الآليات القانونية لمكافحة الجريمة المعلوماتية

د. فاروق خلف

أستاذ محاضر " أ "

كلية الحقوق جامعة حمة لخضر – الوادي

ملخص

لقد أدت التغيرات التي أحدثها التحول إلى الرقمية وربط شبكات الكمبيوتر ببعضها واستمرار عولمتها، وكذا التطور الكبير والمتسارع لدور الكمبيوتر وتزايد الوعي لدى الشعوب لأهمية المعلومة باعتبارها مصدرا للقوة والثروة، ومما يدعم هاته الفكرة هو تعميم استخدام الكمبيوتر والإنترنت على سكان الكرة الأرضية، وانشغالا بمخاطر احتمال استخدام الحاسوب وشبكة المعلومات في ارتكاب جرائم جنائية، وهي جرائم حديثة، تقف حاجزا أمام تطور المجتمع على كامل الأصعدة، الأمر الذي أدى إلى تحرك العديد من المنظمات الدولية والإقليمية لإبرام اتفاقيات في خطورة تهدف إلى مكافحة الجريمة المعلوماتية، ولعل أهمها اتفاقية بودابست المنعقدة في 2001/11/23 تحت إشراف المجلس الأوروبي.

إن موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية أصبح هاجسا يؤرق رجال القانون بصفة خاصة، لذلك بات من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في التقينات الرقمية ورجال القانون والمؤسسات الرسمية في الدولة، وعلى المستوى الدولي أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم. كما تبرز أهمية هاته الدراسة من الناحية النظرية في معرفة مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية وردع مرتكبيها ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة.

مقدمة:

لقد أدت التغيرات التي أحدثها التحول إلى الرقمية وربط شبكات الكمبيوتر ببعضها واستمرار عولمتها، وكذا التطور الكبير والمتسارع لدور الكمبيوتر وتزايد الوعي لدى الشعوب لأهمية المعلومة باعتبارها مصدرا للقوة والثروة، ومما يدعم هاته الفكرة هو تعميم استخدام الكمبيوتر والإنترنت على سكان الكرة الأرضية، وانشغالا بمخاطر احتمال استخدام الحاسوب وشبكة المعلومات في ارتكاب جرائم جنائية، وهي جرائم حديثة، تقف حاجزا أمام تطور المجتمع على كامل الأصعدة، الأمر الذي أدى إلى تحرك العديد من المنظمات الدولية والإقليمية لإبرام اتفاقيات في خطورة تهدف إلى مكافحة الجريمة المعلوماتية، ولعل أهمها اتفاقية بودابست المنعقدة في 2001/11/23 تحت إشراف المجلس الأوروبي.

إن موضوع الآليات القانونية لمكافحة الجريمة المعلوماتية أصبح هاجسا يؤرق رجال القانون بصفة خاصة، لذلك بات من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في التقينات الرقمية ورجال القانون والمؤسسات الرسمية في الدولة، وعلى المستوى الدولي أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم. كما تبرز أهمية هاته الدراسة من الناحية النظرية في معرفة مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية وردع مرتكبيها ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة.

فما هي الآليات القانونية لمكافحة الجرائم المعلوماتية أو الحد منها؟ وما مدى كفايتها وفعاليتها؟

المبحث الأول:
إجراءات التحقيق في الجريمة المعلوماتية

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها من أجل استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه[1]، وهناك تشابه بين التحقيق في الجرائم المعلوماتية وبين التحقيق في الجرائم التقليدية، فهي جميعا تحتاج إلى إجراءات تشابه في عمومها مثل المعاينة والتفتيش والخبرة والاستجواب والشهود وجمع وتحليل الأدلة، إلا أن التحقيق في الجرائم المعلوماتية له خصوصية خاصة؛ لأنه يتم في بيئة رقمية.

المطلب الأول:
جمع الأدلة: (المعاينة والتفتيش وضبط الأدلة)

جمع الأدلة في الجرائم المعلوماتية يستخلص من البيئة الرقمية، والتي تعتبر مسرحا للجريمة، وبما أن الدليل يقوي على إثبات الجريمة، يستلزم أن يكون من ذات طبيعتها التقنية، وتحيط بعملية جمع الأدلة العديد من الصعاب، إلا أنه لا مناص من مواصلة جمع الأدلة مع التطوير المستمر لوسائل البحث، وتكييف جمع الأدلة مع طبيعة الجرائم المعلوماتية.

الفرع الأول: المعاينة

وهي ملاحظة وفحص حسي مباشر لأي شيء له علاقة بالجريمة لإثبات حالته، والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة. وتكمن أهمية المعاينة في دورها لتصور كيفية وقوع الجريمة وظروف ملابساتها، وتوفير الأدلة والمعاينة في مسرح الجريمة تتيح أمام المحقق الكشف عن طريق معاينة الآثار المادية التي خلفها ارتكاب

الجريمة، والتحفظ على الأشياء التي تفيد التحقيق، لكن بالنسبة للجرائم المعلوماتية قلما تخلف آثار مادية، لذلك وجب مراعاة قواعد وإرشادات فنية خاصة مثل: تصوير الحاسوب وملحقاته، إثبات التوصيلات، عدم نقل مادة المعلوماتية من مسرح الجريمة.

