الجريمة الالكترونية عبر مواقع التواصل الاجتماعي ...نحو تفعيل دور الأمن السيبراني المعلوماتي

Cybercrime through social networking sites...towards activating the role of information cybersecurity

د.راضية حميدة

المدرسة العليا العسكرية للإعلام. الجزائر، radhiahamida6@gmail.com

تاريخ الاستلام 2021/08/23 تاريخ القبول 2021/11/09

الملخص:

ظهر جيل جديد من الجرائم اختلف عن الجرائم التقليدية واتسم بخطورته الكبيرة نظرا لصعوبة إثباتها إضافة إلى إشكالية الأمن المعلوماتي الذي مازال في بدايات ظهوره.

إن الأمن السيبراني عبر مواقع التواصل الاجتماعي أصبح حتمية ضرورية و هاجسا أمام رجال القانون خاصة مع الوتيرة المتسارعة لتداول المعلومات و الاستخدام العشوائي لمواقع التواصل و قصور وسائل الرقابة وضعف التشريعات القانونية و فرض العقوبة لتحجيم تأثيرات هذا النوع من الجرائم التي تستهدف الأفراد والدول .إذ تسجل يوميا حالات انتهاكات لبيانات شخصية و قرصنة لقاعدة و بنوك البيانات و المعطيات لمؤسسات وطنية بحيث أصبح الأمن القومي مهدد بهذه الممارسات الإجرامية ، التي استوجبت تجنيد آليات مواجهة الجريمة الالكترونية عبر مواقع التواصل و تبيان أساليب الحماية المعلوماتية أو ما يعرف بالأمن السيبراني و دوره في قمع التجاوزات و الجريمة المعلوماتية التي استحضرتها الممارسات السيئة لتكنولوجيا الاتصال.

الكلمات المفتاحية: الفضاء السيبراني-الجريمة الالكترونية – مواقع التواصل الاجتماعي – الأمن السيبراني والمعلوماتي –آليات القمع.

Abstract:

A new generation of crimes emerged that differed from traditional crimes and was characterized by its great gravity

It is difficult to prove, in addition to the problem of cybersecurity, which is still in its infancy.

Cyber security through social networking sites has become a necessary imperative and an obsession in front of lawmen, especially with the rapid pace of information circulation, the indiscriminate use of communication sites, the lack of means of control, the weakness of legal legislation and the imposition of punishment to limit the effects of this type of crime targeting individuals and countries. It is recorded

daily. Cases of violations of personal data and piracy of the database and data banks of national institutions, so that national security has become threatened, necessitating the recruitment of mechanisms to confront electronic crime through communication sites and showing methods of information protection or what is known as cyber security.

Keys Words: Cyber space - cyber crime - social networking sites - cyber and information security - repression mechanisms.

مقدّمة:

الجريمة السيبرانية هي إحدى الجرائم المعاصرة التي أصبحت تمثل خطرا على الفرد والمجتمع وعلى أمن الدولة ، إذ أنها تتقدم بوتيرة سريعة باستخدام أحدث التقنيات في تنفيذ هجمات سيبرانية ، لذا كان علينا مواكبة الفضاء السيبراني و التعرف على طرق التصدي لهذه الجرائم المستحدثة بسن القوانين والأنظمة التي تختص بمكافحة الجرائم السيبرانية وفرض العقوبات على المجرمين.

لقد سهل ظهور ما يعرف بمواقع التواصل الاجتماعي الفايسبوك عملية الاتصال و التفاعل بين أفردا المجتمعات سواء الوطنية أو الدولية، و هذا من خلال خدماتها المتاحة و تطبيقاتها التي قربت الأفراد و الدول و جعلت العالم غرفة صغيرة يتعارف فيها الأفراد، إلا أن هذه المواقع و التطبيقات باتت سلاحا ذو حدين، فعلى الرغم من القفزات النوعية التي حققتها، والتغييرات الإيجابية الكبيرة التي أحدثتها سواء على صعيد الدول أو الأفراد، إلا أنها وفي الوقت ذاته أتاحت الفرصة لظهور أنواع جديدة ومستحدثة من الجرائم الفنية، والتي تحمل طابع هذه التقنية المعلوماتية وتساير على الدوام تيار تقدمها، باعتمادها على الحاسب كأداة لارتكابها .فهذه المواقع، و التي ساعدت الدول على تطوير أجهزتها الاتصالية و الإعلامية، ساعدت في الوقت نفسه على تطور أساليب و أنماط الجريمة الإلكترونية، خصوصاً مع إقبال المجرمين على استثمار الوسائل ونظم الكترونية حديثة في تنفيذ مشاريعهم الإجرامية. فقد بادرت العديد من الدول، لمحاولة التصدي لهذه الظاهرة من خلال السعي لوضع تشريعات وقوانين تحد قدر الإمكان من حالات اقترافها. ومن هنا تتجلى أهمية الأمن الالكتروني في قمع الجريمة الإلكترونية .

و قد أطلق مصطلح جديد على هذه الاعتداءات الإلكترونية و هو مصطلح الجريمة الإلكترونية أو المعلوماتية أو السيبرانية نظرا لأنها تقع في المجال السيبراني. و التي تنتج من خلال استخدام المعلوماتية الحديثة المتمثلة في الكمبيوتر أو الاستعانة بأحد نظم المعالجة الآلية للبيانات و المعلومات أو أي وسائط إلكترونية أخرى في أعمال غير مشروعة .و هنا قد يمكن القول أن الجريمة الإلكترونية هي نفسها الجريمة التقليدية لكنها طورت من نفسها لتستعمل التكنولوجيا و تواكب العصر. و قد تعددت التسميات حول هذه الجريمة كالقرصنة على الإنترنت الجريمة المعلوماتية ـ

الجريمة الإلكترونية، الفيروسات الإرهاب الإلكتروني . و يتحجج مرتكب الجريمة عن فعله هذا بعدة أسباب كالبحث عن التقدير لنفسه بين أفراد المجتمع أو التحدي و اكتساب كثير من الأموال بطرق غير شرعية، كما تتميز الجريمة الإلكترونية عن غيرها من الجرائم بأنها، قليلة المخاطر، واحتمالية الكشف عنها ضئيلة. كما أنها لا تحتاج إلى أي عنف أو جثث أو سفك للدماء أو آثار اقتحام لسرقة الأموال ، إنما تحتاج لخبرة و دراية و احتراف في مجال استخدام الحاسب الآلي .و هذا ما سهلته الانترنت عامة و شبكات التواصل الاجتماعي و الفايسبوك خاصة و الذي يعتبر ملفا خاصا يحتوي معلومات شخصية حول الفرد (صور، أفلام حصص، برامج، كتب) . كما يتميز الفايسبوك بالتفاعلية و المشاركة بين الأفراد المنخرطين فيه و يتيح أيضا إمكانية التصويت و التعليقات و تبادل المعلومات كذلك إمكانية إضافة صديق أو البحث عن أي فرد موجود على شبكة الفايسبوك بواسطة بريده الالكتروني و التغذية الإخبارية التي تظهر على الصفحة الرئيسية لجميع المستخدمين فتقدم آخر مستجدات الصفحات أو المجموعات التي ينتمي إليها المستخدم . و للفايسبوك إيجابيات على المجتمع و على العلاقات التي تربط أفراده، فقد ساهم كثيرا و تلقائيا في عملية النشر الالكتروني من خلال نشر أفكار خاصة بالأفراد على صفحاتهم و حساباتهم الخاصة، التواصل الدائم بين الأفراد من خلال الرسائل وا لدعوات و ذلك لتنظيم التفاعلات و اللقاءات و النشاطات و مشاركة تفاصيل الحياة مع الأصدقاء من مستخدميه .

