منشورات مجلة المنارة
للدراسات القانونية والإدارية

خصوصية القواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية

-دراسة مقارنة-

يوسف قجاج
باحث في العلوم الجنائية

سلسلة البحوث الجامعية العدد 14 2016

منشورات مجلة المنارة
للدراسات القانونية والإدارية

سلسلة يديرها

الدكتور رضوان العنبي

باحث في القانون العام

الإيداع القانوني 2011 PE 0113 **ردمد** 2028 – 876 X

ملف الصحافة
43/2011

المطبعة
دار السلام للطباعة والنشر والتوزيع – الرباط
شارع طونكان عمارة 23 رقم 2 ديور الجامع
الهاتف : 23 58 72 37 05 الفاكس : 32 13 72 37 05
البريد الإلكتروني : Contact@darassalam.ma
الموقع الإلكتروني : www.darassalam.ma

المراسلة
العنوان: زنقة 13 الرقم 24 حي قصر البحر 2 ق ج
البيضاء 20350
الهاتف: 0665929835
البريد الالكتروني: elanbiredouane@gmail.com

إهداء

إلى الينبوع الذي لا يمل العطاء، إلى من حاكت سعادتي بخيوط منسوجة من قلبها، إلى أمي العزيزة.

إلى من سعى وشقا لأنعم بالراحة والهناء، الذي لم يبخل بشيء من أجل دفعي إلى طريق النجاح، إلى أبي العزيز.

إلى من حبهم يجري في عروقي، ويلهج بذكرهم فؤادي وأشد بهم أزري إلى جميع إخوتي.

إلى رفيقة دربي، إلى جميع أصدقائي وزملائي، إلى جميع أساتذتي.

مقدمة

شكل استخدام التكنولوجيا حدثا هاما في تاريخ البشرية حيث ارتبطت بشكل قوي بمختلف مجالات النشاط الإنساني حتى أصبحت أمرا ضروريا يستحيل الإستغناء عنها ومقوما أساسيا من مقومات دفع عجلة التقدم بالأمم والحضارات ومقياسا لتقدمها، غير أنه في المقابل اقترنت هذه التقنية بظهور أفعال غير مشروعة أصبحت تشكل ظاهرة إجرامية من نوع خاص تختلف عن الظواهر الإجرامية العادية والكلاسيكية، إذ قلبت العديد من المفاهيم القانونية السائدة سواء على مستوى القانون الموضوعي من حيث التجريم والعقاب بفعل ازدواجية طبيعتها بين جريمة معلوماتية محضة تستهدف الأنظمة والبيانات المعلوماتية في حد ذاتها أو كجريمة عادية مرتكبة بواسطة تقنية المعلومات كآلية من أجل التواصل والتخطيط لتنفيذ المشاريع الإجرامية، أو على مستوى القانون الإجرائي بفعل تغلبها على القواعد المسطرية المقررة كأصل عام للبحث وملاحقة مرتكبي الجرائم العادية ومحاكمتهم [1]، مما يتعين القول معه بأن الإجرام المعلوماتي قد أحدث ثورة في فلسفة التجريم والعقاب والإجراءات الجنائية [2].

وإذا كان البحث في مسألة قدرة القواعد الإجرائية التقليدية في ضبط الجريمة الإلكترونية أمرا صعبا فإن الصعوبة تنطلق من إعطاء مفهوم للجريمة الإلكترونية ذاتها، لذلك يذهب معظم المهتمين إلى القول بأن الجريمة الإلكترونية باعتبارها مظهرا جديدا من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال ثلاث مظاهر، إما أن تتجسد في شكل جريمة تقليدية يتم اقترافها بوسائل إلكترونية أو معلوماتية، أو في شكل استهداف للوسائل المعلوماتية ذاتها وعلى رأسها قاعدة المعطيات والبيانات أو البرامج

[1] هشام ملاطي، خصوصية القواعد الإجرائية للجرائم المعلوماتية-محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية-، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص.101

[2] عبد الرحمان اللمتوني، الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص.48

المعلوماتية، أو أن يتم اقتراف الجرائم العادية في بيئة إلكترونية كما هو الأمر بالنسبة لجرائم الصحافة[1].

فلقد أثارت هذه الجريمة بعض التحديات القانونية والعملية أمام الأجهزة المعنية بالبحث عن الجرائم وضبطها وخصوصا عندما يتعلق الأمر بمباشرة إجراءات البحث والتحري التقليدية في بيئة افتراضية لا مكان فيها للأدلة المادية، مما أظهر مدى الحاجة إلى تطوير آليات البحث بما يتلاءم وخصوصيات هذه الجريمة، وجعل مسألة ملاءمة الإجراءات الجنائية في البحث والتحري مع خصوصية الجريمة الإلكترونية تستأثر بإهتمام المشرعين في مختلف الدول، الأمر الذي دفع مجموعة من هذه الدول لإعادة النظر في تشريعاتها المحلية إدراكا منها لعجز وقصور القواعد الإجرائية التقليدية في التعامل مع الجرائم الإلكترونية من جهة، وسعيا منها أيضا لملائمة قوانينها الوطنية مع مختلف المعايير والإتفاقيات الدولية في هذا الإطار وخصوصا اتفاقية بودابست ومختلف المبادرات السابقة لها والإتفاقيات المشتقة عنها من جهة أخرى، حيث عملت هذه الدول على وضع قواعد إجرائية حديثة تستجيب لطبيعة وخصوصية هذا النوع من الجرائم.

ففي سبيل الوقوف في وجه هذا النوع من الجرائم عمل المنتظم الدولي على وضع إستراتيجية تهدف تطوير مختلف الآليات الإجرائية بشكل يجعل المجرم يجد نفسه محاطا بسياج يحول دون إفلاته من مسؤوليته عن الجريمة التي ارتكبها، كما أكد على حتمية التعاون الدولي لتوحيد التشريعات أو على الأقل لتقليص الفوارق بينها [2]، وتعزيز مختلف آليات التعاون حتى لا يستفيد المجرمون من عجز وقصور التشريعات الداخلية من جهة، وغياب التنسيق الدولي الذي يعالج سبل التصدي لهذه الجرائم من جهة أخرى.

كما أن هذه الثورة التقنية خلقت عالما جديدا لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، حيث فقدت الحدود الجغرافية كل آثر لها في بيئة

[1] عبد الحكيم الحكماوي، الإثبات في الجريمة الالكترونية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص.145

[2] فريد منعم جبور، حماية المستهلك عبر الانترنيت ومكافحة الجرائم الإلكترونية-دراسة مقارنة،منشورات الحلبي، بيروت -لبنان، الطبعة الأولى،2010، ص. 216

إلكترونية متشعبة العلاقات، الأمر الذي خلق صعوبات وإشكالات قانونية لا تقتصر على ضبط هذه الجرائم وإثباتها فحسب، وإنما أثارت أيضا تحديات أكثر تعقيدا مرتبطة بتحديد جهة الإختصاص وبالتبعية القانون الواجب التطبيق على هذا الصنف من الجرائم[1].

على ضوء ما تقدم تتحدد إشكالية الدراسة في رصد إحدى أهم الإشكالات التي تثيرها الجريمة الإلكترونية على المستوى الإجرائي والمتمثلة في قدرة القواعد الإجرائية التقليدية في ضبط الجريمة الإلكترونية، ولذلك ارتأينا الإنطلاق من الإشكال المركزي التالي:

إلى إي حد يمكن القول بأن القواعد الإجرائية التقليدية كافية لضبط الجريمة الإلكترونية وقادرة على استيعاب مختلف إجراءات البحث المنجزة بشأنها ؟

ويتفرع عن هذا الإشكال المركزي، الإشكالين الفرعيين التاليين:

هل يمكن فعلا الإكتفاء بالقواعد الإجرائية العادية من أجل البحث عن الجريمة الإلكترونية أم أن الأمر يتطلب استحداث قواعد إجرائية خاصة، وفي انتظار ذلك هل يمكن الإستعانة بالآليات الإجرائية الواردة في الإتفاقيات الدولية ؟

وما مدى كفاية القواعد الإجرائية الواردة في قانون المسطرة الجنائية للقول بإمكانية التصدي للجريمة الإلكترونية ؟

فكل هذه الإشكاليات تلعب دورا رئيسيا في اختيار وتحديد المنهج الذي سيتم إتباعه، ومن هذا المنطلق سنعتمد في دراستنا لهذا الموضوع على المنهج التحليلي المقارن، حيث سنحاول الوقوف عند مدى إمكانية الإستعانة بالقواعد الإجرائية العادية في البحث عن الجريمة الإلكترونية وحدود الإستعانة بمختلف الآليات الإجرائية التي أرساها المنتظم الدولي وكيف سارعت الدول الرائدة في ملاءمة قوانينها الوطنية مع هذه الإجراءات مقارنين موضع قانون المسطرة الجنائية المغربي بين هذه الآليات، وقدرة

[1] نور الدين الواهلي، الإختصاص في الجريمة الإلكترونية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص. 115

القواعد الإجرائية الواردة فيه على استيعاب مختلف شكليات البحث عن الجريمة الإلكترونية.

وعليه، سيتم الإنطلاق من فرضية مفادها أن القواعد الإجرائية العادية لم تعد كافية وقادرة على ضبط الجريمة الإلكترونية وأن البحث فيها يتطلب وضع قواعد إجرائية خاصة تتماشى وتنسجم مع خصوصية وطبيعة هذا النوع من الجرائم، وأن ما أرساه المنتظم الدولي من قواعد شكلية تعتبر إطارا مرجعيا يمكن الإرتكاز عليها واللجوء إليها لتنظيم إجراءات فعالة للبحث عن الجريمة الإلكترونية.

كما أن معالجة إشكالية هذه الدراسة وكذا الوقوف عند صحة هذه الفرضية، يفرض علينا البحث في مدى قدرة القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية وحدود الإستعانة بمختلف الآليات الإجرائية التي أرساها المنتظم الدولي، ثم البحث بعد ذلك في مدى قدرة القواعد الإجرائية الواردة في قانون المسطرة الجنائية على استيعاب مختلف إجراءات البحث في الجريمة الإلكترونية، وذلك كله وفق التصميم التالي:

الفصل التمهيدي: مدى إمكانية الإكتفاء بالقواعد الإجرائية العادية في مجال البحث عن الجريمة الإلكترونية

الفصل الأول :الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية

الفصل الثاني : الإطار الإجرائي الوطني في مجال البحث عن الجريمة الإلكترونية

الفصل التمهيدي: مدى إمكانية الإكتفاء بالقواعد الإجرائية العادية في مجال البحث عن الجريمة الإلكترونية

إن دراستنا لهذا الفصل سنحاول من خلالها الوقوف عند مدى إمكانية الإكتفاء بالقواعد الإجرائية العادية في مجال البحث عن الجريمة الإلكترونية، وكيف اختلف رجال القانون والفقه في هذا الصدد، بين من يرى قدرة القواعد الإجرائية العادية على التصدي وضبط الجريمة الإلكترونية ومن يذهب إلى ضرورة تخصيص قواعد إجرائية في مجال البحث عنها، والتي بمقتضاها يمكن تحقيق نوع من التوازن بين حماية حق الدولة في المحافظة على نظامها من أي فعل يمكن أن يهدد كيانها من ناحية، ومن ناحية أخرى توفير الضمانات التي تكفل للفرد حقوقه وتحمي خصوصياته.

وهذا كله سيكون وفق التقسيم التالي :

المبحث الأول: حدود قدرة القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية

المبحث الثاني : إمكانية إفراد قواعد خاصة لضبط الجريمة الإلكترونية

المبحث الأول : حدود قدرة القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية

لما كانت القواعد الإجرائية عبارة عن مجموعة من الآليات التي تنظم التصرفات التي قد يأتيها المكلفون بإنفاذ القانون وفق ما تقتضيه مصلحة البحث والتحري بغرض جمع الإستدلالات وتمحيصها، فسنحاول من خلال هذا المبحث معرفة مدى اعتبار هذه القواعد الإجرائية العادية كافية للبحث عن الجريمة الإلكترونية وضبطها، أم أن هذه القواعد تبقى قاصرة على القيام بذلك.

لذلك ارتأينا تقسيم هذا المبحث على الشكل التالي :

المطلب الأول :مدى اعتبار القواعد الإجرائية العادية كافية لضبط الجريمة الإلكترونية

المطلب الثاني :محدودية القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية

المطلب الأول : مدى اعتبار القواعد الإجرائية العادية كافية لضبط الجريمة الإلكترونية

إن دراستنا لهذا المطلب ستكون محاولة لمعرفة مدى اعتبار القواعد الإجرائية كافية لضبط الجريمة الإلكترونية، وهذا سيجرنا للوقوف عند الطرح الذي اعتبر بأن القواعد الإجرائية العادية قواعد عامة تنطبق على الجريمة الإلكترونية(الفقرة الأولى) ثم بعد ذلك الوقوف عند مدى إمكانية القول بأن هذه القواعد الإجرائية العادية كافية لضبط الجريمة الإلكترونية (الفقرة الثانية).

الفقرة الأولى : القواعد الإجرائية العادية قواعد عامة تنطبق على الجريمة الإلكترونية

إن القواعد الإجرائية المتعلقة بالبحث والتحري عن الجرائم في شكلها التقليدي هي قواعد لا تخص جريمة معينة دون أخرى، بل هي قواعد عامة يمكنها أن تنطبق على كافة الأفعال المخالفة للقانون الجنائي بما فيها الجريمة الإلكترونية والتي تبقى وتظل وإن اختلفت عن غيرها من الجرائم سواء من حيث طبيعتها أو خصائصها، خاضعة من حيث المبدأ للقواعد العامة التي تسري على جميع الجرائم [1].

هذا وقد أشار البعض إلى أن البحث في الجرائم الإلكترونية يأخذ بجميع عناصر البحث ويمر بذات المراحل الفنية والشكلية المتبعة في الجرائم التقليدية لإحتمال ارتباطها بمختلف أنواع الجرائم الأخرى[2]، وبالتالي فبوسع أجهزة العدالة أن تستعمل القواعد الإجرائية القائمة في تعاملها مع الجرائم الإلكترونية، فهذه القواعد القائمة لم تغيرها أو

[1] الناجم كوبان، الإثبات الجنائي في الجرائم المعلوماتية، رسالة لنيل دبلوم الماستر في العلوم القانونية، وحدة القانون الجنائي وحقوق الإنسان، كلية العلوم القانونية والاقتصادية والاجتماعية- جامعة محمد الخامس اكدال، الموسم الجامعي2011-2010 ، ص.105

[2] مصطفى محمد مرسي، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة-القاهرة، الطبعة الأولى2008، ص.17

لم تؤثر فيها الجرائم الإلكترونية، فقط ينبغي تطوير بعض المفاهيم وتناولها بطريقة قانونية [1].

كما سار البعض الأخر في نفس السياق واعتبر بأن القوانين الإجرائية الحالية تتضمن مجموعة من المقتضيات العامة التي يمكن أن تسري أو تنسحب على الجريمة الإلكترونية فقط تحتاج إلى بعض التعديلات لتضفي على إجراءات البحث والتحري في هذا النوع من الجرائم نوعا من الخصوصية تلاءم طبيعة هذه الجريمة التي تتميز بخصوصية وذاتية متميزة عن باقي الجرائم [2].

إلا أن هذا الطرح – القواعد الإجرائية العادية قواعد عامة يمكنها أن تنطبق على الجريمة الإلكترونية - لا يمكن الأخذ به على إطلاقه وذلك راجع بالتأكيد لطبيعة ولخصوصية الجريمة الإلكترونية وصعوبة ضبطها والتي لا تنسجم مع البيئة التقليدية التي ترتكب فيها مختلف الجرائم الأخرى كما سنتولى تبيان ذلك لاحقا.

الفقرة الثانية: حدود كفاية القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية

لقد اختلفت الإتجاهات في القول بمدى إمكانية الإعتماد على القواعد الإجرائية العادية واعتبارها كافية لضبط الجريمة الإلكترونية، حيث ذهب الإتجاه الأول إلى القول بأنه يصعب حتى هذه اللحظة في بعض الأنظمة القانونية أن تحدد إلى أي مدى تكفي الأساليب التقليدية في قانون الإجراءات الجنائية لضبط الجريمة المعلوماتية والبحث عن الأدلة وتحقيقها، ومن أمثلة هذه الأساليب التحفظ على المعلومات والتفتيش للحصول على الأدلة والحق في مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الاتصال عن بعد وجمعها وتخزينها [3].

---

[1] إيهاب ماهر السنباطي، الجرائم الإلكترونية: قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد!، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 يونيو2007، المملكة المغربية، ص.16 و17

[2] هشام ملاطي، المرجع السابق، ص.96

[3] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنيت، دار النهضة العربية- القاهرة، الطبعة الأولى1999، ص.60

أما الإتجاه الثاني فاعتبر القول بأن هذه القواعد كافية للتصدي وضبط الجريمة الإلكترونية واستيعاب كافة شكليات البحث المنجزة بشأنها لم يعد ممكنا، كما أن البحث والتحري عن الجريمة الإلكترونية عن طريق القواعد الإجرائية التقليدية لم يعد كافيا وميسورا لأنه يواجه تقنيات حديثة في أسلوب وطريقة ارتكاب الجريمة [1].

