جامعة عمار ثليجي –الأغواط–
كلية العلوم الإنسانية والعلوم الإسلامية و الحضارة
قسم: علوم الإعلام والاتصال

الموضوع

دور الأجهزة الأمنية في مكافحة الجريمة الإلكترونية والتواصل الاجتماعي

دراسة ميدانية بمديرية الامن الوطني ولاية الاغواط

مذكرة تخرج ضمن متطلبات نيل شهادة الماستر في علوم الاعلام والاتصال
تخصص : اتصال وعلاقات عامة

من إعداد الطلبة:
– بدوي حمزة
–لوباشرية محمد

إشراف الدكتور
طريف عطاء الله

الدكتور :..... رئيسا

الدكتور :..... مشرفا ومقررا

الدكتور :..... عضوا و مناقشا

السنة الجامعية 2019/2018

كلمة شكر

الحمد لله الذي بيده مفاتيح غيبه واليه المنتهى كل عمل وغاية الذي منحنا العلم وأجراه على يد علماء أجلاء

على إثر إنهاء هذه المذكرة نتوجه بالشكر الجزيل إلى "الله عز و جل" أولا والى كل من قدم لنا يد العون والمساعدة من قريب أو من بعيد ونخص بالذكر الدكتور عطاء الله طريف

والى كل موظفي وأساتذة قسم علوم الاعلام والاتصال

ولله الحمد من قبل ومن بعد على نعمته علينا.

بدوي حمزة

لوباشرية محمد الامين

إهـــــداء

الحمد لله الذي يسر لي ما كان عسيرا وسهل لي سبل العبور لأصل إلى هذه المكانة وأنال بذاك رضاه و رضى كل من يحبون لي الخير

وأهدي اعتزازي وحبي وكل إحساس جميل يملا قلبي إلى من هما وليا نعمتي ولهما فضل تعلمي والى من أعطياني الكثير ولم يبخلا عليا .

أقدم هذا العمل الى أخوتي وأخواتي والى أفراد عائلتي كبيرا و صغيرا

إلى جميع الأهل والأقارب وكل من يحتمل لقب "بدوي".

إلى أساتذتي الأفاضل والى كل طالب علم

اهدي هذا العمل المتواضع.

بدوي حمزة

إهداء

نحمد الله على نعمة الإسلام ونشكره على إتمام عملنا فإليه يرجع الأمر كله والصلاة والسلام على سيدنا محمد وعلي اله صحبه وسلم تسليما كثيرا

اهدي هذا العمل المتواضع إلى من أوصى الله بهما خيرا في كتابه العزيز فقال" وبالوالدين إحسانا " أكرمنا الله ببرهما

امي نور عيني وروح ابي ادام الله وجوده بيننا

وثاني

والى كل الاقارب والاحباب من قريب او بعيد

لوباشرية محمد الامين

الفهرس

الفهرس

كلمة شكر	
الاهداء	
مقدمة	**أ**
الفصل الأول : الاطار المنهجي	
1.الاشكالية	**04**
2. الاسئلة الفرعية	**04**
3. فرضيات الدراسة:	**05**
4. أهمية الدراسة:	**05**
5. اهداف الدراسة	**05**
6. أسباب اختيار الموضوع	**05**
7. منهج الدراسة	**06**
8.أدوات جمع المعلومات	**07**
9. مجتمع الدراسة	**10**
10. حدود الدراسة	**10**
11. ضبط المفاهيم والمصطلحات	**10**
12.الدراسات السابقة	**14**
الاطار النظري	
الفصل الثاني : الجريمة الالكترونية ومواقع التواصل الاجتماعي	
تمهيد	**17**
المبحث الاول :مفهوم الجريمة الالكترونية	**18**
المطلب الأول: ماهية الجريمة الالكترونية	**18**
المطلب الثاني: أركان الجريمة الإلكترونية.	**25**
المبحث الثاني: مواقع التواصل الاجتماعي كأحد انماط الاعلام الالكتروني	**28**
المطلب الأول: نشأة وتطور مواقع التواصل الاجتماعي	**28**
المطلب الثاني:الجريمة الالكترونية عبر مواقع التواصل الاجتماعي	**36**

الفهرس

خلاصة	51
الفصل الثالث: الأجهزة الأمنية المكلفة بمحاربة الجريمة الالكترونية	
تمهيد	53
المبحث الأول: نشأة وتطور الأجهزة الأمنية الجزائرية	54
المطلب الأول: الضبطية القضائية	54
المطلب الثاني: إختصاصات وصلاحيات الضبطية القضائية	55
المبحث الثاني: الاليات المسخرة لمكافحة الجريمة المعلوماتية	72
المطلب الأول: القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية	72
المطلب الثاني: قانون الإجراءات الجزائية الجزائري .	76
المطلب الثالث: القوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية	78
خلاصة	82
الجانب التطبيقي	
الفصل الرابع: الجانب الميداني للدراسة	
تمهيد	84
المبحث الاول : جوانب التصدي للجريمة الالكترونية :	85
المطلب الاول : الجانب القانوني:	85
المطلب الثاني: الجانب التنظيمي	86
المطلب الثالث: العمل الميداني للتصدي للجريمة الالكترونية	88
المبحث الثاني: عرض النتائج وتحليلها	90
المطلب الاول : عرض نتائج الدراسة	90
المطلب الثاني: الاستنتاج العام	92
الخاتمة	94
المراجع	
الملاحق	

مقدمة

مقدمة

تعد الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم، وتعتبر ثورة الاتصالات هي المحرك الأساسي في التطورات الحادثة في الوقت الحالي، إلا أنها ليست المحرك الوحيد في هذه التطورات حيث أن التطور الكبير في تكنولوجيا الحاسبات قد أسهم بصورة كبيرة في تسارع معدلات التقدم في مجال الاتصالات والمعلومات.

وقد كان من نتاج التطور في الجانبين ظهور أدوات واختراعات وخدمات جديدة في مختلف المجالات ولقد نتج عن الثورة التكنولوجية تلك ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التي نعرفها من حيث البيئة التي تتم فيها هذه المعاملات.

ويقصد بالمعاملات الإلكترونية كل المعاملات التي تتم عبر تجهيزات إلكترونية مثل الهاتف، والفاكس، وأجهزة الحواسب، وشبكة الإنترنت، ومؤخراً عن طريق الهاتف المحمول. وتتكون تلك المعاملات من عدد من المكونات الأساسية، يهمنا في هذه الورقة طرح مكون أساسي فيها وهو الجزء الخاص بجرائم تلك المعاملات، أو بمعني أدق القواعد القانونية الجنائية التي تحكم الأفعال التي تتم من خلال أجهزة الحواسب، أو عبر شبكة الانترنت.

لا شك أن التكنولوجيا الجديدة تجلب معها تهديدات جديدة، وهذه التهديدات كبيرة كثيرة أثرت بشكل مباشر على حياة البشر وهددت استقرارهم، فقد انتشرت في الآونة الأخيرة ظاهرة ما يعرف بالجرائم الإلكترونية بشكل كبير ومتزايد، بسبب انتشار أجهزة الحاسب الآلي وأجهزة الهواتف الذكية المتصلة على شبكة الإنترنت، وبلا شك فإن هذا النوع من الجرائم أصبح واقع يهدد وبشكل مريب سمعة وحياة الأفراد، لذلك وجب التنبيه حتى لا نقع ضحيته.

إن جرائم الكمبيوتر والانترنت، أو ما يسمى Cyber Crimes هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل علي المستويات الاقتصادية والاجتماعية والثقافية والأمنية.

إذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، إلا أن هناك دولا عربية كثيرة أضحت مهتمة بتلك الظواهر، ومفهومها القانوني، وسمات المجرم

المعلوماتي، وهو ما سوف نحاول أن نتعرض له بشيء من التفصيل في هذا البحث محاولين أن نضع ولو لبنة صغيرة في الإطار التنظيمي والتشريعي في تلك المسألة.

فالجريمة الإلكترونية هي جريمة تقع على المؤسسات أو الأفراد مستخدمي أجهزة الحاسب الآلي أو أجهزة الهواتف الذكية، وهي بلا شك سلوك لا أخلاقي وغير مصرح به وينكره القانون ويعاقب عليه ويدينه الشرع وينبذه المجتمع، حيث يتم ارتكاب الجريمة الإلكترونية باستخدام أدوات الاتصال الحديثة بالإضافة إلى مجموعة البرامج والتقنيات المعدة لهذا الأرض.

تناولنا الدراسة من خلال مقدمة ثم الاطار المنهجي من الاشكالية والاسئلة الفرعية وفرضيات الدراسة ثم أهمية الدراسة واهدافها أسباب اختيار الموضوع، ومنهجه ثم أدوات جمع المعلومات ومجتمع الدراسة وحدود الدراسة وكذلك ضبط المفاهيم والمصطلحات وفي الاخير الدراسات السابقة ثم الفصل الثاني بعنوان الجريمة الالكترونية ومواقع التواصل الاجتماعي من خلال المبحث الاول حول مفهوم الجريمة الالكترونية وفي المبحث الثاني مواقع التواصل الاجتماعي كأحد انماط الاعلام الالكتروني اما الفصل الثالث فقد تطرقنا الى الأجهزة الأمنية المكلفة بمحاربة الجريمة الالكترونية من خلال المبحث الأول نشأة وتطور الأجهزة الأمنية الجزائرية وفي المبحث الثاني الاليات المسخرة لمكافحة الجريمة المعلوماتية ثم كان الفصل الرابع الجانب الميداني للدراسة من خلال المبحث الاول جوانب التصدي للجريمة الالكترونية والمبحث الثاني عرض النتائج وتحليلها، في الاخير خاتمة عامة للدراسة

الفصل الأول الاطار المنـهجي

1. الاشكالية
2. الاسئلة الفرعية
3. فرضيات الدراسة:
4. أهمية الدراسة:
5. اهداف الدراسة
6. أسباب اختيار الموضوع:
7. منـهج الدراسة
8. أدوات جمع المعلومات
9. مجتمع الدراسة
10. حدود الدراسة
11. ضبط المفاهيم والمصطلحات
12. الدراسات السابقة

1.الاشكالية

تتشابه الجريمة الالكترونية مع الجريمة التقليدية في اطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة وضحية والذي قد يكون شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة ،وهنا يكمن الاختلاف الحقيقي بين نوعي الجريمة ففي الجريمة الالكترونية الاداة ذات تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجانى اليه انتقالا فيزيقيا ولكن في الكثير من تلك الجرائم فان الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجانى ومكان الجريمة

ومن قبيل ذلك ، وبكل تأكيد، أجهزة الأمن باعتبارها القوامة على كفالة الأمن والاستقرار ، وبحسبانها ركيزة للتنمية والتقدم في المجتمع ، ذلك أن الأمن هو التنمية وبدون تنمية لا يوجد امن ، إضافة إلى ذلك ، فان الظروف والأوضاع الاقتصادية والاجتماعية والسياسية وغيرها على الساحتين الإقليمية والدولية فرضت نفسها وبشكل حتمي على ارض الواقع ، واقتضت بالضرورة مواجهة ما أفرزته من مشكلات لها انعكاسات على الأمن بدرجات متفاوتة فضلا عن مواجهة الجريمة في سائر صورها وأشكالها ودرجاتها بأسلوب علمي يواكب النمط العلمي المتخصص الذي ترتكب به الجريمة سواء في جانبه المتعلق بفكرة الجريمة ذاتها أو في طريقة ارتكابها ووسيلة إتمامها ، خاصة ما يعرف بالجريمة المنظمة أو جرائم خارج النطاق ، وجرائم العنف والإرهاب التي أصبحت ظاهرة خطيرة تهدد وجود المجتمعات في ذاتها.

ومما لا شك فيه ، أن مواجهة تلك المخاطر والتحديات تتطلب اجهزة امنية تتمتع بالكفاءة الفنية والتقنية من اجل القدرة على الكشف والبحث والتحري عن مثل هذه الجرائم التي تعتبر وليدة العصر الحديث ، التي تعتمد على منطلقات ومقومات لاغنى عنها حتى تحقق أهدافها المرصودة لها.

ومنه نطرح لاشكالية التالية

ما دور الاجهزة الامنية في مكافحة الجريمة الالكترونية ؟

2. الاسئلة الفرعية

ومن خلال هذا السؤال الرئيسي تتفرع لدينا التساؤلات التالية:

هل يمكن اكتشاف مرتكب الجريمة الإلكترونية؟ بكل سهولة ويسر حيث أن هنالك مختصين يمكنهم تحديد هوية الجاني بسرعة كبيرة.

2. هل يعاقب القانون مرتكب الجريمة الإلكترونية؟

3. هل هناك اجهزة امنية متخصصة لمحاربة الجريمة الالكترونية؟

4.هل تتوفر هذه الاجهزة على التقنيات والمعارف الكافية لمواكبة التطور السريع في مجال الجريمة الالكترونية؟

3. فرضيات الدراسة:

تتمثّل فرضيات الدراسة فيما يلي:

- تطور المعاملات الالكترونية جعلها عرضة للجريمة الالكترونية .
- الإسراع في اتخاذ الإجراءات اللازمة لتطوير آليات التصدي للجرائم الالكترونية هو سبيل للحد منها .

4. أهمية الدراسة:

ترجع أهمية موضوع دور الاجهزة الامنية في مكافحة الجرائم الالكترونية التي تعرف الانتشار الواسع لهذا النوع من الجرائم والذي رافق الاستخدام الواسع للمعاملات الالكترونية على الصعيد الدولي والإقليمي والوطني هذا من جهة، ومن جهة أخرى فقد أصبحت الجريمة الالكترونية مُتلازمة مع التطور السريع والهائل في مجال تكنولوجيا الاتصالات والمعلومات، فنتيجة للتقدم الكبير في استخدامات الشبكة العنكبوتية ، طفت الجرائم الالكترونية بصورها المُختلفة، وأصبحت تهدد الأمن المعلوماتي للأفراد، المؤسسات والحكومات.

5. اهداف الدراسة

- التعرف على ماهية الجريمة الالكترونية و الإطلاع على حجم التطور الذي وصلت إليه .
- التعرف على مسببات تفشي الجرائم الالكترونية وعلى حجم الخسائر التي تحدثها.
- إبراز دور الاجهزة الامنية في التدخل للتصدي لهذا النوع من الجرائم .

6. أسباب اختيار الموضوع:

أ- الأسباب الموضوعية:

- الانتشار الواسع لاستعمال المعاملات الالكترونية ، وكذا أهميتها في حياة الافراد
- نقص الجانب الأمني في العالم الافتراضي مما يجعله أرضية خصبة للتجاوزات والجرائم.

ب- الأسباب الذاتية:

- من أجل توظيف معارفنا المكتسبة من خلال دراستنا في تخصص اعلام واتصال علاقات عامة ، والتناول بالشرح الجريمة الالكترونية والأجهزة الأمنية المكلفة بمحاربتها.
- الميل الشخصي للموضوع وحب الاستطلاع في مواضيع الجرائم الالكترونية التي أصبحت تمس حياة الافراد بشكل كبير مما يستدعي وجود جهاز امني مكلف بمحاربتها والكشف عن المجرم فيها.

7. منهج الدراسة

يعتبر اختيار منهج الدراسة من المراحل المهمة في عملية البحث العلمي اذ يحدد لنا كيفية جمع البيانات والمعلومات حول الموضوع المدروس ،ان دراسة اي ظاهرة تستلزم استخدام منهج علمي الذي يؤدي الى اكتشاف الحقيقة ،ويعرف المنهج العلمي عادة على انه:

يعتبر المنهج خطوة رئيسية في ترتيب و تنظيم أفكار الباحث ،للوصول إلى نتائج منطقية فالمنهج يعرف على انه " الطريق المؤدي الى المعرفة العلمية الصحيحة " .[1]

كما يعرف على انه " الطريق المتبع للكشف عن هذه الدراسة ،بواسطة استخدام مجموعة من القواعد ، و التي ترتبط أساسا بتجميع البيانات و تحليلها ، حتى تساهم في التوصل إلى نتائج ملموسة".[2]

و هو أيضا " مجموعة من الأسس و القواعد التي يتبناها الباحث ،بغرض التوصل إلى نتائج معينة ، ويعتبر من أهم الخطوات المتبعة في انجاز البحث العلمي ". [3]

و قبل التطرق إلى المنهج المستخدم ،لا بد من الإشارة إلى أن لكل منهج شروط و متطلبات وقدرات محدودة في البحث و التقصي، تفرض على الباحث استخدامها في حالات معينة ،و إن عملية اختيار الباحث لمنهج بحثه لا تتم بطريقة اعتباطية ، و إنما طبيعة الموضوع الذي يعالجه و نوعيته هي التي تفرض على الباحث تفضيل منهج على آخر .

---

[1] محي الدين مختار،: **لاتجاهات النظرية و التطبيقية في منهجية العلوم الاجتماعية**، دار المنشورات الجامعية،ط 01، باتنة، 1999، ص7.

[2] محمد الهادي محمد: **أساليب توثيق البحوث العلمية،ا لمكتبة الأكاديمية**، ط 01، الجزائر، 1995، ص287.

[3] محمد الغريب عبد الكريم: **مناهج البحث العلمي و طرق إعداد البحوث**، ديوان المطبوعات الجامعية،ط02، الجزائر، 1999، ص19.

و انطلاقا من أننا نحاول التعرف على الجريمة الالكترونية والأجهزة الأمنية المكلف بمحاربتها ومنه ينتمي هذا البحث إلى الدراسات المسحية بالعينة، وهي التي تهتم برصد ودراسة خصائص ظاهرة معينة من أجل التعرف على سماتها وخصائصها، والبحث اعتمد على منهج المسح بشقيه الوصفي للإجابة عن تساؤلات الدراسة معتمدا أسلوب المسح بالعينة فيما يخص مسح لعينة من عناصر الامن الوطني من أجل التعرف على دورهم في محاربة الجريمة الالكترونية ، واعتمدنا على المنهج التحليلي الوصفي في الجانب النظري من اجل اعطاء المفاهيم الخاصة بموضوع الدراسة.

8.أدوات جمع المعلومات

الملاحظة : يشير لفظ الملاحظة لغويا إلى النظر إلى الشيء الملاحظ بمؤخر العينين دلالة على التدقيق، فهي المعاينة المباشرة للشيء أو مشاهدته على النحو الذي هو عليه و يقال كذلك لاحظه أي رءاه و على ذلك تعني الملاحظة المشاهدة.

فكل منا يهتدي في سلوكه اليومي بما يلاحظ من ظواهر في حياته فالطفل في نشأته الاجتماعية يتعلم ملاحظة و مشاهدة ما يدور حوله من أحداث و ما يبدو على وجوه المحيطين من تعبيرات و رئيس العمل يلاحظ و يشاهد سلوك مرؤوسيه،و منذ أقدم العصور انشغل الكتاب و الشعراء بوصف ما يشاهدونه[1].

المعنى الاصطلاحي للملاحظة:

تعني الاهتمام أو الانتباه إلى الشيء أو حدث أو ظاهرة بشكل منظم عن طريق الحواس حيث نجمع خبراتنا من خلال ما نشاهده أو نسمع عنه، و الملاحظة العلمية تعني الانتباه للظواهر و الحوادث بقصد تفسيرها و اكتشاف أسبابها و الوصول إلى القوانين التي تحكمها. [2]

و تعتبر الملاحظة من أهم الأدوات المستخدمة في الدراسات الوصفية و تكمن أهمية تلك الأداة في جمع البيانات المتعلقة في كثير من أنماط السلوك التي لا يمكن دراستها إلا بواسطة تلك الأداة، كما أن الملاحظة المباشرة يمكن استخدامها في بحث وصفي، لدراسة سلوك

[1]حسين عبد الحميد أحمد رشوان:**أصول البحث العلمي**، الإسكندرية.مؤسسة شباب الجامعة،2006. ص 136

[2]جودت عزت عطوي:**أساليب البحث العلمي:مفاهيمه،أدواته، طرقه الإحصائية**، دار الثقافة للنشر و التوزيع،2007.ص 120

الأطفال و تصرفاتهم عندما يجتمعون بهدف اللعب، حيث يهدف لاكتشاف قدراتهم الحركية و المعرفية و الوجدانية أثناء ممارستهم لنشاط اللعب.[1]

المقابلة في اللغة:[2]

المقابلة: محادثة موجهة بين الباحث والشخص أو أشخاص آخرين بهدف الوصول إلى حقيقة أو موقف معين، يسعى الباحث للتعرف عليه من أجل تحقيق أهداف الدراسة.

المقابلة: وسيلة شفوية – مباشرة أو هاتفية أو تقنية لجمع البيانات– يتم خلالها سؤال فرد أو خبير عن معلومات لا تتوفر عادة في الكتب أو المصادر الأخرى .

كما يمكن تعريف المقابلة بأنها محادث موجهة يقوم بها فرد مع آخر أو أفراد آخرين لاستغلالها في بحث علمي، أو الاستعانة بها في التوجيه و التشخيص للعلاج .[3]

المقابلة : تفاعل لفظي يتم عن طريق موقف مواجهة يحاول فيه شخص القائم بالمقابلة أن يستشير معلومات أو آراء أو معتقدات شخص آخر أو أشخاص آخرين للحصول على بعض البيانات الموضوعية.[4]

المقابلة أو الاستبار ليست منهجا ، و إنمت هي أداة من أدوات جمع المعلومات في البحث العلمي ، بل و أكثرها استخداما و أحسنها وأفضلها على الاطلاق خاصة في المجتمعات التي تنتشر فيها الامية ،و هي ليست أداة منفصلة عن الأدوات الأخرى بل هي أداة إضافية تضاف إلى الادوات التكنيكية الأخرى . تستخدم المقابلة في الكثير من العلوم الانسانية ، خاصة علم النفس و علم الاجتماع و الانثروبولوجيا و لفظ الاستبار مشتقة من سبر و استبر الجرح أو البئر او الماء أي امتحن غوره ليعرف مقداره . و استبر الأمر أي جربه و اختبره، و تعني المقابلة أو الاستبار المواجهة أو المعاينة أو الاستجواب و هي تقوم على الاتصال الشخصي و الاجتماع وجها لوجه بين الباحث أو معاونيه المتمرنين ، و المبحوثين كل على حدى . و تحدث مناقشة أو محادثة موجهة من أجل البيانات التي يريد الباحث الحصول عليه و ذلك لغرض محدد.[5]

---

[1] نبيل الأحمد عبد الهادي: **منهجية البحث في العلوم الإنسانية**،لبنان،الأهلية للنشر والتوزيع،2006. ص 55

[2] نبيل حميدشة،**المقابلة**، مجلة العلوم الإنسانية والاجتماعية، العدد (8) يونيو 2012م، ص 99.

[3] رجاء وحيد دويدري، **البحث العلمي ، أساسياته النظرية، وممارسته العملية**، دار الفكر، ط1، 1421هـ، ص 322.

[4] نفس المرجع، ص323.

[5] فوزي غرايبة، وآخرون، **أساليب البحث العلمي في العلوم الاجتماعية والإنسانية**، الجامعة الأردنية، 1977م، ص 43.

و يعني ذلك ألا تكون المحادثة للتسلية أو لتحقيق أغراض شخصية بين المتقابلين. و خلال هذه المناقشات و المحادثات يكتب الباحث ملاحظاته عن الاشخاص موضوع الدراسة و يتوقف نجاح المقابلة على مستوى التخطيط لها ، و الأسئلة المناسبة التي تتفق و أحداث البحث ، وعلى الكيفية التي تتبع لتسجيل المعلومات و البيانات التي تسفر عنها هذه المقابلة من جهة أخرى ،و يجمع الباحث مع المبحوثين المعلومات عن طريق أسئلة يلقيها السائل لمعرفة رأي المجيب في موضوع معين بالذات ، أو الكشف عن اتجاهاتهم الفكرية ، أو معتقداتهم الدينية أو التعرف على النفس البشرية باستعراض ظروف تنشأة المبحوث اجتماعيا ، و الكشف عن دوافعه و مشاعره ، و اتجاهاته و عقائده و قيمه ، و آماله ، رغباته مما يصعب الحصول عليه عن طريق وسائل جمع البيانات الأخرى. [1].

و يبدأ الباحث بأن يوجه أسئلة عامة ، ثم يركز تدريجيا على محور الاهتمام فيضيق من نطاق الأسئلة حتى يتمكن من الحصول على المعلومات النوعية و الخاصة رويدا رويداً . أو من الأهمية بما كان أن يحاول الباحث الحصول على المعلومات بطريقة تتميز بالتسلسل الزمني . و يتم ذلك بمطالبة المبحوث بأن يستعرض ماضي حياته مبتدئا بالماضي و منتهيا بالحاضر أو العكس ، و يمكن للباحث كذلك أن يحصل علة المعلومات من المصادر الثانوية كالمخبرين الذين لديهم معرفة كاملة بتغير الظروف الاجتماعية أو الذين على اتصال وثيق بالافراد و الجماعات ، مما يمكن من تحليل الحقائق.[2]

تم الاستعانة بالمقابلة في جمع معلومات وبيانات البحث، إذ تم استعمال جملة من الاسئلبة بصفتها أداة لجمع المعلومات من عينة البحث وهي أداة رئيسية وتم تحكيمه من طرف الاساتذ المشرف طريف عطاء الله وجرى تقسيم المقابلة الى 07 اسئلة حول عمل الامن الوطني في اطار مكافحة الجرمة الالكترونية .

تمت المقابلة بمديرة الامن بولاية الاغواط مع المكلف بالاعلام في فرع مكافحة الجريمة الالكترونية عن طريق السؤال والجواب مباشرة .

---

[1] صبحي عبد اللطيف المعروف، **أساليب الإرشاد النفسي والتوجيه التربوي، المقابلة الإرشادية، الملاحظة، السجل، والاختبارات والمقاييس**، دار القادسية، بغداد، ط1، 1986م، ص10

[2] ابراهيم العسل ، **أسس النظرية و الاساليب التطبيقية في علم الاجتماع**، بيروت :1997. ص113

9. مجتمع الدراسة

يعرفه " Grawitz " على انه (مجموعة منتهية أو غير منتهية من العناصر المحددة مسبقا والتي ترتكز عليها الملاحظات[1]

يشير معنى عينة الدراسة إلى "تلك العينة التي تتوزع فيها خصائص المجتمع بنفس النسب الواردة في المجتمع"

تمثل المجتمع الأصلي وتحقق أغراض البحث وتغني الباحث عن مشقات دراسة المجتمع الأصلي، وتعرف العينة بأنها جزء ممثل لمجتمع البحث الأصلي . [2]

وقد اعتمدنا في دراستنا على العينة القصدية وهي اختيار عدد من الأفراد نظرا لأنهم يوفون بغرض الدراسة التي يرغب الباحث في القيام بها ، وهنا لابد من الإشارة إلى انه يجب أن تتمتع هذه العينة بشيء مقبول من الموضوعية في الأقوال والآراء والثقة فيها.

كان مجتمع الدراسة المكلف بالاعلام من عناصر الامن الوطني بمدينة الاغواط

10. حدود الدراسة

الحدود الزمانية للدراسة: بدات الدراسة والشروع في البحث منذ ان تم قبول الموضوع من طرف اللجنة العلمية وبعد اتمام تحديد الخطوط العريضة للدراسة بمساعدة الاستاذ المشرف منذ شهر جويلية لسنة 2019 الى غاية البداية الفعلية وذلك بشهر اوت 2019.

