ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2022 المجلد: السادس العدد: الاول ص.ص: 1734-1752.

معوقات التحقيق الجنائي في الجرائم الالكترونية

Obstacles to the criminal investigation of electronic crimes

حيمي سيدي محمد*
جامعة أبو بكر بلقايد- تلمسان
mohammed.himmi45@gmail.com

تاريخ إرسال المقال: 01-08-2021 تاريخ قبول المقال: 25-01-2022 تاريخ نشر المقال31-03-2022

الملخص:

ترتب على الاستخدام المتزايد لوسائل الاتصال الحديثة وشبكات الانترنيت ظهور نمط جديد من الجريمة أطلق عليه مسميات عدة منها الجريمة الالكترونية والجريمة المعلوماتية، هذه الظاهرة الاجرامية المستجدة باتت تمثل خطرا على أمن الدول وحقوق الافراد الخاصة أو على حقهم في الخصوصية المعلوماتية، فالتحقيق في جرائم المعلوماتية يتطلب مهارات فنية وتقنية ذات طابع خاص إذ يجب أن يتمتع بها أفراد الضبطية القضائية.

موضوع الدراسة يتلاءم مع التطورات الحديثة في مجال المعلوماتية، حيث أدى انتشار الحاسوب إلى إساءة استخدامه ووجود أنواع من السلوك غير المشروع وظهور جرائم من نوع خاص. فالجرائم الالكترونية تختلف عن الجرائم التقليدية حيث أن هذا التباين أوجد تحديات جديدة وغير معهودة لدى جهات التحري والتحقيق وجهة القضاء لمكافحة هذه الظاهرة الاجرامية.

الكلمات المفتاحية: الجريمة الالكترونية، تحقيق، مهارات فنية، معلومات، حاسوب.

Abstract:

The increasing use of modern means of communication and the Internet has resulted in the emergence of a new type of crime, which has been called several names, including electronic crime and information crime. This emerging criminal phenomenon has become a threat to the security of states, the private rights of individuals, or their right to information privacy. Investigating information crimes requires technical and technical skills of a special nature, which must be enjoyed by members of the judicial police.

The subject of the study is consistent with recent developments in the field of informatics, where the spread of computers has led to its misuse and to the presence of types of illegal behavior and the emergence of crimes of a special kind. Cybercrime differs from

* المؤلف المرسل

traditional crimes, as this difference has created new and unusual challenges for the investigation and investigation authorities and the judiciary to combat this criminal phenomenon.

Keywords: *:* Crime electronic, investigation, technical skills, information, computer.

مقدمة:

اقتحمت المعلوماتية الحياة اليومية للأفراد بشكل سريع ورهيب لاسيما وأنّ المجتمع لم يواكب هذا التطور التكنولوجي منذ نشأته، حيث أصبح الحاسوب وجميع وسائل التواصل الاجتماعي أمراً ضرورياً في حياة المجتمع فالأمر لم يعد يقتصر على مختلف شرائح المجتمع بل تعدى إلى السياسة العامة لحكومات الدول، من خلال السعي إلى رقمنة مختلف أجهزة الدولة، مثل الجانب الإداري، المالي والمصرفي[1].

ولقد أدّى هذا الاستخدام المتزايد لهاته التكنولوجيا إلى ظهور أنواع جديدة من الجرائم تختلف عن الجرائم التقليدية في أطرافها، ومكانها، وموضوعها وأساليب ارتكابها، فالطبيعة الخاصّة لهذا النوع من الجرائم المستحدثة أوجد تحدّيات جديدة أمام مختلف جهات التحرّي والتحقيق والقضاء تمثلت في الافتقار التشريعي الإجرائي المنظم للجريمة الإلكترونية ومحاولة تطويع القواعد التقليدية القائمة للتطبيق على الجريمة الإلكترونية، فضلاً عن عدم وجود جهات مختصة ومدربة تقنياً للتحقيق الأوّلي المناط للضبطية القضائية في الجريمة المعلوماتية[2].

كما أنّ الجرائم المعلوماتية جريمة تفتقر إلى الأثر المادي ومسرح الجريمة فيها مسرح معنوي لا مادي وقد يكون ممتداً إلى دولة أو عدّة دول أخرى، ممّا قد ينشأ صعوبات تواجه سلطة التحقيق عند التنقيب عن الدليل الإلكتروني[3].

يعتبر موضوع البحث من الموضوعات الجديدة والمهمة في إطار القسم الاجرائي من القانون الجزائي، وهو من الموضوعات التي لا تزال بكرا ولم تنل حظها من البحث والتمحيص على مستوى الفقه الجنائي، إذ أن أغلب الدراسات المنشورة في مجال الجريمة المعلوماتية، اقتصرت على الجانب

[1] ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، الجزائر، 2018، ص.09.

[2] محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي- دراسة مقارنة-، دار الجامعة الجديدة، مصر، 2018، ص.09.

[3] فالدليل الإلكتروني دليل سهل تغييره وتعديله والعيش به دون أن يترك ذلك أثرا في أغلب أحواله، فضلاً عن ضرورة مراعاة الحق في الخصوصية المعلوماتية أثناء التنقيب لتقديمه كدليل يحوز حجيّة إثباتية أمام القضاء الجنائي، راجع في هذا الصدد: محمد كمال شاهين، المرجع السابق، ص.09.

الموضوعي القائم على سرد المعلومات دون محاولة الغوص في مسألة الاجراءات المتبعة من طرف اجهزة التحقيق والصعوبات التي تواجهها في ظل هذا النوع من الجرائم.

تهدف الدراسة إلى تحديد مفهوم هذه الجرائم وأنماطها وخصائصها، وبيان الأصول الإجرائية والعملية لإجراءات الاستدلال في البيئة الرقمية، كما تسلط الضوء على التحديات التي تواجهها اجهزة التحقيق الجنائي في التعامل مع هذا النمط المستجد من الجرائم، ذلك أن جدة وحداثة الجرائم المعلوماتية وما تتسم به من خصائص سيؤرق كاهل المحقق في فك خيوط هذه الجريمة الغامضة. وبالتالي يمكن طرح الإشكالية الآتية: ما مردّ الصعوبات والعوائق التي تواجه جهات الاستدلال والتحقيق في سبيل إثبات الجرم الإلكتروني؟

وللإجابة على هذه الإشكالية، تم الاعتماد على مجموعة من المناهج المستعملة في الدراسة، حيث اعتمد المنهج الوصفي في تحديد ظاهرة الجريمة المعلوماتية وابراز بعض المفاهيم التي تقوم عليها، وكذلك وصف الاليات الخاصة في الاجراءات المستعملة في استخلاص الدليل والعوائق المستجدّة.