و بالرغم من هذه الإيجابيات إلا أن هناك الكثير من الآثار السلبية على مستخدميه منها إضاعة الوقت من خلال التنقل من صفحة لأخرى و من ملف لآخر دون إدراك للساعات التي تضيع دون فائدة له أو لغيره الإدمان وإضعاف مهارة التواصل و الحوار المباشر عند مستخدميه، فقضاء الوقت الطويل أمام شاشة الكمبيوتر و هدره في تصفح المواقع يؤدي لعزلهم عن واقعهم الأسري و عن مشاركتهم في المجتمع كما ساهم الفايسبوك كثيرا في انتشار الجرائم الإلكترونية من خلال سرقة المعلومات الشخصية و صفحات الأفراد باستغلال بريدهم الإلكتروني أو حتى أرقام هواتفهم و انتهاك الخصوصية من خلال إمكانية وصول للمعلومات واستغلالها في تقمص دور ذلك الشخص أو ما يعرف بانتحال الشخصيات، إذ لا تزال هذه العملية تضرب بقوة في الشبكة العنكبوتية و في مواقع التواصل متخذة منها مكانا خصبا للتهديد و الابتزاز كما يحدث في بعض الصفحات والتي تقوم بنشر المعلومات السرية و الخطيرة عن الأشخاص أو أعمالهم غير القانونية.

أهداف الدراسة : تهدف الدراسة إلى معرفة مفهوم الجريمة السيبرانية أو الالكترونية والاطار القانوني للجريمة السيبرانية ودارسة الجوانب الموضوعية من مفهوم الجريمة السيبرانية وخصائصها، وكذلك الجوانب الإجرائية ببان طرق التصدي للجرائم الالكترونية في الفضاء السيبراني.

أولا: تعريف الجريمة الالكترونية السيبرانية: إن مصطلح الجرائم السيبرانية هو إ حدى الم صطلحات الحديثة والمستخدمة عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإ جرام المرتبط والمتصل بتقنية المعلومات.

إن الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المرا حل الزمنية لتطور ها ، فكانت بداية من مصطلح إساءة ا ستخدام الكمبيوتر ، مرورا بم صطلح احتيال الكمبيوتر ، والجريمة المعلوماتية ، فا صطلاحات جرائم الكمبيوتر إ لى جرائم ا لهاكرز ، فجرا ئم الإنتر نت ، إ لى آ خر الم صطلحات ا لجرائم ا لسيبرانية . ولهذا فإننا نجد في كل مرة مع ظهور م صطلح جديد لجرائم الإنترنت يظهر لنا تعريفا جديدا ، ففقهاء القانون لم يستقروا على تعريف وا حد وذلك ير جع لحداثة ا لجرائم ا لسيبرانية و الاختلا فات الثقا فات وا لقوانين بين ا لدول ، وأيضا خشية في أن يحصروا المصطلح في نطاق ضيق أو محدد . فمنهم من عرف ا لجرائم ا لسيبرانية : بأنها " هي ا لتي تتم بوا سطة الكمبيوتر أو أ حد و سائل التقنية الحديثة ، وا لبعض الآ خر عرفها : بأنها " نشاط إجرا مي تستخدم فيه تقنية الحا سب الآ لي بطريقة مبا شرة أو غير مبا شرة كو سيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.[1]

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تتم الجريمة الإلكترونية. وكما يقول فان دير هلست و ونيف " هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة... وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف" .

ويتراوح تعريف الجريمة الإلكترونية بين ا لجرائم ا لتي ترتكب بوا سطة الحا سوب إ لى ا لجرائم التي ترتكب بأي نوع من المعدات الرقمية كما تعرف ا لجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال .

تتكون الجريمة الإلكترونية أو الافترا ضية cyber crimes من مقطعين هما الجريمة crimeوالإلكترونية cyberويستخدم م صطلح الإلكترونية لوصف فكرة جزء من الحا سب أو عصر المعلومات .أما الجريمة فهي السلوكيات والأفعال الخارجة على ا لقانون. وا لجرائم الإلكترونية هي المخالفات ا لتي ترتكب ضد الأ فراد أو المجموعات بدافع الجريمة وبقصد إ يذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (مثل غرف الدردشة، والبريد الإلكتروني.[2]

وتعتمد تعاريف الجريمة الإلكتروني في الغالب على الغرض من استخدام هذا المصطلح. وتشمل الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة . ويمثل جوهر الجريمةً أبعد من هذا الوصف فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية". [3]

ولقد خلص فان دير هولست ونفيه إلى أن: "حقل علم الجريمة يفتقر إلى التعريف المشترك والإطار المفاهيمي المتسق. ويستخدم ترسانة حية من المصطلحات، وتكون أحيانا فيكون على شكل تركيبة مع البادئات Préfixes مثل الإنترنت، والكمبيوتر، والبريد، والإنترنت، أو المعلومات الرقمية. حيث انتشرت هذه المصطلحات، وطبقت بشكل عشوائي، وهذا يعكس التداخل في المحتوى أو يعكس فجوات مهمة[4].

وتعتمد تعاريف الجريمة الإلكتروني في الغالب على الغرض من استخدام هذا المصطلح. وتشمل عددا محددا من الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة . ويمثل جوهر الجريمةً الإلكترونية. أبعد من هذا الوصف، ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية".

