الأمن المعلوماتي ومواجهة تهديدات البيئة الرقمية لدى الشباب الجامعي نحو رؤية مقترحة من منظور الخدمة الاجتماعية

Information security and facing the threats of the digital environment among university youth Towards a proposed vision from a social work perspective

إعداد

أ.د/ محمود فتحي محمد

Prof. Dammoud Fathi Muhammad

أستاذ مجالات الخدمة الاجتماعية - كلية الخدمة الاجتماعية - جامعة الفيوم

د/ حنان طنطاوي أحمد

Dr. Hanan Tantawy Ahmed

مدرس بقسم مجالات الخدمة الاجتماعية - كلية الخدمة الاجتماعية - جامعة الفيوم

Doi: 10.21608/jinfo.2022.264281

استلام البحث ١٥ / ٧ / ٢٠٢٢

قبول النشر ١٥ / ٨ / ٢٠٢٢

محمد، محمود فتحي & أحمد، حنان طنطاوي (٢٠٢٢). الأمن المعلوماتي ومواجهة تهديدات البيئة الرقمية لدى الشباب الجامعي...نحو رؤية مقترحة من منظور الخدمة الاجتماعية. ***المجلة العربية للمعلوماتية وأمن المعلومات***، المؤسسة العربية للتربية والعلوم والآداب ، مصر، مج٣ ع(٩) ، ص ص ١٤١ – ١٥٦.

https://jinfo.journals.ekb.eg/

الأمن المعلوماتي ومواجهة تهديدات البيئة الرقمية لدى الشباب الجامعي
نحو رؤية مقترحة من منظور الخدمة الاجتماعية

المستخلص :

ظهرت العديد من التحولات التكنولوجية التي أثرت على الكثير من المجتمعات والفئات المختلفة، كما أثرت في تغيير أنماط الحياة الاجتماعية والثقافية وغيرها من أشكال التفكير لهذه الفئات، ومن بين أكثر تلك الفئات تأثرًا "فئة الشباب الجامعي"، فقد أصبح انتشار التقنيات الحديثة ووسائل التواصل الاجتماعي والتطبيقات الرقمية وغيرها يشكل تهديدًا كبيرًا لهذه الفئة باعتبارها أكثر الفئات إقبالًا عليها واستخدامًا لها، فعلى الرغم من أن للبيئة الافتراضية العديد من الإيجابيات على عقول الشباب الجامعي وأنماط تفكيرهم وما يتبنونه من أساليب علمية وحياتية؛ إلا أن ذلك يصاحبه العديد من الآثار السلبية التي أصبحت تمثل تهديدات وتحديات كبيرة للمجتمع بصفة عامة، والشباب على وجه الخصوص، ومن هنا تأتي أهمية الأمن المعلوماتي وكيفية توظيف أساليبه المتنوعة وتطبيقاته المختلفة في مواجهة تلك التهديدات، ويأتي دور الخدمة الاجتماعية كمهنة لها أساليبها ونماذجها ومداخلها العلمية التي تسهم بشكل كبير في حماية الشباب من الوقوع كضحايا للكثير من المشكلات والتحديات المختلفة والتي من بينها تهديدات البيئة الرقمية، ومن هنا جاءت فكرة تلك الورقة البحثية التي استهدفت تحديد تهديدات البيئة الرقمية، ودور الأمن المعلوماتي في مواجهتها، ومن ثم التوصل إلى رؤية مقترحة من منظور الخدمة الاجتماعية في معالجة تلك القضية.

الكلمات المفتاحية: الأمن المعلوماتي، تهديدات البيئة الرقمية، الشباب الجامعي.

Abstract:

There have been many technological transformations that have affected many different societies and groups, as well as changing the patterns of social and cultural life and other forms of thinking for these groups, and among those groups most affected is the “ University youth category”, the spread of modern technologies, social media and digital applications has become And others pose a great threat to this category as it is the most popular and used group, although the virtual environment has many positives on the minds of university youth, their thinking patterns and the scientific and life methods they adopt; However, this is accompanied by many negative effects that have become significant threats and challenges to society in general, and youth in particular. Hence the importance of information security and how to employ its various methods and applications in facing these threats, and here comes the role of social

work as a profession with its methods, models and scientific approaches that contribute significantly to protecting youth from falling as victims of many different problems and challenges, among which are the threats of the digital environment. Hence the idea of this research paper aimed at identifying digital environment threats, and the role of information security in confronting them, and then arriving at a proposed vision from a social work perspective in treating this issue.

Keywords: information security, digital environment threats, university youth.

أولًا: الإشكالية البحثية:

يشهد العالم في وقتنا الراهن نقلة كبيرة في عالم المعرفة ونظم المعلومات والتحول إلى الرقمنة؛ فقد نتج عن التطور التكنولوجي الهائل العديد من الآثار السلبية والتهديدات الناتجة عن استخدام البشر لشبكات الإنترنت بما تشمله من مواقع وتطبيقات ووسائل التواصل الاجتماعي وغيرها.

فقد بلغ عدد مستخدمي الإنترنت في مصر ٧٤ مليون و٤٨٠ ألف مستخدم بنهاية أكتوبر ٢٠٢١ مقابل ٦٣.٤٨ مليون في نفس الفترة من العام الماضي، بزيادة تقدر بنحو ١١ مليون مستخدم خلال عام واحد فقط، بحسب موجز عن مؤشرات الاتصالات وتكنولوجيا المعلومات. **(مؤشرات قطاع الاتصالات وتكنولوجيا المعلومات، ٢٠٢١)**

