جامعة محمد البشير الإبراهيمي برج بوعريريج

كلية الحقوق والعلوم السياسية

جامعة محمد البشير الإبراهيمي برج بوعريريج
كلية الحقوق والعلوم السياسية
المجلس العلمي للكلية
وزارة التعليم العالي والبحث العلمي

الوقاية من الجرائم الإلكترونية

مطبوعة بيداغوجية لمحاضرات

ألقيت على طلبة الثانية ماستر (السداسي الثالث)

تخصص إعلام آلي وأنترنت

إعداد: الدكتورة عمارة زينب

السنة الدراسية 2022/2021

مقدمة:

إن التطور المستمر لكل من تكنولوجيات الإعلام والإتصال التي تمثل قفزة حضارية نوعية في حياة الأفراد والدول، وما نتج عنها في نفس الوقت من انعكاسات سلبية، أفرزتها إساءة استخدام هذا التطور الذي أدى إلى ظهور أنماط مستحدثة من الجرائم أو من خلال إضفاء طبيعة خاصة على الجرائم التقليدية.

حيث تم توظيف المنظومة المعلوماتية والإتصالات الإلكترونية في ارتكاب الجرائم، وأصبح ذلك يشكل هاجسا خطيرا سيما وأن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال تعتبر جرائم عابرة للحدود الوطنية، وهو ما جعل المجتمع الدولي يعمل على إيجاد حلول سريعة لمكافحتها والحد من انتشارها، وذلك من خلال وضع نصوص قانونية دولية وسن تشريعات وطنية تتلاءم مع الإلتزامات الدولية، وهو ما سعت إليه الجزائر على غرار الدول الأخرى، ولعل من أهم النصوص الدولية اتفاقية بودابست المنعقدة في 2001/01/23 تحت إشراف المجلس الأوروبي، وذلك للحد من مخاطر الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ومواجهة مرتكبيها.

والمشرع الجزائري قام بسد الفراغ القانوني في مواجهة هذا النوع من الإجرام من خلال وضع منظومة قانونية متكاملة، ترتكز أساسا على كل من قانون العقوبات وقانون الإجراءات الجزائية، وإفراد قانون خاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، وانتهج في ذلك السياسة الجزائية الوقائية إلى جانب السياسة التجريمية والعقابية والإجرائية، نظرا لأن هذا النوع من الإجرام الذي يرتكب في بيئة غير عادية في العالم الرقمي الإفتراضي الذي لا تحده حدود، ولا تحكمه جغرافيا، كما أن مرتكبي هذه الجرائم جناة محترفين الكترونيا يسعون إلى إخفاء ممارساتهم بكل احترافية، وهو ما يستوجب وضع قانون خاص نص على وضع آليات وقائية وردعية تعمل على الحد من انتشار هذا النوع من الإجرام والوقاية منها ومكافحتها بشكل فعال، ذلك أن المكافحة لوحدها لا تكفي

لوحدها لدرء خطر الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، بل يستلزم الإعتماد على الأسلوب الوقائي، سيما وأن السياسة الجزائية الحديثة تقوم على الاستراتيجية الشاملة للنشاط في المادة الجزائية وتتبع هدفا يتطابق مع التوجهات الكبرى للدولة، تهدف من خلاله مكافحة الإجرام بكل صوره وتحديد طرق الوقاية منه، والجرائم الإلكترونية أو الجرائم المتصلة بتكنولوجيات الإعلام والإتصال تخضع كغيرها من الجرائم إلى كافة الإجراءات والتدابير والمبادئ والأهداف التي تسعى الدولة إلى تكريسها وتجسيدها على أرض الواقع أملا في تحقيق عدالة جزائية، انطلاقا من رسم سياسة جزائية قائمة على استراتيجية متكاملة واضحة المعالم والأهداف بأبعادها السياسية والإجتماعية والإقتصادية والصحية والأمنية والثقافية، التي تعتمد على تفعيل تشريعات الدولة من خلال إشراك مكونات المجتمع في مواجهة الإجرام السيبيراني.

ويتمثل الهدف من دراسة مقياس الوقاية من الجرائم الإلكترونية أو الجرائم المتصلة بتكنولوجيا الإعلام والإتصال في التعرف على القواعد المطبقة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال قبل وقووعها، والإجراءات والآليات المؤسساتية المعمول بها، وسبل التعاون الدولي والمساعدة القضائية في هذا المجال، وعلى هذا الأساس نطرح الإشكالية التالية: **كيف واجه المشرع الجزائري الجرائم المتصلة بتكنولوجيات الإعلام والإتصال لا سيما من خلال انتهاج السياسة الوقائية؟**

وتبعا لما سبق سيتم تقسيم هذه الدراسة إلى ثلاثة مباحث، نخصص المبحث الأول لدراسة الأهداف ومجال التطبيق، والمبحث الثاني نخصصه لدراسة إجراءات وضمانات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وأما المبحث الثالث فسنتاول فيه الآليات الوطنية والتعاون الدولي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

المبحث الأول:

الأهداف ومجال التطبيق:

لتحديد نطاق ودواعي توجه المشرع الجزائري نحو الإعتماد على الأسلوب الوقائي في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال سيتم التطرق في هذا المبحث إلى المواجهة التشريعية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المطلب الأول، وإلى مفهوم الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في المطلب الثاني.

المطلب الأول:

المواجهة التشريعية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال

لقد واجه المشرع الجزائري الجرائم المتصلة بتكنولوجيات الإعلام والإتصال من خلال الإعتماد على أسلوب المكافحة من جهة إلى جانب أسلوب الوقاية من الجهة الأخرى، وهو ما تجلى في التعديلات المختلفة لقانون العقوبات وقانون الإجراءات الجزائية واستحداث قانون خاص للوقاية والمكافحة، بهدف الحيلولة دون انتشار هذه الجرائم الخطرة، وردع مرتكبيها، وسيتم توضيح ذلك فيما يلي:

الفرع الأول: مظاهر المكافحة والوقاية في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

إن المشرع الجزائري اعتمد على المكافحة من خلال انتهاج سياسة التجريم والعقاب إلى جانب السياسة الإجرائية في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، كما انتهج الأسلوب الوقائي وهو ما يظهر من خلال مايلي:

أولا: مظاهر مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

يقصد بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال مختلف النصوص الجزائية التي سنتها الدولة التي تبين أنماط السلوك والصور التي تعد جرائم، وتحدد ما يفترض لها من عقوبات، وكذلك مجموعة الإجراءات التي تستخدم في الكشف عن الجريمة وضبطها وجمع الأدلة عنها ومتابعة الجناة، والتحقيق معهم، وتنفيذ الأحكام ضدهم[1]، وتظهر مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في تجريم ما سماه المشرع" المساس بأنظمة المعالجة الآلية للمعطيات "، وهي الجرائم التي أدرجها المشرع الجزائري من خلال تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 2004/11/10، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات[2]، الذي أفرد له القسم السابع مكرر منه، وذلك في المواد 394 مكرر إلى 394 مكرر7، والذي تم تعديله بموجب القانون رقم 06-23[3]، ثم أضاف المادة 394 مكرر 8 بموجب القانون رقم 16-02 التي نصت على " دون الإحلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاثة سنوات وبغرامة من10.000 إلى 2.000.000 دج، أو بإحدى هاتين العقوبتين فقط، مقدم خدمات الإنترنت بمفهوم المادة 02 من القانون 09-04 المؤرخ في 14 شعبان هام 1430 الموافق لـ 5 غشت سنة 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الذي لا يقوم رغم إعذاره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو

---

[1]- رمسيس بهنام، علم الوقاية، التقويم والأسلوب الأمثل لمكافحة الإجرام، الإسكندرية، منشأة المعارف، 1986،ص187.

[2] القانون 04-15 المؤرخ في 10نوفمبر 2004، المعدل والمتمم للأمر رقم 66 -156 المؤرخ في 08/يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 المؤرخة في 10/نوفمبر/2004.

[3]- القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66 -156 المؤرخ في 08/يونيو 966 المتضمن قانون العقوبات، الجريدة الرسمية عدد84 المؤرخة في 24 ديسمبر2006.

حكم قضائي يلزمه بذلك"[1]، **كما أن المشرع أيضا نص** في المادة 87 مكرر 11 و87 مكرر 12 على الجرائم الإرهابية المتصلة بتكنولوجيات الإعلام والإتصال.

وتظهر أيضا في قانون الإجراءات الجزائية لا سيما من خلال تعديله بالقانون 06-22[2]، الذي استحدث في الفصل الرابع من الباب الثاني اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بموجب المواد من 65 مكرر 5إلى 65 مكرر 11، وهي أساليب التحري والبحث والتحقيق وهي تلك العمليات والإجراءات أو التقنيات التي تستخدمها الضبطية القضائية تحت مراقبة وإشراف السلطة القضائية بغية البحث والتحري عن الجرائم الخطيرة، والتي من أهمها الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وجمع الأدلة عنها والكشف عن مرتكبيها، وذلك دون علم ورضا الأشخاص المعنيين[3].

ولم يكتف المشرع فقط بذلك، بل تدخل واستحدث قانونا مستقلا وهو القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[4]، الذي يتضمن أحكاما قانونية ردعية تجريمية وعقابية وأحكام إجرائية، لا سيما إجراءات البحث والتحري والتحقيق باستخدام المراقبة الإلكترونية للاتصالات والتفتيش في النظم المعلوماتية باعتبارها إجراءات مكافحة التي تسمح للمحقق بالبحث والتحري والتحقيق للكشف عن المجرمين وتتبع الجريمة وحركاتهم لتقديم الأدلة اللازمة لإدانة المتهم أو تبرئته، ثم أصدر المشرع الجزائري المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم

---

[1] – القانون رقم 16-02 المؤرخ في 19 يونيو 2016 المعدل والمتمم للأمر رقم 66 -156 المؤرخ في 08/يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد37 المؤرخة في 22 يونيو 2016.

[2]– القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد84 المؤرخة في 24 ديسمبر 2006.

[3] – عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، الجزائر، دار بلقيس للنشر، 2015، ص95.

[4]– القانون 09-04 المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد47، المؤرخة في 16 غشت 2009.

وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[1]، التي لها دور فعال في المكافحة لا سيما وأنها تتشكل من ضبطية قضائية تقنية ومتخصصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، كما تم إصدار المرسوم الرئاسي 19-172 الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها تنظيمها وكيفيات سيرها[2]، ثم المرسوم الرئاسي رقم 21-439، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[3].

كما أنه استحدث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الباب السادس بموجب الأمر رقم 21-11[4]المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، تعزيزا لفكرة التخصص القضائي في مكافحة الجريمة الخطرة التي تبلورت أساسا في التشريع الجزائي بعد إنشاء جهات قضائية ذات إختصاص إقليمي موسع، الأقطاب الجزائية المتخصصة طبقا للمواد 37، 40 و329 قانون الإجراءات الجزائية كجهات جزائية متخصصة، تعززت بإنشاء قطب جزائي وطني متخصص في

---

[1] – المرسوم الرئاسي 15-261 المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد53 المؤرخة في 8 أكتوبر 2015.

[2]– المرسوم الرئاسي 19-172 المؤرخ في 06 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها تنظيمها وكيفيات سيرها، الجريدة الرسمية العدد37 المؤرخة في 09 يونيو 2019.

[3]– المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/07، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، الجريدة الرسمية العدد 86 المؤرخة في 11 نوفمبر 2021.

[4] – الأمر 21-11 المؤرخ في 25 أوت 2021، المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 65 المؤرخة في 26 غشت 2021.

الجرائم الإقتصادية والمالية بموجب الأمر 20-04[1] المعدل والمتمم لقانون الإجراءات الجزائية.

ثانيا: مظاهر الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

إن المشرع الوطني لم يكتف بوضع نصوص قانونية ردعية تجريمية وعقابية وأحكام إجرائية، بل اتجه نحو إعتماد السياسة الجزائية الوقائية وتبنى أسلوب الوقاية الذي يظهر أيضا في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال نظرا لخصوصية هذا النوع من الإجرام لارتباطه بسائر أشكال الجريمة خصوصا جرائم الإرهاب والجريمة المنظمة عبر الحدود الوطنية والفساد، ذلك أن سياسة المكافحة لوحدها لا تكفي، وإنما يتوجب الإعتماد على السياسة الجزائية الوقائية تماشيا مع توجهات السياسة الجزائية الحديثة.

يظهر توجه المشرع الجزائري نحو اعتماد الأسلوب الوقائي في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في العديد من النصوص القانونية سواء في القانون 09-04 والمرسوم الرئاسي رقم 21 -439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، سواء بصفة صريحة أو بصفة ضمنية.

إذ نصت المادة الأولى من القانون 09-04 على أن هذا القانون يهدف إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ونصت المادة 4 منه في الفقرة أ و ب على " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية:

---

[1] - الأمر 20-04 المؤرخ في 11 غشت 2020، المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 51 المؤرخة في 31 غشت 2020.

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

كما نصت المادة 12 من القانون على بعض الإلتزامات الخاصة بمقدمي خدمة الإنترنت التي لها هدف وقائي من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وهي النصوص الضمنية التي تشير إلى انتهاج الأسلوب الوقائي إذ نصت على التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، وكذلك وضع الترتيبات التنقنية التي تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

وبالرجوع للمادة 13 من القانون 09-04 نجدها نصت على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته التي تتولى عدة مهام لا سيما تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، وبالرجوع للمرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته الذي نصت اغلب نصوصه على الوقاية بصفة صريحة، ونذكر على سبيل المثال ما نصت عليه المادة 04 منه التي نصت على " ..... تكلف الهيئة على الخصوص بما يأتي:

تحديد الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ضمان المراقبة الوقائية للاتصالات الإلكترونية، تحت سلطة القاضي المختص،

قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة"، كما أن المادة 11 منه على أن المديرية العامة للهيئة تضم مديرية المراقبة الوقائية واليقضة الإلكترونية التي تكلف طبقا للمادة 14 منه بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية لا سيما من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

الفرع الثاني: مبررات الإعتماد على الوقاية والمكافحة في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

إن المشرع الوطني وضع نصوص قانونية ردعية تجريمية وعقابية وأحكام إجرائية لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ولم يكتف بذلك بل اتجه نحو السياسة الجزائية الوقائية واعتمد على أسلوب الوقاية، وهو ما تجلى أساسا في القانون 09-04 والمرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، نظرا لخصوصية هذا لنوع من الإجرام لارتباطه بسائر أشكال الجريمة خصوصا جرائم الإرهاب والجريمة المنظمة عبر الحدود الوطنية والفساد، ذلك أن سياسة المكافحة لوحدها لا تكفي، وإنما يتوجب الإعتماد على السياسة الجزائية الوقائية تماشيا مع توجهات السياسة الجزائية الحديثة.

حيث جاء في عرض أسباب القانون 04-15 المعدل والمتمم لقانون العقوبات، " إن التقدم التكنولوجي وانتشار وسائل الإتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام مما دفع بالكثير من الدول إلى النص على معاقبتها وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات وسوف

يمكن لا محالة من مواجهة بعض أشكال الإجرام "[1]، كما أنه جاء في ذكر أهداف القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها " نظرا للتقدم الذي تعرفه العديد من الدول في مجال مواجهة هذا النوع من الجرائم وبهدف تكييف منظومتنا التشريعية مع هذه التحولات وكذا الإتفاقيات الدولية التي صادقت عليها الجزائر ولتكريس إطار قانوني أكثر ملاءمة وانسجاما مع خصوصية هذه الجريمة وخطورتها جاء مشروع هذا القانون ليهدف إلى :

1- تعزيز الحماية الجزائية للأنظمة المعلوماتية التي أقرتها الأحكام الواردة في القانون 04-15 المؤرخ في 2004/11/10 المعدل والمتمم لقانون العقوبات.

2- وضع إطار قانوني أكثر ملاءمة.

3- جعل المتعاملين في الإتصالات السلكية واللاسلكية شركاء في مواجهة هذا النوع من الإجرام"[2].

