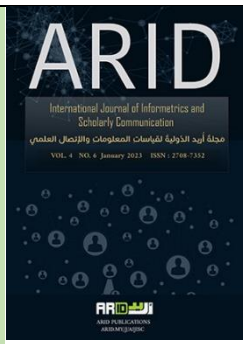
ARID Journals

ARID International Journal of Informetrics and Scholarly Communication (AIJISC)
ISSN: 2708-7352

Journal home page: http://arid.my/j/aijisc



مَجلةُ أُريد الدَّوليةُ لقياسات المعلومات و الإتصال العلمي

العدد 6 ، المجلد 4 ، كانون الثاني 2023 م

Cybercrime and the Social Media

Mohammad Almutasim Bellah Alhamed Alduihi*

Department of Telecommunications Engineering, Faculty of Electrical and Electronic Engineering, University of Aleppo, Syria

الجريمة الإلكترونية ووسائل التواصل الاجتماعي

محمد المعتصم بالله الحامد الضويحي*

قسم هندسة الاتصالات، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب، سوريا

Mohammed.dowaehy@gmail.com

arid.my/0005-9947

https://doi.org/10.36772/arid.aijisc.2023.642

ARTICLE INFO
Article history:
Received 23/08/2022
Received in revised form 21/11/2022
Accepted 20/12/2022
Available online 15/01/2023

ABSTRACT

In this research, each of the electronic crimes will be analyzed in an attempt to reduce the dangerous effects that they entail, and to clarify their true meaning.

A quantitative study was conducted based on a questionnaire, Survey on Cybercrime via Social Media which contains ten questions, with each other question having a measurable scale that was applied to the participants. The survey takes into account the different methods of defrauding innocent victims as well as the number of hours people spend on the internet and the different social media they use. The results showed that 70% of people spend more than 2 hours online and 60% belong to more than 5 social media platforms and 90% of them tried to cheat in a year and 60% of people have lost their money. Cybercrime was noted to be the most common. Mobile phone fraud represented 60% compared to inheritance fraud which represented 10% and fictitious tax refund of 40%.

It was also found through the research that 73% of people did not inform the authorities, as 88% prefer not to report even when they suspected that they have been deceived, and 76% of them have seen and heard advertisements about cybercrime. It was also found that 62% are not interested in victims exposed to cybercrime. These results was enough for countries to enact laws and legislation that limit these crimes and intensify the punishment for the perpetrators, as well as educating societies about their danger to avoid them.

Keywords: Cybercrime, Internet, Hacking, Social media, Facebook, Twitter, Instagram.

الملخص

في هذا البحث ســـوف يتم تحليل كل من الجرائم الإلكترونية في محاولة للحد من الآثار الخطيرة التي تترتب عليها، وتوضـيح المعنى الحقيقي لها. تم عمل دراسـة كمية تسـتند إلى اسـتبيان يحتوي على عشـرة أسـئلة، مع كل سـؤال آخر له مقياس قابل للقياس تم تطبيقه على المشـــاركين. كان بعنوان مســـح على الجريمة الإلكترونية عبر وســـائل التواصـــل الاجتماعي. في الاستطلاع تم الأخذ في الاعتبار الأساليب المختلفة للاحتيال على الضحايا الأبرياء وكذلك عدد الساعات التي يقضيها الأشخاص على الإنترنت ووســـائل التواصـــل الاجتماعي المختلفة التي يســـتخدمونها. من خلال البحث وجدنا بأن 70% من الأشـــخاص يقضـــون أكثر من ســـاعتين على الإنترنت و60% ينتمون إلى أكثر من 5 منصـــات وســـائط اجتماعية و حاول شـــخص ما خداع 90% منهم في العام وأن 60% من الناس فقدوا أموالهم و كانت الجرائم الإلكترونية الأكثر شيوعًا بالنسبة لهم هي الاحتيال عبر الهاتف المحمول والذي مثل نســـبة 60% مقارنة بالخدع المتعلقة بالميراث والتي مثّلت 10% واســـترداد الضـــرائب الوهمي 40%. تبين من خلال البحث أيضـــاً أن 73% من الناس لم يبلغوا الســـلطات حيث أن 88% يفضـــلون عدم الإبلاغ حتى عندما يشـــتبهون في تعرضـــهم للخداع وأن 76% منهم شـــاهدوا وســـمعوا إعلانات عن جرائم الإنترنت وتبين أيضـــاً أن 62% غير مهتمين بالضـحايا المعرضـين للجرائم الإلكترونية ، هذه النتائج كانت كفيلة بأن تقوم الدول بسـن القوانين والتشـريعات التي تحد من هذه الجرائم وتشدد العقوبة على مرتكبها وكذالك توعية المجتمعات بخطرها لتفاديها.

