مجلة العلوم القانونية والسياسية

اسم المقال: حتمية إنشاء ضبطية خاصة بالجرائم الإلكترونية
اسم الكاتب: د. بوقرين عبد الحليم
رابط ثابت: https://political-encyclopedia.org/index.php/library/1062
تاريخ الاسترداد: 2026/11/01 15:58 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة العلوم القانونية والسياسية جامعة ديالى ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

حتمية إنشاء ضبطية خاصة بالجرائم الإلكترونية

The inevitable establishment of a special electronic crimes seizure

الكلمة المفتاحية : **ضبطية، الجرائم الإلكترونية** .

Keywords: ***inevitable , electronic crimes***.

د. بوقرين عبد الحليم

قسم الحقوق - جامعة عمار ثليجي الأغواط - الجزائر

Dr. Bu Qurayn Abdul Halim
Department of Law - University of Laghouat - Algeria
E-mail: halim.ma@yahoo.fr

ملخص البحث

في كثير من الدول يعود الإختصاص في التحقيق والفصل في الجرائم الإلكترونية إلى جهاز الضبطية المكلف بالبحث والتحري، وكذا القضاء العادي في جانبه الجزائي، وهو ما يجعل من اكتشاف وإثبات هذا النوع الجرائم من الصعوبة بما كان، وذلك نظرا لنقص الدراية والخبرة العلمية والفنية لرجال الضبطية والقضاء في هذا المجال، ورغم أن القانون في كثير من الأحيان يجيز الإستعانة بالخبرة لتحديد ملابسات القضية والوصول إلى الحقيقة، إلا أن خبرة المحقق وإحاطته بوقائع ومعطيات الجريمة هو المعول عليه في تحقيق العدالة.

إن صعوبة اكتشاف هذا النوع من الجريمة بالدرجة الأولى وعدم القدرة على التحري والتحقيق فيها دون اللجوء إلى الخبرة بدرجة ثانية، يضعنا أمام معادلة غير متكافئة طرفها أجهزة التحقيق بنقص خبرتهم في مجال الكمبيوتر والأنترنت والمعاملات الإلكترونية من جهة، والطرف الآخر قراصنة محتلون يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية والإتصال من جهة أخرى.

لذا كان من الضروري المناداة بإنشاء ضبطية أو جهاز أو هيئة خاصة للتحري والتحقيق في هذا النوع من الاجرام، لا تعتمد على القوة البدنية والتدريب بقدر ما تعتمد على المهارة الفنية والتقية في مجال تكنولوجيا الاعلام والاتصال، وذلك كمرحلة أولى لإنشاء قضاء مختص يفصل في هذه الجرائم.

المقدمـــــة

يواجه المشرع مختلف الجرائم بالتجريم والعقاب كنوع من المكافحة الموضوعية، وفي سبيل ضبط هذه الجرائم والقبض على مرتكبيها يوفر المشرع الإمكانيات البشرية والمادية اللازمة لذلك كنوع من المكافحة الإجرائية، والامر هنا يبقي عادياً لا يثير أي إشكال ما دمنا بصدد جرائم تقليدية عادية، إلا أنه يختلف إذا ما كنا بصدد جرائم غير عادية جرائم تقع في عالم افتراضي.

الجرائم الإلكترونية وهي كل سلوك غير مشروع يتم بالتدخل في العمليات الإلكترونية أو المساس بأمن النظم المعلوماتية والمعطيات التي تعالجها، هذه الجرائم قلبت موازين التحقيق، فلم يعد الامر يتعلق بقوة بدنية أو مهارات قتالية، وإنما بمدي معرفة المحقق لتقنية المعلومات وإتقانه لمتطلبات الإعلام الآلي والإتصال، فهذه المعرفة هي التي تساهم في القبض على المجرم الإلكتروني.

وفي ظل تزايد الجرائم الإلكترونية وتنوع أنماطها وأساليبها وقفت الأجهزة المختصة بالبحث والتحقيق وعلى رأسها الضبطية القضائية عاجزة عن مواكبة هذا التطور وملاحقة هذا النوع من الجرائم، وهو الأمر الذي دفع بالعديد من الدول إلى إنشاء أجهزة مختصة تستطيع التعامل مع هذا النوع من الإجرام.

ومن هنا نطرح الإشكالية التي تحاول هذه الورقة الإجابة عنها، وهي هل وفرت التشريعات العربية وعلى رأسها المشرع الجزائري الإمكانيات البشرية والمادية للبحث والتحري في الجرائم الإلكترونية ؟

وسنحاول الإجابة عن هذا الإشكال وفق المحورين التاليين :

المبحث الأول : دواعي إنشاء ضبطية خاصة بالجرائم الإلكترونية

المبحث الثاني : نماذج لأجهزة خاصة بالجرائم الإلكترونية "شرطة الأنترنيت "

المبحث الأول

دواعي إنشاء ضبطية خاصة بالجرائم الإلكترونية

تعتبر الجرائم الإلكترونية جرائم العصر الحديث ولا تقل مكانتها عن اكثر الجرائم خطورة، وذلك بالنظر للأضرار الفادحة التي يمكن أن يتسبب فيها هذا النوع من الإجرام، ومن هنا تعالت الأصوات المنادية بضرورة مكافحة الجريمة الإلكترونية، نظراً للخصائص التي تميزها عن بقية الجرائم العادية.

