الجرائم المستحدثة بين الموضوع والوسيلة

Cybercrimes, between objectives and means

د. سميرة عبد الدايم[1*]،

[1] كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر.

تاريخ الاستلام: 2021/05/26 تاريخ القبول للنشر: 2021/06/29 تاريخ النشر: 2021/06/30

ملخص: تعتبر الجرائم المستحدثة من الجرائم ذات الطابع المميز والمعقد سواء من حيث موضوعها، أومن حيث وسيلة ارتكابها، أو من حيث سمات مرتكبيها، وهذا ما يستدعي ضرورة صياغة نظرية تشريعية عامة تعتمد على تطوير وسائل الوقاية منها، وتحديث آليات مكافحتها لدى الجهات الأمنية المختصة بذلك.

الكلمات المفتاحية: الجريمة المستحدثة، الوصف القانوني لها، الأجهزة الأمنية، وسائل الضبط الإداري، وسائل الضبط القضائي.

Abstract:

Modern crimes are characterized by their specific and complex nature whether about their motives; means used to commit them or the characteristics of their perpetrators. This requires the setting of a legislation based on the development of means and mechanisms to fight this form of criminality near the competent security authorities.

Keywords: modern crimes ; legal description ; security services ; means of administrative and judicial regulation.

* **المؤلف المراسل:** samiraabdedaim415@gmail.com

مقدّمة:

شهد القرن الحالي ظهور العديد من التطورات التي مسّت مجالات مختلفة من حياة الفرد والمجتمع، ولعلّ أهمها تلك المتعلّقة بما استحدثته العولمة في مجال التكنولوجيا الحديثة، أين ظهر الحاسوب بما يحتويه من تقنيات ومعدّات وبرامج بات استخدامها أمرا مهما في عدّة مجالات لا تتعلّق بحياة الفرد فحسب، بل أصبحت تمسّ عدّة قطاعات تخصّ مؤسسات وهيئات وشركات محلية وعالمية تعتمد عليه من حيث تنظيم أمورها وإبرام صفقاتها وتسجيل مشاريعها. كذلك لعب الحاسوب دورا لا يستهان به في مجال تعزيز وتفعيل مهام الأجهزة الأمنية إدارية كانت أم قضائية في الدولة، التي باتت تستخدمه في مهام شتى كتسجيل الجرائم ومرتكبيها ودلائل إثباتها وكذلك حيثيات قضياهم والأحكام الصادرة في حقهم. ولقد تعزّزت أهمية الحاسوب خاصة بعد ظهور شبكة الانترنت العالمية التي سهلت عملية الاتصال وإتاحة المعلومة والتي أصبحت في متناول كل فرد في جميع المجالات.

غير أنّه وإن كان للحاسوب والشبكة العنكبوتية الدور الفعّال والايجابي في تحسين المستوى المعيشي للفرد في جميع جوانبه وعلى جميع الأصعدة، إلاّ أنّ لهذا الجانب جانب آخر معاكس يتبلور في الآثار والانعكاسات السلبية التي تنتج عن الاستعمال غير المشروع لهذه التقنية، ممّا جعلها وسيلة هامة وفعّالة في يد أي مجرم لتحقيق أعماله الإجرامية، وهذا ما ساعد على تزايد وتيرة ظهور جرائم مستحدثة متّصلة بالحاسوب وشبكة الانترنت، تمثّلت هذه الجرائم في تمكين المجرم من الولوج إلى الحاسوب وتدمير برامجه التي تعدّ بمثابة العقل المفكر له، واختراق بياناته التي تعدّ بمثابة بنوكه المعلوماتية بغية كشف أسرارها أو سرقتها أو إتلافها. هذا بالإضافة إلى العديد من الجرائم التي سهّل الحاسوب ارتكابها مثل القيام بعمليات الغش والاحتيال المعلوماتي، والقرصنة واختراق النظم المعلوماتية، والقيام بعمليات السطو المصرفي من خلال السحب من الأرصدة والاعتماد على الدفع الالكتروني، وبثّ البرامج الخبيثة واستخدامها في إتمام صفقات مشبوهة، بل الأكثر من ذلك اعتمد الجناة على الحاسوب والشبكة العنكبوتية في ارتكاب جرائم دولية، كأعمال التصنّت والتجسس عن المعلومات المتعلقة بالأمن القومي، وكذلك الاعتداء على حقوق الملكية الفكرية كتقليد برامج الحاسوب وبياناته الخاضعة للحماية، إذ لم تقتصر خطورة هذه الجرائم على المساس بالحياة العامة، بل امتد استخدام هذا السلاح المعلوماتي إلى مستودعات الحياة الخاصة للفرد وانتهاك حرمتها.

نظرا لخطورة هذه الجرائم حاليا على امن المجتمع والتي تنبئ بنشوء جيل على مستوى عالي من الإجرام مستقبلا، كان لزاما على التشريعات الوطنية تكييف نصوصها القانونية مع ما يتماشى وهذه الجرائم المستحدثة، وذلك من خلال العمل على مقاربة ترسانتها الجزائية خاصة الإجرائية منها مع ما يفرضه التطور التكنولوجي

بهدف الحدّ من هذه الجرائم التي أخذت أبعادا دولية، مع خلق جهات أمنية مختصّة تسهر على حصرها ومكافحتها.

استنادا لصعوبة هذا النوع من الجرائم التي تعدّدت تعاريفها بتعدّد صورها، تمحورت الدراسة حول إشكالية أساسية مفادها: فيما يتمثل الإطار القانوني للجريمة المستحدثة، وما مدى فعالية الجهات الأمنية المختصة بمكافحتها؟،

للإجابة على ذلك، كان من الضروري تسليط الضوء على كل من الوصف القانوني للجريمة المستحدثة والتقنيات المستخدمة في ارتكابها، وكذا تحديد مدى فعالية الإجراءات الإدارية والقضائية المتّخذة من الجهات المختصّة بمكافحة هذه النوع من الجرائم وذلك من خلال تقويم السياسات الأمنية المقرّرة لمواجهة هذا السلوك الإجرامي المتطوّر في ظل دراسة قانونية وأمنية متكاملة.

المبحث الأول:

الإطار القانوني للجرائم المستحدثة

يمكن تعريف الجرائم المستحدثة على أنّها تلك الجرائم العابرة للحدود والتي تقع على شبكة الانترنت أو بواسطتها، يختص بتنفيذها أشخاص فائقي القدرة والدراية بمجالاتها.ولقد تعدّدت صور الجرائم المستحدثة بقدر ما تعدّدت الوسائل المستعملة في ارتكابها

المطلب الأول:

التصنيف القانوني للجرائم المستحدثة:

تعدّدت صور الجرائم المستحدثة حتى لا يتسع المجال للحديث عن كل صورها وأنواعها، لذلك سيتم اختيار أكثر الجرائم المثيرة للمشكلات القانونية كجرائم الاعتداء على الحياة الخاصة، وجرائم الأموال، والجرائم الماسة بحقوق المؤلف المادية والمعنوية عبر الشبكة العنكبوتية.

الفرع الأول:

جرائم الاعتداء على الأشخاص:

لا تعتبر الخصوصية من الحقوق الملازمة للشخص الطبيعي بصفته الإنسانية فحسب، بل تعدّ مظهر من مظاهر حق الإنسان في احترام حياته وشخصه، نصّت على هذا الحق أغلب الدساتير الوطنية والنظم القانونية وكذا الاتفاقيات الدولية، كالإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة

بموجب قرارها رقم 217[1] وذلك في مادته 12، والذي يشكل إطارا قويا وشاملا لتعزيز وحماية الحق في الخصوصية، إذ ربط الإعلان ومن خلال المادة السالفة الذكر الحق في الخصوصية بمبدأ الكرامة الإنسانية، فهو شرط أساسي وضمانة هامة لإعمال الحقوق الأخرى، كالحق في بلورة الأفكار وإبداء الرأي بكل استقلالية والتعبير عنها بكل حرية، وهو نفس ما تضمّنته الاتفاقية الأوربية لحماية البيانات، بالإضافة إلى العديد من القواعد التشريعية للاتحاد الأوربي ومجلس أوربا وكذا المفوضية الأوربية، وكل الدول الأعضاء في هذه المنظمات التي تبنت مبادئ قانونية تخصّ حماية الحق في الخصوصية من مخاطر المعالجة الآلية للبيانات[2].

