Journal of Al-Farahidi's Arts, No: 63: 359-380
Doi: https://doi.org/10.25130/jfa.17.63.16

P-ISSN : 2074-9554 | E-ISSN: 2663-811
Journal of Al-Farahidi's Arts
available online at : fja.tu.edu.iq/index.php/fja
Tikrit University
J.F.A
Journal of Al-Frahedis

Social Problems of Cybercrime in the Digital Era

Asst. Lec. Noor Muneer Basheer Eathab
E-Mail: noor.m.b@nahrainuniv.edu.iq

Keywords:
social problems, crime, cybercrime, Digital Era, Technological
Article history:

Received	28/5/2025
Received in revised form	2/6/2025
Accepted	3/7/2025
Available online	30/12/2025

E-mail Jaa@ tu.edu.iq

A B S T R A C T

This research deals with modern technology and the social problems facing individuals in the shadow of cybercrime, which is considered a soft crime that is difficult to prove and has a clear impact on the individual, the family, and society as a whole. The research focused on a number of objectives, including identifying cybercrimes in the digital age in terms of their history of emergence, characteristics, components, and types, and identifying the reasons that limit social problems, as well as the role of Iraqi law towards them. The descriptive analytical approach was adopted by using a questionnaire distributed to the selected sample. The research concluded that cybercrime causes family disintegration, weakens trust between individuals, and fragments social ties, especially in the absence of the implementation of laws that deter weak souls from committing crimes, as well as the absence of awareness programs or security study materials in schools or universities. The most important recommendations of the study are to have awareness and media programs and hold courses, in addition to enacting strict laws that limit the commission of such acts.

المشكلات الاجتماعية للجريمة المعلوماتية في العصر الرقمي

م.م. نور منير بشير عذاب / جامعة النهرين / رئاسة الجامعة

.

المستخلص:

يتناول هذا البحث التكنولوجيا الحديثة وفي اطار المشكلات الاجتماعية التي تواجه الافراد في ظل الجريمة المعلوماتية والتي تعتبر من الجرائم الناعمة التي من الصعوبة اثباتها والتي تسبب اثر واضح على الفرد و الاسرة والمجتمع ككل، وتم تركيز البحث على جملة من الاهداف منها التعرف على الجرائم المعلوماتية في ظل العصر الرقمي من حيث تاريخ ظهورها وخصائصها واركانها وانواعها، ومعرفة الاسباب التي تحد من المشكلات الاجتماعية ، وكذلك دور القانون العراقي تجاهها، وتم اعتماد منهج التحليل الوصفي التحليلي عن طريق استخدام اداة الاستبانة الموزعة على العينة المختارة وتوصل البحث الى ان الجريمة المعلوماتية تسبب التفكك الاسري وتضعف الثقة بين الافراد و تشتت الروابط الاجتماعية خاصة في غياب تطبيق القوانين التي تردع النفوس الضعيفة من ارتكاب الجريمة وكذلك عدم وجود برامج توعوية او مادة دراسية امنية في المدارس او الجامعات، واهم توصيات الدراسة هي ان يكون هناك برامج توعوية واعلامية واقامة دورات بالاضافة الى تشريع قوانين صارمة تحد من ارتكاب هكذا افعال .

الكلمات المفتاحية : المشكلات الاجتماعية، الجريمة، الجريمة المعلوماتية، العصر الرقمي، التكنولوجيا..

الفصل الاول : الاطار العام للبحث:-

اولاً: مشكلة البحث:-

مع ظهور التكنولوجيا الحديثة والتطور الذي يحدث والحواسيب الالكترونية والاجهزة الحديثة واعتماد الافراد على استخدامها بشكل اساسي وعدم تركها في جميع الاوقات وعلى جميع المواقع المتاحة فيها اذ تظهر مع ظهور هذه المواقع اساليب حديثة و مشكلات تواجه الاشخاص انفسهم فكل شي ذو حدين اما ان يتم استخدامه بالطريقة الصحيحة او يتم استغلاله بطريقة سيئة تضر الافراد في المجتمع ويحدث زعزعة في المجتمع يمكن ملاحظته حتى اصبحت مشكله من الصعب ايجاد حلول مناسبة لها، اذ تعتبر سبب ظهورها في المجتمع قله الوعي او سوء استخدام او التسبب بأضرار بسبب ضعف القانون وقله الخبرات التكنولوجيا وصعوبة معرفة الجاني كل ذلك يعتبر تسهيل للجاني في استغلال الضحية من الممكن تكون هذه الجريمة من خارج البلاد ولا يمكن التعرف عليه حتى، وله تأثير على البنى التحتية سواء الاجتماعية او النفسية او الثقافية فمن الممكن ان يؤثر اجتماعياً عن طريق الابتزاز او الاحتيال وتؤثر نفسياً عندما لا يوجد حلول خاصه اذا لم يتم التعرف عليه بالتالي يسبب مشكلات نفسية للمجنى عليه اما المشكلات الثقافية فهي تؤثر بشكل كبير على المجتمع ككل من الناحية الثقافية و الدولية عن طريق نشر المواقع المخلة بالاداب العامة، فهي تؤثر على الروابط الاسرية والاجتماعية لعدم وجود شعور الامان فيها.

ثانياً: اهمية البحث:-

مع ارتفاع نسب الضحايا و كثر المشكلات التي نراها اليوم في مواقع التواصل الاجتماعي في اغلب المجتمعات يجعل من هذا الموضوع مشكلة يجب دراستها والبحث في اسبابها وابعادها فمن المهم النظر الى ابرز الاثار الاجتماعية التي تسببها الجريمة المعلوماتية على الروابط الاسرية والاجتماعية والثقافية وفقدان الثقة فيما بينهم بالاضافة الى توعية المجتمع بها وبالمخاطر التي تسببها دون معرفتهم عن طريق التكنولوجيا المستخدمة وكيف يمكن الحد منها والوقوف على الاسباب وخاصة تأثيرها على الاطفال والمراهقون اذ هم الفئة الاكبر في الاستغلال وقله الخبرة لديهم مما يسهل على الجاني استغلالهم و الوقوع ضحية، ومن المهم ان يتم التطرق لهذه المشكلة وكيفية محاربتها او التعامل معها عند الحدوث بطرق مختلفة سيتم التعرف عليها عند الدراسة .

ثالثاً: اهداف البحث:-

1. التعرف على الجرائم المعلوماتية في ظل العصر الرقمي من حيث تاريخ ظهورها وخصائصها واركانها وانواعها.
2. معرفة الاسباب التي تحد من المشكلات الاجتماعية للجريمة المعلوماتية .
3. معرفة موقف القانون العراقي تجاه الجريمة المعلوماتية.

الفصل الثاني: المفاهيم والمصطلحات

الجريمة (Crime): تعرف الجريمة هي كل فعل ضار بمصالح الجماعة، ومناط تكييف الفعل بأنه إجرامي من عدمه ليس النص التشريعي إنما مبادئ القيم الاجتماعية والأخلاقية التي تسود الجماعة(رزيقي،2015) بما يعني ان السلوك الذي صدر من فرد في المجتمع انما ينتج من تصرفاتهم ويضر شخص اخر يعتبر جريمة .

