مخبر التنمية الإجتماعية وخدمة المجتمع

الملتقى الوطني حول :الأمن السيبراني ورهانات الأمن الشامل في الجزائر

إسم ولقب المشارك الأول:رابح بن عيسى.

الدرجة العلمية للمشارك:أستاذ محاضر أ.

جامعة الإنتساب للمشارك:جامعة الوادي.

الإلكتروني البريد. Rabah.benaissa@gmail.com

إسم ولقب المشارك الثاني :غنام ساسية.

الدرجة العلمية للمشارك:طالبة دكتورا السنة الرابعة علم اجتماع تخصص انحراف وجريمة.

التخصص :علم اجتماع انحراف وجريمة.

جامعة الإنتساب للمشارك:جامعة الوادي.

البريد الإلكتروني:ghanamsasia13@gmail.com

محور المداخلة:جهود الدولة الجزائرية في مواجهة تهديدات الأمن السيبراني/السياسي/القانوني /الإستراتيجي.

عنوان المداخلة :الجريمة الإلكترونية بين القانون والواقع المعاش.

الملخص

ان ظاهرة جرائم الكمبيوترأ والانترنت،او جرائم التقنية العالية ، او الجريمة الإلكترونية كما يطلق عليها، هي ظاهرة إجرامية مستجدة نسبيا ، وجاء تطوّر هذا النوع من الجرائم بالتزامن مع التطورات التي طرأت على التقنيات والتكنولوجيا التي يسرت سبل التواصل وانتقال المعلومات بين مختلف الشعوب وسهلت حركة المعاملات الإجرامية باستخدام شبكة

المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية ، مما يلحق أضرر بالآخرين ، من هنا سعى المشرع الجزائري إلى سن العديد من التشريعات والقوانين للتصدي لهذه الجرائم .

الكلمات المفتاحية:الجريمة السيبرانية ، المعاملات،القانون،المجرم.

Abstract:

The phenomenon of computer and Internet crimes, or high-tech crimes, or electronic crime as it is called, is a relatively new criminal phenomenon, and the development of this type of crime came in conjunction with the developments that occurred in techniques and technology that facilitated the means of communication and the transfer of information between different peoples and facilitated the movement of transactions. Criminal crimes use the information network as an easy means to carry out criminal operations, causing harm to others. Hence, the Algerian legislator sought to enact many legislations and laws to combat these crimes.

Keywords: cybercrime, transactions, law, criminal.

مقدمة:

شهدت الألفية الأخيرة التطور التكنولوجي والرقمي الهائل وما صاحبه من تأثير على كل الدول بشكل أو بآخر خصوصا فيما يتعلق بأمن واستقرار الشعوب من جهة بل وأصبحت تداعيات هذه الثورة التكنولوجية تمس حرمة وخصوصية المواطن من جهة أخرى.في ظل هذا التحدي الرقمي التكنولوجي الجديد سعت الدول إلى سن حزمة من التشريعات والآليات القانونية والمؤسساتية للتصدي لهذه الجريمة التي أضحت تسمى في الأدبيات الأكاديمية بالجريمة الالكترونية أو الجريمة السيبرانية.

والجزائر إحدى هذه الدول التي لم تكن في منأى من تداعيات هذه الظاهرة، حيث انتشرت في الآونة الأخيرة جرائم تمس بالحياة الشخصية للمواطن وتمس أيضا بأمن واستقرار البلاد وبكل جوانب الحياة خصوصا بعد تنامي معدلات الجريمة وتطور أشكالها و تهديدها المباشر لمجتمعات العصر الراهن نظرا لحجم المخاطر وهول الخسائر الناجمة عن هذه الجرائم التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة،لكونها جريمة تقنية تنشأ في الخفاء و توجه للنيل من الحق في المعلومات المنقولة عبر نظم وشبكات الإنترنت ، وتظهر مدى خطورتها في الإعتداءات التي تمس الحياة الخاصة للأفراد الذين أصبحوا ضحايا لهذا النوع من الجرائم وخوفهم من التبليغ عنها كونها تهدد الأمن والسيادة

الوطنيين ونشر فقدان الثقة بالتقنية وتهدد ابداع العقل البشري .الأمر الذي دفع بالدول إلى العمل ملياً للحد من هذه الجرائم من خلال التوعية والوسائل الوقائيّة الأمنية وغيرها ،بحيث بات لزاما أن يواكب تطور الجريمة و أساليبها تطورا في مجال السياسة التشريعية عموما و السياسة الجنائية علي وجه الخصوص ، بعد أن أصبح واضحا التهديد المباشر للمنظومة الحقوقية الذي يتسبب فيه إساءة استخدام شبكة المعلوماتية ،من خلال ما سبق تكمن إشكالية البحث في مجموعة من التساؤلات التالية:ماهي الجرائم الإلكترونية ؟ وما هي الطبيعة الموضوعية لهذه الجرائم ؟وما هو موقف المشرع الجزائري تجاهها للحد منها؟

أهداف الورقة البحثية:

-التعريف بهذه الجريمة من أجل تجنبها.معرفة الدافع من هذه الجريمة .