غير أنّه وبظهور الثورة التكنولوجية الهائلة وشيوع استخدامها على نطاق واسع، فإنّ الممارسات الجارية في العديد من الدول كشفت على قدرة العديد من الأشخاص الدخول إلى البيانات المخزنة بالحاسوب، والاطلاع عليها أو استعمالها استعمالا غير مشروع قد يمسّ بكرامة صاحبها ومصلحته، وهذا ما يعكس ويثبت عدم كفاية إنفاذ التشريعات الوطنية وضعف وعدم فعالية الضمانات الإجرائية المتخذة في هذا المسار، ممّا أسهم في توسع دائرة الإفلات من العقاب على التدخل التعسفي وغير القانوني في الحق في الخصوصية.

يتخذ المساس بالحق في الخصوصية والاعتداء على حرمة الحياة الخاصة أحد الأشكال التالية:

– استعمال الجاني لبيانات شخصية غير حقيقية، أو محوها آليا بغية تحقيق غاية مادية، أو قيامه بجمع ومعالجة بيانات شخصية حقيقية تخصّ أفراد معينة، ولكن هذا الجمع والتخزين يتمّ بصورة غير قانونية من قبل أشخاص ليس لديهم الحق في ذلك[3].

– قيام الجاني بالاستحواذ على معلومات أو صور شخصية عن طريق استعمال المعالجة الآلية لقواعد البيانات التابعة لأشخاص معينة، وإعادة فبركتها في حالات قد تمثل مساس بحرمتهم وكرامتهم.[4]

---

[1]– الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتّحدة بموجب قرارها رقم 217 بتاريخ 1948/12/10 ، ولقد تبني المشرّع الجزائري مبدأ احترام الحق في الخصوصية على غرار العديد من المبادئ الأخرى الذي تضمنها الإعلان في جميع الدساتير المتعاقبة بداية من دستور 1996 إلى غاية دستور 2020. أنظر المادة 47 من المرسوم الرئاسي رقم 251/20 مؤرخ في 15 سبتمبر 2020، المتضمّن استدعاء الهيئة الانتخابية للاستفتاء المتعلّق بمشروع تعديل الدستور، ج.ر عدد 54، صادر في 2020/09/16.

[2]– محمود عبد الرحمن، نطاق الحق في الحياة الخاصة، دراسة مقارنة، دار النهضة العربية، 1994، ص 234.

[3]– مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة،2000 ، ص101.

[4]– لقد جرّم مشروع الاتفاقية الأوربية الخاص بجرائم الانترنت والكمبيوتر (2000–2001) هذا النوع من الأفعال، واعتبره من الجرائم المرتبطة بالمحتوى، والتي تضمّ طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلّقة بالأفعال الإباحية والأخلاقية. محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2007، ص59.
أنظر كذلك: محمد محمد الألفي، المسؤولية الجزائية عن الجرائم اللاأخلاقية عبر الانترنت، المكتب المصري الحديث، 2005، ص102.

–كذلك قد يتخذ الاعتداء على الحق في الخصوصية شكل التجسّس، والذي يعتبر وسيلة تأثير هامة على المعلومات الخاصة بالأفراد سواء تعلّق الأمر بمعلومات سياسية، دينية أو شخصية، ويهدف الجاني من وراء ذلك الحصول على البيانات المخزنة لتغييرها أو تدميرها أو تحويلها.[1]

– من جهة أخرى، قد يتمثل فعل الاعتداء على الحق في الخصوصية كذلك قيام الجاني بجرم القذف والتشهير، وهو جرم تقليدي نصّت عليه معظم قوانين العقوبات، غير أنّه وبدخول تقنيات الاتصال والمعلوماتية أصبحت هذه الجريمة من الجرائم التقليدية التسمية الحديثة الأسلوب في ارتكابها، ويقصد بالقذف والتشهير عملية بث أفكار أو معلومات أو فضائح أو أخبار ترتب أضرار مادية لأصحابها إلى جانب الأضرار المعنوية، فتحط من كرامتهم وقيمتهم.

الفرع الثاني:

جرائم الاعتداء على الأموال

تتعدّد الصور التقليدية لفعل الاعتداء على الأموال كالنصب والسّرقة واختلاس الأموال العامة وخيانة الأمانة، وغيرها من الأفعال التي جرّمت ارتكابها اغلب التشريعات الوضعية، إلاّ أنّ هذا النوع من الجرائم اتخذ طابعا وأسلوبا احترافيا مغايرا منذ ظهور اختراع الحاسوب، أين أصبحت تتمّ هذه الجرائم من قبل جناة يتميزون بقدرتهم الفائقة وثقافتهم العالية في مجال التعامل مع هذه التكنولوجيا الحديثة بما لا يسمح بترك أي أثر مادي لتعقبهم، وما زاد الأمر تعقيدا تدعيم الحاسوب بالشبكة العنكبوتية، أين أصبح القيام بعمليات الاحتيال والسطو وتحويل الحسابات المصرفية من الجرائم العابرة للحدود والتي تتمّ في لحظات معدودة.

فعلى سبيل المثال ساعد التطور التقني في زيادة عمليات غسيل الأموال[2] خاصة بعد اعتماد أغلب شركات العالم والمؤسسات المصرفية التعامل النقدي الالكتروني الذي يتم عبر الشبكة العنكبوتية، فبرز ما يسمى بالغسيل الرقمي، إذ أصبحت تتميّز هذه الجريمة التي تتم عبر الانترنت بسرعة إتمامها وعدم ترك أية أثار لها[3]. فأصبحت هذه الجريمة من الجرائم الدولية المضمون تشفيرها ونجاحها، تتم من خلال تحويل الأموال من حساب لآخر، ومن بلد لآخر، عن طريق الاعتماد على الوسائل التقنية المتطوّرة التي استطاع الفكر البشري تحقيقها

---

[1]– حسن داوود طاهر، جرائم نظم المعلومات، الرياض، 2000، ص 58.

[2]– تعرّف جريمة غسيل الأموال على أنّها إخفاء المصدر الحقيقي للأموال والذي يكون في أغلب حالاته مصدرا غير مشروع، فهي عملية تظهر من خلالها أموال لم يكن بالإمكان التعامل معها إلاّ من خلال إضفاء صفة المشروعية عليها بسبب أنّها كانت ناتجة عن ممارسات غير مشروعة مخالفة للنظم القانونية المعمول بها. أنظر: إبراهيم حسن عبد الرحيم الملا، المواجهة الجزائية لجريمة غسيل الأموال، دراسة مقارنة، دار القلم، 2009، ص251.

[3]– نفس المرجع، ص252.

من أجهزة الحاسوب إلى شبكة الانترنت، وهذا ما ساعد على إخفاء مصدر المكاسب غير المشروعة والتي تخفي في طياتها أفعالا غير مشروعة.

كذلك من بين أهم الجرائم التي ساعد الحاسوب والشبكة العنكبوتية على ارتكابها وتعسير إثباتها ومكافحتها، جريمة السّرقة والاحتيال. إذ تعرّف السّرقة حسب القواعد العامة على أنّها اختلاس مال منقول مملوك للغير بطريق الغش وبنية تملكه[1]، إذ يمكن استعمال الحاسوب كأداة للقيام بجرم السّرقة من خلال الاعتماد على الشبكة العنكبوتية التي تسمح للجناة القيام بعمليات القرصنة الالكترونية على نقود الغير الالكترونية، وهذا ما يعرف بعملية سرقة الحسابات.

إذ يستفيد العديد من المتعاملين من الخدمات المصرفية أو الدّفع عبر شبكات العنكبوتية، غير أنّهم في كثير من الأحيان يتعرضون لاختراق وسرقة حساباتهم المصرفية، من خلال دفعهم إلى كشف معلوماتهم الخاصة بهم لصالح أشخاص خارجين عن العلاقة أو الرابطة التعاقدية التي تربطهم بالمؤسسة المصرفية وبطريقة غير مشروعة[2]، وذلك من خلال استخدام رسائل الكترونية احتيالية تعمل على إغراء المتعاملين ودفعهم إلى استظهار معلوماتهم المالية، هذه الرسائل الالكترونية تتصل بشكل ثابت مع موقع الكتروني مخادع مصمم لكي يظهر بمظهر الموقع الرسمي الخاص بالمؤسسة المالية الأصلية التي يتعاملون معها، إذ يطلب منهم من خلال هذا الموقع الإجابة على بعض الأسئلة التي تخص بيانات حسّاسة متعلّقة بحساباتهم المصرفية، كأرقام بطاقات الائتمان أو الرقم السري الخاص بحسابهم المالي.[3]

بالإضافة إلى جريمة تبييض الأموال وجريمة السرقة الالكترونية، نجد نوع آخر من الجرائم التي أصبحت تطرح إشكالات عديدة من حيث مكافحتها متى أصبحت تقع هذه الأخيرة في نطاق البيئة الرقمية، وهي جريمة النصب الالكتروني أو الاحتيال الالكتروني كما تسميه بعض التشريعات الوضعية كالقانون الأردني والعراقي واللبناني[4]. فلقد انتقلت جريمة النصب والاحتيال من طابعها التقليدي إلى طابع أكثر ذكاء وتطورا وسرعة من خلال شبكة الانترنت، التي أصبحت تستعمل في مجالات عدّة كالبيع والتبادل التجاري والدفع عبر بطاقات الائتمان، كل ذلك أدّى وبشكل بديهي إلى تزايد حالات النصب والاحتيال بسبب تعدّد وتطور وسائل

[1]– طارق حمزة، النقود الالكترونية كإحدى وسائل الدفع وتنظيمها القانوني والمسائل الناشئة عن استعمالها، رسالة دكتوراه، جامعة بيروت العربية، 2010، ص 196.

