Sana'a University Journal of Human Sciences
مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 3| No. 1 | Page 361 – 396 | 2023 |
https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

دور إدارات العلاقات العامة والإعلام في توعية الجمهور بمخاطر الجريمة الإلكترونية
دراسة وصفية على الإدارات المسئولة عن التوعية بمخاطر الجرائم الإلكترونية
(وزارة الاتصالات، وزارة الداخلية، وزارة العدل)

The role of public relations and media departments in educating the public about the dangers of cybercrime, A descriptive study on the departments responsible for raising awareness of the dangers of cybercrime (Ministry of Communications, Ministry of Interior, Ministry of Justice)

فهمي محمد أحمد النعامي
باحث – قسم الإذاعة والتلفزيون – كلية الاعلام
جامعة صنعاء

Fahmi Mohammed Ahmed Al-Naami
Researcher - Radio and Television Department –
Faculty of Mass Communications
Sana'a University -Yemen

الملخص:

هدفت الدراسة إلى الكشف عن واقع الجريمة الإلكترونية في اليمن، ومعرفة دور الجهات المسئولة عن الجريمة الإلكترونية في اليمن في توعية الجمهور بمخاطر الجريمة الإلكترونية، وقد اعتمدت الدراسة على المنهج الوصفي الذي جُمعت بواسطته البيانات الكمية والكيفية للدراسة معاً، وقد استخدم الباحث التصميم التفسيري، حيث جُمعت في المرحلة الأولى من هذا التصميم بيانات كمية باستخدام استبانة الذي جرى تطبيقها على عينة عشوائية بلغت 400 من مستخدمي الإنترنت بأمانة العاصمة صنعاء، تلا ذلك جمع البيانات الكيفية باستخدام أداة المجموعات المركزة، التي شرحت النتائج الكمية وفصلتها، وامتد جمع البيانات الكيفية بهذه الدراسة؛ بحيث شمل أداة المقابلة المعمقة مع مدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية.

توصلت الدراسة إلى ارتفاع معدل الاستخدام اليومي للمبحوثين للإنترنت، وأن نسبة (47%) من الجمهور عينة الدراسة قد تعرضوا لنوع واحد على الأقل من الجرائم الإلكترونية، وأشارت النتائج إلى المعرفة الجيدة للمبحوثين بالمفاهيم العامة للجريمة الإلكترونية، والوعي الضعيف للمبحوثين بطرق الوقاية من الجريمة الإلكترونية، كما توصلت الدراسة إلى فشل إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجرائم الإلكترونية في اليمن في أعمال توعية وتثقيف الجمهور بمخاطر الجريمة الإلكترونية.

الكلمات المفتاحية: الإنترنت، الجريمة الإلكترونية، الوعي بالجرائم الإلكترونية.

Abstract:

The study aimed to reveal the reality of cybercrime in Yemen and to know the role of the authorities responsible for cybercrime in Yemen in educating the public about the dangers of cybercrime. Descriptive method، where in the first stage، quantitative data was collected using a questionnaire that was applied to a random sample of 400 Internet users in the capital، Sana'a، then qualitative data was collected using the focus groups tool that explained and separated the quantitative results، and the qualitative data collection was extended in this study to include On the in-depth interview tool with managers and officials of media and public relations departments in the entities responsible for cybercrime.

The study found a high rate of daily use of the Internet by the respondents، and that (47%) of the study sample audience had been exposed to at least one type of cybercrime. The study concluded that the media and public relations departments of the authorities responsible for cybercrime in Yemen failed to raise awareness and educate the public about the dangers of cybercrime.

Keywords: Internet، cybercrime، awareness of cybercrimes.

المقدمة:

أدى الاستخدام الكبير للإنترنت إلى الكثير من المشاكل والمخاطر، وقدم أصنافاً من الجرائم التي لم تكن متداولة سابقاً سُميت بالجرائم الإلكترونية، التي تعددت صورها وأشكالها، وقد ترافق تزايد معدل ارتكاب الجرائم الإلكترونية على مستوى دول العالم في العقدين الأخيرين على وجه الخصوص، مع استنفار الكثير من الدول من ناحية تشريع قوانين خاصة بمكافحة هذا

النوع من الجرائم واستحداثها إدارات خاصة بمكافحتها وللتوعية بمخاطرها.

وتعد أول خطوة للوقاية من الجريمة هي الوعي، ومع ما تشهده البيئة الرقمية من انتهاكات وجرائم إلكترونية تمس بالصالح العام ومصالح الأفراد؛ تكون بذلك إدارات الإعلام والعلاقات العامة في كلاً من وزارات (الداخلية، والاتصالات وتقنية المعلومات، والعدل) في الجمهورية اليمنية هي الجهات المسئولة بصفة أساسية عن سلامة هذه البيئة الإلكترونية، ويصبح أمن المعلومات والحفاظ عليها ضرورة حتمية بالتعامل والتضامن مع المؤسسات الأمنية و(القوانين والتشريعات، لاسيما مع ضعفها وشبه انعدامها على المستوى الوطني). وتستهدف هذه الدراسة تسليط الضوء على واقع الجريمة الإلكترونية في اليمن وواقع الجهود المبذولة من إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجرائم الإلكترونية في توعية الجمهور بمخاطر الجرائم الإلكترونية.

مشكلة الدراسة:

أصبحت الجريمة الإلكترونية في اليمن تشكل ظاهرة لها انعكاسات سلبية على أمن الأفراد واستقرار المجتمع، في ظل غياب التشريعات والقوانين المحلية المتعلقة بمكافحة الجريمة الإلكترونية، المترافق مع ندرة الدراسات المحلية التي تناولت هذه الظاهرة، وفي إحصائية شاملة للجرائم الإلكترونية المضبوطة بلغ إجمالي القضايا للجرائم الإلكترونية التي تم العمل عليها لدى الجهات ذات العلاقة خلال الأعوام 2015-2021م عدد (10.667) جريمة إلكترونية (سراج والعبالي، 2033، ص16)، وهي لا تعادل 7% من حجم الجرائم الإلكترونية الفعلية الواقعة على الأفراد والمؤسسات؛ نظراً لإحجام الكثير من الأفراد والمؤسسات عن التقدم بالإبلاغ للخشية من الفضيحة أو لعدم الثقة في قدرة الأجهزة الأمنية على ضبط الجناة، وعليه تتبلور مشكلة الدراسة في معرفة الأدوار الفعلية التي تقوم بها إدارات العلاقات العامة والإعلام المسئولة عن الجرائم الإلكترونية في اليمن حيال التوعية بمخاطر الجريمة الإلكترونية .

