# مجلة
# القانون، المجتمع والسلطة

مدير المجلة
د. محمد بوسلطان
مدير التحرير
د. نصرالدين بوسماحة

رقم 3-2014

## باسم الله الرحمن الرحيم

## الافتتاحية

مجلة القانون، المجتمع والسلطة هي مجلة سنوية محكمة، تصدر عن مخبر القانون، المجتمع والسلطة بكلية الحقوق، جامعة السانية وهران، المعتمد بموجب القرار الوزاري رقم 66 المؤرخ في 30 ماي 2010.

تنشر المجلة البحوث القانونية العلمية، وتأمل في هذا الإطار أن تكون منارة جديدة في حقل الدراسات القانونية بفضل مساهمات الأساتذة والباحثين من مختلف الجامعات والمؤسسات ومراكز البحث.

بعد تخصيص العدد الأول من المجلة لموضوع الحكم الراشد ثم العدد الثاني لموضوع العدالة الانتقالية، ارتأت هيئة المجلة أن تفتح المجال أكثر في العدد الثالث لنشر دراسات متنوعة ما بين العلوم القانونية والعلوم السياسية. نتيجة لذلك ورد في هذا العدد دراسات يندرج بعضها في القانون الدستوري وكذلك قانون الأعمال وقانون المالية إضافة إلى القانون الجنائي والبعض الآخر في العلوم السياسية.

# مجلة: القانون، المجتمع والسلطة




**مجلة سنوية محكمة، تصدر عن مخبر**

**القانون، المجتمع والسلطة**

**جامعة وهران**

# الحمايـــة الجنائيـــة للحكومـــة الإلكترونيـــة

**د. بن زحاف فيصل**
أستاذ محاضر "ب"
جامعة عبد الحميد بن باديس مستغانم

**ملخص:**

"تهدف هذه الدراسة إلى تحليل الحماية الجنائية للحكومة الإلكترونية على ضوء سن تشريعات عقابية تتكفل بتجريم كل الأفعال الماسة بتكنولوجيا الإعلام والاتصال، وردع مرتكبي هذه الجرائم من خلال إقرار عقوبات جزائية سواء كان الفاعل شخصا طبيعيا أو شخصا معنويا. فمن خلال النظر إلى جزئيات هذه الدراسة يتضح لنا أن الدول بعد دخول القرن الحادي والعشرين تبنت خيار الحكومة الإلكترونية كطريق مختصر للتنمية، والوسيلة المثلى لتفعيل جهاز الأداء الحكومي، وتعزيز الثقة بين المواطن والإدارة، ولكن

فقد بلغ حجم الإجرام الإلكتروني مستويات أصبحت تهدد السلامة العامة والمصالح الوطنية، ينتج عنها خسائر مالية سنوية تقدر بملايير الدولارات تتكبدها المؤسسات المالية. وبالرغم من الآثار الجسيمة للجريمة الإلكترونية فإن الدول لم تتراجع عن هذا الخيار، وسارعت إلى إضفاء تكنولوجيا الإعلام والاتصال على كل المجالات ذات الصلة بالتنمية، وفضلت آلية الحماية الجنائية للحكومة الالكترونية من خلال التعاون فيما بينها تشريعيا، قضائيا، أمنيا لمكافحة الجريمة الإلكترونية. وهو نفس الخيار الذي سار عليه المشرع الجزائري من التعديلات التي أضفاها على قانون العقوبات."

**مقدمة:**

بدخول القرن الحادي والعشرين تبنّت معظم دول العالم خيّار الحكومة الالكترونية، كطريق مختصر للتنمية الاقتصادية والاجتماعية، وترشيد النفقات يستجيب لتطلعات الأفراد والمؤسسات، لأنّه القادر على إذابة جليد البيروقراطية، وتلبية الطلبات والرغبات بسهولة مطلقة بكل نزاهة وشفافية، وهو الطريق الأمثل لتفعيل الجهاز الحكومي وتطوير أدائه وتخفيف الأعباء الإدارية عنه، كما يعد هذا الخيار أفضل وسيلة لإعادة الثقة إلى المواطنين في الإدارة.

إلاّ أن البعض أساء استخدام تكنولوجيا الإعلام والاتصال، ونتج عنه جرائم خطيرة تهدّد السلامة العامة والمصلحة الوطنية للدول، وكبدتها خسائر مالية سنوية تقدر بملايير الدولارات مقارنة بالخسائر الناجمة عن الجرائم التقليدية.

إنّ هذه الجرائم أصبحت تهدّد أمن الحكومة الالكترونية نظرا لاستفحالها وسرعة انتشارها، وصعوبة إثباتها مما جعل بعض الدول تحتفظ بالحكومة الكلاسيكية، وتحجم عن استخدام تكنولوجيا الإعلام والاتصال، ومن بينها الدول الغربية التي خفضت تعاملها مع الدول الأوروبية في ميدان التجارة الالكترونية، نظرا لما أحدثه الإجرام الإلكتروني من رعب في أوساط المؤسسات الاقتصادية والمالية الضخمة، وخوفا من الخسارة المالية التي لحقت الدول الكبرى الرائدة لفكرة الحكومة الالكترونية[1].

لتأمين الحكومة الالكترونية، بادرت معظم الدول بتبني سياسة تشريعية جنائية بتجريم كل السلوكات التي يرتكبها المجرم الالكتروني، وزجره بعقوبات ردعية لقمع الجرائم الالكترونية، ومن بينها المشرع الجزائري الذي جرّم كل الأفعال التي تعتدي على أنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 وأدرج هذا القانون ضمن القسم السابع مكرر من المواد 394 مكرر إلى 394 مكرر7 من قانون العقوبات، وألحق هذا القانون

---

1 من بين الدول العربية التي تراجعت في استخدام تكنولوجيا الإعلام والاتصال في آخر الإحصائيات التي أوردها المنتدى الاقتصادي العالمي في تقريره 2009-2010 بحيث تراجعت الجزائر بستة مراتب مقارنة بـــ2008-2009 لتحتل المرتبة 113 عالميا، وأورد هذا التقرير جدول تفصيلي للمراتب التي تحتلها الجزائر في استخدامات تكنولوجيا الإعلام والاتصال، فمثلا، في مجال استخدام التكنولوجيا من قبل الحكومة تحتل 128. لمزيد من التفاصيل حول ما ورد في التقرير أنظر: جريدة الخبر، العدد 5948 الصادرة بتاريخ 27 مارس 2010.

بصدور قانون رقم 09-04 المؤرخ في 05 سبتمبر 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الإشكال الذي يطرح في هذه الدراسة هو هل سياسة التجريم كافية لتأمين الحكومة الالكترونية وحمايتها أم أنه يجب إيجاد آليات قانونية وأدوات تقنية أخرى لتأمين هذه الحكومة، وخاصة أنها من الجرائم التي يصعب إثباتها وتتجاوز حدود إقليم الدولة الواحدة؟ وما هي هذه الآليات والأدوات الأخرى لتأمينها؟ هذا ما نحاول الإجابة عليه في هذا البحث ضمن المحاور التالية:

أولا: مفهوم الجريمة الالكترونية

ثانيا: كيفية إثبات الجريمة الالكترونية

ثالثا: مكافحة الجرائم الالكترونية

رابعا: الجريمة الإلكترونية في التشريع الجزائري

## أولا: مفهوم الجريمة الالكترونية:

تستفحل الجرائم الالكترونية كلما توغلت الحكومة في استخدام تكنولوجيا الإعلام والاتصال، وتتنوع هذه الجرائم لدرجة استحالة حصرها فقد تقع على الأموال أو الأشخاص، أو الملكية الأدبية والفنية، وأصبحت أكثر خطورة عندما تمس بأمن الدولة الداخلي والخارجي، ممّا جعل المشرع في معظم الدول يجرّم كل السلوكيات الإجرامية التي ترتكب باستخدام الكمبيوتر أو شبكة الانترنيت، لذا نحاول من خلال هذا المحور تناول تعريف الجريمة الإلكترونية وأركانها، ثم نتناول خصائصها وأنواعها.

