مقدمة

لقد أدى التطور التكنولوجي الذي شهده العالم في العصر الحديث إلى أحداث ثورة حقيقية شكلت قفزة نوعية في حياة الأفراد والمجتمعات بسبب دخولها في جميع مجالات الحياة من أبسط تفاصيلها إلى أكثرها تعقيدا ، فسهلت سبل العيش ويسرت طرق الاتصال وأدت إلى حرية ومرونة وسلامة تنقل الأشخاص والأموال والمعلومات.....

ولقد بلغت تلك الثورة أوج تطورها وازدهارها حينما تم التزاوج والاندماج بين مجالي الحوسبة والاتصال الذي أدى إلى ظهور أنماط مستحدثة من الجرائم لم تتوقف عند حد اضفاء الطبيعة الالكترونية على ما كان موجودا من جرائم تقليدية وإنما تعداها إلى استحداث جرائم أخرى تمس بعض القيم المتصلة بحقوق المجتمع وأفراده والاقتصاد الرقمي وتهدد المصالح العليا للدول وتتسبب في زعزعة أمنها واستقرارها... عن طريق الاعتداء على برامج الحاسوب واختراق الشبكات والمواقع ... فاتسعت دائرة الإجرام ولم تعد آثار الجريمة تقتصر على بلد بعينه وإنما تمتد إلى العديد من البلدان مما أضفى عليها وصف الجريمة العابرة للحدود بسبب ما يتمتع به مرتكبها من إمكانية للدخول عبر شبكة الأنترنت إلى أنظمة معلومات العديد من البلدان دون أن يكلفه ذلك عناء التنقل من مكان أقامته ، ولعل تلك الصفة وغيرها مما تتمتع به تلك الجرائم كان السبب وراء الاختلاف في تعريفها وحول المصطلح الذي يتعين إطلاقه عليها، فتعددت تسمياتها من جرائم الكترونية، جرائم سيبرانية، جرائم معلومات، جرائم رقمية، جرائم افتراضية، جرائم انترنت، تكنولوجيا معلومات.....

بيد أن ما شكلته الجرائم الالكترونية من مخاطر وما تسببت فيه من تهديد قد دفع جميع دول العالم إلى التحرك من أجل وضع آليات مناسبة لمحاربتها والحد من آثارها المدمرة فتداعت إلى سن القوانين وابرام الإتفاقيات ولم يكن المشرع الموريتاني استثناء من ذلك فقد استشعر تلك المخاطر بفعل ما شهدته البلاد من توسع في استخدام نظم المعلوماتية داخل مختلف أجهزة الدولة وغيرها، وما تم تسجيله من انتشار مهول لوسائل الاتصال بين أفراد المجتمع وإفراط غير مسبوق في استخدام وسائل التواصل الإجتماعي من فيسبوك – يوتوب ـ تويتر - واتساب ـ فيبر.....

وما ترتب عن ذلك من تحديات واشكالات قانونية ناتجة عن طبيعة ونوع الجرائم المترتبة على الوافد الجديد بحيث لم يعد بمقدور قواعد القانون الجنائي بشقيه الموضوعي والإجرائي مواجهة تلك الجرائم بفاعليته المعهودة في مجال الجرائم التقليدية ، الشئ الذي دفع بالمشرع الموريتاني إلى سن القانون رقم 07/2016 المتعلق بالجريمة السيبرانية والذي حاول من خلاله وضع مجموعة من القواعد الموضوعية المتعلقة بالأساس بتعريف ما تضمنه هذا القانون من مفاهيم وتحديد موضوعه ومجاله وأنواع الجرائم وعقوباتها والمسؤولية الجنائية للأشخاص الاعتبارية عنما قد ترتكبه في إطار ما حدده هذا القانون من جرائم ولم يستثن من تلك المسؤولية سوى الدولة والمجموعات المحلية والمؤسسات العمومية ، وإلى جانب ما حدده من قواعد موضوعية فقد عمد إلى وضع بعض القواعد الإجرائية الخاصة بالجرائم السيبرانية سواء من حيث آليات البحث والتحقيق أو ضوابط الاختصاص والحكم في مسعا منه لتعزيز ما تضمنه قانون الإجراءات الجنائية من قواعد باعتباره التشريع الإجرائي العام الذي تخضع له تلك الجرائم ابتداء من عملية البحث مرورا بالتحقيق وانتهاء بالحكم فيها.

وعلى ضوء تلك المقاربة يكون من الطبيعي أن نتساءل عن مفهوم وطبيعة وخصائص الجرائم الالكترونية وعما وضعه المشرع الموريتاني من آليات للبحث والتحقيق والحكم فيها؟ وما وفره من وسائل للحد من مخاطرها ومعالجة ما تثيره من إشكالات؟
تلك التساؤلات وغيرها مما يثور من إشكالات بشأن الجرائم الاكترونية سنحاول الإجابة **عليها من خلال الخطة التالية:**

المبحث الأول: مفهوم الجرائم الالكترونية
المطلب الأول: ماهية الجرائم الالكترونية
المطلب الثاني: أركان الجرائم الالكترونية
المبحث الثاني: قواعد إجراءات التحقيق والبت في الجرائم الالكترونية
المطلب الأول: البحث والتحقيق في الجرائم الالكترونية
المطلب الثاني : البت في الجرائم الالكترونية

المبحث الأول: مفهوم الجرائم الإلكترونية

للوقوف عل مفهوم الجرائم الإلكترونية لابد من تحديد ما هيتها وذلك من خلال وضع إطار عام لها يمكن من تعريفها وتحديد خصائصها وأنواعها وطبيعتها القانونية والبحث في أركانها وما تثيره من إشكالات

المطلب الأول: ما هية الجرائم الإلكترونية

يمكن تحديد ما هية الجرائم الإلكترونية من خلال الوقوف على ما أورده الفقه من تعريفات لهذه الجرائم وما حدده من خصائص وأثاره من إشكالات أثناء محاولته تحديد طبيعتها القانونية إضافة إلى ما حدده القانون من أنواع لهذه الجرائم.

الفرع الأول : تعريف الجرائم الإلكترونية

من الصعب جدا تقديم تعريف جامع للجرائم الإلكترونية نظرا لارتباطها بمجال يعد من أكثر المجالات في العصر الحديث تحولا وتغيرا بفعل ما شهدته الأدوات والوسائل الإلكترونية من تطور هائل وبسبب الزاوية التى ينظر من خلالها كل فقيه من فقهاء القانون الجنائي لهذه الجريمة ، ذلك أن البعض يركز في تعريفه لها على الزاوية الفنية والبعض على وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها، وهو ما أدى إلى عدم الاتفاق على المصطلح الذي يتعين ربطه بهذه الجريمة والتسمية القانونية لها – الكترونية –رقمه –افتراضية – سيبرانية – حاسوب – معلوماتية .....
ومهما كانت تسمية هذه الجريمة فقد أحدثت ثورة في مجال الإجرام نظرا لطبيعتها المتأتية من محلها وأداة ارتكابها والتي سمحت لمرتكبها تنفيذها في جو من الأمن والهدوء التام ودون الانتقال من مكانه ، بمجرد كبسه زر قد يتهاوى اقتصاد أكبر الشركات العالمية، ولعل ذلك من ضمن .الأسباب التي دفعت بالبعض إلى تسميتها بالجريمة الناعمة

وأيا كان نوع الاعتداء واختلافه باختلاف الفوارق بين الجرائم الواقعة على الحاسب الآلي وتلك المتعلقة بالإنترنت فقد أصبح من الصعوبة بمكان تلمس تلك الفوارق وجدوائيتها بسبب ما وصل إليه الواقع التقني من اندماج بين ميداني الحوسبة والاتصال والذي أدى إلى ظهور مصطلح (ciber Grme)أو الجريمة السيبرانية ، وإلى محاولة محو ما وضعه البعض من فوارق للتمييز بين تلك، الجرائم تركزت بالأساس على محلها الذي يتعلق في جرائم الحاسوب بالاعتداء على مجموعة الأدوات المكونة للحاسب وبرامجه والمعلومات المخزنة به في حين تتحقق في جرائم الإنترنت من خلال نقل المعلومات والبيانات بين أجهزة الحاسب عبر خطوط الهاتف أو الشبكات الفضائية ، غير أن التزاوج والاندماج بين ميداني الحوسبة والاتصال لم يمنع فقهاء القانون الجنائي من الانقسام حول تحديد مفهوم الجريمة الالكترونية ما بين مستند في تعريفها على مفهوم ضيق يتعلق بكون هذه الأخيرة لا تتحقق إلا إذا كان الفعل الإجرامي يستهدف النظم المعلوماتية في ذاتها الشيء الذي يستبعد الحالات التي تستعمل فيها وسائل التكنولوجيا الحديثة في ارتكاب الجرائم التقليدية ويعد من أبرز أنصار هذا الاتجاه الأستاذ(سيبرSiber) الذي يعرف الجريمة المعلوماتية بأنها (كل سلوك مشروع أو غير مشروع مرخص به يهم المعالجة الآلية للمعطيات أو إرساله)[1] .

