الإثبات الجنائي في الجريمة المعلوماتية وفقاً للتشريع التونسي

د/ سلخ محمد لمين
جامعة الشهيد حمه لخضر الوادي (الجزائر)
selkh-mohammedlamine@univ-eloued.dz

ط.د/ هويدي سامية
جامعة سوسة (تونس)
houidisamia2018@gmail.com

ملخص:

صاحب التطور الإلكتروني المذهل الذي يشهده العالم والمتغيرات الحاصلة في مجال التكنولوجيا ظهور نمط جديد من الجرائم، يتعلق بالجريمة المعلوماتية.

تحتاج هذه الجريمة في كشفها ومعاقبة مرتكبيها إلى إثبات جنائي خاص وفق اجراءات قانونية تمكن من ملاحقة المجرمين وتسليط العقاب.

يعيق الاثبات الجنائي في الجرائم المعلوماتية بعض الصعوبات نظرا لطبيعة هذه الجريمة ومرتكبيها.

الكلمات المفتاحية: الإثبات الجنائي، الجريمة، المعلوماتية، التشريع التونسي.

مقدمة:

مما لا شك فيه أن إثبات أي جريمة يعتمد أساسا على الاجراءات الأولية والتحقيقات التي على ضوئها يمكن التوصل إلى اكتشاف ملابسات الجريمة مما يسهل على القضاء اثباتها ومن ثمة ادانة المتهم أو تبرئة ساحته.

إن طبيعة الجرائم المعلوماتية[1] تتطلب أساليب غير تقليدية لاكتشاف الدليل وإثبات الجرم فجمع الأدلة في مثل هذه الجرائم يتطلب وقفة من قبل المشرع والقضاء لاتخاذ مجموعة من الخطوات الإصلاحية لمواجهتها، على اعتبار أن عالم تقنية المعلومات واسع لا يحده حد وان الوسائل المستعملة في ارتكاب الجريمة المعلوماتية متشعبة ومتنوعة.

إنّ الجرائم المعلوماتية التي لم تُكتشف أكثر بكثير من تلك التي كُشف الستار عنها، لأنها عادة ما يتم اكتشافها عن طريق الصدفة، بل وبعد وقت طويل من ارتكابها، ولعلّ ذلك يرجع إلى صعوبة إجراءات التحقيق في هذا النوع من الجرائم وإلى عدة معطيات اخرى من ذلك اخفاء الجريمة وسهولة وسرعة محو أو تدمير أدلة ومعالم الجريمة والضخامة البالغة لكمية البيانات المراد فحصها على الشبكة، وتبرز الصعوبات كذلك في مسائل جمع الأدلة من المعاينة والتفتيش والضبط وغيرها من الإجراءات فضلاً عن الطابع العالمي الذي تمتاز به هذه الجرائم لكونها من الجرائم التي تتجاوز عنصري الزمان والمكان.

إنّ هذا النقاش يدفعنا لطرح الإشكالية التالية: **كيف يتم الإثبات الجنائي في الجرائم المعلوماتية؟**

إنّ الإجابة على هذا الإشكال تقتضي طرح التساؤلات الفرعية التالية:

- ✓ **الاجراءات المتبعة في الاثبات الجنائي للجرائم المعلوماتية؟**
- ✓ **ما هي صعوبات الاثبات الجنائي في الشكل الالكتروني؟**

ولتسليط الضوء على هذا الموضوع والإجابة على إشكالية الدراسة والتساؤلات المرتبطة نقترح تقسيم العمل إلى مبحثين نخصص الأول للإجراءات المتبعة في الاثبات الجنائي لهذا النوع من الجرائم ثم نتعرض في المبحث الثاني إلى صعوبات الاثبات الجنائي في هذا المجال، وحوصلة البحث لدراسة وتحليل هذه الإشكالية السالفة الذكر سنتوصل حتمًا إلى نتائج جوهرية سنقرنها باقتراحات ذات صلة سيتم إدراجها ضمن الخاتمة.

المبحث الأول:

إجراءات الاثبات الجنائي في الجريمة المعلوماتية

لا شك أن للإثبات أهمية بالغة في هذا المجال، على أساس أن الدليل هو عصب الواقعة أي أنه النتيجة التي حققتها وسائل الاثبات وهذا الاخير يقصد به تلك القواعد المتعلقة بالبحث عن الادلة وإقامتها أمام القضاء وبالتالي فالإثبات هو تلك الاسباب المنتجة لليقين والحقيقة[2].