### 1- تعريف الجريمة الالكترونية وأركانها:

#### أ- تعريفها:

لا يوجد تعريف دقيق للجريمة الالكترونية يجمع بين خبراء القانون والإعلام الآلي نظرا لتنوع هذه الجرائم، وصعوبة حصرها في مجال معين[1]، لذا تعددت تعاريف هذه الجريمة، فجانب من الخبراء عرف الجريمة على أساس موضوعها، وجانب آخر عرفها على أساس الوسيلة التي استخدمت لارتكابها.

---

1 محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص24.

من التعاريف التي عرفتها على أساس موضوعها نجد تعريفا للأستاذ محمد الشوا: "الجريمة المعلوماتية تشمل أي جريمة ضد المال مرتبط باستخدام المعالجة الآلية للمعلوماتية"[1]، ويعرفها خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية بأنها: ''كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أونقلها''[2]؛ ومن التعاريف التي عرفتها على أساس الوسيلة المستخدمة لارتكابها نجد تعريفا للأستاذ جون فورستر FORSTER، والأستاذ إزلي ESLIE بأنها: "كل فعل إجرامي يستخدم فيه الكمبيوتر لارتكابه كأداة رئيسية"، أمّا مكتب تقدم التقنية بالولايات المتحدة الأمريكية يعرفها بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[3]، أمّا الأستاذ PARKER يعرفها بأنها: ''كل فعل اجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق المجني عليه أو كسبا يحققه الفاعل''[4].

الملاحظ على هذه التعاريف بأنّها عرفت الجريمة الالكترونية على أساس موضوعها والوسيلة التقنية المستعملة لارتكابها، إلاّ أنّه رغم ذلك تبقى هذه التعاريف ضيّقة بالنظر للتطور الذي أصبح يشهده مجال تكنولوجيا الإعلام والاتصال، وخاصة تلك الجرائم المرتبكة باستخدام شبكة الانترنيت، كما أن هذه الجرائم لا ترتكب بالكمبيوتر فقط، وإنما ترتكب بالهاتف النقال عن طريق البلوتوت أو عند إيصاله بشبكة الانترنيت.

الجريمة الالكترونية في تعريفها لا تخرج عن نطاق تعريف الجريمة بوجه عام بأنها: ''كل سلوك أو فعل يمكن إسناده إلى فاعله يضر أو يهدّد بالخطر مصلحة محمية بجزاء جنائي''[5]، ويضاف إلى هذا التعريف بأن هذا السلوك يتم ارتكابه باستخدام تكنولوجيا الإعلام والاتصال. واستعملنا مصطلح تكنولوجيا الإعلام والاتصال لإعطاء هذا التعريف معنى واسع ليشمل كل الجرائم الالكترونية.

---

1 محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة 1994، ص 07.

2 O.C.D.E, Reunion de Paris, Mai, 1983.

3 هشام فريد رستم، قانون العقوبات ومخاطر التقنية، مكتبة الآلات الحديثة، أسيوط، 1994، ص31.

4 D.PARKER, combattre la criminalité Informatique, Ed,Otos, 1985, p. 18.

5 عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول، الجريمة، ديوان المطبوعات الجامعية، الجزائر، طبعة 1998، ص59.

**ب- أركانها:**

يستخلص من التعاريف السابقة أن الجريمة الالكترونية تبقى محتفظة بالأركان العامة للجريمة بوجه عام، وهو الركن المادي، المعنوي ثم الركن الشرعي، بالإضافة إلى ركن خاص وهو استخدام تكنولوجيا الإعلام والاتصال.

- الركن المادي: يتكون العنصر المادي للجريمة الالكترونية من ثلاثة عناصر وهي: السلوك الإجرامي، النتيجة، العلاقة السببية بين السلوك والنتيجة، وتجدر الإشارة إلى أن المشرع يشترط في بعض الجرائم تحقق النتيجة لتمام الركن المادي وتسمّى بالجرائم المادية أو جرائم الضرر، وفي بعض الحالات يعتبر المشرع سلوكا ما جريمة دون أن تتحقق النتيجة، وتسمى بالجرائم الشكلية أو جرائم الخطر، وصورة ذلك مثلا في جريمة قرصنة الأرصدة المصرفية يشترط المشرع لتمام الركن المادي هو تحقق النتيجة وذلك باختلاس المال من طرف المجرم وتحويله لحسابه الخاص، كما أن القانون يعاقب على تصفح المواقع الالكترونية المحظورة والمشرع هنا لا يشترط تحقق النتيجة، وإنما يعاقب على السلوك فقط.
- الركن المعنوي: يقصد بهذا الركن أن المجرم الالكتروني يرتكب الجريمة بإرادته وعلمه سواء كان القصد الجنائي قصدا عاما يهدف الجاني من ورائه تحقيق نتيجة معينة كجريمة قرصنة بطاقات الائتمان يهدف المجرم لحيازة المال، أو قصدا جنائيا خاصا يهدف الجاني لتحقيق غاية محددة كجريمة تعطيل موقع إلكتروني لإزالة منافس له في التجارة الالكترونية من السوق.
- الركن الشرعي: المقصود بهذا الركن هو نص التجريم الواجب التطبيق على الفعل الذي يحدّد الفعل والعقوبة المقررة له؛ معظم الدول التي تستعمل تكنولوجيا الإعلام والاتصال سنّت تشريع جنائي تجرّم السلوك الذي يرتكبه المجرم باستخدام وسائل تكنولوجيا الإعلام والاتصال يضر بمصلحة الأفراد المادية والمعنوية، والشركات، وامن الدولة والمصلحة الوطنية.
- الركن الخاص: الجريمة الالكترونية تتميز عن باقي الجرائم بوجه عام بأنها ترتكب من طرف مجرمين أذكياء يملكون مهارات فنية وأدوات المعرفة التقنية يستخدمون أحدث اكتشافات تكنولوجيا الإعلام والاتصال، وهذا ما يضفي ركنا خاصا لها يضاف إلى الأركان العامة، ومن صور هذه الجرائم على سبيل المثال، جريمة سرقة المعلومات أو إتلافها تشترط استخدام الكمبيوتر، وإذا كان جريمة السرقة

تشمل بيانات موجودة على شبكة الانترنيت، فيستخدم الكمبيوتر وشبكة الاتصال[1].

