

ضوابط مكافحة الجريمة المعلوماتية

Regulation for Combating Information Crimes

رابح سعاد*

جامعة جيلالي ليابس - سيدي بلعباس، الجزائر

souad.rabah@univ-sba.dz

- تاريخ الإرسال: 2021/04/27 - تاريخ القبول: 2021/05/21 - تاريخ النشر: 2021/06/09

الملخص: يشهد العالم المعاصر ثورة في مجال تكنولوجيا الإعلام والاتصال، حيث عرف الإنترنت انتشارا واسعا ومعه انتشرت الاعتداءات الإلكترونية، نتيجة للاستخدام غير المشروع للتقنيات الحديثة، فظهر إلى الوجود نوع جديد من الجرائم يختلف عن الجرائم التقليدية، أطلق عليها تسمية الجرائم المعلوماتية نسبة للبيئة التي ظهرت فيها. هو ما استدعى تدخل المشرع لوضع حد لهذا التنامي الخطير في ميدان الإجرام المعلوماتي، عن طريق سنّ نصوص قانونية موضوعية دولية وحتى داخلية، تجرم وتعاقب الأفعال التي تشكل اعتداء أو تهديدا للأمن المعلوماتي، مع استحداث هيئات تعمل على المستوى الميداني من أجل مكافحة هذا النوع من الإجرام.

الكلمات المفتاحية: الجريمة المعلوماتية - التقنيات الحديثة - الأمن المعلوماتي.

Abstract: The contemporary world is witnessing a revolution in the field of information and communication technology, as the Internet has become widespread and with it the spread of electronic attacks as a result of the illegal use of modern technologies, as a new type of crime has emerged that differs from the traditional crime, which is called cybercrime relative to the environment in which it appeared. which required the intervention of the legislator to put an end to the serious increase in cybercrime, by establishing substantive international and even internal legal texts that criminalize and punish acts that constitute an assault or threat to information security, while creating bodies that work at the field level in order to combat this type of crime.

Keywords: Information crime - Modern technologies - Information security.

* المؤلف المرسل: رابح سعاد.

مقدمة:

لطالما رافقت الجريمة على اختلاف أنواعها بيئة الإنسان ومجتمعه، وتطورت بتطوره، هو ما يفسر تزامن ظهور الجريمة المعلوماتية مع التطور الهائل والمتواصل بشكل متنامي في العالم الرقمي.

وإذا كان هذا التطور له جانبه الإيجابي، الذي يساعد المجتمعات المعاصرة على التواصل الحضاري والثقافي وعلى التقديم النوعي للخدمة، فإن له جانبه السلبي إذا ما أسيئ توظيفه، حيث أصبحت المعلومة بل وحتى المنظومة المعلوماتية التي تقوم عليها أنظمة حكومات دول وحتى الحياة الخاصة للأفراد محلا للجريمة.

وما دامت القاعدة القانونية اجتماعية تتطور بتطور المجتمع، وعلى اعتبار أنّ النصوص القانونية خاصة العقابية منها، جاءت خالية من تنظيم أفعال ارتبطت في مفهومها بالجريمة المعلوماتية، حيث وجدت الدول نفسها أمام واقع فراغ تشريعي، وهو ما عرف بأزمة القانون الجنائي. وإن كان البعض يرى أنّ النصوص التقليدية يمكن سحبها وتطبيقها على هذا النوع من الجرائم، باعتبار أن المعلومة مال يمكن تقويمه، ومع ذلك كان لزاما على المشرع الدولي وحتى الداخلي مجارة تطور الفكر والعقل البشري الإجرامي، وسنّ نصوص قانونية لمجابهة هذا النوع من الأفعال.

وعلى شاكلة العديد من الدول تدخل المشرع الجزائري في هذا المجال ضابطا لهذه المسائل بالنظر لخصوصية هذا النوع من الجرائم. من ذلك لنا أن نتساءل عن كيفية مواجهة المشرع الدولي والداخلي لهذه الجريمة من جهة؟ ثم نطرح تساؤلا ثانيا عن مدى كفاية هذه النصوص القانونية وفعاليتها لتوفير الحماية العملية، من خلال تسليط الضوء على الهيئات التي أسندت لها مهمة مكافحة الجريمة المعلوماتية؟

هي أسئلة جالت وصالت في أنفسنا حيال إنجاز هذه الورقة البحثية، محاولين رفع الغطاء عنها باتباع المنهج الوصفي والتحليلي من خلال التطرق لمبحثين إثنين: جاء المبحث الأول تحت عنوان: الضوابط التشريعية لمكافحة جريمة المعلوماتية، أما المبحث الثاني فقد جاء تحت عنوان الضوابط العملية لمكافحة الجريمة المعلوماتية.

المبحث الأول: الضوابط التشريعية لمكافحة الجريمة المعلوماتية

أمام تزايد معدلات الجريمة المعلوماتية، حيث أخذت منحى خطير خاصة بعد ما كشفت عنه الدول من إحصائيات نتيجة الاستخدام الواسع للتقنيات الرقمية بمختلف أنواعها، الأمر الذي ألزم تدخلا فعالا من أجل وضع نصوص وآليات قانونية واضحة لمكافحة الجريمة المعلوماتية. من أجل ذلك بادر المجتمع الدولي من خلال تكثيف الجهود فيما بين الدول لوضع قواعد قانونية دولية كفيلة بمكافحة الجريمة

المعلوماتية(المطلب الأول)، وقد سائر المشرع الجزائري المجتمع الدولي في ذلك من خلال وضع إستراتيجية متكاملة، قام من خلالها بإصدار وتعديل العديد من القوانين بما يتلائم مع التطور الملحوظ في هذا المجال(المطلب الثاني).

