# مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي
# بين اختراق الخصوصية وآليات المواجهة

# *The dangers of cybercrime on social media*
# *Between privacy penetration and confrontational mechanisms*

**د. علواش كهينة***

جامعة الجزائر 3،

(الجزائر)

alouache2013@gmail.com

تاريخ الاستلام: 2022/01/22 تاريخ القبول: 2022/09/03 النشر:2022/11/16

**ملخص:**

ازداد استخدام مواقع التواصل الاجتماعي في الآونة الأخيرة نظرا للامتيازات التي توفرها للأفراد غير أن ذلك قاد للكثير من المشاكل والانعكاسات السلبية فأصبحت فضاء لممارسة الجرائم الالكترونية .

تسعى هذه الورقة البحثية لإبراز مخاطر الجريمة الالكترونية عبر مواقع التواصل الاجتماعي وآثارها المتعددة، فتخلق الخوف وعدم الأمان والتعدي على خصوصية الأفراد. كما تؤثر على أمن المعلومات وسلامة المجتمعات. وتحاول الوقوف على الخصائص التي تميزها عن الجريمة التقليدية. وقد توصلت الدراسة إلى أن هذه التهديدات المنتشرة مست مستخدمي شبكات التواصل الاجتماعي الذين يقعون ضحايا لهذه الجرائم ،كما أن استخدام هذه الشبكات يمثل فرصة لاختراق خصوصية الأفراد والمساس بأمنهم وارتكاب جرائم إلكترونية الأمر الذي يستدعي اتخاذ آليات كفيلة للتصدي والحد من هذه الجرائم .

**الكلمات المفتاحية:** مخاطر؛ جريمة إلكترونية؛ اختراق؛ خصوصية؛ شبكات التواصل الاجتماعي.

**Abstract** :

Individuals' use of social networks has expanded due to the privileges they provide, but they have become an outlet for cybercrime. This research paper seeks to highlight the risks and multiple effects of cybercrime across these sites, posing a threat to information security and the safety of communities and countries.

The study found that the use of these networks represents an opportunity to penetrate the privacy of individuals, compromise their security and commit several cybercrimes, which calls for mechanisms to address and reduce these crimes.

***KeyWords***: Risks ; cyber crime ; penetration ; privacy ; social networks

*د. علواش كهينة

**المقدمة:**

أدت التغيرات التي أفرزتها الثورة الرقمية والتطورات التكنولوجية في مختلف المجالات إلى اهتمام الدول بمسايرة الركب العالمي في مجال التطور ،خصوصا مع زيادة استخدام شبكات التواصل الاجتماعي في الجوانب السلبية،فأفرزت نمط جديد من الجرائم المستحدثة تنفذ عبر الشبكة تسمى بالجرائم الالكترونية،ما خلق مخاوف لدى الأفراد لصعوبة التحكم فيها.

تحاول الدراسة تسليط الضوء على مفهوم الجريمة الإلكترونية كظاهرة جديدة على المجتمعات الحديثة،وهي حسب الكثير من الباحثين نتاج طبيعي للإفرازات السلبية التي أنتجها التطور الهائل في مجال الاتصالات وعالم رقمنة المجتمعات والكيانات البشرية. واستغلالها عن قصد لأمور التجسس والاستعلام.ومواقع التواصل الاجتماعي كالفايسبوك لها يد في حدوث بعض الجرائم الإلكترونية، وذلك من خلال تورطها في التلاعب ببيانات المستخدمين أو القيام بإشهار لبرامج وبرمجيات مشبوهة لا هدف من ورائها غير الربح المادي.

يرى بعض علماء الاتصال أن بداية الألفية الثالثة امتازت بالتفوق التكنولوجي الذي أتاح المجال لهيمنة وسيادة الإعلام الجديد أو البديل أو الاجتماعي، وانتشرت بسرعة مذهلة مواقع التواصل الاجتماعي على الانترنيت مما شجع متصفحيها على الإقبال المتزايد عليها، ما ساعد بشكل أو آخر على انتشار ظاهرة انتهاك الخصوصية، وزاد من حدة الانتقادات التي تتعرض لها الشبكات الاجتماعية.

فظاهرة جرائم الكمبيوتر أو جرائم التقنية العالية أو الجريمة الالكترونية ظاهرة إجرامية مستجدة بحيث تعاني المجتمعات في الآونة الأخيرة من انتهاك للحقوق والخصوصيات وذلك في ظل انتشار الجريمة الإلكترونية.جاء تطوّر هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا التي يسرت سبل التواصل وانتقال المعلومات بين مختلف الشعوب والحضارات، وسهلت حركة المعاملات، وسعي المجرم وراء أطماعه واقتناصه الفرص لتحقيق أغراضه غير المشروعة، فلم يتوان عن استغلال التقنية لتطوير قدراته الإجرامية باستخدام الشبكة المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية، مما يلحق الضرر بالآخرين.

ومع تنامي معدلات الجريمة وتطور أشكالها دق ناقوس مجتمعات العصر الراهن،لحجم المخاطر وهول الخسائر الناجمة عن هذه الجرائم التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة.كونها جريمة تقنية تنشأ في الخفاء، وتستخدم للنيل من الحق في المعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الانترنت.فتظهر مدى خطورتها في الاعتداءات التي تمس الحياة الخاصة للأفراد وتهدد الأمن والسيادة.

من هنا تتمحور إشكالية الدراسة على النحو التالي:فيما تتمثل المخاطر التي تسببها الجريمة الإلكترونية عبر شبكات التواصل الاجتماعي على خصوصية الأفراد؟ وماهي آليات التصدي المتخذة للحد من آثارها؟

تفرعت عن هذه الإشكالية التساؤلات التالية:

-ماذا نقصد بالجريمة الإلكترونية؟ وماذا يميزها عن الجريمة التقليدية؟

-ماهي التهديدات التي تمارسها الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي على خصوصية الأفراد؟
-فيما تتمثل الإجراءات المتخذة للحد من خطورة الجريمة الإلكترونية؟

للإجابة على الإشكالية والتساؤلات المطروحة ركزت الورقة البحثية على بعض المفاهيم الأساسية التي تمثل أساس الدراسة كالتعريف بالجريمة الإلكترونية بمعناها الواسع ثم الإشارة إلى مواقع التواصل الاجتماعي،مع الوقوف على أهم الخصائص التي تميزها حتى يتسنى معرفة الفرق بينها وبين الجريمة التقليدية. لتعكف الدراسة للحديث عن التهديدات التي تمارسها الجريمة الإلكترونية عبر مواقع الشبكات الاجتماعية على خصوصية الأفراد والأضرار التي تسببها. لتصل في الأخير إلى الإجراءات المتخذة للحد من خطورة الجريمة الإلكترونية.ثم خاتمة وتوصيات الدراسة.

## I. تحديد المفاهيم:

### 1. مفهوم الجرائم الإلكترونية:

أدت الحداثة التي تميزت بها الجريمة الإلكترونية واختلاف النظم القانونية والثقافية بين الدول إلى عدم الاتفاق على مصطلح واحد موحد للدلالة عليها.ما أدى إلى عدم وضع تعريف موحد لهذه الظاهرة الإجرامية وذلك خشية حصرها في مجال ضيق؛ لذلك نجد عدة تعريفات تقوم على أسس مختلفة (عربان ، 2004، صفحة 43).