المطلب الأول: حداثة الجرائم الإلكترونية على أجهزة الضبطية القضائية

الفرع الأول: ضبطية قضائية غير جاهزة وغير مجهزة

إعتاد أعضاء الضبطية القضائية على البحث والتحقيق في الجرائم العادية والتي تقع في الواقع المادي، حيث يكون من السهل التنقل إلى مكان وقوع الجريمة والبحث عن الأدلة والاستدلال على مرتكبي الجرائم، والقبض عليهم والتحقيق معهم، وهي عملية تتطلب جاهزية ومهارة بدنية بشكل أساسي، حتي ظهرت الجرائم الإلكترونية وهي تختلف تماماً عن الجرائم التقليدية من حيث كيفية الوقوع والآثار المترتبة عنها والوسائل المستعملة لإرتكابها؛ فأحدثت طوارئ في أجهزة الضبط القضائي والتحقيق، وعندها تعالت الأصوات لإنشاء أجهزة خاصة للبحث والتحري في مثل هذه الجرائم والتي لا تعتمد على التدريبات المادية والفيزيولوجية وإنما تعتمد على مستوى عملي وفكري معين ومهارات خاصة في مجال الاتصال والانترنيت، حتي يستطيع المحقق التحري والاستدلال في العالم الافتراضي ومطاردة المجرمين في البيئة الالكترونية[1].

وهو ما أشارت إليه اتفاقية بودابيست للإجرام المعلوماتي والتي نادت بضرورة إنشاء مثل هذه الأجهزة على المستوى الوطني وسن الإجراءات التشريعية اللازمة لذلك حيث جاء في مادتها (١٤) على أنه "...يجب على كل طرف أن يتبنى من الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل إنشاء السلطات ووضع الإجراءات المنصوص عليها

في هذا القسم بغرض التقنيات أو الإجراءات الجنائية الخاصة[٢]، وقد سمحت الاتفاقية لكل طرف بأن يحتفظ بالحق في عدم تطبيق الإجراءات المشار إليها إلا على جرائم معينة فقط[٣].

هذا ولم ينص قانون الإجراءات الجزائية الجزائري على وجود جهات قضائية مختصة للتحقيق والفصل في الجرائم الإلكترونية، وبالتالي يعود الإختصاص للنظر في هذه القضايا إلى القضاء العادي في جانبه الجزائي، وهو ما يجعل الفصل في مثل هذه الجرائم من الصعوبة بما كان نظراً لنقص الدراية والخبرة العلمية والفنية لرجال القضاء في هذا المجال، ورغم أن القانون يجيز للقاضي الإستعانة بالخبرة لتحديد ملابسات القضية والوصول إلى الحقيقة، إلا أن خبرة القاضي وإحاطته بوقائع ومعطيات القضية هي التي تساهم في كشف الحقيقة.

الفرع الثاني: أعضاء ضبطية غير جاهزين في مواجهة مجرمين محترفين

يعود الإختصاص في البحث والتحري في الجرائم الإلكترونية إلى أعضاء الضبطية القضائية المذكرين في قانون الإجراءات الجزائية، مما يضعنا أمام معادلة غير متكافئة طرفها أجهزة البحث والتحري والتحقيق بنقص خبرتهم في مجال عالم الكمبيوتر والأنترنت والمعاملات الإلكترونية، والطرف الآخر قراصنة محتلون يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية والإتصال.

إستناداً إلى المثل القائل فاقد الشيء لا يعطيه فإنه من المستحيل على أعضاء الضبطية العادية البحث والتحري في الجرائم الإلكترونية والتعامل مع مرتكبيها، ومن هنا لا مناص من الدعوة إلى وجود أجهزة مختصة بهذا النوع من الإجرام، أو على العمل على تنمية خبرة ومهارات الأشخاص المخول لهم البحث والتحري فيها، وكذا وضع مناهج مدروسة للتدريب على التحقيق وإثبات هذه النوع من الجرائم، مراعين في ذلك خصوصية التطور التقني السريع في مجال الإتصال، دون إهمال التعاون الدولي في مثل هذه الحالات .

المطلب الثاني: جرائم معقدة ومسرح جريمة لا حدود له

الفرع الأول: الجرائم الإلكترونية متميزة عن الجرائم العادية :

من أهم العوامل الداعية لإنشاء جهاز مختص بالجرائم الإلكترونية وهو الطبيعة المميزة لهذه الجرائم، كونها جرائم تقع في بيئة إفتراضية ولا تترك آثار مادية مثلما هو الأمر في الجرائم العادية ومن بين الخصائص والمميزات أيضاً نجد :

أولاً: الجريمة الإلكترونية جريمة عبارة للحدود :

الجريمة الإلكترونية لا تعترف بالحدود الجغرافية فهي جريمة تخترق الزمان والمكان، حيث تتمتع الحواسيب وشبكات الأنترنيت بمقدرة هائلة في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة الإلكترونية الواحدة في آن واحد.

ثانياً: صعوبة اكتشاف الجريمة المعلوماتية :

عدم ترك هذا النوع من الجرائم لأي أثر خارجي بعد إرتكابها، يقف وراء الصعوبة في اكتشافها، بالإضافة أن قدرة الجاني على تدمير دليل الإدانة في ظرف وجيز يشكل عاملاً إضافياً في صعوبة اكتشاف هذا النوع من الجرائم[٤].

ثالثاً: صعوبة إثبات الجريمة الإلكترونية :

من الصعوبات العملية التي تواجه المحققين هو أن الجرائم الإلكترونية لا تترك آثار واضحة والخبير أو المختص فقط من يستطيع كشفها وتعقبها وإثباتها[٥]، والسبب في صعوبة إثبات هذه الجرائم هو أن المجرم يقوم بمحو آثارها والآثار الذي توصل إليهم.

الفرع الثاني: مسرح جريمة متلاشي :

مسرح الجريمة هو المكان الذي انتهت فيه أدوار النشاط الإجرامي ويبدأ منه نشاط المحقق الجنائي وأعوانه، بقصد البحث عن الجاني من واقع الآثار التي خلفها في مسرح الجريمة والتي تعد بمثابة الشاهد الصامت، الذي إذا أحسن المحقق الجنائي استنطاقه حصل على معلومات مؤكدة تساهم في شكل كبير في الكشف عن الحقيقة[٦].