الفرع الثاني: التفتيش[2]

هو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في محل يتمتع بحرمة، وذلك وفقا للضمانات والقيود المقررة قانونا، ويعد تفتيش نظم المعالجة الآلية من أخطر المراحل؛ لأنه يكون على طابع غير مادي، ولا يعدو إلا أن يكون معلومات إلكترونية ليس لها مظهر محسوس خارجيا، والتفتيش ينصب على الجانب المادي والمنطقي للحاسوب معا.

1 – تفتش المكونات المادية للحاسوب: إن التفتيش الواقع على المكونات المادية للحاسوب لا توجد فيه مشكلة في التنفيذ؛ لأنه يرد على أشياء مادية، لا خلاف فيها لقواعد القانون؛ لأنه تطبق عليه القواعد التقليدية، لكن مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها، ونظام التفتيش تنطبق عليه الضمانات المقررة قانونا.

2 – تفتيش المكونات المنطقية للحاسوب: لقد اختلف الفقه الجنائي في مسألة مدى قابلية البيانات المعلوماتية؛ لأن تكون موضوعا للتفتيش من عدمه طبقا للنصوص التقليدية، وهو ما حذا بالمشرعين سن قوانين إجرائية جديدة تنص على إمكانية تفتيش المكونات المنطقية للحاسوب، وهذا ما ذهب إليه المشرع الفرنسي في تعديله للنصوص التي تحكم التفتيش، وكما نص المشرع الإنجليزي على جواز تفتيش نظم الحاسوب المادية والمعنوية، وقد صرحت الاتفاقية الأوروبية المتعلقة بجرائم تقنية المعلومات أنه يحق للدول الأعضاء تفتيش نظام الحاسوب أو جزء منه أو المعلومات المخزنة فيه ووسائط التخزين، والتفتيش في البيئة الرقمية يخضع لشروط شكلية وأخرى موضوعية تختلف عن شروط التفتيش في البيئة التقليدية.[3]

الفرع الثالث: ضبط الأدلة

وهو وضع اليد على الشيء يتصل بالجريمة ويفيد في كشف الحقيقة وعن مركبيها، ويفيد في ضبط الأدلة في التحقيق الجاري بشأن الجريمة.[4]

وضبط الأدلة في الجرائم المعلوماتية يتصل بضبط المكونات المادية لأنظمة الحاسوب، وضبط المكونات المنطقية والبرمجيات، وكذا ضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب وما يتصل بها[5]، وعلى هذا الأساس فإن من الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم المعلوماتية والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم هي جهاز الحاسوب وملحقاته، ضبط المعدات المستعملة في الشبكة كجهاز المودم، ووسائط تخزين البيانات والمعطيات، وضبط البرمجيات.

المطلب الثاني:

وسائل الإثبات (الخبرة، الشهود، الاستجواب)

وسائل الإثبات في الجرائم المعلوماتية لها طبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية، فوسائل الإثبات تدخل في إطار اختصاص القضاء، والذي يثبت ويدعم من خلالها القضاء الجريمة المعلوماتية المرتكبة من طرف المجرمين، والتي هي محل التحقيق.

الفرع الأول: الخبرة[6]

وهي إجراء بمقتضاه يكلف القاضي شخصا من ذوي الاختصاص يسمى خبيرا بمهمة معينة تتطلب تحقيقا واستقصاءات قد تكون على جانب من التعقيدات توصلا لإعطاء القاضي معلومات ورأي فني بشأن أمور واقعية لا يمكن الحصول عليها بنفسه، ويثبت الخبير تحقيقه مع الرأي الذي توصل إليه في تقرير خطي إلى القاضي. فالخبرة هي أحد أهم وسائل جمع الأدلة، وتأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات، وبالنظر إلى الطبيعة الخاصة للجرائم المعلوماتية فإن إماطة اللثام عنها تحتاج إلى خبرة فنية منذ بدء مرحلة التحري عن هذه الجرائم، وتستمر إليها في مرحلتي التحقيق والمحاكمة، وتخضع لشروط شكلية وشروط موضوعية لابد من الالتزام بها لتعتمد لدى القضاء.

الفرع الثاني: الاستجواب[7]

ويعرف بأنه مساءلة المتهم ومناقشته عن وقائع القضية المنسوبة إليه ارتكابها ومجابهته بالأدلة وسماع ما لديه من دفوع للتهمة المنسوبة إليه. والهدف من الاستجواب هو كشف الحقيقة واستظهارها بالطرق القانونية، واستجواب المتهم في الجرائم المعلوماتية تحكمه ذات القواعد العامة لاستجواب متهم في أي جريمة تقليدية، إلا أنه لابد أن تكون السلطة المختصة التي تتولى الاستجواب مؤهلة للتحقيق في الجرائم المعلوماتية حتى يمكن الاستيعاب والتعامل مع مفردات الجريمة المعلوماتية، وقد أحاط المشرع الاستجواب بعدة ضمانات لابد من الالتزام بها لضمان حقوق المتهم.

الفرع الثالث: سماع الشهود

سماع الشهود كسائر إجراءات التحقيق في الطريقة التقليدية، فالقاضي له أن يسمع الشهود أو يستغني عنهم، فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه، والأمر متروك للسلطة التقديرية للقاضي، والشاهد في الجرائم المعلوماتية يطلق عليه اسم الشاهد المعلوماتي تميزا له عن الشاهد التقليدي، والمقصود بالشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسوب، والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعاجلة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة[8]، وتضم طائفة الشهود: مشغلو الحاسوب، خبراء البرمجة، محللو البيانات، مهندسو الصيانة، مديرو النظم.