مصطلح " الجريمة الإلكترونية "حاولت العديد من الأعمال الأكاديمية تعريف " الجريمة الإلكترونية"، ومع ذلك فلا تبدو التشريعات الوطنية، مهتمة بتعرف دقيق للمصطلح. فمن أصل حوالي 200 مكون منبثقة من التشريعات الوطنية التي استشهدت بها البلدان في الرد على الاستبيان الدولي في تحديد معنى الجريمة الإلكترونية، أستخدم أقل من خمسة في المائة كلمة " جرائم الإلكترونية " في العنوان أو في السياق التشريعي وبدلا من ذلك فالاستخدام الأكثر شيوعا في التشريعات هو لمصطلح "" جرائم الكمبيوتر" والاتصالات الإلكترونية"، وتكنولوجيا المعلومات"، أو الجريمة ذات التقنية العالية. وفي الممارسة العملية ، فإن العديد من هذه المفردات من التشريعات التي حددت للجرائم الجنائية والتي هي المدرجة في مفهوم الجريمة الإلكترونية مثل الدخول غير المصرح به لنظام الكمبيوتر ، أو التدخل في نظام الكمبيوتر أو البيانات. حيث لم تستخدم التشريعات الوطنية على وجه التحديد مصطلح "الجريمة الإلكترونية" في عنوان فعل أو قانون مثل " قانون الجرائم الإلكترونية " ، ومن النادر أن

يتضمن جزء التعريفات تعريف الجريمة، وعندما يضمن مصطلح" الجريمة الإلكترونية " كتعريف قانون كان التعريف العام له ببساطة باسم " الجرائم المشار إليها في هذه القانون. وبطريقة مماثلة، فإن عددا قليلا جدا من الصكوك القانونية الدولية أو الإقليمية تعرف الجريمة الإلكترونية فلا اتفاقية مجلس أوروبا للجرائم الإلكترونية Convention Cyber crime Europe of Council واتفاقية جامعة الدول العربية ولا مشروع Draft African تضمنت تعريفا للجريمة الإلكترونية.فعرّفت ' الجريمة المتصلة بمعلومات الحاسوب ' بأنها ' العمل الإجرامي الذي يستهدف معلومات الحاسوب [5]

لقد جاء في توصيات مؤتمر الأمم المتحدة العاشر امنع الجريمة المنعقد في فينا 2000 تعريف الجريمة الالكترونية بأنها :"أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة ...و تشمل جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[6]

تأخذ الجريمة الالكترونية أشكالا متعددة يمكن تلخيصها فيمايلي:

- الدخول غير المشروع، اعتراض أو الاستيلاء على بيانات الحاسوب أو نظامه.
- إنتاج أو توزيع أو امتلاك لأدوات إساءة استعمال الحاسوب .
- اختراق الخصوصية أو أساليب حماية البيانات ذات الصلة بالحاسوب لمصالح شخصية أو مادية أو أذى الاحتيال المتعلق بالحاسوب أو التزوير.
- جرائم الحاسوب ذات الصلة بالهوية: حقوق الطبع والنشر أو جرائم العلامة التجارية .
- إرسال أو السيطرة على إرسال البريد المزعج .
- الإغراء أو استمالة الأطفال المتعلق بالحاسوب. التي تنطوي خطاب الكراهية الإنتاج أو توزيع أو حيازة المواد الإباحية عن الأطفال.
- دعم جرائم الإرهاب و جرائم ضد الحكومات تتمثل في مهاجمة المواقع الرسمية و أنظمة الشبكات الحكومية والتي تستخدم لمهاجمة البنية التحتية و هدفها غالبا ما يكون سياسيا.

أساليب المجرم السيبراني يستخدم المجرم السيبراني تقنية الاختراق لتنفيذ جريمته وذلك من خلال التحايل على الأنظمة المعلوماتية ، فيكون الاختراق بالقدرة على وصول هدف معين عن طريق ثغرات في نظام الحماية الخاصة ، و تتم عن طريق برنامجين الأول الخادم و هو بجاهز الضحية إذ ينفذ المهام الموكلة إليه ، والثاني يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد ،كما أنهم يستخدمون عدة برامج منها :

1 -حصان طروادة : وهو عبارة عن برنامج صغير مختبئ ببرنامج أكبر وتؤدي مهامها بشكل خفي في اطالق الفيروسات وا لدودة الـ تي تـ قوم بإر سال البيا نات عن الـ ثـغرات المو جودة في الـ نـظام ، وار سال كلمات المرور السرية الخا صة باـ لهدف ، و من أنوا عه القنا بل المنطق ية الـ تي يزرع ها الم برمج دا خل النظام الذي يطوره.

2- فيروسات الكمبيوتر : وهي برامج صغيرة تستخدم لتعطيل شبكات الخدمات

3- الديدان : وهي تتكاثر عن طريق نسخ نفسها عن طر يق الـ شبكات و هدفها الـ شبكات الما لـ ية مـ ثل البورصات.

4- الأبواب الخلفية : وهي ثغرة تترك عن عمد من مصمم النظام للتسلل إليه وقت الحاجة .

5- الاختناق المروري السيبراني : وهو سد وخنق الاتصالات لدى المستهدف بحيث ال يمكنه تبادل المعلومات 6 . - القصف السيبراني : وهو الهجوم على شبكة المعلومات بحيث يسبب ضغط كبير على الموقع فيفقد قدرة الموقع على استقبال الرسائل من العملاء ، وبالتالي يوقف عن العمل تماما[7].

- **أسباب الجريـمة الإلكترونـية** :هـناك عـدد مـن الأ سـباب الـ تـي يمـكـن حـصرها كأ سـباب للجريـمـة الإلكترونيـة منهـا مـا يقـع علـى مسـتوى كـوني، ومنهـا مـا يـ قـع عـ لـى مـ سـتوى مجتمـعـي، ومنـهـا مـا يقـع علـى مسـتوى فـردي أو شخصـي. كمـا أن أ سـباب الجريـمـة الإلكترونيـة تتفـاوت وفـق نوعهـا ونـوع المسـتهدف ونـوع الجـاني ومسـتوى تنفيـذه فـردي مجتمعـي ، كـوني. فـجرائم الـ شباب والهواة والصغار تختلف عـن أسـباب جـرائم المحتـرفين، وتختلـف وفـق هـدفها سـرقة أو معلومـات أو تجارة بالمعلومات أو شخصية.

البطالـة تـرتبط الجريمـة الإلكترونيـة شـأنها شـأن الجريـمـة التقليديـة بالبطالـة والـظروف الاقتصـادية الصـعبة. وتتركـز البطالـة بـين قطاعـات كبيـرة مـن الشـباب ، مـمـا يولـد مـ شاعر سـلبية عنـد شـرائح كبيـرة مـن النـاس ضـد الظـروف وضـد المجتمـع ممـا يـدفعهم إلـى أسـاليب تـأقلم سـلبية مـع هـذه الـظروف منـها الإتـجار الإلكترونـي بالبـشر والـجنس والجريـمة الإلكترونية وغيرها.

البحـث عـن الثـراء حيـث يـسعى الإنـسان إلـى المتـعـة ويتجـنـب الأ لـم هـكـذا تـقـول النظريـة العامـة فـي الجريـمـة لجتفرد سـون وهير شـي Gottfredson and Hirschi ويـسعى النـاس إلـى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا كما ترى نظرية الأنـومي لمير تـون. فالرغبـة فـي الثـراء يواجهـا صـعوبات بالغـة فـي تحقيقـه بـالطرق المقبولـة اجتماعيـا والقانونـية،

ولـذا يلجـأ بعـض النـاس إلـى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة[8].

