مجلة الرواق للدراسات الاجتماعية والإنسانية | EISSN 2602-6767 ISSN: 2437 - 0363 | المجلد 09 / العـدد: .. (2023)، ص 90- 109

التدابير الأمنية للحماية من الجريمة الالكترونية في الوسط الجامعي.

Security measures to protect against cybercrime in university settings.

ط.د برادة عبد الرزاق [1*]، د.سالى مراد [2]، د. صيشي يسري [3]

[1] جامعة غليزان (الجزائر)، abderrezaq.brada@univ-relizane.dz

مخبر الدراسات الاجتماعية والنفسية والأنثروبولوجية

[2] جامعة خميس مليانة (الجزائر)، mouradsali@yahoo.com

[3] جامعة شلف (الجزائر)، sichiyousri@gmail.com

تاريخ الاستلام: 2022/10/29 تاريخ القبول: 2023/03/24 تاريخ النشر: 2023/06/17

ملخص:

تهدف الورقة البحثية إلى التحقيق في الجرائم الإلكترونية من حيث مفهومها والتدابير الأمنية للحماية منها في الوسط الجامعي فطلاب جامعيون في جامعات الجزائرية يشهد تنوع في العادات والأنماط استخدام الإنترنت بشكل عام.

كما تهدف إلى تحديد مفهوم الجريمة الإلكترونية من وجهة علم الاجتماع في وتفسيرها المختلفة وهذا، بطبيعة الحال، يتطلب الشعور بماهية الجريمة في الوسط الجامعي وتحديد التدابير الأمنية التي تحقق الامن للمنظومة الرقمية للمؤسسة الجامعية.

كلمات مفتاحية: الجريمة الإلكترونية، التدابير الأمنية، الجامعة، تقنيات الجريمة، الوسط الجامعي.

Abstract:

The research paper aims to investigate cybercrime in terms of its concept and security measures to protect it from it in university settings. University students in Algerian universities experience a variety of customs and patterns of Internet use in general.

It also aims to define the concept of cybercrime from the standpoint of sociology and its different interpretation. This, of course, requires a sense of what crime is in the university environment and the identification of security measures that provide security for the university institution's digital system.

Keywords: Cybercrime; security measures; university; crime techniques; university center.

*المؤلف المرسل

1. مقدمة:

منذ أن بدأ الإنسان في استخدام الإنترنت وحياته في تغير مستمر ومتسارع، وهذا واضح وقابل للملاحظة في الواقع من خلال سهولة الوصول إلى المعلومات التي تتناول كافة مناحي الحياة الفكرية والاجتماعية والسياسية ...إلخ، سواء أكانت هذه المعلومات، متجاوزا بذلك بعدي الزمان والمكان، وفي ذات السياق يستطيع الفرد نشر أفكاره وتبادلها بكل يسر وسهولة وقد شهدت هذه الشبكة تحولات جذرية منذ بداية القرن الحادي والعشرين عندما ظهر ما يسمى، بوسائط التفاعل الاجتماعي والتي تتيح للفرد حرية التواصل مع الآخرين بشكل مباشر.

فالتغيرات التي طرأت على عملية التواصل و التفاعل بين أفراد المجتمع الواحد، من خلال استعمال الوسائط الالكترونية التي بدورها غيرت التفاعل الاجتماعي الواقعي، إلى تفاعل اجتماعي افتراضي من خلال منصات التواصل الاجتماعي التي تعتبر أهم نتائج التغير الاجتماعي وتطور التكنولوجي ، فالوسائط التكنولوجية هي الوسائل والتقنيات التكنولوجية الحديثة ذات المنفعة الإنسانية التي واكبت التطور العلمي، ومن بين هذه الوسائل الحاسوب و الهاتف...إلخ ، بالإضافة إلى الوسائط المتعددة ، قصد وصول المعلومة المراد توصيلها ، بسرعة وبأقل تكلفة كخاصية أساسية تميز التفاعل كأحد مميزاتها.

كمأن الوسائط الالكترونية لم تغير الفرد والتفاعل فقط وإنما أثرت حتى على تركيبة الوسط ، من وسط الواقعي إلى الوسط الرقمي ، وأصبحت كل المؤسسات تعتمد على المراسلة الالكترونية ،وتبادل الرقمي، وتحويل الرقمي...إلخ ، كلها مفاهيم جديدة صاحبت استخدام الانترانت، ومن بين هذا الوسط الذي شهدا هذا نوع من تغيرات هو الوسط الجامعي من حيث الجامعة كمؤسسة ، فهي الآن تعتمد على المواقع الالكترونية خاصة بها وبكليتها في إعلام وإعلان بإضافة إلى مستودعاتها الرقمية التي تحفظ باينتها وحيث تسهل في

توصيل المادة علمية للفاعلين بها، من طلبة وهيئة البيداغوجية بإضافة إلى الهيئة التدريسية المخول لها عملية التكوين الأكاديمي.

لكن وبرغم من أن التحول الرقمي والوسائط الالكترونية، يعتبر من النواتج التطور الرقمي، بحكم التسهيلات والمنافع التي كانت موجهة للتسهيل عملية التواصل، التي تخطت كل الحدود السياسية والإقليمية أبانت مع مرور الوقت العديد من السلبيات ،وزيادة في حدة تطور عديد من الظواهر التي تعتبر خطر على حياة الفرد وأبرزها الجريمة الالكترونية ، فمعروف ان الجريمة قد صاحب الإنسان منذ القديم ، الآن مفهوم الجريمة الالكترونية هو مفهوم جديد صاحب الوسائط الالكترونية التي أصبح يستخدمها الفرد في عملية التفاعل .