كا تم الاعتماد على المنهج التحليلي بخصوص بعض المفاهيم والغوص في جزئياتها وطرحها بشكل من التفصيل والتشريح نظرا لأهميتها في الدراسة، أما المنهج المقارن فقد استعمل كلما اتيحت فرصة استخدامه خاصة حينما تم التطرق لأجهزة التحقيق الجنائي لدى بعض التشريعات المقارنة.

أما بخصوص تقسيم الدراسة، فقد اعتمد التقسيم الثنائي الى مبحثين.

المبحث الأول: الإطار المفاهيمي للبحث والتحقيق في الجريمة المعلوماتية

قبل التطرق إلى عقبات التحقيق الجنائي التي تواجهها جهات الضبطية القضائية وجهات التحقيق حول الجريمة الإلكترونية، يجدر بنا أن نعرّف بهذه الجريمة المستحدثة.

المطلب الأول: تعريف الجرائم المعلوماتية

لقد قدم الفقهاء عدداً ليس بالقليل من التعريفات، لكنها تتمايز وتختلف تبعاً لموضوع الدراسة القانونية ذاته، فمن هذه التعريفات ما هو مبني ومرتكز حول وسيلة ارتكاب الجريمة، ومنها ما هو مرتكز حول موضوع الجريمة[1].

[1] بن مكي نجاة ، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية للنشر والتوزيع، الجزائر، 2017، ، ص.09.

بخصوص التعريف المرتكز حول وسيلة ارتكاب الجريمة، نجد أنّ نماذجها عديدة ومتنوّعة في تصوّرها لدى الحاسب الآلي في ارتكاب الجريمة، حيث يعرّفها الأستاذ الألماني TIED MEN بأنها: «كافة أشكال السلوك المشروع أو الضار بالمجتمع المرتكب باستخدام الحاسب الآلي»[1]، كما يعرّفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية: «الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً»[2].

أمّا التعريف المرتكز حول موضوع الجريمة فهو يختلف عن التعاريف السابقة حيث أنّه يركّز على الجريمة التي تقع على الحاسب أو داخل نظامه، وفي هذا الصدد، ومن نماذج مسايرة هذا المنطق ما عبّر عنه الفقيه ROSENBLAIT بأنّها: «كلّ نشاط غير مشروع موجه إلى نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزّنة داخل الحاسب الآلي أو التي تحول عن طريقه».

ولقد اتفقت أغلب التشريعات على تبني التعريف الذي أقرّه المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته، حيث عرّف الجريمة المعلوماتية بأنّها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[3].

المطلب الثاني: سلطات الاستدلال والتحقيق في العالم الافتراضي

في إطار بيان مدى ملائمته القواعد الإجرائية التقليدية في مرحلة جمع الاستدلالات واجراء التحقيقات للتطبيق على الجريمة الإلكترونية، كان من الضروري تحديد الهيئات المؤهلة للقيام بإجراءات التحرّي والتحقيق وذلك للمحافظة على الخصوصية المعلوماتية للأفراد، فمسألة تحديد اختصاص هيئة للقيام بعملية التحرّي والاستدلال في الجرائم المعلوماتية تعدّ من المسائل التي أحدثت أقوى المواجهات بين

[1] KLAUS TIED MEN, Fraude et autre, Délits d'affaires commis à l'aide d'ordinateurs électroniques, Rev. Dr. Pen. crim, N 03, 1984, p.612.

[2] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، مصر، 2007، ص.38.

[3] وعلى وجه العموم، فإنّ الجرائم الإلكترونية قد تكون سرقة أو غسيل أموال وتحويلها من حساب إلى آخر، وقد تستهدف تدمير المعلومات أو الاحتيال أو تزوير البطاقات الشخصية أو بطاقات الائتمان أو باستخدام البريد الإلكتروني، نقلاً عن: زبيحة زيدان، الجريمة المعلوماتية في ظل التشريع الجزائري، دار الهدى، الجزائر، 2011، ص. ص.43-44.

التقليد والتجديد في أطر الإجراءات الجنائية، خاصّة بين تلك القواعد المتعلقة بسلطات التحقيق في العالم الإلكتروني وبين سلطات التحقيق في العالم المادي[1].

وعلى الرّغم من وجود تشابه كبير بين التحقيق في الجرائم المعلوماتية وبين التحقيق في الجرائم الأخرى من حيث الإجراءات، إلاّ أنّها تتفرق في عديد من النقط التقنية، وهو ما يستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بما يتلاءم وهذه الخصوصية[2].

إنّ السلطة المختصة بالتفتيش هي النيابة العامة ومن يساعدها من رجال الضبطية القضائية، كما أنّ التفتيش عن الأدّلة في جرائم المعلوماتية يتطلب مهارات فنية معيّنة في المحقق يجب أن يمتاز بها حتى يتمكّن من العمل بسرعة من أجل المحافظة على الأدّلة من الإتلاف أو الشطب أو التعديل[3].

أولا- السلطة المختصة بالتحقيق الابتدائي في الجزائر:

جدير بالذكر أنّ المشرّع الجزائري قد أسند سلطة التحقيق الابتدائي ووفقاً لقواعد الاختصاص المحلي للنيابة العامة وفقاً للمادة 37 من قانون الإجراءات الجزائية[4].

يتّضح من خلال فحوى النص السابق أنّ النيابة العامة في التشريع الجزائري تعدّ هي صاحبة الاختصاص الأصيل بالتحقيق الابتدائي، أمّا بالنسبة لقاضي التحقيق، وفيما يخص الاختصاص المحلي، فقد نظمته المادة 40 من ق.إ.ج.ج والتي أخذت بالمعايير المنصوص عليها في المادة 37 من ق.إ.ج.ج، وطبقاً لنص المادة 67 فإنّه لا يجوز لقاضي التحقيق أن يجري تحقيقاً إلاّ بموجب طلب من وكيل الجمهورية.