أهمية الدراسة:

1- أهمية معرفة واقع الجريمة الإلكترونية في اليمن وحجم انتشارها في ظل ندرة الأبحاث المحلية التي تناولت هذا الشأن؛ الأمر الذي يحتم إجراء هذه الدراسة.

2- أهمية معرفة الأدوار الفعلية لإدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية في اليمن، وذلك في توعية الجمهور بمخاطرها؛ لاسيما مع ترافق زيادة التطور الحاصل في الجرائم الإلكترونية وتكنولوجيا الاتصال والإعلام مع زيادة أعمال الجرائم الإلكترونية وزيادة قدرات ومهارات مرتكبيها.

3- تأتي أهمية هذه الدراسة المنهجية من أنها من الدراسات البينية لكل من الإعلام والحاسوب وعلوم الاجتماع والأمن والقانون، وعدد من الدراسات أُجريت من قبل باحثين اجتماعيين أو أمنيين خارج القطر اليمني، فاختلفت، من ثَمَّ المفاهيم وأساليب القياس واختيار العينات وكيفية أو طبيعة تناول الموضوع؛ ويُعد هذا الاختلاف مبرراً أساسياً لإجراء الدراسة الحالية.

وسوف تركز الدراسة على مستوى قياس وعي الجمهور اليمني بالجريمة الإلكترونية في ثلاثة مستويات:

- المستوى الأول: الوعي بمفهوم الجريمة الإلكترونية.
- المستوى الثاني: الوعي بأساليب الجريمة الإلكترونية.
- المستوى الثالث: الوعي بطرق الوقاية من الجريمة الإلكترونية.

أهداف الدراسة:

1- الكشف عن معدل استخدام الجمهور اليمني للإنترنت.

2- الكشف عن نسبة الجرائم الإلكترونية التي تعرض لها الجمهور من مستخدمي الإنترنت.

3- الكشف عن نوع الجرائم الإلكترونية التي تعرض لها الجمهور من مستخدمي الإنترنت.

4- معرفة مدى وعي الجمهور بمفهوم الجريمة الإلكترونية.

5- معرفة مدى وعي الجمهور بأساليب الجريمة الإلكترونية.

6- معرفة مدى وعي الجمهور بطرق الوقاية من الجرائم الإلكترونية.

7- معرفة الأدوار الفعلية للجهات المسئولة عن الجريمة الإلكترونية في التوعية بمخاطرها.

الدراسات السابقة:

عُرضت الدراسات التي تناولت الجريمة الإلكترونية من خلال محورين أساسيين:

المحور الأول: الدراسات التي تناولت قياس مستوى الوعي في القضايا الإعلامية والاجتماعية، للاستفادة من طرق قياس الوعي:

1- **دراسة (الزبن والخرابشة، 2021م)، حول (الجرائم الإلكترونية ومستوى الوعي بخطورتها):**

هدفت الدراسة التعرف على الجرائم الإلكترونية ومستوى الوعي بخطورتها من وجهة نظر الشباب الجامعي الأردني، واستخدم استبانة لتحقيق أهداف الدراسة الوصفية، بالتطبيق على عينة مؤلفة من 212 طالب وطالبة من طلبة جامعة البلقاء التطبيقية، كشفت النتائج أن معدل تعرض الطلبة للجرائم الإلكترونية جاء بمستوى منخفض، كما بينت الدراسة أن قرابة 40% يقضون من ساعتين إلى أقل من أربع ساعات على الإنترنت، وتصدر موقع الفيس بوك التطبيقات المفضلة لدى عينة الدراسة، كما خلصت إلى أن نسبة 43% يستخدمون مواقع وتطبيقات الإنترنت بهدف الترفيه والتسلية، أما مستوى الوعي بالجرائم الإلكترونية فقد جاء مرتفعاً .

2- **دراسة (الحزورة وحيدر، 2020م، ص ص97-129) حول (استخدام الشباب اليمني للإنترنت وعلاقته بمستوى وعيهم بالشائعات الإلكترونية حول الأحداث الجارية):**

استهدفت الدراسة التعرف إلى العلاقة بين استخدام الشباب اليمني لشبكة الإنترنت بتطبيقاتها المختلفة ومستوى وعيهم بالشائعات الإلكترونية المنتشرة حول مجريات الأحداث والصراع في اليمن، واستخدمت منهج المسح على عينة عشوائية قوامها 400 مبحوث من الشباب المستخدمين للإنترنت في محافظة صنعاء، وتم جمع البيانات باستخدام استمارة استقصاء.

توصلت الدراسة إلى ارتفاع معدل استخدام الشباب اليمني للإنترنت، وعن وجود ارتباط طردي بين

معدل استخدام الشباب الإنترنت ومستوى وعيهم بالشائعات الإلكترونية حول مجريات الأحداث والصراع في اليمن، وكذلك وجود ارتباط طردي بين مستوى التفكير النقدي للشائعات لدى المبحوثين ومستوى وعيهم بالشائعات، كما أكدت على أن الإنترنت وتطبيقاتها المختلفة عملت على نشر الشائعات لدى أفراد العينة، لأنها أصبحت المصدر الأسرع والمتاح بالنسبة لهم في نقل الأحداث خاصةً في أوقات الأزمات.