ومن هذا المنطلق فالإثبات الجنائي في الجريمة المعلوماتية يتجسد في تلك الأدلة التي تؤكد وقوع السلوك الإجرامي، والتي من شأنها تحقيق حالة اليقين لدى القاضي ليتوصل إلى البراءة أو الإدانة في مواجهة المتهم، فالإثبات الجنائي في مجال مكافحة الجريمة المعلوماتية له عدة إجراءات تنطلق من مرحلة التحري وجمع الأدلة ثم التفتيش والخبرة في هذا المجال[3]، بالإضافة إلى الوسائل الإجرائية الحديثة كتقنية الاعتراض والاختراق حيث ينص مشروع القانون المتعلق بمكافحة جرائم أنظمة المعلومات والاتصالات على أن قاضي التحقيق يأذن بالاعتراض الفوري لمحتوى الاتصالات وتسجيلها أو نسخها[4]، ولا يمكن أن تتجاوز مدة الاعتراض[5] ثلاثة أشهر بداية من تاريخ الشروع الفعلي في إنجازه قابلة للتمديد مرة واحدة وبمقتضى قرار معلل من قاضي التحقيق المتعهد بالقضية[6]

المطلب الأول: التحري وجمع الادلة

من الصعب الإبلاغ عن الجرائم المعلوماتية في حينها لما تتطلبه من مهارات فنية لكشفها، إلا أنّ أي إخبار عن جريمة سواء كان فاعلها مجهولاً أم معلوماً ينبغي أن يتضمن على الأقل معلومات أولية عن الجريمة مثل تحديد محل الجريمة ومكان وقوعها ونوعها، وهي عناصر مهمة وضرورية لمساعدة رجال الضبطية القضائية في أي إخبار متعلق بجرائم تقنية المعلومات، بحيث تُمكنهم من تحديد معالم الجريمة ووضع خطة عمل لمواجهتها[7].

هذا وتتم الاستعانة في الكشف عن هذا النوع من الجرائم بوضع برمجيات حاسوبية معينة[8] كما يتم الحصول على المعلومات من موقع ارتكاب الجريمة بعد أن يتم اكتشافه باستخدام البرمجيات الحديثة، أو من خلال الحصول على المعلومات عن طريق رصد البيانات المنقولة من وإلى الموقع[9]، وفي إطار التحري عن هذه الجريمة لا بد من التحفظ على الأجهزة وملحقاتها و حوامل التخزين المعدة لتخزين المعلومات والمستندات الموجودة وغيرها من الأشياء التي يعتقد أن لها صلة بالجريمة و توضع المحجوزات في ظرف مختوم مع بيان تاريخ الحجز وعدد المحجوزات و رقم محضر الحجز[10] ثم تعرض على المشتبه فيه[11]، إضافة إلى إثبات الطريقة التي تم بواسطتها اعداد النظام والعمليات الالكترونية مع الحفاظ على البيانات من المحو والتبديل، خاصة وأن الأمر يتعلق مسرحين للجريمة، أحدهما تقليدي يقع خارج بيئة الحاسوب، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية

قد يترك فيها الجاني آثارا عدة، كالبصمات وغيرها وربما متعلقات شخصية أو وسائط تخزين رقمية، وثانيهما سيبراني يقع داخل بيئة الحاسوب أو الحاسب الآلي، ويتكون من البيانات الرقمية التي تتواجد وتنتقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الأقراص الصلبة الموجودة بداخله[12].

المطلب الثاني: التفتيـــــش

يعتبر التفتيش[13] إجراءً من إجراءات التحقيق ويُقصد به البحث عن جسم الجريمة والأداة المستعملة في ارتكابها وكل ماله علاقة بها أو بفاعلها، ويهدف عموما إلى الكشف عن الحقيقة والعثور على أشياء تساعد على إظهارها[14]، أما التفتيش في جرائم المعلوماتية فيقصد به الدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويه من مدخلات وتخزين ومخرجات من أجل البحث عن الأفعال والسلوكات المرتكبة غير المشروعة[15] والتفتيش في عالم تقنية المعلومات لا بد أن يكون محله الكيانات المادية والمعنوية أيضا فالأولى مثل البحث في المكونات المادية للحاسوب أو ما يتصل به من أجهزة ويمكن في هذه الصورة أن نطبق القواعد العامة للتفتيش.

