيئات العامة والمنظمات الدولية من مواد أو أحداث أو أعمال إجرامية تمثل تهديدا للنظام العام. النشرة الخاصة وتعنى بتنبيه سلطات الأمن عن مجموعات وأشخاص خاضعين للجزاءات التي تفرضها الأمم المتحدة كالحركات و التنظيمات الإرهابية، انظر في هذا الشأن :**عادل يحي**، مرجع سابق، ص.ص 104–105.

[638]-voir **INTERPOL**, Rapport d'activité 2005 . disponible sur ;

http://www.interpol.int/public/ICPO/interpolAtWork/iaw2005fr.pdf.

في قضايا هذه الجرائم، كما تتولى خلق فرق عمل متخصصة و ورشات تكوين تعمل على تزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات وتوجيهات حول تقنيات التحقيق في مثل هذه الجرائم وتدريبها على سبل مكافحتها.[639] ناهيك عن تأسيسها شراكات إستراتيجية في هذا المجال مع منظمات دولية حكومية وغير حكومية ومع هيئات من القطاع الخاص[640].

نتيجة لهذا التوسع، فقد ساهمت منظمة الانتربول بالمشاركة مع سلطات أمن وطنية في إحباط عدة عمليات إجرامية خطيرة عبر العالم، والكشف عنها وتوقيف مرتكبيها أشهرها، قضية النصب والاحتيال الاستثماري التي شملت أكثر من (2000) ضحية من(60) دولة ومبلغ مسروقات قدّر ب(166) مليون أوروا، أين تول الانتربول التحقيق فيها بالتنسيق مع سلطات الأمن الدول المعنية و توصل إلى الكشف عن المجرمين و توقيفهم بدولة اسبانيا في ديسمبر 2004. [641] وعملية فالكون (FALCON) في أفريل 2005، التي تمت بين كل من الأنتربول والشرطة الفيدرالية الأمريكية (FBI) والشرطة الفرنسية، والتي انتهت إلى تفكيك شبكة إجرامية تنشط في العديد من الدول الأوروبية[642].

ومما لا شك فيه أن سلطات الأمن الجزائرية باشرت العديد من الأعمال الإجرائية في إطار المساعدة القضائية الدولية مع الانتربول، فعلى سبيل المثال تم فتح تحقيق قضائي في

---

[639]- ينظم الانتربول كل سنتين مؤتمر دولـي يضم خبـراء و متخصصين في إنفـاذ القانـون و في تكنولوجيات الإعلام و الاتصال بمشاركة مصالح الشرطة من الدول الأعضاء، يتم فيه تبادل المعارف والخبرات في مجال التحقيق في الجرائم الالكترونية و كذا دراسة المستجدات الأخيرة في هذا الميدان.

[640]- **QUEMENER Myriam et Yves CHARPENEL**, cybercriminalité droit pénal applique, op.cit.pp 208-209.

[641] - **INTERPOL**, Rapport d'activité 2005, op.cit. S.N

[642]– **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 522.

أكثر من (800) قضية متعلقة بالجريمة الالكترونية منذ دخول القانون رقم (09-04) الصادر في عام 2009 حيز التنفيذ، وهي القضايا التي تورط فيها جزائريون وأجانب وتم تسوية معظمها بتعاون مع سلطات الأمن الأجنبية، وقد كانت أول هذه القضايا، عندما تحركت سلطات الضبط ولاية باتنة في عام 2010 بناء على معلومات كافية قدمت إليها من قبل الشرطة الأمريكية حول تقني سامي في الإعلام الآلي جزائري عمره 21 سنة، يقوم باختراق موقع شركة أمريكية متخصصة في حماية المعلومات والبرامج الالكترونية للعديد من الشركات الأمريكية، ثم استغلال تلك المعلومات والبرامج لصالح شركات منافسة مقابل مبالغ مالية ضخمة، والذي أحيل للقضاء ومحاكمته وفقا للقانون بمحكمة الجنح بباتنة.[643]

ومن الأمثلة أيضا، توقيف مصالح الأمن الجزائرية لشاب جزائري صاحب مقهى الانترنت ببلدية بومرداس إثر ورود شكوى من المكتب الفيدرالي الأمريكي للتحقيقات عن طريق مكتب الانتربول بالجزائر، مفادها أنها تلقت رسالة الكترونية باللغة الانجليزية مجهولة الهوية مصدرها جهاز يقع في هذه المقهى، تهدد بوضع قنبلة لإحدى أحياء مدينة جوهانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبيل انطلاق مباراة كرة القدم بين المنتخب الجزائري و الأمريكي في كأس العالم[644]. وبالمقابل تعرضت مؤسسات جزائرية عديدة لإعمال قرصنة و اختراق من طرف أجانب، أين استلزم قمعها تعاون وتنسيق أمني مع السلطات المختصة في الدول المعنية، ومن أمثلتها اختراق موقع الشروق أنلاين ومحاولة تخريبه من قبل هاكرز مصريين[645].

---

[643]-أنظر: **زيدان ربيحة**، مرجع سابق، ص 146.

[644]-جريدة الخبر اليومية، العدد الصادر في 2010/07/21.

[645]- جريدة الشروق اليومية، العدد الصادر 2010/05/26.

2ـــ مساهمة شرطة (الانترنت) الويب الدولية (IWP) في تكريس المساعدة الأمنية:

هي منظمة دولية أنشئت في الولايات المتحدة الأمريكية عام 1986، لتلقي بلاغات وشكاوي مستخدمـي شبكة الانترنت وملاحقة الجـناة الكترونـيا والبحث والتحـري عن الأدلـة ضـدهـم وتقديمهم للمحاكمة[646].

وتضم هذه الهيئة متخصصين من سلطات إنفاذ القانون والمؤسسات الحكومية وضباط شرطة وخبراء فنيين من 61 دولة حول العالم، كما أنها تمارس اختصاصها في تتبع الأنشطة الإجرامية التي ترتكب عبر شبكة الانترنت على المستوى العالمي، وبالتعاون والمشاركة مع سلطات إنفاذ القانون التابعة للدول الأعضاء، أو أية دولة أخرى معنية بالجريمة[647]. وتعتمد منظمة شرطة الانترنت في عملها على قاعدة بيانات مركزية عملاقة يتم من خلالها تسجيل كافة الحوادث والأنشطة الإجرامية التي استخدم فيها الانترنت والتي تم الإبلاغ عنها[648].

ونظرا للمهارات الفنية العالية والقدرات المعرفية والعلمية الخارقة التي يتمتع بها القائمين على هذه المنظمة في مجال التكنولوجيات الحديثة، أضحت مقصدا لطلبات المساعدة الأمنية والقضائية من مختلف دول العالم، وفضاء واسعا للتنسيق وتبادل المعلومات والإجراءات وأدلة الإثبات بخصوص جرائم الانترنت مع مختلف أجهزة المكافحة و الضبط في دول المعمورة، ومختلف المنظمات والوكالات الدولية المتخصصة المنخرطة في محاربة

---

[646] – http://www.web-police.org.

[647]– **سليمان احمد فيصل**، مرجع سابق، ص 417.

[648]– **أيمن عبد الحفيظ**، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، عدد 01 ، القاهرة، صادر في 25 جانفي 2004، ص 226 .

هذا النمط الإجرامي. كما أصبحت مصدرا مهما لتقديم المشورة وإسداء النصيحة والمساعدة الفنية في ذات المجال[649].

3ــ دور الشرطة الأوروبية (EUROPOL) في توفير التنسيق الأمني في أوروبا:

يمثل الأوروبول جهاز للشرطة الجنائية على مستوى الاتحاد الأوروبي، انشأ في لكسمبورغ بموجب الاتفاقية 26 جويلية 1995[650] ودخل حيز الخدمة في عام 1999 بعد أن اتخذ مقره في مدينة لاهاي بهولندا، ليكون همزة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال ملاحقة الجرائم العابرة للحدود بما فيها جرائم الإرهاب والمخدرات، الجريمة المنظمة، وكذا الجرائم الالكترونية[651].

ويهدف أساسا هذا الجهاز إلى تسهيل عملية البحث والتحري وتبادل المعلومات بين سلطات الأمن التابعة لدول الاتحاد، وتجميع، تخزين وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أية دولة عضو بخصوص جريمة من الجرائم المذكورة بما فيها الجريمة الالكترونية،[652] كما يتولى الأوروبول إسداء النصيحة وتقديم التوجيهات والإرشادات المفيدة ومختلف أنواع الدعم (المادي أو اللوجستيكي) لهيئات التحقيق الوطنية. ولتنفيذ هذه

---

[649]– نظرا للإقبال الهائل على خدمات شرطة الويب، فقد تم تدعيمه في عام 2002 بجهاز سمي **بالمركز الدولي للشكاوي الخاصة بجرائم الانترنت** كلّف بتلقي الشكاوي الآتية من أية بقعة من العالم بخصوص جرائم الانترنت و كذا تقديم المساعدة الأمنية والقضائية المطلوبة لغرض التحقيق في هذا الشأن. أنظر: **زيدان زيبحة** ، مرجع سابق، ص 110.

[650] - **JOCE**, n° C 316, 27 November 1995.

[651] -Voir : Europol sur, http://www.europol.eu.int.

[652]– أنظر مبادئ و أهداف الأوروبول في المادة (K1.9) من اتفاقية مستر يخت منشور في الموقع الالكتروني :

http//:fr.wikipedia.org/wiki/Trait%C3%A9 de Maastricht.

المهام يضمن هذا الجهاز اتصالا دائما و متواصلا و سريعا مع السلطات المختصة في الدول الأعضاء عن طريق ما يسمى بنقاط اتصال (les points de contact)[653].

وينشط الأوروبول في مجال مكافحة الجريمة الالكترونية مع نظام معلومات تشنجين(système d information Schengen) وهو نظام أنشأ في عام 1990 يتكون من قسم مركزي مقره مدينة ستراسبورغ و أقسام وطنية في كل دول المنظمة[654]، ويحتوي على بنك معلومات ضخم تسجّل فيه المعلومات التي ترسلها إليه قوات الشرطة والسلطات القضائية من كل دولة عضو، من بينها المعلومات المتعلقة بالأفراد المبحوث عنهم، أو المطلوب تسليمهم من قبل دول أخرى، أو الممنوعين عن دخول أراضي دولة ما، أو المعلن اختفائهم أو المطلوب تقديمهم للعدالة بأمر قضائي لآي سبب كان[655].

كما يتفاعل الأوروبول في أداء مهامه مع جهاز الاوروجيست (Eurojust)[656] باعتباره وحدة للتعاون القضائي والتنسيق بين السلطات القضائية المكلفة بالتحقيق، وذلك عندما تمسّ الجريمة دولتين على الأقل من الدول في الاتحاد الأوروبي، أو دولة عضو مع دولة أخرى

---

[653]- **SABATIER (M)**, la coopération policière européenne, Harmattan, Paris, 2001, p 372.

[654]– نشير الى انه تم وضع نظام جديد لتبادل المعلومات تابع لنظام شنجن(SIS II) بعد عملية التوسع التي شهدها الاتحاد الأوروبي بانضمام 10 دول أخرى إليه سنة 2004 ، و هذا النظام الذي يعد الجيل الثاني من نظام شنجن يعنى بفهم بيانات ذات خصائص دقيقة (الصور الفوتوغرافية، بصمات الأيدي، البصمة الوراثية) ويسمح بمقارنة نتائج البيانات.

[655]– **جان فرنسوا هنروت**، مرجع سابق، ص 109.

[656]– انشأ جهاز الأوروجست بصفته النهائية في عام 2002 بموجب قرار مجلس الاتحاد الأوروبي المؤرخ في 28-02-2002، وهي وكالة تابعة للاتحاد الأوروبي تهتم بتنظيم مسائل التعاون القضائي، تتألف من وكلاء النيابة الوطنيين والقضاة أو ضباط الشرطة من ذوي الكفاءات المتساوية من كل دولة عضو في الإتحاد، انظر قرار الإنشاء في الجريدة الرسمية للمجلس الأوروبي عدد ل 63، صادر في مارس 2002.

خارج الاتحاد. فيتم تبادل المساعدات القضائية فيما بين الجهازين من خلال تبادل المعلومات، تسهيل ونقل الإجراءات المتعلقة بالتحقيق والبحث في الجرائم العابرة للحدود، تبادل الإنبات القضائية، تسليم المجرمين، وكذا التخفيف من مختلف العقبات والحواجز البيروقراطية التي تواجه سلطات إنفاذ القانون على المستوى الأوروبي[657].

ليس هذا فحسب، بل ولتفعيل وتوسيع التعاون الأمني عبر الحدود يتعامل الأوروبول مع وكالات استخباراتية متخصصة وأنظمة مراقبة ذات خبرة عالية، كوكالة فرانتكس (Frontex)، وهي وكالة أوروبية لإدارة التعاون ألعملياتي على الحدود الخارجية للدول أعضاء الاتحاد الأوروبي[658]. ونظام الأورواك (Eurodac)، وهو نظام معلوماتي واسع النطاق يحوي على البصمات الرقمية لطالبي اللجوء والمهاجرين غير الشرعيين الموجودين على إقليم الاتحاد الأوروبي[659]. وكذا نظام الاوروسير(Eurosur)، وهو نظام لتبادل المعلومات بخصوص مراقبة الحدود الأوروبية، يشمل على برنامج مشترك لتكنولوجيا المعلومات و يعمل على تمكين السلطات المشاركة في إطاره من تقييم و رؤية الوضع على الفور في الاتحاد الأوروبي وما وراء الحدود الخارجية للإتحاد.

إلى جانب ذلك، استحدث جهاز على مستوى الأوروبول في عام 2010 أطلق عليه اسم (Internet Crime Reporting Online ICROS) مهمته توفير أكبر قدر ممكن من التعاون والتنسيق الأمني السريع في مجال مكافحة الجريمة الالكترونية بين دول الاتحاد

---

[657]-_**MARMISSE Anne - D'ARRAST**, **D'abbadie**_Coopération et harmonisation (Matière pénale), Dalloz, édition 2013, p 21.

[658]– الفرونتكس هي وكالة أوروبية مسئولة عن تنسيق نشاطات حراس الحدود الوطنية الخاصة بضمان أمن حدود أوروبا مع الدول غير الأعضاء، مقرها بوار شو ببولندا . تأسست في الفاتح ماي 2005، ودخلت حيز الخدمة في أكتوبر 2005.

[659] -Voir Eurodac sur : https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Eurodac.

الأوروبي[660]. وهو الجهاز الذي تم تدعيمه مؤخرا في جويلية 2017 بهيئة أخرى متخصصة تدعى المركز الأوروبي للجريمة الالكترونية (EC3)، والذي سيكون كما قال رئيسه (ترويلس أويرتينج)، همزة وصل بين الدول الاعضاء تتصهر فيها الجهود ومركزًا للدعم الإستخباراتي والتشغيلي والقضائي يقوم بالرد على الجرائم الإلكترونية، بالإضافة إلى قدرته على تعبئة كل مصادر الدول الأعضاء في الاتحاد الأوروبي التي من شأنها تقليص والحد من آثار تهديدات المجرمين الإلكترونيين أينما حلوا. وسيعمل على تزويد الشرطة وسلطات إنفاذ القانون في الدول الأعضاء، بمعلومات حول اتجاهات الجرائم الإلكترونية الجارية، بالإضافة إلى تفاصيل عن التهديدات الناشئة[661].

مواصلة لهذه الجهود، فقد تم استحداث عدة آليات أخرى لتسهيل وتعزيز عملية التعاون الأمني على الصعيد الأوروبي، منها الاعتراف في عام 2002 بمذكرة القبض الأوروبية (Mandat d'arrêt européen) والتي دخلت حيز النفاذ في عام 2004[662]، كإجراء يسمح لسلطات الضبط القضائي في أية دولة عضو في الاتحاد الأوروبي القبض على المتهم الهارب إلى إقليمها تنفيذا لحكم إدانة نهائي صادر عن هيئة قضائية لدولة أخرى عضو دون التقيد بشرط التجريم المزدوج، وتسليمه إلى هذه الأخيرة وفقا لشروط تسليم المجرمين[663]. الاعتراف أيضا في عام 2008 بما يسمى بالمذكرة الأوروبية للحصول على

---

[660] - **QUEMENER Myriam . et CHARPENEL Yves**, cybercriminalité droit pénal applique, op.cit. p 209

[661] - **CONSEIL DE L'UNION EUROPEENNE**, Conclusions du Conseil sur l'établissement d'un Centre européen de lutte contre la cybercriminalité, publier sur : press.office@consilium.europa.eu http://www.consilium.europa.eu./Newsroom

[662]– تم إنشاء مذكرة القبض الأوروبية بموجب القرار الإطار رقم(JAI /584/2002)، 13 جوان 2002، جريدة رسمية للمجلس الأوروبي عدد ل 190، صادر في 18 جويلية 2002.

[663]- **MARMISSE Anne - D'ARRAST D'abbadie**, op.cit. p 35.

الأدلة (Mandat européen d'obtention de preuves)[664]، وهو إجراء يمكن بموجبه لسلطات التحقيق في دولة عضو في الاتحاد الأوروبي الحصول بسرعة و بسهولة و بصفة مباشرة على أدلة مفيدة للتحقيق من مثيلاتها في أية دولة أخرى عضو دون الحاجة إلى إتباع الإجراءات الرسمية الدبلوماسية المعتادة. كما تم إنشاء في عام 2009 مذكرة أوروبية حول تدابير المراقبة (Mandat européen sure les Mesures de contrôle)[665] ، وهي مذكر توجهها سلطات التحقيق المختصة في دولة عضو في الاتحاد إلى مثيلتها في دولة عضو أخرى، تطالبها فيها باتخاذ بعض التدابير التحفظية الرقابية حيال متهم مقيم في دائرة اختصاصها لغرض التحقيق. وقد تشمل هذه التدابير الأمر بالوضع تحت الرقابة القضائية والأمر بالإيداع رهن الحبس المؤقت[666].

ولقد أثبتت الشرطة الأوروبية نجاعتها في التصدي للإجرام الالكتروني العابر للحدود من خلال عديد العمليات نفذتها بالتنسيق مع سلطات أمن تابعة للدول الأعضاء وكلّلت بالنجاح، نذكر منها العملية الشهيرة بمحطم الجليد (icebreaker) التي قامت بموجبها الاوروبول في 14 يونيو 2005 بمداهمة وتفتيش أماكن في ثلاث عشرة دولة أوروبية هي، (النمسا، بلجيكا، فرنسا، ألمانيا المجر، أيسلندا، إيطاليا، هولندا، بولونيا، البرتغال، سلوفاكيا،

---

[664]– استحدث هذا الإجراء بموجب القرار الإطار رقم(JAI /978/2008)، 23 أكتوبر 2009، جريدة رسمية للمجلس الأوروبي عدد **ل** 350، صادر في 30 ديسمبر 2008.

[665]– تم إنشاء هذه الآلية بموجب القرار الإطار رقم (JAI /829/2009)، 23 أكتوبر 2009، جريدة رسمية للمجلس الأوروبي عدد ل 294، صادر في 11 نوفمبر 2009.

[666] – **MARMISSE Anne - D'ARRAST D'abbadie**, op.cit. p 37.

السويد، وبريطانيا العظمى) وتوجت بتوقيف عدد من المجرمين في كل من فرنسا، بلجيكا، المجر، وأيسلندا والسويد [667].

