مجلة العلوم الاجتماعية والتطبيقية
Journal of Social and Applied Sciences

مجلة
العلوم الاجتماعية والتطبيقية

JOURNAL OF SOCIAL AND APPLIED SCIENCES

دورية محكمة ربع سنوية

تصدر عن الجمعية المصرية للدراسات الانسانية والخدمات العلمية

العدد الخامس
يناير 2025 م

رئيس التحرير
الاستاذ الدكتور/ يسري شعبان عبدالحميد

مدير التحرير
دكتور/ محمد عطا عبدالعزيز

سكرتير التحرير
دكتور/ منه حسن عمر

مجلة العلوم الاجتماعية والتطبيقية

ورقة عمل بعنوان

الاتجاهات النظرية والمنهجية الحديثة في طريقة العمل مع الجماعات وتنمية الوعي لدى الشباب الجامعي بمخاطر الجرائم الإلكترونية

Modern Theoretical and Methodological Trends in How to Work with Groups and Developing University Youth Awareness of the Dangers of Electronic Crimes

إعداد

عبد المنعم أحمد إبراهيم حمدان

استاذ مساعد بقسم الخدمة الاجتماعية وتنمية

المجتمع بكلية التربية – تفهنا الاشراف – دقهلية

جامعة الازهر

المخلص

الاتجاهات النظرية والمنهجية الحديثة في طريقة العمل مع الجماعات ، وتنمية الوعي لدى الشباب الجامعي بمخاطر الجرائم الإلكترونية.

هدف البحث إلى التعرف على الاتجاهات النظرية والمنهجية الحديثة في طريقة العمل مع الجماعات وتنمية الوعي لدى الشباب الجامعي بمخاطر الجرائم الإلكترونية ، وقد تم الاعتماد في هذا البحث على المنهج الوصفي التحليلي والمنهج الاستقرائي والاستنباطي، حيث يشهد العصر الحالي ثورة كبيرة في مجال الاتصالات أثرت بشكل مباشر في حياة الإنسان ، ونظرا للتزايد المستمر لأعداد مستخدمي الإنترنت في العالم ، فقد أبرزت شكلًا من الجرائم الإلكترونية وهى من أخطر وأسرع الظواهر الإجرامية نموًا ، وهى نتاج سلبي لتطوير تكنولوجيا المعلومات.

والخدمة الاجتماعية يمكن أن تساهم بشكل مباشر من خلال أدوارها المختلفة في تنمية الوعي للشباب الجامعي بمخاطر الجرائم الإلكترونية من خلال طريقة العمل مع الجماعات وذلك من خلال أدواتها، وأساليبها، واستراتيجياتها .

الكلمات الإفتتاحية : الشباب الجامعى – الجرائم الإلكترونية

Abstract:

Modern Theoretical and Methodological Trends in How to Work with Groups and Developing University Youth Awareness of the Dangers of Electronic Crimes

The study aimed at identifying the theoretical and methodological trends in how to work with groups and developing university youth awareness of the dangers of electronic crimes. This study relied on the descriptive analytical approach and the inductive approach. The current era is witnessing a major revolution in the field of communication that has directly affected human life, and due to the continuous increase of the number of Internet users daily in the world, some crimes, that did not exist before, have appeared including electronic crimes. Such crimes are considered the most dangerous and fastest growing criminal phenomena that directly affect young people due to their ease of use. Social service can contribute directly via its various roles in making university youth aware of these risks through the various tools, methods, techniques and strategies used by specialists working with groups to develop their awareness.

Keywords: university youth – electronic crimes

أولًا: مقدمة :

يشهد العالم اليوم طفرة نوعية في مجال الاتصال وذلك من خلال شبكة المعلومات العالمية والتي جعلت الوصول للمعلومات والتواصل متاحًا في جميع الأوقات ، ونجحت خلال وقت قصير أن تستحوذ على اهتمامات الأفراد في كافة المراحل العمرية ومنها الشباب الجامعي.

ولاشك أن هذه الشبكة العملاقة التي تُعتبر من أحدث التقنيات في هذا العصر يجب أن نتعامل معها بحذر شديد ، فهى إحدى صور العولمة ولا يمكن رفضها بالكلية ، فهى واقع فرض علينا ويجب أن نتعامل معه فيما يُحقق الخير والنفع لنا ، وتعتبر شبكة المعلومات الدولية سلاح ذو حدين فهى نافعة ومفيدة في مجالات كثيرة ومن بينها المجال التعليمى من حيث أنها تساعد على تحسين المستوى الدراسى للطلاب ، وزيادة مشاركتهم في الأنشطة الاجتماعية ، وتشكيل قيمهم واتجاهاتهم ، وتساعد على إثراء العملية التعليمية للطلاب ، ويتوقف ذلك كله على مستخدم الشبكة وليس على الشبكة نفسها ، وعلى الجانب الآخر نجد أن لها بعض المخاطر والتى تقع على مستخدميها نتيجة سوء الاستخدام ، وقد يرجع ذلك لعدة عوامل منها المرحلة العمرية ، الدخل ، التعليم ، وكذلك الدوافع من استخدامها والإشباعات التي تحققها ، وقد ينتج عنها مشكلات كثيرة نتيجة سوء الاستخدام (سليم ، ٢٠٢٢ ، ص ٤١٣) .

ولقد بلغ عدد مستخدمي الإنترنت في العالم ٤,٩٥ مليار شخص وذلك وفقًا لإحصائيات عام ٢٠٢٢ ، وهذا الرقم يُعادل تقريبًا ٦٢% من إجمالي سكان العالم ، كما أن هذا العدد في تزايد مستمر حيث يُوجد حوالى ٢٥٧ مليون مستخدم جديد للإنترنت خلال العام الواحد تقريبًا ، ويُقدر معدل تزايد مستخدمي الإنترنت حاليًا بحسب تقارير إعلامية حوالى ٥,٧% أي ما يُعادل ٧٠٠ ألف مستخدم جديد كل يوم ، حيث بلغ عددهم في مصر ٧٤ مليون مستخدم ، ٤٨٠ ألف مستخدم بنهاية أكتوبر ٢٠٢١م ، مقابل ٦٣,٤٨ مليون في نفس الفترة من العام الماضى (سالم ، ٢٠٢٢) .

وبالنظر إلى هذه الإحصائيات لمستخدمي الإنترنت نستطيع أن نرى مدى الحجم الهائل والمتزايد في الانتشار، ومن هنا يُمكننا القول أن هناك علاقة طردية بين مستخدمي الإنترنت والجرائم الإلكترونية ، فكلما زاد عدد مستخدمي الإنترنت كلما زادت عدد الجرائم الإلكترونية .

والجرائم الإلكترونية ظاهرة اجتماعية تتواجد بتواجد الإنسان وتتطور بتطورها، ولاشك أن المجرمين يحاولون الاستفادة من هذا التقدم التقني، ونحن في عصر ثورة المعلومات وتقدم العلوم الحديثة والتكنولوجيا المتطورة ، وتبعًا لذلك فإنه من البديهى أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق ، وهذا ليس قاصرًا على أسباب التقدم التقني فقط بل يحدث دومًا وبصفة

مستمرة ، فالمجرم والجريمة في تقدم وتجدد مستمر ، فمجرم الأمس ليس كمجرم اليوم ، وقد تمخضت ثورة المعلومات والتكنولوجيا المتقدمة عن وسائل اتصالات متطورة جعلت العالم قرية إلكترونية مفتوحة للعموم ، ألغت معها الحدود الجغرافية والسياسية للدول ، وهذه التقنية الخاصة بنظام نقل المعلومات السريع أو ما يعرف بالإنترنت ليست سيئة في حد ذاتها بل هي سلاح ذو حدين ، فيمكن أن تسخر للخير والمنفعة ، كما يمكن أن تسخر للشر والمضرة (شفلوت ، ٢٠٢١ ، ص ٢٤٠) .

هذا وتحظى قضايا الشباب ومشكلاتهم واهتماماتهم في هذه المرحلة بقدر كبير من الاهتمام نظرًا لمكانتهم الخاصة في المجتمع باعتبارهم الفئة المؤثرة فيه ووضعها الطبيعى على المستوى القومي العام ، وقضايا الشباب مهما كانت خاصة بهم فإنها مرتبطة ارتباطًا عضويًا بالقضايا العامة في المجتمع ، وانعكاس هذه القضايا العامة هو الذي يدفعهم إلى تحركاتهم المرضية أو غير المرضية (فهيم ، ٢٠٠٧ ، ص ١٥٥) .

كما كشف الجهاز المركزي للتعبئة العامة والإحصاء أنه طبقًا لبيان السكان في يناير ٢٠٢٣م فقد بلغ عدد الشباب الجامعي المصري في الفئة العمرية (١٨ – ٢٩ سنة (٢١,٩ مليون نسمة بنسبة ٢١% من إجمالي السكان (٥٠,٥% ذكور – ٤٩,٥% إناث) (الجهاز المركزى للتعبئة العامة والإحصاء ، ٢٠٢٣) .

ومن هنا يجب الاهتمام بقضايا ومشكلات الشباب الجامعي لأنهم أكثر الفئات استخدامًا لتلك المواقع الإلكترونية حيث إن هؤلاء الأكثر استخدامًا لها حيث يمتلكون المهارات الحاسوبية ولديهم اطلاع واسع على الكمبيوتر واستخداماته وشبكات الإنترنت مما يُمكنهم من تصميم صفحات خاصة بهم بكل سهولة (شفرة ، ٢٠٢٠ ، ص ١٤) .

ومن هنا أصبحت مخاطر الإنترنت على أفراد المجتمع وخاصة الشباب الجامعي من الظواهر الجديدة بالبحث والتنقيب وزيادة وعيهم وحمايتهم ، ولضمان المزيد من الأمن والاستقرار لمجتمعاتنا لذلك لابد من مواجهة تلك الجرائم الإلكترونية .

والخدمة الاجتماعية مهنة تهدف إلى تنمية المجتمعات بتفادى جميع الأضرار المهددة لهم كأفراد أو جماعات أو مجتمعات ، وذلك باستثمار الطاقات الشخصية والبيئية وخدمة الجماعة إحدى طرق مهنة الخدمة الاجتماعية التي تعمل مع الجماعات وتستخدمها كأداة ووسيلة لتغيير وتنمية الأعضاء عن طريق توفير الفرص المتنوعة التي تنتجها الجماعة لإحداث تغييرات جوهرية في اتجاهات أعضاء الجماعة وسلوكهم ، وممارسة السلوك الاجتماعي السليم .

هذا ولقد زاد الاهتمام بطريقة العمل مع الجماعات في عصر التكنولوجيا باعتبارها من الطرق الأساسية التي تعمل على تعديل وتغيير عضو الجماعة أثناء وجوده في الجماعة (آخرون ، نصيف منقريوس ، ٢٠٠٤ ، ص ٣٤٩) .

ولقد تناولت العديد من الدراسات الجرائم الإلكترونية وذلك على النحو التالى :

ما أشارت إليه دراسة : حميد مصطفى (٢٠١٩) : والتي هدفت إلى التعرف على طبيعة الجرائم السيبرانية وأنواعها والوقوف على واقع التطرف الرقمي والإرهاب السيبراني والتعرف على معوقات مكافحة الجرائم السيبرانية، مع وضع استراتيجية لمكافحة الجرائم السيبرانية ، وتوصلت الدراسة إلى توسع دائرة الفكر المتطرف عبر شبكة الإنترنت. وأوصت برفع نسبة التوعية بمخاطر الجرائم السيبرانية عبر الوسائل الإعلامية المختلفة و تعزيز المشاركة في الانضمام إلى الاتفاقات الدولية لمكافحة الجرائم .

وفي نفس السياق هدفت دراسة (نظمي ، ٢٠١٩) إلى التعرف على أنماط الجرائم الإلكترونية المرتكبة ضد الإناث من خلال التعرف على تصنيفها وأسبابها وخصائص مرتكبى الجرائم الإلكترونية ، والكشف عن العلاقة بين وسائل الإعلام والجرائم الإلكترونية ، وتوصلت الدراسة إلى أن أهم سبب لظهور تلك الجرائم الإلكترونية هي العولمة وتلك الاستحداثات الجديدة والتي ظهرت في مطلع القرن الحادي والعشرين ومنها التكنولوجيا .

في حين هدفت دراسة (الشهراني ، ٢٠١٩) التعرف على العوامل المؤدية إلى ارتكاب جرائم الإرهاب السيبرانى الأكثر انتشارًا عبر المواقع الإلكترونية والتعرف على آليات ضبط استخدام الشباب للمواقع الإلكترونية للوقاية من مخاطر الإرهاب ومتطلبات وقاية الشباب الجامعى من مخاطر الجرائم مع وضع تصور مقترح يسهم في وقاية الشباب الجامعى من مخاطر الإرهاب السيبرانى وأوصت الدراسة بضرورة توعية الشباب بالاستخدام الأمثل للمواقع ومعرفة مخاطر الإنحراف عبر المواقع الإلكترونية .

بينما هدفت دراسة (القرنى ، ٢٠١٩) إلى التعرف على دور الأسرة السعودية في تحصين أبنائها من مخاطر الإنترنت تبعًا لمتغير الجنس ، المستوى التعليمي مع تقديم مقترحات لتفعيل دور الأسرة في تحصين أبنائها من مخاطر الإنترنت.

في حين أبرزت دراسةNazilah, et al (٢٠١٩) ازدياد استخدام الإنترنت بشكلٍ كبير في السنوات الأخيرة، وأصبح معظم المستخدمين من المراهقين، حيث سهلت تكنولوجيا الإنترنت حدوث

أنشطة التهديدات السيبرانية والجرائم الإلكترونية، وبالتالي يحتاج المستخدمون في مرحلة المراهقة إلى توجيه ودعم الوالدين لأنهم ما زالوا غير ناضجين لفهم مخاطر الإنترنت.

وفي نفس السياق، أكدت دراسة Alemany, et al (٢٠١٩) على أن مخاطر الخصوصية في الشبكات الاجتماعية عبر الإنترنت تعتبر أحد المخاوف الرئيسية التي زادت في السنوات القليلة الماضية. وعلى الرغم من أن تطبيقات الشبكات الاجتماعية توفر آليات للتحكم في المخاطر، إلا أن المراهقين لا يدركون في كثير من الأحيان مخاطر الخصوصية الناجمة عن الكشف عن المعلومات في الشبكات الاجتماعية عبر الإنترنت مما يتسبب في وقوعهم ضحايا للجرائم الإلكترونية.

بينما ركزت دراسة Zwilling, et al (٢٠٢٠ على التعرف على العلاقات بين الوعي والمعرفة والسلوك في مجال الأمن السيبراني، ومدى توفر أدوات حماية الأفراد من الجرائم الإلكترونية بشكل عام في أربع دول: وهي، إسرائيل، وسلوفينيا، وبولندا، وتركيا. وشملت العينة (٤٥٩) طالباً شاركوا في الاستطلاع من أقسام الإدارة وإدارة الأعمال، بواقع ٥٢% إناث و٤٨% ذكور، وأظهرت النتائج أن مستخدمي الإنترنت يمتلكون وعيًا كافيًا بالتهديدات السيبرانية ومخاطر الجرائم الإلكترونية ولكنهم لا يطبقون سوى الحد الأدنى من تدابير الحماية التي عادةً ما تكون شائعة وبسيطة نسبيًا.

إلا أن دراسة (عكة ، مناصرة ، ٢٠٢٠) هدفت إلى التعرف على العوامل الاجتماعية والنفسية لدى مرتكبي الجرائم الإلكترونية ذات الطابع الجنسي من وجهة نظر المختصين لدى الأجهزة الأمنية ، وخلصت الدراسة إلى أن أهم النتائج تكمن في غياب الرقابة على الأبناء والاهتمام سواء من الزوج أو الزوجة تجاه الآخر ، قلة فرص العمل والوضع الاقتصادى السيئ والبطالة ، وأوصت الدراسة بتفعيل قانون الجرائم الإلكترونية لردع الجناة.

هذا ويتفق مع ما سبق دراسة (الزين ، الخرابشة ، ٢٠٢١م) والتي هدفت إلى تحديد نوع الجرائم الإلكترونية التي تعرض لها الشباب الجامعي الأردني ، تحديد مستوى وعى الشباب بالجرائم الإلكترونية ، وأوصت الدراسة إلى توعية الطلاب بأهمية إدارة الوقت واستثمار وقتهم عند استخدام الإنترنت ، وزيادة المحاضرات للتوعية بمخاطر الجرائم الإلكترونية .

كما حاولت دراسة (أحمد ، ٢٠٢١) التركيز على الأهداف الآتية : توفير قواعد الاختصاص القضائي من قبل التشريعات الوضعية والاتفاقات الدولية ، والصعوبات التي تعتري إجراءات التحقق ، وجذب انتباه المشرعين والقانونيين في المجتمع المصري والمغربي بصفة خاصة والمجتمع الدولي بصفة عامة إلى ضرورة إصدار وصياغة العديد من القوانين والتشريعات والتي تعمل على مكافحة الجرائم الإلكترونية.

هذا وقد هدفت دراسة (العنزى ، ٢٠٢١) إلى التعرف على واقع ممارسة نزلاء دار الملاحظة الاجتماعية للألعاب الإلكترونية ، والتعرف على دور الألعاب الإلكترونية في ارتكاب الجرائم لدى نزلاء دار الملاحظة الاجتماعية ، وتوصلت إلى أنه : لبعض الألعاب الإلكترونية دور كبير في تعليم شرب الدخان وتعليم تعاطي المخدرات ، وتساعد بعض الألعاب الإلكترونية في ارتكاب جريمة الابتزاز ، وأوصت الدراسة بضرورة متابعة الجهات الأمنية لمواقع الألعاب الإلكترونية والعمل على توعية الآباء من أضرارها.

في حين هدفت دراسة (الصياد ، ٢٠٢١). إلى تحديد الجرائم الأسرية المترتبة على الإدمان الإلكترونى ودور الأخصائي الاجتماعي كممارس عام وذلك من خلال تحديد أسباب الإدمان الإلكترونى وآثاره وأنواع الجرائم الأسرية الناتجة عن الإدمان واقترحت الدراسة قيام الدولة بحجب المواقع المنافية للقيم الاجتماعية ،اهتمام وسائل الإعلام بالبرامج الوقائية للتوعية بخطورة الإدمان الإلكترونى .

كما هدفت دراسة (سليم ، ٢٠٢١). إلى التعرف على أنواع برامج جماعات النشاط لتوعية الطلاب بالاستخدام غير الآمن للإنترنت.

في حين هدفت دراسة (أحمد ، ٢٠٢١) إلى التعرف على دور خدمة الجماعة المقترح في التعامل مع الآثار السلبية المترتبة على إدمان الأطفال للألعاب الإلكترونية ، وذلك من الناحية الصحية ، الجسمية ، الثقافية ، والتعليمية ، الناحية الاجتماعية والنفسية والأخلاقية مع وضع تصور مقترح لتوعية الطلاب بالآثار السلبية لإدمان الألعاب الإلكترونية ،.