المبحث الثاني:

مواجهة الجرائم المعلوماتية في التشريع الدولي

مع تزايد صور وحجم الخسائر والأضرار الناجمة عن الجرائم المعلوماتية، والتي تتخطى في أغلب أحيانها حدود لتطال اعتداءها دول ومؤسسات أخرى، ومع تميزها بالعالمية، وبكونها عابرة للحدود، وأثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة مواجهة الجريمة المعلوماتية، لذلك عملت الدول على توحيد جهودها لمكافحتها، وهو ما سنعالجه في هذين المطلبين:

المطلب الأول:

على المستوى الدولي

إن مكافحة الجرائم المعلوماتية لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي والجنائي، وفي إطار الجهد الدولي المبذول، فإن هناك العديد من الهيئات والمنظمات الدولية التي تلعب دورا ملحوظا في إطار إبرام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة الجرائم المعلوماتية.

1 – جهود الأمم المتحدة[9]**:** تبذل الأمم المتحدة جهودا لا يستهان بها في مجال محاولة التصدي للجرائم المعلوماتية وتؤكد على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون للحد من انتشارها وتعاظم آثارها، وقد حظيت الجرائم المعلوماتية باهتمام مؤتمرات الأمم المتحدة، وأبرزها ما جاء في هذا المجال مايلي:

عقد منظمة الأمم المتحدة المؤتمر الثالث عشر[10] لمنع الجريمة والعدالة الجنائية من 12 إلى 19 أفريل 2015 بدولة قطر، وكان الموضوع الرئيسي للمؤتمر "إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع للتصدي للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي، ومشاركة الجمهور" وقررت الجمعية العامة قرارها (184/67) النظر في ما يلي: إنشاء حلقات عمل من بينها تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، منها الجرائم المعلوماتية.

عقد منظمة الأمم المتحدة المؤتمر الثاني عشر[11] من 12 إلى 19 أفريل 2010 بالبرازيل تحت عنوان "استراتيجيات شاملة لتحديات عالمية" نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، وتضمن جدول أعمال المؤتمر ثمانية بنود: من بينها جرائم الإنترنت، حيث دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية لدراسة شاملة لمشكلة الجريمة المعلوماتية وتدابير التصدي لها.

قرارات وتوصيات الجمعية العام للأمم المتحدة[12] **:**

- القرار (121/45) العام 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994.

- القرار رقم (63/55) المؤرخ في 2000/12/04، والقرار رقم (121/56) المؤرخ في 2001/12/19 بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عقد وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

- القرار رقم (239/57) في 2003/01/31 والقرار رقم (199/58) المؤرخ في 2004/01/30 بشأن «إنشاء ثقافة عالمية للأمن السيبراني» ودعوة الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.

- قرار لجنة مكافحة المخدرات (5/48) حول "تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات".

- التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات (INCB) التي نشرت العام 2005 توصيات للحد من انتشار المبيعات غير المشرعة من المواد الخاضعة للرقابة ولاسيما المستحضرات الصيدلانية، عبر الإنترنت.

2- جهود الاتحاد الدولي للاتصالات:[13] يوفر الاتحاد الدولي للاتصالات الذي يضم 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية منبرا استراتيجيا للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة، وقد وضع الاتحاد الدولي للاتصالات مخططا لتعزيز الأمن الإلكتروني العالمي، ومن أهم أهدافه الرئيسية ما يلي:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلا للتطبيق محليا وعالميا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

- وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهياكل التنظيمية والسياسات المتعلقة بجرائم الإنترنت.

3- جهود المنظمة الدولية للشرطة الجنائية الإنتربول:[14] وتهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأعضاء وعلى نحو فعال في مكافحة الجريمة، من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأعضاء. وتتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأعضاء، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت.

4- جهود المنظمة العالمية للملكية الفكرية:[15] تهدف إلى تشجيع النشاط الإبتكاري، وتطوير إدارة الاتحادات في مجال حماية الملكية الصناعية وحماية المصنفات الأدبية والفنية، واهتمت بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، وتم الاتفاق على توفيرها بواسطة الاتفاقيات العالمية وخاصة "اتفاقية التريبس" و"اتفاقية بيرن" اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصة تشريعات حقوق المؤلف، كما يلزم الاتفاق الدولي الأعضاء في المنظمة بوجوب فرض إجراءات تنفيذية، وتدابير مدنية وإدارية، وعقوبات جنائية لمواجهة أي اعتداء على حقوق المؤلف وخاصة القرصنة، وتنص المادة (04) من منظمة العالمية للملكية الفكرية[16] المعتمدة سنة 1996 على أنه "تتمتع برامج الحاسوب بالحماية باعتباره مصنفات أدبية وتطبق تلك الحماية على برامج الحاسوب أيا كانت التعبير عنها".