## 2- خصائص الجريمة الالكترونية:

الجريمة الالكترونية تتميز بخصائص عن باقي الجرائم و هي كما يلي:

- الجريمة الالكترونية هي جريمة ينتفي فيها العنف أو سفك الدماء، وإنما هي أرقام ودلالات تنصب على المعلومات والبيانات المخزنة في ذاكرة الكمبيوتر أو المحفوظة على شبكة الانترنيت.
- يتم ارتكاب الجريمة الالكترونية عن بعد، فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وتتجاوز هذه الجريمة حدود إقليم الدولة الواحدة، أي جريمة عابرة للحدود.
- ترتكب الجريمة الالكترونية من طرف مجرمين لهم مهارات تقنية عالية في تكنولوجيا الإعلام والاتصال يستخدمون شبكة الانترنيت، والوسائل الفنية اللازمة لإتمام الجريمة.
- تتميّز الجريمة الالكترونية بسرعة انتشارها، وصعوبة اكتشاف مرتكبيها كالمروّجين للأفلام والصور الخليعة عبر شبكة الانترنيت، جرائم تخريب المعلومات ونشر الفيروسات... الخ.
- الجرائم الالكترونية تلحق خسائر بالاقتصاد الوطني للحكومة الالكترونية يقدّر بملايين الدولارات تفوق الخسائر الناجمة عن الجرائم التقليدية مجتمعة[2].

---

1 عمر فاروق حسني، تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي، مجلة المحاماة، الكويت، العدد12، نوفمبر 1989، ص13.

2 حققت الجرائم الالكترونية خسائر فادحة باقتصاد بعض الدول. على سبيل المثال بريطانيا الدولة الثانية بعد الولايات الأمريكية تعرض اقتصادها لخسائر سنة 1992 بسبب الجرائم الالكترونية بـــ1.1 مليون جنيه استرليني، بعد تعرض أجهزة الحاسوب للتطفل التشغيلي haching، والفيروسات، أما الولايات المتحدة الأمريكية قد خسرت 37 مليون دولار. لمزيد من التفاصيل أنظر: محمد علي العريان، مرجع سبق ذكره، ص 122. وفي آخر إحصائية لمؤسسة الرخصة الدولية لقيادة الكمبيوتر لمجلس التعاون الخليجي قدرت خسائر دول الخليج ب735 مليون دولار في حين أن الاقتصاد الأمريكي لوحده قدرت خسائره بـــ250 مليون دولار.

### 3-أنوع الجرائم الالكترونية:

الجريمة الالكترونية تضمّ أشكال متعددة ومتنوعة يصعب حصرها، قد تقع على الأشخاص، وتقع على الأموال، ومنها من ترتكب ضد أمن الدولة بالتجسس عليها... الخ، ويمكن تقسيم هذه الجرائم إلى خمس مجموعات على سبيل المثال لا الحصر كما يلي:

**المجموعة الأولى:** الجرائم الواقعة على البيانات بحذفها أو تغييرها أو تخريبها أو استغلالها بشكل غير قانوني للقيام بعملية القرصنة.

**المجموعة الثانية:** الجرائم الواقعة على الكمبيوتر وذلك باختراقه لتدمير البرامج والبيانات المحفوظة في ذاكرته عن طريق نشر الفيروسات.

**المجموعة الثالثة:** الجرائم التي يستخدم فيها الكمبيوتر أو شبكة الانترنيت بالتخطيط لارتكاب جريمة معينة كجرائم الإرهاب، الجريمة المنظمة، تجارة المخدرات....الخ.

**المجموعة الرابعة:** جرائم استخدام الكمبيوتر بشكل غير قانوني من قبل أفراد مرخص لهم باستعماله كعمال الشركة، فينتقمون من شركتهم بحذف المعلومات وتخريبها.

**المجموعة الخامسة:** جرائم الانترنيت، وترتكب هذه الجريمة بواسطة كمبيوتر أو هاتف نقال موصول بشبكة الانترنيت التي تسمح لهم بزيارة المواقع الالكترونية وتصفحها، وتبادل الرسائل عن طريق البريد الالكتروني وإجراء محادثات بالصوت والصورة، وغالبا ما ترتكب هذه الجريمة من قراصنة يطلق عليه اسم "الهاكرز" HACHERS أو كراكرز CRACHERS؛ يتسلّون باستخدامهم شبكة الانترنيت كترويجهم للأفلام والصور الخليعة، النصب والاحتيال، تعطيل مواقع الكترونية[1].

كل أنواع الجرائم الالكترونية المذكورة في المجموعات الخمس خطيرة، وتزداد خطورتها عندما ترتبط بجرائم تقليدية خطيرة، كارتباطها بالجريمة المنظمة التي يستعمل فيها مرتكبوها تكنولوجيا الإعلام والاتصال لتنفيذ الجريمة في أسرع وقت

---

1 تعرض موقع جريدة الشروق، الشروق أون لاين إلى عملية قرصنة في شهر مارس 2010 اعتمدت فيها أحدث التكنولوجيات، وذلك بتحايلهم لشراء سيرفيرات الشروق من الشركة الأمريكية الراعية له، كما قام القراصنة باستهداف مؤسسة جيكوس واستغلوا بياناتها وبريده الالكتروني، وقاموا بتحويل عنوان الموقع اسم النطاق لفائدة مؤسسة أخرى. لمزيد من التفاصيل جريدة الشروق الجزائرية، العدد 2876 الصادر بتاريخ 17 مارس 2010.

ممكن دون اللجوء إلى وسائل الترهيب والعنف.فالجريمة المنظمة شكلا من أشكال الإجرام الجسيم الذي يشكل تحديا خطيرا لأجهزة العدالة في العديد من دول العالم، ولاسيّما بعد أن اكتسبت بعدا دوليا في ظل التحولات السياسية والاقتصادية والاجتماعية التي شهدها المجتمع الدولي في العقدين الأخيرين، وخاصة مجال تكنولوجيا الإعلام والاتصال، الذي سهّل وّسرع من ارتكاب الجريمة المنظمة[1]، ويقصد بالجريمة المنظمة أنها مشروع إجرامي يتم بقدر كبير من الاحتراف والتنظيم ينطوي على عدد من الأنشطة الإجرامية يقوم بها مجرمون يستعملون مختلف وسائل الترهيب لتحقيق أهدافهم، والتي تتجسد بالدرجة الأولى في جني الأرباح وبسط السيطرة والنفوذ[2].

تصبح الجريمة المنظمة أكثر خطورة عندما يستخدم مرتكبوها الوسائل التقنية لتكنولوجيا الإعلام والاتصال وشبكة الانترنيت، لتحقيق الأرباح في أسرع وقت ممكن وبأقل جهد، ويستعينون بأشخاص أذكياء لهم مهارات تقنية يقتسمون معهم الأرباح، أو إكراههم على ذلك تحت طائلة التهديد والعنف، وهذا يكسب المنظمات الإجرامية مهارات كبيرة في اكتشاف واستغلال فرص القيام بأعمال ومشاريع جديدة غير مشروعة توفرها لهم الانترنيت والتجارة الالكترونية التي تسمح لهم بتبييض الأموال وغسيلها. ومن أمثلة المنظمات الإجرامية التي اكتسبت المهارات نجد المنظمات الكولومبية لتجارة المخدرات التي استعانت بأشخاص من الخبراء الماليين الالكترونيين من أجل غسل أموالها، ويمنحونهم مقابل ذلك مكافآت سخية أو من خلال تهديدهم وتهديد أفراد أسرهم بالقتل. ومن الأمثلة كذلك استخدمت المنظمات الإجرامية شبكة الانترنيت في أكتوبر سنة 2000 لسرقة الأموال إلكترونيا من بنك صقلية، بحيث قامت مجموعة متكونة من 20 شخصا بعضهم يرتبط بعائلات المافيا، وبمساعدة شخص من البنك الذي مكنهم من نسخة رقمية طبق الأصل لنظام وصل البنك بشبكة الانترنيت، فقررت المجموعة استعمال النسخة الرقمية لتحويل 400 مليون دولار كان الاتحاد الأوروبي قد خصصها لتمويل مشاريع إقليمية في صقلية، وكان من المقرر غسيل هذه الأموال من طرف الشبكة الإجرامية في مؤسسات مالية مختلفة من بينها بنك الفاتيكان، وبنوك في

---

1 أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة، التجريم وسبل المواجهة، مطبعة العشري، بدون بلد النشر، 2006 ، ص12.