- ضـعف تنفـيذ القـانون وتطبيقــه فــي الجريمــة الإلكترونيــة،هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تـتمكن مـن مجاراة التقدم فـي الجـرائم الإلكترونيـة وأ ساليبها. وهـذا لا يتوقـف عنـد التشـريعات وكيفيـة التعامـل مـع الأدلـة الرقميـة علـى المستوى الـوطني، كمـا هـو الحـالي علـى المستوى الـدولي .فممـا يغذي الجريمـة الإلكترونيـة غيـاب التشـريعات الجزائيـة والجنائيـة وضعف الممارسـات العدليـة والشـرطية .

- التحول الرقمـي للمجتمـع: دخل المجتمع اليوم عصـر المعلوماتيـة الجديـدة (أي الفضـاء الإلكترونـي أو العـالم الافتراضـي). فالنـاس يقضون جـزءا مـن حيـاتهم اليوميـة فـي الفضـاء الإلكترونـي، ينشئون الشـبكات والمواقـع ويتمتعـون بـأنواع جديـدة مـن العلاقـات الاجتماعيـة، وهـم علـى تواصل مع ما يجري فـي العـالم الخـارجي، والقيـام بـبعض الأعمـال. كـل مـن هـذه الأنشـطة قـد جعلـت مـن الممكـن للجميـع وبوجـود جهـاز كمبيـوتر أو مـودوم مـع معرفـة التقنيـة القليلـة .وبعبـارة أخـرى، فـإن شـبكة الإنترنــت هــي مــن خلقــت مــا يعــرف الآن باســم الفضــاء الإلكترونــي، أو العــالم الافتراض. يحتاج المجتمع لكـي يقـوم بوظائفـه إلـى أن يعـم الأمـن والأمـان وان يتحقـق النظـام والاسـتمرارية. ولا يتوقــف تــوفر الأمــن والأمــان فــي الواقــع المــادي للمجتمــع بــل أنتقــل ليشــمل العــالم الافتراضــي.

و هناك أسباب تتعلق بخصائص الجريمة الإلكترونية في حد ذاتها و فيما يلي مجموعة من خصائص الجرائم الإلكترونية والتي تؤدي إلى ارتكاب الجريمة الإلكترونية منها :

-الإزالة Removable الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط.

- التوافر Available المعلومات في كل مكان، جاهزة لتستفيد منها الجريمة .

-القيمة Valuable معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم...

-الديمومة Durable : المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة.

- سرعة التنفيذ: لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة علـى لوحـة المفـاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعنى أنها لا تتطلب الإعداد قبـل التنفيـذ أو استخدام معدات وبرامج معينة والتنفيذ عـن بعـد إذ لا تتطلـب الجريمـة الإلكترونيـة فـي أغلبهـا (إلا جـرائم سـرقة معـدات الحاسـب) وجـود الفاعـل فـي مكـان الجريمـة. بـل يمكـن للفاعـل

تنفيذ جريمته و هو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب.

طرق الجريمة الإلكترونية: في الفضاء السيبراني وتشمل على:

-تخريب المعلومات وإساءة استخدامها. ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية.

- سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني، أو الصناعي، أو العسكري، أو تخريبها، أو تدميرها.

- تزوير المعلومات ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب .

-تزييف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي

- انتهاك الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها .

- التصنت وتشمل الدخول لقواعد المعلومات و سرقة المحادثات عبر الهاتف و التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

- التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها و القصد منه اغتيال شخصية الأفراد أو الإساءة.

-السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية و سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها .

- قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى، قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

- خلاعة الأطفال وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة، وللإناث بشكل عام.

- القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملغومة إلكترونية لإحداث خلل في أداء المنظومة أو إتلاف مواردها المعلوماتية .[9]

- الإرهـاب الإلكترونـي و يشـمل جميع المكو نـات الـسـالفة ا لـذكر فـي بيـئـة تقـنـيـة متغـيـرة والـتـي تـؤثر علـى فرص الإرهاب ومصادره، هذه التغ يرات تؤثر ع لى تكتيكات الإر هاب وأ سلحته وأهدا فـه ومـن التكتيكـات الإرهابية ما يعرف بالإرهاب الإلكترونـي.

وتكمن أهداف الجريمة الالكترونية في الوصول إلى المعلو مات بـ شكل غـ ير شرعي و التلا عب بالمعطيات بغرض الابتزاز بهدف تحقيق الكـ سب الـ مادي أو المعـ نوي أو السيا سي عن طر يق عمليات الاختراق ز هدم المواقع على الشبكة العنكبوتية. أمّا المجرم فهو محترف له قدرات و مهارات النـ صب و الاحتيال على حقوق الملكية الفكرية و غيرها .[10]

و عند الحديث عن الجرائم الالكترونية المقترفة عبر موا قع التوا صل الاجتـ ماعي فإنـ ها تـ شمل جميع أشكال القذف والشتم و التهد يد و الابـ تزاز عـ بر البر يد الـ صوتي أو تكـ تب عـ لى صفحات ا لواب و يتحـ قق بذلك ر كن العلنـ ية ا لذي تطلـ به الكثـ ير من التـ شريعات وعليه يمـ كن تطبـ يق مواد الـ سب و القذف.[11]

ضف إلى ذ لك جريـ مة التهد يد و المـ ضايقة الـ تي تـ هدف إ لى زرع الـ خوف و الـ ضغط عـ لى إرادة الإنسان و جريمة صناعة و نشر الإباحـ ية و ما يتر تب عليها من جرائم اغتـ صاب الأطـ فال و القـ صر و الإدمان على تصفح المواقع الإباحية.[12] و جريمة انتحال شخصية الآخرين و شخصية المواقع .

ثانيا: الأمن السيبراني المعلوماتي بين الضرورة و التحدي:

يعد الأمن المعلوماتي من أهم المواضيع التي تشكل أساسا لاستراتيجيات الدول و المنظمات الدولـ ية و الإقليمية الحكومية و غير الحكومية لمواجهة مختـ لف المـ خاوف الـ تي تـ هدد ا ستقرار الفـ ضاء الرقـ مي، لذلك فإنّ الأمن المعلوماتي يرتكز على تعزيز الحماية الناجمة عن تدابير الحد من مخاطر التكنولوجـ يا الرقمـ ية و تطبـ يق العمليات القائـ مة عـ لى ضمان سرية و سلامة المعلو مات و البيا نات من الهجـ مات الالكترونية ، بحـ يث يتـ عاظم دور و مكا نة الأ من المعلو ماتي بتـ طور التكنولوجـ يات الحديـ ثة في ظل الحكومات الالكترونية التي تستدعي آليات التصدي للتهديدات الرقمية مثل الجرائم المنظـ مة كغـ سيل الأموال و التحريض العنصري و الإباحية الالكترونية.