الكلمات المفتاحية: جرائم الإنترنت، الإنترنت، الهاكرز، وسائل التواصل الاجتماعي، فيسبوك، تويتر، انستغرام، اختراق

مقدمة:

تميز القرن الحادي والعشرون باستخدام المعلوماتية، وخلال السنوات القليلة الماضية توسعت شبكة الإنترنت بشكل كبير. حالياً، هناك حوالي 825 مليون شخص يستخدمون الإنترنت، بزيادة قدرها 129 بالمائة عن 2000-2005 (National 2005,White Collar Crime Ctr) . إن السهولة النسبية لاستخدام الإنترنت، والوصول إلى الإنترنت بأسعار معقولة بشكل متزايد، والوصول إلى أجهزة الحاسب المزودة بأجهزة مودم فائقة السرعة، جعلت من الممكن للأشخاص التواصل وتكوين صداقات جديدة، والتجارة، والترفيه، والتعلم، وممارسة الأعمال التجارية، ودفع الفواتير عبر الإنترنت. أنشأت شبكة الويب العالمية ما يسمى بالعالم الافتراضي أو الفضاء الإلكتروني، والذي يُعرَّف بأنه مكان غير محدد يتفاعل فيه الأفراد والتجمعات (Britz, 2009) ، ويتم تصنيف الفضاء الإلكتروني على أنه مكان لا مادي أو اجتماعي الحدود التي تحرم الأفراد من العيش فيها.

لقد انتقل الناس من العالم الحقيقي إلى العالم الافتراضي، وكذلك الجريمة. يمكننا تخيل التفاعلات التي تحدث في الواقع الافتراضي، سواء كانت شخصية أو مؤسسية، أو في مجال الأعمال أو الخدمات أو الثقافة.

إنّ العالم فِي العصر الحالي يقفُ على باب كبير منَ التطوّر العلمي والتكنولوجي لاستخدام الحاسب في العملية التصميمية، وهذا الأمر قد ساهمَ إلى حدٍّ كبير فِي تقدّم الأجيال بمساعدتهم في إكتساب الادوات والمهارات الضرورية التي تساعدهم على الوصول لتصميمات مبتكرة ومعاصرة، وتشجعهم على الإنتاج العلمي المتميز وجعل عملية التعلم أكثر متعة بربط تطبيقات المقرر بمجال التخصص (جمعة ، 2022) . ترجع هذه الأهمية الكبيرة للحاسب بشكل أساسي إلى البرامج التي يعتمد عليها في عمله وأنظمة التشغيل المختلفة. من خلال تنفيذ العديد من الخدمات والعمليات القانونية مثل البيع والشراء، أصبح العالم بأسره في متناول اليد بفضل الإنترنت (العدساني، 2009) . وقد أدى هذا التطور المذهل للحاسب إلى ظهور الجرائم الناتجة عن ذلك الاستخدام، وهذه الجرائم إما تحدث على الحاسب نفسه، أو تحدث من خلاله، حيث يصبح أداة في يد المجرم الذي يستخدمه لتحقيق أغراضه الإجرامية أو ما يسمى بالجريمة الإلكترونية، وهي جريمة تتم باستخدام جهاز حاسب من خلال اتصال بالإنترنت وتهدف إلى اختراق الشبكات والتخريب والتضليل والتزوير والسرقة والاختلاس والقرصنة وسرقة المثقفين حقوق الملكية. يشكل الانحراف جريمة بأركانها المادية والمعنوية، ولا يعبر فيها عن الدافع لارتكابها.