وهناك تعريف اخر للجريمة: اذ تعرف بأنها أي فعل او سلوك يصدر عن الانسان سواء كان ناتج عن دوافع نفسيه أو ماديه أو عاطفيه يؤدي الى انتهاك الأخلاق أو الأعراف الاجتماعية والتقاليد المتعارف عليها أو القوانين والشرائع السماويه و المعتقدات (حمدي، 2013)، يُعد جريمة اي انها اي سلوك منحرف او جنوح يؤدي الى ارتكاب عمل منافي للاخلاق والقانون.

الجريمة المعلوماتية (Cybercrime): عُرفت بأنها سلوك غير قانوني يتم فيه استخدام الحاسوب كأداة اساسية لارتكاب الفعل الاجرامي لا يمكن ان تعرف الجريمة المعلوماتية لكون العالم في طور التقدم وحدوث الجرائم الالكترونية او المعلوماتية حسب ما سميت كونها تتعلق بالمعلومات الشخصية للفرد التي يمكن ان يتم اختراقها او استخدامها بطريقة غير قانونية واضرار الفرد بها وظهرت هذه الجرائم(المومني، 2010).

تعرف الجريمة كذلك بأنها: اي تصرف يصدر يخالف القوانين يتم بأستخدام الاجهزة الالكترونية يؤدي الى حصول الجاني على مكاسب مادية او معنوية مع تحميل الضحية خسارة مقابلة وغالباً ما تكون الغاية منها هي تحقيق مصلحة غير مشروعة كالسرقة او اتلاف المعلومات او ابتزاز الضحايا (عبدالرحمن، مارني، 2018).

الامن السيبراني (Cybersecurity): يعرف بأنه منظومة متكاملة تضم الأدوات والسياسات والمفاهيم والضمانات الأمنية اضافة الى المبادئ الارشادية ونَهج إدارة المخاطر والتدريب الى جانب أفضل الممارسات والتقنيات الحديثة المستخدمة التي يمكن استخدامها في حماية الفضاء

السيبراني المنظم، بما في ذلك أنظمة الاتصالات والتطبيقات والخدمات و تجهيز الحواسيب الموصولة والبنية التحتية (العوادي ،2016)، اي هي عبارة عن مجموعة من الانظمة يديرها اشخاص للمحافظة على معلومات الافراد من الاختراق والذين تقل خبراتهم في استخدام المواقع ويتم مشاركة بياناتهم الشخصية عن طريق الخطأ او عن طريق الاختراق الغير قانوني.

العصر الرقمي (Digital Era): يدل مصطلح " الرقمي " الى التكنولوجيا الإلكترونية التي تستخدم في انتاج البيانات وتخزينها ومعالجتها و يمكن تجهيز البيانات في حالتين: الاولى إيجابية والثانية غير إيجابية ويتم التعبير عن الاولى أو يمكن تمثيلها بالرقم (١)، بينما يتم التعبير عن النوع الاخر أو تمثيلها بالرقم (صفر) ومن ثم، فإن البيانات التي يتم ارسالها أو حفضها بالتقنيات الرقمية يتم التعبير عنها كسلسلة من الأصفار والآحاد و كان نقل البيانات الالكترونية يقتصر على التقنيات التناظرية، التي تعمل على نقل البيانات بشكل إشارات إلكترونية مثال ذلك الإذاعة والنقل الهاتفي، ومع ظهور الحاسبات والإنترنت وتقنيات المعلومات الاخرى، اصبحنا نعيش ملامح العصر الرقمي بشكل جلي، اذا تشمل ايضاً البحث والتطوير المتصلة بتنظيم المعلومات واسترجاعها، التي تنتج في البيئة الرقمية (هتنج تشو، 2018).

عصر التكنولوجيا (Technological Era): يمكن تعريفها بأنها مجمل المعارف والخبرات المتراكمة والمتاحة والأدوات والوسائل المادية والإدارية والتنظيمية، المستخدمة في جميع المعلومات ومعالجتها وإنتاجها وتخزينها واسترجاعها ونشرها وتبادلها، أي توصيلها إلى الأفراد والمجتمعات (السيد، 2022).

وبمعنى اخر هي عبارة عن علم الذي يحقق حرف وصناعات وفنون متنوعة وغير محدودة بواسطة الحاسب الآلي والاجهزة التي لها علاقة به.

الفصل الثالث : المبحث الاول

اولاً: نبذه تاريخية عن بداية ظهور الجرائم المعلوماتية :-

يرجع تاريخ الفقه الجنائي جرائم الحاسوب إلى العام (1960) و ترتبط هذه المرحلة بظهور استخدام الكمبيوتر وربطه بشبكة الإنترنت، وكان ذلك في الستينيات من القرن الماضي، وتميزت هذه المرحلة بعدم الانتشار الواسع النطاق للأجهزة، مما أدى إلى رصد عدد قليل من

الجرائم التي ارتكبها رجل واحد إلى ثلاث جرائم سنويًا، كما أن طريقة معالجة هذه الجرائم كانت في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة، والتدمير الذي يمس أنظمة الكمبيوتر والتجسس، وأما جرائم الإنترنت، فإنها بدأت مع بداية عام (1988) حيث شهد عقد الثمانينيات ارتفاعًا في معدل الجرائم السيبرانية، بحيث بدأ ظهور جديد من الجرائم المرتبطة بالعلاج النفسي، وثم اقتحم نظام الكمبيوتر عن طريق نشر الفيروسات عبر شبكات الكمبيوتر، مما تسبب في تدمير الملفات والبرامج، حيث شاع في هذه الفترة مصطلح الهاكرز، وهو مصطلح يطلق على ما يكفي من النظم، وتعتبر قضية موريس الشهيرة من بين أهم القضايا عبر الآلاف في فترة الثمانينيات حيث تم نشر فيروس إلكتروني عرف بدودة موريس لأجهزة الكمبيوتر من خلال الإنترنت، وما يزال الفقه والتشريع المقارن يستشعر التمييز بين كل من جرائم الحاسوب وبين تلك التي وقعت عند استخدام الإنترنت، حتى إن تقرير الأمم المتحدة عن منع الجريمة عام 1995 يتبنى موقف المقارن الذي واجهه هذا حيث شهدت فترة التسعينات تطوراً هائلاً في مجال الجريمة السيبرانية وبدأت في نطاقاتها ومفاهيمها حيث أصبحت مواقع الإنترنت التسويقية أكثر اندفاعاً للهجمات التي ظهرت بسبب أنماط جديدة من التسلل، ففي عام 1995 تم اختراق موقع البيت الأبيض الأمريكي، لتليها بعد ذلك العديد من الحوادث كحادث شركة أوميجا فيروس وغيرها، ومن أبرزها في هذه المرحلة صبي بريطاني قام بإختراق شبكات الحواسيب العسكرية الأمريكية، وكشف عن أدق الاتصالات مما جعل المرشحين الديمقراطيين أكثر عرضة للاختراق من شبكات الكمبيوتر (الديربي، 2012). وشهدت الفترة الممتدة من سنة (2000) إلى حد الآن، حيث واكبها تطورات كثيرة ومتسارعة مع الانتشار المتزايد لاعداد مستخدمي الانترنت وتطور ادوات الجرائم الرقمية، وضخامة الخسائر المالية، اصبح من الضروري تكثيف الجهود الوطنية والدولية لمواجهة هذا النوع من الجرائم،فعلى سبيل المثال بلغ عدد سكان العالم 6.28 مليار نسمة في عام 2002، وعدد 662 مليون مستخدم للانترنت، ورغم ذلك لم تتفاعل حكومات دول العالم بالقدر المطلوب لتوفير الحماية اللازمة من الاجرام السيبراني، بالرغم من أنها صارت تعتمد بشكل أساسي على شبكات الحاسب الآلي في القطاع العام والخاص وعلى مستوى الافراد، وبعد الهجمات الإلكترونية الشهيرة على دولة إستونيا عام 2007 ، إنتبهت الكثير من الدول لهذا الخطر الذي يدمر قراصنة الكمبيوتر وتقنية الاتصالات والشبكات، ويعطل كل شيء حيوي، فبدأت الدول