منها نذكر ما يلي:

### 1.1. تعريف الجريمة الالكترونية حسب وسيلة الجريمة:

يرى أصحاب هذا الاتجاه أن الجريمة الالكترونية هي التي يتم فيها استخدام الكمبيوتر كوسيلة للجريمة،وأنها ناشئة أساسا من التقدم التكنولوجي ومدى التطور الذي يطرأ عليه، إذن يفضل إطلاق اصطلاح الجريمة الإلكترونية على الجرائم المتعلقة بالحاسوب والانترنيت. (المومني،2008،صفحة47).كما عرفها الفقيه الألماني "تديمان"بأنها شكل من أشكال السلوك غير المشروع أو الذي يلحق أضرار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي(فاريش،نقاوش،2017-2018، صفحة 63).كما تعرف بأنها كل نشاط إجرامي يؤدي فيه نظام الكمبيوتر دورا هاما لإتمامه.

وعرفت أيضا بأنها "تلك الجريمة التي تتم باستخدام الكمبيوتر من خلال الاتصال بشبكة الانترنيت(زيدان،2001 صفحة 43 ) .

ومنه اتفقت جميع التعريفات حول الجريمة الالكترونية على أساس وسيلة ارتكاب الجريمة على وجوب توفر الحاسب الآلي وشبكة الانترنيت كي يتم وقوع الجريمة،فهما وسيلتان أساسيتان في هذا النوع من الجرائم.

### 2.1. تعريف الجريمة الإلكترونية حسب الفاعل:

يرى أصحاب هذا الاتجاه أن الجريمة الإلكترونية تستوجب أن يكون فاعل الجريمة ملما بتقنية المعلومات(عبابنة، 2005 ،صفحة 16 ) إذ نجد وزارة العدل في الولايات المتحدة الأمريكية تعرفها بأنها "أية جريمة لفاعلها معرفة فنية بالحسابات تمكنه من ارتكابها،أن تتوفر لدى الفاعل معرفة كافية بتقنية الحاسوب"( الكعبي،د.ت،صفحة34 )

كما تعرف على أنها"أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقاته قضائيا.فمنه تتفق هذه التعريفات حول الجريمة الالكترونية على هذا الأساس إلى وجوب المعرفة المسبقة للمجرم الالكتروني بتقنية الحاسوب وخباياه حتى يتمكن من تنفيذ جريمته.

**1.3. تعريف الجريمة الإلكترونية حسب موضوع الجريمة:**

يرى أصحاب هذا الاتجاه أنه يجب التركيز على الجانب الموضوعي للجريمة الإلكترونية باعتبار أنها تقع على الحاسب الآلي وفي داخل نطاقه،بمعنى أن الجريمة الإلكترونية المرتكبة ليست هي التي يكون النظام المعلوماتي وسيلة ارتكابها بل هي التي تقع عليه أو على نطاقه(خليفة الملط، ، د.ت، صفحة 85-86).إلا أن هناك من يوسع من مفهوم هذه الجريمة المسماة بالجريمة الإلكترونية حيث يعرفها الخبير الأمريكي "بايكر" بأنها:"كل فعل إجرامي معتمد أيا كان صلته بالمعلوماتية ينشأ عن خسارة تلحق بالمجني عليه فعل أو مكسب يحققه الفاعل.( الشوابكة 2004 صفحة 14).

وتعرف الجريمة الإلكترونية بأنها" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي " أو شبكة حاسوبية، أو داخل نظام حاسوبي،وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها عبر وسط إلكتروني. (جاسم الطائر، 2007، صفحة 121). كما تُعرّف الجرائم الإلكترونية (بالإنجليزية:) Electronic crime or e-crimeبأنّها الممارسات التي تُوقَع ضدّ فرد أو مجموعةٍ مع توفر باعث إجرامي بهدفِ التَّسبُّبِ بالأذى لسمعة الضحيّة عمداً،أو إلحاق الضَّرر النفسيّ والبدني به سواءً بأسلوبٍ مباشر أو غير مباشر بالاستعانة بشبكات الاتّصال الحديثة كالانترنيت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المحادثة والهواتف المحمولة وغيرها.

**2. تعريف مواقع التواصل الاجتماعي:**

هناك عدة تعريفات لمواقع التواصل الاجتماعي ومن بينها نأخذ تعريف "لوي سارج ريل دال سارت" في كتابه الشهير "الشبكات الاجتماعية على الانترنيت.يعرفها على أنها تمثل نتيجة لتطور الانترنيت( Real Del,2010 , Page 26.). فهي إذن ظاهرة جديدة بعد ظهور الويب (Hugo , 2008 page14 ).

من جهته يعرف "مهدي الحوساتي" مواقع التواصل الاجتماعي على أنها "مواقع تصنف ضمن مواقع الجيل الثاني للويب،وسميت اجتماعية لأنها أتت من مفهوم بناء مجتمعات.وبهذه الطريقة يستطيع المستخدم التعرف على أشخاص لديهم اهتمامات مشتركة في تصفح الانترنيت و التعرف على المزيد من المواقع في المجالات التي تهمه وأخيرا مشاركة هذه المواقع مع أصدقائه وأصدقاء أصدقائه.فهي بذلك تسمح للأفراد بتقديم لمحة عن حياتهم العامة وإتاحة الفرصة للاتصال بقائمة المسجلين،والتعبير عن وجهة نظر الأفراد أو المجموعات من خلال عملية الاتصال(الهاشمي ،2015 ،صفحة 21-22 ).كل هذا يتم عن طريق خدمات التواصل المباشر مثل إرسال

الرسائل أو الاطلاع على الملفات الشخصية للآخرين ومعرفة أخبارهم ومعلوماتهم التي يتيحونها للعرض.تعتمد هذه الشبكات بالدرجة الأولى على مستخدميها في تشغيلها وتغذية محتواها .( Boyd, Ellison, 2019).

### 3. خصائص الجريمة الإلكترونية:

تتميز الجريمة الإلكترونية بصفة عامة عن الجريمة التقليدية في عدة نواحي سواء كان هذا التمييز في السمات العامة لها أو في الباعث على تنفيذها أوفي طريقة القيام بها،وذلك نتيجة ارتباطه بتقنية المعلومات وجهاز الكمبيوتر مع ما يتمتع به من تقنية عالية، كما أن لظهور شبكة الانترنيت دورا فعالا في إعطاء شكل جديد للجريمة. ومن أهم خصائص وسمات الجريمة الإلكترونية ما يلي:

-الحاسب الآلي وأداة ارتكاب الجريمة الإلكترونية:يعد الحاسب الآلي الأداة الوحيدة في الجرائم الإلكترونية فهي خاصية منفردة عن الجرائم الأخرى فالحاسب الآلي هو الأداة الوحيدة التي تمكن مرتكب الجريمة الإلكترونية من الدخول إلى شبكة الانترنيت وارتكابه لجريمته مهما كان نوعها.( الطائر، 2002، صفحة 141 )

-جرائم ترتكب عبر شبكة الانترنيت:تعتبر الشبكة العنكبوتية الحلقة الرابطة بين الأهداف المحتملة للجرائم الإلكترونية كالبنوك والشركات الصناعية وغيرها،ما استدعى توخي الحذر من تلك الجرائم التي تحدث عبر الشبكة وذلك باللجوء إلى نظم الأمن الإلكترونية لحماية نفسها من هذه الجرائم أو على الأقل الحد من خسائرها.