إلا أن مسرح الجريمة الإلكترونية يختلف تماماً عن مسرح الجرائم التقليدية، فإذا كانت هذه الأخيرة تقع في واقع ملموس وحدود معينة فإن الجريمة الإلكترونية تقع في واقع إفتراضي لا حدود له، وهو الأمر الذي يخلق العديد من الإشكاليات الواقعية والقانونية للمحققين، فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها لحواسيب وشبكاتها في نقل المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى إمكانية وقوع الجريمة في أماكن متعددة وفي زمن واحد، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل الإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى(٧).

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية بإعتبارها جريمة عابرة للحدود خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه، بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام..، فكيف يمكن لأعضاء الضبطية غير المجهزين وغير الجاهزين متابعة المتهمين في هذا المسرح المتلاشي وقد يكونوا خارج النطاق الإقليمي الإفتراضي للدولة ؟.

إن مسألة الإختصاص القضائي عبر العالم الإفتراضي تعد من المشكلات التي واجهت الفقه الإجرائي، والتي كشفت عجز القواعد الإجرائية العامة، والسبب في ذلك أن فضاء الانترنيت لا يخضع لسلطة شخص أو دولة معينة وبالتالي تتعدد القوانين الإجرائية التي يمكن أن تحكم هذا النوع من الجرائم بتعدد الدول المرتبطة بها، والراجح فقها أنه لابد من التقيد بمبدأ إقليمية النص الجنائي، مع الأخذ بعين الإعتبار المبادئ الإحتياطية، بينما تؤكد إتفاقية بودابيست في مادتها (٢٢) على أنه يتعين على كل دولة طرف العقاب على إرتكاب هذه الجرائم حتى ولو كان المجرم خارج إقليم الدولة، فيعد الإختصاص منعقداً إذا كان نظام حاسوب المعتدي داخل إقليم الدولة وهو خارجها، أو كان نظام الحاسوب العائد للضحية

ضمن النطاق الإقليمي، أو كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة، كما أشارت الفقرة الرابعة من المادة السالفة الذكر أنه يجوز للأطراف إتخاذ أشكال أخرى من معايير الإختصاص بما يتناسب مع قانونها الداخلي[٨]، وإذا كانت الجريمة الواقعة في بيئة إلكترونية تدخل في إختصاص أكثر من دولة فإن هذه الدول تتشاور فيما بينها لتحديد المكان الملائم للمحاكمة حتى يتم تجنب إزدواج التخصص.

وقد لجأ القضاء الأمريكي لحل مشكلة الإختصاص بالإعتماد على مبدأ الإختصاص الشخصي والتي تجعل المحاكم الأمريكية تختص بنظر جرائم الإنترنيت وذلك في حالتين هما:

الحالة الأولى : عند وجود مرتكب الجريمة في إقليم الدولة.

الحالة الثانية : عندما يكون لمرتكب الجريمة حد أدنى من الإتصال داخل الدولة[٩].

المبحث الثاني

نماذج لأجهزة خاصة بالجرائم الإلكترونية "شرطة الإنترنت"

أمام تزايد الأجرام الإلكتروني من جهة وعجز أجهزة الضبطية القضائية عن التحقيق فيها وكشف مرتكبيها اتجهت العديد من التشريعات المقارنة نحو اعتماد أجهزة خاصة للبحث والتحري في الجرائم الإلكترونية.

نعم لقد أحدثت الجرائم الإلكترونية طوارئ في أجهزة القضاء وأجهزة الضبط القضائي والتحقيق، ولذلك تعالت الأصوات بضرورة إنشاء أجهزة خاصة بهذه الجرائم تختلف تماماً عن الضبط العادية[١٠]، وهو ما جعل اتفاقية بودابيست للإجرام المعلوماتي تنادى بضرورة إنشاء مثل هذه الأجهزة على المستوى الوطني[١١] وسن الإجراءات التشريعية اللازمة لذلك حيث جاء في مادتها (١٤) على أنه "...يجب على كل طرف أن يتبنى من الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل إنشاء السلطات ووضع الإجراءات

المنصوص عليها في هذا القسم بغرض التقنيات أو الإجراءات الجنائية الخاصة[١٢] ، وتسمح الاتفاقية لكل طرف بأن يحتفظ بالحق في عدم تطبيق الإجراءات المشار إليها إلا على فئة معينة من الجرائم[١٣].

المطلب الأول: نماذج لشرطة للأنترنيت في التشريعات المقارنة

الفرع الأول: في الولايات المتحدة الأمريكية :

من بين الدول السباقة في مجال إنشاء أجهزة خاصة للبحث والتحري في الجرائم الإلكترونية نجد الولايات المتحدة الأمريكية والتي أحدثت عدداً كبيراً من الوحدات المتخصصة، ومن بين هذه الوحدات نجد المكتب المركزي لمكافحة الجريمة المرتبطة بتكنولوجيا المعلومات والإتصالات، وكذا قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية الذي تم إنشاؤه سنة (١٩٩١)، وقد وصل عدد أعضائه إلى ٢٠ وكيل نيابي سنة (٢٠٠٠)[١٤]، وكذا نجد معهد امن الحواسيب، ووحدة جرائم الانترنيت وهي وحدة مختصة في الجرائم المرتبطة بالتقنية العالية ويترأسها مدير مساعد لمكتب التحقيقات الفدرالي[١٥].