المطلب الأول: الجهود الدولية لمكافحة الجريمة المعلوماتية

عمل المجتمع الدولي من أجل وضع نصوص قانونية تتناسب مع التطور الحاصل في الجانب المعلوماتي، إذ كان لابد من إيجاد القواعد القانونية النازمة لمسألة منع الاعتداء على النظم المعلوماتية أو الاستخدام غير المشروع لها من خلال عديد الاتفاقيات ولعل أهمها:

أولاً- اتفاقية "برن" المتعلقة بحقوق المؤلف، والتي تم التوقيع عليها سنة 1971 في سويسرا، حيث صادقت عليها الجزائر بموجب المرسوم الرئاسي الصادر بتاريخ 1997/06/13 المتضمن انضمام الجزائر لها مع التحفظ¹، ومن بين أهم ما جاءت به هذه الاتفاقية، أنها نصّت على منح المؤلف حق استشاري في التصريح بعمل نسخ من المصنفات بأي طريق وبأي شكل، كما منحت له الاتفاقية حق الترخيص أو منح أي ترجمة أو اقتباس أو بث إذاعي²، وبموجب اتفاقية برن تتمتع برامج الحاسب الآلي "الكمبيوتر" بالحماية باعتبارها أعمال أدبية.

ثانياً- معاهدة الويبو، المتعلقة بحماية حقوق الملكية الفكرية، حيث ظهرت للوجود منظمات عالمية تسعى لتوفير أكبر قدر من الحماية، ومن ثم تشكلت المنظمة العالمية للملكية الفكرية "ويبو" والتي تأسست بموجب معاهدة ستوكهولم سنة 1967، ودخلت حيز التنفيذ سنة 1970³، وعلى إثرها جاءت معاهدات "الويبو الثلاث"، والتي تم التوقيع عليها في 20 ديسمبر 1996 والمتمثلة في:

أ- معاهدة الويبو بشأن حقوق المؤلف (تعرضت لنطاق حماية المؤلف، كحق التوزيع، التأجير ونقل المصنف إلى الجمهور)⁴.

ب- معاهدة الويبو بشأن الأداء والتسجيل الصوتي.

¹مرسوم رئاسي رقم 97-341 المؤرخ في 13/09/1997 المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية برن المؤرخة في 09/09/1869 والمتممة في باريس بتاريخ 04/05/1909 والمعدلة في 28/09/1997، ج.ر.ج.ع.ج.ع. 01 الصادرة بتاريخ 14/09/1997.

²منير محمد الجنيهي، جرائم الأنترنت والحساب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص.201.

³محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، سنة 2009، ص.160.

⁴تم التوقيع عليها في 20 ديسمبر 1996، وتتكون من ثمانية عشر مادة، لتفاصيل أكثر، أنظر، منير محمد الجنيهي، المرجع السابق، ص.202.

ت- اتفاقية تريبس، الخاصة بأوجه التجارة المتصلة بحقوق الملكية الفكرية، والتي تم التوقيع عليها سنة 1994، تناولت هذه الاتفاقية تحرير التجارة العالمية، حيث نصت في المادة العاشرة فقرة أولى على "تتمتع برامج الحاسب الآلي أو الكمبيوتر، بالحماية باعتبارها أعمال أدبية بموجب معاهدة برن"⁵.

ثالثا- معاهدة بوابست، إن أهم الجهود الدولية في هذا المجال تعلق باتفاقية بوابست، والتي تم التوقيع عليها في 23 نوفمبر 2001 في العاصمة المجرية بوابست، وذلك لمواجهة الاستخدام الغير مشروع للحاسب⁶.

رابعا- أما على المستوى العربي، فقد تم وضع القانون العربي النموذجي الاسترشادي لمكافحة الجريمة المعلوماتية⁷، حيث تم اعتماد هذا القانون النموذجي من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بتاريخ 2003/10/08⁸.

خامسا- الاتفاقية العربية لمكافحة الجريمة المعلوماتية، وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة، بتاريخ 2010/12/21⁹، وحسب ما ورد في المادة الأولى منها فإن هذه الاتفاقية تهدف إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدفع أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

المطلب الثاني: المواجهة التشريعية الداخلية لمكافحة الجريمة المعلوماتية

تتمتع الجريمة المعلوماتية بطبيعة مغايرة ومختلفة عن الجريمة التقليدية، لذا كان على المشرع الجزائري التصدي لها مثل باقي دول العالم، وبذلك تنوعت الضوابط التشريعية المتبعة من أجل مواجهة الجريمة المعلوماتية، وذلك على مختلف درجات القانون، انطلاقاً من أحكام الدستور، والتي ضمنت حرية

⁵ منير محمد الجنبهي، المرجع السابق، ص. 204.

⁶ محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011، ص. 25.

⁷ تم إعداد هذا القانون من قبل لجنة مشتركة بين المكتب التنفيذي لوزراء العدل العرب، والمكتب التنفيذي لوزراء الداخلية العرب، حيث جرى إقراره بوصفه منهاجاً استرشادياً للمشرع الوطني عند إعداد تشريع يتعلق بالجرائم المعلوماتية، وقد اعتمدت جامعة الدول العربية ما سمي بقانون الإمارات العربي الاسترشادي، لمكافحة جرائم تقنية المعلومات وما في حكمها نسبة إلى مقدم هذا المقترح، لتفاصيل أكثر حول هذه النقطة أنظر، أمير فرج يوسف، الجريمة المعلوماتية والإلكترونية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، الإسكندرية، 2011، ص. 354.