كما اعتبر نفس الإتجاه أن هذه الجرائم تقع في البيئة الإفتراضية وبالتالي فهي لا تترك أية آثار مادية محسوسة كما يصعب تتبع واقتفاء أدلة ارتكابها لسرعة اندثارها خلافا للجرائم التقليدية [2]، هذه الأخيرة يمكن إدراكها بكافة الحواس، ومن تم فإن طبيعة البيانات المعالجة في هذه البيئة الرقمية وحدود البحث عنها يتطلب قواعد خاصة تحكمها بدلا من محاولة تطويع القواعد التقليدية وتوسيع نطاقها [3]، لذلك فإن هذه القواعد التقليدية لا تتوافق وطبيعة الجرائم الإلكترونية والتي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية التي أرستها القوانين الإجرائية[4].

وعليه، وأمام تضارب هذه الإتجاهات فإن الإتجاه القائل بأن القواعد الإجرائية العادية أصبحت غير كافية وقاصرة على ضبط الجريمة الإلكترونية هو الأقرب للصواب وذلك نظرا لمجموعة من الاعتبارات سنحاول التطرق إليها من خلال المطلب الثاني وذلك عند حديثنا عن محدودية القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية.

---

[1] الناجم كوبان، المرجع السابق، ص.77

[2] محمد العسكري، خصوصيات الإثبات في الجرائم المعلوماتية، مجلة القضاء والتشريع، وزارة العدل وحقوق الإنسان التونسية، العدد 7، جويلية 2005، ص. 163

[3] موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول : المعلوماتية والقانون، 28-29 أكتوبر 2009، طرابلس-ليبيا، ص.3

[4] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، جامعة قاصدي مرباح ورقلة - الجزائر، سنة 2013، ص.66

المطلب الثاني : محدودية القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية

إن دراستنا لهذا المطلب الغاية منها الوقوف عند محدودية وقصور القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية وذلك راجع لبعض الإعتبارات، من بينها أن محدودية هذه القواعد التقليدية والإعتماد عليها للبحث عن الجريمة الإلكترونية وضبطها قد يكون فيه مساس بالشرعية الإجرائية وبحقوق الأفراد، وهذا ما سنحاول التطرق إليه من خلال الفقرة الأولى، ثم بعد ذلك حديثنا سينصب حول معرفة مدى ارتباط محدودية القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية بخصوصية هذه الجريمة من خلال الفقرة الثانية.

الفقرة الأولى : ارتباط البحث عن الجريمة الإلكترونية بمفهوم الشرعية

لطالما كان مبدأ الشرعية الإجرائية يعتبر حجز الزاوية في الإجراءات القانونية للبحث والتحقيق في الجرائم المرتكبة ومتابعة فاعليها وتوقيع العقوبة المناسبة لهم، فهو يرمي إلى حماية حقوق وحريات الإنسان، ويهدف كذلك إلى تحقيق غاية أخرى على مستوى القوانين الإجرائية ألا وهي حسن سير العدالة الذي يقضي من جهة بتقوية الصيانة اللازمة لتلك الحقوق والحريات، وبالتوفيق بينها وبين مستلزمات استقرار النظام المجتمعي[1].

فالقوانين الإجرائية بما تتضمنه من قواعد إجرائية تعتبر بمثابة الوثيقة الأساسية لحماية حقوق الأفراد والتي تؤكد على احترام المبادئ الأساسية المعترف بها دوليا [2] وكذا تحقيق التوازن بين مصلحة الدولة في الوصول إلى الحقيقة والحريات الفردية للمواطنين [3]، فالقواعد الإجرائية تحتك باستمرار مع حقوق الفرد وحريته[4].

---

[1] محمد الإدريسي العلمي المشيشي، المسطرة الجنائية، الجزء الأول، المؤسسات القضائية، منشورات جمعية تنمية البحوث والدراسات القضائية، 1991، ص.20

[2] عبد اللطيف بوحموش، دليل الشرطة القضائية في تحرير المحاضر وتوثيق المساطر، مطبعة الأمنية-الرباط، الطبعة الثالثة، 2013، ص.70

[3] سعيد عبد اللطيف حسن، المرجع السابق، ص.61

[4] أحمد الخمليشي، شرح قانون المسطرة الجنائية، الجزء الأول، مطبعة المعارف الجديدة-الرباط، الطبعة الخامسة، 1999، ص.22

وعليه فإن شرعية الإجراءات تقتضي أن تكون إجراءات البحث عن الأدلة وجمعها موافقة ومحددة وفق القانون ولا تخرج عن روح نصوصه [1]، وبالتالي فإن التوسع في مباشرة إجراءات أو في تفسير هذه الإجراءات المقررة فإنه يهدد حقوق وحريات الأفراد[2]، لذلك فإن النصوص الخاصة ببعض الإجراءات بمفهومها التقليدي لا ينبغي إعمالها بشأن الجريمة الإلكترونية مباشرة، باعتبار أن هذه النصوص تمثل قيدا على الحرية الفردية، ومن ثم يصبح القياس على الأشياء المادية محظورا لمنافاته الشرعية الإجرائية [3].

وعليه، فإنه ينبغي الموازنة بين حقوق الشخص المتهم من جهة وحقوق المجتمع من جهة أخرى، وبين هذه الحقوق وضرورة احترام القواعد الشرعية والقانونية أثناء البحث عن الدليل في البحث الجنائي عموما وفي مجال الجريمة الإلكترونية على وجه الخصوص[4].

لذلك يمكن القول بأن القواعد الإجرائية العادية أبانت عن محدوديتها وقصورها لأن مباشرتها في بيئة لا تنسجم معها قد يشكل مساسا بالشرعية الإجرائية بصفة عامة وبحقوق الأفراد بصفة خاصة، وبالتالي بات من الضروري إفراد قواعد خاصة بالبحث عن هذا النوع من الجرائم تكفل في الوقت ذاته توازنا بين متطلبات الفعالية لأنشطة الأجهزة الجنائية الإجرائية في المجال المعلوماتي ومقتضيات حماية حريات الأفراد وحقهم في الخصوصية [5].

---

[1] كوثر أحمد خالند، الإثبات الجنائي بالوسائل العلمية، مكتب التفسير للإعلان والنشر،اربيل العراق، طبعة 2007، ص.58

[2] سعيد عبد اللطيف حسن، نفس المرجع، ص.61

[3] موسى مسعود أرحومة، المرجع السابق، ص.7

[4] عبد الحكيم الحكماوي، المرجع السابق، ص.154

[5] هشام محمد فريد رستم، الجوانب الإجرائية في الجريمة المعلوماتية-دراسة مقارنة-، مكتبة الآلات المدنية-أسيوط، طبعة 1994، ص.12

الفقرة الثانية: ارتباط القواعد الإجرائية العادية في ضبط الجريمة الإلكترونية بمفهوم الخصوصية

من المعلوم أن الجريمة الإلكترونية لديها العديد من الوجوه فهي كل يوم تظهر بطريقة جديدة [1]، كما أنها تتم خارج واقع الإطار المادي الملموس الأمر الذي يعقد من مهام السلطات المكلفة بالبحث والتحري، فمن خصائص الجريمة الإلكترونية أنها قلما تخلف آثارا مادية[2] إضافة إلى لزوم وقت طويل نسبيا لاكتشافها مما يعطي الفرصة لمرتكبي هذه الجرائم أن يتلفوا أو يعبثوا بالآثار المادية للجريمة، فلما كانت الجريمة الالكترونية ذات طبيعة خاصة وأدلتها غير محسوسة وتحتاج لخبرة فينة وتقنية عالية في التعامل معها [3]، فقد أجمع الفقه ورجال القانون خصائص الجريمة الإلكترونية في أربعة نقط تتمثل أساسا في سرعة ارتكاب الجريمة الإلكترونية وإزالة أثارها وارتكابها بشكل متخف ومستتر، وعدم تركها لأية أثار مادية ملموسة زيادة على طابعها العابر للحدود الوطنية[4]، فالأجهزة المكلفة بالبحث والتحري قد اعتادت على التعامل مع جرائم مادية بوسائل تقليدية، لكن في المحيط الإلكتروني الأمر مختلف لأن هذه الأجهزة لا تستطيع تطبيق هذه الوسائل أو الإجراءات على جريمة معنوية لا مادية[5].

فرجال القانون والفقه لما أكدوا على محدودية وقصور القواعد الإجرائية التقليدية في ضبط الجريمة الإلكترونية كان سندهم في ذلك يقوم على أن البيئة الرقمية

---

[1] Ali El Azzouzi, La cybercriminalité au Maroc, Bishops solutions-Casablanca, juin 2010, p.42

[2] Florence de Villenfagne & Séverine Dusollier, la Belgique sort enfin ses armes contre la cybercriminalité : a propos de la loi du 28 novembre 2000 sur la criminalité informatique, droit et nouvelles technologies,16 Mars 2001, p.17

[3] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الرقمية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت-لبنان، الطبعة الثانية 2007، ص.345

[4] هشام ملاطي، المرجع السابق، ص.75

[5] يوسف صغير، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، جامعة مولود معمري-تيزي وزو-الجزائر، سنة2013 ، ص. 125

لا تستطيع أن تطبق فيها الأجهزة المكلفة بالبحث والتحري الإجراءات التقليدية [1] وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصالات حيث أن مختلف المعلومات تكون في شكل نبضات إلكترونية والتي تعتبر من طبيعة معنوية [2] هذا من جهة، ومن جهة أخرى فقد اعتبروا أن القواعد الإجرائية التقليدية وضعت في الأصل من أجل مكافحة الإعتداءات المادية والجريمة الإلكترونية تخرج من هذا الإطار لأنها تتم خارج واقع الإطار المادي الملموس[3]، بالإضافة إلى هذا فإن هذه القواعد التقليدية تتميز بانعدام أو ضعف الاستجابة لمتطلبات ضبط الجريمة الالكترونية وجمع الأدلة عنها والبحث عن مرتكبيها وإيقافهم وتقديمهم للعدالة[4].

المبحث الثاني : إمكانية إفراد قواعد خاصة لضبط الجريمة الإلكترونية

أمام محدودية وقصور القواعد الإجرائية العادية على ضبط الجريمة الإلكترونية، وعدم استيعاب هذه القواعد لمختلف الإجراءات المتبعة في مجال البحث عن الجريمة الإلكترونية وكذا عدم انسجامها مع البيئة التي ترتكب فيها، أصبحت الحاجة ملحة لتخصيص الجريمة الإلكترونية بقواعد خاصة تحكمها وتنظم مختلف الإجراءات التي ستسلكها وتتبعها أجهزة إنفاذ القانون للبحث عنها وضبطها.

وعليه فإن مسألة إفراد الجريمة الإلكترونية بقواعد خاصة تنسجم مع طبيعتها وخصوصيتها أملتها مجموعة من الإعتبارات، كان من بينها الإختلاف الذي يطبع القواعد الإجرائية العادية عن نظيرتها في مجال البحث عن الجريمة الإلكترونية من جهة، والصعوبات التي تعترض أجهزة إنفاذ القانون لضبط هذه الجريمة من جهة أخرى.

---

[1] Yann padova, Un aperçu de la lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénal comparé, N°4 octobre-décembre 2002, p.767

[2] محمد جوهر، خصوصية زجر الإجرام المعلوماتي، مجلة الملف، العدد 9 نونبر2006 ، ص.15

[3] عبد الفتاح بيومي حجازي، الإثبات في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية-القاهرة، طبعة 2007، ص.137

[4] أحمد ايت الطالب، تقنيات البحث وإجراءات المسطرة المتبعة في جرائم الانترنيت والمعلوميات، مجلة الملف، العدد 9 نونبر2006 ، ص.26

وعليه فدراستنا لهذا المبحث ستكون على الشكل التالي:

المطلب الأول: مبررات إفراد الجريمة الالكترونية بقواعد إجرائية خاصة

المطلب الثاني: الحاجة إلى قواعد إجرائية خاصة للبحث عن الجريمة الإلكترونية وضبطها

المطلب الأول: مبررات إفراد الجريمة الإلكترونية بقواعد إجرائية خاصة

لقد أصبح لزاما توفير قواعد وآليات إجرائية لمجابهة هذه الجرائم وضبطها بما ينسجم وطبيعة البيئة المعلوماتية، حيث كان من بين المبررات والإعتبارات التي تدعو إلى تخصيص قواعد إجرائية للبحث عن الجريمة الإلكترونية، تميز الآليات الإجرائية العادية عن الآليات الإجرائية للبحث عن الجريمة الإلكترونية وهذا ما سنحاول الوقوف عنده من خلال الفقرة الأولى، وكذلك صعوبة ضبط هذه الجريمة الإلكترونية بالآليات والقواعد الإجرائية العادية حيث سنحاول معرفة حدود ارتباط تخصيص الجريمة الإلكترونية بقواعد إجرائية بصعوبة ضبطها من خلال الفقرة الثانية.

الفقرة الأولى: تميز آليات البحث عن الجريمة الإلكترونية بالخصوصية

إن الآليات الإجرائية العادية التي تمكن الأجهزة المكلفة بالبحث والتحري، من البحث عن أدلة ارتكاب الجريمة لا تتماشى ولا تنسجم مع البيئة الرقمية، خصوصا تلك المتعلقة بالتفتيش وحجز الأشياء، بالإضافة إلى لا مادية الدليل وسرعة إتلافه وضياعه الشيء الذي لا يمكن من ضبط الجريمة الإلكترونية[1].

كما أن الحديث عن ممارسة الأجهزة المكلفة بالبحث والتحري مهامها في البحث عن الجريمة الإلكترونية في إطار مسطرة التلبس أو ضبطها في حالة التلبس يختلف عن البحث الذي تنجزه في إطار مسطرة التلبس في باقي الجرائم الأخرى، حيث أن حالة التلبس لا تتوفر في هذا النوع من الجرائم كما هي منصوص عليها في القواعد العادية [2]،

---

[1] Yann padova, op.cit, p.768

[2] لكن هذا لا يمنع من تصور التلبس في الجريمة الالكترونية في حالته العادية وذلك في بعض الحالات، ومثال ذلك الحكم الصادر عن المحكمة الابتدائية بسلا، حيث تم متابعة المتهمين بإدخال معطيات في نظام للمعالجة

وفي هذا السياق ذهبت محكمة النقض، حيث جاء في أحد قراراتها بأن " البحث الذي أجرته الضابطة القضائية مع كل المتهمين تم إنجازه في إطار مسطرة التلبس لأن الجرائم المعلوماتية يصعب اكتشافها في حينها، وإنجاز البحث بشأنها يقتضي السرعة والدقة كي لا تندثر أثار الجريمة أو يتطور الضرر ويصبح من الصعب السيطرة عليه[1]".

فأمام هذا الإختلاف بين القواعد الإجرائية العادية والقواعد الإجرائية للبحث عن الجريمة الإلكترونية، ومدى إمكانية تخصيص قواعد إجرائية للبحث عن الجريمة الالكترونية وضبطها، ظهر اتجاهين:

الإتجاه الأول اعتبر أنه عند اللجوء إلى استخدام إجراءات علمية جديدة في البحث فإن ذلك قد يكون ضد الإنسان وكرامته وحقوقه وحرياته العامة والخاصة[2].

في حين أن الإتجاه الثاني ذهب إلى القول بأن القواعد الإجرائية العادية لا تتواءم مع الطبيعة الخاصة لهذه الطائفة من الجرائم، كما أن الآليات الإجرائية للبحث في الجرائم الإلكترونية تختلف عن الآليات الإجرائية للبحث في الجرائم العادية لإختلاف طريقة ارتكابها وتداعياتها الحقوقية والمادية[3]، وبالتالي أكد على ضرورة إفراد قواعد خاصة بالبحث عن هذا النوع من الجرائم لكن يجب أن تضمن التوازن بين الحق في استعمال التكنولوجيا من جهة وحماية خصوصية مستعملها من جهة[4]، كما ينبغي أن

الآلية عن طريق الاحتيال طبقا للفصل 6-607 من القانون الجنائي حيث جاء في إحدى حيثيات الحكم "....وبقي يساعد الصيني في تحويل المكالمات الدولية وقرصنتها مقابل مبالغ مالية مهمة إلى حدود تاريخ إيقافه متلبسا بهذا الفعل بعدما تم ضبطه من طرف رجال الشرطة داخل الشقة وهو بصدد القيام بتحويل المكالمات الدولية باستخدام تلك التجهيزات...." - حكم صادر عن المحكمة الابتدائية بسلا بتاريخ 24-4-2013، تحت عدد 809، رقم338-13-1 ت، غير منشور

[1] قرار رقم 1/681 المؤرخ في 3 غشت2011 ، الغرفة الجنائية القسم الأول، الملف عدد16080 /2010 ، غير منشور

[2] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية-دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية-، دار الكتب القانونية-القاهرة، الطبعة الأولى 2007، ص.3

[3] حفيظ الزايدي، الآليات القانونية والإجرائية للحد من أثار الجريمة الالكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص.170

[4] هشام ملاطي، المرجع السابق، ص.74

تكون مشروطة بعدم المساس بالخصوصية - أي حماية البيانات الشخصية المتعلقة بالحياة الخاصة المخزنة في نظم المعلومات - وحماية مختلف أسرار الفرد أو الهيئة محل إجراءات البحث[1].

