جامعة القاضي عياض
كلية العلوم القانونية والإقتصادية والإجتماعية
مراكش

ماستر العلوم الجنائية والأمنية
الفصل الأول
الفوج الرابع

عرض حول موضوع:

البحث والتحقيق في الجرائم المعلوماتية

من إنجاز الطلبة:

- عمر الموريف
- محمد حولمدة
- مريم الوكضي
- محمد أضرضور
- نجوى خلفي

تحت إشراف الدكتور:
ضياء علي أحمد نعمان

السنة الجامعية:
2018-2017

مقدمة

عرف العالم في العقود الأخيرة ثورة من نوع آخر همت مجال الاتصال والمعلومات وذلك نتيجة للتطور الذي تمثل أساسا في الاستعمال الواسع لأجهزة الحواسيب ذات المستوى العالي، والتي غالبا ما يتم ربطها بالشبكة العنكبوتية، وببرامج جد متقدمة، إذ مكنت من تحطيم الحواجز بين الأفراد والدول، وأتاحت مجالا واسعاً لتبادل المعطيات والمعلومات، بل حتى للتفاوض وإبرام العقود المختلفة التي تترجم غالبيتها على أرض الواقع.

وطبيعي أن الجريمة – باعتبارها ظاهرة اجتماعية- تتأثر من حيث النوع والحجم بالتحولات الاقتصادية والاجتماعية والثقافية، إن على المستوى الوطني أو الدولي، ونظرا لهذا التطور الذي أشرنا إليه سلفا، فقد ظهر للوجود نمط جديد من الإجرام تجسد بصفة أساسية فيما يسمى بالجريمة المعلوماتية، والتي اكتست من خلالها الجريمة بُعداً جديداً من حيث أدوات تنفيذها، وذلك باستغلال المجرمين أوجه التقدم العلمي والتكنولوجي في تعزيز أهدافهم غير المشروعة، واستغلوا درايتهم بهذه التكنولوجيا فتدخلوا بطريقة غير مشروعة في العلميات المالية والمصرفية بغرض الإثراء بطريق الغش، وذلك بتحويل مبالغ مالية ضخمة لمصالحهم الشخصية[1] ، بل وتتعدى الدوافع كل هذا لتكون فقط من أجل الرغبة في إثبات الذات، والتحدي وإرضاء لرغبات ذات تعاني من جنون العظمة.

وقد أدى ظهور الجرائم المعلوماتية إلى خلق تحديات كثيرة في مواجهة النظام القانوني القائم في العديد من الدول[2]، سيما لما باتت تشكله من خطر يمس أمن المجتمعات وسلامتها ومكتسباتها الأخلاقية، الأمر الذي دفع بالمجتمع الدولي إلى البحث عن آليات جديدة تتلاءم وطبيعتها، وتطوير الوسائل التقليدية بما يكفل تضامن جهود الدول وأجهزتها القائمة بمهمة مكافحة الجرائم المعلوماتية، ولعل أن أول السبل للتصدي لهذا النوع من الجرائم هو إجراءات البحث والتحقيق التي تشكل لبنة أساسية ضمن صرح الكشف عنها ومتابعة مرتكبيها، وزجرهم بما يحقق الردعين العام والخاص، دون الإخلال طبعا بضمانات المحاكمة العادلة.

---

1 ذ عبد الله العلوي البلغيثي مقال له بعنوان " الإجرام المعاصر أسبابه وأساليب مواجهته " منشور بكتاب: السياسة الجنائية بالمغرب: واقع وآفاق" المجلد الأول، الأعمال التحضرية للمناظرة الوطنية التي نظمتها وزارة العدل بمكناس أيام 09 و 10 و 11 دجنبر 2004، منشورات جمعية نشر المعلومة القانونية والقضائية، سلسلة الندوات والأيام الدراسية عدد 3، ط 3 ،س 2004، ص 222.

2 نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع عمان، ط 1 ،س 2008، ص 14.

ولعل ما تطرحه مسألة البحث والتحقيق في الجرائم المعلوماتية هو أن التحري عنها يثير نوعا من الصعوبات، ويفرز العديد من الإشكالات نظرا لأن إعمال قواعد البحث والتحقيق في بيئة رقمية يختلف عما هو عليه في البيئة العادية التي اعتادت أجهزة المكلف بالبحث والتحقيق إنفاذ القانون فيها وفق القواعد العادية، وهذا ما أسهم في ظهور مجموعة من الإجراءات والتدابير المستحدثة المناسبة لهذا النوع من الجرائم، ويعد تنوع المؤسسات المنوط بها مهمة البحث والتحقيق، ومحاولة جعل مقتضيات مشروع المسطرة الجنائية تواكب هذا التطور من أبرز هذه الإجراءات التي يتم العمل على تنزيلها التنزيل الأمثل .

❖ تحديد الإطار المفاهيمي:

من خلال عنوان العرض، فإنه من اللزام علينا تحديد المفاهيم التي تتضمنها كلماته، وبالتالي تحديد مفهوم البحث ثم التحقيق وكذا الجريمة المعلوماتية:

ـ البحث: ويمكن تعريف إجراءات البحث بكونها تلك الإجراءات التي تنظم التحريات، والتي تتولاها الشرطة القضائية سواء في حالة التلبس بالجريمة أو في الأحوال العادية، الغاية منها كشف الجرائم وجمع أدلة إثباتها[3].

ـ التحقيق: يتمثل في تلك الإجراءات التي تأتي بعد توجيه الاتهام إلى من يجرى التحقيق معه، فهي بهذا المعنى تتم ضد شخص متهم قانونا بارتكاب الجريمة موضوع التحقيق، وهذا ما يجعلها تمس غالبا بحرية الظنين وحقوقه فيرغم عن طريق القوة العمومية على الحضور إن امتنع، وتوجه إليه التهمة، ويستنطق، ويصدر الأمر بإلقاء القبض عليه واعتقاله إلى غير ذلك من إجراءات التحقيق[4].

ـ الجريمة المعلوماتية: ولكون الجرائم المعلوماتية ظاهرة حديثة لارتباطها بتكنولوجيا الحاسوب، فقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعتها لكن بدون جدوى حتى قيل أن الجريمة المعلوماتية تقاوم التعريف، لذا اختلفت التعاريف التي تناولت هذه الظاهرة من الإجرام فمنها من تناولها بالتعريف على نحو ضيق، ومنها من عرفها على نحو واسع، ومع ذلك تبقى هذه التعاريف قاصرة عن الإحاطة بأوجه ظاهرة الإجرام المعلوماتي، وقد تبنى المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا للجرائم المعلوماتية بأنها "كل جريمة يمكن ارتكابها

3 الحبيب البيهي، شرح قانون المسطرة الجنائية الجديد، منشورات المجلة المغربية للإدارة المحلية التنمية، سلسلة مؤلفات وأعمال جامعية، مطبعة المعارف الجديدة الرباط، ط 1 ،س 2004، ص 98.

4 أحمد الخمليشي، شرح قانون المسطرة الجنائية الجزء الأول، دار نشر المعرفة للنشر والتوزيع الرباط، مطبعة المعارف الجديدة الرباط، ط 6،س 1999، ص 157.

بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة اليكترونية". ويعد هذا التعريف من أفضل التعريفات التي تناولت ظاهرة الإجرام المعلوماتي إذ شمل الجانبين المادي والمعنوي للحاسوب ومنها شبكة الانترنيت، كما لم يقتصر على كون الحاسوب محلا للاعتداء ، بل أيضًا بوصفه وسيلة للاعتداء وارتكاب الجرائم[5].

❖ أهمية الموضوع:

ـ الأهمية القانونية: ذلك لما تتسم به إجراءات البحث والتحقيق من خصوصيات تمتاز بها عن الجرائم العادية، وما يمكن أن يفرزه البحث في هذا الموضوع من استقراء للنصوص الحالية المنظمة للبحث والتحقيق، ومحاولة إبراز مكامن القوة والخلل فيها متى تم إعمالها في مجال هذا النوع من الجرائم التي نحن بصدد الحديث عنها.

ـ الأهمية الاجتماعية والاقتصادية وذلك لارتباط الجريمة المعلوماتية بهذين الميدانين بشكل وطيد، نتيجة لما تلحقه من خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية، ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع يؤثر بشكل سلب على الاقتصاد والبنية المجتمعية ككل.

❖ الإشكال

إن الغوص في موضوع البحث والتحقيق في الجرائم المعلوماتية يدفعنا إلى التساؤل حول **ماهية هذه الإجراءات المعمول بها في مجال الجريمة المعلوماتية؟** وهذا الإشكال هو يفرض علينا أيضا طرح التساؤلات الفرعية التالية:

- **إلى أي حد استطاعت القواعد التقليدية للبحث والتحقيق استيعاب هذا النوع من الجرائم؟**
- **هل تم اعتماد آليات وأساليب أخرى حديثة قمينة بتحقيق الفعالية المطلوبة ؟**
- **هل تمكنت كل الإجراءات المتاحة حاليا من حل مشكلة الإثبات المرتبطة بالخصوصية التي يمتاز بها مجال البحث والتحقيق في الجرائم المعلوماتية؟**

❖ المنهج المتبع

5 كوثر فرام: الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية التدريب الملحقين القضائيين الفوج 42 2007-2009 ،، ص 5 و 6.

للإلمام بمختلف الجوانب والنقاط التي سيعالجها الموضوع، للإجابة عن الأسئلة التي يتركب منها الإشكال الذي سبقت الإشارة إليه، فإننا سنعمد على تبنى منهج قائم على التحليل والمقارنة، ومستندين على ما توصلنا إليه من عمل قضائي واجتهاد فقهي، للوقوف على خصوصيات البحث والتحقيق في الجرائم المعلوماتية، وما يعرفه هذا المجال من إشكالات عملية.

❖ الإعلان عن التصميم

التساؤلات التي طرحناها أعلاه سنحاول الإجابة عنها قدر الإمكان في هذا العرض المتواضع من خلال الاعتماد على التصميم التالي:

المبحث الأول: خصوصية البحث والتحقيق في الجرائم المعلوماتية

المطلب الأول: الأجهزة المكلفة بالبحث والتحقيق

الفقرة الأولى: على الصعيد الدولي

- أولا: منظمة الأنتيربول (الشرطة الجنائية الدولية)
- ثانيا: هيئة الأيكان: ICANN

الفقرة الثانية: على الصعيد الوطني

- أولا: أجهزة الشرطة القضائية
- ثانيا: المؤسسات غير القضائية

المطلب الثاني: إجراءات البحث والتحقيق في الجرائم المعلوماتية

الفقرة الأولى : اكتشاف الجرائم والتبليغ عنها وتحديد خطة البحث (العمل) .

- أولا : اكتشاف الجرائم المعلوماتية والتبليغ عنها .
- ثانيا : تحديد خطة البحث .

الفقرة الثانية : إجراءات البحث والتحقيق في الجرائم المعلوماتية .

- أولا : المعاينة .
- ثانيا : التفتيش .
- ثالثا : الحجز.

المبحث الثاني: صعوبات التحقيق وإشكالية الإثبات في الجرائم المعلوماتية

المطلب الأول:صعوبات البحث والتحقيق في الجرائم المعلوماتية

الفقرة الأولى: الصعوبات المرتبطة بإجراءات البحث والتحقيق في الجرائم المعلوماتية

- أولا:صعوبات مرتبطة بالدليل

1- غياب الدليل المرئي:

2- افتقاد الآثار التقليدية:

3- صعوبة الوصول إلى الدليل:

4- سهولة إخفاء الدليل؛

5- كثافة البيانات المتعين فحصها؛

- ثانيا:صعوبات مرتبطة بجهات التحري

1-إخفاء الجريمة

2-عدم التبليغ

3-نقص خبرة الجهات المختصة

4-صعوبة التعاون الدولي

الفقرة الثانية:الصعوبات المتعلقة بإشكالية الاختصاص

- أولا:موقف الاتفاقيات

1-اتفاقية بودابست

2-الاتفاقية العربية

- ثانيا:موقف التشريعات المقارنة والوطنية

1-المشرع الفرنسي

2-المشرع المغربي

المطلب الثاني:الأدلة وإشكالية الإثبات

الفقرة الأولى: الدليل الرقمي في الجرائم المعلوماتية

- أولا: التعريف بالدليل الرقمي
- ثانيا: تقسيمات الدليل الرقمي
- ثالثا: خصائص الدليل الجنائي الرقمي

الفقرة الثانية: وسائل الإثبات التقليدية ودورها في الجرائم المعلوماتية

- أولا: بعض الوسائل التقليدية ودورها في الجرائم المعلوماتية

1 - الشهادة

2 - الخبرة

- ثانيا: الإثبات الجنائي في البيئة المعلوماتية بين الحرية والتقييد

1 - مدى حرية الإثبات في الجريمة التقليدية المقترفة بوسيلة معلوماتية

2 - ارتباط تقييد الإثبات في الميدان الجنائي بالجريمة المعلوماتية

خاتمة.