⁸ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دراسة متعمقة في القانون المعلوماتي، دار الكتب القانونية، القاهرة، 2007، ص. 175.

⁹ وتحتوي هذه الاتفاقية على 43 مادة، تضمن الفصل الأول منها الهدف من الاتفاقية، بينما تضمن الفصل الثاني تفصيلاً للأفعال التي تعد مجرمة، وحدد الفصل الثالث نطاق تطبيق الأحكام الإجرائية، وتناول الفصل الرابع التعاون القانوني والقضائي، وورد في الفصل الخامس الأحكام الختامية.

الابتكار وحقوق المؤلف. وفي إطار ذلك وضع المشرع سياجا واضحا، اعتمد على أطر قانونية جاءت على مراحل متفرقة في نصوص متناثرة، بنسب مختلفة، ولعل أهم النصوص القانونية الضابطة لهذه المسألة ما يلي:

أولا-تقرير حماية جزائية لمعطيات الحاسب الآلي في قانون الملكية الفنية والأدبية: وذلك من خلال القانون رقم 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة¹⁰، حيث اعترف المشرع بوصف المصنف الفكري لمعطيات الحاسب الآلي، إذ نجد أنه وسّع من قائمة المؤلفات المحمية، حيث أدمج تطبيق الإعلام الآلي ضمن المصنفات المحمية في المادة الرابعة منه، عندما نص على برامج الحاسوب الآلي، واعتبر أن أي اعتداء على الحق المالي والأدبي لمؤلف البرامج والبيانات يشكل فعلا من أفعال التقليد المنصوص عليها في المادة 151 من الأمر 03-05 والتي تقرر العقوبات الجزائية المكرّسة في المواد 153-154-156-158 من الأمر نفسه.

ثانيا- مكافحة الجريمة المعلوماتية من خلال تعديل قانون العقوبات: في محاولة من المشرّع لتدارك الفراغ القانوني في مجال قانون العقوبات، تم تعديله بموجب القانون 04-15 بأن حدّد لهذا النوع من الجرائم قسما خاص وهو القسم السابع مكرر، والذي جاء تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في ثمان مواد، من المادة 394 مكرر إلى 394 مكرر¹¹.

وحدّد الأفعال التي تشكل جريمة معلوماتية، والتي تنوعت بين الدخول أو البقاء غير المرخص به عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو من يحاول ذلك، بينما تشدّد المشرع في العقوبة إذا ترتب على ذلك حذف أو تغيير أو تخريب نظم اشتغال المنظومة، كما جرّم الاعتداء على معطيات نظام المعالجة الآلية من خلال المادة 394 مكرر¹، حيث جرّم المشرع في هذه المادة: الاعتداء على المعلومات التي يحتويها النظام وتعد جزء منه، إما عن طريق الإدخال بإضافة معطيات غير صحيحة، وإما المحو وذلك بإزالة معطيات مسجلة، التعديل أي تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى. كما جرّمت المادة 394 مكرر²، كل من يقوم عمدا أو عن طريق الغش بما يلي:

أ-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

¹⁰الأمر رقم 03-05 المؤرخ في 19/07/2003 المتعلق بحق المؤلف والحقوق المجاورة، ج.ر.ج.ع.ج.ع.44، الصادرة بتاريخ، 23/07/2003.
¹¹ قانون رقم 04-05 المؤرخ في 10/11/2004 المعدل والمتمم للأمر رقم 66/156 المتضمن قانون العقوبات، ج.ر.ج.ع.ج.ع.71، الصادرة بتاريخ 10/11/2004.

ب-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

مما سبق يستنتج أن المشرع، يعمل على تقرير حماية جنائية لكل المعطيات الداخلية كانت أو خارجية، ويقصد المشرع بالمعطيات المخزنة إما تلك المفرغة في دعامة مادية خارج النظام، كالأقراص أو تلك المخزنة داخل النظام ذاته، مثل الذاكرة، بينما يقصد بالمعطيات المعالجة إما تلك التي أصبحت جزء من النظام، بعد أن تحولت إلى إشارات أو رموز تمثل المعطيات المعالجة، أو تلك المعطيات المرسلّة عن طريق منظومة معلوماتية، مثل تبادل المعلومات بين أجهزة المنظومة المعلوماتية فالأولى تعتبر معطيات داخلية للنظام، أما الثانية فتعتبر معطيات خارجية للنظم المعلوماتية¹².

الملاحظ أن المشرع في إطار قانون العقوبات، قد جرّم الجريمة التامة ومجرد الشروع فيها، وبغض النظر عن تحقق النتيجة الإجرامية من عدمها. كما جرّم أفعال وسلوكات كل من الفاعل والشريك على حد سواء، كما حدّد هذا القانون في حال ارتكاب هذا النوع من الجرائم، إما عقوبات أصلية تتمثل في الحبس والغرامة المالية، أو عقوبات تكميلية وتتمثل في مصادرة الأجهزة والوسائل المستعملة والبرامج، كما كرّس وأقر المشرع بمسؤولية الشخص المعنوي المرتكب لإحدى الجرائم المعلوماتية، ورفع الحد الأقصى للعقاب إلى خمس مرات عن ذلك السقف المحدّد للغرامة المطبقة على الشخص الطبيعي.

وتجدر الإشارة إلى أن المشرع الجزائري في سنة 2006 أدخل تعديلا على قانون العقوبات بموجب تعديل 06 - 23¹³، حيث مس هذا التعديل القسم السابع مكرر والخاص بأنظمة المعالجة الآلية للمعطيات ولقد تمّ تشديد العقوبة المقررة لهذه الأفعال.