كما كشف الجهاز المركزي للتعبئة العامة والإحصاء، أن ٧١.٢% من الشباب في الفئة العمرية (١٨–٢٩سنة) يستخدمون شبكة الإنترنت، ٩٨.٣% منهم يستخدمون وسائل التواصل الاجتماعي (الفيسبوك، تويتر)، ٩٩.٩% منهم ذكور، و٩٧.٢% إناث، وأوضحت المؤشرات الأساسية لقياس مجتمع المعلومات عام ٢٠٢٠، أن ٦٦.٢% من الشباب في الفئة العمرية (١٨- ٢٩سنة) مستخدم للحاسب الآلي، وأن ٧١.٢% من الشباب في الفئة العمرية (١٨ – ٢٩ سنة) يستخدمون شبكة الإنترنت. **(الجهاز المركزي للتعبئة العامة والإحصاء، ٢٠٢٠)**

حيث تواجه البشرية تهديدات رقمية جديدة أكثر تعقيدًا وأشد فتكًا وضررًا، تتسبب في إتلاف منظومات شبكات الكمبيوتر لمؤسسات كبيرة وحساسة داخل الدول التي لا زالت غير آمنة، بالإضافة إلى وجود هجمات إلكترونية موجهة ومعقدة، حيث ينتج تعقيد هذه الهجمات الإلكترونية من كون أنه قد لا يبرز أثرها على الفور، فأغلبية ضحايا هذه الهجمات الإلكترونية من كون أنه قد لا يبرز أثرها على الفور، فأغلبية ضحايا هذه الهجمات يجهلون

باديء الأمر تعرضهم للقرصنة ولا يكتشفوا ذلك إلا بعد مرور الوقت. **(عبد الحميد، أكتوبر ٢٠٢٠، ص٢٢٠)**

فقد تعددت أشكال تللك التهديدات والجرائم المستحدثة على النطاق الدولي بشكل متطور، ومن أبرز أشكالها: الإرهاب الرقمي، التزوير بمختلف أشكاله، انتهاك حقوق الملكية الفكرية وبراءات الإختراع، الإعتداء على خصوصية الأفراد، الملاحقة، التشهير، الهجمات الرقمية، الشائعات الموجهة، الحرب النفسية، الإحتيال المعلوماتي واختراق بيانات المواقع الرسمية للدول وتعطيل خدماتها، وقرصنة وتسريب المعلومات الحساسة السرية والتلاعب الفعال بها، وغيرها من الجرائم التي تستهدف أمن الدولة الإستراتيجي وأمنها المعلوماتي، كاستخدام المنظمات الإرهابية لأساليب التضليل الفكري للشباب، لضرب الأمن الفكري للدول واستقطاب الشباب في القضايا الفكرية المتطرفة ودعم وتمويل الإرهاب وغيرها من الجرائم. **(أحمد، يوليو ٢٠٢١، ص ص١٧٦٧: ١٧٦٨)**

وهو ما أكدت عليه **دراسة الكفارنة، (ديسمبر ٢٠١٤)** على أن هناك العديد من المخاطر والتأثيرات السلبية لاستخدام الشباب للتقنيات الحديثة ووسائل التواصل الاجتماعي على الجوانب الأخلاقية والسياسية، والتبعية الفكرية والثقافية.

كما أكدت نتائج **دراسة الصالح، (٢٠١٨)** إلى أن هناك تغير في النسق القيمي للطالبات الجامعيات نتيجة استخدامهم لوسائل التواصل الاجتماعي وذلك بنسبة ١٠٠% من مجموع عينة الدراسة، وأن هناك العديد من الآثار السلبية الواضحة على القيم ومن أهمها ظهور ألفاظ وعبارات دخيلة على اللغة، وانتشار بعض الألفاظ والعبارات المرفوضة أخلاقيًا، وقلة المشاركة في المناسبات والاجتماعات الأسرية، وتأثر شخصياتهم بالكثير من العادات والتقاليد الوافدة.

فعلى الرغم من الدور الفاعل للإنترنت في مجتمعنا المعاصر، إلا أنه قد حمل الكثير من التأثيرات الجانبية التي تتصل بمسألة أمن المعلومات على مستوى الأفراد والمجتمعات؛ فانفتاح عوالم من المعرفة على مصراعيها، زادت معه المطالبة بالرقابة ووضع القيود والانتباه إلى أهمية المفاهيم الأمنية، والتوعية بحاجة الإنسان إلى الأمن. **(المعيذر & القحطاني، ٢٠١٥، ص٢٢)**

فبجانب ذلك الدور الفاعل لتكنولوجيا المعلومات الحديثة إلا أنه قد صاحب ذلك إساءة الاستخدام للتكنولوجيا مثل التقنيات الأخرى، فيمكن استخدامها بطرق معظمها سوف نعتبره مفيدًا أحيانًا، وكذلك بالطرق التي تكون قد تكون ضارة في أحيانًا أخرى. حيث تعمل تكنولوجيا المعلومات والاتصالات بسرعة ميكروثانية، فقد تشمل البرامج التي طورها البشر بعض المعلومات غير المرئية بالعين المجردة، وقد تكون ضارة جدا، فغالبًا ما يتم تنفيذ النوايا الخبيثة في هذه البيئة الرقمية بسرعة، وبشكل غير مرئي، ويصعب تتبعه، إن لم يكن مستحيلاً. **(Sadosky, George et, al, 2003, p"v")**

فالمراقب للأوضاع الاجتماعية السائدة، يدرك بأن استخدام مواقع الإنترنت بدأ يأخذ منحى خاص، وبدأ يتجه في طريقه للتأثير على البناء الاجتماعي للمجتمعات الإنسانية، كما

أدى إلى الانتشار السريع والفعال لأنماط القيم الغربية في الفن والملبس والمأكل والتسلية والتي تحمل رؤية محددة للعالم تختلف اختلافًا جذريًا مع رؤية المجتمعات غير الغربية. **(محمود، ٢٠١٦، ص ١٧٥)**

فإلى جانب المزايا العديدة التي نتجت عن التطور التكنولوجي الحديث، أفرز لنا الكثير من الجرائم والتعديات التي تختلف في خصائصها وأشكالها وآثارها عن الجرائم التقليدية، وأصبحت تمثل تهديدًا مباشرًا للأمن والاستقرار المحلي والعالمي. خاصة أن هذه الفئة من الجرائم تتميز بأنها معقدة للغاية لتنوعها وسهولة ارتكابها وقدرة الجناة على التخفي والهروب. **(بطيخ، أغسطس٢٠٢١، ص ص٤: ٥)**