وبالتالي فإن الحاجة أصبحت ملحة لتخصيص الجريمة الإلكترونية بقواعد إجرائية خاصة للبحث عنها والتصدي لها، مع الأخذ بعين الاعتبار كيفية التوفيق بين البحث بهذه القواعد الإجرائية الحديثة من ناحية، واحترام حقوق وحريات الأفراد من ناحية أخرى.

الفقرة الثانية: ارتباط تخصيص الجريمة الإلكترونية بقواعد إجرائية بصعوبة ضبطها

لما كانت الجرائم الإلكترونية في أكثر صورها تعتبر جرائم مستترة وخفية، فهذا يجعلها تتميز بصعوبة كشفها وتحديد مصدرها خاصة في حالة ارتكابها عن بعد من داخل دولة أجنبية، أو صعوبة إيقافها بالنظر إلى سرعة انتشار المعلومات وتسجيلها أوتوماتيكيا على الحاسبات الخادمة الموجودة في الخارج [2].

كما تضاف إلى كل هذا مجموعة من الصعوبات منها لا مادية الآثار والمعالم التي يمكن الإستدلال من خلالها على وقوع الجريمة ونسبتها إلى شخص أو أشخاص محددين [3]، وكذا صعوبة الولوج إلى بعض المعلومات المحفوظة تحت رقم سري أو المشفرة كليا[1]

---

[1] مصطفى محمد مرسي، المرجع السابق، ص.19

_ انظر أيضا في هذا الصدد حيثيات القرار الصادر عن محكمة النقض الفرنسية بتاريخ 24 ابريل 2013

attendu qu'en statuant ainsi, alors qu'il lui appartenait de rechercher si les pièces et supports informatiques dont la saisie était contestée par la société étaient ou non couverts par le secret professionnel entre un avocat et son client, et sans annuler la saisie de correspondances dont il a constaté qu'elles relevaient de la protection de ce secret et alors enfin que la violation dudit secret intervient dès que le document est saisi par les enquêteurs,

http://www.legifrance.gouv.fr

[2] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات-دراسة مقارنة، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، 2007، ص.10

[3] ومن الأمثلة التي نسوقها في هذا الباب قضية عرضت على المحكمة الابتدائية بورزازات وتتعلق بشكاية رسمية تقدمت بها دولة قطر مفادها أن الموقع الالكتروني لأمير قطر تعرض لهجوم معلوماتي وأن عملية رصد مصدر

والتي يعمد أصحابها إلى حفظ المعطيات باستعمال أرقام أو رموز سرية أو حتى إلى استعمال تقنية التشفير، مع الإحتفاظ بمفتاح خاص للحل، وعلى صعيد أخر فإن المعطيات التي تعتبر أداة للجريمة وموضوعا لها وأحيانا نتيجة متحصلة عنها هي من الهشاشة، بحيث تكفي عملية ضغط على زر أو نقر على الرمز أو الكتابة أو الإشارة الضوئية المخصصة لذلك لمسح وإزالة المعطيات التي يمكن اعتمادها في نسبة الجريمة إلى فاعلها[2].

فضلا عما تقدم، فإن الوصول إلى الدليل الإلكتروني تعترضه عقبة أخرى تكمن في أن الجناة المتمرسين يجتهدون في إخفاء هوياتهم للحيلولة دون تعقبهم أو كشف أمرهم، بحيث تظل أنشطتهم مجهولة وبمنأى عن علم السلطات المعنية بمكافحة الجريمة[3].

وعليه يمكن إجمالا حصر أهم الصعوبات التي تبرر تخصيص الجريمة الإلكترونية بقواعد إجرائية خاصة فيما يلي [4]:

_ ارتكاب الجريمة عن بعد؛

_سرعة تنفيذ الجرائم الالكترونية ؛

_لجوء الجاني إلى محو آثار الجريمة وإتلاف أدلتها؛

_ صعوبة جمع الأدلة بشأنها؛

الاعتداء أفضت إلى أن المشتبه فيه يقطن بمدينة ورزازات، وبعد متابعة المشتبه فيه الذي كان يتابع دراسته بمعهد التكنولوجيا تبين للمحكمة أن والده هو من اقتنى له الحاسوب وأن فاتورة شراء الحاسوب تحمل تاريخا لاحقا لتاريخ ارتكاب الأفعال موضوع الشكاية، كما أن الخبرة التي أنجزتها الشرطة العلمية على الحاسوب أثبتت أن أجزاءه أصلية ولم يتم تغييرها وانه يحتمل أن يكون الجاني شخص آخر ارتكب الجريمة عبر حاسوب الشخص المتابع باعتماد تقنية الحاسوب الشبح(p.c zombie) فقضت المحكمة ببراءة المتهم.

_ انظر عبد الرحمان اللمتوني، المرجع السابق، ص.51

[1] عبد الرزاق سندالي، التشريع المغربي في مجال الجرائم المعلوماتية، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20يونيو2007، المملكة المغربية، ص. 72

[2] أحمد ايت الطالب، المرجع السابق، ص.23

[3] موسى مسعود أرحومة، المرجع السابق، ص.4

[4] هشام ملاطي، المرجع السابق، ص.75

_ تخزين البيانات والمعلومات المتعلقة بالجريمة بأنظمة وشبكات الكترونية موجودة في دول مختلفة؛

- مساس إجراءات البحث والتفتيش بخصوصيات الأفراد.

المطلب الثاني: الحاجة إلى قواعد إجرائية خاصة للبحث عن الجريمة الإلكترونية وضبطها

إن الحديث عن إفراد قواعد إجرائية في مجال البحث عن الجريمة الإلكترونية الغرض منه تحقيق نوع من التوازن المطلوب بين حق المجتمع في مكافحة الجريمة والكشف عنها بوسائل لا تقل فاعلية وأهمية عن تلك التي يستخدمها الجناة لتنفيذ فعلهم أو أسلوبهم الإجرامي بشكل أفضل وأسهل وحق الفرد في الخصوصية والسرية، لذلك أصبح من الضروري تخصيص قواعد إجرائية تتعلق بالبحث والتحري عن الجريمة الإلكترونية(الفقرة الأولى) وكذلك قواعد إجرائية تحكم وتنظم الإختصاص في هذا النوع من الجرائم (الفقرة الثانية).

الفقرة الأولى: تخصيص قواعد إجرائية متعلقة بالبحث والتحري عن الجريمة الإلكترونية

أمام قصور ومحدودية القواعد الإجرائية العادية أصبح لزاما تخصيص الجريمة الإلكترونية بقواعد إجرائية خاصة تؤكد خصوصيتها وذاتيتها مقارنة مع الجرائم العادية، وتنظم إجراءات البحث والتحري بما يتناسب مع البيئة التي ترتكب فيها هذه الجرائم.

لذا بات من الضروري وضع قواعد خاصة بالتفتيش وحجز بيانات الكمبيوتر المخزنة وسرعة التحفظ عليها وكذلك إمكانية اعتراض محتوى هذه البيانات المخزنة[1].

زيادة على هذا أصبح أيضا من الضروري اتخاذ تدابير إجرائية تمنح السلطات المختصة صلاحية الضبط والتأمين للبيانات وأخذ نسخة منها والإحتفاظ بها أو جعلها غير قابلة للدخول عليها أو حذفها من النظام، وصلاحية هذه السلطات في التجميع الفوري لبيانات الكمبيوتر من خلال جمع أو تسجيل أو إجبار مقدم الخدمة في نطاق قدرته

[1] Lionel Thoumyre, Une Europe unie face à la réglementation de l'internet ? _ Etat des lieux_, droit et nouvelles technologies, 26 septembre 2003, p.9

الفنية على جمع أو تسجيل سير البيانات المرتبطة باتصالات معينة بالإضافة إلى اعتماد تدابير تعزز صلاحيتها بالإعتراض على محتوى البيانات المخزنة بالكمبيوتر[1].

الفقرة الثانية: تخصيص قواعد إجرائية تحكم ضوابط الإختصاص في الجريمة الإلكترونية

لما كانت الجريمة الإلكترونية ذات طبيعة خاصة وتتميز بخصوصيات متعددة منها أنها جريمة عابرة للحدود، فان إجراءات البحث عنها قد يمتد خارج الحدود الإقليمية، فهي لا تحدها حدود خلافا للجرائم التقليدية الأمر الذي يجعلها في كثير من الأحيان تستعصي على الخضوع للقوالب التي تحكم مسألة الإختصاص المكاني، ومن تم فإن الطبيعة الخاصة لهذا الصنف من الجرائم المستحدثة يتطلب تجاوز المعايير التقليدية، الشيء الذي جعل البعض يرى بأن تطبيق القواعد التقليدية على الجرائم الإلكترونية لا تتلاءم مع تحديد محل وقوع الجرم في العالم الإفتراضي[2]، ذلك أن هذه الجرائم لا تعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، بحيث فقدت الحدود الجغرافية كل اثر لها في الفضاء الشبكي المتشعب العلاقات، وأصبحنا بالتالي أمام جرائم عابرة للحدود تتم في فضاء إلكتروني معقد عبارة عن شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأي سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي، له وجود حقيقي وواقعي لكنه غير محدد المكان[3].

وبالتالي أصبح من الضروري العمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم، وسهولة ارتكابها والتخلص من أثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها[4]، ذلك أن الطبيعة العابرة للحدود التي تميز هذه الجرائم عن غيرها من الجرائم التقليدية تجعل من الضرورة تبني قواعد إجرائية تحكم مسألة الإختصاص في البحث عن الجريمة الإلكترونية لتيسير ضبطها وإقامة الدليل على مرتكبيها، وكذا توسيع اختصاص أجهزة إنفاذ القانون للبحث عن الجريمة

[1] هشام ملاطي، المرجع السابق، ص. 102

[2] فريد منعم جبور، المرجع السابق، ص.206

[3] نور الدين الواهلي، المرجع السابق، ص.133

[4] الناجم كوبان، المرجع السابق، ص.71

الإلكترونية خارج الحدود الترابية التي يمارسون فيها اختصاصاتهم العادية، وإمكانية تلقيهم وتزويدهم بمختلف المعلومات الضرورية التي قد تساعدهم في البحث والتحري بأية وسيلة من وسائل الإتصال الإلكترونية حتى لو تعلق الأمر بالحصول على معلومات على أشخاص يوجدون في الخارج[1]، وكذا إيجاد مقتضيات لجلب الإختصاص القضائي والتوسع في مجاله تنضاف إلى القواعد التقليدية التي تحكم الإختصاص المحلي.

وعليه فإن هذا كله ينبغي ألا يترك لمحض اجتهادات الفقه والقضاء وإنما يلزم تدخل تشريعي لتحديد معايير الإختصاص والتي يفترض عدم تضييق نطاقها، وكذلك إيجاد آليات ووضع ضوابط لتعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية[2].

[1] في هذا الصدد جاء في حيثيات إحدى القرارات الصادرة عن محكمة النقض الفرنسية بتاريخ 6 نونبر 2013، الذي نص على إمكانية تلقي ضباط الشرطة القضائية معلومات عن طريق وسائل الاتصال الالكترونية خارج الجدود الترابية التي يمارسون فيها اختصاصاتهم عن شخص يقطن بالخارج

attendu que ..... les officiers de police judiciaire n'ont, en principe, compétence que dans les limites territoriales où ils exercent leurs fonctions habituelles, il ne leur est pas interdit de recueillir, notamment par un moyen de communication électronique, des renseignements en dehors de leur circonscription, fût-ce en adressant directement une demande à une personne domiciliée à l'étranger,

http://courdecassation.fr/jurisprudence_2/chambre_criminelle_578/5362_6_27718.html

[2] نور الدين الواهلي، المرجع السابق، ص.141

الفصل الأول : الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية

لقد فطن المنتظم الدولي منذ بداية التسعينات من القرن الماضي بضرورة تخصيص الجرائم الإلكترونية بقواعد إجرائية ومسطرية خاصة، إيمانا منه بأن المكافحة الفعالة للجرائم الإلكترونية تستلزم تطوير آليات البحث والتحري وتقوية التعاون الدولي وتعزيز قدرات أجهزة إنفاذ القانون[1]، لذلك فقد حاول جاهدا إيجاد آليات إجرائية حديثة تنسجم وتتماشى مع طبيعة وخصوصية الجريمة الإلكترونية في سبيل ضبطها والتصدي لها، وهذا راجع بالأساس إلى قصور القواعد الإجرائية العادية والتقليدية على التعامل مع هذا النمط المستحدث من الجرائم.

ففي سبيل الوقوف في وجه هذا النوع من الجرائم، عمل المنتظم الدولي على وضع إستراتيجية تهدف تطوير مختلف الآليات الإجرائية بشكل يجعل المجرم يجد نفسه محاطا بسياج يحول دون إفلاته من مسؤوليته عن الجريمة التي ارتكبها، كما أكد على حتمية التعاون الدولي لتوحيد التشريعات أو على الأقل لتقليص الفوارق بينها من جهة[2] ومحاولة تعزيز مختلف آليات التعاون حتى لا يستفيد المجرمون من عجز وقصور التشريعات الداخلية من جهة وغياب التنسيق الدولي الذي يعالج سبل التصدي لهذه الجرائم من جهة أخرى.

وعليه، فدراستنا لهذا الفصل ستكون محاولة لمعرفة الآليات والقواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية الواردة في مختلف الإتفاقيات الدولية والتي تبناها المنتظم الدولي في سبيل إيجاد الحلول للمشاكل الإجرائية التي تطرحها هذه الجريمة، وأيضا لتيسير وتسهيل عملية البحث عنها من طرف الأجهزة المكلفة بذلك وضبطها والتصدي لها، ثم الوقوف بعد ذلك عند حدود ملاءمة بعض الدول لتشريعاتها المحلية مع ما أرساه المنتظم الدولي من قواعد إجرائية.

[1] هشام ملاطي، المرجع السابق، ص. 78

[2] فريد منعم جبور، المرجع السابق، ص. 216

لذلك ارتأينا تقسيم هذا الفصل على الشكل التالي :

المبحث الأول : الآليات الإجرائية الواردة في الاتفاقيات الدولية في مجال البحث عن الجريمة الإلكترونية

المبحث الثاني : حدود ملاءمة القوانين المقارنة مع الآليات الإجرائية الدولية

المبحث الأول : الآليات الإجرائية الواردة في الإتفاقيات الدولية في مجال البحث عن الجريمة الإلكترونية

وعيا من المنتظم الدولي بضرورة وضع إطار دولي لحل مختلف الإشكالات التي أصبحت تطرحها الجريمة الإلكترونية ومن بينها الإشكالات الإجرائية، عمل من خلال مختلف الصكوك الدولية من اتفاقيات وبرتوكولات ذات الصلة إلى تضمين مقتضيات خاصة بالقواعد الإجرائية سواء على مستوى البحث والتحري أو ملاحقة مرتكبي الجرائم الإلكترونية أو على مستوى آليات وقواعد الإختصاص في مجال البحث عنها، فلما كان الإجرام المعلوماتي في أغلب مظاهره ذو طابع دولي لم يعد بالإمكان مكافحة هذا النوع من الإجرام مكافحة فعالة على ضوء الآليات العتيقة[1]، لذلك أصبح الحديث عن إمكانية الإستعانة بالقواعد الإجرائية التي أرساها المنتظم الدولي من خلال مختلف المبادرات التي قام بها من اتفاقيات وبروتوكولات وتوصيات أمرا ضروريا.

وعليه فإننا سنحاول من خلال هذا المبحث الوقوف عند مختلف القواعد الإجرائية التي أرساها المنتظم الدولي في مجال البحث عن الجريمة الإلكترونية.

لذلك ارتأينا تقسيمه على الشكل التالي :

المطلب الأول : اتفاقية بودابست المتعلقة بالجريمة الإلكترونية

المطلب الثاني: الآليات الإجرائية الواردة في الإتفاقيات المشتقة عن اتفاقية بودابست

[1] محمد جوهر، المرجع السابق، ص. 16

المطلب الأول : اتفاقية بودابست المتعلقة بالجريمة الإلكترونية

دراستنا لهذا المطلب ستكون محاولة لمعرفة مختلف القواعد الإجرائية التي تضمنتها اتفاقية بودابست في مجال البحث عن الجريمة الإلكترونية، حيث سنحاول الوقوف عند المبادرات السابقة لإتفاقية بودابست وما تضمنته من قواعد إجرائية تهم الجريمة الالكترونية (فقرة أولى) ثم بعد ذلك سنتعرف عن مختلف القواعد الإجرائية التي تضمنتها اتفاقية بودابست (فقرة ثانية).