وقد جاء في القانون السوري تعريف الجريمة المعلوماتية في المادة /1/ منه أن: "الجريمة المعلوماتية هي جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة او تقع على المنظومات المعلوماتية أو الشبكة." (مجلس الشعب السوري ، 2012)

2- أهمية البحث وأهدافه:

تتجلى أهمية البحث في دراسة عن الجرائم الإلكترونية وضحاياها وأشكالها وانتهاكاتها المختلفة وذلك بسبب انتشارها بشدة مع التطور التكنلوجي المتسارع فمثلا موقع الفيسبوك وحده يجمع أكثر من 500 تيرابايت من المعلومات كل يوم (سليمان والبراشـــدية ، 2019) مما يجعل أمن هذه المعلومات أمراً بالغ الأهية وعلى درجة عالية من الخطورة خاصـــة وأن هذه المعلومات هي بيانات لأشـخاص أو مؤسـسـات تقوم بإنشـاء حسـابات لها على موقع فيسـبوك ، ونظرا لازداد اسـتخدام شـبكة المعلومات الدولية والابحار في مواقع التواصـل الاجتماعي مؤخرا نظرا للامتيازات التي توفرها للأفراد (علوش، 2022) كان لا بد من دراسـة أثر هذه الجرائم وخاصـة تلك التي تحدث عبر وسـائل التواصـل الاجتماعي للحد من أثرها وتوعية المجتمعات والأفراد والمؤسسات تجاهها.

ويهدف البحث إلى:

1. الحد من الجرائم الإلكترونية من خلال نشر آثار الجرائم الإلكترونية
2. الكشف عن أكثر الطرق اتباعاً في الجريمة الإلكترونية

3- أسئلة البحث:

تتحدد أسئلة البحث في ما يلي:

1- ما هي أكثر الطرق التي يتبعها المجرم للقيام بالجريمة الإلكترونية؟

2- ما هي نسبة الأشخاص الذين تعرضوا للجريمة الإلكترونية بسبب استخدام وسائل التواصل الاجتماعي ؟

4- منهج البحث وأدواته :

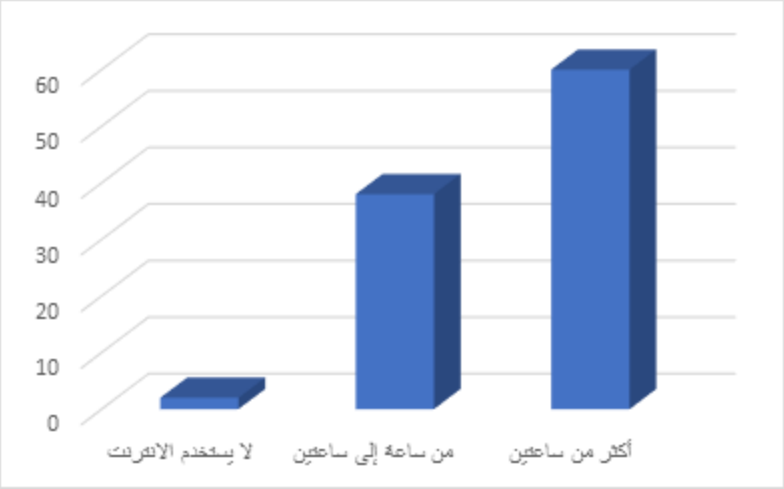
اتبعت الدراسـة المنهج الكمي القائم على استبيان يحتوي على عشـرة أسئلة، مع كل سؤال آخر له مقياس قابل للقياس. كان بعنوان مسح على الجريمة الإلكترونية عبر وسـائل التواصـل الاجتماعي. تم أخذ الأسـاليب المختلفة للاحتيال على الضـحايا الأبرياء وكذلك عدد الساعات التي يقضيها الأشخاص على الإنترنت ووسائل التواصل الاجتماعي المختلفة التي ينتمون إليها في الاعتبار في الاستطلاع.