فقد برزت العديد من الجرائم الإلكترونية المستحدثة على المجتمع تمثل الجانب السلبي لثورة الاتصالات العالمية، فاستخدام وسائل تكنولوجيا الاتصال منتشرًا بين جميع الفئات، لا سيما الشباب الذين يمضون جزءًا كبيرًا من وقتهم على منصات التواصل الاجتماعي، وقد تأثرت معظم الدول بهذه الظاهرة، حيث ظهرت العديد من صور من الجرائم الإلكترونية كجرائم اختراق المواقع الإلكترونية، وجرائم اختراق البيانات الشخصية، وجرائم الاعتداء على الأموال الإلكترونية، وجرائم حماية التوقيع الإلكتروني، وجريمة الاحتيال عبر الهواتف الخلوية، وجرائم الإبتزاز المالي والشخصي. **(الزبن& الخرابشة، ٢٠٢١، ص٢٣١)**

وهو ما أكدت عليه نتائج دراسة **هشام، (٢٠١٨)** أن التقدم التكنولوجي أفرز أنماطًا جديدة من الجريمة، وكذا من المجرمين، فكان للتقدم في العلوم المختلفة أثره على نوعية الجرائم، واستغل المجرم ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، بحيث أن المشكلة لا تكمن في استغلال المجرمين للإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم.

كما أشارت نتائج **دراسة سعيد (يناير ٢٠١٨)** على تعدد صور تهديدات الإجرام المعلوماتي وأنماطه والتي أثرت سلبًا على روح الانتماء العام لدى الشباب، بما ينعكس سلبًا على أمن الدولة.

لذا تتضح أهمية الأمن المعلوماتي في حماية مصالح الدول وحقوق ضحايا جرائم الحاسوب من خلال بلورة مشددة على الجرائم الرقمية المتعلقة بتغيير الانتماء الفكري للفرد، ووضبط الجرائم المرتبطة بنشر الأفكار المتطرفة والمغلوطة وغير من أشكال الجرائم التي تستهدف الشباب بالدرجة الأولى. **(عبد الحميد، ٢٠٢٠، ص١٣٧)**

فالمحافظة على الأمن المعلوماتي يهدف بصفة عامة إلى توفير ثلاث أهداف أساسية هي الحفاظ على سرية المعلومة، وتوافر المعلومة، وحماية المعلومة، إضافة إلى أهداف مكملة للأولى تتمثل في توفير المصداقية والتأكد من مصدر المعلومة وتحديد الجهات التي لها صلاحية للدخول للمعلومة. **(بلجراف& خلود، أكتوبر ٢٠١٧، ص٢٦٠)**

وفي إطار مواجهة تلك الجرائم المعلوماتية والتهديدات المختلفة للبيئة الرقمية أكدت نتائج **دراسة بطيخ (أغسطس ٢٠٢١)** أن العديد من الدول تسعى إلى تطوير نظم المكافحة

التشريعية لهذا الخطر التقني ونظم معلوماتية لضمان الأمن المعلوماتي، بإدخال نصوص تشريعية تتوافق مع ظواهر الإجرام الإلكتروني والمخاطر التقنية.

فقد أشار جلادين **(Gladden, February 2017)** أن أمن المعلومات ليس حالة ثابتة يمكن تحقيقها مرة واحدة وإلى الأبد، بل هو هدف يجب متابعته باستمرار. ففي حين أن المؤسسات الكبيرة قادرة على تنفيذ خطط أمن المعلومات المتطورة للغاية والتي يتم تطويرها وتنفيذها من قبل متخصصين، فإن المستهلكين الأفراد ومستخدمي تكنولوجيا المعلومات لا بد أن يستخدمون أيضًا العديد من ممارسات أمن المعلومات للحفاظ على خصوصية المعلومات الحساسة وأمانها.

وبما أن مهنة الخدمة الاجتماعية من المهن التي تعمل على مواكبة التغيرات الاجتماعية والتصدي للمشكلات المصاحبة لهذه التغيرات، وذلك بإشباع الاحتياجات المختلفة للشباب، والاهتمام بتدعيم وتحسين قدراتهم. **(الصالح، ٢٠١٨، ص٢٠٨)**

فإن ذلك يؤكد على أهمية دورها من خلال التعامل مع الشباب بالأساليب المهنية المختلفة بهدف مواجهة احتياجاتهم وتنمية قدراتهم وإكسابهم القيم والاتجاهات التي تتماشى مع التغيرات التكنولوجية المعاصرة والاعتماد الكبير على الفضاءات الرقمية لوقايتهم من المخاطر المعلوماتية، وتوعيتهم بكيفية التعامل معها.

وتأسيسًا على ما سبق وانطلاقًا من نتائج الدراسات والبحوث السابقة المرتبطة بتهديدات البيئة الرقمية، والدراسات المتعلقة بالأمن المعلوماتي، اتضح أن الشباب وخاصة الشباب الجامعي هو أكثر الفئات المعرضة لتهديدات ومخاطر البيئة الرقمية من جرائم واختراقات وهجمات وغيرها من أشكال التهديدات وما يترتب عليها من آثار سلبية تهدد مستقبلهم ومستقبل مجتمعاتهم؛ باعتباره من أكثر مستخدمي الإنترنت والتطبيقات والمنصات الإلكترونية وغيرها مما يشمله الفضاء الإلكتروني، وتجدر الإشارة إلى أن معظمهم ليس لديه الوعي الكافِ بأنظمة الأمن المعلوماتي وكيفية استخدامها، وهنا يأتي دور مهنة الخدمة الاجتماعية كمهنة لها أساليبها الوقائية والعلاجية، في مواجهة تلك التهديدات، وتعزيز طرق للوقاية منها.