إلا أن دراسة (جاب الله ، ٢٠٢٢م)هدفت إلى التعرف بالأمن السيبرانى، ومعرفة أهميته وبيان الهدف منه ، والتعرف على دور الوسائل الشرعية والنظامية التي تحمي الأمن السيبراني ومدى صلاحية الشريعة الإسلامية لكل زمان ومكان ، ومواكبتها للنظم المعاصرة ، وأوصت الدراسة بضرورة تنمية الوعي المجتمعب بخطورة الجرائم وطرق الوقاية.

أما دراسة (على ، ٢٠٢٢). فقد هدفت إلى تحديد مستوى وعي الشباب الجامعي بمخاطر الجرائم الإلكترونية وتحديد المعوقات التي تحد من التخطيط لتنمية وعي الشباب الجامعي بمخاطر الجرائم الإلكترونية، كما أثبتت الدراسة صحة الفرض الثالث والذى مؤداه توجد فروق معنوية ذات دلالة إحصائية بين استجابات الطلاب وفقا للمرحلة الجامعية في تحديدهم لمستوى تنمية وعي الشباب الجامعي بمخاطر الجرائم الإلكترونية .

وبناءً على ما سبق عرضه من الدراسات السابقة فإن الباحث يؤكد على أهمية وعي الشباب الجامعي بمخاطر الجرائم الإلكترونية وذلك من خلال الاتجاهات النظرية والمنهجية الحديثة في طريقة العمل مع الجماعات ، وذلك في ظل التغيير الاجتماعي والتحول السريع والمتزايد لشبكات التواصل الاجتماعي والتي تُسهم بشكلٍ كبير في استخدامه لجميع فئات المجتمع ومنهم الشباب الجامعي ، فهو وسيلة هامة لسهولة الاتصال ووفرة المعلومات وتدفقها حيث لم تعد تلك المواقع مجرد وسيلة تواصل معلوماتية وترفيهيه بل أصبحت تلعب دورا خطيرًا وحيويًا في كافة المجالات الحياتية المعاصرة ، كما أنها تستطيع أن تؤدي وظائف مستقلة في مجال التأثير ونقل الأحداث .

وفى ضوء العرض السابق يتضح أن ثمة ضرورة للمراجعة النظرية والمنهجية والميدانية للدراسات والبحوث والتجارب التي تناولت الجرائم الإلكترونية لتنمية وعليه فقد تحددت مشكلة الدراسة في التساؤل الرئيس" ما الاتجاهات الحديثة في طريقة العمل مع الجماعات لتنمية وعي الشباب الجامعي بمخاطر الجرائم الالكترونية"

ثانيًا – أهمية الدراسة:

١- نظرًا لزيادة الاهتمام العالمي والإقليمي والمحلي بموضوع الجرائم الإلكترونية الذي ينال اهتمام كبير وواسع في ظل المتغيرات المعاصرة .

٢- لكون الجرائم الإلكترونية تُعد هي القضية الأبرز والأكثر أولوية على الساحة العالمية والمحلية ، وأصبح ضمن أولويات المنظمات العالمية والمحلية والحكومية والأهلية ولذلك أقيمت عدة مؤتمرات لمكافحة الجرائم تصل إلى ١٥ مؤتمر حتى الآن عن أساليب المكافحة ومنها إقامة (الجمعية المصرية لمكافحة جرائم المعلومات والإنترنت).

٣- نظرًا للتقدم الهائل في تكنولوجيا الاتصالات والمعلومات وتأثيره على الجوانب الاجتماعية والثقافية للشباب الجامعي مما أدى ذلك إلى ارتباطهم بالإنترنت .

٤- الاهتمام العالمي والإقليمي والمحلي بقضايا الشباب في المجتمع باعتبارهم أهم العناصر الأساسية لتقدم الشعوب والمجتمعات وهم مصدر القوة الحيوية وسر التقدم وأساس بناء الأمم

٥- لكون الشباب الجامعى شريحة اجتماعية في المجتمع يجب أن تحظى بالمزيد من الرعاية والتوجيه حيث بلغت نسبتهم ٢١% من إجمالي السكان .

٦- تُمثل الدراسة توجيها للمشكلات والقضايا المجتمعية المهددة للشباب الجامعي نتيجة الإفراط في استخدام الوسائل التكنولوجية المختلفة والتي تحتاج إلى تنمية وعي الشباب الجامعب بمخاطرها.

٧- لمسايرة الاتجاهات المعاصرة التي تُنادى بأهمية تنمية الوعي بمخاطر الجرائم الإلكترونية .

٨- لاعتبار مهنة الخدمة الاجتماعية من المهن التي لها دور بتنمية وعي الشباب الجامعى بمخاطر الجرائم الإلكترونية وذلك من خلال التعاون والتكامل مع مختلف التخصصات والمهن والخبرات المتخصصة في عالم مكافحة الجرائم الإلكترونية .

٩- نظرًا للأهمية التطبيقية للبحث ولاسيما طريقة خدمة الجماعة يمكن أن يكون لها دورا فعالًا في تنمية وعب الشباب الجامعي بمخاطر الجرائم الإلكترونية وذلك من خلال استخدام أدوات وأساليب ومهارات وموجهات للأخصائي الاجتماعي .

١٠- لما يمكن أن يسهم به هذا البحث في إثراء الجانب المعرفي والفكري والمهاري من خلال إثراء المكتبات العربية بدراسات في موضوع تنمية وعي الشباب الجامعب بالجرائم الإلكترونية .

ثالثًا: هدف البحث:

يتمثل الهدف الرئيس للبحث في التعرف على ابرز الاتجاهات النظرية والمنهجية الحديثة في طريقة العمل مع الجماعات وتنمية وعي الشباب الجامعي عن مخاطر الجرائم الإلكترونية من خلال تنمية الوعي المعرفي، والسلوكي للشباب الجامعي، المهاري للأخصائي الاجتماعي للعمل مع الجماعات.

رابعًا: مفاهيم البحث :

أ- مفهوم الشباب الجامعي :

لا يوجد إجماع حول تعريف مشترك للشباب الجامعي ، فالشباب في اللغة مشتق من الفعل شب وجمعه شباب وشبان وشيبة وهى خلاف الشيب والمؤنث شابة وجمعها شابات والشباب من أدرك سن البلوغ إلى سن الثلاثين ، وهى تعنى القوة والحداثة ، وشباب النشئ أوله ويقال لقيته في شباب النهار (مجمع اللغة العربية ، ١٩٨٠ ، ص ٣٣٣) .

ويعرفه معجم العلوم الاجتماعية بأنهم الأفراد في مرحلة المراهقة أي الأفراد بين مرحلة البلوغ والنضج وأحيانا يستعمله بعض العلماء ليشمل المرحلة من سن الثلاثين (مدكور ، ١٩٧٥ ، ص ٦٤٤) .

كما تحدد مرحلة الشباب من منظور سلوكى باعتبارها مرحلة تشكل مجموعة من الاتجاهات السلوكية الاجتماعية إذ تميز بها الإنسان وانطبقت على شخصيته وتصرفاته وأفعاله يمكن اعتباره شابا (السكرى ، ٢٠٠٠ ، ص ٦٠) .

كما يعرف الشباب الجامعي بأنهم تلك الشريحة من الشباب المنتمين إلى المؤسسات التعليمية التي يعود عليها احتلال المكانة الاجتماعية المستقلة داخل المجتمع وتربط بينهم اهتمامات

وميول ولغة مشتركة نتيجة انتمائهم إلى المؤسسات التعليمية المشتركة ، حيث تلعب الجامعة دورا هاما في حياة الشباب وتنمية شخصيته (توفيق ، ٢٠٠٢ ، ص ٥) .

ويمكن تعريف الشباب الجامعي هو الشخص الذي يدرس مقرر دراسي في الجلسة أو مؤسسة في التعليم العالى (الصوفى ، ١٩٩٧ ، ص ١٥٩) وهناك من يُعرف الشباب الجامعي أنه كل من يلتحق بالجامعة بهدف الحصول على شهادة علمية ومن التحاقه بالجامعة يتعلم بعض ألوان المعرفة ويكتسب بعض المهارات العلمية والاجتماعية (إبراهيم ، ٢٠٠٠ ، ص ٩١٦) .

ويمكن تعريف الشباب الجامعي إجرائيًا بما يتواكب مع الدراسة الحالية بأنهم هم الطلاب الذين ينتمون إلى الجامعات المصرية تتراوح أعمارهم ما بين (١٨ – ٢٥ سنة) من الذكور والإناث ومنتظمون بالدراسة ويستخدمون وسائل التواصل الاجتماعي بشكل مستمر .

ب- مفهوم الجرائم الإلكترونية :

تُعرف الجريمة عمومًا في نطاق القانون الجنائب فعل غير مشروع صادر عن إرادة جنائية يقر له القانون عقوبة أو تدابير احترازية (منى ، ١٩٨٩ ، ص ٢٥) .

كما تُعرف بأنها نوع من الخروج عن قواعد السلوك التي يضعها المجتمع لأفراده ، فالمجتمع إذن هو الذي يُحدد ماهية السلوك العادي وماهية السلوك الإجرامى أو الانحرافى وفقًا لقيمه ومعاييره ، ويتضح م هذا التعريف أن الجريمة هي الخروج عن القواعد القانونية التي حددها المجتمع (السنهورى ، ٢٠٠٢ ، ص ٣٧) .

ويُقصد بالجريمة ارتكاب فعل أو امتناع عن القيام بواجب منصوص عليه قانونًا ومُعاقب عليه بمقتضى هذا القانون ويُعرف القانون الجريمة بأنها كل فعل أو سلوك يخالف أو تجرمه القواعد القانونية الموضوعة في مجتمع ما فلا جريمة بدون نص (جوهر ، ٢٠١٤ ، ص ١٨).

ويرى عبد الهادى (٢٠١٨ ، ص ١٣٨) على أنها جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية بواسطة نظام حاسوبى أو شبكة حاسوبية وهى متعددة الأشكال والأنواع وتزداد اتساعا كلما زاد الحاسوب الآلى وتوسع في مجال شبكة الإنترنت .

كما تُعرف الجرائم الإلكترونية المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة ويقصد إيذاء سمعة الضحية أو أذى مادى أو عقلى للضحية مباشرة أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (Halder , D & Jaishankar , K , ٢٠١١, P ٩) .

وتبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفًا بأنها أي جريمة يمكن ارتكابها بواسطة نظام حاسوبى أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية الجرائم التي يمكن ارتكابها في بيئة إلكترونية (Zavrsnik , ٢٠٠٨ , P . ٢).

وفي ضوء ما سبق يمكن تعريف الجرائم الإلكترونية إجرائيًا على أنه كل سلوك غير قانوني وغير أخلاقي منافي للسلوك الأخلاقي ، ويتم استخدامها بالحاسب الآلى عن طريق وسائل التواصل الاجتماعى التي يرتكبها ضد أفراد أو مجموعات من الأفراد ويطلق عليها مسميات عديدة جرائم الإنترنت ، الجرائم السيبرانية ، أو الحروب الإلكترونية أو الجرائم المالية .

خامسًا : الموجهات النظرية للدراسة :

نظرية التفاعلية الرمزية :

يرجع أصحاب هذه النظرية جذورها إلى أفكار عالم الاجتماع الألماني ماكس فيبر الذى أكد على أن العالم الاجتماعي يكون من خلال فهم اتجاهات الأفراد الذين يتفاعل معهم .

ويُعرف التفاعل بأنه سلوك موجه نحو تحقيق غايات وأهداف محددة ينتج عنها إشباع الدافع إلى السلوك ، ويعرف بأنه تفاعل بين القائد وجميع المتغيرات المحيطة بالموقف الكلى وهى تلك العملية التي يمكن من خلالها تحقيق الترابط بين الأفراد والجماعات والمؤسسات بالمجتمع سواء كان ذلك في الوسائل أو الغايات ويترتب على ذلك تعديل السلوك (عبد الفتاح السيد ، ٢٠٠٩ ، ص ٣٣) .

وتدور فكرة التفاعلية الرمزية حول مفهومين أساسيين هما الرموز والمعاني ، في ضوء صورة معينة للمجتمع المتفاعل وتشير التفاعلية الرمزية إلى معنى الرموز على اعتبار أنها القدرة التي تمتلكها الكائنات الإنسانية للتعبير عن الأفكار باستخدام الرموز في تعاملاتهم مع بعضهم البعض (جلبى ، ٢٠٠٨ ، ص ٧) .

واستخدام الرموز أمر قائم في كل من التجمعات الحشرية مثل تجمعات النمل والنحل والتجمعات البشرية إلا أن التعامل بالرموز في التجمعات الحشرية يقوم على أساس التفاعل الغريزى ، وذلك على عكس التجمعات البشرية التي تستخدم الرموز للتعبير عن شيء له دلالة اجتماعية ، وتهتم التفاعلية الرمزية بالطريقة التي يختار بها المشاركون في عملية التفاعل الاجتماعى لمعانى الرموز ويفقون على هذه المعانى (شتا ، ١٩٩٧ ، ص ٧٨) .

أما المصطلحات الأساسية للنظرية فهى : (جوناثان ، ١٩٩٩ ، ص ١٨)

- التفاعل : وهو سلسلة متبادلة ومستمرة من الاتصالات بين فرد وآخر أو فرد وجماعة أو جماعة مع جماعة أخرى والتفاعل يكون تفاعل اجتماعى بين الأجناس البشرية وغير البشرية .
- المرونة : ويُقصد بها استطاعة الإنسان أن يتصرف في مجموعة ظروف بطريقة واحدة في وقت واحد وبطريقة مختلفة في وقت آخر .
- الرموز : وهى مجموعة من الإشارات المصطنعة يستخدمها الناس فيما بينهم لتسهيل عملية التواصل وهى سمة خاصة في الإنسان وتشمل اللغة والمعاني والصور الذهنية.
- الوعي الذاتي : وهى مقدرة الإنسان على تمثيل الدور ، فالتوقعات التي تكون لدى الآخرين عن سلوكنا في ظروف معينة هي بمثابة نصوص يجب أن نعيها .

وفى ضوء ذلك يمكن الاستفادة من مستويات التفاعل على النحو التالي:

- من خلال أسلوب المناقشة والحوار البناء بين الأخصائي الاجتماعي ، والشباب الجامعب لتوعيته بالجرائم الإلكترونية وتبادل المعلومات والمعارف وكل ما يخص تلك الجرائم .
- من خلال عرض مادة إعلامية ونماذج من تلك الجرائم وانعكاساتها على الفرد والجماعة والمجتمع .
- التفاعل من خلال التوجيه والنصح والإرشاد بخلق نوع من الحوار والمشاركة الإيجابية بين الأخصائي الاجتماعي للعمل مع الشباب الجامعي لمواجهة الجرائم الإلكترونية .
- زيادة التفاعل من خلال مهارات الاتصال مثل الندوات ، المؤتمرات ، اللقاءات عن تأثير تلك الجرائم على المجتمع .

سادسًا : الإطار المنهجي للبحث :

أ- نوع للبحث :

يندرج هذا ضمن البحوث المكتبية الاستشرافية والتي تعتمد على الفهم المبني من خلال الكتابات والدراسات والبحوث ذات الصلة بموضوع البحث ، ومن أجل تقديم تفسير شامل لمشكلة الجرائم الإلكترونية وذلك من خلال جمع المعلومات والبيانات والإحصاءات ذات الصلة بالجرائم الإلكترونية ومعرفة الاتجاهات النظرية والمنهجية الحديثة في طريقة العمل مع الجماعات لتوعية الشباب الجامعي بأهم تلك المخاطر.

ب- المنهج المستخدم :

اعتمد البحث على الأسلوب العلمي وذلك باستخدام عدة مناهج تتواكب مع طبيعة البحث وأهدافه والتي تمثلت فيما يلى :

- المنهج الوصفي التحليلي:

لرصد ظاهرة الجرائم الإلكترونية ووصفها وصفًا دقيقًا وذلك من خلال التأصيل النظري لهذا البحث مما يُساعد على زيادة وعى الشباب الجامعي بأهم مخاطر الجرائم الالكترونية وذلك من خلال استطلاع الأدبيات والدراسات والبحوث المرتبطة بها .

- المنهج الاستنباطي :

والذى يعتمد على التفكير المنطقي الاستنتاجي من أجل التوصل إلى استنتاجات منطقية متعلقة بالاتجاهات النظرية والمنهجية الحديثة لطريقة العمل مع الجماعات لوعى الشباب الجامعى بالجرائم الإلكترونية .

- المنهج الاستقرائي :

عن طريق عرض الكتابات النظرية والدراسات السابقة المرتبطة بالجرائم الإلكترونية ووعى الشباب الجامعي وذلك من خلال العرض والتحليل والاستنتاج المنطقي لنتائج الدراسات والتجارب العالمية والإقليمية والمحلية ذات الصلة في الطرح العلمى لتلك القضية .

ج- أدوات البحث :

اعتمد البحث على دليل تحليل المضمون للدراسات والبحوث المرتبطة بالحروب الإلكترونية .

- الاتجاهات المنهجية الحديثة والتجارب .
- وسائل وأساليب وأدوات العمل مع الجماعة لتوعية الشباب الجامعي بالحروب الإلكترونية .

سابعاً : نتائج البحث :

المبحث الأول :إسهامات طريقة العمل مع الجماعات في تنمية وعى الشباب الجامعي بمخاطر الجرائم الإلكترونية

أولاً : نشأة الجرائم الإلكترونية وعوامل تطورها

ترتبط نشأة الجرائم الإلكترونية بظهور الإنترنت والأجهزة الذكية مثل الكمبيوتر والهواتف الجوالة ويمكن القول أن فكرة شبكة الإنترنت ظهرت في الستينات خلال الحروب الباردة بين الولايات المتحدة الأمريكية والاتحاد السوفيتى على يد البروفسير (Lendard Klernk). فقد ظهر الإنترنت عام ١٩٦٠ وكانت البداية مقصورة على الجامعات ومراكز البحوث ، وشكلت وزارة الدفاع الأمريكية فريقا من العلماء للقيام بمشروع بحثى عن تشبيك الحاسبات ، وركزت التجارب على تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة ومن ثم نقل هذه الأجزاء بأشكال وطرق مستقلة حتى تصل مجمعة إلى هدفها ، و هذا الأمر يمثل أهمية قصوى لأمريكا وقت الحرب ففي حالة نجاح العدو في

تدمير بعض خطوط الاتصال في منطقة معينة فإن الأجزاء الصغيرة يمكن أن تواصل سيرها (نظمي ، ٢٠١٩ ، ص ١٧٥) .

وكان أغلب العاملين من جيل الشباب المتحمس ولمعرفة المزيد من هذه التقنية الجديدة قام بعض من هذه الفئة من الشباب بارتكاب ما نسميه في الوقت الحاضر بالجرائم الإلكترونية عندما قاموا بالتصنت على المكالمات الهاتفية ، ولم يكتفوا بذلك بل قاموا بإجراء مكالمات على حساب شركات أخرى وزوروا بعض الفواتير فكانت تلك بداية الجرائم الإلكترونية ، وفيما بين الأعوام ١٩٤٦ – ١٩٦٩ عندما ظهر الحاسب الآلى حاول العديد من موظفي شركات الحاسب الآلى ارتكاب جرائم إلكترونية إلا أنهم واجهوا صعوبات كثيرة منها الحراسات القوية التي كانت تفرض على هذه الأجهزة بالإضافة إلى كبر حجم الأجهزة ، وكان المخرب الإلكترونى (Hacker) في ذلك الوقت هو من مبرمجى شركات الحاسب الآلي أما العصر الذهبى للمجرمين الإلكترونيين فقد بدأ منذ التسعينات حيث شهدت هذه الفترة تناميًا هائلًا في حقل الجرائم الإلكترونية ، وتغييرا في نطاقها ومفهومها وكان ذلك بفضل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة إنكار الخدمة التي تقوم على فكرة تعطيل نظام تقنى ومنعه من القيام بعمله المعتاد وأكثر ما مورست ضد مواقع الإنترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة لساعات في خسائر مالية بالملايين (الشهرى ، ٢٠١٥ ، ص ٧) .