لكن لما كانت جريمة المساس بأنظمة المعالجة الآلية للمعطيات جريمة قد ترتكب في مكان معين وتكون آثارها في مكان آخر، فإنّ المشرّع الجزائري بموجب المادة 37 فقرة 2 من ق.إ.ج.ج أجاز

[1] تلك المواجهة أدّت إلى ظهور مصطلح جديد هو «CYber Investigation» والذي يعني تحديد سلطات مختصة بالتحقيق في العالم الافتراضي، وهو ما نادى له مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين المنعقد في هافانا في الفترة الممتدة من 28 أوت إلى 8 سبتمبر 1990، نقلا عن: محمد كمال شاهين، المرجع السابق، ص.175.

[2] ناني لحسن، المرجع السابق، ص.52.

[3] خالد عياد الحلبي، إجراءات التحرّي والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان- الأردن، ط1، 2011، ص. ص.155-156.

[4] تنص المادة 37 من ق.إ.ج.ج على ما يلي: «يتحدّد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشبوهين...».

تمديد الاختصاص المحلي لكلّ من وكيل الجمهورية وكذا قاضي التحقيق بالقطب الجزائي المتخصص إلى دائرة الاختصاص محاكم لأخرى المحدّدة في التنظيم[1].

ثانيا- السلطة المختصة بالتحقيق الابتدائي لدى بعض التشريعات المقارنة:

وفقاً لنص المادة 199 من قانون الإجراءات الجنائية المصري يكون الاختصاص فيما عدا الجرائم التي يختص بها قاضي التحقيق بتحقيقها من صلاحيات النيابة العامة وأنّ جانب سلطة التحقيق المختصة الممثلة في النيابة العامة، توجد سلطات أخرى إمّا أن تكون منتدبة ممثلة في قاضي التحقيق أو أحد مأموري الضبط القضائي، أو سلطات تكميلية تختص بإجراء أو أكثر من إجراءات التحقيق تتمثل في القاضي الجزئي[2] أو محكمة الجنح المستأنفة.

أمّا المشرّع الفرنسي فقد أسند سلطة التحقيق الابتدائي بصفة عامة إلى قاضي التحقيق طبقاً لنص المادة 81 من ق.إ.ج.ف وقصر وظيفة الاتهام على النيابة العامة كما جعل مرحلة التحقيق على درجتين[3].

كما عرّف التشريع الفرنسي جهات تحقيق خاصّة مثل قاضي الأطفال، أمّا في إطار التحقيق في الجرائم الإلكترونية فقد حرص المشرّع الفرنسي على ضرورة إنشاء جهات تحقيق خاصّة بالجريمة الإلكترونية وهو ما تضمنه قانون العقوبات الفرنسي الجديد في المواد 8 و113 على ضرورة القيام بتحقيق خاص في جرائم التقليد الرقمي وذلك بشكوى تقدم لوزير العدل[4].

بعد التطرق للإطار المفاهيمي المتعلق بالجريمة الإلكترونية وكذلك من هم السلطات المؤهلة للقيام بعملية الاستدلال والتحقيق في الجرائم الإلكترونية، نلج من خلال المحور الموالي للحديث عن عقبات التحقيق الجنائي والتي مردّها عوامل عديدة ومختلفة.

---

[1] المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/10 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

[2] ويقصد بالقاضي الجزئي في هذا الصدد قاضي المحكمة الجزئية التي تتبعه النيابة المختصة وفقاً لقواعد الاختصاص العامة وفقا للمادة 218 من ق.إ.ج. المصري والتي تنص على: «يتعيّن الاختصاص بالمكان الذي وقعت فيه الجريمة أو الذي يقيم فيه المتهم أو الذي يقبض عليه».

[3] الدرجة الأولى: من مراحل التحقيق الابتدائي ويختص لها قاضي التحقيق وتمثل أوّل درجة تحقيق والدرجة الثانية هي غرفة التحقيق والتي تمثل جهة التحقيق من الدرجة الثانية. محمد كمال شاهين، المرجع السابق، ص.189.

[4] حيث يجب أن يتضمن تفصيلاً شكلياً للعدوان على حقوق الشاكي ويكون ذلك في شكل ورقة رسمية من قبل البلد التي وقعت فيه جريمة التقليد الرقمي متضمنة وقائع الجريمة. راجع في هذا الصدد:
Merle (R) et Vitu (A), Traite de droit criminel, Tom ''M'', 2ème édition, Cujas, Paris, 1973, p.208.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2022 المجلد: السادس العدد: الاول ص.ص: 1734-1752.

المبحث الثاني: العوامل المؤثرة على الجرائم الإلكترونية كعائق أمام إجراءات البحث والتحرّي

هناك الكثير من المشاكل والمعوقات التي تؤثر على عملية التحقيق تؤدي بها للخروج بنتائج تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها.

ويعتبر الطابع غير الوطني أهمّ السمات التي تميز الجريمة الإلكترونية عن غيرها من الجرائم الكلاسيكية، فهذه الجرائم المستحدثة لا تعترف بالحدود الجغرافية لارتباطها بالشبكة المعلوماتية حيث لا وجود لحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة. فالطابع العابر للحدود التي تتميز به الجريمة الإلكترونية يثير إشكالات عدّة تشكل عقبات فعلية خاصّة مسألة تنازع الاختصاص بين الدول في مسألة التحقيق والتحرّي وكذلك إشكالية احترام سيادة الدولة، والتي تقف عائقاً أمام هيئات الاستدلال عندما يتطلب الأمر البحث والتنقيب عن أدّلة إثبات الجريمة.

المطلب الأول: تنازع الاختصاص بالتحقيق في الجرائم المعلوماتية

تعتبر مسألة تنازع الاختصاص أكبر التحدّيات التي تواجهها عملية التحقيق في الجرائم الإلكترونية، إذ أنّ ما تتميّز به هذه الجرائم من طابعها المتخطى لحدود الدولة الواحدة واتسامها بالبعد الدولي، بالإضافة إلى تجرّد السلوك الإجرامي فيها من الطابع المادي لارتباطه بالعالم الافتراضي والرقمي يجعلها ترتبط بأكثر من ولاية قضائية ويجتمع فيها أكثر من معيار واحد من معايير إسناد الاختصاص، ممّا يؤدي إلى تنازع إيجابي بين عدّة جهات قضائية[1].

فوفقاً لمبدأ الإقليمية ينعقد الاختصاص للقضاء الوطني كما في حالة نشر الصور الإباحية أو العبارات التي تخص على الكراهية العنصرية المنتشرة على شبكة الإنترنت بصرف النظر عن الدولة التي صدر منها هذا العمل الإجرامي طالما يمكن أن تتحقق النتيجة الإجرامية على الإقليم الوطني، كما يختص القضاء الوطني وسلطة التحقيق وفقاً لمبدأ إقليمية النص الجنائي بالجرائم الإلكترونية المرتكبة على السفن والطائرات الوطنية بصرف النظر عن جنسية مرتكب الجريمة أو المجني عليه فيها[2].