أما التفتيش في الكيانات المعنوية وتتمثل في مجموع البرامج والأساليب المتعلقة بتشغيل وحدة معالجة البيانات، وتنقسم إلى كيانات أساسية تضم البرامج الضرورية التي تقوم بتشغيل واستخدام جهاز الحاسب الآلي وكيانات تطبيقية تضم برامج تمكّن المستخدم من أن يُنفِّذ بواسطته عملا معينا. والملاحظ أنه يمكن أن يكون حاسب المتهم متصلا بغيره من الحواسيب عبر الشبكة الإلكترونية، وهنا نفرق بين حالتين:

الحالة الأولى: حالة وجود جهاز متصل بجهاز المتهم داخل الدولة: يمكن تفتيش سجلات البيانات المتصلة في النهاية الطرفية للحاسوب في منزل المتهم مع جهاز أو نهاية طرفية في مكان آخر، حيث يمكن توسيع الحق في تفتيش المساكن إلى نظم المعلومات الموجودة في موقع آخر حينما يهدف إلى إظهار الحقيقة.
الحالة الثانية: حالة وجود جهاز متصل بجهاز المتهم خارج الدولة: حيث يقوم مرتكبي الجرائم الإلكترونية بتخزين بياناتهم في أنظمة معلوماتية خارج إقليم الدولة بهدف عرقلة جمع الأدلة.

ولحل هذا الإشكال يرى جانب من الفقه أن تفتيش أنظمة الحاسب الآلي العابر للحدود لابد أن يتم في إطار اتفاقيات تعاون ثنائية أو دولية.

المطلب الثالث: الاختبار أو الخبـــرة

يقوم المحقق الجنائي في مجال كشف الجريمة المعلوماتية وفاعلها باعتباره أول جهة تتصل بالجريمة بعد وقوعها باتخاذ بعض الإجراءات والوسائل والتي من ضمنها الاستعانة بأهل الخبرة وذلك تحقيقاً لمبدأ هام وهو مبدأ التخصص نظراً لكون الخبرة هي تقدير مادي أو ذهني يُبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق معرفتها وبمعلوماته الخاصة سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أو بجسم الجريمة أو المواد المستعملة في ارتكابها أو آثارها.

ونظراً للطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية كونها مرتبطة بمسائل فنية وعلمية بحتة أصبح من اللازم الاستعانة بالخبراء والمختصين[16] فإذا كانت الاستعانة بالخبراء في المسائل الفنية البحتة في الجرائم التقليدية أمر جوازي فالاستعانة بهم في مجال الجريمة المعلوماتية أكثر من ضرورة وذلك بسبب أن عملية استخلاص الأدلة الجنائية الرقمية تتطلب مهارة ودراية كبيرة في مجال الحاسب الآلي[17]، فينبغي إذا على الخبير

أن يكون ملما بالجوانب الفنية والتقنية و أن تكون لديه خبرة علمية وكفاءة فنية عالية في حقل أو أكثر من حقول تقنية المعلومات ونظمها ووسائلها لأن تصدي المحقق لفحص شيء وإبداء الرأي فيه دون أن تتوافر لديه المعرفة اللازمة يجعل قراره معيباً يضر بمصلحة التحقيق ويعوق الوصول إلى الحقيقة المطلوبة.

وتجدر الملاحظة أن التحقيق في جرائم المعلوماتية قد يتطلب الاستعانة ببعض خبراء مسرح الجريمة التقليدية مثل خبير البصمات، وخبير التصوير، الذين يعدون من الخبراء الأساسيين في معظم أنواع الجرائم، بالإضافة إلى غيرهم من الخبراء الذين قد يفرضهم ارتباط الجرائم المعلوماتية والانترنت محل التحقيق بجريمة أخرى من الجرائم التقليدية كجريمة القتل وغيرها[18].

المبحث الثاني

صعوبات الاثبات في الجريمة المعلوماتية

إن صعوبات الاثبات الجنائي في هذه الجرائم منها ما هو متصل بالجريمة في حد ذاتها ومنها ما هو متعلق بالجهات المتضررة من الجرم، هذا من جهة ومن جهة اخرى قد ترجع الصعوبة لأسباب متعلقة بجهات التحقيق[19] أو للواقع التشريعي الخاص بهذا النوع من الجرائم، وهي الصعوبات التي سنأتي على بيانها من خلال المطالب الآتية.

