2- آليات مكافحة الجريمة الإلكترونية في ضوء قانون العقوبات الجزائري.

Mechanisms to combat cybercrime in light of algeria's penal code

إعداد الدكتور: أحمد برادي

المركز الجامعي تمنراست/قسم الحقوق/ الجزائر.

الملخص:

تعد الجرائم الإلكترونية من أخطر الجرائم المستحدثة جراء التطور التكنولوجي، وهي بصفة عامة كل الجرائم المتصلة بالمعلوماتية، ولقد سعى المشرع الجزائري للتصدي لها، من خلاله استحداثه لعدة جرائم تلحق أضرارا بأنظمة المعالجة الآلية للمعطيات، كجرائم الدخول والبقاء غير المرخصين، وتعديل معلومات النظام أو محوها..وغير ذلك، كما أقر عدة إجراءات غير مألوفة تتمثل في اعتراض المراسلات، تسجيل الأصوات، التقاط الصور والتسرب. ولقد خلصت الدراسة إلى أنه وبالرغم من المجهودات التي قام بها المشرع الجزائري إلا أنها تعد غير كافية لعدة أسباب أهمها سرعة التطور التكنولوجي، وعليه فلا بد من مواكبة هذا التطور بالتعديلات الموازية لقانون العقوبات، وتوسيع الاتفاقيات الإقليمية والدولية من أجل التعاون للحد من هذه الجرائم والتصدي للمجرمين.

الكلمات المفتاحية: الجرائم الإلكترونية، المعلوماتية، أنظمة المعالجة الآلية للمعطيات، جرائم المعلوماتية.

Abstract:

Cybercrime is one of the most serious crimes created by technological development, which is generally all crimes related to informatics, and the Algerian legislature has sought to address them, through which it has developed several crimes that damage the automated data processing systems, such as non-entry and survival crimes. Licensees, modify ing or erasing system information. Otherwise, he also approved several unusual procedures such as interception of correspondence, recording of sounds, taking pictures and leaking. The study concluded that despite the efforts made by the Algerian legislator, it is insufficient for several reasons, the most important of which is the speed of technological development, and therefore it is necessary to keep up with this development with parallel amendments to the Penal Code, and to expand regional and international agreements in order to cooperate to reduce of these crimes and tackling criminals.

Keywords:

Cybercrime, Informatics, Automated Data Processing Systems, Informatics Crimes.

مقدمة:

. يعيش العالم اليوم في بيئة إلكترونية لم يشهدها من قبل نتيجة تطور تكنولوجيات الإعلام والاتصال، وظهور أدوات تقنية حديثة ومتطورة كالإعلام الآلي، الهواتف النقالة، الانترنيت وما يتصل بها من برامج وتقنيات رهيبة، مما أثر على العقود المدنية بين أشخاص القانون الخاص أو حتى تلك التي يكون أحد طرفيها شخصا من أشخاص القانون العام، وتغيرت الخدمات الإدارية المقدمة من قبل الإدارة للمواطنين...وغير ذلك. حيث أن جل هذه المعاملات أصبحت ذات صبغة إلكترونية مما جعلها تتسم بالسرعة الكبيرة جدا، والتقنيات العالية.

. وبعدما أصبحت أركان هذه الأفعال الجرمية المستحدثة ووصفها لا يتناسب مع الجريمة التقليدية، فقد خلق ذلك فراغاً قانونياً، وحال دون تجريم الفاعلين وفقاً للمادة الأولى التي تنص على مبدأ المشروعية في الشق الجنائي، والقاضي بأنه: «لا جريمة ولا عقوبة ولا تدابير أمن إلا بنص.»هذا ما كان الدافع الرئيسي وراء تعديل قانون العقوبات الجزائري بمقتضى قانون 04/15 المؤرخ في: 10 نوفمبر 2004، والذي جرمت بمقتضاه بعض صور الجريمة المعلوماتية، ثم ظهرت فيما بعد نصوص خاصة تجرم صورا أخرى من هذا النوع من الجرائم، من أجل وضع إطار قانوني لمجابهة الانحرافات المتصلة بعالم التكنولوجيا الإلكترونية المتطورة، ووضع حد للمجرمين في هذا المجال.

أولا: أهمية الموضوع: يحظى هذا الموضوع بأهمية كبيرة جداً، نقتصر على أهمها، ضمن النقاط الآتية:

1_ تعد الجريمة الإلكترونية من الجرائم المستحدثة باعتبارها تمس الأنظمة المعلوماتية المتعلقة بالأجهزة الإلكترونية ووسائل الاتصال الحديثة.

2_ ارتكاب هذا النوع من الجرائم يحتاج إلى الذكاء أحياناً، وتحكم الشخص في المجال والإلكتروني وتقنيات الإعلام الآلي والبرمجيات...وغيرها.

3_ قد تؤدي الجريمة الإلكترونية إلى المساس بأمن الدولة والتعدي على سيادتها، وهذا ما يوجب تبيين مدى خطورة هذه الأفعال الجرمية، وعواقب ارتكابها.

الجريمة الإلكترونية تعد من الجرائم المنظمة، التي تدخل في إطار الجرائم الدولية العابرة للحدود، مما يستلزم تضافر الجهود في مكافحتها والحد من انتشارها.

ثانياً: أهداف الموضوع: تتمثل أهداف هذه الورقة البحثية فيما يلي:

1_ تبيين مدى اهتمام المشرع الجزائري بمكافحة الجريمة الإلكترونية، ومتابعته لجميع المستجدات ومواكبتها، والسعي لتكييف قوانينه على حسابها، من اجل مكافحة الجريمة بشتى أنواعها، والمحافظة على امن المواطنين، والسهر على حمايتهم.

2_ توسع دائرة الجريمة، بحيث أصبحت لا تقتصر فقط على الجريمة التقليدية .

3_ تهذيب استخدام الوسائل الإلكترونية دون المساس بالغير وانتهاك حرماتهم والتعدي على أسرارهم.

4_ الحد من انتشار هذه الجرائم، الذي من شأنه أن يؤثر على التعاملات الإلكترونية، ويؤدي إلى عزوف المتعاملين على اللجوء إليها.