المبحث الأول: خصوصية البحث والتحقيق في الجرائم المعلوماتية

يختلف البحث والتحقيق في الجرائم المرتكبة في بيئة معلوماتية عن تلك المتعلقة بالجرائم العادية، هذه الخصوصية التي سنحاول تنولها من خلال الإشارة إلى الأجهزة المكلفة بالبحث والتحقيق في الجرائم المعلوماتية (المطلب الأول)، وذلك قبل التطرق إلى إجراءات بالبحث والتحقيق الخاصة بالجرائم المعلوماتية (المطلب الثاني).

المطلب الأول : الأجهزة المكلفة بالبحث والتحقيق

سنخصص هذه المطلب للحديث عن الأجهزة المكلفة بالبحث والتحقيق سواء على المستوى الدولي أو الوطني:

الفقرة الأولى : على الصعيد الدولي

أولا : الانتربول

الإنتربول Interpol : هي اختصار لكلمة الشرطة الدولية بالإنجليزية International : Police)والاسم الكامل لها هو منظمة الشرطة الجنائية الدولية) بالإنجليزية International : Criminal Police Organization). وهي أكبر منظمة شرطة دولية أنشئت في عام 1923 مكونة من قوات الشرطة لـ 190 دولة[6] و تقع الأمانة العامة للإنتربول في ليون (فرنسا)، وتعمل على مدار الساعة، طيلة أيام السنة. ولدى المنظمة أيضا سبعة مكاتب إقليمية في العالم، ومكتب يمثلها لدى الأمم المتحدة في نيويورك وآخر يمثلها لدى الاتحاد الأوروبي في بروكسل. ولدى كل بلد من البلدان الأعضاء مكتب مركزي وطني يعمل فيه موظفو إنفاذ قانون وطنيون على مستوى عال من الكفاءة والتدريب[7] من خلاله تسعى الدول إلى مكافحة الجريمة المنظمة التي تتميز بكونها عابرة للحدود الجغرافية عبر مد جسر التعاون الدولي على الصعيد الأمني واللوجستيكي بينها , وتعزيزا لهذا التعاون جاءت الاتفاقية الدولية ببودابست الخاصة بمحاربة الجريمة الالكترونية سنة 2001، التي نصت على مجموعة من القواعد الخاصة بالتعاون الدولي والمقررة ضمن أحكام المواد من 23 الى 35, كما أبانت الدول العربية على اهتمامها بخصوصية الجرائم المعلوماتية فأنشأت فيما بينها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في سنة 2011

6 منظمة-الشرطة-الجنائية-الدولية https://ar.wikipedia.org/wiki/ تاريخ الزيارة 2017/12/23)،

7 (https://www.interpol.int تاريخ الزيارة 2017/12/23),

نصت على إمكانية التعاون الدولي فيما بينها ضمن المواد 30 إلى 41 من الاتفاقية وكل هذا خول لمنظمة الانتربول محاربة الجرائم المعلوماتية على الصعيد الدولي وخاصة ما يتعلق بجرائم الإرهاب الالكتروني و تزوير و تزييف بطائق الدفع و كذا جرائم غسل الأموال الذي يتم عبر استخدام الشبكة العنكبوتية وغيرها من الجرائم المعلوماتية الأخرى التي تشكل جرائم عابرة للحدود و التي تستدعي التعاون على الصعيد الدولي.

كما تعمل الانتربول على تعزيز الوعي بأهمية استخدام تقنيات التحقيق و مواكبة كل التطورات التكنولوجية لأجهزة الشرطة القضائية الخاصة بالدول الأعضاء كما تم إحداث مجموعة من الاتفاقيات مع الشركات المزودة للأنترنت في العالم للمساهمة في الحد من عواقب الجريمة الالكترونية. وبناء عليه فانه لابد من الإشارة إلى دور بعض الهيئات المستقلة التي تساهم في محاربة الجريمة المعلوماتية لفعالية أبحاثها و مساعدتها للأطراف المتضررة من دول و حكومات متعاقبة .

ثانيا : هيئة الأيكان ICANN

الأيكان هي اسم مختصر لهيئة الانترنت للأسماء والأرقام المخصصة INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS و هي منظمة غير ربحية تم تأسيسها دوليا سنة 1988 يقع مقرها بمدينة كاليفورنيا بالولايات المتحدة الأمريكية أسندت إليها مسؤولية توزيع مجالات العناوين في بروتوكول الانترنت IP ADRESS و تخصيص معرفات البرتوكول و إدارة نظام السجلات المواقع العامة عالية المستوى وسجلات المواقع عالية المستوى لرمز الدولة كما أنها تضطلع بمسؤولية وظائف إدارة نظام الخوادم المركزية[8].

تلعب هيئة الأيكان دورا داعما في مجال مكافحة الجريمة المعلوماتية من خلال توفير جل المعلومات الاليكترونية التي تحتاجها الدول سواء على صعيد الوكالات أو الأجهزة الحكومية أو على صعيد التعاون الدولي – الشرطة الدولية – كما تشارك الهيئة في دراسة و تحليل وتحديد الاستخدام غير المشروع للنطاقات على شبكة الانترنت ، إضافة إلى مساهمتها في دعم تحديث الخطط الأمنية للبنوك التي تشرف على مواقعها وكدا حل النزاعات المتعلقة بأسماء المواقع UDRPحيث تم استخدامها لحل أكثر من 5000 نزاع على حقوق و أسماء المواقع الاليكترونية[9]

8 (arcive.ican.org) تاريخ الزيارة 2017/12/23

9 (arcive.ican.org) تاريخ الزيارة 2017/12/23)

ذلك تكريسا للجهود المبذولة للمحافظة على الاستقرار الاقتصادي و السياسي للدول مما جعل منها ابرز مثال على التعاون بين العناصر المختلفة لمجتمع الانترنت.

ومما لا شك فيه أن التعاون الدولي لمكافحة الجريمة الالكترونية من خلال المنظمات الدولية الخاصة بهذا المجال لها تأثير كبير في الحد ولو نسبيا من ظاهر ة تؤرق الدول و تؤثر على سياستها الاقتصادية و الاجتماعية ولتكون هته الأخيرة مواكبة للتحركات الدولية لمحاربة الجريمة المعلوماتية لابد للقوانين المعمول بها وطنيا أن تنسجم مع المقتضيات الدولية وهذا ما حاول المشرع المغربي تجسيده في تشريعاته الخاصة بالأجهزة المكلفة بمكافحة الجريمة المعلوماتية.

الفقرة الثانية : على الصعيد الوطني

أولا : الأجهزة القضائية

1 - الشرطة القضائية

إن آليات البحث في الجرائم المعلوماتية تختلف عن الآليات الإجرائية للبحث في الجرائم العادية غير أن المشرع المغربي ورغم محاولاته في اعتماد أجهزة متخصصة في الجريمة المعلوماتية نجده لازال يعتمد على نفس أجهزة البحت والتحقيق في الجرائم العادية فبرجوعنا إلى المادة 18 من المادة قانون المسطرة الجنائية نجده أسندت مهام البحث والتحقيق إلى عناصر الشرطة القضائية و التي تضم حسب المادة 19 من نفس القانون على أن "الشرطة القضائية بالإضافة إلى الوكيل العام للملك ووكيل الملك ونوابهما و قاض التحقيق بوصفهم ضباطا سامين للشرطة القضائية

أولا : ضباط الشرطة القضائية .

ثانيا : ضباط الشرطة القضائية المكلفين بالأحداث.

ثالثا : أعوان الشرطة القضائية .

رابعا : الموظفون و الأعوان الذين ينيط بهم القانون بعض مهام الشرطة القضائية "

من خلال المادة 19 أعلاه نستشف منها أن جهاز الشرطة القضائية ينتمون باختلاف مناصبهم و مهامهم إلى مختلف الأجهزة الأمنية التي تتداخل فيما بينها لتشكل منارة لحماية أسس العدالة الجنائية ومنهم نجد :

المنتمون إلى سلك القضاء وهم : " الوكيل العام للملك ونوابه ووكيل الملك ونوابه و قاض التحقيق بوصفهم ضباطا سامين للشرطة القضائية " ثم المنتمون إلى أسلاك الإدارة العامة للأمن الوطني و الدرك الملكي ووزارة الداخلية .

ومن خلالها يحمل كل المنتمون إلى هاته الأجهزة صفة ضباط الشرطة القضائية حسب المادة 20 من قانون المسطرة الجنائية وتحديد اختصاصاتهم حسب المادة 21 من قانون المسطرة الجنائية ونطاق مزاولة وظيفتهم حسب المادة 22 من قانون المسطرة الجنائية .

2 - الفرقة الوطنية للشرطة القضائية

وبناءا على نص المادة 22/1 من قانون المسطرة الجنائية تم "إنشاء الفرقة الوطنية للشرطة القضائية تتألف من ضباط للشرطة القضائية ينتمون إلى جهات إدارية مختلفة يرأسها ضابط للشرطة القضائية تعينه النيابة العامة المختصة لهذا الغرض"، ويتواجد مقرها بالدار البيضاء وقد عنيت هته الفرقة بمختلف الجرائم الماسة بالأمن الداخلي والخارجي للدولة ، كما أحدثت مؤخرا سنة 2016 فرق جهوية تابعة للفرقة الوطنية بأربع مدن بالمملكة وهي الرباط وفاس ومراكش والعيون ويكون اختصاصها جميع القضايا المحالة عليها متن طرف السلطات القضائية كلما اقتضتها ضرورة البحث وطبيعة الجريمة كملفات الفساد المالي والأموال العامة وقضايا الاتجار في المخدرات و التحقيقات مع رجال الأمن المشتبه بهم[10].

3 -المكتب المركزي للأبحاث القضائية (BCIJ/البسيج)

المكتب المركزي للأبحاث القضائية (أو إف بي اي المغرب) هو مكتب تابع للمديرية العامة لمراقبة التراب الوطني ، تأسس في سنة 2015 وفقا لقرار مشترك بين وزارة الداخلية ووزارة العدل تنفيذا للتعليمات الملكية السامية في إطار تعزيز الحكامة الأمنية الجيدة جعل مقره في مدينة سلا[11]، أنيطت به معالجة الملفات الكبرى كمحاربة الخلايا الإرهابية و الاتجار بالمخدرات و

10 www. Maghress.com) تاريخ الزيارة 2017/12/24

11 المكتب-المركزي-للأبحاث-القضائية/https://ar.wikipedia.org

الاختطاف و حجز الرهائن والقتل والتسميم وجرائم الماسة بأمن الدولة الداخلي و الخارجي وباعتبار الجرائم المعلوماتية تدخل في نطاق جرائم الإرهاب طبقا للمادة 218 الفقرة 3 من مجموعة القانون الجنائي يعتبر هذا المكتب من بين الجهات المختصة بالبحث ومكافحة الجريمة المعلوماتية بالمغرب أسوة بالفرقة الوطنية بالدار البيضاء.

4 - المديرية العامة للأمن نظم المعلومات

تم إحداث المديرية العامة للأمن نظم المعلومات و المعروفة اختصارا ب (DGSSI) والتي أسند إليها مسؤولية تنفيذ السياسة الوطنية في المجال المعلوماتي وتتكون هذه المديرية من أربع مديريات وهي :

- مديرية الإستراتيجية و التقنين؛
- مديرية تدبير مركز اليقظة و الرصد و التصدي؛
- مديرية المساعدة و التكوين والمراقبة والخبرة؛
- مديرية نظم المعلومات المؤمنة.

هذا بالإضافة إلى إنشاء مختبرات تابعة لها في عدة مدن مغربية يكمن دورها في العمل على تحليل الأدلة الرقمية و تقديم المساعدة للأجهزة الأمنية في تتبع ورصد مرتكبي الجرائم المعلوماتية تحديد الطرق الإجرائية المستعملة في ارتكابها[12].

5 - مصلحة المعلوميات التابعة للدرك الملكي

إلى جانب مجموعة من المصالح الأمنية المركزية والجهوي نجد قوات الدرك الملكي باعتبارها مؤسسة عسكرية, يتركز عملها خصوصاً في المجال الغير حضري، أي في المناطق القروية بعيداً عن المدن، ويتكون الدرك الملكي من عدة وحدات منها ما يختص في مراقبة حركة السير خارج المدن، ومنها وحدات أخرى تختص في التحقيق فك ألغاز الجرائم ووحدات أخرى تحمل اسم الدرك الحربي ومهمتا مراقبة القوات المسلحة الملكية المغربية خلال عملياتها في الدول الأجنبية، إضافة إلى هذا كله نجد من ضمن أجهزته الداخلية مصلحة المعلوميات وهو

12 سهام أيت خويا لحسن،الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، رسالة لنيل شهادة الماستر في القانون الخاص تخصص العلوم الجنائية والأمنية، السنة الجامعية: 2016-2017 ،ص 150.

جهاز أمني من ضمن مهامه البحث في الجريمة المعلوماتية من خلاله يلعب دوره بالكشف على المتورطين وكدا استكشاف الأساليب المتبعة لارتكابها .

6 - اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي

أحدثت اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي بمقتضى القانون 08-09 الصادر في 18 فبراير 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

تضطلع اللجنة بمهمة التحقق من أن عمليات معالجة المعطيات الشخصية تتم بشكل قانوني وأنها لا تمس بالحياة الخاصة أو بحقوق الإنسان الأساسية أو بالحريات. تتشكل اللجنة من شخصيات تتمتع بالحياد والنزاهة وتمتلك كفاءة في الميادين القانونية والقضائية وفي مجال المعلوميات.