- معرفة الوسائل الكفيلة لضمان وحفظ المعلومة المنشورة إلكترونيا.

أهمية الدراسة:

- التعرف على طرق التعامل مع البيئة الإلكترونية للتصدي للجريمة الإلكترونية قبل صدور القانون 09-04.

-التعرف على القوانين الخاصة للتصدي لمختلف الجرائم المتعلقة بها.معرفة القوانين اللاحقة المدعمة للقانون 09-04للحد من الإجرام السيبراني.

-1-1-تعريف الجريمة الإلكترونية من الجانب التقني الفنـــي:

الجريمة الالكترونية عبارة عن نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي.كما يعرفها البعض الآخر: بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها)

فقد أنقسم أنصار تعريف الجريمة من الجانب التقني والفني فالبعض استند إلى موضوع الجريمة والبعض الآخر إستند على وسيلة الجريمة. **(عبد الفتاح بيومي حجازي،2006،ص02،01).**

أهم التعريفات التي أستندت على موضوع الجريمة:

انها "نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه "**(هشام محمد رستم،1994،ص31)** كما تم تعريفها بانها " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات او نقل هذه البيانات " **(هدى قشقوش،1992،ص20)**. كما تعتبر بأنها " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة الى أفعال أخرى تشكل جرائم اكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر " **مكتب المحاسبة العامة للولايات المتحدة الامريكية GOA انظر www.goa.gov.**

2- **أهم التعريفات التي أستندت على وسيلة الجريمة:**

إن أنصار هذا الاتجاه ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة ، وبالتالي تعرف" (على أنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" كما تعرف بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب "وكذلك تعرف بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا([1] **Tom forester. 1989, P. 104**).

1-3-أهم التعريفات التي استندت على الجانب القانوني هناك إستنادا إلى قانون العقوبات الجزائري المعدل والمتمم لم يعرف جرائم الانترنت، بل اكتفى بالعقاب على بعض الأفعال ، تحت عنوان " الجرائم الماسة بنظام المعالجة الآلية للمعطيات" (**(القانون رقم 15/04 المؤرخ في 2004/11/10**).

2-أركان الجريمة الإلكترونية: تتمثل أركان الجريمة الإلكترونية مثل الجريمة العادية في الركن الشرعي و المادي والمعنوي**و الركن الشرعي :** معناه إعتراف المشرع والنص على تجريم الفعل المرتكب،"لاجريمة ولا عقوبة إلا بنص " وبالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات"

-**2الركن المادي** يتكون الركن المادي للجريمة الالكترونية من السلوك الاجرامي و النتيجة و العلاقة السببية ،علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقيق نتيجتها ، مثلا: انشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة الا أنه لا مناص من معاقبة الفاعل.يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل ايجابي مرتكب،مثلا: جريمة الغش المعلوماتي : الركن المادي فيها هو تغيير الحقيقة في التسجيلات الكترونية أو المحررات الإلكتروني"- **(محمود نجيب حسني، 1992، ص 4).**

3-الركن المعنوي :يتكون الركن المعنوي للجريمة الإلكترونية من عنصريها**العلم**:هو إدراك الفاعل للأمور – . **أما الإرادة** : فهي اتجاه السلوك الإجرامي لتحقيق النتيجة .طبقا للمبادئ العامة المعروفة في قانون العقوبات ،قد يكون القصد الجنائي عاما و خاصا ،القصد الجنائي العام : هو الهدف المباشر للسلوك الإجرامي و ينحصر في حدود إرتكاب الفعل . أما القصد الجنائي الخاص : هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه الجريمة، بل يذهب إلى التأكد من تحقيق النتيجة)مثلا: في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه).وعليه ما هو القصد الجنائي الذي يجب توافره في الجريمة الالكترونية ؟**القانون رقم04-15 المؤرخ في10 نوفمبر2004، المادة394 مكرر** . الأصل إن الفاعل في الجريمة الالكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام" **– (محمود نجيب حسني، 1992، ص 4).** إذن فالقصد الجنائي العام متوافر في جميع الجرائم الالكترونية دون أي استثناء و لكن هذا لا يمنع أن بعض الجرائم الالكترونية تتوافر فيها القصد الجنائي الخاص (مثلا: جرائم تشويه السمعة عبر الانترنيت ، و جرائم نشر الفيروسات عبر الشبكة) .وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي"**(محمود نجيب حسني،1992، ص 13).**