5-النتائج والمناقشة:

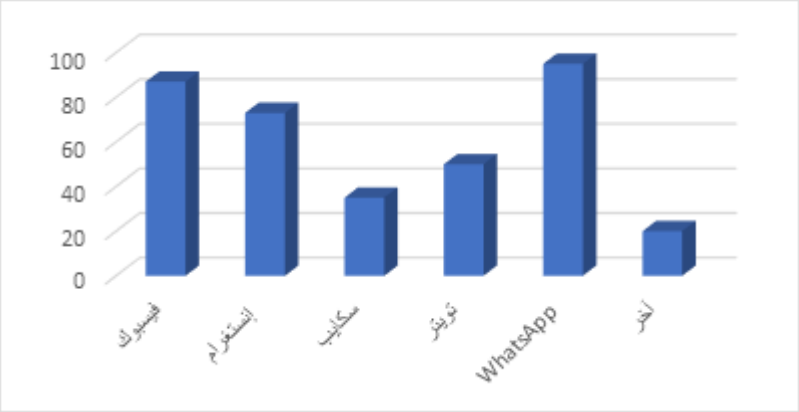
اســتندت النتائج إلى الاســتبيان الذي تم تســليمه إلى 100 فرد على حدة وفي زمان ومكان مختلفين. النتائج التي تم الحصول عليها من المسح المكون من عشرة أسئلة وقد خلصت النتائج إلى ما يلي:

النسبة المدروسة	النسبة المئوية
نسبة الأشخاص الذين ينتمون إلى أكثر من 5 منصات وسائط اجتماعية.	%60
نسبة الأشخاص الذين تعرضوا للخداع عبر الشبكة في العام الماضي .	%90
نسبة الأشخاص الذين فقدوا أموالهم.	%60
نسبة الأشخاص الذين تم الاحتيال عليهم عن طريق الهاتف المحمول	%60
نسبة الأشخاص الذين تم الاحتيال عليهم عن طريق الميراث	%10
نسبة الأشخاص الذين تم الاحتيال عليهم عن طريق استرداد الضرائب الوهمي	%40
نسبة الأشخاص الذين لم يبلغوا الشرطة بذلك.	%73
نسبة الأشخاص الذين يفضلون عدم الإبلاغ حتى عندما يشتبهون في تعرضهم للخداع.	%88
نسبة الأشخاص الذين شاهدوا وسمعوا إعلانات عن جرائم الإنترنت.	%76
نسبة الأشخاص غير مهتمين بالضحايا المعرضين للجرائم الإلكترونية	%62