إن الهدف الرئيسي للجنة الوطنية هو احترام الحريات والحقوق الأساسية للأشخاص الذاتيين تجاه معالجة معطياتهم ذات الطابع الشخصي بالإضافة إلى الإخبار والتحسيس وكذا الاستشارة والاقتراح تضطلع اللجنة إلى مهام كمسؤولة عن حماية المعطيات الشخصية للأفراد ثم التحري و المراقبة تتمكن اللجنة من خلالها من مراقبة عمليات معالجة المعطيات الشخصية للتأكد من توافقها مع مقتضيات القانون 08-09 ونصوصه التطبيقية. لهذا الغرض، يمكن لأعوان اللجنة المفوضين الولوج لكل العناصر الخاصة بالمعالجة (المعطيات، التجهيزات، البنايات، دعائم حفظ المعلومات...). أعمال المراقبة هذه قد تفضي إلى إصدار عقوبات إدارية أو مالية أو جنائية[13].

ثانيا : المؤسسات غير القضائية

7 - الوكالة الوطنية لتقنين المواصلات

أحدثت الوكالة الوطنية لتقنين المواصلات طبقا للقانون رقم 96-24 المتعلق بالبريد والمواصلات، كما تم تغييره وتتميمه بمقتضى القانون رقم 55-01، الذي رسم الخطوط العامة لإعادة تنظيم القطاع. وترتكز اختصاصات الوكالة انطلاقا من مقتضيات القانون السالف الذكر على عدة مهام قانونية و مهام اقتصادية و مهام تقنية هته الأخيرة التي تساهم من خلالها

13 (http://www.cndp.ma تاريخ الزيارة 2017/12/24).

الوكالة الوطنية في تحديد المواصفات التقنية والإدارية للموافقة على المعدات الطرفية والتجهيزات الراديو كهربائية المخصصة لربطها بالشبكات العامة للمواصلات؛

إضافة إلى تدبيرها للموارد النادرة، خاصة منها، طيف الترددات الراديو كهربائية وموارد الترقيم. كما تراقب جودة الخدمات وتتبع التزامات المشغلين في مجال التغطية الترابية, ثم تدبير أسماء مجال الانترنت ".ma" كذلك يدخل ضمن اختصاصات الوكالة الوطنية لتقنين المواصلات. وفي هذا السياق، تضع الإجراءات اللازمة لضمان تدبير إداري وتقني وتجاري للمجال ".ma"يكون متوافقا مع الممارسات الدولية[14]، وفي إطار هذا الدور المهم التي تلعبه الوكالة في مجال التواصل السلكي واللاسلكي داخل الوطن تتكلف الوكالة بمهمة استباق الهجمات التي من الممكن أن يتعرض إليها مستعملوا شبكات الاتصال، ومعاقبة التجاوزات ليكون المجال الالكتروني آمنا,علما بأن المعطيات الشخصية هي المادة الأولية للجريمة الإلكترونية، «فرسائلنا وصورنا وبريدنا الاليكتروني تنقل خارج التراب الوطني وتتداول على نطاق واسع، كما أن كل الدراسات تشير إلى ارتفاع كبير في معدلات الجريمة الإلكترونية في السنوات المقبلة، ذلك أن الابتكار والأخطار متلازمان[15].

8 - مركز النقديات و البنوك

أنشأت المجموعة المهنية للأبناك بالمغرب مركز النقديات والبنوك المعروف اختصارا CMIالذي احدث قانونيا كشركة مجهولة الاسم في 15 فبراير 2001 و بدا عمليا ممارسة مهامه في بداية فبراير 2004 وترنو البنوك في إنشاء هذ المركز إلى تطوير وتوسيع مجال استعمال البطائق البنكية[16].

يسعى هذا المركز في خلق طريقة مضمونة للأداء عبر الانترنت تساهم في تطوير الصفقات عبر التجارة الالكترونية و إنشاء موقع إنقاذ عن بعد للمعلومات البنكية المخزنة لديه ومحاربة الجرائم الماسة بالبطائق البنكية, فمن خلال المركز استطاعت السلطات الأمنية التصدي للجريمة الالكترونية بالكشف عن بطائق الائتمان المزيفة ومرتكبيها من خلال الاتصال بمختلف

14 https://www.anrt.ma/ar/reglementation/presentationتاريخ الزيارة 2017/12/24

15 https://www.maghress.com/assabah/85943 تاريخ الزيارة 2017/12/24

16 كوثر فرام،: الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية التدريب القضائيين الفوج 34 2007-2009 ص 95

البنوك على الصعيد الوطني للإفادة عن جميع عمليات السحب عبر الشبابيك البنكية و خصوصا التي تم ابتلاعها.

9 -شركات الاتصال

ساهمت شركات الاتصال اللاسلكية المتنقلة في التصدي للجريمة المعلوماتية , حيث أنها لعبت دور الكاشف عن الشخصية الحقيقية للشخص المرتكب للجريمة باعتبارها الجهة الوحيدة التي تقدم خدمات الاتصال للجمهور ويبرز دورها هذا في تتبع أثار الرسائل والاتصالات وتحديد هوية المستخدمين التي تتوفر على قاعدة بياناتهم مسبقا , وحيث أن المادة 108 من قانون المسطرة الجنائية التي تنص على إمكانية التقاط المكالمات و الاتصالات المنجزة بوسائل الاتصال و التي يأمر بها قاض التحقيق أو الوكيل العام للملك بعد تقديمه لملتمس كتابي إلى السيد الرئيس الأول بمحكمة الاستئناف , تقوم هذه الشركات بتحديد هويات الأشخاص و التقاط المكالمات ورفع تقرير إلى الجهة المصدرة للأمر, التي تقوم بدورها بإجراء متابعات قضائية للأشخاص الذي ثبت تورطهم.

المطلب الثاني : إجراءات البحث والتحقيق في الجرائم المعلوماتية .

خلال العقود الأخيرة استفحلت الجريمة في بلادنا , وأصبح القضاء المغربي في محك حقيقي , عندما عرضت أمامه قضايا تتعلق بالجرائم الالكترونية .

فأمام الإشكاليات التي كان يجدها القضاء المغربي , وخصوصا وجود فراغ تشريعي في مجال مكافحة الجرائم الالكترونية اضطر المشرع المغربي الى سن تشريعات حديثة أو إضافة نصوص أخرى لمجموعة القانون الجنائي تتلاءم وخصوصية الجريمة الالكترونية .

يختلف قمع ومكافحة الجرائم المعلوماتية عن ضبط الجرائم التقليدية على اعتبار ان هذه الجرائم ذات طبيعة خاصة لتعلقها ببيانات معالجة الكترونيا وكيانات منطقية غير مادية , لذا فهي تحتاج لأجل مواجهتها فرق خاصة لتتبع هذه الجرائم .

سنتطرق في هذا المطلب الى تلقي اكتشاف الجرائم والتبليغ عنها (الفقرة الأولى) , ثم مدى قابلية المعاينة والتفتيش بمفهومهما التقليدي للتطبيق على جرائم المس بنظم المعالجة الآلية للمعطيات وكذلك الأمر بالنسبة للحجز, أم أن الأمر يحتاج الى تدخل تشريعي ليعدل النصوص المتعلقة بهذه الإجراءات حتى تكون قابلة للتطبيق وتشمل هذه الجرائم (الفقرة الثانية) .

الفقرة الأولى : اكتشاف الجرائم والتبليغ عنها وتحديد خطة البحث (العمل).

سنقوم بالحديث عن تلقي البلاغات والشكاوى (أولا) , على أن نتناول الخطة التي يتم تحديدها للانطلاق في عملية البحث (ثانيا) .

أولا : اكتشاف الجرائم المعلوماتية والتبليغ عنها .

إن من أهم الإشكالات التي تواجه أجهزة الأمن والمحققين هي أن الجرائم المعلوماتية لا تصل الى علم السلطات المعنية بالصورة العادية التقليدية وذلك لصعوبة اكتشافها بواسطة الأشخاص العاديين . وحتى في المؤسسات المالية والشركات الكبرى لا يتم اكتشاف هذه الجرائم فور وقوعها لأن المؤسسات والشركات التجارية لا تصفي أو تراجع حساباتها يوميا , وحتى المؤسسات التي تقوم بذلك يصعب عليها التأكد من المفارقات في الأرقام التي قد تبدو وكأنها خسائر عادية أو دفوعات آجلة[17] .

وفي حالة اكتشاف جرائم الحاسوب بواسطة المتضررين من الشركات والمؤسسات المالية نجد أن بعض تلك المؤسسات تتردد في التبليغ عن تلك الجرائم خوفا على سمعتها وتحسبا من ردود فعل حملة الأسهم .

وهنا تظهر أهمية دور الأجهزة الأمنية في رصد مرتكبي الجرائم المعلوماتية واكتشاف الجرائم المرتكبة وذلك عن طريق الرصد الميداني لحركة المعاملات التجارية ومراقبة المشبوهين داخل المؤسسات المالية وحولها .

فيمكن لجهة التحقيق تلقي معلومات أمنية تشير الى ممارسة شخص غير معروف أو غير محدد مكانه أنشطة تندرج تحت تعريف جريمة معلوماتية وذلك في مكان معروف وعلى أجهزة محددة , ووفق لغات برمجية معلومة , أو ضبط شخص وبحيازته أموال مشبوهة أو بطائق بنكية مزورة أو بطائق تعريف مشبوهة .

البلاغ بصورة عامة إخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع أو أن هنالك اتفاقا على ارتكابها[18] . والمبلغ في الجرائم الالكترونية لا بد وأن يكون لديه معرفة مقبولة بالجوانب الفنية للحاسب الآلي وشبكة الانترنت حتى يتمكن من تقديم معلومات تصف الحادث بشكل جيد يمكن للمحقق الوقوف من خلاله الوقوف على طبيعة الجريمة بشكل

17 راجع المواد 27، 40 و 49 من قانون المسطرة الجنائية المغربي.

18 محمد الادريسي العلمي المشيشي , المؤسسات القضائية , منشورات جمعية تنمية البحوث والدراسات القضائية , الرباط , الجزء الأول 1991، ص 84.

مقبول يمكنه من مباشرة التحقيق فيها . وبالتالي يفترض أن يكون لدى من يتلقى البلاغ المعرفة الكافية بالجوانب الفنية للحاسب الآلي والشبكات حتى يستطيع مناقشة المبلغ في الكثير من الجوانب المتعلقة بالجريمة محل البلاغ .

ما هي المعلومات التي يجب استيفاؤها من المبلغ ؟

تتباين المعلومات التي ينبغي أن يدونها المحقق عند تلقي البلاغ بتباين فئات جرائم الحاسب الآلي والانترنت والطبيعة الفنية التي تتميز بها كل فئة عن غيرها . وعلى الرغم من أن لكل فئة من هذه الجرائم المستحدثة معلوماتها الخاصة التي ينبغي الحرص قدر الإمكان على استيفائها عند تلقي البلاغ , إلا أن هناك معلومات تكاد تكون مشتركة بين معظم هذه الفئات , ويمكن الحصول عليها عن طريق طرح أسئلة تتناول جوانب معينة منها ما يلي :

- تاريخ ووقت تلقي البلاغ .
- المعلومات الخاصة بالمبلغ .
- المعلومات الخاصة بمتلقي البلاغ .
- طبيعة ونوع جريمة الحاسب الآلي محل البلاغ .
- الأسئلة الستة المشهورة والمتعلقة بالجريمة ماذا؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟ .
- المعلومات ذات العلاقة بالأنظمة الحاسوبية , مثل طبيعة العتاد ونوعية البرمجيات والمسئولين عن الأنظمة وطريقة الاتصال بهم وغيرها .

وتجدر الإشارة الى أن عملية تلقي البلاغ لا تعدو أن تكون محادثة صغيرة وسريعة تهدف الى تمكين المحقق من وضع تصور مبدئي عن ظروف وملابسات الحادث قبل الانتقال الى مسرح الجريمة[19] . ومع ذلك فإننا نرى أن دقة وتكامل المعلومات محل البلاغ على درجة كبيرة من الأهمية , حيث أنه من الممكن أن تسهم في مساعدة المحقق على :

- تحديد ما إذا كان السلوك محل البلاغ يعد سلوكا إجراميا يندرج ضمن جرائم الحاسب الآلي والانترنت .
- وضع تصور مبدئي عن خطة العمل المناسبة للتحقيق في الحادث .

19 ضياء نعمان , الغش المعلوماتي الظاهرة والتطبيقات , المطبعة والوراقة الوطنية , مراكش , الطبعة الأولى 2011.ص 366.

- تحديد نوع الخبرة الفنية التي يحتاجها في المعاينة ورفع الأدلة من موقع الحادث , والعمل على سرعة استدعاء الخبراء القادرين على انجاز ذلك .