وكما تمّ التطرّق إليه آنفاً، أنّ الجرائم المتصلة بتكنولوجيا المعلوماتية يتجاوز مداها أحيانا حدود الدولة، حينما يتجزأ ركنها المادي أو يتوزع على أكثر من مكان، بحيث يمكن وقوع السلوك في مكان في

[1] CHAWKI Mohammed, Combattre le cyber criminalité, Edition de Saint Amans, Paris, 2008, p.318.
[2] محمد كمال شاهين، المرجع السابق، ص.190.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2022 المجلد: السادس العدد: الاول ص.ص: 1734-1752.

حين أنّ النتيجة المنتظرة تتحقق في دولة أخرى، وهذا يطرح إشكالاً يتمحور حول: هل مكان وقوع الجريمة هو مكان وقوع السلوك الإجرامي أم المكان التي تحققت فيه النتيجة؟.

في هذا الصدد انقسمت الآراء الفقهية إلى ثلاثة اتجاهات، حيث اعتبر الاتجاه الأوّل أنّ العدو في تحديد مكان وقوع الفعل الضار بالمكان الذي وقع فيه السلوك، في المقابل تبنى اتجاه آخر عكس هذه الفرضية، في حين اعتبر اتجاه توفيقي على أنّ الفعل تنازعه ثلاث قوانين؛ قانون دولة الإقليم على أساس مبدأ الإقليمية، قانون دولة الجاني وقانون دولة وقوع الجريمة[1].

فإذا أخذنا أحد نماذج التشريعات المقارنة، فالتشريع الأمريكي يمتد تطبيقه إلى الأفعال المرتكبة في الخارج طالما أنّ آثارها داخل إقليم دولتها[2].

في حين أنّ القضاء الإنجليزي تبنى حلولاً مشابهة فهو يختص بالنظر في الدعاوى الناشئة عن سوء استخدام المواقع الإلكترونية متى كان هناك علاقة بين الفعل المجرّم ودولة بريطانيا[3]. أمّا في فرنسا فيمتد اختصاص القضاء هناك إلى جرائم الإنترنت التي وقعت في الخارج عملاً بقانون العقوبات الجديد متى كانت الظروف الواقعة تبرّر مصلحة فرنسا في أعمال قانونها عليها[4].

ونظراً لتفاقم مسألة تنازع الاختصاص باعتبارها أحد العوامل التي أدّت إلى وجود صعوبة فعلية أمام التصدّي لهذا النوع من الجرائم، تدخل الفقه الجنائي وقدّم حلاً لهذه المشكلة والمتمثلة في إعطاء أولوية النظر في الجريمة الإلكترونية للدولة التي تتوفر على أحد معايير تحديد الاختصاص الذي يكون الأكثر فعّالية لملاحقة المجرمين[5].

---

[1] ناني لحسن، المرجع السابق، ص.59.

[2] حيث تكرّس هذا الاتجاه في العمل القضائي حيث انتهت إليه الدائرة الاستئنافية في قضية قمار ومراهنات عبر الإنترنت، وقد اعتبر القضاء المذكور مجرد وضع برمجية فك التشفير (PGP) على الإنترنت بمثابة تصدير لها وهو ما يخوّل المحاكم الأمريكية للتصدّي لها باعتبارها صاحبة اختصاص بصرف النظر عن مكان وضع البرمجية، راجع في هذا الصدد: عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، ط1، 2004، ص.910.

[3] وذلك عملاً بقانون إساءة استخدام الحاسوب الصادر سنة 1990 (The computer Misuse ACT) فيكفي أن يكون ناتج السلوك الإجرامي تعديلاً محظور في حاسوب موجود في بريطانيا، نقلا عن: عمر محمد بن يونس، المرجع السابق، ص.912.

[4] VERGUCHT Pascal, La répression des délits informatiques dans une perspective internationale, Thèse de doctorat soutenue à l'université de Montpelier, Avril 1996, p.p.347-348.

[5] Conseil de l'Europe, La criminalité informatique, recommandation n° R (89) sur la criminalité en relation avec l'ordinateur, 1990, p.p.94-96.

أمّا بخصوص المشرّع الجزائري، فقد اكتفى في هذا الشأن بالفقرة الثانية من نص المادة 15 من القانون 09-04[1] والتي تنص: «تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبي، وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني».

لكن هل يعدّ هذا الإجراء لوحده كافياً للوقوف والتصدّي أمام الكمّ الهائل لِما يسمى بالإغراق المعلوماتي بكلّ ما فيه من سلبيات تهدّد الهوية الوطنية، النظام العام، والآداب العامة.

هنا تعتبر مبادرة المشرّع الجزائري لا ترقى للمستوى المطلوب لمواجهة هذا النوع من الجرائم، حيث يظهر أنّ المشرّع أعاد صياغة نص المادة 588 من ق.إ.ج.ج والتي نصت على مبدأ الاختصاص العيني، ولم يأتي بأيّة إضافة جديدة إلى قواعد الاختصاص.

المطلب الثاني: إشكالية التفتيش العابر للحدود وانعكاسه على مبدأ السيادة

من المشاكل التي تواجه جهات التحقيق في جمع الأدّلة، حالة تطلب امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر عن جهاتها المختصة الإذن بالتفتيش ودخوله في المجال الجغرافي لدولة أخرى، وهو ما يسمى بالتفتيش العابر للحدود، وقد يتعذر القيام به بسبب تمسك كلّ دولة بسيادتها وحدودها الإقليمية.

ونظراً لكون الجريمة الإلكترونية ترتكب عبر شبكة الإنترنت وكونها جريمة متعدية الحدود، فإنّ الاختصاص القضائي بها يكون في الكثير منها منعقداً لأكثر من دولة، كما في جرائم العدوان الفيروسي والاحتيال المعلوماتي وانتهاك حقوق النسخ، ومن ثمّ تنشأ مشكلة تنازع الاختصاص القضائي نظراً لتطبيق مبدأ الإقليمية والتي يعبّر عن سيادة كلّ دولة وقعت الجريمة كلّها أو جزء منها على إقليمها أو كان أحد أطرافها من رعاياها[2].