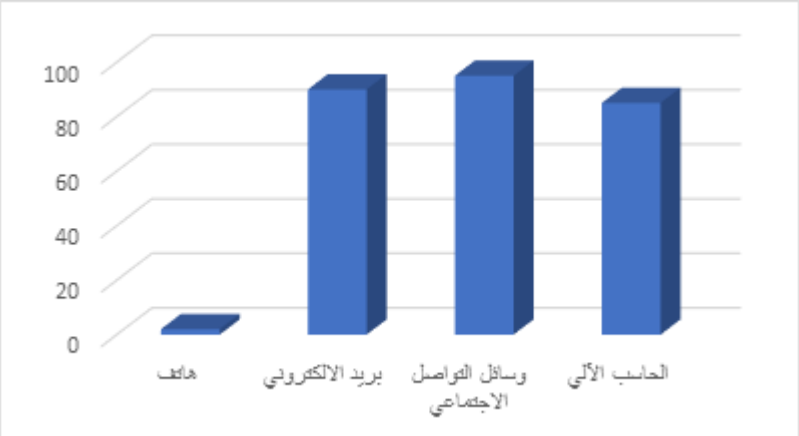
الجدول (1) نتائج المسح



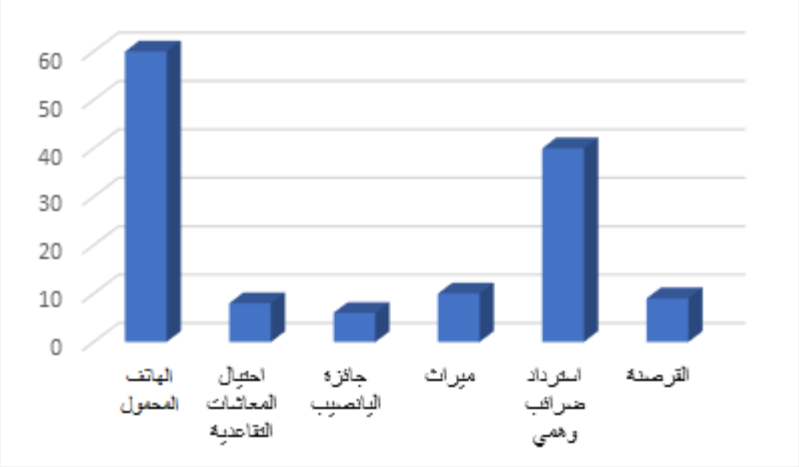
الشكل (1) عدد الساعات على الانترنت



الشكل (2) أي من منصات التواصل الاجتماعي هي المفضلة لديك؟



الشكل (3) ماهي طريقة النهج المستخدمة؟



الشكل (4) مانوع الجريمة أو الجرائم الإلكترونية التي واجهتها؟

لقد ادى الاستخدام المطرد للمعلوماتية إلى ظهور مايعرف بالجريمة الالكترونية إذ أن هذه نتيجة حتمية لكل تقدم علمي أو تقني مستحدث ويرتكز هذا النوع من الاجرام على محورين أحدهما ضد المال والاخر ضد الأشخاص ويستمد نشاطه من الإمكانيات الهائلة للحاسوب.فالحاسوب الآلي بوصفه أداة للتخزين لديه قدرة هائلة على التخزين وتنظيم واستغلال عدد غير محدد من المعلومات وله في الوقت نفسه قدرة على استرجاعها في فترة زمنية وجيزة. ولكي يتحدد الاطار القانوني لهذه الجرائم بشكل أكثر وضوحا ينبغي التمييز بين نوعين من الجرائم أو الاعتداءات المعلوماتية الأول عندما تكون تكنولوجيا المعلومات والاتصالات عن بعد قد استخدمت وسيلة لارتكاب الجرائم بمعنى اخر نكون والحالة هذه أمام أعمال إجرامية ترتكب بمساعدة الحاسوب والوصف الجرمي لهذه الأعمال يتصل بأنواع الجرائم التقليدية كالاحتيال والسرقة وغيرها أما النوع الثاني من الجرائم المعلوماتية فهي حين تكون تكنولوجيا المعلوماتية والاتصالات عن بعد هدف الجرائم وغايتها وبذلك نكون أمام أفعال جرمية جديدة ترتبط في غالبيتها بالتعرض لأمن وسلامة الأنظمة المعلوماتية ولسرية البيانات والمعلومات التي يحتوي عليها ويسمى هذا النوع بالإجرام المعلوماتي في شبكة الانترنيت ويتم ذلك في حالة الدخول غير المشروع إلى هذه الانظمة والتعرض لها وللمعلومات التي تتضمنها (سالم و هجيج ، 2007) . ومع غزو الشبكة لدول العالم، أصبح من الصعب للغاية السيطرة على هذه الجرائم وكشفها لكونها تعبر الحدود، وتحدث بسرعة كبيرة دون إشراف من أي دولة، بما في ذلك هذه أدى إلى ارتكاب جميع أشكال النشاط الإجرامي المعترف به على الإنترنت، مثل سرقة برامج الحاسب بغرض سرقة البيانات وقاعدة بيانات المعلومات، حتى السرية منها، واستخدامها في التجسس، أو تلك المتعلقة بالقرصنة وسرقة المعلومات. الأموال، بالإضافة إلى ظهور ما أطلق عليه الإرهاب الإلكتروني وتهديد الأمن القومي للدول، وكذلك جرائم الآداب العامة والإضرار بالآداب من خلال المواد الإباحية الإلكترونية التي تتجسد في المواقع الإباحية، وخاصة تلك الموجهة للأطفال دون سن البلوغ. استخدام دعارة الأطفال والنساء سواء بالعين أو من قبل القصر بتصويرهم مباشرة أو عن طريق محاكاة الصورة الرقمية وتمثيلها. وسائل الترهيب والترهيب كالإغراء أو التحذير أو التهديد. تتفق جميع النظريات والدراسات المكتملة على نقطة أساسية، وهي الهدف المادي البحت الذي يسعى المجرم الإلكتروني إلى تحقيقه، من سرقة الأموال إلى الهجوم على البيانات السرية وتدمير البرامج الإعلامية لأي دولة لتهديدها بها. أمنها القومي وسلامتها الإقليمية.