إن خصوصية الجرائم المتصلة بتكنولوجيات الإعلام والإتصال هي التي جعلت المشرع الجزائري يتجه نحو الإعتماد على الأسلوب الوقائي في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ذلك أنها جرائم تهدد المجتمع بمخاطر وخسائر جمة سياسية وإقتصادية واجتماعية ومؤسسات الدولة، فهي تلحق بالأفراد والمؤسسات خسائر فادحة، إذ تستهدف الإعتداء على أنظمة المعطيات المعلوماتية والإتصالات الإلكترونية سيما وأن النظام المؤسساتي الحالي يعتمد على الرقمنة في جميع المجالات بسبب الثورة المعلوماتية والتحولات الإقتصادية واستخدام النظم المعلوماتية في عمليات التحكم والإدارة والخدمات الإلكترونية والعمليات المصرفية الإلكترونية، والنقود الإلكترونية. والإدارة الإلكترونية وحتى

---

[1]- الفترة التشريعية الخامسة، الدورة العادية الخامسة، الجلسة العلنية المنعقدة يوم الثلاثاء 21 سبتمبر 2004، ج ر م، السنة الثالثة 122، ص 6.

[2] - الفترة التشريعية السادسة، الدورة العادية الرابعة، الجلسة العلنية المنعقدة يوم السبت 27 يونيو 2009، ج ر م، السنة الثالثة، رقم 122، ص 5.

التقاضي الإلكتروني، فتطال المعلومات الحيوية ورؤوس الأموال، والحياة الخاصة للأفراد، والنظام الإقتصادي والمالي، وأمن الدولة، أو يتم الإستعانة بوسائل تكنولوجيا الإعلام والإتصال لارتكاب الجرائم التقليدية في العالم الإفتراضي، باعتبارها تستهدف المعطيات بدلالتها التقنية الواسعة (البيانات والمعلومات والبرامج بكافة أنواعها المخزنة والمنقولة عبر شبكات المعلومات، إذ يستعين المجرمون بالمنظومة المعلوماتية أو نظم الإتصالات الإلكترونية في ارتكاب جرائمهم ، لما تتصف تلك الوسائل من دقة بالغة في الوصول إلى النتائج الجرمية المرجوة، إذ أصبحت ترتكب عن طريق الهواتف النقالة لاسيما الهواتف الذكية المزودة بتكنولوجيات فائقة الجودة، وكذلك الوسائط الإلكترونية، والتي يمكن نقل وتخزين المعطيات من جهاز لآخر، مما يجعلها عرضة للسرقة والإتلاف بكل سهولة، كما أن آثارها تظهر في عالم غير مرئي، مما يسهل محو الأدلة والتلاعب فيها، لأنها لا تترك آثارا خارجية مادية ملموسة، فهي أدلة رقمية معنوية، كما يتم فيه نقل المعلومات بواسطة النبضات الإلكترونية، وترتكب الجرائم في الخفاء وعن بعد، فلا يظهر الفاعل على مسرح الجريمة، الذي أصبح معنويا، يتمم الإجرام فيه عن بعد، وبسرعة، وتتباعد المسافات بين المجرم والضحية، وهذه المسافات لاتقف عند حدود الدولة الواحدة، إذ استطاعت شبكة الانترنت إزالة الحدود الجغرافية بين الدول، بعد أن أصبحت متاحة لجميع الأشخاص، كما أن المجرمين يرتكبون إجرامهم بهدوء ، ويتميزون بمستوى معرفي ومعلوماتي يعتمدون على الذكاء والمهارات في ارتكاب الجريمة، كما أن الإرهاب الإلكتروني غزا العالم بقوة لا سيما في المرحلة الأخيرة مما يهدد الأمن الوطني والدولي[1]، كما أن متطلبات تحقيق الأمن المعلوماتي تتطلب الإعتماد على أسلوب الوقاية، وهو يعد أولوية من الأولويات التي تعتمد عليها استراتيجية حماية المؤسسات والأفراد، لتحقيق حماية أمنية ضد الإختراقات التي تطال

---

[1]- نهلا عبد القادر المومني ، الجرائم المعلوماتية، الأردن، عمان، دار الثقافة للنشر والتوزيع، ط1، 2008، ص 52-53،

-Anne BRISSET-GIUSTINIANI, aspects juridiques de l'émergence d une sécurité européenne des réseaux et des systèmes d'information, mémoire DESS Droit de l internet –administration –entreprise, université panthéon Sorbonne, paris1,p 25, disponible sur www.univ-paris1.fr/..../2004_sept_ok_Brisset_Giustnani_version_....

الأنظمة المعلوماتية، من خلال الأدوات التي تتحكم في تنظيم العلاقات والإتصالات دون التأثير على قدرة مستخدمي هذا النظام على الأداء، أو إعاقة عملهم من حيث الكفاءة والتوقيت، إذ تحد منها وحتى ولو تم الإختراق فإنه يرهق القائم به، ويجعله يستغرق وقتا طويلا ، ويسهل اكتشافه قبل النجاح فيه[1]، ونظرا للطبيعة الخاصة للجريمة ولخصوصيتها سيما وأنها تتميز بانها جريمة عابرة للحدود الوطنية، ولأسلوب ارتكابها، وصعوبة اكتشافها ونسبتها لشخص معين، وصعوبة اثباتها، ولكونها جريمة منظمة، وتشكل في حد ذاتها إقتصادا موازيا[2]، مما يفرض وضع تدابير وإجراءات مخطط لها، تتخذ للحيلولة دون وقوع هذا النوع من الإجرام أصلا، الذي يتوقع حدوثه، بقصد إعاقته جزئيا أو كليا[3]، والحد من أضراره، وتطوراته وآثاره السلبية على الدولة، من منطلق أن الوقاية خير العلاج، كل ذلك لتحقيق مواجهة فعالة والتصدي للإجرام الإلكتروني، واحتمالية ارتكابه، من خلال اعتماد أساليب وقائية تعتمد على الإحاطة بعوامل الخطورة الإجرامية وايجاد سبل إعاقتها من خلال إعتماد سياسة وقائية أولية، تكون قبل ارتكاب الجريمة المتصلة بتكنولوجيات الإعلام والإتصال، ووقاية بعدية تكون لاحقة لها بعد ارتكابها[4]، وعلى هذا الأساس اتجه المشرع نحو السياسة الجزائية الوقائية واعتمد على أسلوب الوقاية الذي يظهر أساسا من القانون 09-04 والمرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

المطلب الثاني:

---

[1] – طارق ابراهيم الدسوقي عطية، الامن المعلوماتي (النظام القانوني للحماية المعلوماتية)، مصر، الاسكندرية، دار الجامعة الجديدة للنشر، 2009، ص 515.

[2] -Mohamed CHAWKI, Combattre la cybercriminalité, France, Edition de Saint Amans,2008, p 51.

[3] – مصطفى سويف، المخدرات والمجتمع، نظرة تكاملية، الكويت، سلسلة عالم المعرفة، رقم 2050، المجلس الوطني للثقافة والفنون، 1996، ص 155.

[4] – احسن طالب، الوقاية من الجريمة، لبنان، بيروت، دار الطليعة للطباعة والنشر، الطبعة الأولى، 2001، ص 8-12.

مفهوم الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

لتحديد مفهوم الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال يتم التطرق إلى تعريف الوقاية من الجريمة في القانون، ثم إلى تعريف الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ثم التوصل إلى تحديد المفهوم الإجرائي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، سيما وأن المشرع لم يعط تعريفا لها، وسيتم توضيح ذلك فيما يلي:

الفرع الأول: التعريف بالوقاية من الجريمة :

إن الوقاية من الجريمة من المفاهيم الحديثة التي يشوبها الكثير من سوء الفهم، وفي هذا الإطار يذهب الباحث البريطاني دانيل جيلينغ إلى أن "مفهوم الوقاية من الجريمة حيوان صعب الترويض"، وفي هذا القول إشارة واضحة إلى صعوبة السيطرة على هذا المفهوم، كما يذهب باحث آخر Brantingham إلى القول" ربما يكون هذا المفهوم الأكثر استعمالا، لكنه أيضا الأقل فهما"[1]، مما يلاحظ عدم اتفاق العلماء والباحثين على تعريف موحد لهذا المفهوم في كل زمان ومكان، ولتعريف الوقاية من الجريمة يتعين التطرق لما يلي:

تعرف الوقاية في الإصطلاح القانوني بأنها " مجموع التدابير والتعليمات التي يكون هدفها منع تحقق الطارئ أو أن تحد منه على الأقل، أو تحد من حصول ضرر أو القيام بأعمال ضارة[2]، إذ أن الوقاية تسبق وقوع الجريمة، وهي مجموعة التدابير التي تواجه الذين يعبرون بسلوكهم عن تضاد مع معايير وقيم المجتمع، فهي تتميز عن المكافحة التي تعتبر مجموعة من الإجراءات المستخدمة في الكشف عن الجريمة وضبطها، وجمع الأدلة عنها، ومتابعة الجناة، والتحقيق معهم، وتنفيذ الأحكام ضدهم، وتتميز عن المنع الذي هو عدم الوقوع في ارتكاب جريمة سبق الوقوع فيها، أي الحيلولة دون العود للجريمة أي علاج المجرمين يتجلى في اتخاذ الأساليب الإصلاحية من عقوبات وتدابير احترازية في المؤسسات العقابية أو

---

[1]– أحسن طالب، المرجع السابق، ص 12.

[2] – جيرار كورنو، معجم المصطلحات القانونية، ترجمة منصور القاضي، المؤسسة الجامعية للدراسات والنشر، الطبعة الأولى، 1998، ص 1808.

خارجها لإعادة تأهيل المحكومين بها أو المفروضة عليهم كأفراد صالحين اجتماعيا، وتتميز عن الحماية التي هي درجة من درجات الوقاية ولكنها تمثل خط دفاع متأخر لما هو قادم نحو الكائن ويشكل ضررا يوشك أن يقع أو خطرا، فتقف الأسباب الكفيلة لصده بصورة مباشرة، أما الوقاية بالمفهوم الضيق، فهي خط الدفاع الأول باتخاذها الأسباب بصورة مباشرة أو غير مباشرة لمنع ذلك الخطر أو ذلك الضرر، أي بمنع مسبباته[1].

وتعرف الجريمة بأنها كل فعل أو امتناع عن فعل صادر عن شخص مسؤول ينص عليه القانون ويقرر له عقابا جزائيا[2]، كما تعرف بأنها عبارة عن سلوك غير مشروع صادر عن إرادة إجرامية يشكل اعتداء وانتهاك لحق أو مصلحة من المصالح أو الحقوق المحمية جزائيا، يرتب القانون عليها عقوبة أو تدبير احترازي[3].

وانطلاقا مما سبق سيتم التطرق إلى التعريف المركب للوقاية من الجريمة في القانون الوضعي، ولقد اختلف العلماء والباحثون فيما يتعلق بمفهوم الوقاية من الجريمة ولم يضعوا تعريفا موحدا في كل زمان ومكان، إذ يعرف جانب منهم، الوقاية من الجريمة بأنها كل الإجراءات التي ينبغي اتخاذها للحيلولة دون ظهور الشخصية الإجرامية بين أفراد المجتمع وذلك بمنع أسبابها والعوامل التي تؤدي غلى وقوعها، وتقع مسؤولية الوقاية على جميع المؤسسات الإجتماعية في الدولة سواء التربوية أو الإعلامية أو غيرها مع التنسيق والتعاون مع الأجهزة المتخصصة[4].

وتعرف أيضا بأنها " اللجوء إلى اتخاذ كل السبل الكفيلة لمنع الجريمة قبل وقوعها بإزالة كل الأسباب التي تؤدي إلى ارتكاب الجرم سواء كان السبب فرديا أو اجتماعيا أو تقتضي

---

[1] – محجوب حسن سعد، الشرطة ومنع الجريمة، الرياض، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، 2001، ص 30، ورمسيس بهنام، المرجع السابق، ص 187.

[2]– محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي، القاهرة، دار الفكر العربي، 1998، ص 20.

[3] –نبيه صالح، دراسة في علمي الإجرام والعقاب، عمان، دار العليمة الدولية، ط1، 2003، ص 15.

[4]– أحمد حويتي، دور البحث العلمي في الوقاية من الجريمة والإنحراف، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، ط1، 2001، ص 11.

علاجا للخصائص البدنية والعقلية والوجدانية للفرد طفلا أو بالغا"، أي مختلف الجهود التي تقوم بها الشرطة والجمهور والمؤسسات مما يجعل ارتكاب الجريمة أمرا شاقا وعسيرا، وكل ما تقوم به الدولة والأفراد بمختلف أطياف المجتمع للحد من الجريمة ومحاربتها قبل وقوعها فإنها من قبيل الأساليب الوقائية التي تقي الأفراد من الوقوع في الجرائم[1]، أي ان المجتمع لا ينتظر حدوث الأفعال الإجرامية حتى يتحرك لمكافحتها أو محاربتها، بل يهدف إلى الحيلولة دون ظهور الشروط والظروف التي تؤدي أو قد تؤدي إلى وقوعها أصلا، وذلك لدرء الجريمة قبل حدوثها[2]، وهذا التعريف هو التعريف الضيق للوقاية من الجريمة.

وهناك جانب آخر من الباحثين يربط مفهوم الوقاية من الجريمة بوجود مخططات ميدانية معدة لهذا الغرض ومرتبطة بهذا الميدان باعتبارها اي فعل مخطط نقوم به تحسبا لظهور مشكلة معينة، أو مضاعفات لمشكلة كانت قائمة أصلا، وذلك بغرض الإعاقة الجزئية أو الكاملة للمشكلة، أو لمضاعفاتها[3]، وهي كل عمل يؤدي إلى التقليل أو التخفيف من معدلات الجريمة[4]، إذ يتضح أن مفهوم الوقاية من الجريمة ينقسم إلى قسمين أساسيين، المفهوم الشمولي الواسع، والمفهوم الجزئي المحدد الضيق.

المفهوم الشمولي هو ذلك المفهوم الذي لا يفرق بين الوقاية والمكافحة والعلاج، وتعتمد على التدابير الردعية، والعقوبة في مجال الوقاية من الجريمة، لأن العقوبات والإجراءات لا تهدف إلى الردع فقط وإنما الوقاية من العود للجريمة على المستوى الفردي، وعلى المستوى الجماعي تعتمد على مجمل التدابير والإجراءات المجتمعية، فهي تشمل مجمل الإجراءات التي يتخذها المجتمع والدولة للمواجهة والمكافحة والعلاج والدفاع ضد الجريمة والانحراف

---

[1]– عبد الله العزيز اليوسف، المفهوم الحديث للوقاية من الجريمة والإنحراف، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، ط1، 2003، ص10.

[2]– احسن طالب، المرجع السابق، ص 9.

[3] – مصطفى سويف، المرجع السابق، ص 155.

[4] - Irvin waller, "Crime prevention between theory and practice", paper presented at International crime prevention colloque, abu dhabi,1996.

على المستوى الفردي أو الجماعي[1]، ويقصد به مجموعة الإجراءات الوقائية الأولية التي تهدف إلى الحيلولة دون وقوع الجريمة أصلا من جهة ومجموعة الإجراءات الوقائية اللاحقة أثناء ارتكاب الجريمة أو بعدها لوقف وقوع الجريمة والتصدي لها وعدم تكرارها مستقبلا من جهة أخرى[2].

ومن الملاحظ أن علماء العقاب والإجرام في ركزوا على مواجهة الجريمة بعد وقوعها، ولم يهتموا بالبعد الوقائي القبلي، وإنما البعد الوقائي البعدي أي معالجة أشخاص أصبحوا مجرمين، كما أن غالبية الفقه القانوني لا يميز بين التدابير الإحترازية والتدابير الوقائية كنظام قائم بذاته، لكن غالبية الفقه انصب اهتمامهم على الوقاية من أشخاص بعينهم وليس الوقاية من الجريمة بذاتها، رغم اتفاقهم على أن الوقاية تعني التعامل مع الجريمة قبل وقوعها، ومن الملاحظ أيضا أن وضع تعريف دقيق للوقاية يعتبر أمرا صعبا، لذلك تعددت التعريفات، وما يمكن قوله هو اتخذ كافة التدابير الإحتياطية اللازمة من قبل الجهات او المؤسسات للحيلولة دون قيام الشخصية الإجرامية أو ارتكاب الجريمة أصلا، والإتجاه منذ البداية إلى اقتلاع جذور الجريمة أو التصدي إلى الأسباب والعوامل التي تؤدي إلى ارتكابها، واتخاذ مجموعة الإجراءات الوقائية اللاحقة أثناء ارتكاب الجريمة أو بعدها لوقف وقوع الجريمة والتصدي لها وعدم تكرارها مستقبلا.