ثانياً : عوامل تطور الجرائم الإلكترونية:

هناك عوامل متعددة لظهور الجرائم المستحدثة ولارتكاب الجرائم التقليدية بغير طرقها المعتادة منها:

للتكنولوجيا دور كبير في تقدم البشرية وفى تطورها وازدهارها وهذا هو الوجه المشرق للتكنولوجيا والتي من شأنها تسهيل الحياة وأساليبها ولكن كما هو معروف كلما تقدمت الإنسانية بالتوازي زاد الإجرام وسبله ، فالوجه المُظلم للتكنولوجيا أدى إلى ظهور أنماط من الجرائم غير المعهودة والمألوفة من قبل خاصة مع ظاهرة العولمة (الجيد ، عباس محمد ، ٢٠١٧ ، ص ١٩١) .

ظهور العولمة ظهرت معها مجموعة من الظواهر الإجرامية المستحدثة المستجدة والتي ارتبط الكثير منها بالمنظمات الإجرامية الدولية ، وقد أسهمت العولمة في تسهيل وتسخير خيارات متنوعة وتوفيرها أمام تلك المنظمات الإجرامية مما جعل نشاطها يتميز بالطابع الدولى العابر للقارات (سليمان بدون سنة طبع ، ص ١١٥) .

تطور التقنيات و وسائل الاتصالات قد ساهم في انتشار الجريمة و بروز جرائم إجتماعية واقتصادية مستحدثة، مثل التصنت والاحتيال، واعتراض بطاقات الائتمان وسرقتها واستخدامها الغير مشروع بالإضافة استخدام برمجيات التشفير لحماية النشاطات الإجرامية.

ومما سبق يتضح أنه على الرغم من الإيجابيات للتقنيات الحديثة والتقدم العلمي، فقد ساهمت بدور فعال في انتشار الجرائم الإلكترونية، فقد استفاد مرتكبوها من المستحدثات والمتغيرات في استخدام الوسائل والتقنيات الحديثة، فكان لا بد من زيادة الوعي. تلك الجرائم لدى جميع فئات المجتمع بجميع أطيافه، ومنها الشباب الجامعي.

ثالثاً: أنواع الجرائم الإلكترونية وخصائصها :

في ظل التطورات الهائلة لشبكة الإنترنت، ونظرا للعدد. الهائل من الأفراد والمؤسسات الذين يرتادون هذه الشبكة، أصبح من السهل ارتكاب الكثير من الجرائم. وقد قسمت هذه الجرائم الإلكترونية إلى ما يلي:

تقسم الجرائم الإلكترونية إلى أربعة أنواع:(الإبراهيمى ، ٢٠١٣ ، ص ٦٧)

١) جرائم الحاسب: ويُقصد بها الأفعال التي تُشكل اعتداء على أجهزة الحاسب سواء على مكوناته المادية (Hardwear (أو على مكوناته المعنوية (Softwear) كالبيانات والمعلومات المخزنة داخل الحاسب الآلي.

٢) جرائم الإنترنت : وهي كل فعل مشروع يقع على المواقع حفظ تعطيلها أو تعديلها، ونقل الفيروسات، وإرسال الرسائل بكافة أنواعها.

٣) جرائم شبكة المعلومات : وهي كل فعل غير مشروع يقع على وثيقة وجود بالشبكة، ومن أمثلة انتهاك الملكية الفكرية.

٤) الجرائم المتعلقة باستخدام الحاسوب : وهي الجرائم التي يكون الحاسب الآلي وسيلة لارتكابها كالاحتيال والتزوير .

ويستهدف من تلك الجرائم الإلكترونية : (مركز هردو ، ٢٠١٨ ، ص ٩).

- صناعة ونشر الفيروسات وهى أكثر جرائم الإنترنت انتشارا .
- الاختراقات : تتمثل في الدخول غير المصرح به إلى أجهزة وشبكات الحاسب الآلى .
- تعطيل الأجهزة حيث يقوم مرتكبوها بتعطيل أجهزة الحاسب عن تأدية عملها وبدون أن تتم عملية اختراق فعلية لتلك الأجهزة .

- انتحال الشخصية : تتمثل هذه الجريمة في انتحال شخصية أخرى بطريقة شرعية على الإنترنت بهدف الاستفادة من تلك الشخصية أو لإخفاء هوية المجرم لتسهيل ارتكابه لجرائمه .
- المضايقة والملاحقة : وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل تحديث يطال برامج الدردشة والحوارات برسائل تهديد ومضايقة .
- التشهير وتشويه السمعة : يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة عن ضحيته وتعريضه للمضايقات الشخصية أو الإحراج العام .
- النصب والاحتيال : وتتم هذه الجريمة عن طريق عرض سلع أو خدمات تجارية من خلال البريد الإلكترونى أو عرضها على مواقع الشبكة أو ساحة الحوار .

لذلك يجب أن يكون الشباب الجامعى على علم ودراية بكل أنواع تلك الجرائم الإلكترونية وصورها المختلفة حتى لا يقعوا في براثن تلك الجريمة ، فمع تطور وسائل الاتصال بجميع أشكالها وصورها يسهل نقل المعلومة وبالتالي من السهل استقطابهم إلى تلك الجرائم .

رابعاً : خصائص الجرائم الإلكترونية :

للجرائم الإلكترونية خصائص متعددة تجعلها تختلف عن الجرائم العادية وهى :

- جريمة عابرة للحدود وذات بُعد دولي : أي أنها جرائم لا تعترف بالحدود الجغرافية للدول وحتى بين القارات وذلك بسبب الربط الإلكترونى بين جميع الدول والقارات (شاكر ، ٢٠١٤ ، ص ١٣٤) .

وهذا ما يميز الجريمة الإلكترونية عن الجرائم التقليدية فإضافة إلى تضاعف معدل ارتكابها والزيادة في مقدار الخسائر الناجمة عنها تخطيها للحدود الجغرافية واكتسابها بذلك طبيعة دولية ، فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة .

صعوبة اكتشاف أو إثبات أو متابعة الجريمة الإلكترونية : إذ عادة ما يتلاعب المجرم المعلوماتى بمعطيات الحاسوب (برامج – معلومات – بيانات) وذلك من خلال محوها أو تدميرها أو تعطيلها ولا يكلفه ذلك سوى ذرع فيروسات أو استخدام القنابل المنطقية لمعرفة وظيفة الحاسوب وشبكاته ويرى ذلك إلى طابعها التقنى الذى يتميز عادة بالكثير من التعقيد والتفسير ، كما أن الجريمة الإلكترونية تعتريها الكثير من المشاكل القضائية ويصعب تحديد الدولة صاحبة الاختصاص القضائى كما يصعب أيضا تحديد الجهة القضائية (حجازى ، ٢٠٠٢ ، ص ٢٩) .

فهذه الجرائم لا تحتاج إلى جهد عضلى بل تعتمد على التفكير العلمى المدروس القائم على معرفة الوسائل الإلكترونية ، فمرتكب الجريمة شخص من بين ملايين المستخدمين فيصعب معرفته ، صعوبة تحديد حجم الضرر الواقع قياسا بالجرائم العادية ، سهولة إتلاف الأدلة من قبل الفاعل وهو شخص يتميز بالذكاء وذو مهارة تقنية عالية ودراية في مجال أنظمة الحاسب الآلى (النويران ، ٢٠١٥ ، ص ١٧٦) .

خامساً : العوامل المؤدية لارتكاب الجرائم الإلكترونية

لدى مرتكب الجرائم الإلكترونية أسباب متعددة للقيام بها وتتمثل هذه الأسباب فيما يلى : (خير الدين ، ٢٠٠٠ ، ص ٣٦).

- الولع في جمع المعلومات وتعلمها ، حب المغامرة ، الإثارة ، الدوافع الشخصية ، غالبا ما يرتكب المبرمج جرائم الكمبيوتر نتيجة تأثير الرغبة القوية في تحقيق الذات ، تحقيق المكاسب المالية ، دوافع سياسية .

في حين أشار (المايل ، الشربحى ، ٢٠١٩ ، ص ٢٤٩). إلى أن العوامل التي يمكن حصرها كأسباب لارتكاب الجريمة الإلكترونية فيها ما يقع على المستوى الفردى ومنها ما يقع على المستوى المجتمعى ومنها ما يرجع على المستوى الكونى ، وهى تختلف طبقا لنوع المستهدف والجانى ، فجرائم الشباب والهواة والصغار تختلف عن أسباب المحترفين وتختلف وفق هدفها سرقة معلومات أو تجارة بالمعلومات أو شخصية .... الخ .

جدول رقم (١) يوضح عوامل ارتكاب الجريمة الإلكترونية :

أسباب ارتكاب الجريمة الإلكترونية على المستوى الفردي	أسباب ارتكاب الجريمة الإلكترونية على المستوى المجتمعي	أسباب ارتكاب الجريمة الإلكترونية على المستوى الكوني
البحث عن التقدير : هي جرائم يرتكبها شباب طائش وصغار السن وذلك من باب التحدى وحب الظهور في الإعلام.	التحضر : يعد التحضر أحد أسباب ارتكاب الجريمة الإلكترونية عامة حيث الهجرة الكبيرة من الريف إلى المدن إلى المناطق الحضرية والمدن الكبيرة .	التحول المجتمعي الرقمي : ففي القضاء الافتراضى تكونت التفاعلات الافتراضية وحلت محل التفاعل وتكونت السلوكيات الافتراضية والشخصية.
الفرصة : لقد وفرت التقنيات الحديثة والإنترنت فرصا غير مسبوقة لانتشار الجريمة الإلكترونية .	البطالة : ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة.	العولمة : إن ظهور الفضاء الإلكترونى يكون ظواهر جديدة متميزة التي وفرتها أجهزة الكمبيوتر .

أسباب ارتكاب الجريمة الإلكترونية على المستوى الفردي	أسباب ارتكاب الجريمة الإلكترونية على المستوى المجتمعي	أسباب ارتكاب الجريمة الإلكترونية على المستوى الكوني
ضبط الذات المنخفض : إن توفر صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك يعدان عاملين في ارتكاب السلوك الإجرامي .	الضغوط العامة : تعد الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع وخاصة الشباب .	الترابط الكونى : هناك عامل يمكن أن يساهم في دفع مستويات الجريمة هو ظهور الترابط العالمى في سياق تحولات العالم الاقتصادية والاجتماعية .
الضغوط العامة : تلعب العوامل الاجتماعية والاقتصادية دورا في زيادة الجريمة الإلكترونية .	البحث عن الثراء ، حيث المستهدف جمع أكبر وسهولة التنفيذ وقلة الخطورة .	انكشاف البنية التحتية المعلوماتية الكونية حيث تتفاوت بدرجة انكشافها إلى الكوارث الطبيعية والإهمال البشرى وسوء التصرف من الصعب ربط التهديدات الإلكترونية بمكان أو زمان أو جماعة ، فقد تصدر من هاو أو محترف .
النشاط الروتينى : إن تغيرات أنشطة الناس الروتينية من استخدام إنترنت وشبكات التفاعل الاجتماعى مثل الفيس بوك ، الإيميل وغيرها كونت فرصا للجناة مع وجود أهداف قيمة وسهلت في غياب الحراسة .	ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية ، هناك الكير من الدول التي لم تطور تشريعاتها وأجهزة العدالة لكى تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها .	

سادساً : الانعكاسات الاجتماعية للجرائم الإلكترونية :

الجرائم الإلكترونية تُؤثر على حياة المدنيين ورفاهيتهم وحتى ثقافتهم وتستهدف عبر وسائلها للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها وهذا من خلال : (كزيز ، قط ، ٢٠١٨م ، ص ١٢٩).

- الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق مشروعة كحسابات البريد الإلكتونى وكلمات السر التي تخصهم ، وقد تصل إلى انتحال شخصياتهم وأخذ الملفات والصور المهمة من أجهزتهم بهدف تهديدهم بها ليمتثلوا لأوامرهم .
- تخريب منظومة العلاقات الاجتماعية وتخريب النسيج الأخلاقى من خلال المساس بالعلاقات الأسرية وذلك بسبب الكثير من النتائج التي تسببها بعض أنواع الجرائم الإلكترونية كالتشهير ببعض الأفراد ونشر الأخبار الكاذبة والإشاعات .
- ظهور حالات الاختطاف والاغتيالات حتى دفع المبالغ المالية إضافة إلى ظاهرة إدمان الشباب على الألعاب الإلكترونية خصوصا فئة المراهقين .

فمجتمع التكنولوجيا والإنترنت يوجد فيه أطياف مختلفة من الناس أكثرهم الأسوياء ولكن يوجد منهم ذوى الأخلاق السيئة ، فالشباب يكون متشوقا لاكتشاف العوامل الاجتماعية التي يدخلها

وهو ما قد يجعلها عرضة للجرائم ومن ثم فإن الآثار السلبية للتكنولوجيا تتضح فيما يلى : (العمرى ، ٢٠٠٤ ، ص ٢٤٩).

- تسرب الأفكار الهدامة والملل والأديان والباطلة ووصولها إلى متناول الأبناء وضعاف الإيمان .
- الاستدراج إلى أفكار سلبية ونشر ما لا يتناسب مع طبيعة وثقافة البلاد العربية وحضارتها .
- فشل الرقابة في حجب المواد غير المرغوب فيها .
- دخول بعض الأفراد إلى خصوصيات بعض الجهات الحكومية والوصول إلى معلومات سرية قد لا يسمح بالوصول إليها بالطرق الشرعية .
- إبرام بعض العمليات غير المصرح بها إلا من خلال القنوات الشرعية في المجتمع .

سابعاً : الانعكاسات الاقتصادية للجرائم الإلكترونية :

الجرائم المعلوماتية مهما اختلف نوعها ومهما تزايد حجمها تمس النظام الاقتصادى وهى تختلف باختلاف نوع الأنظمة المعلوماتية ، ولهذا تتنوع وتختلف الخسائر الاقتصادية الناجمة عن الجرائم المعلوماتية ، وقد تكون هذه الخسائر مباشرة ، أي يكون ضررها اقتصادى مباشر يرتبط بقيمة التجهيزات والبرمجيات موضوع الجريمة ، وقد يرتبط بالأثر الاقتصادى الناجم عن توقف هذه المنظومات عن العمل مثلا ، وقد تنجم عن خسائر تقدر بعشرات الدولارات أو سرقة الأموال واستخدام الشبكة للاستيلاء على أموال الغير (قويقج ، حورية ، ٢٠٢٠ ، ص ٢٤٣).

ومن ثم فإن الجرائم الإلكترونية لها انعكاسات اقتصادية على مستوى الأفراد تكمن سرقة بطاقات الائتمان ، الابتزاز ، والتهديد وعمليات احتيال وتحويل أو نقل حساب مصرفى أو على مستوى الشركات ، وتكمن في الغش في المعاملات ، وسرقة الأموال ومن هنا لابد من التنبيه على توعية وخاصة للشباب الجامعى لمواجهة مخاطر تلك الجريمة ويكونوا على دراية لمواجهتها.

ثامناً : أساليب الوقاية من الجرائم الإلكترونية للشباب الجامعى

لاشك أن للجرائم الإلكترونية أخطار متعددة بدأت تكبر يومًا بعد يوم بسبب زيادة الاعتماد على العالم الإلكتروني في شتى المجالات ، وقد سارعت الدول المختلفة لوضع ضوابط حماية محددة لمنع الجريمة قبل وقوعها ، وهناك وسائل متعددة للحد من الجرائم الإلكترونية تتمثل فيما يلى : (خير الله ، ٢٠١٢ ، ص ١٣٧).

١- تفعيل دور المكافحة الوقائية التي تسبق وقوع الجريمة الإلكترونية وذلك بالتوعية بخطورة الجرائم الإلكترونية على الأسرة والمجتمع .

٢- إنشاء أقسام في الجامعات تعني بالأمن المعلوماتي والتدريب فيه ومواكبة كل ما هو جديد في هذا المجال .

٣- تنسيق القوانين عالميًا بهدف تسهيل التعاون في مجال الحماية .

٤- سن القوانين والأنظمة الخاصة التي تكافح الجرائم الإلكترونية .

٥- التنسيق وتوحيد الجهود بين الجهات المختلفة في الدولة سواء كانت السلطة التشريعية أو التنفيذية .

٦- عقد الاتفاقيات بين الدول بخصوص الجرائم الإلكترونية والحد منها .

٧- تفعيل اتفاقيات تسليم المجرمين الإلكترونيين .

٨- عقد الدورات وورش العمل المتخصصة للقيام بالجانب التوعوى في هذا المجال .

كما يُشير كل من (المايل ، الشربجى ، ٢٠١٩ ، ص ٢٥١). إلى أنه توجد سبل متنوعة لمكافحة الجريمة الإلكترونية حيث تتباين هذه السبل بدرجة فاعليتها وتعقيدها ، وذلك بحسب البرامج المصممة لهذا الغرض ، ومن بين هذه السبل :

- عمل نسخ من ملفات البيانات ، استخدام البرامج المضادة للفيروسات .
- برامج جدار النار : نظام أو برنامج حماية تحجز البيانات بين الشبكة الداخلية والخارجية أي الجهاز الذى يتحكم في تدفق المعلومات بين جهاز الحاسوب والإنترنت ولكن لا يستطيع من في الخارج الدخول إلى الجهاز من خلاله .
- استخدام الخصائص الفسيولوجية لحماية النظام مثل بصمة الإبهام ، حدقة العين ، الصوت وغيرها والتشفير .

كل هذه الوسائل يمكن من خلالها تنمية وعى الشباب الجامعى في مواجهة مخاطر الجريمة الإلكترونية ، وقد يكون ذلك من خلال الوسائل المختلفة لخدمة الجماعة وعمل الأخصائى الاجتماعى بجهاز رعاية الشباب الجامعى من خلال الندوات وورش العمل وغيرها من الوسائل المختلفة ، مثال أساليب المناقشة الجماعية مع المختصين في هذا المجال .

تاسعاً : المدخل المعرفى لتوعية الشباب الجامعي بمخاطر الحروب الإلكترونية :

يرى أصحاب هذا المدخل أن الأفراد يمكنهم التعلم بشكل جيد من المعارف والمعلومات التي يكتسبونها والتي تسهم في تغيير أفكارهم وتنمية خبراتهم وتعديل سلوكهم واتجاهاتهم نحو المواقف والأحداث التي يمرون بها وعليه فإن هذا المدخل يرتبط ارتباطا وثيقا بمفهوم الوعى والاستبصار لدى النسق المستهدف ، حيث أنه كلما زاد إدراك ووعى النسق المستهدف بالمتغيرات والأحداث

الاجتماعية والاقتصادية والسياسية والثقافية ، كلما زاد قدرته على التعامل مع الأحداث والمواقف التي يمر بها والعكس . (المصيلحى ، ٢٠١٨ ، ص ٢٠ ، ٢١) .

