إشكالات الإثبات والاختصاص في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود

الدكتورة/ آمال فكيري
جامعة لونيسي علي البليدة 2، الجزائر

❖❖❖❖❖❖❖

ملخص:

لقد أثارت الجرائم الخاصة بتكنولوجيا الإعلام والاتصال بعض التحديات القانونية والعملية أمام الأجهزة المعنية بالبحث عن الجرائم وضبطها، وخصوصا فيما يخص مباشرة إجراءات البحث والتحري التقليدية في بيئة افتراضية لا مكان فيها للأدلة المادية، مما أظهر مدى الحاجة إلى تطوير آليات البحث بما يتلاءم وخصوصيات هذه الجرائم، وجعل مسألة ملاءمة الإجراءات الجنائية في البحث والتحري مع خصوصية هذه الجرائم تستأثر باهتمام المشرعين في مختلف الدول. كما أن هذه الجرائم قد خلقت عالما جديدا لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها الأمر الذي أوجد صعوبات وإشكالات قانونية لا تقتصر على ضبط هذه الجرائم وإثباتها فحسب، وإنما أثارت أيضا تحديات أكثر تعقيدا مرتبطة بتحديد جهة الاختصاص وبالتبعية القانون الواجب التطبيق على هذا الصنف من الجرائم.

الكلمات المفتاحية: الدليل الرقمي _ البيئة الرقمية _ تنازع الاختصاص _ الإنابة القضائية الدولية.

Abstract:

The ICT (information and communication technologies) related crimes have created some juridical and operational challenges to the institutions in charge of researching and controlling crime, particularly in terms of undertaking classical procedures of research and investigation amongst a hypothetic environment which lack of material proofs. Therefore, it is necessary to develop research systems which correlate with the characteristics of these crimes and endeavor to consider the adaptation of such criminal procedures, in terms of research and investigation, to the characteristics of these crimes, a case that shall draw legislators' attention throughout the different countries.

Furthermore, these crimes have created a new world that admits neither of geographical and political boundaries of the countries nor their sovereignty, creating thus juridical difficulties and problems, related not only to controlling and proving these crimes, but raise more complicated challenges which consist in defining the jurisdiction and dependency regarding the applicable law on this category of crimes.

Key words: *numerical proof – numerical environment, conflict of competence – international rogatory commission.*

مقدمة:

لقد أعقب اكتشاف الحاسوب ظهور شبكة الانترنت، بحيث أضحى العالم قرية صغيرة بإمكان أي شخص إيصال معلومة بين نقطتين تبعد إحداهما عن الأخرى آلاف الكيلومترات وخلال لحظات. لكن على الرغم من هذه الفوائد الكبيرة للحاسوب وشبكة المعلومات إلا أنه قد تم استغلالها في ارتكاب الجرائم والاعتداء على حقوق الآخرين، حتى أصبح هذا النوع المستحدث من الجرائم المشكلة التي شغلت المشرعين في مختلف البلدان وجعلهم يفكرون في كيفية احتواء هذه الجرائم تشريعيا لاسيما وأن هناك قصورا في التشريعات التقليدية سوء من الناحية الموضوعية أو الإجرائية.

إن مفهوم الجرائم المتصلة بالإعلام والاتصال من المفاهيم الحديثة التي رافقت التطور التكنولوجي الحديث، فهو يرتبط بإحدى أهم مبتكرات التكنولوجيا المعاصرة (الانترنت)، حتى فضل البعض تسميتها " بجرائم التكنولوجيا الحديثة "[1]، فهي جريمة وحيدة الأداة يتم ارتكابها عن طريق الحاسوب الآلي ومن قبل أشخاص لديهم الدراية الفائقة باستعمالات هذه الشبكة، لذلك تتميز بطبيعة خاصة تختلف عن الجرائم العادية كونها تمس بأنظمة المعالجة الآلية للمعطيات المحددة، فهي جريمة خفية يصعب اكتشافها حتى من قبل المجني عليه نفسه. كما أنها جريمة هادئة لا عنف في تنفيذها بل كل ما تتطلبه هو القدرة على التعامل مع الحاسوب بتقنية وخبرة عالية، يضاف إلى ذلك قدرة الجاني على محو وإزالة آثارها لذلك يصعب إثباتها. كما يمكن أن لا تقتصر تلك الآثار بالضرورة على إقليم الدولة التي ارتكبت عليها، فهي جريمة عابرة للحدود تتم في بيئة افتراضية ألغت الحدود الجغرافية بين الدول ذات فاعلية تفوق قدرة الأجهزة الدولية المختصة بمكافحة الجريمة.

إن الجرائم الخاصة بتكنولوجيا الإعلام والاتصال جريمة حديثة النمط، وغير معروفة بين صور الإجرام البشري التقليدي الأمر الذي ميزها بهذه خصائص، حتى عرفها البعض بأنها: عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي[2].

أما من الناحية القانونية فتعرّف أنها كل نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي[3]. حيث يطلق جانب من الفقه على هذا النوع من الجرائم بالجرائم العالمية وهي تختلف عن الجرائم الدولية. فالجريمة الدولية مصدرها القانون الدولي، بينما الجريمة العالمية مصدرها القانون الجنائي الوطني أو القوانين الجنائية الوطنية مجتمعة، حيث ترجع هذه التسمية إلى مزاولة مجموعة من الأنشطة الإجرامية على مستوى عالمي وعبر حدود الدول نتيجة للتقدم المذهل في وسائل الاتصال والمواصلات[4].

بالاستناد إلى ما سبق وبالرجوع إلى الخصوصية التي تميز جرائم تكنولوجيا الإعلام والاتصال من غياب للآثار التقليدية وصعوبة لتحديد مكان ارتكابها. وأمام العوائق التي تواجه سلطات البحث والتحري للإثبات الجنائي في ذلك، ارتأينا من خلال هذه الورقة البحثية الخوض في أهم الإشكالات الإجرائية التي تثيرها هذه الجرائم: فما هي الإشكالات الإجرائية التي تثيرها جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود في ظل زمن أصبحت فيه تكنولوجيا الاتصال ضرورة لا يمكننا الاستغناء عنها؟ ولأجل الإجابة عن

هذه الإشكالية فضلنا اتباع المنهج الوصفي التحليلي والقانوني في نفس الوقت محاولة منا تسليط الضوء على آليات وإجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقّب المجرمين، والمتمثلة في الدليل الرقمي والتفتيش عبر الفضاء المعلوماتي، وكذلك تحديد معايير الاختصاص والقانون الواجب التطبيق عند ارتكاب هذا النوع من الإجرام العابر للحدود، وذلك من خلال مبحثين:

المبحث الأول: إشكالات الإثبات في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود

المبحث الثاني: تنازع الاختصاص في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود

المبحث الأوّل

إشكالات الإثبات في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود

إن الإثبات الجنائي نشاط إجرائي موجه مباشرة للوصول إلى اليقين القضائي طبقًا لمعيار الحقيقة الواقعية، وذلك بشأن الاتهام أو أي تأكيد أو نفي آخر يتوقف عليه إجراء قضائي[5]. وإن طبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها، لذلك فإن جرائم تكنولوجيا الإعلام والاتصال يمكن أن تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها، فالمعطيات التقنية المعلوماتية أضافت إلى مشكلة الجريمة أنماطا إجرامية على درجة عالية من التعقيد، يحتاج إثباتها إلى أسلحة وأدوات علمية نابعة من طبيعة الجريمة[6]. حيث تثير مسألة الإثبات في مجال الحاسوب والإنترنت صعوبات كبيرة أمام القائمين على التحقيق، كما أفرزت أدلة جنائية ذات طبيعة مختلفة يصعب التعامل معها، اصطلح عليها بالأدلة الرقمية. قد يتطلب الأمر لكشفها ولوج البيئة المعلوماتية بحثاً عنها. ولأجل توضيح ذلك نقسم المبحث إلى مطلبين:

المطلب الأول: الدليل الرقمي في مجال الإثبات الجنائي العابر للحدود

المطلب الثاني: التفتيش عبر البيئة الرقمية لإثبات الجرائم العابرة للحدود

المطلب الأوّل: الدليل الرقمي في مجال الإثبات الجنائي العابر للحدود

يعد الإثبات الجنائي بالأدلة الرقمية من أبرز تطورات العصر الحديث في كافة النظم القانونية، لكن عملية ضبط الدليل الرقمي والبحث عنه أمر في غاية الصعوبة والتعقيد، إن لم يكن مستحيلاً أحياناً حينما يكون محل البحث هو شبكة الإنترنت بخصوص الجرائم العابرة للحدود، على اعتبار أن التفتيش والضبط في هذه البيئة الافتراضية يتطلب أن يتم خارج حدود الدول، وفي نطاق دولة أخرى[7]. ما يتطلب الحصول على إذن مسبق بذلك من سلطاتها، لما ينطوي عليه من مساس بسيادة هذه الدولة.