ولم يعرف التشريع الجزائري الوقاية وإنما اكتفى فقط بوضع قواعد خاصة للوقاية في العديد من النصوص الجزائية لا سيما ما تعلق بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال وهو ما يظهر في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

الفرع الثاني: التعريف بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

---

[1] -احسن طالب، المرجع السابق، ص 13.

[2]- رمسيس بهنام، الإجرام والعقاب " علم الإجرام وعلم الوقاية والتقويم"، مصر، الإسكندرية، منشأة المعارف، 1978، ص235.

لقد اختلفت وتعددت تسميات الجرائم المتصلة بتكنولوجيات الإعلام والإتصال عند الفقه، إذ يطلق عليها مصطلح الجريمة المعلوماتية، وجرائم الكمبيوتر، والجرائم الإلكترونية، وجرائم الحاسوب والانترنت، وجرائم التقنية العالية، وجرائم الهاكرز والإختراق، والجرائم السيبيرانية، والجرائم الرقمية، إلا أن المشرع الجزائري استعمل للدلالة على هذا النوع من الإجرام سواء في قانون العقوبات أو القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وكذا الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

ويعرف الفقه الجريمة المعلوماتية بالتعريف الضيق وبالتعريف الواسع، ومن التعريفات الضيقة ماجاء به الفقيه MERWE حيث يعرفها بأنها " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"[1]، ويرى الأستاذ Trédman أن الجريمة المعلوماتية تشمل " أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعطيات"[2]، وهناك من عرفها بأنها " كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي، والتي تحول طريقه"[3]، أو هي " جرائم يكون متطلبا لاقترافها أن يتوافر لدى الفاعل معرفة بتقنية الحاسب"[4].

ويعرف جانب من الفقه الجريمة المعلوماتية بالنظر إلى نتيجة الإعتداء، إذ يرى الأستاذ Mass أن المقصود بالجريمة المعلوماتية يتمثل " بالإعتداءات القانونية التي ترتكب

---

[1] - MERWE Vander, « computer crimes and other crimes against information technology in south africa », R.I.D.P, 1993, p 554. ، مشار إليه لدى د/ هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية (دراسة مقارنة) مصر، دار النهضة العربية، ط1، 2000، ص 13.

[2] – K. Trédmann, Fraud et autres délits d' affaire commis a l'aide d'ordinateurs électroniques, rev dr.pén.crim, 1984, p 612 ، مشارإليه لدى د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مصر، دار النهضة العربية، ط1، 1998، ص 6.

[3] – هشام رستم، "جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة"، بحث مقدم إلى اللجنة العلمية لإعداد التقرير الوطني المصري لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين، جامعة أسيوط، مجلة الدراسات القانونية، العدد 17، 1995، ص 107.

[4] – المرجع نفسه، ص 108.

بواسطة المعلوماتية بغرض تحقيق ربح"[1]، ويرى الأستاذ Parker أن الجريمة المعلوماتية هي " كل فعل إجرامي متعمد، أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل"[2].

ويلاحظ من هذه التعريفات أنها قاصرة على الإحاطة بأوجه ظاهرة الإجرام المعلوماتي، إذ ركز بعض الفقهاء على موضوع الجريمة، وركز البعض الآخر على وسيلة ارتكابها، بينما ركز آخرون على فاعل الجريمة.

ويرى جانب آخر من الفقه أن الجريمة المعلوماتية قد تقع على الحاسب الآلي بشقيه المادي HARDWAR والمعنوي SOFTWARE ممثلا بالكيان المنطقي LOGICAL بالإعتداء على البيانات المخزنة والمتبادلة بين الحاسب الآلي وشبكاته الخاصة والعامة عبر خطوط قنوات الإتصال، وهو التعريف التقني الفني[3].

ولقد حاول بعض الفقه إعطاء تعريف واسع لتفادي أوجه القصور التي شابت التعريفات الضيقة في التصدي لظاهرة الإجرام المعلوماتي، فعرفها بعض الفقه بأنها " كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها"[4] ، ويرى البعض الآخر أنها " كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، ويهدف إلى الإعتداء على الأموال المادية أو المعنوية"[5]، ويرى بعض الفقه أنها " سوء استخدام الحاسب أو الجريمة أو جريمة الحاسب تسهل استخدام الحاسب

---

[1] - M.MASS, Le droit pénal spécial né de l'informatique, in informatique et droit pénal travaux de l'institut de sciences criminelles de poietiers, 4 éd, Cujas, 1981, p 23

[2] - D.B Parker, combattre la criminalité informatique, éd oros, 1985 p 18 ، مشار إليه لدى، محمد سامي الشوا، المرجع السابق، ص6.

[3] – محمد أمين الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، عمان، دار الثقافة للنشر والتوزيع، ط1، 2007، ص 9.

[4] – هلالي عبد ا اللاه أحمد، المرجع السابق، ص 14.

[5] – محمد سامي الشوا، المرجع السابق، ص 7.

كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الإئتمان، وانتهاك ماكينات الحاسب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب، وتمتد أيضا لتشمل سرقة جهاز الحاسب أو مكوناته"[1].

وقد تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا للجرائم المتصلة بتكنولوجيات الإعلام والإتصال أو الجريمة المعلوماتية بأنها " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[2].

ويعتبر هذا التعريف تعريفا شاملا واسعا إذ يشمل جانبين من الإجرام المعلوماتي، المادي والمعنوي للحاسب الآلي، ومنها شبكة الانترنيت، وهو لا يقتصر على مجرد كون الحاسب الآلي وشبكاته محلا للاعتداء، بل أيضا بوصف وسيلة للاعتداء وارتكاب الجرائم.

أما اتفاقية بودابست المتعلقة بالجريمة الإلكترونية فقد وضعت تقسيما للجرائم المعلوماتية، وصنفتها إلى أربعة مجموعات أو فصول، وهي الجرائم التي تستهدف خصوصية وسلامة توفر بيانات ونظم الكمبيوتر، وتشمل النفاذ غير المشروع، والإعتراض غير المشروع، والتدخل في البيانات، والتدخل في النظام، وإساءة استخدام الأجهزة، بالإضافة إلى الجرائم ذات الصلة بالكمبيوتر التي تشمل التزوير المرتبط بالكمبيوتر، والإحتيال المرتبط بالكمبيوتر، والجرائم ذات الصلة بالمحتوى، بالإضافة إلى الجرائم ذات الصلة بمواد إباحية الأطفال،

---

[1] – هلالي عبد اللاه ، المرجع السابق، ص14.

[2]– أحمد المناعسة، جرائم الحاسب الآلي والإنترنت، عمان، دار وائل للنشر والتوزيع، ط1، 2001، ص 78.

بالإضافة إلى الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والقيود ذات الصلة[1]، ولم تعرف الجريمة المعلوماتية.

والمشرع الجزائري عرف الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في المادة 2/أ من القانون 09-04 المتضمن القواعد الخاصة المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، إذ نصت : "يقصد في مفهوم هذا القانون: الجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

ويلاحظ من هذا التعريف القانوني أن المشرع الجزائري صنف الإجرام المعلوماتي إلى مجموعتين المجموعة الأولى الجرائم التي يكون فيها نظام المعالجة الآلية للمعطيات هدفا لارتكاب الجريمة، والمجموعة الثانية الجرائم التي يكون فيها نظام الإتصالات الإلكترونية أو المنظومة المعلوماتية هي الوسيلة التي تقع عن طريقها الجرائم، إذ ترك المجال واسعا لأي جريمة أخرى ترتكب عن طريق المنظومة المعلوماتية أو نظام الإتصالات الإلكترونية، إذ اخذ بالمفهوم الواسع، فقد وفق في تعريفه، وجمع جميع الحالات.

الفرع الثالث: المفهوم الإجرائي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

إن المشرع الجزائري لم يضع تعريفا للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال التي تعتبر أحد عناصر السياسة الجزائية الحديثة، وأورد مظاهرها في القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ومن خلال ما تم التطرق إليه أعلاه يمكن التوصل إلى إعطاء تعريف إجرائي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال باعتبارها صورة من

[1] المجلس الأوروبي، الاتفاقية الأوروبية المتعلقة بالجرائم الإلكترونية، بودابست 2001/11/23، أنظر الرابط الإلكتروني: https://rm.coe.int/budapest-convention-in-arabic/1680739173

صور السياسة الجزائية الحديثة في مواجهة الإجرام المعلوماتي، ويقصد بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال كافة التدابير والآليات اللازمة للحيلولة دون ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية، سواء من خلال الإعتماد على الأساليب الوقائية القبلية الإستباقية لا سيما من خلال دور المحيط الإجتماعي الأسرة، المدرسة، المسجد أو من خلال مؤسسات المجتمع الرسمية وجمعيات المجتمع المدني لمنع وقوع الجريمة أصلا، بالإضافة إلى أساليب الوقاية البعدية اللاحقة أثناء ارتكاب الجريمة أو بعدها لوقف وقوع الجريمة والتصدي لها وعدم تكرارها مستقبلا من جهة أخرى، وهي الإجراءات اللازمة لمنع المجرم من العود إلى ارتكاب الجريمة، أو الأساليب الإجرائية التي تمكن من ايقاف ارتكاب الجريمة أو منع الضرر الذي تحدثه الجريمة، سيما من خلال اتخاذ جميع الإجراءات بالإعتماد على الأسلوب العلمي التكنولوجي لمواجهة الجريمة المتصلة بتكنولوجيات الإعلام والإتصال المتوقعة أو مواجهة مضاعفات الجريمة التي وقعت فعلا، وذلك من خلال إعتماد المفهوم الواسع للوقاية من الجريمة، إذ يتضح ويتبين أن الإجراءات التي وضعها المشرع لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال تستهدف الوقاية من جهة والمكافحة من جهة أخرى، إذ يكون لكل إجراء دور وقائي استباقي يهدف إلى منع وقوع الجريمة أصلا، أو كبح مضاعفاتها أو إعاقتها أو إيقاف الضرر الناتج عنها أو احتمالية ارتكابها، وكذلك دور مكافحة بعد ارتكاب الجريمة للكشف عن مرتكبيها والتحقيق معهم للوصول إلى الدليل الرقمي الذي يدين المتهم أو يبرئه، فالعلاقة بين الوقاية والمكافحة هي علاقة تكاملية تهدف كلاهما غلى التصدي للجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وسيتم إبراز ذلك من خلال ما سيتم عرضه في المبحث الثاني.

المبحث الثاني:

إجراءات وضمانات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

إن المشرع الوطني ونظرا لخطورة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ولما لها من تأثير على كيان الدولة وأمنها الداخلي وإقتصادها، ارتأى أن أسلوب المكافحة لوحده لا يكفي لمواجهتها وإنما يتطلب الإعتماد على الأسلوب الوقائي، إذ جعل لأساليب المكافحة المتمثلة في المراقبة الإلكترونية، والتفتيش الإلكتروني، وحجز المعطيات المعلوماتية[1] دورا وقائيا أيضا، كما أقر إلتزامات لمقدمي الخدمات، وذلك بهدف الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وهو الأمر الذي يمس بالخصوصية الفردية وبسرية المراسلات والإتصالات دون علم ورضا الفرد، مما جعله في نفس الوقت يقر ضمانات قانونية للموازنة بين المصلحة العامة والمصلحة الخاصة، وسيتم توضيح ذلك في مايلي:

المطلب الأول:

الدور الوقائي لمراقبة الإتصالات الإلكترونية والتفتيش الإلكتروني وحجز المعطيات المعلوماتية

إن المراقبة الإلكترونية والتفتيش الإلكتروني تعتبر إجراءات مكافحة كأصل عام، إلا أن القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، جعلها إجراءات وقاية، وسيتم توضيح ذلك فيما يلي:

الفرع الأول: مراقبة الإتصالات الإلكترونية:

---

[1] – لقد نصت المادة 03 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها على " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات، يمكن لمقتضيات حماية النظام العام، أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية، وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية ".

تعتبر إجراء المراقبة الإلكترونية طبقا للقانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال إجراء وقاية، ولتحديد أحكامه سيتم التطرق إلى الأساس القانوني له، ثم إلى تعريفه، ثم إلى محله، ثم إلى مشروعيته فيمايلي:

أولا: الأساس القانوني للمراقبة الإلكترونية للإتصالات:

تعتبر المراقبة كأصل عام وسيلة هامة من وسائل البحث والتحري والتحقيق ويقصد بها " وضع شخص أو مكان معين تحت ملاحظة الشرطة لتسجيل كل ما يحدث من تصرفات غير قانونية في سرية تامة، بقصد منع وقوع الجريمة، أو تقديم دليل على شخص يشتبه في أن يكون هو الجاني "[1].

وتسمى المراقبة عندما نكون بصدد مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المراقبة الإلكترونية، وهو ما أطلق عليه المشرع في القانون 09-04 في الفصل الثاني منه، مراقبة الإتصالات الإلكترونية، تكييفا لمنظومته القانونية مع إلتزاماته الدولية لاسيما ما نصت عليه المادة 21 من اتفاقية بودابست التي ألزمت باعتماد المراقبة الإلكترونية للإتصالات ضمن التشريعات الداخلية.

لقد نص المشرع الجزائري على هذا الإجراء أي إمكانية الوضع تحت المراقبة الإلكترونية في مجال مكافحة الجرائم الخطرة المتمثلة في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أو جرائم تبييض الأموال أو تمويل الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف، وكذا جرائم الفساد، من خلال المواد 65 مكرر 05 إلى 65 مكرر 10 من قانون الإجراءات الجزائية، وذلك تحت الفصل الرابع المعنون باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، حيث

---

[1]- بثينة حبيباتني، الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، أطروحة لنيل شهادة دكتوراه ل . م .د في القانون العام تخصص القانون الجنائي وعلم الإجرام، جامعة الجزائر1، كلية الحقوق،14 سبتمبر 2020، ص 295.

يجوز لوكيل الجمهورية وكذلك لقاضي التحقيق في حال فتح تحقيق قضائي، منح إذن لضباط الشرطة القضائية، يتضمن اعتراض المراسلات وتسجيل الأصوات، التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية دون موافقة المعنيين بها، وذلك لمدة أقصاها 04 أشهر قابلة للتجديد.

وقد تعزز اللجوء إلى هذا الأسلوب سنة 2009 بموجب المادة 03 و04 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، التي وسع من مجال استخدام المراقبة الإلكترونية للإتصالات، من خلال التعريف الموسع للجرائم المتصلة بتكنولوجيات الإعلام والإتصال، كما أصبحت المراقبة الإلكترونية بالإضافة لكونها إجراء مكافحة، مراقبة وقائية استباقية، أي إجراء وقائي استباقي لارتكاب الجريمة، وتكون غايته منع ارتكاب الجريمة، والقبض على الفاعلين أو المخططين قبل الشروع في تنفيذ الجريمة، أو عند بدء التنفيذ، وذلك بقطع ومنع تحقق النتيجة الإجرامية[1]، وذلك **للوقاية** من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فهي تخص كشف خطر أو تهديد لأمن الدول، إذ أنه لمجرد توافر شكوك ولو كانت بسيطة حول شخص حتى ولو لم يكن مشتبها في ارتكابه لجريمة الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة بمفهوم قانون العقوبات، مادامت تحركاته ونصرفاته ونشاطاته تمثل خطرا على الأمن الداخلي واحتمال قيامه بالتحضير لإحدى الجرائم المذكورة، يجعل مراقبة اتصالاته الإلكترونية فعلا مشروعا في إطار الوقاية لكشف الخطر ودرء حدوثه، حتى ولو لم ترتكب الجريمة، سواء كانت البلاغات والشكاوى من طرف السلطات أو المواطنين سيما وأن السياسة التي تعتمدها الدولة تعتمد على عصرنة ورقمنة القطاعات، وكذلك في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني وفقا للمادة 4 الفقرة الأولى أ، ب من

---

[1]- حكيمة بوكحيل وسامية بن عديد، " **الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الإتصال ودورها في تفتيش نظم المعلوماتية**"، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021، ص 1542-1560، ص 1552.

القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، والاحتمال هنا ليس لدرجة توافر دلائل قوية تربط هؤلاء الاشخاص بارتكاب تلك الأفعال، وإنما مجرد الشكوك ولو بسيطة، فالوقاية لا تفترض القيام بأعمال تحضيرية لارتكاب هذه الأفعال وغنما مجرد تكهنات أو حتى دلائل بسيطة قد توحي بأن هؤلاء الأشخاص يمكنهم ارتكاب تلك الأفعال، إذ تهدف إلى منع وقوع الجريمة أصلا، كل ذلك لما تمتاز به من حساسية القطاعات كالدفاع الوطني والإقتصاد الوطني ومؤسسات الدولة التي تعتمد على الأنظمة المعلوماتية في سيرها التي تستوجب المراقبة السابقة لما لها من تأثير على كيان الدولة ككل في حالة المساس بها[1].

ثانيا: تعريف المراقبة الإلكترونية للإتصالات:

إن المشرع الجزائري لم يعرف المراقبة الإلكترونية للإتصالات، وعرفها الفقه واختلف في ذلك، إذ عرفها جانب من الفقه بأنها " العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لا سيما مراقبة شبكة الاتصالات، لجمع بيانات ومعلومات عن المشتبه به سواء أكان شخصا أو مكانا، أم شيئا حسب طبيعته مرتبط بالزمن التاريخ أو الوقت لتحقيق غرض أمني أو لأي غرض آخر"[2]، وعرفها جانب آخر بأنها " الإنصات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة، أو سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الإتصال السلكية واللاسلكية"[3]، ويرى جانب آخر بأنها " إجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة، ويتضح أن المراقبة

---

[1] – فطيمة جبار، " **مراقبة الإتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري**"، **مجلة الدراسات القانونية المقارنة**، جامعة حسيبة بن بوعلي الشلف الجزائر، مخبر القانون الخاص المقارن، العدد الثالث، ديسمبر2016، ص9-22، ص 17، 18.

[2] – بوكر رشيدة، جرائم الإعتداء على نظام المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن، لبنان، منشورات الحلبي الحقوقية، ط1، 212، ص 370.

[3] – عبد الحليم بن بادة، " **المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني**"، **المجلة الأكاديمية للبحث القانون**، جامعة عبد الرحمان ميرة بجاية، المجلد 10، العدد 03، 2019، ص 387-403، ص 390.

الإلكترونية تعني التنصت من جهة ومن ناحية أخرى التسجيل، والمشرع وفق في استعمال مصطلح المراقبة لأنها أوسع وأشمل.

وحقيقة المشتبه فيه الخاضع للمراقبة هو شبكة الإنترنت، وحاسوب الشخص الذي اساء استعمالها، حيث يتم مراقبة الاتصالات الإلكترونية المشتبه فيها وجمع تحركات المشتبه فيه عبر الإنترنت، بما في ذلك البريد الإلكتروني، من طرف ذوي الخبرة [1].

ثالثا: محل المراقبة الإلكترونية للإتصالات:

يتم تنفيذ المراقبة الإلكترونية للاتصالات من خلال استهداف الإتصالات الإلكترونية التي عرفها المشرع الجزائري في القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيات الإعلام والإتصال ومكافحتها في المادة 02 الفقرة و منها على أنها " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة بواسطة وسيلة إلكترونية"، كما عرفها القانون 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية[2] بأنها" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية".

فهي تنصب على مجموعة المعلومات والبيانات المتداولة عبر النظم المعلوماتية التي قسمها الفقه إلى قسمين: القسم الأول: البيانات والمعلومات المتداولة عبر شبكة الإنترنت والتي يتاح الإطلاع عليها من جميع المستخدمين للشبكة، وبيانات الترخيص للولوج إلى الشبكة والتحرك داخلها، وهو ما يعتبر بالمفهوم التقليدي الأماكن والطرق العامة، أي بيانات الولوج للانترنت تعد من قبيل البيانات الشخصية، التي يمكن التحري عنها وفقا للقانون، (معلومات ولوج الشخص للشبكة من رقم الهاتف، وعنوان التعريف IP) لا تعد من

---

[1] – عبد الحليم بن بادة، المرجع السابق، ص 396.

[2]– القانون 18-04 المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، الجريدة الرسمية العدد 27، 2018.

الخصوصيات الشخصية، على سبيل المثال تجول السيارة في الشوارع العامة بياناتها من حيث النوع والرقم والرخصة وبيانات القائد لا تعد من خصوصيات الفرد، كما أن الدخول لمواقع الخدمات التي تقدمها شبكة الانترنت يشبه الدخول للأماكن العامة والمحلات العامة[1].

والقسم الثاني: يشمل الحسابات الشخصية التي لا يتاح للكافة دخولها بل يسمح الدخول إليها إلا من خلال كلمة مرور خاصة بالمستخدم لدى بعض المواقع التي تقدم خدمات للمستخدمين عبر الانترنت والتي تتميز عن الأولى في كونها مرتبطة بالمستخدم ولا يمكن الإفصاح عنها إلا بإرادته أو باختراقها من خلال أدوات وتقنيات خاصة غير مشروعة بالنظام الرقمي، وتعد هذه المعلومات من قبيل الخصوصية الشخصية، التي لا يجوز الإطلاع عليها إلا بموافقة صاحبها من خلال استخدام كلمة مرور بإذن مالكها أو إذن قضائي، فالأمر بالنسبة للحسابات الشخصية عبر الانترنت يشبه الدخول للمسكن وتفتيشه[2].

وبالرجوع لإتفاقية بودابست نجدها ميزت بين نوعين من البيانات المعلوماتية محل الاعتراض، البيانات المتعلقة بالمرور والبيانات المتعلقة بمحتوى الاتصال، والتي عرفت في المادة الأولى منها البيانات المتعلقة بالمرور بأنها " كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي، والتي يتم انتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الإتصال، مع تعيين المعلومات التالية: أصل الإتصال، مقصد الإتصال، أو الجهة المقصودة بالإتصال، خط السير، ساعة وتاريخ، حجم وفترة الإتصال، أو نوع الخدمة".

وأما النوع الثاني فلم تعرفه الإتفاقية لكنها تشير إلى المحتوى الإخباري للإتصال، أي بمعنى مضمون الإتصال أو الرسالة أو المعلومات المنقولة عن طريق الإتصال، ماعدا البيانات المتعلقة بالمرور.

---

[1] –حبيباتني بثينة، المرجع السابق، ص 298.

[2] – المرجع نفسه، ص299.

والإتفاقية ميزت بينهما أيضا من الناحية الشكلية حيث أدرجت كل إجراء تحت عنوان خاص، فالمادة 20 منها خصت تجميع حركة المعطيات بعنوان " التجميع في الوقت الفعلي لمعطيات المرور، وأما المادة 21 فجاءت تحت عنوان اعتراض معطيات المحتوى.

وهو ما ذهب إليه المشرع الجزائري وبالرجوع للقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، نجده يفرق بين تجميع المعطيات المتعلقة بحركة السير تحت اسم " حفظ المعطيات المتعلقة بحركة السير" المادة 11 وبين اعتراض المعطيات المتعلقة بالمحتوى تحت عنوان " مراقبة الإتصالات الإلكترونية في المادة 04 منه.

رابعا: مشروعية المراقبة الإلكترونية للإتصالات:

إن موضوع المراقبة يعتبر موضوع شائك لكونه يمكن من الإطلاع ومراقبة الأمور التي تدخل في نطاق الحريات الشخصية للأفراد التي لا يجوز الإعتداء عليها إلا بأمر قضائي وفقا للقانون، لكون مراقبة الأحاديث والاتصالات الخاصة تمس بحق الإنسان في الخصوصية، المحمي بحماية دستورية وجزائية في مختلف التشريعات الوطنية.

والمشرع الوطني سمح باللجوء إلى هذا الإجراء إذا اقتضت ضرورة الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، **حتى ولو لم ترتكب الجريمة أصلا، لمجرد الشكوك، أو لمنع حدوث مضاعفات ولإعاقة وكبح هذه الجريمة، في إطار الوقاية**، إلا أنه أحاط ذلك بمجموعة من الضمانات لحماية الحق في الخصوصية.

وهو **أن يتم تنفيذ الإجراء تحت سلطة القضاء وبإذن منه، إذ** تعتبر السلطة القضائية الضامن للحقوق والحريات، فاللجوء لهذا الإجراء يكون إلا بعد الحصول على إذن من السلطة القضائية لتكريس دولة الحق والقانون وإضفاء الشرعية على كل الإجراءات المتخذة من قبل الضبطية القضائية، إذ نصت المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بموجب الفقرة

الثانية منها أنه " لا يجوز أن يتم تنفيذ الإجراء تحت سلطة القضاء وبإذن منه، إذ تعتبر السلطة القضائية الضامن للحقوق والحريات، فاللجوء لهذا الإجراء يكون إلا بعد الحصول على إذن من السلطة القضائية لتكريس دولة الحق والقانون وإضفاء الشرعية على كل الإجراءات المتخذة من قبل الضبطية القضائية، إذ نصت المادة 04 من القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بموجب الفقرة الثانية منها أنه " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة"، وهو ما نصت عليه أحكام المادة 65 مكرر 05 قانون الإجراءات الجزائية أيضا.

وإذا ما تعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم إرهابية أو تخريبية أو الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح الإذن لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال حسب ما نصت عليه المادة 04 الفقرة السادسة من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

وأن تكون ثمة ضرورة قصوى تدعو إلى إجراءه، وبالرجوع إلى نص المادة 04 من القانون 09-04 ومن خلال المناقشات التي دارت خلال أعمال جلسة تقديم ومناقشة مشروع القانون، يتبين أن اللجوء غلى هذا الإجراء يكون بهدف الوقاية من وقوع بعض الجرائم، وبذلك فإن ضابط الوقاية سند شرعي مبرر للمراقبة[1]، وكذلك توافر معلومات كافية تنذر باحتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني، أو مؤسسات الدولة أو الإقتصاد الوطني، أو للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الماسة بأمن الدولة، وعلى هذا الأساس يباح اللجوء إلى هذا الإجراء استثناء في حدود ضيقة تحقيقا للمصلحة العليا للوطن حسب ما ذهبت إليه المادة 04 من القانون

[1] – بوكر رشيدة، المرجع السابق، ص 374.

09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

وأن يراعى استخدام الوسيلة المذكورة في نطاق ضيق للغاية، إذ يتم اللجوء لهذا الإجراء للوقاية من عدد محدود من الجرائم، وهي التي تمس حقوق ذات أهمية كبيرة يقدرها المشرع، إذ نص في المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها على الحالات التي يجوز فيها اللجوء لهذا الإجراء، وذلك للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وفي حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني، لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

والمشرع الجزائري نص على اللجوء إليها في الجرائم التي تتسم بالخطورة البالغة والماسة بأهم المجالات الحيوية للمرتبطة ارتباطا وثيقا بكيان الدولة والإقتصاد الوطني وأمن المجتمع وسلامته، كما ترك المجال مفتوحا أيضا ليشمل أي جريمة من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية[1].

وأن يتم تنفيذ المراقبة الإلكترونية خلال مدة معينة، إذ حدد المشرع الجزائري مدة إجراء المراقبة الإلكترونية فيما يخص الفقرة أ من المادة 04 من القانون 09-04 بستة أشهر قابلة للتجديد على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها، عندما يتعلق الأمر بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو

[1] حبيباتني بثينة، المرجع السابق، ص 302.

الجرائم الماسة بأمن الدولة، وأما باقي الحالات فتكون المدة المحددة 04 أشهر قابلة للتجديد حسب المادة 65 مكرر الفقرة الثانية قانون الإجراءات الجزائية، إذ أنه فيما يخص الجرائم الإرهابية والتخريبية والماسة بأمن الدولة، فإن المشرع تركها على مطلقها ولم يقيدها بعدد مرات التجديد أو بوقت محدد التي يجوز فيه المراقبة، إذ اعتبرها مدة خاصة، وذلك لخطورة هذا النوع من الإجرام المهدد لأمن الدولة وكيانها، باعتباره إجراما منظما عابرا للحدود الوطنية وصعب الإثبات[1].

وأن يتم تنفيذ المراقبة الإلكترونية من قبل ضباط الشرطة القضائية المنتمين إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، إذ أشار القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، في المادة 04 منه في فقرتها الثالثة إلى أن ضباط الشرطة القضائية المنتمين للهيئة الوطنية المنصوص عليها في المادة 13 من القانون أي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال هي التي تتولى المراقبة الإلكترونية فيما يخص الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، إذ أعطى لهم الحصرية دون غيرهم من الجهات، كما أنه بموجب المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[2]، وغيره من المراسيم الرئاسية الأخرى التي ألغته[3]، إلى حين صدور المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة

---

[1] – بن بادة عبد الحليم، المرجع السابق، 399.

[2]– المرسوم الرئاسي 15-261 المؤرخ في 2015/10/08، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، الجريدة الرسمية العدد 53، المؤرخة في 2015/10/08.

[3] – المرسوم الرئاسي 19-172 المؤرخ في 2019/03/06 ، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتنظيمها وكيفية سيرها، الجريدة الرسمية العدد 37 المؤرخة في 2019/06/19.

الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[1]، التي بينت المادة 14 منه بأن مديرية المراقبة الوقائية واليقظة الإلكترونية التابعة للمديرية العامة التابعة للهيئة الوطنية للوقاية من المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، هي المكلفة بتنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو المساس بأمن الدولة، ذلك أن مسألة حماية أمن البلاد والمواطن والإقتصاد الوطني تعلو على حق المشتبه فيهم في الحفاظ على الحق في الخصوصية، ومع ذلك أقام المشرع الوطني التوازن بين حق المجتمع في الأمن ومنع الجريمة، وحق الفرد في السرية، من خلال إقرار الضمانات التي تمنع تعسف القائمين على هذا الإجراء، إذ يتم وضع الترتيبات حصريا لتجميع وتسجيل معطيات ذات الصلة بالأفعال الإرهابية أو بالوقاية منها دون غيرها من الحالات، كما أن استخدام المعلومات المتحصل عليها خارج الحدود الضرورية يعرض صاحبه للمسؤولية الجزائية طبقا للمادة 4 الفقرة 7 والمادة 09 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، إذ يتعين على القائمين على هذه العمليات إحترام السر المهني، والمشرع الجزائري وفر الحماية ضد كل من يحاول استغلال عمليات المراقبة لأغراض شخصية تنتهك حرمة الحياة الخاصة[2].

الفرع الثاني: تفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية:

يعتبر إجراء تفتيش المنظومات المعلوماتية طبقا للقانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته إجراء وقاية،

---

[1]- المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/07، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد 86، المؤرخة في 2021/11/11.

[2] - حبيباتني بثينة، المرجع السابق، ص 303.

ولتحديد أحكامه سيتم التطرق إلى الأساس القانوني له، ثم إلى تعريفه، ثم إلى محله، ثم إلى مشروعيته، ثم إلى حجز المعطيات المعلوماتية باعتباره النتيجة النهائية للتفتيش فيما يلي:

أولا: الأساس القانوني لتفتيش المنظومات المعلوماتية:

من خلال ما نصت عليه المادة 3 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، يتبين أن المشرع الجزائري اعتبر تفتيش المنظومات المعلوماتية إجراء وقائيا مثله مثل المراقبة الإلكترونية للإتصالات، وهو ما يتلاءم مع طبيعة الجريمة المتصلة بتكنولوجيات الإعلام والإتصال التي لا يمكن للأساليب التقليدية لوحدها التصدي لها، سيما وأنها ترتكب في الفضاء الرقمي، وهو ما جعل المشرع الجزائري في إطار الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وكذلك في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو مؤسسات الدولة أو الإقتصاد الوطني، وطبقا للمادة 05 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته يجيز اللجوء غلى إجراء التفتيش، إذ أنه يعتبر إجراء من إجراءات المكافحة، وكذلك إجراء من إجراءات الوقاية حسب ما أحالت إليه المادة 05 إلى المادة 04 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، وهو في الأصل إجراء من إجراءات التحقيق القضائي[1]، إلا أن المشرع الوطني اعتبره أيضا تفتيشا وقائيا قد يكشف عن أدلة يمكن أن تكون إثبات لتخطيط مسبق يراد به ارتكاب جرائم ذات خطورة على الأمن الداخلي للدولة، فالهدف منه هو الوقاية إذ يتم حتى في غياب وقوع فعلي للجريمة.