-صعوبة اكتشاف الجريمة الإلكترونية : تتميز الجريمة الإلكترونية كذلك بصعوبة اكتشافها بحيث لا تكتشف بسهولة وإن تم اكتشافها فذلك يكون عادة بالصدفة،بحيث نجد عدد الحالات التي تم فيها اكتشاف هذا النوع من الجرائم قليلة إذا ما قورنت بما يتم اكتشافه من الجرائم التقليدية.

ويمكن القول أن السبب في صعوبة اكتشاف الجريمة الإلكترونية هو عدم ترك هذه الجريمة لأي أثر خارجي مرئي كما أنها ترتكب حتى خارج الدولة.(المومني، 2008 ، صفحة 53-54 ).إضافة إلى أن وسيلة تنفيذها تتميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد و عدم التبليغ عنها في حالة اكتشافها لخشية المجني عليهم فقدان عملائهم،فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة تقل عن الثانية.(المومني، 2008 ، صفحة56).

-الجريمة الالكترونية جريمة عابرة للحدود:تتميز الجريمة الالكترونية كذلك بكونها جريمة عابرة للحدود إذ لا تتم داخل إقليم أو بلد واحد،فبعد ظهور شبكات المعلومات لم يجد هناك حدود مرئية أو ملموسة تقف أمام آلاف الأميال بينها، فقد أعطى انتشار الشبكة إمكانية ربط عدد هائل من أجهزة الحاسوب المرتبطة بها من غير أن تخضع لحدود زمنية ومكانية بحيث يمكن للجاني أن يكون في بلد ما والمجني عليه في بلد آخر.

-مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي:يطلق على مرتكب الجريمة الإلكترونية أو المعلوماتية اسم المجرم الإلكتروني،فهو يختلف عن المجرم التقليدي بتميزه بخصائص معينة، إذ يتمتع المجرم الإلكتروني

بخبرة فائقة في مجال الحاسب الآلي وطريقة استخدامه له، كما يتمتع بمعرفة فائقة في عالم الحاسوب لكي يتمكن من ارتكاب جريمته بطريقة ذكية والعمل على إخفائها وعدم ترك آثار ورائه.

-الجريمة الالكترونية تتسم بالخطورة البالغة:نظرا لأغراضها المتعددة وحجم الخسائر التي تحدث عند ارتكابها مقارنة بالجريمة التقليدية، كما أن هذا النوع من الجرائم تستهدف معنويات وليس ماديات محسوسة، كما تكون سلوكيات غير مألوفة يقوم بها مجموعة من الأشخاص مما يجعل الوصول إلى الجاني أو القائم بالجريمة الإلكترونية أمرا صعبا. (سعيداني نعيم، 2012-2013 ، صفحة 63 ).

## II. تهديدات الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي لخصوصية الأفراد:

تتعدد أشكال الجريمة الإلكترونية التي تتم في فضاء الانترنيت والأجهزة الحديثة فيتغلغل المجرمون والمحتالون في شبكات التواصل الاجتماعي ويمارسون عمليات الخداع لمئات الألوف من المستخدمين من أجل السيطرة على معلومات شخصية أو حسابات خاصة أو بيانات سرية أو مستندات أو وثائق،يختلطون مع الحشود ويحاكون المستخدمين بنشاطاتهم واهتماماتهم،ويستغلون لجوء الناس لشبكات التواصل الاجتماعي ليمارسوا جريمتهم المتمثلة بقرصنة خصوصية المستخدمين عبر الروابط الاحتيالية.

فيُنظر إلى الخصوصية على أنها العملية التي يهدف من خلالها الأفراد تنظيم عملية التفاعل مع الآخرين وهذا من خلال وضع حدود شخصية.( Altman , Dalmas, 1973, Page06 )

تمثل الخصوصية إذن فعل التحكم والسيطرة وحفظ المعلومات الشخصية للأفراد،أي جعل بعض المعلومات متاحة للجميع أو الأصدقاء أو أصدقاء الأصدقاء فقط أو جعلها سرية وقد تطور مفهوم الخصوصية ليضمن الحق في السيطرة على البيانات الشخصية عبر مواقع التواصل الاجتماعي وغيرها.وبالنسبة لإعدادات الخصوصية في موقع الفايسبوك فهي عديدة، تتعلق مثلا بصورك، اقتباساتك، حالتك العائلية، أفلامك المفضلة، الديانة ...إلخ .

فقد يتعرّض الكثير من الأفراد على اختلاف أعمارهم وتوجهاتهم إلى الكثير من الأضرار على شبكات التعارف الاجتماعية فبإمكان أي شخص أن يتعرف على الكثير من خصوصيات شخص آخر بمجرد تمضية دقائق في ملفه الشخصي.الحل لهذه المشكلة من قبل أصحاب الشبكات الاجتماعية كان بإتاحة بعض الخصوصية مثل إتاحة خاصية التحكم في عرض بعض محتويات الملف الشخصي لمجموعة معينة من الأشخاص وإضافة بعض القوانين المتعلقة بإمكانية وصول الآخرين لتلك المحتويات(أبو وردة، 2011).

هناك دراسات حديثة تشير إلى وجود حوادث جنائية على مواقع الشبكات الاجتماعية مثلما وقع في الولايات المتحدة وكندا،حيث أظهرت النتائج الأولية وجود جرائم جنسية،القرصنة الحاسوبية،وأعمال العنف والتهديدات..إلخ. يضاف إلى هذا الاحتيال جرائم الملكية .وأن الشباب البالغين من بين المستخدمين الأكثر عرضة لهذه المخاطر المتصورة من انتهاك الخصوصية أو الأمن. فلا يبدو عائقا للمستخدمين والدليل أن عدد مستخدمي

مواقع التواصل الاجتماعي في نمو متزايد. لذلك تناولت عدة دراسات دوافع المستخدمين في نشر معلوماتهم على الانترنيت. (Tremblay, 2010 , Page.09 )

ويشير "عبد الرزاق محمد الدليمي إلى أن أكثر الأفراد تحديدا لمقدار وحجم المعلومات التي يكشفونها ويفشونها حول أنفسهم هم أكثر الأفراد احتفاظا بشعور الخصوصية،حيث يعتقد العديد من مستخدمي الفايسبوك "الضحايا" أن معلوماتهم ومحتوياتهم المنشورة ستكون محفوظة ومتاحة لمن يختارون فقط، خصوصا إذا كانت المعلومات شخصية جدا ومحرجة،لكنهم اكتشفوا بعد فترة أن تلك المعلومات اطلع عليها آخرون وأصبحت متاحة على الانترنيت،حيث يعمل الفايسبوك الذي ينظم إليه أكثر من مليون عضو شهريا، في طرح المعلومات المتعلقة بأعضائه علنا على محركات البحث على الانترنيت مثل "جوجل" و"ياهو"، بهدف الدخول المبكر في السباق لبناء دليل إلكتروني عالمي يحتوي على أكبر قدر ممكن من المعلومات والتفاصيل الشخصية مثل السير الذاتية وأرقام الهواتف وغيرها من سبل الاتصال بالشخص وهوايات الأعضاء وحتى معلومات عن أصدقائهم .( الدليمي، 2011، صفحة 43)