ثالثا- مكافحة الجريمة المعلوماتية من خلال تعديل قانون الإجراءات الجزائية: إذا كانت القاعدة العامة طبقا للفقرة الأولى من المادة 37 من قانون الإجراءات الجزائية المعدل والمتمم تقضي بتحديد اختصاص وكيل الجمهورية بمكان وقوع الجريمة، أو بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها، أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى لو حصل هذا القبض لسبب آخر، فإنّه وفي إطار مواجهة الجريمة المعلوماتية عمل المشرع الجزائري كذلك على تعديل نصوص قانون الإجراءات الجزائية بما يتلائم وخصوصية الجريمة المعلوماتية، حيث قام بتعديل المادة 37 من قانون الإجراءات الجزائية بإضافة فقرة ثانية تقضي بجواز تمديد الاختصاص المحلي لوكيل الجمهورية

¹²لتفاصيل أكثر حول هذه النقطة أنظر، فضيلة عاقل، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، أعمال المؤتمر الرابع عشر، طرابلس 24-25 مارس، 2017، ص.13-14.

¹³قانون رقم 06-23 المؤرخ في 20 ديسمبر يعدل ويتمم الأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر.ج.ع.ج.ع.84، الصادرة بتاريخ 24 ديسمبر 2006.

إلى دائرة اختصاص محاكم أخرى، إذا تعلق الأمر بالجريمة المنظمة وجرائم المعالجة الآلية للمعطيات، الإرهاب، تبييض الأموال وجرائم الصرف¹⁴.

الملاحظ أن ذات الحكم المتعلق بجواز تمديد الاختصاص المحلي لوكيل الجمهورية ينطبق كذلك على قاضي التحقيق طبقا للمادة 40 من قانون الإجراءات الجزائية المعدل بموجب القانون 04-14¹⁵، وجواز تمديد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني طبقا لنص المادة 16 من قانون الإجراءات الجزائية المعدلة بموجب القانون 06-22¹⁶، وجواز تمديد دائرة اختصاص المحكمة إلى دائرة اختصاص محاكم أخرى إذا تعلق الأمر بذات الجرائم السالف ذكرها¹⁷.

ومن جملة الترتيبات المتخذة من قبل المشرع الجزائري لمواجهة الجريمة المعلوماتية، استحداث أساليب التحري الخاصة بموجب تعديل قانون الإجراءات الجزائية رقم 06-22، ويقصد بأساليب التحري "تلك العمليات أو الإجراءات والتقنيات التي تستخدمها الضبطية القضائية تحت المراقبة والإشراف المباشر للسلطة القضائية بغية البحث والتحري عن الجرائم الخطيرة، وجمع الأدلة عنها والكشف عن مرتكبيها، وذلك دون علم ورضا الأشخاص المعنيين"، حيث أن هذا النوع من الأساليب لا يخصص بها إلا في الجرائم المحددة على سبيل الحصر، من بينها الجريمة المعلوماتية، والتي تتناسب مع متطلبات الإجرام الحديث، ويمكن إجمال أساليب التحري الخاصة في:

أ- اعتراض المراسلات وتسجيل الأصوات والنقاط الصور: جعل المشرع الجزائري من اعتراض المراسلات وتسجيل الأصوات والنقاط الصور أهم الأساليب المستحدثة للكشف عن الجرائم الإلكترونية، وهي إجراءات تباشر بشكل خفي، وذلك تماشيا مع التقدم العلمي والتكنولوجي المعاصر، لاسيما في مجال الاتصال والهندسة الإلكترونية، مما أفرز أساليب علمية عالية الكفاءة والفعالية أحدثت ثورة في مجال التحريات الجنائية¹⁸. وقد نصّ عليه المشرع في قانون الإجراءات الجزائية في المادة 56 دون تحديد مفهومه وإجراءاته، غير أن المشرع استدرك الأمر بموجب القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية حيث استحدث فصلا كاملا من المواد 65 مكرر 5 إلى المادة 65 مكرر 10، حيث

¹⁴ عدلت بالقانون 04-14 المؤرخ في 10 نوفمبر 2004، ج.ر.ج.ع.ج.ع.71.

¹⁵ أنظر المادة 40 من قانون الإجراءات الجزائية المعدلة بموجب القانون 04-014 المؤرخ في 10 نوفمبر 2004، ج.ر.ج.ع.ج.ع.71.

¹⁶ تنص الفقرة الثالثة من المادة 16 من قانون الإجراءات الجزائية المعدلة بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006، ج.ر.ج.ع.ج.ع.84 على: "غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف يجوز تمديد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني".

¹⁷ أنظر المادة 329 من قانون الإجراءات الجزائية المعدلة بموجب القانون 04-014 المؤرخ في 10 نوفمبر 2004، ج.ر.ج.ع.ج.ع.71.

¹⁸ لتفاصيل أكثر حول هذه النقطة، أنظر، بن عمار مقني، عبد القادر بوراس، التتبع على المكالمات الهاتفية واعتراض المراسلات كآلية للوقاية من جرائم الفساد، الملتقى الوطني حول الآليات القانونية لمكافحة الحقوق، جامعة قاصدي مرباح، ورقلة يومي 02 و03 ديسمبر 2008، ص.14.

نصت المادة 65 مكرر 5 من قانون الإجراءات الجزائية على: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي : -
اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

- وضع الترتيبات التقنية دون موافقة المعنيين من أجل النقاط وتثبيت وبث وتسجيل الكلام المتقوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو النقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

- يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

- تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص، في حالة فتح تحقيق قضائي تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة"، وإذا كان هذا الإجراء فرضه التطور الحاصل للحد من الجرائم الإلكترونية، إلا أنه في المقابل يعتبر انتهاك للخصوصية والحريات الفردية لذلك يتعين ممارسته في إطار القانون.