4ـــ **منظمة الشرطة الجنائية الإفريقية (AFRIPOL)** : وهي أكبر منظمة شرطة في القارة الإفريقية مكونة من قوات الشرطة لـ 41 دولة، أنشئت بمبادرة من الدولة الجزائرية يوم 13 ديسمبر 2015 ، ومقرها الرئيسي بالجزائر العاصمة[668]. وتم الإعلان رسميا عن بداية نشاطها يوم الأحد 06/ 07/ 2017 بمناسبة اجتماع مسئولي أجهزة الشرطة للدول الإفريقية الأعضاء في الإتحاد الإفريقي المنعقد بالجزائر، وترتكز مهام الافريبول كما أعلن عنها المدير العام للأمن الوطني الجزائري في، مضاعفة رصيد التعاون الشرطي الإقليمي والدولي، تحديد السياسة العامة للشرطة الجنائية وتوفير التكوين وإعادة تأهيل مختلف أجهزة الشرطة الإفريقية التي تشهد تأخرا أو ضعفا على مستوى الأداء، تعزيز قيم السلم والأمن والاستقرار في القارة الإفريقية، رفع التحديات وإيجاد الحلول الجادة والفعالة للجرائم العديدة التي تواجهها بعض الدول الإفريقية، مثل تنامي الجرائم الإرهابي والمتاجرة بالمخدرات والقرصنة البحرية وتبييض الأموال والجرائم المعلوماتية، السماح بالتحدث بصوت واحد على الصعيد الدولي وتطور الموقف الإفريقي المشترك في سبيل تفضيل الحلول الإفريقية وتفادي الوصفات المفروضة عليها، وكذا السعي إلى تعميق تبادل وجهات النظر حول ترقية العلاقات الثنائية

---

[667]– **جان فرنسوا هنروت**، مرجع سابق، ص 110.

[668]– طرحت الجزائر لأول مرة فكرة إنشاء منظمة الأفريبول بمناسبة الندوة الجهوية الإفريقية ال22 للأنتربول التي احتضنتها في شهر سبتمبر 2013، و تم دعم الفكرة على هامش الجمعية العامة ال 82 للمنظمة الدولية للشرطة الجنائية "الأنتربول" التي انعقدت في أكتوبر 2013 في كولومبيا، قبل أن يتم اعتماد الفكرة من خلال تبني الوثيقة المبدئية وإعلان الجزائر خلال الندوة الإفريقية للمديرين والمفتشين العامين الأفارقة للشرطة المنعقدة في فبراير 2014 بالجزائر العاصمة ثم تبنيها رسميا خلال القمة الـ 23 للاتحاد الإفريقي في غينيا الاستوائية في جوان 2014.

بين المؤسسات الشرطية للبلدان الإفريقية[669].

ثانيا ــ تكثيف التعاون الفني الدولي: لا تكفي المساعدة الأمنية الدولية وحدها لتجاوز العقبات التي يفرضها التحقيق الجنائي في الجرائم الالكترونية، بل لابدّ من مصاحبتها بالمساعدة الفنية وتبادل الخبرات والمعارف بين الدول. لان سلطات الأمن وأجهزة العدالة الجنائية ليست بذات الجاهزية والكفاءة لمواجهة الجريمة الالكترونية في جميع الدول، إنما تختلف من دولة إلى أخرى بحسب درجة تقدمها و رقيها.

من هذا المنطلق، فقد ناشدت معظم الاتفاقيات الدولية والإقليمية ذات الصلة بضرورة وأهمية وجود تعاون متبادل في مجال التدريب ونقل الخبرات والمعارف فيما بين الدول[670]، لأن في اعتقادها أن التقدم المستمر لتكنولوجيات المعلومات والاتصال يفرض على الجهات الأمنية والقضائية أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات، والإلمام بمستجداتها حتى يمكن التصدي للأفعال الإجرامية التي تصاحب هذه التكنولوجيات. كما أن إعمال القانون في مواجهة الجرائم الالكترونية يستلزم اتخاذ تدابير وإجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية لما تتسم به هذه الجرائم من حداثة في الأسلوب والسرعة في التنفيذ والسهولة في التستر عنها ومحو آثارها[671]، وهو ما يشكل تحديا كبيرا على عاتق الأجهزة القضائية المختصة من قضاة تحقيق وقضاة حكم ورجال الضبطية القضائية، يفرض عليهم أن يكونوا على درجة عالية

---

[669]– انظر تصريحات المدير العام للأمن الوطني الجزائري عبد الغاني هامل حول مهام الافريبول في: جريدة الرياض اليومية الصادرة بتاريخ 07-08-2017، منشورة على الموقع التالي: http://www.alriyadh.com/1109557

[670]– نذكر منها على سبيل المثال نص المادة(29) من اتفاقية منظمة الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000، والمادة (09) من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود.

[671]– **هشام محمد فريد رستم**، الجرائم المعلوماتية، أصول التحقيق الجنائي والفني، مرجع سابق، ص 498.

من الكفاءة والمعرفة في التعامل مع الجريمة الالكترونية والمجرم المعلوماتي. ومن هنا كانت الحاجة الملحة إلى التعاون الدولي في مجال تدريب وتكوين رجال الأمن والقضاء للاستفادة من مهارات وتجارب الآخرين من ذوي الكفاءة العلمية والتأهيل الفني بوسائل ميسرة[672].

وقد تتم عملية تبادل المساعدة الفنية بين أجهزة العدالة الجنائية للدول عن طريق ندوات ومؤتمرات أو ورشات عمل جماعية متخصصة تعقد على المستوى الدولي أو الإقليمي[673]، حيث تقدّم هذه الفعاليات العلمية من أبحاثها ودراساتها حول المستجدات المتعلقة بالجرائم الالكترونية المستحدثة من خلال تحليل ومناقشة أبعادها و تحديد أنماطها وأهم الصفات التي يتميز بها المجرم الالكتروني والدوافع وراء ارتكابه للجريمة، وبيان أساليب ارتكابها، مخاطرها وتهديداتها وما يقابلها من وسائل الوقاية والمكافحة، لتتوج في النهاية بتقارير وتوصيات أو اتفاق مشترك يفيد الجميع[674].

كما قد يتحقق ذلك عن طريق تنظيم دورات تدريبية تكوينية عالية المستوى للعاملين في أجهزة القضاء والمعنيين بمكافحة الجرام الالكترونية، يتم من خلالها اطلاع المتدربين على السبل المبتكرة للتحقيق الجنائي في مثل هذه الجرائم، من تقنيات تجميع المعلومات وتحليلها، أساليب المواجهة والاستجواب، طرق مراجعة النظم الفنية للمعلومات، إجراءات التفتيش والضبط، وكذا كيفية استخدام الحاسب الآلي كأداة للمراجعة واستخراج الدليل،

---

[672]– **فهد عبد الله العبيد العازمي**، مرجع سابق، ص.ص 655–656.

[673]– من الأمثلة على ذلك: المؤتمر الدولي الأول لقانون الانترنت المنعقد بمدينة الغردقة بدولة مصر في الفترة من 21 إلى 2005/08/25، بتنظيم مشترك بين السلطات المصرية والمنظمة العربية للتنمية الإدارية.

– ورشة عمل إقليمية حول " تطوير التشريعات في مجال مكافحة الجرائم الافتراضية " التي عقدت بمدينة مسقط عمان في الفترة من 2 الى 2006/4/4، بتنظيم مشترك بين هيئة تنظيم الاتصالات العمانية و مركز التمييز العربي التابع للاتحاد الدولي للاتصالات.

[674]–نستشهد هنا بالاجتماعات التي تم عقدها في إطار التنسيق بين المعاهد القضائية العربية والتي تمخضت عن الاتفاق على إعداد مشروع اتفاقية عمان للتعاون العلمي بين المعاهد القضائية العربية والتي وقعت في 09 أفريل 1997.

بالإضافة إلى كل ما يتعلق بتدابير الوقاية و وسائل الحماية من وقوع الجريمة. مع تشجيعهم على تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين بخصوص الجرائم الالكترونية والعمل على تبادلها مع نظرائهم في مختلف الدول[675]. وغالبا ما يتولى تنظيم مثل هذه الدورات التدريبية، المنظمات أو الدول أو الأجهزة الكبرى ذات قدرات عالية ومستوى أكثر تقدما حتى تضمن مشاركة واسعة[676].

والتدريب المقصود هنا ليس التدريب التقليدي فحسب، إذ لا يكفي أن تتوافر لدى سلطات القضاء والضبطية القضائية الخلفية القانونية و متطلبات العمل الشرطي، بل لا بد من اكتسابهم خبرة فنية وعلمية في مجال مواجهة الجريمة الالكترونية، وهي الخبرة التي لا تتأتى دون تكوين وتدريب تخصصي يراعي فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والاستعدادات الذهنية لتلقي التدريب[677].

ومن أجل تيسير عملية التدريب وضمان أكبر قدر ممكن من المساعدة الفنية المتبادلة بين أجهزة تنفيذ القانون في مختلف الدول، يتم الاعتماد على أسلوب تدريب جديد يسمى بنظام التدريب عن بعد (Distant Training)، وهو نظام يسمح للمتدرب أو المرشح، أيا كان موقعه، أن يلتحق بدورة أو برنامج تدريبي أو يحضر أو يشارك في مؤتمر، ندوة أو

---

[675]– **يوسف حسن يوسف**، مرجع سابق، ص 178.

[676]– تعد الولايات المتحدة رائدة في توفير المساعدة الفنية والتدريب لمكافحة الجريمة الالكترونية عبر العالم، إذ تنظم أكاديمية مكتب التحقيقات الفيدرالية الأمريكي سنويا عدة دورات تدريبية متخصصة مدة كل واحدة منها أربعة أسابيع، وهي مفتوحة لمشاركة كل العاملين في أجهزة العدالة و رجال الضبط القضائي من الدول العالم. كما يتكفل مكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج التابع لوزارة العدل الأمريكية، بشكل مستمر بتوفير المساعدة الفنية اللازمة لتعزيز مؤسسات العدالة الجزائية و إدارة القضاء في مختلف الدول. ناهيك عن الدور الذي يلعبه البرنامج الدولي للمساعدة و التدريب على التحقيق الجزائي (ICITAP) في إيصال خبراته الفنية و قدراته التحقيقية إلى أجهزة الشرطة في الدول النامية عن طريق إنشاء معاهد خاصة بالتدريب.

[677]– **هشام محمد فريد رستم**، الجرائم المعلوماتية، أصول التحقيق الجنائي و الفني، مرجع سابق، ص 495.

حلقة علمية بشكل متزامن أو غير متزامن دون الحاجة إلى الحضور الشخصي لمكان انعقاد التظاهرة أو حتى التقيد بمدتها أو بعدد المتدربين أو الوقت، ودون أن يتحمل أعباءها، بطريقة مرنة عبر وسائل الاتصال الحديثة والانترنت[678].

ولأن نظام التدريب عن بعد يعتمد أساسا على تقنية الاتصال والتعامل مع شبكة الانترنت، فإن إتقان استخدام هذه التقنية يوفر للمتدرب العديد من المزايا أبرزها، التعامل مع أبرز متطلبات العصر، تحيين و تحديث بشكل مستمر لمعارفه و مؤهلاته العلمية، والوصول بسهولة للعديد من مصادر التعلّم، الحصول على كم كبير من المعلومات التي تعزز المعارف والمهارات الأمنية المحدودة، وكذا إتقان ثقافة استخدام تقنية المعلومات وتوظيفها في جودة الأداء الأمني[679].

ونظرا لأهمية التدريب، كانت من أولويات السياسة الوطنية لمكافحة الجرائم الالكترونية في الجزائر تكوين وتأهيل سلك ضباط الشرطة القضائية وأعوانهم، فعلى مستوى الدرك الوطني الذي باشر منذ سنة 2004 في عمليات تكوين مستخدمين من اجل إنشاء مركز وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، فبموجب هذا العمل استفاد الكثير من إطارات الدرك الوطني من تكوين متخصص في الجانبين التقني (إعلام ألي) والقانوني(الإجرام المعلوماتي) بالخارج في جامعات سويسرية، أمريكية وكندية،[680] ودورات تكوينية أخرى في مؤسسات وطنية مثل مركز الدراسات والبحوث في الإعلام العلمي والتقني (CERIST) الذي سطر برنامج تكويني سنوي في الأمن المعلوماتي يهدف إلى تحيين

---

[678]–**محمد علي قطب**، الجرائم المعلوماتية و طرق مواجهتها، الأكاديمية الملكية لشرطة البحرين،الدوحة ، 2010، ص08.

[679]– المرجع نفسه، ص 09.

[680]–**أحمد مسعود مريم**، مرجع سابق، ص 47.

وتطوير كفاءات سلك الدرك، حتى تكون أكثر عملية في مجال مواجهة الجريمة الالكترونية.[681] ناهيك عن النشاطات العلمية من ندوات وملتقيات ومؤتمرات وطنية ودولية التي ينظمها الأمن الوطني بصفة دورية في هذا الميدان.

استمرار في السياسة ذاتها، قامت وزارة العدل منذ سنة 2003 في إطار إصلاح العدالة، بإطلاق برنامج تكوين خاص بسلك القضاة، هدفه رفع مستوى أداءهم ليواكب التطور القانوني الجاري في نطاق الإجرام الالكتروني. ومن خلاله تم إدراج مادة " الجريمة الالكترونية" في برنامج تكوين طلبة المدرسة الوطنية للقضاء يتم دراستها على شكل ملتقيات ينشطها خبراء، وإشراكهم في الدورات التكوينية في مختلف مجالات الجرائم الالكترونية التي تنظم بالخارج خصيصا للسادة القضاة وإطارات وزارات العدل في إطار التعاون الثنائي.

ولا شك أن تخصيص جهات القضاء وتخصص القضاة هما من الركائز الأساسية لبناء نظام قضائي معاصر وكفؤ، على حدّ تعبير اتفاقية التمويل الجزائرية الأوروبية لدعم إصلاح العدالة في الجزائر[682]. لذلك اتجه المشرع الجزائري إلى إرساء فكرة القضاء المتخصص واختار لذلك أسلوب الأقطاب القضائية بدلا من إنشاء هيئات جديدة، عن طريق توسيع دائرة الاختصاص الإقليمي لبعض المحاكم لتشكل أقطاب قضائية يمنحها اختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن

---

[681]–**BOUDER Hadjira**, orientations de la politique pénale de prévention et de lutte contre la criminalité liée aux TIC en Algérie, op.cit. p 8.

[682]– أفصحت هذه الاتفاقية بأنّ " **الهدف من هذا المشروع هو دعم التخصص و تكوين القضاة داخل و خارج الوطن للاستجابة للمتطلبات المستجدة الناتجة عن التزايد المستمر للمنازعات التي يجب عليهم الفصل فيها**..." أنظر : المنشور الصادر عن وزارة العدل حول فعليات الندوة الوطنية لإصلاح العدالة، نادي الصنوبر، 2005، ص 23.

اختصاصها العادي[683]. وأحسب أن التخصيص الذي سيسود النظام القضائي الجزائري وفق هذا الأسلوب سيرتكز أكثر على العنصر البشري أي تخصص القضاة، مما يشكل حجر الزاوية لفكرة الأقطاب القضائية.

من هنا نستنتج، أن التعاون الدولي الأمني والفني بات اليوم ضرورة ملحة لمواجهة الجرائم الناشئة عن استخدام شبكة الانترنت العابرة للحدود، بل يعدّ حلا مهما لتجاوز الكثير من الصعوبات والعقبات التي تثيرها عملية التحقيق والبحث في هذه الجرائم. لذلك يجب على كل الدول بمختلف درجة تقدمها و رقيها المشاركة في تدعيم المساعدة الأمنية والفنية الدولية من خلال إبرام اتفاقيات تعاون ثنائية أو متعددة الأطراف، والانضمام إلى الهيئات الدولية والإقليمية الناشطة في هذا المجال كمنظمة الأنتربول والأوروبول، وكذا تشجيع سلطاتها المكلفة بتنفيذ القانون على الدخول في برامج التكوين العالمية والمشاركة في دورات التدريب المتخصصة في الجرائم الالكترونية لتطوير مهاراتها وخبراتها في ذات المجال. كما يتعين على الدول المتقدمة بذل جهدا أكبر في مساعدة الدول النامية على تعزيز مؤهلات وكفاءات مؤسساتها المكلفة بالتحري والتحقيق والمحاكمة، من خلال توفير التدريب وسائر أنواع المعونة التقنية.

الفرع الثاني: تشجيع المساعدة القضائية الدولية

يقصد بالمساعدة القضائية الدولية، كل إجراء قضائي تقوم به دولة من شأنه تسهيل عملية المتابعة والمحاكمة الجزائية في دولة أخرى بخصوص جريمة من الجرائم[684]. انطلاقا من هذا التعريف تظهر الحاجة الملحة إلى المساعدة القضائية الدولية في عملية مكافحة

---

[683]– يتجسد هذا الأسلوب في المادة 329 التي تنص على أنه" **يجوز تمديد الاختصاص المحلي للمحاكم إلى دائرة اختصاص محاكم أخرى عن تريق التنظيم، في جرائم ...الماسة بأنظمة المعالجة الآلية للمعطيات...**".

[684]– **يوسف حسن يوسف**، مرجع سابق، ص 150.

الإجرام العابر للحدود بصفة عامة والجريمة الالكترونية على وجه الخصوص، بسبب ما تثيره هذه الأخيرة من صعوبات في تحديد هوية المجرم الالكتروني، صعوبات إثباتها وملاحقة مرتكبها، في ظل عالميتها و تشتت عناصرها بين الدول، وكذا المشكلات المتعلقة بكيفية استيراد البيانات التي تم تخزينها عن بعد في حالة اعتبارها دليل إثبات، حيث لا توجد قاعدة عامة لحل هذه المشكلات دون تعاون أو مساعدة قضائية.

اعتبار لهذه الحاجة، أبرمت العديد من الاتفاقيات الثنائية والمتعددة الأطراف بهدف إرساء مختلف أشكال التعاون الجنائي البيني، نذكر منها الاتفاقية الأوروبية للمساعدة المتبادلة في القضايا الجنائية الموقعة في ستراسبوغ بتاريخ 20 افريل 1959. واتفاقية الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية المؤرخة في 14-12-1990، ثم اتفاقية الرياض العربية للتعاون القضائي، النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي في 2003[685].

أما بخصوص التعاون القضائي الدولي في مجال التصدي لظاهرة الإجرام الالكترونية فتعتبر الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001 نموذجا يقتد به، لإقرارها عدة إجراءات تعاون مستحدثة، بالإضافة إلى تعزيزها لصور التعاون القضائي الدولي المتعارف عليها أو التقليدية. والتي سوف نخصها بالدراسة على هذا المنوال:

-**أولا: تثمين الإجراءات التقليدية للتعاون القضائي الدولي:** وتتضمن مختلف صور التعاون التي تسرى على الجرائم الالكترونية وغيرها من الجرائم التقليدية العابرة للحدود على حد سواء، وقد كرستها الاتفاقية الأوروبية في المادة 23 حينما أوصت الدول الأطراف على تطبيق الاتفاقات الدولية حول التعاون الدولي في المسائل الجريمة ذات الصلة، ويمكن تلخيص هذه الإجراءات فيما يلي:

---

[685]- **جورج لبكي**، مرجع سابق، ص.ص 03-04.

1- تبادل المعلومات: يعتبر هذا الإجراء من وسائل التعاون الدولي على المستوى الإجرائي الجنائي، التي تسمح بالاتصال المباشر بين الأجهزة القضائية والأمنية في الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين. وعادة ما يتحقق هذا الإجراء بتقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية، بمناسبة نظرها في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات المتخذة ضدهم والسوابق القضائية الخاصة بهم[686].

كما قد يتحقق تبادل المعلومات أيضا بشكل عفوي مثلما أكدت المادة (26) من الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001، وذلك بقيام السلطات القضائية في دولة ما من تلقاء نفسها بتقديم معلومات مهمة و مفيدة للتحقيقات أو الدعاوي الجنائية التي تقوم عليها مثيلتها في دولة ثانية، ومن دون أن تطلبها منها هذه الأخير أو تدرك حتى بوجودها[687].