[2]-–Cabri lac Michael et Moly Christiane Droit pénal de la banque et du crédit Masson 1982. P 82

[3]– طارق حمزة، مرجع سابق، ص 198.

[4]–حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، مكتبة بدران الحقوقية، 2017، ص165.

النصب من استعمال طرق احتيالية وانتحال اسم كاذب أو صفة غير صحيحة، أو إيهام الغير بوجود مشروع كاذب أو إحداث الأمل بتحقيق ربح وهمي.[1]

الفرع الثالث:

جرائم الاعتداء على حقوق الملكية الفكرية

منحت أغلب الاتفاقيات الدولية كاتفاقية برن[2] ، وكذا التشريعات الوطنية بما فيها التشريع الجزائري[3]من خلال الأمر 05/03 حماية واسعة للحقوق الفكرية الأدبية بغض النظر عن نمط تعبيرها ودرجة استحقاقها وتوجّهها، شرط إفراغها في قالب شكلي مادي معين وكذا تمتّعها بالأصالة المتمثلة في البصمة الشخصية لمؤلفها، والتي تعكس مجهوده الشخصي في إبداع المصنف الفكري، غير أنّه وبتطوّر تقنيات الإعلام والاتصال، أصبحت هذه الأعمال الأدبية وبعد أن كانت تدرج ضمن دعامة ورقية أصبحت في مجملها تدرج ضمن الشبكة العنكبوتية في صيغتها الرقمية، ومن ثمّ أصبح الحاسوب يتضمّن مجموعة من البرامج وقواعد البيانات والصور الثابتة والمتحرّكة واللوحات الفنية والأفلام والخرائط والتصاميم، وكذا الكتب والمنشورات والمطبوعات والأعمال الأدبية الأخرى التي تخضع في مجملها للحماية بموجب قانون حقوق المؤلف، والتي لحق بها ما يسمى بالحقوق المجاورة لحقوق المؤلف المتمثلة في حقوق المؤدين والعازفين والمنتجين في مجال الفونوجرامات والإذاعة، كل ذلك وبعد أن كان يعرض سابقا في دعائم ورقية، أصبح حاليا يطرح في حقل رقمي، ممّا أدى إلى ظهور العديد من الإشكالات القانونية الخاصة بحماية حقوق المؤلف والحقوق المجاورة، سواء كانت حقوقا مادية أو معنوية[4]، بحيث أصبحت تتعرّض هذه الإبداعات الفكرية إلى ما يسمى بالقرصنة الالكترونية أو النسخ الالكتروني غير المشروع، والذي يتمّ دون ترخيص أو تفويض مسبق من صاحب الحق الأصلي، رغم ما منحته لها من حماية كل من المادة 04 من الأمر 05/03 ، والمادة 04 من اتفاقية الويبو لحماية حقوق المؤلف لسنة 1996[5]،

---

[1]–محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، بيروت، 2011، ص 68.

[2]– اتفاقية برن لحماية المصنفات الأدبية والفنية الموقعة سنة 1886، المنظمة إليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 97 / 341 المؤرخ في 21 /1997/09، ج.ر عدد 61، صادر في 14 /1997/09.

[3]– أمر رقم 03 /05 مؤرخ في 07/19/ 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر عدد 44، صادر في 07/22/ 2003.

[4]–محمد محي الدين عوض، حقوق الملكية الفكرية وأنواعها وحمايتها قانونيا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، 102.

[5]– معاهدتي الويبو بشأن حماية حقوق المؤلف والحقوق المجاورة لسنة 1996، وهما معاهدتان جاءتا استكمالا للنقائص التي شابت اتفاقية برن خاصة فيما يتعلّق بحماية المصنّفات الرقمية، تضمنتا مجموعة من الأحكام الخاصة بحماية حقوق المؤلف والحقوق المجاورة، كما تضمنتا حماية خاصة بالمصنّفات الرقمية وهذا استنادا لنص المادة 20 من اتفاقية برن التي تجيز للدول

والمادة 04 من اتفاقية الويبو لحماية الحقوق المجاورة الرقمية لنفس السنة، وكذلك اتفاقية تربس[1] في المادة 1/10 منها، والتي اعتبرت جميعها برامج الحاسوب وقواعد البيانات مصنفات أدبية بموجب اتفاقية برن تخضع في نظامها ونطاق حمايتها لقانون حقوق المؤلف.

ولا يقتصر وقوع الاعتداء على حقوق الملكية الفكرية الرقمية على برامج الحاسوب وقواعد البيانات فحسب، بل تعداه ليشمل كذلك المواقع الالكترونية والصفحات الرقمية العالمية، محركات البحث والمصنّفات الأدبية التي يتم نشرها في المحيط الرقمي وغيرها من الإبداعات الرقمية الخاضعة للحماية[2]، وهذا ما يؤثر سلبا على تمتع المؤلف صاحب الحق الأصلي بالاستئثار بحقوقه المادية والمعنوية التي لم تتغير رغم الثورة التكنولوجية التي شهدها العالم فيما يخص مجال تطور وسائل الإعلام والاتصال ورقمنة المصنّفات الأدبية والفنية، إذ بقي المؤلف يتمتع دائما بحقوق مادية على مصنّفه الرقمي مثل حق النسخ والنشر والتتبع وحق التأجير والتوزيع، وهي حقوق تخول صاحبها سلطة جني أرباح مادية لقاء استغلاله لعمله الفكري في محيطه الرقمي. أمّا الحقوق المعنوية، فهي مجموعة من الحقوق التي تكفلها القوانين الوطنية والاتفاقيات الدولية والتي تسمح لصاحبها التمتع بحقوق أدبية مثل حق الكشف عن مصنّفه ونسبته إليه، وحق المؤلف في سحب مصنّفه من التداول، وكذا حقه في احترام سلامة مصنفه الرقمي .

إذ لا يجوز للغير المساس بهذه الحقوق أو التصرّف فيها إلاّ من خلال الحصول على إذن مسبق من صاحب الحق، والعمل بغير ذلك قد يعرّض الفاعل لعقوبات منصوص عليها بموجب قانون حق المؤلف والحقوق المجاورة وكذا قانون العقوبات، إذ يتمتع المؤلف وأصحاب الحقوق من بعده وحدهم بحق وضع المصنّف الرقمي في متناول الجمهور، وكذا نشره وتوزيعه بما يلاءم وضعه ويخدم مصالحه، وأي عمل من شأنه تمكين الغير من الاطلاع على هذا البرنامج أو طرحه بالأسواق للتداول سواء بالبيع أو الإيجار دون إذن المؤلف، يعدّ عملا غير مشروع يتمثل في الاعتداء على الحق المادي للمؤلف ولصاحب الحق المجاور والمعاقب عليه قانونا.

واقعيا نلاحظ أنّ مثل هذه الاعتداءات واقعة فعلا على حقوق المؤلف والحقوق المجاورة في المحيط الرقمي، ممّا يحدّ من تمتّع المؤلف وأصحاب الحقوق المجاورة وذوي حقوقهم بما خوّلهم القانون من حقوق استئثارية. ويتمّ هذا التعدّي من خلال استعمال الجاني لعدّة وسائل تقنية من خلالها يمكنه الدخول إلى الشبكة

الأعضاء في اتحاد برن أن تبرم فيما بينها اتفاقيات خاصة، طالما أن هذه الأخيرة تمنح المؤلفين حقوقا تفوق الحقوق المنصوص عليها في اتفاقية برن.

[1] – اتفاقية الجوانب التجارية المتعلّقة بحقوق الملكية الفكرية، الموقعة في 15/04/ 1994، ودخلت حيز التنفيذ في جانفي 1995.

[2] –محمد محي الدين عوض، مرجع سابق، ص 18.

العنكبوتية والتلاعب في أمن الأنظمة المعلوماتية وما تحتويه من بيانات ومعلومات، أو تخريبها عن طريق إرسال برامج وفيروسات تهدف إلى تدمير أو إتلاف أو سرقة المعلومات.