الحد الموضوعي: الجريمة الالكترونية والاجهزة الامنية

11. ضبط المفاهيم والمصطلحات

أ. الدور

التعريف اللغوي:يشير الدور لغة إلى الاضطلاع بمهمة [3]

التعريف الاصطلاحي :ولتوضيح معنى الدور لابد من التعرض أولا لمعنى المركز، وهو الوضع الذي يشغله الفرد في مجتمع ما بحكم سنه أو جنسه أو ميلاده أو حالته الاجتماعية أو وظيفته أو تحصيله .[4]

---

[1] موريس انجرس : **منهجية البحث العلمي، ترجمة بوزيد صحراوي وآخرون**، دار القصبة للنشر، الجزائر،2004، ص298.

[2] حمدان محمد زياد، **البحث العلمي كنظام** . سلسلة التربية الحديثة. دار التربية الحديثة .عمان – الأردن. 1989 ،ص 304

[3] المنجد الأبجدي– دار المشرق–بيروت–ط5 –1987–ص451

[4] سلمى محمود جمعة، **طريقة العمل مع الجماعات**، المكتبة الجامعية ، الإسكندرية ،2000–، ص37

وقد حاول البعض أن يخلط بين الدور والمركز من حيث اعتبارهما شيئا واحدا ، وهذا غير صحيح ، رغم أنهما مترابطان ، حيث يرى "لينتون " أن الدور يمثل الجانب الدينامي للمركز ، وعندما يضع الفرد عناصر المركز من حقوق وواجبات موضع التنفيذ ، فإنه حينئذ يمارس دورا ، فالفرد يمارس دورا ولا يشغل دورا بل يشغل مركزا اجتماعيا . [1]

التعريف الاجرائي

الدور هو نمط من الدوافع والأهداف والمعتقدات والقيم والاتجاهات والسلوك التي يتوقع أعضاء الجماعة أن يروه فيمن يشغل وظيفة ما أو يحتل وضعا اجتماعيا معينا والدور الذي يصف السلوك المتوقع من شخص في موقف ما.

والدور بناء على ذلك تتابع نمطي لمعارف واتجاهات ومهارات مكتسبة يقوم به فرد من الأفراد في موقف من المواقف وعادة ما يرتبط دور الفرد بادوار الأفراد لآخرين

والدور هو مجموعة من الأنشطة المرتبطة والأطر السلوكية التي تحقق ما هو متوقع في مواقف معينة ، ويترتب على الأدوار إمكانية التنبؤ بسلوك الفرد في المواقف المختلفة وفي الإدارة تتحدد الأدوار الرسمية للعاملين من خلال أسماء وظائفهم أو توصيفها وترتبط الأدوار أيضا بتوقعات الرؤساء والمرؤوسين وغيرهم . وهذه التوقعات يمكن أن تكون جزء من الوسط أو البيئة المحيطة بجو العمل الذي يعمل فيه رجل الإدارة المرتبط بدوره والمسئول عن هذا التشعب هو المصادر المختلفة للتوقعات والمتطلبات التي تفرضها البيئة والظروف المحيطة والتنظيمات الداخلية وقد يترتب على تعدد هذه التوقعات والمطالب تضارب بعضها مع بعض ومن ثم يواجه رجل الإدارة التوفيق بينها في ممارسته لوظيفته

وانطلاقا من ذلك نقول أن لمدير المدرسة دورا تربويا وإداريا وفنيا خلافا (لأدواره كرب أسرة وعضو في جماعات) داخل مدرسته يتحدد بأنه نمط من السلوكيات الذي يتوقعه أعضاء مهنة التعليم والبيئة والمجتمع ممن يشغل هذه الوظيفة.

ب.الاجهزة الأمنية :

تحتل المؤسسات التي تعني بالأمن في عصرنا أهمية خاصة، وقد تزايدت أهميتها وتطورت تنظيماتها، وتنوعت وظائفها عبر التاريخ، وقبل أن تعرف هذه الأجهزة باسم الشرطة والأمن

[1] محمد بهجت جاد الله كشك، **تنظيم المجتمع من المساعدة إلى الدفاع** ، المكتب العلمي للكمبيوتر والنشر والتوزيع، الإسكندريةJ 1996، ص 36

كان لها أسماء متعددة تدور وظائفها حول ما يعرف بوظائف الحرس هذه الوظائف التي عرفت في الحضارات القديمة.

وقد كان هناك خلافا لغويا حول أصول هذه الكلمة " شرطة" مثلا "ابن منظور" يرى أنها مشتقة من "الشرط"، وهي علامة يتميز بها رجل الشرطة، وجمعها شرط سموا بذلك لأنهم أعدوا لذلك وأعلموا أنفسهم بعلامات[1]، وقيل":هم أول كتيبة تشهد الحرب وتتهيأ للموت ومن الباحثين من أنكر أن تكون تسمية الشرطة بهذا الاسم من الفعل أعلم كما ظن اللغويين، فيفترض أنها جاءت من أصول أخرى وهي كلمة شرطة معربة من كلمة رومانية لاتينية وهي:

أ.الشرطة لغة واصطلاحًا:تضاربت الآراء حول مصطلح (الشرطة) لغة واصطلاحًا، بين الأصالة العربية، وتشكيك من تأثروا بالفكر الاستشراقي على القول بأن الكلمة أصلها يوناني، وكان المستشرق الألماني)شاخت(هو من قال على أنها مشتقة من كلمة (cohort)، في تعليقه على كتاب (Tyan)، المعني بالمؤسسات القانونية الإسلامية، في معرض رده على المعجميين العرب، في تأصيلهم لعروبة المصطلح، وشاخت هذا لا يقدم دليلًا على صحة ما قاله، فاللغة العربية التي وسعت كتاب الله؛ على أن يكون من هذه اللغة، فهل عجزت أن يكون فيها مثل هذه الكلمة.

التعريف الاجرائي

الاجهزة الامنية تقوم بمهمة حفظ الأمن والنظام العام بالمدن الجزائرية الكبرى والمناطق الحضرية بالإضافة إلى ضمان حماية الاشخاص والممتلكات وكذا التحقيق في الجرائم والقبض على الجناة، كما تؤدي مهام الشرطة الروتينية الأخرى كمراقبة حركة المرور، يقع جهاز الشرطة الجزائرية تحت قيادة المديرية العامة للأمن الوطني.

ج. الجريمة الالكترونية

التعريف اللغوي للجريمة الالكترونية:لم يتفق فقهاء القانون الجنائي في القوانين المقارنة على الوصف القانوني السليم أو التسمية الدقيقة لهذا المصطلح، أي الجريمة الإلكترونية لوجود مجموعة من المفاهيم المتقاربة والمشتقة من الإجرام الالكتروني والغش المعلوماتي والانحراف الذي يقع بواسطة الجانب الآلي أو جرائم الانترنيت حيث تطرح إشكالية التشابه والاختلاف

[1] ابن منظور، **لسان العرب**، دار المعارف، الجزء الرابع.، ص 67

بين مصطلحي الجريمة الالكترونية و الجريمة المعلوماتية فهل الجريمة الالكترونية تحوي الجريمة المعلوماتية او العكس[1]

حيث ترى الدكتورة غنية باطلي في هذا الشأن: " ان استعمال مصطلح الجريمة الالكترونية من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية والغش المعلوماتي أو جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الانترنيت وبالتالي كان فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة، مما جعل المشرع يعزز الحماية الجنائية، فلا يستطيع المجرم أن يتحايل ويحقق مآربه عن طريق استغلال التقدم العلمي، وما قد يجلبه من إمكانيات لم تكن في ذهن المشرع وقت وضع النصوص"[2]

وتحليلا لهذا القول ،نرى أن مصطلح الجريمة الالكترونية أدق وأوسع من الجريمة المعلوماتية هذه الأخيرة التي يقصد بها الجرائم المرتكبة على الحاسوب أو الكمبيوتر أو جرائم الحاسوب وجرائم الإنترنيت، فالجريمة الالكترونية هي جريمة محلها المعالجة الآلية للمعطيات سواء على الكمبيوتر أو أية وسيلة الكترونية أخرى، وهذا ما أكدته اتفاقية بودابست أو الاتفاقية المتعلقة بالجريمة الإلكترونية والتي صادق عليها المجلس الأوروبي في بودابست –المجر في 23 نوفمبر 2001.[3]

التعريف الاصطلاحي للجريمة:عرفت الجريمة بصفة عامة على أنها "كل فعل غير مشروع صادر عن إرادة آثمة يقرر لها القانون عقوبة أو تدبير احترازيا" .بينما تعتمد الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الانترنيت على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم[4]

---

[1] محمد علي العريان: **الجرائم المعلوماتية**. دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص: 43.

[2] غنية باطلي: **الجريمة الالكترونية دراسة مقارنة** ، الدار الجزائرية للنشر والتوزيع ، الجزائر، 2015 ,ص12-13

[3] غنية باطلي: المرجع نفسه ، ص: 24

[4] دردور نسيم: **الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن** ، رسالة لنيل شهادة الماجستير ، كلية الحقوق – جامعة منتوري قسنطينة- 2012 -2013، ص: 05.

وبالنسبة للجريمة الإلكترونية، فلقد اختلفت التعريفات الفقهية والقانونية بهذه الجريمة باختلاف وسائلها والنظم القانونية المتعلقة بها، حيث انقسم تعريف هذه الظاهرة الإجرامية إلى عدة اتجاهات تقوم على أسس مختلفة:

التعريف الاجرائي: تمثل الجريمة الالكترونية كل جريمة تحدث من طرف مجرمين عبر الوسائل التقنية الحديثة اما عبر مواقع التواصل الاجتماعي او عن طريق الاختراق والقرصنة في المنظومة والمساس بأمن المعطيات اما بالتزوير او الحذف او الإضافة .

12.الدراسات السابقة

لم تتوفر لدينا دراسات في مجال الاعلام والاتصال حول الجريمة الالكترونية ومعظم الدراسات كانت من دراسات قانونية .

أجرى الشمايله (2006) دراسة بهدف قياس الآثار الاجتماعية المترتبة على استخدام الانترنت لدى عينة من طلاب الجامعة الأردنية مكونة من (2355) من الذكور والإناث وأظهرت النتائج وجود تأثير سلبي منخفض لاستخدام الانترنت على العادات والتقاليد والمعتقدات الدينية، وان التأثير كان سلبيا بدرجة متوسطة في المجال النفسي والأخلاقي، وكان التأثير ايجابيا في المجال الثقافي والعلمي

وقد أجرى دى جارسيا (De Garcia et al.،2002) دراسة لاستكشاف المشكلات السلوكية المرتبطة باستخدام الانترنت وتكونت العينة من (1664) من الجنسين وقد أوضحت نتائج الدراسة وجود مشكلات مرتبطة باستخدام الانترنت مثل الحساس بالذنب إضاعة الوقت وارتفاع القلق وخلل في الوظائف الاجتماعية لعينة البحث

وفى دراسة رو (Rowe،2000) حول استخدام الانترنت كظاهرة اجتماعية على عينة مكونة من (4113) من الشباب من عمر 18سنة فما أكثر وقد أشارتا نتائج الدراسة إلى ان 55%من حجم العينة يستخدمون الانترنت وان 36%منهم كانوا يقضون 5ساعات وأكثر أسبوعيا على الانترنت وانخفض معدل التواصل مع الأسرة والأصدقاء وارتبط استخدام الانترنت بالإحباط والقلق والاكتئاب ونقص في الأنشطة الاجتماعية.

دراسة خضر (2009)، وعنوانها "الآثار النفسية والاجتماعية لاستخدام الشباب المصري لمواقع الشبكات الاجتماعية: دراسة على موقع الفيسبوك". وهدفت الدراسة إلى التعرف على دوافع استخدام الشباب المصري لموقع الفيسبوك، والكشف عن طبيعة العلاقات الاجتماعية والصداقات التي يكونها

الشباب المصري، كما هدفت أيضا إلى رصد وتحليل الآثار النفسية والاجتماعية (السلبية والايجابية) المترتبة على تعامل عينة الدراسة مع موقع الفيسبوك، وذلك من خلال عينة عمديه متاحة من مستخدمي الفيسبوك من طلاب الجامعات المصرية (الحكومية والأجنبية) مقدارها (136) مفردة موزعة بالتساوي بين جامعة القاهرة والجامعة البريطانية. وقد توصلت الدراسة إلى أن دافع التسلية والترفيه يأتي على رأس دوافع استخدام طلاب الجامعة لموقع الفيسبوك، وبنسبة مقدارها (69.9%) من إجمالي عينة المبحوثين، بينما جاء دافع خلق صداقات جديدة، ودافع التواصل مع الآخرين وتطوير علاقات اجتماعية معهم في المرتبتين الثانية والثالثة، وبنسبة (41.2%) و(37.5%) لكل منهما على التوالي، كما أوضحت الدراسة أن تقديم المبحوثين لأنفسهم كما هم بصدق وبدون أي تلوين أو خداع للآخرين، كان لها النصيب الأكبر وبنسبة (82.4%)، مقابل (19.9%) لتقديم المبحوثين أنفسهم للآخرين باستخدام اسم مستعار. كما توصلت الدراسة إلى أن العبارات التي حظيت بأعلى أهمية نسبية لدى طلاب جامعة القاهرة والجامعة البريطانية بمقياس لبكرت الثلاثي تمثلت في العبارات التالية: "التعامل مع الموقع جعلني أشعر بالانفتاح على أخبار الآخرين بوزن نسبي (90.44)، يليها بروز عبارة " أتخلص من الشعور بالوحدة عندما أجلس على موقع الفيسبوك بوزن نسبي (83.09%)، ثم ظهور عبارة "لقد قمت بتطوير علاقات اجتماعية عديدة من خلال التعامل مع الموقع" في المركز الثالث بوزن نسبي (75.25%)، ... مما يعني غلبة الطابع الإيجابي على الآثار الاجتماعية المترتبة على استخدام طلبة الجامعات لموقع الفيسبوك.

الاطار النظري

الفصل الثاني

الجريمة الالكترونية ومواقع التواصل الاجتماعي

المبحث الأول: مفهوم الجريمة الالكترونية

المبحث الثاني: مواقع التواصل الاجتماعي كأحد أنماط الاعلام الالكتروني

الفصل الثاني: الجريمة الالكترونية ومواقع التواصل الاجتماعي

تمهيد

تميز القرن العشرين باختراعات هائلة على المستوى التقني بفضل ظهور وانتشار استعمال الكمبيوتر واستحداث شبكات المعلومات، حتى أصبح يعرف بقرن المعلوماتية ، حيث أصبحت المعلوماتية وأدواتها وسائل ضرورية في العمليات البنكية أو سجلات الشركات وحتى علاقات الدولة مع الأفراد، لقد ترك الحاسب الآلي بصمات واضحة في تطوير عدد كبير من الأنشطة اليومية سواء من حيث المضمون أو الشكل أو الزمن أو المسافة.".

ولم يظهر أي نص قانوني في مجال جرائم المعلوماتية أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات الاسنة 1988 في فرنسا بموجب القانون رقم 88-19[1].

المبحث الاول :مفهوم الجريمة الالكترونية

المطلب الأول: ماهية الجريمة الالكترونية

المطلب الثاني: أركان الجريمة الإلكترونية.

المبحث الثاني: مواقع التواصل الاجتماعي كأحد انماط الاعلام الالكتروني

المطلب الأول: نشأة وتطور مواقع التواصل الاجتماعي

المطلب الثاني:الجريمة الالكترونية عبر مواقع التواصل الاجتماعي

[1] الصادر في 05 جانفي 1988 والمتعلق بالغش المعلوماتي، ولقد عدل هذا القانون بموجب القانون رقم 2004-575 الصادر في 21 جوان 2004، المتعلق بالثقة في الاقتصاد المعلوماتي والمعدل والمتمم في 11جويلية 2011

المبحث الاول :مفهوم الجريمة الاكترونية

ان أكثر مسائل ظاهرة جرائم الكمبيوتر والانترنت اثارة للجدل ، الى جانب تعريفها وتحديد موضوعها او مناط الحماية ومحله ، مسألة تحديد قائمة جرائم الكمبيوتر وتحديد أنماط السلوك الاجرامي والأفعال المكونة له ، وتبين القوام القانوني لهذه الجرائم ، هذه المسألة أفرزت خلافا وتباينا موضوعيا لدى الفقه الجنائي في مختلف النظم القانونية ، اللاتينية والجرمانيه والانجلوسكونية ، حول مدى انطباق نصوص القوانين الجنائية التقليدية على هذه الجرائم – على الاقل في السنوات الاولى لبروز الظاهرة وقبل ان تتجه الاراء للحسم لجهة عدم قابلية النصوص القائمة او عجزها وعدم كفايتها للانطباق على هذه الانماط الجديدة من الجرائم .

المطلب الأول: ماهية الجريمة الالكترونية:

من أجل التعرف على ماهية الجريمة الإلكترونية لابد من البداية من تعريفها وبيان خصائصها وأركانها وهذا ما سنبحثه في الفروع التالية:

الفرع الأول: التعريف اللغوي والاصطلاحي للجريمة الالكترونية.

الفرع الثاني: خصائص الجريمة الالكترونية.

الفرع الأول: التعريف اللغوي والاصطلاحي للجريمة الالكترونية.

أدت الحداثة التي تتميز بها الجريمة الالكترونية واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها، وعدم الاتفاق هذا انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، وذلك خشية حصرها في مجال ضيق[1]

وترتيبا على ذلك ،اختلفت مصطلحات الجريمة الالكترونية وظهر مصطلح الجريمة المعلوماتية وجرائم الانترنيت والجرائم المرتكبة عبر الإنترنيت فما المقصود بهذه المصطلحات؟ وما هو المصطلح الأصلح أو الأدق لهذه الجريمة.؟

كما اختلفت وجهات نظر الفقه والقضاء والتشريع حول ماهية او تعريف الجريمة الالكترونية الاصطلاحي. فتعددت تعريفاتها ومفاهيمها .

[1] القانون رقم 09- 04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (جريدة رسمية رقم 47 الصادرة في 06 أوت 2009)

لذا فسنبحث في هذا الفرع التعريف اللغوي والتعريف الاصطلاحي للجريمة الالكترونية فيما يلي:

أولا: التعريف اللغوي للجريمة الالكترونية:

لم يتفق فقهاء القانون الجنائي في القوانين المقارنة على الوصف القانوني السليم أو التسمية الدقيقة لهذا المصطلح، أي الجريمة الإلكترونية لوجود مجموعة من المفاهيم المتقاربة والمشتقة من الإجرام الالكتروني والغش المعلوماتي والانحراف الذي يقع بواسطة الجانب الآلي أو جرائم الانترنيت حيث تطرح إشكالية التشابه والاختلاف بين مصطلحي الجريمة الالكترونية و الجريمة المعلوماتية فهل الجريمة الالكترونية تحوي الجريمة المعلوماتية او العكس[1]

حيث ترى الدكتورة غنية باطلي في هذا الشأن: " ان استعمال مصطلح الجريمة الالكترونية من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية والغش المعلوماتي أو جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الانترنيت وبالتالي كان فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة، مما جعل المشرع يعزز الحماية الجنائية، فلا يستطيع المجرم أن يتحايل ويحقق مآربه عن طريق استغلال التقدم العلمي، وما قد يجلبه من إمكانيات لم تكن في ذهن المشرع وقت وضع النصوص"[2]

وتحليلا لهذا القول ،نرى أن مصطلح الجريمة الالكترونية أدق وأوسع من الجريمة المعلوماتية هذه الأخيرة التي يقصد بها الجرائم المرتكبة على الحاسوب أو الكمبيوتر أو جرائم الحاسوب وجرائم الإنترنيت، فالجريمة الالكترونية هي جريمة محلها المعالجة الآلية للمعطيات سواء على الكمبيوتر أو أية وسيلة الكترونية أخرى، وهذا ما أكدته اتفاقية بودابست أو الاتفاقية المتعلقة بالجريمة الإلكترونية والتي صادق عليها المجلس الأوروبي في بودابست –المجر في 23 نوفمبر 2001 .[3]

ثانيا: التعريف الاصطلاحي للجريمة:

---

[1] محمد علي العريان: **الجرائم المعلوماتية** ،دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص: 43

[2] نية باطلي: **الجريمة الالكترونية دراسة مقارنة** – الدار الجزائرية للنشر والتوزيع – الجزائر، 2015 ،ص12-13

[3] غنية باطلي: المرجع نفسه ، ص: 24

عرفت الجريمة بصفة عامة على أنها "كل فعل غير مشروع صادر عن إرادة آثمة يقرر لها القانون عقوبة أو تدبير احترازيا" .بينما تعتمد الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الانترنيت على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم[1]

وبالنسبة للجريمة الإلكترونية، فلقد اختلفت التعريفات الفقهية والقانونية بهذه الجريمة باختلاف وسائلها والنظم القانونية المتعلقة بها، حيث انقسم تعريف هذه الظاهرة الإجرامية إلى عدة اتجاهات تقوم على أسس مختلفة:

1- على أساس وسيلة ارتكاب الجريمة: تعتمد هذه التعريفات على وسيلة ارتكاب الجريمة، فطالما كان الحاسوب أو إحدى وسائل التقنية من وسائل ارتكابها حتى تعتبر من جرائم الانترنيت.

حيث يعرف الفقيه " :Mawreالجريمة الالكترونية بأنها الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه"

بينما يعرفها بعض من الفقه أنها "نشاط إجرامي تستخدم فيه التقنية الالكترونية – الحاسب الآلي وشبكة الانترنيت- بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف.[2]

وترتيبا على هذه التعاريف، تعرف هذه الجريمة الالكترونية على أنها الفعل الغير المشروع المرتكب بواسطة الكمبيوتر أو الانترنيت أو أية وسيلة الكترونية، وقد لقي هذا التعريف عدة انتقادات أهمها اتسامه بالعمومية والاتساع لأنه يدخل كل سلوك ضار بالمجتمع يستخدم فيه الجانب الآلي في قائمة الجرائم الالكترونية.

2- على أساس موضوع الجريمة: يعتمد هذا الاتجاه في تعريفه للجريمة الالكترونية، على أساس أن موضوع الجريمة هو المعالجة الآلية للبيانات، فكل تعريف أو تعديل أو نقل أو نسخ غير مشروع لها يعد جريمة الكترونية ،وعليه فقد عرفت الجريمة الالكترونية وفقا لهذا

---

[1] دردور نسيم: **الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن** –رسالة لنيل شهادة الماجستير – كلية الحقوق – جامعة منتوري قسنطينة- 2012 –2013، ص: 05

[2] يوسف صغير: **الجرائم المرتكبة عبر الانترنيت**، رسالة لنيل شهادة الماجستير، كلية الحقوق، جامعة مولود معمري، تيزي وزو الجزائر، ص: 09

الاتجاه بأنها: "الجريمة المرتكبة عبر الانترنيت هي الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر[1]

كما عرفت الدكتورة هدى قشقوش الجريمة الالكترونية بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[2]

ويلاحظ على هذه التعاريف، تركيزها على محل الجريمة أو موضوعها دون الوسيلة المعتمدة فيها، وهذا أهم انتقاد يوجه لهذه التعاريف، لأن أهم ما يميز الجريمة الالكترونية أنها تتم في وسط افتراضي وتمس بمعطيات الحاسب الآلي سواء أكانت مادية أو معنوية.

ثالثا: على أساس توفر المعرفة بتقنيات المعلومات:

تعتمد هذه التعاريف على أساس توافر المعرفة الفنية بتقنية المعلومات لدى الجاني في الجريمة الالكترونية، حيث عرفها الاستاذ David Thomson بأنها "أية جريمة يكون متطلبا لاقترافها أن يتوافر لدى فاعلها معرفة بتقنية الحاسب"[3]

كما عرفت الجرائم الالكترونية بأنها: "الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني"[4]

ولقد اعتمد هذا الاتجاه في تعريفه للجريمة الالكترونية على معيار شخصي وهو مدى معرفة الجاني بتقنية المعلومات والإلمام بها، وحيث أن قصور هذه التعاريف واضحة لأن شخصية الجاني لا تكفي لوحدها لتعريف الجريمة الالكترونية حيث يمكن لشخص عادي غير مؤهل بتقنيات الحاسب الآلي ارتكاب جريمة الغش المعلوماتي أو السرقة المعلوماتية.

رابعا: على أساس الجمع بين عدة معايير:

---

[1] علي كحلوش : **جرائم الحاسوب و اساليب مواجهتها** ، مجلة الشرطة ،المديرية العامة للامن الوطني ، العدد 84، جويلية 2007. ص51

[2] يونس عرب : **جرائم الكمبيوتر و الانترنت** ،ورقة عمل مقدمة الى مؤتمر الامن العربي، المركز العربي للبحوث و الدراسات الجنائية، ابو ظبي 10- 12 فيفري 2002 . ص 08 .

[3] هدى قشقوش: **الحماية الجنائية للتجارة الالكترونية عبر الانترنيت**، دار النهضة العربية، القاهرة، ص: 12.

[4] 16هشام محمد فريد رستم: **الجرائم المعلوماتية**، مؤتمر القانون والكمبيوتر والانترنيت، منذ 1 – 5 ماي 2000 – جامعة الامارات العربية المتحدة، كلية الشريعة والقانون- المجلد الثاني، الطبعة الثالثة، 2004، ص: 407

ونطرا لعدم نجاعة التعاريف السابقة للجريمة الالكترونية، عمد أصحاب هذا الاتجاه إلى الجمع بين عدة معايير وعرفوا الجريمة عبر الانترنيت بأنها: "الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو تمثل إغراء بذلك بأنها، أو جريمة يكون الحاسب نفسه ضحيتها [1] وعرفت كذلك بأنها: كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[2]

وبالرغم من الانتقادات التي وجهت لهذا الاتجاه باعتباره جمع بين عدة معايير لتعريف جرائم الانترنيت أو الجرائم الالكترونية إلا أن هذا التعريف يعد التعريف الراجح والأنجع من الناحية العملية ،نظرا لتعدد صور الجرائم الإلكترونية وتطورها بتطور تقنية المعلومات.

خامسا: تعريف المشرع الجزائري للجريمة الالكترونية:

على خلاف المشرع الفرنسي الذي لم يعط تعريفا للجريمة الالكترونية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وعرفها بموجب المادة الثانية من القانون 09 – 04 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية."

ويلاحظ على هذا التعريف ما يلي:

أولا: أن المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكتروني، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

ثانيا: كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة الالكترونية، كونه أقر أن الجريمة الالكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري.

---

[1] يوسف صغير: المرجع السابق، ص: 11.

[2] هشام محمد فريد رستم، المرجع السابق، ص: 409

وترتيبا على كل هذه التعاريف الفقهية والتشريعية، يمكننا تعريف الجريمة الالكترونية بأنها "كل سلوك غير مشروع يمس بالنظام المعلوماتي المادي أو المعنوي " او كل سلوك غير مشروع يقع على النظام المعلوماتي او بواسطته وبمس بالأشخاص او الاموال او امن الدولة أي أن الجريمة الالكترونية على سبيل الجرائم التقليدية تعرف من خلال أركانها أي توفر القصد الجنائي لارتكاب هذه الجريمة والركن المادي للجريمة وركنها القانوني.