ولأن المساعدة القضائية الدولية بما فيها تبادل المعلومات تتم في الغالب وفق الطرق الرسمية الدبلوماسية التي تتسم بالبطء والتعقيد، فقد أضافت المادة (27 /3) من الاتفاقية المذكورة أعلاه، انه في حالة الطوارئ أو الاستعجال، كما هو الحال عادة بالنسبة للتحقيق في الجرائم الالكترونية، يمكن إرسال طلبات تبادل المعلومات مباشرة من قبل الهيئات القضائية أو الأمنية في الدولة التي قدمت الطلب إلى الهيئات القضائية أو الأمنية التي تحوز على هذه المعلومات في الدولة المطلوب منها. على أن تتولى الهيئات الأولى عقب

---

686 **- OFFICE FEDERAL DE LA JUSTICE,** L'entraide judiciaire internationale en matière pénale, 9ème édition, Unité Entraide judiciaire, Genève, 2010, p 06.

687 **-l' article(26) –Information spontanée** - stipule ; « une partie peut, dans les limites de son droit interne et en absence de demande préalable, communiquer a une autre partie des information obtenues dans le cadre ses propre enquêtes lorsqu'elle estime que cela pourrait aider la partie destinataire a engager ou a mener a bien des enquêtes ou des procédures au sujet d'infractions pénales… »

هـذا الإجـراء إرسـال نسخة عن الطلـب إلى السلطـات المركـزية التـابعة لهـم ليتم نقله إلـى السلطات المركزية التابعة للفريق المطلوب منه[688].

ولقد لقيت هذه الصورة من المساعدة القضائية صدى كبير في العديد من الاتفاقيات الدولية، أهمها ما جاء في المادة الأولى فقرة (2) من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[689]، والمادة 48 فقرتها الأولى البند (د) من اتفاقية الأمم المتحدة لمكافحة الفساد والتعاون الدولي، ثم المادة الرابعة فقرة (1) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي[690]، وكذا ما جاء الفقرات الثالثة والرابعة والخامسة من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[691]، إذ فرضت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي.

ويصدق الأمر كذلك على ما قضت به المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي بشأن ضرورة تبادل المعلومات بين الأطراف والتنسيق بين الأنظمة

---

[688]– أنظر نص المادة (3/27) من الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001، مرجع سابق.

[689]– صدرت هذه المعاهدة بمناسبة اختتام الجلسة العامة 68 للأمم المتحدة المنعقدة في 1990/12/14. وقد أوجبت المادة 2/01 منها على الدول الأطراف التوفير لبعضها البعض أكبر قدر ممكن من المساعدة القضائية وتبادل المعلومات.

[690]– اعتمدت من قبل مؤتمر وزراء خارجية دول منظمة المؤتمر الإسلامي في اختتام اجتماعهم المنعقد في الفترة من 28 جوان إلى 01 جويلية 1999.

[691]–تم التوقيع عليها في مدينة باليرمو عام 2000. متوفرة في الموقع التالي:

http://www.uncjin.org/documents/conventions/dcatoc/final_documents_2/convention_french.

القضائية العربية، وما ورد في المادتين الأولى والثانية من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي[692].

أما على مستوى التشريع الوطني، فلم يغفل المشرع الجزائري عن النص على هذا الإجراء المهم جدا للمساعدة القضائية الدولية في المادة (17) من القانون(09 /04) المتضمن الوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها، إذ أجاز للسلطات المعنية الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات ولو باستعمال مختلف وسائل الاتصال السريعة في خالة الاستعجال، وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل. ليس هذا فحسب، بل قام بإنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجية المعلومات تتشكل من خبراء ومتخصصين في هذا المجال، وجعل من مهامها الأساسية، السهر على تنفيذ طلبات المساعدة الصادرة عن الدول الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها في إطار الاتفاقيات التي توقعها الجزائر[693].

وفي هذا الشأن، اقترح أن يدرج في الاتفاقيات الخاصة بالمساعدة القضائية الدولية أحكاما تسمح بتبادل المعلومات شفويا في حالة الاستعجال القصوى بين السلطات القضائية في الدول الأطراف، على أن يتم تأكيد هذا التبادل كتابة فيما بعد، مثلما هو الحال في الاتفاقية الأمريكية الكندية للمساعدة القضائية.

---

[692]– صدرت الاتفاقية الأولي في 1993/4/6 بمدينة الرياض، أما الثانية في 2003/12/22 بالكويت. مشار إليهما في: **فهد عبد الله العبيد العازمي**، مرجع سابق، ص 534.

[693]– أنظر المادة(2/4) البند السادس من المرسوم الرئاسي رقم (15–261) المؤرخ في 8 أكتوبر 2015، المحدد لتشكيلة وتنظيم و كيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجية الإعلام و الاتصال، مرجع سابق.

2ـ **نقل الإجراءات** : يقصد بهذا الإجراء، قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية على إقليمها بخصوص جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الأخيرة متى ما توافرت شروط معينة، أهمها التجريم المزدوج، وشرعية الإجراءات المطلوب اتخاذها بمنظور قانون دولة المطلوب منها، وأن تكون هذه الإجراءات ضرورية ومهمة لكشف الحقيقة.

ولقد تم النص لأول مرة على نقل الإجراءات كإحدى صور المساعدة القضائية، في المادة الثالثة من الاتفاقية الأوروبية للمساعدة المتبادلة في القضايا الجنائية لعام 1959[694]. ثم تناقلتها عديد الاتفاقيات الدولية والإقليمية، في مقدمتها معاهدة الأمم المتحدة النموذجية بشان نقل الإجراءات في المسائل الجنائية لعام 1990، معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999[695]، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000[696]، وكذا النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي لعام 2003[697].

ومع إشاعة الجرائم المرتبطة بتكنولوجية الإعلام والاتصال الحديثة، زادت الحاجة إلى المساعدة القضائية الدولية عن طريق نقل الإجراءات، لكن ليس على الطريقة التقليدية والبطيئة القائمة على نقل الوثائق الخطية والمختومة عبر القنوات الدبلوماسية أو أنظمة

---

[694]– نصت هذه المادة على أنه : " **يجب على الدولة المطلوب منها أن تنفذ وفقا للنمط المنصوص عليه في قانونها الداخلي، أية رسائل تتعلق بالقضايا الجنائية، والموجهة إليها من السلطات القضائية للدول الطالبة لأغراض لحصول على شهادة، أو إرساء أشياء أو مواد لتقديمها كدليل، أو محاضر رسمية، أو أية وثائق قضائية** ".

[695]– أنظر نص المادة(09) من هذه المعاهدة ، مرجع سابق.

[696]– أنظر المادة (21) من هذه الاتفاقية، مرجع سابق.

[697]– أنظر نص المادة (16) من هذه الاتفاقية، مرجع سابق.

إرسال البريد القديمة، إنما وفق وسائل جديدة فورية وسريعة، ذات مصداقية و دقيقة بالقدر الكافي الذي يتطلبه التعامل مع هذه الجرائم[698]. وهو ما أوصت به الفقرة الثالثة من المادة (25) من الاتفاقية الأوروبية حول الجريمة الالكترونية، بنصها على انه " **يمكن لكل طرف، في حالة الاستعجال، أن يقدم طلبا للمساعدة المتبادلة أو الاتصالات عن طريق وسائل الاتصال السريعة كالفكس أو البريد الالكتروني، وذلك لما تتوفره هذه الوسائل من شروط كافية للأمن و التوثيق(بما في ذلك التشفير إن كان ضروريا)، مع التأكيد الرسمي اللاحق حينما يكون ذلك مطلوبا من طرف الدولة الموجه إليها الطلب. وعلى هذه الأخيرة المـوافقة علـى طلب المساعدة و الـرد عليه عــن طريق إحــدى وسائل الاتصال العاجلة المذكورة**" [699].

إرساء لهذا المبتغى، استحدث مجلس الاتحاد الأوروبي آلية جديدة تسمي بقضاة الاتصال (Magistrats de Liaison)[700]، وهي تقنية تسمح لكل دولة عضو بتعيين هيئة قضاة وطنية يكون اختصاصها الإشراف على عملية المساعدة القضائية الدولية و التنسيق المباشر و الفوري مع نظيرتها الأجنبية في هذا المجال. وقد ذهبت دولة فرنسا إلى أبعد من ذلك، إذ قامت بتعيين قضاة اتصال تعمل مع دول ليست أعضاء في الاتحاد كالجزائر مثلا[701]. ويكمن الدور الأساسي لهذه الآلية في تطوير وتيسير المساعدات القضائية بين

---

[698]– **جميل عبد الباقي الصغير**، الجوانب الإجرائية...، مرجع سابق، ص 86.

[699]– أنظر نص المادة (3/25) من هذه الاتفاقية، مرجع سابق.

[700]– تم تبني هذه الآلية بشكل تجربي بموجب المادة (01) من ورقة العمل المشترك المصادق عليها المجلس الأوروبي في 22 ابريل 1996 عملا بالمادة (k3) من اتفاقية إنشاء الاتحاد الأوروبي.الجريدة الرسمية للاتحاد الأوروبي العدد (L105)، صادر في 27-04-1996.

[701]– للمزيد من التفاصيل عن هذا الموضوع انظر الموقع الالكتروني:

دول الأعضاء من خلال تقصير الوقت و اختصار الإجراءات عن طريق التواصل المباشر فيما بينها، وتبادل نقل الإجراءات بعضها البعض بوسائل سريعة وضوابط ميسرة. كما تقوم هيئة قضاة الاتصال بمساعدة السلطات القضائية والأمنية في بلدها الأصلي على فهم التشريعات الوطنية للدولة الأخرى[702].

وفي نفس الإطار، سمح المجلس الأوروبي للدول الأعضاء بإنشاء ما يسمي بفرق تحقيق مشتركة (Equipes communes d'enquête)، وهي تشكيلات ظرفية ومؤقتة تتضمن أعضاء من سلطات تحقيق دولتين أو أكثر، يتم تأسيسها خصيصـــا لـلانتقال للبحث والتحقيق بكل حرية في كافة أقاليم الدول المؤسسة لها بخصوص جريمة تخصها جميعا[703].

3ـــ تبادل الإنابة القضائية الدولية: وهو طلب تتقدم به دولة ما إلى أخرى يتضمن اتخاذ إجراء قضائي من إجراءات الدعوى الجزائية في إقليمها نيابة عنها، ويكون هذا الإجراء ضروري للفصل في قضية معروضة على السلطة القضائية في الدول الطالبة[704]. وتهدف هذه الصورة من صور المساعدة القضائية إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل إقليم الدول الأخرى،

---

http://www.algeriawatch.org/fr/article/just/magistrat_liaison.htm.

[702]– **VUELTA Simon**, Les nouveaux acteurs de la coopération pénale européenne, LPA n° 13, 2005. P 4 s.

[703] - L'article (13) de la convention d'entraide pénale entre les États membres de l'Union européenne du 29 mai 2000 précise : « Les autorités compétentes de deux États membres au moins peuvent, d'un commun accord, créer une équipe commune d'enquête, avec un objectif précis et pour une durée limitée pouvant être prolongée avec l'accord de toutes les parties, pour effectuer des enquêtes pénales dans un ou plusieurs des États membres qui créent l'équipe… ».

[704]– **حازم الحارون**، الإنابة القضائية الدولية، المجلة الجنائية القومية، العدد الثاني، القاهرة، 1988، ص 20.

كسماع الشهود أو إجراء التفتيش وغيرها. وفي العادة يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية، ومن ثم إرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة المتلقية الطلب، إلا أنه وسعيا وراء الحد من الروتين والتعقيد والبطء الذي تتميز بها الإجراءات الدبلوماسية، أصبحت المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية تشترط على الدول الأطراف تعين سلطة مركزيةـ عادة ما تكون وزارة العدل ـ ترسل إليها الطلبات مباشرة لاختصار الوقت وتسريع الإجراءات بدلا من الولوج إلى القنوات الدبلوماسية التي قد تأخذ وقتا أطول[705].

تجدر الإشارة إلى أن التشريع الجزائري جاء خاليا من أي تنظيم لمسألة الإنابة القضائية الدولية، مما يعني ترك المجال لأحكام الإنابة القضائية الواردة في الاتفاقيات الدولية التي وقعت عليها الجزائر. ويمكن أن نستشهد هنا باتفاقية تبادل الإنابة القضائية الدولية المبرمة بين الجمهورية الجزائرية وفرنسا في 1962/8/28، والتي نصت على أن البلدين " يتعاونان لتقديم المعونة أو المساعدة القضائية التي تطلبها كل دولة"، كما تضمنت شروط تنفيذ الإنابة القضائية، وضوابط المحافظة على النظام العام في الدولة المرسل إليها طلب الإنابة، وكذا الجهة التي تتولى تنفيذ الإنابة، و تتحمل نفقاتها.

4ـــ تسليم المجرمين: يعتبر هذا الإجراء شكل من أشكال التعاون القضائي الدولي لمكافحة الجريمة الذي فرضته التطورات الحاصل في كافة المجالات ومنها مجال تكنولوجية الإعلام و الاتصال، إذ لم تعد الحدود الجغرافية للدول تشكل حاجزا أمام مرتكبي الجرائم،

---

[705]– نذكر منها ما وردة في المادة (27) فقرتها الثانية من اتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001، اذ نصت على انه: " 2– أ– **يجب على كل طرف ان يعين هيئة مركزية أو هيئات تكون مسئولة عن إرسال أو الرد على طلبات المساعدة المتبادلة أو تنفيذ هذه الطلبات أو إرسالها إلى السلطات المختصة.**

ب– يجب على الهيئات المركزية ان تتصل بعضها البعض بشكل مباشر... "

كما أن نشاطهم الإجرامي لم يعد مقتصرا على إقليم معين بل امتد إلى عدة أقاليم[706]. وباعتبار لا يمكن لأي دولة تجاوز حدودها الإقليمية متابعة المجرمين الفارين جزائيا، كان لا بد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها لتفادي إفلات هؤلاء المجرمين من العقاب[707].

ويرتكز أساسا هذا الإجراء، على قيام دولة يتواجد على إقليمها متهم بإحدى الجرائم العابرة للحدود ومنها الجريمة الالكترونية، أو مدان فيها بحكم قضائي، بتسليمه الى الدولة التي وقعت الجريمة على إقليمها أو التي صدر فيها حكم الإدانة، بهدف محاكمته أو تنفيذ الحكم عليه، وذلك بناء على طلب هذه الدولة وتأسيسا على معاهدة تسليم المجرمين بين الدولتين أو على أساس مبدأ المعاملة بالمثل[708]. ومن هنا يتبين أن هذا الإجراء يحقق مصلحة كلتا الدولتين المعنيتين بعملية التسليم، فهو يحقق مصلحة الدولة طالبة التسليم لأنه يضمن معاقبة الشخص الذي أخلّ بقوانينها، ويحقق مصلحة الدولة المطلوب منها التسليم كونه يساعد على تطهير إقليمها من شخص مجرم قد يشكل بقائه تهديدا لأمنها واستقرارها.

ونظرا للمصلحة المشتركة التي يحققها الإجراء المذكور، لم تتأخر معظم الدول في عقد اتفاقيات دولية وإقليمية ثائية[709] ومتعددة الأطراف لتبادل تسليم المجرمين[710]، وقد كانت

---

[706] – **El CHAER Nidal,** op.cit., p 264.

[707] - **CHAWKI Mohamed**, combattre la cybercriminalité, op.cit., p 312.

[708]– **لحمر فاقة**، إجراءات تسليم المجرمين في الجزائر على ضوء الاتفاقيات الدولية، مذكرة لنيل شهادة ماجستير في القانون، كلية الحقوق و العلوم السياسية، جامعة وهران ، 2013، ص 08.

[709]– منها اتفاقية تسليم المجرمين بين الجمهورية الجزائرية و بلجيكا لعام 1980. واتفاقية الجزائرية البريطانيا المؤرخة في 2006/6/11، والتي أثرها استلمت الجزائر المتهم عبد المؤمن خليفة. انظر: جريدة رسمية، عدد 81، صادر في 2006/12/13.

[710]– نذكر منها معاهدة الأمم المتحدة النموذجية لتسليم المجرمين لعام 1990، وملحقها الصادر في عام 1997.

الدول الأوروبية سباقة إذ أبرمت منذ 13 ديسمبر 1957 أول اتفاقية في هذا المجال، نظمت فيها أحكام التسليم، شروطه وإجراءاته. وهي الأحكام التي تم تثبيتها و تدعينها بموجب المادة(24) من اتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001، من خلال إدراج الجريمة الالكترونية ضمن الجرائم التي يجوز فيها تسليم المجرمين[711]، وكذا اقتراح بعض الحلول للمشاكل التي تثيرها عملية التسليم[712].

أما عن المشرع الجزائري، فقد اعترف بدوره بإمكانية تسليم المجرمين كإحدى تدابير المساعدة القضائية و جعل منه مبدأ دستوري ، وذلك بنصه في المادة 82 من الدستور على " **مبدأ جواز تسليم شخص بناءا على قانون تسليم المجرمين وتطبيقا له**"،[713] أما عن الأحكام الموضوعية و الإجرائية المتعلقة بعملية تسليم المجرمين فقد فصل فيها في المواد(694) وما يليها من قانون الإجراءات الجزائية.

ـ ثانيا: إقرار إجراءات جديدة للتعاون الدولي القضائي: لقد بينا كيف أن إجراءات المساعدة القضائية التقليدية، بالرغم من أهميتها، إلا أنها تتم بالطرق الدبلوماسية التي تتسم بالبطء و التعقيد، وهو ما يجعلها في غالب الأحيان غير مجدية في مواجهة الجرائم الالكترونية التي تتميز بمنتهى السرعة. نتيجة لها الوضع ظهرت الحاجة إلى البحث عن سبل بديلة للتعاون القضائي الدولي تتفق مع طبيعة هذا النوع المستحدث من الجرائم، و لعل

---

[711]– تنص المادة (24) على: **1 – أ " تطبق هذه المادة على تسليم المجرمين فيما بين الأطراف بالنسبة للجرائم المنصوص عليها في المواد من (2 – 11)من هذه الاتفاقية..."**

2– تعتبر الجرائم الجنائية الواردة في الفقرة (1) من هذه المادة مدرجة كجرائم يجب فيها التسليم في اية اتفاقية بشان تسليم المجرمين قائمة بين الأطراف، و يتعهد الأطراف بإدراج هذه الجرائم على أنها يتم فيها تسليم المجرمين في أي اتفاقية بشان تسليم المجرمين يتم إبرامها فيها".

[712]– أنظر المادة (24) فقرة 1 (ب) و الفقرات 3 ، 4، 5 و 6 منها.

[713]– أنظر المادة(82) من القانون رقم(16–01) المؤرخ في 6 مارس 2016، يتضمن التعديل الدستوري.

من ضمن هذه السبل التي وجدتها الدول استحداث إجراءات تعاون جديدة معنية بالتحقيق في الجرائم الالكترونية، وهي الإجراءات ذاتها التي تضمنها القسم الثاني من الفصل الثالث من الاتفاقية الأوروبية حول الجريمة الالكترونية و التي سنذكر على النحو التالي:

1ـــ طلب الحفظ العاجل للمعطيات المخزنة (conservation rapide de données stockées) : يعتبر هذا الإجراء آلية جديدة للتعاون القضائي الدولي في مجال مكافحة الجرائم المرتكبة عبر وسائل الإعلام والاتصال الالكترونية، والتي استحدثت بموجب المادة 29 من الاتفاقية الأوروبية لعام 2001 لتمكين أي دولة طرف في الاتفاقية من المطالبة بحفظ البيانات المخزّنة في أجهزة الحاسب الموجودة في أراضي الدولة المطلوب منها على وجه السرعة، خلال الفترة اللازمة لتقديم طلب المساعدة المتبادلة بشأنها بغرض القيام بالتفتيش، أو الدخول بأي طريقة مماثلة، وضبط، أو الحصول، أو الكشف عن هذه البيانات[714].