المطلب الأول: الصعوبات المتعلقة بالجريمة والمتضرر منها

إنّ الجريمة المعلوماتية في حد ذاتها لها بعض الخصوصية[20] التي تميزها عن باقي الجرائم التقليدية من حيث الوسائل التي ترتكب بواسطتها ومن حيث المحل الذي تقع عليه وخاصة من حيث الجناة بحيث يمكن القول أن الأساس في خطر هذه الجرائم يكمن في أنها في طبيعتها تجمع بين الذكاء الاصطناعي والذكاء البشري وهو ما يجعل إثباتها جنائيا يكون في منتهى الصعوبة[21]، نتيجة للأسباب التالية:

- سرعة ارتكابها حيث لا يحتاج الجاني إلا لبعض الثواني في بعض الجرائم.
- سرعة اخفاء آثار الجريمة وغياب الدليل المرئي الممكن فهمه بالقراءة بفضل مهارة مرتكبيها في استخدام التقنيات وبرامجها.
- صعوبة الوصول إلى الدليل المثبت للجريمة بسبب إحاطته من طرف الجناة بوسائل حماية تمنع الوصول إلى الحقيقة.
- سهولة محو الدليل أو تدميره في زمن وجيز يصعب معه كشف الجريمة.
- ضخامة حجم المعلومات والبيانات وإمكانية خروجها عن نطاق إقليم الدولة.
- عدم استخدام الجاني المعلوماتي جهازه الخاص بل يلجأ إلى مقاهي الانترنت التي لا تتقيد بأي ضوابط أو أنظمة أمنية وهو ما يمنع التعرف على مستخدم الجهاز ومصدره.
- اتساع مجالها إذ هي جرائم لا تعترف بالحدود الجغرافية وتتعدى حدود الدولة الواحدة.

وقد ترتبط هذه المعوقات بالمتضرر من الجريمة في حد ذاته من ذلك:

– عدم إدراك الضحية خطورة الجرائم المعلوماتية مع غياب التوعية لإرشاد المستخدمين إلى خطورتها لا سيما إذا تعلق الامر بالمؤسسات المختلفة.

– عدم الابلاغ عن الجرائم المعلوماتية في حينها لعدم اكتشافها أو بسبب عدم رغبة الجهات المتضررة في الظهور كضحية لهذه الجرائم خوفا من نعتها بالإهمال أو قلة الخبرة أو عدم أخذ الاحتياطات اللازمة لحماية معلوماتها.

– تعدد الضحايا المتضررين منها مرتكبيها في معظم الأحيان.

– عدم تركيز الشركات والمؤسسات على الجانب الامني في تقديم الخدمات المعلوماتية واهتمامها بتبسيط الاجراءات وتسهيل استخدام البرامج والخدمات الالكترونية[22].

المطلب الثاني: الصعوبات المتعلقة بجهات التحقيق

مما لا شك فيه أن للتحقيق الامني أو القضائي أهمية بالغة في إثبات الجريمة وكشفها باعتباره أول مرحلة تلي ارتكاب الجريمة جهة تتصل بالجريمة بعد وقوعها، على أن هناك تشابه كبيرا بين التحقيق في جرائم الحاسوب والانترنت وبين التحقيق في الجرائم التقليدية، فهي تمر بنفس المراحل والإجراءات تقريبا، وتهدف للوصول إلى مرتكبيها، إلا أن التحقيق في الجرائم المعلوماتية يتميز عن التحقيق في الجرائم التقليدية بشكل رئيسي بالعدد الكبير من السجلات التي يجب الاطلاع عليها، إضافة إلى أن التحقيق في الكثير من مراحله سيجرى في بيئة رقمية وببعض الخصوصية في عناصر التحقيق الفرعي والإجراءات الشكلية المتبعة كتلقي البلاغات والعناية بمسرح الجريمة وتكوين فرق عمل المحققين، وأساليب تأمين الأدلة المادية[23] هذا ما يترتب عليه صعوبات بالغة ومعوقات كثيرة تتعلق بجهات التحقيق نوجزها فيما يلي:

– عدم مهارة المحقق في استخدام جهاز الكمبيوتر وعدم تمكنه من استعمال تقنيات الاتصالات الحديثة بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الالكترونية.

– عدم توفر الاجهزة والبرامج المناسبة للتحقيق وعدم التنسيق بين المحققين في هيئات التحقيق والعاملين في مجال المعلومات والأنظمة الالكترونية والحاسوب.

– عدم التخصص في مجال التحقيق لإثبات الجرائم المعلوماتية ومواكبة التقنيات العالمية الحديثة.