2 محمد محي الدين عوض، الجريمة المنظمة، المجلة العربية للدراسات الأمنية والتدريب، المركز العربي للدراسات الأمنية والتدريب، الرياض، المجلد 10، العدد 19، جويلية 1995، ص06.

سويسرا، والبرتغال، وأحبطت هذه الخطة عندما أباح أحد أفراد المجموعة بالسر إلى السلطات الرسمية[1].

يلاحظ من خلال هذا الارتباط عن مدى خطورة ارتباط الجريمة المنظمة بالجرائم الالكترونية على أمن الحكومات، والخسائر الناجمة عن هذه الجرائم نتيجة جني المنظمات الإجرامية الأموال الطائلة من العمل المصرفي الالكتروني ثم تقوم بغسلها وتبييضها الكترونيا دون اللجوء إلى العنف وسفك الدماء، ودون أن تترك أثارا تمكّن الحكومة من اكتشاف مرتكبيها وتعقبهم لمحاكمتهم، وخاصة إذا كانوا يقيمون خارج إقليم المجني عليه أو مسرح الجريمة.

**ثانيا: نظام الإثبات في الجرائم الالكترونية:**

من خصائص الجريمة الالكترونية صعوبة إثباتها واكتشاف مرتكبها نظرا لارتكابها من جناة محترفون يمتلكون مهارات فنية عالية يحيطونها بسرية تامة، وكلمات مرورية، وأرقام تشفيرية يصعب اختراقها، كما أنهم يرتكبونها وهم بعيدين عن مسرح الجريمة، وخارج حدود إقليم الدولة، لذا تصعب مهمة المحققين من ضباط شرطة وقضاة في جمع أدلة الإثبات، لذا يبقى الإشكال المطروح كيف تتعامل أجهزة التحقيق بعدما اصطدمت بهذه الصعوبة في جمع أدلة الإثبات وإحالتها على جهة الحكم للفصل فيها؟ هذا ما نحاول الإجابة عليه من خلال دراستنا لوسائل الإثبات طبقا للقواعد العامة، ووسائل الإثبات التقنية.

**1- القواعد العامة للإثبات في الجرائم الالكترونية:**

هذه القواعد تمر بمرحلتين، مرحلة جمع أدلة الإثبات ثم مرحلة وسائل الإثبات التي يستند عليها قاضي الحكم في إدانة مرتكبي الجرائم الإلكترونية. إجراءات جمع أدلة الإثبات:

إجراءات جمع الأدلة طبقا للقواعد العامة التي يباشرها المحققين وهي: المعاينة، التفتيش، ضبط الأشياء، سماع شهود، ندب خبراء، الحجز التحفظي، الحبس الاحتياطي.

**أ-1- المعاينة:** يقصد بإجراء المعاينة هو الانتقال لإلى مسرح الجريمة، ومعاينة كل ماله علاقة بالجريمة من أشياء أو أشخاص، وغالبا ما يكلف بهذا الإجراء ضباط الشرطة القضائية، قضاة النيابة، قضاة التحقيق، وفي الجرائم الالكترونية توسع مهمة

---

1 محمد محي الدين عوض، المصدر نفسه، ص 06.

المحققين في مباشرة إجراء المعاينة، وصورة ذلك قانون الإجراءات الجزائية الجزائري خوّل لضابط الشرطة القضائية إجراء المعاينة بناء على إذن مسبق من النيابة العامة في محلات سكنية أو غير سكنية وفي أي وقت، ولا يشترط تصريح مكتوب من صاحب المسكن، وفي الجرائم الأخرى يحد من صلاحياتهم كتحديد وقت المعاينة، التصريح المكتوب[1]. ويلاحظ على المشرع الجزائري وسع من صلاحيات المحققين في الجرائم الالكترونية والجرائم المنصوص عليها المادة 3/47 نظرا لخطورة هذه الجرائم على المصلحة الوطنية.

**أ-2- التفتيش:** هو البحث عن شيء يتصل بالجريمة، ويفيد في الكشف عن الحقيقة، والتفتيش قد يشمل المحلات السكنية وغير السكنية والأشخاص، وفي الجرائم الالكترونية يشمل جميع وسائل التكنولوجيا والاتصال التي استعملت في ارتكاب الجريمة، وتفتيش البيانات المخزنة فيها، والاطلاع على البريد الالكترونية وتفتيشه، وأسندت مهمة التفتيش للمحققين مع توسيع صلاحياتهم في مجال الكشف عن الجريمة الالكترونية وصورة ذلك ما نصت عليه المادة 3/47 والمادة 64 من قانون الإجراءات الجزائية الجزائري المشار إليهما سابقا.

**أ-3- سماع الشهود:** للمحقق في الجرائم الالكترونية أن يسمع الشهود وهم الأشخاص الذين كانوا في مسرح الجريمة أو لديهم معلومات تقنية تفيد الكشف عن الجريمة، وغالبا ما يكون الشهود من أصحاب الخبرة، والمتخصصين في مجال تكنولوجيا الإعلام والاتصال[2].

**أ-4- ندب خبراء:** يمكن للمحقق أن يندب خبيرا في تكنولوجيا الإعلام والاتصال أو الاستعانة بمخابر مختصة في هذا المجال، لتزويد المحقق عن كيفية

---

1 نصت المادة 3/47 من قانون الإجراءات الجزائية الجزائري: "وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص"، ونصت المادة 64 من نفس القانون: "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه الإجراءات... وعندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة3/47 من هذا القانون تطبق الأحكام الواردة في تلك المادة، والمادة 47 مكرر".

2 محمد فهمي، الموسوعة الشاملة للمصطلحات الالكترونية، مطابع المكتب المصري الحديث، القاهرة 1991، ص23.

ارتكاب الجريمة، ومن أهم المسائل التي تتناولها الخبرة: تركيبات جهاز الكمبيوتر، تاريخ الصنع، الطراز، نوع نظام التشغيل، كلمات المرور، كيف يمكن عزل المعلومات دون إتلاف أدلة الإثبات أو تخريبها، نقل الأدلة في صورة مادية كطبع في أوراق لتمكين القاضي من الاطلاع عليها[1].

**أ-4- ضبط الأشياء المثبتة للجريمة:** يقصد بالضبط هو وضع المحقق يده على كل شيء يتصل بالجريمة، وتفيد في الكشف عن الحقيقة، ومجال الجرائم الالكترونية غالبا ما يضبط المحققين على سبيل المثال: الأوراق سواء المطبوعة أو المسودة، جهاز الكمبيوتر ولواحقه، أقراص الليزر،الشرائط الممغنطة، جهاز المودم الذي يوصل الكمبيوتر بشبكة الانترنيت، البطاقات الممغنطة، وبطاقات الائتمان القديمة، والمادة البلاستيكية المستعملة في إعداد تلك البطاقات، كل ذلك يعد أثرا أو جزء من جسم الجريمة ينبغي البحث عنها وفحصها في التحقيق مع الإشارة أن مثل هذه الآثار تحتاج إلى خبرة فنية لاستعمالها كدليل إثبات.