من جهتها توصلت الباحثة "إليزابات وارفار" إلى أن هناك بعض البحوث التي تفترض أن معرفة إعدادات الخصوصية متعلقة بنوع استخدام الفايسبوك.فكلما ازداد استخدام الشباب له، كلما ازدادت معرفتهم لتلك الإعدادات وخياراتها.ومهما تعددت أنماط الاستخدامات إلا أن جميع مستخدمي الفايسبوك يصرحون برغبتهم في الحصول على مستوى عالي من الحماية.( Elizabeth Warfel, ,2009,Page20 )

هي نتائج تؤكدها دراسة "دانا بويد" و "أزتار أرحيتي"، اللتان اتبعتا أفواجا من مستخدمي الانترنيت منذ أعوام وهم من مستخدمي الفايسبوك بين عامي 2009 و2010، وهي مرحلة عرف فيها الموقع تغيرات كثيرة في إعدادات التحكم في الخصوصية.وقد أخذت الباحثة بعين الاعتبار عملية التردد على استخدام الفايسبوك والتي أثرت على إجابات المبحوثين بعد عام. فالمستخدمون الدائمون للشبكة قد غيروا من إعدادات الخصوصية على بروفايلاتهم لتتماشى مع الإعدادات الجديدة التي يقترحها الفايسبوك لكونهم على علم بكل ما يحدث على عكس المستخدمين غير الناشطين على الموقع. (Hargittai , Boyd, 2010, Page 14 )

وقد تزايدت الأصوات المحذرة من إمكانية سوء استخدام المعلومات المنشورة عبر الشبكات الاجتماعية تحت شعار "فكّر قبل أن تنشر"،فمعظم الشبكات لديها ثغرات فيما يتعلق بحماية الخصوصية، فالشبكات تملك الحق أن تفعل ما تشاء بتلك المعلومات وهو الأمر الذي يعتبر تعدّياً صريحاً على الحقوق الشخصية، لذلك يرى الكثير من مستخدمي الفايسبوك الحذرين أنه يمكن أن يراقب ويستخرج البيانات لمشتركيه لاسيما وقد استطاع "إثنان"من معهد "ماساتشوستس" للتكنولوجيا من إثبات إمكانية الاطلاع على ملفات مستخدمي الموقع .حيث تمكن من تنزيل أكثر من سبعين ألف ملف شخصي من الموقع لأربع جامعات (معهد ماساتشوستس للتكنولوجيا وجامعة نيويورك وجامعة أوكلاهاما وجامعة هافارد)، كجزء من مشروع بحث عن الخصوصية في الفايسبوك والذي نُشر في 14 كانون أول عام2005.

كما أكد برنامج CLICE الذي يقدم من قناة BBC البريطانية إمكانية سرقة البيانات الشخصية لمستخدمي الفايسبوك،ومما زاد من قلق المستخدمين مسالة عدم قدرتهم على إلغاء معلوماتهم الأمر الذي يمكن للآخرين الوصول إليها وربما توظيفها لغير مصلحة أصحابها.

الخطير في الأمر هو أن الشباب العربي يجد نفسه مضطر تحت اسم مستعار ودون أن يشعر للإدلاء بتفاصيل مهمة عن حياته وحياة أفراد أسرته ومعلومات عن وظيفته وأصدقائه والمحيطين به وصور شخصية له ومعلومات يومية تشكل قدرا لا بأس به لأي جهة ترغب في معرفة أدق التفاصيل عن عالم الشباب العربي.(الدليمي، 2011،صفحة 40-41 ).

فمع تلاقي تكنولوجيا الاتصالات والحاسب الآلي و تطور وسائل التواصل الاجتماعي ازدادت معدلات جرائم تقنية المعلومات،الأمر الذي يفرض على سلطات التحقيق وأجهزة العدالة الجنائية تحديات ومخاطر كبيرة تتطلب اتخاذ الإجراءات والتدابير الكفيلة لمواجهة هذه المخاطر والحد منها، ومن أبرزها: سرقة الهوية والإعلانات الوهمية والنصب والاحتيال(حامد مصطفى ، صفحة08 -41).خاصة أثناء قبول دعوات من مجهولين على مواقع التواصل الاجتماعي،ما يمكن الطرف الآخر من اختراق جهاز الكمبيوتر الخاص للشخص المستقبل وبالتالي يمكنه استغلال المعلومات الشخصية في أشياء مشبوهة كحذف أو تغيير المعلومات.( حراز، 25 سبتمبر 2011)

## III. الإجراءات المتخذة للحد من خطورة الجريمة الإلكترونية :

أدى سرعة اتصال الشبكة العنكبوتية من دولة لأخرى إلى عدة اختراقات تتم بواسطة الحاسوب الآلي،وتتعدى هذه الجرائم الحدود الوطنية لتشمل الحدود الدولية.من هنا جاء الاهتمام الدولي بشأن هذه الجرائم لعقد اتفاقيات دولية في مجال حماية شبكات الانترنيت للتعاون والحد من الجرائم الإلكترونية مع اطلاع الجهات التي تضررت جراء هذه المخاطر ومكافحتها. أنظر: (بكر، 2004)

وترتيبا على ذلك لجأت القوانين المقارنة إلى تبني فكرة المساعدة القضائية والتعاون التشريعي والقضائي في مجال مكافحة هذه الجرائم ،حيث تم ابرام العديد من الاتفاقيات الثنائية والدولية من أجل إيجاد القانون الواجب التطبيق والقضاء المختص بها.كما تم عقد العديد من المؤتمرات والندوات في إطار مؤتمر الأمم المتحدة أو الاتحاد الأوربي أو الاتحاد الإفريقي للتصدي لهذه الجرائم ذات البعد العالمي.