5- جهود منظمة التعاون الاقتصادي والتنمية:[17] تضم هذه المنظمة في عضويتها 34 دولة وضعت المنظمة توصيات إرشادية بخصوص أمن نظم المعلومات، ومن مجمل أعمال منظمة التعاون الاقتصادي والتنمية حول الجرائم الإلكترونية حصل اتفاق على ضرورة أن يغطي قانون العقوبات في كل دولة الأفعال التالية:

أ- التلاعب في البيانات المعالجة آليا بما في ذلك محوها. ب- التجسس المعلوماتي. ج-التخريب المعلوماتي. د-قرصنة البرامج. هـ-الدخول غير المشروع على البيانات أو نقلها، واعتراض استخدام المعطيات أو نقلها.

6- جهود الاتحاد الأوروبي: أعلنت "يوروبول"[18] في 2014/09/01، وكالة تطبيق القانون الأوروبية، المتخصصة في مكافحة الجرائم والإرهاب في دول الاتحاد

الأوروبي، عن إنشائها قوة خاصة لمحاربة الجرائم المعلوماتية في دول الاتحاد، كما أن عملها يمتد إلى دول أخرى.

وستكون مهمة القوة الجديدة التنسيق مع التحقيقات الدولية لاتخاذ التدابير اللازمة في مواجهة التهديدات الرئيسية على الإنترنت، مثل البرمجيات الخبيثة وخاصة ما يستهدف منها القطاعات المالية ومكافحة عمليات الاحتيال المعلوماتية والمواقع التي تبيع الممنوعات وغير ذلك، وستبدأ القوة التي أطلق عليها اسم "J-CAT" وسيكون مقرها ضمن المركز الأوروبي للجرائم المعلوماتية "EC3" التابع لليوروبول.

ويتضمن فريق العمل المشترك ضد الجرائم المعلوماتية الأعضاء في الاتحاد الأوروبي بالإضافة إلى شركاء آخرين لا ينتمون إلى الاتحاد الأوروبي من وكالات تطبيق القانون.

وانضمت للتعاون مع هذه القوة الجديدة مجموعة من الدول منها كندا واستراليا وألمانيا وفرنسا وهولندة وإيطاليا وإسبانيا والمملكة المتحدة والولايات المتحدة الأمريكية.

7- جهود اتفاقية المجلس الأوروبي: اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام 1976، وفي العام 1996 أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة السيبرانية، عملت اللجنة بين سنة 1997 و2000 على الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر أفريل 2001، وتم التصديق على الاتفاقية من قبل 30 دولة بحلول العام 2010، واتفاقية جرائم الإنترنت هي المعاهدة الدولية الأولى التي تسعى لمعالجة الجرائم الإلكترونية عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى ومن أهم أهداف الاتفاقية[19]:

أ- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

ب- توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيا.

ج- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخل في محتواها.

د- تتضمن الاتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.

8- جهود مجموعة الدول الثماني "G8":[20] اعتمد وزارة العدل والداخلية لبلدان الثمانية في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى المبادئ التالية:

عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم تدريب الموظفين المكلفين تنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية، بالإضافة إلى ذلك دعت دول الثمانية إلى مواصلة العمل حتى التوصل إلى حلول دولية ناجحة، من خلال عقد اتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة ومن توصيات الـ "G8" بالنسبة للجرائم الإلكترونية موجودة في إطار الباب "D" من المعاهدة وتتلخص بما يلي[21]:

- يتعين على الدول أن تجرم الانتهاكات على حقوق الغير على الشبكة العنكبوتية التي تستوجب العقوبات الجزائية وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال

لمنع الجريمة، وإقامة تعاون دولي في ما يتعلق بمكافحة هذه الانتهاكات وينبغي للدول أن تتخذ خطوات لمنع الجريمة ذات التقنية العالية.

9- جهود الاتحاد الإفريقي[22]**:** طلب المؤتمر الاستثنائي لوزارة الاتحاد الإفريقي المسؤولين عن تكنولوجيا المعلومات والاتصالات المنعقد في جنوب إفريقيا من 02 إلى 05 نوفمبر 2009 من مفوضية الاتحاد الإفريقي القيام بالاشتراك مع لجنة الأمم المتحدة الاقتصادية لإفريقيا بإعداد اتفاقية حول التشريع القضائي على أساس احتياجات القارة والالتزام بالمتطلبات القانونية والتنظيمية للمعاملات الإلكترونية والأمن الإلكتروني وحماية البيانات الشخصية. كما أوصت بضرورة توفير الحماية القانونية لأنظمة المعلوماتية التي تعتبر قيمة بالنسبة للمجتمع مما يجعل من الضروري سن التشريعات ضد الجريمة الإلكترونية. وفي يونيو 2014، اجتمع مجموعة من قادة الاتحاد الإفريقي مكون من 54 حكومة أفريقية في القمة 23 للاتحاد الإفريقي، ووافقوا على اتفاقية الاتحاد الأفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية.

المطلب الثاني:

على المستوى العربي

من أبرز ما يمكن أنت يقال عن الجهود العربية المبذولة على مستوى الدول العربية من أجل الحماية من الجرائم الإلكترونية التي تضررت منها تلك الدول وألحقت بها خسائر نجد:

1- الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتي[23]**:** وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهم المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21 وتحتوي على (43) مادة وجاء في مضمون المادة الأولى منها "تهدف هذه الاتفاقية إلى 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" ونجد في الفصل الثاني تفصيلا للأفعال التي تعد مجرمة، وفي الفصل الثالث تتعرض لنطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع تعرضت للتعاون القانوني والقضائي وفي الفصل الخامس تعرضت إلى أحكام ختامية.