المطلب الثاني:

الوصف القانوني للتقنيات المستخدمة في ارتكاب الجرائم المستحدثة:

يمكن تحديد الوصف القانوني للتقنيات المستخدمة في ارتكاب الجرائم المستحدثة من خلال تحديد مفهومها وطبيعتها القانونية، وكذا تبيان أنواعها وتفاوت درجة خطورتها.

الفرع الأول:

ماهية الفيروس كتقنية لارتكاب الجرائم المستحدثة

تعدّدت الأساليب والتقنيات الرقمية المستخدمة من قبل الجناة للدخول إلى النظم المعلوماتية المحمية والعبث فيها بما يخدم مصالحهم ويلبي رغباتهم، غير أنّ هذه الأساليب تصبّ جميعها ضمن مصطلح واحد هو مصطلح الفيروس الذي يعتبر بمثابة برنامج ذو إمكانية وقدرة كبيرة على تخريب وتدمير الأنظمة المعلوماتية بسبب ما يتمتّع به من قدرة على التخفي والوصول إلى الهدف بوسائل وصور عديدة ومختلفة، ولقد عانت العديد من القطاعات في مختلف المجالات من الفيروسات التي تصل إلى نظمها المعلوماتية وقواعد بياناتها وبريدها الالكتروني التي شلّت بسبب مثل هذه الفيروسات، والتي أدّت كذلك إلى توقيف حتى حركة الشركات المحلية والدولية من خلال التسلّل داخل النظام والبقاء فيه.[1]

وبالتالي يمكن القول أنّ الفيروس مهما كان نوعه هو عبارة عن برنامج من برامج الحاسوب الآلي، غير أنّه ذو طبيعة خاصة له أهداف محدّدة أساسها شلّ نشاط الحاسوب وإخلال توازنه وإتلاف بياناته.

ويعتبر الفيروس ذو طبيعة مادية ومعنوية، مادية من خلال الوسيط الذي يوجد في داخله هذا الفيروس، إذ يقوم بعمل جرمي متعمّد يمسّ برمجة معينة لإلحاق الضرر على أساس الخطأ المتعمّد في المعلومات التي يتضمّنها البرنامج، كما أنّه ذو طبيعة معنوية كونه نتاج العقل البشري، غير أنّه لا يتمتعّ بأي قيمة مالية بالرغم من كل ما يشمل عليه من خورزميات وهندسة وتركيب، كما لا يمكن اعتباره برنامج مشمول بأي نوع من حماية القانونية نظرا لدوره المخالف للقانون[2].

[1]– علي محمد رحومة، الانترنت والمنظومة التكنولوجية (بحث تحليلي في الآلية التقنية للانترنت ونمذجة منظومتها الاجتماعية)، مركز دراسات الوحدة العربية، 2005، ص 160.

[2]–انتصار نور الغريب، فيروسات الكمبيوتر، دار الراتب الجامعية، 1994، ص21.

الفرع الثاني:

أنواع الفيروسات المستعملة لارتكاب الجرائم المستحدثة

يأخذ الفيروس أشكالا عديدة، إذ يمكن للجاني أن يعتمد في تنفيذ أغراضه على العديد منها، والتي تعتبر جميعها بمثابة وسيلة تقنية تسهل العمليات الإجرامية في الفضاء الافتراضي، فهي تعمل على الدخول إلى النظام المعلوماتي من أجل تدمير أنظمة المعالجة الآلية أو تغيير وتخريب بيانات الملفات الرقمية، أو إتلاف جميع المعطيات الموجودة إتلافا كليا أو جزئيا، فهي تتفاوت من حيث الخطورة، إذ نجد البعض منها بسيط وسهل الاكتشاف، كما نجد غيرها خطير وبالغ الأذى ويطول زمن اكتشافها[1]. من بين أنواع الفيروسات المستعملة من قبل الجناة نجد حصان طروادة، وهو عبارة عن رقم سري يضاف إلى البرنامج فيخرب النظام فيه، وتكمن خطورته في أنّ النظام لا يشعر بوجوده حتى تحين اللحظة المحدّدة له ليؤدي دوره التخريبي، كذلك القنبلة المعلوماتية وهي عبارة عن نظام يصمّمه صاحب البرنامج ويثبته ببرنامجه ليقوم خلال وقت معين بتخريب كل المعلومات الموجودة في برنامجه. وتنقسم القنبلة المعلوماتية إلى نوعين:

–القنبلة المنطقية: وهي عبارة عن نوع من الفيروسات المصمّمة للعمل عند ظروف معينة أو لدى تنفيذ أمر معين، وتؤدي القنبلة في هذه الحالة إلى تخريب بعض النظم أو مسح بعض البيانات، أو تعطيل النظام عن العمل.

–القنبلة الموقوتة: وهي فيروس يعمل في ساعة معينة أو في يوم معين أو في سنة معينة، إذ يؤدي إلى تخريب النظام متى حان وقت ذلك .

أمّا الدودة المعلوماتية فهي عبارة عن برنامج له القدرة على الانتقال من حاسوب لآخر، لها إمكانيتها كبيرة على القيام بأعمال التخريب، وكذلك لها قدرة رهيبة على الانتشار والتكاثر الذاتي، فهي عبارة عن كود يسبب أذى للنظام عند استدعائه، وهي تتميز عن غيرها من الفيروسات بقدرتها على إعادة توليد نفسها، هذه الفيروسات وفيروسات أخرى تعمل جميعها على تحقيق هدف واحد هو تدمير أنظمة المعالجة الآلية للبيانات[2].

[1]– خليل عزة، مشكلات المسؤولية المدنية في مواجهة فيروس الكمبيوتر، دراسة مقارنة، القاهرة 1994، ص 220 .

[2]–حسين محمد الغول، مرجع سابق، ص220.

المبحث الثاني:

الأجهزة الأمنية المختصة بمكافحة الجريمة المستحدثة ووسائل تنفيذ اختصاصها

لا يمكن أن تكون هناك مؤسسة أو شركة أو هيئة قد سلمت من الوقوع ضحية مثل هذه الجرائم المستحدثة، أو على الأقل كانت هدفا لها، إذ تبدأ محاربة هذه الجرائم مثلها مثل بقية الجرائم التقليدية بالوقاية، وتحقيقا لذلك، عملت أغلب التشريعات الوطنية والاتفاقيات الدولية على تأسيس أجهزة أمنية تختص بمواجهة هذه الجرائم بمختلف أشكالها، وذلك في إطار قواعد قانونية وإجرائية مستحدثة حداثة هذه الجرائم، سواء تعلّق الأمر بالأجهزة الأمنية التي تمّ إقرارها من خلال التعاون الأمني على المستوى الدولي أو على المستوى الوطني (مطلب أول)، والتي اعتمدت في تنفيذ مهامها الإدارية والقضائية في مجال مكافحة الجريمة المستحدثة على العديد من الوسائل والإجراءات القانونية التي تضمّنت التشريعات القانونية النص عليها.

المطلب الأول:

تحديد الأجهزة الأمنية المختصة بمكافحة الجريمة المستحدثة

تحقيقا للحدّ من الجرائم المستحدثة والتخفيف من أثارها السلبية على الفرد والمجتمع، عملت أغلب التشريعات الوطنية والاتفاقيات الدولية على ضبطها بنصوص عقابية ردعية من جهة، ومن جهة أخرى عملت كذلك على إقرار أجهزة أمنية مختصة بمكافحتها (فرع ثاني)، غير أن ممارسة هذه الأخيرة لمهامها يتخلله العديد من الصعوبات القانونية الإجرائية والأمنية في مجال تجريم هذه الأفعال ومكافحتها (فرع أول).

الفرع الأول:

الصعوبات التي تواجهها الأجهزة الأمنية في مواجهة الجريمة المستحدثة

سبق القول أنّ الثورة التكنولوجية التي طغت على العالم بأسره والتي نتج عنها تطوّر ملحوظ في مجال الاتصال والمعلوماتية، أدّى إلى ظهور جرائم مستحدثة تطلّبت ضرورة إقرار هيئات إدارية وأخرى قضائية تعمل على كشف ملابساتها وتحديد مقترفيها[1]. ولعلّ أغلب التشريعات الوطنية منحت الاختصاص في ذلك إلى أجهزة أمنية مختصة، غير أن الإشكال الذي يثار في هذا الخصوص يتمحور حول أنّ الكشف عن مرتكبي هذه الجرائم ليس بالأمر الهيّن خاصة وأنّها تتميز بالتعقيد، باعتبارها جرائم تتمّ في وسط افتراضي يصعب معه ضبط أدلّته، كما تتمّ من طرف أشخاص فائقي القدرة والمعرفة بهذا المجال الرقمي، ممّا يسمح لهم بارتكاب أفعالهم غير المشروعة دون ترك أي أثار مادية تثبت جرمهم.