من بين الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم الانترنت والحاسوب نذكر:

### 1. الشق التشريعي :

سنت عدد من الدول الأوربية قوانين خاصة بجرائم الانترنت والحاسوب مثل بريطانيا وهولندا وفرنسا والدانمرك والمجر وبولندا واليابان وكندا، كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الانترنت،و خطت خطوة إلى الأمام بإنشاء مراكز لاستقبال ضحايا تلك الجرائم. (مصطفى، سلمان، و الرحمن، 2011، صفحة 49)

**1.1. التعاون الدولي في مجال البحث عن الجريمة الالكترونية:**

تعد هذه الخطوة مهمة لخلق أساليب متشابهة لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية كون عدم التعاون سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول ما يعطي المجرمين فرصة الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية. (العزيز، 1414 هـ ، صفحة 113)

**2.1. اتفاقية بودابيست:**

تضمنت مجموعة من الاجراءات الخاصة بالبحث والتحري جاءت مضامينها مطابقة لمضامين الاتفاقية العربية خاصة القواعد الإجرائية من خلال نص المواد (16)إلى(21) المتضمنة سرعة التحفظ على بيانات الكمبيوتر المخزنة، تفتيش وحجز بيانات الكمبيوتر المخزنة،اجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة وغيرها. (يوسف، 2015، صفحة 186)

تهدف هذه الاتفاقية إلى توحيد السياسة التشريعية من أجل مكافحة الجرائم الإلكترونية المرتكبة في الشبكة وإلى تنسيق التعاون بين التشريعات الوطنية لتسهيل مكافحة الإجرام المعلوماتي وتطبيق إجراءات ملائمة لملاحقة الفضاء الافتراضي مع وضع نظام تعاون دولي يتميز بالسرعة الفعالة في التنفيذ.لمزيد من المعلومات أنظر: (بغدادي، 2018، الصفحات 89-90)

**3.1. المنظمة الدولية للشرطة الجنائية الأنتربول:**

أكدت على تعزيز وتشجيع التعاون بين أجهزة الشرطة بين الدول الأعضاء لمكافحة الجريمة خاصة جرائم الانترنيت.

**4.1. اتفاقية مجلس أوروبا بشأن الإجرام السيبيري لعام 2000:**

تعد الاتفاقية الوحيدة المتعددة الأطراف لمكافحة الجرائم التي تتم عبر الكمبيوتر أو شبكة الانترنيت دخلت حيز التنفيذ سنة 2004 على مستوى مجلس الاتحاد الأوروبي.وقعت على هذه الاتفاقية كل من كندا، اليابان،جنوب إفريقيا وصادقت عليها الولايات المتحدة الأمريكية.أكدت الاتفاقية على ضرورة احترام حقوق الإنسان والحريات العامة التي تضمنتها الاتفاقيات الدولية والتشريعات الوطنية. (السموني و الشرقاوي، د.ت، الصفحات 133-134)

**5.1. جهود الاتحاد الأوروبي:**

يعد من أهم الجهود الدولية لمكافحة الجريمة الإلكترونية،حيث قام بإنشاء قوة خاصة للجرائم المعلوماتية في دول الإتحاد يمتد عملها إلى كندا وأستراليا، ألمانيا، فرنسا،الولايات المتحدة الأمريكية، والمملكة البريطانية. (يونس، 2004، الصفحات 212-214)

**6.1. اتفاقية الاتحاد الإفريقي المتعلقة بمجال الأمن المعلوماتي وحملة البيانات الشخصية:**

اجتمع مجموعة من قادة الاتحاد الإفريقي مكونة من 54 حكومة افريقية ،وافقوا على الاتفاقية ، كما وافق مجلس وزراء الداخلية والعدل العرب في اجتماعهم بالقاهرة في 2001 على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ويتطرق في الفصل السابع منها للتعاون القانوني والقضائي في مجال مكافحة هذه الجرائم. (فاروق، 2015)

**7.1. ميثاق قانون مكافحة جرائم تقنية المعلومات الذي أقرته جامعة الدول العربية بمقر الأمانة العامة بالقاهرة في 2010/02/21:**

تهدف الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات،والحفاظ على أمن الدول العربية ومصالحها ومنع الجرائم الإلكترونية والتحقيق فيها مثل الاعتداء على سلامة البيانات ونشر أفكار جماعات إرهابية والدعوة لها،وجرائم إساءة استخدام تقنية المعلومات والتزوير والاحتيال. (خضران، 2015، الصفحات 92-93)

**8.1. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات:**

جاءت الاتفاقية لحماية المجتمع ومكافحة جرائم تقنية المعلومات التي تهدد أمن الدول العربية ومصالحهم، هذا جله تم صياغته في ديباجة الاتفاقية العربية لمكافحة جرائم المعلومات الصادرة بتاريخ 2010/12/21 في جمهورية مصر العربية، كما أدت هذه الاتفاقية إلى ميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان. وصارت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها سنة 2015 ليكتمل نصاب الدول السبع المطلوبة لسريانها. (مغازي، 2016)

هدفت الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات حفاظا على أمن الدول العربية ومصالحها. (العربية، 2010)

**2. الشق الأمني :**

إن مواجهة مخاطر الجرائم المعلوماتية تعتمد بشكل كبير على تبني إستراتيجية أمنية- مجتمعية متكاملة، والتي تعمل فيها أجهزة مكافحة الجريمة الرسمية في الدولة جنباً إلى جنب مع أفراد المجتمع ومؤسسات القطاع الخاص،وهو ما يمكن مكافحة الأنشطة الإجرامية في الفضاء الإلكتروني والتقليل من مخاطرها والحد من انتشارها.هذه الرؤية تتسق مع نتائج الدراسات التي أجريت في بلدان مختلفة من العالم حول التعامل مع جرائم الانترنت والتي أوضحت أهمية مشاركة العديد من المصادر والمؤسسات الخاصة في تحمل جزء من المسؤولية فيما يتعلق بمكافحة هذه الجرائم والسيطرة عليها. (القرني، 2014)

**3. تجربة الجزائر لمواجهة الجريمة الالكترونية:**

إن هذه الوسائل القانونية والقضائية لمكافحة الجريمة الالكترونية قد أقرتها الجزائر في قانون العقوبات في الشق المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال،حيث أقر المشرع الجزائري موضوع التعاون والمساعدة القضائية في مجال مكافحة الجريمة الإلكترونية وذلك في الفصل السابع من هذا القانون.كما أقر القانون الجزائري الحماية

القانونية لنظم المعلومات في قوانين خاصة منها قانون التأمينات الاجتماعية،قانون الملكية الأدبية والفكرية،القانون المتعلق بعصرنة العدالة والقانون المتعلق بالمواصلات السلكية واللاسلكية.لمزيد من التفاصيل أنظر: (رحيمة، 2017)

كخطوة أولى للحكومة الجزائرية لمواجهة ما يعرف بالجريمة الالكترونية صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 أوت 2009،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.إلا أن تجسيد بنوده على أرض الواقع ضعيف إلى حد الساعة بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها،واقتصرت العقوبات في أغلب الأحيان على الغرامة المالية. ويتضمن القانون 19 مادة موزعة على 6 فصول، أعده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاما خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية وعددت الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية.
بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية. (الرسمية، القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، 2009، الصفحات 5-8)

و نص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم.كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل. (الرسمية، 2009)

رغم اهتمام المشرع الجزائري بالجرائم الإلكترونية وبالعقوبات المقررة لها إلا أن النص عليها في قانون العقوبات أو القانون العام غير كافي لمواجهة الانتشار الرهيب والتطور السريع لهذا النوع من الجرائم الإلكترونية بل يجب اصدار قانون خاص بها مع وجوب تشديد عقوباتها نظرا للآثار السلبية التي تخلفها على أموال المؤسسات العامة وعلى خصوصية الأشخاص وشرفهم، وعلى أمن الدولة.ما يدعو أيضا إلى ضرورة تشريع قوانين جديدة تكرّس العقاب الصارم لكبح مثل هذه الجرائم لخطيرة والمدمّرة للفرد والمجتمع. لمزيد من التفاصيل إطلع على: (القادر و حسام، 2017، صفحة 83)

من بين الإجراءات التي اتخذتها الدولة الجزائرية أيضا نجد:

قيادة الدرك الوطني التي وضعت ملف الأمن المعلوماتي ضمن أولوياتها،حيث سارعت إلى مراجعة سياساتها الأمنية وإدراجها لآليات وميكانيزمات جديدة من شأنها مضاعفة أنظمة الرقابة التي تشكل تهديد لخصوصية الأفراد.

لذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي للأطر القانونية والتكنولوجية الملائمة خصوصا مع ازدياد استخدامات الافراد للتكنولوجيا الرقمية.(رضوان،2016،صفحة40-41).

فلم يعد للخصوصية مكان في عالم الجيل الثالث في الجزائر كون الشركات وحتى الأفراد باتوا معرضين لأكثر من أي وقت مضى لخطر الاعتداء على معلوماتهم الشخصية المخزنة عبر الانترنيت وهو ما يستدعي استعمال أقصى درجات الحيطة في منع ذلك،باستعمال الحلول التكنولوجية المتوفرة. فمختلف وحدات البحث على مستوى مصالح الدرك الوطني الجزائري تدعمت خلال السنوات الأخيرة بدركيين مختصين لمواجهة الجريمة الإلكترونية(غدير 2011 ) أُطلق عليها اسم "دركيو الأنترنيت" تابعين لفرقة البحث والتحري، مهمتها فضح الجرائم الإلكترونية عن طريق ما يسمى "بالتفتيش الإلكتروني" بواسطة تنشيط دوريات أمنية إلكترونية وذلك بعد تفشي ظاهرة نشر صور وابتزاز المواطنين عن طريق شبكة التواصل الاجتماعي الفايسبوك. (باشوش، 2011 )

وتجسيدا لذلك باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية والحد من انتشارها،وإنشاء أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الحاصلة في هذا المجال،حيث بادرت إلى تأمين وحماية الفضاء المعلوماتي للمستخدمين.

هناك العديد من الدراسات أشارت إلى أن خصوصية المستخدمين محل رصد مستمر لا يمكنه مقاومتها،خصوصا أنه يعرض ذاته على الشبكة رغم الوعي والدراية بالمخاطر التي يمكن أن يتعرض لها. لذا كثر النقاش حول ضرورة حماية الخصوصية والتوعية بالمخاطر الناجمة عن جرائم الحاسوب، ووضع حدود فاصلة بين المجالين العام والخاص،وإيجاد سبل كافية لحماية الهوية الرقمية الخاصة بالأفراد قصد رفع مستوى الأمن والحماية الشاملة للموقع.

من جهته صرح المدير التنفيذي و مؤسس فيسبوك "مارك زوكربرغ" عن ما قد يطرأ من تطورات على الموقع حين سُئِل عن مستقبل شركة فيسبوك و ما يطرأ عليها من تغييرات في المستقبل البعيد خلال جلسة عامة عقدت على صفحته ليجيب عن هذا السؤال بمفاجأة أذهلت الجميع ، عن توجه شركة فيسبوك للتوجه نحو "التخاطر الذهني" و "التواصل الذهني".

ما صرح به كان نتيجة ما يؤمن به: بأننا سنتمكن من التخاطر مباشرة من دماغ لدماغ باستخدام التكنولوجيا في يوم من الأيام،و أننا سوف نتمكن من إيصال رسائل سرية لمن نحب دون تطفل الآخرين، وأن ما يؤمن به سيكون نقلة كبيرة في مجال التواصل و التطور التكنولوجي. إن الهدف من تصريح "زوكربرغ" هو إشعار لما قد يقدم على فعله في السنوات القادمة بموقع الفيسبوك،و ذلك بهدف جعل التواصل بين الأشخاص أكثر خصوصية وأماناً من استخدام الحواسيب و الأجهزة الإلكترونية فقط و الاعتماد عليها، و ليست هذه بالفكرة المستحيلة أو الخيالية أو بعيدة المنال، فقد بُني التصريح على عدة دراسات جاءت بصدد موضوع التواصل أو التخاطر الفكري. فقد اكتشف العلماء طرقاً تمكن الحواسيب من ترجمة موجات الدماغ إلى أوامر و العكس،حيث أن جامعة "واشنطن"

الأمريكية تعمل حالياً على إنشاء نظام يتيح للباحثين إرسال إشارات دماغية لبعضهم وتبادل الأفكار عن طريق الانترنت( زكربرغ، 2019)

لإيجاد حل لهذا الخوف الذي يشعر به مستخدمو الفايسبوك، أعلنت مؤخرا شركة الأمن والحماية "تريند مايكرو" أنها وسعت شراكتها مع الشبكة الاجتماعية،لتقدم حلا أمنيا جديدا يدعى "هاوس كول" للمساعدة في اكتشاف الأنشطة الخبيثة وإبقاء مستخدمي الفايسبوك في أمان. حيث أن المستخدمين يقومون بتريليونات النقرات يوميا وهذا ما يساعد تلك البرمجيات الخبيثة على الانتشار.وسيتكامل "هاوس كول" مع "تريند مايكرو" مع أنظمة الفايسبوك القائمة لخفض تلك التهديدات والحد من خطرها على أمن المستخدم وخصوصيته عبر الكشف عنها وتنبيه المستخدمين لها. وسيقوم الموقع بتحديد المستخدمين المعرضين للتهديدات الإلكترونية وتنبيههم إليها، مع إتاحة الخيار أمامهم لتنزيل النسخة المجانية من "هاوس كول" على أجهزتهم. (فاضل، 2014 ).

في نفس السياق يشير الباحث إلى أن الفايسبوك بدأ بإطلاق أداة "التحقق من الخصوصية للجميع"، لمساعدة المستخدمين على مراجعة خصوصياتهم والتحكم بمن يمكنه مشاهدة المحتوى والمنشورات، حيث يبدأ معالج " بريفاسي شيكآب" بالظهور للمستخدمين عندما يدخلون للشبكة كنافذة منبثقة، وعند الضغط على "دعنا نفعلها" سيبدأ معالج التحقق، والذي سيستغرق دقيقتين على الأكثر.

على أن تبقى المواقع الاجتماعية بحدّ ذاتها صفحات إلكترونية تحتوي على برامج تزود المستخدم بأدوات تساعده في عمل ما يريده؛ فالمستخدم هو من يضيف القيمة لهذه المواقع ويجعلها أداة ينتفع بها هو ومجتمعه، فرغم الاتهامات التي تطارد هذه المواقع من انتهاك للخصوصية إلى التّجسس على البيانات الشخصية للمستخدمين،إلاّ أنّ قوتها تزداد يوما بعد يوم، ويزداد تعلق المستخدمين بها.