وبناءًا عليه سوف نحاول من خلال هذه الورقة البحثية الإجابة على تساؤل رئيسي مؤداه: **ما دور أمن المعلومات في مواجهة تهديدات البيئة الرقمية لدى الشباب الجامعي؟**

ثانيًا: أهداف الورقة البحثية:

١- الوقوف على تهديدات البيئة الرقمية على الشباب الجامعي.
٢- تحديد دور الأمن المعلوماتي في مواجهة تهديدات البيئة الرقمية لدى الشباب الجامعي.
٣- التوصل إلى رؤية مقترحة من منظور الخدمة الاجتماعية لمواجهة تهديدات البيئة الرقمية لدى الشباب الجامعي.

ثالثًا: الإطار النظري

المحور الأول: تهديدات البيئة الرقمية

أولًا: مفهوم البيئة الرقمية:

تعرف بأنها: "مجموعة وسائل وأدوات وتطبيقات إلكترونية تتيح للفرد حرية نقل المعلومات والحصول عليها عبر الشبكة، بالإستعانة ببعض البرامج الحاسوبية وتساعد على التواصل والتشارك بينه وبين الآخرين بشكل إلكتروني، بما يكسر حاجزي الوقت والمكان". **(عبد المنعم، ٢٠٢١، ص٢٨٩)**

ثانيًا: أنواع مهددات البيئة الرقمية: (عبد الله، ٢٠١٢، ص ص٣١٧: ٣١٨)

- **يمكن التمييز بين أنواع متعددة من المهددات الرقمية سواءًا من حيث الهدف، أو من حيث المصدر.**

١- المهددات الرقمية من حيث الهدف:

الراجح هو إمكانية تصنيف المهددات الرقمية من حيث الهدف إلى: **مهددات رقمية موجهة، وأخرى عشوائية**. حيث تستهدف المهددات الرقمية الموجهة النيل من سلامة الأصول المعلوماتية الخاصة بأفراد ومؤسسات بعينها. أما المهددات الرقمية العشوائية فتستهدف النيل من سلامة الأصول المعلوماتية لكل الأفراد أو المؤسسات في مكان أو إقليم واحد، ومنعهم من الاستفادة من خدماتها، دون تمييز بينهم.

٢- المهددات الرقمية من حيث المصدر:

تسمح العديد من حوادث المساس بالسلامة المعلوماتية لجهات معينة بالتمييز بين **المهددات الرقمية الخاصة والحكومية.**

فالمهددات الرقمية الخاصة تستهدف النيل من سلامة بعض المؤسسات بواسطة أشخاص القانون الخاص سواءً كانوا أشخاص طبيعيين مثل قراصنة الإنترنت الهواة، أو حتى المحترفين، أو أشخاص معنوية مثل المؤسسات التي تستهدف النيل من سلامة وسرية الأصول المعلوماتية لمنافسين لها.

أما المهددات الرقمية ذات المصدر الحكومي تهدف النيل من الأصول المعلوماتية بواسطة شخص من أشخاص القانون العام، غالبًا ما يكون أحد الأجهزة التابعة لحكومة دولة معينة، كما لو قامت الدولة بوقف خدمة الإنترنت عن إقليمها كليًا، أو جزئيًا، أو بتعطيل أجهزة التحكم في شبكات الحاسب الآلي لمؤسسة ما لمنع تقديم خدماتها للجمهور لمدة معينة أو في مكان معين (كوقف خدمات شبكات الهاتف النقال) سواءًا تم هذا التعطيل بواسطة أجهزة الدولة أو بواسطة المؤسسة نفسها بعد تلقيها أمرًا بذلك من السلطات السياسية في الدولة.

ثالثًا: مهددات البيئة الرقمية وتأثيراتها على الأمن المعلوماتي: (المعيذر & القحطاني، ٢٠١٥، ص٢٦) (صورية، ٢٠١٦، ص٤١).

١- **مهدد الثقافة والمعرفة التقليدية والإنتماء الوطني،** فجميع الأفكار والمعتقدات مهما كانت مسموح لها بدخول الشبكة ويمكن لأي أحد أن يعمم أفكاره ويدعمها؛ بالإضافة إلى سهولتها في العمل الدعائي والتخريب الاجتماعي والقيمي والأخلاقي، والتي لا يمكن أن تعبر عنها وسائل الإعلام التقليدية، على سبيل المثال إشاعة ثقافة الجنس والمخدرات.

٢- **القرصنة واختراق قواعد البيانات** (توظيف كاميرا الويب والمايك لتصوير وتسجيل ما يدور في الغرفة) فمن السهل تسريب المعلومات والوثائق واختراق أمن الدول والمؤسسات والبنوك والمصارف وحتى التجسس على الرسائل الإلكترونية، وتزويرها، وحتى إجبار الفرد على تقديم معلومات عن نفسه تصل إلى معرفة رقم الحساب ورقم التليفون.

٣- **تغيير مفاهيم الأمن،** فعدم القدرة على السيطرة يهدد الأمن والسيادة وينتهك الخصوصية.

٤- **الفيروسات:** وهي من أهم أسباب ارتكاب جرائم الانترنت التي تسبب إتلافًا للبيانات والمعلومات الموجودة داخل النظام المعلوماتي أو ما يسمى"تدمير المعلومات".

ويضيف آخرون بعض تهديدات البيئة الرقمية والتي من بينها:

(محمود، ٢٠١٦، ص ص٢٢١: ٢٢٨)، (مكتب الأمم المتحدة المعني باالمخدرات والجريمة، فبراير ٢٠١٣، ص٢٤)، (سعيد، يناير ٢٠١٨، ص٩٢٥)، (بن يحي & ال ملوذ، ٢٠٢٠، ص٤٧٩)

٥- **انتشار الإباحية الإلكترونية:** حيث أتاحت شبكات الإنترنت بإمكاناتها المتعددة الفرص لعدد من مستخدميها في نشر الإباحية الإلكترونية، وأوجدت أساليب جديدة للقرصنة وتهديد الخصوصية، وانتهاك الملكية الفكرية، وروجت لكثير من السلوكيات المنحرفة وغير من الأخلاقيات الضارة بالمجتمع.