2- المكتب الإقليمي العربي للاتحاد للاتصالات[24]**:** عقد محضر الاجتماع الأول في الجزائر يومي 25 و26 فيفري 213 تم تشكيل فريق العمل حول حماية الأطفال على الإنترنت في المنطقة العربية ويهدف إلى تنسيق الجهود وتوحيد الرؤية في المنطقة العربية من أجل التوصل إلى وضع مبادئ توجيهية لإطار قانوني لحماية الطفل على الإنترنت في المنطقة العربية وتم الاتفاق على ان تكون مهمة الفريق كالتالي:

أ- تحديد الأفعال التي تشكيل خطرا على الأطفال في الفضاء السيبراني

ب- وضع المبادئ التوجيهية للإطار القانوني الإقليمي لحماية الأطفال في الفضاء السيبراني في إطار التعاون والتنسيق الإقليمي في المنطقة العربية.

ج- تقديم توصيات عامة حول الاسترشاد بالمبادئ التوجيهية على المستوى الوطني لكل دولة عند صياغة قوانينها الخاصة.

3- القوانين النموذجية[25]: اعتمدت جامعة الدول العربية عبر الأمانة العامة لمجلس وزراء العدل العرب ما سمي بالقوانين العربية الاسترشادية الخاصة بمكافحة الجرائم الإلكترونية ومنها:

أ- القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة: اعتمده مجلس وزراء العدل العرب بالقرار رقم (771/د24) بتاريخ 2008/11/27 يحتوي على سبعة فصول، و(24) مادة ونجد الفصل الخامس من المادة (23) إلى (32) وما يليه يحتوي على الجرائم والعقوبات الخاصة بالجرائم الإلكترونية.

ب- قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها: اعتمده مجلس وزراء العدل العرب في دورته (19) بالقرار رقم (495/د19) بتاريخ 2003/10/08 واعتمده مجلس وزراء الداخلية العرب في دورته (21) بالقرار رقم (417-د2004/21) ويحتوي على (27) مادة تخص العقوبات للجرائم الإلكترونية.

ج- القانون العربي الاسترشادي لحماية حق الملكية الفكرية: اعتمده مجلس وزراء العدل العرب بقرار رقم (940/د28) سنة 2012 والذي يحوي في الجزء الأول على حماية حق المؤلف والحقوق المجاورة، ويتكون من (10) فصول ونجد الفصل الرابع في المادة (19) الذي يوضح المصنفات المشمولة بالحماية منها "برامج الحاسوب مهما كانت لغتها بما فيها الأعمال التحضيرية" أما المادة (20) تتمتع بالحماية المقررة في هذا القانون المصنفات المشتقة التالية:

قواعد البيانات، سواء أكانت مقروءة أم غير مقروءة من الحاسب وفي الفصل التاسع نجد الإجراءات التحفظية والجزاءات في المادة (74) وما يليها.

4- مجلس وزار العدل العرب[26]**:** بموجب القرار رقم (229) سنة 1996 وباستعراض الباب التاسع الخاص ضد الأشخاص نجد القانون قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية وذلك في المواد (461-464) حيث أشارت المواد (461-463) على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الإطلاع عليها والمادة (464) نصت على عقاب من يقوم بفعل الدخول الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظيفته المعتادة وتغيير المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية وسرقة المعلومات.

المبحث الثالث:
مواجهة الجرائم المعلوماتية في التشريع الجزائري

سارع المشرع الجزائري كغيره من الدول إلى احتواء الجريمة المعلوماتية من خلال التعديلات التي أدخلها على قانون العقوبات وسن نصوص قانونية أخرى جديدة نسترضها كما يلي:

المطلب الأول:
الحماية من خلال قانون العقوبات

يعتبر قانون العقوبات وسيلة ردعية للكف عن ارتكاب الجرائم بصفة عامة، وبما أن الجرائم المعلوماتية تلحق أضرار بالغير فقد أقر المشرع عقوبات ردعية لتلك الجرائم وهي كالتالي:

أولا: المساس بأنظمة المعالجة الآلية للمعطيات وهي من أبرز الجرائم التي عالجتها المحاكم الجزائرية (الملحق 05)، وهذا بموجب القانون رقم (15/04)[27] المتعلق بقانون العقوبات وذلك من خلال المواد (394 مكرر) إلى (394 مكرر7)، فمن خلال استقراء

نصوص المواد حاول المشرع الجزائري حصر هذه الجرائم والعقوبات المقرر لها فيما يلي[28].

1- جريمة دخول معالجة آلية للمعطيات عن طريق الغش: نصت عليها المادة (394 مكرر)[29] من قانون العقوبات، حيث تعاقب بالحبس والغرامة عند الدخول أو البقاء بالغش في المنظومة المعلومة وفرق المشرع في هذه الحالة بين ما إذا كانت الجريمة بسيطة ومضاعفة العقوبة إذا ترتب عنها حذف أو تغيير المنظومة، وبين ما إذا ترتب على ذلك تخريب لنظام اشتغال المنظومة.