ب-التسرب: يعتبر التسرب من أهم التقنيات التي استحدثها المشرع الجزائري بالنص عليه في المواد من 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية المعدل والمتمم. ويسمح التسرب أو الاختراق كتقنية من تقنيات التحري الخاصة، لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية ويوهمهم على أنه شريك لهم¹⁹، وفي سبيل ذلك يمكن لضباط الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وذلك بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية²⁰.

¹⁹مراد حسيني، إجراءات التحقيق المستحدثة في قانون الإجراءات الجزائية الجزائري "عملية التسرب، الجزء الأول، الطبعة الأولى، قراءات في المادة الجنائية، دار النشر للمعرفة، 2013، الجزائر، ص.166.

²⁰أمنة أمحمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر العاصمة، 29 مارس 2017، ص.71-72.

رابعاً-مكافحة الجريمة المعلوماتية من خلال القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم الخاصة المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها²¹: تضمنت المادة الأولى من هذا القانون الهدف منه وهو الوقاية من الجريمة المعلوماتية، ليحدّد في المادة الثانية عديد المفاهيم المرتبطة بتكنولوجيا الإعلام والاتصال، ويصبو هذا القانون إلى التمكين من مكافحة الجريمة المعلوماتية عن طريق مجموعة من التدابير متمثلة في تحديد الحالات التي يجوز فيها لسلطات الأمن مراقبة المراسلات الإلكترونية وهي أربع حالات: -الوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب، والجرائم ضدّ أمن الدولة. -عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدّد مؤسسات الدولة والدفاع الوطني أو النظام العام- لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية، دون اللجوء إلى المراقبة الإلكترونية. -في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما تضمن قانون 04-09 إجراءات جديدة تدعم تلك المنصوص عليها في قانون الإجراءات الجزائية ولاسيما المتعلقة بالجرائم المعلوماتية والتي يمكن تلخيصها في ما يلي:

- جواز التفتيش ولو عن بعد للمنظومة المعلوماتية أو جزء منها من طرف الجهات القضائية المختصة وضباط الشرطة القضائية.

- إمكانية تمديد آجال التفتيش بإذن من السلطة القضائية المختصة.

- إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في المنظومة المعلوماتية الموجودة خارج الإقليم الوطني، وذلك طبقاً للاتفاقيات الدولية ومبدأ المعاملة بالمثل طبقاً للمادة الخامسة من القانون 04-09.

خامساً- مكافحة الجريمة المعلوماتية في قانون التأمينات الاجتماعية: إضافة لما سبق قرر المشرع مواجهة الجريمة المعلوماتية كذلك من خلال قانون 08-01 المعدل للقانون 83-11 المتعلق بالتأمينات الاجتماعية²²، حيث أشارت المادة 6 مكرر 1 منه إلى البطاقة الإلكترونية المسلمة للمؤمن له، بينما أشارت المواد من 93 مكرر 2 إلى 6 إلى العقوبات المطبقة على كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية للمؤمن له اجتماعياً في المفتاح

²¹ قانون رقم 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المعلوماتية المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر.ج.ع.ج.ع. 47، الصادرة بتاريخ 16 أوت 2009.

²² قانون رقم 08-01 يتعلق بالتأمينات الاجتماعية المؤرخ في 23 يناير 2008 يتم القانون رقم 83-11 المؤرخ في 2 يوليو 1983 والمتعلق بالتأمينات الاجتماعية، ج.ر.ج.ع.ج.ع. 2، الصادرة بتاريخ 27 يناير 2008.

الإلكتروني²³، كما جرم كل من أعد أو عدل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له، كما جرم المشرع كل من ينسخ أو يضع أو يحوز أو يوزع بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال البطاقة الإلكترونية وغيرها²⁴.

سادسا- مكافحة الجريمة المعلوماتية من خلال القانون المتعلق بالقواعد العامة للبريد والاتصالات: نجد أن المشرع كذلك أشار لمكافحة الجريمة المعلوماتية من خلال القانون 04-18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات²⁵، خاصة من خلال المادة 164 التي نصت على معاقبة كل من ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو ينفي مضمونه أو ينشره أو يستعمله دون ترخيص، وغيرها من المواد التي تضمن فحواها مكافحة الجريمة المعلوماتية المتعلقة بالبريد والاتصالات الإلكترونية²⁶.

المبحث الثاني : الضوابط العملية لمكافحة الجريمة المعلوماتية

إذا كانت الجزائر قد قطعت شوطا لا يستهان به على مستوى النصوص القانونية الهادفة إلى مكافحة الجريمة المعلوماتية، فإن ذلك يستتبع تطبيقا ميدانيا لها، وذلك من خلال إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (المطلب الأول) وهيئات أخرى تابعة للجهاز الأمني بهدف مواجهة الجريمة المعلوماتية (المطلب الثاني) وسنقف فيما يلي على أهمها:

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

استحدثت هذه الهيئة بموجب المادة 13 من القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال السالف الذكر، حيث نصت على: "تتشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته"، وقد أحالت الفقرة الثانية من ذات

²³ تنص المادة 93 مكرر 2 من القانون 01-08 المعدل للقانون 11-83 المعلق بالتأمينات على: "دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 200.000 دج كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة".
²⁴ أنظر المادة 93 مكرر 3 من القانون 01-08 المعدل للقانون 11-83 المعلق بالتأمينات الاجتماعية السالف الذكر.