٦- **الإساءة إلى الآخرين والتشهير والإبتزاز:** عن طريق استخدام دوافع استغلالية، وانتحال الشخصية الخاصة للأفراد أو الاعتبارية للمواقع والشركات.

٧- **انتهاك الخصوصية والانتقام:** من خلال الهجمات الإلكترونية عبر البريد الإلكتروني أو تدمير الصفحات الشخصية، وكذلك عن طريق إنشاء صفحات شخصية بأسماء الآخرين وصورهم والقيم بنشر محتويات غير أخلاقية عليها بغرض تشويه صورتهم

٨- **بث العنصرية والإرهاب:** حيث اتخذت بعض التنظيمات المتطرفة في زرع الشك والشبهات ومحاولة لتقسيم المجتمع إلى طوائف وفرق على أساس عرقي أو فكري.

٩- **الجريمة السيبرانية:** فعلى الصعيد العالمي تشمل الجريمة السيبرانية طائفة واسعة من الجرائم المرتكبة بدافع مالي، والجرائم المتصلة بالمحتوى الحاسوبي، فضلًا عن الأعمال التي تمس بسرية النظم الحاسوبية، وسلامتها وقابلية النفاذ إليها. فإرهاب السيبرانية يعتمد بشكل كبير لى تجنيد بعض الشباب المحترفين من كافة دول العالم بهدف شن هجمات

معلوماتية خطيرة ولها آثار سلبية على الاقتصاد والأمن وحتى قيمة الانتماء لدى بعض أعضاء المجتمع، التي قد تهتز من خلال معلومات وبيانات كاذبة تفتك في عضد المجتمع وتزرع في أركانه الفتن والأوجاع، والتي بدورها تمكن قيمة الاستبعاد والإقصاء لدى أعضاء المجتمع وبالأخص شبابها.

١٠- **التضليل الإلكتروني:** وهو كل الأنشطة الإلكترونية التي تتم داخل العالم الافتراضي سواء كان عن طريق مواقع التواصل الاجتماعي أو عن طريق المواقع الإلكترونية، ويراد منها التأثير على الرأي العام من خلال تزييف الحقائق، والشحن العاطفي، وإشاعة الفوضى الفكرية وغير ذلك من الوسائل الإلكترونية ذات التأثير السلبي والمشبوه على الجماهير".

رابعًا: المهددات المستقبلية للبيئة الرقمية: (نوفل، ٢٠١٢، ص٥٥)

١- التهديد بالإضطراب في تدفق الاتصالات والتحويلات المالية والحملات المعلوماتية الهامة ومحطات الطاقة والمناقصات السياسية والاضطراب في زمن الحرب قد يؤدي إلى الهزيمة والخسارة.
٢- التهديد باستغلال المعلومات الحساسة والملكية الفكرية والمعلومات السرية حيث إن سرقة المعلومات أو الاحتيال بها أو الجرائم الفضائية لها آثار سلبية على المستوى الفردي وعلى المستوى المؤسسي والمستوى الوطني.
٣- التهديد بانتقاء المعلومات لأغراض سياسية أو اقتصادية أو عسكرية واستغلالها أو تدميرها.
٤- التهديد بتدمير المعلومات: تدمير مكونات البناء المعلوماتي التحتي الحساس، ولهذا نتائج سلبية كبيرة على الاقتصاد والأمن الوطني.

المحور الثاني: أمن المعلومات ومواجهة تهديدات البيئة الرقمية

أولاً: مفهوم الأمن المعلوماتي "Information Security":

الأمن المعلوماتي هو: "العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها من أنشطة الإعتداء عليها". **(نوفل، أبريل ٢٠١٠، ص١١)**

ويُعبر الأمن المعلوماتي عن: "مجموعة من الإجراءات والتدابير الوقائية التي تستعمل في المجال الفني أو الوقائي لصيانة المعلومات الخاصة بالإدارة الإلكترونية، والإجراءات القانونية التي تتخذ، تحمي من حدوث أي تدخلات غير مشروعة سواء عن طريق الصدفة أو بشكل مقصود". **(سيد & أحمد، يناير٢٠٢٢، ص٦٦)**

كما يعرف بأنه: "حماية المعلومات والأنظمة من الوصول غير المصرح به أو الاستخدام أو الكشف أو التعطيل أو التعديل أو التدمير من أجل توفير السرية والنزاهة والتوافر". **(Nieles, 2017,p7)**

ويظن البعض خطأ أن الأمن المعلوماتي لا يخرج عن مفهومه التقليدي القديم إلا أن الدائرة اتسعت لتشمل أنواع كثيرة يأتي في مقدمتها الأمن السيبراني.

ويعرف الأمن السيبراني بأنه: مجموعة من الوسائل التقنية والتنظيمات الإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم المعلومات والاتصالات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. **(خضر & المداح، ٢٠٢١، ص ص١٣٠: ١٣١)**

ثانيًا: أهمية الأمن المعلوماتي في مواجهة تهديدات البيئة الرقمية:

- تكمن أهمية أمن المعلومات في أنه من أهم القضايا التي يتم مناقشتها في مجال الشبكات وأمن وسرية المعلومات، ونتيجة لكثرة برامج الفيروسات وبرامج التجسس وسرعة اقتصر دور الكثير من المختصين في تقنية المعلومات في التعامل مع المنظمات لوضع البرامج المضادة للفيروسات وبرامج الاختراق والتسسل والتركيز على مستوى الاهتمام بتنفيذ الإجراءات الأمنية، وتنبع أهمية أمن المعلومات في مواجهة تهديدات البيئة الرقمية من كلِ مما يلي: **(الشوابكة، أكتوبر ٢٠١٩، ص١٦٨)**

١- إجراءات للسيطرة تحول دون الوصول للبرمجيات مع إجراءات تمنع أو تكشف المتطفل من الدخول للنظام.