تعتبر الجريمة الالكترونية كل سلوك او فعل يمارسه الفرد أو يتعرض إليه من خلال استعمال الانترانت والحاسوب حيث يكون الفعل مخالف للقانون، المعمول به في البلاد وبحكم ان الجريمة الالكترونية أصبحت ذا صدي واسع من طرف وسائل الإعلام التي تعرض دائما عديد من الضحايا الذين يتعرضون الى هذا نوع من الجرائم بإضافة إلى الإحصائيات وتقرير الأمن الوطني ووزارة الدفاع الوطني ،الذين ينوهون دائما بحذر من سواء الاستخدام للوسائط، والمواقع الالكترونية من خلال التوعية بمخاطرها

2 . مشكلة الدراسة:

الفرد اجتماعي بطبعه حيث تفرض عليه تفاعل مع مكونات المحيط الاجتماعي ، وخاصة الجامعيون و أفراد الهيئة التدريسية والإدارية منهم باعتبارهم مكون الأساسي للوسط الجامعي، حيث أنهم يتأثرون بما يصلهم من اختراعات واكتشافات في مجال التكنولوجيا الرقمية، ويحاولون تعرف هذا العالم، والانخراط في اكتشاف أسراره ولعل أبرز التغيرات ،التي حدثت في مجال الإنترنت ظهور ما يسمى وسائط التواصل الاجتماعي، التي يعتقد أنها وراء كثير من التغيرات وهناك تباين في الهدف من استخدامها فبعضهم يستخدمها من أجل تكوين جماعات وصداقات غير تقليدية يبثون من خلالها أفكارهم ومشاريعهم ،ويعبرون عن مشاعرهم تجاه القضايا التي تهمهم، أو بهدف التسلية والمتعة،

أوكمصدر للتعلم ، أو غير ذلك، لكن أصبحت هذا نوع من التفاعل تهدده العديد من المخاطر أبرزها الجريمة الالكترونية ،التي نالت اهتمام الباحثين ومختصين في علم الاجتماع حيث يدفعنا هذا إلى طرح المتسائل التالي: ماهية الجريمة الالكترونية؟ وما علاقتها بالوسط الجامعي؟

حيث نهدف من خلال هذا الإشكال إلى الإجابة عن التساؤلات الفرعية التالية:

أ- التعريف بمفهوم الجريمة الالكترونية وأدوات التي تمارس بها هذا نوع من الجرائم.

ب- التعريف مفهوم سوق الجريمة الالكترونية وتحديد مكونتها كمفهوم حديث بنسبة لقاموس علم الاجتماع.

ت- التعريف بالوسط الجامعي وتحديد الإجراءات الأمنية للحماية من الجريمة الالكترونية.

3. **المفاهيم الإجرائية :**

- وسائط التواصل الاجتماعي: هي عبارة عن مجموعة من التطبيقات العملية التي تقوم على أسس التكنولوجيا الرقمية، وتعتمد على الشبكة العنكبوتية والتي تسمح بإنتاج المحتوى، وتغيير هذا المحتوى الذي تم توليده بوساطة المستخدم.
- الجريمة الالكترونية: اي افعال يتم تسهيلها او ارتكابها باستخدام جهاز كومبيوتر باعتباره واسط الكترونية يمكن ان يكون الجهاز عامل للجريمة .
- سوق الجريمة الالكترونية: هو عبارة عن المحيط الافتراضي الذي يتفاعل فيه كل من المجرم والضحية والمرقبين الضابطين له وتكون مهمته الردع.
- أدوات الجريمة الالكترونية: هي الوسائل والبرامج التي يعتمد عليها الجاني في عملية ممارسته للجريمة عبر الانترانت والتي بدورها تخالف الأدوات المستعملة في الواقع المادي.

- الإجراءات الأمنية: هي الوسائل وأساليب الحماية التي يعتمد عليها الفرد للحماية نفسه من الهجمات الالكترونية.
- الوسط الجامعي: هو المحيط الذي يتفاعل فيه كل من الطلبة لهيئة التدريسية والإدارية.

4. مفهوم الجريمة الإلكترونية

إن لتطور السريع الذي شهده مجتمع المعاصر في عديد من جوانب وخاصة في جانب التكنولوجي ،فقد جلب هذا التطور الكثير من وسائل الراحة في حياتنا مثل الحوسبة والأنترانت، وهذا من ناحية الايجابية لها ومع ذلك ، فقد تسببت أيضًا في حدوث مشكلات وزيادة في حدة عديد من الظواهر التي تهدد استقرار البنية الاجتماعية حيث أصبح يصعب حلها والحد منها وعلى سبيل مثل: ظهور أنواع جديدة من الجرائم فعلى غرار الجرائم المعروفة في الوسط الاجتماعي)السرقة والاحتيال...الخ) فقد أكسبهم التطور التكنولوجي شكلا جديد ،فمن حيث المفهوم فقد أصبحت تدعي "بالجرائم الإلكترونية" وعلاوة عن هذا برزت علاقة تفاعلية بين الظاهرة الإجرامية و وتكنولوجية المعلومات فكلما تستمر هذه التكنولوجية في التطور ، تؤدي إلى تغير في القضايا الجنائية من حيث بروز ممارسين جدد لهذا النوع من الجرائم أي "مجرمين" يقابلها عددًا متزايدًا ومتنوعًا من "ضحايا" نظرًا لأن هذه التكنولوجيا تقدم سهولة ومرونة التنقل بنسبة لمستخدميها وأصبحت وسيلة للمجرمين لتحقيق أهدافهم غير المشروعة. فعولمة الظاهرة الإجرامية عن طريق محو الحدود الدولية وجعل مراقبتها أكثر صعوبة، من خلال الكشف أو المنع أو القبض على مجرمي الأنترانت .H) Çakir, E. Sert, 2010p143)

تمكن تكنولوجية المعلومات الأجهزة الإلكترونية وغيرها من المنتجات عالية التقنية كأجهزة الكمبيوتر والهواتف والإنترنت وجميع أنظمة المعلومات الأخرى المطورة لمنفعة الإنسانية فهي عرضة لنشاط الإجرامي، على الرغم من أن "الجريمة الإلكترونية" أصبحت

عبارة شائعة اليوم، إلا أنه من الصعب تعريفها بدقة. تم تطوير معظم التعريف الموجودة بشكل تجريبي.