---

[1]- رضا هميسي، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، العدد5، جوان 2012، ص 157-182، ص 160.

ومن المتعارف عليه أن إجراء التفتيش في الأصل هو إجراء يستهدف المساكن، وبموجب القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته استحدث المشرع إجراء تفتيش المنظومة المعلوماتية، نظرا لخصوصية مسرح الجريمة البيئة التقنية.

ثانيا: تعريف تفتيش المنظومة المعلوماتية:

يعرف التفتيش بأنه إجراء من إجراءات التحقيق ووظيفته البحث عن أدلة الجريمة ولم يعرف القانون التفتيش، وإنما ترك للفقه والقضاء تعريفه، إذ عرفه البعض بأنه " البحث والتحري داخل سر الأفراد عن أدلة لإثبات جريمة معينة ارتكبت فعلا وهو إجراء من إجراءات التحقيق"[1]، وعرفه البعض الآخر بأنه " إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه[2]، أما تفتيش المنظومة المعلوماتية فقد عرفه جانب من الفقه بأنه " البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه أو هو البحث الدقيق والإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكنا أو جهاز حاسوب أو أنظمة معلوماتية"[3]، وهو إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني يستهدف ضبط أدلة الجريمة مثل البرامج غير المشروعة والملفات المخزنة في الحواسيب والمعطيات المعلوماتية والإتصالات الإلكترونية.

ولقد عرف المشرع الجزائري المنظومة المعلوماتية في المادة 2 الفقرة ب منها من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

---

[1] – سامي حسن الحسيني، النظرية العامة للتفتيش، القاهرة، دار النهضة العربية، 1972، ص 36.

[2] – فضيل العيش، شرح قانون الإجراءات الجزائية بين النظري والتطبيقي، الجزائر، دار البدر، 2008، ص 113.

[3] – حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتاب الحديث، ط1، 2009، ص 12-14.

والإتصال ومكافحته بأنها " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

ومن الملاحظ أن هذه التعريفات عرفت تفتيش المنظومة المعلوماتية باعتبارها إجراء مكافحة باعتباره إجراء لضبط الجريمة واقعة سواء جناية أو جنحة، بينما القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، اعتبر تفتيش المنظومة المعلوماتية إجراء وقاية، وهو ما يعرف بالتفتيش الإلكتروني الوقائي وهو تدبير استباقي تكون غايته منع ارتكاب الجريمة والقبض على الفاعلين أو المخططين قبل الشروع في تنفيذ الجريمة أو عند بدء التنفيذ وذلك بقطعه ومنح تحقق النتيجة الإجرامية، والهدف منه كبح وإعاقة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

ثالثا: محل التفتيش في المنظومة المعلوماتية:

إن نظام المعالجة الآلية للمعطيات يتكون من مكونات مادية ومعنوية بالإضافة إلى شبكات اتصالات بصرية سلكية ولا سلكية سواء على المستوى المحلي أو الدولي، إذ ينصب تفتيش المنظومة المعلوماتية إما على المكونات المادية لنظام المعالجة الآلية للمعطيات للبحث عن شيء يتصل بالجرائم للكشف عن الحقيقة، ويتوقف حكم تفتيش هذه المكونات على طبيعة المكان الموجود فيه سواء في الأماكن العامة أو الخاصة، ذلك أن المكونات المادية تتمثل في وحدات الإدخال التي يمكن إدخال المعلومات والبيانات بها كلوحة المفاتيح الفأرة، مشغل الأقراص الممغنطة، الماسح الضوئي....، ووحدات المعالجة المركزية التي تتمثل في وحدة الذاكرة المركزية...، وحدات الإخراج التي تتمثل في الوسائط المستخدمة في إظهار نتائج التشغيل ومعالجة البيانات، الشاشة، الطابعة، وجميع التجهيزات التي تصنف كتجهيزات اتصال كالمودم، إذ أنه إذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنه لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبالضمانات

المقررة قانونا[1] حسب ما نصت عليه المادة 46 ق إ ج، بتوافر الرضا الصريح من الشخص الذي سيتخذ لديه الإجراءات، الذي يجب أن يكون مكتوب بخط يده، وفي حالة أنه لا يعرف الكتابة بإمكانه الإستعانة بشخص يختاره، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه، إضافة إلى أحكام المواد من 44 إلى 47 ق إ ج، وفي سبيل مواجهة هذا النوع من الإجرام الخطير لم يكتف المشرع بما هو منصوص عليه في المادة 46 ق إ ج بل أورد عليه استثناء بموجب الفقرة 03 من نفس المادة، حيث لا تطبق هذه الضمانات على طائفة من الجرائم بما فيها جرائم المساس بأنظمة المعالجة الآلية للمعطيات محيلا إلى المادة 7 الفقرة 3 والمادة 47 مكرر، إذ يجوز القيام بعمليات التفتيش أو الحجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني، والمشرع الوطني غلب مصلحة المجتمع في تحقيق العدالة ومنع الجريمة على حق الأفراد في الحفاظ على حرمة المسكن باعتباره مستودع الأسرار، لخصوصية الدليل إذ يمكن محوه أو تعديله في أقل من ثانية.

وينصب التفتيش على مكونات الحاسب المعنوية أيضا إذ تعتبر المعطيات المعنوية المعطيات والمعلومات التي يتم تنظيمها ومعالجتها داخل نظام المعالجة الآلية للمعطيات وتخزينها بغية استرجاعها عند طلبها، وهي نبضات الكترونية لا يمكن لمسها، واختلف الفقه الجنائي حول إمكانية أن تكون محلا للتفتيش، وأما المشرع الجزائري ومن خلال نص المادة 05 من القانون 09-04 أجاز صراحة تفتيش المنظومة المعلوماتية من خلال الدخول ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، ومنظومة تخزين معلوماتية، إلا أنه في حالة ما إذا كان نظام المعالجة الآلية مزود بنظام حماية يمنع الولوج دون تدخل القائم على المنظومة ومساعدته، فاختلفت الآراء الفقهية حول جواز إجبار المتهم أو المشتبه فيه عن الإفصاح عن كلمة المرور وتزويد القائم على التفتيش بها من أجل تسهيل الولوج، بين الرأي المعارض الذي يبرر ذلك على أن لا يجوز إجبار

---

[1] – بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الإسكندرية، دار الفكر الجامعي، ط1، 2011، ص 67، 69.

المتهم على تقديم المعلومات، على أساس عدم جواز إجبار المتهم على الإجابة على الأسئلة التي من شأنها أن تفضي إلى إدانته، كما له الحق في الصمت، والرأي المؤيد الذي يرى أنه لا ينبغي أن يكون ذلك حائلا دون إجباره على تقديم معلومات لتسهيل الولوج إلى المنظومة المعلوماتية، متى كانت بحوزته، قياسا على إجبار شخص على تسليم مفتاح الخزانة التي بحوزته[1].

وبالرجوع إلى القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته يتبين أنه أجاز للسلطات المكلفة بالتفتيش إلزام مقدمي الخدمات تقديم المعلومات التي من شأنها تيسير الدخول إلى المنظومة كتقديم بعض معطيات المرور للتمكن من التعرف على مستعملي الخدمة والتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذلك عناوين المواقع المطلع عليه وكذا تاريخ ووقت ومدة اتصال، إذ أن المشرع الجزائري ألزم غير المتهم على تقديم المعلومات، ذلك أن الإكراه الواقع على المتهم يمس بحق الدفاع.

وينصب التفتيش **على شبكات الحاسب الآلي التي تعتبر** مهمة لربط الحواسيب مع بعضها البعض سواء أكان ذلك على المستوى المحلي أم على المستوى العالمي، ومن خلال ما نصت عليه المادة 05 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته فإنه يوجد احتمالين: في حالة اتصال نظام المتهم بنظام آخر موجود في مكان آخر داخل الدولة إذ نص المشرع في الفقرة الثانية من المادة 05 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته على أنه في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، وكانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى

[1] -حبيباتني بثينة، المرجع السابق، ص 317.

هذه المنظومة، أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك، أما في حالة اتصال نظام المتهم بنظام موجود في مكان آخر خارج الدولة أجاز المشرع الجزائري في المادة 05 الفقرة الثالثة تفتيش الأنظمة المتصلة حتى ولو كانت خارج إقليم الدولة وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[1].

رابعا: مشروعية التفتيش الوقائي للمنظومة المعلوماتية:

حماية للحق في حرمة الحياة الخاصة أحاط المشرع تفتيش المنظومة المعلوماتية بضمانات قانونية، سيما التفتيش الوقائي، حتى يكون صحيحا، مثله مثل التفتيش كأسلوب مكافحة، إذ يجب أن يكون التفتيش للوقاية من الأفعال الموصوفة بجرائم إرهابية أو تخريبية أو الجرائم الماسة بأمن الدولة وفي حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني، إذ أجاز المشرع للسلطات القضائية عن طريق الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، القيام بتفتيش المنظومة المعلوماتية في مراحل سابقة على وقوع الجريمة[2]، سيما وأن المشرع قد سمح بتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعلومات التي تتضمنها، قصد مساعدة السلطات القضائية أو ضباط الشرطة القضائية، وتزويدهم بكل المعلومات الضرورية لإنجاز مهامها[3]، ذلك أن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال تملك خبراء ومتخصصين، وتضم مديرية تقنية تعرف بمديرية المراقبة الوقائية واليقظة الإلكترونية التي يمكن لهل تقديم يد المساعدة للسلطة القضائية عن طريق القيام بالتدقيق والتفتيش في أي مكان أو هيكل أو جهاز يحوز أو يستعمل وسائل وتجهيزات

---

[1] – حبيباتني بثينة، المرجع السابق، ص 321.

[2]– حكيمة بوكحيل وسامية بن عديد، المرجع السابق، ص 1554.

[3]– المادة 6 الفقرة 4 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد 47، ص 6.

موجهة لمراقبة الإتصالات الإلكترونية، باستثناء تلك التابعة لوزارة الدفاع الوطني[1]، ويلاحظ أن المشرع من خلال ما نص عليه بموجب المادة 5 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها التي تضمنت " وفي الحالات المنصوص عليها في المادة 04 أعلاه "، التي أجازت للسلطات القضائية وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد، فهو بذلك يكون قد خرج المشرع عن القواعد العامة التي تعتبر التفتيش عملا من أعمال التحقيق التي تفرض أن تكون الجريمة قد وقعت فعلا، إذ لا يمكن إجراء تفتيش من أجل جريمة محتملة الوقوع[2]، ويرجع الأمر لخصوصية الجرائم المعلوماتية ولخطورة الجرائم الإرهابية والجرائم الماسة بأمن الدولة والمهددة للمصالح الحيوية، وهو بذلك خرج عن القواعد العامة للتفتيش.

كما يلاحظ أن المشرع الجزائري في المادة 5 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها سكت عن ضرورة الحصول على إذن قضائي من الجهات القضائية للقيام بإجراء التفتيش الإلكتروني سواء كان ذلك في إطار الوقاية أو المكافحة كما هو منصوص عليه بالنسبة للمراقبة الإلكترونية، إذ أنه هل يجوز الدخول إلى المنظومة المعلوماتية لإجراء تفتيش عن بعد دون الحصول على إذن قضائي، غير أنه نص على إعلام السلطة القضائية عند تمديد التفتيش بسرعة إلى منظومة معلوماتية أخرى أو جزء منها طبقا للمادة 5 الفقرة 2 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، أو أن هذا الإجراء يبقى يخضع غلى القواعد العامة فيما يخص الإذن بالتفتيش حماية للحق في الحياة الخاصة؟، وأغلبية الفقه اعتبر أن الإذن بالتفتيش يستخلص ضمنا

---

[1] – المادة 14 ب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، الجريدة الرسمية العدد47 لسنة 2009، ص 8، والمادة 14 من المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد86 لسنة 2021، ص 7 و8.

[2] – حسن محمد الطوالبة، المرجع السابق، ص 62.

من القواعد العامة طبقا لقانون الإجراءات الجزائية، إذ يتوجب على ضباط الشرطة القضائية الحصول على إذن مسبق لإجراء التفتيش الإلكتروني سواء عند تفتيش المكونات المادية أو عند تفتيش المكونات المعنوية ولو عن بعد، ويكفيهم فقط إعلام السلطة القضائية في حالة التمديد إلى منظومة معلوماتية أخرى أو جزء منها.

ولما كان التفتيش عملا من أعمال التحقيق كأصل عام يتعين تدوين إجراءاته ضمن محضر يثبت فيه الإجراءات والخطوات المتخذة أثناء التفتيش وما أسفر عنه من نتائج، ويتضمن المحضر وصف العملية من بدايتها إلى نهايتها، وإذا تم ضبط أشياء يتعين جردها ثم حجزها مع الإشارة إلى تاريخ وتوقيع المحرر، كما يجب ان يحرر المحضر باللغة الرسمية الوطنية[1].

خامسا: حجز المعطيات المعلوماتية:

يعتبر حجز المعطيات المعلوماتية النتيجة الطبيعية التي ينتهي إليها التفتيش[2]، وهو ضبط الأدلة، أي وضع اليد على المكونات المادية والمعنوية للأنظمة المعلوماتية[3]، ولقد نص المشرع الجزائري في المادة 06 من القانون 09-04 على حجز المعطيات المعلوماتية التي نصت على أنه " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية قابلة للحجز، والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية"، فالمشرع لم يكتف بإقرار حجز المنظومة المعلوماتية بل عالج إشكالية صعوبة ضبط النظام كله لا سيما إذا ما كان الحاسوب ليس حاسوبا شخصيا وإنما جزء من

---

[1]- رضا هميسي، المرجع السابق، ص 169، 170.

[2]- عبد القادر فلاح ، " **حجز وحفظ المعطيات في الجريمة الإلكترونية**"، **مجلة صوت القانون**، المجلد 08، العدد 01، سنة 2021، ص 177-194، ص 179.

[3] - حبيباتني بثينة، المرجع السابق، ص 332.

شبكة معقدة إذ سمح بنسخ المعطيات محل البحث، وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية قابلة للحجز[1].

كما أنه بموجب المادة 07 من القانون 09-04 استحدث إجراء الحجز عن طريق منع الوصول إلى المعطيات، باستعمال التقنيات المناسبة لمنع الوصول إلى المعلومات والمعطيات التي تحتويها المنظومة المعلوماتية أو نسخها إذا استحال إجراء الحجز طبقا للمادة 06 من القانون 09-04.

وهناك طريقتين لضبط المعلومات والأدلة الرقمية التي كانت موضوع التفتيش تتحقق الأولى عن طريق نسخ وتحميل البيانات والمعطيات محل البحث على دعامة تخزين مادية (الأقراص الممغنطة، بطاقات الذاكرة، المودم) التي تكون قابلة للضبط والوضع في أحراز مختومة طبقا للمادة 6 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، وإما من خلال الحجز عن طريق منع الوصول إلى المعطيات وذلك باستعمال تقنيات وتدابير الحماية الفنية كالتشفير والترميز، وبرامج منع الكتابة، في حالة استحالة ضبط المعلومات لأسباب تقنية، كما يتم اللجوء إلى تعطيل تشغيل المعطيات أو محوها بعد أخذ نسخة منها في حالة ما إذا كانت المعطيات تتضمن خطرا على النظام العام والآداب العامة كالبرامج التي تحتوي على فيروسات طبقا لمقتضيات المادة 8 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، وهذا خوفا من ضياع وإتلاف الأدلة الرقمية.