٢- معدات وبرمجيات مضادة للفيروسات.

٣- تغيير مستمر لكلمات السر والتشفير.

٤- خطط استرجاع سريعة في حالة الكوراث الطبيعية والبيئية.

ثالثًا: أهداف الأمن المعلوماتي: (الجعبري، ٢٠١٨، ص١٨)

يتحدد الهدف الأساسي للأمن المعلوماتي في ضمان حماية أصول المعلومات من مخاطر عديدة كالخسارة وتوقف التشغيل وسوء الاستخدام والإفصاح غير المصرح به، مما يقلل التعرض لأي مسائل قانونية أو مدنية ناتجة عن فقدان المعلومات وتسريبها، كما أن أمن المعلومات يهدف إلى حماية كافة موارد المؤسسة المادية أو المالية وكذلك الأفراد والنواحي التكنولوجية خاصة في ظل تزايد الجرائم الإلكترونية.

رابعًا: مكونات الأمن المعلوماتي:

- **للأمن المعلوماتي ثلاث مكونات أساسية وهي كالتالي: (ليتيم& مسكين، ٢٠١٨، ص٢٢٧)**

١- **سرية المعلومات:** ويشمل هذا الجانب كافة التدابير اللازمة لمنع إطلاع غير المصرح لهم على المعلومات الحساسة أو السرية، ومن أمثلة المعلومات التي يُحرص على سريتها؛ المعلومات الشخصية، والموقف المالي لمؤسسة ما قبل إعلانه، والمعلومات العسكرية.

٢- **سلامة المعلومات:** ويمثل اتخاذ التدابير اللازمة لحماية المعلومات من التغيير، وهناك أمثلة كثيرة فقد يتم تغيير أسماء أشخاص مقبولين في وظيفة ما أو تغيير في مبالغ التحويلات.

٣- **ضمان الوصول إلى المعلومات والموارد الحاسوبية:** فالحفاظ على سرية المعلومات وسلامتها أمر مهم، لكن هذه المعلومات تفقد قيمتها إذا كان من يحق له الإطلاع عليها لا يمكنه الوصول إليها، ويتخذ المهاجمون وسائل شتى لحرمان المستفيدين من الوصول إلى المعلومات، ومن هذه الوسائل حذف المعلومات نفسها أو مهاجمة الأجهزة التي تخزن المعلومات فيها وتعطيلها عن العمل.

خامسًا: متطلبات التوعية بالأمن المعلوماتي لدى الشباب الجامعي: (المعيذر& القحطاني، ٢٠١٥، ص٢٦)

١- بناء الثقة على المستوى الفردي داخل الأسرة، وتعزيز الأمن الجماعي، والمشاركة في القضايا الكبرى.

٢- الحفاظ على أمن وسرية المعلومات على المستوى الشخصي وعلى مستوى الدولة ومؤسساتها.

٣- المساهمة في بناء مستقبل الأجيال الواعية المثقفة بما يناسب متطلبات العصر.

٤- تضافر الجهود في مؤسسات المجتمع الواحد (الأسرة، الجامعة، الثقافة العامة...) في نشر التوعية الأمنية للإنترنت.

ويضيف الباحثان أن هناك متطلبان آخران للتوعية بأمن المعلومات وأهمها:

٥- توفير متخصصين بمجال أمن المعلومات لتدريب الشباب الجامعي على نظم أمن المعلومات من خلال أجهزة رعاية الشباب.

٦- استحداث دور فعلي للأخصائيين الاجتماعيين بإدارات رعاية الشباب الجامعي ضمن اللوائح لتنمية وعي الشباب بتهديدات البيئة الرقمية، والجرائم المعلوماتية وغيرها من صور الاختراقات.

رابعًا: استنتاجات الورقة البحثية:

تأسيسًا على ما سبق عرضه في الورقة البحثية الحالية يتضح للباحثان مجموعة من الاستنتاجات والرؤى التحليلية:

١- مع اتساع الفضاء الإلكتروني وتزايد الإقبال عليه بشكل كبير؛ انتشرت العديد من التهديدات التي تمثلت في العديد من أشكال الجرائم الإلكترونية والسيبرانية والاختراقات والسلوكيات المنافية لأخلاقيات وقيم المجتمعات العربية، والتي طالت البشر بكافة فئاتهم وخاصة الشباب باعتباره من أكثر المستخدمين لشبكات الإنترنت.

٢- تنوعت تلك التهديدات ما بين جرائم الاحتيال المعلوماتي، والإرهاب الرقمي، واختراق الملكيات الفكرية، وجرائم الابتزاز المالي والشخصي، والقرصنة... إلى غير ذلك من أشكالها، والتي كان لكلٍ منها العديد من الأغراض الخبيثة على المستوى الفردي، والمستوى المجتمعي على حد سواء.

٣- نتج عن هذه التهديدات العديد من الآثار السلبية التي طالت وبشكل كبير عقول البشر وثقافتهم، وأمن الدول الاجتماعي والاقتصادي والسياسي، كما طرأت على المجتمعات العربية العديد من التحولات في أنماط حياتهم تشبه بشكل كبير المجتمعات الغربية.

٤- اتضح من نتائج الدراسات والبحوث السابقة والأدبيات المرتبطة بالموضوع أن هناك نقص في الوعي بأنظمة الأمن المعلوماتي، وكيفية استخدامها سواء على أجهزة الحاسوب أو الهاتف المحمول وذلك لدى فئة كبيرة من أفراد أي مجتمع، على الرغم من أن أمن المعلومات هو السبيل الوحيد لتأمين هؤلاء الأشخاص ومجتمعاتهم ضد مخاطر الثورة المعلوماتية الهائلة وما أتت به من تهديدات لمستقبل المجتمعات.