لقد أضحى هاجس توفير الأ من للمعلو مات يقـلق بال الكثـير من المؤسـسات و الحكو مات و الأشخاص و ظهر مصطلح الأمن المعلوماتي للتعبير عن المحافظة على دقة و سرية و توفير البيا نات ضد أي مؤثرات سواء كانت متعمدة أم عرضية و يعتبر هذا الموضوع من المواضيع المتجددة في عالم تقنية المعلو مات خا صة و إن علم نا بأ نه شاع ا ستخدامه في نـطاق أنـشطة معالـجة و نـقل البيا نات بواسطة أنظمة الحاسوب [13]، كما نجد أنه يشير إلى توفير السرية و الموثوقية للمعلو مات و اكتمالـها و ضمان استمرارية وجودها .[14]

مفهوم أمن المعلومات :

تتعدد تعريفات أمن المعلومات وتتنوع حسب زاوية الرؤية، فنحن إذا نظرنا من زاو يـة أكاديمـية سنجد أنه العلم الذي يبحث في نظر يات وا ستراتيجيات توفير الحما ية للمعلو مات من المـخاطر الـتي تهددها ومن أنشطة الاعتداء عليها.ولو نظرنا من زاوية تكنولوجية وفنـية بـدـقة يمكنـنا تعريـفه عـلى أنه الوسائل والأدوات والإ جراءات المطـلوب توفير ها لـضمان حما ية المعلو مات من الأخـطار الداخلـية والخارجـية،[15] و من الزاو ية القانونـية نـجد التعر يف قد أ خذ منـحى آ خر لكو نه يركز عـلى الـتدابير والإجراءات التي من شأنها حماية سرية وسلامة وخصوصية محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة المعلوماتية.

وبشكل عام يمكن الـقول إن الأ من المعلو ماتي هو تـلك ا لرؤى والسيا سات والإ جراءات الـتي تصمم وتنفذ على مستويات مختلفة، فردية ومؤسسية ومجتمعية، وتستهدف تحقيق عنا صر الحما ية والـصيانة المختـلفة الـتي تـضمن أن تـحـقق للمعلو مات الـسرية أو الموثوقـية [16]، أي التأ كد من أن المعلومات لا تُكشف ولا يُطَّلع عليها من قبل أشخاص غير مخولين بذلك. والتكاملية و سلامة المحـتوى أي التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعا مل ا لداخلي مع المعلو مات، أو عن طر يق تدخل غـير مـشروع. أ ما الا ستمرارية فتعـني توفر وإتا حة المعلومات أو الـخدمات المبنـية علـيها لمـستخدميها والمـستفيدين منـها والتأ كد من ا ستمرار توفر ها وا لنظم الـتي تـخدمها وا ستمرار الـقدرة عـلى التفا عل معـها والتأكـيد كذلك عـلى أن مـستخدمها لن يتعرض إلى منع الاستخدام أو الحيلولة بيـنه و بين ا لدخول إليـها، كـما تعـني أيـضا ضمان عدم إنـكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنه هو الذي قام بهذا التصرف.

ثالثا: واقع الأمن السيبراني المعلوماتي:

قدرت الفاتورة الإجمالية لجرائم أمن المعلومات عالميا وعربيا في 2011 بحوالي 388 مليار دولار أميركي أما التكلفة النقدية المباشرة لهذه الجرائم والمتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فتقدر بحوالي 114 مليار دولار. ومعنى ذلك أن القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين، والتي تقدر بحوالي 288 مليار دولار، وتقترب من قيمة السوق العالمية للمخدرات عموما والتي تصل إلى 411 مليار دولار، وأعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة "اليونيسيف" بحوالي 100 ضعف، حيث تصل ميزانيتها إلى 3.65 مليار دولار، كما تعادل هذه الخسائر ما تم إنفاقه خلال 90 عاما على مكافحة الملاريا وضعف ما تم إنفاقه على التعليم في 38 عاما.

وقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة واعتداء في الساعة، تأثر بها 589 مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل 9٪ من إجمالي سكان العالم. وقد توزعت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضاروجرائم الاحتيال والنصب والاصطياد (الحصول على معلومات بنكية سرية)، والجرائم المتعلقة باختراق الهواتف المحمولة.

ولقد شهد العام 2011 الكثير من الحوادث والمواجهات في عالم أمن المعلومات، حملت الكثير من الدلائل على أن الأمر تخطى كل الحدود المعتادة، وصار جولات صراع مكشوفة بين الدول وبعضها البعض، حتى أن جرائم المعلومات باتت أداة جديدة في الصراع السياسي والاقتصادي[17].

فعلى سبيل المثال إذا ما أخذنا بعين الاعتبار ما تم اكتشافه بخصوص فيروس دوكو ، فسنجد أن نتائج الدراسات الخاصة بحماية البنية التحتية الحساسة مقلقة، إذ الغرض الذي صمّم من أجله فيروس دوكو هو جمع المعلومات الاستخباراتية ومعلومات عن الأصول من منظمات معيّنة مثل الشركات المصنّعة للمكونات التي توجد عادة في بيئة التحكم الصناعي، كما أن من يقفون وراء هجوم دوكو كانوا يبحثون عن معلومات مثل وثائق التصميم التي يمكنها أن تساعدهم في المستقبل لشن هجوم على منشآت التحكم الصناعي. ويمثل "دوكو" الجيل الأحدث من ستكسنت (Stuxnet) الذي ذكرت تقارير عديدة أن الأميركيين استخدموه في إحداث فوضى داخل البرنامج النووي الإيراني, وفي هذه المرحلة فإن من غير المبرّر الاعتقاد بأن من يقف وراء هجوم "دوكو" لم يتمكن من الحصول على المعلومات الاستخباراتية التي يبحث عنها، وإضافة إلى ذلك فمن المحتمل أن هجمات أخرى لجمع المعلومات قد بدأت بالفعل ولم يتم اكتشافها بعد.

العلاقة بين الأمن السيبراني والأمن القومي: يمكننا القول إن اتساع قضية أمن المعلومات وتطورها على هذا النحو الخطير عالميا وعربيا يعود إلى أمرين:

- الأول: أن أغ لب دول ا لعالم -بـ ما فيـ ها ا لدول العربـ ية- تر فع حا لـ يا شعار التـ حول إ لى مجتـ مع المعلومات والمعرفة وتنفذ خططا واسعة النطاق لتحو يل هذا ا لشعار إ لى وا قع، و فى خـ ضم هذه الخطط يتم إنشاء سلاسل من قواعد البيانات القومية الكبرى، كما يـ جري تـ طوير شبكات الاتصالات ونـ شر الإنتر نت عـ بر خـ طوط الاتـ صالات العاد ية والـ سريعة، وتتـ جه الأ مور لتعـ ميم خدمات نـ قل الـ صوت عـ بر بروتو كولات الإنتر نت، وتنـ شط ا لدول في نـ شر مـ فاهيم و خدمات الحكومة الإلكترونية، وتـ صدر قوانين التوقـ يع الإلكترو ني ا لذي يمـ هد الطر يق صوب تفعـ يل أنشطة التجارة والأعمال الإلكترونـ ية عـ لى نـ طاق وا سع وتتو سع في مـ بادرات توفير الحا سب لفئات المجتمع المختلفة بالمنازل والمدارس وللمهنيين، كما تتبنى عشرات من برامج التنمـ ية المعلومات ية المتكام لة في مخت لف ا لوزارات و الهيـ ئات.