[1] -Bibent Michal ;Le Droit de traitment de l'information ; Paris 2000 ; P13.

إذ رغم محاولة أغلب الدول مواكبة عصر التكنولوجيا من خلال إصدار العديد من التشريعات القانونية المتعلّقة بالجرائم المستحدثة، وكذا الانضمام إلى العديد من الاتفاقيات الدولية المناهضة لمثل هذه الجرائم بهدف حصرها أو على الأقل التخفيف من أثارها، إلاّ أنّ العديد من هذه الدول أخفقت في ذلك نظرا لحداثة هذه الجرائم التي تختلف من حيث أركانها وأساليب ارتكابها عن الجرائم التقليدية، ممّا يصعّب مهام الجهات الأمنية المختصة بمكافحتها نظرا لعدم إمكانية تطبيق النصوص القانونية التقليدية عليها.

ضف إلى ذلك فإنّ ارتكاب مثل هذه الأفعال المجرّمة قانونا في بيئة رقمية افتراضية تعتمد على المعالجة الآلية للبيانات الرقمية، يجعل منها جرائم خفية يكتشفها المجني عليه بعد مرور فترة زمنية معتبرة، بل الأكثر من ذلك وما يزيد الأمر تعقيدا أنّ الجرائم المستحدثة تتمّ في أغلب حالاتها عن بعد، ممّا ينفي وجود الجاني في مسرح الجريمة، وهذا ما يصعّب بالنتيجة على الجهات الأمنية المختصة إثباتها لصعوبة ضبط أدلة مادية محسوسة، كما يندر ضبط الجاني متلبسا، والذي يتمتع بالذكاء والدهاء والخبرة التقنية الكافية لارتكاب مثل هذه الجرائم، مع إزالة وبكل سهولة أي أثر من شأنه إثبات فعله، ممّا يصعب على الجهات المختصة بالتحقيق التي يجب أن تتمتع بدراية علمية عالية بأنظمة الحاسوب وكيفية تشغيلها، مهمّة الكشف عن المجرم ومتابعته قضائيا[1].

وبذلك فإنّ الجريمة المستحدثة تتمّ في بيئة غير تقليدية خارج الإطار المادي الملموس، تقوم أركانها في بيئة افتراضية تتعلّق بالحاسوب والشبكة العنكبوتية، وهذا ما يجعلها أكثر تعقيدا لدى سلطات الأمن والأجهزة المكلفة بالتحقيق والمراقبة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام ألمعلوماتي، ممّا يجعل طمس الدليل من قبل الجاني سهلا.[2]

الفرع الثاني

الجهات الأمنية المختصة بمكافحة الجريمة المستحدثة

تتنوع الأجهزة الأمنية المختصة بمكافحة الجرائم المستحدثة منها ما هو ذو طابع دولي، ومنها ما هو ذو طابع وطني.

---

[1]–أحمد عاصم أحمد عجيلة، رؤية قانونية حول ثبوت جرائم السب والقذف عبر الانترنت في القانون المصري، ورقة عمل في المؤتمر الدولي الأول حول الخصوصية وامن المعلومات في قانون الانترنت، القاهرة 2008.

[2]–خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، بدون سنة نشر، ص 25. أنظر كذلك سيد طنطاري محمد سيد، الجريمة المعلوماتية، الصعوبات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها، مقال منشور على الموقع التالي: www.democratica.de

أولا-الجهات الأمنية المختصة بمكافحة الجريمة المستحدثة ذات الطابع الدولي

من بين أهم الخصائص التي تتميّز بها الجريمة المستحدثة سواء تلك التي تتمّ عن طريق الحاسوب أو عن طريق الشبكة العنكبوتية، أنّها ذات طابع دولي في أغلب حالاتها، إذ أنّها من الجرائم العابرة للحدود والتي تتخطى أثارها حدود الدولة الواحدة، فباعتبار أنّ المجتمعات العالمية أصبحت في وقتنا الحالي منفتحة على بعضها البعض من خلال الشبكات العنكبوتية، فإنّ ذلك أدّى وكنتيجة حتمية إلى اختراقها لأي مكان لاغيه بذلك جميع الفواصل بين الدول ودون أن تخضع لأي دساتير قانونية أو إجراءات حدودية، وهذا ما يجعل من التعاون الدولي في مجال مكافحة الجريمة المستحدثة أمرا في غاية الأهمية والضرورة، تستدعيه حتمية توفير الحماية اللازمة والكافية لأصحاب الحقوق المحمية والمكتسبة في البيئة الرقمية، وهذا ما سينعكس لا محالة على التشريعات الوطنية الخاصة بالحماية ضد الجريمة المستحدثة.

إذ قبل التطرق إلى أهم الأجهزة الأمنية الدولية المختصة في مكافحة هذه الجرائم، لا ضرر من تحديد أهم الجهود الدولية المبذولة من قبل المجتمع الدولي لإرساء أسس قانونية تعمل على حصر ومحاربة الجريمة المستحدثة، إذ وجدت على المستوى الدولي والإقليمي العديد من المنظمات والاتفاقيات الدولية والإقليمية التي نادت بضرورة تكاثف وتضافر الجهود الدولية والإقليمية من اجل إرساء منظومة قانونية وأخرى إجرائية تعمل على مكافحة الجريمة المستحدثة، والتي أصبحت تطلّ بخطورتها على كل المجتمعات الدولية[1]، ومن بين أهم هذه الهيئات الدولية التي تلعب دورا بارزا في كبح هذه الظاهرة بكل فعالية، منظمة الأمم المتحدة التي تنادي دوما بضرورة تعزيز العمل المشترك بين الدول الأعضاء من أجل إقرار نظم وقوانين تكفل الحدّ من انتشار الجريمة المستحدثة، وذلك من خلال عقد العديد من المؤتمرات التي تمحورت موضوعاتها حول ذلك، بداية بالمؤتمر السابع المنعقد سنة 1985 إلى غاية 2010 أين انعقد المؤتمر الثاني عشر. ناهيك عمّا لعبته المنظمة العالمية للملكية الفكرية[2] من دور فعّال لا يستهان به في مجال حماية برامج الحاسوب وقواعد البيانات، وذلك من خلال إقرار نصوص قانونية تبنتها الاتفاقيات الدولية التي أبرمت تحت ظلّها، مثل اتفاقية تربس واتفاقيتي الويبو لحماية حقوق المؤلف والحقوق المجاورة في النطاق الرقمي لسنة 1996. كذلك اتفاقية بودابست الخاصة بمحاربة الجريمة المستحدثة والمبرة بتاريخ 2001/11/23، التي وإن لم تنص على جهاز محدّد يختص بمكافحة هذه الجرائم، إلا أنّها أكّدت من خلال المادة 31 منها على ضرورة التعاون الدولي بين الدول الأعضاء

[1]- منير وممدوح الجنبيهي، جرائم الانترنت والحاسوب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص 200.

[2]-تعتبر المنظمة العالمية للملكية الفكرية من أهم المنظمات الداعمة لحماية الملكية الفكرية على المستوى الدولي،أنشئت بموجب اتفاقية إنشاء المنظمة العالمية للملكية الفكرية الموقعة بستكهولم، والمصادق عليها من قبل الجزائر بموجب الأمر رقم 02/75، المؤرخ في 1975/01/09، ج.ر عدد 13، صادر في 1975/02/14.

من اجل مكافحة هذا النوع من الجرائم العابرة للحدود وذلك من خلال إنشاء شبكة طوارئ دائمة لتشغيل المساعدة المتبادلة[1].

أمّا على المستوى الإقليمي فتمثلت الجهود الأوربية في الدور البارز الذي لعبه الاتحاد الأوربي في مجال حماية المعلومات والبيانات الرقمية، وذلك من خلال إبرام المعاهدة الدولية الخاصة بمكافحة الجرائم المستحدثة عام 2001، وكذلك إنشاء الأجهزة الإقليمية المختصة بمجال المكافحة كجهاز الأربول أو مركز الشرطة الأوربية، وهو أحد الأجهزة الأمنية الذي اتخذ من هولندا مقرا له، وتتمحور مهامه حول معالجة المعلومات المرتبطة بالأنشطة الإجرائية على مستوى الاتحاد الأوربي، وتزويد المحققين بتحاليل علمية ودعمهم بخبرته ومدهم بمساعدته التقنية، كذلك جهاز الانتربول أو المنظمة الدولية للشرطة الجنائية الذي مقرّه باريس، والذي يعمل على نشر ثقافة التعاون المتبادل بين سلطات البوليس في الدول الأطراف على نحو يضمن مكافحة الجريمة، موازاة مع تحديث النظم القانونية الواجب إقرارها للقضاء أو على الأقل السيطرة على مثل هذه الجرائم. ولا يخفى علينا ما لجهاز شرطة الانترنت من دور فعّال في مجال مكافحة الجريمة المستحدثة والذي يهدف إلى تحقيق الأمن وتطبيق القانون وردع كل متطاول عليه[2].