ويمكن الاستفادة من هذا المدخل من خلال ما يلى :

- التحليل المعرفي لأفكار الشباب الجامعى وقيمهم واتجاهاتهم نحو المواقع ذات الأفكار الهدامة المتطرفة على الشبكة المعلوماتية العالمية .
- زيادة المعارف والمعلومات عن الجريمة الإلكترونية ودوافعه ومظاهره وأساليبه في شتى الميادين المختلفة .
- تصحيح الأفكار الخاطئة والمغلوطة لدى الشباب المرتبطة ببعض المواقع .

عاشراً : أدوار الأخصائي الاجتماعي للعمل مع الجماعات في توعية الشباب الجامعي بمخاطر الجريمة الإلكترونية :

أ- دوره كممارس عام (Jorolmen . ٢٥ , ٢٠١٣ , P) :

حيث يهتم الأخصائي الاجتماعي كممارس عام بشكلٍ مستمر للعملاء ، وفى هذا الدور يسعى إلى مساعدة نسق العملاء على اكتشاف مصادر القوة بداخلهم واستخدامها لتحقيق أهدافهم ومساعدتهم على تحديد أهدافهم والعمل على تحقيقها ويقوم بما يلى :

- مساعدتهم على التخلص من المشاعر السلبية ودعم المشاعر الإيجابية .
- مساعدة العملاء على تفهم أنفسهم واكتشاف قدراتهم وإمكانياتهم ، ومساعدتهم على استغلالها لصالحهم تحقيقا لأهدافهم وزيادة ثقتهم بأنفسهم .
- تزويد العملاء بالمهارات المهنية المتنوعة وفقا لقدراتهم وميولهم .
- مساعدة المؤسسة على القيام بوظائفها الاجتماعية وذلك باستغلال إمكانياتها المادية والبشرية لخدمة المجتمع .

ب- دوره كمغير للسلوك :

وفى هذا الدور يعمل على تغيير أنماط سلوك وعادات العملاء والجماعات والمجتمعات (Waller , R , ٢٠٠٨) .

ج- دوره كمعالج :

يقوم بالتأثير في نسق العملاء لمساعدتهم في علاج مشكلاتهم سواء كانوا أفرادًا أو جماعات وعلاج البيئة الاجتماعية كالتأثير في الأسرة أو فريق العمل المؤسسي أو التأثير في المجتمع العام وذلك من خلال :

- مساعدة العملاء على مواجهة مشكلاتهم التي تواجههم في أسرهم وفى المجتمعات مثل المشكلات الاقتصادية والاجتماعية والسلوكية .
- تعديل السلوكيات السلبية لديهم والتي تعوق تعبيرهم الاجتماعى والدراسى الإيجابي .
- تعديل الأفكار والاتجاهات الخاطئة لدى العملاء .

د- دوره كمقوم :

ولا يقتصر القيام بهذا الدور على أخصائى معين ولكن من الضرورى وبالنسبة لجميع الأخصائيين أن يقوموا بتقويم أعمالهم وأعمال الآخرين .

هـ - دوره كمخطط :

حيث يقوم الأخصائى الاجتماعى بوضع مجموعة من الخطط والتي تعمل على تحسين جودة الخدمات والعمل على استفادة أكبر قدر ممكن من العملاء من تلك الخدمات .

ويمكن توظيف أدوار أخصائى العمل مع الجماعات في مواجهة خاطر الجريمة الإلكترونية للشباب الجامعى على النحو التالى :

- دوره كمعالج ليساعد الشباب الجامعي على التخلص من الوقوع في براثن الجريمة الإلكترونية .
- دوره كمستشار حتى يستشيره الشباب في كل ما يُحيط بهم من مخاطر الجريمة الإلكترونية والوقاية منها بشتى السبل .
- كمغير للسلوك من خلال تغيير أنماط سلوك وعادات الشباب الجامعى من الاستخدام السيئ للإنترنت .
- دوره كخبير وموجه للشباب الجامعي للاستخدام الأمثل للمواقع والشبكات .
- دوره كتربوى ومُرشد لتنمية المعارف السليمة للشباب الجامعي لمواجهة تلك الجرائم .
- العلاج بالنمذجة من خلال المشاركة عن طريق مساعدة الشباب لكى يرى نموذج فعلى ليقوم بالاستجابة .
- المناقشة الجماعية مع الجماعات الصغيرة والآثار السلبية لوسائل التواصل وأيضا لعب الدور لتنمية الخبرات حول الآثار السلبية لوسائل التواصل الاجتماعى .

أحدى عشر : أشكال الحماية من الجرائم الإلكترونية للشباب الجامعي :

مبدأ الوقاية والحماية من المبادئ الهامة التي حرصت عليها الشعوب والحضارات على تلقينه لأبنائها وتتعدد صورها منها :

١ - الحماية التقنية : (قواري ، مرحلي ، ٢٠١٧ ، ص ٥٥ ، ٥٦)

وهى متعددة الأشكال منها :

عدم استخدام برامج مجهولة الأصل ، عدم استخدام أسطوانات تتضمن برامج متغيرة وقابلة للتغيير الأمر الذى يُشكك في أنها حاملة للعدوى ، مراقبة استخدام الحاسب للذاكرة للتأكد من عدم وجود فيروسات ، مع ضرورة إجراء دراسات متخصصة في مجال الحاسب يكون هدفها الأساسى هو فيروس الحاسب ودعوة وتشجيع المتخصصين عليها وهذا الإعداد مطلب قرآنى أكيد تبينه آية الأنفال الداعية لإعداد القوة وأخذ الأهبة والحيطة في زمن لا مكان فيه للشعوب الضعيفة والمتخلفة . قال تعالى : (وأعدوا لهم ما استطعتم من قوة ومن رباط الخيل ترهبون به عدو الله وعدوكم وآخرين من دونهم لا تعلمونهم الله يعلمهم وما تنفقوا من شيء في سبيل الله يوف إليكم وأنتم لا تظلمون) (سورة الأنفال : آية ٢٦) فقد جاء لفظ قوة منكرا ليشمل كل ما يتقوى به في الحرب كائنا ما كان .

٢ – الحماية القانونية : (مجذوب ، ٢٠١٤ ، ص ٢٠٠).

وفى هذا الإطار لابد من تفعيل الحماية القانونية الصارمة لحماية حق الخصوصية للمواطنين والتي تعرف بأنها حق الفرد في حياة منعزلة ومجهولة ، فالشخص من حقه أن يعيش بعيدا عن أنظار الناس ، ومن هذا المنطلق وكما ذهبت كل التطورات الحاصلة على حقوق الإنسان يحظر على السلطات العامة داخل الدولة حفاظا على حرمة الحياة الخاصة الشخصية تسجيل معلومات شخصية بقصد حفظها في سجلات لديها .

كما نص الإعلام العالمي لحقوق الإنسان المؤرخ (كانون – ديسمبر ١٩٤٨م). حماية الإنسان من كل أشكال الجريمة الإلكترونية التي يمارسها أي لا يدخل أحد تدخل تعسفى في حياته الخاصة أو أسرته أو مسكنه فلا يجوز انتهاك حرمة حياة المواطن وحرمة شرفه ويحيمها القانون ويعاقب القانون على انتهاك هذا الحكم على أساس يضمنه القانون ويعاقب على انتهاكه (علوان ، ٢٠٠٦ ، ص ٢٩١).

٣ – الحماية الدينية : (قواري ، رحلي ، ٢٠١٧ ، ص ٦٠).

حيث لا يخفى على أحد أن الإسلام قد سبق التشريعات الوضعية في الأخذ بمبدأ الشرعية النصية التي لم تقتصر على المعنى الضيق لها بل توسع فيها كلما اقتضى الحاجة إلى حماية مصالح المجتمع ضد أي خطر إجرامى يتهددها ويتميز الإسلام عن التشريعات الوصفية في عدم خلطه بين انتهاك الحق في السر واستخدام ما تحصل عليه من بيانات في ارتكاب الجريمة . قال رسول الله صلى الله عليه وسلم : (من اطلع في كتاب أخيه دون أمره فإنما اطلع في النار) (رواه البخارى) .

ومن هنا ظهر اتجاه يرى المعاقبة على فعل الانتهاك لحرمة الحياة الخاصة للفرد كجريمة مستقلة بعقوبة تعزيزية يحددها ولى الأمر طالما استوجب شرائطها الشرعية ولا يتم تفعيل هذه الحماية الدينية إلا إذا غرسنا في نفوسنا ونفوس أبنائنا وبناتنا ومجتمعاتنا أننا جميعًا معنيون بحماية كياننا وحقوقنا ووجودنا ، وهذا ما جسده الرسول صلى الله عليه وسلم في الحديث الشريف الصحيح ، فعن النعمان بن بشير رضى الله عنهما عن النبى صلى الله عليه وسلم قال : (مثل القائم في حدود الله والواقع فيها كمثل قوم استهموا على سفينة ، فصار بعضهم أعلاها وبعضهم أسفلها وكان الذين في أسفلها إذا استقوا من الماء مروا على من فوقهم فقالوا لو أنا خرقنا في نصيبنا خرقا ولم نؤذ من فوقنا فإن تركوهم وما أرادوا هلكوا جميعًا وإن أخذوا على أيديهم نجوا ونجوا جميعًا) ويشرح بعض المفسرين هذا الحديث فيقول أن هذا مثل في منتهى الجمال والروعة يضربه الرسول الكريم صلى الله عليه وسلم لأولئك الذين أخطأوا الطريق وضلوا ففهموا الحرية فهما خاطئًا وساروا حسب أهوائهم وشهواتهم ومثل آخر لأولئك الذين رأوا المنكر فسكتوا عنه وأغمضوا عما يدور حولهم من آثار وموبقات كأن الأمر لا يعنيهم وطنوا في أنفسهم الصلاح .

أثنى عشر : وظائف الأخصائي الاجتماعي للعمل مع الجماعات في توعية الشباب الجامعي بمخاطر الحروب الإلكترونية :

يعمل الأخصائي الاجتماعي إلى إكساب الطلاب معارف ومعلومات من خلال البرامج والأنشطة المختلفة منها : (سليم ، ٢٠٢١ ، ص ص ٢٢٤ ، ٢٢٥).

- لا تقبل أو تفتح أية رسائل إلكترونية مجهولة المصدر .
- لا تقم أية إضافة لأشخاص ما لم تكن تعرفهم معرفة شخصية .
- إذا كنت غاضبا فلا تقم بإرسال أية رسائل .
- احذف فورًا أية رسائل مجهولة المصدر أو من أشخاص يبدو عليهم الغضب .
- تعلم كيفية حظر وصول بعض الأشخاص إلى غرف الدردشة والإبلاغ عنهم وكيفية حفظ أو طباعة نسخة من أي حوار ، فقد يحتاج والديك الإبلاغ عنها .
- إعلم بأن أي حوارات عبر الإنترنت ليس ذات خصوصية فقد يقوم آخرون بنسخ هذه الحوارات وطباعتها واطلاع الآخرين عليها .
- توعية أولياء الأمور بخطورة الإنترنت على أبنائهم وضرورة متابعتهم داخل المنزل .
- التواصل المستمر مع أولياء الأمور والأخصائى الاجتماعى .
- غرس القيم الدينية في نفوس الطلاب .

- نشر الوعى المستمر لدى الطلاب بقواعد الاستخدام الآمن للإنترنت .
- تقديم النصح والتوعية للطلاب بعدم إعطاء معلومات شخصية للغرباء عبر وسائل الاتصال التكنولوجية بكافة صورها .
- عقد ندوات ومؤتمرات ومحاضرات حول الاستخدام الآمن للإنترنت .
- عرض قصص ونماذج على الطلاب ببعض المشكلات التي حدثت بالفعل للآخرين نتيجة عدم الالتزام بقواعد الاستخدام الآمن للإنترنت مع توضيح الإيجابيات والسلبيات وطرق معالجتها .
- الاستماع لمشاكل الطلاب المتعلقة بدخولهم على الإنترنت والعمل على مساعدتهم في الوصول لحلول مناسبة .
- إعداد مجلة حائط – إلكترونية أو كتيب ورقى عن الحروب الإلكترونية .
- عقد ندوات يقدمها شخصيات معروفة ذات خبرة في مجال الاستخدام الآمن للإنترنت والحروب الإلكترونية .

المبحث الثاني : التجارب والدراسات التي يمكن تفعيلها من قبل الأنظمة لتحقيق الأمن من الجرائم الإلكترونية

أولا : الجهود المبذولة لمكافحة الجرائم الإلكترونية :

عرف العالم تطورًا علميًا وتقنيًا هائلًا في مجال الاتصالات وتقنية المعلومات أدى إلى تزايد عدد مستخدمى الإنترنت ، وبهذا ظهرت وانتشرت الجرائم الإلكترونية بشكل عام والجريمة الإلكترونية الماسة بالأفراد .

أ – الجهود الدولية في مكافحة الجرائم الإلكترونية :

على الصعيد المؤسسي أولت منظمة الأمم المتحدة لمسألة مواجهة الجرائم الإلكترونية اهتماما كبيرا خصوصا تلك الجرائم الماسة بالمرأة والطفل وذلك من خلال مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين الذى انعقد في فيينا أيام ١٠ – ١٧ أبريل ٢٠٠٠م ، وكذلك خلال مؤتمر الأمم المتحدة الحادى عشر وغيره والذي خُصص لمنع الجريمة والعدالة الجنائية والمنعقد في بانكوك أيام ١٥ – ١٨ أبريل ٢٠٠٥م ، أما على الصعيد التشريعى فقد اهتم المجتمع الدولى بمسألة مكافحة الجريمة المعلوماتية وفى هذا الصدد تشير اتفاقية بودابست التي تم التوقيع عليها بتاريخ ٢٣ نوفمبر ٢٠٠١م بشأن الإجرام الكونى أو المعلوماتى وذلك إيمانا من الدول الأعضاء في المجلس الأوربي والدول الأخرى الموقعة على هذه الاتفاقية بضرورة مواجهة هذا النمط الجديد من الإجرام (المنصورى ، ٢٠٢٠ ، ص ص ٣٦ ، ٣٧) .

كما تعمل الأمم المتحدة منذ فترة طويلة في مجال تأمين سلامة استخدام التكنولوجيا وشبكة المعلومات وتتشارك وكالات الأمم المتحدة المختلفة في مختلف المفاوضات لإيجاد توافق في الآراء بشأن عدة قضايا بما في ذلك وضع معايير توفير الحماية لشبكات الإنترنت ، ومن أبرز المنظمات الدولية التي عملت في موضوع الجرائم الإلكترونية مجموعة الدول الثماني ، مجلس أوربا والاتحاد الدولى للاتصالات . ومن أهم قرارات الجمعية العامة للأمم المتحدة في محاربة الجرائم لإلكترونية :

١- القرارات ٥٣/٧٠ ديسمبر ١٩٩٨ ، ٥٤/ ٤٩ ديسمبر ١٩٩٩ ، ٥٥ /٢٨ نوفمبر ٢٠٠٠ ، ٥٦ / ١٩ نوفمبر (٢٠٠ ، ٥٧ / ٥٣ نوفمبر) ، ٢٠٠ ، ٥٨ / ٣٢ ديسمبر ٢٠٠٣م ، حول موضوع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولى .

٢- القرارات بشأن مكافحة استخدام نظم المعلومات الإدارية الجنائية لتنقية المعلومات ، يدعو هذا القرار الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات على أن تأخذ في الاعتبار عمل لجنة منع الجريمة والعدالة الجنائية .

٣- قرار المجلس الاقتصادي والاجتماعي ٢٦ يونيو ٢٠٠٧م بعنوان التعاون الدولى من أجل منع وتحرى ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادى والجرائم المتصلة بالخدمة ، وتدعو الجمعية العامة في قراراتها المختلفة التي غالبا ما تكون مماثلة لقرارات الاتحاد الدولى للاتصالات الدول الأعضاء عند وضع القوانين والسياسات العامة لمكافحة الجرائم الإلكترونية .

ثانيًا : التعاون الدولى في مجال مكافحة الجرائم الإلكترونية

أمام اتساع نطاق الفضاء الإلكتروني وشموله لجميع مناحي الحياة فقد اتسع نطاق الجريمة الإلكترونية وضخامة الخسائر الناتجة عنها وفى ظل الفراغ التشريعى أصبح من الضرورى إيجاد إطار فعال للتعاون الدولي في مجال مكافحة الجرائم الإلكترونية وذلك من خلال تبادل الخبرات وإيجاد تشريع دولى خاص لمواجهة هذا الخطر إلى جانب تكريس وتشجيع البحث العلمى وتكثيف حجم التبادل في الخبرات وسن القوانين ذات الشمولية الدولية ، وفى هذا المجال الأمني والمساعدة القضائية الدولية (النويران ، ٢٠١٥م ، ص ١٧٨) .

ومن صور التعاون الدولى في هذا المجال :

١) قرار هافانا ١٩٩١ الناتج عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء حيث وضع إطارا دوليا لمكافحة الجرائم الإلكترونية وجاء ذلك القرار بما يلى : (عرب ، ٢٠٠٢ ، ص ٣١٤).

- التأكيد على وضع إطار قانوني دولى ملائم مما يتطلب جهدا جماعيا بين الدول .

- الطلب من الدول الأعضاء القيام بالإجراءات التالية : تحديث القوانين لمواكبة المرحلة خصوصًا في مجال التحقيق وقبول الأدلة والإجراءات القضائية ، تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة الخصوصية وحقوق الإنسان ، زيادة الوعى لدى الجماهير من خلال إبراز أهمية مكافحة الجرائم المتعلقة بالحاسوب ، اعتماد تدابير خاصة لتدريب القضاة والضبطية القضائية لمواكبة متطلبات المرحلة ، زيادة التعاون بين المنظمات ذات العلاقة ووضع قواعد للأخلاق للتعامل معها .

٢) انعقاد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل ١٩٨٤م ، ووضع جملة من الأسس الواجب احترامها ومراعاتها في مكافحة الجرائم منها: (عبد الله ، ٢٠٠٧ ، ص ص ١١٤ ، ١١٥).

- وجوب تحديد السلطات التي تقوم بالتفتيش والضبط في بيئة تكنولوجيا المعلومات .
- السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسوب ذاته مع استخدام الأدلة المحصل عليها أمام المحاكم .
- يجب مراعاة المسائل المرتبطة ببيئة المعلومات وما يمثله ضياع الفرص الاقتصادية وانتهاك الحرمة والحياة الخاصة وكذا كلفة إعادة بناء قاعدة البيانات وهذا قبل كل تفتيش أو تحقيق .
- إعادة النظر في قواعد الإثبات الإلكترونى ومصداقية الأدلة ومراعاة القواعد التشريعية.

٣) اتفاقية بوادبست ٢٠٠١م لمكافحة الجرائم المعلوماتية ، وتتخلص أهداف هذه الاتفاقية (عبد الله ، ٢٠٠٧ ، ص ١٢٤).