هذا ما يستدعي ضرورة الأخذ بعين الإعتبار التوصيات التالية:

-وجوب تعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلاءم مع أنواع الجرائم الالكترونية أو اصدار قانون خاص بالجرائم الالكترونية وطرق مكافحتها.

-انشاء محاكم متخصصة بالجرائم الالكترونية في كل المجالس القضائية لمجابهة هذه الظاهرة.

-تعزيز التعاون والمساعدة الوطنية والدولية في مجال مكافحة جرائم الانترنيت

-تكوين هيئة وطنية لمراقبة ومتابعة جرائم الانترنيت او هيئة استشارية في المجال القانوني والإجرائي في مجال مكافحة الجرائم الالكترونية.

**الخاتمة:**

من هنا نجد أن مواقع التواصل الاجتماعي أصبحت تشكل واقعا متميزا ربطت أجزاء العالم بفضائها الواسع حققت تفوقا على الوسائل الاتصالية التقليدية، ورغم إيجابياتها المتميزة إلا أنها تستعمل لأغراض غير مشروعة وذلك من خلال استغلال مواقعها بالاعتداء على أموال الناس ومصالحهم،وانتهاك خصوصيتهم،وكذا السطو على البيانات

والمعلومات،واستخدام أسلوب التهديد والابتزاز والقرصنة،أو بصفة عامة ما يعرف بالجريمة الإلكترونية أو الجريمة عابرة الحدود.

توصلت الدراسة إلى أن الجرائم المنتشرة في المجتمع مست جميع الشرائح خصوصا مستخدمي مواقع التواصل الاجتماعي الذين وقعوا ضحايا هذه الجرائم،وبالتالي تهديد أمن واستقرار المجتمع،فأصبحت هذه الجرائم من أكثرها انتشارا في المجتمعات المعاصرة.كما أن استخدام هذه الشبكات يمثل فرصة لاختراق خصوصية الأفراد والمساس بأمنهم وارتكاب عدة جرائم إلكترونية،الأمر الذي يستدعي اتخاذ آليات كفيلة للتصدي والحد من هذه الجرائم .

وتبقى شبكات التواصل الاجتماعي وسيلة مهمة، إن استحسن استعمالها تفيد الفرد والمجتمع، أما استعمالها في الجانب السلبي فهي تؤدي إلى أضرار جسيمة تضرب بالأخلاق وتهدد الفرد والمجتمع بفقدان خصوصيته ووجوده ويظل أسير المجرمين والمزورين الإلكترونيين.وتظل التوعية والرقابة وسن قوانين ردعية في هذا المجال أحسن وسيلة للقضاء على الجريمة الإلكترونية أو التقليل من حدة خطورتها.

فالتطورات الهائلة التي عرفتها التكنولوجيات الحديثة للإعلام والاتصال ورغم ما وفرته من تسهيلات،إلا أنها في المقابل فتحت الباب على مصراعيها لتطور أدوات ووسائل وسبل تنفيذ الجرائم الإلكترونية وجعلتها أكثر تعقيدا وصارت مكافحتها تبدو صعبة المنال إذا لم تتضافر جهود جميع الأطراف الفاعلة في الساحة المعلوماتية.وأمام هذا الوضع بات لزاما على حكومات الدول الإسراع في اتخاذ الإجراءات اللازمة لتطوير آليات التصدي لمثل هذه الجرائم وتعزيز التعاون الدولي في هذا المجال.

خلصت هذه الورقة البحثية إلى جملة من التوصيات أهمها:

-ضرورة نشر الوعي بين الأشخاص سواء طبيعيين أو معنويين بمخاطر التعامل مع المواقع السيئة والمشبوهة على الشبكات الالكترونية كون الجريمة الإلكترونية موضوع يحتاج إلى المزيد من البحث والتعمق من قبل الباحثين ودراسته من جوانب مختلفة والاعتناء به لتجلية الأحكام الشرعية الخاصة به.

-ضرورة تجريم كل الممارسات التي تشكل جرائم الكترونية لم ينص عليها قانون جرائم أنظمة المعلومات كالمضايقة الملاحقة الإلكترونية،التشهير،تشويه السمعة عبر مواقع التواصل الاجتماعي والتعدي على الخصوصية،وكذا الاحتيال الإلكتروني.

-ضرورة تبني الدول لفكرة انشاء جهاز خاص بالخبرة الجنائية للجرائم الإلكترونية التي تقع عبر المواقع الاجتماعية وتدريب أفراد الضابطة العدلية والنيابة العامة والقضاة وتأهيلهم على كيفية التعامل مع الجرائم الالكترونية وآليات جمع الأدلة والتفتيش والتحري والملاحقة والتحقيق والاستدلال.

-ضرورة تضافر الجهود بين الدول خصوصا الدول العربية برسم استراتيجيات ردعية،أو سن قوانين من شأنها حماية خصوصية الأفراد من الجرائم الإلكترونية التي تقع عبر المواقع وتسطير آليات وضوابط فعالة تقي الأفراد والمجتمعات من خطر الجريمة الإلكترونية التي تمتد وتتطور بامتداد وتطور التقنية والتكنولوجية.

-ضرورة إصدار تشريع يجرم ويكافح الجريمة الإلكترونية والقضاء على كل العناصر والكيانات من الوصول إلى أهدافها وإجهاض تحركاتها،ويختص القانون المقترح بمكافحة جرائم تقنية المعلومات وتنظيم حماية الفضاء الإلكتروني ومكافحة الجريمة الإلكترونية وأمن الفضاء المعلوماتي والجرائم المعلوماتية.وسن قواعد و قوانين ردعية لمعاقبة المجرم الالكتروني.

-توعية الجيل الصاعد بمخاطر الاستعمالات السلبية لشبكات التواصل الاجتماعي وتعزيز الآثار الايجابية لها والاستفادة منها في المجالات المختلفة والتوعية بشأن الجرائم الإلكترونية التي ترتكب عبر الشبكات لضمان تفاديها أو التقليل من الوقوع فيها.

**قائمة المراجع:**

باللغة العربية:

**الكتب:**

1-الشنيفي،عبد الرحمن عبد العزيز، أمن المعلومات وجرائم الحاسب الآلي، دون دار نشر، الرياض، 1414هـ.

2- الشوابكة أحمد أمين أحمد ، جرائم الحاسوب والانترنت الجريمة المعلوماتية، ، مكتبة دار الثقافة، عمان ، 2004 .

3-المومني نهال عبد القادر ، الجرائم المعلوماتية ،،دار الثقافة للنشر والتوزيع،د.م، 2008.

4-بن يونس، عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الانترنيت ، جامعة المنصور،كلية الحقوق، مصر، 2004.

5-جاسم الطائر جعفر حسن ، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة المعلوماتية، دار البداية، عمان، 2002.

6-جعفر حسن جاسم الطائر، تكنولوجيا المعلومات رؤية جديدة للجريمة المعلوماتية، دار البداية، عمان، 2007.

7-حسن الهاشمي، جبريل ،سلمي بنت عبد الرحمن محمد الدوسري:الشبكات الاجتماعية والقيم رؤية تحليلية، الدار المنهجية للنشر والتوزيع، الأردن ،2015.