شهدت الجريمة السيبرانية مكانة تصاعدية في جداول أعمال الأمن القومي في جميع أنحاء العالم. لقد أصبح جزءًا من استراتيجيات الأمن القومي لعدد متزايد من البلدان، بما في ذلك المملكة المتحدة وأستراليا وهولندا والولايات المتحدة والعديد من

البلدان الأخرى، وأصبح تهديدًا من المستوى الأول، فوق الجريمة المنظمة والاحتيال بشكل عام. (Wall & Williams, 2013).

منذ العقد الماضي، أصبحت شبكات التواصل الاجتماعي جزءًا أساسيًا من حياة الجميع مما يؤثر على الحياة الثقافية والاقتصادية والاجتماعية للناس. وفقًا لموقع internetlivestats.com، وصل مستخدمو الإنترنت في مارس 2019 إلى 4168461500، أي بنسبة 50.08% من تغلغل سكان العالم. (Soomro & Hussain, 2019).

في هذه الأيام، أصبحت منتديات وسائل التواصل الاجتماعي جزءاً من نمط حياة الإنسان حيث يستخدم ملايين الأشخاص منتديات التواصل الاجتماعي القائمة على الإنترنت. وسائل التواصل الاجتماعي عبارة عن مزيج من التطبيقات والمواقع الإلكترونية المصممة لتعزيز مشاركة المعلومات والشبكات عبر الإنترنت (Power, 2014).

في عام 2007، على سبيل المثال، كانت الجرائم الإلكترونية تحدث مرة واحدة كل 3 ثوانٍ في العالم العربي، خلال نفس العام، تم تسجيل 217000 حالة قرصنة وسرقة في دولة الإمارات العربية المتحدة وحدها، مع زيادة كبيرة خلال عام 2008 بلغت 33 نسبه مئوية. تتميز الجريمة السيبرانية بكونها عابرة للحدود، تحدث في مكان معين وضحاياها في مكان آخر، بالإضافة إلى السرعة في تنفيذها والسرعة في إتلاف الأدلة ومحو آثارها، ناهيك عن ارتكابها من قبل أشخاص غير عاديين مع ذكاء خارق وتقنية عالية في التعامل مع تكنولوجيا المعلومات والحاسب الآلي. (عبد الصبور، 2015) .

على الصعيد القانوني حسب الغافري فإنّ الأحكام الموضوعية للجريمة المعلوماتية تقسم جرائم المعلوماتية إلى نوعين (الغافري و عقيدة ، 2006) :

الأول : الجرائم التقليدية التي ترتكب بواسطة نظم المعلومات ، وهي تلك الجرائم التي كانت موجودة قبل عصر المعلومات ، ولكن بعد ظهور هذه التقنية وانتشار الشبكات أصبحت ترتكب بواسطتها ، فراحت تبدو وكأنها جرائم جديدة ، ومن هذه الجرائم : جريمة التهديد بالقتل وجريمتي الذم والقدح التي ترتكب عبر البريد الإلكتروني ، والجرائم المخلة بالأخلاق والآداب العامة التي ترتكب عبر المواقع الإباحية وغير ذلك من الجرائم.

أما النوع الثاني: فهي الجرائم المستحدثة، و يقصد بها تلك الجرائم التي ظهرت في عصر تقنية المعلومات ولم تكن معروفة من قبل وخاصة بعد اختراع الإنترنت، ومن أمثلة هذه الجرائم: جريمة الدخول غير المصرح به إلى أنظمة الحاسوب أو المواقع الإلكترونية، وجريمة تعطيل أو عرقلة نظام معلوماتي، وجريمة إتلاف المعلومات عن طريق زرع الفيروسات وغيرها من الجرائم.