-3-مرتكبو الجريمة الإلكترونية: إن أنواع الجناة في جرائم الانترنت وكما يُطلق عليهم إسم القراصنة، يمكن حصرهم في ثلاث فئات :

أ -الهاكرز :ويُطلق هذا الاسم على القراصنة ، والقرصنة هواية أو فضولي ليس أكثر ويكون غرضها تخريبيّاً ليس هادفاً لغايات ، وتكون غالباً من الفئة الشبابية المصابة بهوس التعمق بالمعلومات الإلكترونية والحاسوب.

ب -الكراكرز :وهم القراصنة المحترفون، ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الإلكترونية.

ت -الطائفة الحاقدة :تستهدف غالباً هذه الطائفة المنظمات والمنشآت وأرباب العمل، ويكون الهدف من ارتكابها للجريمة بحق هذه الأطراف عادة بغية الانتقام والحصول على المنفعة المادية أو السياسية،وقد يكون تطرف أو جاسوس أو مخترق الأنظمة".(**عبد الفتاح مراد ، 2005 ،ص65).**

***دوافع إرتكاب الجريمة الإلكترونية** :يمكن ردها لدوافع مادية، سعياً لإشباع الرغبة بتحقيق الثراء أو دوافع شخصية، التعلّم،الانتقام ،التسلية سياسية حتى يتمكن القراصنة من تنفيذ جريمتهم الإلكترونية يستلزم ذلك توفر أدوات عدة وأبرزها

الاتصال بشبكة الإنترنت، توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب،وسائل التجسس، ومنها ربط الكاميرات بخطوط الاتصال الهاتفي،البار كود، وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز،طابعات ،هواتف رقمية ونقالة " **(عبد الفتاح مراد ،2005 ،ص،68)**.

-4-الطبيعة القانونية للجريمة الإلكترونية و خصائصها :

4-1-الطبيعة القانونية الجريمة الإلكترونية: تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى إرتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة . على أساس أن هذه الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة كما قد ترتكب هذه الجرائم في مجال أو معالجة النصوص . و صعوبة التكييف القانوني للهذه الجرائم تكمن في طبيعتها الخاصة لأن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة ، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات ،و متابعة مرتكبيها وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة". **(محمد زكي أبو عامر وعلي عبد القادر القهوجي ، 1993 ، ص9)**.

-4-2-:خصائص الجريمة الإلكترونية:

- 1 جريمة عالمية:

بمعنى انها تتعدى الحدود الجغرافية للدول،إنها جرائم عابرة للقارات ، حيث يمكن ان يكون الجاني في بلد و المجني عليه في بلد آخر"**(عبد الفتاح مراد، 2005، ص 42)**.

-2 جرائم صعبة الإثبات: صعوبة متابعتها واكتشافها بحيث لا تترك أثرا فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الالكترونية تم إكتشافها بالصدفة وبعد وقت طويل من ارتكابها، ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها على أساس أتها تفتقر إلى الدليل المادي التقليدي كالبصمات. كما يصعب الاحتفاظ الفني بآثارها أن وجدت، تحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي منالها أو التعامل معها،لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع و التضليل بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول الى الدليل وقد يلجا مرتكبيها لتشفير التعليمات لمنع إيجاد أي دليل يدنيه". **(هشام محمد رستم،1999 ، ص،24)**.

3 جرائم ناعمة: الجرائم الالكترونية تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما.**(عبد الفتاح مراد،2006 ص 46).**

عدم التبليغ :عند وقوع الجريمة بواسطة الانترنت نجد ان بعض المجني عليهم يمتنعون عن ابلاغ السلطات المختصة خشية على السمعة و المكانه ،و عدم اهتزاز الثقة في كفاءته خاصة اذا كان كيان او هيئة معينة وقد اقترح في و م أ بان تفرض النصوص المتعلقة بجرائم الحاسوب التزاما على عاتق موظفي الجهة المجني عليها، بالإبلاغ عما يقع عليها من جرائم متى وصل الى علمهم ذلك مع تقرير جزاء في حالة إخلالهم بهذا الالتزام.**(عر الفاروق ،1995 ،ص 15).**