**أ-5- الحجز التحفظي:** لضابط الشرطة القضائية أن يحجز الشخص المشتبه فيه لمدة زمنية قصيرة قبل إطلاق سراحه، القانون الجزائري في المادة 51 إجراءات جزائية نص على مدة الحجز بـــ48 ساعة، وفي الجرائم الالكترونية تمدّد مرة واحدة بإذن مكتوب من وكيل الجمهورية[2]، ويهدف الحجز إلى المحافظة على أدلة الإثبات، وخوفا من طمس أثار الجريمة، وخاصة أن الجناة هم من المحترفين، وذوو المهارات التقنية.

**أ-6- الحبس الاحتياطي:** إجراء الحبس الاحتياطي هو إجراء استثنائي يصدره قاضي التحقيق المختص، واستثناءا النيابة العامة وفقا لإجراءات التلبس، وذلك للمحافظة على أدلة الإثبات، وعندما لا يقدم المتهم الضمانات الكافية للمثول أمام القضاء

**أ- وسائل الإثبات:**

بعد أن ينتهي المحققين من جمع الأدلة في التحقيق الابتدائي، ويحرّرون محاضر وتقارير عن الأدلة المستخلصة، يحيلونها إلى القاضي الجنائي لتقييمها ومناقشة مدى حجيتها كوسيلة إثبات، والتشريعات الجنائية لا تختلف كثيرا عن وسائل الإثبات

---

1 جرائم الكمبيوتر، بحث مقدم من مركز البحوث والدراسات بشرطة دبي، الإمارات العربية المتحدة، 1998، ص 02.

2 أنظر نص المادة 51 من قانون الإجراءات الجزائية الجزائري.

المعتمدة في إثبات الجرائم بوجه عام سواء جرائم تقليدية أو جرائم الكترونية، وللتعرف على هذه الوسائل نتطرق إلى عرض الوسائل التي اعتمدها المشرع الجزائري في إثبات الجرائم في المواد 212 وما بعدها من قانون الإجراءات الجزائية الجزائري وهي كالتالي[1]:

**ب-1- الاعتراف:** نصت عليه المادة 213 ق.إ.ج وهو وسيلة من وسائل الإثبات، وحجيته تخضع للسلطة التقديرية للقاضي، وفي الجرائم الالكترونية فإن القاضي يمكنه الاستعانة بخبير لتقييم هذا الاعتراف لأنه اعتراف من شخص يملك مهارات تقنية في مجال التكنولوجيا.

**ب-2- الشهادة:** تعد الشهادة من أقوى وسائل الإثبات الجنائية، نص عليها المشرع في المادة 220 وما بعدها من ق.إ.ج، ويتم استدعاء الشهود من طرف القاضي عن طريق النيابة، وإذا تخلّفوا عن الحضور يمكن إحضارهم بالقوة، ويدلون بشهادتهم بعد أداء اليمين؛ في الجرائم الالكترونية غالبا ما يكون الشهود من أصحاب المهارات التقنية في الكمبيوتر والانترنيت.

**ب-3- المحاضر والتقارير:** نصّ المشرع الجزائري على هذه الوسيلة في إثبات الجرائم المادة في 214 ق.ا.ج، فمحاضر وتقارير الشرطة القضائية إذا استوفت الشروط الشكلية وحررت من ضابط شرطة مختص مكانا وزمانا تعتبر وسيلة إثبات تأخذ على سبيل الاستدلال، أما المحاضر والتقارير التي يحررونها عند قيامهم بمهام الضبط القضائي لإثبات جنح فإنّها تأخذ على سبيل الحجية، ما لم يثبت العكس بالكتابة أو شهادة الشهود[2]؛ وفي الجرائم الالكترونية نظر لخصوصيتها فإنّ كل المحاضر والتقارير تدخل ضمن الأحكام المنصوص عليه في المادة 216 ق.ا.ج، لذا فإنها تحوز الحجية ما لم يثبت العكس كتابيا أو شهادة الشهود.

**ب-4- المعاينة والانتقال:** نص المشرع الجزائري عل هذه الوسيلة في إثبات الجريمة في المادة 235 من ق.ا.ج، وتلجأ المحكمة إلى هذه الوسيلة جوازيا عندما لم تتمكن من تكوين اقتناع إيجابي أو سلبي كامل بوسائل الإثبات المقدمة لها، ورأت أن إظهار الحقيقة يتطلب انتقالها لمعاينة مكان الجريمة أو إعادة تمثيلها، أو بناء على طلب النيابة العامة أو المتهم أو المجني عليه، وإذا رفضت طلبهم تسبّب طلب

---

1 المشرع الجزائري تناول وسائل الإثبات ضمن فصل خاص من الكتاب الثاني من قانون الإجراءات الجزائية تحت عنوان "طرق الإثبات" من المواد 212 إلى المادة 238، وتبنى مبدأ الإثبات الحر في المواد الجنائية، أي أن هذه الطرق جاءت على سبيل المثال وليس على سبيل الحصر. أنظر المادة 212 من ق.إ.ج.

2 نصت على هذا الاستثناء المادة 216 ق.ا.ج.

الرفض، وعند انتقالها تبلّغ الأطراف ومحاميهم بساعة الانتقال وتاريخه، وعند الانتهاء من المعاينة تحرّر محضرا عن ذلك.

في الجرائم الالكترونية يمكن اللجوء إلى هذه الوسيلة، وفي اعتقادنا أن هذه الوسيلة لا يمكن الاعتماد عليها كثيرا نظرا لطبيعة الجريمة الالكترونية وخاصيتها التي تتميز بالسرعة، وزوال أثار الجريمة بعد ارتكابها مباشرة، وغالبا ما تنصب على معلومات وبرامج، كما أن لا يمكن إعادة تمثيل الجريمة نظرا لهذه الطبيعة.

**ب-5- الخبرة:** نصت على هذه الوسيلة المادة 143 من ق.ا.ج بأنه يجوز للقاضي أن يندب خبيرا كلما عرضت عليه مسألة ذات طابع فني، وذلك إما بناء على طلب الأطراف أو النيابة العامة أو من تلقاء نفسه. والاستعانة بالخبراء هو الطريق الأمثل في إثبات الجريمة الالكترونية، لأنّ هذه الأخيرة ترتكب بوسائل تقنية بحتة عن طريق الكمبيوتر أو الهاتف النقال، كما أنّها تقع على بيانات وبرامج، ممّا يجعل القاضي ملزم باللجوء إلى خبير في تكنولوجيا الإعلام والاتصال يأمره بإعداد تقرير خبرة عن الوسائل المستخدمة في ارتكابها، وجمع أدلة الإثبات لكشف مرتكبيها، ويعتمد عليه كحجة ودليل إثبات فيما تضمنه التقرير لإدانة المتهم أو تبرئته.

## 2- الوسائل التقنية لإثبات الجريمة الالكترونية:

إن وسائل الإثبات التي سبق الإشارة إليها تتعلق بالقواعد العامة للإثبات في كل الجرائم سواء تقليدية أو الكترونية، وهي إجراءات روتينية يقوم بها المحققين من ضباط شرطة وقضاة عند وقوع أي جريمة، وهذه الوسائل ترتبط أكثر بالمسرح المادي للجريمة، إلاّ أنّ الجريمة الالكترونية لها مسرح آخر هو المسرح الالكتروني أو الرقمي الموجود على الجهاز، لذا فإنّ البرامج والتطبيقات والبيانات الرقمية عناصر أساسية لإثبات الجريمة الالكترونية يتعين على أجهزة العدالة الجنائية جمعها واستخلاصها كدليل إثبات[1].