ويوجد في ولاية أوهايو في الولايات المتحدة إحدى المنظمات الدولية التي تهدف إلى حماية المواقع الإلكترونية من عمليات الاختراق شرطة الإنترنت(***internet police***) ، حيث تعمل هذه المنظمة على حماية المواقع التي تتعاقد معها رسمياً، وذلك نظير مقابل مادى عن طريق الحيلولة دون محاولة اختراق أحد المواقع المحمية من قبلها، وإذا تم تكرار المحاولة أكثر من مرة من قبل نفس المجرم الإلكتروني "الهاكر" يتم تجميد الجزء المسؤول عن التواصل مع شبكة الأنترنيت بحيث يفشل نظام الحاسب في التواصل معها، ومن بين المواقع المحمية من قبل هذه المنظمة نجد بعض مواقع التجارة الإلكترونية من على الإنترنت، وموقع المباحث الفيدرالية، ومواقع وزارات الداخلية والدفاع.

الفرع الثاني: في فرنسا

قام المشرع الفرنسي بإنشاء المكتب المركزي لمكافحة الإجرام المتعلق بتكنولوجيا المعلومات والاتصال، وذلك بموجب المرسوم رقم (٤٠٥/٢٠٠٠)، ويتواجد على مستوى المديرية المركزية للشرطة القضائية[١٦]، كما تم إنشاء قسم الانترنيت تابع للمصلحة التقنية للبحوث القانونية والوثائقية سنة (١٩٩٨)، وهو قسم تابع للدرك الوطني ويتكون من (١٣) دركياً من بين مهندسين وتقنيين ويتولى هذا القسم مهمة معالجة المعلومات، والقيام بعمليات التفتيش الإلكتروني المعقدة، كما نجد أيضاً القسم المعلوماتي التابع لمعهد البحوث الجنائية في الدرك الوطني، الذي أنشأ سنة (١٩٩٢) وتتمثل مهمته في تقديم المساعدة التقنية على شكل خبرة أو اعتراض أو رقابة، وكذا تحليل البيانات المدمجة في الحواسب خاصة تلك المتعلقة بالمعاملات التجارية الإلكترونية والمالية[١٧].

ومن بين الأجهزة المختصة في فرنسا نجد أيضاً المكتب المركزي لمكافحة الإجرام المتعلق بتكنولوجيا المعلومات والاتصال، والذي أنشأ بموجب المرسوم رقم (٤٠٥/٢٠٠٠)، ويتواجد على مستوى المديرية المركزية للشرطة القضائية[١٨]، وهناك ثلاث وحدات يستعين بها المكتب لمباشرة مهامه، وهي وحدة العمليات وتتكون من أربعة فرق تختص بجرائم الاحتيال بواسطة وسائل الدفع وكذا الجرائم الواقعة على شبكات الاتصال، ووحدة المساعدات التقنية وهي وحدة مجهزة ببرامج ووسائل تكنولوجية متطورة، تعمل على تسهيل التدخلات القضائية في شبكة الانترنيت، في حين تعمل وحدة التحليل والتوثيق العلمي على معالجة المعلومات المتحصلة من النشاطات القضائية[١٩].

الفرع الثالث: ضرورة التعاون الدولي في مجال تكوين أجهزة مختصة بالجرائم الإلكترونية :

لأنه ما من دولة يمكنها النجاح في مواجهة الجرائم الإلكترونية من دون تعاون وتنسيق مع غيرها من الدول، فإن يكون من الضروري وجود تعاون دولي في مجال تكوين رجال العدالة[٢٠]، فتدريب الكوادر البشرية ليس بنفس المستوى في جميع الدول وإنما يختلف تبعاً لتقدم الدولة من عدمه، ولو أمعنا النظر في بعض التشريعات الدولية أو الإقليمية لوجدنا أنها

دعت وبصريح النص إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينها[٢١].

ويشترط أن تتوفر في المدرب الصلاحيات العلمية والقدرات الذهنية والنفسية حتى يأتي التكوين والتدريب ثماره، وتشترط بعض الجهات أن تتوفر في متلقي التكوين والتدريب خبرة كافية في مجالات عمليات الحاسب الآلي، والبرمجة وتصميم النظم وتحليلها وإدارة المشروعات، ومن بين أهم العناصر التي يجب أن يتلقاها المؤهل للتكوين هي معرفة كل ما يتعلق بالمخاطر والتهديدات التي يتعرض لها نظام الحاسب الآلي، وكذا أنواع الجرائم الناشئة عن إساءة استخدامه، ثم أهم إجراءات التحري والبحث والتخطيط، وكيفية تجميع المعلومات وتحليلها، وأساليب مواجهة الهجمات الإلكترونية وكيفية الرقابة عليها، ويضمن التدريب أيضاً التعرف على أدلة الإثبات في المجال الإلكتروني وكذا إجراءات التفتيش والضبط[٢٢].

هذا وتجتهد الجزائر في سبيل تطوير أجهزتها الضبطية والقضائية حيث أشرف خبراء من الاستخبارات المركزية الأمريكية وعملاء من مكتب التحقيقات الفدرالي، على ورشة تكوينية سنة (٢٠١٠)، وكانت حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة، وهي تهدف إلى إطلاعهم على آخر التكنولوجيات لمحاربة الجريمة وكيفية استخدام الأدلة الإلكترونية في التحقيق والمقاضاة، وقد شارك في الإشراف على الورشة التدريبية خبراء في الجرائم الحاسوبية والملكية الفكرية، وقسم الجريمة المنظمة وابتزاز الأموال التابعة لوزارة العدل الأمريكية، وقد استفاد من هذه الورشة التدريبية قرابة (١٠) ضباط من الشرطة القضائية و (٦٠) متخصصاً في الجريمة المنظمة في الجزائر، وقد انصب التدريب على الجانب النظري والتطبيقي معاً، كما تم التعرف على تقنيات إجراءات التحري وإقامة الدليل على الجرائم المعلوماتية، وعلاقة الجريمة المعلوماتية بالجريمة المنظمة وأمن المعلومات والمعطيات وكيفية استغلال الانترنت والبريد الالكتروني وكذا التعاون الدولي في هذا المجال[٢٣].