3- دراسة (Khan2018،(، حول (الوعي بالجريمة الإلكترونية عبر الإنترنت بين طلاب كلية العمل الاجتماعي ومدرسة الخدمة الاجتماعية في مدينة مانجالور الهندية):

استهدفت الدراسة معرفة درجة الوعي بالجريمة الإلكترونية بين طلاب كلية العمل الاجتماعي مدرسة الخدمة الاجتماعية بمدينة مانجالور بالهند، ومعرفة إذا كانوا على دراية بالجرائم الإلكترونية وطرق مواجهتها، وتوصلت إلى ظهور أشكال جديدة من الجرائم الإلكترونية مع النمو السريع للإنترنت وتكنولوجيا الحاسوب، ومن تلك الجرائم الاحتيال وانتحال الشخصيات والسطو على بطاقات الائتمان وتتبع كلمات المرور الوصول غير المصرح به للأجهزة، وأن أغلب مستخدمي مواقع التواصل الاجتماعي والإنترنت في الهند يجهلون بآليات ومراكز الإبلاغ عن الجرائم الإلكترونية، جرى الاستقصاء بواسطة استبانة جرى تطبيقها على عينة بلغت 100 من الطلبة، وأظهرت الدراسة أن 58% من المبحوثين ليسوا على دراية بالجرائم الإلكترونية، و33% لا يغيرون كلمة المرور مطلقاً، و62% لا يعلمون المقصود بكلمة المرور القوية، وأجاب 32% بأن المؤسسات المالية معرضة بشكل أكبر للجرائم السيبرانية تليها المؤسسات الخاصة فالشركات القانونية، خلصت الدراسة إلى أهمية وعي طلبة الجامعات بطرق الوقاية من الجرائم الإلكترونية وعلى أهمية اضطلاع الحكومة الهندية بالقيام بمسئولياتها في التوعية التكنولوجية عن طريق برامج العمل والورش والمنتديات التثقيفية التوعوية.

4- دراسة (محمد، 2017م) حول (توظيف برامج العلاقات العامة في التوعية بمخاطر الجرائم الإلكترونية):

استهدفت الدراسة معرفة دور العلاقات العامة في التوعية بالجرائم الإلكترونية وخطورة الاستخدام الخاطئ للتكنولوجيا، وأجريت الدراسة التحليلية الوصفية على (الإدارات المسئولة عن الجرائم الإلكترونية بوزارة العدل، ووزارة الداخلية، ووزارة الاتصالات وتكنولوجيا المعلومات، والمركز السوداني لأمن المعلومات، الهيئة القومية للاتصالات بالسودان)، وحوت الدراسة الميدانية على استبانتين وزعت الأولى على الجمهور الداخلي من العاملين بالعلاقات العامة بالمؤسسات المسئولة عن الجرائم الإلكترونية، ووزِّعت الاستبانة الثانية على عينة من الجمهور الخارجي لقياس درجة الوعي بالجرائم الإلكترونية لديهم .

توصلت الدراسة إلى أن إدارات العلاقات العامة والإعلام بالمؤسسات المسئولة عن الجرائم الإلكترونية في السودان نجحت في تأسيس شراكات فاعلة واتفاقيات فيما بينها بخصوص التوعية بمخاطر الجرائم الإلكترونية بناءً على معرفتهم الجيدة بمخاطرها، وبوجود اتفاقيات دولية

قيد التنفيذ، وكانت أكثر الوسائل التي استخدمت لتلك الغاية هي الصحف والتلفاز، لكنها لم تهتم باستخدام الإعلام الرقمي في التوعية، كما بينت الدراسة أن مستخدمي الإنترنت لا يتمتعون بالحذر أثناء استخدام الإنترنت ولا يستخدمون برامج حماية ويفتحون الرسائل البريدية من المصادر المجهولة، وأن عدداً كبيراً من أفراد المجتمع يحرص على تثقيف نفسه بمخاطر التكنولوجيا الحديثة.

المحور الثاني: الدراسات التي تناولت الجرائم الإلكترونية، وذلك للاستفادة من تحديد متغيرات ومفاهيم الجرائم الإلكترونية وطرق قياسها:

5- دراسة (الهادي، 2020م) حول (تعرض المراهقين للجرائم الإلكترونية عبر الإنترنت وتأثيرها على إدراكهم للأمن الاجتماعي المصري):

استهدفت الدراسة الكشف عن مدى تعرض المراهقين للجرائم الإلكترونية، ورصد مواقع الإنترنت التي يتعرض لها المراهقون وتجعلهم عرضة للوقوع في الجرائم الإلكترونية، وكذا تحديد آثار الجرائم الإلكترونية التي يمكن أن تؤثر في المجتمع.

استخدمت الدراسة الوصفية أسلوب المسح الإعلامي الذي جرى تطبيقه باستمارة استقصاء على عينة قوامها 350 مفردة من المراهقين في محافظتي القليوبية والمنوفية، وقد خلصت إلى أن الجرائم الإلكترونية، التي يتعرض لها المراهقون هي الرسائل الضارة، يليها سرقة بعض الملفات من الحاسوب، ثم قرصنة البرامج، يليها إرسال رسائل إباحية، وأخيراً الفيروسات، كما أفاد المبحوثون أن أكثر أنواع الجرائم الإلكترونية انتشارا عبر الإنترنت هي الهجوم المتعلق بطلب فدية أو أموال من الآخرين عبر الإنترنت، ثم انتحال الشخصية فجرائم النصب والاحتيال، ثم استغلال الأطفال عبر الإنترنت ونشر مواد إباحية متعلقة بالأطفال، وبيع المواد المحرمة والممنوعة، كما خلصت إلى التأثيرات السلبية للجرائم الإلكترونية المتمثلة في انحراف الأحداث وعلى الأمن الاقتصادي وزعزعة الاستقرار الأسري والمجتمع، كما وجدت علاقة ارتباط ذات دلالة إحصائية بين معدل استخدام المراهقين للإنترنت وإدراكهم للأمن الاجتماعي.