حيث عرف كل من جوردون وفورد الجرائم الإلكترونية على أنها: "أي جريمة يتم تسهيلها أو ارتكابها باستخدام جهاز كمبيوتر أو شبكة أو جهاز" حيث قد يكون جهاز الكمبيوتر أو الجهاز هو عامل الجريمة، الميسر لجريمة أو هدف الجريمة، ومن خلال هذا التعريف يمكن اعتبار الجريمة الإلكترونية هي نشاط أجرامي و جريمة تمارس بواسطة الأنترانت أو نظام الكمبيوتر أو تكنولوجية الكمبيوتر(Becker & Landes,2006,p14)

لكن هناك من يري للجريمة الإلكترونية هي نتيجة لنشاطات السيبرانية للفرد من خلال مواقع الويب والشبكات الاجتماعية وتطبيقات الدردشة والمدونات والألعاب عبر الإنترنت والمراسلين والبريد الإلكتروني وتعد مشكلة أخلاقية تتجمع فيها العديد من الأسباب: يمكن أن تنشئ أشكالًا من التمييز ،الإساءة ، والترهيب ، والتهميش ، وأخرى ، تغيب فيها صفات الأنسانية وتبرز جانب الغير الأخلاقي للفرد عادةً ما يكون لدى الكارهين نية إيذاء المجموعة أو الشخص الآخر و من إظهارها ككائن قابل للتطبيق لمزيد من الهجمات ، بما في ذلك الهجمات الجسدية في العالم "غير الافتراضي ."

ومع ذلك ، فإننا نسمح بإمكانية مشاركة الأشخاص عن غير قصد في الإنترنت ، من خلال التواصل بلا مبالاة بطرق من شأنها أن استخدام تعبيرات مسيئة بطبيعتها وتعرض الآخرين كهدف قابل للتطبيق لمزيد من الهجمات. يمكن متابعة (Cyberhat) من قبل أفراد واحد ومع ذلك ، فإن السيبرانية لها طابع حركي بشكل أكثر شيوعًا. كظاهرة الكراهية العلنية بذلك إظهار هدف المرء ، في الوقت نفسه يستدعي انتباه الكارهين الآخرين ، ويشجعهم على أن يصبحوا نشطين ضد نفس الأهداف أو أهداف مشابهة أيضًا، علاوة على ذلك ، يمكن للنشاط الجماعي المتمثل في الكراهية معًا أن يزيد من قوة الكراهية وحزم الكارهين في إلحاق

الضرر بأهدافهم إلى حد كبير، السيبرانية هي أيضًا ظاهرة تسمم متبادل (Dilek et al., 2015p23)

ومن خلال هذا يمكن إعطاء تعريف إجرائي من الباحث للجريمة الالكترونية فالجريمة هي مرحلة تطورية للجريمة التقليدية من حيث أدواتها والمسرح ممارساتها و أصبحت لا تتقيد بالحدود السياسية والجغرافية كما عرفت تنظيم واسع من حيث تشكل المجرمين و تواصلهم بحكم العولمة التي كان سبب بارز في تغيرها حيث أصبح المجرم يعتمد على الانترانت والوسائط الالكترونية كالحاسوب والهاتف واللوحات الالكترونية التي تعتبر تقنيات ذات منفعة إنسانية إلى أن استخدام السيئ لها من طرف المنحرفون الكترونيا أدت ببروز ظاهرة الجريمة الالكترونية وتطور أنواع هذي الجريمة حيث حافظت الجريمة على تقليدها الكلاسيكي مثل (السرقة العنف الرمزي) إلى إن تنوعت أشكال مرساتها مثل(السرقة الالكترونية العنف الرمزي بالتعليقات العنصرية.....الخ)

5. وسط الجريمة (سوق الجريمة الإلكترونية)

يعتبر مفهوم "السوق" من المفاهيم الدخيلة على قاموس علم الاجتماع، وقد برز مفهوم سوق للجريمة في أعمال العالمين الاقتصاديين الأمريكيين غاري بيكر (Gary. Becker) تحت عنوان" الجريمة والعقاب مقاربة اقتصادية" أما بنسبة للعالم أساحق ايرليش (Isaac Ehrlich)جاء عمله بعنوان " الجريمة والعقاب وسوق الجرائم" ويعتمد "نموذج السوق للجريمة" على خمسة افتراضات رئيسية نسبة للأفكارهم.

•حيث يرى ان سوق الجريمة هو تفاعل بين الجناة الذي يعتبر مقدم للخدمات الغير القانونية والضحايا المحتملون وهو مشتري السلع وكما يعتبر القانون مجموعة من القواعد التي تضبط وتحسن السلوك في البيئة الافتراضية .

•كمان، الجناة المحتملون عادة ما يشكلون توقعات(التنبؤ) حول الفرص النسبية بنسبة للخدمات للقانونية وغير القانوني المقدمة عبر الأنترانت، بما في ذلك شدة العقوبة

واليقين، بناءً على المعلومات المتاحة، وبالتالي فهم يربطون التوقعات الذاتية والفرص الموضوعية.

•إضافة الى هذا، يكون تفضيل الجناة المحتملون بين الوقوع في الجريمة أو تفضيل السلامة الجنائية خلال أي عملية تخالف القوانين الوضعية .

•وبحكم الجريمة عامل خارجي مزعزع للاستقرار، فإن تطبيق القانون هو تحقيق للمصلحة العامة وحماية للأشخاص متفاعلين في الواقع الافتراضي .