ثالثاً: إشكالية البحث:

. سعى المشرع الجزائري إلى مكافحة الجريمة الإلكترونية، والحد من انتشارها، عن طريق استحداثه للعديد من القوانين، فما مدى فاعلية هذه النصوص القانونية في الحفاظ على الأنظمة المعلوماتية والمعطيات الإلكترونية وحمايتها؟

رابعاً: منهج البحث:

. اعتمدت في هذا البحث المنهج الاستقرائي، الذي أقوم من خلاله بتتبع النصوص القانونية وتفسيرها وشرحها، من أجل الوصول إلى مضمونها وما يصبوا إليه المشرع من أهداف بمقتضاها.

خامساً: خطة البحث:

للإجابة عن هذا الإشكالية المطروحة قسمت البحث إلى محورين: المحور الأول يتحدث عن ماهية الجريمة الإلكترونية، أما المحور الثاني فخصص لآليات مكافحة الجرائم الإلكترونية.

سادساً: صلب الموضوع:

المحور الأول: ماهية الجريمة الإلكترونية:

. تعتبر الجريمة الإلكترونية من الجرائم الحديثة التي ظهرت بالموازاة مع انتشار الثورة التقنية، في إطار التطور الذي شهدته الجريمة، حيث أصبح هناك نوع جديد من الجرائم، يرتبط بالتكنولوجيا المعلوماتية والانترنيت أطلق عليه مصطلح الجريمة الإلكترونية، لذا سأتحدث تحت هذا المحور عن مفهوم الجريمة الإلكترونية وتفريقها عما يشابهها من جرائم، ثم انتقل إلى خصائصها.

أولاً: مفهوم الجريمة الإلكترونية:

. لم يتطرق المشرع الجزائري إلى تعريف الجريمة الإلكترونية وإنما ترك الأمر للفقهاء.

. وتتكون الجريمة الإلكترونية أو الافتراضية بوجه عام من مقطعين هما: الجريمة (crime)، والإلكترونية (cyber)، ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون[1].

. ولقد تعددت التعاريف الفقهية حول الجريمة الإلكترونية، لذا سنقتصر على البعض منها:

أ_ عرفها الفقيه **باركر** بقوله: «هي كل فعل إجرامي متعمد إذا كانت صلته بالمعلوماتية تنشأ عن خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.[2]»

ب_ كما عرفها الفقيه **ناديمان** على أنها: «الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا، وأنها تستهدف سرية المعلومات وسلامتها ووجودها والأجهزة ومحتوياتها بغرض تخريبها.[3]»

(1) مقال بعنوان: الجرائم الإلكترونية «الأهداف–الأسباب–طرق الجريمة ومعالجتها–، منشورة بتاريخ:. أوت 2016م على الموقع الإلكتروني: de.democraticac.www، تاريخ الاطلاع: 03/05/2019.

(2) عبد القادر ورسمه غالب، مقال منشور على الموقع الإلكتروني: com.makkahnewspaper.www، بتاريخ: 19 أكتوبر 2017م. تاريخ الاطلاع: 05/09/2019م

(3) عبد القادر ورسمه غالب، نفس الموقع.

ج_ وساق الفقيه **علي العريان** تعريفا للجريمة الإلكترونية، حيث قال إنها: «كل فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على تقنية المعلوماتية أية كان غرض الجاني.[1]»

د_ وعرفها الفقيه الفرنسي **ماس** بقوله: «الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض الربح.[2]»

من هذه التعاريف نرى أن الفقهاء اتفقوا على أن هذا النوع من الجرائم يتصل بالمعلوماتية، ويستهدف الاعتداء العمدي على البيانات الإلكترونية، ولو أن العريان ذهب إلى أن مجرد الاعتداء العمدي يحقق النتيجة دون النظر إلى غرض الجاني أو النتيجة الجرمية من وراء ارتكابه للجريمة، بينما الفقهاء الآخرين باركر ونانديمان وماس ركزوا على الغرض من وراء الجرم، وجعلوه ركنا أساسيا في تحقق الفعل المادي للجريمة، والذي هو التخريب في نظر نانديمان أي أنه غلب الجانب السلبي، أما الفقيه ماس فقد آثر الجانب الإيجابي والمتمثل في الربح الذي يحققه الفاعل، بينما باركر كان أشمل حيث أنه جمع بين الجانب السلبي الذي هو خسارة المجني عليه، والجانب الإيجابي للجريمة وهو حصول الجاني على أرباح من ورائها.

2_ خصائص الجريمة الإلكترونية:

. اتسمت الجريمة الإلكترونية بعدة ميزات وخصائص جعلتها تختلف عن غيرها من الجرائم، تتمثل في ما يلي:

1_ الجريمة الإلكترونية من الجرائم العابرة للحدود:

. . بمعنى أنها جريمة تتخطى الحدود الجغرافية للدول، لارتباطها بتقنية المعلومات وعالم الانترنيت، وما يتصف من سرعة هائلة، والقدرة التي تتمتع بها في الربط بين الأنظمة المعلوماتية لعدة دول رغم المسافات الكبيرة جدا التي تفصل بينها، ومنحت القدرة لخبراء الحاسوب والمعلومات في التحكم في أنظمة متعددة في آن واحد وفي دول مختلفة وهم في دول محايدة أخرى، مما أدى إلى إمكانية ارتكاب الجريمة الإلكترونية في أماكن متعددة في العالم في آن واحد، كما يمكن أن يكون الجاني في دولة والمجني عليه في دولة أخرى[3].

وتبعاً لتغير الظروف التي تحيط بوقوع الجريمة، فإننا نقع في إشكالية تنازع القوانين حولها، وهنا يثار التساؤل الآتي: من هي الدولة المختصة في محاكمة المتهمين في ارتكاب الجريمة، والقانون الواجب التطبيق؟ وهل يتم اعتبار مكان ارتكاب الجريمة أو مكان وجود الجاني في تحديد الاختصاص؟ ويزداد الأمر تعقيدا عندما يتعدد الجناة مع اختلاف أمكنة تواجدهم، وفي حالة ما إذا كان الضرر المترتب عن الجريمة في بلد ثالث أيضاً، فكيف يتم التصرف مع هذه الحالة حينئذ؟ وإشكالات أخرى عديدة قد تثار فيما يخص الإجراءات القضائية لملاحقة المجرمين، وكيفية تسليمهم...وغير ذلك.