وقبل أن ينهي المحقق عملية تلقي البلاغ يجب أن يحرص على التأكيد على المبلغ بضرورة القيام بالأمور التالية :

1. تجهيز قائمة بأسماء العاملين في المؤسسة ممن لهم علاقة بالأجهزة المتضررة , أو علاقة بأي مشروع للأجهزة المتضررة .
2. تجهيز النسخ الاحتياطية من بيانات الأجهزة المتضررة , لاستخدامها من قبل فريق التحقيق فور وصوله الموقع .
3. التأكيد على عدم إبلاغ أحد بالحادث إلا من كانت الضرورة القصوى تحتم إبلاغه .

إن الخصوصية التي تتميز بها هذه المرحلة أي مرحلة تلقي البلاغ هي أن يكون مصدر البلاغ على درجة من الوعي والقدرة والمعرفة بتفاصيل ما يدلي به من معلومات . ولا يصلح هنا كبلاغ يبرر تحريك الإجراءات القول بأن هنالك جريمة معلوماتية أو ترتكب في مكان ما . فعلى المبلغ هنا أن يقدم وصفا علميا محددا للنشاط الإجرامي مع بيان الأسماء واللغات والبرامج وأنواع الأجهزة المستخدمة وأماكنها قدر المستطاع .

ثانيا : تحديد خطة البحث

بعد الانتهاء من جمع المعلومات اللازمة عن الحادث يبدأ المحقق وعلى ضوء تلك المعلومات التي توافرت لديه تحديد خطة العمل المناسبة وفريق العمل اللازم للتحقيق في الحادث . ففي الغالب يكون مكان ارتكاب الجريمة المعلوماتية مثل مكان ارتكاب الجرائم الأخرى عندما يكون الهدف منها التخريب أو إتلاف البرامج أو تزوير المستندات والوثائق أو تفجير المباني والمنشآت .

ففي الحالة الأولى يكون التحرك لموقع ارتكاب الجريمة بقصد المداهمة وضبط الأدلة على حالتها الطبيعية . ويعد هذا النوع من التحرك الأوفر حظا في النجاح وتحقيق الأهداف . أما الحالة الثانية , والتي يتم فيها التحرك بعد وقوع الجريمة وتحقق نتائجها التخريبية فالنجاح فيها مرهون بتوفر اعترافات المتهمين , وشهادات الشهود والقرائن . وفي كلتا الحالتين تتبع عدة مراحل قبل التحرك لمعاينة موقع ارتكاب الجريمة .

فخطة العمل تعني التخطيط الذي يقوم به المحقق لتحديد الأسلوب الأمثل في التعامل مع حادثة معينة , وذلك في الإطار العام للإجراءات الواردة في الخطة ووجود درجة عالية من التفصيل للبحث في هذه الجرائم .

هناك العديد من الأمور التي يجب القيام بها في خطة العمل قبل الانتقال الى موقع ارتكاب الجريمة وهي على النحو التالي :

- توفير معلومات مسبقة عن مكان الجريمة , نوع وعدد الأجهزة المتوقع مداهمتها وشبكاتها .
- إعداد خريطة للموقع الذي سيتم التحرك إليه وتفاصيل المبنى أو الطابق من المبنى موضوع البلاغ , وتحديد مواقع الأجهزة والخزائن والملفات , ويتم ذلك عبر مصادر المعلومات السرية .
- تحديد عدد وأنواع الأجهزة المحتمل تورطها في الجريمة لتحديد إمكانات التعامل فنيا من حيث الضبط والتأمين وحفظ المعلومات .
- الحصول على الاحتياجات الضرورية من أجهزة وبرامج صعبة ولينة للاستعانة بها في الفحص والتشغيل .
- إعداد قائمة دائمة بالاحتياجات العامة لجميع التحركات مسبقا ومراجعة احتياجات كل حالة على حدة .
- إعداد فريق التفتيش المتخصص وفق قائمة تحدد الأسماء والاختصاصات والمهام الموكولة للكل بدقة .
- إخطار أعضاء الفريق قبل وقت كاف من التحرك لمسرح الجريمة لتمكينهم من خططهم الخاصة .
- كتابة بيانات بالمهام المطلوبة من كل عضو في الفريق وتوزيعها على الجميع لضمان الانجاز مع عدم التداخل .
- إعداد خطة الهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق , على أن تكون الخطة موضحة الرسومات وتتم مراجعتها مع أعضاء الفريق قبل بدء التحرك.

-إعداد الأمر القضائي اللازم للتفتيش[20] حسب الأصول لأن الجرائم المعلوماتية عادة ما تكون داخل أمكنة لها خصوصيتها .

-الاحتفاظ بسرية التحرك حتى نهاية التفتيش إذ أن المعلومات التي يتم البحث عنها يمكن إتلافها بسهولة من قبل المتهمين أو المتورطين في الجريمة .

-تأمين التيار الكهربائي بحيث لا يتم التلاعب أو التخريب عن طريق قطع التيار أو تعديل الطاقة الكهربائية .

الفقرة الثانية : إجراءات البحث والتحقيق في الجرائم المعلوماتية .

بعد الحديث عن تلقي البلاغات والشكايات وتحديد خطة البحث , يجب التطرق الى إجراءات البحث المتمثلة في المعاينة (أولا) , والتفتيش (ثانيا) , قبل الانتقال الى الحجز كإجراء لا يقل أهمية عنهما (ثالثا) .

أولا : المعاينة .

يقصد بها الإثبات المادي والمباشر لحالات الأشخاص والأشياء والأمكنة ذات الصلة بالحادث . والقيام عند الاقتضاء بجمع الأدلة والحجج المادية المتخلفة في مكان الحادث لإثبات وجود عمل جرمي من عدمه ونسبته عند الاقتضاء إلى فاعل أو عدة فاعلين أو مشاركين[21] .وعلاوة على ذلك تستعمل المعاينة في كثير من المواضع بمعنى التأكد أو التثبت من واقعة أو إدعاء يكتسي صبغة جريمة بإثبات وجودها أو نفيها، وبهذا المعنى وردت عبارة المعاينة في الفقرة الأخيرة من المادة 56، وفي المادة 62 من قانون المسطرة الجنائية المغربي[22]، وقد أشار أيضا المشرع الفرنسي إلى المعاينة في معرض حديثه عن اختصاصات الشرطة القضائية في المادة 18 من قانون المسطرة الجنائية الجديد[23].

ويرى البعض أن أهمية المعاينة تتضاءل في الجريمة المعلوماتية وذلك لندرة تخلف آثار مادية عند ارتكاب الجريمة المعلوماتية , كما أن طول الفترة ما بين وقوع الجريمة أو ارتكابها وبين اكتشافها قد يكون له الأثر السلبي بسبب احتمالية العبث أو المحو أو التلف لأثارها .

---

20 نظم المشرع المغربي التفتيش في المواد من 69 إلى 63 من قانون المسطرة الجنائية.

21 محمد الادريسي العلمي المشيشي , المؤسسات القضائية , منشورات جمعية تنمية البحوث والدراسات القضائية , الرباط , الجزء الأول 1991، ص 84.

22 أحمد أيت الطالب، مساطر المعاينة والبحث الجنائي،ج 2، مطبعة المعارف الجديدة، الرباط، 2014 ص 34-35.

23 " Elle est chargée (la police judiciaire) suivante les distinctions établies au présent titre de constater les infractions a la loi pénale..." راجع احمد ايت الطالب، المرجع السابق ، ص 35.

.

ففي حالة تلقي بلاغ بوقوع إحدى الجرائم المعلوماتية , وبعد التأكد من البيانات الواجب توافرها في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته . حيث تنص المادة 57 من قانون المسطرة الجنائية على انه " يجب على ضابط الشرطة القضائية الذي أشعر بحالة تلبس بجناية أو جنحة أن يخبر بها النيابة العامة فورا وأن ينتقل في الحال إلى مكان ارتكابها لإجراء المعاينات المفيدة " , مما يتبين لنا أن السلطة المختصة بإجراء المعاينة هي الضابطة القضائية .

إن مسرح الجريمة المعلوماتية يختلف عن مسرح الجريمة التقليدية , فلها مسرح تقليدي يقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه وهو أقرب ما يكون الى المسرح التقليدي للجريمة وقد يترك فيه الجاني أثار عدة كالبصمات وغيرها , وهناك أيضا مسرح غير تقليدي ويقع داخل بيئة الحاسوب , ويتكون من البيانات الرقمية التي تتواجد وتنقل داخل بيئة الحاسوب وشبكاته , في ذاكرته وفي الأقراص الصلبة الموجودة بداخله .

فالجريمة المعلوماتية قد تكون مستمرة كجرائم السرقة وقد يكون مسرحها إتلاف البرامج , ومهما يكن فانه عند إجراء المعاينة في الجرائم المعلوماتية يجب مراعاة العديد من الأمور على النحو التالي :

- تصوير الحاسب الآلي والأجهزة المتصلة به , على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة ؛
- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعملية , وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها ؛
- إعداد خطة المعاينة , موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل؛
- العناية بالطريقة التي تم بها إعداد النظام ؛
- ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة ؛
- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة .

قصر مباشرة المعاينة على الباحثين والمحققين .

وعموما فان الجرائم المعلوماتية وباعتبارها جرائم غير تقليدية لا تخلف أثار مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جناية السرقة , فالعديد من الجرائم المعلوماتية تتم عبر اعتراض النبضات الالكترونية والتلاعب بالأنظمة المعلوماتية هذا بالإضافة الى أن الجناة عادة ما يعمدون إلى إخفاء معالم الجريمة وإزالة آثارها , كما أن الجهات التي تقوم بعملية المعاينة غالبا ما تفتقر إلى الكفاءة والخبرة اللازمتين لمواجهة هذا النوع المتطور من الجرائم .

ثانيا : التفتيش .

هو البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها , وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة , وقد أحاط القانون التفتيش بضمانات عديدة ومحل التفتيش قد يكون مسكنا أو شخصا , وقد نظم المشرع المغربي التفتيش بمقتضى المادة 62 من ق م ج حيث نص على أنه لا يمكن الشروع في تفتيش المنازل أو معاينتها قبل السادسة صباحا وبعد التاسعة ليلا إلا إذا طلب ذلك رب المنزل أو وجهت استغاثة من داخله , أو في الحالات الاستثنائية التي ينص عليها القانون[24] .

فالقيام بالتفتيش قد يساعد في ضبط الأدلة المشبوهة وحجزها تمهيدا لفحصها وإجراء التحليلات التقنية عليها بحثا عن ما تتضمنه من معطيات أو أدلة رقمية , وأيضا الأدلة التقليدية ذات العلاقة بأنظمة وبرامج الحاسب الآلي والأوراق والمستندات إلى غير ذلك .

غير أن عملية البحث تلك قد تدفع الباحث الجنائي إلى توسيع دائرة التحريات إلى حاسب آلي أو مركزي موجود في محل آخر يشغله المشتبه به أو شخص آخر , كما قد يجد نفسه مضطرا للدخول الى معطيات آلية أو قواعد بيانات أو مواقع محمية ومؤمنة . وهو ما يثير إشكالا بخصوص إمكانية الولوج إليها بناء على الإذن المحصل عليه أصلا عند الدخول إلى المنزل الذي قام فيه بتحرياته الأولية , أم أن هذا الإذن لا يخوله للقيام بعمليات تحري في وسط معلوماتي , باعتبار أن الأنظمة المعلوماتية المحمية لا تعتبر منازل بمفهوم القانون .

في غياب إطار قانوني خاص يسمح بالولوج إلى هذه الأنظمة , يمكن القول أن قانون المسطرة الجنائية المغربي ورغم حداثته , إلا أنه لا يتضمن استجابة صريحة لمتطلبات البحث وتفتيش قواعد المعطيات الآلية باستعمال الشبكة .

---

24 من اهم الحالات الاستثنائية التي نص عليها القانون هي حالة وجود عمل إرهابي والذي نظمه القانون 03-03 الصادر سنة 2003.

ثالثا : الحجز .

إن حجز أو كل ما له علاقة بالجريمة من أسلحة أو أدوات استعملت في ارتكابها من الصلاحيات الموكولة لضابط الشرطة القضائية والتي يتم التوصل إليها بأحد الطرق التالية :

- عن طريق التفتيش (المنظم في قانون المسطرة الجنائية) .
- إيجادها وضبطها بمكان الجريمة أو بحوزة الجاني .
- تقديمها من طرف أحد الأشخاص .

فيقوم ضابط الشرطة القضائية بضبطها وإحصائها فورا ويضعها في غلاف مختوم يشير فيه إلى طبيعتها وغيرها , ورقم المحضر المنجز بشأنها إلى حين تقديمها إلى النيابة العامة التي تقوم بدورها بإحالتها إلى المحكمة أو قاضي التحقيق , وتتم هذه العملية بحضور الأشخاص الذين حضروا عملية التفتيش[25] .

على صعيد الجرائم المعلوماتية يتم القيام بهذا الإجراء من قبل فريق متخصص يتكون من اثنين أو أكثر من الخبراء الذين يتولون ضبط وإدخال المعلومات المضبوطة في الحاسب الآلي وتصنيف الأدوات وتحريزها في صناديق ووضع العلامات عليها , ويقوم هذا الفريق بنقل هذه الأجهزة المضبوطة بعد تكملة إجراءات الرسم والتصوير ويجب أن يكون بين أعضاء هذا الفريق شخصان على الأقل احدهما محقق في مجال الحاسب الآلي , والثاني خبير في الحاسب الآلي مدرب على التعامل مع الأدلة وطرق تقييمها .