---

[1] – حبيباتتي بثينة، المرجع السابق، ص 335.

المطلب الثاني:

الدور الوقائي لمقدمي الخدمات

إن المشرع الوطني في إطار الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال نص على مساعدة مقدمي الخدمات للسلطات المكلفة بالوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، كما أن الإلتزامات المفروضة عليهم طبقا للقانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال تعتبر مظهرا من مظاهر السياسة الوقائية التي اعتمدها المشرع في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وسيتم توضيح ذلك في ما يلي:

الفرع الأول: مفهوم مقدمي الخدمات:

إن تكنولوجيات الإعلام والإتصال تتعلق بخدمات الإتصال السلكية واللاسلكية والشبكات الإلكترونية التي يتم فيها تبادل المعلومات عن طريق توصيل الخدمات المتنوعة لهذه التكنولوجيات إلى مستعمليها، ويتطلب ذلك تدخل مقدمي الخدمات الذين يقومون بربط مستخدمي الإنترنت بالمواقع وبالغير من المستخدمين[1]، وسيتم توضيح ذلك فيما يلي:

أولا: تعريف مقدمي الخدمات:

لقد عرف المشرع الجزائري مقدمو الخدمات في المادة 2 الفقرة د من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، بأنهم : أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعملها".

---

[1]- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم 09-04، مذكرة ماجيستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، تخصص قانون جنائي، 2013/2012، ص96، 97.

ومن الملاحظ أن المشرع الجزائري في تعريفه لمقدمي الخدمات قام بتصنيفهم سواء كانوا في القطاع العام أو في القطاع الخاص، بالنظر إلى الدور الذي يقومون به، أو نوع الخدمة التي يؤدونها من خلال ربط شبكات الإنترنت والإتصال وتمكين العملاء من الوصول إلى الأنظمة المعلوماتية، إلا أنه لم يعط لكل وسيط اسم خاص أو تعريف خاص مثل المشرع الفرنسي، بل جاء تعريفه تعريفا عاما مصنفا لأصناف مقدمي الخدمات، وجمعهم بنفس الإلتزامات وأخضعهم لنفس المسؤوليات على اختلاف أدوارهم، وذلك لصعوبة حصرهم[1].

ثانيا: أصناف مقدمي الخدمات:

إن أصناف مقدمي الخدمات هم الوسطاء ما بين المستخدم والشبكة بأنواعهم سواء كان دورهم معلوماتي أو تقني، لا يمكن حصرهم، وإنما يمكن تحديدهم على سبيل المثال، وهو ما ذهب إليه المشرع الجزائري نظرا للتطور السريع في مجال تقنية المعلومات الذي قد يظهر أشخاص آخرون يقومون بأدوار لتزويد الخدمات عبر الإنترنت، ونذكر على سبيل المثال متعهد الوصول، والذي يطلق عليه أسماء كثيرة، وهو متعهد الدخول أو مورد الدخول ، أو مزود خدمة الدخول، وقد يكون شخصا من أشخاص القانون العام، أو جمعية أو شركة تجارية، ودوره يتمثل في توفير إمكانية الإتصال بشبكة الانترنت للجمهور، يربط اتصال مستخدمي الانترنت بالمواقع التي يرغبون بالدخول إليها، ومن الوسائل المودم، وهو الآلة التي تسمح بنقل المعطيات الرقمية التي يتضمنها الحاسوب إلى قوة دفع كهربائية، ومن أمثلة مقدمي خدمات الوصول في الجزائر DJAWEB و FAWRI في القطاع العام، ASSILA BOX في القطاع الخاص[2].

ونجد كذلك متعهد الإيواء وهو الذي يطلق عليه مورد الإيواء، أو المورد المستضيف، المضيف، وهو المورد الذي يؤمن تخزين المحتوى أو المضمون، وإدارته، واسترجاع

---

[1] – أحمد مسعود مريم ، المرجع السابق، ص 98.

[2]– عكو فاطمة الزهرة، المسؤولية المدنية لمقدمي الخدمة الوسيطة في الانترنت، رسالة لنيل درجة الدكتوراه في القانون، جامعة الجزائر 1، كلية الحقوق، 2016/2015، ص 25.

المعلومات التي يتضمنها ويرغب مورد المضمون بجعلها في متناول الجمهور على شبكة الإنترنت، وقد يكون شخصا طبيعيا أو معنويا عاما أو خاصا[1]، كما نجد أيضا ناقل المعلومات وهو الشخص الطبيعي أو المعنوي الذي يدير شبكة الإتصالات سلكية أو لاسلكية عن بعد، ويسمح للمستخدم بالإتصال عبر شبكاته للدخول إلى النظام المعلوماتي، وفي الجزائر يعتبر ناقلا للمعلومات اتصالات الجزائر، وكذلك بعض الشركات الخاصة مثل موبيليس وأوريدو وجيزي[2]، كما نجد مورد المعلومات وهو الشخص الذي يقوم بتحميل الجهاز أو النظام بالمعلومات، لوضعها في متناول الجمهور، سواء كان منتجها أو جامعها أو مؤلفها[3]، ونجد كذلك مزود خدمة البحث وخدمة إنشاء خطوط الربط بالمادة المعلوماتية وجد لتغطية بعض الأنشطة الدقيقة التكميلية التي يتم تقديمها لتسهيل وزيادة جودة الخدمة، ويدخل عمل تلك الطائفة في المرحلة ما بين مقدم المعلومات والمستفيد منها، ومن أهمهم مزود خدمة البحث، ومزود خدمة إنشاء خطوط الربط بالمادة المعلوماتية[4].

الفرع الثاني: إلتزامات مقدمي الخدمات:

لقد نص المشرع الجزائري على مجموعة من الالتزامات المفروضة على عاتق مقدمي الخدمات والتي تساهم في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، سيما وأن دورهم تمكين المستخدم من الدخول إلى الشبكة والإطلاع على المنظومة المعلوماتية، وتتميز هذه الإجراءات بطابعها الوقائي، لما تكرسه من أساليب وقائية أولية تمنع من وقوع الجريمة أصلا، وسيتم توضيح ذلك فيما يلي:

---

[1]- عكو فاطمة الزهرة ،المرجع السابق، ص 27

[2] – المرجع نفسه، ص27.

[3] –محمد حسين منصور، المسؤولية الإلكترونية، مصر، الإسكندرية، دار الجامعة الجديدة، 2003، ص 199.

[4] – عكو فاطمة الزهرة، المرجع السابق، ص 32.

أولا: الأساس القانوني لالتزامات مقدمي الخدمات:

بالرجوع إلى المادة 10 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، نجد أن المشرع الوطني ألزم مقدمي الخدمات على تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 ، تحت تصرف السلطات المذكورة، وبالرجوع أيضا للمادة 15 من المرسوم الرئاسي 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال يتبين أن مديرية المراقبة الوقائية واليقظة الإلكترونية لدى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال تضع على مستوى المنشآت القاعدية لمتعاملي ومقدمي خدمات الإتصالات الإلكترونية، التجهيزات والوسائل والأجهزة التقنية الضرورية لتنفيذ مهامها، كما أن المتعاملون ومقدمو الخدمات يلزمون بتقديم المساعدة الضرورية لهذه المديرية من أجل ممارسة مهامها.

وذلك إدراكا من المشرع على ضرورة إلزام الأطراف المتدخلة في خدمات الانترنت بتقديم المساعدة لصعوبة البيئة الرقمية، وهو الإجراء الذي أقرته اتفاقية بودابست في المادتين 16 و17 منها.

وعليه فإن مزود الخدمة بإمكانه مراقبة ومعرفة جميع الخطوات التي يتبعها المستخدم لمعرفة المواقع التي زارها والمعلومات التي خزنها، وكل الإتصالات التي أجراها، وبناء على ذلك فإن المراسلة بالبريد الإلكتروني التي يتم استقبالها بواسطة مزود الخدمة المرسل إليه التي لم يطلع عليها بعد تستقر في حالة تخزين إلكتروني، ففي هذه المرحلة فإن النسخة من الاتصال المخزنة تتواجد فقط كإجراء أو وسيط مؤقت في انتظار استقبال المرسل إليه لها من مزود الخدمة، وبمجرد استلام المرسل إليه المراسلة بالبريد الإلكتروني فإن الإتصال

يكون قد وصل إلى وجهته الأخيرة، وفي هذه الحالة فإن مزود الخدمة إما أم يقوم بمسح تلك الرسالة أو أن يقوم بتخزينها فتبقى الرسالة مخزنة لدى مزود الخدمة[1].

ثانيا: إلتزام حفظ المعطيات المتعلقة بحركة السير:

يقصد بإجراء أو إلتزام حفظ المعطيات المتعلقة بحركة السير قيام مزود الخدمات بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش وغيره، وحدد المشرع الوطني المعطيات الواجب حفظها من طرفهم وهي معطيات المرور التي أطلق عليها المشرع حركة السير[2].

ولقد عرف المشرع الوطني المعطيات المتعلقة بحركة السير في الفقرة هـ من المادة 02 من القانون 09-04 بأنها " المعطيات المتعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة".

وقد حدد المشرع في المادة 11 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها عدة طوائف من معطيات المرور، التي تدخل في نطاق الإلتزام بالحفظ من طرف مزود الخدمة وحصرها في المعطيات التي تسمح بالتعرف على مستعملي الخدمة، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال، المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها، المعطيات التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه.

---

[1]- حبيباتتي بثينة، المرجع السابق، ص 308.

[2] - المرجع نفسه، ص308.

ويعتبر هذا الإجراء مهم يساهم في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال سيما وأن البيانات المعلوماتية تكون قابلة للتلاشي، أو محلا للتلاعب أو التغيير، وبالتالي تحديد معالم الجريمة والكشف عن المجرمين قبل ضياع الأدلة.

ثالثا: إلتزام السحب الفوري للمحتوى غير المشروع:

إن المشرع الوطني زيادة على الإلتزامات المنصوص عليها في المادة 11 ألزم مقدمي الخدمات أيضا بموجب المادة 12 بالتدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، وذلك لخصوصية الجريمة المتصلة بتكنولوجيات الإعلام والإتصال التي اعتمد من خلال هذه المادة على الأسلوب الوقائي الذي يعتمد على الطرق التقنية للتصدي لها ومواجهتها وتفادي مخاطرها، والتي من بينها اعتماد نظام الترشيح والحجب وهو أسلوب لحجب صفحات معينة يمكن أن تكون مؤذية أو عدوانية أو إباحية بالنسبة لمستخدم الإنترنت، إذا حاول المستخدم الوصول إلى صفحة محجوبة ظهرت له رسالة تبلغه أن الوصول إلى الصفحة غير مسموح به[1]، إذ يتم من قبل مزودي الخدمات الذين يقدمون يد المساعدة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، التي تتكفل بها مديرية المراقبة الوقائية واليقظة الإلكترونية، فهذه التقنية تمنع النفاذ إلى المواقع، وتقيد حرية الإبحار عبر الإنترنت، إلا أنها تبقى ضرورية لحماية المنظومة المعلوماتية والمواطنين لكونها تساهم في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال لا سيما منع الشباب من والقصر من مواقع المخدرات والإرهاب والمواقع الإباحية، وذلك من خلال قيام مزودي الخدمات بإغلاقها.

---

[1]- أنيس العذار، " **مكافحة الجريمة الإلكترونية**"، **المجلة الأكاديمية للبحث القانوني**، المجلد 17، العدد01، 2018، ص 721-744، ص 734، 735.

رابعا: إلتزام وضع الترتيبات التقنية لمنع الوصول إلى الجمهور للمحتوى غير المشروع:

إن المشرع الوطني ونظرا لخصوصية الجريمة الإلكترونية اعتمد من خلال هذه المادة على الأسلوب الوقائي الذي يعتمد على الطرق التقنية للتصدي لها إضافة إلى أسلوب تنشيط أو تنظيم أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والإتصال، وحول المخاطر المتصلة بها، سيما وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة، وإخبار المشتركين لديهم بوجودها، إذ اعتمد تقنية التشفير وهي استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها، وتعتبر من أنجع الوسائل للحفاظ على سرية الوثائق الإلكترونية استنادا إلى نظام العد العشري الذي يسمح بجعل البيانات غير مفهومة بالنسبة لمن لا يملك المفتاح اللازم لفك الرموز، وكلما كانت هذه الرموز معقدة كلما كان اختراقها أصعب، إذ تضمن هذه التقنية تقنية التشفير الأمن على مستوى مواقع الانترنت الحساسة، سيما التي تمس الأمن القومي أو تلك المخصصة في التجارة والمبادلات المالية الإلكترونية، فتقنية التشفير تكفل درجة عالية من تحقيق السلامة المعلوماتية، وهي بذلك الحل الأمثل لقطع الطريق أمام القرصنة المعلوماتية[1].

خامسا: إقرار المسؤولية الجزائية عن عدم التقيد بالإلتزامات المقررة قانونا:

إن المشرع الوطني ألزم مقدمي الخدمات بموجب الإلتزامات المنصوص عليها في المادة 11 و12 من القانون 09-04 فضلا عن الإلتزامات المذكورة في دفتر الشروط، سيما وأنهم يتعاملون مع هيئات معينة لديهم التزامات يتوجب عليهم احترامها، وفي حالة عدم التزامهم قد يتعرضون للمتابعة الجزائية حتى لا يعرقلوا السير العادي للعدالة، إذ أن ذلك يعتبر صورة من صور الوقاية البعدية التي تجعلهم يلتزمون ولا يخلون بالإلتزامات المفروضة عليهم،

[1] – أنيس العذار، المرجع السابق، ص 736.

وتتراوح العقوبة من 6 أشهر حبس إلى 5 سنوات إضافة إلى الغرامة المالية من 50000 دج إلى 500000 دج، ويعاقب كذلك الشخص المعنوي، بالإضافة للعقوبات الإدارية، فيما يتعلق بالتزام حفظ المعطيات المتعلقة بحركة السير، كما يتعين عليهم كتمان سرية العمليات تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق طبقا للمادة 9 الفقرة الأخيرة منها، كما ان المادة 23 من المرسوم الرئاسي 21-439 في المادة 23 منه ألزم مستخدمي مقدمي الخدمات في علاقاتهم مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بواجب التحفظ ، وبالرجوع لنص المادة 394 مكرر 8 التي جاء بها القانون 16-02 المعدل والمتمم لقانون العقوبات نجدها أقرت المسؤوولية الجزائية لمقدمي خدمات الإنترنت الذي لا يقوم رغم إعذاره من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها أو صدور حكم أو أمر قضائي يلزمه بالإلتزامات المفروضة عليه بموجب المادة 12 من القانون 09-04، إذ يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 10000 دج إلى 2000000 دج أو بإحدة هاتين العقوبتين.

المبحث الثالث:

الآليات الوطنية والتعاون الدولي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال :

إن إعتماد المجرمين على تكنولوجيات الإعلام والإتصال في ارتكاب الجرائم، وما نجم عنه من سرعة في التنفيذ، جعل المشرع الوطني يعتمد أيضا على استخدامها أيضا في الوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وذلك من خلال إنشاء هيئة متخصصة تعتمد على التكنولوجيا الحديثة للوقاية من تلك الجرائم الخطرة على المستوى الوطني، كما أن الطابع العابر للحدود الوطنية الذي تتميز به هذه الجرائم حث على تعزيز التعاون الدولي في مجال الوقاية لأن الإعتماد على القدرات الوطنية الداخلية لا يكفي لوحده،

وإنما يتطلب تضامن جميع الجهات سواء على المستوى الوطني أو الدولي، وسيتم التطرق إلى ذلك فيما يلي:

المطلب الأول:

الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والإتصال ومكافحتها

لقد نص القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في المادة 13 منه على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والتي تتولى تنشيط وتنفيذ عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وسيتم توضيح ذلك فيما يلي:

الفرع الأول: التعريف بالهيئة:

إن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها تعد سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى رئيس الجمهورية، ويحدد مقرها بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي حسب المادة الثانية والثالثة من المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، وتجدر الإشارة إلى أنه في ظل المرسوم الرئاسي رقم 15—261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، كانت تعتبر سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى وزير العدل، وأما في ظل المرسوم الرئاسي رقم 19-172 المعدل بالإلغاء لأحكام المرسوم الرئاسي 15-261، فكانت الهيئة تعد مؤسسة عمومية ذات

طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني.