8-خليفة الملط حمد ،الجرائم المعلوماتية، ، الإسكندرية، ط2 ، دار الفكر الجامعي ، د.م.دت

9-زيدان زيحة ، الجريمة المعلوماتية في التشريع الجزائري والدولي، د.ط، دار الهدى، 2001.

10-عبابنة محمود أحمد ، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005 .

11-عبد القادر المومني نهال ،الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ،الأردن، 2008.

12-عبيد الكعبي محمد ،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت،دار النهضة العربية، القاهرة د.ت.

13-عريان علي محمد ،الجرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية، 2004.
14-عمر محمد بن يونس، الجرائم الناشئة عن استخدام الانترنيت، دار النهضة العربية،القاهرة،2004،
15-نعيم سعيداني ،آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، 2012-2013.

**الرسائل والمذكرات:**

1-أدهم باسم نمر بغدادي،وسائل البحث والتحري عن الجرائم الإلكترونية،رسالة مقدمة للحصول على درجة الماجستير في القانون العام بكلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2018.
2-المالكي محمد بن أحمد خضران، رؤية استراتيجية لربط المعلومات الأمنية بين دول مجلس التعاون لمكافحة الجرائم الإلكترونية،رسالة ماجستير منشورة،جامعة نايف العربية للعلوم الأمنية، الرياض،2015.
3-فاريش رشيدة ، قاوش نورة ، تأثير مواقع التواصل الاجتماعي في انتشار الجريمة الإلكترونية في وسط المراهقين دراسة ميدانية بثانوية كريم بلقاسم بولاية البويرة، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام والإتصال تخصص اتصال مجتمع، كلية العلوم الانسانية والاجتماعية ، جامعة آكلي محند والحاج البويرة، 2017-2018.

**المجلات والجرائد:**

1-الدليمي محمد عبد الرزاق،"الفيسبوك والتغير في تونس ومصر" ، مجلة الاتصال والتنمية، Communication and Develppment ، العدد 03، دار النهضة العربية للطباعة والنشر والتوزيع، الزيدانية، بيروت، أيلول 2011.
2-السموني، خالد الشرقاوي، مكافحة الجرائم الإلكترونية على ضوء التشريعين الوطني والدولي، المجلة المغربية للإدارة المحلية والتنمية، العدد 102-127-137،(دت).
3-باشوش نوارة:" 5 سنوان سجن وغرامات مالية ضد المتورطين في السب والابتزاز والتشهير: "كومندوس" مدرب لمطاردة مجرمي "الفيسبوك" "، جريدة الشروق اليومي، العدد 6391 ليوم 20 جوان 2011، الجزائر.
4-حامد مصطفى خالد: "المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي" ،رؤى إستراتيجية، العدد02، مارس، دولة الإمارات العربية المتحدة.
5-حراز سلمى: "المطلوب تأمين الأنترنيت وحملة تحسيسية في أوساط الشباب: شبكات التواصل الاجتماعي تشجععلى انتشار الجريمة الإلكترونية"، جريدة الخبر، ليوم 25 سبتمبر 2011، الجزائر.
6- ج. رضوان، "الأمن السيبراني: أولوية في استراتيجيات الدفاع"، مجلة الجيش. العدد: 630 ،جانفي 2016.
7-سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الانترنيت أثرها وسبل مواجهتها، مجلة التقني، المجلد 24، الإصدار 9، 2011.
8-فاروق غدير: "القضية هي الأولى من نوعها في الجزائر: توقيف شاب شهر بصديقته السابقة على الفايس بوك"، جريدة الخبر، العدد 6391، ليوم الإثنين 20 جوان 2011، الجزائر.

9-فاضل زبير:" "تريند مايكرو" تحمي مستخدمي الفايس بوك"، جريدة الخبر، العدد7462، ليوم 13 جوان 2014، الجزائر.

10-قجاج يوسف، الإطار الإجرائي الدولي في مجال البحث عن الجريمة الإلكترونية، مجلة الفقه والقانون، العدد 28، 2015.

11-الإتفاقية العربية لمكافحة جرائم المعلومات الصادرة بتاريخ 2010/12/21 في جمهورية مصر العربية ، المادة الأولى.

12-الجريدة الرسمية، القانون رقم 09-04 المؤرخ في 05 أوت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47.

**المؤتمرات:**

1-حفوظة الأمير عبد القادر،غرداين حسام، *الجريمة الالكترونية و آليات التصدي لها. كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد في الجزائر العاصمة، مخبر الحوكمة العمومية والاقتصاد الاجتماعي، جامعة أبو بكر بلقايد تلمسان، يوم 29 مارس 2017 .*

2-عمر خلف فاروق، الآليات القانونية لمكافحة الجريمة الالكترونية، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية ، أشغال المؤتمر الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 2015.

**المواقع الإلكترونية:**

1-أبو وردة أمين:"الشبكات الاجتماعية تتبوأ الصدارة على الشبكة العنكبوتية" ، متاح على:
http://www.amin.org/articles.php?t=opinion&id=1338703 9.20101

2-زكربرغ يفجر مفاجأة.. مستقبل فيسبوك هو "تخاطر الأفكار" و"التواصل الذهني"، متاح على:
http://arabic.cnn.com/scitech/2015/07/02/facebook-telepathy, (28 .01 .2019 )

3-عبدالله بن فازع القرني، مواجهة جرائم الإنترنت: نحو إستراتيجية أمنية – مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض على الرابط http://www.alriyadh.com/912032 : بتاريخ 2014/02/21

4-عزة مغازي، عزة مغازي، قانون الجريمة الإلكترونية.. التورنت يحملك إلى طرة، مقال منشور على موقع المنصة على الرابطhttps://almanassa.com/ar/story/1019 : بتاريخ 2016/02/04

5-نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر،الجرائم الإلكترونية، طرابلس،24-25 مارس 2017 ، متاح على الموقع:
https://drive.google.com/file/d/1vhDOposSu1tFqVTq7N1eiJDVWZp_bKev/view

باللغات الأجنبية:

**Livres:**
1-Altman Irwin , Dalmas Taylor:Social penetration :The development of interpersonal relationships, New York: Holt ,Rinehart and Winston , 1973.
2-Real Del Louis Serge: Les réseaux sociaux sur internet, Alphée, la Passion d'éditer, Paris, 2010 .
**Revues :**
1-Boyd Danah, & Hargittai Ezter, :"Facebook Privacy Settings: Who Cares ?" , First Monday , 15, Vol. 15 , N°08, 2010.
2-Liu Hugo : " Social Network profiles as taste performances ", Journal of Computer –mediated communication , N°13, 2008
3-Warfel Elizabeth, :"Perceptions of privacy on Facebook" , Masters Abstracts International, Vol. 47 , N° 01,2009.
**Rapport:**
1-Tremblay Monica :"Réseaux sociaux sur Internet et sécurité de la vie privée ENAP" , Université de l'administration publique, Analyse des impacts de la mondialisation sur la sécurité - Rapport 9, Septembre 2010 .
**Sites :**
1-Boyd Danah Michel, Ellison Nicole: "Social Network Sites: Definition, History,andScholarship."Available :http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, (02.01.2019)