التفكير بجدية في إعداد إستراتيجيات للامن السيبراني (الحسبان، الخزاعله، 2024). ولقد كبرت وتوسعت إدارة العدل الأمريكية في ربط الحاسوب بالتقنيات الحديثة ككل، واشار الباحث الامريكي الى وجود ثلاثة انماط من الجرائم الرئيسية ، وهي:

أولا : الجرائم التي يعد الحاسوب فيها الهدف الرئيسي

ثانيا : الجرائم التي الحاسوب فيها اداة لارتكابها.

ثالثا : الجرائم التي يكون فيها الحاسوب وسيلة لحفظ البيانات او تحويلها عبر الشبكات دون أن يكون هناك وسيط في الحصول عليها (الديربي، ص25).

ثانياً: خصائص الجريمة المعلوماتية :-

وتتكون الجريمة الإلكترونية من عدة خصائص أهمها:

1 – **عالمية الجريمة:** اي أنها لا تقتصر على نطاق جغرافي معين اذ انها تتصف بالعالمية، وذلك بسبب امتداد اثارها الى خارج حدود الدولة بسهولة عن طريق شبكة الاتصالات العالمية " الانترنيت" اذ يمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم لهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر، وهذا ما يجعل مكافحتها امر بالغ الصعوبة (المصري، 2012)، أي لا تأتي هذه الجرائم في نتيجتها إلا باستخدام الوسيلة وهي كركن حاسب وشبكة معلوماتية مفترضة للتحقق منها (البقلي،2010).

2– **صعوبة الإثبات:** تعد متابعة الجرائم الالكترونية واكتشافها امراً معقداً نظراً لانها لاتترك اثراً او ادلة مادية واضحة، بل تقتصر اثارها غالباً على تغييرات رقمية في السجلات، فغالباً ما يتم اكتشافها بالصدفة وبعد فترة طويلة من ارتكابها، تفتقر إلى الدليل المادي التقليدي كالبصمات مثلاً (رستم،2019).

3– **جرائم سهلة الإيقاع:** اي بمعنى إذا كانت الجريمة تقليدية تحتاج الى مجهود عضلي في ارتكابها، كالقتل والسرقة، والاغتصاب، فالجرائم إلكترونية لا تحتاج ادنى مجهود عضلي بل تعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم عن معرفة تقنية بالحاسب الالي وتكون الجرائم الكاملة لا يتصور الشروع بها، اي أن الشروع يمثل في الغالب جريمة أخرى وهي حياة صور أو أفلام أو منشورات أو مواقع تحتوي على ما يجرمه القانون، أما الصور الأخرى فلا يتصور الشروع بها لعدم إمكانية الضبط البدء في التنفيذ لعدم التواجد الجسدي بين

الجاني والمجني عليه، بل ترتكب بوسيلة إلكترونية تجرم الأفعال التي أتاها الجاني بسلوك مادي (البقلي،2010).

ثالثاً: اركان الجريمة المعلوماتية :-

لا تختلف الجريمة الالكترونية، عن أي جريمة أخرى، إذ أنها تتطلب لتحققها اكتمال الأركان المتفق عليها، و قد انقسم الفقة الجنائي الي مذاهب شتي في تحديد اركان الجريمة، الركن شرعي والركن المادي والركن المعنوي، وهناك من يكتفي بوجود الركنين المادي و المعنوي فقط اما الركن الشرعي فيعتبرونة شرطاً اولياً للتجريم ومن شروط التجريم التي يتعين البحث في توافرها قبل البحث في اركان الجريمة ذاتها (الشاذلي، 1998). اي بمعنى لابد من وجود ركن مادي للجريمة المعلوماتية لاثبات جريمة الفاعل (المجرم) بشكل ملموس، وايضاً وجود الركن المعنوي يعبر عن ارادة المجرم المعلوماتية.

1. الركن المادي للجريمة:

إن النشاط أو السلوك المادي في جرائم الالكترونية يتطلب وجود بيئة رقمية واتصال عبر الإنترنت، ويتطلب أيضًا معرفة بداية هذا النشاط والروع فيه ونتيجته، ويقوم بنشر برامج كمبيوتر متميزة، أو أن يقوم بتنقية هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلوطة بالآداب العامة، وتحميلها على الجهاز المضيف الخادم، كما يمكن أن يقوم بجريمة إعداد برامج الفيروسات تمهيدًا لبثها، لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية، والحقيقة كما هو الحال مع اثنين، أنه يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإلكترونية حتى لو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر مختلفًا بعض الشيء، ففساد برامج الاختراق، وبرامج الفيروسات، ومعدات فك الشفرات وكلمات المرور، وحياة صور للأطفال فمثل هذه الأشياء تمثل جريمة في حدها (محمد،2025).

واشاره اخرون الى ان الركن المادي هو عبارة عن فعل ظاهري والذي يبرز فيها الجريمة ويعطيها وجودها وكيانها في الخارج(حسني، ص32). اذ يعتمد هذا الركن على ثلاث عناصر اساسية وهي الفعل والذي يراد به، والنتيجة يقصد بها الاثر المترتب على السلوك الاجرامي، اما العلاقة السببية فهي تلك الرابطة التي دفعت الجاني الى الاتيان بهذا الفعل وما يترتب عليه فيما بعد(لطفي،2020).