والحقيقة أنه لا يمكن لأي دولة مهما بلغت من التقدم والتطور أن تواجه هذه الأنماط المستحدثة من الجرائم لوحدها، ولذلك فلا مفر من تعزيز التعاون الدولي في الجانب الإجرائي، ثم لا مفر لهذه الدول من تقديم المساعدة للدول النامية لتعزيز مؤسساتها المتخصصة بالتحري والتحقيق .

المطلب الثاني: موقف المشرع الجزائري

الفرع الأول: موقف المشرع على المستوى الداخلي :

أولاً: رغبة المشرع في إنشاء جهاز خاص للجرائم الالكترونية :

أما عن موقف المشرع الجزائري فقد حاول على غير العادة تنظيم الجانب الإجرائي للجرائم الإلكترونية وذلك عن طريق إصداره للقانون رقم (٠٤/٠٩) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام[٢٤]، وقد نص القانون السالف الذكر على إنشاء هيئة وطنية للوقاية من جرائم تكنولوجيا الاعلام والإتصال، كما أنه أشار إلى مسألة تفتيش المنظومات المعلوماتية في المادة (٥) من القانون ولكنه جعل الجهة المختصة به هي الجهات المنصوص عليها في القواعد العامة.

وحسب المادة (١٠) من القانون رقم (٠٤/٠٩) السالف الذكر فإنه يمكن للمكلفين بالتحريات القضائية الإستعانة بمقدمي خدمات الانترنيت، وذلك بهدف جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها، ولا يتم ذلك إلا تحت تصرف ورقابة السلطات المختصة بالتحري والتحقيق، ويتعين على مقدمي الخدمات في هذه الحالة كتمان سرية العمليات التي ينجزونها وكذا المعلومات المتصلة بها وذلك طائلة قانون العقوبات[٢٥].

وإلى جانب مقدمي خدمات الأنترنيت أنشأ المشرع هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال كما ذكرنا، مهمتها مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها، بما في ذلك جمع المعلومات وإجراء الخبرة، كما

تعمل على تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بالإضافة إلى أن الهيئة تعمل على تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذه الجرائم، وقد أحال المشرع على التنظيم لبيان الهياكل البشرية والقاعدية لهذه الهيئة.

ثانياً: إنشاء هيئة لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام :

وتطبيقاً لذلك صدر المرسوم الرئاسي رقم (٢٦١/١٥) الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[٢٦].

١ – مهام الهيئة : من مهام الهيئة نذكر ما يلي:

– اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية .

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

– تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية .

–السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

– المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

وتتكون الهيئة من عدة أجهزة نذكرها باختصار:

٢– أجهزة الهيئة

– لجنة مديرة[٢٧] : هذه اللجنة تضطلع بالمهام التالية :

– توجيه عمل الهيئة والإشراف عليه ومراقبته.

– دراسة كل مسألة تخضع لمجال اختصاص الهيئة لاسيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية .

– ضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه.

– القيام دورياً بتقييم حالة الخطر في مجال الإرهاب والمساس بأمن الدولة، للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها.

– اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– دراسة مشروع النظام الداخلي للهيئة والموافقة عليه.

– دراسة مشروع ميزانية الهيئة والموافقة عليه.

– دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه.

– إبداء رأيها في كل مسألة تتصل بمهام الهيئة.

– تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة.

– مديرية عامة[٢٨]: تتولى المديرية العامة الصلاحيات الآتية :

– السهر على حسن سير الهيئة.

– السهر على تنفيذ برنامج عمل الهيئة.

– تنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها.

– تحضير اجتماعات اللجنة المديرة.

– تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية.

– تمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية[٢٩].

– مديرية للمراقبة الوقائية واليقظة الإلكترونية : وهي مكلفة بما يلي :

– تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول .

– إرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة.

– تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم.

– جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال[٣٠].

– مديرية للتنسيق التقني : وهي مكلف بما يلي:

– إنجاز الخبرات القضائية في مجال اختصاص الهيئة .

– تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها.

– إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– القيام بمبادرة منها أو بناء على طلب اللجنة المديرة بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها.

– تسيير منظومة الإعلام للهيئة وإدارتها.

ورغم هذا تبقى تحركات الدولة الجزائرية في هذا المجال بطيئة جداً لا تتماشى مع تزايد الجرائم الإلكترونية.

الفرع الثاني: موقف المشرع على المستوي الخارجي :

يتجسد موقف المشرع الجزائري من مسألة إنشاء جهاز لمكافحة الجريمة الإلكترونية في المصادقة على الاتفاقية العربية لمكافحة لجرائم تقنية المعلومات، بموجب المرسوم الرئاسي رقم (٢٥٢/١٤) المؤرخ في (٠٨ سبتمبر ٢٠١٤)[٣١] ، وبالرجوع إلى نصوص الاتفاقية نجد أنها تحث الدول الأطراف على إنشاء جهاز متخصص ومتفرغ لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الإلكتروني في جريمة معينة، وذلك في سبيل تنفيذ توفير المشورة الفنية، أو حفظ المعلومات[٣٢]، أو جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشتبه فيهم.

وقد أكدت الاتفاقية على ضرورة أن يكون لدى ذلك الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة[٣٣].

وتؤكد الاتفاقية على كل دولة طرف ضمان توفر العنصر البشري الكفء من أجل تسهيل عمل الجهاز.

هذا وقد تطرقت الاتفاقية إلى مسألة الإختصاص ونصت على أن أحكام الاتفاقية تطبق على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها وذلك في الحالات الآتية :

- ارتكبت في أكثر من دولة.
- ارتكبت في دولة والإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.
- ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.

– ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.

ولأن الإجراءات السالفة الذكر قد تمس بسيادة الدول فقد حثت الاتفاقية أن تلتزم كل دولة طرف وفقاً لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ إلتزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.

كما أشارت الاتفاقية إلى أنه ليس هناك ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي[٣٤].

الخاتمـــــة

مهما أعدت الدولة العدة وجهزت الوسائل والإمكانيات المادية والبشرية لمواجهة جريمة ما، فإن الحد من هذه الجريمة والقبض على مرتكبيها لن يتأتى إلا إذا كان هذا الاستعداد متناسباً مع طبيعة الجريمة، والجريمة الإلكترونية تختلف إختلافاً جذرياً عن الجرائم الأخرى، من حيث تكوينها وإرتكابها وآثارها ونطاقها وحتي مرتكبيها، لهذا فإنه من غير الممكن أن يبحث ويتحرى فيها إلا من كان ملماً بطبيعة هذه الجرائم ومتمكنا من تقنيات الإعلام والإتصال والمعلوماتية، ومن هنا ندعو المشرع إلى ما يلي :

- ضرورة تكوين قضاة متخصصين في جرائم تكنولوجيا الاعلام والاتصال.
- ضرورة تكوين أعضاء الضبطية العادية في مجال الإعلام والإتصال وتزيدهم بالوسائل اللازمة، لكشف الجرائم الإلكترونية كخطوة إستباقية إلى حين إنشاء جهاز خاص.
- إنشاء مراكز متخصصة لدارسة هذا النوع من الإجرام.
- ضرورة التعاون الدولي لمكافحة الجريمة الإلكترونية وتكوين أجهزة مختصة في البحث والتحري.
- ضرورة إستقطاب مرتكبي الجرائم الإلكترونية للعمل كمساعدين لأعضاء الضبطية.

الهـــوامـــش

(١) أنظر أكثر تفاصيل.. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر، ١٩٩٤، ص٤٥.

(٢) كما يتوجب على كل طرف أن يطبق السلطات والإجراءات المشار إليها في الفقرة ١ على الجرائم الجنائية المنصوص عليها وفقا للمادة ٢ إلى ١١ من الاتفاقية، وهي الجرائم الماسة بسرية وسلامة إتاحة البيانات والنظم المعلوماتية والجرائم المعلوماتية المتصلة بالحاسب الآلي، والجرائم الواقعة على الملكية الفكرية وكل الجرائم الجنائية المتركبة عن طريق نظام معلوماتي..، أنظر الفقرة الثانية من المادة المذكورة أعلاه.

(٣) ويشير التقرير التفسيري للنص المذكور أعلاه أن جميع الدول الأطراف في الاتفاقية يجب عليها النص في قانونها الداخلي على أن المعلومات سواء اتخذت شكلا إلكترونيا أو رقميا يمكن أن تستخدم كدليل أمام القضاء... ينظر، هلالي عبد الله احمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، ص ١٧٤.

(٤) ومن بين أسباب التي تحول دون اكتشاف هذا النوع من الإجرام هو إحجام المجني عليه عن التبليغ عنها..، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها..، أنظر أكثر تفاصيل نهلا عبد القادر المؤمني، الجرائم المعلوماتية، مقال منشور على الموقع التالي، ***http://kenanaonline.com/users/ahmedkordy/posts/409974***

(٥) أنظر، احمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم ٠٤/٠٩، مذكرة ماجستير كلية الحقوق جامعة ورقلة، ٢٠١٣، ص ١٢.

(٦) أنظر، عبد الفتاح مراد، التحقيق الفني الجنائي، الإسكندرية، مصر، ص ٧٠ .

(٧) أنظر، نهلا عبد القادر المؤمني، الموقع السابق.

(٨) أنظر، محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الإنترنيت، منشورات الحلبي الحقوقية، ط١، ٢٠١١، ص٢٠٠.

(٩) ويعتمد القضاء الأمريكي في تطبيقه لهذا المبدأ على عدة نظريات أنظر ذلك في محمد طارق عبد الرؤوف، المرجع السابق، ص ٢٠٧.

(١٠) يجب أو تتوفر لدى المدرب الصلاحيات العلمية والقدرات الذهنية والنفسية حتى يأتي التكوين والتدريب ثماره، وتشترط بعض الجهات أن تتوفر في متلقي التكوين والتدريب خبرة لا تقل عن ٥ سنوات في مجالات عمليات الحاسب الآلي، والبرمجة وتصميم النظم وتحليلها وإدارة المشروعات.

ومن بين أهم العناصر التي يجب أن يتلقاها المؤهل للتكوين كل ما يتعلق بالمخاطر والتهديدات التي يتعرض لها نظام الحاسب الآلي، وكذا أنواع الجرائم الناشئة عن إساءة استخدامه ثم أهم إجراءات التحري والبحث والتخطيط، وكيفية تجميع المعلومات وتحليلها، وأساليب مواجهة الهجمات الإلكترونية وكيفية الرقابة عليها، ويضمن التدريب أيضاً التعرف على أدلة الإثبات في المجال الإلكتروني وكذا إجراءات التفتيش والضبط..، أنظر أكثر تفاصيل.. هشام محمد فريد رستم، المرجع السابق، ص٤٥.

(١١) وقد نص على ذلك أيضاً توجيه المجلس الأوروبي رقم ١٣/٩٥ المؤرخة في ١٩٩٥/٠٩/١١ المتعلق بمشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، حيث دعت إلى إنشاء وحدات خاصة بمكافحة جرائم الحاسب الآلي وإعداد برامج خاصة لتأهيل تكنولوجيا المعلومات... أنظر، نبيلة هبة هروالة، الجوانب الإجرائي لجرائم الإنترنيت، دار الفكر الجامعي، ٢٠٠٧، ص ١٠٤.