الفرع الثاني: خصائص الجريمة الالكترونية:

تتميز الجريمة الالكترونية بطبيعة خاصة تميزها عن الجريمة التقليدية ، ولذا أضحت هذه الخاصية بهذا النوع من الجرائم عدة سمات وحقائق سواء تتعلق الأمر بمرتكبيها أو ما يسمى بالمجرم المعلوماتي أو بالنسبة لحدودها باعتبارها جريمة ذات بعد عالمي.

وعليه سنحاول البحث في خصائص الجريمة فيما يلي:

أولا: الجريمة الالكترونية جريمة عالمية الحدود:

من أهم الخصائص التي تميز الجريمة الالكترونية أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الانترنيت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، وبسبب السرعة الهائلة في تنفيذها وحجم الأموال والأشخاص المستهدفة من خلالها.

ومن أهم القضايا التي أكدت هذه الخاصية، قضية عرفت باسم مرض نقص المناعة المكتسبة إيدز، وتتلخص وقائعها عام 1989، حيث قام أحد الأشخاص وهو "جوزيف بيب" بنسخ أحد البرامج بهدف إعطاء بعض النصائح الخاصة بمرض الإيدز، لكن في الحقيقة يحتوي هذا البرنامج على فيروس يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل فيقوم الفاعل أو الجاني بطلب مبلغ مالي للحصول على عنوان إلكتروني مضاد للفيروس، وفي الثالث من فبراير تم إلقاء القبض على الجاني في أوهايو بالولايات المتحدة الأمريكية وطلبت المملكة المتحدة تسليم الجاني لإرسال البرنامج على أراضيها، وبالفعل تمت محاكمته أمام القضاء الانكليزي، إلا أن إجراءات محاكمته لم تستمر بسبب حالته العقلية"[1]

[1] سوير سفيان: **الجرائم المعلوماتية**، رسالة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010، ص: 12.

وتثير خاصة عالمية الحدود للجريمة الالكترونية عدة آثار قانونية أهمها القانون الواجب التطبيق عليها، والقضاء المختص بها، فهل هو قانون الدولة التي وقع فيها النشاط الإجرامي ،أم الدولة التي يقيم فيها الجاني أو الدولة التي أضرت بمصالحها هذا التلاعب.

لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إبرام الاتفاقيات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم.

ولقد قام المشرع الجزائري بموجب القانون 09 – 04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بسن أحكام خاصة بالتعاون والمساعدة القضائية والدولية المتبادلة عن طريق المواد 16 و17 و18 من هذا القانون.[1]

ثانيا: مرتكبو الجريمة الالكترونية ذوو صفات خاصة:

يتميز المجرم المعلوماتي عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامي النمطي بعدة خصائص عددها الأستاذ Parker فيما يلي:[2]

-1 المجرم المعلوماتي مجرم متخصص ومحترف في تنفيذ جريمته الالكترونية، حيث ان ارتكابها يتطلب التغلب على تقنيات حماية أنظمة الكمبيوتر.

-2 خلافا على المجرم العادي المجرم المعلوماتي لا يلجأ إلى العنف في تنفيذ جرائمه، فهو مجرم ذكي يتمتع بالمهارة والمعرفة وبدرجة عالية من الثقافة.

-3 يوجد عدة أنواع من المجرمين المعلوماتيين، فهناك:

-1 طائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون إحداث أي ضرر ويسمونهم .Pranskers

[1] القانون 09 -04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها (الجريدة الرسمية رقم 47 الصادرة في 6 أوت 2009.(

[2] عبد العال الديربي: **الجريمة المعلوماتية – تعريفها – أسبابها وخصائصها**، تم الاطلاع عليه بتاريخ 2019/08/10 ،منشور على الموقع التالي www.acconline.com/article.detail.aspr?id:7509

-2 طائفة الأشخاص الذين يستهدفون الدخول إلى أنظمة الحاسبات الآلية الغير المصرح لهم بهدف الفضول أو اكتساب الخبرة أو لمجرد القدرة على اختراق هذه الأنظمة ويسمون Hackers.

-3 طائفة الأشخاص الذين يستهدفون الحاق خسائر بالمجني عليهم ،دون ان يكون الحصول على مكاسب مالية ضمن هذه الاهداف،ويندرجون تحت طائفة مخترعي فيروسات الحاسبات الآلية وموزعيها ويسمون .Malicieuses hackers

-4 طائفة الأشخاص الذين يهدفون إلى إلحاق الأذى بالمجني عليهم، ويكون الباعث إيجاد حلول لمشاكل مادية تواجه الجاني لا يستطيع حلها بالطرق العادية ويسمون بـ : Personnel problème solvers .

-5 طائفة الأشخاص الذين يهدفون إلى تحقيق ربح مادي بطريق غير مشروع ويسمون بـ : Creen criminals)

ثالثا: الجريمة الالكترونية جريمة صعبة الإثبات:

من أهم خصائص الجريمة الالكترونية أنها صعبة الإثبات لأسباب ترجع إلى الجاني أو إلى المجني عليه، وإلى وسيلة تنفيذها، حيث تتم هذه الجريمة بشكل منظم من إقليم دولة واحدة باستخدام الانترنيت، أضف إلى أن الجاني المجرم المعلوماتي كما أسلفنا الذكر مجرم محترف ذكي مثقف لا يترك آثارا جانبية خارجية للجريمة مما يصعب إثباتها، كما أن المجني عليهم وهم غالبا مؤسسات عامة أو خاصة يحجمون عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة، فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية.[1]

المطلب الثاني: أركان الجريمة الإلكترونية.

تتمثل أركان الجريمة الإلكترونية مثل الجريمة العادية في الركن الشرعي و المادي والمعنوي:

1- الركن الشرعي : معناه إعتراف المشرع والنص على تجريم الفعل المرتكب،"لاجريمة ولا عقوبة إلا بنص"... **بالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في**

[1] غنية باطلي: المرجع السابق، ص: 28 – 32.

القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات.[1]

2- الركن 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 الإلكترونية)[2]

3-الركن المعنوي: يتكون الركن المعنوي للجريمة الإلكترونية من عنصريها أي العلم و ارادة

- 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 إرنكاب 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 ؟

الأصل إن الفاعل في الجريمة الالكترونية يوجه سلوكه ألإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام.

---

[1] القانون رقم04-15 المؤرخ في10 نوفمبر2004، المادة394 مكرر.

[2] محمود نجيب حسني، **شرح قانون العقوبات –** القسم الخاص، بدون رقم الطبعة، دار النهضة العربية، القاهرة 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[1]

4- مرتكبو الجريمة الإلكترونية:أنواع الجناة في جرائم الانترنت كما يُطلق عليهم إسم القراصنة،و يمكن حصر هؤلاء في ثلاثة فئات :

أ- **الهاكرز:** ويُطلق هذا الاسم على القراصنة الذين يتّخذون من الجرائم الإلكترونية، 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[2]

ويمكن رد **دوافع إرتكاب الجريمة الإلكترونية** إلى دوافع مادية، سعياً لإشباع الرغبة بتحقيق الثراء أو دوافع شخصية، التعلّم، 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).[3]

---

[1] نفس المرجع. ص 13.

[2] عبد الفتاح مراد ، **شرح جرائم الكمبيوتر و الانترنت** ، دار الكتب والوثائق المصرية ، 2005 ،65.

[3] نفسه،ص،68.

المبحث الثاني: مواقع التواصل الاجتماعي كأحد انماط الاعلام الالكتروني

إن ظهور مواقع التواصل الاجتماعي وفرت "فتحاً تاريخياً" نقل الإعلام إلى آفاق غير مسبوقة وأعطى مستخدميه فرصاً كبرى للتأثير والانتقال عبر الحدود بلا رقابة إلا بشكل نسبي ومحدود. وابرز حراك الشباب العربي الذي تمثل بالثورات التي شهدتها بعض الدول العربية قدرة هذا النوع من الإعلام على التأثير في تغيير ملامح المجتمعات، وإعطاء قيمة مضافة في الحياة السياسية، وانذار لمنافسة الإعلام التقليدي.[1]

استخدم الشباب في بداية الأمر مواقع التواصل الإجتماعي للدردشة ولتفريغ الشحن العاطفية، ولكن يبدو أن موجة من النضج سرت، وأصبح الشباب يتبادلون وجهات النظر، من أجل المطالبة بتحسين إيقاع الحياة السياسية والإجتماعية والإقتصادية ومن هنا تشكلت حركات الرفض الشبابية التي إنتظمت في تونس مروراً بمصر واليمن وليبيا والبحرين والأردن. وتخطت تلك الأفكار الرافضة للسياسات بسهولة عبر مواقع التواصل الإجتماعي الوطن العربي.

واستخدم كبار الشخصيات هذه الوسائل الجديدة واقتطعوا وقتاً معيناً من الأنشطة الأخرى لصالحها، لإيمانهم بأنها البوابة الحقيقة والجادة للتواصل وسماع الناس والمواطنين، وبهذا سيتغير المشهد الإعلامي قريباً بشكل واضح للعيان في عالمنا العربي.

المطلب الأول: نشأة وتطور مواقع التواصل الاجتماعي

الفرع الأول : يمكننا القول بان نشات مواقع التواصل الاجتماعي مرت بمجموعة من المراحل والتي يمكن سردها كما يلي:

المطلب الأول: مراحل نشاة وتطور مواقع التواصل الاجتماعي

المرحلة الأولى:بدأت مجموعة من المواقع الاجتماعية في الظهور في أواخر التسعينات مثل (كلاس ميتس) عام 1995 للربط بين زملاء الدراسة، و موقع سكس (دجريزس) عام 1997 حيث ركز الموقع على الروابط المباشرة بين الأشخاص، و كانت تقوم فكرته أساسا على فكرة بسيطة يطلق عليها –الدرجات الست للانفصال– ، وظهرت في تلك المواقع الملفات الشخصية للمستخدمين و خدمة إرسال الرسائل الخاصة لمجموعة من الأصدقاء، و ظهر أيضا عدة مواقع أخرى مثل "لايف جورنال" و موقع "كايوورلد" الذي أنشئ في كوريا

[1] أبو أصبع صالح خليل :**الاتصال والإعلام في المجتمعات المعاصرة**، ط 2 ، دار الآرام، الأردن، 2003 م، ص520

سنة 1999، و كان ابرز ما ركزت عليه مواقع التواصل الاجتماعي في بدايتها خدمة الرسائل القصيرة و الخاصة بالأصدقاء.[1]وهذا ما عرف بالمرحلة الأولى .

المرحلة الثانية : تشهد المرحلة الثانية من تطور المواقع الاجتماعية على الإقبال المتزايد من قبل المستخدمين لمواقع المواقع العالمية، ويتناسب ذلك مع تزايد مستخدمي الانترنيت على مستوى العالم.

حيث ظهرت بعد المحاولات الأخرى إلا أن الميلاد الفعلي للمواقع الاجتماعية كما نعرفها اليوم كان مع بداية عام 2002، حيث ظهر موقع "فرندر " الذي حقق نجاحا دفع "غوغل" إلى محاولة شرائه سنة 2003، لكن لم يتم التوافق على شروط الاستحواذ، و في النصف الثاني من نفس العام ظهر في فرنسا موقع "سكا يروك" تحقيق « skyrock » كمنصة للتدوين ثم تحول بشكل كامل إلى شبكة اجتماعية سنة 2007، و قد استطاع موقع "سكا ي روك " تحقيق انتشار واسع ليصل في جانفي 2008 إلى المركز السابع في ترتيب المواقع الاجتماعية وفقا لعدد المشتركين.

و مع بداية 2005 ظهر موقع "ماي سبايس " الأمريكي الشهير الذي تفوق على "غوغل" في عدد مشاهدات صفحاته، و يعتبر موقع "ماي سبايس" من أوائل المواقع الاجتماعية و أكبرها على مستوى العالم و معه منافسه الشهير "فيسبوك facebook " و الذي كان قد بدأ في الانتشار المتوازي مع "ماي سبايس" ، حتى قام "فيسبوك" في 2007 بإتاحة تكوين تطبيقات للمطورين، وهذا أدى إلى زيادة إعداد مستخدمي "فيسبوك" بشكل كبير، وعلى مستوى العالم، و نجح بالتفوق على منافسه اللذوذ "ماي سبايس " عام 2008، أيضا ظهرت عدة مواقع أخرى "twitter " "youtube"، لتستمر ظاهرة مواقع المواقع الاجتماعية في التنوع و التطور.

[1] عادل امينة ،هبة خليفة: **الشبكات الاجتماعية و تاثيرها على الاخصائي و المكتبة**، دراسة شاملة للتواجد و الاستخدام ، تم الاطلاع عليه بتاريخ:2019/08/12 عبر الموقع

httlp://.eleagypt.com/downloads/2009/amina heba.doc..

الفرع الثاني: تعريف مواقع التواصل الاجتماعي وخصائصها

مفهوم "مواقع التواصل الاجتماعي" مثير للجدل، نظرا لتداخل الآراء والاتجاهات في دراسته. عكَس هذا المفهوم، التطور التقني الذي طرأ على استخدام التكنولوجيا، وأُطلق على كل ما يمكن استخدامه من قبل الأفراد والجماعات على الشبكة العنكبوتية العملاقة.

الإعلام الاجتماعي: "وهو المحتوى الإعلامي الذي يتميز بالطابع الشخصي، والمتناقَل بين طرفين أحدهما مرسِل والآخر مستقبِل، عبر وسيلة/ شبكة اجتماعية، مع حرية الرسالة للمرسِل، وحرية التجاوب معها للمستقبِل".

وتشير ايضاً إلى: "الطرق الجديدة في الاتصال في البيئة الرقمية بما يسمح للمجموعات الأصغر من الناس بإمكانية الإلتقاء والتجمع على الإنترنت وتبادل المنافع والمعلومات، وهي بيئة تسمح للإفراد والمجموعات بإسماع صوتهم وصوت مجتمعاتهم إلى العالم جمعا"[1].

ويعرف زاهر راضي مواقع التواصل الاجتماعي على أنها: "منظومة من الشبكات الإلكترونيّة التي تسمح للمشترك فيها بإنشاء موقع خاص به، و من ثم ربطه عن طريق نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم الإهتمامات والهوايات نفسها"[2]

وتضع كلية شريديان التكنولوجية Sheridan تعريفاً اجرائياً للإعلام الجديد بأنه: "انواع الاعلام الرقمي الذي يقدم في شكل رقمي وتفاعلي، ويعتمد على اندماج النص والصورة والفيديو والصوت، فضلا عن استخدام الكومبيوتر كأداة رئيسة له في عملية الانتاج والعرض، اما التفاعلية فهي تمثل الفارق الرئيس الذي يميزه وهي اهم سماته" ويمكن تقسيم مواقع التواصل الاجتماعي بالاعتماد على التعريفات السابقة الى الاقسام الآتية:

1- شبكة الانترنت Online وتطبيقاتها، مثل الفيس بوك، وتويتر، اليوتيوب، والمدونات، وشبكات الدردشة، والبريد الالكتروني... فهي بالنسبة للإعلام، تمثل المنظومة الرابعة تضاف للمنظومات الكلاسيكية الثلاث.

---

[1] فريال مهنا، **علوم الاتصال والمجتمعات الرقمية** ، دمشق سوريا ، ط01 ، دار الفكر2006 ص147

[2] زاهر راضي، "**استخدام شبكات التواصل الاجتماعي في العالم العربي**"، عمان، مجلة التربية، ع15 ، جامعة عمان الأهلية، 2003، ص23.

2- تطبيقات قائمة على الادوات المحمولة المختلفة ومنها اجهزة الهاتف الذكية والمساعدات الرقمية الشخصية وغيرها. وتُعدّ الاجهزة المحمولة منظومة خامسة في طور التشكل.

3- انواع قائمة على منصة الوسائل التقليدية مثل الراديو والتلفزيون "مواقع التواصل الاجتماعي للقنوات والاذاعات والبرامج" التي اضيفت اليها ميزات مثل التفاعلية والرقمية والاستجابة للطلب.[1]

ويمكن ان نخلص إلى أن مواقع التواصل الاجتماعي تشير إلى حالة من التنوع في الاشكال والتكنولوجيا والخصائص التي حملتها الوسائل المستحدثة عن التقليدية، لاسيما فيما يتعلق باعلاء حالات الفردية والتخصيص ، وتأتيان نتيجة لميزة رئيسة هي التفاعلية. فإذا ما كان الاعلام الجماهيري والاعلام واسع النطاق وهو بهذه الصفة اعلام القرن العشرين، فإن الاعلام الشخصي والفردي هو اعلام القرن الجديد. وما ينتج عن ذلك من تغيير انقلابي للنموذج الاتصالي الموروث بما يسمح للفرد العادي ايصال رسالته إلى من يريد في الوقت الذي يريد، وبطريقة واسعة الاتجاهات وليس من أعلى الى اسفل وفق النموذج الاتصالي التقليدي. فضلا عن تبني هذه الشبكات تطبيقات الواقع الافتراضي وتحقيقه لميزات الفردية والتخصيص وتجاوزه لمفهوم الدولة الوطنية والحدود الدولية.[2]

مداخل نظرية لفهم خصائص مواقع التواصل الاجتماعي

لا يعمل الإعلام في فراغ بل يستمد من السياقات الاقتصادية والسياسية والثقافية، سواء كانت محلية أو قومية أو إقليمية أو دولية. ولكي نفهم أهمية مواقع التواصل الاجتماعي "الإعلام البديل" يجب أن نضعها في النظريات السياسية والديمقراطية التي وفرت سنداً نظرياً وفكرياً لهويتها وممارستها، ويتطلب مراجعة بعض المقاربات على مستويات عدة، يلتزم بعضها الجوانب المتعلقة بالتطورات في تكنولوجيا الاتصال، وبعضها يعلق على الموضوع من جانب الدراسات الاجتماعية والسياسية وغيرها، بما يمثل مدخلا لفهم خصائص الاعلام الجديد:

فتشدد نماذج الديمقراطية القائمة على المشاركة على أهمية "مشاركة المواطنين الحقيقيين وانخراطهم الأكثر فاعلية ونشاط في الديمقراطية، ولذلك فهي تنتقد الفصل

[1] نفس المرجع، ص 23

[2] عباس مصطفى صادق، "**الإعلام الجديد: المفاهيم والوسائل والتطبيقات**"، عمان، دار الشروق، 2008م، ص17.

الراديكالي للمواطنين عن السلطة والنخب والمؤسسات الديمقراطية عن طريق التمثيل". "وإن وجود المؤسسات النيابية على المستوى القومي ليس كافياً للديمقراطية، فلكي تتحقق المشاركة القصوى من جانب الشعب جميعه على ذلك المستوى، يجب أن تحدث تنشئة اجتماعية أو "تدريب اجتماعي" على الديمقراطية في مجالات أخرى لكي يتسنى تطوير الاتجاهات والصفات السيكولوجية الضرورية. وهذا التطوير يحدث عن طريق عملية المشاركة ذاتها.[1]

وتطرح أوجه التنظير للإعلام تساؤلات حول مفهوم **New Media** وممارساته فهل تعبر مرحلته هذه عن انتقال أدوات الاتصال وتطبيقاته من المؤسسات إلى الجمهور؟ أو كما يرى البعض بظهور أنماط جديدة من الأشكال الإعلامية، إن النقد الموجه للإعلام الجديد يتمحور حول ضرورة تحديد المجالات التي يتحرك فيها هذا الصنف من الإعلام، فإمكانية الوصول إلى نموذج نظري للإعلام الجديد والراديكالي لا يتم عن طريق ما هو موجه من نقد للإعلام السائد بل إنطلاقا من مخرجات وتجارب وسائل الإعلام التي تطرح نفسها كبديل عن الإعلام الرسمي التقليدي. ويذهب بعض النقاد إلى الدعوة لدراسة الإعلام الجديد ليس إنطلاقا مما يجب أن يكون عليه بل عن طريق ما هو عليه، وهو ما سيمكننا من الحكم عليه إنطلاقا من مقدرته على عرض بدائل في مواجهة الإمبراطورية الإعلامية السائدة[2].

كما أن حصر الإعلام البديل في الرؤية القائلة بأنه عبارة عن حركة مضادة للثقافة الجماهيرية السائدة إجراء نظري قاصر، فالإعلام الجديد منتج أيضا لثقافة إتصالية بديلة، وعادة ما يكون في تعارض مع ما هو سائد. ويقع بين مفترق مناهج نظرية متداخلة فهو يعاني من طابعه المهمش خارج السياق الإجتماعي وخصوصيته في كونه بديل عن النظام الإعلامي القائم. ولهذا ركزت بعض المداخل على خدمة المجتمع ويعدّ مواقع التواصل الاجتماعي، او إعلام المواطن وغيرها من التسميات، بأنها جزء من المجتمع المدني. "وطرح فكرة مجتمعات الممارسة ذات الصلة، بوجود ممارسة مشتركة ومجتمع الممارسة هو مشروع مشترك يوجد تفاعل متبادل بين الأفراد العاملين فيه وله مجموعة من الموارد المشتركة".

---

[1] أولجا جوديس بيلي، بيلي كاميرتس، نيكوكاربنتيير، "**فهم الإعلام البديل**"، ترجمة: علا أحمد إصلاح، القاهرة، مجموعة النيل العربية، 2009م، ص24.

[2] أولجا جوديس بيلي، بيلي كاميرتس، نيكوكاربنتيير ،مرجع سبق ذكره، ص31.

ويعبر وينجر وزملاؤه عن هذه الفكرة كالتالي: "مجتمعات الممارسة عبارة عن جماعات من البشر يشتركون في غاية واحدة ومجموعة من المشكلات، ويقومون بتعميق معرفتهم وخبراتهم في هذه الناحية عن طريق التفاعل بصورة مستمرة". ولقد أظهر تحليل تأثير تكنولوجيات الاتصال على الحياة اليومية أن المجتمعات المحلية لا تتشكل فقط في المساحات الجغرافية المحددة بل ايضاً في الفضاء الاليكتروني وتسمى "المجتمعات الافتراضية"[1].

ويمكن أن تعمل مواقع التواصل الاجتماعي على تفعيل الطاقات المتوافرة لدى الإنسان ويوجهها للبناء والإبداع في إطار "تطوير القديم وإحلال الجديد من قيم وسلوك، وزيادة مجالات المعرفة للجمهور، وازدياد قدرتهم على التقمص الوجداني وتقبلهم للتغيير، وبهذا فإن الاتصال له دور مهم، ليس في بثَ معلومات، بل تقديم شكل الواقع، واستيعاب السياق الاجتماعي والسياسي الذي توضع فيه الأحداث"[2].

وقد ارتكزت البحوث العلمية حول وسائل الاتصال الحديثة على نموذجين تفسيريين، الأول، ويتمثل في الحتمية التكنولوجية، وينطلق من قناعة بأن قوة التكنولوجيا هي وحدها المالكة لقوة التغيير في الواقع الاجتماعي، والنظرة التفاؤلية للتكنولوجيا تهلل لهذا التغيير، وتراه رمزا لتقدم البشرية، وعاملا لتجاوز إخفاقها في مجال الاتصال الديمقراطي والشامل الذي تتقاسمه البشرية. والنظرة التشاؤمية التي ترى التكنولوجيا وسيلة للهيمنة على الشعوب المستضعفة، والسيطرة على الفرد، فتقتحم حياته الشخصية وتفكك علاقاته الاجتماعية[3].

أما النموذج الثاني، ويتمثل في الحتمية الاجتماعية التي ترى أن البُنى الاجتماعية هي التي تتحكم في محتويات التكنولوجيا وأشكالها، أي أن القوى الاجتماعية المالكة لوسائل الاعلام هي التي تحدد محتواها.

وإن البحوث النوعية التي تتعمق في دراسة الاستخدام الاجتماعي لتكنولوجية الاتصال لا تنطلق من النموذجين، لأنها لا تؤمن بأن ما هو تقني ويتمتع بديناميكية قوية،

---

[1] نفس المرجع، ص31.

[2] مي العبد الله، **الاتصال والديمقراطية**، بيروت، دار النهضة العربية،2005م، ص21 .

[3] نصر الدين لعياضي، "**الرهانات الابستمولوجية والفلسفية للمنهج الكيفي/ نحو أفاق جديدة لبحوث الإعلام والاتصال في المنطقة العربية**"، أبحاث المؤتمر الدولي، "الإعلام الجديد: تكنولوجيا جديدة... لعالم جديد"، جامعة البحرين، من 7-9 ابريل 2009م، ص18.

يوجد في حالته النهائية، كما أن البُنى الاجتماعية ليست منتهية البناء. ولعل هذه الحقيقة تنطبق أكثر على المجتمعات العربية التي تعرف حركية اجتماعية متواصلة لم تفض إلى صقل اجتماعي تتمايز فيه البنى الاجتماعية والسياسية، فالقوى الاجتماعية المتدافعة، في المنطقة العربية، مازالت قيد الصياغة والتشُّكل. كما أن المنطلقات الفلسفية للبحوث الكمية لا تسمح بالاعتقاد بوجود خط فاصل بين ما هو تقني وما هو اجتماعي، لأنهما يتفاعلان، باستمرار، في الحياة اليومية. بمعنى أن البعد الفكري للمنهج النوعي يسمح بالملاحظة الدقيقة لكيفية ولوج ما هو تقني في الحياة الاجتماعية، ولا يعطي الفرصة للأشخاص الذين يتعاملون مع وسائل الاتصال الحديثة بتشخيص ما هو تقني أو اجتماعي فقط، بل يسمح بإبراز تمثلهم لما هو تقني، والذي على أساسه يتضح استخدامهم له[1].

وقد أدى النمو الهائل في استخدام الانترنت، جعلت الباحثين في مجال الاستخدامات والإشباعات يزيدون من اهتماماتهم، والتحول من كيف يستخدم الأفراد الانترنت إلى دراسة الأسباب والدوافع التي تدفعهم لاستخدام هذا الوسيط ، وأن نموذج الاستخدامات والإشباعات يركز على الفرد المستخدم لوسائل الاتصال ويبني سلوكه الاتصالي على أهدافه بشكل مباشر، فضلاً عن أنه يختار من بين البدائل الوظيفية ما يستخدمه لكي يشبع احتياجاته. ولتحديد استخدامات الوسائل التكنولوجية الحديثة، فإن كثير من الدراسات السابقة تحققت من الافتراض بوجود ارتباط بين الدوافع الشخصية والدوافع المتعلقة بالوسيلة، ولتجديد دوافع الاستخدام. وأن الناس يستخدمون الكمبيوتر لإشباع ما يلي[2]:

أ- الحاجات الشخصية على سبيل المثال السيطرة، الاسترخاء، السعادة والهروب.

ب- الحاجات التي يمكن إشباعها تقليدياً من الوسيلة مثل التفاعل الاجتماعي وتمضية الوقت والعادة واكتساب المعلومات والتسلية.

ويعدّ المدخل، مدخلاً اتصالياً سيكولوجياً، فقد افترض وجود جمهور نشط له دوافع شخصية ونفسية واجتماعية، تدفعه لاستخدام الانترنت كوسيلة تتنافس مع غيرها من الوسائل

---

[1] نصر الدين لعياضي،المرجع السابق، ص19.