كل هذا يحتاج إلى زيادة توضيح، ولا يتأتى ذلك في نظري إلا بمقتضى معاهدات دولية تفصل في الأمر أو إقليمية، ويمكن أن تكون هناك اتفاقيات حول هذا الإشكال، ولو أن الحلول التي تقدمها هذه الأخيرة تبقى نسبية لقصورها على بعض الدول التي تبني علاقتها على التفاهم فيما بينها دون غيرها

(1) بوشعرة أمينة وموساوي سهام، الإطار القانوني للجريمة الإلكترونيةدراسة مقارنة_، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2017/2018، ص10.

(2) بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري _دراسة مقارنة_، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص: قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2015/2016، 12.

(3) خالد ممدوح إبراهيم، امن الجريمة الإلكترونية، ر ط، الدار الجامعية الإسكندرية_ مصر، 2008، ص82.

من دول المجتمع الدولي.

2_ صعوبة اكتشاف وإثبات الجريمة الإلكترونية:

بما أن الجريمة الإلكترونية تمثل جريمة ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي[1]، فإنها تتسم بصعوبة كبيرة في اكتشافها وإثباتها، وذلك راجع لعدة أسباب: من أهمها وسيلة التنفيذ التي تتسم في أغلب الأحيان بالطابع التقني، فهي تتم بواسطة رموز وأرقام دقيقة يصعب اكتشافها، وعادة ما يكون بمحض الصدفة[2].

كما أنها لا تترك آثارا ملموسة ولا أدلة مادية يمكن فحصها، ولا يمكن الاعتماد على أقوال الشهود بصددها، كونها تقع في بيئة افتراضية يطلق عليها اسم البيئة الرقمية، يتم فيها نقل المعلومات وتناولها بواسطة نبضات إلكترونية غير مرئية[3]، وقد تكون الشبكة مشفرة ولا يعرف فك التشفير إلا من قبل المنتسبين لتلك الشبكة[4]...وغير ذلك من المعضلات التي تقف عائقا وراء إثباتها، لذلك فإن الكثير من الجناة يفلتون من العقاب.

3_ الجريمة الإلكترونية جريمة ناعمة:

على عكس الجرائم التقليدية التي تتطلب الوسائل المادية واستعمال العنف والقوة كجرائم المخدرات وتبييض الأموال، الضرب والجرح وجرائم الإرهاب...إلخ، فإن الجريمة الإلكترونية تمتاز بنعومتها، حيث أنها لا تحتاج إلى العنف ولا تتطلب استخدام القوة والعضلات، وإنما تستدعي التحكم في المعلوماتية والقدرة على التعامل مع جهاز الحاسوب الآلي والبرمجيات بمستوى تقني وذكاء ومهارة علمية، تمكن الجاني من توظيف ذلك في تنفيذ الجريمة عن طريق تحريك الأنامل على جهاز الكمبيوتر دون أي عنف أو قوة[5].

4_ امتناع المجني عيهم على التبليغ:

لا يتم في الغالب التبليغ من قبل المجني عليه على الجريمة الإلكترونية، خوفا من التشهير وضياع ثقة المساهمين، خاصة المؤسسات المالية كالبنوك ومؤسسات القرض وكذلك السماسرة، حيث تخشى أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها، إلى زوال الثقة بينهم وبين المتعاملين معهم، وهو ما يؤدي إلى استغنائهم عن خدماته[6].

5_ سرعة محو الدليل على ارتكاب الجريمة الإلكترونية:

يمتاز هذا النوع من الجرائم بسهولة محو الدليل من على شاشة جهاز الكمبيوتر، في زمن قياسي ووقت قصير جداً، باستعمال البرامج المخصصة لذلك، إذ يتم عادة في لمح البصر، وبمجرد لمسة

(1) عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون_دراسة مقارنة_. ر ط، منشورات الحلبي الحقوقية، الإسكندرية، 2007م، ص270.

(2) بعرة سعيدة، مرجع سابق، ص. 37.

(3) محمد ياسر أبو الفتوح، خصائص وتصنيفات الجريمة المعلوماتية، مقال منشور بتاريخ: 04 فيفري2013، على الموقع الإلكتروني: https//almohakmoonalarab.ahlamontada.com. سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012/2013، ص. 34.

(4) بوشعرة أمينة ومواساوي سهام، مرجع سابق، ص. 17.

(5) خليفة محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، ر ط، جار الجامعة الجديدة، الإسكندرية_مصر، س ط، ص37.

(6) صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة مقدمة لنيل شهادة الماجستير في القانون، تخصص: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012/2013، ص18.

خاطفة على لوحة المفاتيح بجهاز الحاسوب، على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما إن يحس الجاني بأن أمره قد كشف، حتى يبادر بإلغاء هذه الأوامر، وهو ما يؤدي إلى طمس آثار الجريمة كلية وصعوبة الكشف عنها وتحديد مرتكبيها[1].

المحور الثاني: القواعد الموضوعية المقررة لمكافحة الجريمة الإلكترونية.

استحدث المشرع الجزائري القسم السابع مكرر تحت الفصل الثالث بعنوان الجنايات والجنح ضد الأموال، ضمن قانون العقوبات، بمقتضى تعديل 04/15 المؤرخ في 10 نوفمبر 2004م، تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، جرم من خلاله هذا النوع من الجرائم.

. وتأخذ هذه الجرائم ثلاث صور: تتمثل الصورة الأولى في الاعتداء على نظام المعالجة الآلية، والصورة الثانية هي الاعتداء على معطيات نظام المعالجة الآلية، أما الصورة الثالثة فتشمل جرائم الاعتداء على سير نظام المعالجة الآلية.

أولا: الاعتداء على نظام المعالجة الآلية للمعطيات:.