أما الاتجاه الثاني فقد استند في تعريفه للجريمة الالكترونية على المفهوم الواسع لهذه الجريمة معتبرا إياه كل سلوك مجرم كان محله الإلكترونيات أو تم استخدامها كأداة في ارتكابه ومن أبرز أنصار هذا الاتجاه الاستناد ماس Masse والفقيه الألماني tiedemenn.

ويعد هذا الاتجاه الأقرب للصواب في تحديد مفهوم الجريمة الالكترونية لاعتماده في ذلك على استخدام الحاسب الآلي في كل نوع من أنواع السلوك غير المشروع والاستجابة للفضاء الرقمي واعتبار الجريمة الالكترونية جريمة من نوع خاص وهو ما تبناه المؤتمر العاشر للأمم المتحدة المتعلق بمنع الجريمة ومعاقبة المجرمين من خلال تعريفه للجريمة الالكترونية معتبرا إياها كل سلوك غير مشروع يمكن ارتكابه بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل حاسوب وتشمل تلك الجرائم من الناحية المبدئية الجرائم التي يمكن ارتكابها في بيئة الكترونية و هو نفس ما يمكن أن نتلمسه من خلال ما نص عليه المشروع الموريتاني في القانوني رقم 07/2016 المتعلق بالجريمة السيبرانية الذي نص في القسم الثاني منه المعنون بموضوع ومجال هذا القانون على أنه يتعلق بكل الجنايات والجنح المرتبطة باستخدام تقنيات الإعلام والاتصال باستثناء البث الإذاعي والتلفزي وعلى كل الجرائم المرتكبة بواسطة نظام معلوماتي ومع ذلك يظل التباين الحاصل بين هذين الاتجاهين حول تحديد مفهوم الجريمة الالكترونية يلغي بظلاله على أية معالجة قانونية تستهدف وضع تعريف لها نظرا لما يحمله من معايير للتمييز بين الجريمتين التقليدية والالكترونية والتي يبدو أن أصحاب الاتجاه الضيق قد ركزوا في ذلك على التمييز بين محل الجريمة وآداة ارتكابها معتبرين أن أية جريمة لا يمكن أن تتصف بالوصف الالكتروني بمجرد ارتكابها بوسيلة الكترونية وإنما تظل من قبيل الجرائم التقليدية

[1]- لقد اطلق المشروع الموريتاني على الجرائم الالكترونية مصطلح الجرائم السيبرانية وذلك من خلال القانون رقم07/2016 الصادر بتاريخ: 20/يناير 2016 المتعلق بالجريمة السيبرانية.

كالسرقة و التحايل وخيانة الأمانة..... عكس الجرائم التي يكون محلها أو موضوعها المعطيات المخزنة في نظم المعالجة الآلية التي تعد من قبيل الجرائم الالكترونية الصرفة.
وبغض النظر عن التباين الحاصل بين هذين الاتجاهين يجب أن يكون أي مصطلح يتم إطلاقه على هذا النوع من الجرائم شاملا لنقطتي التقنية المتمثلة في الحوسبة والاتصال[2].

الفرع الثاني: خصائص الجرائم الالكترونية :
تتميز الجرائم الالكترونية بمجموعة من الخصائص النابعة بالأساس من طبيعتها وحقيقة مرتكبها ويمكن إجمال هذه الخصائص في النقاط التالية :
أولا : إن مرتكب الجرائم الالكترونية يتمتع في الغالب بالذكاء ويتملك قدرات وخبرات عالية في مجال أنظمة الحاسب الآلي تمكنه من اختراق أي نظام معلوماتي والقيام بما هو عازم عليه من أعمال إجرامية وهو في معظم الجرائم لا يستهدف من خلال ارتكابها الحصول على منفعة مادية وإنما بدافع الرغبة في قهر النظام الآلي .
وبما أن مجال الجرائم الالكترونية يتعلق بالحوسبة والاتصال تكون أداة ارتكابها تختلف عن أدوات ارتكابه غيرها من الجرائم.
ثانيا: الجرائم الالكترونية جرائم عابرة للحدود :
لقد أدى الانتشار المهول لشبكة الانترنت إلى أن أصبح العالم قرية واحدة يستطيع من خلالها مستخدم الشبكة العنكبوتية الدخول إلى النظام المعلوماتي لأي بلد دون عناء التنقل من مكان إقامته مما يضفي على مجال مسرح الجريمة الالكترونية الطابع العالمي ويخلق العديد من الإشكالات القانونية والإدارية والفنية بشأن السبل الكفيلة بمواجهتها خصوصا ما تعلق منها بإجراءات الملاحقة الجنائية.
ثالثا: صعوبة اكتشاف الجرائم الالكترونية : لقد أدي الطابع الافتراضي للجريمة الالكترونية إلى صعوبة اكتشافها وتتبع آثار مرتكبها لما يمتنع به هذا الأخير من قدرة فائقة على أخفاء أدلة ارتكابها من خلال التلاعب بالبيانات وتغيرها وتعديلها أو محوها من السجلات المخزنة في ذاكرة الحاسب في فترة وجيزة ، ولانعدم الآثار المادية المترتبة على ارتكابها باعتبارها العنصر الجوهري في اكتشاف الجرائم ووضع اليد على مرتكبها ، و هي بذلك تعد أقل عنفا وأكثرها اكتشافا يتم عن طريق الصدفة نظرا لقلة الإبلاغ عنها بسبب الخشية من التشهير أو عدم اكتشاف الضحية لها. مما جعل ما يتم اكتشافه منها أقل بكثير مما لم يكتشف بعد[3].
رابعا:ارتفاع الخسائر الناجمة عن الجرائم الاكترونية : لقد أدى ما شهده العصر الحديث من تطور تكنولوجي إلى ارتفاع الخسائر الناجمة عن الجرائم الالكترونية مقارنة بالجرائم التقليدية نظرا لربط شتى مناحي الحياة «تبادلات ، معاملات، خدمات .... » بالشبكات المعلوماتية ونظم المعالجة الآلية للبيانات وهو ما أكدته الشركة العالمية المختصة في حماية أمن المعلوماتية ((انتل سكريتى)) من خلال ما قدمته من أرقام تتعلق بما يلحق قطاعات الأعمال العالمية من إضرار جراء الجرائم الالكترونية حيث أكدت أن تلك

---

[2]- للتوسع أكثر في مجال تعريف الجرائم الالكترونية راجع: دياب موسى البداينة الجرائم الالكترونية المفهوم والأسباب ذ/ يا سمنية بو نعارة الجريمة الالكترونية د- كامل مطر الجريمة الالكترونية د- مفتاح بوبكر المطردي الجريمة الالكترونية والتغلب على تحدياتها نبيلة هبه الهروال الجوائب. الإجرائية لجرائم الأنترنت.
[3]-راجع د/ مفتاح بو بكر المطردي الجريمة الالكترونية والتغلب على تحدياتها مرجع سابق ود/ جعفرعلى جرائم اتكلوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة ص .98

القطاعات تخسر سنويا ما يقدر ب 400 مليار دولار بسبب الهجمات الالكترونية وأن هذه الأخير أصحبت اقتصادا متناميا قائما بذاته تبلغ قيمته ما بين 2 إلى 3 ترليون دولار سنويا وهو ما يشكل 18إلى 20% من قيمة الاقتصاد الناتجة عبر الانترنت.

الفرع الثالث:الطبيعة القانونية للجرائم الالكترونية .

أن الحديث عن الطبيعة القانونية للجريمة الالكترونية يتمحور بالأساس حول الوضع القانوني للبرامج والمعلومات وذلك من خلال تحديد ما إذا كانت ذي طبيعة مادية بحته أم أنها مجرد مجموعة من القيم المعنوية .