أمّا على مستوى التعاون العربي، فقد أسفر الاجتماع المشترك لمجلس وزراء العدل العرب المنعقد بالأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21 عن توقيع اتفاقية مكافحة الجرائم المستحدثة، والتي تضمّنت العديد من البنود التي تخصّ عملية الحصر لهذه الجرائم ومكافحتها، وذلك من خلال تحديد نطاق الأعمال المجرّمة التي تدخل ضمن إطار الجريمة المستحدثة (م06 إلى م18)، أين ألزمت الدول الأعضاء من خلال المادة 21 وبموجب تشريعاتها الوطنية تشديد العقوبة على الجرائم التقليدية التي يتم ارتكابها بوسائل تقنية المعلومات. كما لم تغض الاتفاقية النظر عن ضرورة تكاثف الجهود العربية لمكافحة هذا النوع من الجرائم المتطوّرة، من خلال إلزام الدول الأعضاء بتبني تشريعاتها الوطنية مجموعة من القواعد الإجرائية والقضائية التي تضمن من خلالها الجهات الأمنية المختصة أداء مهامها في هذا المجال، خاصة ما يتعلق منها بإجراءات التفتيش وضبط وتأمين المعلومات التقنية، والجمع الفوري لمعلومات تتبع المستخدمين.[3]

[1]– اتفاقية بودابست الخاصة بمحاربة الجريمة المستحدثة المبرمة بتاريخ 2001/12/23.

[2]–عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية، دار منشأة المعارف، الإسكندرية (بدون سنة نشر)، ص 474.

[3]–الاتفاقية العربية الخاصة بمكافحة جرائم تقنية المعلومات الموقعة بتاريخ 2010/12/21، المصادق عليها من قبل الجزائر بموجب الأمر رقم 252/14 المؤرخ في 2014/09/08، ج.ر عدد 57 صادر بتاريخ 2014/09/28.

ثانيا- الأجهزة الأمنية المختصة بمكافحة الجريمة المستحدثة ذات الطابع الوطني

لقد كانت الولايات المتحدة الأمريكية من الدول السباقة إلى الانتباه لمخاطر الجرائم المستحدثة ومحاربتها، باعتبارها مهد نشوء وتطور تقنيات الإعلام والاتصال، فلقد عانت الكثير من الجرائم الماسة بنظمها المعلوماتية خاصة ما يتعلّق منها بالأمن الوطني ونظامها العسكري، ممّا دفعها إلى إقرار العديد من الأجهزة الأمنية المختصة بمكافحتها، ولعلّ أهمها مكتب التحقيقات الفدرالي الأمريكي، والذي من بين اختصاصاته حماية المنشآت الوطنية من مخاطر الهجمات الالكترونية والجرائم المستحدثة عالية المستوى والمحتمل حدوثها، مع إصدار تحذيرات في حالة اكتشاف أي ثغرة أمنية جديدة تمسّ بالأنظمة المعلوماتية.

من جهة أخرى عرفت الهند بإنشائها لإدارة متخصّصة في مكافحة الجرائم المستحدثة تابعة لمكتب التحقيقات المركزي، وهو اكبر هيئة أمنية متخصّصة في متابعة الجرائم المستحدثة والتحقيق فيها، كما تضمّنت العديد من الدول الأخرى مثل أستراليا وبريطانيا مراكز خاصة بحماية أنظمة الاتصال والمعلوماتية التي يشكل اختراقها أثارا سلبية على امن الدولة والمجتمع.[1]

أمّا على المستوى العربي فوجدت في مصر مثلا العديد من الأجهزة المحلية لمكافحة الجرائم المستحدثة والمتعلّقة بالكمبيوتر والشبكة العنكبوتية، مثل الإدارة العامة لمباحث الأموال التي تضطلع بمكافحة الجرائم الاقتصادية المستحدثة التي يكون الحاسوب أداة لارتكابها. كذلك الإدارة العامة لمكافحة جرائم الحاسوب وشبكة المعلومات، والإدارة العامة لحماية المصنّفات الفنية، وهو جهاز يهتمّ بحماية الملكية الفكرية وحرّية الإبداع والتعبير من الأعمال غير المشروعة كالنسخ والتقليد الرقمي.

أمّا المشرّع الجزائري واقتداء بأغلب دول العالم، وأمام قصور القواعد القانونية التقليدية في مواجهة الجريمة المستحدثة، وجد نفسه أمام حتمية استحداث قوانين تنسجم وحداثة الجريمة، ممّا أدّى إلى تعديل القانون الجزائي بشقيه الموضوعي والإجرائي، من خلال التدخل بنصوص آمرة مستحدثة لتجريم الظاهرة وتحديد سبل وآليات مكافحتها، وذلك باستصدار قوانين خاصة تتلاءم والطبيعة الخاصة لهذه الجريمة، حيث استحدث المشرّع الجزائري القسم السابع مكرر من قانون العقوبات من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال الموسوم بأنظمة المعالجة الآلية للمعطيات من خلال نص المادة 394 مكرر إلى المادة 394 مكرر 7.

كما تضمنت التعديلات المختلفة لقانون الإجراءات الجزائية الجزائري عدّة قواعد إجرائية مستحدثة تتماشى وحداثة الجريمة، حيث خصّ المشرّع الجزائري هذه الجرائم بمجموعة من الإجراءات التي تمسّ كل من

[1]- الياس بن سمير الهاجري، أمن المعلومات على شبكة الانترنت، مركز الدراسات والبحوث، الرياض، 2004، ص125.

مرحلة التحري والتحقيق والمحاكمة. كما اصدر قانون 04/09[1] المتضمّن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي تضمّن مجموعة من النصوص القانونية التي تحدّد سبل متابعة الجريمة وتحديد مرتكبيها.

كما دعّم المشرع الجزائري ترسانته القانونية المتعلّقة بمكافحة الجرائم المستحدثة بهياكل وأجهزة أمنية متخصّصة بالبحث والتحري، أهم هذه الأجهزة ضباط الشرطة القضائية، الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتصال التي تمّ إقرارها بموجب أحكام المادة 13 من الأمر 04/09، المعهد الوطني للأدلة الجنائية وعلم الإجرام الذي تمّ استحداثه بموجب الأمر رقم 183/04[2] والذي يقوم باختصاصاته تحت القيادة العامة للدرك الوطني، أين يحتوي على قسم خاص بالتحقيق بكل ما يتصل بالجرائم المستحدثة، أمّا على مستوى المديرية العامة للأمن الوطني، فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية، وقد أسند لجميع هذه الأجهزة مجموعة من الاختصاصات في مجال ضبط الجريمة المستحدثة ومكافحتها، تعتمد في تحقيقها على نوعين من الوسائل: وسائل الضبط الإداري، ووسائل الضبط القضائي.

المطلب الثاني:

وسائل تنفيذ الأجهزة الأمنية لاختصاصاتها في مجال مكافحة الجريمة المستحدثة

يمكن تصنيف وسائل تنفيذ الأجهزة الأمنية للاختصاصات المنوطة بها قانونا في مجال مكافحة الجريمة المستحدثة إلى نوعين من الوسائل: وسائل خاصة بالضبط الإداري (فرع أول)، ووسائل أخرى خاصة بالضبط القضائي (فرع ثاني)، وتختلف كلا الوظيفتين عن الأخرى من حيث أنّ الأجهزة الأمنية تسعى من خلال الوسيلة الأولى إلى الوقاية من وقوع الجريمة من خلال اتخاذ الإجراءات والوسائل اللازمة للحيلولة دون ذلك، وتسمى هذه السلطة لدى بعض التشريعات بسلطة المنع. أمّا الضبط القضائي فيقصد به جميع الإجراءات التي تهدف إلى التحري عن الجريمة والبحث عن مرتكبيها، وجمع كافة العناصر والدلائل اللازمة للتحقيق في الدعوى الجنائية للتصرّف على ضوئها، وهي إجراءات يتم اتخاذها منذ لحظة وقوع الجريمة.[3] وتسمى هذه السلطة

---

[1]– أمر رقم04/09 المؤرخ في 05 /08/ 2009 المتضمّن القواعد الخاصة بالوقاية من الجرائم المتّصلة بالتكنولوجيا والإعلام والاتصال ومكافحتها، ج.ر عدد 47 ، صادر في 08/16/ 2009.