الفـرع الأول: مفهوم الأدلة الرقمية

المادية، وذلك عن طريق بحث أو تأكيد الاتهام أو نفيه[8]. والدليل الجنائي هو معلومة يقبلها المنطق والعقل يتم الحصول عليها بإجراءات قانونية ووسائل فنية أو مادية أو قولية ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة أو فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه[9]. أما عن الدليل الرقمي فهو الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة[10].

وللتوضيح أكثر سوف نحاول التعريف بالأدلة الرقمية وخصائصها من خلال ما يلي:

أولا- تعريف الدليل الرقمي:

إن الدليل الرقمي (Digital Guide) هو الدليل المأخوذ من أجهزة الكمبيوتر في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكوّن من رقمي لتقديم معلومات في أشكال متنوعة، مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء[11].

ثانيا- خصائص الدليل الرقمي وقيمته القانونية في مجال الإثبات الجنائي:

أ- خصائص الدليل الرقمي:

يمتاز الدليل الرقمي بعدة خصائص منها أنه دليل علمي من طبيعة تقنية، فهو يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، ونتيجة للطبيعة التقنية له فإنه اكتسب مميزات عن الدليل المادي من حيث قابليته للنسخ، بحيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير. كما أن الأدلة الرقمية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها مما يؤدي إلى صعوبة الخلاص منها، بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله، وذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة.

والدليل الرقمي متنوع ومتطور[12]. وهو دليل صعب التخلص منه، حيث يمكن استرجاعه بعد محوه وإصلاحه بعد إتلافه وإظهاره بعد إخفائه، وهي ميزة يتمتع بها عن غيره من الأدلة التقليدية. فنشاط الجاني في عملية محو الدليل يشكل في حد ذاته دليلا ضد الجاني لأن هذا النشاط يتم تسجيله في الحاسوب الآلي، ويمكن استخلاصه لاحقا. ويترتب على هذه الخاصية مسائل قانونية هامة أبرزها مسألة التخلص أو إخفاء الدليل، وهو يعد فعلا آخر موضوع تجريم بمقتضى القانون.

لكن الدليل الرقمي هو دليل معنوي غير مرئي سهل الإخفاء ومحمي، يشكل عائقا كبيرا أمام أجهزة العدالة الجنائية لجملة من الأمور، كالتخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة، وتشفير البيانات المخزنة إلكترونيًا أو المنقولة عبر شبكات الاتصال عن بُعد الذي يشكل عقبة كبيرة أمام إثبات جرائم التكنولوجيا الحديثة والبحث عن الأدلة.

ب- القيمة القانونية للدليل الرقمي في مجال الإثبات الجنائي:

إن القيمة القانونية للدليل الرقمي في مجال الإثبات الجنائي تتمثل في مشروعية الدليل الرقمي وحجيته.

فطبقا لمبدأ الشرعية الإجرائية فلا يكون الدليل مقبولا في عملية الإثبات إلا إذا كان مشروعا، بأن تم البحث عنه والحصول عليه وفقا لطرق مشروعة، وعلى هذا الأساس فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون

باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية، وهو ما أخذت به معظم التشريعات الجنائية.

ومشروعية الدليل تتطلب صدقه في مضمونه، وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة تدل على الأمانة والنزاهة من حيث طرق الحصول عليه، وهو ما يرتب عدم القبول بدليل رقمي 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 من أجل فك شفرة للدخول إلى النظم المعلوماتية أو كلمة السر اللازمة للدخول إلى ملفات المعلومات المختزنة، أو القيام بإجراء لتنصت أو المراقبة الإلكترونية عن بعد دون سند قانوني.

وقد أشار المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في مجال حركة إصلاح الإجراءات الجنائية وحماية حقوق الإنسان إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في بيئة تكنولوجيا المعلومات وإلا ترتب عليه بطلان الإجراء[13].

لكن هل الدليل الرقمي غير المشروع دليل براءة؟

الراجح هو أن المشروعية تقتصر على دليل الإدانة دون البراءة، لأن عدم قبول دليل البراءة بحجة أنه غير مشروع يؤدي إلى نتيجة خطيرة وهي إمكانية إدانة بريء وهو ما لا يستقيم عدلا ولا منطقا[14].

الفرع الثاني: إشكالية الإثبات بالدليل الرقمي في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود

إن سهولة محو الدليل في زمن قصير تُعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال الإجرام الالكتروني العابر للحدود، وتتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصال عن بُعد، فالقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثًا عن الأدلة وتحقيقها، كما أن أدلة الإثبات على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنية ودراية فائقة في هذا المجال ولذلك فإن نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدي إلى ضياع الدليل بل تدميره أحيانًا[15].

ويضاف إلى ذلك أن كل المعطيات ليس لها تجسيد دائم على أية دعامة، وهي غير مسجلة على أسطوانة صلبة أو مرنة، ولا على أية دعامة مادية منقولة أيًا كانت، فقد توجد هذه المعطيات في الذاكرة الحية للحاسوب، ويتم محوها في حالة عدم حفظها أو تسجيلها على أية أسطوانة، وحتى لو كانت المعطيات قد تم تخزينها على دعامة مادية، إلا أنه قد يكون من الصعب الدخول إليها بسبب وجود نظام معلوماتي للحماية، وعلاوة على ذلك قد يتقاعس المجني عليه عن التبليغ عن هذه الجرائم إلى السلطات المختصة[16]. وسنبين ذلك من خلال:

أولا- القواعد الإجرائية التقليدية لكشف الدليل الرقمي:

إن ظهور الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتي باتت تتخذ أنماطا جديدة، أصبح لا يجدي معها اتباع الطرق التقليدية في تحصيل الدليل لإثباتها، لما تثيره طبيعتها غير المادية من إشكالات. كما أن الطبيعة الخاصة للدليل الرقمي سيؤدي حتما إلى تغيير كثيرٍ من المفاهيم السائدة حول إجراءات وطرق الحصول عليه، واستحداث قواعد ووسائل إجرائية تتلاءم مع طبيعة البيئة التقنية وتتمثل في كل من:

أ- تفتيش نظم المعالجة الآلية:

إن محل التفتيش في الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال هو الحاسوب بمكوناته المادية والمعلوماتية وشبكاته، وهو تفتيش ذو الطابع غير المادي، ولا يعدو أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي.

ب- الخبرة في البحث عن الدليل الرقمي:

لما كانت أدلة الإثبات المتحصلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنية ودراية فائقة في هذا المجال، فإن نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدي إلى ضياع الدليل بل تدميره أحيانًا[17].