ومن الملاحظ أن المشرع الوطني كان يعتبرها أول مرة مؤسسة مدنية ثم أصبحت مؤسسة أمنية تخضع لوصاية وزارة الدفاع الوطني ، ثم عاد وجعلها تحت وصاية رئيس الجمهورية مرة أخرى، وكان ذلك نتيجة للظروف السياسية والأمنية التي عرفتها البلاد في تلك الفترة مما أدى إلى ظهور مخاطر فعلية على الأمن القومي والمؤسسات الدستورية للخطر مما يحتم أن تصبح هيئة ذات طابع أمني[1] سيما وأنها تهدف للوقاية من الأفعال الموصوفة بإعمال إرهابية أو تخريبية والمساس بأمن الدولة، إلا أن المشرع الوطني عاد مرة أخرى في آخر التعديلات إلى ضمان الحقوق والحريات أكثر سيما وأنها أصبحت مؤسسة تابعة لرئيس الجمهورية وأخضعها للرقابة القضائية باعتبار السلطة القضائية الضامن للحقوق والحريات.

الفرع الثاني: تنظيم وتشكيلة الهيئة:

تتكون الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها حسب المادة 05 من المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال من مجلس توجيه ومديرية عامة، يوضعان تحت سلطة رئيس الجمهورية، ويقدمان له عرضا عن نشاطاتهما.

ويتولى رئاسة مجلس التوجيه الأمين العام لرئاسة الجمهورية، ويتشكل من الأمين العام لوزارة الخارجية والجالية الوطنية بالخارج، والأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية، الأمين العام لوزارة العدل، الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية، قائد الدرك الوطني، المدير العام للأمن الداخلي، المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي، المدير العام للأمن الوطني، رئيس مصلحة الدفاع السيبيراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي، ممثل عن رئاسة الجمهورية

[1] -حكيمة بوكحيل وسامية بن عديد، المرجع السابق، ص 1544.

يعينه رئيس الجمهورية، كما يتولى المدير العام للهيئة أمانة مجلس التوجيه، طبقا لمقتضيات المادة 06 من المرسوم الرئاسي 21-439.

كما تتكون أيضا من المديرية العامة التي يديرها مدير عام يعين بموجب مرسوم رئاسي، وتنهى مهامه بنفس الأشكال.

كما أن المديرية العامة تضم مديرية الإدارة والوسائل ومصلحة للدراسات والتلخيص وملحقات جهوية، كما تضم مديرية المراقبة الوقائية واليقظة الإلكترونية بالإضافة إلى مصلحة للتعاون واليقظة التكنولوجية وهما المديريتان اللتان لهما اختصاصات وقائية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[1].

الفرع الثالث: الدور الوقائي للهيئة:

إن الهيئة تمارس العديد من الإختصاصات في سبيل الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ويظهر ذلك من خلال تكليف مجلس التوجيه على الخصوص بتوجيه عمل الهيئة والإشراف عليه ومراقبته، ودراسة كل مسألة تخضع لمجال اختصاص الهيئة والبت فيها، لاسيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للإتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمداولة حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ودراسة مخطط عمل الهيئة والموافقة عليه، والقيام بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والإتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة بدقة، واقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمداولة حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية

[1]- المادة 11 من المرسوم الرئاسي 21-439، الجريدة الرسمية العدد86 لسنة 2021، ص7.

والأجنبية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وتقييم كل اقتراح مفيد يتصل بمجال إختصاص الهيئة وإبداء رأيه في كل مسألة تتصل بمهامها وهي المهام التي تعتبر تفعيلا للدور الوقائي للهيئة، إذ يجتمع المجلس في دورة عادية مرة واحدة في السنة بناء على استدعاء من رئيسه، ويمكن الاجتماع في دورة غير عادية كلما كان ذلك ضروريا، بناء على استدعاء رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة، كما يعد تقريرا بعد كل دورة[1].

كما يسهر المدير العام للمديرية العامة للهيئة على حسن سير الهيئة ويتولى في هذا المجال المساهمة في الوقاية عن طريق اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها والسهر على تنفيذها، بالإضافة إلى مجموعة من المهام الإدارية التي يتولاها، المنصوص عليها في المرسوم الرئاسي 21-439، يقوم بإخطار رئيس الجمهورية فورا عن كل حادثة من شأنها المساس بأمن الدولة أو تلك المرتبطة بالأعمال الإرهابية أو التخريبية، كما يخطر أيضا رئيس أركان الجيش الوطني الشعبي عندما يتعلق الأمر بمسائل تخص الدفاع الوطني[2].

ومن بين المهام التي تقوم بها الهيئة في إطار الوقاية لا سيما ما ذكرته المادة 14 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمادة 04 من المرسوم الرئاسي 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم من خلال القيام بجمع المعلومات والتزويد بها والخبرات القضائية، تحديد الاستراتيجية الوطنية للوقاية

---

[1]- المادة 7 و8 من المرسوم الرئاسي 21-439، الجريدة الرسمية، العدد86 لسنة 2021، ص 6 و7.

[2] - المادة 9 و 10 من المرسوم الرئاسي 21-439، الجريدة الرسمية، العدد86 لسنة 2021، ص7.

من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ووضعها حيز التنفيذ، ضمان المراقبة الوقائية للإتصالات الإلكترونية تحت سلطة القاضي المختص قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية والتخريبية والتي تمس أمن الدولة، وضمان الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني المراقبة الإلكترونية عندما يتعلق الأمر بأمن الجيش، تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية، وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية، تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، والسهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي.

وتدعيما للدور الوقائي للهيئة وتأكيدا عليه فإن مديرية المراقبة الوقائية واليقظة الإلكترونية تكلف بتنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها، وتنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم والتعرف عليهم، وتنظيم والمشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والإتصال وحول المخاطر المتصلة بها، والسهر على إنجاز مهام اليقظة الإلكترونية، كما تضع مديرية المراقبة الوقائية واليقظة الإلكترونية على مستوى المنشآت القاعدية لمتعاملي ومقدمي خدمات الإتصال الالكترونية الأجهزة التقنية الضرورية لتنفيذ مهامها، كما يلزم متعاملوا ومقدمو الخدمات بمدها المساعدة الضرورية [1] ، كما تكلف مصلحة التعاون واليقظة التكنولوجية بالتعاون مع الشركاء فيما يخص تنفيذ عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، واليقظة الدائمة في متابعة تكنولوجيات الإعلام والإتصال المتعلقة بنشاطات الهيئة[2].

---

[1] – المادة 14 و15 منمن المرسوم الرئاسي 21–439، الجريدة الرسمية، العدد86 لسنة 2021، ص8.

[2]– المادة 18 من المرسوم الرئاسي 21–439، الجريدة الرسمية، العدد86 لسنة 2021، ص8.

كما أن المشرع ألحق بالهيئة بعض الموظفين المتخصصين لا سيما وأن لها صلاحيات فرض تدابير وقائية للوقاية من الجرائم الإرهابية والتخريبية والجرائم الماسة بأمن الدولة، وبالإقتصاد الوطني، ضباط وأعوان الشرطة القضائية مؤهلون من المصالح العسكرية للأمن والدرك الوطني والأمن الوطني، ومستخدمي الدعم التقني والإداري للمصالح العسكرية للأمن المختصة والدرك الوطني والأمن الوطني، نظرا لخصوصية الجرائم المتصلة بتكنولوجيات الإعلام والإتصال طبقا للمادة20 من المرسوم الرئاسي 21-439، ومن الملاحظ على هذا التعديل الأخير أنه ألحق القضاة بالهيئة لتسييرها قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو التي تمس بأمن الدولة ومكافحتها، عندما تكلف حصريا في مجال اختصاصها بمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها داخل منظومة معلوماتية تحت سلطة قاض لدى الهيئة، والخضوع لأحكام قانون الإجراءات الجزائية لا سيما فيما يخص التفتيش والحجز طبقا للمادة 20 و25 من المرسوم21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، فالمشرع الوطني أخضع الإجراءات التي تقوم بها إلى الإشراف القضائي تدعيما للحقوق والحريات، كضمانة لتحقيق التوازن بين المصالح العليا للوطن وحقوق الأفراد وحماية حرياتهم.

المطلب الثاني:

التعاون الدولي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

نظرا لاتساع رقعة الإجرام المعلوماتي العابر للحدود الوطنية، فارتكاب الجريمة يتم عن طريق المنظومة المعلوماتية في إقليم دولة، ويتم التنفيذ في إقليم دولة أخرى، نتيجة التطور التكنولوجي ووسائل الإتصال، فأصبحت الجماعات الإجرامية تنافس سلطات الدول وتزعزع النظام الإقتصادي والديمقراطيات الحديثة وتهدد أمن الدول، ونتيجة لذلك وجب على الدول اللجوء إلى التعاون الدولي لا سيما في مجال الوقاية، لمنع وقوع الجرائم المتصلة

بتكنولوجيات الإعلام والإتصال أصلا ودرء خطرها وتجنب آثارها السلبية، تماشيا مع توجهات السياسة الجزائية الحديثة وسيتم توضيح ذلك فيما يلي:

الفرع الأول: مفهوم التعاون الدولي في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

لقد عمل المشرع الوطني على رسم سياسة جزائية فعالة في مجال منع الجريمة وتحقيق العدالة، وبالنظر لخصوصية الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، يتطلب اللجوء إلى التعاون الدولي الأمني أو التعاون الدولي في مجال الوقاية مثلما هو عليه الأمر بالنسبة للمكافحة، وذلك من خلال اتخاذ جميع الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة، وسيتم توضيح ذلك فيما يلي:

أولا: التعريف بالتعاون الأمني الدولي في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

يقصد بالتعاون الدولي تكاثف جميع الدول على المسائل الدولية ذات الصبغة الإقتصادية الاجتماعية والثقافية والانسانية وعلى تعزيز احترام حقوق الإنسان والحريات الأساسية للناس جميعا في العالم وقد جاء هذا المبدأ في سياق أهداف أو مقاصد الأمم[1]، ويقصد به تقديم الدول لبعضها البعض أكبر قدر ممكن من المبادرات القانونية المساعدة في مجال التحقيقات والإجراءات القضائية خاصة فيما يتعلق بالجرائم المحددة في الإتفاقيات المبرمة فيما بينهم[2]، ويدل مصطلح التعاون الدولي على إحساس بتضامن الدول فيما بينها لتلاقي الأخطار التي تهدد أمن وسلم كل منهما[3]، وهو استجابة دولة بناء على طلب دولة أخرى لتمد شتى أنواع المعلومات المساعدة في مسائل الجرائم ذات الطابع العابر للحدود[4].

---

[1]– عمر سعد الله، معجم في القانون الدولي المعاصر، الجزائر، ديوان المطبوعات الجامعية، ط2، 2007، ص 127.

[2] –جهاد محمد البريزات، الجريمة المنظمة، عمان، دار الثقافة للتصميم والإنتاج، 2010، ص 168.

[3] – عبد الله نوار شعت، تسليم المجرمين، الإسكندرية، مكتبة الوفاء القانونية، ط1، ص 168.

[4] – مختار شلبي، الجهاز العالمي لمكافحة الجريمة المنظمة، الجزائر، دار هومه للطباعة والنشر، ص 228.

والتعاون الدولي في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال يتمثل في اتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة المتصلة بتكنولوجيات الإعلام والإتصال، وهي الآليات الأمنية[1]، وهي لا تتعلق بإجراءات الملاحقة والمتابعة بعد ارتكاب الجريمة وإن كان للردع أيضا أثرا وقائيا.

ثانيا: صور التعاون الدولي في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

تتخذ صور التعاون الدولي في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال صورة تبادل المعلومات، وصورة الإنابة الدولية، وترتبط هذه الصور بما تقدمه الدولة من إجراءات من شأنها تسهيل الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في دولة أخرى بصدد الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وتعتبر الإتفاقيات الدولية منبع الالتزامات بين الدول على أن يظل ما ليس ملزما ممكنا وفقا لما ينص عليه القانون الداخلي في كل من الدولتين، ويقصد بتبادل المعلومات تقديم أو إعطاء المعلومات والوثائق والمواد الاستدلالية التي تطلبه سلطة قضائية أو أمنية أجنبية متى كانت بصدد جريمة من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، عن الشكوك أو الشبهات التي وجهت على رعاياها في الخارج، أو إحتمالية ارتكاب إحدى الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الماسة بأمن الدولة أو الإقتصاد الوطني أو الجرائم الإرهابية، وقد يشمل أيضا السوابق القضائية للأفراد، الذي تتعرف من خلاله الجهات القضائية أو الأمنية على الماضي الجنائي للفرد[2] .

وأما الإنابة الدولية فهي تعبر عن قيام دولة ما بمباشرة إجراء من الإجراءات الوقائية يتعلق الأمر بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال داخل الحدود الإقليمية لدولة

---

[1] – فريد ناشف، " **آليات التعاون الدولي في مكافحة الجرائم الإلكترونية**"، **مجلة البحوث في الحقوق والعلوم السياسية**، المجلد 8، العدد 01، 2022، ص 430-450، ص 437.

[2] –المرجع نفسه، ص440.

أخرى نيابة عنها، وبناء على طلب تلك الدولة المناب عنها، ووفقا لما تقرره بنود الإتفاقية بين الدولتين في هذا الشأن، وتهدف الإنابة على تسهيل الإجراءات بين الدول وتذليل العقبات التي تعترض سير الإجراءات أم التطور السريع لهذا النوع من الإجرام، والتغلب على عقبة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال داخل أقاليم الدول الأخرى تماشيا مع سرعة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

وفي إطار الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال أقرت اتفاقية بودابست تبادل المعلومات في المادة 23 منها بنصها صراحة على وجوب توافر التعاون الدولي بين الدول الأطراف وتعميقه، وتقليل العوائق، بما يوفر أكبر قدر من السهولة والسرعة لتبادل المعلومات والأدلة بين الأطراف.

ثالثا: آليات تنفيذ التعاون الدولي في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

تتمثل آليات تنفيذ التعاون الدولي في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، في الجهود التي تبذلها الشرطة الجنائية الدولية الأنتربول باعتبارها الكيان الدولي الذي ياخذ على عاتقه القيام بمهمة التعاون الأمني الدولي لا سيما من خلال تبادل المعلومات المتعلقة بالمجرمين والجريمة بأقصى سرعة ممكنة، وتهدف هذه المنظمة على تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف من تجميع البيانات والمعلومات حول الجريمة والمجرم، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها، كما تتمثل أيضا في إبرام الإتفاقيات الدولية المتعددة الأطراف أو الثنائية للمحافظة على الثقة المتبادلة بين الدول في تقديم المساعدة الفنية والتقنية والأمنية ومن بين الاتفاقيات الدولية التي تعمل على التعاون الدولي في مجال الجرائم المتصلة بتكنولوجيات الإعلام والإتصال معاهدة بودابست لا سيما ما نصت عليه في المادة 23 منها " تتعاون كل الأطراف وفقا لنصوص هذا الفصل على تطبيق الوسائل

الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وكذلك بشأن الحصول على الأدلة في الشكل الإلكتروني لمثل هذه الجرائم" والمادة 25 منها التي نصت " تتفق الأطراف على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وجمع الأدلة في الشكل الإلكتروني" والمادة 25 الفقرة الثالثة على أنه " يمكن لكل طرف في الحالات الطارئة أن يوجه طلبا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها (ويدخل ضمن ذلك الكتابة السرية إذا لزم الأمر) مع تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك، وتقوم الدولة بالموافقة على هذا الطلب والرد عن طريق إحدى وسائل الإتصال السريعة".