المطلب الثالث: الصعوبات المتعلقة بالواقع التشريعي

مما لا شك فيه أن عالم تقنية المعلومات عالم متطور ومتسارع بشكل مذهل، نظرا للابتكارات الجديدة في هذا المجال لذلك يجب توافر اطلاع دائم وكاف على هذا العالم اللامتناهي، كي تتمكن الجهات التشريعية بكشف كل مستجد في مجال تقنية المعلومات حتى تعمل بدورها على سد الثغرات في مجال التشريعات الالكترونية، ومع كل ذلك تظهر عدة مسائل على الصعيدين الوطني والدولي تعيق الاثبات في مجال الجرائم المعلوماتية.

إنّ مسألة الواقع التشريعي يمكن أن نعالجها من خلال قانون العقوبات بمفهومه الواسع وكذا قانون الاجراءات الجزائية، فالأول يتصدى للظواهر الاجرامية فيُحددها ويضع العقوبات الرادعة لكل منها، أما الثاني

فيحدد القواعد الاجرائية والضمانات التي ينبغي أن تحترمها الجهات المعنية وصولا إلى محاكمة عادلة، وتبرز إشكالية التشريع في مدى نجاعة وكفاية النصوص التقليدية لوضع حد لهذه الظواهر المتجددة والمتنامية التي حتمت على المشرع ضرورة تعديل هذه النصوص أو إضافة نصوص جديدة لتشمل كافة الجرائم المعلوماتية بإضافة البعد الخاص بالحاسب الآلي أو استحداث أقسام جديدة للجرائم الالكترونية على غرار الأقسام التقليدية.

كما أن الطبيعة الخاصة للجريمة المعلوماتية تطرح عدة إشكالات تتعلق بالاختصاص الإقليمي[24] على أساس أن هذه الجريمة قد تقع في مكان ما في العالم وتُنتج آثارها في أماكن أخرى خارج اقليم الدولة وهو ما يدعو إلى التعاون الدولي بهذا الخصوص، غير أن الصعوبة تُطرح حول اختلاف منظور الدول للجريمة و تباين الرؤى وفلسفة النظم القانونية وتفاوت دول العالم في هذا المجال وصعوبة توحيد الجهود لمكافحة الجرائم المعلوماتية، ولعل من أبرز المنظمات الدولية التي عملت في هذا الشأن **الاتحاد الدولي للاتصالات التابع للأمم المتحدة**.

وعلى هذا الأساس ينبغي الإسراع في المصادقة على مشروع القانون المتعلق بمكافحة جرائم أنظمة المعلومات والاتصالات[25] و إصداره أسوة ببعض الدول[26] مع تثمين خطوة استهلال المشروع بالتعريف ببعض المصطلحات التقنية المتعلقة بالجرائم المعلوماتية والتي لها دور كبير في تحديد السلوك الإجرامي و بالنتيجة تكوين أركان الجريمة نظرا لصعوبة هذه المصطلحات واستحالة ضبطها سواء من طرف القانونيين أو غيرهم، ولكنها غير كافية، مع ضرورة تشجيع التعاون و التنسيق الدوليين لمواجهة هذا الخطر المحدق باعتبارها من الجرائم العابرة للحدود الوطنية.

الخـاتمة:

إنّ الجريمة المعلوماتية تطال الحقوق وتمس حرمة الحياة الخاصة للأفراد وتُهدد الأمن الوطني وتُؤدي إلى فقدان الثقة بالتقنية وغيرها من مفاصل الحياة العامة المختلفة.

من بين الاشكالات المتعلقة بهذه الجريمة مسألة الاثبات الجنائي للجريمة في حد ذاتها ومعرفة زمانها ومكانها ومرتكبها.

اهتمت جل التشريعات بهذه المسألة لما لها من أهمية خاصة في مواجهة ومكافحة هذا النوع من الجرائم، فرتبت عدة إجراءات قانونية وطرق حديثة ومواكبة للجريمة كل ذلك بهدف إقامة الدليل الجنائي على ارتكابها ومن ثم الكشف على الجناة، وذلك أمام تأكد قصور الوسائل التقليدية في الإثبات وعدم نجاعتها.