أشار المشرع الجزائري لهذا النظام في الفقرة «ب» من المادة. من قانون 09/04، عند تعريفه للمنظومة المعلوماتية، بقوله: «أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.[2]»

وهو التعريف الذي أوردته الاتفاقية الدولية المتعلقة بالجريمة الإلكترونية المنعقدة ببودابست سنة 2001م، حيث جاء في الفقرة «أ» من المادة الأولى منها ما يلي: يقصد بـ: «منظومة الكومبيوتر»: «أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر وفقا لبرنامج، بالمعالجة الآلية للبيانات.[3]»

وعليه فإن المعالجة الآلية للمعطيات تكون في إطار تنفيذ البرامج المعلوماتية، عن طريق الأنظمة المتاحة في هذا المجال.

وقد وضح المشرع أيضا في نفس المادة ضمن الفقرة «ج» معنى المعطيات المعلوماتية، حيث تعرف بأنها: «أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.[4]»

. وقد وافق ما جاءت به اتفاقية بودابست، ضمن الفقرة «ب» من المادة الأولى، والتي وردت كالآتي: يقصد بـ: «بيانات الكومبيوتر»: «أي عمليات عرض للحقائق أو المعلومات أو المفاهيم، في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر، بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معينة.[5]»

هذا ما يجعل المعطيات المعلوماتية تأخذ معنا واسعا لتحوي كل عملية عرض معلوماتية داخل

(1) حفوظة الأمير عبد القادر، وغرداين حسام، الجريمة الإلكترونية وآليات التصدي لها، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد بتاريخ: 29 مارس 2019، الجزائر العاصمة، ص83. الموقع الإلكتروني: poli-.www com.dz-tics، تاريخ الاطلاع: 16/10/2019.

(2) قانون 09/04 مؤرخ في: 14 شعبان 1430هـ الموافق لـ:. أوت 2009م، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.. ر لسنة 2009م، عدد 47، صادرة بتاريخ: 16 أوت 2009م. ص05.

(3) الاتفاقية الدولية المتعلقة بالتجارة الإلكترونية، بودابست، بتاريخ: 23/11/2001م، ص3.

(4) المادة. من قانون 09/04.

(5) اتفاقية بودابست، مرجع سابق، ص3.

الأنظمة المعلوماتية، لتأدية وظيفتها على أتم وجه.

فالتعدي على نظام المعالجة الآلية للمعطيات يعد جريمة، وتتخذ صورتين، الصورة البسيطة والصورة المشددة كالآتي:

1_ الصورة البسيطة: نص المشرع الجزائري في المادة 394/ مكرر. ع. على ما يلي: «يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000دج إلى 100.000دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.»

وعلى هذا الأساس فإن هاتين الصورتين تتخذان الفعلين التاليين:

أ- فعل الدخول غير المرخص: يعد فعل الدخول هنا بمثابة الركن المادي للجريمة.

ويقصد به: «الوصول إلى المعلومات المخزنة داخل النظام عن طريق الوسائل التقنية والفنية الإلكترونية.[1] »

وتتحقق الصفة غير المشروعة في فعل الدخول عندما يتم بدون رضا صاحب النظام المعلوماتي، ويفتقر للإذن أو الترخيص من طرفه.

وتعد على هذا النحو جريمة شكلية، لأنها لا تشترط تحقق النتيجة، حيث يكفي الوصول إلى المعلومات المخزنة داخل نظام المعالجة الآلية للمعطيات لقيام الجريمة.

كما لم تشترط المادة لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة الآلية للمعطيات، أن يكون محاطاً بحماية فنية تمنع الاختراق كالتشفير مثلا، بل جاءت عامة ومطلقة، لا تستثني أي نظام معلوماتي مهما كان[2].

وهذا التوسيع في دائرة الجريمة وعدم حصرها في الأنظمة المعلوماتية المشفرة، يعتبر إجراء احترازيا يحسب لصالح المشرع الجزائري، والذي غلق بموجبه الباب أمام كل الحيل التي قد يلجأ إليها مرتكب الفعل كأن يحتج مثلا بعدم إضفاء الحماية اللازمة على النظام المعلوماتي...إلخ.

ب_ البقاء غير المرخص:

يقصد بالبقاء غير المرخص لنظام المعالجة الآلية للمعطيات: «استمرار التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام بعد الدخول إليه عن طريق الخطأ أو الصدفة...، رغم علمه بأن هذا البقاء غير قانوني.[3]»

وقد عبر المشرع الجزائري عن هذه الجريمة ضمن المادة 394/ مكرر. ع. بقوله: «... أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.»

. ويتحقق الركن المادي لجريمة البقاء غير المرخص في منظومة المعالجة الآلية للمعطيات المملوكة للغير في صورتين:

الصورة الأولى: تتمثل في تحقق فعل البقاء داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل

(1) بعرة سعيدة، مرجع سابق، ص51.

(2) براهيمي جمال، مكافحة الجرائم الإلكترونية في التشريع الجزائري، مقال منشور في المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد2، نوفمبر2016م، ص127.

(3) آمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق، جامعة الجزائر، 2001/2002م، جامعة الجزائر، ص44.

الدخول، ويتجسد هذا عندما في حالة الدخول المشروع، الذي يتصور في الولوج عن غير قصد إما عن طريق الصدفة أو الخطأ، ثم يبقى داخل النظام ولا يخرج فور علمه بأنه قد اخترق منظومة الغير، فهنا يتحقق فعل البقاء غير المرخص[1].

الصورة الثانية: تتجسد في الحالة التي يجتمع فيها فعل البقاء غير المرخص مع فعل الدخول الغير مشروع، ومن أمثلة هذا التداخل: الدخول إلى نظام المعالجة الآلية للمعطيات المملوك من قبل الغير بدون أخذ من صاحبه، والاستمرار في البقاء داخله، فهنا تتداخل جريمتا الدخول والبقاء غير المرخصين[2].

وأمام انعدام التطبيقات القضائية التي توضح فعل البقاء، فإن الرأي الغالب في الفقه يذهب إلى أن فعل البقاء غير المرخص، يتحقق منذ اللحظة التي يبدأ فيها الشخص بالتجوال داخل النظام مع علمه بذلك، فإن دخل وظل ساكناً فإنها تعتبر جريمة دخول فقط، ولا يقتضي هذا البقاء تحميل معلومة أو التقاط صور...وغير ذلك، وإنما مجرد التجوال يؤدي إلى قيام الجريمة[3].