- السعي لتوحيد التدابير التشريعية بين الدول للوقاية من هذه الجرائم .
- ضرورة تفعيل خطة العمل على الجانب الموضوعى والإجرائى للحد من هذه الظاهرة .
- التأكيد على أهمية التعاون الإقليمى والدولى للوقاية من هذه الجرائم .
- العمل على تحقيق التوازن بين حقوق الإنسان الأساسية وحرية الرأي وحرية الحصول للمعلومة وحرية البحث وغيرها من الحقوق الأساسية الثابتة في العلاقات الدولية .

٤) اتفاقية مجلس أوربا بشأن الإجرام الإلكترونى لعام ٢٠٠١م (الحوفى ، ٢٠١٢ ، ص ٨) : هي الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر باستخدام شبكة الإنترنت وهى تمثل ركيزة أساسية منذ دخولها حيز النفاذ في الأول منيوليو لعام ٢٠٠٤م على مستوى الدول أعضاء مجلس الاتحاد الأوربي ، وقد وقعت عليها العديد من الدول غير أعضاء مجلس أوربا مثل كندا واليابان وجنوب أفريقيا ، كما صارت عليها

الولايات المتحدة وهى بمثابة دعوة مواجهة إلى دول العالم للتفاعل مع الإنترنت جاءت نتيجة محاولات كثيرة منذ ثمانينات القرن العشرين وقد تلت هذه الاتفاقية الأقسام الآتية :

تحديد المصطلحات ، الخطوات الواجب اتخاذها في إطار التشريع الوطنى ، التعاون الدولى ، الشروط النهائية حول الانضمام إلى الاتفاقية ، كما حدد الجرائم التي يجب أن تتضمنها التشريعات الوطنية للدول الأعضاء وذلك على النحو التالى :

- الجرائم المتعلقة بأمن الشبكات ، الدخول والمراقبة غير المشروعة والعدوان على الثقة في البيانات أو على النظام .
- الجرائم المعلوماتية كما هو الشأن في الاختلاف والانتحال والنص .
- جرائم الأخلاق ، جرائم العدوان على حقوق الملكية الأدبية كاستنساخ المصنفات المشمولة بالحماية المسئولية الجنائية للأشخاص .

ثالثًا : نماذج لتجارب بعض الدول في مكافحة الجرائم الإلكترونية :

تسعى الدول والحكومات بشكل جدى للحد من الجرائم الإلكترونية وآثارها عبر طرق كثيرة منها ، فرض سياسات دولية وعقوبات كبيرة على مرتكبى هذه الجرائم وتفعيل أحدث التقنيات والوسائل للكشف عن هوية مرتكبى الجرائم الإلكترونية ونشر التوعية في المجتمعات حول هذه الجرائم ومخاطرها ، معرفة الأفراد بكيفية الحفاظ على معلوماتهم وخصوصياتهم وتوجيه التشريعات والقوانين وتحديثها بما يتماشى مع التطورات التكنولوجية ومن أهم القوانين والتشريعات الدولية في مكافحة الجرائم الإلكترونية في العديد من الدول .

١ – التجربة الأمريكية :

الولايات المتحدة الأمريكية تعتبر من الدول السباقة إلى إعداد وإصدار قوانين تخص الحروب الإلكترونية ، فمباشرة بعد أحداث ١١ سبتمبر ٢٠٠١ ظهرت أول اتفاقية أمريكية والتي بمقتضاها يتم تعزيز سلطات البحث والتحقيق السريع وتوسيع صلاحيات الرقابة الإلكترونية ومن بين البنود العملية التي ينص عليها القانون الأمريكي تلك التي تنص على الصلاحية المخولة للقاضي والنيابة ومكتب التحقيق الفيدرالي بالتقاط الرسائل الإلكترونية المشتبه فيها بدون إذن القاضي شريطة إثباتهم بأن الأمر يتعلق بقضية الجرائم الإلكترونية ، ومن المقتضيات التي ينص عليها القانون تلك التي تسمح للنائب الفيدرالي أو العام وبدون اشتراط الحصول على إذن القاضي بمراقبة أنشطة المشتبه فيهم على شبكة الإنترنت بواسطة نظام DCs ١٠٠٠ المتطور ، كما يجبر القانون الأمريكي الخاص بالمراقبة الإلكترونية كل المزودين بحق الولوج إلى الإنترنت وشركات استغلال خطوط الهاتف بتقديم جميع

المعلومات المطلوبة عن عملائهم المشتبه فيهم من قبل الشرطة الفيدرالية وذلك في حالة ما إذا كانت التسجيلات المطلوبة لها علاقة بأبحاث وتحقيقات مسموح بها في إطار الوقاية من الجرائم الإلكترونية ، كما وسع القانون الأمريكي الجديد على إنشاء مراكز للخبرة والتكوين المعلوماتى يوضع رهن إشارة السلطات الفيدرالية (باسو ، ٢٠٠٦ ، ص ٢١) .

٢ – التجربة البريطانية : (حميد ، مصطفى ، ٢٠١٩ ، ص ٩٣).

هدفت الاستراتيجية البريطانية للأمن السيبرانى ومكافحة الجرائم السيبرانية ٢٠١١ تحقيق أربعة أهداف استراتيجية :

١– جعل المملكة المتحدة واحدة من أكثر الأماكن أمانا في العالم للقيام بأعمال التجارة على الإنترنت .

٢– زيادة المرونة والفاعلية التقنية لصد هجمات القرصنة والتسلل السيبرانى .

٣– ضمان الاستقرار في نظم الحماية التقنية والأمان أمام المستخدمين .

٤– الاستثمار في علوم التكنولوجيا وأمن المعلومات والمكافحة السيبرانية بما يعزز التفوق المعرفى والقدرة البريطانية في أمن الفضاء السيبرانى .

كذلك خصصت الاستراتيجية البريطانية مبلغ ٦٥٠ مليون جنيه استرلينى لصالح البرنامج الوطنى للأمن السيبرانى والمكافحة الشاملة للجريمة السيبرانية وحددت سلطة الإشراف والتنفيذ الحكومى من أجل تنفيذ ومراجعة الاستراتيجية القومية لصالح المكتب المركزى للأمن السيبرانى والحماية السيبرانية تحت الإشراف المباشر لمكتب رئيس الوزراء .

إن الاستجابة البريطانية للتدابير التشريعية الجديدة في حقل تقنية المعلومات وضعت بأنها متأخرة غير غيرها من الدول الأوربية ومتأخرة عن الاستجابة الأمريكية إلا أن السنوات الأخيرة تشهد تميزا في التجربة البريطانية سواء من حيث المحتوى أو الحلول التشريعية المقررة .

٣ – التجربة الصينية :

اعتمدت الاستراتيجية الصينية العامة على أسلوب الرقابة المركزية في تحقيق أمنها من خلال مشروعها (الدرع الذهبى) حيث تتم رقابة الفضاء السيبرانى في الصين عبر مجموعة من القوانين والتي بلغ عددها حوالى ستين قانون ولائحة وتختص الفروع الأمنية العليا في المقاطعات الصينية على تنفيذ نظم المراقبة بقوة على مزودى خدمات الإنترنت وشركات الأعمال والتكنولوجيا والاتصالات ، وتمكنت التجربة الصينية من خلال مشروع الدرع الذهبى من السيطرة على المحتوى السيبرانى المتداول عبر مراقبة المواقع والمستخدمين واستطاعت حجب شبكات التواصل الاجتماعى

مثل (الفيس بوك ، تويتر ، يوتيوب) واتبعت سياسة نفاذ المستخدمين المحدود على الإنترنت (منصور ، ٢٠١٧ ، ص ١٧٨) .

ومن خلال عرض هذه التجارب العالمية نلاحظ أن كل تجربة تحاول المحافظة على أمن وسلامة معلوماتها بشتى الطرق .

رابعًا : التعاون على المستوى الإقليمي لمواجهة الجرائم الإلكترونية

أما على المستوى الإقليمي العربي فنجد القانون العربي النموذجي لمكافحة جرائم قضية أنظمة المعلومات والذى صادق عليه مجلس وزراء العدل العرب في ٨ / ١٠ / ٢٠٠٣م في دورته التاسع عشر (www.Arabic,mjusticdz) وقد جاء هذا القانون بجملة من الأحكام الموضوعية والإجرائية تعمل على الحد من الجريمة المعلوماتية واعتمد القانون في مجال الاختصاص على مبدأ العينة وفقا للمادة ٢٦ والتي تنص على أنه (تسرى أحكام هذا القانون على أيا من الجرائم المنصوص عليها فيه ولو ارتكب كليا أو جزئيا خارج إقليم الدولة متى أخذت بإحدى مصالحها ويختص القضاء الوطنى بنظر الدعاوى المترتبة عليه) .

أ- الجهود المصرية لمواجهة الحروب الإلكترونية :

وفى مصر نجد أن مكافحة جرائم الكمبيوتر تمت معالجتها بقوانين عامة كالقانونيين المدنى والجنائى ، ففي المادة التاسعة من القانون ٢٦٠ لسنة ١٩٨٠م نجد في شأن الأحوال المدنية المعدل بالقوانين رقمى ١١ لسنة ١٩٦٥ و ١٥٨ لسنة ١٩٨٠ على أن البيانات التي تحويها سجلات الأحوال المدنية تعتبر سرية وقد جاء بالمذكرة الإيضاحية للقانون أنه لما كانت هذه السجلات تحوى أدق البيانات عن حالة الشخص ، فقد أسبغت عليها السرية حتى يطمئن كل شخص على ما يقدمه من بيانات ، إن نطاق السرية يمتد إلى كل من لا يفرض عليه واجبه طبقا لقانون الأحوال ولائحته التنفيذية والقرارات المنفذة له بالاطلاع على هذه البيانات ، وذلك لم تصدر سلطة قضائية أو سلطة تحقيق قرارا بالاطلاع عليها أو فحصها لأن الصالح العام يفضل صالح الشخص في المحافظة على سرية بياناته وباعتبارها البيانات سرا ، فإن إفشائها من قبل الموظف الملزم بكتمانها يوقعه تحت العقاب المنصوص عليه في المادة ٣١٠ من قانون العقوبات (السمولى ، ٢٠١٢ ، ص ص ١٣٥ ، ١٣٦) .

ومثل هذه الحماية لا وجود لها في التشريعات العربية إنما هي مجرد نصوص فرعية متفرقة في قوانين مختلفة .

ولقد أبدت مصر استعدادها في مجال الأمن السيبرانى عام ٢٠١٧م حيث أصدر الاتحاد الدولى للاتصالات تقرير مؤشر قياس استعداد ا لدول في هذا المجال من أجل دفع المزيد من الجهود في مجال اعتماد الأمن السيبرانى وتكامله على نطاق عالمى ، وقد تقدمت سنغافورة ، الولايات المتحدة الأمريكية وماليزيا وعمان وأستونيا وموريشيوس وأستراليا وجورجيا وفرنسا وكندا وروسيا ، كما جاءت مصر في المرتبة الرابعة والعشرين من ١٩٣ دولة من دول أعضاء الاتحاد ، وكذلك جاءت في المرتبة الثانية عربيا فيما يتعلق بمستويات الالتزام بالأمن السيبرانى بعد سلطنة عمان التي جاءت في المركز الرابع عالميا والأول عربيا ، كما توجد مؤشرات للتعاون الدولى الإقليمى ومنها مصر شاركت في مؤتمر بودابست للقضاء الإلكترونى في المجر ٢٠١٢ ، وشاركت أيضا في التدريبات السيبرانية العلمية التي يظهرها فريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامي والاتحاد الدولى للاتصالات ، كما عقدت مصر اتفاقية تعاون مع فريق الطوارئ للحاسوب بالولايات المتحدة ووكالة أمن الأنترنت الكورية في مدينة سيول ، والهيئة الماليزية للأمن السيبراني فقد أسهمت مصر بدون حيوى في أعمال المركز ٢٠١٣ وفى ٢٠١٤ انضمت إلى اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء وحماية البيانات ذات الطابع الشخصي ، أما في عام ٢٠١٦ فقد تم توقيع اتفاقية تعاون بين المعهد القومى للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيسكو العالمية فضلا عن مشاركتها في المنتدى الإقليمى للاتحاد الدولى للاتصالات ومنظمة فرست وورش عمل لتنقية الجاهزية لاستجابة الطوارئ ، وفى عام ٢٠١٧ شاركت مصر في مؤتمر المنطقة المركزية للاتصالات الذى استضافته القيادة المركزية الأمريكية في واشنطن للتبادل وجهات النظر في استراتيجيات الأمن السيبرانى الوطنية ومبادرات تكنوولجية المعلومات ٢٠١٧م ، وكذلك شاركت مصر في المؤتمر الإقليمى السادس للأمن السيبرانى والذي نظمه الاتحاد الدولي للاتصالات ٢٠١٨ ثم شاركت في مؤتمر قمة أفريقيا للدفاع السيبرانى في اجتماع لجنة الدراسات التابعة للاتحاد الدولى ، وتبع ذلك مشاركتها في المؤتمر الإقليمى ٢٠١٨م (فوزى ، ٢٠١٩ ، ص ١٢٥) .

وهكذا هيأت البيئة المصرية للأمن السيبرانى الممارسات والأنشطة والتفاعل القائم على أطر تشريعية وتنظيمية وتقنية وتعاونية جيدة وهذا يساعد في تشكيل بنية منضبطة وآمنة ويزيد من إمكانية التنمية .

ب- جهود المملكة العربية السعودية في مكافحة الجرائم السيبرانية :

استهدفت رؤية المملكة العربية السعودية ٢٠٣٠م التطوير الشامل للوطن وأمنه وإنقاذه ورفاهية مواطنيه وعيشهم الكريم ، ولقد كان من الطبيعى أن هناك تطور طبيعى في استخدام نظم المعلومات في جميع أجهزة الدولة ومؤسساتها ، كما أن المجتمع السعودى في الوقت ذاته ليس بمنأى عن التأثيرات العالمية ، فقد أصبح مستهدفا من المنظمات الإجرامية الدولية ، لما تتمتع به المملكة من مكانة اقتصادية وجغرافية ، ولقد حققت المملكة إنجازا عالميا بحصولها على المركز الثالث عشر والأول عربيا من بين ١٧٥ دولة في المؤتمر العلمى للأمن السيبرانى الذى يصدره الاتحاد الدولى للاتصالات التابع للأمم المتحدة لعام ٢٠١٨ متقدمة ٣٣ مرتبة عن تقييمها في الإصدار السابق للمؤشر العالمى لعام ٢٠١٦ (القحطاني ، ٢٠١٩ ، ص ٨٧) .

أما بالنسبة للتشريعات القانونية في المملكة العربية السعودية :

لديها أيضا قانون للجرائم الإلكترونية صادر بموجب مرسوم ملكى في عام ٢٠٠٧ وهو يهدف إلى مكافحة الجرائم الإلكترونية عن طريق تحديد الجرائم وتحديد العقوبات لحماية أمن المعلومات وحماية الحقوق المتعلقة بالاستخدام المشروع لأجهزة الكمبيوتر وشبكات المعلومات وحماية المصلحة العامة بالإضافة إلى ذلك يمكن لوزارة الخارجية السعودية ولجنة تكنولوجيا المعلومات معاقبة مرتكبى الجرائم الإلكترونية بشدة مثل سرقة الهوية والتشهير والقرصنة الإلكترونية وسرقة البريد الإلكترونى وغير ذلك من الأعمال غير القانونية (أبو زيد ، ٢٠١٩ ، ص ص ٥٧ ، ٥٨) .

وانطلاقا من إدراك المملكة العربية السعودية لأهمية تعزيز الأمن السيبراني تم إنشاء:

١- الهيئة الوطنية للأمن السيبراني حيث صدر بإنشائها الأمر الملكى رقم (٦٨٠١) وتاريخ ١١/ ٢ / ١٩٣٩هـ وقد نصت الفقرة الأولى من المادة الثانية من تنظيم الهيئة الوطنية للأمن السيبرانى على أنها ترتبط بمقام الملك ، كما نصت المادة السادسة من ذات التنظيم على أن تشكيلها وفق النحو الآتى رئيسها بأمر ملكي وأعضاؤها رئيس أمن الدولة ، ورئيس الاستخبارات العامة ونائب وزير الخارجية ومساعد وزير الدفاع ومحافظ الهيئة (الهيئة الوطنية للأمن السيبرانى ، ٢٠١٨ ، ص ٦) .

٢ – فتح المسارات الأكاديمية في تخصص الأمن السيبرانى : وقد كان ذلك في غالب الجامعات ومنها جامعة الملك سعود وجامعة الملك عبد العزيز ، وجامعة الأمير سلطان بن عبد العزيز .

٣ – إقامة الملتقيات والدورات والندوات وورش العمل المتعلقة بالأمن السيبرانى : من ذلك ما أقامته وتقيمه الهيئة الوطنية للأمن السيبرانى وما أقامته الجامعات المحلية ، كجامعة شقراء

بعنوان دور الجامعات في تعزيز مفهوم الأمن السيبرانى ، التحديدات والرؤى في تاريخ ١٨ / ٣ / ٢٠١٩ وجامعة نايف العربية للعلوم الأمنية .

ج – التجربة الأردنية في مجال الجرائم الإلكترونية :

وتبرز التجربة الأردنية عبر عدد من المحاور :

الجانب القانوني (إبراهيم ، ٢٠٠٧ ، ص ٥٨)

وهنا يذكر أن المادة ٣٨ من فصل العقوبات لقانون المعاملات رقم ٨٥ لسنة ٢٠٠١ تنص على : " يعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الإلكترونية بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة ، وبغرامة لا تقل عن ثلاث آلاف ولا تزيد على عشرة آلاف دينار أو بكلتا العقوبتين .

كما أقرد مجلس الوزراء قانون جرائم أنظمة المعلومات لسنة ٢٠١٠ ويأتي هذا القانون بعد أن أصبحت جرائم أنظمة المعلومات تنطوى على مخاطر جسيمة وتهدد وقوع خسائر للمؤسسات والأفراد على حد سواء إضافة إلى أنها قد تهدد الأمن الوطنى حيث يستدعى ذلك وجود آليات قانونية للحماية من هذه الأخطار خاصة فيما يتعلق بقضايا الإرهاب الإلكترونى والسرقة الإلكترونية.

وكان دور مديرية الأمن العام في هذا المجال فعال عبر ما يلى :

إنشاء قسم خاص للجرائم الإلكترونية في مديرية الأمن العام تتبع لإدارة البحث الجنائى ٢٠٠٨ (موقع مديرية الأمن العام الأردنية على شبكة الإنترنت) . حيث تبنت مديرية الأمن العام خطة لإعداد مجموعة من الضباط المؤهلين وتزويد القسم بالقوى البشرية المؤهلة من مهندسين وفنيين ومبرمجين وبالمعدات والأجهزة اللازمة للقيام بالعمل ، وذلك لملاحقة هذه الجرائم والتصدى لها حيث تم إنشاء قسم الإسناد والتحقيق الفني في بداية ٢٠٠٨م في شعبة المتابعة والتحقيق الخاصة ، ويعنى هذا القسم بالتحقق من جرائم تكنولوجيا المعلومات والاتصالات والإنترنت ، وسرقة محتويات الخوادم الرئيسية للشركات والمؤسسات ، سرقة حسابات البنوك عبر الإنترنت ، جرائم التهديد والابتزاز ، جرائم القرصنة ومختلف جرائم تكنولوجيا المعلومات ، ويعمل على تقديم الدعم الفني والتقنى لجميع شعب وأقسام إدارة البحث الجنائى .