وعليه، فقد انتهت الاتفاقية الأوروبية للجريمة الإلكترونية سنة 2001 وذلك في محاولة منها للحدّ من مشكلة تنازع الاختصاص واحترام مبدأ سيادة الدول، على أن يقوم الأطراف المعنيون متى كان

[1] قانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، رقم 47، 2009، ص.05.

[2] شمسان ناجي صالح الخيلي، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت-دراسة مقارنة-، دار النهضة العربية، القاهرة، 2009، ص.68.

ذلك ملائماً بالتشاور من أجل تحديد الاختصاص القضائي وذلك في حالة مطالبة أكثر من طرف من الأطراف بالاختصاص القضائي بشأن أحد الجرائم الإلكترونية[1].

وعلى الرّغم من أهمية الحلول الأنفة ذكرها، وذلك كسبيل لحل مسألة تنازع الاختصاص بين سيادات الدول في إطار التفتيش الإلكتروني، إلاّ أنّه يُؤخذ عليه أنّه ترك مسألة التشاور فيما بين الدول اختيارية وتخضع لمبدأ الملائمة، أي حسب ما تقتضيه ظروف كلّ دولة، وهو ما يبقى معه حالة التنازع قائمة إذا ما رفضت إحدى الدول التشاور، فضلاً عن أنّ الوزن السياسي للدولة والتي تأبى المحادثات والمشاورات له دور فعّال في تحديد الاختصاص الجنائي.

وفي ظلّ تلك الإشكاليات تبقى مشكلة اختيار الاختصاص لسلطة التحقيق المختصة بالتحقيق الابتدائي بالجريمة الإلكترونية أمراً قائماً، فهل يبقى الاختصاص منعقداً طبقاً للقواعد العامة والذي يعبر عن سيادة الدولة على أرضها أم أنّ الأمر يتطلب البحث عن معالجة قانونية جديدة ضدّ تنازع الاختصاص القضائي.

وعملاً بالقوانين السالفة الذكر، امتنع المشرّع الجزائري بدوره عن التفتيش عن بعد لأنظمة الحاسوب المتواجدة خارج القطر الوطني باستثناء الاتفاقيات الدولية ذات الصلة وذلك في إطار المساعدة المتبادلة مع السلطات المختصة الأجنبية وفي إطار المعاملة بالمثل[2].

بناءً على المعطيات السابقة، فإنّ إشكالية التفتيش الإلكتروني وعلاقته بسيادة الدول تعدّ إشكالية عويصة يصعب حلّها، حيث نجد أنّ معظم التشريعات حظرت استعمال هذه الآلية بحجة تصادم هذا الإجراء مع مبدأ السيادة.

المطلب الثالث: معوّقات مصدرها مدى ملائمة إجراءات التحقيق الابتدائي لمبدأ الشرعية في ظلّ غياب نص تشريعي

إنّ عدم وجود أيّ نصوص تجريمية ضدّ مجرمي جرائم الحاسوب والإنترنت يؤدي إلى تفاقم هذا النوع من الجرائم، حيث تصل إلى مرحلة تصبح فيها عملية التغلب على هذه الظاهرة أصعب ممّا يتوقع خصوصاً وأنّ جميع المعاملات والإجراءات ستكون إلكترونية.

[1] شمسان ناجي صالح الخيلي، المرجع السابق، ص.71.

[2] وهو الموقف الذي عبّر عنه من خلال نص المادة 5 فقرة 2 مكن القانون 04/09 على النحو التالي: «إذا تبيّن مسبقا بأنّ المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى مخزنة في منظمة معلوماتية تقع خارج الإقليم الوطني، فالحصول عليها يكون بمساعدة السلطات الأجنبية وفقاً لمبدأ المعاملة بالمثل».

حيث أنّ القضاء لا يعتمد على الأدلة والقوانين التي تعدّها هيئات التحقيق عند التفتيش والضبط والتحقيق مع مرتكبي الجرائم الإلكترونية وذلك ناتج عن غياب القوانين والعقوبات التي توضح السلوك الإجرامي غير المشروع.

فالمحقق الجنائي يجد نفسه غير قادر في مواجهة هذا النوع من الجرم المستجدّ ودون وجود تنظيم تشريعي يستند إليه فيساءل إلى أيّ مدى تكون الإجراءات، التي باشرتها تنطبق ومبدأ المشروعية حتى لا يهدر وقته وجهده في مباشرة إجراءات باطلة مسبقاً لعدم وجود نص تشريعي يحكمها[1].

بين هذا وذاك أدّى إلى وجود العديد من المعوّقات والصعوبات التي تقف حائلاً دون تطبيق النصوص الموجودة في القانون الجنائي سواءً أكان الموضوعي أو الإجرائي[2].

أولا- عدم مواكبة النصوص الجزائية الكلاسيكية للجرائم الإلكترونية:

نظراً لِما تتمتع به الجريمة الإلكترونية من طبيعة خاصة تميّزها عن غيرها من الجرائم التقليدية ونحن أمام ظاهرة إجرامية يتبع في ارتكابها استخدام أحدث الوسائل والتكنولوجيا، هذه الطبيعة الخاصيّة جعلت النصوص الجنائية القائمة عاجزة عن التطبيق على الجريمة الإلكترونية، ضف إلى ذلك أنّ النصوص التقليدية قد وضعت لتطبّق وفق معايير معينة ومنذ زمن بعيد، في حين أنّ محل الجريمة الإلكترونية هي معطيات ذات طبيعة معنوية[3]، كما أنّ هناك العديد من الأفعال الجديدة خاصّة في الدول المتخلفة مرتبطة باستعمال الإنترنت غير مجرّمة وفقاً للقواعد العقابية التقليدية ولا تمتد إليها لمجابهتها رغم تهديدها للمصالح العامة.

فالدخول مثلاً في نظام حاسب مملوك للغير وسرقة المعلومات منه لا يعدّ جريمة بمفهوم القوانين التقليدية أنّ السرقة لا ترد الأعلى على المال المنقول، وهذه الصفة لم تثبت بعد للمعلومات كونها تعتبر سوى أفكار معنوية بحتة، زيادة على ذلك فغنّ جريمة السرقة بالمفهوم التقليدي يعني أخذ مال الغير

[1] أمام هذه المشكلة فقد كان الحل متمثلاً في محاولة تطويع النصوص الجنائية القائمة، وذلك بالتوسع في تفسيرها لتطبق على الجريمة الإلكترونية، نقلاً عن: خالد عياد الحلبي، المرجع السابق، ص.220.