-5 أنواع الجرائم الإلكترونية:

إن الجرائم الالكترونية جرائم متعددة ومتنوعة، ويستعصي حصرها بسهولة ،بحيث توجد عدة تصنيفات لجرائم الحاسب الآلي والانترنت فهناك من يصنفها بحسب الفئات مثل جرائم ترتكب على نظم الحاسب الآلي ، أو بحسب الأسلوب المتبع في الجريمة أو الباعث الدافع لارتكابها ،غير أننا يمكن أن نجمل الجرائم التي وردت في أغلب التشريعات على النحو الآتي:

_ 1جريمة الدخول غير المشروع :

معناه دخول الشخص إلى شبكة الانترنت بدون ترخيصا من الجهة المخولة منح هذه الصلاحية ،هذا الفعل يؤكد إرتكاب الجريمة عمدا عن طريق خرق التدابير الأمنية بقصد الحصول على بيانات الكمبيوتر.

_ 2تخريب أو إتلاف أجهزة المعلومات أو احدي مكوناتها:

إن حماية شبكة المعلوماتية يستلزم التدخل لتجريم الأفعال التي تهدف إلي تخريب أو تعطيل أو إتلاف الأجهزة المادية و المتمثلة في الحاسوب أو البيانات و المعلومات الموجودة بداخله لأن علة التجريم هي حماية المعلومات والأجهزة المادية من أفعال التخريب.

_صناعة الفيروسات أو نشرها:

هي وسيلة تستخدم لتدمير المعلومات و البيانات و البرامج و تعطيل شبكة المعلومات.**(محمد السعيد رشدي،1999،ص3ومايليها).**

-4الغش أو التغيير في مواصفات و خصائص تقنية المعلومات:

تتحقق الجريمة بتغير الخصائص أو المواصفات بسلوك إيجابي يأتيه الفاعل بطرق تدليسية إحتيالية بحيث تعرض تقنية المعلومات أو مكوناتها وما في حكمها إلى الغش الذي يعد انتهاكا لحقوق الملكية الفكرية.

- 5سرقة الأجهزة أو المكونات أو المعلومات و ما في حكمها:

تعتبر جريمة سرقة وإخلال بحقوق الملكية الفكرية أو براءة الاختراع أو العلامات المسجلة على أساس أن محل السرقة الحاسوب ككيان مادي.

-6جرائم النظام العام والآداب العامة الاتجار في الجنس البشري:

الإخلال بالنظام العام والآداب، إنشاء أو نشر مواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام الآداب، انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة، الإساءة إلى السمعة،والدعارة والمخدرات وغسيل الأموال.

-7 -الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية.

إن التمعن في قراءة النصوص المنظمة لجرائم الانترنت في التشريعات العربية تكشف عن حقيقة متواترة في جل هذه التشريعات، ألا وهي اهتمامها الكبير عند تنظيم الانترنت وضبطه، بجعل حماية الدولة وأمنها كهدف أسمى من طرف المشرع قبل حماية أمن المواطن، وهذه مسألة واضحة على مستوى النصوص

-8جرائم الإرهاب الاعتداء على الملكية الفكرية :

إن المتضرر الأول من إساءة إستخدام شبكة المعلوماتية حقوق الملكية الفكرية سواء ما يتعلق منها بحقوق المؤلف أو الحقوق المجاورة والمتعلقة بالبرامج والإصدارات الخاصة بنظم المعلومات أو بالمصنفات الفكرية أو الأدبية أو الأبحاث العلمية التي باتت متاحة على شبكة المعلوماتية ويتم نسخها و تداولها دون أن تنسب إلي صاحبها الأصلي وهو ما يلحق ضررا بليغا بهذه الطائفة من الحقوق التي تعرف بالذهنية أو الفكرية.**(عز الفاروق 1995،ص15).**

مما لا شك فيه إننا بأمس الحاجة إلي التشدد في مواجهة منتهكي حقوق الملكية الفكرية خاصة وأ ن القوانين ذات العلاقة لم تجرم الأفعال التي تتم بإساءة استخدام تقنية المعلوماتية هذا من ناحية و من ناحية أخري أن قانون حماية المؤلف والحقوق المجاورة الوطني لا زال قاصرا في مواجهة هذه الانتهاكات.

7--مشكلة إثبات الجريمة الإلكترونية .الجريمة الإلكترونية ظاهرة اجرامية مستجدة مع تطور أنماطها يوما بعد يوم وما أتاحته الشبكة من فرص جديدة لارتكابها،ما جعل إثباتها من العقبات التي يعمل الخبراء على كسرها من أجل إيجاد وسائل إثبات ناجعة على أساس أنها تتطلب خبرة فنية عالية واعتماد أسلوب واضح في التحقيق.