وتجدر الإشارة هنا إلى أن المشرع الجزائري وطبقا لنص المادة 394/1 مكرر. ع ج، فإنه قد أفرد لهاتين الجريمتين المتمثلتين في فعل الدخول لمنظومة المعالجة الآلية للمعطيات، وفعل البقاء غير المرخص بها، الحبس من ثلاثة أشهر إلى سنة والغرامة التي تتراوح ما بين 50.000دج إلى 100.000دج.

2_ الصورة المشددة: تكون العقوبة مشددة في حالة ما إذا صاحب فعلَ الدخول أو البقاء أفعال أخرى أحدثت ضررا بنظام المعالجة الآلية للمعطيات، وقد أشار المشرع الجزائري إلى ذلك في نفس المادة 394/ مكرر. ع. بقوله: «تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000دج إلى 150.000دج.»

يتضح من خلال هاتين الفقرتين من نص المادة 394 مكرر. ع ج، أن المشرع الجزائري قد أورد ثلاثة ظروف لتشديد لجريمتي الدخول والبقاء غير المرخصين لنظام المعالجة الآلية للمعطيات، وهي كالآتي:

_ محو معطيات المنظومة.

_ تعديل معطيات المنظومة.

_ تخريب نظام تشغيل المنظومة.

وهذا ما يجعل هذه الصور تختلف عن سابقتها، حيث يشترط فيها تحقق النتيجة الإجرامية، واثبات وجود العلاقة السببية بين الأفعال المخالفة للقانون والنتيجة الإجرامية، أي يجب أن تربط بين المحو أو التعديل لمعطيات المنظومة أو تخريب نظام تشغيلها وبين فعلا الدخول أو البقاء غير المرخصين علاقة سببية. وإلا كنا بصدد الجريمة في صورتها البسيطة.

---

(1) بعرة سعيدة، مرجع سابق، ص53.

(2) موهوب ابتسام، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص: القانون الجنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2013/2014م، ص19.

(3) آمال قارة، مرجع سابق،. 45، 46.

من هذا المنطلق يتضح أن تحقق النتيجة الإجرامية يعتبر في حد ذاته ظرفا مشددا للجريمة، سواء كانت مقصودة أو غير مقصودة من قبل الجاني.

وهذا ما يؤدي إلى رفع حدة العقوبة المسلطة على الجاني، لتصبح الحبس من ستة أشهر إلى سنتين، والغرامة التي تتراوح ما بين 50.000دج إلى 150.000دج.

ثانيا: الاعتداء على معطيات نظام المعالجة الآلية.

الاعتداء في هذه الصورة يتعدى عادة الدخول والبقاء غير المرخصين لنظام المعالجة الآلية للمعطيات، ويهدف إلى تخريب معلومات الكمبيوتر أو الإضرار بمعطياته ووظائفه، ويتخذ عدة صور تتمثل في ما يلي:

1_ الاعتداء على المعطيات الداخلية للنظام: جرمت بمقتضى نص المادة 394 مكرر. ق. ج التي نصت على ما يلي: «يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من 500.000دج إلى 2000.000دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.»

ويقصد بالمعطيات محل الجريمة: «تلك المعطيات والمعلومات التي يحتويها النظام وتشكل جزءا منه، والتي تمت معالجتها آليا وأصبحت عبارة عن رموز وإشارات تمثل تلك المعلومات، وليس المعلومات ذاتها باعتبارها أحد عناصر المعرفة.[1]»

يتضح من خلال هذا النص أن المشرع الجزائري حدد بصفة حصرية صور الاعتداء على المعطيات الداخلية للنظام، والمتمثلة في ما يلي[2]:

أ- الإدخال: يقصد به إضافة معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام، والتي تمت معالجتها آلياً.

ب- المحو: يعني إزالة من معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الآلية أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة.

ج- التعديل: يعني تغيير المعطيات الموجودة داخل نظام المعالجة واستبدالها بمعطيات أخرى.

ولا يشترط ان يجتمع جميع هذه الصور لتتحقق الجريمة، وإنما تكفي واحدة فقط، فمن قام بفعل واحد من بين هذه الأفعال، يعتبر مرتكبا لجريمة الاعتداء على النظام الداخلي للمعطيات.

ويقع الإشكال هنا بين ما ذكرناه سابقا في الصورة المشددة التي أشرنا إليها سابقا، وذلك في حالة ما إذا صاحب فعلا الدخول أو البقاء غير المرخصين تعديل المعطيات أو محوها، وكيف نفرق بين تلك الصورة. الأفعال التي ضمن تطرق إليها المشرع الجزائري ضمن نص المادة 194 مكرر. ق. ج؟

وفي هذا الإطار فإن بعض الفقهاء المتخصصين فرقوا بين الحالتين أو الصورتين، على أساس أن الصورة المذكورة ضمن نص المادة 194 مكرر. ق. ج، قد تقع بدون الحاجة إلى الدخول أو البقاء داخل النظام، أي تقع على بعد كاستخدام القنابل المعلوماتية الخاصة بالمعطيات، برامج الفيروسات... وغير ذلك[3]، فالفرق بينهما هو أن الأولى مصاحبة للفعلين أما الصورة الثانية فلا.

(1) براهيمي جمال، مرجع سابق، ص133.
(2) آمال قارة، مرجع سابق، ص52، 53.
(3) براهيمي جمال، مرجع سابق،. 134.

وقد جاء النص القانوني بصفة مطلقة، أي أن العبرة بالنتيجة دون النظر إلى الوسيلة المتبعة لتحقيق ذلك، كما أن القصد الجنائي العام يكفي لتوافر الركن المعنوي، والمتمثل في اتجاه إرادة الجاني لارتكاب الجريمة غشا أو عن طريق التدليس أي بدون ترخيص من قبل صاحب النظام وبصفة مخالفة لإرادته، مع العلم بأن ما يقدم عليه يعتبر فعلا مخالفا للقانون.

ولقد حدد المشرع الجزائري لمن يرتكب إحدى الصور المذكورة والمتمثلة في الإدخال أو التعديل أو المحو، عقوبة الحبس من ستة أشهر إلى ثلاثة سنوات، بالإضافة إلى الغرامة التي تتراوح ما بين 500.000دج. 2000.000دج.