وفي حالة قبول الطلب المذكور، تلتزم الدولة المطلوب منها بحفظ تلك البيانات لمدة لا تقل عن ستون (60) يوما، حتى يتسن للدولة طالبة الحفظ تقديم طلب القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط، أو الحصول، أو الكشف عن هذه البيانات. ولكن بعد تلقي هذا الطلب تستمر عملية حفظ البيانات إلى غاية النظر فيه بالرفض أم بالقبول[715].

ومن مميزات هذا الإجراء أنه بمثابة تدبير تحفظي احترازي سريع تسعى من ورائه الدول إلى حماية بيانات الجريمة من أي تغيير أو إزالة أو محو قد يمسها من قبل المجرم،

---

[714]- أنظر المادة(29 فقرة 1) من الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001، مرجع سابق

[715]– أنظر المادة (29 فقرة 7) من الاتفاقية نفسها.

خاصة بعد علمه بوجود إجراءات التحقيق و المتابعة اتخذت ضده. كما يكفل المحافظة على سرية البيانات التي تهم الشخص المعني.

2ـــ طلب الكشف العاجل عن البيانات المحفوظة (divulgations rapide de données conservées): يعتبر هذا الإجراء مكمل للإجراء الأول (الحفظ السريع للبيانات) نصت عليه المادة 30 من الاتفاقية الأوروبية أعلاه، بحيث تلتزم بموجبه الدولة المطلوب منها حفظ بيانات المرور المتعلقة بأي بث أو اتصال عبر أجهزة الحاسب التابعة لها، والتي تبين لها أن هذا البث أو الاتصال انتقل من مورّد خدمات موجود في دولة ثالثة، بان تفصح وتكشف على وجه السرعة إلى الدولة مقدمة الطلب أكبر نسبة ممكن من البيانات المارة حتى يتسنى الكشف عن هوية مورد الخدمات هذا، ومصدر الاتصال، وكذا المسار الذي تم من خلاله الاتصال.

ولا يحقّ للطرف الموجه إليه هذا الطلب رفض الإفصاح أو الكشف عن البيانات المارّة إلا للأسباب نفسها المتعلّقة برفض طلب حفظ البيانات المخزّنة في جهاز الحاسب، وهي عندما ينصب الطلب على جريمة سياسية، أو من شأنه الإخلال بسيادة الدولة، أو بأمنها أو

نظامها العام، أو بمصالحها الأساسية [716].

3ـــ طلب الدخول لغرض التفتيش والضبط والكشف عن البيانات المخزنة(L'accès pour pérquisitionner, saisir, divulguer les données stockers): تم النص على هذا الإجراء في المادة (31) من الاتفاقية الأوروبية حول الجريمة الالكترونية، التي أجازت لأية دولة طرف أن تطلب من دولة طرف أخرى السماح لها بإجراء التفتيش،

[716]– أنظر المادة (30) من الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001، مرجع سابق.

أو الدخول بأية طريقة مماثلة، للكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف، بما فيها تلك البيانات المحفوظة وفقا للمادة(29) أعلاه[717].

وقد أوجبت هذه المادة على الدول الأطراف الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات الآتية:

أ-إذا كانت هناك أسباب تدعو للاعتقاد بأن البيانات المعنية معرضة لمخاطر الفقد أو التعديل.[718]

ب-إذا كانت الوسائل والاتفاقيات والتشريعات الواردة في الفقرة 2 تستلزم تعاونا سريعا.

أكثر من ذلك، فان المادة (32) من الاتفاقية ذاتها تسمح للأي دولة طرف بالولوج للبيانات المخزنة داخل إقليم دولة طرف أخرى دون الحصول على إذن مسبق من هذه الأخيرة، بشرط أن يتم ذلك بموافقة صاحب الجهاز المخزّن فيه تلك البيانات أو الذي يتمتع بسلطة الإفصاح عنها، أو تكون هذه البيانات متاحة للجمهور.

4ـ تبادل المساعدة لجمع البيانات في الوقت الحقيقي (entraide dans la collecte en temps réel de données relative au trafic): بيّنا فيما سبق أنه عادة ما يستغرق المحققون وقتا كثيرا في تعقب اتصال الكتروني ما قبل الوصول إلى مصدره، وقد يحدث أثناء هذه الفترة إقدام مورد الخدمات على محو بيانات المرور المتعلقة

[717]- أنظر الفقرة الأولى من المادة (31) من الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001، مرجع سابق.

[718]- أنظر الفقرة الثالثة من المادة(31) من الاتفاقية نفسها.

بهذا الاتصال قبل التمكن من حفظها. الأمر الذي يحول دون إمكانية الحصول على هذه البيانات في وقتها الحقيقي.

ولحل هذه المشكلة، وضعت المادة (33) من الاتفاقية الأوروبية المنوه عنها أعلاه التزاما على الدول الأطراف بالتعاون بعضها البعض في جمع بيانات المرور المرتبطة بالاتصالات الجارية عبر إحدى وسائل الاتصال المتواجدة على إقليمها في وقتها الحقيقي.

وبما أنّ جمع البيانات المرور في وقتها الحقيقي يشكّل الوسيلة الأولى لتحديد هوية المجرم الالكتروني، ونظراً لطبيعة هذا الإجراء الذي يقلّ تطفّلاً على الخصوصية عن غيره من إجراءات البحث والتحقيق، فقد أوصت الاتفاقية الدول الأطراف بتقديم أوسع مساعدة ممكنة في هذا الشأن ولو في غياب شرط التجريم المزدوج.

ومع هذا، فقد يحدث ألا يكفي جمع بيانات المرور الخاصة بالاتصال في وقتها الحقيقي وحده لإزالة اللثام عن حقيقة الجريمة و المجرم الالكتروني، بل يتطلب الأمر كذلك الاطلاع على البيانات الخاصة بمحتوى وفحوى هذا الاتصال. لذلك جاءت المادة (34) من الاتفاقية الأوروبية أعلاه لتستجيب لهذه الضرورة، من خلال السماح للدول الأطراف بالتعاون في مجال اعتراض و التقاط البيانات المتعلقة بمضمون الاتصالات النوعية التي تتم عن طريق إحدى شبكات المعلومات[719].

ومن أجل إضفاء الفعالية والحيوية على مختلف صور المساعدة القضائية الدولية السالفة الذكر، ألزمت المادة (35) من الاتفاقية المذكورة كل دولة طرف بإنشاء نقطة اتصال وطنية تعمل 24 ساعة طوال أيام الأسبوع، تكون مهمتها ضمان توفير المساعدة المباشرة و

[719]– أنظر نص المادتين(33 و 34) من الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001، مرجع سابق.

الفورية في مجال التحقيقات و المتابعات الجزائية المتعلقة بالجرائم الالكترونية للسلطات القضائية التابعة للدول الأطراف الأخرى[720].

وتجدر الإشارة إلى أن المشرع الجزائري لم ينص بشكل صريح على هذه الإجراءات الجديدة للتعاون القضائي الدولي، ولكن يمكن أن نجد لها مكان في تفسير نص المادة (16) من القانون (04/09) المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها، إذ جاءت هذه المادة(16) بصيغة العموم بنصها على أنه " **في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن لسلطات المختصة تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني** ".

ينبغي التنويه بأن الاتفاقية الأوروبية حول الإجرام الالكتروني أوجدت حلولا فعالة من شأنها التغلب على الكثير من المشاكل و العقبات التي تواجه عملية التحقيق والمتابعة الجزائية في الجرائم الالكترونية عبر الوطنية، خاصة ما تعلق منها باختلاف النظم الإجرائية أمام التعاون الدولي، ومشكلة الاختصاص والولايات القضائية، ومشكلة التجريم المزدوج، وعدم وجود قنوات اتصال دولية مباشرة بين سلطات إنفاذ القانون، وكذا الصعوبات الأخرى الخاصة بالمساعدة القضائية الدولية والتباطئ في الردّ عيها. لذلك ينبغي على جميع الدول خاصة المتخلفة منها الإسراع إلى تبني هذه الحلول، وذلك إما بإدراجها ضمن قوانينها الداخلية ثم الالتزام بالعمل بها، أو من خلال الانضمام إلى الاتفاقية الأوروبية (ما دام أنها متاحة للتوقيع من جميع الدول) ومن ثم يسري عليها من هذه الأحكام ما يسري على الأطراف الأخرى.

[720]– أنظر نص المادة(35) من الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001، مرجع سابق.

المطلب الثاني

الاستعانة بالتدابير الوقاية والحماية الفنية

أثبتت العديد من الدراسات المتخصصة[721] بأن إتباع أسلوب الردع و العقاب الجنائي وحده لا يشكل حلا كافيا لمكافحة الجرائم الالكترونية، فحتى تكون هناك الفعالية في الحركة والأداء لابدّ أن يعزز هذا الأسلوب بوسائل الوقاية والحماية الفنية التي تعمل على الحيلولة دون وقوع هذه الجرائم، أو الإنذار بها بمجرد وقوعها.

وما يهمنا أكثر في هذه التدابير ليس الدور الوقائي الذي تلعبه في منع حدوث الجريمة الالكترونية، إنما كونها وسيلة فعالة تستعين بها سلطات التحقيق للكشف عن هوية المجرم الالكتروني من خلال الاطلاع على المعلومات و البيانات التي يخلفها فيها عن محاولاته لارتكاب الجريمة. وهو ما يجعلها مخرجا مهما لمعضلتي سهولة اختفاء وتعديل الدليل الالكتروني و صعوبة اقتفاء آثار المجرم الالكتروني[722].

ويمكن تقسيم هذه التدابير حسب غرضها المذكور إلى أنظمة الحماية الفنية الكترونية (الفرع الأول)، و وسائل الوقائية الأخرى (الفرع الثاني).

---

[721]– نذكر منها، الدراسة التي أعدها مؤتمر كاركاس سنة 1980، والتي أوصى فيها بضرورة إرساء سياسة وقائية شاملة من الجريمة، باعتبارها مكملة للسياسة الاجتماعية العامة. والدراسة التي أعدها مؤتمر للأمم المتحدة الثامن لمنع الجريمة و معاملة المجرمين (هافانا) سنة 1990، والتي أوصت كذلك بضرورة إعداد البرامج الوقائية في مجال الجريمة المنظمة. أنظر: **عادل يحي**، مرجع سابق، ص 111.

[722] - **CHAWKI Mohamed**, combattre la cybercriminalité, op.cit. 248.

الفرع الأول: تقنيات الحماية الفنية مصدرا موثوقا لإثبات الجريمة الإلكترونية

تتحقق هذه العملية بتزويد وسائل الاتصالات الالكترونية منها الحواسيب الآلية ببرمجيات وتطبيقات تكفل الحماية الكافية للمعلومات الالكترونية من خلال التعريف بالمستخدم وموثوقية الاستخدام ومشروعيته، وكذا ضمان سرية المعلومات، تكاملها واستمرارها وسلامة محتواها. وهو ما يرشحها لان تكون مصدر غنيا وموثوقا للأدلة الالكترونية. وتتعدد تقنيات الحماية الفنية المتعين استخدامها في بيئة المعالجة الآلية إلى الحماية عن طريق البرامج (أولا)، والحماية عن طريق الرقابة الوقائية(ثانيا).

أولا ـــ الحماية الفنية عن طريق البرامج الأمنية: وهي الحماية التي يتم توفيرها اعتمادا على البرامج الأمنية التالية:

1ـ برامج التعريف بالشخص المستخدم وموثوقية الاستخدام ومشروعيته: وتهدف هذه البرامج إلى ضمان استخدام الجهاز أو النظام أو الشبكة من قبل الشخص المرخص له بهذا الاستخدام فقط، وتضمّ هذه الطائفة كلمات السر بأشكالها المختلفة، رموز المرور، بطاقات التعريف الذكية، ووسائل التعريف البيومترية التي تعتمد على سمات معينة في الشخص المستخدم متصلة ببنائه المرفولوجية، كبصمة اليد أو الأصبع، أو بصمة العين أو الوجه، بصمة الصوت، البصمة الوراثية، أو متصلة بتصرفاته مثل طريقة التوقيع، طريقة استخدام لوحـــة المفاتيح، طريـقة التنفس. كمـا تضم أيضـا مفـاتيح التشفير، ومـا يعرف بالأقفـال الالكترونية التي تحدد دخولها لأشخاص بذاتهم[723].

[723] -**ASSEMBLE NATIONALE FRANÇAISE**, rapport sur les méthodes scientifiques d'identification des personnes a partir de données biométriques et les techniques de mise en œuvre, Paris, juin 2003. Sans numérotation.

2- برامج التحكم في النفاذ إلى الشبكة: تهتم هذه البرامج أساسا بالحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات، وكذا التأكد من أن الشبكة قد استخدمت بطريقة مشروعة[724]. ومن أهمها ما يعرف بالجدران النارية (fire wall) الذي يثبت داخل نظام الحاسب بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من و إلى الجهاز أثناء التعامل مع شبكة الانترنت، فيبدأ بإجبار جميع عمليات الدخول إلى الشبكة أو الخروج منها، على المرور من خلال هذا الجدار الناري، ثم يقوم بصدّ المستخدمين غير المرغوب فيهم عن الوصول إلى الشبكة، عن طريق مراقبة الحزم التي يتم إرسالها واستقبالها من الحاسب الآلي الخاص بالمستخدم، وتنبيه هذا الأخير بذلك[725].

ومن مزايا هذه البرامج، أنها تقوم بتسجيل وتخزين جميع العمليات والمعلومات والبيانات التي تمرّ عبرها، وهو ما يسمح لسلطات البحث والتحقق استخدام بعض الوسائل المساعدة لتحليل هذه العمليات وتتبع محاولات الدخول إلى النظام و رصد المعلومات الكاملة عن هذا الاختراق، من حيث الزمان و المكان، من ثم معرفة المجرم.

3ــ برامج الحفاظ على سرية المعلومات: الغرض منها ضمان عدم إفشاء المعلومات للجهات غير المصرح لها بذلك، وتشمل تقنيات تشفير المعطيات والملفات، إجراءات حماية نسخ الحفظ الاحتياطية، ومختلف برامج التمحيص و الغربلة (filtration).

4ــ برامج حماية التكاملية وسلامة المحتوى: يكمن دور هذه البرامج في حماية محتوى المعطيات أو البيانات الالكترونية من مخاطر العبث بالتعديل أو الإتلاف أو الإلغاء من قبل جهة غير مخول لها بذلك، بعد الاطلاع عليها أو أثنــاء عملية إدخالها أو نقلها. و من بين

---

[724]- **أشرف السعيد احمد**، تكنولوجيا المعلومات في المجال الأمني، مطابع الشرطة، القاهرة، 2013، ص 69.

[725]- **ياسر محمد الكومي محمود أبو حطب**، مرجع سابق ، ص 402.

أهم هذه البرامج، تقنيات (PDF)، ومختلف برامج مضادات الفيروسات(antivirus)[726].

5ــ برامج منع إنكار التصرف: مهمة هذه البرامج هو تأكيد انتساب تصرف ما على الوسائل الالكترونية إلى مصدره الحقيقي، و ضمان عدم قدرة شخص المستخدم من إنكار التصرف الذي صدر عنه، أو إنكار بأنه هو مصدر هذا التصرف. وتكمن هذه البرامج في تقنيات التوقيع الالكتروني، و شهادات التوثيق الصادرة عن الطرف الثالث[727].

6ــ برامج مراقبة الاستخدام وتتبع سجلات النفاذ والأداء: وتتمثل في مختلف التقنيات التي تستخدم لمراقبة العمليات الالكترونية الجارية على نظام حاسب معين، وتحديد مصدرها والوقت والمدة التي استغرقتها، وتسجيل كل ذلك في ملفات خاصة يطلق عليها (Logs). ومن ضمن هذه البرامج نذكر:

أ-**برنامج (tracer):** وهو برنامج يتولى تقديم تقارير مفصلة حول المسار الذي سلكه مستخدم شبكة الانترنت من خلال تحديد موقع الولوج و عنوانه الشخصي (IP)، المواقع والصفحات التي اطلع عليها، الوقت والفترة التي قضاها في كل صفحة أو موقع، ومختلف العماليات التي أجراها وتحديد نوعها.

ب-برنامج (net stat) : وهو برنامج مناط به عرض جميع الاتصالات التي أجراها المستخدم، ومنافذ التصنت، وعرض المنافذ والعناوين بصورة رقمية، و تقديم تقرير كامل لجدول التوجه[728].

---

[726]- **أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، بدون دار النشر، القاهرة ، 2005، ص.ص147 -149.

[727]- **أيمن عبد الحفيظ**، مرجع سابق، ص.ص151-152.

[728]- **حسين بن سعيد الغافري**، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مرجع سابق، ص.ص 17-18.

ج-برنامج كشف الاختراق (IDS) : يتولى مراقبة العمليات التي يجرى حدوثها على أجهزة الحاسب أو شبكة الانترنت و تحليلها بحثا عن أية إشارة قد تنبئ بوجود خطر قد يهدد أمن الحاسب أو الشبكة. وفي حالة اكتشاف النظام وجود هذا التهديد يقوم برصد كل البيانات المتعلقة به، مصدره، طبيعته، ودرجة خطورته، من ثم إنذار صاحب النظام فورا بهذا التهديد[729].

والملاحظ في هذه التدابير هو أنه بالإضافة إلى كونها إجراءات وقائية فعالة لمنع وقوع الجرائم الالكترونية أو الإنذار عنها فور وقوعها، فهي أيضا مفيدة جدا لعملية التحقيق والإثبات في هذه الجرائم، إذ تقدم معلومات قيّمة و موثوقة لفريق التحقيق تساعده على فهم لغز الجريمة، وتحديد معالمها وإبعادها، وإظهار أسلوب ارتكابها، مما قد يضفي إلى الكشف عن مرتكبها.

واعتبارا لهذه الأهمية، فقد أجاز المشرع الجزائري الاستعانة بهذه التدابير لغرض التحقيق في الجرائم الالكترونية، وذلك حينما ألزم في نص المادة(10) من الفصل الرابع من القانون رقم (09-04) مقدمي الخدمات بالعمل على حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، من خلال تحديد مصدر الاتصال و مكانه، تاريخ و وقت ومدة كل اتصال، بالإضافة إلى حفظ المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها[730].

ثانيا- الحماية الفنية عن طريق أنظمة الرقابة الالكترونية الوقائية: يعد نظام الرقابة الالكترونية أهم آليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الحديثة،

---

[729]- **أشرف السعيد أحمد**، مرجع سابق، ص78.

[730]- أنظر المادة (10) من القانون رقم (04/09) المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

إذ تسمح بالرصد المبكّر للاعتداءات المحتملة على النظام والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، من ثم القبض عليهم ومحاكمتهم. فهي بذلك تختلف تماما عن وسائل الرقابة الالكترونية التي تتخذ بعد وقوع الجريمة الالكتروني أو بمناسبة البحث والتحقيـق فيـها كـاعتراض المراسلات والتقـاط الصـور، الجـمع والحـفظ والكـشف العـاجل لمعطيات المرور أو المحتوى.

ويقصد بالرقابة الالكترونية للاتصالات، العمل الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع معطيات ومعلومات عن المشتبه فيه، سواء تعلق الأمر بمراقبة شخص أو مكان أو شيء حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني[731].