لا شك أن هناك عدة صعوبات ومعوقات تعترض سبيل المحققين قصد كشف معالم الجريمة وتشخيص الجناة وبسط الرقابة وصولا لمحاكمة عادلة، من بين هذه المعوقات ما يتصل بالجريمة في حد ذاتها من حيث الطبيعة والأشخاص ومنها ما يتعلق بنوع التحقيقات التي تتطلبها هذه الجرائم المتطورة ومنها ما يتعلق بالنص العقابي الذي يجعل المشرع متأهبا لمواكبة هذه الجرائم المتنامية والتي لم يرد النص على تجريمها في النصوص التقليدية.

وينطوي نظام الإثبات في جرائم المعلوماتية في التشريع التونسي على عديد النقائص أيضا يتمثل أساسا في تقييد سلطات البحث من جهة، إضافة إلى غياب التنصيص على حجية الأدلة الرقمية في المادة الجزائية من جهة أخرى

وهذا ما يؤكد أن النظام العقابي للجريمة المعلوماتية في التشريع التونسي يحتاج إلى تطوير مستمر لمواكبة مكافحة هذا النوع من الجرائم التي تتميز بالحداثة والتنامي

أما الاقتراحات التي يمكن لنا إثارتها حول هذا الموضوع فارتأينا طرح ما يلي:

✓ تكثيف التكوين لرجال الأمن والقضاء لا سيما في المجال الالكتروني وفقا للمعايير الحديثة حتى نكون أمام جهات أمنية وقضائية تمتاز بالمهارة والدقة، كل ذلك قصد السيطرة على هذه الجرائم المتطورة وكشف مرتكبيها.

✓ تطوير التشريعات العقابية لمكافحة هذا النوع من الجرائم حتى تكون النصوص الجزائية قابلة للتطبيق محلياً وعالمياً على الجرائم المعلوماتية ومرتكبيها.

✓ نشر الوعي العام المساند للتحول الإلكتروني من جهة والتنبيه من وعن المخاطر التي يسببها للجمهور وضرورة التبليغ عن هذه المخاطر عند حدوثها حتى تسهل السيطرة عليها.

✓ إنشاء هيئات متخصصة في التحقيق والإثبات الجنائي في مجال الجرائم المعلوماتية.

✓ الاستفادة من التجارب الأجنبية والعربية في مجال مكافحة الجريمة المعلوماتية، دراسة وتبادلاً للمعلومات والخبرات مع تحقيق التواصل بين الدول العربية في هذا المجال.

الهوامش:

(1) يطلق عليها أيضا مصطلح "الجرائم الإلكترونية"، "الجرائم السبرانية"، "جرائم الفضاء الإلكتروني"،"الجرائم المستحدثة".

(2) ثنيان ناصر آل ثنيان، اثبات الجريمة الالكترونية، رسالة ماجستير، تخصص السياسة الجنائية، كلية الدراسات العامة، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الامنية، الرياض السعودية، 2012.

(3) نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، مداخلة في اعمال المؤتمر الدولي الرابع عشر المتعلق بالجرائم الإلكترونية، يومي 24 و25 مارس 2017، طرابلس ليبيا.

(4) الفصل 13 من مشروع القانون المتعلق بمكافحة جرائم أنظمة المعلومات والاتصالات.

(5) حماية للخصوصية وحتى لا يتم التوسع في الاجراءات الاستثنائية فقد نص الفصل 34 من مشروع القانون المتعلق بمكافحة جرائم أنظمة المعلومات والاتصالات على إحداث هيئة عمومية مستقلة تتمتع بالشخصية المعنوية والاستقلال الإداري والمالي تسمى " الهيئة التونسية لمراقبة الاعتراض "تكلف بمراقبة احترام إجراءات تنفيذ عمليات النفاذ إلى قواعد البيانات والاعتراض على حركة الاتصالات ومحتواها .

(6) الفصل 14 من مشروع القانون المتعلق بمكافحة جرائم أنظمة المعلومات والاتصالات.

(7) محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنيت، رسالة ماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية جامعة نايف العربية للعلوم الأمنية، الرياض السعودية، 2004.

(8) منها برامج تُنصَّب على أجهزة الحاسوب قبل وقوع الجريمة وتهدف إلى حماية الشبكات من الاعتداءات المختلفة وما يميزها حفظ الأنشطة والعمليات التي تتم على الحاسوب في سجلات هذه الأخيرة تحوي الكثير من المعلومات التي قد تساعد المحققين في الوصول إلى الجاني. ومن أمثلتها: الجدار الناري، الخادم الوكيل، نظام كشف الاختراق، نظام جرة العسل، أدوات تدقيق ومراجعة العمليات الحاسوبية، بالإضافة إلى أن هناك برامج خاصة بالحقيق الجنائي وتتنوع بحسب متطلبات وطبيعة كل قضية منها: برمجيات النسخ الاحتياطي الجنائي، برامج البحث عن المفردات النصية، برامج استعادة البرامج المحذوفة، برامج

تحرير الملفات الست عشرية، برامج كسر كلمات السر في بعض الملفات، برامج تتبع الاتصال الشبكي، برامج استعراض الصور، وغيرها من البرامج.