2_ الاعتداء على المعطيات الخارجية للنظام:

نصت المادة 394 مكرر. ق. ج: «يعاقب بالحبس من شهرين إلى ثلاث سنوات، وبغرامة من 1000.000دج إلى 5000.000دج كل من يقوم عمدا وعن طريق الغش بما يلي:

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

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

يتضح من نص هذه المادة أن هذه الجريمة تتخذ صورتين: التعامل في معطيات صالحة لارتكاب جريمة، وكذا التعامل في معطيات متحصلة من جريمة.

ويقصد بالتعامل في هذين الصورتين: «كل سلوك له علاقة يكشف عن وجود صلة بين الشخص ومعطيات غير مشروعة.[1]»

أ_ التعامل في معطيات صالحة لارتكاب جريمة: وهي ما عبرت عنه اتفاقية **بودابست** بـ «**إساءة استخدام الأجهزة**»، وطالبت بإدراجه ضمن نصوص قوانين الدول الأعضاء بمقتضى المادة. التي جاء فيها: «تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير حق:

أ.عملية إنتاج، بيع شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة بأية طرق أخرى:

1. جهاز بما في ذلك برنامج كومبيوتر، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من. إلى 5.

2. كلمة سر خاصة بكومبيوتر، رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من. إلى 5.....

لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية طالما أن عملية الإنتاج، البيع، الشراء بغرض الاستخدام، الاستيراد، التوزيع، الإتاحة بطرق أخرى...ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من. إلى. من هذه الاتفاقية...»

نستشف من هذا النص أن هذه الصورة تتخذ عدة سلوكيات تتمثل في الإنتاج الذي تدخل تحته العديد من الأفعال، وهي تصميم وخلق أو إيجاد معطيات صالحة لارتكاب الجريمة، يقوم به المختصون في مجال المعلوماتية: مثل: تصميم البرامج الخبيثة كتلك التي تحمل فيروساً، والبحث عن

(1) موهوب ابتسام، مرجع سابق، ص31.

كيفية تصميم هذه المعطيات وإعدادها، أو القيام بجمع العديد من المعطيات مثل: كلمة السر الخاصة بالكمبيوتر، رمز الولوج...إلخ، أو إتاحتها ووضعها تحت تصرف الغير وفي متناوله بأي شكل من الأشكال وتسهيل وصوله إليها بتوفيرها أو نشرها أو الاتجار فيها عن طريق توزيعها سواء بمقابل أو بدون مقابل أو استيرادها...وغير ذلك، وهذا من أجل القيام بجريمة من الجرائم المذكورة آنفاً، كجريمة الدخول والبقاء غير المرخصين، تعديل أو حذف معطيات المنظومة.. وغير ذلك.

ولا يكفي حسب الفقرة الثانية من المادة. من اتفاقية بودابست، القصد الجنائي العام لقيام الركن المعنوي لهذه الجريمة، وإنما يجب توافر القصد الجنائي الخاص أو الدافع من وراء هذا التعامل، والمتمثل في السعي إلى ارتكاب إحدى الجرائم السابقة الذكر..

وهو ما أشار إليه المشرع الجزائري بقوله: «يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.»

ب_ التعامل في معطيات متحصلة من جريمة:

تتحقق هذه الصورة بارتكاب أحد الأفعال المذكورة ضمن نص المادة 394 مكرر. ق. ج، والمتمثلة في حيازة معطيات متحصلة من إحدى الجرائم المذكورة آنفاً كجريمة البقاء غير المرخص، تعديل معطيات النظام...وغيرها، أو إفشائها أي نقلها للآخرين أو نشرها عن طريق أي وسيلة كانت من وسائل الإعلام والنشر وأحدث هذه الطرق تتمثل في الفايسبوك أو التويتر...وغير ذلك أو استعمالها واستغلالها لأي غرض كان.

ولا تتطلب لتجريمها حدوث نتيجة فعلية ولا يشترط فيها تحقق ضرر فعلي يقع على معطيات أو أنظمة معلوماتية، فهي على هذا الأساس تجرم بوصفها أفعالا خطرة يمكن أن تؤدي إلى ضرر فعلي[1].

ويكفي لتوافر الركن المعنوي في هذه الصورة القصد الجنائي العام، والمتمثل في علم الجاني بأن الفعل الذي يقدم عليه غير مشروع، ومع ذلك تتجه إرادته الفعلية الحقيقية لارتكابه.

وقد أقر المشرع الجزائري للجاني الذي يرتكب أي فعل من الأفعال المذكورة ضمن الصورتين حسب نص المادة 394 مكرر. ق. ج عقوبة الحبس من شهرين إلى ثلاث سنوات، وبغرامة من 1000.000دج إلى 5000.000دج.

وتجدر الإشارة هنا إلى أن كل هذه الجنح المذكورة يجوز فيها للقاضي في حالة الإدانة، بالإضافة إلى العقوبات الأصلية المتمثلة في الحبس والغرامة، الحكم بعقوبات تكميلية جوازية حسب القواعد العامة المذكورة ضمن المادة 14. ع ج، والمتمثلة أساسا في: الحرمان من ممارسة حق أو أكثر من الحقوق الوطنية والمدنية والعائلية، المذكورة ضمن المادة. مكرر. ق. ج، منها: العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة، الحرمان من حق الانتخاب أو الترشح ومن حمل أي وسام، عدم الأهلية لأن يكون وصيا أو قيما، سقوط حقوق الولاية كلها أو بعضها... وغيرها.

المحور الثالث: القواعد الإجرائية المقررة لمكافحة الجريمة الإلكترونية.

استحدث المشرع الجزائري بمقتضى القانون 06/22 المتضمن تعديل قانون الإجراءات الجزائية، عدة قواعد وأساليب إجرائية في إطار مكافحة الجريمة الإلكترونية، من شأنها أن تساعد في الكشف

(1) محمد زكي، قانون العقوبات_القسم الخاص_، ر ط، دار الجامعة الجديدة، الإسكندرية–مصر، 2005م، ص763.

عن الجريمة والتحري على مرتكبيها. والعمل من أجل الحد من انتشارها، والمتمثلة أساساً في اعتراض المراسلات. تسجيل الأصوات والتقاط الصور، بالإضافة إلى التسرب.