•حيث تضمن الأحكام المجمعة لسلوك جميع الأطراف ذات العلاقة توازنًا واضحًا. تؤدي هذه الافتراضات إلى توازن في نموذج الجريمة.

فمن خلال أفكار نموذج السوق الجريمة التي تري أن تفاعل الضحايا المحتملون و تعاقدهم فالمعاملات غير المشروعة التي يقدمها الجناة لا تتم بالضرورة في الأماكن المادية (العالم الواقعي) يتم التعاقد أيضا في العالم الافتراضي ، كما يمكن تنسيق السلوك الذي يسير عليه للموردين والمطالبين وجعلها متسقة بشكل متبادل حيث يقول بيكر .Gary) (Beckerفي هذا الصدد "يتحقق التوازن فقط من خلال التفاعل بين الجناة و تنفيذ قانون، في الواقع" فكلما كان ردع من طرف مؤسسات الكفيلة بمحاربة الجريمة الإلكترونية لكل ممارس لنوع من أنواع جرائم باستعمال الحاسب وشبكة العنكبوتية في العالم الواقعي ويقصد أن كلما كان ردع للأفعال الممارسة في الواقع افتراضي كان هناك استقرار في البيئة الافتراضية(Becker & Landes, 1974p20)

أما إيرليش يري سوق الجرائم الإلكترونية على أنه هو" محيط تفاعل بين فئة الأفراد الغير المجرمين والضامنين للقانون الوحيدين الذين يتدخلون في هذا السوق ,Ehrlich) 1996p46).

أما في التعريف الإجرائي للمفهوم سوق للجريمة الإلكترونية هو المحيط الذي يتفاعل فيه كل من الجاني و الضحية و الضامنين من القانونين بصفتهم المرقبين وكل فرد من الأفراد

يجب أن تتوفر فيهم خصائص التي إذا غابت تقع الجريمة فالسوق يعتبر المحيط الافتراضي الذي يجمعهم فالضحية هو عنصر الأساسي فيكون هدف من طرف الجاني ومحمي من طرف الضامنين من القانونين فبحكم أن سوق الالكتروني يقدم العديد من الخدمات للضحية مثل التجارة والتحويل المالي وشراء عبر الانترانت كلها تعاملات يمارسها الضحية في هذا السوق تستوجب عليه أن يتوفر فيه الوعي السيبراني من حيث وسائل الحماية التي يعتمد عليها في حماية بطاقته وحسابه المصرفي بإضافة إلى الأشخاص الذين يتعامل معهم ومواقع الالكترونية التي يقتني منها أغراضه يجب أن تكون موثقة في حالة تقيد بهذه الشروط فتكون نسبة وقع ضحية للجريمة بنسبة ضئيلة وتحدث الجريمة الإلكترونية.

أذا قدم الجاني خدمة غير قانونية للضحية وتكون هذي خدمة إما سلعة وهمية على مواقع الكتروني أو عمولة مالية قام الضحية من خلالها بتحويل المالي ولم تقدم له الخدمة بإضافة إلي غياب الردع القانوني للجاني في الواقع المادي يؤدي إلى اختلال التوازن بين الفاعلين في الواقع الافتراضي وبهذا يزيد من حجم المجرمين مستغلين للثغرات القانونية تتبعها سقوط عديد من الضحايا الجريمة الالكترونية.

6. مكونات وسط الجريمة الإلكترونية

1.6مجرم الإنترنت:

المجرم الإلكترونية مفهوم واسع يشمل جميع الإفراد التي يُحتمل أن يرتكب جريمة على نظام الكمبيوتر أو عن طريقه وسائط متصلة بشبكة الانترانت حيث تتنوع أشكال الجرائم الإلكترونية التي يمارسها. حيث يعتبر سلوكه راجع لسوء استخدامه للوسائط الالكترونية حيث تعتبر هذي ممارسات انتهاكات ،وتتعدد في عديد من الصور والأشكال بما في ذلك خروقات البيانات والنظام وأجهزة الكمبيوتر (القرصنة) ، تزوير بيانات الكمبيوتر ، الاحتيال أجهزة الكمبيوتر والاحتيال. نشر مواد إباحية، تظهر مشهد الأطفال وانتهاكات حقوق النشر (مثل نشر المحتوى المقرصنة).(Przyswa, 2010p12)

ورغم أنه حتى الآن لم تظهر ملامح الصورة واضحة في تحديد صفات مجرمي الإنترنت والمعلومات وشرح سماتهم النفسية وتحديد دوافعهم ، خاصة مع قلة الدراسات الخاصة، بهذه الظاهرة من ناحيه ولصعوبة الفهم الجيد لمداها الحقيقي من ناحية ثانية ، والتطورات السريعة الحاصلة في ميدان الكمبيوتر والإنترنت من ناحية ثالثة ، فالمزيد من الوسائل والتكنولوجيا يعني المزيد من التغير في أنماط الجريمة وطرق الاعتداء ، مما يساهم في إحداث تغير في سمات مجرمي الإنترنت ومع ذلك يمكن تصنيف مجرمي الإنترنت حسب المنظور النفسي إلى فئة المتطفلين والمحترفين حيث أن فئة المتطفلين يرتكبون الجريمة للتحدي والأبداع كما ينصبون أنفسهم أوصياء على أمن الحاسوب في المؤسسات المختلفة وحمايتها ام بنسة لفئة المحترفين هم مختلفون بحكم الخبرة والفهم الواسع للمهارات التقنية بأضافة الى التخطيط والتنظيم خلال أنشطة الجرائم المرتكبة .