2. **الركن المعنوي للجريمة:** هو الحالة النفسية للجاني، اي بمعنى العلاقة التي تقع بين ماديات الجريمة وشخصية الجاني، ويطلق البعض عليه الركن الادبي أو الشخصي وهو المسلك الذهني أو النفسي للجاني، وقد بدأ المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم (محمد،2025)، اي هو وجود سوء نية، وإرادة حرة لمعرفة يقين للولوج في الشبكة المعلوماتية، وإحداث أضرار بها، ويقسم الركن المعنوي في الجريمة الإلكترونية إلى الاعتداء على نظام التشغيل لخلق مشكلة تؤدي إلى إبطاء النظام في تنفيذ العمليات المطلوبة، والدخول غير المرخص لأنظمة المنظمة الإلكترونية، ويتم هنا تدمير البيانات والمعلومات كلياً الموجودة في النظام، وما يكون عائقاً أمام المنظمة في تنفيذ عملياتها أو الحد من اتخاذ القرارات السليمة (حبابية،2022) ، اذ يعتبر من الأركان المهمة لقيام المسؤولية الجزائية، فهذه الجريمة لا تقوم إلا عمدية، واتجاه إرادته لارتكاب جريمة الغش عن طريق الدخول في الجهاز الرقابي الذي يحمي النظام، أما جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات هي جريمة عمدية لأن أفعال العرقلة والتعطيل من الأفعال العمدية، فالجريمة بأنواعها تتطلب لارتكابها وجود القصد العام أي علم إرادة ولا يكفي لقيام الجريمة تحقق الركن المادي فحسب بل لا بد من أن يكون الفعل أو الامتناع وليد إرادة حرة، وتكون الارادة الحرة صادرة ممن يملك أهلية جنائية وهي ما تعرف بالأرادة أو التمييز، حيث تتجه إرادة الجاني إلى إرتكاب خطأ مقصود فتقوم الجريمة العمدية أو خطأ غير مقصود وحينها تنشأ الجريمة غير عمدية، فالقصد الجرمي يتحقق بإرادة الفعل وإرادة النتيجة التي حققها السلوك، إضافة الى العلم بأركان الجريمة كما عرفها القانون، ويشترط بالعلم الذي هو أحد عناصر الركن المعنوي أن يكون معاصراً لفعل الدخول واتجاه الارادة لإرتكاب الفعل (العتيبي،2014).

رابعاً: انواع الجرائم المعلوماتية :

1. **الاختراق وانتحال الهوية :** من الممكن الاختراق او سرقة الهوية وانتحالها اما مادياً او الكترونياً فالاختراق المادي يسمح بالدخول إلى مناطق خاضعة للسيطرة عن طريق بوابات إلكترونية أو آلية، وأسلوب الاختراق المادي هو أن يكون الشخص غير مسموح له بالدخول أمام البوابة المغلقة حاملاً بين ذراعي متعلقة بالكمبيوتر الآلي كالشرائط الممغنطة أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب

ويدخل معه في الوقت نفسه (رسلان،2016) اما المقصود بانتحال الهوية اغتصاب الهويات سرقة شخصية مستخدم آخر ويتطلب الوصل إلى الحاسب الآلي أو إلى الأطراف كشف دقيقة لم يتم استخدام الجهاز، وإن فحص الهوية يرتكز على مجموعة معلومات متوافقة تستخدمها ككلمة السر أو أي جملة خاصة بالمستخدم أو أي خاصية كالبصمة الرقمية أو ملامح الوجه أو هندسة الكف أو الصوت بالإضافة إلى أي شيء يمتلكه المستعمل كالمغناطيس أو المفتاح المعدني او حتى صورة شخصية وعن طريقها انشاء حساب بأسمه..الخ(ابراهيم،2010).

2. **الاحتيال الالكتروني :** ويعني ان يدفع الفرد إلى الإفصاح عن معلومات شخصية قد تضر به، وتكشف للغير ما لا يود كشفه، مثال ذلك كلمة المرور، واسم المستخدم، وأرقام بطاقة الائتمان، ومعلومات عن حسابات بنكية ... الخ، وللتمويه تظهر رسائل الاحتيال وكأنها أرسلت من مؤسسات تتعامل كالبنك، وخدمات تشترك فيها كاليوتيوب You tube أو الفيس بوك Facebook مثلاً، وتقدم رسالة الاحتيال رابطاً إلى موقع ويب كأنه الموقع الحقيقي، وبمجرد أن تدخل إلى موقع الويب يطلب منك إدخال معلومات شخصية لتسجيل الدخول أو التحقق من هويتك، واستخدام هذه المعلومات من قبل أشخاص لغايات غير شرعية ولا قانونية، مما قد يتسبب في وقوع عمليات احتيال مالية مما تسبب خسارة كبيرة(وداعة الله،2020).
3. **نشر البرامج الخبيثة:** البرمجيات الخبيثة وتشمل أي برنامج مصمم لأهداف غير مشروعة، ويتم تشغيله على حاسوب المستخدم دون علمه ولا رضاه، ويتراوح أذى هذه البرمجيات من مجرد إزعاج بسيط الى ازعاج اكبر مثال ذلك بعض النوافذ الإعلانية غير المرغوب بها التي تسبب أذى للمستخدم وأدلته وبياناته، وقد يتطلب الأمر إعادة تهيئة القرص الصلب من جديد على سبيل المثال، ومن أمثلة هذه البرمجيات الفيروسات والديدان، وأحصنة طروادة ... إلخ. وهذه البرمجيات لا يتم شراؤها، ولا يسبب خلل في الحاسوب، بل هي برمجيات صممها مبرمجون أو شركات بشكل متعمد ومحترف ومتقن، بالإضافة إلى تصميم هذه البرمجيات ونشرها جريمة من الناحية القانونية العالمية، وبنفس الطريقة من الناحية الشرعية (Itmazi,2018). اذ تتميز هذه الحزمة بالاستمرارية والتخفي، حيث يتم تصميمها من أنظمة الحماية والبقاء داخل الشبكة ويستخدم هذا البرنامج

أيضًا مجموعة للهجوم، مثل إلغاء الاشرطة الأمنية وملفات ضارة عبر البريد الإلكتروني لأدوات اختراق البريد الإلكتروني وتستخدم في عمليات الاحتيال المالي وسرقة الهوية (عبدالحق، عبدالعال،2025).

4. **التشهير والابتزاز الالكتروني:** قد يأخذ الابتزاز الالكتروني عدة صور من اهمها ان يكون الابتزاز بشكل عاطفي او بشكل مادي او على شكل استغلال لتحقيق مصالح ذاتية او حتى عن طريق استغلال المعلومات الشخصية او معلومات دولية او تخص مصلحة عامة وذلك يكون بسبب دوافع مالية او دوافع غير اخلاقية جنسية او دوافع انتقامية او دوافع خارجية ويرجع سبب هكذا افعال اما ان يكون بسبب ضعف الوازع الديني عند المبتز او سهولة التصوير او التقاط الصور الفاضحة اوضعف الوازع الاخلاقي او سوء الاوضاع المادية والاقتصادية للمجرم مما يدفعه لارتكاب هذه الافعال(سلبي،2021).

5. **التحرش الالكتروني:** يعد التحرش الإلكتروني واحداً من الممارسات السلبية الشائعة التي تُستخدم خاصةً على مواقع التواصل الاجتماعي؛ حيث يقوم المتحرش الإلكتروني مع الضحية بشكل متكرر وغير مرغوب فيه، كما يقوم بتتبع كافة أنشطة الضحية على الإنترنت بقصد الإزعاج وإحداث الضرر النفسي للضحية أو تهديدها، أو إذلالها أو أخذها بالثأر منها، ويعد الفارق الجوهري بينه وبين الابتزاز الإلكتروني هو حرص المتحرش على تعريف الضحية بما يقوم به من تتبع لأفعالها، حتى يرى ردود أفعال الضحية ويشعر بنجاحه في إزعاج ضحيته ويتم ذلك من خلال عدة أدوات منها نشر رسائل نصية وتعليقات على مواقع التواصل الاجتماعي، أو إرسال بريد إلكتروني، أو نشر صور توضيحية للضحية على مواقع التواصل الاجتماعي أو على الهاتف المحمول، وظهرت العديد من الحملات الإلكترونية لتتبع المتحرشين سواء في العالم الافتراضي أو في الواقع من خلال نشر المعلومات المتاحة عن الشخص وصوره والفيديوهات التي تؤكد ما قام به من تحرش حتى يتم منع هذه الظاهرة من الانتشار اكثر (خليفة،2016).