أولا: اعتراض المراسلات. تسجيل الأصوات والتقاط الصور.

نص المشرع الجزائري على هذا الإجراء بمقتضى نص المادة 65 مكرر 5/. إ. ج، بقوله: إذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

_ اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

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

_ يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ول خارج المواعيد المحددة في المادة 47 من هذا القانون، وبغير علم أو رضا الأشخاص الذين لهم حق عن تلك الأماكن

_ تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص.

_ في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة.[1]»

نستنتج من فحوى هذه المادة أن المشرع قد أذن باعتراض المراسلات ووضع الترتيبات التقنية من أجل تسجيل الكلام المتفوه به والتقاط الصور، في بعض الجرائم المحددة بمقتضى القانون حفاظا على سرية المعلومات الشخصية وحماية الحياة الخاصة للأشخاص، والتي من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ويقصد باعتراض المراسلات مراقبة المحادثات والرسائل الهاتفية والتنصت التليفوني وجميع ما يتم عن طريق جميع وسائل الاتصالات السلكية واللاسلكية وشبكات المعلوماتية المتوفرة، كالفاكس والرسائل المتبادلة عبر الشبكة العنكبوتية كتلك التي تكون عبر الواتساب، الفايسبوك، التويتر، الفايبر والبريد الإلكتروني...وغيرها[2].

. أما التسجيل الصوتي فيقصد به: تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية في أماكن عامة أو خاصة كالمنازل والمحلات التجارية وغيرها، ووضع الترتيبات التقنية لذلك دون موافقة المعنيين أو علمهم بذلك[3].

. وأضاف المشرع الجزائري التقاط الصور أي أخذ صور لشخص أو عدة أشخاص يتواجدون في

(1) الأمر 66/165 المؤرخ في : 18 صفر 1386هـ الموافق لـ:. جوان 1966م، يتضمن قانون الإجراءات الجزائية المعدل والمتمم، الجريدة الرسمية لسنة 1966م، عدد 47، صادرة بتاريخ: 19 صفر 1386هـ الموافق لـ:. جوان 1966م.

(2) جميلة محلق، اعتراض المراسلات: تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مقال منشور ضمن مجلة التواصل في الاقتصاد والإدارة والقانون، كلية الحقوق والعلوم السياسية، جامعة باجي مختار عنابة، عدد 42، جوان 2015م،. 178.

(3) نفس المرجع والصفحة.

أماكن خاصة باستخدام الأساليب العلمية الحديثة في إطار الحد من تفاقم الجريمة[1].

ولا يلجأ لهذا الإجراء إلا بتوافر عدة شروط في إطار التوفيق بين حماية الحقوق الخاصة، والحفاظ على المصلحة العامة بوضع حد لهذا النوع من الإجرام عن طريق كشف المجرمين وتبيين الحقائق.

وتتمثل هذه **الشروط** في ما يلي:

1_ الإذن القضائي: نستشف من نص المادة 65 مكرر. ق. ج ج، أن المشرع الجزائري اشترط أن يتم هذا الإجراء بناء على إذن مسبق من وكيل الجمهورية، وفي حالة فتح تحقيق قضائي فإن الاختصاص يؤول إلى قاضي التحقيق.

ويعرف الإذن بأنه: «تفويض يصدر من السلطة المختصة إلى أحد ضباط الشرطة القضائية، مخولا إياه إجراء تلك العمليات.[2]»

ويشترط في الإذن القضائي الشروط الآتية[3]:

_ ضرورة تضمنه لجميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن السكنية المقصودة أو غيرها، والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

_ يشترط أن يسلم الإذن مكتوبا لأحد ضباط الشرطة القضائية.

2_ يجب احترام المدة القانونية: تحدد مدة الإذن بـ:. أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية[4].

3_ كتمان السر المهني: يسمح الإذن لضابط الشرطة المناب باعتراض المراسلات السلكية واللاسلكية وتسجيل الصوت والتقاط الصور أو ينفذ ذلك دون المساس بالسر المهني المتعلق بالتفتيش المنصوص عليه ضمن المادة 45. إ. ج، وجسد المشرع هذه الحماية من خلال تعيين الأشخاص المؤهلين للاطلاع على الأسرار، وفرض عقوبات على من يفشي الأسرار غير المخالفة للقواعد القانونية[5].

4_ تحرير محضر العمليات: يجب على ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص تحرير محضرا عن كل عملية اعتراض وتسجيل المراسلات، وكذا عن كل عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها[6]. كما ينسخ جميع المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف[7].

5_ ضرورة التقيد بالجرائم التي يجوز فيها إجراء الاعتراض: ذكرت بصفة حصرية ضمن نص المادة 65 مكرر. ق. ج ج، وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود، الجرائم الماسة

(1) نفس المرجع، 179.

(2) صالح شنين، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مقال منشور في المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، عدد1، مجلد2، ديسمبر 2010م، ص68.

(3) نص المادة 65 مكرر. ق. ج ج.

(4) الفقرة. من نص المادة 65 مكرر. ق. ج ج.

(5) جميلة محلق، مرجع سابق، 181.

(6) نص المادة 65 مكرر. ق. ج ج.

(7) الفقرة الأولى من نص المادة 65 مكرر 10. إ. ج.

بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، جرائم الصرف وجرائم الفساد.

6_ التسبيب: يعتبر التسبيب أساس العمل القضائي، وعليه فإن عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور يجب أن يكون الغرض منها الكشف عن الحقيقة وإظهار ملابسات الجريمة وضبط الجناة والحد من هذا النوع من الجرائم[1]..

ثانيا: التسرب:

عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة ضمن المادة 65 مكرر. ق. ج ج، يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار الوكيل، أن يأذن تحت رقابته بمباشرة عملية التسرب[2].

وقد عرف المشرع الجزائري التسرب ضمن المادة 65 مكرر 12. إ. ج، بقوله: «يقصد بالتسرب: قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.»