- الثاني: أن تشييد بنية معلوماتية قومية واسعة المـ جال وتبـ ني التو جه نـ حو مجتـ مع المعلو مات نقل المجتمع والدولة والمؤسسات إلى مرمى المخاطر، وحتم عليها مواجـ هة التـ حديات الـ شاملة والواسعة النطاق في أمن المعلومات بمعنى أن تحديات أمن المعلومات في مجتمع يمتـ لك بنـ ية معلوماتية واسعة يجعله يواجه تهديدات في أمن المعلو مات تتـ سم بالـ شمول والاتـ ساع وعـ مق التأثير وتنوع الأدوات وتعدد مصادر الهجوم وأدواته وغزارة الأهداف التي تشكل إغراء ومـ ناطق جذب لمن يستهدفونه، فمخاطر أمن المعلومات في عصر مجتمع المعلومات تضمّ مستويين:

- مستوى تعقب وجمع المعلومات، ويشمل الوسائل التقليدية لجمع المعلومات التي تعتمد بشكل كبـ ير على العناصر البشرية من الجواسيس و و سائل الا ستطلاع الحديـ ثة و فى مـ قدمتها الأقـ مار الـ صناعية التي تطورت بشكل كبير, حيث بلغت الصور والمعلومات الواردة منها حدا فائقا من الـ جودة والد قة لم تبلغها من قبل، كما يشمل هذا المستوى العديد من أدوات تعقب وجـ مع من دا خل البنـ ية المعلوماتـ ية الأساسية للجهة المستهدفة ومنها "البوابات الخلفية" ويقصد بها الثغرات أو نقاط الضعف الأمنية الـ تي توجد بشبكات ونظم المعلومات والبرامج المختلفة و"الر قائق الإلكترونـ ية" الـ تي تعتـ بر الـ جزء الـ حيوي بجميع أجهزة التعامل مع المعلومات من حاسبات ومعدات بناء شبكات وو سائط تـ خزين وغير ها والـ تي يمـ كن ا ستخدامها في تعـ قب وجـ مع المعلو مات وأدوات التلـ صص عـ لى شبكات المعلو مات وعملـ يات الاعتراض.

- مستوى يستهدف إفساد وتعطيل المعلومات، وتستخدم فيه العديد من الأدوات كفيروسات الحاسب والاختراق المباشر لشبكات المعلومات والهجوم بفيض الرسائل والطلبات وهجمات الاختناق المروري الإلكتروني على نطاق واسع وغيرها.

وكما هو واضح فإن هذه الأخطار لا تتوقف عند كونها تهديدا لأمن المعلومات داخل شركة أو مؤسسة أو منشأة بل تعد تهديدات جدية للأمن القومي للدول والمجتمعات ككل.

وتضعنا المعطيات السابقة أمام حقيقة واضحة وهى أن تحقيق تقدم ملموس في قضية أمن المعلومات عالميا أو عربيا لن يتم إلا بتغيير المنهج القائم حاليا والذي يتعامل مع القضية باعتبارها قضية "تقنية بحتة" تقع مسؤوليتها على الفنيين والمختصين في علوم الحاسب وتأمين الشبكات، والانتقال للأخذ بالمنهج الذي يعتبر أمن المعلومات ركيزة أساسية من ركائز الأمن القومي الشامل، ومن ثم يتعين رفعها من مستوى التعامل "الفني والتقني"، إلى مستوى التعامل السياسي والاستراتيجي، وألا تترك للتعامل العفوي غير الخاضع لاستراتيجية أو سياسة وطنية عامة ترشد مساره.

لقد أخذت الدول العربية على عاتقها -كما سبقت الإشارة- تنفيذ خطط وبرامج متنوعة تسعى لتشييد ما يمكن أن نطلق عليه (بنية معلوماتية قومية شاملة على كل المستويات) تتغلغل في مفاصل المجتمع وشرايينه الرئيسية والفرعية وتضطلع بعبء تداول المعلومات التي يديرها ويستخدمها، وكل هذه الأمور تقلص فارق الأهمية بين ما هو معلومات أمنية وعسكرية محضة تتجه الأنظار لحمايتها تلقائيا، وبين ما هو معلومات مدنية ارتقت أهميتها بحكم شموليتها وضرورة استمرارية إتاحتها لتصبح موردا حيويا يوميا بالغ الأهمية والتأثير في مجموع الشعب ككل أي تصبح المعلومات المتداولة داخل البنية المعلوماتية المدنية ركيزة من ركائز الأمن القومي التي يتعين حمايتها وتأمينها بمنظور استراتيجي كما هو الحال مع المعلومات العسكرية والأمنية.

من هنا يصبح من الخطأ تخطيطيا وإداريا أن تنشط أي دولة في تشييد بنية معلوماتية قومية متعددة الأوجه والمستويات على هذا النحو ثم لا تطور سياسة أو استراتيجية قومية لحماية هذه البنية وصيانة أمنها وأمن ما يتداول داخلها من بيانات ومعلومات، وتترك ذلك للتصرفات العفوية والمبادرات الفردية والمشروعات والخطط الجزئية المنفرطة التي تجري هنا أو هناك دون سياسة أو استراتيجية واضحة، فالبنية المعلوماتية الأساسية الشاملة تتطلب بالتبعية سياسة أمن معلوماتية شاملة، وليس هناك أدنى مبالغة في القول بأن المضي قدما في تشييد بنية معلوماتية قومية ضخمة بلا استراتيجية أمنية شاملة وكافية يشكل خللا جسيما في مسيرة التنمية المعلوماتية، ويؤثر سلبيا على الأمن القومي، لأنه يجعل البنية المعلوماتية القومية -وهى تتحول مع الزمن إلى مورد استراتيجي للدولة- كيانا هشا يمكن أن يتعرض لانكشاف أمني في كل أو بعض جوانبه.