(9) أقر المشرع التونسي في الفصل 32 من قانون منع الاتجار بالأشخاص وسائل إثبات خاصة تتمثل في اعتراض اتصالات ذي الشبهة والاختراق، ويشمل **الاعتراض** الحصول على بيانات المرور والتنصت أو الاطلاع على محتوى الاتصالات وكذلك نسخها أو تسجيلها باستعمال الوسائل الفنية المناسبة. كما نص الفصل 35 من نفس القانون " في الحالات التي تقتضيها ضرورة البحث يمكن اللجوء إلى الاختراق بواسطة عون أمن متخفي أو مُخبِر معتمد من قبل مأموري الضابطة العدلية"، كما نص القانون الاساسي عدد: 26 لسنة 2015، المتعلق بمكافحة الإرهاب ومنع غسل الأموال، إلى تقنية الاعتراض في الفصل 54 وتقنية الاختراق في الفصل 57.

(10) الفصل 97 من مجلة الإجراءات الجزائية.

(11) الفصل 76 من مجلة الإجراءات الجزائية.

(12) تركي بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض السعودية، 1433 هـ-2012م، ص165-166.

(13) نظرا لأهمية هذه الوسيلة في الإثبات فقد خصصت اتفاقية المجلس الأوروبي المتعلقة بالإجرام السيبيري العنوان الرابع للتفتيش وحجز البيانات المعلوماتية المخزنة، وأوصت الدول الأطراف بإرساء التدابير والإجراءات القانونية التي تخول للسلطات المختصة، التفتيش أو النفاذ إلى الأنظمة المعلوماتية وحوامل التخزين وكذلك إلى البيانات التي تحتوي عليها ونسخها.

(14) الفصل 93 مجلة الإجراءات الجزائية.

(15) جابر غنيمي، اثبات الجرائم الإلكترونية، مقال منشور على الموقع التالي:

https://m.facebook.com/permalink.php?id=106334717726289&story_fbid=188576589502101 تاريخ الاطلاع: 20-نوفمبر 2021، على الساعة: 18:53.

(16) نظرا لأن التحقيق في جرائم المعلوماتية يتطلب مهارات فنية وتقنية عالية وخاصة لا تتوفر بالتأكيد عند رجال الضبطية القضائية بسبب طبيعة تكوينهم التقليدية في أغلب الأحيان فإن تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أصبح أمرا ضروريا مادام أسلوب عمل الفريق أمر معمول به في جرائم أخرى. لأكثر معلومات حول تكوين فريق التحقيق أنظر: تركي بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، ص162 وما بعدها.

(17) جابر غنيمي، المرجع السابق.

(18) تركي بن عبد الرحمان المويشير، المرجع السابق، ص161-162.

(19) بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة ماستر، تخصص القانون الجنائي، كلية الحقوق، جامعة محمد خيضر، بسكرة الجزائر، 2015/ 2016.

(20) تتميز أيضا الجرائم المعلوماتية في التشريع التونسي عن الجرائم التقليدية في الجهات المختصة في تحريك الدعوى العمومية بشأنها فقد نص الفصل80 من مجلة الاتصالات على أن الوزير المكلف بتكنولوجيا الاتصال يحيل المحاضر إلى وكيل الجمهورية المختص ترابيا(إقليما) وبالتالي تكون الوزارة هي الطرف الأصلي في تحريك الدعوى و النيابة طرف منضم وتتمتع الوزارة المعنية بنفس سلطة الملاءمة التي تمتلكها النيابة، كذلك الهيئة الوطنية لحماية المعطيات طبقا للفصل 77 من القانون عدد: 64 لسنة 2004، كذلك منظمات الدفاع عن حقوق الإنسان في خصوص الجرائم المرتكبة بواسطة الصحافة الواردة بمرسوم عدد: 115لسنة 2011 المتعلق بحرية الصحافة والطباعة والنشر وفقا للفصل 69 منه.