6- دراسة (Rahmi & Hussain، 2019، pp 9-17) وكانت حول (الوقاية من الجرائم الإلكترونية الناجمة عن استخدام مواقع التواصل الاجتماعي):

استهدف الباحثان الخروج بحزمة توصيات تقنية تجنب مستخدمي مواقع التواصل الاجتماعي الوقوع ضحايا للجرائم الإلكترونية، خلصت الدراسة الوصفية إلى أن وسائل التواصل الاجتماعي تعد أداة ناجحة لمنع الجرائم الإلكترونية والتحقيق فيها، وإمكانية استفادة رجال الشرطة من ذلك إذا جرى التعامل معها بذكاء وحنكة، من خلال خبراء أمن المعلومات المناط بهم العمل على تصميم وابتكار تطبيقات للهواتف الذكية تعزز الوعي لدى مستخدمي وسائل التواصل الاجتماعي بطرق تجنب الوقوع ضحايا للجرائم الإلكترونية، كما خلصت الدراسة إلى حزمة من التنبيهات والتوصيات لتجنب 9 أنواع من الجرائم الإلكترونية، التي منها عدم فتح روابط المواقع المشكوك فيها أو المرسلة من مصادر مجهولة، وعدم الاستجابة للمكالمات غير المرغوب فيها، وأهمية نشر الوعي

العام والنشر والبث للمجتمع بجميع أساليب وطرق الاحتيال الإلكتروني والجرائم الإلكترونية التي يرتكبها بها المجرمون من خلال وسائل التواصل الاجتماعي، وطرق الوقاية منها وتجنبها، وعدد من المقترحات التقنية والهندسية للتقنيين فيما يتعلق بتعزيز أمن المعلومات للأفراد وللمؤسسات، كما خلص الباحثان إلى التحذير من انتحال الشخصية باستخدام مواقع التواصل الاجتماعي، بحيث يتلقى البعض رسائل من أصدقائهم من خلال مواقع التواصل بأرقامهم، يطلبون فيها مساعدة مالية فورية، وفي الواقع لم يتم إرسال تلك الرسائل من اصدقائهم بل من خلال المجرم الإلكتروني الذي سرق رسائل البريد الإلكتروني وكلمات المرور الخاصة بأصدقائهم.

7- **دراسة (الأطرش، عساف، 2019م، ص ص632-662) حول (معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية):**

استهدفت الدراسة التعرف على معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية، والمتعلقة بكل من (الجريمة المعلوماتية ذاتها، والمجني عليهم، والتحقيق الجنائي) وذلك من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية.

استخدم الباحثان المنهج الوصفي التحليلي والمقارن، وطبقا استمارة الاستبيان على 125 من العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية الفلسطينية (الشرطة، الأمن الوقائي، المخابرات العامة)، جرى اختيارهم بطريقة العينة المتيسرة، وقد توصلت الدراسة إلى النتائج تمثل المعوقات المتعلقة بالجريمة المعلوماتية ذاتها في البعد الجغرافي بين مرتكب الجريمة والضحية، وصعوبة الدليل الرقمي، وإمكانية خروجها عن إقليم الدولة، بالإضافة إلى المعوقات المرتبطة بالمجني عليهم في قلة وعي المستخدمين بخطورة الجرائم المعلوماتية، وإحجام بعض ضحايا الجرائم المعلوماتية عن إبلاغ السلطات المختصة.

8- **دراسة (الدحلة، 2018م) حول (دور صفحة وحدة مكافحة الجرائم الإلكترونية على موقع الفيسبوك في التوعية الأمنية):**

استهدفت الدراسة معرفة دور صفحة وحدة مكافحة الجرائم الإلكترونية (التابعة لشعبة البحث الجنائي لمديرية الأمن العام في الأردن)، في مجال التوعية الأمنية على موقع الفيسبوك، استخدم الباحث أداة تحليل المضمون لأربعة وخمسين منشورًا، توصلت الدراسة إلى أن القائمين على صفحة مكافحة الجرائم الإلكترونية ركزوا على المعلومات والضوابط التي توجه المتابعين لكيفية استخدام الإنترنت، أي استبعاد وقوع الجريمة، وعلى أساس أن الوقاية خير من العلاج، وبأسلوب التعليمات الإرشادية بنسبة 30،94% ما ينعكس بالإيجاب في زيادة الوعي التكنولوجي، كما ركزت صفحة وحدة مكافحة الجرائم الإلكترونية على المحتوى البصري في إيصال المعلومة بنسبة 65،07%، وهوما تعجز النصوص المكتوبة في إيصالها.

وتوصلت إلى أهمية إبراز العقوبات المفروضة على الجرائم الإلكترونية في وسائل الإعلام؛ بحيث تكون رادعاً للجمهور لتجنب ارتكابها، وتضمين بعض التعليمات والإرشادات بما يخص الجرائم الإلكترونية في المقررات الدراسية لتجنب ارتكابها

أو الوقوع بها كضحية، وعمل برامج توعية تخاطب الأسرة لدورها الكبير في تنمية المجتمع.

9- دراسة (Otter al. et 2015)، وهي دراسة حول (الجريمة الإلكترونية والشرطة):

عمل الدراسة باحثون في مفتشية الشرطة الملكية البريطانية HMIC باشتراك 6 قوى أمنية وعدلية بريطانية، استهدفت معرفة واقع الجريمة الإلكترونية وواجبات الشرطة البريطانية حيالها، استخدمت الدراسة المنهج الوصفي التحليلي بأسلوب المقابلة المعمقة مع 8 من ضحايا جرائم إلكترونية مختلفة، الذين قدموا بسخاء وصفاً لتجاربهم مع كونهم ضحايا للجرائم الإلكترونية، وقد ساعد ذلك الشرطة البريطانية على تطوير استجابة الخدمة لتلبية احتياجات الضحايا.

وأرجعت الدراسة صغر حجم العينة نظراً لأن تصنيفات الجرائم الإلكترونية ليست كبيرة بما يكفي لاستخلاص نتائج صحيحة إحصائياً.