6. **الجرائم الاخلاقية عبر الانترنت:** تقوم شبكات المعلومات ووسائل تقنية المعلومات بتدمير واسع في نقل المواد المرسلة واستقبالها بحيث تصل إلى الإنسان في مجلسه

دون أن يغير مكانه وقد تصبح هذه الوسائل التقنية هي بمثابة الثورة الثالثة التي اجتاحت العالم بعد الثورتين الزراعية والصناعية، إلا أن البعض أساء استخدام هذه الوسيلة، فقد وجد القائمون على نشر هذه الصور من الرذيلة وترويجها في شبكة الإنترنت ووسائل تقنية المعلومات والقدرة والكفاءة على الترويج لبضائعهم الرخيصة مما أفرز مجموعة من الجرائم باتت تهدد الأخلاق والآداب العامة في المجتمع وكان من الضروري التصدي لهذه الصور الإجرامية، ولم يجحد الشارع حق الأفراد في التمتع بحرية المعلومات والاستفادة من وسائل تقنية المعلومات طالما كان في الحدود القانونية الغير ماسة بالآداب العامة والقواعد الأخلاقية فإذا ما تضمنت سلوكاً ماساً بالآداب فخرج هذا السلوك عن إطار العادات والتقاليد المشروعة اندرج تحت طائلة التجريم لما فيه من مساس بممارسة الآخرين وخصوصيتهم وحقهم في الحفاظ على الجسد والأخلاق والحياء(البقلي،2010)، فما نراه اليوم على مواقع التواصل الاجتماعي يجعلنا في حذر دائم لما له من اثار سلبية على المجتمع ككل والاطفال بشكل خاص.

7. **القرصنة الفكرية:** مع تزايد الجدل وتشعب مواضيعه طرح مفهوم السرقة في الأعمال الأدبية وان من يقتبس النصوص دون اذن من أصحابها إلا أن هناك فرق بين التعريفين فالسرقة والقرصنة تعتبر جريمة وسرقة صريحة تحرم صاحب العمل الشرعي من جنى ثمار جهده، في حين أن اقتباس النصوص دون إذن من أصحابها أعتبر مجرد سوء أخلاق وليست جريمة وهي قضية فرضت سرعة إصدار قانون حقوق الملكية الفكرية خصوصاً وأن اثارها في الأبحاث العلمية والطبية كان أكثر فداحة منها في الأعمال الأدبية (هياناثان،2004)
8. **جريمة الارهاب السيبيراني:** وتعرف بأنها لا تحتاج عند ارتكابها إلى العنف والقوة بل يتطلب حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة وتكون جريمة إرهابية متعدية الحدود وعابرة للدول والقارات وغير خاضعة لنطاق إقليمي محدد ومن الصعوبة اكتشاف جرائم الإرهاب الإلكتروني بسبب نقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذه الجرائم بالاضافة الى صعوبة الإثبات نظراً لسرعة غياب الدليل الرقمي وسهولة اتلافه وتدميره ويتم بتعاون

أكثر من شخص على ارتكابه تسمى بالخلية ومن المحتمل يكونون الاشخاص منتشرين في اكثر من مكان او دولة ومن الممكن يكون من ذوي الاختصاص في مجال تقنية المعلومات أو من شخص لديه على الأقل قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية(كمال،2022).

9. **جرائم ضد الدولة :** ان الطبيعة الخاصة التي تتمتع بها جرائم أمن الدولة والقدرة على وقوع العديد منها عن طريق الوسائل المقروءة ، فهي تعتبر جرائم ملائمة لتقع فيها الوسائل الإلكترونية سواء فيما يتعلق بأمن الدولة الداخلي أو الخارجي ، مثل جرائم التجسس والإتصال بالعدو ، والجرائم الماسة بالوحدة الوطنية (جاسم،2019).

المبحث الثاني : اسباب المشكلات الاجتماعية وعلاقتها بالجريمة المعلوماتية:-

ترجع اسباب المشكلات الاجتماعية والاسرية والتفكك الذي يحصل بها الى اسباب عدة ترجع ايضاً الى علاقتها بالجريمة المعلوماتية وكيف يمكن ان تؤثر على الروابط الاسرية وحتى الاجتماعية بشكل عام، ومن اهمها :

1. **التحضر**: اذ يعنى التحضر من الاسباب العامة للجريمة المعلوماتية حيث الهجرة التي حدثت من الريف الى المدينة المناطق الحضرية حيث يواجه الشباب صعوبة المعيشة في هذه المدن وصعوبة التأقلم لما لها من بيئة مختلفة و نظام حياة صعب.
2. **الفقر والبطالة** : وترجع الاسباب ايضاً الى انتشار الفقر بشكل كبير في المجتمع العراقي وترجع اسبابه ايضاً الى كثرة البطالة لدى الشباب مما يسبب التفكير في احداث جريمة معلوماتية في سبيل الحصول على المال بأي طريقة كانت (كالقرصنة او الاحتيال او الابتزاز).
3. **ضعف الوعي الثقافي والتعليمي** : عدم المعرفة التامة بالتكنولوجيا الحديثة وكيفية استخدامها بالطريقة السليمة والصحيحة التي لا تمس الاخرين بضرر عن طريق اما التجسس او النشر المسيئ او الفضائح الالكترونية التي نراها اليوم على مواقع التواصل الاجتماعي(البدانية،2014).
4. **التفكك الاسري والفراغ العاطفي**: نرى هنا اما ان يكون السبب غياب الرقابة الاسرية وعدم الاهتمام بتربية الابناء وعدم وجود علاقة اسرية فيما بينهم و العولمة هي ما تسبب الفراغ الاسري والعاطفي مما يؤدي الى انجراف المراهقون سواء من الذكور او الاناث

نحو الجرائم المعلوماتية او الانضمام الى الاصداقاء السيئين مما يسهل استغلالهم لعدم خبرتهم الكافية بالافراد (احمد،2000).

5. **ضعف القانون:** عدم تشريع قانون صارم او ضعف تنفيذ القوانين يدفع الافراد الى استغلال هذا السبب مما يشجع على ارتكاب الجرائم الالكترونية بشكل اكبر بدون خوف من العقاب (البهنساوي،2025).
6. **الضغط النفسي والانحراف:** ان عدم الشعور بالتقدير وضعف العلاقات بين الافراد الاسرة والتهميش يدفع الفرد الى ابراز قدراته بطريقة غير قانونية ومخلة بالاداب العامة مما يدفعه الى الانتقام بأستخدام الانترنيت اما عن طريق الاختراق واخذ المعلومات الشخصية او التهديدا او الابتزاز او حدوث فوضى مجتمعية عن طريق نشر الشائعات لسد النقص الحاصل داخله(فكية،2019).