6-القوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية:

أولا:قانون البريد والاتصالات السلكية واللاسلكية :

باستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات بحيث لاحظنا أنه تسارع مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان اجراء التحويلات المالية عن الطريق الالكتروني ذلك ما نصت عليه المادة 87 منه (**المادة87 من قانون البريد والإتصالات السلكية واللاسلكية رقم 03-2000 المؤرخ في2000/08/05.** ، كما نصت المادة84 /2 منه على استعمال حوالات دفع عادية أو الكترونية أو برقية)" **المادة 2/84 من نفس القانون،" تطبق أحكام المادة 89 من هذا القانون عن استعمال حوالات دفع عادية أو الكترونية أو برقية'**

كما نص في المادة 105منه على إحترام المراسلات(**المادة 105من نفس القانون"لايمكن في أي حال من الأحوال انتهاك حرمة المراسلات**) بينما أتت المادة 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات. (**المادة127 من نفس القانون،" كل موظف أو عون.....)**

ثانيا:قانون التأمينات:

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي في نصوص قانونية عديدة تخص البطاقة الالكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني،وكذا للجزاءات المقررة في حالة الاستعمال غير المشروع او من يقوم عن طريق الغش بتعديل أو نسخ أو حذف

كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 93مكرر2.

ثالثا:القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها:

جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والإتصال وكل ما يتعلق بالمنظومة

المعلوماتية، والمعطيات المعلوماتية، ومقدموا الخدمات، والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية.(**أنظر:المواد من المادة الثانية حتى 14من قانون رقم04-09 المؤرخ في 2009/08/05 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا ٱلإعلام والإتصال ومكافحتها.**

من مراقبة و تفتيش المنظومات المعلوماتية عند الضرورة،و حجز المعطيات المعلوماتية،و حفظ المعطيات المتعلقة بحركة السير.على الإلتزامات الخاصة بمقدمي خدمة الإنترنت ،وأخيرا على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

6-2- الهياكل الخاصة للتصدي للجرائم الإلكترونية

أولا :الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال :

وأنشئت بموجب القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقاية، ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية،في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية أللاقتصاد الوطني **(أنظر:القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السابق ذكر).**

ثانيا:الهيئات القضائية الجزائية المتخصصة

أنشئت بموجب القانون 14/04المؤرخ في 10/11/2004المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد329،37،و40 من ق.إ.ج.تتمتع اختصاص إقليمي موسع طبقا

للمرسوم التنفيدي رقم 348/06 المؤرخ في .05/01/2006بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04(**هواري عياش،2016،ص3**).

ثالثا:المعهد الوطني للأدلة الجنائية وعلم الجرائم .

يتكون من احدى عشرة دائرة متخصصة في مجالات مختلفة ، جميعها تضمن إنجاز الخبرة ، التكوين والتعليم و تقديم المساعدات التقنية ،و دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات . (**د/حملاوي عبد الرحمان،2016،ص33**).

رابعا:المديرية العامة للأمن الوطني

تتصدى هده المديرية للجريمة الإلكترونية من عدة جوانب وأ منها الجانب التوعوي بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعية وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

ودائما في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم ،فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائيةINTERPOL هاته الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين ، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا.(**د/علي عبد القادر القهوجي. 1999،ص120**).

موقف المشرع الجزائري من الجريمة الإلكترونية :رغم صعوبة ضبط و مكافحة جرائم الانترنت على الصعيد الوطني إلا أن هناك جهود معتبرة قام بها المشرع الجزائري في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم، متأثرا بجل الدول العربية التي وضعت قوانين لمكافحة جريمة الانترنت، فعلى امتداد الوطن العربي من المحيط إلى الخليج، نجد ترسانة قانونية تنظم جرائم الانترنت، وبدأت هذه الحركة في الظهور والانتشار منذ بداية الألفية الثالثة وعلى الأخص منذ منتصف العشرية الأولى منها، ومن أهم الأمور التي أعطى لها المشرع الجزائري أهمية قصوى أمن الدولة والحفاظ على النظام العام. كما أنه ركز كل اهتماماته على حماية الدولة، وجعلها من أسمى أهدافه.لذلك حاول المشرع الجزائري ، إصدار قوانين عامة وخاصة ووضع هياكل وأجهزة للتصدي للجرائم الإلكترونية، ويعود أسباب الاهتمام بتنظيم جرائم

الانترنت من جهة تطور تكنولوجيا الإعلام لاتساع نطاق الجريمة الإلكترونية فهي أصبحت لا تقتصر على جريمة واحدة وإنما إتسعت إلى عدة جرائم ترتكب عن طريق الهاتف وعن طريق الكمبيوتر ،ولا ترتكب هذه الجريمة من طرف شخص طبيعي فقط بل تعدت إلى الشخص المعنوي ومن جهة أخرى كون القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الالكترونية الحديثة وعدم القدرة على المحافظة على مبدأ الشرعية الجنائية ، متكلا على تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها.