توصلت الدراسة إلى أن ضحايا الجرائم الإلكترونية للمبحوثين في الدراسة لم يكونوا على وعي أو دراية بالتهديد الذي تشكله الجرائم الإلكترونية لهم، وهم يجهلون بشكل عام انتشار مثل هذه الجرائم، وكانوا غير متأكدين من الجريمة المحددة التي ارتكبت، وعدم اليقين هذا يعني أن الضحايا لم يكونوا قادرين على اتخاذ خطوات لمنع الجريمة أو تكرارها، وقد أظهر الضحايا في الدراسة تردداً في إبلاغ جهاز الشرطة، كما أظهرت الدراسة ضعف استجابة الشرطة البريطانية لشكاوى ضحايا الجرائم الإلكترونية، خلصت الدراسة إلى أهمية زيادة الوعي لدى رجال الشرطة ولدى الضحايا عند وقوع الجريمة.

أوجه الاستفادة من الدراسات السابقة:

1- الاستفادة في تحديد وتوصيف المشكلة البحثية، وفي وضع أهداف الدراسة وفي صياغة التساؤلات والفروض العلمية والإفادة في تحديد مصطلحات الدراسة.

2- اعتماد الدراسة على المنهج المسحي باستخدام استبانة أداة رئيسة لجمع بيانات ومعلومات الدراسة، مثل دراسة (الزبن والخرابشة 2021) ودراسة (الحزورة وحيدر، 2020م) ساعدت على تحديد المواقف والتقييم، وتعميق فهم الباحث لظاهرة الجرائم الإلكترونية، وبطبيعة وأهمية أدوار وسائل الإعلام في بث الوعي والتثقيف بخطورة الجرائم الإلكترونية.

3- استفادت الدراسة الحالية من الدراسات السابقة في التعرف إلى أساليب قياس وعي الجمهور بالجريمة الإلكترونية، مثل دراسة (الحزورة وحيدر، 2020م) التي استهدفت التعرف إلى أساليب قياس الوعي بمفهوم الشائعات وكيفية إدراك الجمهور للشائعات الإلكترونية، إلا أن الدراسة الحالية ركزت على دراسة مستوى وعي الجمهور اليمني بالجريمة الإلكترونية من خلال مقياس ثلاثي: (الوعي بمفهوم الجريمة الإلكترونية – الوعي بأساليب الجريمة الإلكترونية– الوعي بطرق الوقاية من الجريمة الإلكترونية).

تساؤلات الدراسة:

ترتكز هذه الدراسة على مجموعة من التساؤلات وفقاً للمحورين الآتيين:

المحور الأول: التساؤلات الخاصة بالمبحوثين:

1- ما معدل استخدام المبحوثين للإنترنت؟
2- ما هي نسبة تعرض المبحوثين للجرائم الإلكترونية؟
3- ما نوع الجرائم الإلكترونية التي تعرض لها المبحوثون؟
4- ما مستوى وعي المبحوثين بالجرائم الإلكترونية، من حيث:
أ- مفهوم الجريمة الإلكترونية.
ب-أساليب الجريمة الإلكترونية.
ت-طرق الوقاية من الجرائم الإلكترونية.
5- ما تقييم المبحوثين لجهود الجهات المسئولة عن الجرائم الإلكترونية من ناحية تلقيهم لتوعية من الجهات ذات العلاقة بمخاطر الجريمة الإلكترونية؟

المحور الثاني: التعرف إلى أدوار القائمين بالاتصال في إدارات الإعلام والعلاقات العامة في الجهات المسئولة عن التوعية بالجرائم الإلكترونية من ناحية التوعية بمخاطر الجريمة الإلكترونية:

1- ما مدى معرفة القائمين على الاتصال بمخاطر الجرائم الإلكترونية؟
2- هل توجد لوائح منظمة لعمل الإدارات فيما يتعلق بشأن واجباتها تجاه التوعية بمخاطر الجريمة الإلكترونية؟
3- هل تبذل الإدارات جهودًا في توعية المستخدمين بمخاطر الجرائم الإلكترونية؟
4- ما مقدار رضا القائمين بالاتصال عن الأدوار التي يقومون بها في مجال توعية الجمهور بمخاطر الجرائم الإلكترونية؟
5- من وجهة نظر القائم بالاتصال، هل يدرك الجمهور اليمني مخاطر الجريمة الإلكترونية، ويتمتع الجمهور بالوعي الكافي للوقاية من مخاطرها؟
6- هل تتحمل الجهات المسئولة عن الجرائم الإلكترونية مسئولية مباشرة في ضعف توعية وتثقيف الجمهور اليمني بمخاطر الجرائم الإلكترونية؟
7- ما المعوقات والصعوبات التي تحول دون قيام الجهات المسئولة عن الجرائم الإلكترونية بأدوارها المطلوبة في التوعية بمخاطر الجرائم الإلكترونية إن وجدت؟

التعريفات الإجرائية لمصطلحات الدراسة:

يقصد بالإنترنت في الدراسة الحالية: هو شبكة اتصالات إلكترونية تربط بين شبكات الكمبيوتر، وتربط بين ملايين الحواسيب حول العالم، وتتكون من ملايين الشبكات المنزلية والأكاديمية، والتجارية، والحكومية الصغيرة، ويقدم الإنترنت خدماته الفورية في التواصل المتجاوز لحدود الزمان والمكان مثل البريد الإلكتروني ومواقع التواصل الاجتماعي، التي أصبحت أدوات بيد المجرمين الإلكترونيين، سواء من داخل القطر اليمني أو من دولة أخرى لتنفيذ جرائمهم الإلكترونية، الذي يسهل عملهم التطورات الهائلة في تكنولوجيا الاتصالات والمعلومات بالإضافة إلى ضعف برامج التوعية والتثقيف بمخاطر الجرائم الإلكترونية وطرق الوقاية منها، إضافة إلى ضعف التشريعات والقوانين الوطنية الرادعة لمثل هذا النوع من الجرائم المستحدثة .