من خلال هذا التعريف يمكن تصور عملية التسرب في نطاق جرائم أنظمة المعالجة الآلية في قيام ضابط أو عون الشرطة القضائية بالدخول مع المشتبه بهم في اختراق أنظمة المعلوماتية في الدردشة بواسطة الانترنيت، ويسلك جميع الوسائل كالأسماء المستعارة حتى وإن استدعى الأمر اعتماد بطاقات هوية مزورة، أو الظهور بمظهر صاحب شركة وهمية...وغير ذلك[3]، ليتمكن من الحصول على مهمة في هذا الإطار، ليتمكن من معرفة كيفية اختراق الأنظمة أو بث الفيروسات، ويعرف جميع أعضاء الشبكة الإجرامية وطريقة عملهم، من أجل الإطاحة بها والقبض على المجرمين.

وهو ما جعل المشرع الجزائري يرخص لهم ببعض الأفعال مع رفع صفة التجريم على قيامهم بها أثناء تنفيذ عملية التسرب، والمتمثلة في: اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها، وكذلك استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي، ووسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[4].

ولقد أحاط المشرع الجزائري هذه العملية بعدة ضمانات أهمها:

1_ صدور إذن قضائي بالتسرب: لا تكون عملية التسرب إلا بناء على إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، وتنفذ تحت رقابة المصدر للإذن[5]، مع ذكر هوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته[6].

2_ احترام المدة القانونية للتسرب: حدد المشرع الجزائري مدة التسرب بأربعة أشهر، قابلة للتجديد

(1) صالح شنين، مرجع سابق، ص69.

(2) نص المادة 65 مكرر. ق. ج ج.

(3) لا يجوز إظهار أو كشف هوية ضباط أو أعوان الشرطة، الذين باشروا عملية التسرب تحت هوية مستعارة، تحت طائلة العقاب بالحبس من. إلى. سنوات وبغرامة من 50.000دج إلى 200.000دج، وتشدد هذه العقوبة حسب الظروف المحددة في القانون. للاستزادة انظر: المادة 65 مكرر16. إ. ج.

(4) نص المادة 65 مكرر 14. إ. ج.

(5) نص المادة 65 مكرر 11. إ. ج.

(6) نص المادة 65 مكرر2/15. إ. ج.

حسب مقتضيات التحري أو التحقيق، ويجوز للقاضي الذي رخص بإجراء العملية، أن يأمر بوقفها قبل انقضاء المدة المحددة[1]. وفي هذه الحالة أو في حالة عدم تجديدها بعد انقضاء المهلة المقررة، يحق للعون المتسرب مواصلة النشاط للوقت الضروري الكافي دون أي يكون مسؤولاً جنائياً، على أن تتجاوز المدة. أشهر، مع إشعار القاضي المصدر للإذن، الذي يحق له تمديده إذا اقتضى الأمر لفترة. أشهر للمرة الثالثة كحد أقصى[2].

3_ ضرورة التقيد بالجرائم التي يجوز فيها إجراء عملية التسرب: لا يمكن لعملية التسرب أن تخرج عن الجرائم التي ذكرت بصفة حصرية ضمن نص المادة 65 مكرر. ق. ج ج، وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، جرائم الصرف وجرائم الفساد[3].

4_ التسبيب: انطلاقا من أهمية التسبيب في اتخاذ الإجراءات القضائية، فإن المشرع الجزائري اشترط في اللجوء إلى عملية التسرب، ذكر نوع الجريمة التي تبرر ذلك من قبل الجهة المصدرة للإذن، سواء وكيل الجمهورية أو قاضي التحقيق تحت طائلة البطلان[4].

. وتجدر الإشارة إلى أن المشرع الجزائري قد أقر بتمديد الاختصاص لضباط الشرطة القضائية ليشمل كافة الإقليم الوطني، فيما يخص ببحث ومعاينة الجرائم المذكورة ضمن نص المادة 65 مكرر 5. إ. ج، والتي تدخل ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهو ما يمنحهم الحق في القيام بإجراءات اعتراض المراسلات. تسجيل الأصوات والتقاط الصور، وكذا عملية التسرب عبر كافة تراب الإقليم الجزائري.

خاتمة:

من خلال ما سبق نستنتج أن المشرع قد انتهج نهجا مزدوجا في مكافحة الجريمة الإلكترونية، ومحاولة التصدي للجرائم المتعلقة بالمعلوماتية، حيث أقر تعديلا لقانون العقوبات أدرج من خلاله أنواع الجرائم المتعلقة بأنظمة المعلوماتية، ليمنحها صفة التجريم بعدما كانت بمنأى عن ذلك، وثم تلاه تعديل آخر لقانون الإجراءات الجزائية، واللذين من خلالهما أقر جملة من التدابير العقابية والإجراءات الاستثنائية، والتي منح من خلالها للسلطات القضائية رخصاً إجرائية لمواجهة هذه الجرائم.

لكن ورغم الجهود المبذولة من قبله، إلا أنها تبقى قاصرة في التصدي لجميع الجرائم المستحدثة في هذا الجانب، بسبب التطور التكنولوجي السريع جدا وما يصاحبه من تطور في الجانب الآخر والمتعلق بالجرائم المتعلقة بأنظمة المعلوماتية، بالإضافة إلي طبيعة هذا النوع من الجرائم العابرة للحدود الوطنية، مما يؤدي إلى صعوبة ضبط المجرمين وتتبع الجرائم، وهو ما يجعلنا نقترح التوصيات الآتية:

1. على المشرع الجزائري التعديل السريع والدوري لقانون العقوبات بما يتماشى مع السرعة الفائقة للمعلوماتية، وما ينجر عنها من جرائم.
2. القيام بعقد اتفاقيات إقليمية مع الدول العربية والإفريقية في إطار التعاون الأمني.
3. تفعيل ما نصت عليه المعاهدات والاتفاقيات الدولية، كاتفاقية باليرمو 2000 وغيرها، في ما يخص التعاون القضائي خاصة، كتسليم المجرمين وتبادل المعلومات التي من شأنها المساعدة في الكشف عن الشبكات الإجرامية.

(1) نص المادة 65/2 مكرر15. إ. ج.
(2) نص المادة 65 مكرر11. إ. ج، والتي أحالت إلى الجرائم المنصوص عليها ضمن المادة 65 مكرر5ق. ج ج
(3) نص المادة 65 مكرر17. إ. ج.
(4) نص المادة 65 مكرر3/15. ق. ج ج.