وتتم هذه العملية بواسطة أجهزة الكترونية ذات تكنولوجية عالية تضمن الرقابة بصفة مستمرة دون انقطاع حسب الغرض، وغالبا ما يتم ربط هذه الأجهزة بأنظمة الإنذار أو الإشارة التي تتولى الإخبار أو التبليغ عن الخطر، أو عن وقوع جريمة الكترونية كلما اكتشفت أجهزة المراقبة ذلك. مع العلم أن هناك من أنظمة إنذار ما هو متصل مباشرة بمراكز الأمن فتقوم بإرسال الإشارة من دائرة المراقبة إلى وحدة الشرطة[732]، وهو ما يجعلها تؤدي دور المبلّغ عن الجريمة، وبالتالي تشكل مخرجا لعقبة الإحجام عن التبليغ بالجريمة.

ولقد أدرج المشرع الجزائري هذه الآليات ضمن الوسائل المفيدة للوقاية من الإجرام الالكتروني ومكافحتها التي استحدثها في القانون رقم (04/09)، حينما نص في المادة(03) منه على إمكانية وضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها، كلما تطلبت ذلك حماية النظام العام أو مستلزمات التحريات أو

---

[731]– **بوكر رشيدة**، مرجع سابق، ص 370.

[732]–**أيمن عبد الحفيظ**، مرجع سابق، ص.ص 118–119.

التحقيقات القضائية الجارية، وذلك مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات.

ليس هذا فحسب، بل أنشأ المشرع الجزائري بموجب المادة (13) من القانون رقم (04/09) هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وجعل من مهامها الأساسية ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم الالكترونية منها المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.[733] وإرسال المعلومات المتحصل عليها من هذه العملية إلى سلطات الأمن والقضاء المختصة[734].

الفرع الثاني: التوعية و التحسيس

لقد سبق البيان أنه من ضمن العقبات التي تعتري عملية البحث والتحقيق في الجرائم الالكترونية، تقاعس المجني عليه عن الإبلاغ بوقوع الجريمة، ما قد يستغرق اكتشافها من قبل سلطات الضبط القضائي وقتا كبير، قد يحول دون الوصول إلى الأدلة والقرائن في الوقت المناسب أو عدم الوصول إليها إطلاقا، بسبب إمكانية محوها أو التخلص منها بسهولة في الفترة بين حدوث الجريمة واكتشافها.

ومن أجل التصدي لهذه العقبة اتخذت عدة مبادرات جريئة منها، إقرار قاعدة تجريم عدم الإبلاغ عن الجريمة، وذلك من خلال وضع نصوص عقابية تعتبر الشخص الذي يعلم بوقوع جريمة الكترونية ويتماطل في تبليغ سلطات الأمن عنها، شريكا فيها يستوجب معاقبته. ولكن رغم اشتقاق هذا الحل من المنطق ذاته الذي تقوم عليه جريمة "**عدم مساعدة شخص**

---

[733]– أنظر المادة(04 فقرة 06) من المرسوم الرئاسي رقم (15–261)، المحدد لتشكيلة و تنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مرجع سابق.

[734]– أنظر المادة (11 فقرة 03) من المرسوم الرئاسي رقم (15–261)، المرجع نفسه.

في حالة خطر"، إلا انه لم يفعّل، وسرعان ما استبدل بقاعدة أخرى تعرف بالالتزام برفع شكوى (L'obligation de porter plainte)، وهذه القاعدة و إن تمّ فعلا العمل بها في بعض الولايات الأمريكية كجيورجيا و آوتاه، إلا أنها لقيت رفضا كبير من غالبية دول العالم بحجة تناقضها مع منطق التجريم و العقاب، إذ لا يعقل معاقبة الضحية فقط لمجرد عدم انصياعه للقانون الذي يقضي بواجب التبليغ، في حين يترك المجرم الحقيقي حرا طليق[735].

أمام هذا الوضع، لم تجد الدول حلا أخر لمشكلة الإعراض عن التبليغ بالجريمة الالكترونية إلا اللجوء إلى سياسة التحريض على التبليغ (L'incitation a la dénonciation)، وذلك عن طريق وضع تحت تصرف مستخدمين الانترنت آليات سهلة ومجانية تشجع المتضررين من جريمة على التبليغ عنها إلى سلطات الأمن، كإنشاء ما يسمى بخطوط اتصال خضراء أو الأرقام الساخنة[736]، وهي قنوات مرتبطة مباشرة بمصالح الأمن، تسمح لأي شخص الاتصال من أي مكان وفي كل وقت وحين وبدون أن يكشف عن هويته، للإبلاغ عن وقوع جريمة الكترونية ما. أو خلق لدى مراكز الأمن بوابات أو أنظمة الكترونية تعمل (24سا/24سا) مخصص لاستقبال شكاوى أولية عبر الانترنت (Pré-plainte)[737]، كما فعلت المملكة السعودية بإنشائها نظام استقبال الشكاوي الالكترونية " **أبشر**"، والجزائر باستحداثها مؤخرا موقع للشكاوى الأولية لدى مصالح الدرك الوطني يسمي (PPGN.MDN.DZ). ومن أجل تفعيل وتعزيز هذه الآلية قامت بعض شركات التامين

---

[735] -**VERGUCHT Pascal**, op cit, p 326 - 327.

[736]. نذكر منها الرقم الساخن في مصر وهو (108)، الرقم (1909) في المملكة السعودية، الرقم الأخضر للشرطة (1548) في الجزائر.

[737]– سميت بشكاوى أولية لأنها عبارة عن بلاغ يقدمه الشخص عبر الانترنت، لا يتم بموجبه مباشرة إجراءات المتابعة الجزائية إلا بعد انتقال المبلغ أو الشاكي شخصيا إلى مركز الأمن لتأكيد و تدعيم بلاغه .

في بعض الدول بإدراج شرط رفع شكوى ضمن بنود عقد التأمين الالكتروني الذي يؤدي تخلفه إلى فقدان الحق في التعويض[738].

ومع ذلك، فقد كشفت الدراسة الاستقصائية التي أجرها مؤخرا فريق خبراء حول الجريمة السبيرانية والتدابير التي تتخذها الدول والمجتمع الدولي والقطاع الخاص للتصدي لها[739]، بأن أحسن وسيلة للقضاء على مشكلة العزوف عن التبليغ بالجريمة الالكترونية بل لمنع وتفادي وقوعها هي التوعية والتحسيس، وذلك من خلال تنظيم حملات زيادة الوعي العام تشمل كل شرائح المجتمع، والمؤسسات والإدارات العمومية، بما فيها حملات التوعية بالتهديدات والمخاطر الناشئة عن هذا النمط الإجرامي، وعن سياسات وممارسات تدبّر هذه المخاطر والوقاية منها. وكذا تحسيسهم بأن مهمة الإفصاح عن الجريمة الالكترونية ومكافحتها هي مسؤولية مشتركة وتستلزم تضافر جهود الجميع دون استثناء[740].

وفي هذا الإطار، تؤدي المؤسسات الأكاديمية مجموعة متنوعة من الأدوار، منها تثقيف المهنيين وتدريبهم، اقتراح القوانين والسياسات، والعمل على تطوير المعايير والحلول التقنية لظاهرة الاجرام الالكتروني. كما تقوم الجامعات بنشاطات وتظاهرات علمية (ندوات، ملتقيات وأيام دراسية) في هذا الشأن تشرك فيها خبراء في مجال الجرائم الالكترونية ومختصين في مواجهة الطوارئ الحاسوبية ، للاستفادة من مهاراتهم و خبرتهم وما يضطلعون به من أعمال.

---

[738] **VERGUCHT Pascal,** op cit, p 328.

[739]-**GROUPE D'EXPERTS ,** Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, UNODC, Vienne, 25-28 février 2013, p 17.

[740]-**BRETANT Thierry,** chantier sur la lutte contre la cybercriminalité, op.cit. p 11.

بالإضافة إلى ذلك، فقد أشادت بعض الدراسات بأهمية إشراك القطاع الخاص بشكل عام(مؤسسات اقتصادية، مزودي الخدمات، جمعيات، مجتمع مدني) في مهمة التصدي ومنع الجرائم السبيرانية، وذلك من خلال توقيع اتفاقات وشراكات غير رسمية بين القطاع العام والخاص يلتزم فيه الطرفين معنويا على تيسير تبادل المعلومات عن التهديدات التي تثيرها هذه الجرائم، والعمل ندا لند على تنفيذ السياسة الوقاية التي ترسمها الدولة[741].

[741]-**CISSE Abdoullah,** Exploration sur la cybercriminalité et la sécurité en Afrique : État des lieux et priorités de recherche - Synthèse des rapports nationaux, Centre de recherches pour le développement international(CRDI), 2011, pp 47, 49-50 . voir aussi. **GROUPE D'EXPERTS, op.cit.,** p 18.

الخـــاتمة:

تتضمن هذه الدراسة في متنها إيضاحا لرؤية إجرائية تتناول مسألة البحث و التحقيق الجنائي في الجرائم الإلكترونية، والمشكلات الإجرائية المترتبة عليها، وكذا الحلول الممكنة المقترحة لمعالجة تلك المشكلات.

وقد اتضح لنا أن الجرائم الإلكترونية تعد من الأنماط الإجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد، و التي تتميز بخصائص مختلفة تماما عن الجرائم التقليدية، وأنها من المستجدات التي لم تكن معروفة في القانون الجزائي بشقيه الموضوعي والإجرائي، من ثمة فأي محاولة للتعامل إجرائيا مع هذا النمط الإجرامي الجديد في إطار عملية البحث والتحقيق سوف يخلق إشكالات إجرائية أمام السلطات المكلفة بهذه العملية.

وتتجلى أولى هذه الإشكالات في القصور الذي يعتري النصوص الجزائية الإجرائية القائمة في مواجهة مثل هذه الجرائم، لأن أحكام هذه النصوص إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها مع خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع.

وقد بينا أنه من أجل تغطية و تلافي هذا القصور من جهة، وتفادي إفلات المجرم الالكتروني من المتابعة الجزائية و العقاب، بادر المشرع في الكثير من الدول إلى إعادة النظر في بعض القواعد الإجرائية المتعلقة باستخلاص الدليل كالتفتيش و الضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية الالكترونية. فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع الطبيعة الخاصة التي يتميز بها هذا النوع من الجرائم، كالمراقبة الالكترونية واعتراض المراسلات والتسرب الالكتروني، وهو ما أقدم عليه المشرع الجزائري من خلال

الخـاتمة:

تعديل قانون الإجراءات الجزائية في عام 2006، وإصداره القانون رقم (04/09) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

في السياق ذاته تبين أن الإجراءات الجديدة لاستخلاص الدليل في البيئة الالكترونية قد تشكل خطرا كبيرا يهدد الحق في الخصوصية، نظرا لما تتيحه لسلطات التحقيق من إمكانية الاطلاع على أسرار خاصة بأشخاص قد لا يكون لهم يد في الجريمة، مما جعل المشرع يحرص كل الحرص على حصر اللجوء إلى هذه الإجراءات في الحالات التي تستدعي ضرورة التحقيق والتحري الى ذلك، كما أحاطها بجملة من الضمانات القانونية التي يتعين على المحقق احترامها عند استعماله لهذه الإجراءات.

وقد أظهرت الدراسة كذلك أنه من المشكلات التي تواجه سلطات البحث و التحقيق ما يتعلق بالقيمة القانونية للأدلة الالكترونية المتحصل عليها في عملية الإثبات الجنائي أو بمعنى أخر مدى قبول هذه الأدلة كوسيلة إثبات من طرف القاضي الجزائي، إذ أن عملية استخلاص الدليل الالكتروني سواء بالطرق الإجرائية التقليدية أو المستحدثة ليست بالسهولة بما كان، بل تعيقها في غالب الأحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الالكتروني أو بالعامل البشري. كما أن مجرد وجود دليل يثبت وقوع الجريمة ونسبتها الى شخص معين قد لا يكفى للتعويل عليه، بل يلزم أن يكون لهذا الدليل قيمة قانونية، التي تتوقف على مسألتين أساسيتين، الأولى هي مشروعية الدليل، والثانية هي حجيته على الوقائع المراد إثباتها.

فالأدلة الإلكترونية وإن كانت تتمتع بقيمة علمية قاطعة في الدلالة على الحقائق التي تتضمنها، إلا أن ذلك لا يغني عنها ان تكون مشروعة، سواء من حيث الوجود، بان تكون من ضمن الأدلة المقبولة قانونا كوسيلة إثبات. أو من حيث التحصيل، وذلك بان يتم

الحصول عليها بالطرق القانونية وأن تقدم للمحكمة على الهيئة نفسها التي تم جمعها عليها، بدون أن يطرأ عليها أي تغيير أو تحريف خلال فترة حفظه.

وقد استخلصنا أيضا بأن مسألة قبول الدليل الالكتروني من عدمه إنما تخضع لمطلق تقدير القاضي الجزائي، الذي يتمتع بدور ايجابي في مناقشة وموازنة القيمة القانونية للدليل الالكتروني قبل أن يطمئن إليه، شأنه في ذلك شأن باقي الأدلة. ولكن أكدنا في الوقت نفسه أنه لا يجب الخلط بين القيمة العلمية القاطعة للدليل الالكتروني، التي لا يملك للقاضي الفصل فيها لأنها مسألة فنية بحتة والقول فيها هو قول أهل الاختصاص، وبين الظروف والملابسات التي تحيط بالدليل، و التي يجوز للقاضي أن ينصّب نفسه فيها مكان الخبير ويطرح رأيه وفق أسباب سائغة مقبولة، وله في ذلك أن يرفض هذا الدليل إن لم يقتنع بظروف القضية وملابساتها.

بالموازاة مع ذلك اتضح أن عملية البحث والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الحديثة تتخللها عقبات كثيرة، يعود البعض منها إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم ، فالطابع العابر للحدود الذي تتسم به الجريمة الالكترونية قد يثير العديد من المشاكل القانونية، من بينها تحديد الدولة التي يختص قضاءها بملاحقة مرتكب هذه الجريمة، والمعيار المعتمد في ذلك، ناهيك عن مشكلة احترام سيادة الدولة التي تقف حاجزا امام سلطات التحقيق عندما يستوجب البحث عن أدلة إثبات جريمة الكترونية خارج الإقليم الوطني وفي أقاليم عدة دولة أجنبية، خاصة إذا اقترن ذلك بغياب وسائل وآليات دولية فعالة تضمن التعاون القضائي والأمني بين الدول في هذا المجال.

أما البعض الأخر فمرده هو قصور القواعد الإجرائية عن مواكبة تطورات ومتغيرات الجرائم الالكترونية المتسرعة، ما قد يقف حجر عثرة في سبيل الاستفادة من معطيات التكنولوجيا الحديثة في الكشف عن الجرائم الالكترونية وملاحقة مرتكبيها.

الخـاتمة:

ومن أجل تجاوز هذه العقبات والمشكلات، نقدم جملة من الحلول التي نعتقد انها فعالة وممكنة التجسيد، وهي حلول مستوحاة من تجارب بعض الدولة المتقدمة و كرستها عدد من القوانين والاتفاقيات الدولية على رأسها الاتفاقية الأوروبية حول الجريمة الالكترونية المبرمة في بودابست عام 2001، و التي أردنا أن نعرضها في شكل اقتراحات على النحو التالي :

- يتعين على الدول التي لم تسن بعد قوانين جزائية موضوعية وإجرائية خاصة بالجرائم الالكترونية، كما هو الحال بالنسبة لغالبية الدول العربية، الإسراع إلى تعديل وترشيد قوانينها القائمة بما يجعلها تسرى وتطبق على مثل هذه الجرائم، وذلك لتفادي القصور التشريعي وتخطي الثغرات القانونية الحاصلة في هذا المجال، التي قد يستفيد منها المجرم الالكتروني للإفلات من المتابعة الجزائية و العقاب.
- لا يكفي الاعتماد على التشريعات القائمة لتجاوز الصعوبات الإجرائية التي تثيرها عملية البحث والتحقيق في الجرائم الالكترونية، بل لا بد من تدعيمها بنصوص خاصة حديثة تتضمن إجراءات تحقيق ملائمة مع طبيعة هذا الشكل الجديد من الإجرام، ومسايرة للمتغيرات والتطورات الحاصلة في تقنيات وأساليب ارتكابها. كما فعل المشرع الجزائري من خلال القانون رقم (09-04) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. حينما استحدث تقنيات ومعالم جديدة توضح القواعد الإجرائية في مجال تحريك و مباشرة الدعوى الجزائية وإتباع آثار المجرم الالكتروني من خلال تحديد الترتيبات التقنية للمراقبة الالكترونية، وكيفية تفتيش المنظومة المعلوماتية عن بعد، ثم إجراءات حجز المعطيات الالكترونية، ورسم معالم الاختصاص القضائي تحسبا للطابع الدولي الذي تكتسيه الجرائم الالكترونية .
- ضرورة تكثيف التعاون والتنسيق الدولي بين الدول من اجل تطوير وتوحيد التشريعات الجزائية الموضوعية والإجرائية التي تعنى بمكافحة الجرائم الالكترونية، عن طريق إبرام

اتفاقيات دولية وإقليمية ثنائية ومتعددة الأطراف في هذا المجال، أو الانضمام إلى الاتفاقيات المبرمة في هذا الخصوص كالاتفاقية الأوروبية حول الجريمة الالكترونية المبرمة في بودابست عام 2001، مع مراعاة المصلحة الوطنية و مبدأ السيادة .

- ضرورة اعتماد سياسة واضحة وفعالة بخصوص التعاون الأمني المتبادل والمساعدة القضائية والفنية بين الدول في مجال مكافحة الجريمة الالكترونية، من خلال تبني إجراءات التحقيق والمتابعة الجزائية السريعة والمناسبة، وخلق قنوات اتصال ثنائية أو متعددة الأطراف تسمح للسلطات القائمة على التحقيق، الاتصال بسهولة بمثيلتها الأجنبية والتنسيق معها. أو التدخل السريع للتحقيق في إقليم دولة أجنبية دون ان يشكل ذلك مساسا بسيادة هذه الدولة.
- دعوة الدول العربية إلى إنشاء منظمة شرطة عربية تهتم بالتنسيق الامني في مجال مكافحة الجرائم المعلوماتية عبر الانترنت ؛ مع تشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي.
- ضرورة إنشاء وحدات أمن وأجهزة قضائية متخصصة في مكافحة الجرائم الالكترونية، يكون لديهم الإلمام الكافي بالجوانب التقنية والفنية لمتابعة وكشف وضبط تلك الجرائم ومرتكبيها، مع إخضاعهم لبرامج تدريبية خاصة دورية ، تساعدهم على تحيين و تحديث معارفهم و خبراتهم و اطلاعهم بآخر المستجدات الحاصلة مجال التقنية المعلوماتية.
- إتاحة الفرصة للمواطنين للمشاركة في مكافحة الجرائم الالكترونية؛ من خلال إنشاء خطوط ومواقع اتصال ساخنة أو خضراء تعمل على مدار الساعة، و تسمح لأي كان بالإبلاغ عن بعد بوقوع جريمة الكترونية دون قيد أو شرط.
- ضرورة نشر الوعي في أوساط المجتمع بالمخاطر الاقتصادية والاجتماعية و النفسية وغيرها الناجمة عن الاستخدامات غير المشروعة وغير الآمنة للانترنت، وبما يترتب عنها من انعكاسات سلبية على حياة الفرد والمجتمع.

الخـاتمة:

- تفعيل دور المجتمع المدني و الحراك الجمعوي المؤهل في التحسيس والوقاية من الوقوع في الممارسات الخاطئة والسلوكيات الإجرامية عبر شبكة الانترنت.
- يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم ما قبل الجامعي .
- دعوة المؤسسات التعليمية المعنية بتأهيل الأطر القانونية إلى تضمين موضوع الإجرام الالكتروني أو المعلوماتي ضمن خططها الدراسية.
- ضرورة اهتمام الباحثين و رجال القانون الجزائريين بالدراسات القانونية التي تعنى بالجوانب الإجرائية للجرائم الالكترونية والعمل على إثراء محتواها، لأنها لم تنل بعد حظها من البحث والتشريح، و لا تزال لحد اليوم في منطقة الظل في بلادنا رغم ما يثيره الزحف الهائل للإجرام الالكتروني من مخاطر.