ولقد ترتب على الخوض في تحديد طبيعة الجرائم الالكتروني[4]. تباين واضح بين مختلف فقهاء القانون حيث انقسموا ما بين اتجاه يعتبر محل تلك الجرائم لا يعدو كونه ذي طبيعة معنوية صرفة تخرج عن مجال القيم القابلة للحيازة والاستحواذ باستثناء ما تعلق منها بمجال الملكية الفكرية ويستبعدها من مجال السرقة الذي يتطلب في الواقع أن يكون للشيء المسروق كيان مادي ملموس حتى تمكن حيازته وانتقاله ، وردا على ذلك فقد اعتبر البعض أن المعلوماتية ما هي إلا قيم قابلة الاستحواذ نظرا لما لها من قيمة اقتصادية قابلة للحيازة المشروعة لارتباطها حسب الاستاذين ViVant وcatala بمؤلفها عن طريق علاقة التبنى ، فالبرامج والمعلومات من الناحية القانونية تعد ملكا لمن ابتكرها وهو ما يفرض ضرورة الاعتداد بفكرة الكيان المادي للشيء المعنوي وقد اعتمد أصحاب هذا الاتجاه على ما توصلت إليه محكمتا النقض الفرنسية والمصرية بخصوص سرقة الكهرباء التي لا تعد في ذاتها كيانا ملموسا إلا أن مرورها عبر الأسلاك والتوصيلات يجعل منها كيانا ماديا وهو نفس ما أكدته محكمة النقض الفرنسية في حكم لها بشأن خطوط الهواتف[5].

الفرع الرابع: أنواع الجرائم الالكترونية :

حسب ما أورده المشرع الموريتاني من أحكام في القانون رقم 07/2016المتعلق بالجريمة السيبرانية فإن الجرائم الالكترونية تشتمل على العديد من الصور والأنواع كما هو مبين من خلال ما اعتمده المشرع من تقسيم لتلك الجرائم

أولا: جرائم الاعتداء على سرية وسلامة وتوفر البيانات والنظم المعلوماتية : وتشمل

1-جريمة المساس بالبيانات المعلوماتية: وهي حسب ما يفهم من خلال ما نظمه المشرع الموريتاني من أحكام في المادتيين 4 و 5 من القانون المتعلق بالجريمة السيبرانية كل اعتراض أو محاولة اعتراض عن قصد وبدون حق بواسطة وسائل تقنية خلال اتصالات غير عمومية لبيانات معلوماتية قادمة أو موجهة أو داخلة في نظام معلوماتي بما في ذلك البث أو كل قيام عن قصد أومحاولته بإلحاق ضرر أو محو أو إتلاف أو تشويه أو حذف بيانات معلوماتية.

---

[4]-راجع د/ مفتاح بو بكر المطردي الجريمة الالكترونية والتغلب على تحدياتها مرجع سابق ود /جعفرعلي جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة ص 98.

[5]-راجع د / عبد السلام بنسلمان الإجرام المعلوماتي في التشريع المغربي ص 30 أ/ ياسمينة بونعارة الجريمة الالكترونية مرجع سبق ذكره .

2-**جرائم المساس بالنظم المعلوماتية** : وتنقسم هذه الجرائم إلى :

أ –**جرائم المساس بسرية النظم المعلوماتية** : وقد اعتبرها المشرع الموريتاني من خلال

المادتين 6 و 7 من القانون المتعلق بالجريمة السيبرانية كل نفاذ أو محاولته عن قصد أو بدون حق إلى كل أو جزء من نظام معلوماتي أو الاستمرار داخله

ب- جرائم المساس بسلامة وتوفر النظم المعلوماتية : وهي حسب قانون الجريمة السيبرانية كل إعاقة أو تخطئ أو محاولته عن قصد أو بدون حق لسريان نظام معلوماتي عن طريق الدخول أو الإرسال أو إلحاق الضرر أو المحو أو الإتلاف أو التشويه أو حذف بيانات معلوماتية أو إدخال بيانات في نظام معلوماتي أو إنتاج أو بيع أو استيراد أو نشر أو استخدام أو منع أو تنازل أو مساعدة أو توفير أيه طريقة آلية برامج معلوماتية مصممة أومكيفة على أساس ارتكاب إحدى الجرائم المنصوصة في هذا القانون أو كلمة مرور أو رمز نفاذ أو بيانات معلوماتية مماثلة أو أية طريقة فنية تمكن من النفاذ إلى كل أو جزء من نظام معلوماتي بغية استخدامه لارتكاب واحدة أو أكثر من الجرائم أعلاه أو كل تواطأ عن قصد وبدون حق في المساعدة على ارتكاب تلك الجرائم.

3- **الجرائم المعلوماتية :** يقصد بها حسب نص المادتين 12و13 من قانون الجريمة السيرانية كل فعل تم ارتكابه عن قصد أو بدون حق من أجل إدخال أو تشويه أو محو أو حذف بيانات معلوماتية أو إنتاج بيانات غير أصلية بهدف استخدامها لأغراض قانونية كما لو كانت أصلية أو إلحاق الضرر بأملاك الغير أو الحصول بغير حق بصفة احتيالية أو إجرامية على ربح اقتصادي لنفسه أو لغيره عن طريق أي من تلك الأفعال أو بشكل أيا كان من أشكال المساس بسير نظام معلوماتي.

ثانيا: الجرائم المتعلقة بالمحتوى: وتشمل هذه الجرائم

1-**جرائم المساس بالملكية الفكرية والحقوق المرتبطة** : وهي حسب نص المادة 14 من القانون المتعلق بالجريمة السيبرانية كل فعل يرتكب من أجل المساس عن قصد في نطاق تجاري وبواسطة نظام معلوماتي باحد حقوق الملكية الفكرية والحقوق المرتبطة المحددة في التشريع الوطني ووفقا للإلتزمات الدولية .

2- **الجرائم المتعلقة بالمادة الإباحية :** وقد تناول المشرع الموريتاني هذه الجرائم من خلال نقطتين خصص أولاهما لتناول الجرائم المتعلقة بالمادة الإباحية بشكل عام في حين تناول في الثانية الجرائم المتعلقة بالمادة الإباحية للأطفال .

أ- الجرائم المتعلقة بالمادة الإباحية عموما: وقد تناولها المشرع الموريتاني من خلال المادتين 15 و 16 من قانون الجريمة السيبرانية معتبرا إياها كل إنتاج أو تسجيل أو عرض أو توفير أو نشر أو اقتناء أو إيراد أو تصدير صور أو أي شكل من أشكال التمثيل المرئي لمحتوى ذي طابع إباحي لنفسه أو لغيره عبر نظام معلوماتي.

ب- الجرائم المتعلقة بالمادة الإباحية للأطفال : وهي حسب المواد 17 و 18 و 20 من القانون المتعلق بالجريمة السيبرانية كل إنتاج أو تسجيل أو عرض أو توفير أو نشر أو إرسال أو تصدير أو حيازة أو تخزين أو نفاذ أو تسهيل النفاذ إلى مادة إباحية للأطفال عبر نظام معلوماتي.

3- **جرائم المساس بالقيم والأخلاق الحسنة :** وهي حسب نص المادة 21 من القانون المتعلق بالجريمة السيبرانية كل إنشاء أو تسجيل أو توفير أو نقل أو نشر رسالة نصية أو صورة أو صوت أو أي شكل آخر من أشكال التمثيل السمعي البصري الذي يمس قيم الإسلام وذلك عبر نظام معلوماتي.

4- الجرائم المتعلقة بالإعمال العنصرية والكراهية: ، وهي حسب نص المادتين 22 و 23 من القانون المتعلق بالجريمة السيبرانية كل شتم بواسطة نظام معلوماتي لشخص أو مجموعة من الأشخاص بسبب إنتمائهم إلى مجموعة تتميز بالعرق أو اللون أو النسب أو الأصل الوطني أو الاثنى وكل إنتاج أو تسجيل أو عرض أو توفير أو نشر أو رسالة نصية أو صورة أو صوت أو أي شكل آخر من أشكال تمثيل الأفكار والنظريات التي تمجد الجرائم ضد الإنسانية أو تحرض على العنف أو على الكراهية أو العنصرية عبر نظام معلوماتي .