2- جريمة إزالة أو تعديل معطيات في نظام المعالجة آلية بطرق تدليسية: نصت عليها المادة (394 مكرر1)[30] من قانون العقوبات، حيث اعتبر المشرع الجزائري أن إزالة أو تعديل المعطيات التي يتضمنها النظام بطريق الغش عملا إجراميان ويقصد بإزالة المعطيات سواء جزئيا أو كليا أما محوها أو إتلافها أو تخريبها من أجل منع النظام القيام بمهامه أو تعطيل النظام المعلوماتي، والطرق متعدد شرحناها في مبحث سابق مثل نشر الفيروسات، أما تعديل المعطيات ويقصد به إما إدخال معلومات وهمية أو تزويرها في النظام المعلوماتي.

4- جرائم نشر حيازة أو الاتجار بالمعطيات المخزنة أو المعالجة: نصت عليها المادة (394 مكرر2)[31] من قانون العقوبات، حيث تعد هذه الجريمة من أكثر الجرائم وقوعا في العالم الافتراضي ولقد اعتبر المشرع الجزائري عملية اصطناع برنامج مخصص لارتكاب فعل الغش المعلوماتي أو إعداد برنامج ناقص من الناحية الفنية وخاصة المبرمج من أجل خلق فجوات وثغرات فيه لممارسة فعل الغش أو تجميع أو التقاط البيانات بغرض استغلالها أو نشرها خاصة عن طريق الإنترنت أو الاتجار فيها من الجرائم المعاقب عليها، بحكم أن جريمة الإفشاء والنشر تتسم بخطورة على الحياة الخاصة.

5-جرائم المعالجة الآلية الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام طبقا للمادة (394 مكرر)[32] من قانون العقوبات: حيث اعتبر المشرع الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي مؤسسة رسمية بمثابة ظرف تشديد ويستخلص من نص المادة (394 مكرر3) من قانون العقوبات أن العقوبة المشددة على جميع الجرائم المنصوص عليها في المادة (394 مكرر) والمادة (394 مكرر1) و (مكرر2) من قانون العقوبات وحرص المشرع الجزائري على ضمان حماية مطلقة لهيئات الدفاع الوطني ولمؤسسات الدولة الجزائرية وتوسع في هذه الحماية وذلك بإدراج جميع الجرائم[33] المنصوص عليها في المادة (394 مكرر) من قانون العقوبات كلها.

6- الجرائم المعلوماتية للشخص المعنوي: نصت عليها المادة (394 مكرر4)[34] من قانون العقوبات حيث أقر المشرع الجزائري المسؤولية الجزائرية للأشخاص المعنوية، وشدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية، حيث أن الغرامة المطبقة على الشخص المعنوي تتراوح بين واحد إلى خمس أضعاف الغرامة المقررة على الشخص الطبيعي.

7- جريمة تكوين جمعية أشرار المعلوماتيين لغرض التحضير للجرائم الماسة بأنظمة المعالجة الآلية طبقا للمادة (394 مكرر5)[35] من قانون العقوبات: ويتضح من خلال نص المادة أن العقوبات يطال من يشارك أي مجموعة أو في اتفاق الغرض منه التحضير أو الإعداد لارتكاب الجرائم المعلوماتية مع توفر القصد الجنائي، كما يستخلص أن

مجرد المشاركة أو الاتفاق المجسد بفعل مادي يوحي بالتحضير للجريمة خاصة أن ذلك يمكن أن يتم عبر الشبكات المعلوماتية.

8- العقوبات التكميلية وفقا للمادة (394 مكرر6)[36] من قانون العقوبات: نص المشرع في هذه المادة على العقوبات التكميلية للجرائم السالفة الذكر وتمثل في المصادرة للأجهزة المستعملة والبرامج والوسائل المستعملة مع إلحاق ذلك بغلق المواقع وأماكن الاستغلال شريطة أن تكون بعلم صاحبها.

9- العقاب على الشروع في الجريمة المعلوماتية طبقا لنص المادة (394 مكرر7) [37]من قانون العقوبات: أن فعل الشروع أو البدء في ارتكاب الجريمة يعاقب عليه بنفس العقوبة المقررة للجنحة ذاتها، ونظرا لكون جرائم الاعتداء على نظام المعالجة الآلية ذات وصف جنحوي أقر المشرع العقاب لها بمثل الجريمة نفسها.

ثانيا: حماية حرمة الحياة الخاصة: من خلال التعديل الذي جاء في القانون رقم (06-23)[38] المتعلق بقانون العقوبات فالمادة (303 مكرر)[39] من قانون العقوبات تعاقب بالحبس والغرامة كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت سواء بالتقاط أو تسجل أو نقل صور أو مكالمات خاصة أو سرية دون إذن رضا صاحبها أما المادة (303 مكرر1)[40] من قانون العقوبات، تعاقب بالعقوبة ذاتها على من يحتفظ أو يضع في متناول الجمهور الصور أو الوثائق بأية وسيلة كانت.

ثالثا: حماية حرمة رموز الدولة: من خلال التعديل الذي جاء في القانون رقم (14/11)[41] المتعلق بقانون العقوبات، حيث نصت المادة (144 مكرر)[42] منه، على عقوبة الغرامة المالية فقط كل من أساء لرئيس الجمهورية بأية وسيلة كانت أو بوسيلة إلكترونية وفي حالة العود تضاعف الغرامة.