[2] عزة مصطفى الكحكي، "**استخدام الانترنت وعلاقته بالوحدة النفسية وبعض العوامل الشخصية لدى عينة من الجمهور بدولة قطر**"، أبحاث المؤتمر الدولي، "الإعلام الجديد: تكنولوجيا جديدة... لعالم جديد"، جامعة البحرين، من 7-9 ابريل 2009م،ص269

لإشباع احتياجاته، وتطبيقاً على ذلك فإن فئات جمهور مستخدمي الانترنت أكثر نشاط ومشاركة في العملية الاتصالية بتأثير التفاعلية التي يتميز بها الاتصال الرقمي، وبالتالي فإننا نتوقع أن يتخذ الفرد قراره في الاستخدام عن وعي كامل بحاجاته التي يريد إشباعها، ويتمثل الاستخدام في اتجاهين: الاتصال بالآخرين عن طريق الوسائل المتاحة على الانترنت، سواء كان المستخدم مرسلاً أو مستقبلاً. وتصفح الشبكات المختلفة لتلبية الحاجات.

وتطبيقاً على مدخل الاستخدامات والإشباعات تتضح الدوافع التالية لاستخدام الانترنت:

1- كبديل عن الاتصال الشخصي.

2- الإدراك الذاتي عن الجماعات المختلفة من الناس.

3- تعلم السلوكيات المناسبة.

4- كبديل أقل تكلفة عن الوسائل الأخرى.

5- المساندة المتبادلة مع الآخرين.

6- التعلم الذاتي.

7- التسلية والأمان والصحبة.

ويحصر مدخل نيغروبونتي الميزات التي يتحلى بها الاعلام الجديد في: "استبداله الوحدات المادية بالرقمية، وتشبيك عدد غير محدود من الاجهزة مع بعضها البعض، ويلبي الاهتمامات الفردية والاهتمامات العامة، أي أن الرقمية تحمل قدرة المخاطبة المزدوجة للاهتمامات والرغبات وهي حالة لا يمكن تلبيتها بالاعلام القديم. والميزة الاكثر أهمية، هي أن هذا الاعلام خرج من أسر السلطة التي كانت تتمثل في قادة المجتمع والدولة إلى أيدي الناس جميعا"[1].

ويشترك فين كروسبي مع نيغروبونتي في الافكار نفسها، ويعقد مقارنة بين الاعلام الجديد والقديم عن طريق النماذج الكلاسيكية، ابتداء من اول نموذج اتصالي بين البشر، الاتصال الشخصي، وله حالتان تميزانه[2]:

[1] عباس مصطفى صادق، مرجع سبق ذكره، ص9.

[2] المرجع السابق ، ص10.

النموذج الاول: الاتصال الشخصي

1- يملك كل فرد من طرفي الاتصال درجة من درجات السيطرة المتساوية على المحتوى المتبادل بين الطرفين.

2- يحمل المحتوى ترميزا يؤكد حالة الفردية التي تحقق احتياجات ومصالح صاحب المحتوى.

3- التحكم المتساوي وميزة الفردية ينخفضان في حالة ازدياد عدد المشاركين في العملية الاتصالية، مما جعل خبراء الاتصال يطلقون عليه الاتصال من نقطة الى اخرى او من فرد لآخر One-to-one.

النموذج الثاني: الاعلام الجديد ويتميز حسب كروسبي بما يأتي:

1- يمكن للرسائل الفردية ان تصل في وقت واحد الى عدد غير محدود من البشر.

2- ان كل واحد من هؤلاء البشر له درجة السيطرة نفسها ودرجة الاسهام المتبادل نفسها.

وتصف نظرية ثراء وسائل الإعلام Media Richness Theory لدراسة معايير الاختيار بين الوسائل الإعلامية التكنولوجية وفقاً لدرجة ثرائها المعلوماتي، وتوضح أن فعالية الاتصال يعتمد على القدر الذي تستخدم به الوسيلة، وتركز بشكل أكبر على الأشكال التفاعلية للاتصال فى اتجاهين بين القائم بالاتصال والجمهور المستقبل للرسالة، وطبقاً للنظرية فإن الوسائل الإعلامية التى توفر رجع صدى تكون أكثر ثراء، فكلما قل الغموض كلما كان الاتصال الفعال أكثر حدوثاً، فثراء المعلومات يقوم بتخفيض درجة الغموض وإيجاد مساحة من المعاني المشتركة باستخدام وسيلة اتصالية معينة. وتفترض هذه النظرية فرضين أساسين هما[1]:

الفرض الأول: أن الوسائل التكنولوجية تمتلك قدراً كبيراً من المعلومات، فضلاً عن تنوع المضمون المقدم من خلالها وبالتالي تستطيع هذه الوسائل التغلب على الغموض والشك الذي ينتاب الكثير من الأفراد عند التعرض لها.

الفرض الثاني: هناك أربعة معايير أساس لترتيب ثراء الوسيلة مرتبة من الأعلى إلى الأقل من حيث درجة الثراء وهي سرعة رد الفعل، قدرتها على نقل الإشارات المختلفة

[1] أولجا جوديس بيلي، وآخرون، مرجع سبق ذكره، ص71.

باستخدام تقنيات تكنولوجية حديثة مثل: الوسائط المتعددة، والتركيز الشخصي على الوسيلة، واستخدام اللغة الطبيعية.

وبرزت نظرية التسويق الاجتماعي بين نظريات الاتصال المعاصرة، لتجمع بين نتائج بحوث الإقناع وانتشار المعلومات، في إطار حركة النظم الاجتماعية والاتجاهات النفسية، بما يسمح بانسياب المعلومات وتأثيرها، عن طريق وسائل الاتصال الحديثة ومنها "مواقع التواصل الاجتماعي"، وتنظيم استراتيجيات عن طريق هذه النظم المعقدة، لاستغلال قوة وسائل وأساليب الاتصال الحديثة لنشر طروحات وايديولوجيات يراد نشرها في المجتمع.

المطلب الثاني:الجريمة الالكترونية عبر مواقع التواصل الاجتماعي

لقد اختلف الفقه والقانون في تصنيف الجرائم الالكترونية باختلاف الزاوية التي ينظر منها إزاء الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي.

وعليه سنقوم في هذا المطلب بتقسيم الجرائم الالكترونية وفقا لما أقره فقهاء القانون الجنائي ثم تقسيمها وفقا لما أقرته التشريعات المقارنة.

اختلف الفقه الجنائي حول تقسيم الجرائم الالكترونية، حيث قد يكون النظام المعلوماتي هو نفسه موضوع أو محل الجريمة الالكترونية ومن ناحية أخرى، قد يكون النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها[1]

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة .

وتنقسم هذه الجرائم بدورها إلى:

رغم تطور الحياة اليومية للأفراد والمجتمع بفضل استعمالهم للفضاء الافتراضي إلا أنه أصبح سلاحا فتاكا في يد المجرمين للدخول إلى المعلومات الخاصة للأشخاص ،وعليه ظهرت عدة أنواع خاصة من الجرائم الالكترونية الواقعة على الاشخاص كجريمة التهديد والمضايقة والملاحقة، خاصة عن طريق البريد الالكتروني بإرسال رسالة خاصة للترويع

[1] صالح شنين: **الحماية الجزائية لبرامج الحاسب الآلي**، دراسة مقارنة رسالة لنيل شهادة الماجيستير، جامعة بسكرة –كلية الحقوق والعلوم السياسية، 2007 – 2008، ص: 107.

والتهديد أو عن طريق وسائل الحوارات المختلفة على شبكة الانترنيت: كالفيسبوك، والفايبر والواتساب.[1]

الفرع الاول :جريمة القذف على شبكة الانترنت:

إن جريمة القذف تعد من الجرائم التقليدية المنصوص عليها في اغلب المدونات العقابية أصبحت في الوقت الحالي ومع التطور الكبير في تكنولوجيا المعلومات ووسائل الاتصال تتم بواسطة وسائل مستحدثة منها شبكة الانترنت ولذلك سوف نتطرق إلى جريمة القذف على شبكة الانترنت.

اولا: جريمة القذف على الانترنت:

المقصود بجريمة القذف على شبكة الانترنت: عرفها الدكتور حسنين ابراهيم صالح عبيد، هو "إسناد علني عمدي لواقعة محددة تستوجب عقاب أواحتقار من أسندت إليه"[2]وعلى ذلك فان جريمة القذف عن طريق الانترنت هي جريمة يلازم وصفها طبيعة فعل النشر وهي تبدأ وتنتهي بارتكاب هذا الفعل ومن ثم فهي جريمة وقتية.

ثانيا :الطبيعة القانونية لجريمة القذف عبر شبكة الانترنت:

انتهت الدراسة المعنونة" دور الوسائل الالكترونية في المواد الجنائية "إلى أن الوسائل الالكترونية كانت فعلا خصيبا لتطوير قانون العقوبات ،كما كان للقضاء الجنائي دوره في وضع الحلول الكفيلة بمواجهة تلك الوسائل، فقد كان لجهاز قياس سرعة السيارة دوره في إثبات تجاوز السرعة المقررة ومدى اعتبارها عناصر مكونا لجريمة تعريض الغير للخطر.

كما كان للهاتف سواء كان محمولا أوعاديا أثره كعنصر مكون لجرائم قائمة من قبل وفي ظهور صور جديدة من التجريم.

وأخيرا كان للانترنت تأثيره على تحديد الطبيعة القانونية لبعض الجرائم.

فقد ظهرت العلاقة بين الانترنت والقانون الجنائي ،عندما ثارت مشكلة تحديد الطبيعة القانونية لجريمة القذف المرتكب عن طريق الانترنت أمام المحاكم الفرنسية بمناسبة قضية

[1] يوسف صغير: المرجع السابق، ص: 50.

[2] مصطفى محمد موسى،**التحقيق الجنائي في الجرائم الالكترونية** ،الطبعة الأولى ، 2009 ،مصر، ص430

اتهم فيها متهم بنشر تعليق يتضمن قذفا في حق شخصية سياسية . وتم تداوله عبر شبكة الانترنت وعند محاكمته دفع بانقضاء الدعوى الجنائية بالتقادم تأسيسا على أن جريمة القذف بطريق الانترنت هي من جرائم النشر التي تنقضي فيها الدعوى بمضي ثلاثة أشهر من تاريخ ارتكاب الجريمة.[1]

ثالثا :صور القذف عبر شبكة الانترنت

أثار إجرام تقنية المعلومات تحديات كبيرة بالنسبة لقانون العقوبات ففي إطار مجتمع المعلومات الالكترونية أدى العابثون أغراضهم في تشويه رسائل تحوي عبارات ذم وقدح وتحقير لأشخاص مستهدفين بذاتهم أو غير مستهدفين ، مما يؤدي بنا إلى التساؤل حول مدى انطباق النصوص التقليدية المتعلقة بجرائم القذف والتحقير على مثل هذه الأفعال فيما لو ارتكبت عبر الانترنت من خلال مجلات استخدامه المختلفة.

وتتنوع صور القذف والذم والتحقير بتنوع الغرض من استخدام الانترنت ، والطريقة التي يستخدم بها ، فقد يكون الذم والقذف والتحقير وجاهليا عبر خطوط الاتصال المباشرة ، أوقد يكون كتابيا أوقد يكون غيابيا ، أوقد يكون بواسطة المطبوعات ، وجميع هذه الصور ترتكب عبر الانترنت من خلال المبادلات الالكترونية الكتابية أو الصوتية أو الفيديوية وهي أما أن تكون بين طرفيتا انترنت متصلة (الحواسيب) وإما أن تكون بواسطة طرفية انترنت منفصلة (مستقلة) [2]وعليه سوف نقوم بدراسة هذا المطلب في مطلبين حيث نتناول في المطلب الأول المراسلات الالكترونية عبر طرفية انترنت متصلة والمطلب الثاني المراسلات الالكترونية عبر طرفية انترنت منفصلة.

1. المراسلات الالكترونية عبر طرفية انترنت متصلة:

يشكل كل جهاز حاسب آلي متصل بشبكة الانترنت بواسطة موديم عبر خطوط الهاتف طرفية متصلة بشبكة الانترنت ، مما يؤدي إلى تيسير التبادل الالكتروني للبيانات فيما بين

[1] نفس المرجع السابق ، ص428

[2] محمد أمين الشوابكة ، مرجع السابق ، ص31

المتراسلين عبر خدمات الانترنت المتاحة بمختلف وسائل نقل البيانات ، ولكن قد يساء استخدام الخدمات المتاحة لتحقيق غايات الجاني.

أ :البريد الالكتروني

يعد البريد الالكتروني من أقدم التطبيقات في شبكة الانترنت وأكثرها انتشار حيث أصبح يشكل وسيلة اتصال لا غنى عنها في كثير من مجالات العمل [1]وعليه فهوأكثر شيوعا وستزيد أهميته ، عند اكتمال الطريق السريع للمعلومات وهويتكون من جزئيين رئيسيين: رأس headersونص body ويحتوي ال أ رس على معلومات حول ال ا رسل والمتلقي والمعلومات اللازمة لتوصيل الرسالة إلى العنوان المناسب ويحتوي النص على الرسالة التي تم تكوينها وعندما يرسل شخص ما رسالة إلى شخص آخر فإنها تنتقل من كومبيوتر المرسل عبر خط تليفون إلى كومبيوتر الخادم أو ما يسمى ملقم البريد والذي يوجد به صندوق بريد المرسل ومن ثم تنتقل على نحومباشر أو غير مباشر إلى أي كومبيوتر خادم يخزن صندوق بريد الم رسل إليه وعندها يستطيع المرسل إليه استرجاع محتويات صندوق بريده الالكتروني عند اتصاله بالخادم الخاص به ، وفق ما يسمى بالتحميل التحتي ، ويتم ذلك كله وفق بروتوكولات مثل عدة مثل pop و imapو. smtp

ويستطيع الجاني من خلال البريد الالكتروني أن يسند مادة معنية إلى شخص عاقد يكون معين بذاته وهي الصورة الغالبة ، أو غير معين بحيث تنال من شرفه أو كرامته وتعرضه إلى بغض الناس واحتقارهم ، ولا يلزم أن تكون هذه المادة جريمة تستلزم العقاب.

وقد يقوم الجاني بالاعتماد على كرامة الغير أو شرفه أو اعتباره ولوفي معرض الشك والاستفهام[2] من دون بيان مادة معينة ، فإذا استخدم الجاني البريد الالكتروني للقيام بالأفعال السابقة عدة مرتكبا لجريمة القذف وإذا كانت عمليات الإرسال والمراسلات الالكترونية تتسم بأنها لا تزامنية.

---

[1] طارق عثمان، **الحماية الجنائية للحياة الخاصة عبر الأنترنت** ، دراسة مقارنة ، مذكرة ماجيستر جامعة بسكرة ،2006، ص39

[2] محمد أمين الشوابكة ، مرجع سابق ، ص32

-بمعنى أنه يتم تبادل الرسائل في أي وقت

-فإن ذلك لا يثير أي مشاكل فيما يتعلق بالقذف الغيابي والذي يشترط أثناء الاجتماع بأشخاص كثيرين مجتمعين أومنفردين ، فإذا ما كان هناك أشخاص أي اثنان فأكثر أثناء إرسال الجاني رسالته الالكترونية ورأوا أوسمعوا ما تم إسناده ، فعندئذ يعد الفاعل مرتكبا لفعله ، وخاصة إن إمكانية نقل الصور والأصوات متاحة عبر شبكة الانترنت ، ومن خلال أكثر تطبيقات الشبكة شيوعا البريد الالكتروني ولكن الأمر يدق في صور الذم والقذف ال وجاهي الذي يوجب النص لإيقاع العقاب عليه إن يتم في مجلس بمواجهة المعتدى عليه ، أوفي مكان يمكن لأشخاص آخرين يسمعوه قل عددهم أوكثر.

إن الذم والقذف لا تتحقق صورته إذا ما تم تبادل الرسائل الكترونيا عبر البريد الالكتروني حيث أن هذه المراسلات تتسم بأنها لا ت ا زمنية على فرد ثبوتها فإن فكرة المجلس تثير الكثير من الاستفهامات[1] إذ تقتضي الوحدة في المكان والزمان وهي إن تحققت من حيث الزمان فإنه لا يمكن اعتبار بيئة شبكة الانترنت مجلسا يجمع الجاني بالغير وإذا كان القذف وجاهي لا يتحقق في صورته الأولى .

إلا انه يتحقق في صورته الثانية ، حيث يلزم إن يقع في مكان يمكن لأشخاص آخرين إن يسمعوه قل عددهم أوكثر ويستوي لن يكون المكان عاما أوخاصا طالما كان بإمكان ما كان متواجدا في مكان عام سماعه.

وبما أن الكتابة تشكل الاستخدام الأكبر للانترنت فان الذم والقذف والتحقير الخطي يشكل الصورة الغالبة لمثل هذا النوع من الجرائم ،ويقع بما ينشر بين الناس ويذاع ويتم النشر والإذاعة عبر البريد الالكتروني من خلال إرسال الرسالة المتضمنة المادة التي تشكل ذما أو قدحا.

ب. : شبكة الويب العالمية:يمكن تعريف شبكة الويب العالمية بأنها عبارة عن كم هائل من المستندات المحفوظة في شبكة الحاسوب ، والتي تتيح لأي شخص أولأي جهة الاطلاع على معلومات تخص جهات أخرى أوأشخاص آخرين قاموا بوضعها على هذه الخدمة ،

[1] محمد آمين الشوابكة ، نفس مرجع سابق،ص33

حيث تقدم خدمة معلومات واسعة النطاق من خلال خاصية الخطوط المحورية المتعددة[1] والتي تسمح للمستخدمين بالارتباط عبر أنظمتها والملفات للحصول على المعلومات التي يعلق عليها النص المحوري ولكل مستخدم شبكة الانترنت أن ينشئ له موقع على شبكة الويب العالمية ، تتضمن معلومات يمكن إعادة تخزينها والتي يمكن لأي مستخدم آخر في جميع إنحاء العالم استقبال لهذه المعلومات من خلال نظم الاستقبال وهذه المعلومات قد تكون مفيدة ومتعددة (ثقافية، علمية ، ترفيهية ، دعائية) . . . مما يخدم الغرض من إنشاء هذه الشبكة ، أوقد تكون معلومات معرضة تهدف إلى الإساءة إلى الآخرين ومن شأنها أن تنال من شرفهم أوكرامتهم ، أوتعرضهم إلى بعض الناس واحتقارهم مما يستتبع بالضرورة توافر الركن المادي لجريمة القذف والتحقير.

فقد يرتكب الذم والقدح والتحقير عبر شبكة الويب العالمية من خلال إسناد مادة كتابية صوتية، فيديوية صوتية (سمع ، بصري استفئ إلى احد الأشخاص ، ومن شأنها أن تنال من شرفه أوكرامته أوتعرضه إلى بغض الناس واحتقارهم ، وهوغالبا ما يتخذ صورة الذم والقذف الخطي بواسطة المطبوعات ، حيث انه من خلال صفحات الويب يتم نشر اوذاعة وتوزيع الكتابات أوالرسوم أوالصور الاستهزائية أومسودات الرسوم) قبل أن تزين أوالمكاتب المفتوحة وبطاقات البريد التي تنشئ إلى المعتدى عليه.

وكذلك فإن الجرائد والصحف اليومية أوالموقوتة الالكترونية أخذت غيرها على شبكة الويب العالمية ، ويمكن ارتكاب أفعال الذم والقذف والتحقير من خلالها والتي تثير الكثير من الصعوبات حول تكيفها، حيث أن صحائف الويب توضح على الحاسب الخدمي بصورة دائمة بهدف أن يستطيع أي شخص الاطلاع عليها وهي تختلف عن الرسائل الالكترونية والتي تعد من قبيل المرسلات الخاصة إذا كانت موجهة لشخص أوأشخاص محددين مقدما وتستخدم كذلك صفحات الويب في الترويج للأفكار عن طريق نشر الدعاية التي قد تتضمن عبارات ذم وقدح وتحقير بحق الآخرين ، أفرادا كانوا أم مؤسسات فيقع القذف والذم والتحقير على الأشخاص الاعتبارية بجانب الأشخاص الطبيعيين.

[1] مصطفى محمد موسى ، المرجع السابق،ص428

ومن أشهر قضايا الإساءة استخدام شبكة الانترنت ما يتعلق باستخدام المنظمات النازية لشبكة الانترنت العالمية لنشر أفكارها العنصرية حيث زودت بعض مواقعها بمواد السمع بصرية والنصوص الفاشية والتي تضمنت قوائم بأسماء وعناوين الشخصيات اليسارية الألمانية لتحريض أعضاءها على استخدام التصفية الجسدية[1]

إن القانون الألماني يمنع نشر الدعاية النازية فقد حاولت المحكمة العليا الألمانية أن تطبق القوانين الألمانية على من يروجون للأفكار النازية أويتاجرون بآثارها على الشبكة العالمية من خلال مزودات خدمة أجنبية يمكن الوصول إليها من قبل المقيمين على الأراضي الألمانية.

في حين يرى الألمان أن هذه الحرية يجب أن تنتهي عندما توضع في خدمة النازية حيث قدموا شكاوى ضد دعاة النازية للسلطة القضائية [2]لاتخاذ إجراءات عملية لإغلاق مواقعهم لدى مزودات الخدمة الأمريكية وأيضا عن طريق إغلاق هذه المواقع بالرسائل الالكترونية واستهدافها بالفيروسات الحاسوبية وقد ذهب القضاء الفرنسي الذي تمنع قوانينه الاتجار بالسلع ذات الطابع النازي إلى إصدار إنذار شركة Yahoo الأمريكية يمهلها مدة ثلاثة أشهر للحيلولة دون ولوج المشتركين الفرنسيين لديها إلى مواقع تروج للسلع النازية وفي حال امتناع Yahoo عن هذا الأمر القضائي ، تفرض عليها السلطات الفرنسية غرامة تصل قيمتها إلى 15.245 يوروفي اليوم الواحد.

وعليه نخلص إلى نتيجة مفادها أن الأنشطة المادية لجرائم الذم والقدح والتحقير قد تمارس عبر الانترنت من خلال شبكة الويب العالمية مما يثير مسألة تنازع الاختصاص القضائي بين بلدان عدة تجيز حرية التعبير عن الرأي ولا تعد بعض الأفعال من قبيل أفعال القذف والذم والتحقير وبين بلدان أخرى تسعى الى تطبيق قوانينها المحلية على كل ما يمكن أن يمس حرية الأفراد أوشرفهم واعتبارهم[3]

---

[1] طارق عبد الحق ،**برمجيات الانترنت ،الملاحة و الاستكشاف** ،قصر الكتاب ، 2005 ، الجزائر، ص22

[2] محمد أمين الشوايكة ، مرجع سابق ص34

[3] نفس المرجع السابق ص21

ج. مجموعة الأخبار:مجموعات الأخبار عبارة عن مناطق مناقشات عامة عبر الانترنت ،يمكن من خلالها التحدث حول أي موضوع ، مع إمكانية تبادل الصور والمعلومات المقروءة أوالمكتوبة ويتم ذلك من خلال نظام news groups نيوز حروب أونظام يوزنت usenetوكلاهما عبارة عن مجموعات أخبار ، لكن يختلف أحدهما عن الآخر من ناحية إقامة المسؤولية الجنائية حول مراقبة وتوزيع الوثائق[1].

ففي مجموعات أخبار نيوز جروب news group لانتثار مشكلات خاصة من ناحية المسؤولية الجنائية ولا ينطبق عليها نظام المسؤولية المطبقة في مواد وسائل الإعلام المرئية والمسموعة والتي تعني بأن شخصيا يمارس صحافة ويقوم بمراقبة وتوزيع هذه الوثائق حيث أن نظام نيوز جروب يستخدم بواسطة الانترنت ويتم بواسطة الانترنت ويتم بواسطة إدارة المعلومات ومراقبة توزيعها إما نظام يوزنت usenet فهوعبارة عن احد الأنظمة التي تقدم خدمة بالانترنت ويقوم بواسطتها المستخدم عن طريق استخدام نظام أوتوماتيكي ليست رسالة أو عدد الرسائل إلى مجموعة من المستخدمين أو المشتركين وبالتالي يمكن إقامة المسؤولية الجنائية للأشخاص الدين يقومون بإدارة بوزنت إذا ما تبث أنهم قد أخذوا موقع أحد المجوعات غير المشروع (أي رسائل ومعلومات يعاقب عليها القانون)[2].

وعليه فإنه لا يلزم إقامة المسؤولية الجنائية على الأشخاص الذين يديرون هذه الشبكات ، إذ لا يملكون السيطرة والرقابة على مضمون الرسائل التي ترد إلى هذه المجموعات ، والتي يمكن أن يشكل مضمونها جريمة جنائية كأن تحوي عبارات قذف أو سب أو أية مادة من شأنها أن تنال من شرف المجني عليه أو كرامته أو تعرضه لبعض الناس واحتقارهم مما يشكل بالتالي جريمة الذم والقدح والتحقير ،ولكن يذهب بعض الفقهاء في هذا الفرض إلى القول بضرورة إقامة المسؤولية الجنائية على الأشخاص الذين يديرون هذه الشبكات.

---

[1] أحمد حسام طه تمام ، **الحماية الجنائية لتكنولوجيا الاتصالات** ، دراسة مقارنة ، دار النهضة العربية ، 2002 ، مصر ، ص832

[2] منير محمد الجنبهي ، **ممدوح محمد الجنبهي، تبادل إلكتروني للمعلومات** ، دار الفكر الجامعي،2004، مصر ، ص12

ونجد أن صور الذم والقذف والتحقير يمكن أن تمارس خلال مجموعات الأخبار فيكون الذم والقذف والتحقير وجاهيا متى كان كل من الجاني والمجني عليه يتبادلون الرسائل عبر مجموعات الأخبار ، أوفي صدد تعليقهم ومشاركتهم على موضوع معين[1]

وكذلك تتحقق صورة الذم والقذف والغيابي عبر مجموعات الأخبار فيما لوترك المستخدم عنوان بريده الالكتروني على مجموعات الأخبار ليتسنى له استقبال الرسائل حول موضوع معين ولمعرفة أخبار موضوع يشغل اهتمامه ، سواء من قبل القائمين على إدارة مجموعات الأخبار أومن قبل المشتركين في هذه المجموعات على حد سواء.

وكذلك تتحقق صورة الذم والقذف الخطي عبر مجموعات الأخبار حيث أن عبارات الذم والقذف والتحقير تنشر وتذاع بين الناس عبر حلقات النقاش هذه ، أوقد توزع على فئة منهم على شكل كتابات أو صور استهزائية أو مسودات الرسوم قبل أن تزين وترسل إلى بريدهم الالكتروني. [2]

وكذلك قد يتم إرسال المكاتب المفتوحة وبطاقات البريد الالكتروني المتضمنة عبارات ذم وقذف وتحقير بحق المجني عليه إلى مجموعات الأخبار وعلاقات النقاش فيتحقق بذلك الركن المادي لجريمة القذف والتحقير الخطي.

وأيضا تتحقق صورة القذف بواسطة المطبوعات من خلال الجرائد والصحف اليومية أو الموقوتة والتي تتضمن مقالات تحتوي على أفعال ذم وقذف فيتحقق الركن المادي لهذه الجريمة بواسطة المطبوعات.