وبالتالي فهي الأخطر مقارنة بباقي الفئات ، وأساس الاعتداءات هو تحقيق الكسب المادي لهم أو للجهات التي كلفتهم أو مولتهم أو سخرتهم ، وقد تهدف إلى تحقيق أغراض سياسية أو التعبير عن موقف معين فكري أو نظري أو فلسفي . (الرومي، 2003،ص12)

2.6 ضحايا الجرائم الإلكترونية:

يمثل ضحايا الجرائم الإلكترونية هو كل فرد متفاعل مع شبكة العنكبوتية وقد تعرض إلى نوع من أنواع الجرائم السيبرانية من طرف مجرمي الإنترنت ، وهي تشمل كلاً من أفراد جميع أنواع (الأسرة ، الشركات والحكومات): كل أولئك الذين يلجئون إلى احتياجات معينة الإنترنت أو الكمبيوتر من الضحايا المحتملين لأسباب مختلفة(Salu, 2005p161) .

3.6هياكل المراقبة :

هي المؤسسات التنظيمية التي تعتبر مهمتها الأساسية ، هو منع إساءة استخدام للوسائط الإلكترونية وضمان تنفيذ الخدمات التي تتم عبر الواقع السيبراني، من خلال المراقبة وتحقيق الأمن السيبراني فهياكل الأمنية التقليدية مثل الدرك والشرطة ، فقد أظهر

هذا نوع من الأمن التقليدي عدم قدرته على ضبط هذا نوع جديد من الجريمة. بحكم غياب مسرح الجريمة عن الواقع المادي وغياب الأدلة الجنائية وبالتالي فهي محدودة في قدرة في ردع ضد جريمة عالمية، بوسائل الرادعة لـ الجرائم التقليدية .

مثل احتمال الاعتقال وشدة العقوبة تكاد تكون غير فعالة في مكافحة الجرائم الإلكترونية. ، حيث أن من خصائص الجريمة الإلكترونية هي جريمة غير شخصية وعالمية تكاد تلغي احتمالية القبض على الجاني بوسائل التقليدية متاح للشرطة ويتم الردع هذا النوع من الجرائم من خلال تطوير هيكل المراقبة بالاعتماد على الأمن الجديد وهو الأمن السيبراني فهو الكفيل بمجابهة هذا نوع من الجرائم وردعها حيث يهتم هذا نوع من الأمن بالجرائم التي تكون في الواقع الافتراضي و تُرتكب على نظام الكمبيوتر (Wall, 2007p185)

ومن خلال هذا يمكن أن نعتبر وسط الجريمة، هو تركيبة للثلاث فاعلين أساسين هم :

•المجرم الذي يتميز بسلوك انحرافي الكترونيا، يمارسه في أشكال متنوعة من الجرائم عبر الوسائط الالكترونية، متصلة بالأنترانت

•الضحية الذي يعتبر المتضرر من فعل المجرم، ويكون ضحية بصدفة لعدم وعيه السيبراني وبأساليب الحماية التي تجعله امن من السلوكيات الإجرامية الالكتروني،

•أما هيكل المراقبة فهو المسئول الأول على توازن سوق الالكتروني من خلال الردع القانونية، ومراقبة التفاعل باعتماد على تطوير وسائل الأمن التقليدي متعرف عليه، مثل الشرطة والدرك ويكون تطوير القطاع الأمن من خلال تطوير أجهزة المراقبة وربطها بالأنترانت لتسهيل الرقابة الالكترونية .

7. أدوات الجريمة الإلكترونية :

تعتبر أداة الجريمة من ابرز النقاط التي يركز عليها في الأدلة الجناية، لتعرف على اثر التي تساعد المحقق في تعرف على مجرم من خلال بصماته بإضافة إلى أنا المشرع القانوني يركز في تحديده للعقوبة التي تخص المجرم، وهذا المتعرف عليه فيما يخص الجرائم الواقعية، أما أدوات الجريمة الالكترونية قد تطورت بحكم تغير مسرحها ومن خلال هذا

،سوف نعرض التقنيات التي يستخدمها المجرمون لتنفيذ جرائم الإنترنت. الأدوات شائعة والتي ركزت عليها العديد من الدارسات العلمية وهي على النحو التالي: قنابل البريد الإلكتروني، ومفرقعات كلمات المرور، وشبكات الروبوت.

1.7قنابل البريد الألكتروني:

تعتبر قنابل البريد الإلكتروني كواحدة من أكثر أدوات الجرائم الإلكترونية استخدامًا،حيت تعرف على انها شكل من أشكال سوء استخدام الإنترنت التي يتم ارتكابها من خلال إرسال كميات هائلة من البريد الإلكتروني إلى عنوان بريد إلكتروني محدد بهدف تجاوز صندوق البريد وإغراق خادم البريد الذي يستضيف العنوان ، مما يجعله في شكل من أشكال رفض الخدمة هجوم في هذه الحالة ، فإن الجاني يرسل أعدادًا هائلة من رسائل البريد الإلكتروني إلى صندوق بريد ضحيته إلى الحد الذي تتسع له سعة استنفاد صندوق البريد. وبالتالي، فإن الضحية الذي يكون فردًا أو منظمة ، يصبح غير قادر على الوصول وقراءة رسائل البريد الإلكتروني الشرعية الخاصة به. يمكن لحالات قصف البريد الإلكتروني الخطيرة أن تشل نظام المنظمة بأكمله. نية المتسللين هي إغلاق موقع الضحية أو الشبكة أو نظام التشغيل (Wilson, 2008p44).

2.7مفرقعات كلمة المرور:

يمكن للمستخدمين مواقع التواصل الاجتماعي و ذات طابع العلمي أو العملي التي تفرض على مستخدميها بريد الالكتروني و كلمة مرور وفي عديد من المرات كثير من المستخدمين الذين ينسون كلمات المرور لشبكاتهم أو أجهزة الكمبيوتر الخاصة بهم يستخدمون مفرقعات كلمة المرور للاسترجاع حسابهم الشخصي كما توفر أيضًا فرصًا للمجرمين الوصول غير المصرح به إلى الشبكات وأجهزة الكمبيوتر خاصة بالضحايا. حيث تعتمد هذه تقنية على أداة تكسير كلمات المرور فللبحث من خلالها يتم تحديد كلمة المرور الصحيحة. حيث تسمح البرامج للمفرقعات كلمة المرور بالبحث عن الأرقام وإدخالات

القاموس افترض أن هذه البرامج يمكن أن تكون مفيدة في الشبكات التي تتطلب كلمات مرور المستخدمين للجمع بين الأرقام والحروف. في دراسة حول عينات مجرمي الإنترنت أهمية اختراق كلمة المرور كأداة لتنفيذ الجرائم الإلكترونية (Al-Alawi et al., 2020p260) .