الفقرة الأولى : المبادرات السابقة لإتفاقية بودابست

لقد كان السبق لمبادرة لجنة الوزراء بمجلس أوروبا من خلال توصيتها الصادرة سنة 1995 تحت رقم R(95)13 في شأن المشاكل الإجرائية المرتبطة بتكنولوجيا المعلومات، والتي تبنتها لجنة الوزراء بالدول الأعضاء بمجلس أوروبا[1] بتاريخ 11 شتنبر من نفس السنة[2]، وذلك - حسب ما ورد في ديباجتها – بهدف تجنب مخاطر الأنظمة المعلوماتية وضرورة مسايرة الأنظمة الإجرائية للدول الأعضاء في جمع الأدلة الجنائية وملاءمة الوسائل القانونية لتمكين أجهزة البحث والتحري من الكشف عن الجرائم المعلوماتية[3].

وقد جاءت التوصية الأوروبية رقم R(95)13 في إطار استكمال مضامين التوصيات السابقة الصادرة عن مجلس أوروبا في مجال مكافحة الجريمة الإلكترونية[4].

---

[1] تبني لجنة الوزراء بمجلس أوروبا لهذه التوصية جاء على اثر اجتماع مندوبي الوزراء عدد 543 بتاريخ 11 شتنبر 1995

[2] Bertrand Warusfel, Procédure pénale et technologie de l'information/de la convention sur la cybercriminalité à la loi sur la sécurité quotidienne, Revue droit et défense, Numéro 2002/1,p. 1

[3] Lionel Thoumyre, op.cit , p.8

[4] وخاصة التوصيات التالية :

- La recommandation n° R (81) relative à l'harmonisation des législations en matière d'exigence d'un écrit et en matière d'admissibilité des reproduction de documents et des enregistrements informatique ;
- La recommandation n° R (85) 10 sur les commissions rogatoires pour la surveillance des télécommunications ;
- La recommandation n° R (87) 15 visant à règlements l'utilisation de données à caractère personnel dans le secteur de la police ;
- La recommandation n° R (89) sur la criminalité informatique

هذا وتشمل التوصية الأوروبية الخاصة بالمشاكل الجنائية المرتبطة بتكنولوجيا المعلومات على ملحق يضم سبعة محاور أساسية تهم التفتيش والحجز، والحراسة التقنية، وواجبات التعاون مع السلطات المكلفة بالبحث، والإثبات الإلكتروني، واستعمال التشفيرات، بالإضافة إلى مقتضيات تخص البحث والإحصائيات والتكوين والتعاون الدولي[1]، كما أكدت هذه التوصية على ضرورة مراجعة القوانين في مجال الإجراءات الجنائية للسماح بإعتراض الرسائل الإلكترونية وتجميع البيانات المتعلقة بتداول المعلومات في حالة التحريات المتعلقة بجريمة من الجرائم الخطيرة الماسة بسرية أو سلامة الإتصالات أو أنظمة الكمبيوتر[2].

كما نصت هذه التوصية على بعض التدابير، التي تهم تجميع الأدلة وإلزام أي شخص بحوزته هذه الأدلة على مساعدة الأجهزة المكلفة بالبحث والتحري، وإمكانية اعتراض البيانات أو الدخول إليها والتحفظ السريع على هذه البيانات[3] كما نصت أيضا على ضرورة تسليم مزودي الخدمات معلومات عن المستخدم بناء على أوامر السلطات المختصة المكلفة بالبحث[4].

الفقرة الثانية : القواعد الإجرائية الواردة في اتفاقية بودابست

في إطار تأكيد الإقتناع بضرورة إتباع سياسة جنائية مشتركة تهدف إلى حماية المجتمع ضد الجريمة الإلكترونية، واستكمال المبادرات التشريعية الدولية والوطنية في هذا الصدد لاسيما فيما يخص دعم الأبحاث والإجراءات الجنائية المتعلقة بالجرائم الإلكترونية وجعلها أكثر فاعلية، تم اعتماد الإتفاقية المتعلقة بالجريمة الإلكترونية من

[1] هشام ملاطي، المرجع السابق، ص.79

[2] نزيهة مكاري، وسائل الإثبات في جرائم الاعتداء على حق المؤلف عبر الانترنيت، مجلة المناهج القانونية، عدد مزدوج13/14_2009، ص.74

[3] Enderlin Clément, Les moyens juridique et institutionnels nationaux et européens de lutte contre la cybercriminalité dans le cyberspace, Mémoire de recherche Diplôme Universitaire Sécurité intérieure / extérieure dans l'union européennes, institut d'études politiques de Strasbourg, 2010-2011, p.79

[4] Bertrand Warusfel, op.cit, p.5

طرف لجنة الوزراء بالمجلس الأوروبي بتاريخ 8 نونبر 2001 [1]، والتي رأت في إقرارها تحقيق التعاون الدولي وكبح جماح مجرمي الكمبيوتر لأغراض غير مشروعة[2].

فهذه الإتفاقية تهدف إلى توحيد السياسة الواجب إتباعها في مكافحة الجرائم المعلوماتية المرتكبة في الفضاء الإفتراضي وإلى التنسيق بين التشريعات الوطنية لتسهيل مكافحة الإجرام المعلوماتي، وتطبيق إجراءات تحقيق وملاحقة تتلاءم مع الفضاء الافتراضي ووضع نظام تعاون دولي يتميز بالسرعة والفعالية في التنفيذ[3].

هذا، وقد اتخذت المقتضيات المتعلقة بالقواعد الإجرائية حيزا هاما ضمن أحكام اتفاقية بودابست، وذلك من خلال تخصيص 22 مادة من أصل 48 مادة مكونة للإتفاقية المذكورة للقواعد الإجرائية، حيث تم التأكيد عند تحديد نطاقها على ضرورة اعتماد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقرار القواعد الإجرائية الواردة في الإتفاقية لأغراض الأبحاث والإجراءات الجنائية[4].

وقد تضمنت الإتفاقية المذكورة مجموعة من القواعد الإجرائية الخاصة بالبحث والتحري من خلال المواد من 16 إلى 21 حيث يمكن إجمالها فيما يلي [5]:

- سرعة التحفظ على بيانات الكمبيوتر المخزنة [6] ؛
- إجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة [7] ؛

---

[1] عرضت للتوقيع بتاريخ 23 نونبر 2001 للإطلاع عليها يرجى زيارة الموقع التالي :
http://conventions.coe.int/Treaty/fr/treaties/Html/185.htm

[2] إدريس النوازلي، قراءة في الجريمة السيبيرية على ضوء الاتفاقية الأوروبية، مجلة المحاكم المغربية، العدد 104، شتنبر-أكتوبر 2006، ص. 46

[3] فريد منعم جبور، المرجع السابق، ص.219

[4] انظر في هذا الصدد المادة 14 من اتفاقية بودابست

[5] Jean-François Tyrode , Eléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercriminalité en droit européen , Mémoire pour obtenir le master en droit de l'internet public-administration-entreprise, Université paris 1, année universitaire 2006-2007, p.58
Voir aussi -Bertrand Warusfel , op.cit , p.3

[6] انظر في هذا الصدد المادة 16 من اتفاقية بودابست

[7] المادة 18 من اتفاقية بودابست

- تفتيش وحجز بيانات الكمبيوتر المخزنة [1] ؛
- التجميع الفوري لبيانات الكمبيوتر وإمكانية اعتراض هذه البيانات [2].

كما تضمنت الإتفاقية قواعد إجرائية متعلقة بالإختصاص القضائي في المادة 22 [3] منها ضوابط سريان الإختصاص القضائي على الجريمة الإلكترونية، مؤكدة على ضرورة اعتماد الدول الأطراف على ما يلزم من تدابير تشريعية وتدابير أخرى لإقرار الإختصاص القضائي على الجرائم الواردة في الإتفاقية، فالمادة 22 وضعت مجموعة من المعايير والتي بمقتضاها تنسق الأطراف المتعاقدة حدود صلاحياتها المتعلقة بالجرائم الواردة في الإتفاقية[4]، وذلك عندما ترتكب الجريمة في إقليم الدولة أو على متن إحدى السفن التي ترفع علمها أو على متن إحدى الطائرات المسجلة بموجب قوانينها وكذا على كل جريمة مرتكبة من جانب أحد مواطنيها إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي

---

[1] المادة 19 من اتفاقية بودابست

[2] المادتين 20-21 من اتفاقية بودابست

[3] حيث جاء في الفقرة الأولى من المادة 22 من اتفاقية بودابست :

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:

a sur son territoire; ou

b à bord d'un navire battant pavillon de cette Partie; ou

c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou

d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإقرار الاختصاص بشأن أي جريمة تنص عليها هذه الاتفاقية وذلك عندما ترتكب الجريمة :

أ- في إقليمه ؛ أو

ب- على متن إحدى السفن ترفع علم ذلك الطرف ؛ أو

ت- على متن إحدى الطائرات المسجلة بموجب قوانين ذلك الطرف ؛ أو

ث- من جانب أحد مواطنيه إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان ارتكابها أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأية دولة.

[4] انظر التقرير التفسيري لإتفاقية بودابست، القسم الثالث المتعلق بالإختصاص، البند 232، ص.73

بمكان ارتكابها أو في حالة ارتكاب الجريمة خارج الإختصاص القضائي لأية دولة، كما نصت الإتفاقية على عدم استبعاد الإختصاص الجنائي الذي ينص عليه أحد الأطراف وفقا لقانونه الوطني ومطالبة الدول الأطراف في الإتفاقية بالتشاور حول الإختصاص القضائي الأكثر ملاءمة لمحاكمة مرتكبي الجرائم الإلكترونية في حالة تعدد المطالبة من طرف الأطراف بإختصاصه القضائي حول واقعة معينة[1].

كما أن هذه الإتفاقية تضمنت مجموعة من الآليات في مجال التعاون بين الدول في مجال الإجراءات، حيث يمكن لإحدى الجهات أن تطلب من جهة أخرى من أن تأمر أو تفرض حماية سريعة وبطريقة مختلفة لبيانات مخزنة في نظم معلوماتية داخل حدود هذه الجهة الثانية لتسهيل عملية البحث عنها والوصول إليها، فهذه الآلية يصبح الوصول إلى البيانات المخزنة خارج الحدود ممكنا وسهلا لأي جهة تود أو تطلب ذلك[2].

وعليه فإنه يظهر من خلال كل هذه التدابير الإجرائية التي تضمنتها اتفاقية بودابست، أن الهدف منها إجراء تحقيقات أكثر فعالية فيما يتعلق بالجرائم الإلكترونية، كما يجب التأكيد على أن هذه التدابير الإجرائية يمكن استخدامها في مواجهة أي جريمة تستخدم فيها تكنولوجيا المعلومات والإتصالات[3].

المطلب الثاني : الآليات الإجرائية الواردة في الإتفاقيات المشتقة عن اتفاقية بودابست

بعد الوقوف عند مختلف القواعد الإجرائية التي تضمنتها اتفاقية بودابست في مجال البحث عن الجريمة الإلكترونية، ستكون دراستنا لهذا المطلب محاولة لمعرفة مختلف الآليات الإجرائية التي تهم الجريمة الإلكترونية والتي تضمنتها مختلف المبادرات التي تلت اتفاقية بودابست، حيث سنحاول الوقوف عند الآليات الإجرائية التي تضمنها

[1] هشام ملاطي، المرجع السابق، ص.91

[2] جان فرونسوا هرنوت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 يونيو2007، المملكة المغربية، ص. 103

[3] كريستينا سكولمان، المعايير الدولية المتعلقة بجرائم الانترنيت (مجلس أوروبا)، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 يونيو2007، المملكة المغربية، ص.63

بروتوكول ستراسبورغ (فقرة أولى) ثم بعد ذلك سنتعرض للآليات الإجرائية الواردة في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات (فقرة ثانية).

الفقرة الأولى : الآليات الإجرائية الواردة في بروتوكول ستراسبورغ

تم وضع هذا البروتوكول الإضافي خلال سنة 2003 [1] بهدف تتميم مضامين اتفاقية الجريمة المعلوماتية[2]، حيث تضمن هذا البروتوكول 17 مادة وقد ورد ضمن أحكام الفصل الثالث من البروتوكول المعنون ب" العلاقة بين الإتفاقية وهذا البروتوكول" في المادة الثامنة منه إلى أن القواعد الإجرائية المضمنة باتفاقية بودابست تطبق على الجرائم المشار إليها في البروتوكول، وذلك فيما يخص أحكام الإختصاص المشار إليها في المادة 22 من اتفاقية بودابست مع ما قد يلزم من تعديل " Mutatis mutandis " [3]، وكذا أحكام المواد من 14 إلى 21 المتعلقة بنطاق تطبيق القواعد الإجرائية والشروط والضمانات المرتبطة بها والقواعد الإجرائية المتعلقة بسرعة التحفظ على بيانات الكمبيوتر المخزنة وإصدار الأوامر وتفتيش وحجز بيانات الكمبيوتر والتجميع الفوري لها[4].

---

[1] والذي يطلق عليه البروتوكول الإضافي لاتفاقية الجريمة المعلوماتية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهة الأجانب التي ترتكب عبر أنظمة الكمبيوتر، عرض للتوقيع بستراسبورغ بتاريخ 28 يناير 2003، بمناسبة الدورة الأولى للجمعية البرلمانية لسنة 2003.

للإطلاع على البروتوكول، يرجى زيارة الموقع التالي :

http://conventions.coe.int/treaty/fr/Treaties/Html/189.htm

[2] حيث نصت المادة الأولى على أن الهدف من تقديم بروتوكول ستراسبورغ هو تكميل المقتضيات التي تضمنتها اتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة 2001.

Le but du présent Protocole est de compléter, pour les Parties au Protocole, les dispositions de la Convention sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001 (appelé ci-après « la Convention ») eu égard à l'incrimination des actes de nature raciste et xénophobe diffusés par le biais de systèmes informatiques.

[3] « Les articles 1.12.13.22.41.45 et 46 de la convention s'appliquent mutatis mutandis à ce protocole »

[4] « Les parties étendent le champ d'application des mesures définies aux articles 14 à 21, aux articles 2 à 7 de ce protocole » (art 8)

الفقرة الثانية : الآليات الإجرائية الواردة في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

بادرت الدول العربية إلى وضع اتفاقية عربية لمكافحة الجرائم الإلكترونية[1] وذلك في إطار مواكبة الجهود المبذولة على مستوى المنتظم الدولي، بهدف تعزيز التعاون بين الدول العربية وتدعيمه في مجال مكافحة جرائم تقنية المعلومات[2].

وجاءت مضامين الإتفاقية العربية المذكورة مطابقة لأحكام اتفاقية بودابست خاصة على مستوى القواعد الإجرائية، سواء من حيث نطاق التطبيق أو طبيعة هذه القواعد، حيث نصت على مجموعة من القواعد الإجرائية أوجبت على الدول الأطراف ملاءمتها مع قوانينها الوطنية فيما يتعلق بالأبحاث الجنائية كتدابير التحفظ على بيانات الكمبيوتر المخزنة وكشفها وإصدار الأوامر بتسليمها، وإجراءات التفتيش على المعلومات المخزنة وحجزها والتجميع الفوري لها واعتراض محتواها وذلك من خلال المواد من 23 إلى 29 من الاتفاقية[3].

هذا وقد تناولت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، الإختصاص من خلال المادة الثلاثون منها، حيث نصت على التزام كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في هذه الإتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت وذلك في الحالات التالية :

- في إقليم الدولة الطرف ؛

---

[1] تجدر الإشارة إلى انه كانت هناك مبادرة سابقة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تتمثل في القانون العربي الإسترشادي حيث اعتمد كل من مجلس وزراء العرب ومجلس وزراء الداخلية قانونا عربيا استرشاديا لمكافحة جرائم تقنية المعلومات وما في حكمها خلال سنة 2004 وذلك بهدف الاسترشاد به من طرف الدول العربية في وضع قوانينها الوطنية وملاءمتها مع أحكامه، إلا أن الملاحظ على مضامين القانون العربي الإسترشادي المذكور هيمنة القواعد الموضوعية المتعلقة بالتجريم والعقاب بشكل كبير حيث خصصت لها حوالي 25 مادة من أصل 27 مادة مكونة للقانون المذكور، باستثناء مادة فريدة تعرضت للاختصاص القضائي (المادة 26).

[2] وافق على هذه الاتفاقية مجلس وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة بجامعة الدول العربية بالقاهرة بتاريخ 21 دجنبر 2010

[3] هشام ملاطي، المرجع السابق، ص. 83

- على متن سفينة تحمل علم الدولة الطرف ؛

- على متن طائرة مسجلة تحت قوانين الدولة الطرف ؛

- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة ؛

- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

فالملاحظ من خلال مقتضيات الإتفاقية العربية المتعلقة بالإختصاص القضائي على أنها لم تخرج عن الضوابط التي أقرتها اتفاقية بودابست واعتمدت نفس ضوابط سريان الإختصاص القضائي على الجريمة الإلكترونية.

لذلك يمكن القول أن ما أرساه المنتظم الدولي من آليات إجرائية تشكل في حد ذاتها وسائل تأمينية للدول فيما بينها وتتفق وطبيعة هذا النوع من الإجرام من الناحية القانونية [1]، ومع خصوصية هذا النمط المستحدث من الجرائم وتساير وتنسجم مع الطبيعة الخاصة للجريمة الإلكترونية، وتطويرها بشكل يسمح بجعلها أكثر فعالية في مكافحة هذا الإجرام التقني العنكبوتي [2].