²⁵ قانون 04-18 المؤرخ في 10 ماي 2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر.ج.ع. 27. الصادرة بتاريخ 13 ماي 2018.

²⁶ أنظر المادة 165 و 166 من القانون 04-18 السالف الذكر.

المادة مسألة تحديد تشكيلة الهيئة وتنظيمها وكيفيات سيرها للتنظيم، وهو ما تضمنه المرسوم الرئاسي رقم 261-15²⁷.

أولاً- طبيعة تشكيل الهيئة ومهامها: طبقاً للمادة الثانية من المرسوم الرئاسي 261-15 تعد الهيئة بمثابة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، يوجد مقرها بالجزائر وضعت لدى الوزير المكلف بالعدل، وعليه فقد تضمنت النصوص تحديد تشكيل الهيئة، وتبيان المهام الموكلة لها، وهو ما سنتناوله تباعاً:

أ- تشكيل الهيئة: وفقاً للمادة السادسة من المرسوم الرئاسي 261-15 تتشكل الهيئة من لجنة مديرة، مديرية عامة، مديرية للمراقبة الوقائية واليقظة الإلكترونية مديرية للتنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية.

- اللجنة المديرة: يرأس اللجنة الوزير المكلف بالعدل، تتشكل من الأعضاء التالية: 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 العليا²⁸، وطبقاً للمادة الثامنة من المرسوم الرئاسي 261-15 تمارس اللجنة المديرة المهام التالية: توجيه عمل الهيئة والإشراف عليه ومراقبته، دراسة كل المسائل المتعلقة باللجوء للمراقبة الوقائية للاتصالات الإلكترونية وضبط برنامج عمل الهيئة، وتحديد شروط وكيفيات تنفيذه، بالإضافة إلى قيام اللجنة بشكل دوري بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة، كما تتولى عملية اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالإضافة إلى دراسة مشروع النظام الداخلي للهيئة وميزانيتها والموافقة عليه دون إغفال دراستها للتقرير السنوي لنشاطات الهيئة والمصادقة عليه.

- المديرية العامة: يتولى إدارتها مدير عام يعين بموجب مرسوم رئاسي وتنتهى مهامه بنفس الطريقة التي عين بها²⁹، وفي إطار المهام المخولة له، على المدير العام العمل على حسن سير الهيئة الوطنية عن طريق ضمان تنفيذ برنامج عملها وتحفيز نشاطات هيكل الهيئة وتنسيقها ومتابعتها

²⁷ مرسوم رئاسي رقم 261-15 المؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر.ج.ع. 53. الصادرة بتاريخ، 08 أكتوبر 2015.

²⁸ المادة السابعة من المرسوم الرئاسي 261-15.

²⁹ تنص المادة التاسعة من المرسوم الرئاسي 261-15 على: " يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي. وتنتهى مهامه حسب الأشكال نفسها".

ومراقبتها، وتحضير اجتماعات اللجنة المديرية، بالإضافة لقيامه بتمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية ولدى القضاء وفي جميع أعمال الحياة المدنية³⁰.

- مديرية المراقبة والوقاية واليقظة الالكترونية: تمارس مديرية المراقبة العديد من المهام تضمنها المرسوم الرئاسي 15-261 ولعل أهمها ما يلي: القيام بتنفيذ عمليات المراقبة والوقاية للاتصالات الالكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بناء على رخصة مكتوبة تمنح من السلطة القضائية وتتم تحت مراقبتها، كما تقوم بإرسال المعلومات المحصل عليها من خلال القيام بالمراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة، مع العمل على تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة، وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم، كما تتولى المديرية أيضا مهمة جمع واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والعمل على تنظيم أو المشاركة في عمليات التوعية حول كيفية استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها، بالإضافة إلى تنفيذ التوجيهات المقدمة إليها من قبل اللجنة المديرية، وتزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مع وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة، والسهر على حسن سيره والحفاظ على الحالة الجيدة لمنشآته وتجهيزاته ووسائله التقنية مع ضرورة تطبيق قواعد الحفاظ على السر في نشاطاتها الممارسة³¹.

- مديرية التنسيق التقني: في سبيل قيام الهيئة بكافة المهام المنوطة بها على أكمل وجه، تكلف مديرية التنسيق التقني بممارسة مهام يمكن إجمالها في: إنجاز الخبرات القضائية في مجال اختصاص الهيئة، وتكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها، وإعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والقيام بمبادرة منها أو بناء على طلب اللجنة المديرية بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها مع ضمان تسيير منظومة الإعلام للهيئة وإدارتها³².

- مركز العمليات التقنية: طبقا للمادة الثالثة عشر من المرسوم الرئاسي 15-261 يتم تزويد مركز العمليات بالمنشآت والتجهيزات والوسائل المادية، وبالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الالكترونية مع العلم أن المركز تابع لمديرية المراقبة الوقائية واليقظة الالكترونية

³⁰ لتفاصيل أكثر حول هذه النقطة، أنظر المادة العاشرة من المرسوم الرئاسي 15-261.

³¹ لتفاصيل أكثر حول هذه النقطة، أنظر المادة الحادية عشر من المرسوم الرئاسي 15-261.

³² لتفاصيل أكثر حول هذه النقطة، أنظر المادة الثانية عشر من المرسوم الرئاسي 15-261.

حيث يتم تشغيله من طرفها، بالإضافة إلى الملحقات الجهوية التي يتم تشغيلها من طرف مديرية المراقبة والوقاية واليقظة الإلكترونية التابعة لها³³.