إن القوانين المتعلقة بالجرائم الإلكترونية كانت حديثة على صعيد العالم العربي ، ويوجد ثلاث عشرة دولة عربية لديها قوانين مخصصة لمكافحة الجرائم الإلكترونية. الأولى كانت دولة الإمارات العربية المتحدة ، التي سنت قانون جرائم تقنية المعلومات (القانون الاتحادي رقم 2 لعام 2006 ، المعدل ثلاث مرات في 2012 و 2016 و 2018) (البوابة الإلكترونية لحكومة دولة الامارات العربية المتحدة ، ب.ت) . وأصدرت المملكة العربية السعودية قانون جرائم تقنية المعلومات في عام 2007 (1428 هـ) (هيئة الخبراء ، 2007) ، وأصدر السودان قانونًا لمكافحة هذه الجرائم في عام 2007 (معدل في 2018) (بنك السودان المركزي ،2007) ، تليها الجزائر في عام 2009 (الجريدة الرسمية للجمهورية الجزائرية، 2009) والأردن في عام 2010 (قانون مؤقت أصبح دائمًا في عام 2015) (قوانين الأردن، 2015) . و سنت عمان تشريعات لمكافحة جرائم تكنولوجيا المعلومات في عام 2011 بعد إدراج بعض الأحكام لمكافحة هذه الجرائم في قانون العقوبات (قانون ، 2011) . وأصدرت سوريا قانون الجرائم الإلكترونية عام 2012 (مجلس الشعب السوري ، 2012) ، تلتها البحرين (هيئة التشريع ، 2014) وقطر (الميزان ، 2014) عام 2014 ، ثم الكويت عام 2015 (وزارة الداخلية لدولة الكويت ، 2015) ، ثم موريتانيا عام 2016 (بوابة تقنيات الإعلام والاتصال ، 2016) ، وأخيراً مصر (محكمة النقض المصرية ، 2018) وفلسطين (منظومة القضاء والتشريع ، 2018) عام 2018.

6- الخاتمة :

من خلال البحث وجدنا بأن 70% من الأشخاص يقضون أكثر من ساعتين على الإنترنت و60% ينتمون إلى أكثر من 5 منصات وسائط اجتماعية و حاول شخص ما خداع 90% منهم في العام الماضي و طريقة التعامل كانت البريد / التواصل الاجتماعي / الحاسب 80% وأن 60% من الناس فقدوا أموالهم و كانت الجرائم الإلكترونية الأكثر شيوعًا بالنسبة لهم هي الاحتيال عبر سرقة رصيد الهاتف المحمول والذي مثل نسبة 60% مقارنة بالخدع المتعلقة بالميراث والتي مثّلت 10% واسترداد الضرائب الوهمي 40% .

تبين من خلال البحث أيضاً أن 73% من الناس لم يبلغوا السلطات حيث أن 88% يفضلون عدم الإبلاغ حتى عندما يشتبهون في تعرضهم للخداع وأن 76% منهم شاهدوا وسمعوا إعلانات عن جرائم الإنترنت وتبين أيضاً أن 62% غير مهتمين بالضحايا المعرضين للجرائم الإلكترونية.

وبناءاً على هذه النتائج نوصي بما يلي :

1. سن القوانين والتشريعات التي تحد من هذه الجرائم وتشدد العقوبة على مرتكبها.

2. الحث على الإبلاغ عن هذه الجرائم سواء من الضحايا أو من الأشخاص والمؤسسات.
3. العمل على تأهيل كوادر مؤهلة بشكل عالٍ للتصدّ لمثل هذه الجرائم .
4. إنشاء محاكم خاصة بهذا النوع من الجرائم .
5. ضرورة توعية المجتمعات بخطرها لتفاديها.

7- المراجع

1- *National White Collar Crime Ctr*, United States of America, US Federal Bureau of Investigation, Office for Victim Assistance, & United States of America. (2005). IC3 2004 Internet Fraud--Crime Report, January 1, 2004-December 31, 2004.

2- MARJIE T. Britz., 2004 - *Computer Forensics and Cyber Crime*. New Jersey: Pearson Education Inc.

3- جمعة, س. (2022). أهمية التقنية الحديثة للحاسب في منظومة التعليم الجامعى تطبيقاً على مقرر كمبيوتر جرافيک للفرقة الثانية (مجموعة 2). مجلة التراث والتصميم. https://doi.org/10.21608/jsos.2022.129040.1190

4- العدساني طارق، (2009) - *مفهوم الحماية القانونية لبرامج الحاسب الآلي ووسائلها* ، مجلة معهد القضاء – الكويت ، مج8, ع17 – ص 105-133 ، https://cutt.ly/t4AF100

5- العدساني طارق. (2009). مفهوم الحماية القانونية لبرامج الحاسب الآلي ووسائلها. مجلة معهد القضاء – الكويت, 8(17), 105-133. https://cutt.ly/t4AF100

6- القانون السوري. (2012). المرسوم التشريعي رقم /17/ لعام 2012 ، قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية. موقع وزارة الداخلية السوريّة. تم الاسترجاع من &http://moia.gov.sy/portal/site/arabic/index.php?node=55222&cat=86

7- أحمد البراشدية, ح. (2019). الفيسبوك والجرائم الإلكترونية في عمان: هل هناك علاقة؟. Journal of Information Studies and Technology, 2019(2), 7.