ومنذ ظهور جرائم التكنولوجيا الحديثة فإن الضبطية القضائية وسلطات التحقيق عموما تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسوب الآلي والمنظومات المعلوماتية، وذلك بغرض كشف غموض الجريمة وتجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق. وقد أشار المشرع الجزائري في المادة الخامسة الفقرة الأخيرة من القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أنه يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[18]. وبالإضافة الى مصالح الضبطية القضائية التابعة للشرطة أو الدرك فإنه وبموجب المرسوم الرئاسي رقم 183/04 المؤرخ في 2004/06/26 تم إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام تحت وصاية القيادة العامة للدرك الوطني[19]. أما على مستوى المديرية العامة للأمن الوطني فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية، ومن الفروع التقنية التي تضمها هذه المخابر، خلية الإعلام الآلي والتي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية بناء على تسخيرات أو إنابات قضائية، كما تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[20].

ثانيا- القواعد الإجرائية الحديثة لكشف الدليل الرقمي:

من ضمن المقومات التشريعية الحديثة التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ما جاء به في القانون الإجراءات الجزائية من خلال إجرائي التسرب واعتراض المراسلات ثم من خلال القانون 09-04 أين استحدث إجراءين آخرين وهما المراقبة الإلكترونية وحفظ المعطيات.

أ- التسرب واعتراض المراسلات:

حدد المشرع نطاق إجراء التسرب بالجرائم المذكورة على سبيل الحصر في المادة 65 مكرر5 و 65 مكرر11 من قانون الإجراءات الجزائية التي من بينها الجرائم الماسة بأنظمة المعالجة الآلية المعطيات، حيث نظم المشرع مفهوم التسرب وشروطه في المواد من 65 مكرر 11 إلى المادة 65 مكرر. أما عن اعتراض المراسلات السلكية واللاسلكية فقد ضمنه ستة مواد من المادة 65 مكرر5 إلى المادة 65 مكر10، ويعتبر البريد الإلكتروني أهم وسيلة تقنية في مجال التراسل الإلكتروني ومن ثم فعملية الاعتراض تنصب عليه.

ب-المراقبة الإلكترونية وحفظ المعطيات:

استحدث المشرع إجراء المراقبة الالكترونية بموجب المادة الثالثة من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حينما أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم، اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها. بأن تكون هناك ضرورة تتطلب هذا الإجراء، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، وأن يتم تحت سلطة القضاء وبإذن منه، مثل تقنية مراقبة البريد الإلكتروني. ولأجل هذا الغرض استحدث المشرع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال السابق الإشارة إليها، التي تكلف بضمان المراقبة الوقائية للاتصالات الإلكترونية وتجميع وتسجيل وحفظ المعطيات الرقمية قصد الوقاية والمكافحة لهذه الجرائم.

المطلب الثاني: إشكالية التفتيش عبر البيئة الرقمية لإثبات الجرائم العابرة للحدود

التفتيش في مدلوله القانوني بالنسبة للجرائم التكنولوجيا الحديثة لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية، فيقصد به أنه إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات، لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم.

والتفتيش في نطاق البيئة الرقمية يُنظر إليه في كثير من الأحيان على أنه غير مجدٍ لما يكتنفه من صعوبات أثناء تنفيذه خاصة بالنسبة للجرائم العابرة للحدود، فالصعوبات الإجرائية التي تعيق خضوع البيانات المخزنة آليا لقواعد التفتيش التقليدية، ما تعلق منها بتعدد الأماكن التي يوجد بها النظام ألمعلوماتي داخل أو خارج الدولة، فقد يكون حاسوب المتهم متصلاً بغيره من الحواسيب عبر شبكة والذي سوف نحاول توضيحه لاحقا.

الفرع الأول: شروط التفتيش في البيئة الرقمية

لقد حرصت القوانين الإجرائية على إحاطة إجراء التفتيش بشروط وضمانات أساسية منها ما هو موضوعي ومنها ما هو شكلي.

أولا- الشروط الشكلية للتفتيش:

وهي إجراءات وشكليات تضمن صحة ودقة النتائج التي يصل إليها القائم بالتفتيش، وتتمثل في:

إجراء التفتيش بحضور أشخاص معينين بالقانون:

إن كان المشرع الجزائري قد أوجب ضرورة حصول إجراء التفتيش المتعلق بالمساكن وملحقتها بحضور المشتبه فيه عندما يتم تفتيش مسكنه من طرف الضبطية القضائية، وإن تعذر ذلك بامتناعه عن حضور التفتيش أو كان هاربا يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش، إلا أنه استثنى تطبيق هذه الشروط عندما يتعلق الأمر بالجرائم المعلوماتية[21]. وقد كان ذلك لبسط نوع من السرية أثناء جمع الدليل الرقمي والإسراع في استخلاصه قبل فقدانه.

أ- الميعاد الزمني لإجراء التفتيش:

لقد حدد المشرع الجزائري ميقات تنفيذ إجراء التفتيش عامة من الساعة الخامسة صباحا إلى الساعة الثامنة مساء، وهناك حالات استثنائية يجوز فيها الخروج عن هذا الميقات ويصح إجراؤه في أي ساعة من ساعات الليل والنهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها بالمواد 342 إلى 348من قانون العقوبات المرتكبة في أماكن معينة أو في حالة رضا صاحب المسكن صراحة[22]. لكن في نطاق التفتيش المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، فإن الاستثناء الوارد بالفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية والمتعلق بجواز إجراء ضابط الشرطة القضائية للتفتيش في كل ساعة من ساعات الليل أو النهار عندما يتعلق التحقيق بنوع معين من الجرائم قد شمل هذه الجرائم.

ثانيا- الشروط الموضوعية للتفتيش:

وتمثل في كل من سبب التفتيش، تحديد محل التفتيش، الإذن بالتفتيش وتحديد مجاله.

أ- وجود سبب للتفتيش ومحله:

يشترط لإجراء التفتيش ضرورة وقوع جريمة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال التي نص عليها المشرع في نصوص التجريم والعقاب طبقا لمبدأ شرعية الجرائم والعقوبات بالإضافة إلى أن تكون هذه الجريمة قد وقعت فعل.

إلا أنه وبالرجوع الى نص المادة 05 من القانون 09-04 السابق نجد أن المشرع قد أجاز إمكانية اللجوء إلى إجراء تفتيش النظام المعلوماتي إما للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة الرابعة من نفس القانون.

كما يشترط ضرورة الاشتباه في شخص معين أو اتهامه بارتكاب الجريمة أو المشاركة فيها، فلا بد من تتوافر دلائل كافية تدعو للاعتقاد بارتكابه للجريمة، كأن يتم تحديد هوية الحاسوب الذي تم ارتكاب الجريمة به وكان ذلك الحاسوب يخص شخصا بعينه.

أما عن تحديد محل التفتيش، فهو الحاسوب بمكوناته المادية والمعلوماتية وشبكاته. وهذا المحل إما أن يكون موجودا في مكان معين كالمسكن، أو بحوزة شخص كالحاسوب المحمول[23].

فبالنسبة للتفتيش الواقع على المكونات المادية لنظام المعالجة الآلية لا توجد فيه أي مشكلة في التنفيذ لإمكانية ذلك وسهولته لأنه يرد على أشياء مادية لا خلاف حول خضوعها للتفتيش طبقا لقواعد قانون الإجراءات الجزائية الخاصة بهذا الإجراء[24]. أما فيما يخص تفتيش المكونات المعنوية لنظام المعالجة الآلية، فهل يمكن اعتبار البحث عن أدلة الجريمة المعلوماتية في نطاق نظم الحاسوب نوعا من التفتيش باعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها ليس لها مظهر مادي محسوس في المحيط الخارجي. لكن يتضح موقف المشرع الجزائري من خلال القانون 09-04 حينما أجاز صراحة تفتيش المنظومات المعلوماتية بموجب المادة الخامسة منه[25].