رابعا: الحماية من خلال قانون الإجراءات الجزائية: حيث أن المادة (16) من قانون الإجراءات الجزائرية[43] وسعت من الاختصاص المحلي لضباط الشرطة القضائية فيما يتعلق بالبحث ومعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ويمتد الاختصاص إلى كامل الإقليم الوطني، كما جاءت المادة (37) من قانون الإجراءات الجزائية[44] والمادة (40) منه لتمكن كل من وكيل الجمهورية وقاضي التحقيق على تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

المطلب الثاني
الحماية من خلال قوانين خاصة[45]

وهذه القوانين الخاصة شملت الحماية في قانون التأمينات الاجتماعية، وكذلك الحماية من خلال نصوص الملكية الفكرية، وأيضا الحماية في نصوص التوقيع الإلكتروني بالإضافة إلى الحماية المتعلقة بالمواصلات السلكية واللاسلكية.

أولا: الحماية في قانون التأمينات الاجتماعية: بمقتضى أحكام قانون التأمينات الاجتماعية رقم (01/08)[46] المؤرخ في 2008/01/23 شدد العقوبة فيما يتعلق بالمساس غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا، وعاقب المشرع الجزائري كل من يسلك أو يستسلم بهدف الاستعمال غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا المفتاح الإلكتروني لهيكل العلاج أو المفتاح لمهني الصحة طبقا للمادة (93 مكرر2)[47] من نفس القانون، كما يشمل العقاب التعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية أو نسخ البرمجيات المتعلقة باستعمال البطاقة

الإلكترونية، أو المحاولة على ارتكاب الفعل طبقا لنص المادة (93 مكرر3) منه[48]، كما أقر المشرع أيضا عقوبة للشخص المعنوي تتمثل في الغرامة ضعف المقررة للشخص الطبيعي طبقا لنص المادة (93 مكرر 5)[49] من ذات القانون، ومصادرة الأجهزة والوسائل المستعملة وكذا غلق المحلات وأماكن الاستغلال التي تكون محل الجنح.

ثانيا: الحماية من خلال قانون الملكية الأدبية والفنية: حاول المشرع الجزائري مواجهة الجريمة الإلكترونية من خلال قانون الملكية الأدبية والفنية المتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم (05/03)[50] المؤرخ في 2003/07/23 المتعلق بحقوق المؤلف والحقوق المجاورة، حيث وسع قائمة المؤلفات المحمية، وذلك بإدماج برامج المعلوماتية، ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج المعلوماتية، كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المصنفات الرقمية التي تشملها الحماية.

ثالثا: الحماية في نصوص التوقيع الإلكتروني: أصدر المشرع الجزائري قانون رقم (03/15)[51] المتعلق بعصرنة العدالة، حيث تطرق في الفصل الثاني إلى المنظومة المعلوماتية المركزية لوزارة العدل والإشهاد على صحة الوثائق الإلكترونية وضمان حمايتها، أما الفصل الثالث تعرض إلى إرسال الوثائق والإجراءات القضائية بالطريق الإلكترونية، والفصل الخامس تعرض إلى الأحكام الجزائية لحماية التوقيع والتصديق الإلكترونيين، حيث أن المادة (17)[52] منه تعاقب على كل من يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر. أما المادة (18)[53] تعاقب كل شخص حائز على شهادة إلكترونية يستعملها بعد انتهاء صلاحيتها أو إلغائها.

رابعا: الحماية المتعلقة بالموصلات السلكية واللاسلكية: تضمن الفصل الثاني من الباب الرابع من القانون رقم (03/2000)[54] المتعلق بالبريد والمواصلات السلكية واللاسلكية الأحكام الجزئية المترتبة على مخالفة النظام القانوني، فالأشخاص المرخص لهم تقديم خدمة المواصلات السلكية واللاسلكية والعمال متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات السلكية واللاسلكية أو المساعدة على ذلك يعاقبون طبقا لنص المادة (137) من قانون العقوبات أم غيرهم ممن يرتكب هذه الأفعال يعاقب بالحبس والغرامة.

خامسا: الحماية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها رقم (04/09)[55] : وتكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية ويبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، وقد جرم الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا. وقد حدد القانون الحالات التي يسمح فيها اللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات عن احتمال اعتداء منظومة معلوماتية. وقد تعرض الفصل الأول من القانون إلى أهدافه وتحديد مفهوم التقنية، أما الفصل الثاني فقد تعرض إلى أحكام خاصة بمراقبة الاتصالات الإلكترونية، والفصل الرابع تعرض إلى القواعد الإجرائية الخاصة

بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والفصل الرابع تعرض إلى تحديد الالتزامات التي تقع على المتعاملين في الاتصالات الإلكترونية، ثم الفصل الخامس نص على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحتها والفصل السابع فقد نص على التعاون والمساعدة القضائية الدولية بخصوص مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خاصة منها بالمساعدة وتبادل المعلومات.[56]

التهميش

(1) – سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير علوم جنائية، جامعة الحاج لخضر، باتنة، 2013، ص110 إلى 120.

(2) – عبد الفتاح بيومي حجازي، مبادئ في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص192.

(3) – محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير، قسم علوم الشرطة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص76-80.