[2] فالملاحظ أنّ الأسباب المحاطة بالجريمة المعلوماتية لا تشكل جزءً منها، فهي أسباب لا دخل للجريمة المعلوماتية فيها، إذ ما كان على المشرّع الجنائي إلاّ مواكبة ما استجدّ على أرض الواقع من أفعال وانتهاكات تلحق الإضرار بأفراد المجتمع، بإصدارة التشريع الخاص بهذا الغرض، راجع في هذا الموضوع: علي بن هادي البشري، الجهود القانونية للحد من جرائم الحاسب الآلي، مكتبة فهد الوطنية، الرياض، 2005، ص54.

[3] أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق، ط4، 2006، ص.31.

بدون وجه حق في حين أنّ اختلاس المعلومات يتمثل في أخذ نسخة منها مع الإبقاء بأصلها عند صاحبها، لذا فإنّها لا يحميها التجريم المقرّر في جرائم الأموال[1].

ولقد حاولت العديد من الدول المتقدمة ونظراً للعجز الكبير الذي أثبتته القوانين القديمة استدراك الوضع بسن تشريعات جديدة تتجاوب مع الطبيعة الخاصة لهذه الجرائم الحديثة، فمنها من اختارت آلية تعديل القوانين وإضافة نصوص جديدة ومنها من فضلت إلغاء النصوص القديمة واستحداث نصوص جديدة.

ثانيا- عدم مواكبة جهات التحقيق للتطور السريع للجرم المعلوماتي:

هناك معوّقات للتحقيق في جرائم الحاسوب والإنترنت تتعلق بالسلطات القائمة بالتحقيق وقد ترجع لعدّة أسباب ونذكر منها: قلة خبرة القائمين بالتحقيق، حيث أنّ هذه الجرائم تقع على التقنية التكنولوجية وهذه التقنية دائمة التطوّر وبشكل سريع، ومن هنا يتوجب على المحقق أن يكون على دراية تامة ومواكباً للتطور فيما يتعلق بالحاسوب والمعلوماتية[2]، كما أنّ صعوبة معاينة الجرائم الإلكترونية من طرف المحققين تصعب عليهم مسألة القبض على الجناة، حيث لا تتمتع المعاينة في مجال كشف غموض وملابسات الجرائم الإلكترونية وإثباتها بالدرجة نفسها من الأهمية التي تتمتع بها في مجال الجرائم التقليدية[3].

كما أنّه من الممكن أن يتردّد عدد كبير من الأشخاص على مكان أو مسرح الجريمة خلال الفترة الزمنية الممتدّة منذ لحظة وقوع الجريمة حتى اكتشافها والتي تكون في الغالب طويلة المدة ممّا قد يُتيح الفرصة لإحداث تلف أو عبث بالمخلفات المادية أو إنهاء بعضها. وهو ما يلقي نوع من عدم اليقين على الدليل المتحصل عليه من خلال المعاينة، ناهيك عن إمكانية تلاعب الجاني في البيانات أو المعطيات محل المعاينة عن بُعد أو محوها عقب الدخول إليها عبر الإنترنت بواسطة جهاز آخر مرتبط بها.

---

[1] غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات في الفترة الممتدة من 01 إلى 03 ماي 2003، ص.325.

[2] ولكن هذا الأمر يتحقق دائما، وعليه فهناك صعوبات في هذا المجال كعدم التدريب، حيث اهتمت أجهزة الأمن في و.م.أ استحدثت وحدة متخصصة للمكافحة والتحقيق في هذه الجرائم من ضمن مكتب التحقيقات الفيدرالي حيث يكون تدريب هذه الوحدات مستمراً ليُواكب تطور جرائم الحاسوب والإنترنت، نقلا عن: خالد عياد الحلبي، المرجع السابق، ص.225.

[3] وذلك راجع إلى عدّة أسباب أوّلها أنّ هذه الأخيرة لها مسرح تجري عليه الوقائع والأحداث وتخلف آثاراً مادية تقوم عليها كالبصمات وقطرات الدم، راجع في هذا الصدد، غنام محمد غنام، المرجع السابق، ص.635.

إضافةً إلى أنّ التحقيق في هذه الجرائم يحتاج إلى تكوين هؤلاء المحققين الأمر الذي يتطلب تكاليف باهظة وكذلك التفتيش عن الأدّلة يحتاج إلى فحص آلاف الصفحات خصوصاً عندما لا تثبت تلك الصفحات شيئاً[1].

المطلب الرابع: الصعوبات المتعلقة بالشق الميداني للتحرّي وجمع الاستدلالات في الجرائم المعلوماتية

نتيجة لمختلف الصعاب التي تواجهها الضبطية القضائية في أعمال التحرّي وجمع الاستدلال نتيجة للطبيعة الخاصّة للجريمة الإلكترونية، فلقد بادرت مختلف الدول إلى إنشاء وحدات متخصصة في مجال البحث والتحرّي وأجل الأجهزة الحكومية. ففي فرنسا مثلاً قامت بإنشاء عدّة وحدات متخصصين وغير متخصصين ضمن جهازي الشرطة والدرك لمكافحة هذا الإجرام كالمكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات والذي من بين مهامه تقديم المساعدة التقنية لجهات التحقيق وتنسيق الأعمال التحضيرية اللازمة على المستوى الوطني، إضافةً إلى قسم الإنترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية المعروف اختصاراً (STRTD) والقسم الإلكتروني التابع لمعهد البحوث الجزائية للدرك الوطني المعروف بـ(IRCGN) وكذا وحدات أقسام الاستعلامات والتحقيقات المعروف بـ (BDRIJ)[2].

أولا- المعوّقات المتعلقة بإجراءات الحصول على الدليل:

إذا كان من السهل على جهات التحرّي أن تتحرّى عن الجرائم التقليدية عن طريق المشاهدة أو التتبع أو سماع الشهود، فإنّه قد يصعب عليها ذلك بهذه الآليات بالنسبة للجرائم المعلوماتية، وهذا راجع إلى الطبيعة الرقمية التي يتكوّن منها الدليل التقني سواء من حيث كونه غير مرئي في شكل نبضات مغناطيسية أو كهربائية لا يدركها الرجل العادي بالحواس الطبيعية.