الفرع الثاني: الأحكام الوقائية للتعاون الدولي في القانون الجزائري:

إن المشرع الجزائري نص على الأحكام الوقائية في إطار التعاون الدولي ضمن القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ويظهر ذلك من خلال ما نصت عليه المادة 04 التي نصت على إمكانية اللجوء إلى استخدام المراقبة الإلكترونية الوقائية في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، وذلك بالنسبة للأشخاص المقيمين بالخارج الذين يحتمل تورطهم في عمل إجرامي يمس بمصالح الدولة الأجنبية وفي إطار المعاملة بالمثل.

ولقد نصت المادة 17 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، أنه تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية

الثنائية ومبدأ المعاملة بالمثل، كما نصت المادة 16 أنه في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، وأنه في حالة الإستعجال ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها، وهي المهام المسندة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها طبقا للمادة 14 الفقرة ج التي نصت تتولى الهيئة تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وتحديد مكان تواجدهم، ووضعت المادة 18 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، قيودا عن هذه الإجراءات بنصها أنه يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام، وألزمت أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

الخاتمة:

لقد واجه المشرع الجزائري الجرائم المتصلة بتكنولوجيات الإعلام والإتصال من خلال الإعتماد على أسلوب المكافحة من جهة إلى جانب أسلوب الوقاية من الجهة الأخرى، وهو ما تجلى في التعديلات المختلفة لقانون العقوبات وقانون الإجراءات الجزائية واستحداث قانون خاص للوقاية والمكافحة، بهدف الحيلولة دون انتشار هذه الجرائم الخطرة

والمشرع الوطني لم يكتف بوضع نصوص قانونية ردعية تجريمية وعقابية وأحكام إجرائية، بل اتجه نحو إعتماد السياسة الجزائية الوقائية وتبنى أسلوب الوقاية الذي يظهر أيضا في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والمرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال نظرا لخصوصية هذا النوع من الإجرام لارتباطه بسائر أشكال الجريمة خصوصا جرائم الإرهاب والجريمة المنظمة عبر الحدود الوطنية والفساد، ذلك أن سياسة المكافحة لوحدها لا تكفي، وإنما يتوجب الإعتماد على السياسة الجزائية الوقائية تماشيا مع توجهات السياسة الجزائية الحديثة.

يظهر توجه المشرع الجزائري نحو اعتماد الأسلوب الوقائي في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في العديد من النصوص القانونية سواء في القانون 09-04 والمرسوم الرئاسي رقم 21 -439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، سواء بصفة صريحة أو بصفة ضمنية.

بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال كافة التدابير والآليات اللازمة للحيلولة دون ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية، سواء من خلال الإعتماد على الأساليب الوقائية القبلية الإستباقية لا سيما من خلال دور المحيط الإجتماعي الأسرة، المدرسة، المسجد أو من خلال مؤسسات

المجتمع الرسمية وجمعيات المجتمع المدني لمنع وقوع الجريمة أصلا، بالإضافة إلى أساليب الوقاية البعدية اللاحقة أثناء ارتكاب الجريمة أو بعدها لوقف وقوع الجريمة والتصدي لها وعدم تكرارها مستقبلا من جهة أخرى، وهي الإجراءات اللازمة لمنع المجرم من العود إلى ارتكاب الجريمة، أو الأساليب الإجرائية التي تمكن من ايقاف ارتكاب الجريمة أو منع الضرر الذي تحدثه الجريمة، سيما من خلال اتخاذ جميع الإجراءات بالإعتماد على الأسلوب العلمي التكنولوجي لمواجهة الجريمة المتصلة بتكنولوجيات الإعلام والإتصال المتوقعة أو مواجهة مضاعفات الجريمة التي وقعت فعلا، وذلك من خلال إعتماد المفهوم الواسع للوقاية من الجريمة، إذ يتضح ويتبين أن الإجراءات التي وضعها المشرع لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال تستهدف الوقاية من جهة والمكافحة من جهة أخرى، إذ يكون لكل إجراء دور وقائي استباقي يهدف إلى منع وقوع الجريمة أصلا، أو كبح مضاعفاتها أو إعاقتها أو إيقاف الضرر الناتج عنها أو احتمالية ارتكابها، وكذلك دور مكافحة بعد ارتكاب الجريمة للكشف عن مرتكبيها والتحقيق معهم للوصول إلى الدليل الرقمي الذي يدين المتهم أو يبرئه، فالعلاقة بين الوقاية والمكافحة هي علاقة تكاملية تهدف كلاهما إلى التصدي للجرائم المتصلة بتكنولوجيات الإعلام والإتصال،

إن المشرع الوطني اعتمد على الأسلوب الوقائي، إذ جعل لأساليب المكافحة المتمثلة في المراقبة الإلكترونية، والتفتيش الإلكتروني، وحجز المعطيات المعلوماتية دورا وقائيا أيضا، كما أقر إلتزامات لمقدمي الخدمات، وذلك بهدف الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وهو الأمر الذي يمس بالخصوصية الفردية وبسرية المراسلات والإتصالات دون علم ورضا الفرد، مما جعله في نفس الوقت يقر ضمانات قانونية للموازنة بين المصلحة العامة والمصلحة الخاصة.

وقد أنشأ المشرع هيئات ومؤسسات على المستوى الوطني تتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها التي لها دور فعال ومساعد في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، كما أقر قواعد التعاون الدولي نظرا للطابع العابر للحدود الوطنية، وذلك للتصدي لهذا الإجرام.

قائمة المصادر والمراجع:

أولا: المصادر:

1-القوانين:

- القانون 04-15 المؤرخ في 10نوفمبر 2004، المعدل والمتمم للأمر رقم 66 -156 المؤرخ في 08/يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 المؤرخة في 10/نوفمبر/2004.

- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد84 المؤرخة في 24 ديسمبر 2006.

- القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66 - 156 المؤرخ في 08/يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد84 المؤرخة في 24 ديسمبر 2006.

- القانون 09-04 المؤرخ في 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد47، المؤرخة في 16 غشت 2009.

- القانون رقم 16-02 المؤرخ في 19 يونيو 2016 المعدل والمتمم للأمر رقم 66 -156 المؤرخ في 08/يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد37 المؤرخة في 22 يونيو 2016.

- القانون 18-04 المؤرخ في 10 ماي 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، الجريدة الرسمية العدد 27، 2018.

2-الأوامر:

- الأمر20-04 المؤرخ في 11 غشت 2020، المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد51 المؤرخة في 31 غشت 2020.

- الأمر 21-11 المؤرخ في 25 أوت 2021، المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 65 المؤرخة في 26 غشت 2021.

3-المراسيم:

- المرسوم الرئاسي 15-261 المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد53 المؤرخة في 8 أكتوبر 2015.
- المرسوم الرئاسي 19-172 المؤرخ في 06 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها تنظيمها وكيفيات سيرها، الجريدة الرسمية العدد37 المؤرخة في 09 يونيو 2019.
- المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/07، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، الجريدة الرسمية العدد 86 المؤرخة في 11 نوفمبر 2021.

ثانيا:المراجع:

1-المراجع باللغة العربية:

أ-الكتب:

- احسن طالب، الوقاية من الجريمة، لبنان، بيروت، دار الطليعة للطباعة والنشر، الطبعة الأولى، 2001.
- أحمد المناعسة، جرائم الحاسب الآلي والإنترنت، عمان، دار وائل للنشر والتوزيع، ط1، 2001.
- أحمد حويتي، دور البحث العلمي في الوقاية من الجريمة والإنحراف، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، ط1، 2001.
- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الإسكندرية، دار الفكر الجامعي، ط1، 2011.
- بوكر رشيدة، جرائم الإعتداء على نظام المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن، لبنان، منشورات الحلبي الحقوقية، ط1، 2012.

- جهاد محمد البريزات، الجريمة المنظمة، عمان، دار الثقافة للتصميم والإنتاج، 2010.
- جيرار كورنو، معجم المصطلحات القانونية، ترجمة منصور القاضي، المؤسسة الجامعية للدراسات والنشر، الطبعة الأولى، 1998.
- حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت، عالم الكتاب الحديث، ط1، 2009.
- رمسيس بهنام، الإجرام والعقاب " علم الإجرام وعلم الوقاية والتقويم"، مصر، الإسكندرية، منشأة المعارف، 1978.
- رمسيس بهنام، علم الوقاية، التقويم والأسلوب الأمثل لمكافحة الإجرام، الإسكندرية، منشأة المعارف، 1986.
- سامي حسن الحسيني، النظرية العامة للتفتيش، القاهرة، دار النهضة العربية، 1972.
- طارق ابراهيم الدسوقي عطية، الامن المعلوماتي (النظام القانوني للحماية المعلوماتية)، مصر، الاسكندرية، دار الجامعة الجديدة للنشر، 2009.
- عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، الجزائر، دار بلقيس للنشر، 2015.
- عبد الله العزيز اليوسف، المفهوم الحديث للوقاية من الجريمة والإنحراف، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، ط1، 2003.
-عبد الله نوار شعت، تسليم المجرمين، الإسكندرية، مكتبة الوفاء القانونية، ط1،2016.
-عمر سعد الله، معجم في القانون الدولي المعاصر، الجزائر، ديوان المطبوعات الجامعية، ط2، 2007.
- فضيل العيش، شرح قانون الإجراءات الجزائية بين النظري والتطبيقي، الجزائر، دار البدر، 2008.
- محجوب حسن سعد، الشرطة ومنع الجريمة، الرياض، أكاديمية نايف العربية للعلوم الأمنية، الطبعة الأولى، 2001.
- محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي، القاهرة، دار الفكر العربي، 1998.
- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت الجريمة المعلوماتية، عمان، دار الثقافة للنشر والتوزيع، ط1، 2007.

-محمد حسين منصور، المسؤولية الإلكترونية، مصر، الاسكندرية، دار الجامعة الجديدة، 2003.

- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مصر، دار النهضة العربية، ط1، 1998.

-مختار شلبي، الجهاز العالمي لمكافحة الجريمة المنظمة، الجزائر، دار هومه للطباعة والنشر،2003.

- مصطفى سويف، المخدرات والمجتمع، نظرة تكاملية، الكويت، سلسلة عالم المعرفة، رقم 2050، المجلس الوطني للثقافة والفنون، 1996.

-نبيه صالح، دراسة في علمي الإجرام والعقاب، عمان، دار العليمة الدولية، ط1، 2003 .

- نهلا عبد القادر المومني ، الجرائم المعلوماتية، الأردن، عمان، دار الثقافة للنشر والتوزيع، ط1، 2008.

-هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية (دراسة مقارنة) مصر، دار النهضة العربية، ط1، 2000.

ب-الأطروحات ورسائل الماجستير:

- بثينة حبيباتني، الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، أطروحة لنيل شهادة دكتوراه ل . م .د في القانون العام تخصص القانون الجنائي وعلم الإجرام، جامعة الجزائر1، كلية الحقوق،14 سبتمبر 2020.

- عكو فاطمة الزهرة، المسؤولية المدنية لمقدمي الخدمة الوسيطة في الانترنت، رسالة لنيل درجة الدكتوراه في القانون، جامعة الجزائر1، كلية الحقوق، 2016/2015.

- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم 09-04، مذكرة ماجيستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، تخصص قانون جنائي، 2013/2012.

ج-المجلات:

- أنيس العذار، " **مكافحة الجريمة الإلكترونية**"، **المجلة الأكاديمية للبحث القانوني**، المجلد 17، العدد01، 2018.

- حكيمة بوكحيل وسامية بن عديد، " **الهيئة الوطنية للوقاية من جرائم الإعلام وتكنولوجيا الإتصال ودورها في تفتيش نظم المعلوماتية**"، **مجلة الدراسات القانونية المقارنة**، المجلد 07، العدد 01، 2021.

- رضا هميسي، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، **مجلة العلوم القانونية والسياسية**، العدد5، جوان 2012.

- عبد الحليم بن بادة، " **المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني**"، **المجلة الأكاديمية للبحث القانون**، جامعة عبد الرحمان ميرة بجاية، المجلد 10، العدد 03، 2019.

- عبد القادر فلاح، " **حجز وحفظ المعطيات في الجريمة الإلكترونية**"، **مجلة صوت القانون**، المجلد 08، العدد 01، سنة 2021.

- فريد ناشف، " **آليات التعاون الدولي في مكافحة الجرائم الإلكترونية**"، **مجلة البحوث في الحقوق والعلوم السياسية**، المجلد 8، العدد 01، 2022.

- فطيمة جبار، " **مراقبة الإتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري**"، **مجلة الدراسات القانونية المقارنة**، جامعة حسيبة بن بوعلي الشلف الجزائر، مخبر القانون الخاص المقارن، العدد الثالث، ديسمبر2016.

- هشام رستم، "جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة"، بحث مقدم إلى اللجنة العلمية لإعداد التقرير الوطني المصري لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين، جامعة أسيوط، مجلة الدراسات القانونية، العدد 17، 1995.

د- المواقع الإلكترونية:

https://rm.coe.int/budapest-convention-in-arabic/1680739173

2-المراجع باللغة الأجنبية:

-Mohamed CHAWKI, Combattre la cybercriminalité, France, Edition de Saint Amans,2008.
-Irvin waller, "Crime prevention between theory and practice", paper presented at International crime prevention colloque, abu dhabi,1996.
-MERWE Vander, « computer crimes and other crimes against information technology in south africa », R.I.D.P, 1993.
-K. Trédmann, Fraud et autres délits d' affaire commis a l'aide d'ordinateurs électroniques, rev dr.pén.crim, 1984.
- M.MASS, Le droit pénal spécial né de l'informatique, in informatique et droit pénal travaux de l'institut de sciences criminelles de poietiers, 4 éd, Cujas, 1981
-D.B Parker, combattre la criminalité informatique, éd oros, 1985.
-Anne BRISSET-GIUSTINIANI, aspects juridiques de l'émergence d une sécurité européenne des réseaux et des systèmes d'information, mémoire DESS Droit de l internet –administration –entreprise, université panthéon Sorbonne, paris1, disponible sur www.univ-paris1.fr/..../2004_sept_ok_Brisset_Giustnani_version_....

الفهرس:

مقدمة.....ص 01.

المبحث الأول: الأهداف ومجال التطبيق.....ص03.

المطلب الأول: المواجهة التشريعية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....ص03.

الفرع الأول: مظاهر المكافحة والوقاية في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص03.

الفرع الثاني : مبررات الإعتماد على الوقاية والمكافحة في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص09.

المطلب الثاني: مفهوم الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص13

الفرع الأول: التعريف بالوقاية من الجريمة.....ص13.

الفرع الثاني: التعريف بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص16.

الفرع الثالث: المفهوم الإجرائي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص20.

المبحث الثاني:إجراءات وضمانات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص22.

المطلب الأول:الدور الوقائي لمراقبة الإتصالات الإلكترونية والتفتيش الإلكتروني وحجز المعطيات المعلوماتية.....ص 22.

الفرع الأول: مراقبة الإتصالات الإلكترونية.....ص 22.

جامعة محمد البشير الإبراهيمي برج بوعريريج
كلية الحقوق والعلوم السياسية
المجلس العلمي للكلية
وزارة التعليم العالي والبحث العلمي

الفرع الثاني: تفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية.....ص32.

المطلب الثاني:الدور الوقائي لمقدمي الخدمات.....ص42.

الفرع الأول: مفهوم مقدمي الخدمات.....ص42.

الفرع الثاني: إلتزامات مقدمي الخدمات.....ص44.

المبحث الثالث:الآليات الوطنية والتعاون الدولي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص49.

المطلب الأول:الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والإتصال ومكافحتها.....ص50.

الفرع الأول: التعريف بالهيئة.....ص50.

الفرع الثاني: تنظيم وتشكيلة الهيئة.....ص51.

الفرع الثالث: الدور الوقائي للهيئة.....ص52.

المطلب الثاني:التعاون الدولي للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص55.

الفرع الأول: مفهوم التعاون الدولي في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.....ص56.

الفرع الثاني: الأحكام الوقائية للتعاون الدولي في القانون الجزائري.....ص59.

الخاتمة.....ص61

قائمة المصادر والمراجع.....ص63.

الفهرس.....ص69.