3.7بوت نت:

مصطلح "botnet" مشتق من مزيج للكلمتين ، هما .(Robot Network) تستعمل هذه الروبوتات في تحكم مجرمي الانترانت بأجهزة الكمبيوتر المخترقة متصلة بشبكة الإنترنت عن بعدكما يشار إلى هذا نوع من أجهزة الكمبيوتر المخترقة باسم الطائرات بدون طيار فمجرم الانترانت يتحكم في الجهاز من خلال الأوامر المرسلة عبر الإنترنت فكمبيوتر المهاجم وهو الخاص بالمجرم فهو القيادي ومتحكم في بوت نت عن بعد ويملي عليه الأوامر ومن أنواع الهجمات التي تتم من خلال البوت نت تعد هجمات DDos ورسائل البريد الإلكتروني العشوائية من الأشكال الشائعة لهجمات الروبوتات حيث ان هجمات "DDos" تعتبر هذا نوع من الهجمات الالكترونية التي تتم عبر بوت نت حيث يعرف نوع هذا من الهجمات باسم هجمات حجب خدمة الموزع حيث توجه نحو شبكات مثل مواقع الالكترونية خاصة بالمنظمات والشركات والمؤسسات وتأدي هذي الهجمات الى عدم استجاب الموقع للعمل مم يجعله خارج عن نطاق العمل وتحجب عمله أما بنسبة لرسائل البريد الإلكتروني العشوائية تعتبر هذا نوع من الهجمات الالكترونية التي تتم بأرسال الجاني عدد هائل من الرسائل وبطريقة عشوائية يكون الهدف من خلالها هو النصب على كل فرد يقوم بفتح الرسالة المواجهة او الحصول على كلمة المرور او ارقام بطاقة الائتمان وتفاصيل الحساب المصرفي ونشر الفيروسات الضارة. (Al-Alawi et al., 2020p262)

وبحكم التطور الذي عرفته الجريمة الالكترونية أدي هذا إلى تطوير أدواتها فالمعروف على أدوات القديمة أن يعتمد المجرم على السلاح أو تهديد والخطف أو النصب بالقوة إلى أن هذا يعتبر من الماضي فقد ظهرت العديد من الوسائل المتمثلة في قنابل البريد الالكترونية التي من خلالها يادي هذا الفعل الى خروج البريد عن الخدمة او فتح الرسائل تؤدي إلى تضرر

شبكة الضحية التي تسمح للمجرم من سرقة بيانات الضحية وكل فيما يخص سحابته الشخصية والمصرفية.

8. الوسط الجامعي والإجراءات الأمنية للحماية من الجريمة الإلكترونية :

1.8مفهوم الوسط الجامعي:

الجامعة هي مؤسسة لتنمية وتنشئة أفراد المجتمع في أعلى مستوياته فهي تعد من أهم المؤسسات الاجتماعية التي تؤثر وتتأثر بالجو الاجتماعي المحيط بها، فهي من صنع المجتمع كمانها هي أداته في صنع قيادته الفنية والمهنية والسياسية والفكرية، ومن هنا كانت لكل جامعة رسالتها التي تتولى تحقيقها، ولكل نوع من المجتمعات جامعته التي تناسبه من حيث اتصال الجامعات بمجتمعاتها وتقديم مجموعة من الأدوار والأنشطة والخدمات لهذا المجتمع، فأصبح أمر ضروري تفرضه المتغيرات المعاصرة وهي معقل الفكر الإنساني في أرفع مستوياته، ومصدر لاستثمار وتنمية أهم ثروات المجتمع وأغلاها وهي الثروة البشرية (راشد،2008،ص12).

وقد أثر التقدم التكنولوجي واستخدام الإنترنت على نمط التعليم التقليدي المتمركز على المحاضرة الذي يكون فيه عملية التعليمة من خلال عملية التفاعل التي تكون بين الأستاذ والطالب في قاعة بوسائل تقليدية أما النمط التعليمي الذي أصبحت تعتمد عليه الجامعة هو التعليم الإلكتروني هو تعلّيم يقوم أساسا على استخدام الحاسوب والإنترنت ويكون بين الطالب والبرنامج ويمكن أن يكون تفاعل بين الطالب وعضو هيئة التدريس. وقد تطورت أدوات التعلّم الإلكتروني لتشمل النص والصورة والفيديو والصوت والألعاب، ويمكن أن تثري برامج PowerPoint تجربة التعلّم الإلكتروني ومؤتمرات الفيديو والعالم الافتراضي.(Earle, 2002,p22)

حيث أن ربط الوسط الجامعي بالإنترانت قد غير عملية التفاعل بين الفاعلين الأساسين في الوسط الجامعي المثلين في الطلبة الهيئة تدريسية والإدارية من خلال الاعتماد

على الوسائط الالكترونية فهي عبارة عن عبارة عن مجموعة من التطبيقات العملية التي تقوم على أسس التكنولوجيا الرقمية، وتعتمد على الشبكة العنكبوتية؛ والتي تسمح بإنتاج المحتوى، وتغيير هذا المحتوى الذي تم توليده بوساطة المستخدم؛ أي إنها أحد أشكال التواصل الذي يتم من خلال الإنترنت، وتسمح للأفراد والمجموعات بإنتاج المواضيع ونشرها، بشكل مباشر ، ومشاركة هذه الموضوعات مع الآخرين، ومناقشتهم بها، والاستماع إلى آرائهم.(Kaplan & Haenlein, 2010,p60)