٥- كما اتضح أن هناك نقص في وعي العديد من فئات المجتمع بالتشريعات والقوانين المرتبطة بالجرائم الإلكترونية والعقوبات المرتبطة بها، والأنظمة القانونية لضمان الأمن المعلوماتي.

٦- اتضح أن هناك حاجة ماسة لتدخل العديد من الجهات والمؤسسات والمهن المختلفة لتنمية وعي أفراد المجتمع بأهمية أنظمة الأمن المعلوماتي وأنواعها وكيفية استخدامها، وكذا ضمان الوقاية من مخاطر الهجمات والاختراقات التقنية ذات الأغراض الخبيثة التي أصبحت تهدد كيان المجتمعات البشرية بكافة فئاتها وخاصة الشباب.

وبناءًا عليه تم وضع رؤية مقترحة من منظور الخدمة الاجتماعية لمواجهة تهديدات البيئة الرقمية لدى الشباب الجامعي، وفيما يلي عرض لذلك...

خامسًا: رؤية مقترحة من منظور الخدمة الاجتماعية لمواجهة تهديدات البيئة الرقمية لدى الشباب الجامعي:

- **تتضح تلك الرؤية من خلال مجموعة من الآليات تتمثل فيما يلي:**

١- تنظيم الأخصائيين الاجتماعيين بإدارات رعاية الشباب الجامعي لحملات توعية للشباب الجامعي بمهددات استخدام البيئة الرقمية والآثار المترتبة عليها.

٢- تدريب الشباب الجامعي على كيفية استخدام أنظمة الأمن السيبراني لتحديد أنماط الهجمات المحتملة ومحاولة تلاشيها ومواجهتها.

٣- تنمية وعي الشباب بالتهديدات الرقمية وأهم العقوبات التي وردت بشأنها في القوانين والتشريعات الدولية والمحلية سواء ما للضحية من حقوق، أو المجرم من عقوبات.

٤- توجيه الشباب لتوظيف استخدام المنصات الرقمية في أنشطة مفيدة لتنمية روح الإنتماء وغرس القيم والأخلاقيات التي يرتضيها المجتمع.

٥- تدريب الشباب الجامعي على كيفية الإبلاغ عن المواقع والصفحات والمنصات الرقمية التي تستهدف نشر الشائعات والسلوكيات المنافية لقيم وأخلاقيات المجتمع.

٦- وضع تشريعات داخل الجامعة مستنبطة من التشريعات الخاصة بكل ما يتعلق بالرقمنة تطبق على الشباب الجامعي الذي يثبت عليه أي سلوك رقمي غير أخلاقي أو خارج عند استخدام المنصات الرقمية التعليمية أو غيرها فيما يتعلق بالأنشطة الجامعية.

٧- تنظيم أجهزة رعاية الشباب الجامعية لندوات تثقيفية للشباب الجامعي تستهدف توعيته بمخاطر استخدام الفضاء الإلكتروني بما يشمله من منصات وصفحات وتطبيقات، وكيفية ضمان الأمن المعلوماتي عند استخدامها.

٨- التوسع في عمل البحوث الاجتماعية المرتبطة بالجرائم الإلكترونية ومحاولة وضع الآليات المناسبة للحد منها.

٩- السعي نحو تضمين مناهج دراسية حول الأمن المعلوماتي، والمواطنة الرقمية بجميع كليات الجامعة.

١٠- تأسيس مركز أكاديمي متخصص في الأمن السيبراني بجميع الجامعات تضم "متخصصين مهنيين في في مجال الفضاءات الإلكترونية والذكاء الإصطناعي- أخصائيين نفسيين- أخصائيين اجتماعيين- تربويين...إلخ"، بحيث يقوم المركز بالعديد من الأنشطة من بينها دورات تدريبية وورش عمل وندوات تثقيفية وأبحاث اجتماعية ونفسية بمجال الأمن الرقمي والسيبراني ومجال مواجهة الجرائم والتهديدات الرقمية، بحيث يخدم هذا المركز الشباب الجامعي والمجتمع الخارجي أيضًا.

قائمة المراجع:

١. أحمد، أميرة محمد محمد سيد، (يوليو٢٠٢١): **استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزًا لرؤية مصر ٢٠٣٠**، مجلة البحوث الإعلامية- كلية الإعلام، جامعة الأزهر، ع٥٨، ج٤، ص ص١٧٦٧: ١٧٦٨

٢. بطيخ، حاتم أحمد محمد (أغسطس ٢٠٢١): **تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات**، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات، ع١، مج٧، ص ص١: ١٤٣

٣. بلجراف، سامية & خلود، كلاش (أكتوبر ٢٠١٧): **الإدارة الإلكترونية وإشكالية الأمن المعلوماتي**، مجلة الناقد للدراسات السياسية، ع١، ص٢٦٠

٤. بن يحي، أم كلثوم حكوم & ال ملوذ، حصة محمد (٢٠٢٠): **الأنشطة الطلابية ودورها في الحماية من مخاطر التضليل الإلكتروني طالبات جامعة الملك خالد (أنموذجًا)**، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، ع٢٨، مج٢، ص٤٧٩.

٥. الجعبري، هناء يوسف إبراهيم: **أثر الأمن المعلوماتي على أداء شركات التأمين العاملة في فلسطين، رسالة ماجستير غير منشورة**، كلية الدراسات العليا، جامعة الخليل.

٦. الجهاز المركزي للتعبئة العامة والإحصاء، ٢٠٢٠.