–والجديد فيما تثيره رسائل مجموعات الأخبار المتضمنة أفعال الذم والقذف والتحقير والتي يتم استقبالها في جميع أنحاء العالم إمكانية الشخص مرتكب الفعل أن يدفع بحسن النية بعدم علمه بأن رسالته تسئ بالشرف أوالاعتبار أي أن يدفع بعدم توفر الركن المعنوي على انه إذا

[1] محمد أمين الشوايكة ، مرجع سابق ، ص44

[2] أحمد حسام تمام ، **الحماية الجنائية لتكنولوجيا الاتصالات** ، دراسة مقارنة ، دار النهضة العربية ، 2002، مصر ، ص237

أمكن قبول مثل هذا الدفع فإنه يصعب نفي الطابع العام للذم والقذف والتحقير والذي يتم بحق مجموعة المشتركين في مجموعات الأخبار

وعلاوة على ذلك فإن هنالك مشكلة أخرى تتمثل باستحالة حذف وازالة هذه الرسالة بالكامل حتى ولو صدر قرار قضائي بالحذف حيث يمكن السيطرة على مثل تلك الأفعال بعد صدور القرار القضائي أما الأفعال التي تمت قبل صدور القرار القضائي فإنه لا يمكن السيطرة عليها

د. غرف المحادثات والدردشة: غرف المحادثات أو الثرثرة عبارة عن ساحات معروفة في الفضاء الالكتروني cyber space تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض ، بإرسال البريد الالكتروني الذي يمكن قراءته من قبل الشخص المشترك في غرف المحادثة.

وفي الواقع عندما تتخاطب عبر الانترنت فإن ما يحدث هوانك تكتب رسالة باستخدام لوحة المفاتيح بحيث يمكن للآخرين رؤية ما تكتب وبعدها يكتبون رسائل على لوحات المفاتيح الخاصة بهم ، فالقائم على عملية التخاطب لا يحدث بالفعل مع الشخص الآخر ولا يسمع ما يقوله[1]، ويمكنك التخاطب مع المجموعة كلها أو مع فرد واحد ،ولذلك بإمكانك أن تختار موضوع التخاطب الذي تريد ، ونوعه الذي توفره تقنيات الانترنت أكثر هذه التقنيات شيوعا هي:

- Internet chat realy: ويلزم برنامج خاص للمشاركة فيه مثل برنامج chat chanmts ويسمى هذا النوع التخاطب بقنوات التخاطبchat channels
- American line: وتقوم بالتخاطب من خلالها باختيار الموضوع الذي تريد ولكن عيوبه الأمنية كثيرة.
- I seek you: ويتيح تلك هذا البرنامج معرفة متى يكون أصدقائك على اتصال بالانترنت onlime لإرسال رسائل فورية.

[1] طارق عبد الحق ، نفس المرجع ، ص27

- رسائل وأوراق مباشرة حيث يمكنك مخاطبة فرد لفرد ، وتوجد هذه الخدمة بالإضافة A O N في Yahoo pager America Online instan messenger
- التخاطب القائم على الويب ، من خلال الاتصال بموقع الويب نفسه
- عزف تخاطب خاصة ، حيث يمكنك عملها وزيارتها أنت ومن تقوم بدعوتهم[1]

بما أن التخاطب يتم بالكتابة بإستخدام لوحة المفاتيح لدى كل من المتخاطبين فإن الصورة الغالبة للذم، والقذف والتحقير التي ترتكب ،بواسطة غرف المحادثة ، هي صور الذم والقذف الخطي والذي يشترط أن يقع بما ينشر ويذاع بين الناس أو بما يوزع على فئة منهم من الكتابات أو الرسوم أو الصور الاستهزائية أو مسودات الرسوم.

بما يرسل إلى المعتدى عليه من الرسائل المفتوحة (غير مغلقة) وبطاقات البريد فإذا ما قام الجاني ينشر وتوزيع أي مادة من شأنها أن تنال من شرف المجني عليه وتعرضه إلى بعض الناس واحتقارهم ، سواء كانت تلك المادة جريمة تستلزم العقاب أم لا ، يعد الفاعل مرتكبا لفعل القذف ولو قام بذات الاعتداء دون بيان مادة معينة ع د قدحا وكذلك كل ما يتم بالكتابة أو الرسم عبر غرفة المحادثة يعتبر تحقيرا ولوحم يكن علانيا.

2. المراسلات الالكترونية عبر طرفية انترنت منفصلة: تتمثل طرفية الانترنت المستقلة ،كل تقنية علمية حديثة غير الحاسوب ، تسمح بصورة مباشرة أو غير مباشرة بالتبادل الالكتروني للبيانات وهي ما تعرف بتسمية الشريك الالكتروني.[2]

ولم تعد الثورة الرقمية مقصورة على التبادل الالكتروني للبيانات عبر الشبكات المحلية أو حتى في نطاق الشبكة العالمية بين الحواسيب فقط ، بل أصبح من الممكن الدخول إلى شبكة الانترنت أو لانتفاع من الخدمات المتاحة وإجراء المبادلات الالكترونية من خلال أجهزة الهواتف الخلوية ويمكن من خلال الهاتف النقال استقبال أو إرسال البيانات على شكل رسالة قصيرة كما يمكن إرسال بيانات أو رسائل منها إلى أي بريد الكتروني ، وكذلك يمكن الاتصال بأي موقع على الشبكة للاستفسار عن أية معلومة يريدها المستخدم (

[1] منير محمد الجنبهي ، ممدوح محمد الجنبهي ، المرجع السابق ، ص11

[2] محمد أمين الشوايكة،المرجع السابق، ص45

كأسعار العملات والبورصة أو الأخبار ، أو المعلومات الترفيهية) . . . وكذلك يمكن إجراء التحويلات الالكترونية للأموال من هذه الطرفية ،وذلك كله وفقا لما تنتجه خدمة بروتوكول التطبيق اللاسلكي ويهدف بروتوكول التطبيق اللاسلكي (W A P) إلى نقل المعلومات البيانية بشكل نقطي ،للسماح بالولوج إلى صفحات الويب عبر الهاتف النقال من أي مكان و للعرض على شاشة الهاتف ،وكذلك يهدف إلى تحويل الهاتف النقال إلى طرفية انترنت بحيث يمكن

النفاذ إلى شبكة الانترنت وتصفحها واستعراض صفحاتها بشكل يماثل شاشة صغيرة إذ يمكن ممارسة الأعمال الالكترونية من خلالها والهاتف النقال شأنه شأن الانترنت قد يساء استخدامه في غير الغرض الذي خصص من أجله لاقتراف أفعال مختلفة تكون مجرمة ،أو غير مجرمة وذلك وفقا للتفسيرات المختلفة للنصوص التقليدية[1]

والحقيقة أن جريمة القذف عبر شبكة الانترنت تعد أحد صور إساءات استخدام هذه الأجهزة . وعليه فإن انطباق النصوص التقليدية على مثل هذه الممارسات يكون في حالتين لارتكاب جرائم الذم والقدح والتحقير من خلال تلك الظرفيات.

الحالة الأولى : تتعلق بالرسائل الالكترونية المتضمنة مواد القدح أو الذم أو التحقير من شبكة الانترنت بواسطة الخدمات المتاحة إلى الهاتف النقال سواء كانت رسائل كتابية أو رسوم أو صور أو محادثات صوتية (أي رسائل السمع بصرية)

الحالة الثانية : تتعلق بالرسائل الالكترونية من الهاتف النقال إلى شبكة الانترنت من خلال خدمتها المتاحة (البريد الالكتروني ،أو شبكة الويب أو غرفة المحادثة أو مجموعة الأخبار..الخ)

ونرى أن الحالة الأولى وإن تضمنت مواد قذف أو ذم أو تحقير إلا أن الجريمة لا تقوم لانتفاء ركن العلانية الذي تطلبه المشرع ، إذ أن المجني عليه وحده يمكنه رؤية أو سماع ما أسند إليه من مواد إذ يعد من قبيل المراسلات الخاصة بينما يمكن أن تتحقق الجريمة في

[1] جميلة عبد الباقي الصغير ،**ادلة الاتبات الجنائي و التكنولوجيا الحديثة** ،الطبعة الأولى دار النهضة العربية ،2001ص 111

الحالة الثانية وعليه فإنه يمكن إثبات ما يتم إسناده من مواد مجرمة تمس بشرف المجني عليه أو كرامته أو سمعته واعتبا ره إذا ما كانت الرسالة الالكترونية مرسلة من الهاتف النقال إلى شبكة الانترنت حيث يمكن الرجوع إلى البيانات الخاصة بمنشئ الرسالة من خلال رقم الهاتف وعلى العكس من ذلك تثار مشكلة الاتباث ، فيما لو أرسلت الرسالة من شبكة الانترنت إلى تلك الطرفية[1]

كما تعتبر من أهم الجرائم الالكترونية الواقعة على الأشخاص صناعة ونشر الإباحة والجنس سواء للبالغين والأطفال خاصة، حيث يتعرض الأطفال للاستغلال الجنسي على الانترنيت بأشكال متعددة انطلاقا من الصور إلى التسجيلات المرئية للجرائم الجنسية العنيفة، حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنيت .[2]

ويضاف إلى الجرائم الالكترونية الشخصية جرائم انتحال الشخصية والتغرير والاستدراج باستخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحياته أو تتخذ هذه الجريمة وجهان: انتحال شخصية الفرد وانتحال شخصية المواقع.[3]

الفرع الثاني: الجرائم الواقعة على الأموال:

لقد صاحب تطور شبكة الإنترنيت تطور وسائل الدفع والوفاء، وأضحت جزء لا يتجزأ من المعاملات الإلكترونية وفي خضم هذه التداول المالي عبر الإنترنيت ظهرت عدة جرائم الكترونية على الأموال مثل: السطو والسرقة، والتحويل الالكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة، حيث أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريقة الغير المشروعة ممكنة عبر قنوات شبكة الانترنيت.[4]

كما ظهرت جريمة القمار وغسيل الأموال عبر الانترنيت بظهور الكازينوهات الافتراضية أو أندية القمار الافتراضية التي أصبحت فيما بعد مسرحا كذلك لجريمة غسيل الأموال، حيث

---

[1] محمد أمين الشوايكة ،مرجع سابق ، ص48

[2] كريستاسكولمان: **عن جرائم الانترنيت طبعتها وخصائصها**، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية 19 و20 يونيو 2007، ص: 40.

[3] عمرو عيسى الفقي: **الجرائم المعلوماتية، جرائم الحاسب الآلي والانترنيت في مصر والدول العربية** ،المكتب العربي الحديث، الاسكندرية 2006، ص: 102.

[4] خالد ممدوح إبراهيم: **أمن الجريمة الالكترونية**، الدار الجامعية، الاسكندرية،2010، ص: 76 وما بعدها

ساعدت الشبكة العنكبوتية في انتشارها وتطورها بنقل هذه الجريمة من دولة إلى دولة أخرى لاستثمارها في مجالات مشروعة .[1]

ومن أهم الجرائم الالكترونية على الأموال ، نذكر جريمة المخدرات على الانترنيت حيث تتخذ المواقع الالكترونية للترويج للمخدرات وتسويقها للناشئ لاستخدامها، وتعليمه كيفية صناعتها بكافة أصنافها وأنواعها.[2]

الفرع الثالث: الجرائم الواقعة على أمن الدولة:

تعد هذه الجرائم من أخطر الجرائم الالكترونية خاصة الارهاب المعلوماتي والجريمة المنظمة المعلوماتية، حيث أتاحت الانترنيت للكثير من المنظمات الارهابية الترويج لأفكارها ومعتقداتها ،وأدت إلى ظهور جريمة أخرى أخطر منها وهي جريمة التجسس الالكتروني على الدول بالإطلاع على مختلف الأسرار العسكرية والاقتصادية بين الدول المتصارعة، كما تعطى الشبكة العنكبوتية فرصا للتأثير على المعتقدات الدينية وتقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة والمساس بأمنها الداخلي وبنظامها العام .[3]

الفرع الرابع: الترويج أو تسهيل تعاطي أو توزيع المخدرات أو المؤثرات العقلية

التعاطي للمخدرات والمؤثرات العقلية هو في حد ذاته جريمة يعاقب عليها القانون في المملكة العربية السعودية، لكن استخدام وسائل التواصل الاجتماعي للترويج أو تيسير تعاطيها يعتبر أيضا جريمة تستوجب الملاحقة القانونية اقترانا مع الجريمة الرئيسية.

هذا وتشير التقارير من حين لآخر إلى محاكمات لمستخدمي وسائل التواصل الاجتماعي عقب اعتقالهم من قبل سلطات مكافحة المخدرات بتهمة ارتكاب هذا النوع من الجرائم المعلوماتية.

---

[1] صالحة العمري: **جريمة غسل الأموال وطرق مكافحتها–**،مجلة الاجتهاد القضائي، العدد الخامس، مخبر اثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة، ص: 179..

[2] محمد صالح الألفي: **أنماط جرائم الانترنت** ، تم الاطلاع عليه بتاريخ 2019/08/02 متوفر على الموقعwww.eastlaws.com

[3] سامي علي عياد حامد: **الجريمة المعلوماتية وإجرام الانترنيت**، دار الفكر الجامعي ،الاسكندرية، 2007، ص: 77.

وفي إحدى الحالات الحديثة العهد، تم اعتقال أحد مستخدمي الشبكة المعلوماتية لنشره محتويات تروج وتيسر التعاطي للمخدرات[1].

[1] الجرائم المعلوماتية لمستخدمي وسائل التواصل الاجتماعي في السعودية تم الاطلاع عليه بتاريخ 2019/08/10 عبر الموقع الالكتروني:
https://www.wajeh.co/%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9-%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9/

خلاصة

أن التطور العالمي ودخول التقنية الالكترونية والشبكة العالمية (الانترنيت) والحاسوب الالي والخدمات المرتبطة به في حياة الناس قرب من المسافات البعيدة وجعل العالم قرية صغيرة وإمكانية التواصل في ظل وسائل الاتصال الحديثة والبث الرقمي فائق الجودة ووسائل التواصل الاجتماعي (فيس بوك، تويتر، تانغو، جات، فايبر،....) وهذا مما ساعد حركة الانتشار الاجتماعي عالمياً مما أدى والى تمادي المتطفلين والمجرمين واصحاب النيات السيئة والمغرضة من المباشرة في استخدام هذه التقنية الالكترونية بالاعتداء بجرائم الكترونية منها(جرائم التهديد والاحتيال وجرائم الابتزاز المالي وجرائم التشهير والمقامرة والاستغلال الجنسي، والجرائم المتعلقة بالصور الفاضحة أو الاعتداء على حرية الحياة الخاصة، أو تطفل أو ازعاج أو الدخول عمداً بدون تصريح أو اعتراض دون وجه حق ما هو مرسل أو استخدم عبارات أو صور أو أصوات أو أية وسيلة أخرى تنطوي على القذف والسب،.....) باستخدام تقنية اجهزة الحاسوب وشبكة المعلومات أو سائل التواصل الاجتماعي وهي تتعدى بأثارها القانونية والشرعية الى اثارها الاجتماعية والمادية والمعنوية والنفسية على حياة وحقوق وحريات المواطنين.

الفصل الثالث

الاجهزة الامنية المكلفة بمحاربة الجريمة الالكترونية

المبحث الأول:

نشأة وتطور الاجهزة المنية في الجزائر.

المبحث الثاني:

الآليات المسخرة لمكافحة الجريمة الالكترونية

الفصل الثالث: الأجهزة الأمنية المكلفة بمحاربة الجريمة الالكترونية

تمهيد

بالرغم من ما للثورة المعلوماتية من ايجابياتها وقدرتها على تغيير أوجه الحياة إلى الأحسن والأفضل، إلا أن هذه الثورة المعلوماتية ذاتها تحمل في طياتها أيضا العديد من السلبيات التي تتمثل في الاستخدام غير المشروع لنظم الحاسوب الآلي، ومن هذا المنطلق استطاع الجناة تطوير طرق الإجرام على نحو عال من التقنية في بيئة تكنولوجيا المعلومات.

وفي ظل تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، استدعى الأمر تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي، فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي، أما على المستوى الوطني، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات بموجب القانون 15/04 باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من (394 مكرر) إلى (394 مكرر7)، وكذلك تقررت عقوبات للاعتداء على أنظمة المعلومات في قانون حماية حقوق المؤلف رقم 05/03، كما تقررت عقوبات للاعتداء على أنظمة المعلومات في إطار نفس القانونين، كذلك إضافة إلى الإجراءات المتبعة في التحري في مجال الجرائم المعلوماتية؛ تم استحدث إجراءات تحري خاصة بموجب المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري وما بعدها؛ كذلك كرس المشرع الجزائري من خلال القانون رقم 04/09 قواعد تحري وحجز وتحقيق خاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

المبحث الأول: نشأة وتطور الأجهزة الأمنية الجزائرية

المطلب الأول: الضبطية القضائية

المطلب الثاني: إختصاصات وصلاحيات الضبطية القضائية

المبحث الثاني: الاليات المسخرة لمكافحة الجريمة المعلوماتية

المطلب الأول: القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية

المطلب الثاني: قانون الإجراءات الجزائية الجزائري .

المطلب الثالث: القوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية

المبحث الأول" نشأة وتطور الأجهزة الأمنية الجزائرية

لا شك أنّ القانون الجزائي الإجرائي باعتباره إحدى فروع القانون الجزائي يهدف إلى الموازنة بين تحقيق الفعالية في مكافحة الجريمة بما يمنحه من سلطات واسعة للأجهزة المكلفة بذلك، و بين حماية حقوق الإنسان و ما ينبثق عنها من حقوق و حريات، من خلال الضمانات الإجرائية التي تقيد تلك الأجهزة.

و هذا الطرح يجد أهميته بالنسبة لكامل مراحل الإجراءات الجزائية، لكنه أكثر أهمية بصدد مرحلة التحريات التي تناط بجهاز الضبطية القضائية، ذلك أنه بوقوع الجريمة و نشأة حق الدولة في إيقاع العقاب على مرتكبيها تكون الضبطية القضائية أول المتدخلين للبحث و التحري عن الجريمة والمجرمين.

و قد عُني قانون الإجراءات الجزائية بتحديد أحكام الضبط القضائي في المواد 12 إلى 28 و 42 إلى 55 و 63 إلى 65 منه و تشمل الضبطية القضائية طبقا لهذه المواد ضباط الشرطة القضائية و أعوانهم، و بعض الموظفين المنوطة بهم بعض مهام الشرطة القضائية و يقوم بمهمة الضبط القضائي أيضا الولاة الذين خول لهم المشرع بعض الصلاحيات في مجال الضبط القضائي بصفة استثنائية و في حالات خاصة فبالنسبة الضباط الشرطة القضائية و أعوانهم.[1]

المطلب الأول: الضبطية القضائية

قبل تعريف الضبط القضائي يجب التفريق بين الضبط الإداري والضبط القضائي فالدولة تحرص على سيادة حكم القانون وعدم الإخلال به الذي يتخذ أشبه صورة في الجريمة ويقوم بهذا العبء رجال الضبط الإداري الذين يعملون على ضبط الجريمة قبل وقوعها باتخاذ تدابير الوقاية واحتياطات الأمن العام فإذا وقعت الجريمة بالرغم من ذلك إجتهدت الدولة في البحث عن الجاني تمهيدا لعقابه ويتم ذلك بواسطة رجال الضبط القضائي ، لكن كلا

[1] فقد تولى قانون الإجراءات الجزائية تعدادهم حصرا في المواد 15 و 19 منه، أما بالنسبة للموظفين و الأعوان المكلفين ببعض مهام الضبط القضائي فقد ذكر قانون الإجراءات الجزائية البعض منهم في نص المادة 21 و أشار إلى الآخرين بصفة إجمالية و بدون تحديد في المادة 27 منه و يمكن أن نذكر منهم أعوان الجمارك، مفتشو العمل، موظفو إدارة التجارة و قمع الغش... إلاّ أن هؤلاء الموظفون يباشرون فقط بعض أعمال الشرطة القضائية المحددة بتلك القوانين لهذا يصفهم بعض فقهاء القانون بذوي الاختصاص الخاص، بالمقارنة مع الاختصاص العام للشرطة القضائية في البحث و التحري عن الجرائم بوسقيعة أحسن: **الوجيز في القانون الخاص**، الجزء الأول، دار هومة، طبعة 2002، ص243

الوظيفتين مرتبطتين فيما بينهما ويهدفان سويا إلى مكافحة الجريمة والتأكيد على إحترام القانون فضلا على أن الكثير من رجال الضبط الإداري يختارون الضبط القضائي فيسهرون على حماية الأمن العام

والسعي في جمع الأدلة عقب وقوع الجريمة ويختلف التحقيق الإبتدائي عن جمع الإستدلالات في أن للأول شروط معينة تكفل ضمانات منها وجود كاتب ضبط يحرر التحقيق وتحليف المجني عليه والشهود واليمين وحضور محامي المتهم وتنبيه المتهم إلى حقه في أن لا يجيب.[1]

أعضاء الضبطية القضائية:

نصت عليهم المادة 14 ق.إ.ج حيث أن الضبط القضائي يشمل:

1-مأمور الضبط القضائي

2-أعوان الضبط القضائي

3-الموظفين والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي .

نصت المادة 19 من نفس القانون على أعوان الضبط القضائي فحددتهم:"يعد من أعوان الضبط القضائي موظفوا إدارة الشرطة العاملين وذوي الرتب في الدرك الوطني ليست لهم صفة مأموري الضبط القضائي وأعوان وحراس البلديات" كما نصت المادة21 من نفس القانون على الموظفين والأعوان المكلفين ببعض مهام الضبط القضائي.أما المادة15 فقد حددت من هم مأموري الضبط القضائي.

المطلب الثاني: إختصاصات وصلاحيات الضبطية القضائية

الفرع الأول : الإختصاصات:

1/الإختصاص الإقليمي: تنص المادة 16 على أن يكون لمأمور الضبط القضائي إختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة إلا أن لهم في حالة الإستعجال أن يباشروا مهمتهم في كل دائرة إختصاص المجلس الملحقين به ولهم أيضا مباشرة مهمتم في كل أراضي الجمهورية إذا طلب منهم آداء ذلك أحد رجال القضاء المختصين قانونا،أي أن الأصل أن يتحدد الإختصاص في الحدود التي يباشر فيها المأمور وظيفته المعتادة وأن الإستثناء هو الخروج على هذا الأصل في حالة الإستعجال ويقاس

[1] بوسقيعة أحسن: **المرجع السابق**، ص243.

عليها حالة الضرورة ،كما يسمح بمخالفة ذلك في حالة وجود ضرورة لمطاردة المتهم اي تجاوز الإختصاص المكاني لمأمور الضبط القضائي الذي يطارد

2/الإختصاص الشخصي: ويتحدد بما تفرضه الوظيفة العامة على شخص معين بالذات من إختصاصات محدودة وبالتالي لا يجوز له التفويض إلا في الحالات المحددة في القانون.

3/الإختصاص النوعي: ويقصد به الإختصاص الموضوعي أي يتحدد الإختصاص بنوع معين من الجرائم دون سواه كإختصاص رجال شرطة المخذرات في ضبط المحاضر المتعلقة بإحرازها أو تداولها أو الإتجار فيها.

4/الإختصاص الزمني: يتحدد بوقت معين يجب إتخاذ الإجراء خلاله وإلا بطل كتحديد التفتيش في أحوال التلبس بالنسبة للمساكن ما بين الخامسة صباحا و الثامنة مساءا المادة47.

الفرع الثاني : سلطات وصلاحيات مأمور الضبط القضائي وأعوانهم:

1/تلقي البلاغات والشكاوى:المادة17 الواجب على مأمورى الضبط القضائي هو قبول وتلقي التبليغات والشكاوى التي ترد عليهم بشأن الجرائم وإرسالها فورا إلى النيابة العامة والتبليغ هو مجرد إيصال خبر الجريمة للسلطات العامة سواء من مجهول أو معلوم شفهيا أوكتابيا وهو حق مقرر لكل إنسان مجنيا عليه أم غير مجني عليه وهذا التبليغ غير الشكوى التي تقدم من المجني عليه وحده ويتخذ مأموري الضبط القضائي عدة إجراءات للتمكن من جمع الإستدلالات عن الجرائم في غير حالة التلبس وإجراءات الإستدلال يصح أن تكون قبل ظهور الجريمة أو بعد ظهورها بالفعل هذه الإجراءات لا تتجه حتما إلى شخص معين بالذات فتتميز عن إجراءات التحقيق في كونها تكون بعد ظهور الجريمة ويتجه فيها التحقيق إلى متهم دون سواه وتقوم إجراءات الإستدلال على[1]:

1-جمع الإيضاحات عن الجريمة من المبلغ والشهود بعد التوصل إليهم.

2-سماع أقوال المتهمين والتحري عنهم بجمع المعلومات ممن يعلم عنها.

3-الإنتقال إلى مكان الجريمة للمعاينة والبحث عن آثار الجريمة فيها والمحافظة عليها .

4-ضبط المنقولات المختلفة بعيدا عن المنازل وعن حيازة أصحابها بلا تفتيش عنها.

5-ندب أحد الخبراء لفحص الأشياء المضبوطة أو في مكان الجريمة إذا خيف ضياعها.

[1] أحمد الشلقاني: **مبادئ الإجراءات الجزائية في التشريع الجزائري**، ديوان المطبوعات الجامعية، 1999، ص 88

2/جمع الإستدلالات: يقصد بها كل ما من شأنه إثبات التهمة على المتهم ولو لم تكن الجريمة في حالة تلبس وبلا إستئذان سلطة التحقيق وقد تكون هذه المرحلة قبل ظهور الجريمة أو بعدها ولا تتطلب حتما إتجاه الشبهات نحو شخص معين وإتخاذ الإجراءات السابق ذكرها كرفع البصمات وتقصي الأثر... وتنهي مهمة جمع الإستدلالات بمجرد البدء في التحقيق مالم يفوض المأمور من سلطة التحقيق في مهمة واحدة .

3/تحرير محضر الإستدلال: نصت على ذلك المادة18 وعلى المأمور أن يثبت في محضره كل إجراء إتخذه كما يجب عليه إثبات صفته القضائية وطريقة كشفه للجريمة ويتضمن المحضر توقيع كل من سأل فيه أيا كانت صفته وترسل إلى النيابة العامة وكيل الدولة المختص مع الأوراق والأشياء المضبوطة ويمكن طلب مساعدة مأمور الضبط القضائي لتسهيل المهمة.أما أعوان الضبط القضائي فمهمتم مساعدة مأموري الضبط القضائي في ممارسة إختصاصاتهم السابقة وجمع المعلومات للكشف عن الجرائم،كما يخول للوالي عند وقوع الجريمة أو جنحة ضد أمن الدولة أو عند الإستعجال إذا لم يكن وصل إلى علم السلطة القضائية حيث يقوم الوالي بنفسه باتخاذ جميع الإجراءات الضرورية لاثباتها ويخبر وكيل الدولة بهذه الإجراءات خلال48 ساعة من هذه الإجراءات.[1]

الفرع الثالث: اجراءات البحث والتحري في الجريمة الالكترونية

أولا: إشكاليات التفتيش وما في حكمه في البيئة المعلوماتية

قد يتطلب الأمر في كثير من الأحيان ولوج البيئة المعلوماتية بحثاً عن الدليل وكشف مرتكبي هذه الطائفة من الجرائم وتعقبهم . ومع ذلك ، فإن التفتيش وما في حكمه في نطاق هذه البيئة يُنظر إليه في كثير من الأحيان على أنه غير مجدٍ لما يكتنفه من صعوبات أثناء تنفيذه ، وبالذات ما يتم في الفضاء الافتراضي (في بيئة الإنترنت) مقارنة بالجرائم التقليدية.