[2]– أمر رقم 183/04المؤرخ في 07/26/ 2004 المتضمّن استحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانون الأساسي له، المعدل والمتم بموجب الأمر رقم 118/09 المؤرخ في 2009/04/14، ج.ر عدد 24، صادر في 2009/04/22.

[3]– عفيفي كامل عفيفي، مرجع سابق، ص471.

أنظر كذلك: Christiane Feral; Cyber droit-Le droit a l'preuve de l'internet. Dalloz 3rd édition ;2004 ; P33

بسلطة العقاب، وعمليا يصعب التمييز بين سلطتي المنع والعقاب نظرا لوحدة الجهاز الأمني الذي يتحمل في الغالب مهام الوظيفتين بهدف تحقيق الفاعلية وتبسيط الإجراءات.

الفرع الأول:

وسائل الضبط الإداري للجرائم المستحدثة

اعتمد المشرّع الجزائري من خلال المادة 03 من الأمر 04/09 المتعلّق بالقواعد الخاصة بالوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية متى تعلّق الأمر بحماية النظام العام، على مجموعة من الإجراءات الأولية التي يمكن لضباط الشرطة القضائية اتخاذها بهدف الوقاية من وقوع الجريمة المستحدثة، أهم هذه الإجراءات ما يلي:

1-المراقبة الالكترونية للاتصالات، وتتمّ عن طريق تقنية الكترونية يختص بها المشرف على المراقبة من ضباط الشرطة القضائية الذي يراقب الاتصالات الالكترونية قصد تسجيلها واثبات كل ما هو مخالف للقانون، وقد حدّد المشرّع الجزائري بموجب أحكام المادة 04 من الأمر 04/09 الحالات التي يمكن اللجوء من خلالها إلى هذا الإجراء، أهمها تلك الأفعال المتعلّقة بجرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة، كذلك في حالة توفر معلومات عن احتمال وقوع اعتداء على المنظومة المعلوماتية متى كان من شأن ذلك تهديد النظام العام أو الدفاع والاقتصاد الوطنيين أو إحدى مؤسسات الدولة. كما يمكن اللجوء إلى هذا الإجراء الوقائي متى كان من الصعب الوصول إلى نتيجة تهمّ أبحاث خاصة بتحريات وتحقيقات قضائية، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

2-التفتيش الوقائي في المنظومة المعلوماتية، والذي يعتبر من بين الإجراءات التي تدخل ضمن الصلاحيات التي تساعد ضباط الشرطة والسلطات القضائية على أداء مهامهم في الوقاية من الجرائم المستحدثة، وذلك من خلال التفتيش في منظومة معلوماتية أو جزء منها من خلال المعطيات المعلوماتية المخزنة فيها، أو الدخول إلى منظومة تخزين معلوماتية بهدف نسخ المعطيات محل البحث على دعامة تخزين الكترونية قابلة للحجز، متى وجدت أنّ مثل هذه المعلومات من شأنها أن تفيد في الكشف عن الجرائم المستحدثة ومرتكبيها، شرط عدم المساس بسلامة ومضمون المنظومة المعلوماتية من معلومات تقنية.

من جهة أخرى استحدث المشرّع الجزائري وبموجب المادة 13 من الأمر 04/09 الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي اسند لها بموجب أحكام المادة 14 مجموعة من الاختصاصات تدور في مجملها حول مد المساعدة إلى السلطات القضائية وأجهزة الشرطة القضائية في إجراءات التحري بشان الجريمة المستحدثة، بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية، كما لها

صلاحية تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعطيات ذات الأهمية في التعرّف على مرتكبي الجريمة المستحدثة وتحديد مكان تواجدهم.

بالإضافة إلى هذه الإجراءات أقرّ المشرّع الجزائري وبموجب المادة 15 من الأمر السالف الذكر إجراء آخر يتمحور حول التعاون الدولي في مجال الوقاية من الجريمة المستحدثة وحماية الشبكة العنكبوتية، خاصة بعد أن سهلت هذه الأخيرة الحصول على المعلومات من أي مكان كان في العالم، إذ يجوز في حالة الاستعجال مع مراعاة الاتفاقيات الدولية المنظّمة لهذا المجال ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية إذا وردت عن طريق وسائل الاتصال السريعة كالفاكس أو البريد الالكتروني بعد التأكد من صحّتها.

كما أقرّ المشرّع الجزائري وسائل وآليات أخرى يمكن من خلالها للأجهزة الأمنية الوقاية من وقوع الجريمة المستحدثة، كقيام أجهزة الشرطة بعمل دوريات لمراقبة مؤسسات إنتاج الحواسب لضمان عدم حدوث نسخ أو تقليد لبرامجه بطريقة غير مشروعة، أو إساءة تصنيع مكونات الحاسوب بطريقة تستهدف الإضرار بمستخدميه. كذلك إضفاء صفة الضبطية القضائية على العاملين في المجال المعلوماتي من غير رجال الشرطة، كمزودي الدخول وخدمات الانترنت الذين بإمكانهم القيام بأعمال الرقابة، وتحديد بذلك مدى الخضوع للنظام والقانون من قبل العاملين والمتعاملين مع الشبكة العنكبوتية.

التوعية بإجراءات امن المعلومات: وهو إجراء مهمّ يتمثّل في مجموعة من الاحتياطات التي يجب على المختصين بمحاربة الجرائم المستحدثة والوقاية منها اتخاذها لمنع وقوعها، وذلك من خلال تحديد المعلومات الهامة، ثم تحديد المخاطر والتهديدات والقابلية للعدوان، حتى يتمّ اتخاذ الإجراءات اللازمة من خلال العمل على توعية العاملين في المنشآت الحيوية بضرورة وأهمية هذه الإجراءات في درء وقوع جرائم الكمبيوتر والانترنت على السواء.[1]

الفرع الثاني:

وسائل الضبط القضائي للجرائم المستحدثة

تتمثل وسائل الضبط القضائي في مجموعة من الإجراءات التي خوّل المشرّع الجزائري صلاحية القيام بها إلى ضباط الشرطة القضائية والهيآت التابعة لهم، أهم هذه الإجراءات نجد إجراء التفتيش[2] الذي لا يعتبر

[1]– عفيفي كامل عفيفي، مرجع سابق، ص 471.

[2]–يعد التفتيش من إجراءات التحقيق التي تختص بها أصلا سلطة التحقيق واستثناءا مأموري الضبط القضائي في جهاز الشرطة، ويمكن تعريفه على انه إجراء من إجراءات التحقيق التي يقوم بها موظف مختص طبقا للإجراءات المقررة قانونا، في مكان يتمتع

غاية في حدّ ذاته، وإنّما هو وسيلة لتحقيق غاية مفادها الوصول إلى ضبط أدلة مادية تساهم في بيان مرتكب الجريمة، ولقد تضمّنت الاتفاقيات الدولية خاصة اتفاقية بودابست وكذا التشريعات الوطنية بما فيها التشريع الجزائري مجموعة من البنود والنصوص القانونية التي تضبط عملية التفتيش في جريمة العالم الافتراضي. فاستنادا لنص المادة 05 من الأمر رقم 04/09، فانّ المشرّع الجزائري جعل من التفتيش اختصاصا استثنائيا لضباط الشرطة القضائية الذين يستعينون في ذلك بخبراء مختصين في مجال الحاسوب والنظم المعلوماتية، وذلك ضمن الحالات المنصوص عليها في المادة 04 من نفس الأمر، إذ يتمّ التفتيش وفقا لإجراءات قانونية مقرّرة بموجب المادة 12 و18 من قانون الإجراءات الجزائية.

كذلك من بين إجراءات الضبط القضائي نجد إجراءات المعاينة والبحث والتحري اللذان يعتبران من الإجراءات التي لا غنى عنها للوصول إلى ضبط أدلة تفيد في كشف ملابسات الجريمة المستحدثة، إذ تكمن أهمية المعاينة والتحري وفعاليتهما في التيسير على ضباط الشرطة الوصول إلى أدلّة مادية قبل أن تمتد إليها يد العبث أو قبل زوال معالمها، وما تجدر الإشارة إليه أنّ القيام بهذه الإجراءات في جرائم العالم الافتراضي يثير العديد من الإشكالات والصعوبات أهمها قلّة الآثار المادية التي قد تتخلّف عن ارتكاب الجريمة المستحدثة، مع إمكانية تردّد العديد من الأشخاص على مسرح الجريمة خلال المدّة الفاصلة بين ارتكابها والكشف، عنها ممّا يؤدي إلى العبث بالآثار المادية أو زوالها، استنادا لذلك انتهجت بعض التشريعات الوضعية بما فيها التشريع الجزائري مجموعة من القواعد والإرشادات الفنية عند إجراء المعاينة والتحري، أهمها عدم التسرّع في نقل أي مادة معلوماتية من مكان وقوع الجريمة قبل إجراء الاختبارات اللازمة حتى لا يحدث أي إتلاف للبيانات المخزّنة، كذلك حفظ المستندات الخاصة بالإدخال وكذا مخرجات الحاسب الورقية التي قد تكون ذات صلة بالجريمة، من اجل رفع ومضاهاة البصمات التي قد تكون موجودة، مع حفظ ما تحتويه سلّة المهملات من أوراق وشرائط وأقراص ممغنطة وفحصها...وغيرها من الإجراءات الضرورية الأخرى.