ويجب الإشارة الى أن الغاية من الحجز تكمن في المحافظة على الأدلة من الاندثار, ونظرا لما لهذه الأخيرة من دور في إظهار الحقيقة فان المشرع منع أي شخص غير مؤهل قانونا من تغيير حال المكان الذي وقعت فيه الجريمة ومحو آثارها تحت طائلة العقوبة من ثلاث أشهر إلى ثلاث سنوات وغرامة من 3000درهم إلى 12000 درهم . فإذا خيف على الأشياء المحجوزة من سرعة اندثارها , يمكن الاستعانة بأي شخص مؤهل أو خبير للمساعدة .

فكل هذه العمليات التي أنجزها ضابط الشرطة القضائية بمناسبة التفتيش وحفظ المحجوزات يضمنها لزوما في محضر قانوني يذكر فيه الأسباب الداعية إلى التفتيش والمكان الذي أجري فيه , والوقت الذي أنجز خلاله . ويتضمن المحضر كذلك حصيلة التفتيش ونوع ووصف المحجوزات التي تم حجزها مع الإشارة إلى الأشخاص الذين حضروا التفتيش الذين

25 احمد قيلش و محمد زنون، الشرطة القضائية، الكتاب الأول مطبعة النجاح الجديدة الدار البيضاء، 2013، ص 139

يوقعون وجوبا مع الضابط القضائي على محضر التفتيش والحجز أو يشار الى امتناعهم عن التوقيع أو الإبصام أو تعذره .

ومما نخلص إليه أن ظاهرة الإجرام المعلوماتي متجددة ومعقدة . مما يجعل المشرع ملزما بمواكبة التطورات عبر سن تشريعات جديدة أو تعديلات أخرى , مع توفير تكوين مستمر للأفراد المكلفين بالحث والتحقيق في هذا النوع من الجرائم , وهنالك صعوبات أخرى تطفو على السطح منها عدم فعالية التعاون القضائي الدولي وتشبث الدول بسيادتها وهو أمر خارج عن إرادة دولة معينة .

المبحث الثاني:صعوبات البحث والتحقيق وإشكالية الإثبات في الجرائم المعلوماتية

إن الحديث عن الصعوبات التي يعرفها مجال البحث والتحقيق في الجرائم المعلوماتية، والإشكال الذي يثيره إثبات وقوعها يقتضي منها الإشارة أولا إلى تحديد هذه الصعوبات (المطلب الأول)، قبل التطرق إلى الأدلة المعتمدة في هذا النوع من الجرائم وما يثير من إشكالات (المطلب الثاني)

المطلب الأول:صعوبات البحث والتحقيق في الجرائم المعلوماتية

تتحدد صعوبات البحث والتحقيق في الجرائم المعلوماتية في صعوبات مرتبطة بالإجراءات نفسها (الفقرة الأولى)، وأخرى متعلقة بجهات التحري (الفقرة الثانية):

الفقرة الأولى:الصعوبات المرتبطة بإجراءات البحث والتحقيق في الجرائم المعلوماتية

لما كانت الجرائم المعلوماتية تتسم بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفاء معالمها ودقة وسرعة محو أثارها ،فقد ظهرت نتيجة عنها جملة من الصعوبات والإشكالات العملية التي تعرقل وتقف كحجر عائق أمام أجهزة العدالة في مواجهتها لهذه الطائفة من الجرائم ولا سيما أجهزة البحث والتحري والتي تعمل من اجل استيفاء الدليل الالكتروني،إذ أصبحت هذه الأخيرة تواجه مشاكل وصعوبات إجرائية أثناء مباشرة مهامها للكشف عن هذا النوع من الجرائم وملاحقة مرتكبيها وتقديمهم للعدالة[26]،يمكن إجمال هذه الصعوبات فيما يلي:

[26]-www.alkanounia.comموقع،تاريخ الولوج 24-12-2017،نشر به مقال للباحث يوسف قجاج حول الجريمة الالكترونية واشكالية القواعد الاجرائية

أولا: صعوبات مرتبطة بالدليل

10 - غياب الدليل المرئي:

ان الجرائم المعلوماتية التي تعتمد في ارتكابها على النبضات والأكواد والتشفير والتخزين الالكتروني من الصعب ان تخلف وراءها آثار مرئية قد تكشف عنها أو يستدل من خلالها على مرتكبيها ،وبالتالي فالدليل في هذه الجرائم يكون غير مرئي في هيئة رموز ونبضات مخزنة على دعائم أو وسائط التخزين الممغنطة أو الضوئية ،لا يمكن للإنسان قراءتها أو إدراكها[27]،مما يقطع غالبا كل صلة بين المجرم وجريمته ويحول دون الكشف عن هويته

11 - افتقاد الآثار التقليدية:

وذلك لان بعض العمليات يتم فيها إدخال البيانات مباشرة في جهاز الحاسب دون ان يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها ،بالإضافة لجرائم التجسس التي تتم عن طريق اعتراض النبضات الالكترونية وجرائم الاختلاس التي تتم عبر تعديل البرامج والتلاعب بالأنظمة المعلوماتية[28]

12 - صعوبة الوصول إلى الدليل:

الملاحظ أن البيانات المخزنة الكترونيا أو المنقولة عبر الشبكات قد تحاط بحماية فنية لا علاقة المحاولات الرامية للوصول غير المشروع لها إما بالاطلاع عليها أو استنساخها، يمكن كذلك للمجرم المعلوماتي من اجل زيادة صعوبة عملية التفتيش المتوقع عن الأدلة التي تدينه بوضع مجموعة من التدابير،كاستخدام كلمات سر للوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة ومنع الاطلاع عليها.وتعد تقنية التشفير من اكبر العقبات التي تعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة والتي تحد من قدرة جهات التحري على قراءتها [29]

[27]--سهام ايت خويا لحسن،الجرائم المعلوماتية بين ثبات النص ونتطور الجريمة ،رسالة لنيل شهادة الماستر في القانون الخاص تخصص العلوم الجنائية والامنية ،كلية العلوم القانونية الاقتصادية والاجتماعية،جامعة القاضي عياض،مراكش،السنة الجامعية 2016-2017،ص45

[28]--سهام ايت خويا لحسن ،مرجع سابق،ص143

[29]-ضياء علي احمد نعمان،الغش المعلوماتي الظاهرة والتطبيقات،سلسلة الدراسات القانونية في المجال المعلوماتي1،المطبعة والوراقة،مراكش

13 - سهولة إخفاء الدليل:

تعتبر سهولة إخفاء ومحو الدليل أو تدميره من بين الصعوبات التي تثار في مرحلة البحث عن الأدلة ،فالجاني يمكنه محو الأدلة التي قد تدنيه أو يدمرها في وقت وجيز وبمجرد كبسة زر،بحيث لا تتمكن سلطات البحث والتحقيق من كشف جرمه وإقامة الدليل ضده[30]

5-كثافة البيانات المتعين فحصها:

يعتبر الكم الهائل من البيانات التي يتعين على أجهزة البحث و التحقيق فحصها ،احد ابرز التحديات والصعوبات التي تواجهها نظرا لضخامتها وكمها الهائل ،فطباعة كل ما هو موجود من المعلومات والوثائق على دعامات الكترونية لحاسب آلي تم استخدامه مدة من الزمن يتطلب مئات الآلاف من الصفحات التي قد لا تقدم شيئا مفيدا للبحث ،وذلك بخلاف ما عليه الأمر في الجرائم التقليدية التي تعد فيها وفرة المعلومات أمرا ايجابيا يساعد أجهزة البحث والتحقيق على التثبت من وقوع الجريمة وضبط مرتكبيها.

لذلك يجب عند وقوع جريمة معلوماتية نذب خبراء فنيين لديهم معرفة متعمقة في سائر أنواع الحسابات الآلية وبرمجتها وشبكاتها،ولديهم القدرة على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها[31]

ثانيا:صعوبات مرتبطة بجهات التحري

1 -إخفاء الجريمة:

الجرائم التي تقع على الحسابات وشبكات المعلومات او بواسطتها،مستترة خفية في أكثر صورها،لا يلاحظها المجني عليه غالبا أو يدري حتى بوقوعها والملاحظ انه ليس عسيرا في الكثير من الأحوال حجب وإخفاء السلوك المكون لهذه الجرائم وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل البيانات عن طريقها،بحكم توافر المعرفة والخبرة الفنية في مجال الحسابات لدى مرتكبها[32]

2011،، ص342 343 344

[30] - سهام ايت خويا لحسن،مرجع سابق،ص146

-عبد الله ادعول،الدليل الالكتروني في الاثبات الجنائي،رسالة لنيل دبلوم الماستر في القانون الخاص،ماستر العلوم الجنائية والامنية،كلية العلوم القانونية

[31] الاقتصادية والاجتماعية،جامعة القاضي عياض،مراكش،السنة الجامعية2011\2012 ،ص23

[32] -ضياء نعمان،مرجع سابق،ص341

2 -عدم التبليغ:

تحرص اغلب الجهات التي تتعرض أنظمتها المعلوماتية للاختراق وتمنى بخسائر فادحة من جراء ذلك،إلى عدم الكشف حتى بين موظفيها عما تعرضت له،وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وفقدان ثقة المتعاملين معها في كفاءتها[33]

3 -نقص خبرة الجهات المختصة:

إن خصوصية البحث والتحقيق في الجرائم المعلوماتية يستدعي بالضرورة المعرفة التقنية بمهارات خاصة تسمح بتفهم ومواجهة تقنيات الحاسب الآلي المتطورة وأساليب التلاعب المعقدة التي تستخدم في ارتكاب هذه الجرائم عادة،الشئ الذي يتطلب والأمر هذا استخدام أساليب وتقنيات مبتكرة ومتوفرة لتحديد نوعية الجريمة وشخصية مقترفها وكيفية ارتكابها مع تطبيق وسائل جديدة لضبط الجاني والحصول على أدلة إدانته[34]

4 -صعوبة التعاون الدولي:

إن الطابع الدولي لجرائم المس بنظم المعالجة الآلية للمعطيات والذي تستمده من كونها عابرة للحدود الجغرافية للدول،وأن تأثير غير منحصر داخل إقليم دولة واحدة التي وقعت فيها،إنما أثارها السلبية والخطيرة تمتد لتصل الى عدد كبير من الدول مستفيدة من الترابط الدولي عبر شبكة الانترنت[35]وقد تسبب أضرارا فادحة يغدو التعامل الدولي واسع المدى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للبيانات أمرا محتما،ومع ضرورة هذا التعامل،إلا أن عقبات عدة تقف في سبيله،أهمها ما يلي:

- عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات الواجب تجريمها؛
- عدم الاتفاق على مفهوم عام حول التعريف القانوني للنشاط الذي يفترض الاتفاق على تجريمه؛

[33]-عبد الله ادعول،مرجع سابق،ص24
[34]-ضياء نعمان،مرجع سابق،ص347
[35]-عبد الله ادعول،مرجع سابق،ص25

- اختلاف مفاهيم الجريمة لاختلاف التقاليد القانونية وفلسفة النظم القانونية المختلفة؛
- عدم التناسق بين قوانين الإجراءات المختلفة فيما يتعلق بالتحري والتحقيق في الجرائم المعلوماتية؛
- تعقد المشاكل القانونية والفنية الخاصة بتفتيش نظام معلوماتي خارج حدود الدولة أو ضبط معلومات مخزنة فيه؛
- عدم وجود معاهدات للتسليم أو التعاون الثنائي أو الجماعية بين الدول تسمح بالتعاون الدولي أو عدم كفايتها إن وجدت، لمواجهة المتطلبات الخاصة للجرائم المعلوماتية وديناميكية وسرعة التحريات فيها[36] .

الفقرة الثانية:الصعوبات المتعلقة بإشكالية الاختصاص

تعتبر الجرائم المعلوماتية من أكثر الجرائم التي تثير مشكلات الاختصاص على المستوى المحلي والدولي بسبب شبكات المعلومات،حيث قد تقع الجريمة في مكان معين وتنتج أثارها في مناطق أخرى داخل الدولة أو خارجها.

وهنا تنشأ مشكلة البحث عن الأدلة الجنائية خارج دائرة الاختصاص التي سجل فيها البلاغ وتم فيها تحريك الإجراءات الجنايات،كما تنشأ مشكلات فحص البيانات في مراكز معلومات دول أخرى الشئ الذي يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدولة[37].

وإذا كانت قواعد الاختصاص التقليدية قائمة على مبدأ إقليمية القانون الجنائي كأصل مع ما يرد عليه من استثناءات صيغت لكي تحدد بالأساس الاختصاص المتعلق بجرائم قابلة للتحديد المكاني،فإننا نتساءل عن مدى إمكانية الاعتماد على هذه القواعد لتحديد الجهة المختصة للنظر في الجريمة المعلوماتية العابرة لكل الحدود الجغرافية؟

ان الاختصاص هو السلطة التي يقررها المشرع للقضاء لان ينظر في دعاوى معينة حددها القانون وهو نوعان، اختصاص دولي ويقصد به الحالات التي يكون فيه القانون الجنائي لدولة ما مختصا بالنظر في دعاوى معينة،إما الاختصاص الداخلي فيقصد به توزيع الدعاوى الجنائية وفق معايير محددة داخل الدولة.