وفيما يخص محل التفتيش وما في حكمه في البيئة المعلوماتية ، فهو قد يرد على المكونات المادية للحاسب الآلي وملحقاته ، وهذه لا خلاف يُذكر حول خضوعها للتفتيش والضبط طبقاً لقواعد قانون الإجراءات الجنائية ، بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية ، وذلك تبعاً للمكان أو الحيز الموجودة فيه.

[1] أحمد الشلقاني: مرجع سابق، ص 89

ومن ثم ، إذا كانت موجودة بمسكن المتهم أو أحد ملحقاته فتحكمها القواعد ذاتها التي يخضع لها تفتيش المسكن ؛ إذ يجوز تفتيشها وضبطها متى كان تفتيش المسكن جائزاً ، والعكس صحيح .

في حين أنه إذا كان الحاسب في حوزة شخص خارج مسكنه ، فإن تفتيشه عندئذٍ يخضع للقواعد ذاتها التي يخضع لها تفتيش الشخص بوصفه أحد متعلقاته ، يستوي أن يكون الحائز هو مالك الجهاز أم سواه .

ومن ناحية أخرى ، وهو الأهم الذي يعنينا بالذات ، أن التفتيش وما في حكمه قد يرد على الجانب المنطقي للحاسوب ، المتمثل في المعلومات والبيانات المعالجة إلكترونياً ، وهي محل جدل كبير حول صلاحيتها لأن تكون موضوعاً للتفتيش والضبط من عدمها[1]. فثمة اتجاه يرى أن هذه المكوّنات المنطقية لا تصلح بطبيعتها لأن تكون كذلك، على اعتبار أن التفتيش يهدف في المقام الأول إلى ضبط أدلة مادية ، وهذا يستلزم وجود أحكام خاصة تكون أكثر ملاءمة لهذه البيانات اللامحسوسة.

وفي المقابل ، انبرى اتجاه آخر مؤدّاه أن المكونات المعنوية لا تختلف عن الكيان المادي للحاسب الآلي من حيث خضوعها لأحكام التفتيش وما في حكمه ، بدعوى أن البيانات، التي هي عبارة عن نبضات إلكترونية ، قابلة للتخزين على أوعية أو وسائط مادية كالأشرطة الممغنطة والأقراص والأسطوانات ، كذلك يمكن تقديرها وقياسها بوحدات قياس خاصة معروفة، وعلى هذا الأساس تكون صالحة كموضوع للضبط والتفتيش شأنها شأن الوسائط المادية ذاتها

وبتقديرنا ، فإن الاتجاه الأول أكثر منطقية ؛ ذلك أن القواعد التي تحكم التفتيش والضبط إنما وُضِعت في زمن مبكر وقبل ظهور الحاسوب وتطبيقاته ، وأياً كانت المبررات التي ساقها معتنقو المساواة بين الكيان المادي والمنطقي ، فإن طبيعة البيانات المعالجة تتطلب قواعد خاصة تحكمها بدلاً من محاولة تطويع القواعد التقليدية وتوسيع نطاقها ، وهذا يتأتّى من خلال إجراء تعديل عليها من شأنه توسيع نطاق الأشياء التي تكون مشمولة بالتفتيش والضبط وتضمينها من الأحكام بما يتلاءم ومتطلبات هذه التقنية الجديدة . فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا ينبغي إعمالها بشأنها مباشرة ، باعتبار أن

[1] أسامة المناعسة وآخرون ، المرجع السابق، ص278

هذه النصوص تمثل قيداً على الحرية الفردية ، ومن ثَم يصبح القياس على الأشياء المادية محظوراً لمنافاته الشرعية الإجرائية

وباستقراء موقف التشريعات الحديثة نجدها قد ذهبت إلى تأكيد هذا الاتجاه ، بحيث أضحت المكونات المعنوية للحاسب الآلي ضمن الأشياء التي تصلح أن تكون محلاً للتفتيش والضبط . ففي التشريع الأمريكي على سبيل المثال تقضي المادة (34) من القواعد الفيدرالية الخاصة بالإجراءات الجنائية الصادرة سنة 1970 بعد تعديلها بمد نطاق التفتيش ليشمل ضمن ما يشمل أجهزة الحاسب الآلي وأوعية التخزين والبريد الإلكتروني والصوتي والمنقول عن طريق الفاكس . فضلاً عن أن الاتفاقية الأوروبية للجريمة الافتراضية (اتفاقية بودابست) تقضي في المادة (19) منها بإلزام الدول الأطراف في هذه الاتفاقية بضرورة تبني التدابير والإجراءات التشريعية التي تخول السلطات المختصة ولوج البيئة المعلوماتية ، وذلك من أجل تيسير إثبات هذه الجرائم . [1]

ومع هذا ، نلاحظ أن بعض أحكام القضاء المقارن قد تبنت التفسير الموسع لمدلول الأشياء محل الضبط والتفتيش ، بحيث ينسحب على بيانات الحاسب الآلي حتى في غياب نصوص خاصة تحكم هذه المسألة . وهو اتجاه نرى أنه محل نظر ، ولا يمكن التسليم به في ضوء الاعتبارات سالفة الذكر .

ولكن ، ماذا لو كان النظام المعلوماتي مزوداً بنظام حماية يمنع من ولوجه دون تدخل القائم على هذه المنظومة ومساعدته ؟ فهل يا ترى يجوز إجبار المتهم مثلاً على تزويد السلطات المختصة بالتحقيق بمفاتيح المرور إلى النظام المعلوماتي ؟ أو بالأحرى هل يمكن إكراهه على الإفصاح عن كلمة السر وما في حكمها من أجل تسهيل الولوج إلى البيئة المعلوماتية ؟

هنا تباينت الآراء بصدد هذه المسألة ، فثمة رأي يرفض إجبار المتهم على تقديم المعلومات اللازمة لتسهيل ولوج النظام المعلوماتي . والحجة التي يستند إليها هذا الرأي تتجسد في قاعدة معروفة ومستقرة أن المتهم لا يجوز إجباره على الإجابة عن الأسئلة التي من شأنها أن تفضي إلى إدانته ؛ إذ من حقه الاعتصام بالصمت دون أن يُفسَّر ذلك الصمت ضد مصلحته .

[1] هشام فريد رستم ، **قانون العقوبات ومخاطر تقنية المعلومات** ، مكتبة الآلات الكاتبة ، أسيوط ،طبعة 1995 ، ص64

وهذا الاتجاه اعتنقته بعض التشريعات الحديثة ، ومنها القانون الياباني الذي يحظر على الأجهزة المختصة إكراه مالك الحاسب الآلي على الإفصاح عن كلمة المرور أو السر Password ، والنهج ذاته كان قد تبناه مشروع قانون الإجراءات الجنائية البولندي .

وفي المقابل ، ذهب رأي آخر إلى القول بأنه ، وإن كان لا يجوز إجبار الشخص على الإدلاء بأقواله ضد نفسه ، بيد أن ذلك لا ينبغي أن يكون حائلاً دون إجباره على تقديم معلومات يقتضيها ولوج النظام المعلوماتي للسلطات المختصة ، متى كانت هذه المعلومات بحوزته ، قياساً على إجبار الشخص على تسليم مفتاح الخزنة الذي بحوزته[1].

ولكن هذا الرأي الأخير أياً كانت المبررات التي يقوم عليها ، لا يمكن القبول به ، فقياس المعلومة التي بحوزة المتهم على مفتاح الخزنة وما في حكمه قياس مع الفارق . ذلك أن المعلومة (المتمثلة في كلمة السّر وما في حكمها) هي أمر معنوي بخلاف المفتاح الذي هو شيء مادي محسوس قابل للتسليم . هذا من ناحية ، ومن ناحية أخرى فإن هذا الرأي الأخير لا يتفق مع الأصول المستقرة في الإثبات الجنائي ، ويتنافى مع مقتضيات حق الدفاع أمام القضاء الجنائي . ومن ناحية ثالثة ، وحتى على فرض التسليم بجواز إكراه المتهم أو المشتبه به على تقديم مفاتيح الشفرة التي تمكّن من ولوج النظام المعلوماتي ، فإن الأمر تكتنفه صعوبات عملية لا يمكن التغلب عليها ، لعل أبرزها أن المتهم يستطيع التذرع بنسيان المعلومة أو عدم إمكان تذكرها أو ما شابه ذلك .

وهذا يعني ببساطة أن الرأي الأول أدعى إلى القبول ، ولكن ليس على إطلاقه ؛ إذ يجوز إجبار غير المتهم على تقديم المعلومة التي من شأنها تيسير الدخول إلى المنظومة كمقدم الخدمة مثلاً ، وذلك بحمله على الإفصاح عن كلمة السر التي بحوزته للوصول إلى المصدر أو شبكة الاتصالات ؛ لأن الإكراه الواقع على غير المتهم لا يمس حقوق الدفاع خلافاً للوضع بالنسبة للمتهم .

قد يكون حاسب المتهم متصلاً بغيره من الحواسيب عبر شبكة ، وهنا ينبغي التمييز بين ما إذا كان حاسوب المتهم متصلاً بآخر داخل إقليم الدولة أو كان متصلاً بحاسوب يقع في نطاق إقليم دولة أخرى.

---

[1] علي عبد الله القهوجي، **الحماية الجنائية لبرامج الحاسب الآلي**، الدار الجامعية للطباعة والنشر، بيروت، 1999، ص7.

1. في حالة ما يكون حاسوب المتهم متصلاً بجهاز آخر داخل إقليم الدولة : فهل يمتد التفتيش إلى الأجهزة الأخرى المتصلة بجهاز المتهم أو المشتبه فيه ، أم يقصر على جهازه فقط ؟

بالرجوع إلى القواعد العامة للتفتيش في قانون الإجراءات الجنائية الليبي ، نجدها تقضي بأن تفتيش غير المتهمين أو تفتيش منازل غير المتهمين لا يجوز إجراؤه من النيابة العامة إلاّ بعد الحصول على إذن من القاضي الجزئي. هذا إذا كان التحقيق يباشر من قِبلها ، أما إذا كان الذي يباشره قاضي التحقيق نفسه، فلا يستلزم حصول هذا الإذن . وبناءً على ذلك ، فإذا كان الحاسوب موجوداً بمنزل غير المتهم فلا يجوز تفتيشه من قِبل النيابة العامة إلاّ بعد استصدار إذن من القاضي الجزئي قبل ولوجه ، وإلاّ كان الإجراء باطلاً وغير مثمر .

غير أن صدور الإذن قد يستغرق بعض الوقت ، ما قد يؤدي إلى تلاشي الدليل واندثاره بالمحو والإتلاف ، وهذا ربما يعيق الوصول إلى الدليل وتحصيله .[1].

فالجاني . كما تقدم . قد يحاول العبث بالدليل كي لا ينكشف أمره قبل صدور الإذن ، لاسيما وأنه يستلزم تحديد محل الإذن بدقة حتى يتسنى تنفيذه ، وهذا دون شك ينطوي على شيء من العنت والصعوبة سواء بالنسبة للنادب (مصدر الإذن) أو الجهة المنفذة للإذن ، سيما إذا أخذنا في الاعتبار أن هذه الأجهزة تفتقر إلى الخبرة اللازمة في هذا المجال الفني .

ولهذا رُئي . بحق . ضرورة معالجة هذه المشكلة بنص خاص يقضي بتوسيع سلطات الجهة المعنية بإجراء التفتيش ، ولو استلزم الأمر ولوج النظام المعلوماتي دون الحصول على إذن عند الضرورة ، إذا كان من شأن انتظار صدور الإذن أن يفوت فرصة الحصول على الدليل .

وقد تبنت بعض التشريعات المقارنة هذا الاتجاه ، ومنها قانون تحقيق الجنايات البلجيكي الصادر في 23 نوفمبر 2000 ، الذي يجيز امتداد التفتيش إلى نظام معلوماتي آخر غير مكان البحث الأصلي ، ولكن ليس بصورة مطلقة وإنما بقيود معينة ، يمكن

---

[1]. هلالي عبداللاه أحمد ، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي** . دراسة مقارنة ، الطبعة الأولى ، دار النهضة العربية . القاهرة ، 1997 ، ص77

إجمالها في أن تكون ثمة ضرورة لكشف الحقيقة فيما يخص الجريمة موضوع البحث أو أن تكون الأدلة معرضة لمخاطر معينة كالإتلاف أو التدمير وما شابه .

كذلك ، تقر الاتفاقية الأوروبية للجرائم المعلوماتية ذلك متى كانت المعلومات المخزنة بحاسوب غير المتهم يتم الدخول إليها من خلال الحاسب الأصلي محل التفتيش.

وفي الولايات المتحدة الأمريكية تجيز المادة (a) 41 من قانون الإجراءات الجنائية الفيدرالي الأمريكي لقاضي التحقيق إصدار إذن تفتيش ملكية داخل منطقة أو خارجها ، متى كانت الملكية عند طلب الإذن موجودة داخل المنطقة ، ولكن يخشى أو يتوقع تحركها خارج المنطقة قبل تنفيذ الإذن ، وربما المشكلة التي تواجه رجال الضبط عند تنفيذهم التفتيش أنه لا يكون باستطاعتهم التحقق من أن البيانات المضبوطة جرى تخزينها داخل المنطقة أم خارجها.

2. في حالة اتصال حاسوب المتهم بآخر موجود بإقليم دولة أخرى : قد تكون البيانات غير المشروعة جرى تخزينها في حاسوب خارج إقليم الدولة . وكثيراً ما يتم اللجوء إلى هذا الأسلوب من قِبل الجناة المحترفين بغية إعاقة الوصول إلى الدليل .

وقد تباينت الاتجاهات حول مدى امتداد التفتيش للحواسيب الأخرى خارج الدولة[1]. فذهب رأي إلى رفض امتداد التفتيش للحواسيب المتصلة بحاسوب المتهم خارج الدولة ، بدعوى أن ذلك ينطوي على انتهاك لسيادة دولة أخرى ، أو بالأحرى يشكّل اعتداءً على ولاية الدولة التي يجري التفتيش في نطاق إقليمها ، ومن ثَم فالأمر يتطلب لجوء سلطات التحقيق إلى سلوك الإجراءات المعتادة بطلب المساعدة القضائية أو الإنابة القضائية من السلطات الموازية في الدولة الأخرى .

بعبارة أخرى ، إن مباشرة هذا الإجراء تستلزم وجود اتفاقية (ثنائية أو متعددة الأطراف) وإلاّ يفقد مشروعيته . ولأجل مواجهة هذه المشكلة في نظر الفقه المقارن (الهولندي على سبيل المثال) ينبغي التماس طلب من سلطات الدولة الأخرى بنسخ البيانات المخزنة في الحواسيب الموجودة على أراضيها وإرسالها إلى الدولة الطالبة . غير أن هذا الأسلوب . المعروف بأسلوب التفويض والالتماس . يُعاب عليه أنه يفتقر إلى الفعالية نتيجة الإجراءات الروتينية التي تفضي إلى تأخير الوصول إلى الدليل وربما ضياعه أو إتلافه.

[1] هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي ، المرجع السابق، ص77

والاتجاه الرافض لامتداد التفتيش إلى الحواسيب الأخرى لا يقر هذا الإجراء إلاّ بموجب اتفاقية دولية ، وهو يعبر عن الرأي السائد في الفقه الألماني .

وسيراً في هذا الاتجاه ، عرضت على القضاء الألماني واقعة تتعلق بالغش المعلوماتي، حيث كانت طرفية الحاسب الموجودة بألمانيا متصلة بأخرى بسويسرا . وبالرغم من أن السلطات الألمانية (سلطات التحقيق) قد حاولت استرجاع البيانات المخزنة بالخارج ، إلاّ أنها لم تتمكن من ذلك إلاّ من خلال التماس المساعدة المتبادلة .

وفي المقابل ، يؤيد جانب آخر من الفقه أمر امتداد التفتيش إلى الحواسيب الموجودة خارج إقليم الدولة ، وهذا الرأي يقوم على أساس واقعي ؛ إذ إن معتنقيه والمدافعين عنه يحاولون التعامل بواقعية مع ما يعترض سلطات التحقيق من مشكلات . وهذا الاتجاه أخذ به القانون الفرنسي من خلال المادة (17) من قانون الأمن الداخلي الفرنسي . كما يسمح قانون التحقيق البلجيكي (مادة 88) لقاضي التحقيق الحصول على نسخة من البيانات التي هو في حاجة إليها دونما انتظار إذن من سلطات الدولة الأخرى ، ويحاول الفقه الفرنسي تبرير هذا الاتجاه بأن العالم الافتراضي لا يعرف الحدود ، ومع هذا فالفقه هناك يسلّم بأن النص المذكور يمثل انتهاكاً لسيادة الدول الأخرى .

كذلك تجيز المادة (32) من الاتفاقية الأوروبية للجرائم الافتراضية ولوج شبكة المعلومات التابعة لدولة أخرى لأجل التفتيش والضبط متى كان هذا الإجراء يتعلق بمعلومات أو بيانات مباحة للجمهور ، وأيضاً في حالة الحصول على رضا صاحب أو حائز هذه البيانات بالتفتيش[1].

في حين يتوقّف الأمر في الولايات المتحدة الأمريكية على وضع الشخص الذي ينفذ التفتيش، فإذا كان قبل مباشرته يعلم بأن البيانات والمعلومات المراد بحثها مخزنة بعيداً في نطاق دولة أخرى ، فعندئذٍ يستلزم التماس طلب مساعدة يتم توجيهه إلى سلطات الدولة الأخرى ، أما إذا كان القائم بالتفتيش يجهل أو ليس في وسعه معرفة أن البيانات المراد تفتيشها خارج المنطقة ، فإن ما يسفر عنه التفتيش من ضبط لا يهدر ، ويمكن قبوله والركون إليه في الإثبات بوصفه دليلاً مشروعاً متى ما اطمأنّت إليه المحكمة .

[1] . عكاشة محي الدين، **محاضرات في الملكية الأدبية**، ديوان المطبوعات الجامعية، الجزائر 2001، ص 48. .

والجدير بالذكر في هذا المقام أن المحاكم الأمريكية درجت على رفض دعاوى بطلان الدليل في حالة عدم استطاعة رجال الضبط معرفة ما إذا كان تنفيذ التفتيش يشكل انتهاكاً للمادة (41) قانوناً أو فعلياً ما لم يتعمد هؤلاء عدم إعمال القاعدة المذكورة ، أو أن يكون لديهم حدس مسبق[1].

هذا من ناحية ، ومن ناحية أخرى أن تنفيذ إذن التفتيش يثير بعض المشكلات في مجال الجرائم المعلوماتية في القانون المذكور ، ففي هذا القانون ثمة مبدأ يجب أن يلتزم به رجال الضبط القضائي ، ألا وهو ضرورة الإعلان عن وجودهم والإفصاح عن السلطات المخولة لهم (أو ما يُعرف بقاعدة الاستئذان والإعلان) . بيد أن هذه القاعدة العامة يمكن التحلل منها وعدم الالتزام بها على حد تعبير المحكمة الفيدرالية الأمريكية العليا متى كان مأمور الضبط القضائي قد توافر لديه شك مبرر في أن إعمال هذه القاعدة أو التقيد بها سيكون غير مجدٍ أو من شأنه إعاقة فعالية التحقيق ، أو من المتوقع أن تنجم عنه خطورة ما[2].

وهذا الاستثناء على قاعدة الاستئذان ينسحب بوجه خاص وفي كثير من الأحيان على تنفيذ إذن التفتيش في الجرائم المعلوماتية ما يسمح لرجال الضبط مباشرة ذلك دون استئذان تحسباً لما يمكن أن يقوم به الجناة (الهكرز) من تلاعب بالدليل ومحاولة العبث به متى تولد لديهم الشعور بأن أمرهم سينكشف .

ذلك أن المتهمين والمشتبه فيهم يلجأون في الغالب إلى تقنية المفاتيح الساخنة أو أسلوب تسخين الأسلاك Hot Wire من أجل إتلاف الدليل وتدميره قبل تمكن رجال الضبط من الوصول إليه. ولهذا ، فإن التمسك بالقاعدة سالفة الذكر ربما يحرم رجال الضبط من فرصة كشف الدليل .

وبناءً عليه ، فإن أمر تقدير المخاطر الناجمة عن التمسك بهذه القاعدة في القانون الأمريكي متروك لرجال الضبط القائمين بتنفيذ إذن التفتيش . فإذا توافر لديهم ما يبرر

---

[1] عمر بن يونس ، **الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي** "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية" ، الطبعة الأولى ، 2004 . 2005 ، ص201 . 204 .

[2] عمر بن يونس ،المرجع السابق، ص205 .

الخروج على هذه القاعدة يمكنهم عندئذٍ التماس الإذن من قاضي التحقيق بالسماح لهم بتنفيذ التفتيش أو الضبط دون حاجة للاستئذان أو الإعلان المسبق[1].

وللاعتبارات ذاتها يجوز تخويل دخول المكان خلسة دون إبلاغ الشخص الذي ستكون ممتلكاته محلاً للتفتيش المزمع مباشرته من قِبل المحكمة ذاتها . كما يخولها القانون منح الإذن بتأخير أو تأجيل الإعلام بالتفتيش كلما توافر سبب يبرر أن إخطار المالك يحتمل أن يكون له أثر سلبي ، مثل العبث بالدليل أو تعريض حياة الأفراد أو سلامتهم للخطر أو للإفلات من الاتهام أو تهديد أحد الشهود أو الإضرار بسير التحقيق أو تأخير المحاكمة[2].

وهذا الاستثناء تبرره الضرورة الإجرائية ، ومضمونه تغليب مصلحة التحقيق والوصول إلى الدليل على مصلحة الأفراد الذين يتقرر تفتيش ممتلكاتهم ، وهذه التضحية قد تكون مستساغة ومقبولة بشرط عدم التوسع في هذا الاستثناء من أجل الافتيات على الحرية الفردية وأن يكون تفسير الضرورات التي ألجأت مأمور الضبط إلى ذلك خاضعاً لمراقبة القضاء تفادياً لأي شطط أو تعسف من جانب رجال الضبط القضائي[3].

ثانيا: ضبط الاتصالات والمراسلات عبر شبكة الحاسب الآلي :

بموجب المادة 65 من قانون الإجراءات الجزائية فأنه يجوز لقاضي التحقيق أن يأمر ضابط الشرطة القضائية بترخيص كتابي، وتحت إشرافه مباشرة للقيام باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع الترتيبات التقنية دون موافقة الشخص المعني من أجل القيام بالتقاط وتثبيت وبث وتسجيل الكلام في سرية من طرف أي شخص وفي أي مكان عام أو خاص والتقاط الصور ولكل شخص .

فقد تضطر الشرطة القضائية لاستعمال كاميرات خفية أو أجهزة تصنت لكن يجب أن يكون ذلك في إطار احترام الشرعية الإجرائية حفاظا على كرامة الحياة الخاصة للإنسان كما يمكن لضابط الشرطة القضائية تصوير جسم ومكان الجريمة بشكلها العام في إطار ممارسة مهامهم، ولكن يمنع من الاطلاع أو تسجيل المكالمات أو الأحاديث الخاصة إلا بإذن مسبق

---

[1] نفس المرجع ، ص206 .

[2] نفس المرجع ، ص208 .

[3] عمر بن يونس ،المرجع السابق، ص210 . 215 .

من طرف السلطات القضائية وفق ما ينص عليه الدستور في مادته " 39 على انه لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون وسرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة." إن سير مفعول هذه المادة ليس مطلقا بل تدخل عليه بعض الاستثناءات عن طريق تشريع قواعد إجرائية تعمد على تقييد هذه الحرمة من اجل الحفاظ على المصلحة العامة للمجتمع و أمنه وسلامته و هذا لأجل حسن سير التحريات والتحقيقات حيث انه منح للشرطة القضائية حق اعتراض المراسلات التي تتم عن طريق / القضائية كل هذه القواعد نظمها القانون 06-22 وسائل الاتصال السلكية واللاسلكية ووضع ترتيبات تقنية دون موافقة المعنيين من اجل التقاط الصور وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن عامة أو خاصة[1] .

1- اعتراض المراسلات:لم ينص المشرع الجزائري ضمن قانون الإجراءات الجزائية على تعريف خاص محدد لعملية اعتراض المراسلات إلا انه حدد تنظيم سير العملية والإجراءات الخاصة بها في المواد من 65 مكرر 05 إلى 65 مكرر 10 من قانون الإجراءات الجزائية.

تعريف اعتراض المراسلات: يقصد باعتراض المراسلات التتبع السري والمتواصل للمشتبه به قبل وبعد ارتكابه للجريمة ثم القبض عليه متلبسا بها.

ويعرف على انه إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، وهي تعتبر أيضا وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية واجهة الإجرام الخطير وتتم عبر وسائل الاتصال السلكية واللاسلكية.

يقصد بالمراسلات قانونا هي جميع الخطابات المكتوبة سواء أرسلت بطريق البريد أو بواسطة رسول خاص، وكذلك المطبوعات والطرود والبرقيات التي توجد لدى مكاتب البريد أو البرق وسوي أن تكون داخل مظروف مغلق أو مفتوح كما تعد من قبل المرسلات الخطابات التي

[1] تسريات ميلود، محاضرة ألقيت بمجلس قضاء قالمة بعنوان :**أساليب البحث والتحري الخاصة وإجراءتها وفق قانون الإجراءات الجزائية والقانون 06-22 المعدل و المتتم له**، ص: 7-8

تكون في بطاقة مكشوفة متى كان واضحا أن المراسل قصد عدم اطلاع الغير عليها دون تمييز. [1]

التخابر والاتصال بين الأفراد فيما بينهم سواء بالكتابة أو غيرها أي سواء « إلا أن هناك من يرى أن المراسلات يقصد بها كانت رسائل بريدية أو مكالمات هاتفية والملاحظة أن المشرع الجزائري عندما تكلم على اعتراض المراسلات طبقا للمادة 65 مكرر 05 من ق.إ.ج فإنه حدد نوع المراسلات وهي تلك التي تتم بواسطة الاتصال السلكي واللاسلكي وأستبعد الوسائل البريدية أي الخطابات الخطية التي تتم عن طريق البريد، وذلك حرصا منه على ضمان حرية وسرية المراسلات بين الأفراد المكفولة دستوريا، وهذا من جهة، ومن جهة أخرى فان أفراد الشبكات والعصابات المنظمة كثيرا ما ينفذون خططهم الإجرامية باستعمال أدوات وتجهيزات متطورة.