5- جرائم المساس بالأشخاص : وهي حسب المواد 24 و 25 و 26 من قانون الجريمة السيبرانية كل تسجيل عن قصد بأية وسيلة أو على أية دعامة كانت صورا أو أصواتا أو نصوصا عبر نظام معلوماتي بغية الأضرار بشخص أوحصوله علي فائدة أو الاستفادة من مزايا لنفسه أو لغيره أو تقديم المساعدة بغرض اقتراف واحدة من تلك الجرائم.

ثالثا: جرائم المساس بالممتلكات:

وهي حسب المواد 28 و 29 و 30 من قانون الجريمة السيبرانية كل فعل يتعلق بنسخ بيانات معلوماتية من أجل الإضرار بشخص معين وكل استخدم لحيل أو أسماء أو صفات مزيفة من أجل الحصول على بيانات معلوماتية شخصية أو سرية أو إخفاء بيانات معلوماتية منتزعة ومملوكة أو متحصل عليها أثر الجريمة.

رابعا : الجرائم المتعلقة بالمساس بالدفاع والأمن:

يعد المساس بالدفاع والأمن الوطني من قبيل جرائم الاعتداء على أمن الدولة بواسطة وسائل وأجهزة الكترونية تستهدف تدمير البنية التحتية المعلوماتية للدولة وشل أنظمة القيادة والاتصال وتعطيل أنظمة الدفاع الجوي والتحكم في خطوط الملاحة الجوية والبرية والبحرية واختراق النظام المصرفي..... ومن مظاهر هذه الجرائم حسب ما نص عليه القانون المتعلق بالجريمة السيبرانية مساعدة قوة أجنبية أو عملائها على الحصول على معلومات تتعلق بالدفاع الوطني وإتلافها أو السماح بإتلافها من اجل مساعدة دولة أو هيئة أجنبية أو حيازة وجمع المعلومات لاستغلالها إضرارا بالدفاع الوطني .

المطلب الثاني: أركان الجريمة الالكترونية:

لا تختلف أركان الجريمة الالكترونية عن غيرها مما يجب توافره في أية جريمة أخرى من أركان اتفق فقهاء القانون على حصرها في ثلاثة وهي الركن المادي والركن المعنوي والركن الشرعي .

الفرع الأول : الركن المادي:

إن التباين الحاصل في الجرائم الإلكترونية وغيرها من الجرائم الأخرى والذي يعود بالأساس إلى الاختلاف البين في نوع وطبيعة وحقيقة تلك الجرائم من منظور ما تم التعارف عليه فقها بالأركان الخاصة[6]. للجريمة والتي لا تتفق في حقيقتها ومدلولها مع الركن المادي للجريمة الذي هو واحد في جميع الجرائم سواء الكترونية كانت أم تقليدية من منطلق أنه بمثابة السلوك الإرادي الهادف إلى تحقيق نتيجة إجرامية ترتبط في الواقع بالفعل الإجرامي عن طريق علاقة سببية[7].

ولقد أدت طبيعة الوسائل المستخدمة في ارتكاب الجرائم الالكترونية وارتباطها بالعالم الافتراضي بسبب الظروف التقنية المحيطة بها والمتمثلة في وجود بيئة رقمية واتصال دائم بالإنترنت إلى إثارة جملة من الإشكالات المتعلقة بعناصر الركن المادي لهذه الجريمة المرتبطة في الواقع بالفصل بين الأعمال التحضيرية لارتكابها والشروع فيها على اعتبار أن القاعدة العامة في المسؤولية عن ارتكاب الجريمة أيا كانت لا تبدأ إلا من لحظة الشروع في ارتكابها وهذا المبدأ إن صح في الجرائم التقليدية إلا أن المسؤولية في مجال العديد من أنواع الجرائم الالكترونية قد تترتب بمجرد البدء في عملية التحضير لارتكابها باعتبار تلك العملية تعد جريمة في حد ذاتها كحيازة صور دعارة للأطفال أو اقتناء معدات لفك الشفرات وكلمات المرور....ضف إلى ذلك أن ما تتميز به الجرائم الالكترونية من تباين من حيث المكان في مختلف مراحل ارتكابها قد أثار هو الآخر العديد من التساؤلات حول قواعد الاختصاص الواجبة التطبيق في حالة ما إذا تم الشروع في ارتكاب الجريمة في مكان وتحقق النتيجة في مكان آخر[8].

كما أن الطبيعة التقنية للجرائم الالكترونية قد جعل منها أكثر الجرائم انتشارا لما دأب البعض على تسميته النتيجة المحتملة التي ترافق ما تم حدوثه من نتائج كما لو تحققت نتيجة القرصنة ورافقها انتشار للفيروسات داخل الأنظمة المعلوماتية محل الجريمة [9].

الفرع الثاني : الركن المعنوي :

لا يختلف الركن المعنوي من حيث المبدأ في الجرائم الالكترونية عن غيرها من الجرائم الأخرى وهو مايعبر عنه بالحالة الذهنية والنفسية للجاني أو بالعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني والتي تجعل من عنصر القصد الجنائي أو العمد جوهر الركن المعنوي للجريمة الذي يعد افتراض حصوله في مجال الجرائم الالكترونية على خلاف الجرائم التقليدية أمر واقع نظرا لما يتمتع به مرتكب هذا النوع من الجرائم من معرفة ودراية فائقة بمجالها بل إن ذلك الافتراض يمتد إلى ما ينتج عنها من جرائم كما هو الشأن مثلا بالنسبة لجريمة الإختراق التي قد يتعدى فيها الجاني إلى أكثر من مجرد اختراق نظام

---

[6]-راجع في مجال الأركان الخاصة د/عبد القادر عودة التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي الجزء الأول.

[7]- في تعريف الركن المادي للجريمة راجع د/ عبد الله سلمان شرح قانون العقوبات الجزائري القسم العام الجزء الأول.

[8]-في الولايات المتحدة الامريكية أقر القضاء بولاية (Tennessee)باختصاصه في البت فيما عرف يقتضيه توماس المجرد النتيجة تحقيق بالولاية .

[9]-راجع نبيلة هبة هروال الجوانب الإجرائية لجرائم الانترنت مرجع سابق راجع كذلك د/ كمال مطر الجرائم الالكترونية .

معلوماتي فيقوم بالتعديل أو الإلغاء أو التعدي على الخصوصية ففي مثل هذه الحالات ذهب اتجاه في القضاء المقارن إلى اعتبار تلك الجرائم مجرد جرائم موضوعية لا تحتاج لركن معنوي[10]

الفرع الثالث : الركن الشرعي أوالقانوني:

يقصد بالركن الشرعي النص القانوني المجرم للفعل والمحدد للعقوبة المترتبة عليه ويعد تطبيقا لمبدأ شرعية الجرائم والعقوبات المنصوص عليه في مختلف التشريعات الجنائية للدول.

وأيا كان الخلاف الدائر حول طبيعة هذا الركن واعتبار البعض أنه مجرد صفة تقترن بالسلوك فتجعله مجرما أو معاقبا إلا أن تلك الصفة مع ذلك تظل ركنا لا غنى عنه في إضفاء الوصف الجرمي على الفعل أيا كان نوعه.

ومهما يكن من وصف قانوني للسلوك فإنه لا يعدو مجرد نتيجة حتمية لمبدأ الشرعية الذي لا يتجاوز نطاق تطبيقه الحدود الإقلمية للدولة مما يثير الأشكال حول مدى تطبيقه في مجال الجرائم الالكترونية التي تتسم بخصوصية كونها عابرة للحدود بحيث تتجاوز تجلياتها نطاق المحلية إلى العالمية نظرا لارتباط محل ارتكابها الذي هو تقنية المعلومات و الاتصال بشتى مناحي الحياة الاقتصادية الاجتماعية والخدمات الصحية والأمنية ..... في العالم بأسره ، الشيء الذي فرض على دول العالم التفكير بشكل جاد لوضع نصوص قانونية قادرة على مواجهة ما تفرضه تلك الجرائم المستجدة من تحديات إلا أن التباين الحاصل في خضم تلك التحديات من دولة لأخرى قد انعكس بشكل كبير على حجم استعداد كل دولة لسن تلك القوانين فمنها ما استشعر الخطر مبكرا كما هو الشأن بالنسبة للسويد التي أصدرت قانون البيانات 1973 والولايات المتحدة الأمريكية التي أصدرت قانون حماية أنظمة الحاسب الآلي ما بين سنتى 1976-1985 أما البلدان العربية فلم تبدأ في سن تلك القوانين إلا في بداية القرن الواحد والعشرين فأصدرت المملكة العربية السعودية 2007 نظام المعاملات الالكترونية ومكافحة الجرائم المعلوماتية أما الإمارات العربية المتحدة فقد أصدرت القانون الاتحادي رقم 02/2006 المتعلق بمكافحة جرائم تقنية المعلومات في حين سن المشرع الموريتاني سنة 2016 القانون رقم 07/2016 المتعلق بالجريمة السيبرانية والذي جاء استجابة لحجم ما فرضه الانتشار الواسع للمعلوماتية وشبكات الاتصال والاستخدام غير المسبوق لمواقع التواصل الاجتماعي وغيرها من تحديات على المستوى الوطني[11].