المبحث الثالث :- موقف القانون العراقي تجاه الجريمة المعلوماتية (قانون العقوبات):

بدأ مشروع سن قانون محاربة ومكافحة الجرائم المعلوماتية في كيفية استخدام شبكات المعلومات واجهزة الحاسوب والانظمة الالكترونية وكان قراءة المقترح امام مجلس النواب في يوم 27/يوليو/2011، وعدل اكثر من مرة اذ ينص المقترح على "توفير الحماية القانونية للاستخدام المشروع للحاسوب وشبكة المعلومات ومعاقبة مرتكبي الافعال التي تشكل اعتداء على حقوق مستخدميها" واخذ القانون يفرض عقوبات على كثير من مستخدميه مما اثار جدلاً واسعاً واخذ نطاق واسع غير خاضع لقواعد ودون الرجوع الى معايير محددة مما يعني تقليص للحريات والتعبير عن الرأي(ووتش، 2012)، وذلك فأن القانون العراقي رقم (111) لسنة 1969 لا يقتصر في استهدافه على نطاق محدود انما جرم افعال استخدام الحاسوب مع افعال اخرى اكثر اتساعاً بالاضافة الى غياب الضمانات القانونية الكافية، اي بمعنى لا يوجد قانون يجرم الجريمة المعلوماتية بالمعنى الصريح الى وقتنا الحاضر ولايزال قيد المناقشة في مجلس النواب مايو/2025 منذ تقديمه لاول مره عام 2011 ومع ذلك صادق العراق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب قانون 31 لسنة 2013 والذي نشر في جريدة الوقائع العراقية ذي العدد(4292 في 2013/9/30) اذ تعد هذه الاتفاقية جزء من الاطار القانوني الذي يستخدم حالياً لمكافحة الجرائم المعلوماتية وتطبق حالياً احكام قانون

العقوبات العراقي رقم (111) على الجرائم الالكترونية بالاستناد الى المواد العامة التي يمكن استخدامها .

الفصل الرابع: الجانب الميداني :-

1. **ادوات البحث :** تم الاعتماد في جمع البيانات على اداة الاستبيان وذلك نظراً لملاءمتها طبيعة الدراسة واهدافها وتم وضع اسئلة بشكل منطقي تغطي محاور الدراسة بشكل كامل لما لها من اسئلة مغلقة ووشبه مغلقة ومفتوحة لتسهل عليه الاجابة.
2. **مجالات البحث :**

أ المجال المكاني للبحث: اذ تحدد في بغداد / جامعة النهرين – المجمع الجنوبي التابع الى وزارة التعليم العالي والبحث العلمي .

ب المجال الزماني للبحث: بدأ في شهر اذار/ 2025 وحتى شهر نيسان /2025.

ت المجال البشري للبحث: تم اخذ العينة بشكل عشوائي من الجامعة بواقع (92) من الذكور والاناث.

3. **منهج البحث :** اعتمدت الدراسة على المنهج الوصفي وذلك لوصف المشكلة الاجتماعية بدقة وتحليل ابعادها من خلال جمع البيانات الميدانية بما يتناسب مع اهداف البحث من حيث دور الجريمة المعلوماتية في التأثير على البيئة الاجتماعية والاسرية بغرض الوصول الى اسباب ونتائج وتوصيات من الممكن الاستفاده منها اما بتوخي الحذر من المسببات او ايجاد الحلول المناسبة التي تقي افراد المجتمع في المستقبل ومن الممكن تطويرها.
4. **مجتمع البحث:** وهم التابعين الى جامعة النهرين من الذكور والاناث وهم طلبة البكالوريوس وطلبة الماجستير وبعض الموظفين ايضاً وتم اختيارها بشكل عشوائي والبالغ عددهم (92) اذ تعتبر هذه النسبة قليلة جداً مقارنة بأعداد الافراد في الجامعة.
5. **تحليل مجتمع البحث وعينته :**

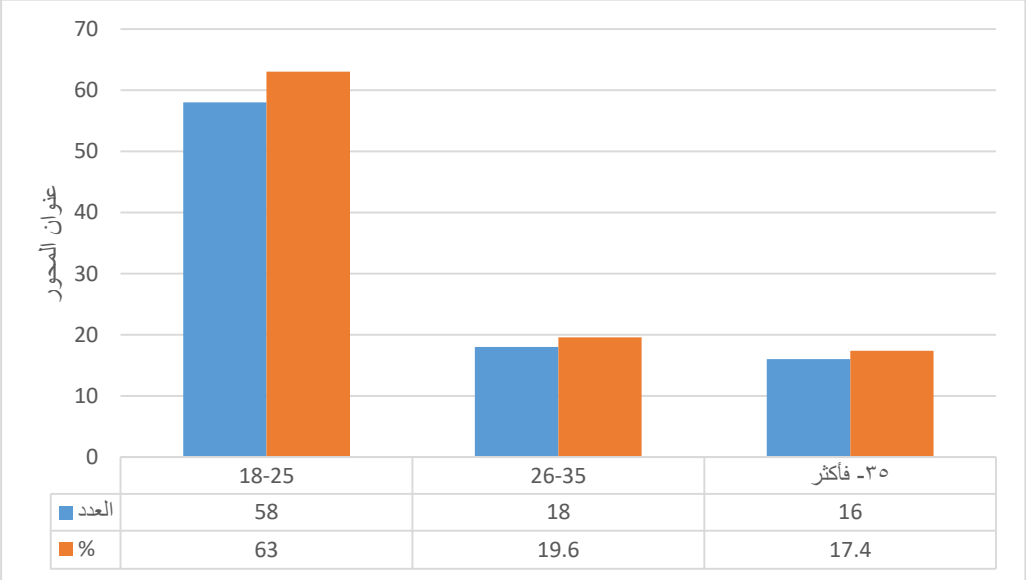
تم استخدام قانون اختبار t لعينات واحدة :(One-Sample t-test) لاختبار فرضيات الدراسة وكذلك استخدام المتوسط الحسابي والانحراف المعياري للبيانات العددية .

المحور الأول : البيانات الاولية

1. الجنس		
الاجابات	العدد	%
ذكر	27	29.3
انثى	65	70.7
المجموع	92	100

من خلال الجدول اعلاه يتضح ان العينة بلغت (92) من الذكور والاناث وبلغ عدد الذكور (27) من اجمال العينة، وبلغت الغالبية من الاناث اذ بلغ عددهم (65) اي بنسبة 70.7% .

المتوسط الحسابي للعمر هو 27.35 سنة، والانحراف المعياري هو 8.81 جدول رقم (2)



يوضح الرسم البياني اعلاه، وحسب التوزيع النسبي بين الافراد اذ يبين ان الفئة الاكثر هم الاعمال التي تتراوح بين (18–25) اذ بلغت نسبتها (63%) .

3. المستوى التعليمي		
الاجابات	العدد	%
اعدادي	10	10.9
بكالوريوس	62	67.4
دراسات عليا	20	21.7
المجموع	92	100

الجدول رقم (3) يوضح التوزيع النسبي للتحصيل العلمي للمبحوثين حيث تبين ان اعلى نسبة من المشاركين هم الحاصلين على شهادة البكالوريوس وبلغت نسبتها (67.4%) وادنى فئة مشاركة من الحاصلين على شهادة الاعدادية وبلغت نسبتها (10.9 %) من مجموع (92) .