يقصد بالوعي في الدراسة الحالية: هو المعرفة التي يكتسبها الجمهور اليمني المستخدم للإنترنت، من المصادر الإعلامية التقليدية والجديدة المختلفة، التي يترتب عليها معرفته بمخاطر التحديات التكنولوجية المعاصرة المتمثلة بالجرائم الإلكترونية، وينعكس عليه سلوكاً من ناحية معرفة مخاطرها وتجنب الوقوع فيها وطرق التعامل السليم معها حال حدوثها، وتسهم الجهود المنظمة والاحترافية للجهات المسئولة عن الجرائم الإلكترونية في أعمال التوعية والتثقيف بمخاطر الجرائم الإلكترونية في حماية المواطنين والمنظمات والمؤسسات ضد التهديدات التي تواجه سلامتهم ورفاهية مجتمعهم.

يقصد بالجريمة الإلكترونية في الدراسة الحالية: هي الجريمة التي يمكن أن يرتكبها شخص ما، باستخدام جهاز حاسوب أو هاتف محمول ذكي أو الأجهزة اللوحية، وتتم من خلال الاتصال بشبكة الإنترنت من خلال البريد الإلكتروني أو مواقع في الإنترنت أو عبر مواقع التواصل الاجتماعي، ويكون هدفه إلحاق الضرر بالمجني عليه، سواء في ماله أو سمعته أو حالته النفسية والعقلية أو مكانته أو شرفه، ويشترط على مرتكب الجريمة الإلكترونية توفره على حاسب آلي أو هاتف محمول ذكي وشبكة إنترنت وتقنيات استعمالها، ويتميز مُرتكِب هذا النوع من الجرائم بالذكاء وعدة خصائص تمكنه من ارتكاب الجريمة.

يقصد بالإدارات المسئولة عن التوعية بمخاطر الجريمة الإلكترونية في الدراسة الحالية: هي إدارات العلاقات العامة والإعلام بالجهات المسئولة عن الجريمة الإلكترونية في اليمن، والمناط بها التوعية والتثقيف بمخاطر الجرائم الإلكترونية، وبما يخدم تحقيق الأمن الإلكتروني المجتمعي بالمفهوم الحديث، وهي:

1- إدارة الإعلام الأمني بوزارة الداخلية.
2- إدارة الإعلام بالمؤسسة العامة للاتصالات.
3- إدارة الوعي التكنولوجي الرقمي بالمؤسسة العامة للاتصالات.
4- إدارة التسويق بشركة تيليمن.
5- إدارة التسويق بشركة يمن نت.
6- إدارة العلاقات العامة والتوعية القضائية بوزارة العدل.

7- **حدود الدراسة:**

الحدود الموضوعية:

ركز الباحث على دراسة واقع الجريمة الإلكترونية في المجتمع اليمني، وعلى مسئولية الجهات ذات العلاقة بالجريمة الإلكترونية في توعية الجمهور اليمني بمخاطر الجريمة الإلكترونية.

الحدود المكانية:

تم تنفيذ الدراسة الوصفية في العاصمة اليمنية صنعاء؛ كونها تتمتع بكثافة سكانية كبيرة، والنسيج السكاني فيها ينحدر في غالبيته من سائر محافظات الجمهورية، وباعتبار وجود الجهات الرسمية ذات العلاقة بالجرائم الإلكترونية في صنعاء، الذي سهل جمع معلومات وبيانات الدراسة.

الحدود الزمنية:

تم تنفيذ الدراسة خلال المدة 15 مايو 2021م إلى 31 أكتوبر 2022م

الإجراءات المنهجية:

تنتمي هذه الدراسة للبحوث الوصفية التي تعتمد على منهج المسح للحصول على البيانات الكمية التي تساعد على تحديد المواقف والتقييم، باستخدام استبانة أعدت لتحديد واقع الجريمة الإلكترونية في المجتمع اليمني وتقييم الجمهور لأداء الجهات الرسمية ذات العلاقة بالجريمة الإلكترونية من ناحية التوعية بمخاطر الجريمة الإلكترونية، وبعد ذلك جمع الباحث البيانات الكيفية باستخدام أداة "المجموعات المركزة Focus groups" من الجمهور اليمني المستخدم للإنترنت من ذوي الاهتمام بموضوع الجريمة الإلكترونية لشرح النتائج الكمية وتفصيلها، كما امتد جمع البيانات الكيفية ليشمل أداة " المقابلة المقننة Structured interview" مع مدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية كجانب مهم يفسر العوامل المؤثرة في تشكيل وعي الجمهور اليمني بالجريمة الإلكترونية ومسئولية الجهات ذات العلاقة حيال ذلك الوعي.

عينة الدراسة:

أجريت الدراسة الميدانية (الكمية) على عينة عشوائية من الجمهور اليمني المستخدم للإنترنت، وبلغ عدد أفراد العينة 400 مفردة (204 من الذكور و196 من الإناث)، وتكونت عينة الدراسة في المرحلة (النوعية) من ثلاث مجموعات مركزة، حيث شملت المجموعة الأولى (7 ذكور)، والمجموعة الثانية (7 إناث)، والمجموعة الثالثة (7 ذكور وإناث)، بالإضافة إلى إجراء المقابلات الكيفية المقننة مع القائمين بالاتصال وعددهم (12) من مدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية.

أدوات جمع البيانات:

استخدمت الدراسة ثلاث أدوات لجمع المعلومات في الدراسة، الأولى: الاستبانة جرى توزيعه يدوياً وإلكترونياً على عينة الدراسة، خلال المدة 15 يوليو 2022م حتى 31 أكتوبر 2022م ، الذي تضمن عدداً من المحاور التي تحقق أهداف الدراسة وتجيب عن تساؤلاتها وفروضها، حيث يعتبر الأداة الرئيسية الملائمة للدراسة الميدانية التي تهدف الحصول على البيانات والمعلومات من الأفراد، أما الأداة الثانية فقد تمحورت حول جمع البيانات من خلال المجموعات المركزة (البؤرية) كأداة مهمة من أدوات البحث النوعي الكيفي، وقد عقدت ثلاث مجموعات مركزة بهدف الحصول على معلومات بشأن واقع الجريمة الإلكترونية في اليمن وحجم انتشارها.