كل هذا جعل مجموعة من الدول تعيد بناء نصوصها الإجرائية بشكل يتناسب مع خصوصيات البحث والتحري في هذا النوع من الجرائم، وتبني قواعد إجرائية تسمح للأجهزة المكلفة بالبحث والتحري بالبحث عنها بطرق تلاءمها في إطار الشرعية الإجرائية، وإدراكا من هذه الدول بأن هذه الجرائم ترتكب بتقنيات حديثة في عالم يختلف عن العالم المادي كما سنقف عند ذلك عند حديثنا عن بعض نماذج الدول التي أفردت قواعد إجرائية خاصة للبحث عن الجريمة الإلكترونية من خلال المبحث الثاني.

[1] عفيفي كامل عفيفي، المرجع السابق، ص.337

[2] محمد جوهر، المرجع السابق، ص.16

المبحث الثاني : حدود ملاءمة القوانين المقارنة مع الآليات الإجرائية الدولية

إن دراستنا لهذا المبحث ستكون محاولة للوقوف عند نماذج بعض الدول الرائدة في ملاءمة قوانينها الوطنية مع مختلف القواعد والآليات الإجرائية التي تضمنتها الإتفاقيات الدولية وأرساها المنتظم الدولي من أجل ضبط الجريمة الإلكترونية والتصدي لها، لذلك ارتأينا الوقوف عند معرفة مدى ملاءمة بعض النماذج من التشريعات العربية مع الآليات الدولية (مطلب أول) ثم بعد ذلك الوقوف عند بعض النماذج من الدول الأجنبية (مطلب ثان).

المطلب الأول : ملاءمة بعض القوانين العربية مع الآليات الإجرائية الدولية

لازالت القواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية لم تجد لها موقعا في مختلف التشريعات العربية باستثناء بعض التشريعات التي كان لها السبق في إرساء قواعد إجرائية تتوافق وطبيعة الجريمة الإلكترونية، حيث أن مختلف القوانين العربية ما تزال تقتصر على القواعد الإجرائية العادية في مجال البحث عن الجريمة الإلكترونية.

لذلك سنحاول الوقوف عند النموذجين الجزائري (فقرة أولى) والأردني (فقرة ثانية) باعتبار أنهما أفردا بعض القواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية.

الفقرة الأولى : التشريع الجزائري

أصدر المشرع الجزائري القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[1] حيث أرسى قواعد إجرائية جديدة تستطيع معها أجهزة إنفاذ القانون ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم الإلكترونية[2]، إذ تضمن

[1] كانت هناك محاولة سابقة من المشرع الجزائري قبل صدور هذا القانون تتمثل في القانون 22/06 المعدل لقانون الإجراءات الجزائية الجزائري الذي حوى مجموعة من الإجراءات الجديدة لمكافحة أنواع محددة من الجرائم ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

[2] أحمد مسعود مريم، المرجع السابق، ص. 66

الفصل الثالث من هذا القانون القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن، حيث خول هذا القانون لأجهزة إنفاذ القانون الدخول والتفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي (المادة الخامسة)، كما سمح القانون المذكور باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها (المادة السادسة)، بالإضافة إلى الإلتزامات التي ألقاها هذا القانون على مقدمي الخدمات وذلك بمساعدة السلطات العمومية في مواجهة هذه الجرائم والكشف عن مرتكبيها وذلك من خلال الفصل الرابع من نفس القانون[1]، حيث فرض المشرع الجزائري من خلال المادتين 10 و 11من قانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على مقدمي الخدمات حفظ المعطيات بشكل يسمح بالتعرف على الأشخاص المساهمين في إنشاء المحتويات على الانترنيت وذلك من أجل التبليغات المحتملة للسلطات القضائية أو في حال طلب هذه الأخيرة لأجل التحريات أو المعاينات أو المتابعات القضائية للجرائم المرتكبة[2]، والقيام بحفظ المعطيات المتعلقة بحركة السير، منها المعطيات التي تسمح بالتعرف على مستعملي الخدمة وكذا الخصائص التقنية وتاريخ ووقت ومدة الإتصال.

كما عالج هذا القانون مسألة الإختصاص من خلال مقتضيات المادة 15 حيث نصت هذه المادة " على أنه زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني. "

[1] يوسف صغير، المرجع السابق، ص.114

[2] أحمد مسعود مريم، نفس المرجع، ص.100

علاوة على هذه الآليات الإجرائية التي تضمنها القانون 04/09، فقد تضمن قانون الإجراءات الجزائي الجزائري مجموعة من الآليات الخاصة بالتحريات والتحقيقات في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مثل الآلية المتعلقة باعتراض المراسلات (المواد من 65 مكرر 5إلى المادة 65 مكرر 10 من قانون الإجراءات الجزائري)، كما سمح بامتداد اختصاص الأجهزة المكلفة بالبحث والتحري إلى كامل الإقليم الوطني إذا تعلق الأمر بجريمة إلكترونية من خلال المادة 16 من قانون الإجراءات الجزائري على امتداد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني إذا تعلق الأمر ببحث ومعاينة لجرائم ماسة بأنظمة المعالجة الآلية للمعطيات، وكذا من خلال ما نصت عليه المادة 37 على جواز امتداد الاختصاص المحلي للنيابة العامة إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1].

الفقرة الثانية : التشريع الأردني

أصدر المشرع الأردني سنة 2010 قانونا أطلق عليه قانون جرائم أنظمة المعلومات، حيث يتضمن هذا القانون 17مادة موزعة بينما هو موضوعي وما هو إجرائي ويظهر من خلال استقراء مختلف المواد التي جاء بها قانون جرائم أنظمة المعلومات الأردني أنه خصص بعض مقتضيات المادة 12 منه للقواعد الإجرائية التي تسمح للأجهزة المكلفة بالبحث بإمكانية الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من جرائم ينص عليها القانون المذكور، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لإرتكاب أي من تلك الجرائم كما أعطت الفقرة الثانية من نفس المادة المذكورة الإمكانية لأجهزة البحث لضبط الأجهزة والأدوات

[1] تنص الفقرة ما قبل الأخيرة من المادة 16 من قانون الإجراءات الجزائري :

" غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية **والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني.

_ كما نصت المادة 37 : " يجوز تمديد الإختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية **والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف."

والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها القانون المذكور والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها[1].

كما تعرضت المادة 16 لمسألة الإختصاص حيث أعطت الصلاحية للقضاء الأردني إذا ارتكبت أي من الجرائم التي نص عليها قانون جرائم أنظمة المعلومات باستخدام أنظمة معلومات داخل الأردن أو ألحقت إضرار بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت أثار الجريمة فيها كليا أو جزئيا أو ارتكبت من أحد الأشخاص المقيمين فيها.

المطلب الثاني : ملاءمة بعض القوانين الأجنبية مع الآليات الإجرائية الدولية

سنحاول من خلال هذا المطلب الوقوف عند ما أرسته بعض الدول الأجنبية من قواعد إجرائية خاصة للبحث عن الجريمة الإلكترونية، تماشيا مع ما أقرته التوصية الأوروبية لسنة 1995 وكذا اتفاقية بودابست لسنة 2001، لذلك سنكتفي ببعض نماذج من الدول الرائدة في هذا المجال ونخص بالذكر، التشريعين البلجيكي(فقرة أولى) والفرنسي (فقرة ثانية).

الفقرة الأولى : التشريع البلجيكي

يعد القانون البلجيكي المتعلق بالجريمة الإلكترونية الصادر بتاريخ 28 فبراير 2000 نموذجا للقوانين الرائدة في مجال مكافحة الجرائم الإلكترونية، حيث تم تخصيص القسم الثالث بأكمله للمقتضيات الإجرائية المعدلة لقانون التحقيق الجنائي للقواعد الإجرائية للجرائم الإلكترونية.

---

[1] حيث جاء في المادة 12 من قانون جرائم أنظمة المعلومات لسنة 2010

أ – مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لإرتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لإرتكاب أي من تلك الجرائم.....

ب_ مع مراعاة الفقرة (أ) من هذه المادة.... يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لإرتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

فقد منح المشرع البلجيكي للنيابة العامة وقضاء التحقيق صلاحيات جد مهمة من قبيل نسخ المعطيات والبيانات المخزنة في حالة تعذر حجزها واتخاذ جميع التدابير لمنع الولوج لها مع إمكانية جعلها غير ممكنة الولوج متى شكلت البيانات المخزنة جريمة أو وسيلة لارتكاب الجريمة أو ماسة بالنظام العام أو الأخلاق الحميدة أو تشكل خطرا على سلامة الأنظمة المعلوماتية أو البيانات المخزنة [1]، وكذا أحقية قاضي التحقيق بإجراء بحث بنظام معلوماتي أو جزء منه المتواجد في مكان أخر إذا كان هذا الإجراء ضروري للوصول إلى الحقيقة أو مخافة ضياع وسائل الإثبات أو وجود خطر وكذا أخذ نسخ من البيانات إذا كانت غير موجودة على التراب البلجيكي[2]، إذ نصت المادة 88 من قانون التحقيق البلجيكي على أنه " إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو جزء منه، فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي أخر يوجد في مكان أخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقا لضابطين :

- إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث
- إذا وجدت مخاطر تتعلق بضياع الأدلة، نظرا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث[3].

---

[1] حيث جاء في الفقرة الثانية من المادة 39 مكرر من قانون التحقيقات الجنائية البلجيكي:

Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi ou l'auditeur du travail utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

L'Article 39 bis et l'alinéa 2 du paragraphe 3

[2] Florence de Villenfagne & Séverine Dusollier, op. cit, p.21

[3] وفيما يلي نص المادة 88 من قانون التحقيقات الجنائية البلجيكي باللغة الفرنسية :

كما سمح قانون التحقيق البلجيكي لقاضي التحقيق من خلال المادة 90 بأن يأمر أي شخص يفترض فيه بأن يكون على معرفة خاصة بخدمة الإتصالات والتي تكون موضوع الرصد أو الخدمات التي تسمح بحماية أو تشفير البيانات التي يتم تخزينها، والتي تمت معالجتها أو نقلها عن طريق نظام الكمبيوتر، بتوفير معلومات عن عملية من هذا النظام وكيفية الوصول إلى محتويات الإتصالات التي تم إرسالها، بطريقة مفهومة[1].

كما يمكن لقاضي التحقيق بتوجيه أمره لهؤلاء الأشخاص من أجل إتاحة محتوى هذه الإتصالات على الشكل الذي طلبت من أجله وتتبعها وذلك في حدود إمكانياتهم[2].

الفقرة الثانية : التشريع الفرنسي

كانت فرنسا[1] من الدول السباقة للتوقيع على اتفاقية بودابست وذلك بتاريخ 23 نونبر2001 [2]، لذلك سعى المشرع الفرنسي إلى ملاءمة قانون المسطرة الجنائية مع الآليات

1er. Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée :

- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et

- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

[1] وفيما يلي نص المادة 90 من قانون التحقيقات الجنائية البلجيكي :

Le juge d'instruction peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.

[2] Il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

والقواعد الإجرائية التي جاءت بها اتفاقية بودابست في مجال البحث عن الجريمة الإلكترونية [3]، كان من بينها القواعد التي تسمح بالتفتيش والحجز في البيئة الإلكترونية حيث نصت المادة 56 على أنه " في حالة ما إذا كانت الجريمة المرتكبة مما يمكن إثباته بواسطة معطيات أو وثائق معلوماتية توجد في حوزة الغير، فإنه يمكن لضابط الشرطة القضائية أن ينتقل إلى مقر هذا الأخير لإجراء تفتيش وتحرير محضر في الموضوع" [4]، كما نصت الفقرتين الخامسة والسادسة من المادة56 أيضا على أنه " يتم حجز المعطيات والبرامج المعلوماتية الضرورية لإظهار الحقيقة بوضع الدعامات المادية المتضمنة لهذه المعلومات رهن إشارة العدالة أو بأخذ نسخ منها بحضور الأشخاص الذين حضروا التفتيش[5]."

---

[1] عرفت فرنسا ترسانة من القوانين ذات الصلة بالجريمة الالكترونية والمعلوميات انطلاقا من قانون الحريات والمعلوميات1978 ، بالإضافة إلى قانون جودفران 5 يناير سنة 1988، وقانون 15 نونبر 2001 المتعلق بالسلامة اليومية وقانون 18 مارس 2003 المتعلق بالسلامة الداخلية

Voir - Emmanuelle Matignon, La cybercriminalité : un focus dans le monde des télécoms, Mémoire pour obtenir le master en droit du numérique administration- entreprises, université paris 1 panthéon-sorbonne, année universitaire 2011/2012, p. 42 et

Voir aussi – Ali Azzouzi, op.cit, p.135

[2] Yann padova, op.cit, p.777

[3] Eric A.carprioli, Les moyens juridique de lutte contre la cybercriminalité, revue risques n°5, juillet-septembre 2002, p.50-55

[4] وفيما يلي مقتضى هذه المادة باللغة الفرنسية:

Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal

[5] وفيما يلي المقتضى الكامل للفقرتين الخامسة والسادسة من المادة56

Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.

الفقرة الثانية من المادة 57-1 من قانون المسطرة الجنائية والتي سمحت صراحة بمباشرة بعض إجراءات البحث عن الجريمة الإلكترونية خارج الحدود الإقليمية كإمكانية تفتيش الأنظمة المعلوماتية المتصلة حتى ولو كانت متواجدة خارج إقليم الدولية، حيث سمحت المادة المذكورة لضباط الشرطة القضائية بأن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية[1].

كما سمحت المادة 60-1 لضابط الشرطة القضائية في أن يستدعي أي شخص لسماعه، إذا تبين له أن بوسع هذا الشخص أن يمده بمعلومات حول الأفعال أو الأشياء أو الوثائق أو المستندات أو المعطيات المعلوماتية أو الأشياء المحجوزة، وأن يرغمه على الحضور في حالة امتناعه بعد إذن النيابة العامة[2].

Si une copie est réalisée, il peut être procédé, sur instruction du procureur de la République, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

[1] حيث أضيفت هذه المادة بمقتضى المادة 17 من قانون الأمن الداخلي، وفيما يلي نص الفقرة الثانية من المادة 57-1 من قانون المسطرة الجنائية الفرنسي :

Article 57-1 :

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements.

[2] Article 60-1

L'officier de police judiciaire peut requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel

بالإضافة إلى بعض القواعد الإجرائية التي تضمنتها بعض القوانين الخاصة، كما هو الحال في القانون المتعلق بحرية الإتصال لسنة 2000 الذي فرض على مزودي الخدمات من خلال المادة 9-43 بضرورة اتخاذ تدابير للحفاظ على البيانات.[1]

هذه إذن كانت نظرة على بعض القوانين المقارنة وحدود ملاءمتها مع مختلف الآليات الإجرائية التي أرساها المنتظم الدولي، وعليه سنحاول من خلال الفصل الثاني الوقوف عند الوضع في قانون المسطرة الجنائية المغربي.

[1] Bertrand Warusfel, op.cit, p.4

الفصل الثاني : الإطار الإجرائي الوطني في مجال البحث عن الجريمة الإلكترونية

تعد إجراءات البحث والتحري أكثر إجراءات المسطرة الجنائية تأثرا بالتحولات العامة الإجتماعية والإقتصادية والتكنولوجية التي يعرفها محيطها القانوني[1]، لذلك فإن إجراءات البحث والتحري في الجريمة الإلكترونية أصبحت تتطلب قواعد حديثة على اعتبار أن البحث فيها أصبح يواجه تقنيات حديثة في أسلوب وطريقة ارتكابها.

فإذا كان النقاش والجدل الذي قسم رجال القانون والفقه إلى مؤيدين ومعارضين حول حدود كفاية القواعد الإجرائية العادية للبحث عن الجريمة الإلكترونية، ومدى إمكانية استحداث مقتضيات إجرائية جديدة مواكبة للمستجدات في المحيط العلمي والتقني، فإن دراستنا لهذا الفصل ستعرف نفس النقاش أيضا، حيث ستكون محاولة للوقوف عند معرفة حدود كفاية القواعد الإجرائية الواردة في قانون المسطرة الجنائية للبحث عن الجريمة الإلكترونية وضبطها، ومدى استيعاب وانسجام هذه القواعد مع مختلف الآليات الإجرائية التي أرساها المنتظم الدولي.