[36]-ضياء نعمان،مرجع سابق،ص348

[37]-ضياء نعمان،مرجع سابق،ص384و 385

ويبقى مبدأ الإقليمية أهم ضابط محدد للاختصاص المكاني ولمجال تطبيق قواعد القانون الجنائي بمختلف التشريعات الداخلية والدولية،ويقصد به تطبيق أحكام القانون الجنائي على جميع الجرائم المرتكبة فوق إقليم الدولة أياً كانت جنسية مرتكبها وبصرف النظر عن جنسية المجني عليه ويستند هذا المبدأ على فكرة سيادة الدولة على إقليمها.

أولا:موقف الاتفاقات

ان اختلاف الإجراءات الجنائية والتنازع حول القانون الواجب التطبيق بخصوص الجرائم المعلوماتية، دفع بالمجتمع الدولي للتدخل وسن اتفاقيات دولية تهدف بالأساس الى محاولة توحيد الإجراءات الجنائية ومنها الضوابط المحددة للاختصاص المكاني والقانون الواجب التطبيق .

5 -اتفاقية بودابست:

تناولت اتفاقية بودابست في مادتها 22 المبادئ التي يجب على الدول الأطراف الاعتماد عليها لتحديد الاختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها في هذه الاتفاقية، وبرجوعنا للفقرة الأولى من المادة المذكورة نلاحظ أنها طلبت من الدول الأطراف في هذه الاتفاقية اعتماد ما يلزم من الإجراءات التشريعية والإجراءات الأخرى لإقرار الاختصاص القضائي على الجرائم المنصوص عليها في المواد من 2الى 11من هذه الاتفاقية عندما ترتكب هذه الجرائم على أرضها أو على متن إحدى سفنها التي تحمل علمها أو على متن إحدى الطائرات المسجلة بموجب قوانينها.

وكذلك على كل جريمة مرتكبة من طرف احد مواطنيها إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان ارتكابها أو في حالة ارتكاب الجريمة خارج نطاق السلطة القضائية الإقليمية لأية دولة.

كما نصت اتفاقية بودابست في فقرتها 3 من المادة 22 على مبدأ العالمية وذلك في حال رفض أي طرف في هذه الاتفاقية تسليم مرتكب الجريمة المتواجد على أرضها على أساس مبدأ الجنسية فيجب على الدولة الرافضة القيام بإجراءات التحقيق والمحاكمة وفقا لقانونها الوطني.

كما طلبت الاتفاقية المذكورة من الدول الأطراف التشاور فيما بينها حول التشريع القضائي الأكثر ملائمة لمحاكمة مرتكبي الجرائم المعلوماتية في حالة تعدد حالات المطالبة من طرف الأطراف باختصاصها القضائي حول واقعة معينة.

6 -الاتفاقية العربية:

المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لم تخرج فيما نصت عليه بخصوص الاختصاص على ما جاء في المادة 22 الأنفة الذكر من اتفاقية بودابست ،وبالتالي فقد ألزمت المادة30 من الاتفاقية الدول الأطراف تبني الإجراءات الضرورية لمد اختصاصها على كل الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية نفسها وذلك متى ارتكبت الجريمة كليا أو جزئيا أو تحققت في إقليم الدولة الطرف أو على متن طائرة مسجلة تحت قوانينها أو على متن سفينة تحمل علمها،أو إذا ارتكبت الجريمة من قبل احد مواطنين الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأي دولة أو إذا كانت الجريمة تمس احد المصالح العليا للدولة الطرف في الاتفاقية صاحبة الاختصاص في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة ولا يتم تسليمه الى طرف أخر بناء على جنسية بعد طلب التسليم وذلك فيما يخص الجرائم المنصوص عليها في المادة 31 من الاتفاقية.

وفي الفقرة الأخيرة من المادة 30 من نفس الاتفاقية وضعت هذه الأخيرة الحل في الحالة التي يدعي أكثر من دولة طرف الاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية،وذلك بتقديم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم بعد ذلك في الحالة التي تحدد فيها الظروف فتقدم الدولة الأسبق في طلب التسليم.

ثانيا:موقف التشريعات المقارنة و الوطنية

ولنوضح أكثر سنقوم بالتطرق لبعض التشريعات المقارنة لمعرفة مدى امتثالها للاتفاقية الدولية ،وكيفية تعاملها مع الاختصاص في الجرائم المعلوماتية

7 -المشرع الفرنسي:

تضمن قانون العقوبات الفرنسي لعام 1992 القواعد المتعلقة بتنازع القوانين الإجرائية من حيث المكان والمنصوص عليها في المواد 113\1 إلى 113\7 منه وقد تضمنت هذه القواعد مبادئ الإقليمية والعينية والشخصية

فقد اخذ التشريع الفرنسي بمبدأ الإقليمية من خلال المادة 113\2 من قانون العقوبات ف،وعليه فأحكام القانون الجنائي المرتكبة فوق إقليم الجمهورية الفرنسية أياً كانت جنسية مرتكبها وبغض النظر عن جنسية الضحية،وتعتبر الجريمة قد ارتكبت على إقليم الجمهورية متى كان احد العناصر الجريمة قد وقع عليه،بالإضافة للجرائم الواقعة على السفن والطائرات الوطنية الخاضعة للقانون الفرنسي.

بالإضافة إلى مبدأ الإقليمية أخذ المشرع الفرنسي بمبدأ عينية النص الجنائي وبمقتضاه يمتد التشريع الجنائي ليطبق على الجرائم التي ترتكب في الخارج وبصرف النظر عن جنسية مرتكبها،ويستند هذا الامتداد إلى ما للدولة من حق في الدفاع الذاتي ضد كافة صور الاعتداء على مصالحها الأمنية ولو وقعت خارج إقليمها.

واخذ المشرع الفرنسي بمبدأ العينية بالنسبة لجرائم معينة وردت على سبيل الحصر فالمادة 113\10 من قانون العقوبات الفرنسي نصت على تطبيق القانون الفرنسي على الجنايات و الجنح التي ترتكب في الخارج والتي تشكل اعتداءا على المصالح الأساسية للأمة المنصوص عليها في الباب الأول من الكتاب الرابع،وكذلك على جرائم تقليد وتزوير أختام الدولة وتزييف العملة المعدنية أو الورقية او السندات العامة والمعاقب عليها بالمواد1-442 2-442 و 5-442 و 15-442 و1-443 1-444

وعلى أية جناية ترتكب ضد أعضاء أو أماكن البعثات الدبلوماسية أو القنصلية في الخارج.

ويعتبر مبدأ شخصية النص الجنائي احد المبادئ التي تؤدي إلى امتداد القانون الجنائي خارج إقليم الدولة وتوسيع مساحة الاختصاص،فبمقتضى هذا المبدأ تسري قواعد القانون الجنائي على الجرائم المرتكبة خارج فرنسا متى تعلقت الجريمة بمواطن فرنسي سواء كان فاعلا أو ضحية

113\6 الجنح اشترط ان تكون معاقبا عليها في قانون الدولة المرتكبة فيها الجريمة الجنايات على مطلقها سواء عاقبت عليها الدولة أو لا

والشخصية السلبية أي جريمة معلوماتية تمثل جناية أو جنحة ارتكب على إقليم دولة أجنبية من طرف أجنبي أو فرنسي في حق فرنسي تطبق عليها مقتضيات قانون الفرنسي

8 -المشرع المغربي:

القانون المغربي بدوره يأخذ بمبدأ الإقليمية من خلال الفصول 10 11 12 من مجموعة القانون الجنائي، ويشمل إقليم المغرب الأراضي الخاضعة لسيادة المغرب والمياه الإقليمية والأنهار التي تقع داخل أراضي مغربية والبحيرات الداخلية،فضلا عن الإقليم البحري،بالإضافة الى الإقليم الجوي المتمثل في المجال الذي يرتفع فوق أراضي اليابسة وفوق المياه الإقليمية التي تدخل في السيادة المغربية،ويشمل كذلك الإقليم المغربي السفن والطائرات المغربية أينما وجدت باستثناء الحالات التي تكون فيها خاضعة لتشريع أجنبي بمقتضى قانون دولي،أياً كانت جنسية مرتكب الجريمة وبالتالي فالاختصاص يرجع للمحاكم المغربية عن كل جريمة سواء وقعت بأكملها أو جزء منها داخل المملكة المغربية حسب الفقرة 2 من المادة470 قانون المسطرة الجنائية.

فالجريمة تقع بأكملها عند ارتكاب المتهم النشاط المعاقب عليها وحدوث النتيجة على إقليم المملكة،أما إذا وقع النشاط بالمغرب ووقعت النتيجة الإجرامية في دولة أخرى فإننا نكون أمام وقوع جزء من الجريمة بالمملكة كمن يرسل من المغرب فيروسا مدمرا للمعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات لإحدى المؤسسات الفرنسية حيث ينعقد الاختصاص في هاته الحالة للمحاكم المغربية ويطبق على كثير من الجرائم المعلوماتية طالما أن الاختصاص ينعقد لمجرد وقوع أحد العناصر المكونة للجريمة أو حتى وقوع النتيجة على هذا الإقليم أو ذاك

فتطبق هذه القوانين على الرسالة ذات الطابع الإجرامي أو الصورة الإباحية التي تنشر على الشبكات العنكبوتية بصرف النظر عن الدولة التي صدرت منها هذه الرسالة،طالما انه يمكن الدخول إليها في فرنسا أو في المغرب وذلك لان تلقي المستخدم لهذه الرسالة أو تلك الصورة على إقليمه يعد أحد العناصر المكونة للجريمة كما ثم توضيح أعلاه،وذلك حتى لو كان الفعل غير معاقب عليه في بلد المنشأ

- اعتمد المشرع المغربي مبدأ عينية النص الجنائي في الفصل 12 الذي أحال على المادة 711 من ق م ج التي توجب محاكمة كل أجنبي يرتكب خارج أراضي المملكة سواء كان فاعلا أصليا مساهما أو مشاركا جناية أو جنحة ،ضد امن الدولة أو تزيف خاتم الدولة أو تزوير النقود أو أوراق بنكية متداولة بصفة قانونية او جناية ضد أعوان أو مقار البعثات الدبلوماسية أو

القنصلية أو المكاتب العمومية، وهذا الامتداد راجع للنص الجنائي راجع لكون هذه الجرائم من الجرائم الخطيرة التي تلحق الضرر بالمغرب وحده دون غيره من باقي الدول التي لا يهمها أن يمس كيان المغرب السياسي أو الاقتصادي

- وقد اخذ المشرع المغربي كنظيره الفرنسي بمبدأ الشخصية في جانبيه السلبي والايجابي، فالمادة 710 من ق م ج تنص على انه: "كل أجنبي يرتكب خارج أراضي المملكة جناية يعاقب عليها القانون المغربي إما بصفته فاعلا أصليا أو مساهما أو مشاركا يمكن متابعته والحكم عليه حسب مقتضيات القانون المغربي ،إذا كان ضحية هذه الجناية من جنسية مغربية" وهو مبدأ شخصية سلبية ،إما مبدأ الشخصية الايجابية فيستند الى الفصل 12 من م ق ج والفقرة 1 من المادة 707 من ق م ج والفقرة 1 من المادة 708 ولإعمال مبدأ الشخصية الايجابية لابد ان يكون المتهم مغربيا سواء وقت ارتكاب الجريمة أو بعدها ،فالمادة 709 من ق م ج تنص على إمكانية إجراء المتابعة ولو لم يكتسب المتهم الجنسية المغربية إلا بعد ارتكاب الجناية أو الجنحة وان يكون الفعل معاقب عليه في القانون المغربي وضعه جناية، وفق الفقرة1 من المادة 707 أو جنحة وفق 708 من ق م ج ،وان لا يكون قد صدر في حقه في الخارج حكم اكتسب قوة الشئ المقضي به في نفس الجريمة وأن يعود الفاعل إلى الأراضي المغربية سواء طواعية أو جبرا، بالإضافة إلى ضرورة وجود شكاية من طرف المتضرر أو إبلاغ صادر من طرف سلطات البلد الذي ارتكبت فيه الجنحة[38]

المطلب الثاني: الأدلة وإشكالية الإثبات

سنتناول في هذا المطلب الدليل الرقمي في الجرائم المعلوماتية (الفقرة الأولى)، وذلك قبل الحديث عن بعض الأدلة التقليدية ودورها في الجرائم المعلوماتية (الفقرة الثانية):

الفقرة الأولى: الدليل الرقمي في الجرائم المعلوماتية

ترتكز عملية الإثبات الجنائي للجرائم الرقمية على الدليل الجنائي الرقمي باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم.