(4) – خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2001، ص170-171.

(5) – خالد عياد الحلبي، المرجع السابق، ص281-282.

(6) – محمود الشنكيات، الإثبات بالمعاينة والخبرة في القانون المدني، دراسة الثقافة للنشر والتوزيع، الأردن، 2008، ص98.

(7) – عبد الأمير العكيلي وسليم حربة، أصول المحاكمات، ج1 و2، دار الكتب للطباعة والنشر، القاهرة، 1980، ص44.

(8) – عبد الفتاح بيومي حجازي، المرجع السابق، ص339.

(9) – محمود أحمد عبابنة، المرجع السابق، ص155.

(10) – حكومة قطر الإلكترونية، صفحة المؤتمر،
http://www.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congresses.html

(11) – المرجع نفسه.

(12) – موقع خاص بقرارات الأمم المتحدة
http://www.un.org/arabic/documents/instruments/subj_ar.asp

(13) – موقع الاتحاد الدولي للاتصالات
http://www.itu.int/osg/csd/cybersecurity/gca/global-strategic-report/index.htm

(14) – أمير فرج يوسف، المرجع السابق، ص462 - 463.

(15) – محمود أحمد عبابنة، المرجع السابق، ص159-160.

(16) – المنظمة العالمية للملكية الفكرية www.wipo.int

(17) – علي حسن الطوالبة، المرجع السابق، ص102-104.

(18) – الموقع الإلكتروني لليروبول www.eurpol.europa.eu
(19) – علي حسن الطوالبة، المرجع السابق، ص100.
(20) – موقع مجموعة الثمانية
G8recommandations on transnational crimes, 2011,
www.Canadainternationalgc.ca/G8
(21) – المرجع نفسه.
(22) – موقع القانون الإفريقي www.africa-union.org
(23) – الشبكة القانونية العربية www.arabegalnet.org
(24) – الاتحاد الدولي للاتصالات
https://www.itu.int/ITU.../Minutes-of-1st-meeting.doc
(25) – القوانين العربية النموذجية https://www.protectionproject.org
(26) – محمود أحمد عبابنة، المرجع السابق، ص180-181.
(27) – القانون (15/04) المؤرخ في 2004/11/10 المتعلق بقانون العقوبات الرسمية عدد 71 صادر في 2004/11/10.
(28) – مولود ديدان، قانون العقوبات، دار بلقيس للنشر، الدار البيضاء، الجزائر، ط2012، مصححة ومحيثة، ص135-137
(29) – المادة (364 مكرر) من القانون (15/04) ،المرجع السابق.
(30) – المادة (394 مكرر1)، المرجع نفسه.
(31) – المادة (394 مكرر2)، المرجع نفسه.
(32) – المادة (394 مكرر3)، المرجع نفسه.
(33) – زيبحة زيدان، المعلوماتية في التشريع الجزائري، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2001، ص100.
(34) – المادة (394 مكرر4) من القانون رقم (15/04)، المرجع السابق.
(35) – المادة (394 مكرر5)، المرجع نفسه.
(36) – المادة (394 مكرر6)، المرجع نفسه.
(37) – المادة (394 مكرر7)، المرجع نفسه.
(38) – القانون (23/06) المؤرخ في 2006/12/20، المتضمن قانون العقوبات، الجريدة الرسمية، عدد48، الصادرة في 2006/12/24.
(39) – المادة (303 مكرر)، المرجع نفسه.
(40) – المادة (303 مكرر1) من القانون (23/06)، المرجع السابق.
(41) – القانون (14/11) مؤرخ في 2011/08/02 المتضمن قانون العقوبات، الجريدة الرسمية، عدد 44، صادرة في 2011/08/10.
(42) – المادة (144 مكرر)، المرجع نفسه.
(43) – القانون (22/06) المؤرخ في 2006/12/20 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 84 صادرة في 2006/12/24.
(44) – المادة (37) والمادة (40) من القانون رقم (14/04) مؤرخ في 2004/11/10 يعدل ويتمم الأمر (155/66) المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد، 71 صادرة في 2004/11/10.

(45) – بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، عدد1، 2013، جامعة جيلالي اليابس سيدي بلعباس، ص63 – 74.

(46) – القانون (01/08) المؤرخ في 2008/01/23 المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، عدد 04، صادرة في 2008/01/27.

(47) – المادة (93 مكرر2) من القانون رقم (01/08)، المرجع السابق.

(48) – المادة (93 مكرر 3)، المرجع نفسه.

(49) – المادة (93 مكرر 5)، المرجع نفسه.

(50) – الأمر (05/03) المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 44، صادرة بتاريخ 2003/07/23.

(51) – القانون (03/15) المؤرخ في 2015/02/01 المتعلق بعصرنة العدالة، الجريدة الرسمية، عدد2، صادرة في 2015/02/10.

(52) – المادة (17)، المرجع نفسه.

(53) – المادة (18)، المرجع نفسه.

(54) – القانون (03/2000) المؤرخ في 2000/08/05 الذي يحدد القواعد العامة المتعلقة بالبريد السلكية واللاسلكية، الجريدة الرسمية، عدد، المؤرخة في 2000/08/06.

(55) – القانون (04/09) المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد47، الصادرة في 2009/08/16.

(56) – صغير يوسف، المرجع السابق، ص112.