4. المهنة		
الاجابات	العدد	%
طالب	56	60.9
موظف	34	37
غير ذلك	2	2.2
المجموع	92	100

يوضح الجدول رقم (4) التوزيع التنسبي بين المبحوثين حيث بلغت اعلى نسبة هم الطلبة بواقع (60.9%) واقل نسبة كانت هم من غير وظيفة وبلغت (2.2%) الذين يعملون بأجور يومية في الجامعة.

المحور الثاني : البيانات الاساسية

ت	السؤال	نعم	لا	ربما	% (نعم)	% (لا)	% (ربما)	المجموع
5	هل سبق وتعرضت الى جريمة معلوماتية (ابتزاز او سرقة)؟	10	78	4	10.9	84.8	4.3	%100
6	برأيك هل تؤدي الجرائم المعلوماتية الى التفكك الاسري؟	69	2	21	75	2.2	22.8	%100
7	هل تتعرض النساء والمراهقون بشكل خاص الى مخاطر الابتزاز الالكتروني ؟	79	1	12	85	1.1	13	%100
8	هل تؤثر الجرائم المعلوماتية على الثقة بين افراد المجتمع ؟	81	1	10	88	1.1	10.9	%100
9	هل هناك ضعف في وعي المجتمع بخطورة هذه الجرائم ؟	84	–	8	91.3	–	8.7	%100
10	هل تؤثر الجرائم المعلوماتية على سمعة الضحايا بشكل كبير؟	68	2	22	73.9	2.2	23.9	%100

11	هل الخوف من العادات والتقاليد تمنع الضحية من طلب المساعدة	80	2	10	87	2.2	10.9	%100
12	هل عدم المعرفة التامة بحماية البيانات هي سبب رئيسي للمجرم ؟	55	7	30	59.8	7.6	32.6	%100
13	أتؤيد ادراج مادة عن الامن الرقمي ضمن المناهج الدراسية الجامعية ؟	70	12	10	76.1	13	10.9	%100

يوضح الجدول اعلاه الذي ضم البيانات الاساسية للبحث واجابات المبحوثين والتوزيع النسبي حسب الاسئلة الموجودة والتي يمكن من خلال اجاباتهم معرفة نحو اين يتم تسليط الضوء في دراسة الباحث وكما مبين ادناه :-

- السؤال (5) الفئة الاكثر هم من لم يتعرضوا الى جريمة معلوماتية وبلغت نسبتها(84.8%) وإن القيمة المحسوبة لـ t هي 47.989 مع درجة حرية 91 و *Sig. (2-tailed)* = 0.000، مما يشير إلى أن معظم المشاركين تعرضوا إلى نوع من الجرائم المعلوماتية. يقدر الفرق المتوسط بـ 1.93478 مع فاصل الثقة بين 1.8547 و 2.0149. هذه النتيجة تدعم فرضية أن الجرائم المعلوماتية مثل الابتزاز والسرقة منتشرة بشكل كبير بين الأفراد.
- السؤال (6) يوضح مدى تأثير الجريمة على الاسرة وكانت الاجابة بالتأييد على النعم وبلغت نسبتها (75%).
- السؤال رقم (7) يبين ان الفئة الاكبر التي تتعرض الى الجرائم المعلوماتية هم المراهقون والنساء وكانت نسبتها (85%) فإن القيمة المحسوبة لـ t هي 17.911 مع درجة حرية 91 و *Sig. (2-tailed)* = 0.000، مما يشير إلى أن النساء والمراهقين هم الأكثر عرضة لهذه المخاطر. يقدر الفرق المتوسط بـ 1.27174 مع فاصل الثقة بين 1.1307 و 1.4128. هذه النتيجة تدعم فرضية أن النساء والمراهقين هم أكثر عرضة للابتزاز الإلكتروني.

- السؤال رقم (8) يوضح بأن الجرائم المعلوماتية تؤثر بشكل كبير على الثقة اذ اجابت العينة بالموافقة و بلغت نسبتها (88%) مما يبين ان الافراد يفقدون الثقة فيما بينهم بسبب هذه الجرائم .
- السؤال رقم (9) اذ تشير النتائج الى ضعف وعي الافراد وخطورة هذه الجرائم عليهم وبلغت نسبهتا (91.3 %) وتعتبر هذه النسبة عالية جداً.
- السؤال رقم (10) يتضح من الجدول ان الجرائم المعلوماتية تؤثر على سمعة الضحايا مما يجعلهم يتسترون بسبب العادات والتقاليد والغالبية بلغت نسبتها (73.9%).
- السؤال رقم (11) يرتبط هذا السؤال بالسؤال الذي سبقه اذ ان سمعة الضحايا مرتبطة بالعادات والتقاليد التي تمنع الضحية من طلب المساعدة او اللجوء الى جهات مختصة في معالجة المشكلة وبلغت نسبتها (87%) .
- السؤال رقم (12) يتضح من هذا السؤال ان وجود فئة ليست قليلة متفقة بأنه عدم وجود الخبرة الكافية في حماية البيانات سبباً ايضاً في حدوث الجريمة وبلغت نسبتهم (59.8%).
- السؤال رقم (13) يمكن ملاحظة اتجاه واضح نحو ادراج مادة دراسية تخص الامن الرقمي ضمن المناهج الدراسية لتوعية الافراد منذ الصغر بهذه الجرائم وبلغت نسبتها (76.1%) .

14 . برأيك مع هو السبب الذي يدفع الفرد الى ارتكاب الجريمة المعلوماتية ؟		
الاجابات	العدد	%
ضعف القانون	28	30.4
حب التجربة والفضول	1	1.1
البطالة والفقر	5	5.4
صعوبة معرفة الجاني	3	3.3
اسباب شخصية	5	5.4
جميع ماذكر اعلاه	50	54.3
المجموع	92	100

يوضح الجدول رقم (14) ان القيمة المحسوبة لـ t هي 16.676 مع درجة حرية 91 و *Sig. (2-tailed)* = 0.000، مما يدل على أن الأسباب وراء ارتكاب الجرائم المعلوماتية متنوعة.

يقدر الفرق المتوسط بـــ 4.75 مع فاصل الثقة بين 4.1842 و 5.3158. هذه النتيجة تـــدعم فرضية أن هناك عدة أسباب تؤدي إلى ارتكاب الجرائم المعلوماتية ويتبين ان اعلـــى نســـبة احصائية هي جميع الاسباب المذكوره وبلغت نسبتها (54.3%) واقل نسبة هي حب التجربـــة والفضول لدى المجرم وبلغت (1.1%) .

الفصل الخامس : نتائج البحث والتوصيات

اولاً : نتائج البحث :

1. اوضحت النتائج ان فئة النساء والمراهقون هم الاكثر عرضة الى الجرائم المعلوماتية وبلغت نسبتها (85%)
2. اظهرت النتائج ان الجريمة المعلوماتية تؤثر بشكل كبير على العلاقات الاسرية وتتبعها تفكك واضح في المجتمع اذ اشارت الاجابات بأنها تؤثر بنسبة (75%).
3. تبين من خلال النتائج ان ضعف الوعي لدى افراد المجتمع هو السبب الكبير ايضاً في حدوث الجريمة واجاب المبحوثون بنسبة (91.3%)
4. خوف المجتمع من التكلم عند حدوثها او الابلاغ عنها يسبب تمرد المجرم وحدوثها بشكل اكبر وتؤثر على المجني عليه بشكل كبير نفسياً واجتماعية وبلغت نسبه التكتم عليها (73.9%) المقتنعون بأن الابلاغ عنها يضر بسمعة الضحية.