وبما أن مخاطر أمن المعلومات باتت ترقى إلى مستوى تهديد الأمن القومي ككل، فإن و سائل المواجهة والحماية لابد وأن تظللها منظومة أمن قومي، لأنه من الخ طأ أن ت كون الأخ طار والتهد يدات شاملة وربما منسقة ومخططة أحيا نا ثم تأتي سبل وو سائل مواجهتها جزئ ية وعفو ية وخال ية من التخطيط وتفتقر للتنسيق والر شد، و قد قدمت اليا بان نموذ جا لـ هذا الم ستوى من التعا مل مع أ من المعلومات حينما أعلنت منذ أوائل أكتوبر 2005 البدء في تنفيذ برنامج شامل ع لى م ستوي مؤسسات وهيئات الدو لة وال شركات الخا صة ي ستهدف ال تدريب صد الهج مات الإلكترون ية لـ شاملة بتنويعاتها المختلفة سواء بالفيروسات أو عمليات القر صنة والتل صص والتج سس الاقت صادي وهج مات تعط يل شبكات الاتصالات والمعلومات وجاء هذا البرنامج التدريبي المستمر حتى في إطار استراتيجية متكاملة لأمن المعلومات باليابان تنفذها الدولة حماية لاقتصادها .[18]

لقد أ صبح من ال ضروري المحاف ظة ع لى المعلو مات و توفر ها و در جة موثوقيتها ، حـ يث أن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة و تقلص من اختراق المعلومات و التلاعب بها .كـ ما أنّ أ من المعلو مات هو ق ضية تبـحث في نظر يات و ا ستراتيجيات توفير الحما ية للمعلومات من المخاطر التي تهددها و من أنشطة الاعتداء عليها. إضافة إلى تكريس ترسانة قانون ية تحمي سرية المعلومات و سلامة المحتويات من خلال ت شريعات حما ية المعلو مات من الأن شطة غ ير المشروعة.[19]

يمكننا الجزم بأنّ الغاية الأساسية من الأمن المعلو ماتي تتلخص في الإجا بة عن ال سؤال : ما ا لذي نريد أن نحميه؟

و بالنظر إ لى الا ستخدام المتزا يد لـ شبكات التوا صل الاجت ماعي من ق بل شرائح المجت مع و بف ضل الخصائص التي تتميز بها هذه المواقع و التي نذكر منها : التفاعلية و المشاركة و الانف تاح و المحاد ثة [20] فلقد أصبح من السهل اختراق حسابات المستخدمين و انتحال الشخ صية و ابـتزاز الأ فراد و لا سيما منهم الأطفال و استدراجهم من قبل مجهولين .

لذلك أصبح من الضروري إتـ باع ا ستراتيجية وطن ية م ستعجلة لـ ضمان الأ من المعلو ماتي و ذ لك من خلال:

- وضع أسس قوية لبرنامج أمني يتضمن تفاصيل شاملة للمعايير و الإجراءات التقنية.
- تحديد مسؤوليات مختلف الأج هزة و الإدارات فيما تع لق بـ شروط ال سرية و التعا مل مع المعلو مة و البيانات التي تستقطب اهتمام القراصنة أو المجرمين الرقميين.

- مراقبة التهديدات و التعامل معها بصرامة و جدية مع التأكيد على وضع خطط استباقية لحل الأز مات المتعلقة بالاختراقات الالكترونية فور وقوعها . و أخذها على محمل الجد .فلا مجال للتقاعس .

- وضع منظومة أمنية متوافقة و ملتزمة بالسياسة الأمنية و التعليمات الخاصة بها ، مع الحرص على تكوين شرطة مختصة في الأمن المعلوماتي و توفير كل الإمكانات التكنولوجية و الترسانة القانونية لتطبيق العقوبات وقت اقتراف الجريمة الالكترونية لتحقيق مرونة الأداء و صرامة التطبيق و ردع المجرم .

و كما هو معروف فإنه ليس هناك حماية مطلقة في مجال التكنولوجيات الحديثة و أمن الشبكات ، فالمطلوب هو الحرص على تحقيق الفاعلية في حماية بيانات مستخدمي الشبكة و على وجه الخصوص المواقع الاجتماعية للتواصل و لن يتأتى ذلك إلاّ عن طريق الوعي و التدريب.

-توعية الأفراد بمخاطر مواقع التواصل الاجتماعي و المشاكل التي قد تواجهه على إثر استخدامهم لهذا الموقع وتوعية مستخدمي موقع الفايسبوك بضرورة إخفاء معلوماتهم الشخصية عن الأشخاص الغرباء و عدم محادثتهم حتى لا يكونوا عرضة للجريمة الإلكترونية.

- يتعين إدخال مادة أخلاقيات الانترنت ضمن المناهج الدراسي في التعليم و نشر الوعي بين صفوف المواطنين خاصة الشباب بمخاطر التعامل مع الصفحات و المجموعات السيئة عبر موقع الفايسبوك .

- ضرورة زيادة الجهود الدولية لمكافحة الجرائم الإلكترونية من خلال مجموعة تشريعات وطنية واتفاقيات إقليمية .

- تخصيص شرطة علمية ضبطية وقضائية مؤهلة في التعامل مع الجرائم الإلكترونية .

- استشراف رؤية جديدة لأساليب ومناهج وأدوات تداول المعلومات بين أطراف المجتمع وبعضها البعض داخليا وكذلك مناهج وأدوات وأساليب إدارة و تداول المعلومات بينها و بين الجهات الخارجية، كشركاء السياسة والتجارة والأعمال والتعليم والبحث العلمي والتصنيع...، وهذه قضية مهمة ومعقدة في آنٍ معا، ولا يصح تركها لاجتهادات أفراد ومؤسسات وخبراء من هنا وهناك مهما علا شأنهم وتجاربهم وقدراتهم، بل تحتاج جهدا مؤسسيا لن يتحقق على النحو المطلوب إلا عندما تتبوأ قضية أمن المعلومات مكانها الصحيح كركيزة أساسية للأمن القومي.

إنّ القانون وحده لا يكفي لمحاربة الجريمة الالكترونية لأنه يبقى يعاني من التلاعب القانوني و الاصطلاحي، وصعوبة تحديد الفاعل لقدرته على التخفي و عدم سهولة إثبات النوايا بسهولة ، كما ـنّ القانون تواجهه مشكلة من نوع آخر و هي إمكانية حدوث تغيرات على مستوى الوسائل الالكترونية و طرق التعامل معها ممّا لا يتماشى مع القوانين التي سنّت في فترة سابقة ، لذلك كان من الضروري توفير آلية الأمن المعلوماتي التي تنطلق من مسؤولية الفرد المستخدم لمواقع التواصل الاجتماعي و ذلك بالامتثال لأخلاقيات استخدامها و نذكر مثلا:

- إجراء دورات تدريبية حول استخدام الحاسوب بطريقة أمنة.
- توعية الشباب و خاصة الأطفال بخطورة الجريمة الالكترونية و ببشاعة الاعتداءات التي تطالهم.
- عدم استخدام الأسماء و الصور و المعلومات الخاصة على صفحات الواب إلاّ للضرورة.
- تغيير كلمة السر من حين لآخر، التشفير و التخزين الاحتياطي للمعلومات.
- عدم الانسياق وراء الإعلانات المغرية و التي تنشرها جهات مجهولة.
- عدم دخول مواقع مشبوهة لأنها الواجهة التي يستخدمها القراصنة و المجرمون.
-القيام بمسح دوري على جهاز الكمبيوتر.
-تعزيز التعاون الدولي في مجال مواجهة القرصنة و الجريمة الالكترونية و تبادل الخبرات و التجارب في مجال مكافحة و ردع الجريمة.
- التدريب و التكوين للكوادر البشرية في مجال الأمن المعلوماتي و استحداث شهادات عليا متخصصة في مجال التقنية و القانونية المتعلقة بمكافحة و اجتثاث الجرائم الالكترونية.
- تنظيم حملات توعية لمستعملي الوسائط الالكترونية و تعريفهم بحجم خطورة التهديدات التي تترصد بهم
وذلك من خلال تنظيم ملتقيات و ندوات و أيام دراسية حول الأمن المعلوماتي و دوره في التصدي للجرائم الالكترونية.