وقد تمثلت الأداة الثالثة في استمارة المقابلة المقننة التي جرى تطبيقها على مديري ومسئولي إدارات العلاقات العامة والإعلام بالجهات المسئولة عن الجريمة الإلكترونية.

إجراءات الصدق والثبات:

الصدق: تم الاعتماد على صدق المحتوى، أو ما يسمى بالصدق الظاهري في التأكد من صدق أداة الدراسة وبأنها تقيس ما صممت فعلاً لقياسه، حيث جرى عرض الاستمارة مع الأهداف والتساؤلات والفروض على مجموعة من المحكمين [1]، وجرى

(1) السادة المحكمون، هم:
أ. د/ على العمار- أستاذ الصحافة بكلية الإعلام – جامعة صنعاء.
أ. م. د/ على البريهي – أستاذ الإذاعة والتلفزيون المشارك بكلية الإعلام – جامعة صنعاء.

الأخذ بآرائهم وتعديل صياغة العبارات التي اتفق المحكمون عليها.

الثبات: للتحقق من ثبات أداة الدراسة استُخدم أسلوب إعادة الاختبار Test-Retest على عينة عشوائية مقدارها 10% من إجمالي حجم العينة الأصلية، حيث طبق الباحث الاستمارة على عدد (40) شخصاً من مستخدمي الإنترنت بأمانة العاصمة، ثم أعيد تطبيق الاستمارة على تلك المجموعة نفسها؛ وذلك بعد مرور أسبوعين من تطبيق الاختبار الأول، وقد بلغت قيمة معامل الثبات (0.88)، وهي قيمة عالية تشير إلى ثبات المقياس ودقته.

الإطار النظري لمفاهيم الدراسة:

أولاً: محور تخطيط برامج العلاقات العامة الحديثة:

المفهوم الحديث للعلاقات العامة:

أصبحت العلاقات العامة في المجتمع الحديث معقدة وليست بسيطة، واصبح على ممارسي العلاقات العامة في المجتمع الحديث أن يوجهوا عناية خاصة إلى الدراسات العلمية للعلاقات الإنسانية بين الفرد والجماعة وبين المؤسسات الحكومية والأهلية، وتعد العلاقات العامة هي الوظيفة التي تقوم بها الإدارة لتقويم الاتجاهات وتحديد السياسات نحو الأفراد أو المنظمة بما يتفق مع مصلحة الجمهور والسعي لكسب رضاه، وينبثق عن ذلك أهمية وجود اتصال بين المنظمة والجمهور، ومن هنا يتضح أنه لابد من النظر في الآتي عند الحديث عن مفهوم العلاقات العامة:

1- الاتصال: هو وسيلة نشر المعلومات والأفكار والحقائق ونقل آراء الجمهور إلى المنظمة، وهذا الاتصال نظام سلوكي يستوجب مراعاة أخلاق الجمهور وأذواقهم.
2- الأساليب: تختلف من مجتمع إلى آخر، ولا بد من فهم السلوك البشري؛ لأنه يمثل الركيزة الأساسية لنجاح أي برنامج للعلاقات العامة.
3- البعد الإداري: وهي نشاط إداري يحتاج إلى كل العمليات الإدارية كالتخطيط والتنظيم والتنسيق والتوجيه والرقابة، وتحتاج إلى مهارة فن وعلم.
4- البعد الإنساني: يعني أن تتمتع الإدارة بالإنسانية في تعاملها مع الجمهور ليفهم هذا الجمهور دور العلاقات العامة وما تقدمه له الإدارة (سعيد، 2013، ص22).

وبات من المسلمات أن أي كيان مهما كان صغيراً أو محدوداً لا يمكن أن يصيب الهدف ويحقق الغاية دون أن يكون لعملية التخطيط دور فيه، كما أن من أهم دعائم العلاقات العامة قيامها بعملية الاتصال بالجماهير لمعرفة آرائهم واتجاهاتهم ورغباتهم وحاجاتهم وحل مشاكلهم، ثم تعديل سياسات المؤسسات بما يتفق والسياسات التي

د/ حسين جغمان – رئيس قسم الإذاعة والتلفزيون الأستاذ المساعد بكلية الإعلام – جامعة صنعاء.
د/ مهدي حيدر – رئيس قسم العلاقات العامة الأستاذ المساعد بكلية الإعلام – جامعة صنعاء.
د/ نوال الحزورة – أستاذة الإذاعة والتلفزيون المساعدة بكلية الإعلام – جامعة صنعاء.
د/ هزاع شرف – أستاذ العلاقات العامة المساعد بكلية الإعلام – جامعة صنعاء.
د/ يوسف سلمان – رئيس قسم العلوم الاجتماعية والإعلام الأستاذ المساعد جامعة العلوم والتكنولوجيا.
د/ إسماعيل حميد – أستاذ علوم الحاسوب المساعد بكلية الحاسبات جامعة العلوم والتكنولوجيا.
أ م. د/ نديم الترزي - نائب رئيس أكاديمية الشرطة للشئون التعليمية، أستاذ القانون الجنائي المشارك.

تحقق الأهداف المشتركة للمنشآت وجماهيرها (حجاب، وهبي، 1993، ص14)، وتقوم العلاقات العامة من جهة أخرى بإعلام الجماهير بنوعية وحجم الأنشطة والخدمات التي تقدمها المنشآت المختلفة، فمن أهداف العملية الاتصالية الإقناع وتحقيق الفهم المتبادل بين الأطراف كافة من خلال وائل مؤثرة تستطيع التعرف إلى مدى تفهم الجماهير للمعلومات والمعارف المقدمة إليهم (الجوهري، 1997، ص4) .

أهمية الاتصال الإقناعي في الحملات الإعلامية الخاصة بتنمية وعي الجمهور:

تعد الحملات التوعوية والتفكير بشأن تحسين سلوك الجمهور المستهدف ووعيه بالقضايا المختلفة من أهم أهداف الحملات الإعلامية، التي يدخل في إطارها أيضاً ترقية السلوك وتفادي الكثير من الإشكاليات الناتجة عن قلة الوعي أو عن الحملات التوعوية غير المدروسة التي تتم عبر جهات غير مختصة وليست ذات دراية بدراسة الاتجاهات والآراء والسلوك، ويتطلب نجاح ذلك استخدام جميع الأساليب الاتصالية الإقناعية المختلفة في التوعية (خيرالدين، 1986م، ص ص50-53).