وعليه ارتأينا تقسيم هذا الفصل على الشكل التالي :

المبحث الأول : مدى قدرة القواعد الإجرائية الواردة في قانون المسطرة الجنائية على استيعاب شكليات البحث الخاصة عن الجريمة الإلكترونية

المبحث الثاني : مدى قدرة القواعد الإجرائية الواردة في قانون المسطرة الجنائية على استيعاب خصوصية التفتيش والحجز في الجريمة الإلكترونية

[1] أحمد ايت الطالب، المرجع السابق، ص.28

المبحث الأول : مدى قدرة القواعد الإجرائية الواردة في قانون المسطرة الجنائية على استيعاب شكليات البحث الخاصة عن الجريمة الإلكترونية

وعيا وإيمانا بأن القواعد الإجرائية العادية أبانت عن عدم كفايتها ومحدوديتها في التعامل مع الجريمة الإلكترونية، تم إيجاد مجموعة من الشكليات والتي تعتبر مستحدثة تهم البحث عن الجريمة الإلكترونية تضفي نوعا من الفعالية والخصوصية في مجال البحث عنها وتلاءم طبيعة هذه الجريمة، لذلك يقتضي منا ذلك معرفة مختلف هذه الشكليات ثم البحث في مدى قدرة القواعد الإجرائية الواردة في قانون المسطرة الجنائية على استيعاب هذه الشكليات الخاصة، وهذا ما سنحاول الوقوف عنده من خلال هذا المبحث وذلك على الشكل التالي:

المطلب الأول : تقييد البحث عن الجريمة الإلكترونية ببعض الشكليات الخاصة

المطلب الثاني : مدى استيعاب قانون المسطرة الجنائية لشكليات البحث الخاصة

المطلب الأول : تقييد البحث عن الجريمة الإلكترونية ببعض الشكليات الخاصة

أمام تميز الجريمة الإلكترونية عن باقي الجرائم الأخرى ظهرت الحاجة إلى اللجوء إلى أدوات وآليات مستحدثة للبحث عن الجريمة الإلكترونية (فقرة أولى) كما ظهرت الحاجة إلى تعاون بعض الجهات الخاصة مع الأجهزة المكلفة بالبحث والتحري في سبيل ضبطها والتصدي لها (فقرة ثانية).

الفقرة الأولى : الحاجة إلى شكليات خاصة من أجل البحث عن الجريمة الإلكترونية

إن البحث عن الجريمة الإلكترونية في بيئة رقمية تختلف عن البيئة التي اعتادت أجهزة إنفاذ القانون البحث والتحري فيها، أسهم في ظهور مجموعة من الإجراءات والتدابير المستحدثة للبحث عن الجريمة الإلكترونية تتناسب مع خصوصية وطبيعة هذا

النوع من الجرائم، وقد كان من بين هذه الإجراءات المستحدثة، إجراء التحفظ العاجل على البيانات والذي يعتبر إجراء أولي تمهيدي الهدف منه محاولة الإحتفاظ بالبيانات قبل فقدانها وضمان السرعة اللازمة للحفاظ على الأدلة المتعلقة بالجريمة الإلكترونية وتجميعها، لاسيما أن آثارها يمكن أن تندثر بسرعة وفي ظرف وجيز، فهو يتلاءم وطبيعة البيئة المعلوماتية من حيث قابلية البيانات فيها للمحو والفقد بسرعة[1].

ولما كان التحفظ العاجل والتجميع الفوري للمعطيات والبيانات يتطلب أحيانا اعتراض محتوى هذه البيانات الإلكترونية، فقد استحدثت آليات تعطي الصلاحية للسلطات المختصة في التجميع الفوري لبيانات الكمبيوتر من خلال جمع أو تسجيل أو إجبار مقدم الخدمة في نطاق قدرته الفنية على جمع أو تسجيل سير البيانات المرتبطة باتصالات معينة وكذا صلاحية الإعتراض على محتوى هذه البيانات.

فأمام هذه الشكليات المستحدثة التي تهم البحث عن الجريمة الإلكترونية كان لابد من وجود جهة معينة تتعاون مع الأجهزة المكلفة بالبحث والتحري وتزودهم بمختلف المعلومات التي قد تساعدهم في الوصول إلى الحقيقة وهذا ما سنحاول التطرق إليه من خلال الفقرة الثانية.

الفقرة الثانية : الحاجة إلى تعاون بعض الجهات الخاصة من أجل ضبط الجريمة الإلكترونية

إذا كان الأصل أن البيانات المتعلقة بمستخدمي الشبكة تدخل في إطار الحق في الخصوصية، فلا يجوز لمزود الخدمة أو غيره أن يقوم بإفشاء ما لديه من معلومات إلى الغير[2]، إلا أنه ولضمان البحث في مواجهة الأشخاص الذي يحوزون إحدى الوثائق أو البيانات المعلوماتية ظهرت إلى الوجود إجراءات وتدابير مستحدثة تفرض على مزودي الخدمات الإلكترونية التعاون مع الأجهزة المكلفة بالبحث عن الجرائم الإلكترونية وتضع إلتزاما على عاتق هؤلاء الأشخاص بتزويد هذه الأجهزة بكل المعلومات المفيدة التي يتوفرون عليها في سبيل إظهار الحقيقية.

[1] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي – في القانون الجزائري والقانون المقارن-، مطبعة دار الجامعة الجديدة، الإسكندرية، طبعة 2010، ص.159

[2] عائشة بن قارة مصطفى، المرجع السابق، ص. 161

كما ظهرت إجراءات تفرض على مزودي الخدمات بتسجيل والحفاظ على جميع البيانات المتعلقة بمستعملي خدماتهم في مدة معينة وتعطي للأجهزة المكلفة بالبحث والتحري بأن يأمروا مزودي الخدمات بتسليم ما تحت أيديهم من بيانات متعلقة بالمشترك وذلك من أجل إجراءات البحث والمتابعة الجنائية، وفي هذا الصدد جاء في إحدى حيثيات حكم صادر عن المحكمة الإبتدائية بباريس بتاريخ 30 يناير 2013 أن مزودي الخدمات ملزمون بحكم القانون بتمكين الجهات القضائية بالبيانات والمعطيات التي تدخل في إطار حوزتهم وذلك لأغراض بحث مدنية وجنائية، وأن الجهات المذكورة لا تتحمل أية مسؤولية قانونية مادام القانون الفرنسي والقوانين الأوروبية تجيز لها ذلك[1].

وعليه يمكن القول أن طبيعة الجريمة الإلكترونية أملت على الأجهزة المكلفة بالبحث عنها اللجوء إلى شكليات خاصة في سبيل الوصول إليها وضبطها، لكن السؤال الذي يبقى مطروحا وسنحاول الإجابة عليه من خلال المطلب الثاني مدى قدرة قانون المسطرة الجنائية على استيعاب مختلف هذه الشكليات الخاصة.

المطلب الثاني : مدى استيعاب قانون المسطرة الجنائية لشكليات البحث الخاصة

سنحاول من خلال هذا المطلب معرفة مدى استيعاب القواعد الإجرائية الواردة في قانون المسطرة الجنائية لمختلف الشكليات الخاصة والتي وقفنا عندها من خلال المطلب السابق، لذلك سيكون لزاما علينا الوقوف عند معرفة حدود استيعاب القواعد الإجرائية الواردة في قانون المسطرة الجنائية الحالي للشكليات الخاصة المتعلقة بالبحث عن الجريمة الإلكترونية (فقرة أولى) ثم بعد ذلك سنقف عند مدى انسجام القواعد الإجرائية الواردة في مسودة مشروع قانون المسطرة الجنائية مع هذه الشكليات على اعتبار أنها جاءت بمجموعة من المستجدات والتي تهم الجريمة الإلكترونية (فقرة ثانية).

[1] انظر عبد الحكيم الحكماوي، المرجع السابق، ص.152

الفقرة الأولى: حدود استيعاب قانون المسطرة الجنائية الحالي لشكليات البحث الخاصة عن الجريمة الإلكترونية

إن الهدف من خلال مختلف الشكليات الجديدة والتي تهم البحث عن الجريمة الالكترونية وإلزام بعض الجهات الأخرى بالتعاون مع أجهزة إنفاذ القانون، هو تسهيل عمل هذه الأجهزة للتصدي للجريمة الإلكترونية وضبط مرتكبيها.

وعليه، وبالرجوع إلى أحكام قانون المسطرة الجنائية نجده قد ألزم في المادة 57 ضباط الشرطة القضائية بالإنتقال في الحال إلى مكان إرتكاب الجريمة وإجراء المعاينات المفيدة والحفاظ على الأدلة القابلة للإندثار وعلى ما يمكن أن يساعد على إظهار الحقيقة.

لذلك اعتبر البعض على أنه وباستقراء مقتضيات المادة 57 من قانون المسطرة الجنائية يظهر أن هذا النص قد راعى عامل الزمن في جمع الأدلة المرتبطة بالجريمة، فوفقا لهذه المادة فإن ضابط الشرطة القضائية يتعين عليه أن ينتقل فورا إلى مكان إرتكاب الجريمة وأن يجري المعاينات اللازمة، وأن يحافظ على الأدلة القابلة للإندثار، وذلك بغض النظر عن طبيعة هذه الجريمة، علما بأن الجريمة الإلكترونية ينطبق عليها هذا الوصف لأنها يمكن أن ترتكب في وقت قصير، ثم تختفي معالمها بعد ذلك بسرعة[1]،

---

[1] الناجم كوبان، المرجع السابق، ص.108

_ فالملاحظ في هذا الطرح انه استند على القرار الصادر عن محكمة النقض والذي أشرنا إليه سابقا الذي جاء فيه " بأن البحث الذي أجرته الضابطة القضائية مع كل المتهمين تم إنجازه في إطار مسطرة التلبس لأن الجرائم المعلوماتية يصعب اكتشافها في حينها، وإنجاز البحث بشأنها يقتضي السرعة والدقة كي لا تندثر أثار الجريمة أو يتطور الضرر ويصبح من الصعب السيطرة عليه"

- كما أن نفس القرار اعتبر أن مدلول مدة الوقت القصير المنصوص عليها في الفقرة الثالثة من المادة56 من قانون المسطرة الجنائية لا تعني في الجرائم المعلوماتية بضع دقائق آو ساعات، طالما أن المجرم المعلوماتي يمكنه أن يرتكب جريمته من خارج الحدود على بعد آلاف الكيلومترات"

قرار رقم 1/681 المؤرخ في 3 غشت2011 ، الغرفة الجنائية القسم الأول، الملف عدد16080 /2010 ، غير منشور

كما اعتبروا أنه وبمقارنة المقتضيات الواردة في اتفاقية بودابست مع نظيرتها في قانون المسطرة الجنائية، فإن هناك تطابق ولو بشكل نسبي بين هذه المقتضيات[1].

إلا أن الملاحظ من خلال المادة 57 من قانون المسطرة الجنائية أنها لم تنص على ما يفيد التأكيد على سرعة حفظ البيانات، أو ما يلزم مزود الخدمة بالكشف عن البيانات، وعليه فإن كان مقتضى المادة 57 يوحي بأنه قد ينطبق على الجريمة الإلكترونية، إلا أنه يتحسن وضع مقتضيات خاصة بالجريمة الإلكترونية تفيد التأكيد على سرعة التحفظ على البيانات الإلكترونية وتلزم مزود الخدمة بالكشف عن هذه البيانات[2].

كما أنه وإن كان قانون المسطرة الجنائية يتضمن بعض المقتضيات التي تتعلق بجمع أو تسجيل الإتصالات، حيث نص المشرع المغربي ضمن أحكام المادة 114 من قانون المسطرة الجنائية على السماح أثناء القيام بعمليات إلتقاط الإتصالات المأذون بها وتسجيلها وأخذ نسخ منها وحجزها، بإمكانية الحصول على المعلومات والوثائق الضرورية للتعرف على الإتصال الذي سيتم إلتقاطه من أي مستغل لشبكة عامة أو مصلحة للإتصالات، فإنها تبقى قاصرة لإرتباطها بمسطرة إلتقاط المكالمات والإتصالات المنجزة عن بعد، والمتعلقة بجرائم لا تدخل ضمن زمرتها الجريمة الإلكترونية، زيادة على ارتباطها

[1] هشام ملاطي، المرجع السابق، ص. 87

[2] وإن كان الثابت أنه لا يوجد ما يفيد إلزام مقدم الخدمة على تقديم بيانات تتعلق بالمشترك، فإن الملاحظ من خلال حيثيات الحكم القضائي الصادر عن المحكمة الابتدائية بسلا والمشار إليه سابقا، لجوء الشرطة القضائية إلى شركة اتصالات المغرب من اجل إفادتها بمعلومات تتعلق بالمشترك حيث جاء في حيثيات هذا الحكم "..... وأن الشركة تمكنت من تحديد عناوين يتم داخلها إجراء هذا النوع من المكالمات الهاتفي المقرصنة باستعمال خط هاتفي ثابت، وبناء عليه تم الانتقال إلى العنوانين المذكورين..."

- كما جاء في حيثيات الحكم الصادر عن المحكمة الإبتدائية بالرباط ".... وبعد مراسلة الضابطة القضائية لشركة اتصالات المغرب للتعرف على صاحب العنوان الخاص بالانترنيت الذي هو ip2141140156 جاء عن تلك الشركة بأن صاحب ذلك العنوان هو احد صاحب الرقم الهاتفي عنوان سكناه حي المغرب العربي المسيرة 2، وعلى اثر هذه المعطيات انتقلت الضابطة إلى العنوان أعلاه...."
- حكم جنحي ابتدائي رقم 806، صادر بتاريخ 2010/06/14، ملف جنحي تلبسي رقم21/10/733 ، 21/10/758

بسلطات قضائية محددة في شخص قاضي التحقيق والرئيس الأول لمحكمة الإستئناف والوكيل العام للملك لديها[1].

كما يظهر عدم التطابق بين الشكليات الخاصة في مجال البحث عن الجريمة الإلكترونية والمتعلقة بصلاحية السلطات المختصة في التجميع الفوري لبيانات الكمبيوتر من خلال جمع أو تسجيل أو إجبار مقدم الخدمة في نطاق قدرته الفنية على جمع أو تسجيل سير البيانات المرتبطة بإتصالات معينة وصلاحية الإعتراض على محتوى هذه البيانات، وقواعد قانون المسطرة الجنائية إذ يتضح من خلال الرجوع إلى أحكام قانون المسطرة الجنائية أنها لم تنظم آليتي التجميع والإعتراض على البيانات، بل الأبعد من ذلك ذهب المشرع المغربي إلى تجريم كل اعتراض للبيانات ضمن أحكام الفصلين 232 و448 من مجموعة القانون الجنائي[2].

مما يتعين معه وضع مقتضيات تعطي للجهة المشرفة على البحث إمكانية اعتراض محتوى البيانات والتجميع الفوري لهذه البيانات وتلزم مزودي الخدمات بتقديم المعلومات المطلوبة في الوقت المناسب[3].

الفقرة الثانية : انسجام مسودة مشروع قانون المسطرة الجنائية مع شكليات البحث الخاصة

لقد حاول واضع مسودة مشروع قانون المسطرة الجنائية[4] أن يحقق من خلال المقتضيات التي جاء بها نوعا من الإنسجام مع مختلف الشكليات الخاصة في مجال البحث عن الجريمة الإلكترونية، لذلك عرفت مسودة هذا المشروع بعض القواعد

---

[1] هشام ملاطي، المرجع السابق، ص. 89

[2] هشام ملاطي، نفس المرجع، ص.90

-كما انه وبالرجوع إلى المادة 26 من القانون الصادر في 7 غشت 1997 المتعلق بالبريد والمواصلات نجدها تنص على انه " يتعين على متعهدي الشبكات العامة للمواصلات وعلى مقدمي خدمات المواصلات وعلى مستخدميهم احترام سرية الخطابات المنقولة عبر وسائل المواصلات وشروط الحماية الخاصة والمعلومات الشخصية للمستفدين، تحت طائلة العقوبات التي حددتها المادة 92 من نفس القانون ".

[3] الناجم كوبان، المرجع السابق، ص. 113

[4] أعلنت وزارة العدل عن النسخة الأولى لمسودة مشروع قانون المسطرة الجنائية بتاريخ 08 ماي 2014، والنسخة الثانية بتاريخ 17 نونبر2014

الإجرائية الجديدة والتي بإمكانها أن تساعد أجهزة إنفاذ القانون في البحث عن الجريمة الإلكترونية وضبطها، حيث خولت المادة 60 من المسودة لضابط الشرطة القضائية في أن يستدعي أي شخص لسماعه، إذا تبين له أن بوسع هذا الشخص أن يمده بمعلومات حول الأفعال أو الأشياء أو الوثائق أو المستندات أو المعطيات المعلوماتية أو الأشياء المحجوزة، وأن يرغمه على الحضور في حالة امتناعه بعد إذن النيابة العامة.

فالملاحظ من خلال هذه المادة أن واضع مسودة المشروع قد جاء بمقتضى جديد يمكن من خلاله استدعاء أي شخص في وسعه التعاون مع السلطات المشرفة على البحث من كل المعلومات التي يتوفر عليها واللازمة لسير أعمال البحث والتحري عن الجريمة الالكترونية المرتكبة، فهذا المقتضى يمكن أن ينطبق أيضا على مزودي الخدمات باعتبارهم أيضا يحوزون مستندات ومعطيات معلوماتية من شأنها المساعدة في البحث.