في الختام، فإنني لا أزعم من خلال هذا البحث بلوغي جادة الصواب، ولكن أملي أن يحقق قدر من العزم منه، وما أنا إلا بشر اجتهد فأخطئ و أصيب، فان أصبت فأجري على الله وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين، ولله الأمر من قبل ومن بعد، والحمد لله رب العالمين.

قائمة المراجع

-اولا: المراجع باللغة العربية

أ- الكتب:

1-**أحمد يوسف الطحطاوي**، الأدلة الالكترونية و دورها في الإثبات الجنائي، دار النهضة العربية، القاهرة ، 2015.

2-**أسامة أحمد المناعة**، جرائم الحاسب الآلي و الانترنت، دار وائل للنشر، عمان، 2001.

3-**إسحاق إبراهيم منصور**، المبادئ الأساسية في قانون الإجراءات الجزائية الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1995.

4-**أشرف السعيد احمد**، تكنولوجيا المعلومات في المجال الأمني، مطابع الشرطة، القاهرة، 2013.

5-**العربي شحط عبد القادر و نبيل صقر**، الإثبات في المواد الجزائية، دار الهدى، الجزائر، 2006.

6-**أمال قارة**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، طبعة ثانية ، دار هومة للطباعة و النشر والتوزيع، الجزائر، 2007.

7-**أيمن عبد الحفيظ**، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، بدون دار النشر، القاهرة، 2005.

8-**إيمان محمد علي الجابري**، يقين القاضي الجنائي، طبعة الأولى، منشاة المعارف، الإسكندرية، 2005.

9-**بكري يوسف بكري**، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الاسكندرية، 2011.

10- **بوكر رشيدة**، جرائم الاعتداء علـــى أنظمة المعـالجة الآلية فـــي التشريـع الجزائـري والمقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2012.

11- **بوسقيعة أحسن**، قانون الإجراءات الجزائية على ضوء الممارسات القضائية، برتـــي للنشر، الجزائر،2014.

12- **جميل عبد الباقي الصغير**، أدلة الإثـــبات الجنائـــي و التكنولـــوجية الحديثة، دار النهضة العربية، القاهرة، 2002.

13- **حسام محمد نبيل الشنراقي**، الجرائم المعلوماتية-دراسة تطبيقية مقـارنة علـــى جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، القاهرة، 2013.

14- **حسن طاهر داود**، جرائم نظم المعلومات، الطبعة الأولـــى، أكـــاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.

15- **خالد عياد الحلبي**، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر والتوزيع، عمان، 2011.

16- **خالد ممدوح ابراهيم**، فن التحقيق الجنائـــي في الجـــرائم الالكترونـــية، دار الفكـــر الجامعي، الاسكندرية، 2009.

17- **رشاد خالد عمر**، المشاكـل القانـــونية و الفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، بغداد،2013.

18- **رمزي رياض عوض**، سلطة القاضي الجنائي في تقدير الأدلـــة، دار النهضة العربية، القاهرة، 2004.

19- ـــــــــــــــــــ، مشروعية الدليل الجنائي فـــي مرحلة المحاكمة و ما قبلها ـ دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 1997.

20- **زبده مسعود**، الاقتناع الشخصـــي للقاضـــي الجزائـــي، المؤسسة الوطنية للكتاب، الجزائر، 1989.

21- **زيبحة زيدان**، الجريمة المعلوماتية في التشريع الجزائري و الدولـــي، دار الهـدى، الجزائر، 2011.

22- **سامي جلال فقي حسين**، الأدلة المتحصلة من الحاسوب و حجيتها في الإثبات، دار الكتب القانونية، القاهرة، 2011.

23- ـــــــــــــــــــــ، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، القاهرة، 2011.

24- **سعيد عبد اللطيف حسن**، إثبات جرائم الكمبيوتر و الجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

25- **سيد محمد حسن الشريف**، النظرية العامة للإثبات الجنائي، دار النهضة العربية، القاهرة ، 2002.

26- **عادل يوسف عبد لبني شكري**، الجريمة المعلوماتية و ازمة الشرعية الجزائية، مركز دراسات الكوفة، 2008.

27- **عبد الفتاح بيومي حجازي**، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006.

28- ـــــــــــــــــــــ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.

29- ـــــــــــــــــــــ، الدليل الرقمي و التزوير في جرائم الكمبيوتر و الانترنت، دراسة معمقة في جرائم الحاسب الآلي و الانترنت، بهجت للطباعة و التجليد، القاهرة، 2009.

30- **عفيفي كامل عفيفي**، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، منشورات الحلبي، دمشق، 2007.

31- **علاء عبد الباسط خلاف**، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 2002.

32- **علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسب و الانترنت، عالم الكتب الحديثة، القاهرة ، 2004.

33- **علي عدنان الفيل**، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، بغداد، 2012.

34- **عمر محمد أبوبكر بن يوسف**، الجرائم الناشئة عن استخدام الانترنت – الأحكام الموضوعية و الجوانب الإجرائية، دار النهضة العربية، القاهرة، 2004.

35- **غنام محمد غنام**، دور قانون العقوبات في مكافحة جرائم الكمبيوتر و الانترنت و جرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر و القانون، القاهرة، 2013.

36- **محمد أمين الرومي**، جرائم الكمبيوتر ة الانترنت، دار المطبوعات الجامعية، القاهرة، 2004.

37- **محمد الأمين البشري**، التحقيق في الجرائم المستحدثة، الطبعة الأولى، مركز الدراسات و البحوث، الرياض، 2004.

38- **محمد عبد الشافي اسماعيل**، مبدأ حرية القاضي الجنائي في الاقتناع ـ دراسة مقارنة، دار المنار، القاهرة، 1992.

39- **محمد عبد الكريم عبادي**، القناعة الوجدانية للقاضي الجزائي و رقابة القضاء عليها، الطبعة الأولى، عمان، 2002.

40- **محمد طارق عبد الرءوف الحن**، جريمة الاحتيال عبر الأنترانت (الأحكام الموضوعية و الأحكام الإجرائية)، الطبعة الأولى، منشورات الحلبي الحقوقية، دمشق، 2011.

41- **محمود احمد عبابنة**، جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر و التوزيع، عمان، 2005.

42- **مصطفى محمد موسى**، المراقبة الالكترونية عبر شبكة الانترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية و الالكترونية، الطبعة الأولى، دار الكتب و الوثائق القومية المصرية، القاهرة، 2003.

43- ـــــــــــــــــــ، أساليب إجرامية للتقنية الرقمية (ماهيتها و مكافحتها)، دار الكتب القانونية، القاهرة، 2005.

44- ـــــــــــــــــــ، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2009.

45- **ممدوح عبد الحميد عبد المطلب**، البحث و التحقيق الجنائـــي الرقمـــي في جرائـم الحاسب الآلي و الانترنت، دار الفكر القانونية، القاهرة، 2006.

46- **نبيلة هبة هروال**، الجوانب الإجرائية لجرائـــم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013.

47- **نجيمي جمال**، إثبـات الجريـــمة على ضوء الاجتهاد القضائي، دار هومة، الجزائر، 2011,

48- **وهـــاب حمزة**، الحماية الدستورية للحرية الشخصية خلال مرحلة الاستدلال و التحقيق في التشريع الجزائري، دار الخلدونية، الجزائر، 2011.

49- **هدى حامد قشقوش**، السياسة الجنائـية لمواجهة الجريـــمة المعلوماتية، دار النهضة العربية، القاهرة، 2012.

50- **هشام محمد فريد رستم**، الجـوانب الإجرائية للجرائم المعلوماتية-دراسة مقارنة، مكتبة الآلات الحديثة، القاهرة ، 1994.

51- **هلالي عبد أللاه أحمد**، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2003.

52- ـــــــــــــــــــــ، تفتيش نظـم الحاسب الآلي و ضمانات المتهم ألمعلوماتي دراسة مقارنة، دار النهضة العربية، القاهرة، 2006.

53- ـــــــــــــــــــــ، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلـــقا عليها، دار النهضة العربية، القاهرة، 2011.

54- ـــــــــــــــــــــ، النظرية العامة للإثبات الجنائي، المجلد الأول، دار النهضة العربية للنشر، القاهرة، بدون سنة.

55- **ياسر محمد الكومى محمود أبو حطب**، الحمـــاية الجنائـــية و الأمنـــية للتوقـــيع الإلكتروني، منشاة المعارف، الإسكندرية، 2014.

56- **يوسف حسن يوسف**، الجـــرائم الدولـــية للانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011.

ب- الرسائل و المذكرات

أ- رسائل الدكتوراه:

1- **أحمد سعد محمد الحسيني** ، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية، رسالة لنيل درجة دكتوراه في القانـــون، كلية الحقـــوق بجامعة عين الشمس، القاهرة، 2012.

2- **أحمد ضياء الدين محمد خليل**، مشروعية الدليل فـــي المواد الجنائية، رســـالة لنيل درجة دكتوراه في القانون، كلية الحقوق، جامعة عين الشمس، القاهرة، 2012.

3- **جلاد سليـــم**، الحق في الخصوصية بين الضمانات و الضوابط في التشريع الجزائري والفقه الإسلامي، مذكرة لنسل شهادة الماجستير في الشريعة و القانون، تخصص حقوق الإنسان، كلية العلوم الإنسانية و الحضارة الإسلامية، جامعة وهران، 2013.

4- **حسين بن سعيد بن سيف الغافري**، السياسة الجنائية في مواجهة جرائم الانترنت، رسالة لنيل درجة الدكتـــوراه في القانون، كلية الحقوق، جامعة عين الشمس، القاهرة، 2005.

5- **عمر محمد أبو بكر بن يونس**، الجرائم الناشئة عن استخدام الانترنت، رسالة لنيـــل درجة دكتوراه، كلية الحقوق، جامعة عين الشمس،القاهرة، 2004.

6-**غازي عبد الرحمن هيان الرشيد**، الحماية القانـــونية من جرائم المعلوماتية، رســـالة لنيل درجة دكتـــوراه في القانون، كلية الحقوق، الجامعة الإسلامية ، بيروت، 2004.

7-**فايز محمد راجح غلاب**، الجرائـــم المعلومـاتية في القانون الجزائري و اليمني، رسالة لنيل درجة الدكتـــــوراه في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر (1)، 2011.

8-**فهد عبد الله العبيد العازمي**، الإجراءات الجنائية المعلوماتية ، رسالة لنيل درجة دكتـــوراه في القانون، كلية الحقوق بجامعة القاهرة، 2012.

ب- مذكرات الماجستير:

1- **أحمد بن زايد جوهر الحسن المهندي**، تفتيش الحاسب الآلـــي و ضمـــانات المتهم، مذكـرة لنيل شهـادة المـاجستير في القانــون، كلـية الحقوق، جامعة القاهرة، 2009.

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

3-**بن بلاغة عقيلة**، حجية أدلـــة الإثبـات الجنائية، مذكرة لنيل شهادة المـاجستير في القانـــون، فرع القانون الجنائي، جامعة الجزائر، 2011.

4-**بوعمرة آسيا**، النظـام القانونـــي لقـواعد البيانات، مذكر لنيل شهادة الماجستير في القانون، فرع الملكية الفكرية، كلية الحقوق، جامعة الجزائر، 2005.

5-**حقاص صونية**، حماية الملكـية الفكـرية الأدبية و الفنية في البيئة الرقـمية في التشريع الجزائـــري، مذكـــرة لنيل شهـادة الماجستير في علم المكتبات، تخصص المعلومات الالكترونية، الافتراضية و الإستراتيجية البحث عن المعلومـات، كلية العلوم الإنسانية و الاجتماعية، جامعة قسنطينة، 2012.

6-**صغير يوسف**، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري بتيزي وزو، 2013.

7-**طاهري شريفة**، تأثير أدلة الإثبات على الاقتناع الشخصي للقاضي الجنائي، مذكرة لنيل شهادة الماجستير في القـانـون ، كلية الحقوق بجامعة الجزائر، 2003.

8-**طرشي نورة**، مكـافحة الجريـمة المعلومـاتية، مذكرة لنيل شهادة الماجستير في القـانـون الجنائي، كلية الحقوق بجامعة الجزائر (1)، 2012.

9-**عبد محمد بحر**، معوقات التحقيق في جرائم الانترنت، مذكرة لنيل شهادة الماجستير فـــي العلوم الشرطية، قسم العلوم الشرطية، معهد الدراسات العليا، جامعة نـــايف العربية للعلوم الأمنية، دبي، 1999.

10- **لحمر فاقة**، إجـراءات تسليم المجرمين في الجزائر علـى ضوء الاتفاقيـات الدولـية، مـذكرة لنيل شهادة ماجستير في القانون، كلية الحقوق و العلوم السياسية، جامعة وهران ، 2013.

11-**محمد بن نصير السرحاني**، مهـارات التحقـيـق الجنائي الفني في جرائم الحاسـوب و الانترنت، دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسـالة لنيل درجة ماجستير في العلوم الشرطية، كلـية الدراسـات العـليا، جامعة نـايف العربية للعلوم الأمنية، الرياض، 2004.

ج-المقالات و البحوث:

1-**أرحومة موسى مسعود** « الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبـر الوطنية » بحث مقدم إلى المؤتمر ألمغاربي الأول حول المعلومـات و القانون، المنظم من طرف أكاديمية الدراسات العلـيا طرابلس الفترة من 28-2009/10/29. دون ترقيم الصفحات.

2-**إسماعيل عبد النبي شاهين** « امن المعلومـات فـي الانترنت » بحث مقدم إلـى مؤتمر القانون و الكمبيوتر و الانترنت، كلية الشريعة و القانون دبـي، الإمارات العربية المتحدة، 2000، ص.ص 01-43.

3-**أيمن عبد الحفيظ** « حدود مشروعـية دور أجهزة الشـرطة فـي مواجـهة الجرائم المعلوماتية » مجلة مركز بحوث الشرطة، عدد 01 ، صـادر في 25 جانفي 2004، ص.ص 201- 246 .

4-**إيهاب ماهر السنباطي** « الجرائم الإلكترونية(الجرائم السيبيرية) قضـية جديدة أم فئة مختلفة؟ التنـاغم القانـونـي هو السبيل الوحيد ! » بحث مقدم إلـى الندوة الإقليمية حول " الجرائم المتصلة بالكمبيوتر"، المنعقدة بالربـاط في 19 و 20 جويلية 2007، ص.ص 11-38.

5-**تيطاوني الحاج**«الانترنيت عملاق العولمة» بحث مقدم إلى الملتقـى الوطنـي الأول تحت عنوان، القانون و قضـايا الساعة –النظـام القانونـي للمجتـمع الالكتروني، المنظم من طرف المركز الجامعـي لخميس مليانة، ولاية

عين الدفلة ، الجزائر، من 09 إلى 11 مارس 2008، ص.ص 04-19.

6-**جان فرانسوا هنروت** « أهمية التعاون الدولي و التجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة و التعاون القضائي » بحث مقدم إلى الندوة الإقليمية حول " الجرائم المتصلة بالكمبيوتر"، المنعقدة بالرباط في 19 و 20 جوان 2007، ص.ص95- 109.

7-**جورج لبكي**« المعاهدات الدولية للانترنت حقائق و تحديات » مجلة الدفاع الوطني اللبناني، عدد 83، بيروت، 2014، ص.ص 01- 19.

8-**حازم الحارون**« الإنابة القضائية الدولية » المجلة الجنائية القومية، العدد الثاني، القاهرة، 1988، ص.ص 01- 32.

9-**حسين بن احمد الشهري** « قانون دولي موحد لمكافحة الجرائم الإلكترونية » المجلة العربية للدراسات الأمنية و التدريب، مجلد 27، عدد 53، 2010، ص.ص05-53.

10-ـــــــــــــــــ، نظم المعلومات و تكاملها مع النظم الخبيرة، مجلة الفكر الشرطي، عدد 82، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مارس 2012، ص. ص 45-91.

11-**حسين بن سعدي الغافري** « التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت» ص.ص 01-29 مقال متوفر في الموقع التالي: www .eastlaws.com .

12- **خالد ممدوح إبراهيم** « الدليل الالكتروني في جرائم المعلوماتية » بحث منشور في الموقع الالكتروني التالي:
.http://Kenanaonline.com/users/KhaledMamdouh/posts/79345

13-**خنفوسي عبد العزيز**« تجسيد مبدأ حرية الإثبات الجزائي في القانون الجنائي الجزائري » ص.ص 01-20، مقال منشور في الموقع التالي:
http://ifttt.com/images/no_image_card.pn

14- **راسل تاينر**« أهمية التعاون الدولي في منع جرائم الانترنت » بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، الجارية بالرباط في الفترة 19 و 20 جوان 2007، ص.ص 110-128.

15- **زورو هدى** « التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري » مجلة دفاتر السياسة و القانون، العدد الحادي عشرة، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر ببسكرة، 2014، ص.ص 119-147 .

16- **سرحان حسن المعيني** « التحقيق في جرائم تقنية المعلومات » مجلة الفكر الشرطي، مجلد 20، عدد 79، صادر عن مركز بحوث الشرطة القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، عام 2011، ص.ص 15- 53.

17- **سيناء عبد الله محسن**« المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية » بحث مقدم إلى الندوة الإقليمية حول "الجرائم المتصلة بالكمبيوتر"، المنعقدة بالرباط في 19 و 20 جويلية 2007، ص.ص 45- 60.

18- **صالح احمد البربري**« دور الشرطة في مكافحة جرائم الانترنت في إطار اتفاقية بودابست » مقال مأخوذ من الموقع التالي: www.Arablaw.Com

19- **طارق محمد الجملي** « الدليل الرقمي في مجال الإثبات الجنائي » بحث مقدم إلى المؤتمر ألمغاربي الأول حول المعلوماتية و القانون، المنظم من طرف أكاديمية الدراسات العليا بطرابلس، في الفترة الممتدة من 28-2009/10/29، ص.ص 01-34.

20- **عادل عبد الله خميس المعمري**« التفتيش في الجرائم المعلوماتية» مجلة الفكر الشرطي، مجلد 22، عدد 86، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشرقة، الإمارات العربية المتحدة، 2013، ص.ص243- 272.

21- **عاكوم وليد**« التحقيق في جرائم الحاسوب» بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، منعقد بإمارة دبي في الفترة الممتدة من 26 إلى 28 ابريل 2003،ص.ص 01-13 .

22- **عبد الناصر محمد محمود فرغلي**« الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية » بحث مقدم الى المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، المنظم بالرياض، في الفترة الممتدة بين 12 و 14 نوفمبر 2008، ص.ص 01-45.

23- **علاوة هوام** « التسرب كآلية للكشف عن جرائم في القانون الجزائري » مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر بباتنة، 2012 ، ص ص 01- 22.

24- **علي حسن الطوالبة** « مشروعية الدليل الرقمي المستمد من التفتيش الجنائي» 2009. بحث منشور على موقع الانترنت التالي: www.policemc.gov.bh/reports/2009/...7.../633843953272369688.doc

25- **علي محمود على محمود**« الأدلة المحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي » بحث مقدم إلى المؤتمر العلمي الاول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، دبي، الإمارات العربية المتحدة، 2003، ص.ص 01-31.