ان للجامعة عديد من الاختصاصات التي تهتم بها لتطوير البنية التحتية للمجتمع المحلي الذي: يعتبر أساس وشرط في تحقيق الاهتمام بالتعليم الجامعي والبحث العلمي الذي تقوم به كلياتها ومعاهدها في سبيل خدمة المجتمع والارتقاء به حضارياً، ومساهمة في رقي الفكر وتقدم العلم وتنمية القيم من خلال تزويد لمجتمع بالمختصين الفنين والخبراء في مختلف المجالات وإعداد مورد بشري المزود بأصول المعرفة وطرائق البحث المتقدمة والقيم الرفيعة، ليساهم في بناء وتدعيم المجتمع، وصنع مستقبل الوطن وخدمة الإنسانية كون أن للجامعة وللجامعة ثلاث وظائف أساسية تعمل دائما على تجسيده على الواقع الاجتماعي في تحقيقها تطوير وتنمية الوعي والفكر البشري من التعليم والتدريس وخدمة المجتمع(الزكي، أحمد عبد الفتاح،2007،ص160).

وبحكم دور الحساس والأساسي الذي يشغله الوسط الجامعي في تطور المجتمع يبقي تحت تهديد الهجوم الإلكتروني نتيجة لربطه بالأنترانت وتحول بنيته المادية الى بنية افتراضية تسمح بنوعين من التفاعل الواقعي والتفاعل عبر الوسائط الإلكترونية فكل ظواهر الجريمة القديمة أصبحت مستحدثة لهذا فكل مكان يواجه الفرد في الواقع أصبح يوجهه عبر الأنترانت.

2.8 تدابير مواجهة وحماية من تقنيات الجرائم الإلكترونية في الوسط الجامعي:

باعتبار أن الوسط الجامعي يبقي دائما تحت تهديد عديد من الهجمات الإلكترونية التي تشكل خطر على مكوناته المادية والبشرية وأضرار على تجهيزاته (ذياب،2014ص14) من

حواسيب وشبكة العنكبوتية ونظامه المعلوماتي ولهذا يستوجب على القائمين على المؤسسة الجامعية أخذ الحيطة من خلال انتهاج التدبير اللزمة التي يمكن من خلالها مواجهة تقنيات الاختراق التي يعتمد عليها مجرمي الأنترانت وهذا من خلال التنظيم للوسط الجامعي و حماية الخصوصيات و التوفير الحماية وهي على النحو التالي :

8.1.2 تنظيم الوسط الجامعي: ان تنظيم الوسط الجامعي يعتبر من وظائف الأدراة الجامعية بحكم لكل مؤسسة هيكل تنظيم مختلف عن الأخرى نتيجة للوظائف المقدمة أوللمجال الذي تتخصص فيه اما باعتبار الجامعة من المؤسسات المعتمدة في مجال التعليم والتكوين العالي فتنظيمها وتفاعلها يشمل جميع المجالات للأن موكل اليها تكوين وتأهيل الكفاءة في مستوي عالي لهذا يتوجب عليها ربط علاقة على مستويين الداخلي وخارجي للتحقيق الجودة والتطور للكن في اطارة ما يوجهها من مخاطر الكترونية تفرض عليها تنظيم محكم للأنشطة الإدارية وهذا لسيطرة على نظام المعلومات للجامعة وقواعدها البيانية من التحكم ببرامجها الخاصة والأشراف والمتابعة على أنشطة المؤسسة في شقيها الداخلي والخارجي والرقابة من خلال انتهاج مجموعة من التعليمات والارشادات التي تكون في اطار الحماية المعلوماتية من مخاطر الإلكترونية وهذا لضبط السلوك بنسبة للعاملين والطلبة داخل الوسط الجامعي وزيادة وعيهم تجاها تدابير الحماية والموجهة بنسبة لتقنية الجريمة الإلكترونية (جبرا، 2015 ص122).

8.2.2 حماية الخصوصيات: تدخل في أطار حماية الموظفين والعاملين ومنتمين ومسجلين في النظام المعلوماتي للجامعة وبما نسميه حماية البيانات والمعلومات الشخصية للأفراد بحكم هم الحلقة الأساسية للوسط الجامعي وهم عرضة لتهديدات الإلكترونية كما يمكن أن يكون سبب فيها نتيجة لخطاء الاستخدام لوسائط الإلكترونية المتصلة بنظام المعلوماتي لهذا فحماية خصوصياتهم من طرف الجامعة تكون من خلال الاعتماد على التعريف الخاص باعتماد على كلمة المرور خلال عملية الدخول الى نظام المعلوماتي للجامعة إضافة الى

التدريب والتأهيل و التوعية بمخاطر الالكترونية وطرق موجهتها والإجراءات المساعدة على ذلك .

8.3.2 الحماية التقنية: تعتبر الحماية التقنية أساسية بنسبة للمؤسسة الجامعية وهذا يفرض عليها ان تشمل الحماية كل من النظام المعلوماتي والعاملين عليه من خلال الكشف وإزالة كل البرمجيات الضارة والخبيثة ومحوها وهذا لكونها تهدد البيئة الافتراضية للمؤسسة الجامعية من خلال الاعتماد على مكافحات الفيروسات التي تكون مضادة لكل فيروسات المنتشرة في الفضاء الإلكتروني ومن أشهرها Avira , Avast بإضافة الى هذا يستوجب تأمين منافذ الموجودة في الحواسيب والتي من خلالها يمكن توفير الأنترانت من خلال الاعتماد على جدران النار التي تمنع وصول الفيروسات الخبيثة عن طريق المنافذ المفتوحة كما ستوجب أيضا حماية سرية المعلومات التي بحوزة المؤسسة الجامعية في مستودعاتها الرقمية والأرشيف من خلال الاعتماد على التشفير وكلمة السر التي تكون معرفة عند المرسل والمرسل اليه (رحموني، 2017ص444).