كما أن تفتيش الشبكات المعلوماتية المتصلة بالحاسوب، وهي مجموعة مكونة من اثنين فأكثر من أجهزة الحاسوب والمتصلة ببعضها اتصالا سلكيا أو لا سلكيا[26]. وهو جائز وفقا لنص الفقرة الثانية من المادة الخامسة من القانون 09-04، ففي حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة 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.

ب- الإذن بالتفتيش وتحديد مجاله:

فيما يخص الإذن بالتفتيش، نجد أن المشرع الجزائري لم يقدم حلا لهذه المسألة بصورة صريحة، ذلك أن القواعد الخاصة بإجراء التفتيش المذكورة في قانون الإجراءات الجزائية تتعلق بالتفتيش التقليدي الذي محله المساكن وملحقاتها، وأن القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة بالقانون 09-04 لم يشر فيه إلى هذا الشرط إطلاقا، ولكن جاء المشرع بحالة إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى.

وهو الشيء الذي يمكن من خلاله التساؤل عن إمكانية جواز تفتيش المنظومة المعلوماتية دون حاجة إلى إذن آخر بالتفتيش يخص المنظومة المعلوماتية، ويكفي فقط الإذن المتعلق بالمسكن الذي يتواجد فيه الحاسوب. لكن طبقا لمعيار خصوصية النظام المعلوماتي وما يحتويه من أسرار الأشخاص، فإنه يخضع بالتبعية لمبدأ عدم جواز الدخول إلى هذا النظام المعلوماتي وتفتيشه دون إذن من السلطة القضائية المختصة، ومؤدى ذلك أن ضابط الشرطة القضائية من أجل تفتيش منظومة معلوماتية فإنه يحتاج في الغالب إلى إذنين بالتفتيش، الأول يخص المسكن الذي يتواجد به الحاسوب، والثاني يتعلق بتفتيش المنظومة المعلوماتية في حد ذاتها أو على الأقل إذنا واحدا يجيز لضابط الشرطة القضائية تفتيش جهاز الكومبيوتر الخاص بالمتهم إلى جانب تفتيش المسكن.

أما بالنسبة لتحديد مجال الإذن بالتفتيش في نطاق الأنظمة المعلوماتية، فمن المعلوم أن التخزين هو البيئة الرقمية، ولا شك أن في تحديد إذن التفتيش تحديدا دقيقا بالنسبة للبيئة الرقمية قد يخلق صعوبة أثناء الممارسة العملية في تفتيش نظم المعالجة الآلية، ويرجع ذلك إلى الطبيعة الخاصة لهذه الأخيرة من حيث

كونها تحتوي على عدد كبير من الملفات. وهو ما لم يقدم بشأنه المشرع الجزائري حلا في القانون 09-04 الخاص بجرائم تكنولوجيات الإعلام والاتصال.

لكن هناك من الدول التي نصت تشريعاتها على ضرورة تحديد مجال الإذن بالتفتيش كالولايات المتحدة الأمريكية وكندا.

الفرع الثاني: إشكالية التفتيش العابر للحدود في البيئة الرقمية

فمن المشاكل التي تواجه جهات التحقيق في جمع الأدلة، حالة تطلب امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر عن جهاتها المختصة الإذن بالتفتيش، ودخوله في المجال الجغرافي لدولة أخرى. وهو ما يسمى بالتفتيش العابر للحدود، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها وحدودها الإقليمية، لذلك يثار التساؤل حول تفتيش الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة. فقد يكون حاسوب المتهم متصلاً بغيره من الحواسيب عبر شبكة. وهنا ينبغي التمييز بين ما إذا كان حاسوب المتهم متصلاً بآخر داخل إقليم الدولة أو كان متصلاً بحاسوب يقع في نطاق إقليم دولة أخرى وهو ما يثار بشأنه الجدل.

أولا- اتصال حاسوب المتهم بحاسوب آخر موجود في مكان آخر داخل الدولة:

فهل يمتد التفتيش إلى الأجهزة الأخرى المتصلة بجهاز المتهم، أم يقتصر على جهازه فقط؟

في هذه الحالة عمدت بعض التشريعات الإجرائية إلى حل هذه المشكلة من خلال نصها على إجازة تفتيش نظم المعلومات المتصلة بالحاسوب الذي يجري تفتيشه (الشبكة وما يتصل بها) وتسجيل كل البيانات اللازمة كأدلة إثبات لإدانة المتهم أمام المحكمة، حيث يعتبر المشرع الجزائري من بين هذه التشريعات حيث نصت الفقرة الثانية من المادة الخامسة من القانون 09 -04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بأنه في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة 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[27].

ثانيا- حالة اتصال حاسوب المتهم بآخر موجود بإقليم دولة أخرى:

قد تكون البيانات غير المشروعة جرى تخزينها في حاسوب خارج إقليم الدولة، وبصدد ذلك تباينت الاتجاهات حول مدى امتداد التفتيش للحواسيب الأخرى خارج الدولة، فذهب رأي إلى رفض امتداد التفتيش، وفي المقابل يؤيد جانب آخر أمر امتداد التفتيش إلى الحواسيب الموجودة خارج إقليم الدولة، وهذا الاتجاه أخذ به القانون الفرنسي، كما سمح به قانون التحقيق البلجيكي والاتفاقية الأوروبية لجرائم تقنية المعلومات لعام 2001 التي سمحت للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كومبيوتر معين إلى غيره من الأجهزة المرتبطة به في حال الاستعجال، إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش[28].

ولمواجهة ذلك نجد أن المشرع الجزائري قد أجاز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج الإقليم الوطني، وهو الوارد بالفقرة الثالثة من نص المادة الخامسة من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي تنص: " ....إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل... ".

وفي نفس الإطار أصدر المجلس الأوربي توصية تحمل رقم 13 لسنة 1995 والمتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات، يجيز من خلالها أن يمتد تفتيش الحاسوب إلى الشبكة المتصلة بها ولو كانت تلك الشبكة تقع خارج إقليم الدولة[29].

لكن وبالرغم من ذلك فإن الاتفاقية الأوربية الخاصة بجرائم تقنية المعلومات أجازت في المادة 32 منها إمكانية الدخول بغرض التفتيش إلى أجهزة وشبكات تابعة لدولة أخرى بدون إذنها في حالتين: إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، وإذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش[30].

المبحث الثاني

تنازع الاختصاص في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود

يعتبر مبدأ الإقليمية هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان؛ غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة لجرائم تكنولوجيا الإعلام والاتصال، التي تتجاوز حدود المكان، فجرائم الإنترنت عابرة للحدود، والشبكة العنكبوتية لا تستأثر بها دولة بعينها، لكن عملاً بمبدأ الإقليمية، فإن كل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها داخل حدودها، بصرف النظر عن جنسية مرتكب الجريمة الذي يحتمل معه تنازع القوانين حيال الواقعة الواحدة، والذي يستتبع بالضرورة تنازع الاختصاص وبالذات فيما يتعلق بالجرائم العابرة للحدود التي ترتكب عبر شبكة الإنترنت.

توضيحا لكل ما سبق قسم المبحث ثلاث مطالب:

المطلب الأول: مبادئ تطبيق النص الجنائي.

المطلب الثاني: الجهود الدولية لإقرار الاختصاص القضائي في جرائم الانترنت.

المطلب الثالث: مظاهر التعاون الدولي لمكافحة جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود.

المطلب الأوّل: مبادئ تطبيق النص الجنائي

إن تحديد القانون الواجب التطبيق في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود يقتضي معرفة المبادئ التي يعتمد عليها في تحديد هذا القانون، وبالتبعية تحديد الولاية أو الاختصاص القضائي.