26- **عمر بن يونس**« الإجراءات الجنائية عبر الانترنت في القانون الامريكي» المرشد الفدرالي الأمريكي لتفتيش و ضبط الحواسيب وصولا الى الدليل الالكتروني في التحقيقات الجنائية، د.م ، 2008، ص.ص 55- 78.

27- **عمر محمد بن يونس**« مذكرات في الإثبات الجنائي عبر الانترنت » بحث مقدم إلى ندوة الدليل الرقمي، بمقر جامعة الدول العربية بالقاهرة، في الفترة الممتدة من 05 إلى 08 مارس 2006، ص.ص 01- 27.

28- ـــــــــــــــــ .« أدلة الإثبات الجنائي و الجرائم الالكترونية » بحث مقدم الى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في

الوطن العربي، المنعقد بمقر الجامعة الدول العربية، القاهرة، خلال الفترة الممتدة من 26-27 أفريل 2008، ص.ص 01- 16.

29- **عمرو حسين عباس** « أدلة الإثبات الجنائي و الجرائم الالكترونية » بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، المنعقد بمقر الجامعة الدول العربية، القاهرة، خلال الفترة الممتدة من 26-27 أفريل 2008، ص.ص 01-26.

30- **غنام محمد غنام** « عدم ملائمة القواعد التقليدية في القانون العقوبات لمكافحة جرائم الكمبيوتر » بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الانترنت المنعقد بكلية الشريعة و القانون بجامعة الإمارات العربية المتحدة في الفترة الممتدة من 01 إلى 03 ماي 2003، ص.ص 625- 659.

31- **فشار عطاء الله** « مواجهة الجريمة المعلوماتية في التشريع الجزائري » بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية المنعقد بأكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص.ص 28- 49.

32- **كحلوش علي**« جرائم الحاسوب و أساليب مواجهتها » مجلة الشرطة، عدد 84، صادر عن مديرية الأمن الوطني، جويلية 2007، ص.ص 50-68.

33- **كريستينا سكولمان**« المعايير الدولية المتعلقة بجرائم الانترنت » بحث مقدم الى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المنعقدة بالمملكة المغربية، في الفترة من 19-20 جوان 2007، ص.ص 61- 76.

34- **محمد أبو العلاء عقيدة** « التحقيق و جمع الأدلة في محال الجرائم الالكترونية » ص.ص 1-16 مقال منشور في الموقع التالي:

.www.osamabahar.com

35- **محمد الأمين البشري**« تأهيل المحققين في جرائم الحاسب الالي و شبكات الانترنت » بحث مقدم في الحلقة العلمية بعنوان "الانترنت و الإرهاب"، المنظمة من طرف جامعة نايف العربية للعلوم الأمنية

بالتعاون مع جامعة عين الشمس، بدبي، في الفترة الممتدة من 15 إلى 11/19/ 2008، ص.ص 01- 51.

36- ـــــــــــــــــ« التحقيق في جرائم الحاسب الآلي » بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الانترنت، كلية الشريعة و القانون بجامعة الإمارات العربية المتحدة في الفترة من 1 إلى 3 ماي 2004، الطبعة الثالثة، 2004، ص.ص 1033- 1081.

37- ـــــــــــــــــ و محسن عبد الحميد محسن« معايير الأمم المتحدة في مجال العدالة الجنائية و منع الجريمة » أكاديمية نايف للعلوم الأمنية، رياض، 1998، ص.ص 01- 36.

38- **محمد حسام محمود لطفي** « الجرائم التي تقع على الحاسبات او بواسطتها » بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص.ص 490-539.

39- **محمد زلايجي** « حجية دليل الحاسوب الالي في النطاق الجنائي » مجلة مخبر القانون الخاص الأساسي، العدد 07، كلية الحقوق، جامعة تلمسان، 2010، ص.ص61-112.

40- **محمد علي قطب** « الجرائم المعلوماتية و طرق مواجهتها » الأكاديمية الملكية لشرطة البحرين، مملكة البحرين، 2010، ص.ص 01- 32.

41- **محمد قدري حسن عبد الرحمن** « جرائم الاحتيال الالكتروني» مجلة الفكر الشرطي، عدد 79، صادر عن مركز بحوث الشرطة القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011، ص.ص 55- 174.

42- **مراد عبد الرحمان مكاوي** « الستيغانوغرافي » مقال منشور في مجلة المعرفة، العدد 147، نيسان، 2009، ص 41 متاح على الموقع التالي:
http://www.almarefh.org/news.php?action-shawgid-6,4

43- **ممدوح عبد الحميد عبد المطلب** « استخدام بروتوكـــول TCP/IP في بحث و تحقيق الجرائم على الكمبيوتر » بحث مقدم الى المؤتمر العلمـي الأول حول الجوانب القـانــونية و الأمنية للعمليات الالكترونية، المنعقد بدبـي، فـــي الفترة الممتدة من 26-2003/08/28، ص.ص 01-27. مقال منشور علـــى الموقع الالكتروني التالي: WWW.arablaw.info.com

44- ـــــــــــــــ« أدلة الصور الرقمية في الجرائم عبر الكمبيوتر » مركـــز شرطة دبي، 2005، ص.ص 01- 29.

45- ـــــــــــــــ **و زبيدة محمد جاسم و عبد الله عبد العزيز**« نموذج مقترح لقـــواعد اعتمـــاد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر » مـــؤتمر الإعمـال المصرفية الالكترونية بين الشريعة و القانون، المجلد الخـــامس، المنعقد بدبـــي فـــي الفترة من 10-12 ماي، 2003 ، ص.ص 2244- 2286.

46- ـــــــــــــــ « جرائم استخدام شبكة المعلومـــات العالمية » بحث مقدم إلى مؤتمر القانون و الكمبيوتـر و الانترنت، كلية الشريعة و القـــانون دبي، الإمارات العربية المتحدة ، 2000، ص.ص 23-51 .

47- **نبيل إسماعيل عمر** « قاعدة عدم قضاء القاضي بعلمه الشخصي» المجلة العربية للدراسات الأمنية، المجلد الأول، العدد الأول، الرياض، 1989، ص 24.

48- **هشام محمد فريد رستم**« الجـرائم المعلوماتية أصول التحقيق الجنائي الفني و آلية التدريب التخصصي للمحققين » مجـلة الأمـن و القانون، عدد 02، صادر عن كلية شرطة دبي، 1999، ص.ص 74-107.

49- ـــــــــــــــ« الجرائم المعلوماتية – أصـول التحقيق الجنائـــي الفني و اقتراح إنشاء آلية عربية موحدة للتدريب التخصصي » بحث إلى مؤتمر القانـون و الكمبيوتر و الانتـرنيت، جـامعة الأمارات المتحدة » كلـــية الشريـعة و القانـــون، المجلد الثاني، الطبـعة الثالـــثة، من 1 -3 ماي 2000، ص.ص401-506.

50- **هـودة رشيدة**« دور الشرطة الجزائرية في محاربة الجريمة الالكترونية» مداخلة مقدمة إلى الملتقى الوطني حول" الجريمة الالكترونية وأمن المعلومات" المنظم بكلية العلوم والتكنولوجيا بجامعة وهران، يوم 06 ديسمبر 2016، بدون ترقيم. مقال منشور في الموقع التالي: www.univ-usto.dz.id=257.

د-النصوص القانونية:

1- الدساتير:

Ù قانون رقم(16-01)مـــؤرخ في 6 مـــــارس 2016، يتضمن التعديل الدستـــوري الجزائري، جريدة رسمية عدد 14، صادر في 7 مارس 2016.

2- الاتفاقيات الدولية:

1- اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومـــات لأغراض إجرامية، رقـــــم (55/ 63)، صـــادرة عن هيئة الأمم المتحدة، بالجمعية العامة 81، 19 ديسمبر 2000. متاحة على الموقع الالكتروني: http://www.unodc.org/pdf/crime/a_res_56/121f.pdf

2- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 متـاحة في الموقـــع الالكتروني التالي:Www.arablegalnet.org

3- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية باليرمو عام 2000. متوفرة في الموقع التالي: http://www.uncjin.org/documents/conventions/dcatoc/final_documents_2/convention_french

4- اتفاقية مكافحة إســـاءة استخدام تكنولوجـــــيا المعلومات لاغراض اجرامية، رقم (55/63)، صادرة عن منظمة الأمم المتحدة، الجلسة العامة 81، ديسمبر 2000.

5- **اتفاقية تسليم المجرمين** بين الجزائر و بريطانيا، مؤرخة في 2006/6/11، جريدة رسمية عدد 81، صادر في 2006/12/13.

3- النصوص التشريعية:

1- **قانون رقم(04-15)** مؤرخ في2004/11/10 يعدل ويتمم الأمر رقم(66-156) يتضمن قانون العقوبات، جريدة رسمية العدد 71، صادر بتاريخ 2004/11/10، معدل و متمم.

2- **قانون رقم(06-22)** مؤرخ في2006/12/20، يعدل ويتمم الأمر رقم 66-155 يتضمن قانون الإجراءات الجزائية، جريدة رسمية العدد 84، صادر بتاريخ 2006/12/24. معدل و متمم

3- **قانون رقم(4/09)** مؤرخ في14 شعبان 1430 الموافق ل 05 غشت سنة 2009 و المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام و الاتصال و مكافحتها، جريدة رسمية العدد 47، صادر بتاريخ 16 أوت 2009.

4- **قانون رقم(03/2000)** مؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية. جريدة رسمية العدد 48، صادر بتاريخ 06 أوت 2000.

4- النصوص التنظيمية:

1-**قرار وزاري مؤرخ في 14-04-2007**، يتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، ج. ر للجمهورية الجزائرية العدد 36، صادر بتاريخ 03 جويلية 2007.

1- **مرسوم رئاسي رقم(183/04)** مؤرخ في 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني و تحديد قانونه الأساسي، ج. ر للجمهورية الجزائرية العدد 49، صادر بتاريخ27 جوان 2004.

2- **مرسوم رئاسي رقم(15-261)** مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة و

تنظـيم و كيفيات تسيير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصـال، ج.ر للجمهورية الجزائـرية العدد 53، صـــادر في 8 أكتوبر 2015 .

ه- الوثائق:

1- **اجتماع فريق خبراء حول الجريمة الالكترونية (السيبرانية)**، مشـــــروع المواضيع المطروحة للنظر في إطار دراسة شاملة بخصوص الجريمة الالكترونية (السيبرانية) و تدابير التصدي لها، المنعقد بفيـنا، في الفتـرة الممتدة من 17 إلى 21 جانفي 2011. رقم UNOD/CCPCJ/EG4/2011/2

2- **التوصية رقم (1)** الصادرة عن المؤتمر الإقليمي للدول العربية حول جرائم الإنترنت المنعقد في الدار البيضاء بتاريخ 19و 20 جوان 2007، متـاحة باللغة العربية على الموقع:
http://www.arabniaba.org/publications/crime/casablanca/recommendations-a.pdf.

3- **التوصية رقم (2)** الصادرة عن المؤتمر الإقليمي للدول العربية حول جرائم الإنترنت المنعقد في القاهرة بتاريخ 26 و 27 نوفمبر 2007 متاحـــة باللغة العربية على الموقع:
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_Arabic.pdf

4- **اللجنة الاقتصادية و الاجتماعية لدول غرب أسيا (ESCWA)** ، ورشة عمل حـول التشريعات المتعلقة بالجريمة الالكترونية (السبيرانية) و تـطبيقها فـــي منطقة الاسكـوا، بيروت، يومـــي 15 و 16 ديسمبر 2008، المجلس الاقتصـــــادي و الاجتمـاعـــي التـــابع لـلأمـــم المتـحـــــدة، رقم E/ESCWA/ICTD/2009/1

5- **تقرير لجنة منع الجريمة و العدالة الجنائية** " دراسة شـاملة عن مشكـلة الجـــريمة

السيبيرانية و التدابير التي تتخذها الدول الأعضاء و المجتمع الدولـي و القطاع الخاص للتصدي لها" الجمعية العامة لمنظمة الأمـــم المتحدة، 25-28 فيفري 2013، منشور في الموقع:
1UNODC/CCPCJ/EG4/2013/1

6- **مؤتمر الامم المتحدة الثامن عشر لمنع الجريمة و العدالة الجنائية**، البند الثـــامن من جدول الأعمـــال المؤقت، التـطورات الأخيرة في استخدام العلم و التكنولوجـــيا من جانب المجرمين و السلطات المختصة في مكافحة الجريـمة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل 12-19 أفريـل 2010، رقم A/conf.213/9

7- **منظمة الأمم المتحدة، اتفاقية حقوق الطفل** ـ النظر في التقارير المقدمة من الـدول بموجب المادة 1/12 من البرتوكول الاختياري لاتفاقية حقـوق الطـفل حول بيع و بغاء الأطفال في المواد الإباحية، لجنة حقوق الطفل، الدورة 57، المنعقدة من 30 ماي إلـى 17 جويلية 2011، الأمـــم المتحدة، رقم :CRC/c/opsc/egy/co/1

8-**قـرار المجلس الأوروبي** رقم JAI /584/2002، مـؤرخ 13 جوان 2002، يتضمن إنشاء مذكرة القبض الأوروبية، جـريدة رسمـية للمجـلس الأوروبي العدد ل 190، صادر في 18 جويلية 2002.

9-**قرار المجلس الأوروبي** رقم JAI /978/2008،23 مـؤرخ أكتـوبر 2009، يتضـمن إنشـاء المذكرة الأوروبـية للحصـول على الأدلـة، ج. ر للمجلس الأوروبي العدد **ل** 350، صادر في 30 ديسمبر 2008.

11- **قرار المجلس الأوروبي** رقم JAI /829/2009، مؤرخ في 23 أكتـوبر 2009، يتضمـن إنـشـاء مذكـرة أوروبـية حـول تدابير المراقـبة، ج. ر للمجلس الأوروبي العدد ل 294، صادر في 11 نوفمبر 2009.

12- **قرار المجلس الأوروبـي** مـؤرخ في 28-02-2002، يتضمن إنـشاء منظمـة الشرطة الأوروبية (الأوروجست)، ج. ر للمجلس الأوروبي العدد ل 63،

صادر في مارس 2002 .

- ثانيا :المراجع باللغة الأجنبية:

A- Ouvrages;

1- **CHAWKI Mohamed**, combattre la cybercriminalité, édition de saint-amans, Paris, 2008.

2- **FOURMENT. (F)**, procédure pénale-la perquisition du disque d'un ordinateur a chaud, CPU, Paris, 2002- 2003, mise a jour de 2004 .

3- **LEBRUN. (M),** Interpol, PUF, que sais-je ? 1997.

4- **QUEMENER Myriam**, **FERRY Joël**, cybercriminalité défi mondial, 2ème édition, édition Economica, Paris, 2009.

5- **QUEMENER Myriam - Charpenel Yves** « cybercriminalité droit pénal appliqué » édition Economica, Paris, 2010.

6- **ROGGEN François Et DE VALKENEEK Christian**, Actualité de droit pénal, bruyant, Bruxelles, 2005.

7- **SABATIER.M**, la coopération policière européenne, Harmattan, Paris, 2001.

B- Thèses Et Mémoires ;

1- **DOSTE AMEGEE Maximilien**; La Cyber-surveillance et le secret professionnel, paradoxes ou contradictions?, mémoire D.E.A, université Paris, Nante, P 51 sui, disponible en ligne l'adresse suivante ; http://mémoire online.free.fr.

2-**EL CHAER Nidal**, la criminalité informatique devant la justice pénale, thèse de doctorat en droit, faculté de droit de l'université Poitiers, 2003.

3-**HABHAB Mohamad Ahmad ,** le droit pénal libanais a l'épreuve de la cybercriminalité, thèse de doctorat, soutenue a la Faculté de droit de Université de Montpellier, le 10 juillet 2009.

4- **MEIER MARSELLA Carole** , l'effectivité du processus répressif dans le traitement de la cybercriminalité- enquête sur le système juridique français, thèse pour l'obtention du doctorat en droit, soutenue a la faculté du droit de l'université Paris 2, le 13-05-2005.

5-**MIGNARD Jean-Pierre**, cybercriminalité et cyber— répression entre désordre et harmonisation mondiale, thèse de doctorat, Université de Paris panthéon- Sorbonne, 2004.

6-**VERGUCHT Pascal** , la répression des délits informatiques dans une perspective internationale, thèse pour l'obtention du doctorat en droit, soutenue a la faculté du droit de l'université de Montpellier 1, Paris, 1996.

.

c- Articles ;

1- -**AMORY (B) et POULLET (Y)** « le droit de la preuve face a l'informatique et la télématique » Revue International de Droit Comparé, N 2, Avril 1985, pp 330-361.

2- **BENNOUAR Abdelhakim** «Les techniques spéciales d'enquête et d'investigation en Algérie » article publié sur ; www.mémoireonline.com.

3- **BOSSAN Jérôme** « le droit pénal confronté a la diversité des Intermédiaires de l'internet » édition Dalloz, 2013, pp 295-319.

4- **BOUDER Hadjira** « protection des systèmes d'informations : Aspects juridiques » centre de recherche sur l'information scientifique et technique, Alger, 2012, pp 01- 36.

5- ——————— « Quel cadre juridique pour la lutte contre la criminalité liée aux TIC en Algérie » séminaire national sur le cadre juridique des TIC en Algérie ; entre opportunité et contraintes, CERIST, Alger, du 16 au 17 Mai 2012, pp 01-15.

6- **BRIAT Martin**, La Fraude Informatique: une approche de droit compare, Revue D.P.C, N04 Avril, 1985, pp 185-199.

7- **BOURGUIGNON Jonathan** « la recherche de preuves Informatiques et l'exercice extraterritorial des compétences de l'Etat » article présenté au colloque de Rouen sur « internet et droit

International » organisé par la société Française pour le droit international du 30 Mai au 01 juin 2013, édition Pedone, Paris, 2014, pp 357-372.

8- **CASILE Jean François** « plaidoyer en faveur d'aménagement de la preuve de l'infraction informatique » Revue des sciences criminelles et de droit pénal comparé (R.S.C.D.P.C) , N 01, 2004, pp 65-82.

9- **CHOPIN Frederique** « Les politiques publiques de lutte contre la cybercriminalité» AJ Pénal 2009, pp 100-131.

10- **DEMARCHI Jean-Raphael** « La loyauté de la preuve en procédure pénale, outil transnational de protection du justiciable » Recueil Dalloz, 2007, pp 2009-2042

11- **DIOP Abdoulaye** « Cour de Procédures Pénales et TIC » article publier sur le cite ; http ;//www.196.1.99.9/moodle/mod/book/print.

12- **D. Ammar** « preuve et vraisemblance, contribution a l'étude de la preuve technologique » RTD Civ, juillet-septembre, 1993, pp 495-513.

13- **FALQUE Pierrotin** « la gouvernance du monde en réseau, in gouvernance de la société de l'information» Cahier du C.R.I.D. n 22, Bruxelles, Bruylant, 2002, PP 109-136.

14- **FIRAL- SCHUHL Christiane**«cyber droit-le droit a l'épreuve de l'internet » 6ém édition Dalloz , Paris, 2012, pp 989-1020.

15- **FORGERON Jean François** « le projet de loi portant Approbation de la convention sur la cyber

criminalité » Gazette du palais N 22, 22 janvier 2004, article publier sur ; http://www.lextenso.fr/weblextenso/article/print.

16- **FLORENCE De Villenfagne** « La Belgique sort enfin ses armes contre la cybercriminalité : A propos de la loi du 28novembre 2000 sur la criminalité informatique, droit et nouvelles technologies », 2001. article publier sur ; **http://www.droit-technologie.org**

17- **GEORGO Antoniu** « les crimes informatiques et d'autre crimes dans le domaine de la technologie informatiques en Romanie » Revue internationale de droit pénal, 1993,pp 551-593.