---

[10]-راجع في مجال الركن المعنوي د/ عبد القادر عودة التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي مرجع سبق ذكره . نبيلة هبة هروال الجوانب الإجرائية لجرائم الأنترنت برز هذا الاتجاه فيما ذهب إليه القضاء الأمريكي في قضية موريس الذي أسس دفاعه على انتفاء الركن المعنوي والعمد لديه بحيث إعتبر القضاء أن العمد يتحقق بالإرادة في جريمة الولوج .

[11]- أصدرت البحرين القانون رقم 60 لسنة2012 كما أصدرت الجزائر القانون رقم 04/09 بتاريخ 2009 المتعلق بالوقاية في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال واصدرت مصر 2018 قانون يتعلق بمكافحة جرائم الانترنت في حين اصدرت الأدرن قانون الجرائم الالكترونية 2015.....

المبحث الثاني : قواعد وإجراءات التحقيق والبت في دعاوي الجرائم الالكترونية:

لقد أدت الطبيعة الفنية للوسائل المستخدمة في ارتكاب الجرائم الالكترونية إلى صعوبة البحث والتحقيق فيها لما يتطلبه وضع اليد على أدلة ارتكابها من إجراءات فنية معقدة قد تتجاوز حدود الحيز الجغرافي للمحقق إلى مجالات أرحب وأوسع من ذلك من شأنها أن تتسبب في الكثير من الصعوبات للمحاكم المختصة بالبت في تلك الجرائم وذلك أثناء معالجتها للقضية

المطلب الأول :البحث والتحقيق في الجرائم الالكترونية

لم يتوسع المشرع الموريتاني كثيرا في تحديد إجراءات البحث والتحقيق في الجرائم الالكترونية من خلال ما نظمه من أحكام في القانون رقم 07/2016 المتعلق بالجريمة السيبرانية وإنما أبقى في الغالب الأعم على اعتماد ما هو منصوص عليه في قانون الاجراءات الجنائية من ترتيبات سواء من حيث انعقاد الاختصاص في البحث والتحقيق أو من حيث إجراءاتة وهو توجه إن دل على شيء فإنما يدل على أن المشرع الموريتاني رغم إصداره للقانون المتعلق بالجريمة السيبرانية إلا أنه لم يستشعر في الواقع خطورة هذا النوع من الجرائم وانتشارها الغير مسبوق وتأثيرها المباشر على حركة رأس المال في العالم مقارنة بغيرها من الجرائم الأخري التي قام بإستحداث أجهزة خاصة للبحث والتحقيق فيها كجرائم الإرهاب والجرائم الاقتصادية التي أنشئت ضبطيات قضائية وأقطاب أو فرق للبحث والتحقيق فيها ولعل السبب في ذلك عائد إلى قلة الجرائم الالكترونية المسجلة على المستوى الوطني كما ونوعا منذ دخول القانون المتعلق بالجريمة السيبرانية حيز التنفيذ ليبقى الاختصاص في البحث في هذه الجرائم منعقد لقضاة التحقيق والضبطيات القضائية وفق ما هو منصوص عليه في المادتيين21 و45 من قانون الإجراءات الجنائية حيث نصت هذه الأخيرة على أن اختصاص قاضي التحقيق يتحدد بمكان وقوع الجريمة أو

محل إقامة مرتكبها أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافهما أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض حصل بسبب آخر.
ونظرا للطبيعة الافتراضية للجرائم الالكترونية فإن عملية البحث والتحقيق فيها تتطلب أن تكون الجهة المخولة بذلك مسلحة بقدر كبير من الإمكانيات الفنية والدراية المعرفية بواقع هذا النوع من الجرائم وهو ما تفتقر إليه جهات البحث والتحقيق على المستوى الوطني نظرا لعدم تركيز تلك المهمة في جهة بعنيها حتى يتسنى تكوينها على أساليب البحث والتحقيق في هذه الجرائم ، ومع ذلك يظل من أكثر الإجراءات التي يتعين على المحقق القيام بها ومن أكثرها تأثيرا في التحقيق معاينة مسرح الجريمة والتنقل والتفتيش والحجز على أدلة ارتكابها قبل أن يتم العبث بها وهي إجراءات إن كانت ذي أهمية كبيرة في مجال الجرائم التقليدية فإن الطبيعة الرقمية للجرائم الالكترونية قد تجعل من ذلك مصدرا ثانويا نظرا لكون هذه الجرائم لا تترك أثرا ماديا يمكن من خلاله الاستدلال على مرتكبها ومع ذلك فلا إشكال في انتقال المحقق إلى مكان يفترض أن تكون فيه مكونات مادية لنظام معلوماتي كحاسب آلي .... أو وسائط لبيانات معلوماتية متعلقة بالجريمة أو أوراق أو مستندات أو وثائق[12] لتفيد في كشف الحقيقة مع رفع ما عليها من بصمات وبما أن النفاذ إلى البيانات المخزنة فيما تم ضبطه من أدوات وحواسب يتطلب توفر الخبرة الفنية اللازمة لضبط ما بداخل تلك الأجهزة من معلومات والمحافظة عليها من التلف والتلاعب والحذف وهي أمور قد لا تكون متوفرة في المكلفين بالتحقيق ، فقد أتاح المشرع الموريتاني لجهة التحقيق الحق من تعيين أي شخص[13] مؤهل لاستخدام الوسائل التقنية المناسبة من أجل منع النفاذ إلى البيانات أو إلى النظام المعلوماتي أو إلى نسخ البيانات المتوفرة لدى الأشخاص المأذونيين باستخدام النظام المعلوماتي و ضمان سلامة تلك البيانات وعند الاقتضاء سريتها كما يمكن كذلك للسلطة القضائية أن تأمر أي شخص يعرف استخدام النظام المعلوماتي أو الإجراءات المطبقة لحماية البيانات المعلوماتية أو يوفر كل المعلومات الضرورية لتطبيق إجراءات التفتيش وكذا الحجز المعلوماتي إذا كانت ضرورة التحقيق تتطلب حماية بيانات الكترونية معينة مخزنة بواسطة نظام معلوماتي ومعرضة بصفة خاصة للضياع فلسلطة القضائية أن تأمر أي شخص بحوزته أو تحت رقابته تلك البيانات بحفظها وحمايتها لمدة تسعين يوما على الأكثر حتى تتمكن جهات البحث والتحقيق من وضع اليد عليها ، ومن جهة أخرى يمكن لقاضي التحقيق أن يأمر أي شخص موجود على التراب الوطني أن يقوم بالإبلاغ عن بيانات معلوماتية معينة مخزنة في نظام معلوماتي أو على دعامة معلوماتية موجودة بحوزته بحوزته من بيانات أو تحت رقابته ، كما يمكنه أن يأمر أي مورد خدمات على التراب الوطني بالإبلاغ عنما بحوزته من بيانات أو تحت رقابته تتعلق بتلك الخدمات أو المشتركين فيها.
هذا وقد تدفع عملية البحث في المكونات غير المادية للبرامج بالمحقق إلى اكتشاف ارتباط حاسوب المتهم بحواسب أخرى داخل إقليم الدولة أو خارجه ، مما يثير الأشكال حول إمكانية امتداد البحث إلى تلك الحواسب أم أنه بحاجة إلى أذن من السلطة القضائية المختصة على اعتبار أنه خارج حدود اختصاص المحقق المكاني ، في هذا الإطار عمد المشرع

---

[12]-راجع المادة 42 من قانون الإجراءات الجنائية.
[13]-راجع المواد في ذلك 41، 42، 43، 44، 45، 46، من القانون رقم 07/2016 المتعلق بالجريمة السيبرانية

الموريتاني من خلال ما أورده من أحكام في المادة 39من القانون المتعلق بالجريمة السيبرانية إلى السماح بامتداد التفتيش إلى نظام معلوماتي يرتبط به موجود على التراب الوطني أما إذا ارتبط النظام الأصلي موضوع التفتيش بنظام معلوماتي خارج التراب الوطني فإن مسألة النفاذ إليه لا بد وأن يتم وفق النظم والإجراءات المحددة في الإلتزامات الدولية المعمول بها.