10-القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية :قد خص المشرع الجزائري تنظيم الجريمة الإلكترونية بقوانين عامة وأخرى خاصة منها:

1-الدستور الجزائري :كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016حماية الحقوق الأساسية و الحريات الفردية، و على أن تضمن الدولة عدم إنتهاك حرمة الإنسان. و قد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات و الإجراءات الجنائية وقوانين خاصة أخرى و التي تحظر كل مساس بهذه الحقوق. ومن أهم المبادئ الدستورية العامة:

المادة : 38الحرّيّات الأساسيّة وحقوق الإنسان والمواطن مضمونة.

المادة :44حرّيّة الابتكار الفكريّ والفنّي والعلمي مضمونة للمواطن .حقوق المؤلّف يحميها القانون .لا يجوز حجز أيّ مطبوع أو تسجيل أو أيّة وسيلة أخرى من وسائل التّبليغ والإعلام إلاّ بمقتضى أمر قضائيّ.الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون .تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.

لا يجوز انتهاك حرمة حياة المواطن الخاصة ، وحرمة شرفه ،ويحميها القانون ، سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة". أن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائي .

2-قانون العقوبات :لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون بموجب القانون العقوبات رقم 04-15 المؤرخ – في 10 نوفمبر 2004 المتمم لأمر رقم- 66-156 المتضمن قانون العقوبات تحت

عنوان المساس بأنظمة المعالجة الآلية للمعطيات " ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394المادة مكرر 7.

*وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون- رقم 06-23 المؤرخ في 20 ديسمبر 2006حيث مس هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص ، الواردة في هذا القسم من القانون 04-15 وربما يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث من الإجرام بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى وشيوع إرتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وإنتشار الأنترنت كوسيلة لنقل المعلومات.

أولا -أنواع الجرائم الإلكترونية في قانون العقوبات الجزائري والعقوبات المقرر لها:

طبقا لقانون العقوبات الجزائري المعدل والمتمم والذي أستحدث فيه المشرع الجزائري قسما خاصا في القسم السابع مكرر من الفصل الثالث الخاص بالجنايات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات(،وعلى هذا الأساس يمكن تصنيفها إلى مايلي:

-1الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات

-2حذف أو تغيير لمعطيات المنظمة.

- 3-تصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار.

-5 - حيازة أو إفشاء أو نشر أو استعمال المعطيات.)

-6 تكوين جمعية أشرار.

ثانيا:العقوبات المقررة لهذه الجرائم:

طبقا لقانون العقوبات وبناءا على للمواد 11،12و13 من الاتفاقية الدولية للإجرام المعلوماتي فإن العقوبات المقررة للإجرام ألمعلوماتي يجب أن تكون رادعة وتتضمن عقوبات سالبة للحرية والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، و الشخص المعنوي.

1-العقوبات المطبقة على الشخص الطبيعي :أ -**العقوبات الأصلية** -عقوبة الحبس تتراوح مدتها من شهرين إلى ثلاثة سنوات، حسب الفعل المرتكب و الغرامة تتراوح قيمتها من خمسين ألف دج إلي خمسة مائة ألف دج،حسب الفعل المرتكب :الدخول والبقاء بالغش (الجريمة البسيطة)،الدخول والبقاء بالغش (الجريمة المشددة)و تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة ،الاعتداء ألعمدي على المعطيات ·

ب-العقوبات التكميلية:المصادرة تشمل الأجهزة و البرامج و الوسائل المستخدمة في إرتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير في حسن النية.