18- **JRANDIDIER Wilfrid** « interprétation de la loi pénale » juris- class, penal ,art 111- 2 a 111- 5, n 38 .

19- **KALINA. (L)**« lutte contre la cybercriminalité, vers la construction d'un modèle juridique normalise » article disponible sur ; http://www.adie.sn

20- **KARY. (T)** « Etats Unis ; projet de loi prend à nouveau pour ciblé le crime informatique » 04 février 2002. disponible a l'adresse suivante ; http://news.zdnet.fr/story/ot118-s20104405.00.hunl

21- **LEDERMAN Eli And SHAPIRA Ron_**« computer crimes and other crimes against information technology in Israel » R.I.D.P, 1er et 2e trimesters, 1992, pp 420-455

22- **LINGLET Monique** « délinquance informatique, sur le front de la nouvelle criminalité, une parade concerné » Revue internationale de

police criminelle, mai 1995, pp 182-211.

23- **MARMISSE Anne - d'ABBADIE D'ARRAST** « Coopération et harmonisation (matière pénale) » Dalloz, édition 2013.pp 122-159.

24- **MEUNIER,C** « La loi du 28 novembre 2000 relative à la riminaclité informatique, formation permanente » CUP, n°103, 2001, s.p

25- **MICHEL Prud'homme** « droit criminel écoutes et enregistrements clandestins » R.D .P, N 59, Paris, 2010, pp 47-78

26- **MITONGO Kalonji** « notion de cybercriminalité : praxis d'une pénalisation de la délinquance électronique en droit pénale Congolais » article publier sur ; www.tgk.centerblog.net

27- **PADOVA Yann** « un aperçu de lutte contre la cybercriminalité en France » R.S.C.P, N04, Dalloz, 2002, pp 768-803.

28- **QUEMENER Myriam** « conseil de l'Europe et lutte contre la Cybercriminalité » Revue expertises des systèmes d'information, Mai 2010, pp 170-202.

29- **ROBILLARD Yves** « la preuve des communication a l'ère économique» in : www.Avocat.qc.ca/affaires/iitechno.htm

30- **SASSI Ben Helma** « les crimes informatiques et d'autres crimes dans le domaine de technologie informatique en Tunisie » Revue internationale de droit pénal, N 01, 1993, pp 610-641.

31- **STEPHEN . J et autre** « la preuve en procédure pénale

comparée, rapport de synthèse pour les pays de Common Law » association internationale de droit pénal, 1992, pp 01- 33.

32- **VUELTA Simon** « Les nouveaux acteurs de la coopération pénale européenne» LPA n° 13, 2005. pp 01-29

C- les Textes de lois ;

1- **loi N 2001-1062**, du 15 novembre 2001 portant code de procédures pénales, JORF du 16 nov 2001.

2- **Loi n° 2001-1062,** du 15 novembre 2001 relative à la sécurité quotidienne, JORF du 16 nov. 2001.

3- **Loi n° 2003-239,** du 18 mars 2003 relative a la sécurité intérieure, JORF du 19 mars 2003.

4- **Loi n° 2004-204,** du 9 mars 2004, portant adaptation de la justice aux évolutions de la criminalité, JORF du 10 mars 2004.

5- **Loi n° 2004-575,** du 21 juin 2004 pour la confiance dans l'économie numérique, JORF du 22 juin 2004.

6- **Loi n° 2004-669,** du 9 juillet 2004 relative aux Communications électroniques et aux Services de communication, JORF du 10 juillet. 2004.

7- **Loi n° 2007-297,** du 5 mars 2007 relative à la prévention de la délinquance, JORF du 7 mars 2007.

8- **Loi n° 2009-669** du 12 juin 2009 favorisant la diffusion et la Protection de la création sur internet Dite Hadopi1, JORF du 13 juin 2009.

9- **Loi n° 2009-1311,** du 28 octobre2009 relative a la protection pénale de la propriété littéraire et artistique sur internet dite Hadopi2, JORF du 31

décembre 2009.

E- documents ;

1- **ASSEMBLEE NATIONALE FRANÇAISE**, rapport sur les méthodes scientifiques d'identification des personnes a partir de données biométriques et les techniques de mise en œuvre, paris, juin 2003.

2- **CONSEIL DE L'EUROPE**, la criminalité informatique, recommandation N° R (89) sur la criminalité en relation avec l'ordinateur et rapport final du comité européen pour les problèmes criminels, Strasbourg, 1990.

3- **CONSEIL DE L'EUROPE**, la recommandation N° (95) 13 sur les problèmes de procédures pénales liées a la technologie de l'information et Exposé des motifs, Strasbourg, 1996.

4- **CONSEIL DE L'EUROPE**, conclusions du conseil sur l'établissement d'un centre européen de lutte contre la cybercriminalité, publier sur ; press.office@consilium.europa.euhttp://www.consilium.europa.eu./Newsroom.

5- **Groupe d'experts ,** étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États membres, la communauté Internationale et le secteur privé pour y faire face, UNODC, Vienne, 25- 28 février 2013.

6- **OFFICE FEDERAL DE LA JUSTICE,** L'entraide judiciaire Internationale en matière pénale, 9ème édition, unité en judiciaire, Genève, 2010, p 06.

7- **OCDE**, la fraude liée a l'informatique : Analyse des politiques Juridiques, PIIC, n 10, 1986.

8- **O.N.U** : Manuel pour la prévention et la répression de la criminalité informatique, Revue Internationale de politique pénale, N° 43 et 44, 1995. (Publication des Nations Unies, numéro de vente: F.94.IV.5).

9- **UNODC**, Étude approfondie sur le phénomène de la Cybercriminalité et les mesures prises par les États membres, la communauté internationale et le secteur privé pour y faire face, commission pour la prévention du crime et la justice pénale EG.4, 2013 .

10- **Interpol**, Rapport d'activité 2005 . disponible sur ; http://www.interpol.int/public/ICPO/interpolAtWork/iaw2005fr.

11-**la convention sur la cybercriminalité**, STE no 185, rapport Explicatif, adopté le 8 novembre 2001.

فهرس الموضوع	
مقدمة	01
الباب الأول **آليات التحقيق في الجرائم الالكترونية**	07
الفصل الأول **إجراءات التحقيق في الجرائم الإلكتروني**	11
المبحث الأول: محدودية سريان إجـــراءات التحقيق المألـوفة علـى الجـرائم لالكترونية	12
المطلب الأول: التفتيش في البيئة الالكترونية	13
الفرع الأول: محل التفتيش الالكتروني	14
أولا – تفتيش المكونات المادية للحاسوب	15
ثانيا– مدى صلاحية مكونات الحاسوب المنطقية للتفتيش	17
ثالثا– مدى قابلية شبكات المعلومات المتصلة بالحاسوب الآلي للتفتيش	20
الفرع الثاني : ضمانات التفتيش في البيئة الالكترونية	31
أولا– الضمانات الموضوعية للتفتيش الالكتروني	31
ثانيا–الضمانات الشكلية للتفتيش الالكتروني	40
المطلب الثاني: ضبط الأدلة في الجرائم الالكترونية	46
المطلب الثالث: المعاينة في العالم الافتراضي	56

الفرع الأول : مفهــوم المعايــنة	56
الفرع الثاني : نطاق إعمال المعاينة الالكترونية	59
أولا– معاينة مكونات الحاسب	59
ثانيا– معاينة أنظمة الاتصال بشبكة الانترنت	64
المطلب الرابع: الخبرة التقنية في الجريمة الالكترونية	67
الفرع الأول: دور الخبرة التقنية في إثبات الجريمة الالكترونية	68
الفرع الثاني: الجـوانب القانــونية والفنية التــي تحكم الخبرة في مجــال الجرائم الالكترونية	73
أولا– الجوانب القانونية للخبرة الالكترونية	73
ثانيا– الجوانب الفنية للخبرة الالكترونية	76
المبحث الثاني: استحداث إجراءات تحقيق خاصة بالجرائم الالكترونية	81
المطلب الأول: التسـرب الالكترونــي	82
الفرع الأول: المقصود بالتسرب	83
الفرع الثاني: الضوابط التي تحكم التسرب في الجرائم الالكترونية	85
أولا–الضوابط الإجرائية	85
ثانيا–الضوابط الموضوعية	86
المطلب الثاني: اعتراض المراسلات و المراقبة الالكترونية	87
الفرع الأول : مفهوم الاعتراض و المراقبة الالكترونية	88
الفرع الثاني : القيود الواردة على عملية اعتراض ومراقبة المراسلات	94
أولا– الحصول على إذن السلطة القضائية المختصة	94

ثانيا– تسبيب اللجوء إلى اعتراض أو مراقبة المراسلات	96
ثالثا– تحديد الجرائم محل الاعتراض و المراقبة	97
رابعا–سرية الإجراءات و كتمان السر المهني	98
المطلب الثالث :الحفظ و الإفشاء العاجلان للمعطيات المتعلقة بالسير	99
الفرع الأول: الحفظ العاجل للمعطيات المتعلقة بالسير	101
أولا– مفهوم الحفظ العاجل للمعطيات المتعلقة بالسير	101
ثانيا –ضمانات المشتبه فيه أثناء عملية التحفظ للمعطيات الالكترونية	104
الفرع الثاني: الإفشاء العاجل لمعطيات السير	106
المطلب الرابع: إنتـــاج المعطيات المعلوماتـــية	108
المطلب الخامس: تجميع معطيات المرور في وقتها الفعلي	112
الفصل الثاني: القيمـة الثبوتـية للدليل الالكتروني أمام القضاء الجزائي	117
المبحث الأول: الطبيعة القانونية للدليل الالكتروني	118
المطلب الأول: مفهـوم الدليـل الالكترونـــي	120
الفرع الأول: مقاربة في تعريف الدليل الالكتروني	121
الفرع الثاني: مميزات الدليل الالكترونـــي	124
أولا–الدليل الالكتروني دليل علمي	124
ثانيا–الدليل الالكتروني دليل تقني	125

ثالثا– صعوبة التخلص من الدليل الالكتروني	126
رابعا– الرقمية الثنائية للدليل الالكتروني	126
المطلب الثاني: تصنيفات الدليل الالكترونـي و نطاق الإثبات به	127
الفرع الأول: تصنيفات الدليل الالكتروني	128
أولا– تصنيف الدليل الالكتروني من حيث هيئته	128
ثانيا– تصنيف الدليل الالكتروني من حيث قيمته الاستدلالية	130
الفرع الثاني: نطـاق الإثبات بالدليل الالكتروني	131
أولا – الجرائم المرتكبة بواسطة الحاسب	132
ثانيا– الجرائم المرتكبة على الحاسب و الانترنت	133
المبحث الثاني: قبول القاضي الجزائي للدليل الالكتروني	135
المطلب الأول: مشروعية الدليل الالكترونـــي	137
الفرع الأول: مشروعية الدليل الالكتروني في الوجود	137
أولا – نظام الإثبات المقيد	138
ثالثا–نظام الإثبات الحرّ	140
ثالثا–نظام الإثبات المختلط	143
الفرع الثاني: مشروعية الدليل الالكتروني في التحصيل	144
المطلب الثاني: حجية الدليل الالكتروني في الإثبات الجزائي	150

الفرع الأول : شروط اكتساب الدليل الالكتروني حجية في الإثبات	151
أولا– يقينية الدليل الالكتروني	152
ثانيا– وجوب مناقشة الدليل الالكتروني	157
الفرع الثاني: دور القيمة العلمية للدليل الالكتروني في تكوين اقتناع القاضي الجزائي	161
المطلب الثالث : موقف المشرع الجزائري من الإثبات بالأدلة الالكترونية	166
الفرع الأول: موقف المشرع الجزائري من أنظمة الإثبات الجنائي	167
الفرع الثاني: أثر تبني نظام الإثبات الحر على سلطة القاضي الجزائي الجزائري في قبول الدليل الالكتروني	171
أولا– مفهوم الاقتناع الشخصي للقاضي الجزائي	171
ثانيا– سلطة القاضي الجزائي الجزائري في تقدير الدليل الالكتروني	175
البـــاب الثاني **عقبات التحقيق الجنائي في الجرائم الإلكترونية والحلول المقترحة لتجاوزها**	181
الفصل الأول **عقبات التحقيق الجنائي في الجرائم الإلكترونية**	184

فهرس الموضوع

المبحث الأول: عقبات ناتجة عن الطبيعة الخاصة لجرائم الالكترونية	185
المطلب الأول:انعكاسات الطـــابع العابر للحدود لجرائـــم الالكترونية علـــى التحقيق	186
الفرع الأول: تنــازع الاختصاص بالتحقيق في الجرائم الالكترونية	186
الفرع الثاني: مشكلة احترام سيادة الدولة	192
المطلب الثاني: صعوبات الاستدلال و الإثبات في الجرائم الالكترونية	195
الفرع الأول : صعوبة اكتشاف الجريمة	196
أولا–غياب الآثار المادية للجريمة و سهولة محو الدليل	196
ثانيا–العزوف عن التبليغ بوقوع الجريمة	199
الفرع الثاني: صعوبة اكتشاف هوية الجناة	201
أولاـ تعذر تحديد عنوان المجرم الالكتروني	201
ثانيا – فرض الجناة لتدابير أمنية	206
الفرع الثالث: نقص خبرة و كفاءة سلطات الاستدلال	209
الفرع الرابع : تعارض إجراءات التحقيق مع مبدأ احترام الحياة الخاصة	212
الفرع الخامس : ضخامة كم البيانات الواجب التحقيق فيها	217
المبحث الثاني:عقبات ناتجة عن ضعف قوانين مكافحة الجرائم الالكترونية	219
المطلب الأول: قصور التشريعات العقابية القائمة	219

الفرع الأول:عدم كفاية النصوص العقابية التقليدية	220
الفرع الثاني:عدم ملائمة إجراءات التحقيق المألوفة مع الجرائم الالكترونية	223
أولا- صعوبة إخضاع المكونات المنطقية للحاسوب الآلي للتفتيش والضبط	224
ثانيا- صعوبة معاينة الجرائم الالكترونية	229
الفرع الثالث: ضعف ا لحجية الثبوتية للأدلة الالكترونية	230
المطلب الثاني: عدم فعالـية التعـــاون الدولـــــي في مجـــال مكافحة الجرائم الالكترونية	233
الفرع الأول: تباين التشريعات العقابية للدول	233
أولا-غياب نموذج موحد للنشاط الإجرامي	234
ثانيا- تباين النظم القانونية الإجرائية	235
الفرع الثاني: صعوبات متعلقة بالمساعدات القضائية الدولية	237
الفصل الثاني **الحلول المقترحة لتجاوز عقبات التحقيق في الجرائم الإلكترونية**	241
المبحث الأول: الحلـول القانونية المقترحة لتدارك عقبات التحقيق في الجرائم الالكترونية	242
المطلب الأول: حوكمة المنظومة التشريعية الـوطنية لمـواجـهة الجـريمة الالكترونية	243
الفرع الأول : تطبيق النصوص الجنائية التقليدية على الجرائم الالكترونية	244

الفرع الثاني: ضمان مـواكبة التشريعات الجزائية الوطنية لمتغيرات الجريمة الالكترونية (التحين و التحديث)	249
أولا – التشريعات المقارنة	249
ثانيا– سياسة المشرع الجزائري في مواكبة تطورات الإجرام الالكتروني	254
المطلب الثاني: تكثيف التعاون الدولي في مجال التشريع	267
الفرع الأول: الجهود المبذولة على الصعيد الدولي	268
أولا –التنسيق التشريعي في إطار الأمم المتحدة	268
ثانيا–التنسيق التشريعي في إطار منظمة التعاون و التنمية الاقتصادية	276
الفرع الثاني: الجهود المبذولة على الصعيد الجهوي	278
أولا–على المستوى الأوروبي	278
ثانيا– على مستوى الوطن العربي	287
ثالثا ـ على مستوى مجموعة دول الثمانية G8	291
المبحث الثاني: الحلـول القضائية المقترحة لتدارك عقبات التحقيق في الجرائم الالكترونية	294
المطلب الأول : تعزيز التعاون القضائي الدولي	295
الفرع الأول : تدعيم المساعدة الأمنية و الفنية المتبادلة بين الدول	296
أولا ـ تفعيل التعاون الأمني أو الشرطي الدولي	296
ثانيا ـ تكثيف التعاون الفني الدولي	309

الفرع الثاني: تشجيع المساعدة القضائية الدولية	314
–أولا: تثمين الإجراءات التقليدية للتعاون القضائي الدولي	315
–ثانيا: إقرار إجراءات جديدة للتعاون الدولي القضائي	324
المطلب الثاني: الاستعانة بالتدابير الوقاية و الحماية الفنية	330
الفرع الأول: تقنيات الحماية الفنية مصدرا موثوقا لإثبات الجريمة الالكترونية	331
أولا ـ الحماية الفنية عن طريق البرامج	331
ثانيا- الحماية الفنية عن طريق أنظمة الرقابة الالكترونية الوقائية	334
الفرع الثاني: التوعية و التحسيس	336
الخاتمة	340
قائمة المراجع	346
فهرس الموضوع	373

ملخص

تعد الجرائم الالكترونية من الأنماط الإجرامية الجديدة التي أفرزتها تكنولوجيات الإعلام والاتصال الحديثة، فهي تختلف تماما عن الجرائم التقليدية، في ذاتية أركانها و أساليب ارتكابها والبيئة الافتراضية و اللامادية التي ترد عليها و خصوصية مرتكبيها. مما جعلها ظاهرة غريبة عن نصوص القانون الجزائي التقليدي بشقيه الموضوعي و الإجرائي، من ثمة فأية محاولة إخضاع هذا النمط الإجرامي الجديد لإجراءات التحقيق و الإثبات المألوفة سيؤدي حتما إلى عدم الوفاء بمتطلبات مبدأ الشرعية الإجرائية، وينجر عنه عقبات كثيرة أمام سلطات التحقيق.

ولكن مع تزايد معدلات الجرائم الالكترونية وامتداد آثارها إلى كافة مجالات الحياة بسبب ارتباطها بشبكة الانترنت، اضطرت الدول إلى ترشيد نصوصها الإجرائية التقليدية لتصبح نافدة في مواجهة هذه الجرائم. إلى حين إرساء نصوص جديدة تتلاءم مع الطبيعة الخاصة لظاهرة الإجرام الالكتروني، وتواكب التطورات و المتغيرات التي صاحبتها.

فإلي أي مدى يمكن التعويل على هذه النصوص الإجرائية للتصدي لهذا النمط الإجرامي المتجدد والمتطور ؟ تلك هي الإشكالية التي حاولنا الإجابة عنها من خلال هذه الأطروحة.

Résumé ;

Les infractions électroniques sont l'un des nouveaux types de la criminalité engendré par les technologies modernes de l'information et de la communication, qui se diffère des infractions classiques par ses éléments particulières, en l'occurrence ses modes de commission, son environnement virtuel et les caractéristiques de ses auteurs, se qui en fait un phénomène étrange aux textes objectifs et procédurales de droit pénal actuel. Alors toute tentative de soumettre cette nouvelle forme de criminalité aux procédures d'enquête et de preuve familières, ne satisfera pas aux exigences du principe de légalité procédurale et créera de nombreux obstacles aux autorités chargées d'enquête.

Cependant, comme les cybercrimes ont augmentés et leurs effets se sont étendus a tous les domaines de la vie en raison de leur connexion a l'internet, les Etats ont du rationaliser leurs lois procédurales traditionnelles pour devenir applicables et efficaces contre ces infractions. Jusqu'à la mise en place de nouveaux textes adaptés a la nature particulière de la cybercriminalité, et aux évolutions et changements qui les accompagnent.

Dans quelle mesure ces procédures peuvent-elles être invoquées pour répondre a ce type de criminalité renouvelé et évolutif ? Telle est la problématique a la quelle nous avons essayé de répondre a travers cette thèse.