فما المقصود بالدليل الرقمي؟ وهاهي خصائصه؟ وماذا يميزه عن الدليل التقليدي؟

[38]-سهام ايت خويا لحسن،مرجع سابق،ص من 157الى164

أولا: التعريف بالدليل الرقمي

يعرفه بعض الفقه على أنه مكون رقمي لتقديم معلومات في أشكال متنوعة، النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك لأجل الربط بين الجريمة والمجرم والمجني عليه، وشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ تطبيق القانون[39].كما عرفته المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001 بأنه " المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية[40].

بشكل عام يعرف الدليل الرقمي بأنه الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة، مثلا النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه، وشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ القانون[41].

ثانيا: تقسيم الدليل الرقمي

الدليل الرقمي ليس صورة واحدة بل يوجد له العديد من الصور والأشكال، وقد قسمها البعض إلى الأقسام الرئيسية التالية:

1. أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها؛
2. أدلة رقمية خاصة بالشبكة العالمية للمعلومات الأنترنيت؛
3. أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات؛
4. أدلة خاصة بالشبكة العالمية للمعلومات.

وهذا التقسيم يتطابق وتقسيم الجريمة عبر الحاسب الآلي.

ووفقا لما قررته وزارة العدل الأمريكية سنة 2002 فإن الدليل الرقمي يمكن تقسيمه إلى ثلاث مجموعات وهي كالتالي:

السجلات المحفوظة في الحاسب وهي الوثائق المكتوبة والمحفوظ مثل البريد الالكتروني وملفات برامج معالجة الكلمات ووسائل غرف المحادثة على الانترنيت؛

---

[39]-عبد الناصر محمد محمود فرقي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة،جامعة نايف العربية للعلوم الأمنية، الرياض 2007، ص 130.

[40]-علي أحمد نعمان ضياء،الغش المعلوماتي الظاهرة والتعليقات،سلسلة الدراسات القانونية في المجال المعلوماتي،مراكش 2011، ص 283.

[41]-ممدوح عبد الحميد عبد المطلب البحث والتحقيق الجنائي الرمي في جرائم الكمبيوتر والأنترنيت، دار الكتب القانونية، مصر ، 2006، ص 88

السجلات التي تم إنشاؤها بواسطة الحاسوب وتعتبر مخرجات برامج الحاسوب، وبالتالي لم يلمسها الإنسان مثلا سجلات الهاتف وفواتير أجهزة السحب التالي: ATM.

السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب، ومثال ذلك أوراق العمل المالية التي تحتوى عل مدخلات تم تلقيمها إلى برامج أوراق العمل مثل Excel، ومن تم تمت معالجتها من خلال البرامج بإجراء العمليات الحسابية عليها[42]

ثالثا: الدليل الجنائي الرقمي وتميزه عن نظيره التقليدي

يتميز الدليل الرقمي عن الدليل الجنائي الرقمي بالخصائص التالية:

1. باستخدام التطبيقات والبرامج الصحيحة، يكون من السهولة تحديد ما إذا كان الدليل الرقمي قد تم العبث فيه أو تعديله وذلك لإمكانية مقارنته بالأصل؛
2. الصعوبة النسبية لتحطيم أو محو الدليل، حتى في حالة إصدار أمر من قبل الجاني بإزالته من أجهزة الكمبيوتر، فيمكن للدليل الرقمي أن يعاد تظهيره من خلال الكمبيوتر ديسك[43]؛
3. الأدلة الجنائية الرقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان[44].

رابعا: الخصائص التي يمتاز بها الدليل الاليكتروني

1. الدليل الالكتروني دليل علمي: ما ينطبق على الدليل العلمي ينطبق على الدليل الاليكتروني، فالأول يخضع إلى لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن هي قاعدة أن القانون مسعاه العدالة أم العلم فمسعاه الحقيقة، إضافة إلى أنه يجب عدم تعارضه مع القاعدة العلمية السليمة، فإن الدليل الرقمي له ذات الطبيعة إذ لا يجب أن يخرج الدليل العلمي عما توصل إليه العلم الرقمي وإلا فقد معناه.
2. الدليل الاليكتروني ذو طبيعة تقنية: لا وجود لدليل إليكتروني خارج البيئة التقنية الرقمية وأن يكون مستوحى أو مستنبط أو حتى مستجلبا من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية وهي في إطار جرائم الانترنيت ممثلة في العالم الرقمي

[42]-عبد الناصر محمد محمود فرقي،محمد عبيد سيف سعيد المسماري، م.س، ص 14
[43]-ممدوح عبد الحميد عبد المطلب، م.س، ص 91-92
[44]-عبد الناصر محمد محمود فرقي، محمد عبيد سيف المسماري، م.س، ص 15

الذي يطلق عليه العالم الافتراضي وهو العالم الكامن من أجهزة الحاسوب الآلي والخوادم والشبكات؛

3. صعوبة التخلص من الدليل الاليكتروني: موضوع التخلص من الدليل الاليكتروني باستخدام التخلص من الملفات في الحاسب الآلي أو الانترنيت كخاصية DELET ...الخ. لا تعد من العوائق التي تحيل دون استرجاع الملفات المذكورة إذ تتوفر برمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد الملفات التي يتم إلغاؤها أو إزالتها[45].

خامسا: صعوبة جمع الدليل الرقمي

إن جمع الأدلة الرقمية من بروتوكولات النقل والشبكات والاتصالات يمكن أن يشكل صعوبة نسبية من وجهة نظر أجهزة إنفاذ القانون، فهي تحتوي على كمية هائلة من المعلومات التي قد تفيد البحث والتحقيق، إلا أن الصعوبة في جمع هذه المعلومات الجنائية أنها عادة ما تكون مختلطة بغيرها من معلومات مستخدمي الكمبيوتر الأبرياء مما قد يشكل تهديدا لخصوصية هؤلاء ويعتبر في ذات الوقت ضبطا بدون تفويض أو تصريح أو أمر قانوني أو قضائي، لذلك تعتمد بعض منظمات تشغيل الكمبيوتر أو الشبكات المعلوماتية إلى عدم إفشاء أسرار جميع ملفات الولوج الخاصة بالمتورطين فقط بناء على أمر قضائي[46].

سادسا: البرامج المستخدمة في جمع الأدلة الاليكترونية

من بين الطرق والأدوات التي تساهم في جمع الأدلة الاليكترونية نجد:

1. برامج إذن التفتيش: هو برنامج قاعدة البيانات، يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل؛

2. قرص بدأ تشغيل الكمبيوتر: هو قرص يمكن المحقق من تشغيل الكمبيوتر إذا كان نظام التشغيل فيه محميا بكلمة المرور، ويجب أن يكون القرص مزدوجا ببرامج مضاعفة المساحة، فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب؛

[45]-علي أحمد ضياء نعمان ، م.س، ص 296

[46]-ممدوح عبد الحميد عبد المطلب، م.س، ص 93

3. برامج معالجة الملفات : الهدف منه أنه يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية كما يمكن من البحث على كلمات معينة أو عن أسماء ملفات أو غيرها؛

4. برامج النسخ: هو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي أو على التوالي وهو برنامج مقيد للحصول على نسخة من المعلومات قبل أية محاولة لتدميرها من جانب المتهم؛

5. برامج كسف الدسك: الهدف من الحصول على محتويات القرص المرن مهما كانت أساليب تهيئة القرص وهذا البرنامج له نسختان عادية وخاصة بالأفراد ونسخة خاصة بالشرطة؛

6. برامج الاتصالات: يستطيع هذا البرنامج ربط جهاز حاسوب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات تعود حفظها في جهاز نسخ المعلومات تم إلى القرص الصلب [47].

الفقرة الثانية: بعض وسائل الإثبات التقليدية ودورها في الجرائم المعلوماتية

أولا: بعض وسائل الإثبات التقليدية ودورها في الجرائم المعلوماتية

تمثل وسائل الإثبات أهمية خاصة إذ أن الحق موضوع التقاضي يتجرد من كل قيمة إذا لم يقم الدليل على الواقعة التي يستند إليها.

لكن التطور في شبكة الأنترنيت سوف يقود دون شك إلى تغيير كبير إذا لم يكن كليا في المفاهيم السائد حول الدليل[48]

9 -الشهادة:

الشهادة في الجريمة المعلوماتية لا تختلف من حيث ماهيتها عنها في الجريمة التقليدية، وأمر سماع الشهود متروك للمحقق ومرتبط بظروف التحقيق. والشهادة في الجريمة المعلوماتية ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، الذي تكون

[47]-عبد الناصر محمد محمود فرقي، محمد عبيد سيف سعيد المسماري، م. س، ص 21

-عبد الله ادعول، الدليل الليكتروني في الإثبات الجنائي، رسالة لنير دبلوم الماستر في القانون الخاص ، ماستر العلوم الجنائية والأمنية، كلية العلوم [48]القانونية والاقتصادية والاجتماعية ، جامعة القاضي عياض مراكش، 2011-2012، ص 41.

لديه معلومة جوهرية أو هامة لازمة للدخول في نظام المعالجة الآلية للبيانات ويطلق عليه اسم الشاهد المعلوماتي.

والشاهد المعلوماتي بهذا المفهوم قد يكون واحد من عدة طوائف منها:

أ -**مشغلوا الحاسب الآلي:** هم الخبراء الذين تكون لديهم الدراية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به واستخدام لوحة المفاتيح وتكون لديهم معلومات عن قواعد كتابة البرامج؛

ب **المحللون**: المحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة واستنتاج العلاقات الوظيفية منها ، كذلك يتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات؛

ت **المبرمجون**: هم الأشخاص المتخصصون في كتابة أوامر البرامج؛

ث **مهندسوا الصيانة والاتصالات:** وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به؛

ج **مديروا النظم:** وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[49].

ويعتمد القضاء الزجري أساسا على الشهادات في بناء قناعاته، حيث اعتمدت محكمة الإستئناف ببني ملال على الشهادة أساسا للقول بثوب المنسوب إلى المتهم، من حيثيات قرارها: " وحيث أكد الشاهد عبد العزيز... أن المتهم سرق بطريقة معلوماتية حوالة بعد أن غير رقم الصفقة ومبلغها.

وهي شهادات قضائية تثبت إدانة المتهم من أجل المنسوب إليه"[50].

10 - الخبرة:

هي وسيلة من وسائل الإثبات المباشرة التي يلجأ فيها القضاء إلى الغير للاستعانة به في أمور تقنية يستعصى عليه معرفتها من أجل الوصول إلى اكتشاف الحقيقة، وقد كرس المشرع المغربي مشروعية لجوء قاضي التحقيق إلى الخبرة في الفصل 1 م 194 م.ج حيث جاء فيها: " يمكن لكل هيئة من هيئات التحقيق أو الحكم كلما عرضت مسألة تقنية أن تأمر بإجراء خبرة إما تلقائيا وإما بطلب من النيابة العامة أو من الأطراف". كذلك خول المشرع المغربي للنيابة

40 بلمحجوب ادريس ، تأثير الجريمة الاليكترونية على الائتمان المالي ، سلسلة الندوات بمحكمة الاستئناف بالرباط، العدد 17، مطبعة الأمنية الرباط،2014، ص 147

41 – قرار جنائي عدد 11/48 بتاريخ: 2011/03/10 ملف رقم: 2011/48 (غير منشور)

العامة في الفقرة الأخيرة من المادة 47 من قانون المسطرة الجنائية التي جاء فيها: " يمكن لوكيل الملك للضرورة البحث إذا عرضت عليه مسألة فنية أن يستعين بأهل الخبرة والمعرفة".

إنطلاقا من هذه المواد أعطى المشرع المغربي الضوء الأخضر لكل هيئة من هيئات التحقيق أو الحكم وكذا النيابة العامة اللجوء إلى الخبرة متى عرضت عليهم مسألة فنية أو تقنية شأن جرائم المس بنظم المعالجة الآلية للمعطيات قصد التثبيت منها لكشف الحقيقة[51].

ومن العمل القضائي الذي وقفنا عليه بخصوص الاعتماد على الخبرة التقنية في مجال الإثبات المرتبط بالجرائم المعلوماتية، ما أوردته المحكمة الإبتدائية بمراكش في أحد أحكامها الصادرة حديثا، إذ ورد في حيثياته: " وحيث إن الخبرة التقنية التي أنجزت من طرف المختبر الجهوي لتحليل الآثار الرقمية التابع للمصلحة الولائية للشرطة القضائية بمراكش والتي انصبت على محتويات الهواتف النقالة الثلاثة المحجوزة من المتهمين قد أسفرت على مكالمات وصور وصولات استلام وتحويل أموال بين المتهمين عبر تقنية – الواتساب- تدل على تعاملهما في إطار تحويل واستلام حوالات مالية،ولا يمكن أن يستشف من تقرير الخبرة المذكور أي دليل على وجود أية عملية تزوير محررات أو وثائق معلوماتية منجزة من قبلهما. وحيث تبين للمحكمة أن العناصر التكوينية لهذه الجنحة لا أثر لها واقعيا، وبالتالي خلصت إلى عدم مؤاخذة المتهمين من أجلها." [52]

ثانيا: الإثبات في البيئة الالكترونية بين الحرية والتقييد

ينطلق الحديث حول مدى حرية الحصول على الدليل لإثبات الجريمة الالكترونية من الخلاف الفقهي حول صور الجريمة الالكترونية، إذ يمكن جمع صور الجريمة في فئتين: الأولى تضم مختلف الجرائم التقليدية التي تتم بوسائل إليكترونية، الفئة الثانية هي الجرائم التي تستهدف النظم والبرامج وقواعد البيانات المعلوماتية، هذا يمكن تصور تقييد الإثبات كقاعدة[53].