الفرع الأول: مبدأ إقليمية الاختصاص

يقتضي مبدأ الإقليمية أن يخضع كل من يرتكب عمل إجرامي على إقليم الدولة لقانون العقوبات المعمول به لتلك الدولة، ولا فرق في ذلك بين مواطن أو أجنبي، وتطبيقا للمبدأ نص قانون العقوبات الجزائري في المادة الثالثة على أنه: "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي

الجمهورية...". ويعني هذا المبدأ أن قانون العقوبات يطبق على أي جريمة تقع داخل الإقليم الوطني بغض النظر عن جنسية مرتكبيه أو المجني عليه، وينعقد الاختصاص وفقا له بتحقق أحد العناصر المكونة للجريمة سلوكا أو نتيجة ولو كان الفعل غير معاقب عليه في البلد الأصلي، ومن ثم يجب تطبيق قانون العقوبات الوطني.

كما يمكن بناء على هذا المبدأ متابعة الجاني خارج القطر متى كان مساهما أو شريكا في الجريمة التي وقعت داخل الوطن، غير إن هذا المبدأ يجد صعوبة كبيرة في تطبيقه بالنسبة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وهذا بالنظر لطبيعتها وخصائص التي تميزها عن الجريمة التقليدية وخصوصا صعوبة تحديد مكان وقوعها وارتكابها بدقة وكذا زمان حدوثها . فتطبيق المبدأ هنا يصطدم بعقبة مادية تتمثل في صعوبة تحديد مكان وقوع الفعل الأصلي باعتباره شرط أولي لعقد الاختصاص للقاضي الوطني.

الفرع الثاني: الاستثناءات الواردة على مبدأ إقليمية النص الجنائي

إن قانون العقوبات يبسط سلطانه في حدود إقليم الدولة على الجرائم التي ترتكب فيه سواء كان الجاني أو المجني عليه مواطنا أو أجنبيا، لكن لهذه القاعدة استثناءات في بعض الحالات.

أولا- مبدأ عينية النص الجنائي:

إن مبدأ العينية ينسجم مع حق الدولة في حماية مصالحها الأساسية والجوهرية من الاعتداء عليها، حيث يعطى لها الحق في هذه الحالة بتطبيق قانونها الجنائي بغض النظر عن مكان وقوع هذه الجرائم أو عن جنسية مرتكبيها[31]. وقد تلقى هذا المبدأ عدة اعتراضات بالإضافة إلى وجود صعوبات في تنفيذه، في حين أخذت به بعض الدول مع تحديد لنوع الجرائم مثل ما فعل المشرع الجزائري في نص المادة 588 من قانون الإجراءات الجزائية. لكن في الواقع يصادف المبدأ العديد من الصعوبات ترجع بالأساس إلى طبيعة وخصائص جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود، حيث لا تظهر مادياتها بوضوح، كما أن الفاعل يبقى مجهولا، مما يترتب عليه التعقيد في الإجراءات.

ثانيا- مبدأ شخصية النص الجنائي:

وهو احتفاظ الشخص الأجنبي بقانونه الشخصي وهو خارج إقليم دولته وذلك في مواضيع معينة كحقه في التقاضي، ويأخذ المشرع الجزائري بمبدأ الشخصية في نص المادتين 582- 583 من قانون الإجراءات الجزائية، إلا أن هذا المبدأ وردت عليه قيود بصفة عامة وبالتالي فإن الاختصاص لا ينعقد في المحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج.

كما أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته والتعرف عن جنسيته وهي معلومات تعد صعبة المنال في جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود من جهة، ومن جهة ثانية فإن محاكمة المجرم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات خاصة.

ثالثا- تطبيق مبدأ عالمية النص الجنائي على جرائم الانترنت:

يطبق وفقا لهذا المبدأ النص الجنائي على كل جريمة يقبض على مرتكبها في إقليم الدولة أيا كان مكان ارتكابها وجنسية الفاعل أو الجاني فالدولة التي تضبط المجرم عليها بمعاقبته ومحاسبته بحسب قانونها الوطني.

لكن الأخذ بمبدأ عالمية النص الجنائي على إطلاقه، أين يطبق قانون العقوبات على كل مجرم يقبض عليه في إقليم الدولة، أيا كانت الدولة التي ارتكب فيها الفعل الإجرامي وأيا كانت جنسية الجاني قد يؤدي إلى تعارض بين قوانين الدول، إذ يجعل لكل دولة اختصاص بالنظر في أية قضية هي بالأصل من اختصاص قانون آخر، ويتعارض مع مبادئ قانون العقوبات نفسه الذي هو بالأصل قانون إقليمي[32]. كل هذا يجعل تطبيق المبدأ أمرا صعبا من الناحية العملية، ولذا فقد درج البعض على تقييد المبدأ لينطبق على بعض الأنواع من الجرائم، منها جرائم الانترنت العابر للحدود، فتضافرت الجهود في مكافحة هذا النوع من الإجرام تشريعيا وقضائيا وتنفيذيا.

المطلب الثاني: الجهود الدولية لإقرار الاختصاص القضائي في جرائم الانترنت

إذا كان الاختصاص على المستوى الداخلي (الوطني) لا يثير أي إشكال، إذ يتم الرجوع في تحديده إلى المعايير المحددة سلفا في قانون الإجراءات الجزائية، فإن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي بين الدول، وذلك في ظل عالمية وخصوصية جرائم الانترنت من جهة، ولاختلاف التشريعات والنظم القانونية من جهة ثانية.

وإبراز أثر ذاتية أو خصوصية هذه الجرائم في تحديد الاختصاص القضائي. فقد يحدث أن ترتكب جريمة من هذه الجرائم في إقليم دولة معينة من طرف أجنبي فتكون الجريمة هنا خاضعة للاختصاص الجنائي للدولة التي ارتكبت الجريمة في إقليمها استنادا إلى مبدأ الإقليمية، وكذا لاختصاص الدولة التي ينتمي إليها الجنائي انطلاقا من مبدأ الشخصية، وقد تلحق هذه الجريمة تهديدا لأمن وسلامة دولة أخرى فتدخل أيضا في اختصاصها استنادا إلى مبدأ العينية، وهو الأمر الذي قد يترتب عليه تنازع في الاختصاص بين هذه الدول.

وقد لعبت المنظمات الدولية وعلى رأسها منظمة الأمم المتحدة دور مهما في مجال مواجهة الجريمة الالكترونية العابرة للحدود،عبر إقرار العديد من الاتفاقيات وعقد المؤتمرات أهمها مؤتمر "منع الجريمة ومعاملة المجرمين"، كما أنشأت وكالاتها متخصصة لهذا الغرض كالمنظمة العالمية للملكية الفكرية (wipo) بالإضافة الى هذه جهود دولية، هناك جهود الإقليمية تترأسها منظمات الاتحادية بين بلدان يجمعها قاسم مشترك كالاتحاد الأوربي وجامعة الدول العربية.