إغلاق المواقع :الأمر يتعلق بالمواقع (les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية، **وإغلاق المحل أو مكان الاستغلال** إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها ·

عقوبة الشروع في الجريمة :جاءت به المادة 11 من الاتفاقية الدولية للإجرام ألمعلوماتي واعتمده المشرع الجزائري بالنسبة للجرائم الماسة بالأنظمة المعلوماتية ،بحيث توسع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ،إذ أصبح الشروع معاقب عليه بنفس عقوبة المقررة على الجنحة ذاتها ·

* -**الظروف المشددة**:نص القانون على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول و البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة، تضاعف العقوبة اذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات العامة ·

2- العقوبات المطبقة على الشخص المعنوي :يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها ،كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه .وبالتالي عقوبة الشخص المعنوي تتمثل في الغرامة التي تعادل خمس مرات الحد الأقصى المقرر.

للشخص الطبيعي علما أن نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات تحدد المسؤولية الجزائية للشخص المعنوي والعقوبات المقررة.

-**عقوبة الاتفاق الجنائي:**تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5 بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ،وعقوبة الاشتراك في الاتفاق تكون نفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تكون العقوبة هي عقوبة الجريمة الأشد.

11-قانون الإجراءات الجزائية الجزائري :

بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية،كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة . غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية .

كما نص على التفتيش في المادة 45 الفقرة 7من نفس القانون المعدلة حيث أعتبر إن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه ، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطته المشرع بقواعد صارمة،وبالتالي لا تطبق الأحكام الواردة في المادة 44 من فانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم ٱلكترونية. ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة6 وكذا على "اعتراض.المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5/ 10. كما أن قانون الإجراءات الجنائية نص على ألا يجوز ضبطها إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة. غير أنه طبقا لقانون الإجراءات المعدل و المتمم في الفصل الرابع تحت عنوان "في إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور". نصت المادة (65 مكرر5/3)على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن بالإعتراض و وضع ترتيبات تقنية دون موافقة المعنيين من أجل إلتقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية .

الخاتمة: ،لقد توصلنا إلى نتائج جد هامة كما قدمنا بعض الاقتراحات التي رأيناها مفيدة لموضوع المداخلة.

-**النتائج:**أهم النتائج التي توصلت لها الدراسة:لم يتفق على تعريف جامعا مانعا للجريمة الإلكترونية.

- تبين من خلال دراسة خصائص الجريمة الإلكترونية أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية.

- قصور القوانين التقليدية أمام هذه الجرائم المستحدثة.رغم إجتهاد المشرع الجزائري للتصدي لهذه الجريمة،إلا أنه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة.
- إن التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية ، خاصة فيما يتعلق بحقوق الملكية الفكرية والحقوق المجاورة لم تعد قابلة للتطبيق في البيئة الرقمية. كماأن النصوص الوضعية لحماية حقوق المؤلف والحقوق المجاورة تعتبر غير كافية لمواجهة الاعتداءات الواقعة عليها عبر الانترنت.

ب –الاقتراحات :

- من واجب المشرع أن يضع نصوصا قانونية واضحة وخالية من الغموض، بحيث أنها ستؤطر ظواهر اجتماعية جديدة مستقبلا.
- عند وضع النصوص يجب أن يدقق في حماية المواطن، على أساس أن حماية الأمن الرقمي يمكن أن تحيل على مفاهيم متعددة تتراوح مابين حماية الأشخاص، وحماية المجموعات وغيرها.
- ضرورة التعاون الدولي لمكافحة هذه الجرائم من خلال مجموعة تشريعات وطنية واتفاقيات دولية وإقليمية
- عقد الدورات التدريبية التي تعتني بمكافحة الجرائم الإلكترونية. مع ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم وبالتعاون مع التقنيين من أصحاب الخبرة.

- احتراما لحقوق الإنسان عامة ولحقوق المواطن خاصة وحتى تتكامل يجب أن يكفلها المشرع الجنائي بالحماية القانونية الرادعة، وهذا بالتصدي لمواقع ووسائل اختراق المواقع بمختلف صورها.

قائمة المراجع:

أولا: المصادر باللغة العربية:

1- –أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الأنترنت ، دار المطبوعات الجامعية الأسكندرية ، 2009
2- حملاوي عبد الرحمان ، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ،جامعة بسكرة كلية الحقوق ، 2016 .

3-عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية مصر 2006 .

4-عبد الفتاح مراد ، شرح جرائم الكمبيوتر و الانترنت ، دار الكتب والوثائق المصرية ، 2005 .

5- عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي ، دار الكتب والوثائق المصرية،2006

6-عر الفاروق ، المشكلات الهامة فى الجرائم المتصلة بالحاسوب الالي وأبعادها الدولية ، دراسة مقارنة ،مصر، ط 2 ،1995 .