واجبات قسم الإسناد والتحقيق الفني في مواجهة الجرائم المستحدثة :(النوير ، ٢٠١٥ ، ص ١٨٠).

التحقق في الجرائم الواقعة من خلال شبكة الإنترنت وتشمل : جرائم الاحتيال الإلكترونى ، المالى ، مراقبة تكنولوجيا المعلومات للمنظمات الإجرامية ، الإتجار بالوثائق المحمية ، جرائم التسويق الغير شرعى للبضائع والمعلومات ، جرائم التجارة الإلكترونية ، الإساءة للأطفال والإتجار

بهم ، جرائم الاتصالات ، انتحال الشخصية الإلكترونية ، جرائم البرمجيات ، التحقق في أي جريمة إلكترونية .

توقيع اتفاقية للحد من الجرائم الإلكترونية :

وتم ذلك مع مواقع إلكترونية عالمية للتعاون والتنسيق معها من أجل العمل على الحد من الجرائم الإلكترونية والكشف عن مرتكبيها مثل الشرطة البريطانية وإف بى إف ، شرطة نيويورك والاتحاد الأوربي ، وفيس بوك .

إطلاق مشروع تطوير قدرات التعامل مع الجرائم الإلكترونية:

حيث تم إطلاق هذا المشروع في إدارة البحث الجنائى التابعة لمديرية الأمن العامة الأردنية بالتعاون بين الحكومة الأردنية والمملكة المتحدة وجمهورية التشيك ، وبدعم من الاتحاد الأوبى ويشكل قسم مكافحة الجريمة الإلكترونية في إدارة البحث الجنائى .

محور التشارك من خلال تعزيز أداء العاملين في قسم الجرائم الإلكترونية لدى البحث الجنائى ، إعطاء العاملين الخبرات للتعامل مع هذا النوع من الجريمة ، ومن أحدث الأساليب العلمية تنظيم ورش عمل .

ومما سبق يتضح أن أبرز معالم التجربة الأردنية في مجال مكافحة الجريمة الإلكترونية تتمثل في إقرار مجلس الوزراء قانون جرائم أنظمة المعلومات لسنة ٢٠١٠ وإنشاء قسم خاص للجرائم الإلكترونية في مديرية الأمن العام ، وتوقيع اتفاقيتا للحد من الجرائم الإلكترونية ، وإطلاق مشروع تطوير قدرات التعامل مع الجرائم الإلكترونية ، بالإضافة إلى تنظيم ورش عمل وإنشاء مركز وطنى للاستجابة لحوادث الكمبيوتر .

د- الجريمة الإلكترونية في المجتمع الليبى والتشريعات القانونية : (المايل ، الشريحى ، ٢٠١٩ ، ص ٢٥٣).

تعدد الجرائم الإلكترونية في ليبيا وفق النظرة التي نظر من خلالها المختصين والباحثين بهذا المجال والتي في الواقع تعانى منها أغلب البلدان بصفة عامة وفى ليبيا بشكل خاص ومن هذه الجرائم :

- جريمة استنساخ برامج الحاسب الآلى والمتاجر فيها وتكون هذه الجريمة إما بنسخ البرامج من مواقع الشركات من أشخاص يعملون فيها ثم يقوم بوضعها في أقراص ممغنطة أو أسطوانات وبيعها .
- تحميل برمجيات مضادة للفيروسات غير أصلية ومقرصنة من الإنترنت .

- التزوير والانتحال حيث أنه مع تطور التكنولوجيا وظهور أنظمة الحاسب الآلية بمختلف أنواعها.

التشريع الليبى في مجال الجرائم الإلكترونية (المعلوماتية) :

في الواقع لا يوجد أي تشريع في ليبيا للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال وأمن المعلومات يوجد فقط مسودة بقانون لمكافحة الجرائم الإلكترونية تقدمت بها وزارة العدل لمجلس النواب لم يناقشها بعد ويصادق عليها هذا ، ولم يظهر في القانون الليبى تشريع خاص يحدد الجرائم الإلكترونية أسوة بالتشريعات المقارنة وإن كان هذا النوع من الجرائم دلائل ظهرت في نصوص القانون رقم ٣ لسنة ٢٠١٤ الصادر عن مجلس النواب وتنص المادة الأولى في تحديد مفهوم الأموال ونص المادة الثانية في تحديد العمل الإرهابى ونص المادة ١٥ والمادة ١٧ من قانون مكافحة الإرهاب .

إجراءات التحقيق في الجرائم الإلكترونية :

وتساهم هذه الإجراءات جميعها في الوصول إلى الآتى :

- التأكد من وقوع الجريمة ، تحديد نمط وصفة الجريمة المرتكبة ، التعرف على التقنيات المستخدمة في ارتكابها ، معرفة الأسباب والدوافع المحتملة لارتكابها ، توضيح طبيعة الأدلة الجنائية ومصادرها .

هـ- سبل مكافحة الجرائم المعلوماتية في الجزائر : (رضا ، ٢٠٢١ ، ص ص ١١٦ – ١١٨)

تعديل قانون العقوبات :

بدأ الشرع الجزائرى في مواكبة التطورات التكنولوجية من خلال إدخاله لمجموعة تعديلات على قانون العقوبات وإدراج قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون ١٥ – ٠٤ المؤرخ ١٥ نوفمبر ٢٠٠٤ ثم توالى التعديلات وإدراج بعض السلوكيات الإجرامية المتعلقة بذلك بموجب القانون ٢٣ – ٠٦ المؤرخ ٢٠ ديسمبر ٢٠٠٦ .

آليات مكافحة الجرائم السيبرانية في ضوء القانون :

كخطوة جديدة قام المشرع الجزائرى بسن القانون ٠٤ – ٠٩ المتعلق بالوقاية من تكنولوجيا الإعلام والاتصال ومكافحتها وإن كان تجسيد بنوده على أرض الواقع مازال ضعيفا ، ووضع مجموعة تدابير وقائية وإجرائية للوقاية من هذه الجرائم ومكافحتها .

التدابير الوقائية :

- المراقبة الإلكترونية .

- الاستعانة بمزودى الخدمات للوقاية من الجرائم السيبرانية .

التدابير الإجرائية :

- تفتيش وحجر المنظومة المعلوماتية .
- تمديد الاختصاص بنظر هذه الجرائم .
- تبادل المساعدة القضائية الدولية .
- الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

القوانين المدعمة للحد من الإجرام السيبرانى :

- القانون ٠٤ – ١٨ المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية .
- القانون ٧ – ١٨ المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصى .

المبحث الثالث : الإجراءات المنهجية لطريقة العمل مع الجماعات في تنمية الوعى لدى الشباب الجامعي بمخاطر الجرائم الإلكترونية

هدفت الدراسة إلى التعرف على الاتجاهات النظرية والمنهجية الحديثة لطريقة العمل مع الجماعات لتنمية الوعى لدى الشباب الجامعى بمخاطر الجريمة الإلكترونية ، وذلك من خلال الوعى المعرفى ، العلاجى بالنسبة للشباب الجامعى وتنمية المهارات لدى الأخصائى الاجتماعى وذلك على النحو التالى :

- نتائج البحوث والدراسات السابقة المرتبطة بموضوع البحث .
- الإطار النظرى للدراسة الحالية المرتبطة بالشباب الجامعى والجرائم الإلكترونية .
- الأساس النظرى لطريقة العمل مع الجماعات وما يتضمنه من نظريات ، ونماذج علمية واستراتيجيات ، تكنيكات ، أدوار ، مهارات مهنية يستخدمها الأخصائي الاجتماعي للعمل مع الجماعات عند التعامل مع الشباب الجامعى لتنمية وعيهم بمخاطر الجريمة الإلكترونية.
- المعلومات التي تم تحصليها من المقابلات مع التي عقدها الباحث مع أعضاء هيئة التدريس وأخصائى رعاية الشباب ببعض الكليات بجامعة الأزهر والخبراء المهتمين بالجرائم الإلكترونية .

أولًا : الأساليب المنهجية لطريقة العمل مع الجماعات لتنمية الشباب الجامعي بمخاطر الجرائم الإلكترونية:

الأسلوب الوقائى :

- توجيه الشباب الجامعي نحو التحلي بالسلوك السليم واحترام النظم والقوانين والأعراف الجامعية .

- تزويد الشباب الجامعي بالمعارف والمعلومات عن الجرائم الإلكترونية ومظاهرها وأشكالها ، وأسبابها الاقتصادية والاجتماعية والسياسية والتكنولوجية والآثار المترتبة عليها .
- تنمية المسئولية الاجتماعية لدى الشباب الجامعى من خلال التمسك بالقيم الاجتماعية والمبادئ الأخلاقية السليمة من خلال الدين الإسلامي القويم .
- تشجيع إدارة الجامعة الطلاب للإبلاغ عن الجرائم الإلكترونية .
- توظيف وسائل الإعلام المختلفة في توعية الشباب الجامعى بمخاطر الجرائم الإلكترونية والتي تمثل تهديدا للمجتمعات البشرية .
- تفعيل رعاية الشباب الجامعى لإنشاء مواقع إلكترونية لتوعية المتدربين بالجرائم الإلكترونية المستخدمة .
- إجراء البحوث والدراسات في هذا المجال الحيوى للوقوف على حجم هذه الظاهرة وانتشارها بين الشباب الجامعى ووضع الحلول المناسبة لها .

الأسلوب العلاجى :

- وضع إطار قانوني للحد من مخاطر الجرائم الإلكترونية .
- إقامة معسكرات تثقيفية تسهم في تنامى المشاعر الطيبة وتكوين الصداقات والعلاقات الاجتماعية والقيم السليمة .
- تعديل اتجاهات الشباب الجامعي نحو التواصل عبر الشبكات الاجتماعية واستثمار أوقات فراغهم بما يعود عليهم وعلى اسرهم ومجتمع بالنفع .
- الجدية في تفعيل وتطبيق القوانين والتشريعات التي تُحد من الجرائم الإلكترونية .
- الاستعانة بالخبراء في هذا المجال لتوعية الشباب الجامعى بالمواقع المنافية لتقاليد وقيم مجتمعنا ، والتي يتم بثها للشباب من الدول الغربية لتدمير القوى والطاقات البشرية لمجتمعاتنا .
- حجب المواقع الإباحية من قبل الشركة التي تقدم خدمة الإنترنت .

الأسلوب التنموي الإنشائى :

- تكثيف الأنشطة الطلابية داخل الجامعة .
- التنسيق والتعاون مع مؤسسات المجتمع المدنى للقيام بحملات توعية للمجتمع تحذر من الآثار السلبية المترتبة على تواصل الشباب الجامعى عبر الشبكات واكتسابهم القيم التي تتعارض مع ضوابط الشريعة الإسلامية .

- الوقوف على أسباب الجريمة الإلكترونية لوضع أنسب الحلول للحد من مخاطر الجرائم الإلكترونية .
- تنمية الوعى الدينى لدى الشباب الجامعى من خلال إلمامه بالقضايا والأبعاد الدينية الإسلامية التنت حكم سلوك المسلم وتصرفاته الموجهة بالقرآن الكريم والسنة النبوية.
- نشر الوعى بين الشباب الجامعى بمخاطر التعامل مع المواقع السيئة على الإنترنت والتطرف الإيديولوجى .
- عمل إعلانات لزيادة الوعى للشباب الجامعى بمخاطرها .

ثانيًا : الاستراتيجيات التي يستخدمها الاخصائي الاجتماعي للعمل مع الجماعات لتنمية وعي الشباب الجامعي بمخاطر الجريمة الإلكترونية

الاستراتيجية هي إطار العمل أو المنهج التي يستعين بها أخصائى العمل مع الجماعات بهدف التوعية للشباب الجامعى بمخاطر الجريمة الإلكترونية .

١ – استراتيجية الإقناع :

- وتهدف إلى إقناع الشباب الجامعي بأهم القيم والمعايير الإسلامية والارتباط بها .
- إقناع الشباب الجامعي باستثمار أوقات فراغهم بما يعود عليهم بالنفع .
- اشتراكهم في الأنشطة الطلابية المختلفة التي تتوافق مع ميولهم واتجاهاتهم وثقافتهم.
- إقناعهم من خلال المناقشات الجماعية الموجهة ، الندوات والمحاضرات بالتمسك بالقيم الدينية السليمة .

٢ – استراتيجية الاتصال الموجهة :

- تبادل الآراء والأفكار والمعلومات مع الشباب الجامعي والقيادات الجامعية للتوعية بمخاطر الجرائم الإلكترونية .
- حل المشكلات المختلفة التي تعترض بعض الشباب الجامعي من خلال العلاقة المهنية بين الأخصائيين والطلاب .
- إزالة المعوقات التي تواجه الشباب الجامعي والأخصائي الاجتماعي.
- المتابعة المستمرة والفعالة بين الشباب الجامعى والطلاب لضمان التواصل الجيد والفعال وبين البيئة الخارجية والمجتمع .
- التواصل بين منظمات المجتمع المدنى والشباب الجامعى في التوعية بمخاطر الجرائم الإلكترونية .

٣ – استراتيجية التوضيح :

- توضيح الجوانب السلبية والإيجابية للإنترنت في ظل التحولات الدولية .
- توضيح الآليات الحديثة للوقاية من الجرائم الإلكترونية .
- توضيح الأساليب والأسباب المواجهة للتوعية بمخاطر الجريمة الإلكترونية لدى الشباب الجامعي .
- توضيح كيفية المشاركة في الأنشطة الطلابية واستثمارها فيما يفيد .

٤ – استراتيجية التفاعل الجماعي الإيجابى بين الشباب الجامعى والأخصائى الاجتماعي للعمل مع الجماعات :

- تشجيع الشباب الجامعي على الاتصال البناء وتبادل الآراء والأفكار الإيجابية حول مخاطر الجرائم الإلكترونية .
- مواجهة الصعوبات التي تواجه الشباب الجامعي للحد من التفاعلات السلبية فيما بينهم.
- تفعيل العلاقات الاجتماعية الجيدة بين الطلاب وبعضهم البعض والأخصائى الاجتماعى.

٥ – استراتيجية التشجيع والتدعيم الإيجابى :

- من خلال تشجيع الشباب الجامعي على نبذ روح التشاؤم واللامبالاة داخل المجتمع وخارجه.
- تشجيع الشباب الجامعي على الاستثمار الجيد للإمكانيات المادية والبشرية بمايعود عليهم بالنفع .
- تعريف الشباب الجامعي على مواجهة الواقع وتغييره وتجاوزه .
- استقطاب الشباب الجامعي المبدعين والمبرزين للاستفادة منهم كوسيلة جذب للطلاب للمشاركة في الأنشطة المختلفة والاستفادة من الاستخدام غير الآمن للإنترنت .
- إعداد كوادر طلابية قادرة على تخطيط وتنفيذ الأنشطة الطلابية .
- تشجيع مشاركات وإبداعهم ونشرها في الوسائل الإعلامية .

٦ – استراتيجية النمذجة السليمة :

- تعديل الأفكار السلبية عند الطلاب نحو الاستخدام غير الآمن للإنترنت .
- تصحيح وتغيير الأفكار والمعتقدات المتطرفة والمشبوهة لدى الشباب الجامعى .
- تقديم النماذج الناجحة لمعرفة كيف كانت بدايتهم واستثمارهم الأمثل لأوقات الفراغ بما يفيد المجتمع .
- تقديم القدوة والمثل الذى يحتذى به الشباب الجامعى والاستفادة منهم بشكل فعلى.

التكنيكات التي يُمكن أن يستخدمها الأخصائى الاجتماعي للعمل مع الجماعات :

- تكنيك العمل الجماهيري : يستخدم هذا التكنيك لإحداث التغير المطلوب والمرغوب وهو إحداث تغيير وعى الشباب الجامعى بمخاطر الجرائم الإلكترونية .
- تكنيك لعب الدور الموجه :

- التعرف على الاستخدام غير الآمن للإنترنت .
- التعرف على مخاطر الجرائم الإلكترونية وانعكاساتها على الشباب الجامعي والمجتمع .
- إتاحة فرصة للشباب الجامعي لعرض مواقف واقعية أو تمنعه من الوقوع في الجرائم الإلكترونية .

- تكنيك التنسيق : ويستخدم هذا التكنيك في التنسيق بين الجامعات والجهات المختلفة للحد من مخاطر الجرائم الإلكترونية بين الشباب الجامعى .
- تكنيك المحاضرات والندوات وورش العمل :

- تبادل المعلومات مع الخبراء والمتخصصين في مجال التكنولوجيا لتوعية الشباب الجامعى بمخاطر الجريمة الإلكترونية .
- تكثيف المحاضرات حول الجرائم الإلكترونية .
- تشجيع أعضاء هيئة التدريس للطلاب المشاركين في الأنشطة والندوات المرتبطة بالجرائم الإلكترونية .
- الإعلان الجيد للطلاب عن الندوات وورش العمل المرتبطة بالجرائم الإلكترونية .

- تكنيك الرحلات والمعسكرات :
- إكساب الشباب الجامعى قيمة العلم والتمسك بقيم المجتمع السليمة .
- إكساب الطلاب تنمية الجانب الروحى من خلال الرحلات للأماكن الدينية .
- تحقيق التفاعل الجماعى نحو الآخرين بما يساعدهم على الاعتماد على أنفسهم .
- توفير فرص التعلم والتثقيف في المعارف والأفكار .
- إكسابهم خبرات حياتية في كيفية التعامل مع الآخرين وتحمل المسئولية .

رابعًا : الأدوار المهنية للأخصائي الاجتماعي للعمل مع الجماعات لتنمية وعي الشباب الجامعي بمخاطر الجرائم الإلكترونية

١ – دور المستثير وذلك :

- استثارة الشباب الجامعي لاكتشاف قدراتهم واستثمارها فيما يفيد وخاصة في مجال الجرائم الإلكترونية .
- حثهم على التفاعل الجماعى والتنافس الإيجابى بين الطلاب وبعضهم البعض من خلال التفكير السليم والاستخدام الآمن للإنترنت .
- استثارة الشباب الجامعى على ضرورة التعبير عن وجهات نظرهم وما يدور داخلهم لحل المشكلات التي يتعرضون لها .

٢ – دوره كمخطط ومنمى من خلال :

- المساهمة في رسم السياسات والخطط واقتراح البدائل المتاحة واختيار أفضل البدائل والحلول لمواجهة الاحتياجات العامة للشباب الجامعى في خطط الجامعات للاهتمام بمخاطر الجرائم الإلكترونية .
- تنمية قدرات الشباب الجامعي لاتخاذ أنسب القرارات فيما يتعلق بهم وبحياتهم ومعلوماتهم عن المجتمع الافتراضى .
- الاتصال المباشر مع الإدارة العليا في الجامعة وربطه بالأجهزة الأخرى المعنية في الجامعات والمؤسسات والمراكز المرتبطة بالجرائم الإلكترونية .