---

[1] أدى انتشار استخدام الكمبيوتر وشبكة الانترنيت عالميا إلى ضرورة تطوير وسائل الإثبات بما يواكب التطور في وسائل الإجرام المعلوماتي، وأصبح متطلبا من أجهزة العدالة الجنائية أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي الالكتروني، وهذا الأمر هو الذي دفع المنظمة الأوروبية للاقتصاد والتعاون OCDE والمجلس الأوروبي إلى إعداد دليل لقواعد استخدام الكمبيوتر، ودور القانون في مختلف الدول تجاه هذا النوع المستحدث من الجرائم. لمزيد من التفاصيل أنظر ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول IP/TCP في بحث وتحقيق الجرائم على الكمبيوتر، مقال ورد على موقع الدليل الالكتروني العربي: www.arablawinfo.com.

خبراء تكنولوجيا الإعلام والاتصال وضعوا بروتوكولات اتصالات والتطبيقات المعلوماتية لتمكين المحقق من التحقق من وصول الاتصال أو الرسالة للجهة المقصودة فعلا، كما يمكنه معرفة جهة الإرسال، وهذه البروتوكولات تحظى بالأهمية في الكشف عن الجرائم الالكترونية نظرا لاحتوائها على كافة المعلومات والبيانات المتعلقة بنشاط مستخدم شبكة الانترنيت إذا كان نشاطه إجراميا سواء من حيث التحدي الزمني للاستخدام غير المشروع أو من حيث تحديد مكان صدور أو نشأة الفعل الإجرامي، ومدى اتساع هذا النشاط وتحديد المجني عليهم من حيث المكان والزمان أو تحديد من أصابهم الضرر الجرمي، ومن بين أهم البروتوكولات استخداما في مجال كشف الجرائم الالكترونية بروتوكول IP/TCP[1].

رغم أهمية البروتوكولات والبرامج في الإثبات الجنائي إلاّ أنها طرحت عدة إشكاليات تتعلق بمدى حجيتها القضائية ؟ وهل يمكن أن تكون أدلة إثبات لإدانة متهم يتمتع بحصانة قرينة البراءة الأصلية؟ الإجابة على هذه الإشكاليات تناولها المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في ري ودي جانيرو، ومؤتمر الأمم المتحدة المتعلق بمكافحة والحد من جرائم الكمبيوتر المنعقد بيناير سنة 2000، وخلصت هذه البحوث إلى أن الوسائل التقنية تحوز على الحجية القضائية بشرط أن تستكمل اختبارات الثقة للتأكد من صحة ودقة الأدلة الرقمية المستخلصة من أجهزة الكمبيوتر، والتأكد من الجهاز المستخدم، وإذا اجتازت هذه الأدلة باختبارات الثقة فإنها تصبح تتمتع بالحجية القضائية[2]؛ والمرور باختبارات الثقة

---

1 protocol بروتوكول التحكم بالنقل، IP/ Internet protocol بروتوكول الانترنيت هما من عائلة البروتوكولات الاتصالات بين عدة أجهزة، وهي المقياس المستخدم لنقل البيانات الرقمية عبر شبكة الانترنيت بواسطة الاتصال الهاتفي، البروتوكولين مستقلين لكن يعملان مع بعض من وبشكل متزامن، ويرتكزان على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية packet بين مختلف الوصلات السلكية واللاسلكية المتخصصة الموصولة فيما بينها، ويستعملان كدليل رقمي للإثبات الجنائي أو المدني، فبروتوكول IP يحتوي على معلومات عن الكمبيوتر، ولكن ليس عن الأشخاص، لذلك فمن الصعوبة إثبات أن شخص أحدث فعلا غير مشروعا، ومع ذلك يمكن استخدامه كقرينة قضائية ضد المالك أو صاحب الجهاز إلى أن يثبت العكس، ذلك أن نقطة بدء نشوء مسار بروتوكول IP/TCP يمكن أن تساعدنا في للوصول إلى المشتبه فيه، حيث أن مجموعة صغيرة من الأفراد هي التي يمكن أن تستخدم أجهزة محددة، وبأرقام وعناوين محددة.

2 ممدوح عبد الحميد، استخدام أدوات التحليل النظري الرقمي في تحقيق الجرائم عبر الكمبيوتر، مجلة الفكر الشرطي، المجلد الحادي عشر، العدد 44، الإمارات العربية، 2003.

قبل اعتماد الأدلة الرقمية كوسيلة إثبات شرط ضروري لان جمعها قد يمس بحريات وحقوق الأفراد، إذا لم يحسن استخدامها، لذلك يجب مراعاة الأحكام القانونية عند استخلاص الأدلة العلمية حتى يمكن قبولها، وتجدر الإشارة أن المحققين عند جمع الأدلة وعرضها على اختبار الثقة يستعينون بخبراء تكنولوجيا الإعلام والاتصال المعتمدين لدى القضاء.

إذا كان استخدام الوسائل التقنية والأدلة الرقمية للكشف عن الجرائم الالكترونية قد لقي اهتماما دوليا فإن الاهتمام على المستوى العربي مازال مترددا، واكتفت التشريعات العربية بالحماية الجنائية المعلوماتية، وقواعد الإثبات في الجرائم التقليدية، دون التطرق إلى الدليل الالكتروني في الإثبات الجنائي، وتحديدها كيفية استخلاص الأدلة الرقمية لإثبات الجريمة الالكترونية.

التشريع الجزائري لم يهتم بهذه الوسائل والأدلة الرقمية لاستخلاصها كأدلة إثبات، واكتفى بإضفاء الحجية على الترتيبات التقنية التي يضعها المحققين بإذن من النيابة للكشف عن بعض هذه الجرائم من بينها الجرائم المعلوماتية، وتتمثل هذه الوسائل التقنية اعتراض المراسلات السلكية واللاسلكية، تسجيل الأصوات، والتقاط الصور[1].

## ثالثا: مكافحة الجرائم الالكترونية:

تزايد الجرائم الالكترونية وخطورتها أصبح يهدّد أمن الحكومة الالكترونية في إنجاح خططها التنموية في المجالات السياسية والاجتماعية والاقتصادية، وتتضاعف خطورتها أكثر عندما ترتبط بجرائم خطيرة تهدّد الدول والمجتمع الدولي في أمنه واستقراره كجريمة غسل الأموال، الجريمة المنظمة، تجارة المخدرات، الجرائم الماسة بأمن الدولة، ممّا جعل الدول أمام خيارين إما خيار العودة إلى الحكومة الكلاسيكية، وهذا مستبعد تماما بعدما أثبتت الحكومة الالكترونية نجاعتها في بناء اقتصادي قوي ساهم في حل المعضلات الاقتصادية، وبناء مجتمع قوي بأداء أعلى وكلفة أقل، كما أنها فعّلت من أداء الجهاز الحكومي الذي اجتاز كل مظاهر التأخر والبطء أو رسم إستراتيجية لمكافحة الجرائم الالكترونية وقمعها بتظافر الجهود الدولية والإقليمية لكشفها وكشف مرتكبيها، وهو الخيّار الذي لقي اهتماما

---

1 أنظر المادة 65 مكرر 05 من ق.ا.ج.

دوليا بمواجهته بآليات قانونية وطنية ودولية، واليات تقنية وقائية قبل حدوث الجريمة وبعدها.