كما خولت المادة 108من مسودة المشروع للوكيل العام للملك إذا اقتضت ذلك ضرورة البحث، أن يلتمس كتابة من الرئيس الأول لمحكمة الاستئناف إصدار أمر بالتقاط المكالمات الهاتفية أو الإتصالات المنجزة بوسائل الاتصال عن بعد وتسجيلها وأخذ نسخ منها أو حجزها وذلك إذا كانت الجريمة موضوع البحث تمس بالجرائم الماسة بنظام المعالجة الآلية للمعطيات.[1]

غير أنه يجوز للوكيل العام للملك في حالة الاستعجال القصوى بصفة استثنائية أن يأمر كتابة بالتقاط المكالمات الهاتفية أو الاتصالات المنجزة بوسائل الاتصال عن بعد

[1] حيث جاء في نص المادة 108من مسودة مشروع قانون المسطرة الجنائية"يمكن للوكيل العام للملك إذا اقتضت ذلك ضرورة البحث، أن يلتمس كتابة من الرئيس الأول لمحكمة الاستئناف إصدار أمر بالتقاط المكالمات الهاتفية أو الاتصالات المنجزة بوسائل الاتصال عن بعد وتسجيلها وأخذ نسخ منها أو حجزها وذلك إذا كانت الجريمة موضوع البحث تمس بأمن الدولة أو جريمة إرهابية أو جريمة منظمة أو تتعلق بالعصابات الإجرامية أو بالقتل أو التسميم أو بالاختطاف وأخذ الرهائن أو بتزييف أو تزوير النقود أو سندات القرض العام أو بالمخدرات والمؤثرات العقلية أو بالأسلحة والذخيرة والمتفجرات أو بحماية الصحة أو بغسل الأموال أو بالرشوة أو استغلال النفوذ أو الغدر أو اختلاس أو تبديد المال العام، أو بالجرائم الماسة بنظام المعالجة الآلية للمعطيات، والجرائم ضد الإنسانية والاتجار بالبشر."

وتسجيلها وأخذ نسخ منها وحجزها متى كانت ضرورة البحث تقتضي التعجيل خوفا من اندثار وسائل الإثبات، إذا تعلق الأمر بالجرائم الماسة بنظام المعالجة الآلية للمعطيات.

ويظهر من خلال مقتضيات المادة 108 من مسودة مشروع قانون المسطرة الجنائية، أن المشرع تدارك النقص الموجود في المادة 108 الحالية وذلك بالسماح للوكيل العام للملك بإمكانية إصدار أمر بالتقاط المكالمات الهاتفية أو الاتصالات المنجزة بوسائل الاتصال عن بعد وتسجيلها وأخذ نسخ منها أو حجزها سواء بعد اخذ إذن من رئيس المحكمة أو دون إذن لذلك عند الاستعجال وذلك إذا كانت الجريمة موضوع البحث تمس بالجرائم الماسة بنظام المعالجة الآلية للمعطيات.

إلا أن الملاحظ أن واضع مسودة مشروع قانون المسطرة الجنائية احتفظ بالمادة 57بشكلها الحالي ولم يشر إلى إمكانية التحفظ العاجل على البيانات أو ما يفيد التأكيد على سرعة حفظ هذه البيانات[1].

المبحث الثاني : مدى استيعاب القواعد الإجرائية الواردة في قانون المسطرة الجنائية لخصوصية التفتيش والحجز في الجريمة الإلكترونية

إن دراستنا لهذا المبحث سنحاول من خلالها الوقوف عند خصوصية الشكليات التي تطبع التفتيش والحجز في الجريمة الإلكترونية، ثم بعد ذلك سنعمل على تقريب وضعية القواعد الإجرائية الواردة في قانون المسطرة الجنائية ومدى قدرتها على استيعاب خصوصية هذه الشكليات.

[1] كما أن الانتقال الوارد في المادة 57 والذي يمكن أن يقوم به ضابط الشرطة القضائية هو انتقال يتم في العالم المادي، على خلاف الجريمة الالكترونية فإن الانتقال إلى مسرح الجريمة يعد من الموضوعات المستجدة، ذلك أن مسألة الانتقال هذه قد لا تكون بالضرورة عبر العالم المادي وإنما عبر العالم الافتراضي فتستطيع أجهزة إنفاذ القانون أن تقوم بالمعاينة من خلال المكان الذي توجد فيه من خلال جهاز الكمبيوتر الخاص بها، وعليه فإن مسألة الانتقال المادي إلى محل ارتكاب الجريمة لا تشكل عائقا أمام أجهزة البحث والتحقيق، وإنما المشكلة تكون من خلال الانتقال في العالم الافتراضي حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال أثار الجريمة.

ومن تم ارتأينا تقسيم هذا المبحث على الشكل التالي :

المطلب الأول: خصوصية التفتيش والحجز في الجريمة الإلكترونية

المطلب الثاني : التفتيش والحجز في الجريمة الإلكترونية في ظل قواعد قانون المسطرة الجنائية

المطلب الأول : خصوصية التفتيش والحجز في الجريمة الإلكترونية

سنحاول من خلال هذا المطلب الوقوف عند الخصوصيات التي تطبع التفتيش عن الجريمة الإلكترونية (فقرة أولى) وكذا الخصوصية التي تطبع الحجز فيها (فقرة ثانية) وذلك من خلال استعراض مختلف الإتجاهات وموقفها من مدى صلاحية مكونات جهاز الحاسوب للتفتيش والحجز.

الفقرة الأولى : خصوصية التفتيش عن الجريمة الإلكترونية

إن الأصل في التفتيش أنه إجراء يستهدف ضبط أشياء مادية تتعلق بجريمة معينة أو تفيد في كشف الحقيقة، وغايته دوما هي الحصول على الدليل المادي، وهذا ما يتنافر مع الطبيعة غير المادية لبرامج وبيانات الكمبيوتر، بإعتبارها مجرد برامج وبيانات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي[1].

وقد اختلف رجال الفقه والقانون حول مدى إمكانية تطبيق القواعد الإجرائية التقليدية أو تقرير قواعد جديدة للتفتيش عن الدليل الإلكتروني، فالإتجاه الأول اعتبر أن الأمر لا يحتاج إلى تقرير قواعد جديدة للتفتيش عن الدليل الإلكتروني وذلك لكفاية القواعد التقليدية لمواجهة هذه الأحوال أيا كانت الوسيلة المستخدمة لإرتكاب الجريمة سواء كانت تقليدية أو كان غالبا عليها الطابع الفني التقني حيث يمكن إثباتها عن طريق الإلتجاء إلى الفنيين المختصين في هذا الصدد[2].

أما الإتجاه الثاني فقد اعتبر أن تفتيش نظام معلومات الحاسب إجراء يندرج ضمن التفتيش بمعناه القانوني وبالتالي يخضع لأحكامه ومنها الشروط الواجب توفرها

[1] نبيلة هبة هروال، المرجع السابق، ص. 223

[2] عفيفي كامل عفيفي، المرجع السابق، ص.364

فيه مع نوع من الخصوصية تتماشى مع نوع الجريمة المراد جمع الأدلة بشأنها وكذا البيئة الإفتراضية التي تتعامل معها الأجهزة التي قامت بذلك الإجراء [1].

في حين أن الإتجاه الثالث اعتبر أن مكونات الحاسوب لا تصلح أن تكون بطبيعتها صالحة للتفتيش، على اعتبار أن التفتيش يهدف في المقام الأول إلى ضبط أدلة مادية وهذا يستلزم وجود أحكام خاصة تكون أكثر ملاءمة لهذه البيانات اللامحسوسة عبر التدخل التشريعي، وذلك من أجل تقرير القواعد والضوابط القانونية الكفيلة للتغلب على مختلف الصعوبات الإجرائية التي تثار عند تفتيش الأنظمة المعلوماتية، من خلال إجراء تعديلات على نصوص القوانين التي ترى في التفتيش وسيلة لجمع الأدلة المادية، بحيث يصبح هدف التفتيش جمع أية بيانات معالجة أليا، بالإضافة إلى جمع الأدلة المادية[2].

فبإستقراء هذا الإختلاف الحاصل بين الإتجاهات تبقى الحاجة لوضع قواعد خاصة تحكم تفتيش البيانات المعالجة إلكترونيا، بدلا من محاولة تطويع القواعد التقليدية وتوسيع نطاقها وهذا لا يتأتى إلا من خلال إجراء تعديل عليها لجعلها تتلاءم ومتطلبات الجريمة الإلكترونية.

الفقرة الثانية : خصوصية الحجز في الجريمة الإلكترونية

لما كان الحجز في الجريمة الإلكترونية يرد على أشياء ذات طبيعة غير مادية [3]، فقد أثار هذا الحجز الذي يترتب على أعمال التفتيش والواقع على بيانات ومعطيات الكمبيوتر مجموعة من الإشكالات، ذلك أن هذا الإجراء وإن كان يمكن تصور وقوعه بالنسبة لمكونات الكمبيوتر المادية وشبكاته حيث يمكن رصد الاتصالات التي تتم خلالها وتسجيل محتوياتها، فإن اتخاذه سيكون في منتهى الصعوبة بالنسبة لمكونات الحاسوب المعنوية[4]، لذلك اختلف الفقه كما هو الحال في التفتيش كما رأينا ذلك سابقا، حول مدى إمكانية

[1] نبيلة هبة هروال، المرجع السابق، ص. 228

[2] الناجم كوبان، المرجع السابق، ص.84

[3] عائشة بن قارة مصطفى، المرجع السابق، ص.114

[4] الناجم كوبان، نفس المرجع، ص. 96

حجز الأدلة الإلكترونية [1] والتي تتميز بأنها ذات طبيعة معنوية، بين اتجاه اعتبر من غير المتصور أن يرد الحجز على بيانات الحاسوب الإلكترونية لإنتفاء الكيان المادي عنها، وأن هذا الإجراء لا يمكن أن يتم إلا في حالة إذا تجسد في دعامات مادية، واتجاه ثان لا يرى مانعا في أن يرد الحجز على بيانات إلكترونية، واتجاه ثالث دعا إلى ضرورة تدخل تشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الحجز لتشمل إلى جانب الأشياء المادية الأشكال المختلفة للبيانات الإلكترونية[2].

المطلب الثاني : التفتيش والحجز في الجريمة الإلكترونية في ظل قواعد قانون المسطرة الجنائية

إن دراستنا لهذا المطلب سنحاول من خلالها معرفة مدى استيعاب القواعد الإجرائية الواردة في قانون المسطرة الجنائية الحالي للشكليات المتعلقة بالتفتيش والحجز في الجريمة الإلكترونية (فقرة أولى)، ثم بعد ذلك سنحاول الوقوف عند حدود انسجام القواعد الإجرائية الواردة في مسودة مشروع قانون المسطرة الجنائية مع الشكليات المتعلقة بالتفتيش والحجز في الجريمة الإلكترونية (فقرة ثانية).

الفقرة الأولى : مدى استيعاب قانون المسطرة الجنائية الحالي لشكليات التفتيش والحجز في الجريمة الإلكترونية

لقد وقفنا من خلال المطلب السابق عند الخصوصية التي تطبع التفتيش والحجز في الجريمة الإلكترونية، لذلك فإن الحديث عن مدى استيعاب القواعد الإجرائية الواردة في قانون المسطرة الجنائية للخصوصية التي تطبع التفتيش والحجز في الجريمة الإلكترونية قد قسم رجال القانون إلى اتجاهين:

---

[1] وإن كانت المادة 19 من اتفاقية بودابست جاءت صريحة في هذا الصدد وأعطت الصلاحية لسلطة كل دول طرف في أن تتخذ الإجراءات التي تمكنها من حجز نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر وأن تحافظ على سلامة تلك المعلومات المخزنة.

[2] نبيلة هبة هروال، المرجع السابق، ص.265

_ انظر أيضا هشام محمد فريد رستم، المرجع السابق، ص.93 وما يليها

فالإتجاه الأول اعتبر أن مقتضيات المادتين59 و 60من قانون المسطرة الجنائية نصت على قواعد إجرائية يمكن أن تستوعب كمبدأ عام حتى الجريمة الإلكترونية[1] وأن هناك تطابق مع ما نصت عليه المادة 19 من اتفاقية بودابست [2]، حيث أن المادة 60 من قانون المسطرة الجنائية نصت على مقتضيات عامة تنظم التفتيش كإجراء تخضع له كافة الجرائم بغض النظر عن طبيعتها بما فيها الجريمة الإلكترونية، في حين منحت المادة 59 من نفس القانون لسلطات البحث والتحري صلاحية حجز الأوراق والوثائق أو أشياء أخرى في حوزة الأشخاص أو الأشياء المتعلقة بالأفعال الإجرامية[3].

في حين اعتبر الإتجاه الثاني أن المادة59 بشكلها الحالي لا تفي بالمطلوب لأنها مادة قاصرة فقط على الوثائق، والحال أنه يتعين اعتماد صيغة تشمل جميع الوثائق بما في ذلك الرقمية وبالتالي إتاحة إمكانية الولوج إلى الوسائط الإلكترونية والتحفظ على البيانات واستغلال مضامينها في البحث لإعتمادها كأدلة عند الإقتضاء[4]، لأنه وفي غياب إطار قانوني خاص يسمح بالولوج إلى النظام المعلوماتي ويحدد الشروط التي يمكن معها الدخول إليها وإجراء التحريات اللازمة فيها بحثا عن المعطيات المفيدة للبحث فيمكن القول بأن قانون المسطرة الجنائية لا يتضمن استجابة صريحة لمتطلبات البحث وتفتيش قواعد المعطيات الآلية كما وأنه من الصعب اعتبارا لسكوت قانون المسطرة الجنائية عن تنظيم حجز المعطيات غير المادية وفي غياب نص صريح القبول بتسجيل أو تحميل المعطيات الرقمية دون اللوازم أو أجزاء الحاسب التي وجدت فيها[5].

---

[1] الناجم كوبان، المرجع السابق، ص.105

[2] حيث أن المادة 19 من اتفاقية بودابست المرتبطة بتفتيش وحجز بيانات الكمبيوتر المخزنة، أوصت بضرورة تامين عملية التفتيش والدخول على أي نظام كمبيوتر أو أي جزء منه والبيانات المخزنة فيه وضمان عملية البحث أو الدخول المماثل بسرعة على نظام لكمبيوتر أخر أو جزء منه موجود في مكان أخر بإقليم الدولة، زيادة على منح السلطات المختصة صلاحية الحجز والتامين للبيانات واخذ نسخة منها والاحتفاظ بها أو جعلها غير قابلة للدخول عليها أو حذفها من النظام.

[3] هشام ملاطي، المرجع السابق، ص.88 و89

[4] حفيظ الزايدي، المرجع السابق، ص.176

[5] أحمد ايت الطالب، المرجع السابق، ص.30 و32و35

وأمام تضارب هذه الإتجاهات فإن الإتجاه الأخير يبقى الأقرب للصواب[1]، إلا أنه وتجاوزا للجدل الدائر حول مدى إمكانية إجراء التفتيش والحجز بقواعد تقليدية في بيئة افتراضية غير محسوسة، ونظرا لسكوت قانون المسطرة الجنائية الحالي عن تنظيم تفتيش وحجز البيانات غير المادية، فإنه يتعين على المشرع المغربي اعتماد صيغة تشمل كيفية التفتيش والحجز إذا تعلق الأمر بجريمة إلكترونية[2]، وتتيح إمكانية تفتيش الأجهزة

[1] وما يزكي هذا الاتجاه : حيث انه في غياب نص قانوني يسمح بإمكانية تفتيش جهاز الكمبيوتر وحجز الأدلة الالكترونية الموجودة فيه، فان الأجهزة المكلفة بالبحث والتحري لا زالت في تعاملها مع الجريمة الالكترونية تلجأ للقواعد التقليدية، وتلجأ للتفتيش والحجز بمفهومه المادي، حيث جاء في حيثيات الحكم الصادر عن المحكمة الابتدائية بالرباط ".....حجزت الضابطة القضائية من المنزل المذكور المكترى مجموعة من الحواسيب ومعدات الكترونية في حالة تشغيل عاينت الضابطة القضائية بها مجموعة من المقاطع لمواد إباحية لعدة أشخاص..."
".....ودلها على الحاسوب وقامت الضابطة القضائية بفتح بعض الملفات الظاهرة على مكتب الحاسوب فاتضح لها أنها تتوفر على مشاهد اباحية كما دلها على مكان وجود مقطع الفيديو الخاص بالضحية ففتحته الضابطة القضائية وأجرت معاينة له وحجزت الحاسوب....."
_حكم صادر عن المحكمة الابتدائية بالرباط بتاريخ 2013/12/09، تحت عدد 1967، ملف جنحي تلبسي رقم 2105/1866/2013، غير منشور

- في نفس السياق جاء أيضا في حيثيات الحكم الصادر عن المحكمة الإبتدائية بالرباط المشار إليه سابقا "..... تقدم عناصر الشرطة القضائية من باب الشقة وقاموا بطرقه حيث فتح لهم المتهم وبعد إجراء تفتيش بأرجاء الشقة بحضوره المتواصل تكمنوا من حجز وحدتين مجهولتين النوع ووحدتين محمولتين لتخزين المعطيات المعلوماتية من نوع "لاسي" ومجموعة من الأقراص المدمجة...." حكم جنحي ابتدائي رقم 806، صادر بتاريخ 2010/06/14، ملف جنحي تلبسي رقم 21/10/733 ، 21/10/758