(21) الجرائم الالكترونية الواقعة على الأشخاص في القانون التونسي، مساهمة الوفد التونسي ضمن المؤتمر التاسع لرؤساء المحاكم العليا، بيروت 17-19 ديسمبر 2018، ص-21-20.

(22) جدي نسيمة، جرائم المساس بأنظمة المعالجة الالية للمعطيات، رسالة ماجستير، تخصص القانون الجنائي، كلية الحقوق، جامعة وهران، 2013/2014.

[23] تركي بن عبد الرحمان المويشير، المرجع السابق، ص146.

[24] وضعت الاتفاقية الدولية المتعلقة بالجريمة السيبرية الصادرة في 23 نوفمبر2001 مجموعة مبادئ حددت بموجبها الاختصاص بالنسبة إلى الجرائم المتعلقة بالأنظمة المعلوماتية والمحتوى المعلوماتي. فقد حدَّدت مبدأ الاختصاص الترابي كقاعدة عامة بحيث يؤول الاختصاص إلى مكان ارتكاب الجريمة، فتختص مثلا البلاد التونسية بالنظر في هذه القضايا إذا كان الفاعل والنظام المعلوماتي يوجدان على التراب التونسي أو إذا وجد أحدهما فقط، كما يلحق بالاختصاص الجرائم المرتكبة بالسفن أو الطائرات الحاملة لعلم البلاد التونسية. كما اعتمدت على ضابط الجنسية لتحديد الاختصاص وذلك في حالة ارتكاب الجريمة ببلاد أجنبية أو خرجت عن اختصاص أية دولة في العالم فإن الاختصاص يعود إلى الدولة التي ينتمي إليها المتهم، وأبقت الاتفاقية على حرية تحديد الاختصاص إلى القوانين الوطنية للدول الأطراف فيها. وقد يؤول الاختصاص لعدة دول بسبب تورط عدة أطراف في ارتكاب نفس الجريمة، كأن يلحق الضرر بعدة أنظمة معلوماتية في عدد من الدول في وقت واحد وبسبب نفس الجريمة نصت الاتفاقية إلى ضرورة التشاور بين الدول المتعاقدة لتحديد الجهة المختصة، وقد يفضي التشاور إلى إسناد الاختصاص إلى دولة معينة، كما قد ينتهي إلى توزيع الاختصاص بين عدة دول وفي نقاط معينة غير أن مسألة التشاور غير ملزمة.

[25] جاء في شرح الأسباب لهذه المبادرة أن المجلة الجزائية أصبحت غير ملائمة في بعض فصولها للتطور التكنولوجي مع ضرورة المحافظة على حرية الصحافة والتعبير باعتبارهما مكسب من المكاسب التي لا يمكن المساس بها.

إن استفحال ظاهرة الإجرام السيبيري في ظل النسق السريع لتطور وسائل الاتصال الحديثة يؤدي حتما إلى التفكير في ضرورة تنقيح المجلة الجزائية لمواكبة تفشي هذه الجرائم فإن النصوص الجزائية الواردة بالقوانين الخاصة غير كافية لزجر وتجريم كافة الأفعال المحتملة باعتبار أن الانترنت ساهمت في ظهور جرائم مستحدثة يصعب حصرها وتحديد نطاقها.

وحيث وعلاوة عن ذلك فان البعد الإجرائي للجرائم المعلوماتية على اختلاف وسائلها ينطوي على مشكلات وتحديات جمّة، عناوينها الرئيسية الحاجة إلى سرعة الكشف عن الجريمة خشية ضياع الدليل وخصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم وقانونيّة وحجيّة أدلة هذه الجرائم ومشكلات الاختصاص القضائي والقانون الواجب التطبيق والحاجة إلى تعاون دولي شامل في حالة امتداد إجراءات التحقيق والتتبع خارج الحدود.

لقد أضحت الحاجة إلى تنظيم تشريعي لإجراءات وقواعد الإثبات في حقل الجرائم الالكترونية تجد موجبها في الحاجة إلى توفير معيار مقبول يقيم التوازن بين حقوق وحريات الأفراد وحماية خصوصياتهم من جهة، وبين موجبات المكافحة والتصدي لهذه الجرائم وحاجتها إلى قواعد خاصة فرضتها تحديات هذه الجرائم من جهة أخرى.

[26] تعد السويد من أوائل الدول التي سنت تشريعات قانونية جديدة خاصة بجرائم الانترنت والحاسب الآلي سمّي بـ"قانون البيانات" سنة 1973.