٧. خضر، كمال فتحي كامل& المداح، سمر وصفي علي (٢٠٢٠): **العلاقة بين الاقتصاد الرقمي وأمن المعلومات "دراسة تطبيقية على عينة من عملاء البنك الأهلي المصري**، المجلة العلمية للاقتصاد والتجارة، ص ص١٣٠: ١٣١

٨. الزبن، غدير برنس & الخرابشة، عبد الكريم عوده الله (٢٠٢١): **الجرائم الإلكترونية ومستوى الوعي بخطورتها- دراسة ميدانية على عينة من الشباب الجامعي الأردني**، مجلة الجامعة الإسلامية للعلوم الإنسانية ع٢، مج٢٩، ص٢٣١

٩. سعيد، محمد محمود خضر (يناير ٢٠١٨): **تهديدات الإجرام السياسي والمعلوماتي على روح الإنتماء لدى الشباب "دراسة ميدانية للأبعاد الأمنية بمحافظة الأقصر**، مجلة كلية الآداب جامعة بورسعيد، ع١١، ص ص٩١٣: ٩٣٩

١٠. سيد، آية طارق عبد الهادي & أحمد، منار علي محمد (يناير ٢٠٢٢): **دور الإعلام الإلكتروني في التوعية بأهمية الأمن المعلوماتي وتفاعل الجمهور معه: دراسة تطبيقية على البنوك المصرية**، مجلة مستقبل العلوم الاجتماعية، ع٨، ص٦٦

١١. الشوابكة، عدنان عواد (أكتوبر ٢٠١٩): **دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف**، المجلة العربية في العلوم الإنسانية والاجتماعية، ع١، مج١١، ص١٦٨.

١٢. الصالح، إكرام بنت محمد (٢٠١٨): **دور الممارس العام في مواجهة التغير في النسق القيمي لدى الطالبة الجامعية الناتج عن استخدام وسائل التواصل الاجتماعي من خلال النموذج المعرفي**، مجلة الجامعة الإسلامية للدراسات الإنسانية، ع٢، مج٢٦، ص ص٢٠٤: ٢٣٩

١٣. صورية، بورباية: **قواعد الأمن المعلوماتي – دراسة مقارنة-**، رسالة دكتوراه غير منشورة، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس. سيدي بلعباس، ٢٠١٦

١٤. عبد الحميد، عائشة (أكتوبر ٢٠٢٠): **دور جهاز الدفاع الوطني في تحقيق الأمن المعلوماتي في ظل تنامي الإجرام السيبراني**، المجلة العربية للمعلوماتية وأمن المعلومات، ع١، مج١، ص٢٢
١٥. عبد الله، أمال كامل (٢٠١٢): **نحو مفهوم موسع لحماية الاستثمارات الأجنبية (الالتزام بحماية الأمن المعلوماتي)**، مجلة الحقوق، ع١، مج١٠، ص ص٣١٧: ٣١٨
١٦. عبد المنعم، رانية عبد الله (٢٠٢١): **البيئات الرقمية القائمة على التعلم التكيفي وفاعليتها في تنمية مهارات الفهم العميق**، الجامعة العلمية لجامعة الملك فيصل، ع١، مج٢٢، ص٢٨٩
١٧. الكفارنة، أحمد عارف أرحيل (ديسمبر ٢٠١٤): **مخاطر التقنيات المعاصرة على الأمن الفكري "دراسة مطبقة على طلبة جامعة البلقاء التطبيقية"**، مجلة العلوم الإنسانية، جامعة العربي بن مهيدي أم البواقي، ع٢.
١٨. ليتيم& مسكين (٢٠١٨): **المستهلك الإلكتروني وإشكالية التسويق الشبكي لخصوصية وأمن المعلومات: دراسة حالة خدمات مواقع التواصل الاجتماعي**، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، ع٣٣، مج١١، ص٢٢٧
١٩. محمود، عماد عبد اللطيف (٢٠١٦): **رؤية تربوية مقترحة لمواجهة مخاطر شبكات التواصل الاجتماعي**، مجلة دراسات في التعليم الجامعي، ع٣٤، ص ص ١٧٤: ٢٨٩.
٢٠. المعيذر، ريم عبد الله & القحطاني، أمل سفر (٢٠١٥): **فاعلية استراتيجية الصف المقلوب في تنمية مفاهيم الأمن المعلوماتي لدى طالبات المستوى الجامعي**، المجلة الدولية التربوية المتخصصة، ع٨، مج ٤، ص٢٢، ٢٦
٢١. مكتب الأمم المتحدة المعني بالمخدرات والجريمة (فبراير٢٠١٣): **دراسة شاملة عن الجريمة السيبرانية**، نيويورك ٢٠١٣، ص٢٤.
٢٢. نوفل، هالة كمال أحمد (٢٠٢١): **جرائم اختراق البيئة المعلوماتية في المجتمعات الافتراضية واستشراف الاتجاهات الحديثة في مجال أمن المعلومات دراسة أبستمولوجية في ضوء أراء عينة من المتخصصين**، مجلة كلية الآداب بقنا، ع٢، مج٣٩، ص٥٥
٢٣. نوفل، هالة كمال أحمد نوفل: **استطلاع رأي النخبة حول جرائم اختراق البيئة المعلوماتية الافتراضية واستشراف الاتجاهات الحديثة في مجال أمن المعلومات**، المؤتمر السادس لجمعيات المكتبات والمعلومات السعودية "البيئة المعلوماتية الآمنة- المفاهيم والتشريعات والتطبيقات"، الرياض، ٦: ٧ أبريل ٢٠١٠، ص١١
٢٤. هشام، فريجة محمد (يونيو ٢٠١٨): **النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الإلكتروني**، حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، ع٢٤، ص ص١٤١: ١٦٣.
٢٥. وزارة الاتصالات وتكنولوجيا المعلومات: **مؤشرات قطاع الاتصالات وتكنولوجيا المعلومات**، أكتوبر ٢٠٢١، جريدة الوطن، ٧ يناير ٢٠٢٢.
26. Sadosky, George et, al (2003): **Information technology security handbook**, O'Reilly & Associates, Inc., 3rd edition, pv.
27. Gladden, Matthew (February 2017): **An Introduction to Information Security in the Context of Advanced Neuroprosthetics**, https://www.researchgate.net

28. **Nieles,** Michael et. al (June 2017): **An introduction to information Security,** National Institute of Standards and Technology, p7 https://doi.org