٣ – دوره كمساعد ومعين :

- مواجهة الصعوبات التي تواجه الشباب الجامعي ومنها الجرائم الإلكترونية .
- التعرف على قضاياهم وتحديد مصادر مشكلاتهم .
- تعديل بعض الأفكار الخاطئة عن الاستخدام السئ للإنترنت والمواقع الخارجة عن قيم المجتمع .
- مساعدة الشباب الجامعى على الشعور بقيمهم في ضوء التعبير عن آرائهم وأفكارهم.

٤ – دور الموجه والخبير :

- يقوم أخصائى العمل مع الجماعات بتزويد الشباب الجامعي بالمعلومات والخبرات التي يحتاجونها عن براثن الوقوع في الجرائم الإلكترونية .
- توجيه الشباب الجامعي نحو الاستفادة من المشاركة في الأنشطة الطلابية .
- يوجه الشباب الجامعي إلى نوعية الأنشطة التي تتفق مع ميولهم واحتياجاتهم .

- توجيه الشباب الجامعي بصفة الخبير بمصادر المعلومات الصحيحة عن الاستخدام الأمثل للإنترنت فيما يعود عليهم بالنفع .

٥ – دور المشجع والمناقش :

- تشجيع الشباب الجامعي على المشاركة الإيجابية وفاعلية في الحوار والمناقشة بحرية عن الجرائم الإلكترونية .
- تشجيعهم على الربط بين ما يتم مناقشته وبين السلوك الفعلى عن الجرائم الإلكترونية.
- مناقشتهم حول أهمية الاستفادة من الموارد المتاحة والاحتياجات الفعلية .
- تحديد أهدافهم بوضوح بما يتلاءم مع قيم المجتمع الدينى والإسلامى .

٦ – دور القائد :

- يساعد على إشعار الشباب الجامعي بالأمن عند ممارسة الأنشطة المختلفة .
- يلتزم بالسلوك الديمقراطى قولًا وفعلًا أمام الشباب الجامعى .
- يقوم بالبدء في عرض الأفكار والآراء الجديدة لمساعدة الشباب الجامعى على التغلب على الجرائم الإلكترونية دون خجل .

وهذه الأدوار يتم الاستفادة منها من خلال الأنشطة الطلابية المختلفة سواء كانت اجتماعية أو ثقافية أو فنية او دينية أو علمية أو دينية حسب اتجاهات وميول الشباب الجامعي لتلك الأنشطة التي تتناسب مع إمكاناتهم ، ويستخدم العصف الذهنى ، حل المشكلات واتخاذ القرارات.

خامسًا : المهارات المهنية التي يستخدمها الأخصائى الاجتماعي للعمل مع الجماعات في تنمية وعي الشباب الجامعي بمخاطر الجرائم الإلكترونية

١ – مهارة القدرة على الملاحظة الجيدة :

تُعتبر الملاحظة المقصودة واحدة من المهارات اللازم توافرها في الأخصائي الاجتماعي بوجه عام وأخصائى العمل مع الجماعات بوجه خاص .

- ملاحظة الأخصائي لسلوك الشباب الجامعي داخل المحاضرات وخارجها وتحليل هذا السلوك سواء كان سلبى أو إيجابى .
- ملاحظة جميع الطلاب كل على حدة أثناء تفاعلاته مع الجماعة وذلك لفهم وتفسير والتعرف على مدى التغيير الذى لحق بالطلاب .
- ملاحظة الأخصائي الاجتماعي للمشكلات ومنها الجرائم الإلكترونية وانعكاساتها على الشباب الجامعي.

٢ – مهارة القدرة على تكوين علاقة مهنية :

- فيتكون العلاقة المهنية الجيدة والإيجابية بينه وبين الطلاب وتكون على الثقة والتقدير والاحترام المتبادل .
- التأكيد على إشعار الطلاب بالأمن والثقة المتبادلة بينهم وبين الأخصائي الاجتماعي للعمل مع الجماعات فيما يتعرضون لهم من مخاطر ومنها الجرائم الإلكترونية .
- مساعدة الطلاب على التعبير عما بداخلهم من الاستخدام غير الآمن للإنترنت .
- مساعدة الطلاب التفاعل الإيجابى البناء مع زملائهم وأساتذتهم داخل المحاضرات ومن خلال الندوات وورش العمل عن مخاطر الجرائم الإلكترونية .

٣ – مهارة القدرة على الاتصال الفعال :

- لفهم ما يدور داخل أذهان الشباب الجامعي من آراء وأفكار عن الجرائم الإلكترونية وكيفية الوقاية منها .
- الاستماع الجيد إلى مشكلات الطلاب وإشراكهم في إيجاد حلول لهذه المشكلات .
- مساعدة الطلاب على كيفية الاتصال الفعال على المستوى الرأي والأفقى .
- مساعدتهم على الإفراغ الوجدانى لكل ما يؤهلهم ويشعرهم بالخوف من الجرائم الإلكترونية.

٤ – مهارة التوجيه الجماعى الإيجابى :

- توجيه الأخصائي الاجتماعي الجماعات للتفاعلات الإيجابية بين الطلاب حول موضوع الجرائم الإلكترونية .
- الحرص على مشاركة الطلاب في مشكلاتهم وأفراحهم وأحزانهم التي تؤثر عليهم .
- تجنب إحراج الطلاب لتنفيذهم بض الأدوار المنوطة عليها مع ضرورة المشاركة الفعلية لتذليل الصعاب .

٥ – مهارة القدرة على التأثير :

- قدرة الأخصائي الاجتماعي في التأثير على الشباب الجامعي في التعامل مع الجرائم الإلكترونية.
- مساعدة الطلاب على مواجهة أمورهم المختلفة داخل الحرم الجامعى .
- التأثير وتنمية الجوانب الإيجابية التي تساعدهم على حل مشكلاتهم .

٦ – مهارة المتابعة والتقويم :

- قدرة الأخصائي الاجتماعي على معرفة تفاعلات وعلاقات وتصرفات الشباب الجامعى مع غيرهم من الزملاء والبيئة المحيطة .
- متابعة أوجه القصور في الأنشطة المقدمة للشباب الجامعى وأوجه الاستفادة منها .
- متابعة ما تم من أنشطة فعلية والمعوقات التي تعوق قيامه بدوره .

سادسًا : النظريات والنماذج التي يستخدمها الأخصائي الاجتماعي للعمل مع الجماعات في تنمية وعي الشباب الجامعى بمخاطر الجرائم الإلكترونية

أ- نظرية الأنساق الأيكولوجية :

وقد استفاد الباحث منها تحديد الأنساق المختلفة لظاهرة الجرائم الإلكترونية لدى الشباب الجامعى نسق الشباب الجامعى ، نسق الجامعة ، نسق المجتمع ، نسق الأسرة .

ب-نموذج العلاج المعرفى السلوكى:

وقد استفاد الباحث منها في تحديد أهمية الجوانب المعرفية لدى الشباب الجامعى والتي تكون لها الآثار في اتخاذ الجرائم الإلكترونية ، وأهمية البناء المعرفى لدى الشباب الجامعى في إعادة التوجيه الصحيح للسلوك في بناء القناعات الفكرية من خلال التحليل المعرفى لأفكار الشباب الجامعى ، زيادة المعارف والمعلومات عن الجرائم الإلكترونية .

ج- نموذج حل المشكلة :

تحديد المشكلة للتعرف على المشكلة وتحديدها قبل اتخاذ إجراء نحوها فيجب التعرف على الطلاب الذين يعانون من مشكلة الجرائم الإلكترونية .

وضع خطة للحل : من خلال المقارنات بين الحالة الراهنة والمرغوب فيها كذلك بين المعلومات التي لدى الشباب الجامعى والمعلومات التي يحتاجها أثناء حل المشكلة .

تنفيذ الحل وتشمل المرحلة تطبيق الخطة الفكرية أو الاستراتيجية وفى هذه المرحلة يتاح القائم بالحل بمعرفة مدى صحة اختياره للاستراتيجية المناسبة لمواجهة الجريمة الإلكترونية وأن الاستراتيجية قد تتغير أو تتعدل حسب العقبات التي تقابل أخصائى العمل مع الجماعات .

تقويم الحل : عندما تحل المشكلة فإن الأخصائى الاجتماعى يكون في حاجة إلى تقويم هذا ومعرفة مدى صحته وذلك طبقا للأهداف الموضوعة ومحكات التقويم وتختلف عملية التقويم باختلاف ، فالمشكلة المحددة كالجرائم الإلكترونية يكون تقويمها أكثر وضوحا وتحديدا .

د- نموذج مارتن بلوم :

يستهدف النموذج منع المشكلات المتوقع حدوثها والتي يمكن التنبؤ بها وتجنب الوقوع ضحية لها ويسترشد النموذج بجمع المعلومات عن مشكلة الجرائم الإلكترونية ، تحديد الأهداف ، اتخاذ القرارات ووضع البرامج والخطة للوقاية من المشكلة ،تنفيذ البرامج والخطط الوقائية .

سابعًا : الاستنتاجات العامة لتنمية وعى الشباب الجامعي بمخاطر الجرائم الإلكترونية

- إجراء دراسات تبين الآثار النفسية والاجتماعية لإدمان الإنترنت .
- مخاطبة وسائل الإعلام المختلفة لتسليط الضوء على الجرائم الإلكترونية .
- الاستفادة من التجارب التي تقدمها الجامعات الدولية الإيجابية في مجال الجرائم الإلكترونية .
- رسم سياسة وطنية تفرض عقوبات صارمة على الشباب مرتكبى الجرائم .
- الإعداد الجيد للبرامج والأنشطة الهادفة لتنمية وعى الشباب في الجامعات بمخاطر الجرائم الإلكترونية .
- الاهتمام بالدراسات والبحوث العلمية التي تعرض مخاطر الجرائم الإلكترونية .
- الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكب الجريمة.
- التعاون المستمر بين العديد من التخصصات والمؤسسات منها الإدارة العليا للجامعات وإدارة رعاية الشباب وأعضاء هيئة التدريس وإدارة الكليات لتنمية وعى الشباب الجامعى في الجامعات بمخاطر الجرائم الإلكترونية .
- العمل على تعيين إدخال مادة الإنترنت ضمن المناهج الدراسية في التعليم الجامعى .
- تأسيس نظام وطنى لرصد أمن المعلومات للشباب الجامعى لمخاطر الجرائم الإلكترونية.
- حث الجامعات والمراكز البحثية على تسليط الضوء على أكثر من هذه الجرائم الإلكترونية بمختلف أنواعها .
- عدم الكشف عن كلمة السر نهائيا وتغييرها بشكل مستمر واختيار كلمة سر صعبة .
- الاستعانة بأجهزة تكنولوجيا حديثة لمنع مواقع التواصل الاجتماعى بمخاطر الجرائم .
- تشجيع الشباب الجامعى للكشف والإبلاغ عن الجرائم الإلكترونية .
- وضع سياسات قومية ودولية تعمل على التقليل من حدة المخاطر الإلكترونية خاصة فيما يتعلق بالشباب الجامعى التي تمثل الركيزة الأساسية لنهوض ورفعة المجتمعات.

- لابد من زيادة آليات اقتصادية أكثر مواءمة للمخاطر الاقتصادية التي يتعرض لها الشباب الجامعى وذلك من خلال شراكة بين المؤسسات المعرفية ومؤسسات العمل بحيث تمكن الشباب من مواجهة المخاطر .
- ضرورة إعطاء مساحة من الوقت لجلسات الحوار والمناقشة بين كل من الآباء والأبناء.
- العمل على مصاحبة الآباء لأبنائهم والتواصل مع أصدقائهم والتعرف عليهم .
- توعية الآباء بالجوانب الإيجابية والسلبية للألعاب الإلكترونية .
- عدم انشغال الآباء عن الأبناء لفترات طويلة .
- تنمية هواية القراءة في نفوس الأبناء .
- توعية الأبناء بخطورة وأضرار الجلوس لفترات طويلة امام الأجهزة الإلكترونية .
- ضرورة إنشاء جهات رقابية تتولى الرقابة ومتابعتها على ما يطرح في الأسواق ويتم تداوله بين الشباب .
- حث علماء التربية وعلم النفس والاجتماع والخدمة الاجتماعية والدين الإسلامي والقانون إجراء بحوث توعية عن مخاطر الجرائم الإلكترونية .
- زيادة التأكيد على القيم الدينية والأخلاقية للشباب الجامعى من خلال المؤسسات المختلفة في المجتمع .
- زيادة فاعلية رقابة الأسرة على الأبناء من خلال محو الأمية المعلوماتية للآباء .
- تشديد الرقابة على مقاهى الإنترنت وسن القوانين اللازمة وتغليظ العقوبة على المخالف.
- يجب أن تلعب وسائل الإعلام دور هام في توعية الشباب بمخاطر الإنترنت .
- تضمين مقررات دراسية على مادة عملية تجعل الشباب قادرين على التفاعل مع إيجابيات الإنترنت .
- يجب على الدولة أن تضع استراتيجية لحل مشكلات الشباب وإدماجهم في المجتمع وتدعيم مفهوم الهوية الوطنية .
- يجب أن تتضافر مؤسسات المجتمع المدنى مع بعضها البعض لتوعية الشباب الجامعى بالآثار الجانبية للثورة المعلوماتية .
- مناشدة الجهات المختصة بتطبيق القوانين أو استحداث قوانين تكفل التصدي للاستخدام السئ لهذه الشبكة .

- تحذير الأبناء من إعطاء معلومات شخصية عن أنفسهم الذين يتم التعارف بينهم عن طريق الإنترنت .
- إقامة مؤسسات بحثية داخل وحدات مكافحة الجرائم الإلكترونية تهتم بالأمن البشرى والتعامل مع التطورات التكنولوجية .
- تحذير الأبناء من مخاطر تنظيم لقاء مع أحد آخر من الأشخاص من معارف الإنترنت.
- تعليم الأبناء عدم الرد على ما ينقلونه من رسائل إلكترونية وبخاصة من الأشخاص الذين لا تربطهم بهم صلة .
- إلقاء محاضرات وندوات ودروس لتوعية الأفراد وأولياء الأمور وتوجيههم إلى كيفية الاستخدام الآمن للإنترنت .
- عقد لقاءات لخطباء المساجد والمؤسسات الدينية الأخرى لتبصيرهم بأخطار الإنترنت والأسلوب الأمثل لطرح الموضوع في المساجد والكنائس فقد يؤدى طرح الموضوع بصورة غير مناسبة إلى تفشى الأخطار بين الشباب .
- التنسيق والتعاون مع مزودى الإنترنت وأصحاب مقاهى الإنترنت وشركات الاتصال لضمان السلامة في استخدام الإنترنت .
- متابعة المشاكل الناجمة عن الاستخدام السيئ للإنترنت في المجتمع ومناقشة كل ما يستجد من مخاطر .
- تدريب وتأهيل الكوادر البشرية العامة في مجال مكافحة الجرائم الإلكترونية على كيفية التعامل مع هذا النوع من الجرائم .
- التنسيق والتعاون مع المدارس والجامعات لضمان سلامة الطلاب والحصول على تمويل من الخيرين للقيام بمشروع شبكة تعليمية محلية كبيرة ، وحث الجامعات على فتح بريد إلكترونى للطلاب .
- دراسة أوضاع الشباب العاطلين عن العمل وتوفير فرص عمل تؤمن لهم مستقبلهم سواء كان ذلك في أجهزة الدولة أو القطاع الخاص بعد تعليمهم وتدريبهم حتى يكونوا منتجين ويبعدهم عن الجرائم الإلكترونية .

المراجع

أولاً : المراجع العربية :

١. إبراهيم ، حامد (٢٠٠٧). طرق التصدي للجريمة المعلوماتية ، دار الرحاب ، القاهرة ، الطبعة الأولى .

٢. إبراهيم ، مجدى عزيز (٢٠٠٠). موسوعة المناهج التربوية ، القاهرة ، مكتبة الأنجلو المصرية .

٣. الإبراهيمى ، علاء الدين (٢٠١٢). الجرائم الإلكترونية الوسائل وطرق الوقاية منها ، مكتبة عناية للنشر ، الجزائر ، الطبعة الأولى .

٤. أبو زيد ،عبد الرحمن عاطف (٢٠١٩). الأمن السيبرانى الوطن العربى ، دراسة حالة المملكة العربية السعودية ، آفاق سياسية ، المركز العربى للبحوث والدراسات ، العدد ٤٨ ، أكتوبر .

٥. أحمد ، جمال زين العابدين أمين أحمد (٢٠٢١). الاختصاص القضائى وإجراءات التحقيق في الجرائم الإلكترونية ، دراسة مقارنة ،مجلة مستقبل العلوم الاجتماعية ، العدد الرابع ، ينابر .

٦. أحمد، أمانى صالح صالح (٢٠٢١). دور مقترح لخدمة الجماعة في التعامل مع الآثار السلبية المترتبة على إدمان الأطفال للألعاب الإلكترونية ، مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية ، جامعة الفيوم ، العدد الثالث والعشرون.

٧. آل سعود ، على يحى (٢٠٢٠). الأمن السيبرانى وآلياته في الحد من السلوكيات الانحرافية للأحداث في المملكة العربية السعودية ، دراسة نظرية تحليلية ، مجلة كلية التربية ، جامعة كفر الشيخ ، المجلد ٢٠ ، العدد ٤ .

٨. أمين ، ياسر فيصل (٢٠١٩). جرائم الإرهاب عبر الوسائل الإلكترونية ، دراسة مقارنة ، مجلة مصر المعاصرة ، الجمعية المصرية للاقتصاد السياسى والإحصاء والتشريع ، مجلد ١١٠ ، العدد ٥٣٦ ، أكتوبر .

٩. باسو ، عبد الحق (٢٠٠٦). الإرهاب الإلكترونى في القانون المغربى الدولى ، المؤتمر العام لمكافحة الجرائم الإرهابية المعلوماتية بالمغرب ، ١١ – ١٥ فبراير .

١٠. البخارى (٢٠٠٧). ينظر شرح بعض مفردات الحديث في كتاب دليل الراغبين إلى رياض الصالحين للإمام يحيى بن شرف النووي (ت ٦٧٦هـ) ، فاروق حمادة ، دار السلام ، القاهرة ، الطبعة الأولى ، ج (١) ، ص ١١٠ .

١١. جاب الله ، عادل موسى عوض (٢٠٢٢). وسائل حماية الأمن السيبرانى ، دارسة فقهية تأصيلية مقارنة بالنظم المعاصرة ، جامعة الأزهر ، كلية الشريعة والقانون بأسيوط ، العدد ٣٤ ، جـ٣ يناير .

١٢. جاب الله ، عادل موسى عوض (٢٠٢٢). وسائل حماية الأمن السيبرانى ، دراسة مفتاحية تأصيلية مقارنة بالنظم المعاصرة ، مجلة كلية الشريعة والقانون بأسيوط ، جامعة الأزهر ، العدد ٣٤ ، الجزء ٣ ، يناير .

١٣. جلبى ، عبد الرازق وآخرون (٢٠٠٨). نظرية علم الاجتماعى ، الاتجاهات الحديثة المعاصرة ، الإسكندرية ، دار المعرفة الجامعية .