الفرع الأول: الاتفاقية الأوربية الخاصة بجرائم تقنية المعلومات ببودابست

تحقيقا للتعاون الدولي في مجال مكافحة الجرائم الالكترونية تم اعتماد الاتفاقية المتعلقة بالجريمة الالكترونية من طرف مجلس الوزراء بالمجلس الأوروبي ببودابست بتاريخ 8 نوفمبر 2001[33]. وقد جاءت هذه الاتفاقية لتوحيد السياسة الواجب اتباعها في مكافحة الجرائم الالكترونية، ذلك عن طريق التنسيق بين التشريعات الوطنية، وتطبيق إجراءات تحقيق وملاحقة تتلاءم مع البيئة الافتراضية. ولذلك جاء

بالاتفاقية 22 مادة من أصل 48 مادة تبين القواعد الإجرائية الخاصة بالبحث والتحري في الجرائم الالكترونية. كما نصت الاتفاقية على قواعد خاصة بالاختصاص القضائي في المادة 22 منها ضرورة اعتماد الدول الأطراف على ما يلزم من تدابير تشريعية وتدابير أخرى لإقرار الاختصاص القضائي على الجرائم الواردة في الاتفاقية، وذلك عندما ترتكب الجريمة في إقليم الدولة أو على متن إحدى السفن التي ترفع علمها أو على متن إحدى الطائرات المسجلة بموجب قوانينها، وكذلك على كل جريمة مرتكبة من جانب أحد مواطنيها إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان ارتكابها، أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي لأية دولة. كما نصت الاتفاقية على مطالبة الدول الأطراف بالتشاور حول الاختصاص القضائي الأكثر ملائمة لمحاكمة مرتكبي الجرائم الالكترونية المعلوماتية في حالة تعدد المطالبة من طرف الأطراف بالاختصاص القضائي حول واقعة معينة[34].

الفرع الثاني: الاتفاقيات المنبثقة عن الاتفاقية الخاصة بجرائم تقنية المعلومات ببودابست

لقد جاءت الجهود الدولية ببعض المبادرات التي تلت الاتفاقية الخاصة بجرائم تقنية المعلومات، وذلك صد توحيد التعاون الدولي في مجال تنظيم الآليات الإجرائية في مجال البحث والتحري عن الجرائم المتعلقة بتقنية المعلومات، إضافة إلى السعي نحو مكافحة هذا النوع من الإجرام العابر للحدود، فانبثقت اتفاقيات أخرى عن اتفاقية جرائم تقنية المعلومات بودابست تمثلت في كل من بروتوكول ستراسبورغ والاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

أولا- بروتوكول ستراسبورغ الإضافي لاتفاقية الجريمة المعلوماتية:

وهو بروتوكول جاء بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهة الأجانب التي ترتكب عبر أنظمة الكومبيوتر، تم وضعه في 28 جانفي 2003 بهدف تكملة مضمون اتفاقية الجريمة الالكترونية بودابست، حيث تضمن البروتوكول 17 مادة، نص ضمن المادة 8 منه أن القواعد الإجرائية الموجودة بالاتفاقية تطبق عل الجرائم المشار إليها في هذا البروتوكول، خاصة ما تعلق منها بأحكام الاختصاص القضائي المشار إله في المادة 22 من الاتفاقية[35].

ثانيا- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

اتفاقية مكافحة جرائم تقنية المعلومات محررة بالقاهرة بتاريخ 21 ديسمبر 2010 الموقعة بين الدول الأعضاء في جامعة الدول العربية التي ألزمت الدول الموقعة عليها بإصدار تشريعات داخلية تكافح جرائم المعلوماتية، وهي تهدف الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها. وقد تناولت الاتفاقية الاختصاص القضائي من خلال المادة 30 منها، فنصت على التزام كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عنها في الاتفاقية[36].

ثالثا- الاختصاص القضائي في القانون الجزائري:

على نفس المنهج فقد تدخل المشرع الجزائري بموجب القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وفي المادة 15 منه، حيث اعتبر أنه بالإضافة إلى

قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية فإن 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 الاستراتيجية للاقتصاد الوطني.

المطلب الثالث: مظاهر التعاون الدولي لمكافحة جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود

إن الطبيعية الدولية للجريمة الالكترونية عبر الانترنت استوجبت تعاونا دوليا من أجل مكافحة فعالة. ويقصد بالتعاون الدولي في هذا المجال ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم، وذلك من خلال تدابير وقائية تستهدف مواجهة الصيغة العابرة للحدود للجريمة، وتستجمع الأدلة بمختلف الطرق، وهو ما يستغرق وقتاً، ويتطلب إمكانات لا تملكها سلطات قانونية لدولة واحدة ما لم تدعمها وتساندها جهود السلطات القانونية في الدول الأخرى.

وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه، بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات، وتعزيز التعاون بينها واتخاذ تدابير فعّالة للحد منها والقضاء عليها ومعاقبة مرتكبيها.

إن جرائم تكنولوجيا الإعلام والاتصال وغيرها أدت إلى ظهور تحديات جديدة للمنظومة القانونية على المستوى الدولي، فأجهزة تطبيق القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين، لذا كان لا بد من إيجاد آلية معينه للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها. ولكي يتم ذلك كان لزاما تنظيم هذا النوع من التعاون الدولي تشريعيا وقضائيا وتنفيذيا. ومما تقدم سوف نتناول بالبحث التعاون الدولي لمكافحة جرائم تكنولوجيا الإعلام والاتصال ضمن فرعين: التعاون القضائي والتعاون الدولي في مجال تسليم المجرمين

الفرع الأول: التعاون القضائي

إن التعاون القضائي الدولي هو الآلية الرئيسية للكفاح ضد الجريمة العابرة للحدود بأبعادها المختلفة ففعالية التحقيق والملاحقة القضائية غالبا ما تقتضي تتبع أثر النشاط الإجرام، لذلك فان أجهزة إنفاذ القانون تكون أحيانا بحاجة إلى مساعدة نظائرها في ولايات قضائية، من أهم صور التعاون القضائي التعاون الأمني والمساعدة القضائية الدولية.

أولا- التعاون الأمني على المستوى الدولي:

باتت الجرائم الالكترونية تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية. ومع تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها[37].

لكن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المتصلة بالحاسوب الآلي وملاحقتها قضائيا تؤكد على أهمية المساعدة القانونية المتبادلة والتعاون الأمني بين الدول، الذي أولى له الفقه الجنائي اهتماماً بالغاً لتحقيق القدرة على التصدي للإجرام العابر للحدود وسد أوجه القصور القانوني الذي ساعد المنظمات الإجرامية على اختراق النظم القانونية، فقد يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها، فمتى ما فرّ المجرم خارج حدود الدولة يقف الجهاز الشرطي عاج، لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من العادلة، وقد كان ذلك بإنشاء المنظمة الدولية للشرطة الجنائية "الإنتربول"، التي أسست عام 1923 ومهمتها تقديم المساعدة إلى أجهزة إنفاذ القانون في بلدانه الأعضاء لمكافحة جميع أشكال الإجرام عبر الحدود، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف.

ثانيا- المساعدة القضائية الدولية:

وهي كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم[38]. فملاحقة مرتكبي الجرائم الالكترونية وتقديمهم للعدالة من أجل توقيع العقاب عليهم، يستلزم القيام بإجراءات إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها. ومن هذه الإجراءات معاينة مواقع الإنترنت في الخارج، أو ضبط الأقراص الصلبة أو تفتيش نظم الحاسب الآلي، وهذا كله قد يصطدم بمشاكل الحدود والولايات القضائية[39].

ولقد نص المشرع الجزائري في القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وفي المادة 16 منه على المساعدة القضائية الدولية المتبادلة.

وتتخذ المساعدة القضائية صور عدة منها:

أ- تبادل المعلومات:

الجريمة الالكترونية تتميز بالعالمية وبكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين الأجهزة القضائية والأمنية من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين[40]. وعلى المستوى التشريعي الوطني فقد نصت المادة 17 من القانون 04/09 السابق، على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل.

ب- نقل الإجراءات:

ويقصد بها قيام دولة ما بمقتضى اتفاقية أو معاهدة باتخاذ إجراءات جنائية، وهي بصدد التحقيق في جريمة الالكترونية ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، متى توفرت مجموعة من الشروط ،أهمها التجريم المزدوج في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها[41].

ج- الانابة القضائية الدولية:

ويقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها[42]. وتهدف هذه الصورة 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 أقاليم الدول الأخرى كسماع الشهود أو إجراء التفتيش وغيرها. وعادة وكما هو معهود يتم إرسال طلب الإنابة القضائية عبر القنصل الدبلوماسي[43]، ولأجل ذلك أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق. مثال ذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 21 ديسمبر 2010.