8- علواش, و كهينة. (2022). مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي" بين اختراق الخصوصية وآليات المواجهة". دراسات, 11(2), 88-105.

9- محمد علي سالم, و حسون عبيد هجيج. (2007). *الجريمة المعلوماتية*. Journal of University of Babylon, 14(2). ، مجلة جامعة بابل ، المجلد 14, العدد 2, الصفحات 85- 100. تم الاسترجاع من https://www.iasj.net/iasj/article/37484

10- Wall, D. S., & Williams, M. L. (2013). Policing cybercrime: networked and social media technologies and the challenges for policing. Policing and society, 23(4), 409-412.

11- Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. Appl. Comput. Syst., 24(1), 9-17.

12- A. Power, (2014). *What is social media? British Journal of Midwifery*, vol. 22, pp. 896-897.

13- عبد الصبور عبد القوي علي، 2015 - *الجريمة الإلكترونية والجهود الدولية للحد منها*، مجلة الدراسات المالية والمصرفية، مج. 23، ع. 1، ص: 13-17. تم الاسترجاع من https://search.emarefa.net/detail/BIM-546370

14- الغافري، حسين بن سعيد بن سيف, & عقيدة، محمد أبو العلا. (2006). *السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة* (Doctoral dissertation, جامعة عين شمس).

15- البوابة الإلكترونية لحكومة دولة الإمارات العربية المتحدة. (ب.ت). قوانين الجرائم الإلكترونية. تم الاسترجاع من https://u.ae/ar-ae/resources/laws

16- هيئة الخبراء بمجالس الوزراء، المملكة العربية السعودية. (2007). نظام مكافحة جرائم المعلوماتية. في أنظمة المواصلات والاتصالات، مجموعة الأنظمة السعودية (المجلد السابع). تم الاسترجاع من https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1

17- بنك السودان المركزي. (2007). قانون جرائم المعلوماتية لسنة 2007. تم الاسترجاع من https://cbos.gov.sd/ar/content/قانون-جرائم-المعلوماتية-لسنة-2007

18- الجريدة الرسمية للجمهورية الجزائرية. (2009). العدد /47، قوانين. تم الاسترجاع من https://www.mpt.gov.dz/sites/default/files/loi%20N%C2%B009-04%20ar.pdf

19- ديوان التشريع والرئي. (2015). قانون الجرائم الإلكترونية. المملكة الأردنية الهاشمية. تم الاسترجاع من https://www.lob.jo/?v=1.14&url=ar/LegislationDetails?LegislationID:3184,LegislationType:2,isMod:false

20- قانون. (2011). قانون مكافحة جرائم تقنية المعلومات. سلطنة عمان. تم الاسترجاع من https://qanoon.om/p/2011/rd2011012/

21- هيئة التشريع والرئي القانوني. (2014). قانون جرائم تقنية المعلومات. مملكة البحرين. تم الاسترجاع من https://www.lloc.gov.bh/HTM/K6014.htm

22- الميزان – البوابة القانونية القطرية. (2014). قانون مكافحة الجرائم الإلكترونية. تم الاسترجاع من https://almeezan.qa/LawView.aspx?opt&LawID=6366

23- موقع وزارة الداخلية لدولة الكويت. (2015). مكافحة جرائم تقنية المعلومات. تم الاسترجاع من https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf

24- الجمهورية الإسلامية الموريتانية، بوابة تقنيات الإعلام والاتصال. (2016). قوانين المجتمع الموريتاني للمعلومات – قانون الجريمة السبرانية. تم الاسترجاع من http://tic.gov.mr/article287

25- محكمة النقض المصرية. (2018). قانون رقم ١٧٥ لسنة ٢٠١٨ – مكافحة جرائم تقنية المعلومات. تم الاسترجاع من https://www.cc.gov.