(١٢) وأشارت الفقرة الثانية من المادة أنه يجب على كل طرف أن يطبق السلطات والإجراءات المشار إليها في الفقرة ١ على الجرائم الجنائية المنصوص عليها وفقا للمادة ٢ إلى ١١ من الاتفاقية، وهي الجرائم الماسة بسرية وسلامة إتاحة البيانات والنظم المعلوماتية والجرائم المعلوماتية المتصلة بالحاسب الآلي، والجرائم الواقعة على الملكية الفكرية وكل الجرائم الجنائية المتركبة عن طريق نظام معلوماتي.

(١٣) ويشير التقرير التفسيري للنص المذكور أعلاه أن جميع الدول الأطراف في الاتفاقية يجب عليها النص في قانونها الداخلي على أن المعلومات سواء اتخذت شكلا إلكترونيا أو رقميا يمكن أن تستخدم كدليل أمام القضاء... أنظر، هلالي عبد الله احمد، المرجع السابق، ص ١٧٤.

(١٤) وقد بدأ هذا القسم كوحدة تابعة لوزارة الدفاع ثم أصبح قسما قائم بذاته عندما كثرت أعماله... أنظر، نبيلة هبة هروالة، المرجع السابق، ص ١٠٨.

(١٥) كما يوجد مكتب رئيس التكنولوجيا وهو مكتب مفوض من طرف مدير التحقيقات الفدرالي لملاحقة مرتكبي الجرائم الواقعة في بيئة الأعمال الإلكترونية...، وقد تم إنشاء المركز الوطني لحماية البنية التحتية تابع للمباحث الفدرالية الامريكية سنة ١٩٩٨ بالمشاركة مع وزير الدفاع، ويتكون من فريق سري عدد أعضائه ١٣٥ عضو.. أنظر، نبيلة هبة هروالة، المرجع السابق، ص ١١٠.

كما قام مكتب التحقيقات الفدرالي بالاشتراك مع المركز الوطني لجرائم ذوي الياقات البيضاء بإنشاء مركزاً لتلقي الشكاوى من الاحتيال الإلكتروني وتلي ذلك إنشاء وكالة تابعة لمكتب التحقيق الفدرالي تهدف إلى التنسيق في مكافحة القرصنة المعلوماتية.

(١٦) ويستعين هذا المكتب بثلاث وحدات لمباشرة مهامه، تتكون الوحدة الأولى وهي وحدة العمليات من أربعة فرق تختص بجرائم الاحتيال بواسطة وسائل الدفع وكذا الجرائم الواقعة على شبكات الاتصال، أما الوحدة الثانية فهي وحدة المساعدات التقنية وهي وحدة مجهزة ببرامج ووسائل تكنولوجية متطورة، تعمل على تسهيل التدخلات القضائية في شبكة الانترنيت، في حين تعمل وحدة التحليل والتوثيق العلمي على معالجة المعلومات المتحصلة من النشاطات القضائية.

(١٧) ومن الدول تصدت لهذا النوع من الجرائم المستحدثة نج أيضاً هونكونج، حيث أنشأت قوة خاصة تدعى بقوة مكافحة قرصنة الانترنيت، وقد ساهمت هذه القوة في إيقاف عدد كبير من الأشخاص في مدة وجيزة من تأسيسها..، كما نجد أيضاً الصين حيث أنشأت جهة مختصة تدعى بالقوة المضادة للهاكرز سنة ٢٠٠٠... أنظر أكثر تفاصيل... نبيلة هبة هروالة، المرجع السابق، ص ١٣٩.

(١٨) ويسهر على مساعدة المكتب كل من وزارة الدفاع والإقتصاد والمالية والصناعة.

(١٩) نشير أن المكتب المركزي لمكافحة الإجرام المتعلق بتكنولوجيا المعلومات والاتصالات يتكون من ٣٢ شرطيا و٣ رجال من الدرك الوطني وهو في تزايد مستمر حسب الحاجة.

(٢٠) حيث تهدف هذه العملية إلى تغير سلوكهم ورفع مستوى مهارتهم واتجاهاتهم، بما يكفل حسن إنجاز العمل القانوني والقضائي والتنفيذي...، أنظر، حسين بن سعيد بن سيف، الجهود الدولية في مواجهة جرائم الإنترنت، مقال منشور على الموقع التالي ..***www.minshawi.com***

(٢١) أنظر مثلا المادة ٢٩ من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة لسنة ٢٠٠٠ م، والمادة ٩ من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود.

(٢٢) جدير بالذكر حيث يتواجد لدى الولايات المتحدة الأمريكية مكتب مساعدة وتدريب وأجهزة الإدعاء العام في الخارج، وهو تابع لوزارة العدل الأميركية، مكلف تحديداً بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى، وتعزيز إدارة القضاء في الخارج، كما تقدّم وزارة العدل الأميركية مساعدات لتطوير القطاع القضائي في عدد من البلدان في أفريقيا، وآسيا، وأوروبا الشرقية والوسطى وأميركا اللاتينية ومنطقة حوض الكاريبي، والدول المستقلة حديثاً، بما ذلك روسيا والشرق

الأوسط، مستعينة في ذلك بخبرة الوحدات المتخصصة التابعة لها.. أنظر، حسين بن سعيد بن سيف، المرجع السابق، على الموقع ***www.minshawi.com***

(٢٣) من جانب آخر، قال سفير الولايات المتحدة الأمريكية بالجزائر، دافيد بيرس خلال تلك المناسبة، أن واشنطن مهتمة بإرساء "شراكة أكثر فعالية بين الجزائر وبلاده في مجال مكافحة الجريمة المعلوماتية، حيث أنه من المفيد معرفة سلوك مقترف هذه الجريمة في الدول المختلفة".. أنظر عثمان لحياتي، ورشة حول الجريمة الإلكترونية وأمن المعلومات، مقال منشور على الموقع التالي ***http://www.elkhabar.com/ar/index.php?news=235287***

(٢٤) القانون رقم ٠٤/٠٩ الصادر سنة ٢٠٠٩ والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها المؤرخ في ٥ غشت ٢٠٠٩، جريدة رسمية عدد ٤٧.