11 مدى حرية الإثبات في الجريمة التقليدية المرتكبة بوسيلة إليكترونية

مفهوم نظام الإثبات الحر: يقصد به أن المشرع قد ترك للقاضي الجنائي كقاعدة عامة حرية تقديم الأدلة المقدمة في الدعوى دون أن يقيده بأي دليل معين، كما ترك له حرية ترجيح

[51]-عبد الله ادعول، م.س، ص 64-65

[52]-حكم عدد 7929 بتاريخ: 2017/10/03، ملف جنحي رقم: 2017/2103/6256 (غير منشور).

[53]-بلمحجوب ادريس، م.س، ص 150-151

أي دليل يقتنع به على آخر لإدانة المتهم أو تبرئته، وبمقتضى هذا النظام يترك للخصوم الحرية في تقديم أي دليل وللنيابة العامة إثبات التهم بكل الطرق المشروعة

نظام الإثبات الحر هو الذي يحكم الجرائم بصفة عامة ووجد أنصار هذا النظام صداه في معظم التشريعات الجنائية، ومنها التشريع المغربي عندما نص في المادة 286 من قانون المسطرة الجنائية مادة تؤكد أن الأطراف سواء جهة الإدعاء أو المتهم كامل الحرية في أن يقدموا ما يتوفرون عليه من وسائل الإثبات أمام المحكمة، وتناقش شفاهيا حتى يحصل الاقتناع الوجداني للمحكمة التي تنظر في النزاع الجنائي.

في هذا السياق يطرح التساؤل حول ما إذا كانت الطريقة التي ارتكبت بها الجريمة؟

هذا التساؤل يبقى مشروعا متى تعلق الأمر بالجرائم التقليدية التي يتم ارتكابها بطرق الكترونية، ففي الوقت الذي نسلم فيه بكون حرية الإثبات تبقى الأصل ما دام الأمر يتعلق بجريمة تقليدية، نجد أن ارتباط هذا الإثبات بالوسيلة التي ارتكبت بها الجريمة يثير صعوبة بين ما يدخل في استطاعة الأطراف أن يثبتوه بقدراتهم الخاصة وما لا يدخل، فتطرح فكرة إثبات ارتكاب جريمة تقليدية ما ونسبتها إلى شخص معين تتعلق بضرورة إثبات أن الشخص مرتكب الجريمة ارتكبها بوسيلة الكترونية تدخل تحت سيطرته وهو من يتحمل المسؤولية عنها.

هذا التحدي الذي تطرحه الوسائل الاليكترونية في إثبات الجرائم العادية ما جعل واضعي اتفاقية بودابيست يؤكدون على فكرة ضرورة ملائمة القوانين الداخلية لما جاءت في تلك الاتفاقية.

بذلك يظهر أن الإثبات في الجرائم التقليدية التي يتم اقترافها بوسائل اليكترونية يذهب نحو التقييد وهو ما يتماشى مع طبيعة تلك الوسائل التي يستحيل على الأفراد العاديين وحى الأجهزة المكلفة بإنفاذ القانون أن تتوفر عليها اللهم إذا ما خول لها القانون إمكانية التعاون مع الجهات المتحركة للخدمات المعلوماتية.

12 ارتباط تقييد الإثبات في الميدان الجنائي بالجريمة الالكترونية

يقصد بنظام الإثبات المقيد: أن المشرع هو الجهة التي تتولى مقدما تحديد الأدلة التي تقبل في الإثبات والقيمة القانونية الخاصة بكل دليل، فالقاضي لا يملك في ظل هذا النظام أن يختار دليلا لم يسمح به المشرع ولا أن يحيطه قيمة أكبر أو أقل مما رسمه المشرع[54].إذ أن المشرعون الوطنيون واستلهاما منهم للمبادئ التي جاءت بها إتفاقية بودابيست والاتفاقية المرتبطة بها،

[54]-عبد الله ادعول ، م.س ، ص 58-59

شرعوا في وضع مجموعة من المقتضيات القانونية التي تفرض على مزودي الخدمات الالكترونية التعاون مع الأجهزة المكلفة بالبحث عن الجرائم الالكترونية.

ويظهر أن انحصار الحصول على الدليل الالكتروني من طرف الجهات الرسمية المكلفة بالتحقيق في الجرائم الاليكترونية وإلزام الجهات المشرفة على تقديم الخدمات الالكترونية على تزويدهم بالبيانات والمعطيات الضرورية يدخل في نطاق مفهوم الاستثناء الوارد بقانون المسطرة الجنائية الذي نصت عليه المادة 288 من نفس القانون[55].

كما أن القوانين المنظمة لوظائف الجهات المكلفة بتسيير وحفظ البيانات الشخصية ذات الطبيعة الالكترونية ترفض على هذه الجهات الحفاظ على السر المهني إلا ما استثني بمقتضى القانون، لذلك فرغبة الأفراد العاديين في الحصول على تلك المعطيات والبيانات تصطدم بهذا المقتضى القانوني ما يجعل الحصول على الدليل المستعمل في إثبات الجريمة الالكترونية يخضع لشكليات وقيود قانونية لم تنص عليها مواد المسطرة الجنائية، بل نصت عليها قوانين خاصة تدخل في نطاق مفهوم " الأحكام الخاصة الواردة في المادة 288 من قانون المسطرة الجنائية".

[55]-بلمحجوب ادريس، م.س ، ص 152-153

خاتمة

صفوة القول، ففي اعتقادنا فإنه وبالرغم من المجهودات الجبارة المبذولة إن على الصعيد الوطني أو الدولي لمكافحة الإجرام المعلوماتي، فإننا نعتقد أن النصوص القانونية، سيما تلك المتعلق بجانب البحث والتحقيق، لم تواكب بعد التطور الذي عرفه – ويعرفه- هذا النوع من الإجرام، بل التطور الإجرامي في البيئة المعلوماتية يسير بسرعة كبيرة قد لا تواكبه القنوات التشريعية التقليدية عن سن النصوص ووضعها والمصادقة عليها، فقد يحدث في الفترة – التي قد تكون وجيزة – بين وضع النص القانوني ومناقشته والمصادقة عليه ونشره في الجريدة الرسمية عدت تحولات في ميدان الإجرام المتطور، وهو ما سيجعلنا في دوامة مفرغة بين ظهور نمط جديد من الأفعال المضرة، سيما في مجال المعلوميات، وبين وضع النصوص التشريعية الملائمة.

وعيه سجلنا مجموعة من الملاحظات ووضعنا بعض الاقتراحات التي ظهرت لنا بعد إنجاز هذا العرض والتي نحددها في التالي:

الملاحظات:

1. تتسم الجرائم المعلوماتية بحداثة أساليب ارتكابها وسرعة تنفيذها وإخفاء معالمها؛
2. لا زال الاعتماد بشكل كبير على القواعد الإجرائية العادية في مجال البحث والتحقيق في هذه الجرائم؛
3. إشكال الاختصاص الذي يطرحه البحث والتحري عنها؛
4. يعاني مجال البحث والتحقيق من صعوبة إثبات الجرائم المعلوماتية بالنظر إلى طبيعة الأدلة التي تقوم عليها هذا النوع من الجرائم؛
5. بذلت الدولة المغربية جهودا كبيرة لمواجهة الظاهرة الإجرامية في مجال المعلوميات من خلال إحداث مؤسسات أخرى يعهد إليها البحث في هذا النوع من الجرائم إلى جانب الأجهزة الأصلية المنظمة بمقتضى قانون المسطرة الجنائية كاللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، والمديرية العامة لأمن نظم المعلومات (DGSSI)، والخلايا المتخصصة في الجريمة المعلوماتية بجهاز الأمن الوطني، وإنشاء

مجموعة من المختبرات التابعة لذات الجهاز على صعيد العديد من المدن المغربية كالمختبر الجهوي لتحليل ومعالجة الآثار الرقمية بفاس.

الاقتراحات:

1. ضرورة وضع إستراتيجية واضحة لمواجهة الجرائم المعلوماتية؛
2. تعديل قانون المسطرة الجنائية حتى يستجيب لمتطلبات البحث والتحقيق في المجال المعلوماتي، وذلك بإفراد قواعد خاصة تحقق السرعة والفعالية؛
3. دعم المؤسسات المكلفة بالبحث والتحقيق ماديا ولوجيستيكيا، وبموارد بشرية مؤهلة مع الحرص على التكوين والتكوين المستمر في مجال مكافحة الجرائم المعلوماتية.

قائمة المراجع:

أولا: الكتب

1ـ الكتب العامة

1 - الحبيب البيهي، شرح قانون المسطرة الجنائية الجديد، منشورات المجلة المغربية للإدارة المحلية التنمية، سلسلة مؤلفات وأعمال جامعية، مطبعة المعارف الجديدة الرباط، ط 1 ،س 2004،

2 - أحمد الخمليشي، شرح قانون المسطرة الجنائية الجزء الأول، دار نشر المعرفة للنشر والتوزيع الرباط، مطبعة المعارف الجديدة الرباط، ط 6،س 1999،

3 - السياسة الجنائية بالمغرب: واقع وآفاق" المجلد الأول، الأعمال التحضرية للمناظرة الوطنية التي نظمتها وزارة العدل بمكناس أيام 09 و 10 و 11 دجنبر 2004، منشورات جمعية نشر المعلومة القانونية والقضائية، سلسلة الندوات والأيام الدراسية عدد 3، ط 3 ، 2004،

4 - أحمد قيلش، محمد زنون، الشرطة القضائية الكتاب الأول، مطبعة النجاح الجديدة، الدرا البيضاء، 2013؛

2ـ الكتب المتخصصة:

1 - مصطفى محمد موسى،دليل التحري عبر شبكة الانترنت،دار الكتب القانونية،المجلة الكبرى،مصر،2005.

2 - مصطفى محمد موسى،التحقيق الجنائي في الجرائم الالكترونية،الطبعة1 ،مطابع الشرطة،شارع المرور،الدراسة القاهرة،2009.

3 - عبد الرحيم بن بوعيدة , ضياء نعمان , موسوعة التشريعات الالكترونية المدنية والجنائية , المطبعة والوراقة الوطنية , مراكش الجزء الأول 2010.

4 - عبد الناصر محمد محمود فرقي، محمد عبيد سيف المساري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، جامعة نايف العربية للعلوم الأمنية، الرياض 2007؛

5 - علي أحمد نعمان ضياء، الغش المعلوماتي الظاهرة والتعليقات، سلسلة الدراسات القانونية في المجال المعلوماتي ، مراكش، 2011.

6 - ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنيت، دار الكتب القانونية، مصر، 2006.

7 - بلمحجوب إدريس، تأثير الجريمة الالكترونية على الائتمان المالي، سلسلة الندوات محكمة الاستئناف بالرباط، العدد 17، مطبعة الأمنية، الرباط،2014؛

8 - نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع عمان،س 2008،

9 - محمد الادريسي العلمي المشيشي , المؤسسات القضائية , منشورات جمعية تنمية البحوث والدراسات القضائية , الرباط , الجزء الأول 1991.

10 - عبد الناصر محمد محمود فرغلي , محمد عبيد سيف سعيد المسماري , الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية .دراسة تطبيقية مقارنة , جامعة نايف العربية للعلوم الأمنية , الرياض , 2007. .PDF؛

11 - أحمد أيت الطالب، مساطر المعاينة والبحث الجنائي،مطبعة المطبعة الجديدة الرباط، 2014.

ثانيا: الرسائل والأطروحات

1 - عبد الله ادعول،الدليل الالكتروني في الإثبات الجنائي،رسالة لنيل دبلوم الماستر في القانون الخاص،ماستر العلوم الجنائية والأمنية، كلية العلوم القانونية والاقتصادية والاجتماعية،جامعة القاضي عياض،مراكش،2012-2011

2 - سهام أيت خويا لحسن،الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، رسالة لنيل شهادة الماستر في القانون الخاص تخصص العلوم الجنائية الملحقين والأمنية، السنة الجامعية: 2016-2017؛

3 - كوثر فرام،: الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية التدريب القضائيين الفوج 42 2007-2009 ،

ثالثا:المواقع الالكترونية:

1. www.alkanonia.com ،تاريخ الولوج 24-12-17،نشر به مقال للباحث يوسف قجاج، الجريمة الالكترونية واشكالية القواعد الاجرائية.

2. www.maghress.comK ، تاريخ الولوج: 2017/12/24، مقال لرضوان حيافي بعنوان: إحداث فرق وطنية وجهوية للشرطة القضائية؛
3. موقع الجامعة www.aljami3a.com , تاريخ الزيارة 24.12.2017.
4. www.Archive.Icann.org ، الموقع الرسمي لهيئة الأيكان.

رابعا: الإتفاقيات

1 - إتفاقية بودابيست 2001 لسنة؛
2 - الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2011.

الفهرس