وبهذا يمكن أن نعتبر أساس الحماية الوسط الجامعي من الجريمة الإلكترونية وتقنيات الاختراق تفرض علينا التزام بتدابير الحماية والمواجهة من التنظيم وحماية الخصوصيات مع دمج تقنيات الحماية من برامج وتطبيقات الحاسب الالي التي يمكن من خلالها ابعاد الضرر وكشف عن الفيروسات الخبيثة وحذفها مم يعود بالأمن على الحاسوب ونظام المعلوماتي وشبكة الأنترانت.

9. خاتمة :

يعتبر السلوك الإجرامي الرقمي على أنه أحد الأنماط السلوكية الفردية أو الجماعية التي تعبر عن رفض الآخر نتيجة للشعور بالإحباط في إشباع الحاجات الإنسانية. فهو يعتبر أي نوع من الإيذاء أو التهديد غير المبرر باستخدام الألفاظ التي تكون عبارة عن تعليقات للإكراه او العنصرية والتحريض على استعمال القوة وتتعدد في عديد من أنماط السلوكيات العدائية تجاه الآخرين، والتي تتضمن الإساءة الجسدية، والإساءة النفسية، وتدمير الأجهزة المملوكة للآخرين من خلال الوسائط الالكترونية ومواقع النت .

أما التطور الذي عرفته الجريمة الالكترونية أدي هذا إلى تطوير أدواتها فالمعروف على أدوات القديمة أن يعتمد المجرم على السلاح أو تهديد والخطف أو النصب بالقوة إلى أن هذا يعتبر من الماضي فقد ظهرت العديد من الوسائل المتمثلة في قنابل البريد الالكترونية التي من خلالها يؤدي هذا الفعل إلى خروج البريد عن الخدمة او فتح الرسائل تؤدي إلى تضرر شبكة الضحية التي تسمح للمجرم من سرقة بيانات الضحية وكل فيما يخص سحابته الشخصية والمصرفية.

كان ربط الوسط الجامعي بالإنترانت قد غير عملية التفاعل بين الفاعلين الأساسين في الوسط الجامعي المثلين في الطلبة الهيئة تدريسية والإدارية من خلال الاعتماد على الوسائط الالكترونية فهي عبارة عن عبارة عن مجموعة من التطبيقات العملية التي تقوم على أسس التكنولوجيا الرقمية، وتعتمد على الشبكة العنكبوتية والتي تسمح بإنتاج المحتوى، وتغيير هذا المحتوى الذي تم توليده بوساطة المستخدم أي إنها أحد أشكال التواصل الذي يتم من خلال الإنترنت، وتسمح للأفراد والمجموعات بإنتاج المواضيع ونشرها بشكل مباشر ، ومشاركة هذه الموضوعات مع الآخرين، ومناقشتهم بها، والاستماع إلى آرائه.

10. قائمة المراجع:

1. الزكي، أحمد عبد الفتاح. (2007). دور التعليم الجامعي في خدمة المجتمع بمحافظة دمياط، دراسات تربوية ونفسية. مجلة كلية التربية بالزقازيق، 22(57)، 157-202.
2. علي راشد. (2008). الجامعو التدريس الجامعي. الأردن: دار ومكتبة الهلال - دار الشروق للنشر والتوزيع .
3. محمد أمين الرومي. (2003). جرائم الكمبيوتر والأنترنت. اسكندرية،مصر: دار المطبوعات الجامعية.
4. كمال محمود جبرا. (2015). التأمين وادارة الخطر. القاهرة: الأكادميون لنشر والتوزيع.
5. محمد رحموني. (2017). خصائص الجريمة و مجالات استخدامها. مجلة الحقيقة،16(3)، الصفحات 432-451.
6. موسي ذياب. (2014). الجرائم الألكترونية:المفهوم والأسباب/. الجرائم المستحدثة في ظل التتغيرات والتحولات الأقليمية والدولية (الصفحات 1-28). عمان: المملكة الأردنية الهاشمية كلية العلوم الأستراتجية.
7. *Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications, 6(1), 21–39* .
8. *Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20* .
9. *Ehrlich, I. (1996). Crime, Punishment, and the Market for Offenses. Journal of Economic Perspectives, 10(1), 43–67* .
10. *Salu, A. O. (2005). Online crimes and advance fee fraud in Nigeria - are available legal remedies adequate? Journal of Money Laundering Control, 8(2), 159–167* .
11. *.Wall, D. S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. Police Practice and Research, 8(2), 183–205.*

12. *Al-Alawi, A. I., Al-Kandari, S. M. H., & Abdel-Razek, R. H. (2016). Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University. Journal of Innovation and Business Best Practice, 2016, 1–24* .
13. *Al-Alawi, A. I., Mehrotra, A. A., & Al-Bassam, S. A. (2020). Cybersecurity: Cybercrime Prevention in Higher Learning Institutions. In Y. A. Albastaki & W. Awad (Eds.), Advances in Computational Intelligence and Robotics (pp. 255–274). IGI Global* .
14. *Goutam, R. K. (2015). Importance of Cyber Security. International Journal of Computer Applications, 111(7), 14–17.*
15. *Earle, R. S. (2002). The Integration of Instructional Technology into Public Education: Promises and Challenges. 42(1), 22.*
16. *Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53(1), 59–68* .
17. *H. Çakir, E. Sert. (2010). Bilişim Suçları ve Delillendirme Süreci. Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu Bildirisi (123-143) Ankara: Polis Akademisi Yayınları, Ankara.*.
18. *Wilson, C. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress...30- 44.*