1-**آليات قانونية:** تباشر الدول هذه الآليات المتمثلة في المواجه التشريعية للإجرام على الصعيد الوطني وذلك بمساهمة كل دولة بتشريعها الداخلي بإيجاد النصوص القانونية الكفيلة بمكافحة الجريمة وقمعها، والتشريع الدولي من خلال الاتفاقيات الدولية الثنائية ومتعددة الأطراف.

أ- **التشريع الداخلي:**

- **التجريم:** الدولة لما تظهر فيها سلوكيات من الأشخاص الطبيعية أو المعنوية تهدد استقرارها وأمنها القومي فإنها تواجه هذه السلوكيات بالتجريم وذلك بإصدار تشريع جزائي يشتمل على عقوبات رادعة ضد من يرتكب هذا الفعل، وما يتبعها من إجراءات لمحاكمته أمام القضاء الوطني. والدولة لما اقتحمت مجال تكنولوجيا الإعلام والاتصال لبناء الحكومة الالكترونية، أساء بعض الأشخاص استخدامها ونجم عنها ارتكاب سلوكيات خطيرة تهدد سلامتها، فواجهتها بإصدار قانون جزائي يجرم هذه الأفعال لمكافحتها، سمي بقانون مكافحة الجرائم الالكترونية، يقضي عدم شرعيتها، وتسلّط عقوبات زجرية ضد من يثبت ارتكابها، وأغلب الحكومات الالكترونية أصبحت تتمتع بهذه الحماية الجنائية[1].
- **تطوير قواعد الإثبات الجنائي:** إن معظم الدول أدركت أن الصعوبة في الجرائم الالكترونية تكمن في إثباتها نظرا لسرعتها واختفاء أثارها المادية، لذا اعتمد المشرع الوطني وسائل إثبات تقنية يستعين بها القاضي لإثبات الجريمة كالأدلة الرقمية، والاستعانة بالخبراء، كما أعطى للمحققين صلاحيات واسعة في الكشف عن الجريمة، ولو كانت إجراءات جمع الأدلة تمس بحقوقهم وحرياتهم.
- **عالمية النص الجنائي:** إن أغلب الدول تطبق قانونها الجزائي طبقا لمبدأ الإقليمية إذا وقعت الجريمة على إقليمها، ومبدأ الشخصية إذا كان الجاني أو المجني عليه يحملان جنسيتها، أو مبدأ العينية إذا كانت الجريمة تمس بأمن الدولة، وفي الجرائم الخطيرة تعطي الدولة لنصها الجنائي العالمية أي ينعقد الاختصاص لقضائها الوطني، رغم عدم توافر أي مبدأ من المبادئ المشار إليها، ويستند هذا

---

1 أغلب دول العالم جرمت الجرائم الالكترونية للحد منها في تشريعاتها الوطنية، ومن بين هذه الدول نجد الدول العربية من بينها: الجزائر، السعودية، الإمارات العربية المتحدة، الأردن، تونس...الخ.

الاختصـــاص للتضامـــن الدولي والالتزام الدولي[1]، وهذا المبدأ هو من أهم الآليات في مكافحة الجريمة الالكترونية نظرا لطبيعتها بأنها تتجاوز إقليم الدولة الواحدة، ويرتكبها الجاني في أغلب الحالات من خلف شاشة الكمبيوتر في دولة أجنبية.

**ب- الاتفاقيات الدولية:**

تمثل الاتفاقيات الدولية الإطار القانوني للتعاون بين الدول في مجال مكافحة الجريمة الالكترونية، بخلق آليات لتعقب المشتبه فيهم، ومحاكمتهم والقبض عليهم لتنفيذ الحكم الصادر ضدهم عن طريق المساعدة القضائية، الإنابة القضائية، تسليم المجرمين، وتسخير المنظمات الدولية المتخصصة كالانتربول لتنفيذ أوامر المحاكم الوطنية التي أصدرت أوامر بالقبض ضد مرتكبي الجرائم الالكترونية.

**1- الآليات التقنية لمكافحة الجريمة الالكترونية:**

لجوء الدول إلى الآليات القانونية والقضائية غير كافي نظرا لصعوبة الإثبات هذه الجرائم، واختفاء أثارها مباشرة بعد ارتكابها، لذا فإن خبراء تكنولوجيا الإعلام والاتصال وبالتعاون مع الحكومة قاموا بوضع آليات تقنية تستمد الزاميتها من إجراءات الضبط الإداري بإصدار مجموعة من المراسيم التنفيذية، القرارات الوزارية واللوائح من أجل منع وقوع الجرائم الالكترونية، ويتحقق ذلك بأعمال التدخل الوقائي للحيلولة دون وقوع الجريمة، ومن بين الآليات التقنية الوقائية نذكر منها على سبيل المثال لا الحصر ما يلي:

- متابعة الإدارة يوميا لشبكات الاتصالات ومراقبتها، واتخاذ كافة الإجراءات تجاه المخالفين، كما تعمل على حذف المواقع الالكترونية ذات الأنشطة الإجرامية، وتشكل خطرا على المجتمع.
- مراقبة مقاهي الانترنيت، وتوجيه لها تعليمات وإرشادات حول تحمل مسؤولياتها تجاه زبائنها الذين يحاولون ارتكاب جرائم الكترونية، وضرورات تعاونهم مع مصالح الأمن لإخبارهم بالتخطيط لارتكاب جرائم الكترونية، والعمل على تشديد إجراءات منح الرخص بفتح مقهى الانترنيت بتعميق البحث الاجتماعي، والتأكد من أن طالب الرخصة غير مسبوق قضائيا.

---

1 فتحي سرور، المواجهة القانونية للإرهاب، دار النهضة العربية، القاهرة 2008، ص380.

- إعطاء الحماية للمعلومات الشخصية عند معالجة البيانات الالكترونية، وفقا للمبادئ التي حددتها معاهدة المجلس الأوروبي.
- اتخاذ إجراءات صارمة وتكثيف الجهود الرامية إلى توعية المجتمع بالأمن الالكتروني، وطرق الحماية من الجرائم الالكترونية.
- خلق مراكز وطنية تختص بالوقاية من الجرائم الالكترونية ومكافحتها.
- الأنظمة الوقائية الخاصة بتأمين شبكة المعلومات، ورصد عمليات الاختراق ومنعها، ووضع خطط لمواجهة الفيروس المعلوماتي الذي قد يؤدي إلى إتلاف البرامج وتدميرها، وكذلك تعطيل الأجهزة عن العمل والحيلولة دون وقوع الجرائم الالكترونية.
- خلق برامج تهدف للحماية الالكترونية، كالبرنامج الذي وضعته شركة ماكافي يهدف لمساعدة مستخدمي الكمبيوتر وشبكة الانترنيت للتعرف على أساليب الاحتيال، وتعتمد الطريقة على سؤال وجواب، وهذه الأسئلة يخضع لها الزائرون ليحددوا بأنفسهم إذا كان بإمكانهم إعاقة محاولات سرقة معلومات شخصية عنهم مثل كلمة السر، أرقام البطاقة الائتمانية.....الخ.
- التقيد بالدليل الالكتروني الذي وضعه الاتحاد الدولي للاتصالات للتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة على الانترنيت،، ويعتبر هذا الدليل خارطة الطريق فيما يتعلق بمعايير الأمن الخاصة بتكنولوجيا المعلومات والاتصالات.
- إسراع الدول لوضع ضوابط الحماية الالكترونية، وإنشاء أمن خاص لشبكات الاتصالات لمنع الجريمة قبل وقوعها، وهذا النظام يضبط كل من يحاول استخدام بطاقات الائتمان المسروقة.