ومن الصعوبات التي تُعيق رجال الضبطية القضائية في مجال الجريمة المعلوماتية والمرتبطة بالدليل الرقمي هي سهولة محو الدليل أو تدميره في زمن قصير جدا، فارتباط الجريمة المعلوماتية بالبيئة التقنية انعكس على طبيعة الدليل المتركب عنها من حيث أنّ أمر طمسه ومحو آثاره من قِبل الفاعل يعدّ

[1] خالد عياد الحلبي، المرجع السابق، ص.228.

[2] غنام محمد غمام، مرجع سابق، ص290.

أمراً في غاية السهولة، إذ يمكن للمستخدم الذي يتحكم في المعلومات التي تعتبر موضوعاً للتنقيب الجنائي، وبالتالي تدمير كلّ الأدّلة[1].

وبالنسبة للتشريع الجزائري، فنلاحظ أنّه واكب التطوّر التكنولوجي بتمهيده للطريق أمام استخلاص الدليل الإلكتروني في القانون رقم 09-04 بالنص عليه في المادة السادسة منه وذلك بحجز المعطيات المعلوماتية وذلك بإفراغها أو نسخها في دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز.

ثانيا- معوّقات مرّدها كثرة المعلومات المطلوب التحرّي عنها:

يُشكل الكم الهائل من البيانات[2] والمعلومات المتعيّن فحصها من قِبل سلطات التحرّي والتحقيق وصولاً للدليل في الجريمة الإلكترونية صعوبة بالغة ممّا يثير تساؤلاً حول إمكانية القائمين على أعمال التحرّي فرز الملفات المذنبة من الملفات البريئة.

فالبيانات المتداولة في النظم الإلكترونية والمتميزة بكمّها الهائل تشكل إحدى العوائق البارزة التي تُعيق التحقيق في الجرائم التي تقع عليها أو بواسطتها، إذ عادةً ما يتطلب البحث عن الأدّلة في حاسب واحد، الإطلاع والفحص الدقيق لكلّ المعطيات التي تتضمنها آلاف الملفات المخزّنة في ذاكرته ويكلف المحقق وقتاً وجهداً كبيرين[3].

وفي نهاية المطاف لا يستطيع المحقق حصر هذا الكمّ الهائل من المعلومات وبالتالي لا يصل إلى الدليل الإلكتروني.

ثالثا- معوّقات مرّدها الامتناع عن التبليغ بوقوع الجريمة المعلوماتية:

من بين الأسباب الرئيسية التي تحول دون اكتشاف الجريمة، تكتم المجني عليه عنها وعدم تبليغ السلطات المختصة عن وقوعها بعد اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة منت جرّاء ذلك على عدم الكشف حتى بين موظفيها عمّا تعرّضت له، وتكتفي عادةً باتخاذ إجراءات إدارية داخلياً دون إبلاغ السلطات المختصة تجنباً للأضرار

[1] فالجاني يمكنه أن يمحوا الأدّلة التي تكون قائمة ضدّه أو تدميرها بحيث لا تتمكّن السلطات من كشف الجريمة وإذا ما علمت بها لا تستطيع إقامة الدليل ضدّه. نقلا عن: غنام محمد غنام، المرجع السابق، ص.04 وما بعدها.

[2] تعتبر قاعدة البيانات نظام فعّال يستخدم لترتيب الملفات التي تحتوي على معلومات محدّدة في بطاقات خاصة، وقاعدة بيانات واحدة يمكنها أن تشمل على عدد لا يُحصى من الملفات، ويمكن استخراج هذه البطاقات بنظام أبجدي باختيار عناصر معينة وترتيبها للاستفادة منها، نقلاً عن: علي بن هادي البشري، مرجع سابق، ص

[3] محمد كمال شاهين، المرجع السابق، ص.ص.87-88.

بسمعتها ومكانتها وهزّ الثقة في كفاءتها، ومن ثمّ تظل الجريمة الإلكترونية مستترة ما لم يتم التبليغ عنها لتصل لعلم السلطات المختصة[1].

رابعا- تعذّر تحديد عنوان المجرم الإلكتروني:

إنّ الوصول إلى الدليل الرقمي تعترضه عقبة تكمن في أنّ الجاني المتمرن يجتهد في إخفاء هويته للحيلولة دون تعقبهم أو كشف أمرهم، بحيث تظل أنشطتهم مجهولة بمنأى عن علم السلطات المعنية بمكافحة الجريمة، فاستخدام المجرم لحاسوب آخر مملوك لغيره كاستخدام حواسب مقاهي الإنترنت التي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هويتهم يصعب المهام على رجال الشرطة على تحديد عنوان الجاني[2].

الخاتمة:

إنّ التطوّر الذي أبهر العالم، لم يكن بمنأى عن الأخطار المهدّدة لأمن الإنسان واستقرار المجتمعات، ذلك أنّ عالم المعلوماتية خلق إلى جانب مزاياه ظاهرة جديدة وخطيرة تسمى بالجريمة الإلكترونية، إضافةً إلى أنّ المجرم الإلكتروني الآن يوجد في عالم افتراضي لا يعرف الحدود، فهو ذكي ويتسم بقدر عالٍ من الكفاءة العلمية والتقنية ويستطيع الوُلوج إلى عمق الأنظمة الإلكترونية دون أن يكلف نفسه عناء التنقل، يُضاف إلى ذلك أنّه من الصعوبة بمكان ملاحقة هؤلاء المجرمين وضبط الأدّلة دون الحديث عمّا يطرح أمام ذلك من تحدّيات بخصوص الاختصاص القضائي والمحاكمة العادلة.

ولقد لُوحظ في هذا المجال مدى الصعوبة التي تشكل عائقاً أمام تحقيق التوازن بين إقرار الحرية في تداول المعلومات وحرية الرأي والتعبير عن طريق الإنترنت.

فالتشريع الجزائري هو الآخر حاول تذليل الصِعاب أمام جهات التحقيق الجنائي من أجل تسهيل مأمورياتهم، حيث سارع إلى تعديل قانون العقوبات حيث أفرد باباً خاصاً بالجرائم الإلكترونية، وبالموازنة مع ذلك وسّع من اختصاصات ضباط الشرطة القضائية ووكلاء الجمهورية وقضاة التحقيق بغية ملاحقة الجرائم المعلوماتية وإنشاء ما يسمى بالأقطاب الجزائية، إضافةً إلى القانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

[1] محمد كمال شاهين، المرجع نفسه، ص.85

[2] وفي هذا الإطار نجد أنّ المشرّع الفرنسي قد أوجب على جميع مزوري خدمات الاتصال للجمهور أن يحدّدوا على مواقعهم هوية ناشر مضمون الرسالة وبياناته وذلك بموجب المادة 43 من قانون 1986/09/30. أنظر في هذا الصدد، صالح أحمد البربري، دور الشرطة في مكافحة جرائم الإنترنت في إطار اتفاقية بودابست، عن الموقع الإلكتروني: www.arablaw.com (25-09-2020، 15:15)

والذي جاء بتقنيات جديدة تُوضح القواعد الإجرائية في مجال تحريك الدعوى العمومية وتقضي آثار مجرمي، من خلال مراقبة الاتصالات ورصدها وكيفية تفتيش المنظومة المعلوماتية.