ب- المهام الموكلة إلى الهيئة: بالنسبة لمهام الهيئة فقد أحالت بخصوصها المادة الرابعة من المرسوم الرئاسي 15-261 إلى المادة 14 من القانون 09-04، حيث تمارس الهيئة العديد من المهام والتي يمكن إجمالها في: اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالإضافة إلى مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها فيما يتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، من خلال جمع المعلومات وإنجاز الخبرات القضائية، مع ضمان المراقبة والوقاية للاتصالات الإلكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص، وتجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية، مع ضرورة العمل على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية، وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم، وتطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بالإضافة إلى المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال³⁴.

ثانيا- طريقة سير الهيئة: طبقا للمادة السادسة عشر من المرسوم الرئاسي 15-261 تجتمع الهيئة بناء على استدعاء من رئيسها أو بناء على طلب أحد أعضائها، إذ تقوم بإعداد نظامها الداخلي والمصادقة عليه وفقا لنص المادة السابعة عشر من المرسوم الرئاسي السالف الذكر، حيث يتم تزويدها بقضاة³⁵، وضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني، ويتم تحديد عددهم بموجب قرارات مشتركة بين وزير العدل والدفاع والداخلية³⁶، وطبقا للمادة الثامنة عشر من المرسوم الرئاسي 15-261 تزود الهيئة بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح

³³ المادة الرابعة عشر من المرسوم الرئاسي 15-261 .

³⁴ لتفاصيل أكثر حول هذه النقطة، أنظر، آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، مداخلة الملتقى الدولي حول "الإجرام السيبراني المفاهيم والتحديات" 11-12 أفريل 2017، جامعة 8 ماي 1945 قالمة، الجزائر، ص. 6-7.

³⁵ المادة 18 فقرة أولى من المرسوم الرئاسي 15-261 السالف الذكر.

³⁶ المادة 18 فقرة ثانية من المرسوم الرئاسي 15-261 السالف الذكر.

العسكرية للاستعلام والأمن والدرك الوطني، كما يمكن لها الاستعانة بأي خبير أو أي شخص يمكن تعيينه في أعمالها شرط التزامهم بالسراية المهني وواجب التحفظ وخضوعهم لإجراءات التأهيل³⁷.

وفي سبيل الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة، تكلف الهيئة بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاض مختص، وذلك طبقاً لنص المادة الحادية والعشرون من المرسوم 15-261.

وفي ذات السياق يمكن للهيئة وضع وحدة مراقبة واحدة أو أكثر تزود بالوسائل والتجهيزات التقنية الضرورية، وتتكون الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط من الشرطة القضائية أو أكثر ينتمي إلى الهيئة³⁸، وطبقاً للمادة 23 من ذات المرسوم الرئاسي لا يمكن أن يشارك في عملية مراقبة الاتصالات الإلكترونية إلا أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة، كما يتخذ مسؤول الوحدة أثناء سير العملية كل التدابير اللازمة بالاتصال مع المسؤولين المعنيين في الهيئة من أجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة، كما تقوم بحفظ المعلومات المستقاة أثناء عملية المراقبة³⁹، حيث يتم تسجيل الاتصالات الإلكترونية التي تكون موضوع مراقبة وتحرر وفق الشروط والأشكال المنصوص عليها قانوناً خاصة في إطار قانون الإجراءات الجزائية، وفي إطار ذلك تسلم التسجيلات والمحركات إلى السلطات القضائية ومصالح الشرطة القضائية المختصة، وتحفظ دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع طبقاً للمادة 25 من المرسوم الرئاسي 15-261، مع العلم أنه يجب عدم استخدام المعطيات والمعلومات التي تستلمها أو تجمعها الهيئة لأية أغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها⁴⁰.

المطلب الثاني: الهيئات التابعة للجهاز الأمني

إضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، هناك هيئات تابعة للجهاز الأمني، مكلفة بالتدخل لمواجهة العملية على المستوى التطبيقي للجرائم المعلوماتية، وتصنف الهيئات التابعة للجهاز الأمني والمكلف بمكافحة الجرائم ذات الصلة إلى نوعين:

³⁷ المادة 19 من المرسوم الرئاسي 15-261 السالف الذكر.

³⁸ المادة 22 من المرسوم الرئاسي 15-261 السالف الذكر.

³⁹ المادة 24 من المرسوم الرئاسي 15-261 السالف الذكر.

⁴⁰ المادة 26 من المرسوم الرئاسي 15-261 السالف الذكر.

أولاً- الهيئات التابعة لسلوك الأمن الوطني: يوجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي:

أ- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.

ب- المخبر الجهوي للشرطة العلمية بقسنطينة.

ت- المخبر الجهوي للشرطة العلمية بوهران.

يتولى كل مخبر سواء المركزي أو الجهوي لولاية قسنطينة أو وهران، مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها⁴¹.

ثانياً- الوحدات التابعة للقيادة العامة للدرك الوطني: إضافة إلى الهيئات التابعة للأمن الوطني، هناك هيئات تابعة للدرك الوطني، حيث تلعب مختلف المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني دوراً هاماً في مجال مكافحة الجريمة المعلوماتية، وتتميز مختلف الفصائل بخبرة وكفاءة عالية في مكافحة الجريمة المعلوماتية⁴²، كما يوجد على المستوى المركزي هيئات تتكفل بمكافحة الجريمة المعلوماتية يمكن إجمالها في:

أ- المعهد الوطني للأدلة الجنائية وعلم الإجرام: أنشأ المعهد بموجب المرسوم الرئاسي 04-183⁴³، ويعتبر هذا المعهد مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلف بإجراء الفحوص العلمية في إطار التحريات الأولية، وإجراء بحوث متعلقة بالكشف عن الإجرام باللجوء إلى التكنولوجيا الدقيقة⁴⁴، ويحتوي على مجموعة من المصالح: مصلحة البصمات، ومصلحة الإعلام الآلي حيث يتم على مستوى هذه المصلحة رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وتفكيك البرامج المعلوماتية⁴⁵.