## رابعا: الجريمة الإلكترونية في التشريع الجزائري:

المشرع الجزائري على غرار باقي التشريعات الوطنية جرّم كل الأفعال المتصلة بتكنولوجيا الإعلام والاتصال على مرحلتين:

- **المرحلة الأولى** كانت بتعديل قانون العقوبات بموجب قانون 04-15 المؤرخ في 10 نوفمبر 2004 وأدرج الجرائم الماسة بالمعالجة الآلية للمعطيات في قسم خاص وهو القسم السابع مكرر من قانون العقوبات من المواد 394 مكرر إلى 394 مكرر 07، وحددت هذه المواد الأفعال الجرمية التي تمس بالنظام المعلوماتي والعقوبات المقررة لكل فعل التي تتنوع إلى عقوبة الحبس ثلاث سنوات، والغرامة

المالية التي تصل إلى 5000.000 مليون دينار جزائري، كما عاقب المشرع الجزائري على الشروع في كل الجرائم التي تضمنها القسم السابع مكرر[1].

– **المرحلة الثانية** وهو صدور قانون 09-04 المؤرخ في 5 سبتمبر 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، وهذا القانون جاء يوسع من السلوكيات الإجرامية المتصلة بتكنولوجيا الإعلام والاتصال التي كانت محصورة في الجرائم الماسة بالمعالجة الآلية للمعطيات لتشمل كل الجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية[3]، وتضمن قواعد إجرائية خاصة بمراقبة الاتصالات الالكترونية من قبل الأجهزة الأمنية والسلطات القضائية، وحدد الحالات التي تسمح باللجوء إلى هذه المراقبة[4]، وقواعد إجرائية خاصة بتفتيش المنظومات المعلوماتية من قبل السلطات القضائية وضباط الشرطة القضائية، والسماح لها بحجز المعطيات المعلوماتية المكتشفة بعد التفتيش[5]، كما فرض هذا القانون على مقدمي خدمات تكنولوجيا الإعلام والاتصال[6] التزامات تتعلق بمساعدة السلطات القضائية والأمنية، وعدم عرقلتهم لسير التحقيقات، والتزامات تتعلق بالخدمات التي يقدمونها بحفظ كل المعطيات التي يلجأ لها عند الحاجة أو متى طلب منهم ذلك، ويقع مقدمي هذه الخدمات تحت طائلة عقوبات إدارية وجزائية عند امتناعهم تنفيذ هذه الالتزامات.

وأخيرا أنشأ هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، ثم خص هذا الجرائم بإجراءات خاصة بالتعاون

---

1 المادة 394 مكرر 7 من قانون العقوبات الجزائري.

2 قانون 09-04 مؤرخ في 5 سبتمبر 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة بتاريخ 16 سبتمبر 2009، ص 5 إلى ص 9.

3 المادة 2 من قانون 09-04.

4 المادة 4 من قانون 09-04.

5 المواد من 5 إلى 9 من قانون 09-04.

6 مقدمو الخدمات عرفتهم المادة 2 فقرة د من قانون 09-04 بنصها: "1- أي كيان عام او خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".

القضائي الدولي التي يجب على القضاء الجزائري التجاوب مع طلب المساعدة القضائية الدولية الموجه له من أي دولة ما لم يتعارض مع السيادة الوطنية والنظام العام[1].

ويلاحظ من خلال قانون 04-15 الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أن كلاهما لم يعرفا الجريمة الالكترونية، واكتفوا بتحديد سلوكيات الإجرامية ذات الصلة بتكنولوجيا الأعلام والاتصال، وتحديد القواعد الإجرائية الخاصة بالتحري والبحث والتفتيش التي يقوم بها ضباط الشرطة القضائية والنيابة العامة مع التطرق إلى حتمية التعاون القضائي الدولي لمكافحة الجرائم الإلكترونية، وفي غياب هذا التعريف تبقى الجريمة الالكترونية في التشريع الجزائري تخضع في مفهومها وبنيانها القانوني، وطرق إثباتها إلى مفهوم الجريمة الالكترونية بصفة عامة التي تطرقنا لها في مستهل هذه الدراسة.

**خاتمة:**

الحكومة الالكترونية أصبحت خيارا لا رجعة فيه للدول التي ترغب تحقيق التنمية الاقتصادية والاجتماعية، كما أنه الخيار الذي يستجيب لتطلعات الأفراد والشركات التجارية، إلاّ أن أمن الحكومة مهدد بفعل تنامي الإجرام الالكتروني وتنوعه، مما جعل الدول تولي أهمية لمكافحة الجريمة الالكترونية بوضع آليات قانونية وتقنية كما سبق الإشارة إليه، غير أن هذه الآليات تبقى غير كافية للحد من الجريمة الالكترونية نظرا لخطورتها وصعوبة إثباتها وتجاوزها حدود إقليم الدولة الواحدة، وتسارع تكنولوجيا الإعلام والاتصال، كالتدفق السريع للانترنيت، والهواتف الذكية. وصورة ذلك أن المشرع الجزائري اكتفى بصدور قانون 04-15 المعدل والمتمم لقانون العقوبات، وقانون 09-04 الخاص بالوقاية من الجرائم الالكترونية فهما في اعتقادنا غير كافيين في المرحلة الراهنة، وخاصة بعد إطلاق خدمة الجيل الثالث للهاتف النقال الذي تتميز بالتدفق السريع لتكنولوجيا الاتصال عن طريق الانترنيت، وأن رجل القانون سواء كان ضابط شرطة قضائية أو قاضي سيجد فراغا تشريعا بين تطور التكنولوجيا المتسارع والنصوص التشريعية.

---

1 المواد من 13 إلى 18 من قانون 09-04.

لذا خلصنا من خلال هذه الدراسة لبعض التوصيات قد تجد لها تطبيقا في الدول التي عجزت عن حماية حكومتها الالكترونية، أو أنها تستلهم منها بما يسمح لها من مراجعة منظوماتها التشريعية من خلال تحيين النصوص بما يتلاءم مع تطور تكنولوجيا الإعلام والاتصال المتسارع، وهي كالآتي:

- عقد مؤتمر دولي برعاية الأمم المتحدة لمكافحة الجرائم الالكترونية والوقاية منها، وسن قواعد قانونية دولية آمرة ملزمة لجميع الدول العضوة وغير العضوة.
- إبرام اتفاقيات دولية ثنائية وإقليمية لمكافحة الجرائم الالكترونية ن وتفعيل دور المنظمات الإقليمية كالجامعة العربية ومجلس التعاون الخليجين الاتحاد الأوروبي.
- سد الفراغ التشريعي في مواجهة الجرائم الالكترونية التي هي في تنامي مستمر وذلك من خلال تطوير النصوص القانونية وتحيينها باستمرار بما يستجيب لتطور تكنولوجيا الإعلام والاتصال المتسارع .
- تطوير وسائل الإثبات التقنية، وإضفاء الحجية عليها.
- تخصيص أجهزة أمنية خاصة بمكافحة الجريمة الالكترونية.
- إعداد الكوادر الأمنية والقضائية، والمخابر الجنائية لمعالجة الإجرام الالكتروني.
- إدخال مادة تكنولوجيا الإعلام والاتصال في المناهج التربوية، وفي كل الشعب الجامعية لنشر الوعي عن خطورة الجرائم الالكترونية.
- إنشاء مراكز وطنية خاصة بمكافحة الجرائم الالكترونية والوقاية منها، تسهر على أمن المعلومات والنظم المعلوماتية بالتعاون مع جميع القطاعات العامة والخاصة.