[2] وإن كان البعض قد اقترح صيغة جديدة للمادة 59 على الشكل التالي " إذا كان نوع الجنائية او الجنحة مما يمكن إثباته بحجز أوراق او وثائق او بيانات تتضمنها وسائط الكترونية أو أشياء أخرى في حوزة أشخاص يظنوا أنهم شاركوا في الجريمة، او يحوزون مستندات او وسائط الكترونية او أشياء تتعلق بالأفعال الإجرامية، فان ضابط الشرطة القضائية ينتقل فورا إلى منزل هؤلاء الأشخاص ليجري فيه طبقا للشروط المحددة في المادتين 60 و62 تفتيشا يحرر محضر بشأنه
غير انه إذا تعلق الأمر بحجز وسائط الكترونية يجوز لضابط الشرطة القضائية أن يستعمل هو او من يساعده كل التقنيات التي تمكنه من الولوج إلى تلك الوسائط ولو دون إذن أصحابها مع حفظ حق الغير حسن النية والتحفظ على البيانات التي تحويها لاعتماد الأدلة..... (الباقي دون تغيير)"
_ انظر في هذا الصدد حفيظ الزايدي، المرجع السابق، ص.176

أو الأنظمة المعلوماتية، وحجز البيانات والوثائق الإلكترونية على غرار ما فعلت بعض القوانين المقارنة، كقانون المسطرة الجنائية الفرنسي[1] الذي نص من خلال المادة 56 على أنه " في حالة ما إذا كانت الجريمة المرتكبة مما يمكن إثباته بواسطة معطيات أو وثائق معلوماتية توجد في حوزة الغير، فإنه يمكن لضابط الشرطة القضائية أن ينتقل إلى مقر هذا الأخير لإجراء تفتيش وتحرير محضر في الموضوع"، كما نصت الفقرتين الخامسة والسادسة من المادة56 أيضا على أنه " يتم حجز المعطيات والبرامج المعلوماتية الضرورية لإظهار الحقيقة بوضع الدعامات المادية المتضمنة لهذه المعلومات رهن إشارة العدالة أو بأخذ نسخ منها بحضور الأشخاص الذين حضروا التفتيش"

الفقرة الثانية : انسجام مسودة مشروع قانون المسطرة الجنائية مع شكليات التفتيش والحجز في الجريمة الإلكترونية

لقد حاول واضع مسودة مشروع قانون المسطرة الجنائية إدخال تعديلات بشكل يجعل إجراءات التفتيش والحجز تتسع لتشمل حتى البيانات والوثائق والأدوات والمعطيات المعلوماتية، حيث جاء في المادة 59 من هذه المسودة على أنه "إذا كان نوع الجناية أو الجنحة مما يمكن إثباته بحجز أوراق ووثائق أو أشياء أخرى في حوزة أشخاص يظن أنهم شاركوا في الجريمة، أو يحوزون مستندات أو وثائق أو معطيات أو أدوات معلوماتية أو أشياء تتعلق بالأفعال الإجرامية...."[2]

[1] كما سمح قانون جرائم أنظمة المعلومات الأردني لسنة 2010 من خلال مقتضيات المادة 12 منه للأجهزة المكلفة بالبحث بإمكانية الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من جرائم ينص عليها القانون المذكور، والقيام بتفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم كما أعطت الفقرة الثانية من نفس المادة المذكورة الإمكانية لأجهزة البحث لضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها القانون المذكور والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

[2] الملاحظ من خلال هذا المقتضى أن واضع مسودة مشروع قانون المسطرة الجنائية قد تبنى نفس الصيغة المنصوص عليها المادة 56 من قانون المسطرة الجنائية الفرنسي :

Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés,

كما أعطت نفس المادة الصلاحية بالتفتيش في جميع الأماكن التي يمكن أن يعثر بها على مستندات أو وثائق أو معطيات معلوماتية أو أشياء مفيدة في إظهار الحقيقة.

كما نصت المادة 60 إذا كان التفتيش سيجرى في منزل شخص من الغير يحتمل أن يكون في حيازته وثائق أو مستندات أو معطيات معلوماتية أو أشياء لها علاقة بالأفعال الإجرامية، فإنه يجب حضور هذا الشخص لعملية التفتيش، وإذا تعذر ذلك وجب أن يجري التفتيش طبقا لما جاء في الفقرة السابقة.

أما فيما يخص حجز المعطيات والبيانات الإلكترونية والتي قد تشكل دليلا لإثبات الجريمة فقد نصت المادة 59 من مسودة المشروع على أنه :" يتم حجز المعطيات والبرامج المعلوماتية الضرورية لإظهار الحقيقة بوضع الدعامات المادية المتضمنة لهذه المعلومات رهن إشارة العدالة أو بأخذ نسخ منها بحضور الأشخاص الذين حضروا التفتيش توضع رهن إشارة العدالة[1].

لا يحجز ضابط الشرطة القضائية إلا المستندات أو الوثائق أو المعطيات أو الأدوات المعلوماتية أو الأشياء المفيدة في إظهار الحقيقة."

وهكذا نلاحظ أن واضع مسودة مشروع قانون المسطرة الجنائية ومن خلال هذه التعديلات، قد وضع حدا للجدل الذي كان دائرا حول مدى إمكانية تفتيش الكمبيوتر وحجز الأدلة غير المادية، والمتمثلة في بيانات ومعطيات الكمبيوتر المعنوية استنادا إلى قواعد المسطرة الجنائية التقليدية من خلال الإنتصار لصالح الإتجاه الذي كان ينادي بضرورة التنصيص صراحة على قابلية بيانات ومعطيات الكمبيوتر للتفتيش والحجز، وذلك لعجز النصوص التقليدية وقصورها عن استيعابها.

---

l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal

[1] نفس الشيء يمكن قوله من خلال هذا المقتضى، أن واضع مسودة مشروع قانون المسطرة الجنائية قد تبنى نفس الصيغة المنصوص عليها في الفقرة الخامسة المادة 56 من قانون المسطرة الجنائية الفرنسي :

Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.

غير أن ما يعاب على هذه التعديلات، أن المشرع لم يحدد ما إذا كان بإمكان أجهزة إنفاذ القانون تفتيش الحواسيب وحجز البيانات والمعطيات الموجودة في مكان أخر غير مكان البحث الأصلي والمفيدة لإظهار الحقيقة، حيث غالبا ما يخزن المجرمون صورا غير مشروعة من الأفعال ليس في حواسيبهم الخاصة فحسب، بل أيضا في مواقع التخزين الواقعة في مكان آخر، على غرار ما فعلت بعض التشريعات المقارنة كالمشرع البلجيكي من خلال المادة 88 من قانون التحقيق البلجيكي[1] والتي تنص على أنه " إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو جزء منه، فان هذا البحث يمكن أن يمتد إلى نظام معلوماتي أخر يوجد في مكان أخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقا لضابطين :

-إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث

- إذا وجدت مخاطر تتعلق بضياع الأدلة، نظرا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث[2].

وكذا ما نصت عليه الفقرة الثانية من المادة 57-1 من قانون المسطرة الجنائية الفرنسي والتي سمحت صراحة بمباشرة بعض إجراءات البحث عن الجريمة الإلكترونية خارج الحدود الإقليمية كإمكانية تفتيش الأنظمة المعلوماتية المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، حيث سمحت المادة المذكورة لضباط الشرطة القضائية بأن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية[3].

---

[1] كما أن اتفاقية بودابست خولت هذه الإمكانية، حيث سمحت للدول الأطراف بان يمتد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال وذلك من خلال الفقرة الثانية من المادة19.

[2] Florence de Villenfagne & Séverine Dusollier, op. cit, p. 20

[3] وفيما يلي نص الفقرة الثانية من المادة 57-1 من قانون المسطرة الجنائية الفرنسي :

Article 57-1 :

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du

ختاما فقد كانت هذه الدراسة مناسبة حقيقية لإبراز بعض جوانب النقص التي تعترض البحث عن الجريمة الإلكترونية، حيث كانت محاولة للوقوف عند مدى إمكانية الإكتفاء بالقواعد الإجرائية العادية في مجال البحث عن الجريمة الإلكترونية وحدود قدرة هذه القواعد فعلا على ضبط الجريمة الإلكترونية التي تتميز بصعوبة ضبطها وترتبط بمفاهيم عدة منها مفهوم الخصوصية ومفهوم الشرعية وذلك لرفع اللبس عن مجموعة من الإشكالات التي تعترض الجهات المكلفة بالبحث عن الجريمة الإلكترونية وكذا مختلف جهات إنفاذ القانون ولو في الدول التي كانت سباقة إلى وضع قواعد قانونية تنظم آليات البحث عن الجريمة الإلكترونية.

وقد رأينا من خلال هذه الدراسة أن القواعد الإجرائية في البحث عن الجريمة الإلكترونية لم تنل حظها من الإهتمام داخل التشريع المغربي، فإذا كان المشرع المغربي قد حاول وضع تشريع جنائي يعنى بتجريم مختلف الأفعال التي تشكل جرائم إلكترونية فإنه لم يخصص الجريمة الإلكترونية بأية قواعد إجرائية خاصة وتركها خاضعة للقواعد الإجرائية الواردة في قانون المسطرة الجنائية، حيث كان من المستحسن أن تأتي في إطار نص قانوني خاص أو بموجب قانون معدل للقانون الجنائي والمسطرة الجنائية معا في آن واحد.

كما أنه لا بد من التشديد على صعوبة التحديات الإجرائية التي تعترض البحث في الجرائم الإلكترونية وكذا التحديات والإشكاليات الإجرائية التي يطرحها موضوع الإختصاص في هذا النوع من الجرائم وتقديم المخالفين أمام القضاء لإنفاذ القانون في مواجهتهم باعتبار الطابع العابر للحدود للجريمة وهو ما بات يستدعي بالإضافة إلى الآليات التشريعية إيجاد مقاربات وطنية تقوم على مبادئ التعاون الدولي لملاحقة مقترفي هذه الجرائم.

territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements.

لائحة المراجع

❖ باللغة العربية

- **الكتب**

▪ **الكتب العامة**

-أحمد الخمليشي، شرح قانون المسطرة الجنائية، الجزء الأول، مطبعة المعارف الجديدة-الرباط، الطبعة الخامسة، 1999

-عبد اللطيف بوحموش، دليل الشرطة القضائية في تحرير المحاضر وتوثيق المساطر، مطبعة الأمنية-الرباط، الطبعة الثالثة،2013

-كوثر أحمد خالند، الإثبات الجنائي بالوسائل العلمية، مكتب التفسير للإعلان والنشر، أربيل العراق، طبعة 2007

-محمد الإدريسي العلمي المشيشي، المسطرة الجنائية، الجزء الأول، المؤسسات القضائية، منشورات جمعية تنمية البحوث والدراسات القضائية، 1991

▪ **الكتب الخاصة**

-جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية القاهرة، الطبعة الأولى 1998

-سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنيت، دار النهضة العربية-القاهرة، الطبعة الأولى1999

-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي – في القانون الجزائري والقانون المقارن-، مطبعة دار الجامعة الجديدة، الإسكندرية، طبعة 2010

-عبد الفتاح بيومي حجازي، الإثبات في جرائم الكمبيوتر والأنترنيت، دار الكتب القانونية-القاهرة، طبعة 2007

-عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية-دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية-، دار الكتب القانونية-القاهرة، الطبعة الأولى 2007

-عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الرقمية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت-لبنان، الطبعة الثانية 2007

-فريد منعم جبور، حماية المستهلك عبر الأنترنيت ومكافحة الجرائم الإلكترونية-دراسة مقارنة،منشورات الحلبي، بيروت -لبنان، الطبعة الأولى2010

-مصطفى محمد مرسي، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة-القاهرة، الطبعة الأولى 2008

-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنيت في مرحلة جمع الإستدلالات-دراسة مقارنة، دار الفكر الجامعي الإسكندرية، الطبعة الأولى 2007

-هشام محمد فريد رستم، الجوانب الإجرائية في الجريمة المعلوماتية-دراسة مقارنة- ، مكتبة الآلات المدنية-أسيوط، طبعة 1994

-هلالي عبد الإلاه أحمد، اتفاقية بودابست لمكافحة الجريمة المعلوماتية معلق عليها،دار النهضة العربية القاهرة، الطبعة الأولى 2007

- **<u>الرسائل الجامعية</u>**

- الناجم كوبان، الإثبات الجنائي في الجرائم المعلوماتية، رسالة لنيل دبلوم الماستر في العلوم القانونية، وحدة القانون الجنائي وحقوق الإنسان، كلية العلوم القانونية والاقتصادية والاجتماعية- جامعة محمد الخامس أكدال، الموسم الجامعي 2010-2011

- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، جامعة قاصدي مرباح ورقلة - الجزائر، سنة 2013

- يوسف صغير، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، جامعة مولود معمري-تيزي وزو-الجزائر، سنة 2013

- **مجلات ومقالات**

-أحمد ايت الطالب، تقنيات البحث وإجراءات المسطرة المتبعة في جرائم الأنترنيت والمعلوميات، مجلة الملف، العدد 9، نونبر 2006

-إدريس النوازلي، قراءة في الجريمة السيبيرية على ضوء الإتفاقية الأوروبية، مجلة المحاكم المغربية، العدد 104، شتنبر- أكتوبر 2006

-حفيظ الزايدي، الآليات القانونية والإجرائية للحد من أثار الجريمة الإلكترونية على الإئتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014

-عبد الحكيم الحكماوي، الإثبات في الجريمة الإلكترونية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014

-عبد الرحمان اللمتوني، الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014

-محمد العسكري، خصوصيات الإثبات في الجرائم المعلوماتية، مجلة القضاء والتشريع، وزارة العدل وحقوق الإنسان التونسية، العدد 7، جويلية 2005

-محمد جوهر، خصوصية زجر الإجرام المعلوماتي، مجلة الملف، العدد 9، نونبر 2006

-نزيهة مكاري، وسائل الإثبات في جرائم الاعتداء على حق المؤلف عبر الانترنيت، مجلة المناهج القانونية، عدد مزدوج 13/14_2009

-نور الدين الواهلي، الإختصاص في الجريمة الإلكترونية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014

-هشام ملاطي، خصوصية القواعد الإجرائية للجرائم المعلوماتية-محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية-، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014.

- **ندوات**

-إيهاب ماهر السنباطي، الجرائم الإلكترونية: قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد!، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 يونيو2007، المملكة المغربية

- جان فرونسوا هرنوت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 يونيو2007، المملكة المغربية

-عبد الرزاق سندالي، التشريع المغربي في مجال الجرائم المعلوماتية، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20يونيو2007، المملكة المغربية

-كريستينا سكولمان، المعايير الدولية المتعلقة بجرائم الانترنيت (مجلس أوروبا)، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 يونيو 2007، المملكة المغربية

-موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول: المعلوماتية والقانون، 28-29 أكتوبر 2009، طرابلس-ليبيا

En Français

باللغة الفرنسية

- Les ouvrages

- Ali El Azzouzi, La cybercriminalité au Maroc, Bishops solutions-Casablanca, juin 2010
- Myriam Quéméner &Yves charpenel, cybercriminalité – droit pénal appliqué- Economica paris France, 2010

- Les mémoires

- Emmanuelle Matignon, La cybercriminalité : un focus dans le monde des télécoms, Mémoire pour obtenir le master en droit du numérique administration- entreprises, université paris 1 panthéon-sorbonne, année universitaire 2011/2012

- Enderlin Clément, Les moyens juridique et institutionnels nationaux et européens de lutte contre la cybercriminalité dans le cyberspace, Mémoire de recherche Diplôme Universitaire Sécurité intérieure / extérieure dans l'union européennes, institut d'études politiques de Strasbourg, 2010-2011
- Jean-François Tyrode, Eléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercriminalité en droit européen, Mémoire pour obtenir le master en droit de l'internet public-administration-entreprise, Université paris 1, année universitaire 2006-2007

- Les Articles

- Bertrand Warusfel, Procédure pénale et technologie de l'information/de la convention sur la cybercriminalité à la loi sur la sécurité quotidienne, Revue droit et défense, Numéro 2002/1
- Eric A.carprioli, Les moyens juridique de lutte contre la cybercriminalité, revue risques n°51, juillet-septembre 2002, p.50-55
- Florence de Villenfagne & Séverine Dusollier, la Belgique sort enfin ses armes contre la cybercriminalité : a propos de la loi du 28 novembre 2000 sur la criminalité informatique, droit et nouvelles technologies ,16 Mars 2001
- Lionel Thoumyre, Une Europe unie face à la réglementation de l'internet ? _ Etat des lieux_, droit et nouvelles technologies, 26 septembre
- Yann padova, Un aperçu de la lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénal comparé, N°4 octobre-décembre 2002

- Les sites internet

http://bu.univ-ouargla.dz
http://www.caprioli-avocats.com
http://conventions.coe.int
http://www.courdecassation.fr
http://www2.droit.parisdescartes.fr
http://www.droit-technologie.org/
http://www.legalis.net

http://www.legifrance.gouv.fr
http://www.lepetitjuriste.fr
ftp://pogar.org
http://www.univparis1.fr
http://www.ummto.dz
http://www.vho.org

الفهرس