7--علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الالي ، دار الجامعية للطباعة والنشر ، بيروت ، د ط ، ص120 ،1999.

8-محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، بدون رقم الطبعة، دار النهضة العربية، القاهرة 1992.

9- محمد عادل ريان ، جرائم الحاسب الالي و أمن البيانات،بيروت،2002.

10-مكتب المحاسبة العامة للولايات المتحدة الامريكية GOA انظر :www.goa.gov –

11- محمد زكي أبو عامر وعلي عبد القادر القهوجي ، قانون العقوبات القسم الخاص ، دار النهضة العربية القاهرة 1993 .

12-محمد السعيد رشدى ، الانترنت والجوانب القانونية لنظم المعلومات ، بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق ،جامعة حلوان بعنوان الاعلام والقانون الذي عقد فى الفترة من 14-15/ مارس 1999م ص 3 وما يليها.

13-مني الاشقر ، القانون والانترنت " تحدي التكيف والضبط " ، بيروت ، الناشر ش م م 2008 ص 70 وما يليها

14-هشام محمد رستم : الجوانب الاجرائية للجرائم المعلوماتية . مكتبة الالات الحديثة. اسيوط 1994.

15 هشام محمد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد(2)،1999.

16-هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1992

17- هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ،المعهد الوطني للأدلة الجنائية وعلم الإجرام ، جامعة بسكرة كلية الحقوق،2016.

ثانيا :الملتقيات:

18-المقدم عز الدين عز الدين ، ملتقى حول الجرائم المعلوماتية ، الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ،بسكرة في:2015/11/16.

ثالثا:القوانين والأتفاقيات:

19- القانون رقم 16-01 المؤرخ في 6-03-2016 المعدل للدستور عدد الجريدة الرسمية 14.

20- القانون رقم04-15 المؤرخ في10 نوفمبر 2004 ،المعدل والمتمم

21 -أنظر :المادة394 مكرر1 "يعاقب بالحبس من06 اسهر الى03 سنوات و بغرامة من500.000 دج الى2000.000 كل من ادخل بطريقة الغش معطيات في نظام أو أزال او عدل بطريقة الغش المعطيات التي يتضمنها"

22- أنظر :المادة394 مكرر2 "يعاقب بالحبس من شهرين الى03 سنوات و بغرامة من1000.000 دج الى5000.000 دج كل من يقوم عمدا و عن طريق الغش .

23- أنظر :المادة394 مكرر6 "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

24-أنظر:المادة394 مكرر7 "يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها".

25- أنظر :المادة394 مكرر3 "تضاعف العقوبة المنصوص عليها في هذا القسم اذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات اشد".

26-أنظر :المادة394 مكرر4 "يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي"

27- أنظر المادة: 394مكرر5،السابق ذكرها.

28--أنظر:المادة 37 من قانون الإجراءات الجنائية المعدل والمتمم بأمر رقم 15-02 مؤرخ في 23 يوليو سنة 2015 ،يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية،الجريدة الرسمية عدد40

29- أنظر:المادة 45 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84

30- أنظر:المادة 51 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84،.

31- أنظر:تمم الباب الثاني من الكتاب الأول بقانون رقم قم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 ص8 ،بفصل رابع بعنوان "في اعتراض المراسلات و تسجيل الأصوات والتقاط الصور"ويشمل المواد من 65 مكرر5حتى 65مكرر10.

32-المادة87 من قانون البريد والإتصالات السلكية واللاسلكية رقم 03- 2000 المؤرخ في2000/08/05. على أنه " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق البريد الإلكتروني"

33-أنظر :المادة 2/84 من نفس القانون،" تطبق أحكام المادة 89 من هذا القانون عن استعمال حوالات دفع عادية أو الكترونية أو برقية'

34- أنظر:المادة 105من نفس القانون"لايمكن في أي حال من الأحوال ابتهاك حرمة المراسلات"و المادة127 من نفس القانون.

35-أنظر المادة 6 مكرر1،والمادة 65مكرر1 من القانون رقم 08/01 المؤرخ في 2008/01/23والمعدل والمتمم لقانون 83/01 المتعلق بالتامينات.

36-أنظر المادة 93 مكرر2و3 من نفس القانون، "دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 100.000 دج إلى 200.000 دج كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهن الصحة"

37- أنظر:المواد من المادة الثانية حتى 14من قانون رقم04-09 المؤرخ في 2009/08/05 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا آلإعلام والإتصال ومكافحتها.

38-أنظر:القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السابق ذكره.

رابعا:المصادر باللغة الانجليزية:

39- Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989,