بالحرمة بهدف الوصول إلى أدلة مادية لجريمة تحقق وقوعها بهدف إثباتها ونسبتها لمرتكبها. أنظر عفيفي كامل عفيفي، مرجع سابق، ص 323.

خاتمة:

عملت اغلب الدول على سن قواعد قانونية تضمن من خلالها حصر الجريمة المستحدثة وضبطها، وقد دعّمت هذه القواعد بمجموعة من الهياكل الأمنية التي تعمل على اتخاذ مجموعة من الإجراءات القانونية والتدابير الوقائية من اجل الوقاية منها ومكافحتها، وهذا ما حذا حذوه المشرّع الجزائري الذي ارتكز في تدخله التشريعي لمواجهة هذه الجريمة على كل من القانون الجزائي بشقيه الموضوعي والإجرائي، كما استحدث قانون 04/09 الذي تضمّن مجموعة من النصوص القانونية التي سعى من خلالها إلى وضع أسس قانونية للوقاية من الجريمة المستحدثة. كما منح المشرّع الجزائري الاختصاص الواسع لمجموعة من الهياكل الأمنية في مجال الوقاية والمكافحة وضمان سلامة المعلومات والبيانات التي يحتوي عليها نظام الحاسوب وأنظمة المعالجة الآلية، غير أنّ ما هو جدير بالملاحظة أنّ الجريمة المستحدثة تتميز بتطوّر التقنية المستعملة في ارتكابها، ممّا يستلزم معه مواكبة القانون والأجهزة الأمنية المكلفة بالوقاية والمكافحة لهذا التطور اللامتناهي، وذلك من خلال وضع أنظمة قانونية حاسمة لضبط هذه الجرائم وردع مرتكبيها، ويتحقق ذلك من خلال:

– سرعة إصدار وتحديث المنظومة التشريعية بصفة مستمرة حتى تكون ملائمة ومتكاملة ومسايرة دائما لما تتطلبه إجراءات الوقاية والمكافحة، وذلك من خلال إرساء مجموعة من التدابير الوقائية والقواعد القانونية العقابية والإجرائية الحاسمة لضبط هذه الجرائم وردع مرتكبيها.

– تشجيع إنتاج برامج المكافحة الالكترونية والتوعية بأهميتها كبرامج التصنت والمراقبة والتتبع.

–الاهتمام بالدورات التدريبية للمكلفين بالوقاية والمكافحة وتوعيتهم بالأساليب المستحدثة والمتطوّرة في هذا المجال.

– كذلك وعلى المستوى الدولي ضرورة التأكيد على عقد المزيد من الاتفاقيات الدولية الخاصة بهذا المجال، مع تفعيل الاتفاقيات المبرمة وقواعد القانون الدولي ذات الصّلة.

–التعاون مع الدول ذات الخبرة الواسعة في هذا المجال والاستفادة من خبراتها في مجال المكافحة.

- الاتفاقية العربية الخاصة بمكافحة جرائم تقنية المعلومات الموقعة بتاريخ 2010/12/21، المصادق عليها من قبل الجزائر بموجب الأمر رقم 252/14 المؤرخ في 2014/09/08، ج.ر عدد 57 صادر بتاريخ 2014/09/28.

– أمر رقم 183/04المؤرخ في 07/26/ 2004 المتضمّن استحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانون الأساسي له، المعدل والمتم بموجب الأمر رقم 118/09 المؤرخ في 2009/04/14، ج.ر عدد 24، صادر في 2009/04/22.

قائمة المراجع والمصادر:

أولا- بالغة العربية:

- **الكتب**

1- إبراهيم حسن عبد الرحيم الملا، المواجهة الجزائية لجريمة غسيل الأموال، دراسة مقارنة، دار القلم، 2009.

2- الياس بن سمير الهاجري، أمن المعلومات على شبكة الانترنت، مركز الدراسات والبحوث، الرياض، 2004.

3- انتصار نور الغريب، فيروسات الكمبيوتر، دار الراتب الجامعية،.1994

4- حسن داوود طاهر، جرائم نظم المعلومات، الرياض، 2000

5- حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، مكتبة بدران الحقوقية، 2017.

6- خليل عزة، مشكلات المسؤولية المدنية في مواجهة فيروس الكمبيوتر، دراسة مقارنة، القاهرة 1994.

7- خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، بدون سنة نشر.

8- علي محمد رحومة، الانترنت والمنظومة التكنولوجية (بحث تحليلي في الآلية التقنية للانترنت ونمذجة منظومتها الاجتماعية)، مركز دراسات الوحدة العربية، .2005

9- عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية، دار منشأة المعارف، الإسكندرية (بدون سنة نشر).

10- محمود عبد الرحمن، نطاق الحق في الحياة الخاصة، دراسة مقارنة، دار النهضة العربية، 1994.

11- مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة،2000

12- محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2007.

13- محمد محمد الألفي، المسؤولية الجزائية عن الجرائم اللاأخلاقية عبر الانترنت، المكتب المصري الحديث، 2005.

14- محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، بيروت، .2011

15- محمد محي الدين عوض، حقوق الملكية الفكرية وأنواعها وحمايتها قانونيا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

16- منير وممدوح الجنبيهي، جرائم الانترنت والحاسوب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.

- **الرسائل والمذكرات الجامعية:**

1-طارق حمزة، النقود الالكترونية كإحدى وسائل الدفع وتنظيمها القانوني والمسائل الناشئة عن استعمالها، رسالة دكتوراه، جامعة بيروت العربية، 2010.

- **المقالات والمداخلات:**

1- أحمد عاصم أحمد عجيلة، رؤية قانونية حول ثبوت جرائم السب والقذف عبر الانترنت في القانون المصري، ورقة عمل في المؤتمر الدولي الأول حول الخصوصية وامن المعلومات في قانون الانترنت، القاهرة 2008.

2- سيد طنطاري محمد سيد، « الجريمة المعلوماتية، الصعوبات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها»، مقال منشور على الموقع التالي: www.democratica.de

- **النصوص القانونية:**

1-الاتفاقيات الدولية:

- اتفاقية برن لحماية المصنفات الأدبية والفنية الموقعة سنة 1886، المنظمة إليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 97 / 341 المؤرخ في 21 /1997/09، ج.ر عدد 61، صادر في 14 /1997/09.

- الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتّحدة بموجب قرارها رقم 217 بتاريخ 1948/12/10.

- اتفاقية الجوانب التجارية المتعلّقة بحقوق الملكية الفكرية، الموقعة في 04/15/ 1994، ودخلت حيز التنفيذ في جانفي 1995.

- معاهدتي الويبو بشأن حماية حقوق المؤلف والحقوق المجاورة لسنة 1996.

- اتفاقية بودابست الخاصة بمحاربة الجريمة المستحدثة المبرمة بتاريخ 2001/12/23.

- الاتفاقية العربية الخاصة بمكافحة جرائم تقنية المعلومات الموقعة بتاريخ 2010/12/21، المصادق عليها من قبل الجزائر بموجب الأمر رقم 252/14 المؤرخ في 2014/09/08، ج.ر عدد 57 صادر بتاريخ 2014/09/28.

2-النصوص التشريعية:

- أمر رقم 02/75 مؤرخ في 1975/01/09، يتضمن مصادقة الجزائر على اتفاقية إنشاء المنظمة العالمية للملكية الفكرية،ج.ر عدد 13، صادر في 1975/02/14.

- أمر رقم 03 /05 مؤرخ في 07/19/ 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر عدد 44، صادر في 07/22/ 2003.

- - أمر رقم04/09 المؤرخ في 05 /08/ 2009 المتضمّن القواعد الخاصة بالوقاية من الجرائم المتّصلة بالتكنولوجيا والإعلام والاتصال ومكافحتها، ج.ر عدد 47 ، صادر في 08/16/ 2009.

ثانيا: باللغة الفرنسية:

1- CABRI lac Michael , Moly Christiane, Droit pénal de la banque et du crédit, Masson, 1982.

2 –BIBENT Michal, Le Droit de traitement de l'information ; Paris 2000.

3- FERAL Christiane, Cyber droit-Le droit a l'preuve de l'internet, 3 em édition, Dalloz, Paris, 2004.