لم يتطرق المشرع الجزائري إلى تحديد مفهوم اعتراض المراسلات فهل يقصد بها التصنت الهاتفي أم مجرد الاطلاع عليها ؟أو يمتد إلى أكثر من ذلك من خلال ضبط كل ما له علاقة بوسائل المواصلات السلكية واللاسلكية كالبرقيات، الفاكس، التلكس، الرسائل القصيرة للجهاز المحمول المواقع المفتوحة على شبكة الانترنيت ؟

وبالرجوع إلى المادة 08 فقر 11 من قانون 2000-03 المتعلق بالبريد والمواصلات السلكية واللاسلكية فكل مراسل أو إرسال أو استقبال علامات أو إشارات كتابات، صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي، إذا كان الحال كذلك فكل إشارة أو كتابة أو صورة أو صوت مهما كانت وسيلة الاتصال يصلح أن يكون محلا للاعتراض.

خصائص اعتراض المراسلات:يتضمن أسلوب اعتراض المراسلات خصائص معنية تساعد على تحديد مفهومه وطبيعة العمل به وتتمثل هذه الخصائص في:

اعتراض المراسلات يتم خلسة دون علم ورضا صاحب الشأن:اعتراض المراسلات إجراء يتم من دون رضا وعلم المشتبه وهو أهم خاصية فبعلم أصحاب الشأن تنتفي خاصية الاعتراض وهنا لا يمكننا القول أننا أمام أسلوب الاعتراض فهدا الأخير يمحو خصوصية الاعتراض ويزيل السرية.

[1] احمد فتحي سرور، **الوسيط في قانون الإجراءات الجزائية**، دار النهضة، ص9 :

اعتراض المراسلات إجراء يمس بحق الشخص في السرية:اعتراض المراسلات إجراء يمس بحق الإنسان في سرية حديثة [1]إلا أن إجراء اعتراض المراسلات ينتهك هده الحرمة ويستلق السمع على المكالمات السلكية كانت أو اللاسلكية، هذا الاستثناء وضعه المشرع الجزائري بغية السير الحسن للتحريات والتحقيقات

والحفاظ على الأمن العام. وهنا يعتبر اعتراض المراسلات إجراء يساعد دون شك الجهات القضائية والأمنية للوصول إلى أدلة ومعلومات كانت تعتبر شخصية ولا يمكن المساس بها ا تحت ذريعة الحريات الشخصية.

تستهدف عملية اعتراض المراسلات الحصول على دليل غير مادي:تعتبر تقنية التصنت على الأحاديث الهاتفية دليل غير مادي ينبعث من عناصر شخصية مما يصدر عن الغير من أقوال وأحاديث تقنع القاضي بطريقة غير مباشرة تفيد في الكشف عن الجريمة، فتعتبر الأحاديث دليل معنوي غير مادي، فهدف اعتراض

المراسلات هو التقاط الأدلة المعنوية بغية تأكيد أدلة الاجرام.[2]

تستخدم اعتراض المراسلات أجهزة قادرة على التقاط الأحاديث:مع مضي عهد استراق السمع من وراء الأبواب والنوافذ وتطور عهد التكنولوجيا الحديثة، أصبح من الضروري إيجاد تقنيات جديدة ذو فعالية كبيرة لاقتحام خصوصيات الأشخاص المشتبه بهم وخصوصا مع التطور الذي عرفته العمليات الإجرامية التي شكلت قلقا رهيبا في أوساط المجتمع لذا تستلزم عملية اعتراض المراسلات استخدام أجهزة ذو تقنية واسعة قادرة على التقاط الأحاديث الصوتية بدقة و جودة عالية ، إلا أن استعمال هذه الوسائل دون أية ضمانات تقيدها تشكل خطرا على حرية الأفراد فهي تتعارض أيضا مع أصول الديمقراطية .

حيث أن هذه الخصائص الأربعة تعد العناصر الأساسية لقيام عملية اعتراض المراسلات.[3]

3. تسجيل الأصوات:لم ينص المشرع الجزائري على تعريف التسجيل الصوتي، كما لم ينص على إجراء اعتراض المراسلات، وإنما أشار لها في المادة 65 مكرر 05 فقرة 02 من قانون

---

[1] رغم إن نص المادة 39 من الدستور تنص على حرية الحياة الخاصة وتحمي سرية المراسلات والاتصالات الخاصة دون أي قيود

[2] أحمد غاي، مرجع سابق، ص231

[3] ياسر الأمير الفاروق، مرجع سابق، ص165

الإجراءات الجزائية فيما يلي: وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية .

تعريف تسجيل الأصوات:يعرف تسجيل الأصوات بأنه النقل المباشر والآلي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمل من عيوب في النطق إلى شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه.

والتسجيل الصوتي المتخذ كوسيلة للتحري عن الجرائم يشمل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية.

حيث يهدف هذا الإجراء على متابعة المحادثة أو المكالمات الهاتفية ومعاينتها، فهو يعني من ناحية مراقبة المكالمات ومن ناحية أخرى التصنت عليها و يكفي مباشرة إحدى هاتين العمليتين لقيام عملية تسجيل الأصوات وقيام عملية تسجيل الأصوات معتمد على وضع رقابة على الهواتف ونقل الأحاديث وتسجيلها التي يتم عن طريقها أو بوضع مكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية التي يجريها ضباط الشرطة القضائية غرض الاستعانة به في التحري والبحث والإثبات الجنائي.

إلا أن هده الترتيبات التقنية لا تكون إلا بإذن من وكيل الجمهورية أو قاضي التحقيق حسب الحالة وتحت مراقبتها.[1]

وعليه فإن التسجيلات التي يقوم بها الأفراد فيما بينهم لا تعد من قبيل الإجراءات الجنائية نظرا لأنها لم تصدر في شأن دعوى

جنائية حركتها السلطات القضائية قصد الوصول إلى الحقيقة، كما لا يعتبر أدلة واستغلال التسجيل الذي لا يتضمن اعتداء على حق من تم تسجيل صوته أو حديثه، كما هو الحال في حالة تسجيل الأحاديث الإذاعية أو التلفزيونية أو الصحفية.

[1] مقني بن عمار بوراس عبد القادر، **التنصت على المكالمات الهاتفية و اعتراض المراسلات كآلية للوقاية من جرائم الفساد**، الملتقى الوطني حول الآليات القانونية لمكافحة الفساد، جامعة ورقلة، 8-9 ، 2008، ص 14

حيث تكون هده الترتيبات دون حاجة إلى موافقة المشتبه فيه، وذلك حتى نكون أمام جميع معالم الجريمة الكاملة وحتى لا يلجا المشتبه فيه إلى إخفاء الأدلة والحقائق وأثار الجريمة مما يعيق الوصول إلى الحقيقة والحصول على الاستدلالات اللازمة.

فتباشر هذه الوسائل خفية دون علم من تباشر عليه حيث أن الشخص محل استراق السمع عليه لا يعلم أن حديثه محل مراقبة لأنه لو علم دلك لما أفصح عما في مكنون نفسه وضميره، وفيما يخص مهمة تسجيل الأصوات والتقاط الصور داخل المحلات

السكنية وغيرها فلعناصر الضبطية القضائية إذن يخول لهم القيام بهذه الترتيبات التقنية من عملية تفتيش ودخول المنازل والمحلات من حيث التوقيت والرضا لمن لهم حق اعتراض هذه الأماكن.[1]

إلا أن تسجيل الأصوات يعتبر اعتداءا على حق الحياة الخاصة للأفراد ويتعارض مع مبادئ الدستور، وكذا مع قواعد الأعمال العامة فهي تعد انتهاكا لخصوصيات حياة الأفراد.

وحسب ما أتى به المشرع الجزائري في نص المادة 65 مكرر 8 من قانون الإجراءات الجزائية، انه يجوز لكل من وكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له أو قاضي التحقيق أو ضابط الشرطة القضائية الذي أنابه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات.

يجب أن يتضمن الإذن لمباشرة هذا الأسلوب شروط نصت عليها المادة 65 مكرر 7 و هي:

حيث يجب أن يكون الإذن مكتوبا متضمنا كل العناصر التي تسمح بالتعرف على الاتصالات المطلوبة التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير.

– ويحدد في الإذن المدة المطلوبة التي تتم خلالها الإجراءات اللازمة على أن لا تتجاوز المدة أربعة أشهر فيقوم ضابط الشرطة القضائية المكلف بتحرير محضرا عن الإجراء المطلوب القيام به بوصفه لنوع وطبيعة العملية المقيدة في إظهار الحقيقة وتاريخ وساعة

[1] المادة 65 مكرر 07 قانون الإجراءات الجزائية

بدايتها ونهايتها، حتى يودع هدا المحضر في ملف خاص مع إمكانية نسخ وترجمة المكالمات التي تتم بالغات الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهدا الغرض [1] .

وتجدر الإشارة أن المشرع الجزائري في الفترة الثانية من المادة 65 مكرر 05 من ق.إ.ج ، إعتبر طبيعة الكلام واتخذه كمعيار لإجراء عملية التصنت إذ أنه لم يولي الاهتمام لطبيعة المكان الذي يجرى فيه الحديث إذ انه سوى بين المكان العمومي والمكان الخاص فلا يهم طبيعة المكان بقدر ما يهم خصوصية الحديث وسريته، على خلاف التقاط الصور فإنه اتخذ طبيعة المكان كمعيار.

إن الحديث لا يفقد خصوصية حتى ولو تم في مكان عام ما دام أنه يتم بصوت يحرص صاحبه أن لا يسمعه إلا متلقيه، ومن ثم فهو لا يفقد الحماية الجنائية له، وعلى ذلك ما دام الحديث خاص فلا بد من إجراءات قانونية حتى و لو كان في مكان عمومي.

الطبيعة القانونية لتسجيل الأصوات:اختلفت الآراء حول الطبيعة القانونية لعملية تسجيل الأصوات، فاعتبرها البعض أن لها علاقة كبيرة بعملية التفتيش حيث يهدفان كلاهما للكشف عن الجريمة ، لكن أوجه الاختلاف بينهما جوهرية، فالغرض من التفتيش هو ضبط الأدلة المادية المتعلقة بالجريمة، أم الأحاديث الصوتية ليس لها كيان مادي يمكن ضبطه.

ويعتقد البعض الأخر إن عملية تسجيل الأصوات تنشا عن ضبط الرسائل التي تتضمن حديث كتابي وإن التسجيلات الصوتية تتضمن حديث شفوي، إلا أن هناك فرق واضح بين عملية ضبط الرسائل وتسجيل الأصوات، تكمن في كون ضبط الرسائل تعتبر أدلة مادية إلا إن التسجيلات الصوتية ليست بأدلة مادية ولا تقبل الضبط بالمعنى القانوني.

فالطبيعة القانونية للتسجيلات الصوتية تكمن في أنها إجراء من نوع خاص، فهي مستقلة عن عملية التفتيش وكذا عن ضبط الرسائل، وهذا ما أخذ به المشرع الجزائري في تقنينه لقانون الإجراءات الجزائية[2].

[1] المادة 65 مكرر9 –10 قانون الإجراءات الجزائية

[2] ياسر الأمير فاروق، مرجع سابق، ص182

المبحث الثاني: الاليات المسخرة لمكافحة الجريمة المعلوماتية

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 ترسنة 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 أولها المشرع الجزائري أهمية قصوى أمن الدولة والحفاظ على النظام العام. كما أنه ركز كل اهتماماته على حماية الدولة، وجعلها من أسمى أهدافه.[1]

حاول المشرع الجزائري ، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الإلكترونية، ويعود أسباب الاهتمام بتنظيم جرائم الانترنت من جهة تطور تكنولوجيا الإعلام أدى إلى اتساع 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 ضيف إلى ذلك المحافظة على مبدأ الشرعية الجنائية ، متكلا على تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحتها،وعليه خصصنا هذا المبحث إلى ،القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية(المطلب الأول)،القانون الإجراءات الجزائية(المطلب الثاني)،والقوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية(المطلب الثالث)

المطلب الأول: القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية:

قد أخص المشرع الجزائري تنظيم الجريمة الإلكترونية بقوانين عامة وأخرى خاصة، وعليه قسمنا المطلب الأول، الدستور(الفرع الأول)، القانون العقوبات(الفرع الثاني)،قانون الإجراءات الجزائية(الفرع الثالث)

[1] آمال قارة، **الحماية الجزائرية للمعلوماتية في التشريع الجزائري**، دار هومة للطباعة و النشر، الجزائر 2006، ص 66

الفرع الأول: الدستور الجزائري :

كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016[1]حماية 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 : 38 الحرّيّات الأساسيّة وحقوق الإنسان والمواطن مضمونة

لمادة :44 حرّيّة 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 .

الفرع الثاني: 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 2006 حيث مس هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة

[1]القانون رقم 16-01 المؤرخ في 6-03-2016 المعدل للدستور عدد الجريدة الرسمية 14 ا

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 لمشرع الجزائري قسما خاصا في القسم السابع مكرر من الفصل الثالث الخاص بالجنايات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات[1]وعلى هذا الأساس يمكن تصنيفها إلى مايلي:

1. الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات.
2. حذف أو تغيير لمعطيات المنظمة[2]
3. ادخال او تعديل في نظام المعطيات [3].
4. تصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار
5. حيازة أو إفشاء أو نشر أو استعمال المعطيات[4]
6. تكوين جمعية أشرار[5]

---

[1] القانون رقم04-15 المؤرخ في10 نوفمبر2004 ،المعدل والمتمم

[2] المادة 394 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"

[3] المادة394 مكرر " يعاقب بالحبس من ثلاثة اشهر الى سنة و بغرامة من خمسين ألف الى مائة ألف دينار كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الالية للمعطيات أو يحاول ذلك . تضاعف العقوبة اذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظمة . و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من06 اشهر الى سنتين وغرامة من خمسين ألف الى مائة و خمسون ألف دينار"

[4] 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

[5] المادة394 مكرر2 " يعاقب بالحبس من شهرين الى03 سنوات و بغرامة من1000.000 دج الى5000.000 دج كلمن يقوم عمدا و عن طريق الغش بما يلي :

تصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

من خلال المواد القانونية السابقة والتي تمثل الركن الشرعي للجريمة الإلكترونية في التشريع الجزائري يمكن تكييف هذه الأفعال المجرمة بأنها جرائم ضد أموال الغير والمضرة بالمجتمع وهي تعتبر من ضمن جرائم الاختلاس و خيانة الأمانة و النصب غير السرقة لاعتبار أن السرقة فعل الاستيلاء على مال الغير ماديا.

ثانيا:العقوبات المقررة لهذه الجرائم:

طبقا لقانون العقوبات وبناءا على للمواد 11،12و13 من الاتفاقية الدولية للإجرام ألمعلوماتي 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[1]

ب-العقوبات التكميلية:

المصادرة تشمل الأجهزة و البرامج و الوسائل المستخدمة في إرتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية. **و إغلاق المواقع** والأمر 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[2]

حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم

[1] المادة394 مكرر5 " كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".

[2] المواد القانونية السابقة،394مكرر،394مكرر1، 394مكرر2.

ت- 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** [1].

ث -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]

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 ممثه وبالتالي عقوبة الشخص المعنوي تتمثل في الغرامة التي تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي [3]. علما أن نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات تحدد المسؤولية الجزائية للشخص المعنوي والعقوبات امقررة.

-3 **عقوبة الاتفاق الجنائي:**تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5 [4]، 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.

---

[1] 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".

[2] المادة394 مكرر7 " يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها".

[3] 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".

[4] المادة394 مكرر4 " يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مراتالحد الأقصى المقرر للشخص الطبيعي"

المطلب الثاني: 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[1]

كما نص على التفتيش في المادة 45 الفقرة 7من نفس القانون[2]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 الفقرة 06 [3](وكذا على "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5/ 10[4].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

[1] المادة: 394مكرر5،السابق ذكرها

[2] 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 عدد 40.

[3] المادة 45 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 ص 6.

[4] المادة 51 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 2 ديسمبر2006،الجريدة الرسمية عدد84،ص7.

من أجل إلتقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة[1]

. أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية.

المطلب الثالث: القوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية:

تناولنا في هذا المطلب،القوانين الخاصة للتصدي للجرائم الإلكترونية (الفرع الأول)، والهياكل

الخاصة للتصدي للجرائم الإلكترونية(الفرع الثاني) كما يلي:

الفرع الأول: القوانين الخاصة للتصدي للجرائم الإلكترونية

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 المادة87 منه [2] ، كما نصت المادة2/ 84 منه على استعمال حوالات دفع عادية أو الكترونية أو برقية[3] ."كما نص في المادة 105منه على إحترام المراسلات" بينما أتت المادة 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن

---

[1] 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.

[2] ا لقانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل و يتمم الأمر رقم 155-66 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966. و المتضمن قانون الإجراءات الجنائية الجزائري. المادة 65 مكرر 3/5 "إذا أقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخذرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أوالإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف و كذا جرائم الفساد، يجوز لوكيل الجمهورية المختص بأن يأذن بما يأتي : – وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية."...

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

يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.

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.[1]

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، ومقدمو الخدمات، والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية.[2]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.

الفرع الثاني: 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

[1] المادة 6 مكرر1،والمادة 65مكرر1 من القانون رقم 08/01 المؤرخ في 2008/01/23والمعدل والمتمم لقانون 83/01المتعلق بالتامينات

[2] 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"

والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية،في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية الاقتصاد الوطني.[1]

ثانيا:الهيئات القضائية الجزائية المتخصصة: أنشئت بموجب القانون 14/04المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد329،37،و40 من ق.إ.ج.ج.تتمتع اختصاص إقليمي موسع طبقا للمرسوم التنفيدي رقم 348/06 المؤرخ في 2006/01/05.بحيث تنظر فيالقضايا 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.[2]

ثالث: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.[3]

رابعا:المديرية العامة للأمن الوطني: تتصدى هده المديرية للجريمة الإلكترونية من عدة جوانب ومنها 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.

---

[1] المواد من المادة الثانية حتى 14من قانون رقم04-09 المؤرخ في 2009/08/05 والمتعلق بالوقاية من الجرائم المتصلةبتكنولوجيا ألإعلام والإتصال ومكافحتها.

[2] القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السابق ذكره.

[3] هواري عياش، مداخلة حول **مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية** ،المعهد الوطني للأدلة الجنائية وعلم الإجرام ، جامعة بسكرة كلية الحقوق،2016،ص3

سجلت الفرق المختصة في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بالمديرية العامة للأمن، خلال السداسي الأول من السنة الجارية 742 جريمة إلكترونية، تورط في إرتكابها 720 شخص من بينهم 30 قاصر، وقع ضحيتها إطارات في فخ الابتزاز والتهديد والتشهير والمساس بحريتهم الشخصية، عبر مواقع التواصل الاجتماعي.

وفي التفاصيل التي قدمتها المديرية العامة للأمن الوطني، فقد قامت فرقها المختصة في مكافحة الجرائم المتصلة بتكنولوجيات بمعالجة 742 قضية تتعلق بجرائم الانترنت، خلال السداسي الأول من سنة 2017، تورّط فيها 720 شخص من بينهم 30 قاصر.

وحسب بيان الأمن، فإن جهود محاربة الجريمة الإلكترونية مكنت من معالجة قضايا تتعلق بالمساس بالأشخاص، التشهير، والقذف، جرائم المساس بأنظمة الحاسب الآلي، اختراق الأنظمة المعلوماتية، الاطلاع وتحريف البيانات، الجرائم التقليدية التي تستعمل في التكنولوجيات كالتهديد والنصب الاحتيال.

ويضيف البيان برمجت المديرية العامة للأمن، عدة دورات تكوينية حول الوقاية ومكافحة الجريمة السيبرانية، حيث تأتي في إطار تجسيد مساعي اللواء عبد الغني هامل المدير العام للأمن الوطني، لتوفير دورات تكوينية تقنية عالية المستوى في مجال مكافحة الجريمة الالكترونية ومسايرة فرق المحققين من الشرطة لأحدث التكنولوجيات والتحكم فيها.

وحسب البيان ذاته، فالأمن يبذل جهودا معتبرة في الوقاية والتحسيس من هذه الجرائم الناجمة عن سوء استعمال الشبكة العنكبوتية خاصة من طرف الشباب والأطفال باللجوء إلى العمل الاستباقي لإزالة الأخطار المحتملة وحماية الأفراد والمجتمع من هذا النوع من الجرائم الالكترونية، وهذا ما تسعى إليه المديرية العامة للأمن الوطني من خلال تنظيم مثل هذه الدورات التكوينية المتخصصة[1].

[1] الشرطة توقف 720 شخص بينهم 30 قاصرا خلال السداسي الأول742جريمة تشهير وتهديد وإبتزاز عبر "الفايسبوك" ، جريدة الشروق تم الاطلاع عليه بتاريخ 2019/09/08 عبر الموقع الالكتروني:
https://www.echoroukonline.com/742%D8%AC%D8%B1%D9%8A%D9%85%D8%A9%D8%AA%D8%B4%D9%87%D9%8A%D8%B1%D9%88%D8%AA%D9%87%D8%AF%D9%8A%D8%AF%D9%88%D8%A5%D8%A8%D8%AA%D8%B2%D8%A7%D8%B2%D8%B9%D8%A8%D8%B1%D8%A7%D9%84%D9%81%D8%A7%D9%8A/

خلاصة

في الأخير نخلص، إلى أن المشرع الجزائري لا يتوفر على آليات قادرة على الاضطلاع بالآثار الخطيرة التي ترتبها جرائم المساس بأنظمة المعالجة الآلية للمعطيات سواء على مستوى النصوص التشريعية أو على مستوى طبيعة الكوادر والأجهزة المتخصصة لمواجهة هذا النوع من الإجرام، ومن ثم كان لابد أن يبادر إلى تبني سياسة موسعة ومحكمة، تستهدف إيقاف كل التحديات التي يطرحها هذا الإجرام، وإيمانا بأهمية الوقوف أمام التحديات التي تفرضها هذه الجريمة، ارتأينا ختم هذا البحث ببعض الاقتراحات والتوصيات التي قد تساهم في التقليل من الآثار السلبية لكثير من التحديات المصاحبة لوسائل الاتصال الجديدة.

الاطار التطبيقي

الفصل الرابع

الجانب الميداني للدراسة

المبحث الاول : جوانب التصدي للجريمة الالكترونية

المبحث الثاني: عرض النتائج وتحليلها

تمهيد

استطاعت التكنولوجيا أن تحل جميع مجالات الحياة ، فقد اعتمد عليها في المجال العلمي و الاقتصادي و الاجتماعي و أمام هذا الاتساع الكبير لاستغلالها ظهر نوع جديد من الجرائم استطاع أن يحقق نتائج عجزت الجرائم التقليدية عن تحقيقها ، ففي الجانب الاقتصادي استطاع المختصون في الجرائم الالكترونية تحقيق أرقام خيالية من خلال النصب والاحتيال و تحويل الأموال ، التزوير و غيرها من الأساليب التي كانت في الماضي صعبة التحقيق ، كما أن الاستغلال السيئ للتكنولوجيا أتاح لهؤلاء المجرمين أن يعبروا الحدود الإقليمية لبلدانهم و عبروا بجرائمهم القارات و حققوا أغراضهم المرجوة ، كما لا نغفل عن الجانب الاجتماعي و السياسي و الديني و الأمني و غيرها من الجوانب الأخرى التي استغلت من طرف المختصين في الجرائم الالكترونية، أمام هذا التسارع الجرائم الالكترونية و الغير مسبوق لأي نوع من الجرائم الأخرى قامت الحكومات بتشريع قوانين و أنظمة تكافح و تواجه بها الجرائم الالكترونية ، كما خلقت أجهزة أمنية و قضائية مختصة في مكافحة هذا النوع من الجرائم.

الجزائر و كعادتها كانت دائما في الواجهة و مسايرة لما تواجهه الدول التي تضررت مبكرا من هذا النوع من الجرائم ، فقامة الدولة بكل ما من شأنه أن يحمي مصالحها و مصالح شعبها و يوفر لهم الاستغلال الأمن التكنولوجيا ، فقامت مبكرا بتشريع قوانين تواجه الجرائم الالكترونية و احتلت الميدان سريعا بجميع أجهزتها الأمنية و القضائية وخلقت اطر وأنظمت كفيلة بمواجهة الانتشار المتسارع لهذا النوع من الجرائم الخطير جدا على جميع الأصعدة.

و من خلال هذا الفصل سنتطرق إلى دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية ، والتي عملت طيلة السنوات الأخيرة تنفيذا لتعليمات الجهات العليا على توفير الأمن و الحماية للوطن و المواطن ضد الجرائم الالكترونية.

المبحث الاول : جوانب التصدي للجريمة الالكترونية :

المديرية العامة للأمن الوطني و تحت إشراف مديرها العام سيادة اللواء عبد الغاني هامل ، وكعادتها عملت بجدية و تفطن اتجاه تسارع انتشار هذا النوع من الجرائم حيث قامت في سنة 2003 بإرسال إطارين إلى دولة فرنسا للتكوين في مجال مكافحة الجرائم الالكترونية بالإضافة إلى ذلك المديرية العامة للأمن الوطني لم تفوت أي فرصة لحضور الملتقيات الدولية التي تنظم من الدول الأجنبية التي عانت مبكرا من هذا النوع من الجرائم ، كما تم فتح دعوة فريق من المحققين المختصين في هذا المجال يفرنسا لتكوين دفعة من 22 ضابط شرطة خلال سنة 2003.

المديرية العامة للأمن الوطني ومنذ سنة 2000 م سبقت المجرمين في التمركز في الميدان و سبقت حتى صدور قانون جزائري يجرم الجرائم الالكترونية فشاركت في الملتقيات الدولية و كونت إطارات و رتباء و أعوان في مجال مكافح الجرائم الإلكترونية ، قامت بجميع الوسائل التي من شأنها كبح جماح المجرمين المختصين في هذا النوع من الجرائم.[1]

المطلب الاول : الجانب القانوني:

القانون 22-06 المؤرخ في 2006/ 12 / 10 المعدل و المتمم لقانون الإجراءات الجزائية و الذي صنف جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن الجرائم الخطيرة ووضع لها تدابير إجرائية خاصة منها:

- تمديد الاختصاص المحلي لضابط الشرطة القضائية إلى كافة التراب الوطني .
- مراقبة الأشخاص وتسليم المراقب .

امكانية اللجوء الى الاساليب الخاصة في التحري لا سيما اعتراض المراسلات والتقاط الصور وتسجيل الصور والاصوات والتسرب.

القانون 05-03 الخاص بحماية الملكية الفكرية الذي صنف برامج الحاسوب من المصنفات المحمية و اعتبر نشر المصنفات عبر أنظمة المعالجة الآلية للمعطيات كوسيلة من وسائل التقليد المعاقب عليها. القانون المدني الذي أكد أن المعطيات الرقمية وسيلة من وسائل الإثبات.

القانون 04-09 المؤرخ في 2009/ 08 / 05 : المتضمن القواعد الخاصية للوقاية من جرائم تكنلوجيا الإعلام و الاتصال و مكافحتها و الذي جاء ب:

[1] معلومات مقدمة من طرف المكلف بالاعلام في مديرية الامن الوطني

• تفتيش المنظومات المعلوماتية أو التفتيش الألكتروني مع إمكانية تمديد التفتيش من منظومة إلى أخرين ولو خارج الوطن [1]

• حجز معطيات المعلوماتية (الحجز المباشر أو عن طريق منع الوصول للمعلومات).