ثانياً : التوصيات و المقترحات:

1. من الضروري تشريع قانون واضح وصريح يشمل جميع الجرائم المعلوماتية فقط وليس ادراجه مع جرائم اخرى
2. تفعيل التعاون بين الجهات الامنية والاتصالات وذلك لرصد الاتصالات السريعة الخاصة بالجرائم المعلوماتية والابتزاز وغيرها.
3. من الممكن التعاون مع ذوي الخبرة في التكنولوجيا لصنع برنامج خاص للابلاغ في الحالات الخطرة التي لا يمكن للفتيات الابلاغ عنها عن طريق الاتصال او الخوف.
4. زيادة الوعي المجتمعي عن طريق استخدام وسائل الاعلام وادراج مادة الامن الرقمي ضمن المناهج الدراسية
5. تشجيع الاسر على التواصل الفعال ومتابعة البرامج التي يتم استخدامها وتقوية الحوار الاسري معهم حول الموضوع

ثالثاً: الهوامش والمصادر:

1. احمد عبد الحكيم عبد الرحمن، نور عز الليل بن مارني، شروط قبول الادلة الالكترونية امام القضاء الجنائي الفلسطيني، مجلة العلوم السياسية والقانون، عدد7 فبراير 2018، مجلد 2، عن المركز الديمقراطي العربي المانيا–برلين، ص 123.
2. اوس مجيد غالب العوادي، الامن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، اغسطس 2016،ص6.
3. ايمن رسلان، الجرائم المعلوماتية في دولة الامارات والوطن العربي، الامارات العربية المتحدة ، ط1 ، 2016، ص55–56.
4. ايهاب خليفة، حروب مواقع التواصل الاجتماعي، العربي للنشر والتوزيع،2016، ص 118.
5. بهاء الدين حمدي، الاعلام الجنائي واثاره في الحد من الجريمة، دار الراية للنشر والتوزيع، المملكة الاردنية الهاشمية، ط1 ، 2013، ص16.
6. تكرس هيومن رايتس ووتش، منظمة دولية، بحث بعنوان (قانون الجرائم المعلوماتية العراقي قانون سيئ الصياغة وعقوبات غاشمة تخرق الحق في اجراءات التقاضي السليمة وتنتهك حرية التعبير)،يوليو 2012، ص1.
7. حشمت قاسم، تأليف هتنج تشو، تنظيم المعلومات واسترجاعها في العصر الرقمي، المركز القومي للترجمة، القاهرة، ط1، 2018، ص 70–71.
8. خالد حسن احمد لطفي، الدليل الرقمي ودوره في اثبات الجريمة المعلوماتية، دار الفكر الجامعي، 2020، ص45.
9. خالد عبدالحق، دعاء عبد العال، الجرائم الالكترونية والتحقيقات الجنائية، كتاب رقمي، ط1، 2025، ص141.
10. خالد مرزوق سراج العتيبي، الجوانب الاجرائية في الشروع في الجرائم المعلوماتية، دراسة مقارنة، كتاب رقمي، ط1، 2014، ص45.
11. خالد ممدوح ابراهيم، امن الجريمة الالكترونية، دار الجامعية للنشر والتوزيع، الاسكندرية، ط1، 2010، ص76.

ذياب موسى البدانية، الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، ورقة علمية، كلية العلوم الاستراتيجية، عمان، المملكة الاردنية الهاشمية، 2014، ص14-15.

12. Jamil Ahmed itmazi, Fundamentals of Computers and Programming an Arabic Textbook, 2018, P228.

13. زهراء عادل سلبي، جريمة الابتزاز الالكتروني دراسة مقارنة، دار الاكاديميون للنشر والتوزيع، 2021، ط1، ص 49-50.

14. سماح سالم، بهاء رزيقي، محمد سالم، الخدمة الاجتماعية في مجال الجريمة والانحراف، دار المسيرة للنشر والتوزيع، عمان، ط1، 2015، ص16.

15. سيفافيد هياناثان، حق الملكية الفكرية الانجازات والتجاوزات، المكتبة الاكاديمية للنشروالتوزيع، 2004، ص26.

16. شريف حسين محمد، القانون الواجب التطبيق على الجريمة الالكترونية، كتاب رقمي، 2025، ص32.

17. صبيح شهاب احمد، التفكك الاسري واثره في ظاهرة جنوح الاحداث، مجلة الاداب- جامعة بغداد، العدد(50) ، 2000م ،ص201 .

18. عبد العال الديربي، الجرائم الالكترونية ، المركز القومي للاصدارات القانونية، ط1 ، 2012، ص23 .

19. عبدالصبور عبد القوي علي المصري، المحكمة الرقمية والجريمة المعلوماتية، مكتبة القانون والاقتصاد، الرياض، ط 1، 2012، ص50.

20. عماد الحسبان،عدنان الضمور،عزالدين التميمي،ياسر الخزاعلة، الجرائم المستحدثة (المعلوماتية،الالكترونية، السيبرانية)،دار الخليج للنشر والتوزيع،ط1، 2024، ص135-136.

21. فادية حافظ جاسم، التعاون الدولي للحد من الجريمة المعلوماتية، مجلة النهرين للعلوم القانونية، مجلد 21، عدد 4، سنة 2019، ص383.

22. فتوح عبدالله الشاذلي، شرح قانون العقوبات القسم العام، دار المطبوعات الجامعية، الاسكندرية، ط1، 1998، ص66.

23. فكية محمد جمعة محمد، التفكك الاسري واثره على استقرار المجتمع، مجلة الشريعة والقانون، العدد(35) 2019م ، ص 522.

24. ليلى البهنساوي، الاسرة في عصر الرقمنة الفرص والتحديات، دار المجلة العربية للنشر والترجمة، مصر، العدد (584) مايو 2025.

25. محمد العوض محمد وداعة الله، مواقع التواصل الاجتماعي وقضايا الشباب الجامعي، كتاب رقمي، ط1، 2020، ص67.

26. محمد عبد البديع السيد، تكنولوجيا الاعلام في العصر الرقمي، دار الكتب المصرية للنشر والتوزيع، مصر، ط1، 2022 ، ص5.

27. محمد كمال، الارهاب السيبراني عندما يستخدم الارهابي الكيبورد بدلاً من القنبلة، دار كليم للنشر والتوزيع، 2022، ص13.

28. محمود نجيب حسني، شرح قانون العقوبات، دار النهضة العربية، مصر– القاهرة، ط1، ص32.

29. ميرفت محمد حبابية، مكافحة الجريمة الالكترونية، كتاب رقمي، ط1، 2022، ص175–176.

30. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار النشر الثقافة للنشر والتوزيع، عمان، ط2، 2010، ص48.

31. هشام محمد فريد رستم، الجرائم المعلوماتية اصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الامن والقانون، دبي، العدد2، 2019.

32. هيثم عبدالرحمن البقلي، الجرائم الالكترونية الواقعة على العرض بين الشريعة والقانون المقارن، 2010،ص22.