الفرع الثاني: التعاون الدولي في مجال تسليم المجرمين

هو شكل من أشكال التعاون الدولي وذلك كنتيجة حتمية للتطورات الحاصلة في كافة المجالات ومنها مجال الاتصالات تقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول حاجزا أمام مرتكبي الجرائم وبما أن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القانونية، كان لا بد من إيجاد آلية معينة للتعاون مع الدول باعتبارها عضو في المجتمع الدولي من بينها الارتباط بعلاقات دولية وثنائية تتعلق باستلام تسليم المجرمين أين تسلم دولة لدولة أخرى شخصا منسوبا إليه اقتراف جريمة ما أو صدر ضده حكما بالعقاب كي تتولى محاكمته أو تنفيذ العقاب عليه [44]. إضافة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال العدالة الجزائية قصد تنفيذ ذلك.

فبالنسبة لتسليم المجرم المعلوماتي، يجب على الدول أن تتعاون بعضها مع البعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرمين. ويعتبر تطبيقا عمليا للتضامن الدولي في مكافحة الإجرام الالكتروني، لما فيه من خروج عن الحدود الجغرافية للدول لملاحقة المجرمين والتصدي للجريمة، وغالبا ما يتم بناء على اتفاقية خاصة بين دولتين[45]، أو بناء على اتفاق عام كما هو الحال في الاتفاقيات والمعاهدات المتعددة الأطراف[46]. والجدير بالذكر أن منظمة الأمم المتحدة وضعت عام 1990 معاهدة نموذجية لتسليم المجرمين لتكون إطاراً يساعد الدول التي بصدد التفاوض على اتفاقيات التسليم الثنائية، ولذلك فقد حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين، ومنها المشرع الجزائري الذي أخذ هذا الإجراء كمظهر

من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الإجراءات الجزائية، والمادة 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 21 ديسمبر سنة 2010[47].

خاتمة:

إن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال قد خلقت عالما جديدا لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، الأمر الذي خلق صعوبات وإشكالات قانونية لا تقتصر على ضبط هذه الجرائم وإثباتها فحسب، وإنما أثارت أيضا تحديات أكثر تعقيدا مرتبطة بتحديد جهة الاختصاص وبالتبعية القانون الواجب التطبيق على هذا الصنف من الجرائم.

لقد حاولنا من خلال هذه الورقة البحثية الكشف عن تلك الإشكالات الإجرائية من جهة، وإبراز الجهود الدولية المبذولة لمكافحة جرائم تكنولوجيا الإعلام والاتصال، في إطار تلك المؤتمرات التي عقدت لهذا الغرض أو تلك الاتفاقيات الثنائية والجماعية، الموقعة من طرف الدول قصد التعاون من أجل مكافحة الجرائم الالكترونية العابرة للحدود، عن طريق المساعدة القضائية بواسطة تبادل المعلومات ونقل الإجراءات الجنائية عند تحقق ما يسمى بالتجريم المزدوج للفعل المرتكب، إضافة إلى الإنابة القضائية الدولية للفصل في تلك الجرائم. هذا إلى جانب التعاون الدولي في مجال تسليم المجرمين. فتوصلنا إلى أن:

1- الأدلة الرقمية ما هي إلا تطبيق من تطبيقات الدليل العلمي، بما تتميز به من حياد وكفاءة لذلك لا بد أن لا تثير أية إشكال عند تقديمها كأدلة إثبات، فالوصول إلى الحكم السديد في جرائم تكنولوجيا الإعلام والاتصال يتوقف على قدرة القاضي على مناقشة الدليل الرقمي مناقشة علمية صحيحة.

2- قصور القواعد العامة في التفتيش المنصوص عنها في القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. نظرا لاختلاف التفتيش في جرائم تكنولوجيا الإعلام والاتصال عنه في الجرائم التقليدية اختلافا جذريا من الناحية الفنية، مما يؤدي إلى بروز الحاجة إلى الاستعانة بالخبير المعلوماتي. نظرا لنقص الخبرة عند المكلفين بإجراء تفتيش الحاسوب.

3- صعوبة تطبيق القوانين المعاقبة على الجريمة الإلكترونية في الجزائر، لقلّة خبرتها في هذا الشق وغياب المختصين والخبراء القادرين على تشخيص الجريمة قبل عرضها على المحكمة للفصل فيها.

4- مواجهة مشكلة الاختصاص في الجرائم خاصة المستحدثة منها، تبين حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي، بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب مع سرعة انتشار هذا النوع من الجرائم.

5- استصدار الجزائر قوانين لمعاقبة مرتكبي الجرائم الإلكترونية غير كاف، مع عدم تهيئة الأسس التقنية الكفيلة بتصنيف درجات هذه الجرائم وحدّة أضرارها قبل إصدار العقوبة، هذا فضلا عن

غياب التواصل الدائم بين القضاء والمختصين في الاتصالات، ما أفرز شبه تذبذب وغموض في شأن العقوبات الدقيقة في مثل هذه الجرائم.

6- يعد التعاون الدولي نتيجة حتمية لجأت إليه الدول بسبب تقيد سلطات كل دولة بحدود إقليمها، لذا انحصر التعاون الدولي في التخلص من مشكلة الحدود الإقليمية بين الدول، وقد أولى المجتمع الدولي الاهتمام لتوسيع نطاق التعاون في مجال تنفيذ الأحكام الجنائية من خلال الاتفاقيات والمعاهدات الدولية.

كل ما سبق دفعنا إلى ضرورة تقديم بعض المقترحات منها:

1- سَنّ القوانين والأنظمة الخاصَّة التي تسدُّ كافَّة ثغرات الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مثل القوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية، وحفظها، والنصِّ على طرق ثبوتها.

2- استحداث استراتيجيات عقابية وتقنية لحماية ضحايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خاصة فئة الأطفال ورجال المال كونهم الأكثر عرضة لها.

3- التنسيق وتوحيد الجهود بين الجهات المختلفة، التشريعيّة، القضائيّة، الضبطية، الفنية، وذلك من أجل سد منافذ الجريمة الالكترونية قدر المستطاع، والعمل على ضبطها وإثباتها بالطرق القانونية والفنيّة.

4- إنشاء قانون دولي مُوَحَّد، ومحاكم خاصَّة دوليَّة محايدة تتولَّى التحقيق في هذه الجرائم، يكون لها سلطة الأمر بضبط وإحضار المجرم للتحقيق معه أيًّا كان موقع هذا المجرم وبلده.

5- التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية الالكترونية التخريبية الواقعة في أراضيها ضدّ دول أو جهات أخرى خارج هذه الأراضي، إضافة إلى تفعيل اتفاقيات تسليم المجرمين.

الهوامش:

(1) فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، 2003، ص 33.

(2) عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر سنة 2002، ص 01.

(3) عبد الفتاح بيومي حجازي، المرجع السابق، ص 6.

(4) عمر فاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسوب وأبعادها الدولية دراسة تحليلية نقدية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، ط2، دار النهضة العربية، القاهرة، 1995، ص 133 وما بعدها.

(5) آمال عبد الرحيم عثمان، الإثبات الجنائي ووسائل التحقيق العلمية، دار النهضة العربية، القاهرة، 1975، ص 4.

(6) سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – الجرائم الواقعة في مجال تكنولوجيا المعلومات – ط1، دار النهضة العربية، القاهرة، 1999، ص 95 وما بعدها.

(7) جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص 116.

(8) آمال عبد الرحيم عث، الإثبات الجنائي ووسائل التحقيق العلمية، دار النهضة العربية، القاهرة، 1975، ص 4.