خاتمة :

في الختام يمكننا القول أن الفايسبوك شبكة اجتماعية واسعة المجالات و متعددة الخدمات ساهمت كثيرا في تقريب الأفراد، توطيد العلاقات و خلق صداقات جديدة و غيرها من جهة ،و من جهة أخرى أصبح مكانا خصبا يستغله أصحاب التفكير الذكي و المتحكمين في جهاز الحاسب الآلي و الإنترنت و الميالين للإجرام الإلكتروني لارتكاب أفعالهم و جرائهم ضد مستخدمي هذه المواقع سواء كانوا من أقاربهم أو أصدقائهم و على اختلاف أجناسهم و أعمارهم. و بالرغم من هذه الإيجابيات إلا أن هناك الكثير من الآثار السلبية على مستخدميه منها إضاعة الوقت من خلاا التنقل من صفحة لأخرى و من ملف لآخر دون إدراك للساعات التي تضيع دون فائدة له أو لغيره، الإدمان و إضعاف مهارة التواصل و الحوار المباشر عند مستخدميه، فقضاء الوقت الطويل أمام شاشة الكمبيوتر و هدره في تصفح المواقع يؤدي لعزلهم عن واقعهم الأسري و عن مشاركتهم في المجتمع، كما ساهم الفايسبوك كثيرا في انتشار الجرائم الإلكترونية من خلال سرقة المعلومات الشخصية و صفحات الأفراد باستغلال بريدهم الإلكتروني أو حتى أرقام هواتفهم و انتهاك الخصوصية من خلاا إمكانية وصول للمعلومات واستغلالها في تقمص دور ذلك الشخص أو ما يعرف بانتحال الشخصيات، إذ لا تزال هذه العملية تضرب بقوة في الشبكة العنكبوتية و في مواقع التواصل متخذة منها مكانا خصبا للتهديد

و الابتزاز كما يحدث في بعض الصفحات و التي تقوم بنشر المعلومات السرية و الخطيرة عن الأشخاص أو أعمالهم الغير قانونية.

وانطلاقا مما سبق يمكن رصد بعض التوصيات التي تندرج تحت لواء آليات مكافحة و ردع الجريمة السيبرانية التي تمس بالأمن الوطني و القومي أهمها: إنشاء هيئة وطنية مختصة بالجرائم السيرانية تشمل على :

- مركز استقبال جميع البالغات المتعلقة بالجرائم السيبرانية .
- كوادر من الفنيين والتقنيين يمتلكون الخبرة والمهارة العالية في المجال السيبراني . خبراء معنيين في مجال الاستدلال والتحقيق السيبراني .
- اعتماد المحاضر الموثقة من الهيئة الناتجة من التحقيق كأوراق رسمية تقدم لدى المحكمة المختصة.

الهوامش والمراجع :

1- محمود أحمد القرعان ، (2017)،الجرائم الإلكترونية ، ط1،دار وائل للنشر والتوزيع: عمان ، ص 11.

2-Halder, D., & Jaishankar, K. Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global..2011

3-UNODC United Nations Office on Drugs and Crime(...2003) .**Comprehensive Study on Cybercrime**. United nations

[4] موسى ذياب البداينة ، **الجرائم الالكترونية : المفهوم و الأسباب** ، ورقة علمية في ملتقى دولي حول الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية و الدولية. الأردن.2-2014/9/4.

5- UNODC United Nations Office on Drugs and Crime(2013.)، **Comprehensive Study on Cybercrime.** United nations.

[6] خالد عياد الحلبي،(2011.) **إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنيت**،دار الثقافة للنشر : الأردن. ص30.

7- خالد حسن أحمد لطفي ، (2020.) **الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية** ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ،ص 43.

8- M. R Gottfredson. and T. Hirschi(1990), **A General Theory of Crime**, California: Stanford University Press..

9- حسن مظفر الرزو، **القانون العراقي و المفاهيم المعلوماتية لجرائم الفضاء الافتراضي بالحاسوب**، مؤتمر القانون العراقي وتطور المجتمع، جامعة الحدباء، 2001/3/25/21. الموصل.ص 11.

10- أمير فرج يوسف، **الجريمة الالكترونية و المعلوماتية و الجهود الدولية لمكافحة جرائم الكمبيوتر و الانترنيت**،ط1، مكتبة الوفاء للنشر: الإسكندرية ، بدون سنة.ص 121.

11- محمد الكعبي ، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت** ، دار النهضة العربية: القاهرة.ص 88.

12- محمد منشاوي، **جرائم الانترنيت من منظور شرعي و قانوني**، http://www.ba-menoufia.com/books-pdf

13-عبد الرحمن بن عبد اللّه السند، (2005) **أحكام تقنية المعلومات ، الحاسب الآلي و شبكة المعلومات**، رسالة دكتوراه في الفقه المقارن، جامعة الإمام محمد بن سعود الإسلامية، المعهد العالي للقضاء،.ص.30.

14- D.Marcus Odom Anand Kumar and Laura Saunders, **Web assurance seals.How and Why they influence consumers decisions? Journal of information systems**. Vol 16.No 2. Fall 2002.p.231-250.

15السالمي علاء عبد الرزاق،(2008)،**الإدارة الالكترونية** ، دار وائل للنشر، الأردن ،ص 281.

16- غيطاس محمد جمال،(2007)،**عصر المعلومات القادم مذهل أكثر**، مركز الخبرات المهنية :القاهرة.ص58.

17- حقائق و أرقام، http/www.csooline.com/cybersecurity

18- شريف درويش اللبان، **خبرة عربية منقوصة، أمن المعلومات في ظل تحديات البيئة الرقمية**، المركز العربي للبحوث والدراسات، 2015. http://www.acrseg.org

19-مريم نريمان نومار: **استخدام مواقع الشبكات الاجتماعية و تأثيره في العلاقات الاجتماعية**، مذكرة ماجستير في علوم الإعلام والاتصال غير منشورة، جامعة الحاج لخضر: باتنة . 2012 ، ص 14.