بيد أن المشرع الموريتاني وإن كان قد حسم الإمتداد المكاني للتفتيش عن أدلة الجريمة الالكترونية فيما نظمه من أحكام في القانون المتعلق بالجريمة السيبرانية فإنه لم يولي كبير اهتمام لمجال امتداده الزماني وذلك حينما لم يعالجه فيما نظمه من أحكام تاركا ذلك على ما يبدو لما تضمنته المادة 52 من قانون الإجراءات الجنائية من أحكام والتي لا تجيز البدء في التفتيشات والزيارات المنزلية قبل الساعة الخامسة صباحا ولا بعد العاشرة مساء ، صحيح أن المشرع الموريتاني قد استثنى من تلك الحالة التي يكون فيها الطلب صادرا من داخل المنزل محل التفتيش أو في الأحوال لاستثنائية المقررة قانونا والتي لم يحدد المشرع نوعها وطبيعتها.

وانطلاقا مما حدده المشرع الموريتاني من مجالات للبحث والتحقيق في الجرائم الالكترونية يمكن التنويه إلى أن ضابط الشرطة القضائية المختص يتمتع بحرية كبيرة في التحري واتخاذ القرارات من منطلق ما نصت عليه المادة 47 من القانون المتعلق بالجريمة السيبرانية من ترتيبات خولت ضابط الشرطة القضائية المختص الحق في إطار عملية البحث أو تنفيذ إنابة قضائية أن يقوم بالإجراءات المنصوص عليها في المواد 39 و45 من هذا القانون والتي بالعودة إلى ما تضمنته من أحكام يمكن لضابط الشرطة القضائية أن يجمع أو يسجل عن طريق التقنيات المتوفرة في دائرة اختصاصه وله في سبيل ذلك إلزام أي مورد خدمات في إطار قدراته التقنية أن يقوم بالتسجيل الحي والمباشر للمعلومات المتعلقة بالنقل والمرتبطة باتصالات محددة مرسلة في دائرته الترابية بواسطة نظام معلوماتي.

على أن تلك العمليات وإن كان بمقدور ضابط الشرطة القضائية القيام بها في إطار عملية البحث إلا أن ثمة إجراءات لا يمكنه القيام بها إلا بإذن من وكيل الجمهورية التابع له وهذه الإجراءات هي ما نص عليه المشرع الموريتاني في المادة 46 من القانون المتعلق بالجريمة السيبرانية والمتمثلة في اعتراض أو تسجيل البيانات المتعلقة بمحتوى اتصالات محددة ومرسلة في دائرة اختصاصه الترابي بواسطة نظام معلوماتي وذلك بخصوص الجرائم التي لا يقل الحد الأقصى للعقوبة فيها عن أربع سنوات وهو تحديد يسمح كما هو مبين في المادة 45 من القانون المتعلق بالجريمة السيبرانية لضابط الشرطة القضائية القيام بتلك الإجراءات بدون إذن من وكيل الجمهورية في الجرائم التي يقل الحد الأقصى لعقوبتها عن أربع سنوات وهو إجراء يتعارض مع مبدأ احترام وصيانة الحياة الشخصية للأفراد من أية مراقبة أو ضبط أو تسجيل وكذلك الارتباط بالحرية الشخصية لهؤلاء والتي لا تمكن مراقبتها إلا في حالات خاصة نص عليها القانون وأناط النيابة العامة الحق في الإذن بها وإن كان المشرع الموريتاني لم يحدد جرائم بعينها يتعين أن تخضع لتلك الإجراءات نظرا لطبيعتها وإنما اكتفى بضبطها من خلال فترة عقوبتها.

هذا ويعد حجز أدلة الجريمة أيا كان نوعها أثرا مباشرا لما يقوم به المحقق من تفتيش يستهدف من ورائه وضع اليد على أدلة الجريمة والمحافظة عليها إلى أن يتم تقديمها أمام

المحاكم كأدلة على ارتكاب المتهم لما نسب إليه من وقائع ومع ذلك يظل وجه التباين والاختلاف فيما يتعلق بحجز أدلة الجرائم الالكترونية والجرائم الأخرى واضحا وجليا نظرا للطبيعة المعنوية لأدلة الجرائم الالكترونية وما تتطلبه من وسائل فنية وتقنية لضبطها ، ذلك أن الحجز لا يقع على أشياء مادية فقط كما هو الحال في الجرائم التقليدية وإنما يقع إلى جانب المعدات والتجهيزات والأليات...الألكترونية[14]، على ما اصطلح على تسميته بالدليل المعلوماتي....المتعلق في الواقع بالكيانات المعنوية المخزنة فيما تم حجزه من أدوات أو أجهزة الكترونية وهو حسب تعبير جانب من الفقه بمثابة مجموعة من المعلومات التي يقبلها المنطق والعقل ويعتمدها العلم يتم الحصول عليها بإجراءات قانونية وعملية وبترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال ويمكن استخدامها في أية مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه.

فالدليل المعلوماتي وإن كان يعد جوهر حقيقة الأدلة في مجال الجرائم الالكترونية ، إلا أن ما يتمتع به من صفة افتراضية قد أثار جدلا فقهيا وتباينا تشريعيا واسعا حول مدى إمكانية حجزه من حيث المبدأ وما إذا كان نسخه أو تحويله إلى دليل مادي قد يؤثر على صفته أو قيمته الثبوتية حيث ذهب جانب من الفقه إلى القول بأن الكيانات المعنوية للحاسب الآلي لا يمكن أن تكون محلا للحجز من منطلق أن القوانين الاجرائية تشترط لذلك الطابع المادي الملموس للأدلة المراد حجزها مما يتعين معه تحويل تلك الكيانات من طابعها المعنوي إلى كيان مادي عن طريق نسخها مثلا في شكل وسائط مادية ملموسة كطباعتها أو تصويرها .....بحيث يمكن تقديمها إلى الجهات القضائية المختصة دون أن يؤثر ذلك على قيمتها الثبوتية وحجيتها القانونية ، ويعد من أبرز التشريعات التي سارت في هذا الاتجاه التشريع البلجيكي من خلال ما نص عليه في المادة 39 من قانون 28 نوفمبر 2000 المتعلق بالجرائم المعلوماتية.

وعلى خلاف ما ذهب إليه أصحاب هذا الاتجاه فقد ذهب البعض إلى أن الكيانات المعنوية للأجهزة الالكترونية تصلح لأن تكون محلا للحجز متى ما تمت مراعاة طبيعتها الافتراضية التي تفرض أن تتم عملية الحجز في بيئة خاصة تناسبها وتتوافق مع الطبيعة التقنية الخاصة بها وتحافظ على صفتها الالكترونية وحقيقتها كدليل معلوماتي ويعد من أبرز التشريعات التي أخذت بهذا الاتجاه المشرع الفرنسي في المادة 57 من قانون المسطرة الجنائية والتشريع الجزائري في المادة 06 من القانون رقم04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات كما تبنى المشرع الكويتي نفس الاتجاه في القانون رقم 20 لسنة 2014 المتعلقة بالمعاملات الالكترونية وهو ما تبناه المشرع الموريتاني من خلال ما نص عليه من أحكام في المادة 40 من القانون 07/2016 المتعلق بالجريمة السيبرانية التي تنص على أنه إذا ما تم اكتشاف بيانات مفيدة لإظهار الحقيقة مخزنة في نظام معلوماتي وكان حجز الدعامة التي تحملها غير مستحب تقوم السلطات القضائية بنسخ هذه البيانات وتلك الضرورية لفهمها على دعائم تخزين معلوماتية يمكن حجزها ووضعها تحت الأختام[15]

---

[14] المتعلق بالجريمة السيبرانية على حجز المعدات والتجهيزات والآليات والبرامج المعلوماتية 07/2016 من القانون رقم 38- لقد نصت المادة وكل الوسائل والبيانات المرتبطة بالجرائم المحددة في هذا القانون.