على ضوء الاشكاليات التي أظهرتها الدراسة يمكن استخلاص جملة من النتائج والتي يمكن ايجازها فيما يلي:

– إن مفهوم الجرائم المعلوماتية ينصرف الى الافعال التي تشكل اعتداءا على نظم المعالجة الآلية للمعطيات والتي تستهدف بشكل خاص المعلومات المختلفة في البيئة الرقمية.

– إن الطبيعة الخاصة للجريمة المعلوماتية دعت المشرع الى إعادة تقييم بعض القواعد الاجرائية المتاحة في استخلاص الدليل كالتفتيش والضبط وجعلها صالحة للاستعمال في مجال البيئة الرقمية وهو ما تجسد بموجب القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، فضلا عن استحداث نوع من القواعد الاجرائية الاخرى والتي تتلاءم مع الطبيعة الرقمية التي يكون عليها الدليل المناسب في اثبات هذا النوع من الجرائم كالمراقبة التقنية.

– كما أظهر البحث ان عملية الاستدلال والتحري سواء بالطرق الاجرائية التقليدية او المستحدثة ليس من السهولة بما كان، إذ تعترضها في غالب الاحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الرقمي أو بالعامل البشري.

وبخصوص الاقتراحات والتوصيات التي يمكن أن تتجسد من خلال هذا الطرح، تقتضي مواجهة هذه الظاهرة المستحدثة والمعقدة من الاجرام تحقيق أمور عدة منها:

- إن الجزائر وهي تخطوا الخطوات الاولى في تطبيق مشروع الحوكمة الالكترونية، والذي من خلاله يتم السعي الى استخدام تقنية المعلومات والاتصالات الالكترونية في توفير وتقديم معلومات وخدمات الحكومة للمواطنين وجعلها متاحة للجمهور، فهذا المشروع لابد ان يستتبعه خطوة تشريعية هامة يكون الهدف منها توفير الحماية القانونية الشاملة لهذا المفهوم بصورة منسجمة ومتزامنة مع هذا التحوّل من اجل تخطي الثغرات القانونية التي قد يستفيد منها العابثون بأمن المعلومات.
- الاسراع بالانضمام الى الاتفاقيات الدولية الخاصة بمكافحة جرائم المعلوماتية، حتى لا تستفحل هذه الظاهرة، خاصة أن القانون الوطني لا يشمل كل صور هذا الاجرام ونذكر بعض هذه الاتفاقيات على سبيل المثال، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنعقدة بالقاهرة

بتاريخ 21 ديسمبر 2010، كذلك اتفاقية بودابيست(الاتفاقية الاوروبية المتعلقة بالجرائم المعلوماتية) بتاريخ 8 نوفمبر 2001.

- انشاء المزيد من الشرطة المتخصصة لمكافحة جرائم الحاسوب والانترنيت حيث ان الشرطة الالكترونية لا تقتصر على بعض الدول النامية.
- عقد دورات تدريبية لضباط وافراد الشرطة وأعضاء النيابة العامة لمعرفة كيفية التعامل مع هذا النوع من الجرائم.
- إطلاق حملات وطنية للتحسيس عبر وسائل الاعلام من أجل الرفع من درجة الوعي الاجتماعي حول مخاطر جرائم المعلوماتية.
- ضرورة اتخاذ التدابير اللازمة للحيلولة دون وقوع المجني عليه فريسة للاجرام المعلوماتي، اضافة الى سرعة الابلاغ عن الجريمة الالكترونية فور وقوعها او بمجرد علم المجني عليه بها.

قائمة المصادر والمراجع:

أولا– القوانين والمراسيم:

1. قانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، رقم 47، 2009، ص.05.
2. المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/10 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

ثانيا- الكتب:

1- باللغة العربية:

1. أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق، ط4، 2006.
2. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية للنشر والتوزيع، الجزائر، 2017.
3. خالد عياد الحلبي، إجراءات التحرّي والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان- الأردن، ط1، 2011.

4. زبيحة زيدان، الجريمة المعلوماتية في ظل التشريع الجزائري، دار الهدى، الجزائر، 2011.
5. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، مصر، 2007.
6. شمسان ناجي صالح الخيلي، الجرائم المستحدثة بطرق غير مشروعة لشبكة الإنترنت-دراسة مقارنة-، دار النهضة العربية، القاهرة، 2009.
7. علي بن هادي البشري، الجهود القانونية للحد من جرائم الحاسب الآلي، مكتبة ملك فهد الوطنية، الرياض، 2005.
8. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، ط1، 2004.
9. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي- دراسة مقارنة-، دار الجامعة الجديدة، مصر، 2018.
10. ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، الجزائر، 2018.

2- باللغة الأجنبية:

1. CHAWKI Mohammed, Combattre le cyber wminalité, Edition de Saint Amans, Paris, 2008.
2. Conseil de l'Europe, La criminalité informatique, recommandation n° R (89) sur la criminalité en relation avec l'ordinateur, 1990.
3. KLAUS TIED MEN, Fraude et autre, Délits d'affaires commis à l'aide d'ordinateurs électroniques, Rev. Dr. Pen. crim, N 03, 1984.
4. Merle (R) et Vitu (A), Traite de droit criminel, Tom ''M'', 2ème édition, Cujas, Paris, 1973.
5. VERGUCHT Pascal, La répression des délits informatiques dans une perspective internationale, Thèse de doctorat soutenue à l'université de Montpelier, Avril 1996.

ثالثا- المقالات:

1. غنام محمد غمام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد بكلية الشريعة والقانون بجامعة الإمارات في الفترة الممتدة من 01 إلى 03 ماي 2003، ص.325.

رابعا- المواقع الالكترونية:

صالح أحمد البربري، دور الشرطة في مكافحة جرائم الإنترنت في إطار اتفاقية بودابست، عن الموقع الإلكتروني: www.arablaw.com (25-09-2020، 15:15)