• المراقبة الالكترونية. : إلزام مقدمي خدمة الانترنيت بسحب المحتويات المخالفة للقوانين أو جعل الدخول إليها غير ممكن .

• إلزام مقدمي خدمة الانترنيت بمساعدة السلطات و حفظ المعطيات..

• وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام و إخبار المشتركين لديهم بوجودها.

قانون العقوبات : المواد من 394 مكرر الى غاية 394 مكرر 7.

المطلب الثاني: الجانب التنظيمي

حرصت المديرية العامة للأمن الوطني على تكوين العنصر البشري قصد مسايرة الوتيرة المتسارعة للجرائم الالكترونية حيث وضعت برنامجا مدروسا في هذا الخصوص يتضح من خلال بما يلي:

1. التكوين الأولي

• تم تسطير برنامج لتكوين الملازمين الأوائل الشرطة يتطرق إلى موضوع الجرائم الالكترونية

• التكوين المتواصل و التكوين المتخصص:

سطرت المديرية العامة للأمن الوطني برنامج تكويني لفائدة اطارتها و رباتها و أعوانها انطلقت في هذا البرنامج منذ سنة 2016 على النحو التالي:

[1] معلومات مقدمة من طرف المكلف بالاعلام في مديرية الامن الوطني

	التكوين بالداخل بمشاركة خبراء أجانب		التكوين بالخارج		التكوين بالداخل بمشاركة كفاءات وطنية	
السنوات	الدوريات	الضباط المستفيدون	الدوريات	الضباط المستفيدون	الدوريات	الضباط المستفيدون
2016	01	6				
2017	03	5	01	02	01	6
2018	01	20	01	05	/	/
المجموع	05	31	02	7	01	06

2. تدعيم و هيكلة مصالح الشرطة القضائية للتصدي للجريمة:

تعد الجريمة الالكترونية وجه جديد للجرائم يستلزم استحداث هياكل جديدة و تدعيم الهياكل القديمة المختصة في مكافحة الجرائم على مستوى المديرية العامة للأمن الوطني ، و عليه قررت القيادة العليا للأمن الوطني استحداث مخابر و فصائل و خلايا مختصة في مكافحة الجرائم الالكترونية أهمها: [1]

- مخابر الشرطة العلمية:

في سنة 2007 استحدث بمخابر الشرطة العلمية الكائن مقرها بالجزائر العاصمة ووهران و قسنطينة أقسام مختصة في تتبع الأدلة الرقمية من خلال استغلال أجهزة الكترونية قصد استخراج و تتبع ما من شأنه أن يفيد في التحقيق و يساعد العدالة في تقرير الأحكام في القضايا التي تكون من هذا النوع .

و أهم هذه الأجهزة المستغلة من طرف الأقسام المختصة في الأدلة الرقمية :

1.أدوات التخزين الرقمية أجهزة التصوير، بطاقات الذاكرة الأقراص الصلبة....الخ)

2. أجهزة الكمبيوتر وجميع لواحقها الأخر

3. تدعيم المصالح الولائية للشرطة القضائية

خلقت المديرية العامة للأمن الوطني سنة 2010 م ما يقارب 23 خلية لمكافحة الجرائم الالكترونية موزعة على النحو التالي:

08 خلايا على مستوى ولايات الشرق

[1] معلومات مقدمة من طرف المكلف بالاعلام في مديرية الامن الوطني

08 خلايا على مستوى ولايات الوسط

06 خلايا على مستوى ولايات الغرب

01 خلية على مستوى ولايات الجنوب

لتقوم بعدها المديرية العامة للأمن الوطن بتعميم الخلايا على جميع مصالح أمن ولايات الوطن.

– للإشارة : خلايا مكافحة الجرائم الالكترونية يتم انتقاء عناصرها على أساس الشهادات الجامعية والمؤهلات التي يحملونها ، كما لم تغفل المديرية عن أهم جانب و هو جانب الخبرة في الشرطة القضائية ، كل هذه المزايا التي تم انتقاء العناصر بها تم تدعيمها في الأخير بدورات تكوين متخصص و على أعلى مستوي قبل تنصيبهم في مراكز عملهم الجديدة على مستوى الخلايا الولائية المختصة في مكافحة الجرائم الالكترونية. [1]

3– الجانب التوعوي:

لم تغفل المديرية العامة للأمن الوطني عن الجانب الوقائي التوعوي ، ففي إطار سياسة الشرطة الجوارية التي تنتهجها قيادة المديرية ، قام الأمن الوطني بفتح موقع الكتروني خاص بالشرطة الجزائرية على الانترنيت يستطيع من خلاله أي مواطن مهما كان مستواه العلمي أو الاجتماعي طرح انشغاله و التبليغ عن أي شيء يثير الشبهة .

كما برمجت المديرية العامة خطوات استباقية للتصدي للجريمة الالكترونية عن طريق تنظيم دروس توعوية في مختلف الأطوار الدراسية و كذا المشاركة في الملتقيات و الندوات الوطنية و جميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

المطلب الثالث: العمل الميداني للتصدي للجريمة الالكترونية

بعد العمل الميداني أهم ما تركز عليه المديرية العامة للأمن الوطني ، فقد احتلت الميدان قبل وجود هذا النوع من الجرائم بالجزائر وقبل حتى صدور قانون جزائري يعاقب على الجرائم الالكترونية.

أ–**القضايا المعالجة** : عالجت المديرية العامة للأمن الوطني على المستوى الولائي مجموعة من القضايا المتعلقة بالجانب الالكتروني نذكر منها:[2]

[1] معلومات مقدمة من طرف المكلف بالاعلام في مديرية الامن الوطني

[2] معلومات مقدمة من طرف المكلف بالاعلام في مديرية الامن الوطني

السنوات	عدد القضايا المعالجة	عدد الاشخاص المتورطين
2016	29	21
2017	245	
2018	409	347

المبحث الثاني: عرض النتائج وتحليلها

المطلب الاول : عرض نتائج الدراسة

1. هل الجريمة الالكترونية في مدينة الاغواط في تزايد ؟

نعم الجريمة الالكترونية في ولاية الاغواط في تزايد في مختلف الفضاءات الاتصالية على شبكة الانترنت بما فيها مواقع التواصل الاجتماعي.

ومنه نستنتج ان لجريمة الالكترونية أصبحت اكثر انتشارا وقد يكون ذلك بسبب الانتشار الهائل للوسائط الالكترونية وتوفر غالبية المواطنين على شبكة الانترنت

2. ما هي الفئة العمرية الأكثر عرضة لهذا المشكل(الجريمة الالكترونية)؟

نجد ان اكثر فئة تتعرض لهذا المشكل الا وهو الجريمة الالكترونية هي فئة الشباب خصوصا فيما يخص جرائم الابتزاز والتشهير او السب والقذف.

نستنتج ان الكثير من الشباب يتعرضون للابتزاز والقذف والسب والتشهير عبر شبكات التواصل الاجتماعي وقد يكون ذلك بسبب اعتقاد مرتكبي هذه الأفعال انه في منأى عن الحساب والعقاب باستعمال حسابات غير حقيقية.

3. هل هناك أيام معينة لمحاربة الجريمة الالكترونية؟

لا يوجد أيام معينة حيث انه سمح القانون باساليب خاصة للتحري في هطا النوع من الجرائم من حيث تمديد الاختصاص في التفتيش ومواعيده.

نستنتج ان العمل في التحري في الجريمة الالكترونية له خصوصية مقارنة بالجرائم العادية وقد يكون ذلك بسبب طبيعة هذه الجريمة التي تقع في فضاء لا يعرف حدود زمنية ولا مكانية.

4. كيف يمكنكم التعامل مع الجريمة الالكترونية في حال ما اذا كان مرتكبها من القصر؟

اذا كان مرتكب الحريمة قاصرا فإن مصال الامن تباشر بتحرياتها والتحقيق فيها مع القاصر بحضور ولي امره الشرعي .

انجد انه قد يقوم احد قاصر بجريمة الكترونية والغالب انه يجهل ان فعله يشكل جريمة معاقب عليها وبما ان القانون شدد في التعامل مع القصر لا يمكن ان يقوم ضابط الشرطة باستدعاء التحقيق مع الشخص القاصر الا بحضور ولي امره الشرعي وهذا يعود بسبب خصوصية الفئة العمرية هذه.

5. ما هي الوسائط الإعلامية التي تتمك عبرها الجريمة الالكترونية (فيسبوك–تويتر ... الخ)؟

اغلب القضايا التي عالجتها فرقة مكافحة الجريمة الالكترونية كانت عبر الفضاء الاتصالي فيسبوك.

نجد ان معظم الجرائم تقع عبر شبكة التواصل الاجتماعي فيس بوك وهذا قد يكون راجع الى الانتشار الهائل للفيس بوك عبر المجتمع .

6. كيف يتم التبليغ عن الجريمة الالكترونية؟

يتم التبليغ عن الجريمة الالكترونية عن طريق الشكوى المباشرة من قبل الضحية او بناءا على تعليمات من الجهة الوصية او أحيانا يتم اكتشافها عن طريق التحريات التي تقوم بها مصالح الشرطة القضائية المكلفة بمحاربة الجريمة الالكترونية عبر مراقبة الوسائط المختلفة.

لا نجد طريقة محدد للتبليغ عن الجريمة الالكترونية لانه قد تكون عبر شكو او يتم اكتشافها وهو ما يمكن لعناصر الامن ان يباشر التحقيق فيها بحسب صلاحياته دون شكوى او تبليغ.

7. ما هي اخطر أنواع الجرائم الالكترونية التي يتم رصدها من طرف الأجهزة الخاصة بكم؟

من بين اخطر الجرائم الالكترونية نجد جرائم النصب والاحتيال والتشهير والابتزاز.

نجد ان معظم الجرائم التي تقع عبر الانترنت هي جرائم الابتزاز والتشهير والنصب والاحتيال باعتبارها اسهل ولا تحتاج الى معدات كالقرصنة والتزوير .

8. هل تتوفر مصالح الامن على تقنيات يمكنها التقصي والبحث في الجرائم الالكترونية؟

نعم تم تدعيم فرق البحث والتحري في الجريمة الالكترونية بتقنيات حديثة وكذاك بالاساليب الخاصة في التحري .

لقد تم تزويد فرق مكافحة الجريمة الالكترونية بمعدات عالية التقنية وقد يكون هذا بسبب طبيعة الجريمة الالكترونية التي تستلزم مثل هذه المعدات من اجل الوصول الى الأدلة فيها .

9. ما هي الصعوبات التي تعترض مكافحة الجريمة الالكترونية؟

جهل الضحايا بالقانون : أي أن الضحية لا يعتقد انه يوجد هناك قانون يجرم تلك الأفعال فيعدلون عن التبليغ عن هذه الجرائم ، كما لا نغفل طبيعة المجتمع الجزائري الذي يخشى نظرة المجتمع للضحية الذي يقع في مثل هاته الجرائم.

عملية تحصيل المعطيات خاصة المتعلقة بالارتباط لمزودي الخدمة تطلب وقت كبير نظرا لتمركزها بالجزائر العاصمة فقط .

–صعوبة تحصيل الأدلة خاصة ما يتعلق منها بالجرائم التي ترتكب من الجزائر و من طرف جزائريين و لكن أثارها خارج الوطن فتعتمد مصالح الأمن تحصيل الأدلة من محيط المشتبه فيه نظرا لصعوبة تحميلها من موقع ظهور الجريمة بالخارج

10. ماهي في نظركم عوامل انتشار الجريمة الالكترونية؟

الجانب الأسري: نظرا لحداثة هذا النوع من الجرائم و نظرا لقلة وعي الأولياء بخطورته نجد أن الرقابة الأسرية تقل إن لم نقل تنعدم في كثير من الأحيان فيبقى الطفل عرضة لمخاطر الانترنيت وضحية سهلة للمختصين في هذا النوع من الجرائم.

• الجانب الوقائي: دائما في إطار قلة الوعي و أيضا اللامبالاة في كثير من الأحيان نجد أن الأشخاص المرتبطين بشبكة الانترنيت لا يولون اهتمام ببرامج الحماية الخاصة بتأمين الأجهزة الالكترونية عند ربطها بشبكة الأنترنيت.

• الجانب التعليمي: نجد أن برامج التعليمية بمختلف الأطوار تخلو من دروس تتطرق إلى مخاطر الاستغلال السيئ التكنولوجيا و الأنترنيت.

• عدم وجود تنظيم خاص بمقاهي الانترنيت ، خاصة عندما يتعلق الأمر بدخول القصر لهذه المقاهي .[1]

المطلب الثاني: الاستنتاج العام

من خلال النتائج المتحصل عليها من المقابلة مع المكلف بالاعلام في مديرية الامن بولاية الاغواط لاحظنا الانتشار الرهيب للجريمة الالكترونية خصوصا في وسط الشباب باعتبارهم الفئة الاكثر تعرضا للانترنت.

كما ان غالبية الجرائم التي تقع نجدها جرائم النصب والاحتيال والابتزاز والتشهير كما وجدنا ان الجريمة الالكترونية قد تقع من طرف اطفال لا يعرفون ان افعالهم تعد جريمة في نظر القانون.

وفي اطار التصدي للجريمة الالكترونية نجد مديرية الامن بولاية الاغواط قد تم تعزيزها بمعدات عالية التقنية كما ان القوانين اعطت اساليب خاصة في البحث والتحري في الجريمة الالكترونية وهذا نظرا للطبيعة الخاصة لهذه الجريمة واساليب ارتكابها.

[1] معلومات مقدمة من طرف المكلف بالاعلام في مديرية الامن الوطني

الخاتمة

الخاتمة

قامت المديرية العامة طيلة السنوات الأخيرة بتسطير برنامج محكم للحد من الانتشار السريع للجرائم الالكترونية ، كما لا تزال في سباق و تحدي مع المختصين في هذا النوع من الجرائم.

كما أن المديرية العامة للأمن الوطني و من خلال شعارها (المواطن هو أساس الأمن الشرطة ما هي إلا أداة) فهي على قناعة تامة أنه لن يتحقق الهدف من أي جهود تقوم بها الدولة بمختلف أجزتها لمكافحة الجرائم الإلكترونية إلا إذا كان المواطن على أتم الاستعداد للتعاون رو لا يتجلى هذا التعاون إلا من خلال الإبلاغ الفوري عن المجرمين و عدم الانسياق وراء ما يبثونه من سموم و إغراءات عبر شبكات الإنترنيت ، كما يجب أن يستغل كل ما من شأنه أن يسهل على مصالح الأمن القيام بدورها الذي هو دور أساس و رئيس في مكافحة الجريمة الإلكترونية.

الحلول المقترحة للتصدي للجريمة الالكترونية

باعتبار الأسرة هي أساس المجتمع يجب أن يتم توعية الأولياء و توفير الوسائل التي من شأنها أن تساعدهم للقيام بدور هم كاملا كمراقب أولي .

إدراج مواد أساسية أو على الأقل دروس توعية على مستوى جميع الأطوار التعليمة تركز فيها على مخاطر الاستغلال السيئ لتكنولوجيا الإعلام و الاتصال.

إشراك الإعلام بمختلف وسائله السمعية و البصرية للتوعية بمخاطر هذه الجرائم و الطرق المتبعة من طرفة المجرمين لاصطياد ضحاياهم ، كما يجب أن تكون هذه الحصص دورية و تمص جميع فئات المجتمع و تبسط لهم المعلومة لكي تصل بسهولة و يتم استيعابها و العمل بها مستقبلا.

يجب إنتاج و توفير الأدوات التي من شأنها أن تعطي الحماية اللازمة لمتصفحي الانترنيت خاصة ما تعلق منها بالبرامج الخاصة أو الأنظمة العامة

المراجع

المراجع

الكتب

1. ابراهيم العسل ، أسس النظرية و الاساليب التطبيقية في علم الاجتماع، بيروت :1997
2. ابن منظور، لسان العرب، دار المعارف، الجزء الرابع
3. أبو أصبع صالح خليل :الاتصال والإعلام في المجتمعات المعاصرة، ط 2 ، دار الآرام، الأردن، 2003 م
4. أحمد الشلقاني: مبادئ الإجراءات الجزائية في التشريع الجزائري ديوان المطبوعات الجامعية، 1999
5. أحمد حسام تمام ، الحماية الجنائية لتكنولوجيا الاتصالات ، دراسة مقارنة ، دار النهضة العربية ، 2002، مصر
6. احمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، دار النهضة
7. آمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة و النشر، الجزائر 2006،
8. أولجا جوديس بيلي، بيلي كاميرتس، نيكوكاربنتيير، "فهم الإعلام البديل"، ترجمة: علا أحمد إصلاح، القاهرة، مجموعة النيل العربية، 2009م
9. بوسقيعة أحسن: الوجيز في القانون الخاص، الجزء الأول، دار هومة، طبعة 2002
10. جميلة عبد الباقي الصغير ،ادلة الاتبات الجنائي و التكنولوجيا الحديثة ،الطبعة الأولى دار النهضة العربية ،2001
11. جودت عزت عطوي:أساليب البحث العلمي:مفاهيمه،أدواته، طرقه الإحصائية، دار الثقافة للنشر و التوزيع،2007
12. حسين عبد الحميد أحمد رشوان:أصول البحث العلمي، الإسكندرية.مؤسسة شباب الجامعة،2006
13. حمدان محمد زياد، البحث العلمي كنظام . سلسلة التربية الحديثة. دار التربية الحديثة . عمان – الأردن. 1989 ،
14. خالد ممدوح إبراهيم: أمن الجريمة الالكترونية، الدار الجامعية، الاسكندرية،2010
15. رجاء وحيد دويدري، البحث العلمي ، أساسياته النظرية، وممارسته العملية، دار الفكر، ط1، 1421هـ،

المراجع

16. سامي علي عياد حامد: الجريمة المعلوماتية وإجرام الانترنيت، دار الفكر الجامعي ,الاسكندرية، 2007،
17. سلمى محمود جمعة–طريقة العمل مع الجماعات–المكتبة الجامعية –الإسكندرية –2000
18. صبحي عبد اللطيف المعروف، أساليب الإرشاد النفسي والتوجيه التربوي، المقابلة الإرشادية، الملاحظة، السجل، والاختبارات والمقاييس، دار القادسية، بغداد، ط1، 1986م
19. طارق عبد الحق ،برمجيات الانترنت ،الملاحة و الاستكشاف ،قصر الكتاب ، 2005 ، الجزائر
20. عباس مصطفى صادق، "الإعلام الجديد: المفاهيم والوسائل والتطبيقات"، عمان، دار الشروق، 2008م
21. عبد الفتاح مراد , شرح جرائم الكمبيوتر و الانترنت , دار الكتب والوثائق المصرية , 2005
22. عكاشة محي الدين، محاضرات في الملكية الأدبية، ديوان المطبوعات الجامعية، الجزائر 2001
23. علي عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999
24. عمر بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي "المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية" ، الطبعة الأولى ، 2004 . 2005
25. عمرو عيسى الفقي: الجرائم المعلوماتية، جرائم الحاسب الآلي والانترنيت في مصر والدول العربية ,المكتب العربي الحديث، الاسكندرية 2006،
26. غنية باطلي: الجريمة الالكترونية دراسة مقارنة – الدار الجزائرية للنشر والتوزيع – الجزائر، 2015
27. فريال مهنا، علوم الاتصال والمجتمعات الرقمية ،، دمشق سوريا ، ط01/ دار الفكر 2006
28. فوزي غرايبة، وآخرون، أساليب البحث العلمي في العلوم الاجتماعية والإنسانية، الجامعة الأردنية، 1977م

المراجع

29. محمد الغريب عبد الكريم: مناهج البحث العلمي و طرق إعداد البحوث، ديوان المطبوعات الجامعية،ط02، الجزائر، 1999،
30. محمد الهادي محمد: أساليب توثيق البحوث العلمية،ا لمكتبة الأكاديمية، ط 01، الجزائر، 1995
31. محمد بهجت جاد الله كشك–تنظيم المجتمع من المساعدة إلى الدفاع –المكتب العلمي للكمبيوتر والنشر والتوزيع– الإسكندرية– 1996
32. محمد علي العريان: الجرائم المعلوماتية دار الجامعة الجديدة للنشر، الإسكندرية، 2004
33. محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، بدون رقم الطبعة، دار النهضة العربية، القاهرة 1992.
34. محي الدين مختار،: لاتجاهات النظرية و التطبيقية في منهجية العلوم الاجتماعية، دار المنشورات الجامعية،ط 01، باتنة، 1999،
35. منير محمد الجنبهي ، ممدوح محمد الجنبهي، تبادل إلكتروني للمعلومات ، دار الفكر الجامعي،2004، مصر
36. موريس انجرس : منهجية البحث العلمي، ترجمة بوزيد صحراوي وآخرون، دار القصبة للنشر، الجزائر،2004
37. مي العبد الله، الاتصال والديمقراطية، بيروت، دار النهضة العربية،2005م،
38. نبيل الأحمد عبد الهادي: منهجية البحث في العلوم الإنسانية،لبنان،الأهلية للنشر والتوزيع،2006.
39. هدى قشقوش: الحماية الجنائية للتجارة الالكترونية عبر الانترنيت، دار النهضة العربية، القاهرة،
40. هشام فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الكاتبة ، أسيوط ،طبعة 1995 ،
41. هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي . دراسة مقارنة ، الطبعة الأولى ، دار النهضة العربية . القاهرة ، 1997

المراجع

المذكرات

1. دردور نسيم: الجرائم المعلوماتية على ضوء القانون الجزائري والمقارن –رسالة لنيل شهادة الماجستير – كلية الحقوق – جامعة منتوري قسنطينة– 2012 –2013،
2. سوير سفيان: الجرائم المعلوماتية، رسالة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010،
3. صالح شنين: الحماية الجزائية لبرامج الحاسب الآلي، دراسة مقارنة رسالة لنيل شهادة الماجيستير، جامعة بسكرة –كلية الحقوق والعلوم السياسية، 2007 – 2008،
4. طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الأنترنت ، دراسة مقارنة ، مذكرة ماجيستر جامعة بسكرة ،2006،
5. يوسف صغير: الجرائم المرتكبة عبر الانترنيت، رسالة لنيل شهادة الماجستير، كلية الحقوق، جامعة مولود معمري، تيزي وزو الجزائر،

المحاضرات

1. تسريات ميلود، محاضرة ألقيت بمجلس قضاء قالمة بعنوان :أساليب البحث والتحري الخاصة وإجراءتها وفق قانون الإجراءات الجزائية والقانون 06–22 المعدل و المتتم له

المجلات

1.زاهر راضي، "استخدام شبكات التواصل الاجتماعي في العالم العربي"، عمان، مجلة التربية، ع15 ، جامعة عمان الأهلية، 2003

2. صالحة العمري: جريمة غسل الأموال وطرق مكافحتها–,مجلة الاجتهاد القضائي، العدد الخامس، مخبر اثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة،
3. عزة مصطفى الكحكي، "استخدام الانترنت وعلاقته بالوحدة النفسية وبعض العوامل الشخصية لدى عينة من الجمهور بدولة قطر"، أبحاث المؤتمر الدولي، "الإعلام الجديد: تكنولوجيا جديدة... لعالم جديد"، جامعة البحرين، من 7–9 ابريل 2009م،
4. علي كحلوش : جرائم الحاسوب و اساليب مواجهتها , مجلة الشرطة ,المديرية العامة للامن الوطني , العدد 84, جويلية 2007.
5. كريستاسكولمان: عن جرائم الانترنيت طبعتها وخصائصها، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية 19 و20 يونيو 2007،

6. مقني بن عمار بوراس عبد القادر، التنصت على المكالمات الهاتفية و اعتراض المراسلات كآلية للوقاية من جرائم الفساد، الملتقى الوطني حول الآليات القانونية لمكافحة الفساد، جامعة ورقلة، 8-9 ، 2008،
7. نبيل حميدشة،المقابلة، مجلة العلوم الإنسانية والاجتماعية، العدد (8) يونيو 2012م،
8. نصر الدين لعياضي، "الرهانات الابستمولوجية والفلسفية للمنهج الكيفي/ نحو أفاق جديدة لبحوث الإعلام والاتصال في المنطقة العربية"، أبحاث المؤتمر الدولي، "الإعلام الجديد: تكنولوجيا جديدة... لعالم جديد"، جامعة البحرين، من 7-9 ابريل 2009م
9. هشام محمد فريد رستم: الجرائم المعلوماتية، مؤتمر القانون والكمبيوتر والانترنيت، منذ 1 – 5 ماي 2000 – جامعة الامارات العربية المتحدة، كلية الشريعة والقانون- المجلد الثاني، الطبعة الثالثة، 2004
10. هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ،المعهد الوطني للأدلة الجنائية وعلم الإجرام ، جامعة بسكرة كلية الحقوق،2016
11. يونس عرب : جرائم الكمبيوتر و الانترنت ,ورقة عمل مقدمة الى مؤتمر الامن العربي, المركز العربي للبحوث و الدراسات الجنائية, ابو ظبي 10- 12 فيفري 2002

القوانين

1. القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004
2. القانون رقم 08/01 المؤرخ في 2008/01/23والمعدل والمتمم لقانون 83/01المتعلق بالتامينات
3. القانون رقم 16-01 المؤرخ في 6-03-2016 المعدل للدستور عدد الجريدة الرسمية 14
4. 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 عدد 40.
5. القانون 09 -04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها (الجريدة الرسمية رقم 47 الصادرة في 6 أوت 2009)

المراجع

6. القانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل.

المواقع الالكترونية

1. httlp://.eleagypt.com/downloads/2009/amina heba.doc
2. https://www.echoroukonline.com
3. https://www.wajeh.com
4. www.acconline.com/article.detail.aspr?id:7509
5. www.eastlaws.com

الملاحق

صحيفة القابلة

1. هل الجريمة الالكترونية في مدينة الاغواط في تزايد ؟

.....

.....

.....

.....

2. ما هي الفئة العمرية الأكثر عرضة لهذا المشكل(الجريمة الالكترونية)؟

.....

.....

.....

.....

3. هل هناك أيام معينة لمحاربة الجريمة الالكترونية؟

.....

.....

.....

.....

4. كيف يمكنكم التعامل مع الجريمة الالكترونية في حال ما اذا كان مرتكبها من القصر؟

.....

.....

.....

.....

5. ما هي الوسائط الإعلامية التي تتمك عبرها الجريمة الالكترونية (فيسبوك–تويتر ... الخ)؟

.....

.....

.....

.....

6. كيف يتم التبليغ عن الجريمة الالكترونية؟

.....

.....

.....

.....

7. ما هي اخطر أنواع الجرائم الالكترونية التي يتم رصدها من طرف الأجهزة الخاصة بكم؟

.....

.....

.....

.....

8. هل تتوفر مصالح الامن على تقنيات يمكنها التقصي والبحث في الجرائم الالكترونية؟

.....

.....

.....

.....

9. ما هي الصعوبات التي تعترض مكافحة الجريمة الالكترونية؟

.....

.....

.....

.....

10. ماهي في نظركم عوامل انتشار الجريمة الالكترونية؟

.....

.....

.....

.....

.....

.....

.....

.....