المطلب الثاني: البت في الجرائم الالكترونية :

حسب ما نظمه المشرع الموريتاني من أحكام في قانون الإجراءات الجنائية والقانون رقم 07/2016 المتعلق بالجريمة السيبرانية والأمر القانوني رقم 12/2007 المتضمن التنظيم القضائي فإن الاختصاص في النظر والبت في الجرائم الالكترونية ينعقد للغرف الجزائية والمحاكم الجنائية حسب نوع وطبيعة الجريمة موضوع النظر وذلك انطلاقا من مجموعة من القواعد الآمرة التي لا يجوز للأطراف الإتفاق علي خلافها إذ تتعهد تلك المحاكم حسب ما هو منصوص عليه في قانون الإجراءات الجنائية إما بإحالة مباشرة أو بطلب من وكيل الجمهورية في حالة ما إذا كانت الجريمة تلبسية أو بإحالة من قاضي التحقيق المكلف بالتحقيق فيها أو غرفة الاتهام[16].

كما أن المحاكم الأعلى درجة كما هو الحال بالنسبة للغرف الجزائية بمحاكم الاستئناف والغرفة الجزائية بالمحكمة العليا تتعهد هي الأخرى في القضية بموجب الطعن المقدم من أحد الأطراف سواء كان طعنا بالاستئناف أو بالنقض .

ولما كانت قواعد وإجراءات تعهد المحاكم بالقضايا كما حددها المشرع تختلف من حيث المعني والمبني عن قواعد اختصاص تلك المحاكم المحددة من حيث المبدأ في المادة 45 من قانون الإجراءات الجنائية بمكان وقوع الجريمة أو محل إقامة مرتكبها أو أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو محل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض حصل بسبب آخر فإن تلك المحددات لا تتلاءم والطبيعة الافتراضية للجريمة الالكترونية التي تجعل منها جريمة عابرة للحدود بحيث لا يمكن تحديد مكان وقوعها نظرا لاستعصائها على الخضوع للقوالب القانونية التي تحكم مسألة الاختصاص المكاني ذلك أن قواعد الاختصاص كما هي محددة في قانون الإجراءات الجنائية تمت صياغتها لتحديد الاختصاص المتعلق بالجرائم القابلة للتحديد المكاني وهو بطبيعة الحال ما يتنافى وطبيعة الجرائم الالكترونية ولعل ذلك مما دفع المشرع الموريتاني من خلال المادة 48 من القانون رقم 07/2016 المتعلق بالجريمة السيبرانية إلى تحديد مجال اختصاص المحاكم الموريتانية في النظر والبت في هذه الجرائم وذلك عند ما تكون قد تم ارتكابها على التراب الوطني أو على متن سفينة ترفع العلم الموريتاني أو طائرة مسجلة حسب قوانينها أو عند ما تكون الجريمة تضر بمصالح الدولة أو يكون ضحيتها شخص خاضع للقانون الموريتاني ولم يتم تسليميه بناء على جنسيته لأي دولة أخرى وليظل مع ذلك ما وضعه المشرع الموريتاني من خلال تلك المادة من قواعد لضبط مجال اختصاص المحاكم الموريتانية في النظر والبت في الجرائم الالكترونية وإحالته إلى إمكانية تطبيق ما نظمه من قواعد ومبادئ للاختصاص في قانون الإجراءات الجنائية قاصر عن تحديد معايير من شأنها أن تضع الحد النهائي لما يثره موضوع الاختصاص في مجال الجرائم الالكترونية من إشكالات لعل من أبرزها تنازع الاختصاص ، صحيح أن المشرع الموريتاني قد تناول من خلال الباب الخامس من قانون الإجراءات الجنائية مسألة تنازع الاختصاص بين قضاة التحقيق ومحاكم الحكم محددا قواعد فك الاشتباك بينها إلا أنه لم

---

[15]- للمزيد من التوسع في مجال البحث والتحقيق في الجرائم الالكتروني راجع يوسف خليل يوسف العفيفي الجرائم الالكترونية في التشريع الفلسطني (دراسة مقارنة) بحث لنيل درج الماجستير في القانون العام كلية الشريعة والقانون بالجامعة الإسلامية غزة راجع كذلك د/عبد السلام بنسلمان الأجرام المعلوماتي في التشريع المغربي مرجع سابق راجع كذلك د/مفتاح بوبكر المطردي الجريمة الالكترونية والتغلب على تحدياتها مرجع سابق.

[16]- راجع المواد 63، 179، 181، 209، من قانون الإجراءات الجنائية

يتطرق لما قد يحصل من تنازع في الاختصاص بين القضاء الوطني وغيره من الجهات القضائية في الدول الأخرى معولا في ذلك على ما تمت صياغته وتنظيمه في الاتفاقيات والمواثيق الدولية المتعلقة بالجرائم الالكترونية وما أصدرته بعض الجهات القضائية من اجتهادات في هذا الصدد وما عرضه فقه القانون من مقترحات بهذا الشأن .
لقد زادت اتفاقية بودابست المتعلقة بالجريمة المعلوماتية في مادتها 22 على ما حدد المشرع الموريتاني في القانون المتعلق بالجريمة السيبراينة من قواعد لاختصاص المحاكم الموريتانية في معيارين هما أن تكون الجريمة قد تم ارتكابها عن طريق أحد مواطني الدولة وأن يكون معاقب عليها بموجب القانون الجنائي الخاص بمكان ارتكابها أو في حالة ارتكابها خارج الاختصاص القضائي الإقليمي لأية دولة لتضيف بعد ذلك في البند الخامس من نفس المادة أنه في حالة مطالبة أكثر من طرف بالاختصاص القضائي بشأن جريمة مما تقره هذه الاتفاقية يقوم الأطراف المعنيون بالتشاور من أجل تحديد الاختصاص القضائي الأكثر ملاءمة للاختصاص للمحاكمة وهو ما يسميه البعض بالاختصاص طبقا للكفاءة الافتراضية وقد تبنت هذا التوجه الاتفاقية العربية في مكافحة جرائم تقنية المعلومات في مادتها 30 وإن كانت هذه الاتفاقية قد سايرت المشرع الموريتاني في البند المتعلق باختصاص القضاء المورتياني حينما تكون الجريمة تضر بمصالح البلد.

فإذا كان القانون الموريتاني والاتفاقيات المذكورة أعلاه قد عقدت الاختصاص لقضاء البلد المتضرر من الجريمة الالكترونية إلا أنها مع ذلك لم تتطرق للمحل في حالة ما إذا كانت الجريمة قد تسببت في الضرر الأكثر من دولة ولعل من أبرز الأمثلة على ذلك قضية الدودة الحاسوبية المسماة(Love-bug) التي أعدت في الفلبين سنة 2000 وعطلت ملايين الحواسيب في جميع أنحاء العالم .
لقد تصدى الفقه القانوني لهذا الإشكال حيث اعتمد جانب منه معيار القانون الأكثر ملاءمة والذي يجعل قضاء الدولة التي كان قانونها الأكثر تعرضا للانتهاك جراء الجريمة هو القضاء المختص بالنظر والبت وقد أخذ على هذا المعيار عدم حسمه للأشكال ذلك أن حجم الضرر قد يتساوى في جميع الدول التي طالتها الجريمة ، وإلى جانب ذلك فقد ذهب اتجاه آخر إلى القول بمعيار الضرر المرتقب من منطلق أنما تتسبب فيه الانترنت من أضرار قد يطال الكثير من الدول بنفس المستوى مما يجعل تطبيق قاعدة الدولة الأكثر تضررا وبالتالي لم يبقى بدا من عقد الاختصاص للدولة التي ارتكبت فيها الجريمة و هو ما أكد عليه المجلس الأوربي للعدل في أحد قراراته.
وفي هذا الصدد دائما حاولت المحاكم الفرنسية من خلال ما صدر عنها من اجتهادات قضائية إيجاد معايير أخرى لتحديد الاختصاص في الجريمة الالكترونية تختلف عن تلك التقليدية إذ أصدرت الغرفة الجزائية بمحكمة النقض الفرنسية في مجال الجرائم الالكترونية المرتبطة بالصحافة قرارا بتاريخ 28 سبتمبر 2009 يقضي بأن مكان ارتكاب الجريمة هو المكان الذي تم فيه التلفظ بالتهديد وليس في الدولة التي تم نقل الخبر فيها عبر التلفاز أوالصحافة المكتوبة أو الالكترونية.
هذا وتخضع محاكم الحكم في الجرائم الالكترونية لنفس المساطر المحددة في قانون الإجراءات الجنائية المتعلقة بالبت في غيرها من الجرائم الأخرى سواء تعلق الأمر بإجراءات انعقاد جلساتها أو تقديم وبحث أدلتها أو بالحكم بناء على قناعة أعضائها بما تمت