(٢٥) أنظر المادة ١٠ من القانون رقم ٠٤/٠٩.

(٢٦) المرسوم الرئاسي رقم ٢٦١/١٥ المؤرخ في ٠٨ أكتوبر ٢٠١٦، جريدة رسمية عدد ٥٣.

(٢٧) وتتكون من :

– الوزير المكلف بالداخلية.

– الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال.

– قائد الدرك الوطني.

– المدير العام للأمن الوطني.

– ممثل عن رئاسة الجمهورية.

– ممثل عن وزارة الدفاع الوطني.

– قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

ويعيين ممثل رئاسة الجمهورية ووزارة الدفاع الوطني وجب مرسوم رئاسي

(٢٨) يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي وتنهى مهامه حسب الأشكال نفسها.

(٢٩) ومن بين المهام أيضاً :

– ممارسة السلطة السلّمية على مستخدمي الهيئة. –

–السهر على احترام قواعد حماية السر في الهيئة.

– السهر على القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين.

– إعداد التقرير السنوي لنشاطات الهيئة وعرضه على اللجنة المديرة للمصادقة عليه.

– ضمان التسيير الإداري والمالي للهيئة.

(٣٠) ومن المهام أيضاً :

–تنظيم و/أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها .

– تنفيذ توجيهات اللجنة المديرة.

–وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيرها وكذا الحفاظ على الحالة الجيدة لمنشآتها وتجهيزاتها ووسائلها التقنية.

– تطبيق قواعد الحفاظ على السر في نشاطاتها.

(٣١) المرسوم الرئاسي رقم ١٤/٢٥٢ جريدة رسمية عدد ٥٧.

(٣٢) ويتم حفظ المعلومات إستناداً إلى نص المادة ٣٧ و٣٨ من الاتفاقية.

(٣٣) وإذا لم يكن الجهاز المذكور المعين من قبل أي دولة طرف جزءا من سلطات تلك الدولة الطرف المسؤولة عن المساعدة الثنائية الدولية فيجب على ذلك الجهاز ضمان القدرة على التنسيق مع تلك السلطات بصورة عاجلة.

(٣٤) أنظر المادة ٣ و٤ من الاتفاقية العربية السالفة الذكر.

المصـــــادر

١-الاتفاقية العربية لمكافحة لجرائم تقنية المعلومات المصادق عليها بموجب المرسوم الرئاسي رقم ٢٥٢/١٤ المؤرخ في ٠٨ سبتمبر ٢٠١٤ على جريدة رسمية عدد ٥٧.

٢-إتفاقية بودابيست للإجرام المعلوماتي لسنة ٢٠٠١.

٣-القانون رقم ٠٤/٠٩ الصادر سنة ٢٠٠٩ والمتعلق بالوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والإتصال ومكافحتها المؤرخ في ٥ غشت ٢٠٠٩، جريدة رسمية عدد ٤٧.

٤- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر، ١٩٩٤.

٥-هلالي عبد الله احمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة.

٦-احمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم ٠٤/٠٩، مذكرة ماجستير كلية الحقوق جامعة ورقلة، ٢٠١٣.

٧-عبد الفتاح مراد، التحقيق الفني الجنائي، الإسكندرية، مصر.

٨-محمد طارق عبد الرؤوف، جريمة الاحتيال عبر الإنترنيت، منشورات الحلبي الحقوقية، ط١، ٢٠١١.

٩-نبيلة هبة هروالة، الجوانب الإجرائي لجرائم الإنترنيت، دار الفكر الجامعي، ٢٠٠٧.

١٠- حسين بن سعيد بن سيف، الجهود الدولية في مواجهة جرائم الإنترنت، مقال منشور على الموقع التالي *www.minshawi.com.*

١١- نهلا عبد القادر المؤمني، الجرائم المعلوماتية، مقال منشور على الموقع التالي، *http://kenanaonline.com/users/ahmedkordy/posts/409974*

١٢- عثمان لحياتي، ورشة حول الجريمة الإلكترونية وأمن المعلومات، مقال منشور على الموقع التالي *http://www.elkhabar.com/ar/index.php?news=235287*

The inevitable establishment of a special electronic crimes seizure

Dr. Bu Qurayn Abdul Halim
Department of Law - University of Laghouat - Algeria

Abstract

In many states, the specialization in investigation and in rule on the electronic crimes relates to the seizure device in charge of research and investigation. Besides, the ordinary jurisdiction in its criminal aspect. Making such kinds of crimes too difficult to be explored or to be proved. This is due to the lack of know-how scientific and technical experience for the judiciary men in this area. Though the law often permits the expertise support to determine the circumstances of the case and then to approach the truth. However, the investigator's experience as well as his briefed at the crime's given data are what we have to rely upon to achieve justice.

The difficulty of discovering such kind of crimes, primarily, and the inability of doing an investigation without resorting to experience, secondly, make us in front of un equitable equation. Its first party is the investigation devices lacking experience in the field of computers, the internet and e-transactions. Its second party is the hackers that are highly skilled and well coped with the recent information and communication in the world of technology. Therefore, there is a necessity to calling for the establishment of a seizure, a device or a special body to investigate and search this type of crimes. It does not have to be relied on physical strength or training but to be dependent on technical skills in the field of information and communication technology as a first stage to create a specialist jurisdiction ruling in these crimes.