ب- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني: أنشأ هذا المركز سنة 2008، ويهدف إلى تحليل معطيات وبيانات الجرائم المعلوماتية، وتحديد هوية أصحابها سواء كانوا

⁴¹ لتفاصيل أكثر حول هذه النقطة، أنظر، ربيعي حسين، آليات البحث والتحري في الجرائم المعلوماتية، أطروحة دكتوراه علوم، جامعة باتنة، 2015-2016، ص. 177-178.

⁴² سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، مجلد 30، ع. 03، 2019، ص. 52-53.

⁴³ مرسوم رئاسي 04-183 المؤرخ في 26 يونيو 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، ج.ر.ج.ع.ج.ع. 41 الصادرة بتاريخ 27 يونيو 2004.

⁴⁴ لتفاصيل أكثر حول هذه النقطة، أنظر المادة الرابعة من المرسوم الرئاسي 04-183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني السالف الذكر.

⁴⁵ هوارى عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، جامعة بسكرة، كلية الحقوق، 2016، ص. 12.

ففرادى أو جماعات، والتي قد تستهدف خاصة المؤسسات الرسمية، البنوك وحتى الأفراد، كما يهدف إلى مساعدة باقي الأجهزة الأخرى في أداء مهامها، وخاصة فيما يلي: - ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت. - القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية. - مساعدة الوحدات الإقليمية للدرك الوطني في معاناة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة. - المشاركة في عمليات التحري والتسرب عبر شبكة الإنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية. - المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

وفي هذا الإطار عالج هذا المركز في سنة 2015 ما يقارب 240 قضية متعلقة بالجرائم المعلوماتية، شملت جرائم التهديد، المساس بالنظام العام، جرائم الاختراق، التحرش الجنسي بالقصر وتحريضهم على الفسق والدعارة، إهانة هيئات ورموز وطنية، النصب والاحتيال، الاعتداء على حرمة الحياة الخاصة⁴⁶.

ت- مديرية الأمن العمومي والاستغلال: وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

ث- المصلحة المركزية للتحريات الجنائية: وهي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والاتصال⁴⁷.

وقد استطاعت قيادة الدرك الوطني من خلال ما كشف عنه قسم مكافحة الجرائم الإلكترونية من إحصائيات أنه عالج أكثر من 1100 قضية تتعلق بالاستخدام السيئ للإنترنت والإجرام الإلكتروني خلال سنة 2018، وأشار إلى أن 30 في المائة من هذه الجرائم تتعلق بـ"الابتزاز والتشهير"، و136 قضية خاصة بالقاصرين ما دون سن 18 سنة⁴⁸.

الخاتمة: من خلال ما سبق يتضح أن عالم الجريمة المعلوماتية له خصوصيته التي تميزه بالنظر للبيئة الرقمية التي تحيط بمقومات هذا النوع من الإجرام، وله خطورته التي تصعب عملية الاكتشاف والإثبات، مما أدى بالمجتمع الدولي لإرساء نصوص دولية بهدف مكافحة الجريمة الإلكترونية. وقد سائر المشرع الجزائري في ذلك المجتمع الدولي حيث بادر إلى وضع إستراتيجية شملت استحداث نصوص

⁴⁶ لتفاصيل أكثر، أنظر، عز الدين عز الدين - قيادة الدرك الوطني - الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة 16 - 17 نوفمبر 2015 كلية الحقوق، جامعة بسكرة، ص. 29.

⁴⁷ لتفاصيل أكثر حول هذه النقطة، أنظر، ربيعي حسين، آليات البحث والتحري في الجرائم المعلوماتية، المرجع السابق، ص. 183.

⁴⁸ إحصائيات تم نشرها على الموقع: <https://www.alaraby.co.uk/> تم الإطلاع عليه بتاريخ 12 جويلية 2019.

قانونية خاصة كفيلة بالحد من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من جهة، وتعديل النصوص القانونية السارية المفعول بما يتناسب مع هذا النوع من الجرائم من جهة ثانية، مع إعطاء أهمية عملية لمكافحة الجريمة المعلوماتية عن طريق إرساء أجهزة وهيئات أسندت لها ذات المهمة، خاصة الهيئة الوطنية المكلفة بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، دون إغفال الدور الفعال للجهاز الأمني في هذا المجال، إلا أن ما يمكن الوقوف عليه هو أن النصوص القانونية لوحدها غير كافية لمكافحة الجريمة المعلوماتية، بل لابد بالموازاة مع ذلك القيام بما يلي من توصيات:

- التوعية بالجريمة المعلوماتية، وإقامة الحملات التحسيسية على مستوى مختلف المؤسسات خاصة التربوية منها، وللتقليل كذلك من الجريمة المعلوماتية لابد من تفعيل نظام الأمن المعلوماتي.
- إعطاء الفرص لأصحاب الكفاءات للاستفادة من مهاراتهم وخبراتهم، والاستعانة بها في مجال مكافحة الجريمة المعلوماتية.
- تحسين التكوين المستمر للعناصر المكلفة بمكافحة الجريمة المعلوماتية، من أجل الرفع من الكفاءة لمختلف الفئات من رجال الأمن ومهندسي الإعلام، ورجال القانون.
- تحفيز الملتقيات الوطنية وتبادل الخبرات مع الدول الأخرى في هذا المجال.