إثارته من أدلة ومثبتات على ارتكابها ويعد تناول المحكمة لأدلة الإثبات الفيصل في نتيجة جلسة الحكم فإما أن يكون بالبراءة أو الإدانة ويخضع القاضي في تعاطيه مع وسائل الإثبات لمجموعة من القواعد من أهمها حريته في تكوين عقيدته فله الحكم في الجريمة حسب ما تكون لديه من قناعة دون إلزامه بالأخذ بدليل بعينه وهو في ذلك لا يقيده سوى القانون وفي هذا المعنى نصت المادة 386 من قانون الإجراءات الجنائية على أنه باستثناء الحالات التي ينص فيها القانون على خلاف ذلك فإن الجرائم يمكن أن تثبت بجميع الأدلة الشرعية ويحكم القاضي اعتمادا على اقتناعه الشخصي المعتمد على البيانات والمثبتات القانونية.
إضافة إلى حرية القاضى في تكوين عقيدته في المجال الجنائي فإنه يتصف بالدور الإيجابي أثناء بحثه عن الحقيقة مع استحضاره الدائم لقاعدة كون عبئ الإثبات يقع على عاتق سلطة الادعاء من منطلق أن الأصل في المتهم البراءة مما نسب إليه من وقائع .
فإذا كانت تلك القواعد لا خلاف فيها بين الجرائم الالكترونية والتقليدية إلا أن الطابع الفني والتقني للجرائم الالكترونية حتم على المحاكم لفهم أبعاد تلك الجرائم الاستعانة بخبراء وفنيين في مجال تقنية المعلومات والاتصال وهو ما أدى في الواقع إلى الحد من حرية القاضي في تكوين قناعته ما دام أنه قد لا يكون على المام شامل بالدليل المعروض أمامه حتى يتمكن من تقييمه بحرية.

الخاتمة

كخاتمة لهذه الدراسة فإن إقرار المشرع الموريتاني للقانون رقم07/2016 ما هو إلا استشعار منه لخطورة الجرائم الالكترونية وتأثيرها على قيم وأخلاق المجتمع وكيان الدولة ومقدراتها الاقتصادية والاجتماعية والأمنية.....بفعل الانتشار المهول لاستخدام الوسائل الالكترونية داخل المجتمع بل وتعاطي الجميع بشكل غير معقلن مع ما أفرزته الانترنت من وسائط شكلت تحديا كبيرا أصبحت معه مواجهتها بقواعد الإجراءات القديمة أمر غير مستساق نظرا لما تمتاز به هذه الجرائم من طبيعة تجعل آثارها لا تقتصر على حدود بلد بعينه وإنما تتعداها إلى العديد من البلدان ، ونظرا لتلك الطبيعة فقد اتجه المشرع الموريتاني من خلال مارسمه في القانون رقم 07/2016 المتعلق بالجريمة السيبرانية إلى التعاطي

مع ما تطرحه الجرائم الالكترونية من إشكالات انطلاقا من رؤية أكثر شمولية بموضوعها ومجالها لدرجة اعتباره كل الجرائم المتركبة بوسائل الالكترونية من قبل الجرائم الالكترونية فحدد مجموعة من الجرائم وعقوباتها ووضع قواعد واضحة للمسؤولية عن تلك الأفعال خصوصا ما يتعلق منها بمسؤولية الأشخاص لاعتبارية كما نظم إجراءات البحث والتحقيق ومجال الاختصاص والحكم .

غير أن المشرع الموريتاني وإن كان قد استجاب لما يمليه واقع التطور والتحول الذي شهده العالم بوضع نص قانوني لتجريم ومعاقبة الأفعال الناتجة عن استخدام ظاهرة تعد الوجه الأبرز لما شهده العالم من تحول والمتمثلة في السيل الجارف للوسائل الالكترونية ، فإن معالجة الجرائم الالكترونية والحد من مخاطرها تبقى بجاجة إلى العديد من الإجراءات التي من أهمها :

1-العمل على وضع آليات حديثة للبحث والتحقيق في الجرائم الالكترونية وجمع أدلتها وذلك من خلال رصد الوسائل اللازمة لتلك العميلة وتكوين الطواقم المكلفة بذلك من قضاة وكتاب ضبط وضباط شرطة قضائية.....وفي هذا الإطار يجب العمل على إنشاء ضبطيات قضائية أو إنشاء فرق خاصة بالبحث والتحقيق ومحاكم متخصصة في الحكم في مجال الجرائم الالكترونية على غرار ما قام به المشرع الموريتاني في بعض الجرائم الأخرى كجرائم الإرهاب والجرائم الاقتصادية ...

2-في ظل الاستخدام اللامحدود لما أفرزه التطور من وسائل وأدوات الكترونية أصبح معه التوجه في العالم بأسره نحو إقرار ما يسمى بالإدارة الالكترونية وحوكمت الانترنت .

أمرا لا مناص منه فقد بات من اللازم العمل على وضع إستراتجية متكاملة لمراقبة الأمن في مجال تقنية المعلومات دون أن تقتصر تلك الإستراتجية على المجال الوطني لوحده وإنما يجب أن تتعداه إلى مختلف الدول والهيئات العالمية في إطار ما يسمى بتعزيز التعاون بين الدول في محاربة الجريمة الالكترونية وحل ما قد يترتب عليها من إشكالات كتلك المتعلقة بالاختصاص وتسليم المجرمين وغير ذلك.

وفي هذا الإطار يتعين على الدولة الموريتانية وضع الأسس اللازمة لإنشاء معهد أو مركز يعنى بتتبع الجريمة بصورة عامة والالكترونية منها على وجه الخصوص ورصد حركيتها .

كما يجب اتخاذ تدابير تشريعية في ميدان الإثبات والأدلة من خلال وضع قواعد إجرائية تتناسب وطبيعة هذه الجرائم مع احترام ما يكفله الدستور من ضمانات وما يفرضه مبدأ المشروعية من قواعد وما يتطلبه الحق في احترام خصوصية الأشخاص.

نواكشوط بتاريخ:09/12/2018

قائمة المراجعة

الكتب والبحوث

1) د/ عبد الله بنسليمان الإجرام المعلوماتي في التشريع المغربي الطبعة الأولى 2017 دار الأمان الرباط.
2) نبيلة هبة هروال الجوانب الإجرائية لجرائم الانترنت بحث لنيل شهادة الماجستير في القانون دار الفكر الجامعي الاسكندرية مصر.
3) د/ على جعفر جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة منشورات زين الحقوقية.
4) بلال أمين زين الدين الجرائم المعلوماتية في التشريع المقارن والشريعة الإسلامية بحث لنيل ماجستير في القانون دار الفكر الجامعي.
5) منير محمد الجنيهي وممدوح محمد الجنيهي جرائم الانترنت والحاسب الآلي ، دار الفكر الجامعي.
6) أيمن عبد العال الجرائم الالكترونية في التشريع الفلسطيني بحث لنيل شهادة الماجستير الجامعة الإسلامية بغزة.
1) القاضي محمد حمو الجريمة الالكترونية في المغرب الندوة الدولية الأولى المنظمة من طرف المحكمة العليا بالجمهورية الإسلامية الموريتانية.
2) د/ دياب موسى البداينة الجريمة الالكترونية المفهوم والأسباب.
3) د/ كامل مطر الجريمة الالكترونية
4) د/ مفتاح بوبكر المطردي الجريمة الالكترونية والتغلب على تحدياتها المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية المنعقد بالسودان.
5) أ/ ياسمين بونعارة الجريمة الالكترونية
6-د/عبد القادر عودة التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي الجزء الأول
7-د/عبد الله سليمان شرح قانون العقوبات الجزائري القسم العام الجزء الأول

النصوص القانونية

1) الأمر القانوني رقم 36/2017 المتضمن مدونة الإجراءات الجنائية
2) القانون رقم 07/2016 المتعلق بالجريمة السيبراينة.
3-الأمر القانوني رقم 12/2007 المتضمن التنظيم القضائي