١٤. الجهاز الركزى للتعبئة العامة والإحصاء (٢٠٢٣). جمهورية مصر العربية ، يناير.

١٥. جوناثان ، برتر (١٩٩٩). بناء نظرية في علم الاجتماع ، ترجمة دكتور محمد سعيد فرح ، الإسكندرية ، منشأة المعارف .

١٦. جوهر ، عادل محمد موسى وآخرون (٢٠١٤). الممارسة العامة المتقدمة للخدمة الاجتماعية في مجال الدفاع الاجتماعى ، القاهرة ، دار النور للطباعة والإعلان .

١٧. الحبيب عباس محمد (٢٠١٧). الجريمة المنظمة العابرة للحدود ، رسالة دكتوراه ، كلية الحقوق والعلوم السياسية ، جامعة أبى بكر بلقاير ، عمان .

١٨. حجازى ، عبد الفتاح بيومى (٢٠٠٢). الدليل الجنائى والتزوير في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، مصر .

١٩. حسنى ، محمود نجيب (١٩٨٩). شرح قانون العقوبات ، القسم العام ، دار النهضة العربية ، القاهرة ، ط٦ .

٢٠. حميد ، محمد مسعد ، مصطفى ، مصطفى جاد (٢٠١٩). رؤية استراتيجية لمكافحة الجرائم السيبرانية ، اليمن دراسة حالة ، المجلة العربية الدولية للمعلوماتية ، اتحاد الجامعات العربية ، جمعية كليات الحاسبات والمعلومات ، المجلد ٧ ، العدد ١٢ .

٢١. خير الدين ، عماد (٢٠٠٠). القانون الدولى في مواجهة الجرائم المعلوماتية ، عمان ، دار عاصم .

٢٢. خير الله ، سامى (٢٠١٢). الإنترنت وأمن المعلومات ، دار عصمت للنشر ، القاهرة ، الطبعة الأولى .

٢٣. رضا ، مهدى (٢٠٢١). الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائرى ، مجلة ايلزا للبحوث والدراسات ، المركز الجامعى المقاوم ، الشيخ آمود بن مختار إيليزى ، المجلد ٦ ، العدد ٢ .

٢٤. 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 للدراسات الانسانية، ٢٩ (٢)، .٢٤٨-٢٣٠

٢٥. الزين ، غدير برنس عضوب ، الخرابشة عبد الكريم عودة (٢٠٢١). الجرائم الإلكترونية ومستوى الوعى بخطورتها ، دراسة ميدانية على عينة من الشباب الأردني ، مجلة الجامعة الإسلامية للبحوث الإنسانية ، شئون البحث العلمى والدراسات العليا ، مجلد ٢٩ ، العدد ٢ .

٢٦. سالم ، عبد الحميد (٢٠١٢). تقارير عالمية ، اليوم السابع .

٢٧. السكرى ، أحمد شفيق (٢٠٠٠). قاموس الخدمة الاجتماعية ، القاهرة ، الهيئة المصرية العامة للكتاب .

٢٨. سليم ، نشوى محمد أبو يحيى محمد (٢٠٢١). تقويم برامج العمل مع جماعات النشاط المدرسى لتوعية الطلاب بالاستخدام غير الآمن للإنترنت ، مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية ، جامعة الفيوم ، العدد الثانى والعشرون.

٢٩. سليمان ، محمد عبد المجيد (بدون سنة). الاقتصاد الحفنى أسبابه وانعكاساته وطرق التغلب عليه ، دار التعليم الجامعى ، بيروت .

٣٠. السنهورى ، أحمد محمد ، وآخرون (٢٠٠٢). الممارسة العامة المتقدمة للخدمة الاجتماعية ، القاهرة ، دار النهضة العربية .

٣١. الشبلي، عبد الله .(٢٠١٩). الجريمة الإلكترونية في سلطنة عمان: التحديات والحلول القانونية، مجلة العلوم الًقتصادية والإدارية والقانونية،٣ (٢)، ٨٣-٩٨.

٣٢. شتا ، السيد على (١٩٩٧). نظرية علم الاجتماع ، الإسكندرية ، مطبعة الإشعاع.

٣٣. الشربجي، عادل محمد؛ المايل، عبدالسلام محمد؛ قابوسة، علي. (٢٠١٩). الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم – الأسباب – سُبل المكافحة مع التعرض لحالة ليبيا. مجلة آفاق للبحوث والدراسات، مجلة دولية محكمة، المركز الجامعي ايليزي، العدد ٤، ٢٤٢-٢٥٥.

٣٤. شفرة على خليل (٢٠١٤). الإعلام الجديد (شبكات التواصل الاجتماعى) ، عمان ، دار أسامة للنشر والتوزيع .

٣٥. شفلوت ، جعفر بن محمد بن ذيب (٢٠٢١). العوامل الاجتماعية المؤدية لارتكاب الجرائم الإلكترونية في المجتمع السعودى ، مجلة كلية الخدمة الاجتماعية للدراسات والبحوث الاجتماعية ، جامعة الفيوم ، العدد السابع والعشرون .

٣٦. الشهرانى ، معلوى بن عبد الله (٢٠١٩). تصور مقترح لوقاية الشباب الجامعى من مخاطر جرائم الإرهاب السيبرانى ، مجلة المشكاة للعلوم الإنسانية والاجتماعية ، جامعة العلوم الإنسانية العالمية ، مجلد ٦ ، العدد الثانى .

٣٧. الشهرى ، حسن أحمد (٢٠١٥). الإرهاب الإلكترونى حرب الشبكات ، المجلة العربية الدولية للمعلوماتية ، المجلد الرابع ، العدد الثامن .

٣٨. الشوابكة، عدي محمد علي. (٢٠٢٢). مُعوقات مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الإختصاص. المجلة العربية للنشر العلمي، العدد ٤٣، ٣٣١- ٣٥٦.

٣٩. الصانع، نورة عمر أحمد. (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية، جامعة أسيوط، ٣٦(٦)،٩٠ – ٤١

٤٠. الصوفى ، عبد الله إسماعيل (١٩٩٧). معجم التقنيات التربوية ، عمان ، دار المسيرة ، الطبعة الأولى .

٤١. الصياد ، حلمى فتحى حافظ (٢٠٢١). الجرائم الأسرية المترتبة على الإدمان الإلكترونى ودور الأخصائى الاجتماعى كممارس عام في مواجهتها ، مجلة مستقبل العلوم الاجتماعية ، العدد الخامس ، أبريل .

٤٢. عبد الفتاح محمد ، السيد ، هالة مصطفى (٢٠٠٩). ممارسة تنظيم المجتمع في الأجهزة والمنظمات المختصة ، الإسكندرية ، المكتب الجامعى الحديث .

٤٣. عبد الله ، عبد الله عبد الكريم (٢٠٠٧). جرائم المعلوماتية والإنترنت دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا ، ط١ ، منشورات الحلبى الحقوقية ، لبنان .

٤٤. عبد الهادى ، مسعودى (٢٠١٨). الأعمال المصرفية الإلكترونية ، عمان ، دار اليازورى ، ط

٤٥. عرب ، يونس (٢٠٠٢). جرائم الكمبيوتر والإنترنت ، منشورات اتحاد المعارف العربية ، بيروت ، الطبعة الأولى .

٤٦. عكة ، محمد إبراهيم ، مناصرة ، كفاح محمد (٢٠٢٠). العوامل الاجتماعية والنفسية لدى مرتكبى الجرائم الإلكترونية ذات الطابع الجنسى من وجهة نظر المختصين لدى الأجهزة الأمنية في جنوب الضفة الغربية ، مجلة دراسات في العلوم الإنسانية والاجتماعية ، مركز البحث وتطوير الموارد البشرية ، المجلد الثالث ، العدد١.

٤٧. علوان ، محمد يوسف ، الموسى ، محمد خليل (٢٠٠٦). الحقوق الإنسانية ، الحقوق المحمية ،دار الثقافة ، عمان ، الأردن ، الطبعة الأولى .

٤٨. على ، هالة مصطفى محمد (٢٠٢٢). التخطيط لتنمية وعى الشباب الجامعى بمخاطر الجرائم الإلكترونية ، مجلة دراسات في الخدمة الاجتماعية ، كلية الخدمة الاجتماعية ، جامعة حلوان ، العدد ٦٠ ، الجزء الثانى ، أكتوبر .

٤٩. علي، هالة مصطفى. (٢٠٢٢). التخطيط لتنمية وعى الشباب الجامعى بمخاطر الجرائم الإلكترونية. مجلة دراسات في الخدمة الإجتماعية، العدد (٦٠)، الجزء الثاني، ٣٧٩- ٤١٨.

٥٠. العمرى ، علاء الدين يوسف (٢٠٠٤). المراهق وشبكة الإنترنت الفوائد والمخاطر ، مجلة كلية التربية ، اللجنة الوطنية القطرية للتربية والثقافة والعلوم ، العدد الثامن والأربعون ، مارس .

٥١. العميري، مطلق سعد. (٢٠٢٢). دور الإعلام التربوي في تنمية الوعي بالأمن السيبراني والمعلومات لطلاب جامعة الكويت. مجلة العلوم التربوية، كلية الدراسات العليا، جامعة القاهرة،٣٠(٤) الرقم المسلسل للعدد ٢ جزء ٢ ، ص ٢٤١-٢٧٧.

٥٢. العنزى ، ماجد عواد (٢٠٢١). دور ممارسة بعض الألعاب الإلكترونية في ارتكاب الجرائم لدى عينة من نزلاء دار الملاحظة الاجتماعية ، المجلة الدولية لآفاق المستقبل ، المجلة الدولية للبحوث في العلوم التربوية ، السعودية ، المجلد ٤ ، العدد ٢ .

٥٣. فهيم كلير (٢٠٠٧). طريق نجاح الشباب في الحياة ، مكتبة الأنجلو المصرية ، القاهرة .

٥٤. فوزى ، إسلام (٢٠١٩). الأمن السيبرانى الأبعاد الاجتماعية والقانونية تحليل سوسيولوجى ، المجلة الاجتماعية القومية ، المركز القومى للبحوث الاجتماعية والقانونية ، مجلد ٥٦ ، العدد ٢ ، مايو .

٥٥. فوزى إسلام (٢٠١٩). الأمن السيبرانى ، الأبعاد الاجتماعية والقانونية تحليل فسيولوجى ، المجلة الاجتماعية القومية ، المركز القومى للبحوث الاجتماعية والجنائية ، مجلد ٢٦ ، العدد ٢ ، مايو .

٥٦. القحطانى ، نور بنت ناصر (٢٠١٩). مدى توافر الوعى بالأمن السيبرانى لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعى ، دراسة ميدانية في شئون اجتماعية ، جمعية الاجتماعية ، الشارقة ، المجلد ٣٦ ، العدد ١٤٤ .

٥٧. القرنى ، حسن بن عبد الله حسن الرزقى (٢٠١٩). دور الأسرة السعودية في تحصين أبنائها من مخاطر الإنترنت ، مجلة العلوم التربوية والنفسية ، جامعة البحرين ، مركز النشر العلمى ، مجلد العشرون ، العدد الثانى .

٥٨. قوارى ، سليمان ، رحلى ، سعاد (٢٠١٧). دور التربية والتوجيه في الحماية والوقاية من الجرائم الإلكترونية ، أعمال المؤتمر الدولى الرابع عشر ، مركز جيل البحث ، جامعة تلسان طرابلس .

٥٩. قويقح ، حورية (٢٠٢٠). الأبعاد الاقتصادية للجريمة الإلكترونية ، مجلة الإصلاحات الاقتصادية والاندماج في الاقتصاد العالمى ، المدرسة العليا للتجارة ، مخبر الإصلاحات الاقتصادية ، التنمية واستراتيجيات الاندماج في الاقتصاد العالمى ، مجلد ١٤ ، العدد ٢ .

٦٠. كزيز ، صباح ، قط سمير (٢٠١٨). أثر الجرائم الإلكترونية على أمن واستقرار الدول ، قرصنة الموقع الإلكترونى لوكالة الأنباء القطرية أنموذجا ، مجلة الناقد للدراسات السياسية ، جامعة محمد خيضر سكرة ، كلية الحقوق والعلوم السياسية ، العدد ٣ ، أكتوبر .

٦١. المايل ، عبد السلام محمد ، الشريحى ،عادل محمد على (٢٠١٩). الجريمة الإلكترونية في الفضاء الإلكترونى المفهوم ، سبل المكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات ، المركز الجامعى المقام الشيخ آمود بن مختار إيليزى ، العدد ٤ .

٦٢. مبروك ، فاطمة ، زيب محمد (٢٠٢٣). الجرائم المستحدثة ضبط المفهوم وتحديد الأنماط ، مجلة الفكر القانوني والسياسى ، كلية الحقوق والعلوم السياسية ، جامعة عمار تسليجى ، الأغواط ، المجلد ٧ ، العدد ١ ، مايو .

٦٣. مجذوب ، محمد سعيد (٢٠١٤). النظرية العامة لحقوق الإنسان تطور الحقوق والحريات العامة الآليات القانونية لحمايتها ، المؤسسة الحديثة للكتاب ،بيروت ، لبنان ،الطبعة الأولى .

٦٤. مجمع اللغة العربية ، المعجم الوجيز (١٩٨٠). القاهرة ، دار التحرير للطباعة والنشر ، الطبعة الأولى .

٦٥. مدكور إبراهيم ، وآخرون (١٩٧٥). معجم العلوم الاجتماعية ، القاهرة ، الهيئة المصرية العامة للكتاب .

٦٦. المدنى ، خالد الشرقاوى (٢٠١٢). مكافحة الجرائم الإلكترونية في ضوء التشريعين الوطنى والدولى ، المجلة المغربية للإدارة المحلية والبحثية ، العدد ١٠٢ ، يناير– فبراير .

٦٧. مركز هردر لدعم التعبير الرقمى (٢٠١٨). التنظيم القانوني والجرائم الإلكترونية ما بين أمن المعلومات وتقييد الحريات ، مركز هردر ، القاهرة .

٦٨. مصطفى ، مصطفى جاد الحق (٢٠١٩). رؤية استراتيجية لمكافحة الجرائم السيبرانية ، اليمن ، دراسة حالة ، المجلة العربية الدولية للمعلوماتية ، اتحاد الجامعات العربية ، جمعية كليات الحاسبات والمعلومات ، مجلد ٧ ، العدد ١٢ .

٦٩. المصيلحى ، نجلاء احمد (٢٠١٨). برنامج مقترح من منظور الممارسة العامة في الخدمة الاجتماعية لوقاية الشباب الجامعى من جرائم الإرهاب الإلكترونى ، المؤتمر العلمى الدولى الحادى والثلاثون ، كلية الخدمة الاجتماعية ، جامعة حلوان ، مارس – أبريل .

٧٠. المطيري، مشاعل شبيب مطيران. (٢٠٢١). واقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. المجلة الدولية للدراسات التربوية والنفسية، *(٣)١٠*، ٦٥٥-٦٣٥.

٧١. منصور ، وحيد محمد (٢٠١٧). الجريمة السيبرانية في مجتمع دول مجلس التعاون لدول الخليج العربية ، دراسة تأصيلية ، مقدمة لجائزة الأمير نايف للأمن العربى ، المنامة ، البحرين.

٧٢. المنصورى ، سالم بخيت طربيش (٢٠٢٠). الجرائم الإلكترونية الماسة بالأشخاص ، مجلة القانون المغربى ، دار السلام للطباعة ، العدد ٤٣ ، يناير .

٧٣. موقع مديرية الأمن العام الأردنية على شبكة الإنترنت (٢٠٢٣). http://www.psd.gov.jo/index-php/ar.

٧٤. نظمى ، كرستينا لطيف (٢٠١٩). أنماط الجرائم الإلكترونية المرتكبة ضد الإناث دراسة تحليلية ، مجلة الاستواء ، جامعة قناة السويس ، مركز البحوث والدراسات ، العدد ١٤ .

٧٥. النويران ، تامر على (٢٠١٥). الجرائم الإلكترونية وطرق الحد منها تجربة الأردن ، المؤتمر الدولى الأول لمكافحة الجرائم المعلوماتية ، جامعة الأمام محمد بن سعود الإسلامية ، كلية علوم الحاسب والمعلومات ، نوفمبر .

٧٦. الهديب ، مفتاح ميلاد ، شنيب ، جمعة عبد الحميد أحمد (٢٠٢٢). الجرائم الإلكترونية ، جامعة المرقب ، كلية التربية بالخمس ،العدد ٢٠ ، يناير .

٧٧. الهديف ، مفتاح ميلاد ، شنيب ، جمعة عبد الحميد أحمد (٢٠٢٢). الجرائم الإلكترونية ، مجلة التربوى ،جامعة المرقب ، كلية التربية بالخمس ، العدد ٢٠ ، يناير.

٧٨. الهيئة الوطنية للأمن السيبرانى (٢٠١٨). الضوابط الساسية للأمن السيبرانى ، المملكة العربية السعودية (http:nacgovsa) .

٧٩. وآخرون ، نصيف فهمى منقريوس (٢٠٠٤). نماذج ونظريات في ممارسة خدمة الجماعة ، مركز نشر وتوزيع الكتاب الجامعى .

أولاً : المراجع الأجنبية :

٨٠. Venter, I.; Renette, J. Renaud, K. & Venter, M. (٢٠١٩). Cyber security education is as essential as “the three R's”. Heliyon ٥, e ٠٢٨٥٥, ١-٨.

٨١. Alemany, J.; Del Val, E.; Alberola, J. & García-Fornes, A. (٢٠١٩). Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. International Journal of Human-Computer Studies, ١٢٩, ٢٧-٤٠.

٨٢. Halder , D & Jaishankar , K (٢٠١١): Cybercrime and the victimization of women laws rights and regulations . Hershey PA . USA , ١٦ Clobal ds BW .

٨٣. Jalali, M.; Siegel, M. & Madnick, S. (٢٠١٨). Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment. *J Strategic INF Syst;* ٢٨ *(١)*, ٦٦-٨٢.

٨٤. Lee, K.; Chong, C. & Ramayah, T. (٢٠١٧). Website characteristics and web users’ satisfaction in a higher learning institution. *Int J Manage Educ;* ١١*(٣)*, ٢٦٦-٨٣.

٨٥. Nazilah, A.; Arifin, A.; Mokhtar, U.; Hood, Z.; Tiun, S. && Jambari, D. (٢٠١٩). Parental awareness on cyber threats using social media. Journal Komunikasi: Malaysian Journal of Communication, ٣٥(٢), ٤٨٥-٤٩٨.

٨٦. Zavrsmik , Ales (٢٠٠٠) : Cybercrime definitional challenges and crimminologic al particularities , masaryk university Journal of law and technology .

٨٧. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, L.; Cetin, F. & Basim, H. (٢٠٢٠). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, *Journal of Computer Information Systems*. Available online at: https://doi.org/١٠,١٠٨٠/٠٨٨٧٤٤١٧,٢٠٢٠,١٧١٢٢٦٩.

٨٨. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, L.; Cetin, F. & Basim, H. (٢٠٢٠). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems. Available online at: https://doi.org/١٠,١٠٨٠/٠٨٨٧٤٤١٧,٢٠٢٠,١٧١٢٢٦٩.