(9) أحمد أبو القاسم، الدليل الجنائي المادي ودوره في الإثبات في الفقه الجنائي الإسلامي، دار النهضة، القاهرة، 1991، ص. 183.

(10) عمر محمد بن يونس – مذكرات في الإثبات الجنائي عبر الإنترنت - ندوة الدليل الرقمي بمقر جامعة الدول العربية بجمهورية مصر العربية في الفترة من 5-7 مارس 2006، ص 5.

(11) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت، دار الفكر القانونية مصر، 2006، ص 88.

- كما عرفت المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001 الدليل الرقمي "بأنه المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية"، نقلا عن: مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص 213.

(12) يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات، وقد يكون بيانات مفهومة كما لو كان وثيقة معدة بنظام المعالجة الآلية، كما من الممكن أن يكون صورة ثابتة أو متحركة (أفلام رقمية) أو معدة بنظام التسجيل السمعي البصري أو يكون مخزنا في البريد الالكتروني، وقد يكون أيضا مرتبطا بالتشفير.

(13) قرارات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 4-9 تشرين أول 1994 – البرازيل / ريودي جانيرو بشان جرائم الكمبيوتر.

(14) ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر "الأعمال المصرفية والالكتروني" كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من10-15/ 12 2003، المجلد الخامس، ص 2247.

(15) أسامة أحمد المناعسة وجلال محمد الزعبي ، وصايل الهواوشة ، جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة، ط1، دار وائل للنشر، عمان، الأردن، 2001، ص 289-297.

(16) جميل عبد الباقي الصغير، المرجع السابق، ص 116.

(17) أسامة أحمد المناعسة وجلال محمد الزعبي، وصايل الهواوشة، جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة، ط1، دار وائل للنشر، عمان، الأردن، 2001، ص 289-297.

(18) القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 5 أوت 2009، ج ر عدد 47 الصادرة في 16 أوت 2009، ص 5.

(19) راجع في ذلك المادة الثانية من هذا المرسوم الرئاسي رقم 183/04 المؤرخ في 2004/06/26 يتضمن احداث المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر عدد 41 الصادرة في 27 جوان 2004، ص 18.

(20) راجع المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 53 الصادرة في 8 أكتوبر 2015.

- تُعد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتضم أساسا أعضاء من الحكومة معنيّين بالموضوع ومسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعيّنهما المجلس الأعلى للقضاء .وستضم الهيئة قضاة وضباطا وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين وفقا لأحكام قانون الإجراءات الجزائية، وتكلَّف الهيئة بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. كما تُعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وضمان مراقبة الاتصالات الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة وذلك تحت سلطة القاضي المتخصص.

(21) راجع في ذلك الفقرة الأخيرة من المادة 45 من الأمر 155/66 المتضمن قانون الاجراءات الجزائية الجزائري المعدل والمتمم.

(22) راجع في ذلك المادة 47 من قانون الاجراءات الجزائية المعدل و المتمم.

(23) سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، مصر، 2011، ص 127.

(24) راجع في ذلك المواد 44، 64 من الأمر 155/66 المتضمن قانون الاجراءات الجزائية المعدلة بموجب القانون 22/06 المؤرخ ف 20 ديسمبر 2006، ج ر عدد 84.

- لكن المشرع استثنى بموجب الفقرة الثالثة من المادة 45 والفقرة الثانية من المادة 47 والفقرة الثالثة من المادة 64 تطبيق هذه الضمانات عند إجراء التفتيش بمناسبة تحقيق مفتوح بخصوص الجرائم المعلوماتية.

(25) راجع المادة 05 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال السابق.

(26) علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت - دراسة مقارنة -، الطبعة الأولى عالم الكتب الحديثة، الأردن، 2004، ص 34

(27) إلى جانب المشرع الجزائري نجد المشرع الألماني في المادة 103 من قانون الإجراءات الجزائية ينص على:

" إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر، وكذلك المشرع البلجيكي في المادة 88 من قانون تحقيق الجنايات البلجيكي، وفي الولايات المتحدة الأمريكية تجيز المادة 41 من قانون الإجراءات الجنائية الفيدرالي الأمريكي لقاضي التحقيق إصدار إذن تفتيش ملكية داخل منطقة أو خارجها، متى كانت الملكية عند طلب الإذن موجودة داخل المنطقة، كما حسم المشرع الفرنسي هذه المسألة أيضا بمناسبة تعديله لقانون الإجراءات الجزائية:

- V : QUEMENER Myriam , FERRY Joël, Cybercriminalité Défi mondial, 2em edition, 2009 , p2

(28) تنص المادة 19 فقرة 2 من القسم الرابع من الاتفاقية على أنه: " من حق السلطة القائمة بتفتيش الكومبيوتر المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الحاسب الأصلي محل التفتيش".

- للاطلاع على النص الكامل للاتفاقية الأوروبية لجرائم تقنية المعلومات لعام 2001، راجع الموقع الالكتروني الخاص بالمجلس الاوروبي:
www.conventions.coe.int/treaty/fr/treaties/html/185.htm

(29) Bertrand Warusfel, "Procedure pénale et technologies de l'information: de la Convention sur la cybercriminalité à la loi sur la sécurité quotidienne", Revue Droit et Défense, 2002/1, p 1.

(30) راجع في ذلك المادة 32 من الاتفاقية الأوربية الخاصة بجرائم تقنية المعلومات.

(31) محمود نجيب حسني، شرح قانون العقوبات، القسم العام، الطبعة الخامسة، دار النهضة العربية، مصر، 1982، ص 121.

(32) عمر خوري، شرح قانون العقوبات، القسم العام، ديوان المطبوعات الجامعية، الجزائر، 2008/2007، ص 34.

(33) الاتفاقية الأوربية الخاصة بجرائم تقنية المعلومات على الموقع السابق.

(34) راجع في ذلك المادة 22 من الاتفاقية الأوربية الخاصة بجرائم تقنية المعلومات.

(35) الموقع الإلكتروني للبروتوكول هو: htm89www.conventions.coe.int/treaty/fr/treaties/html/1.

(36) صادقت الجزائر على الاتفاقية بموجب المرسوم الرئاسي 14-252 المؤرخ في 8 سبتمبر 2014 ، ج ر عدد 57 الصادرة في 28 سبتمبر 2014.

(37) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998، ص 75.

(38) سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية – دراسة مقارنة-، رسالة دكتوراه كلية الحقوق جامعة عين شمس، القاهرة، 1997، ص 425.

(39) وقعت الجزائر العديد من اتفاقيات التعاون القضائي مع العديد من الدول منها: المغرب، تونس، مصر، ليبيا، موريتانيا، سوريا، الأردن اليمن، الامارات العربية والسودان ...

(40) وردت المساعدة القضائية في الفقرة الثانية من المادة الأولى لمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية الصادرة بتاريخ 1990/12/14. وكذا ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

(41) سالم محمد سليمان الاوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس،1997، ص425.

(42) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 83.

(43) المادة 2 من معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية 1990.

(44) نجد في هذا الصدد الأمر رقم 65-194 المؤرخ في 29 جوان 1965 المتضمن المصادقة على اتفاقية تسليم المجرمين وتنفيذ الأحكام بين الجزائر وفرنسا.

(45) نجد في هذا الصدد تصديق الجزائر على اتفاقية حديثة لتسليم المجرمين مع حكومة دولة الكويت، الموقّعة بالجزائر بتاريخ 12 أكتوبر سنة 2010، بموجب المرسوم الرئاسي رقم 15-256 المؤرخ في 5 أكتوبر 2015، الجريدة الرسمية، العدد 53 الصادرة في 8 أكتوبر 2015.

(46) هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، القاهرة، 2006، ص 24.

(47) راجع ج ر عدد 57 الصادرة في 28 سبتمبر 2014.