فالإعلام عملية تهدف إلى توعية وتثقيف وإقناع مختلف فئات الجماهير باختلاف ثقافاتهم وعاداتهم ودرجة وعيهم من خلال فكرة محددة تدور حول معنى معين يهدف إلى تزويد الناس بأكبر قدر ممكن من المعلومات الصحيحة والحقائق الواضحة، التي تثير الرأي العام حول القضايا والأحداث ذات الصلة بحياتهم، مما يساعد على تكوين رأي عام صائب عن طريق الإقناع بالمعلومات والحقائق الموثوقة القائمة على الصراحة والوضوح والدقة؛ لذلك يجب أن تقام البرامج الإعلامية على أساس تخطيط علمي مدروس وبحوث دقيقة تتناول الموقف الإعلامي بكافة مكوناته، حيث إن التخطيط الإعلامي بشكل عام يهدف إلى تغيير السلوك والعادات والممارسات الضارة، وتحويلها إلى قيم وعادات وممارسات صادقة تنبع من عقيدة الأمة؛ لهذا لا بد من دراسة اتجاهات المتلقين وأفكارهم وعاداتهم وتقاليدهم، إضافة إلى الرأي العام، علاوة على أن التخطيط الإعلامي يجب أن يترجم إلى برامج واقعية تنفيذية خاضعة للتقييم وذلك من أجل معرفة مدى نجاحها أو قصورها في تحقيق الأهداف المنشودة (كافي، 2015، ص ص 66-67).

ويتطلب الاتصال الإقناعي للحملات الإعلامية تخطيطاً ناجحاً قائماً على مجموعة من المتطلبات من أهمها:

1- وجود مخططين أكفاء مدربين مؤهلين علمياً وعملياً.
2- وجود دعم مالي وإمكانيات مساعدة وتوفر الوسائل المطلوبة.
3- وجود منفذين مهرة وذوي خبرة وكفاءة ووجود تنسيق فعال يشمل توزيع المسؤوليات.
4- العمل على وضع خطة تراعي كل الجوانب وتعمل على معالجة كافة القضايا.
5- دعم أدبي بالموافقة على كل تصورات ومشروعات كوادر رجال العلاقات العامة (محمد، 2017م، ص62).

ويعتبر الوعي حالة فكرية متقدمة من الفهم ينتج عن تراكم معرفي يتجاوز العلم أو التعرض العابر

للرسائل، ليصبح جزء من منظومة الفرد الفكرية للتأصيل لسلوكيات محددة، التي مع مرور الزمن تصبح جزءًا ضمن أنساق المجتمع الثقافية، وعادة ما يتكون الوعي مع تراكم الرسائل الاتصالية المتنوعة في الوسائل والشكل والمضمون (بيت المال، 2014، ص16).

أنواع الحملات الإعلامية:

أصبح الإعلام الأداة الأولى للتأثير في الجماهير والمجتمعات، لاسيما بعد تسارع الأحداث وضيق الوقت وانتشار البدائل الكثيرة للوسائل المرئية والمسموعة والمقروءة، بحيث أصبح الرأي بحد ذاته يضغط من أجل الحصول على الأفكار من وسائل الإعلام، وقد أحدث النشاط الاجتماعي العديد من القضايا الاجتماعية، التي يهدف البعض منها إلى إصلاح مشكلة اجتماعية كتعاطي المخدرات، وتهدف كل قضية إلى تحقيق هدف اجتماعي ويضمن هذا الهدف إحداث تغيير كما يلي (الحديدي، 2004، ص ص13-14) :

1- حملات التغيير المعرفي:

التي تهدف غالباً إلى تزويد الأفراد بالمعلومات وزيادة وعيهم بقضية ما أو تصحيح معارفهم المغلوطة أي العمل على إحداث التغيير المعرفي، وهذا النوع من المعلومات العامة أو التعليم العام يشمل كذلك الحملات التي تتعلق بزيادة وعي الأفراد كيفية تجنب الإصابة بمرض ما، أو بالتوعية بطرق الوقاية من الجرائم الإلكترونية، ويعتبر هذا النوع من الحملات من أسهل حملات التغيير الاجتماعي؛ لكون هدفها ينحصر في إعطاء الأفراد المعلومات التي تتعلق بالقضية محور الحملة الاجتماعية.

2- حملات تغيير الفعل:

التي تهدف إلى إقناع أكبر عدد ممكن من الأفراد للقيام بضرورة التطعيم مثلاً للوقاية من مرض معين، أو حث الأمهات على تطعيم أطفالهن، وتتجاوز أهداف هذا النوع من الحملات مجرد إخبار الجماهير بمعلومات معينة إلى حثهم على عمل أو فعل ما، وقد يتطلب هذا الفعل صرف وقت وجهد ومال.

3- حملات التغيير السلوكي:

تهدف إلى حث الأفراد على تغيير بعض أنماط سلوكهم كالحملات التي تحث الأفراد على الإقلاع عن التدخين، وتعد من أصعب الحملات، حيث يصعب تغيير بعض أنماط السلوك والعادات التي اعتاد الأفراد على قيامهم بها لمدة طويلة.

4- حملات تغيير القيم:

التي تستهدف تغيير القيم والمعتقدات، مثل حملات تنظيم الأسرة، وتلجأ إليها هيئات معينة بدلاً من القوانين التي تلزم الأفراد بتغيير معتقداتهم، التي لا يمكن تغييرها من تلقاء أنفسهم.

مسئولية وواجبات إدارات الإعلام والعلاقات العامة بالجهات ذات العلاقة حيال أعمال التثقيف والتوعية بمخاطر الجرائم الإلكترونية:

يعد الباحث أن عمل إدارات الإعلام والعلاقات بالجهات المسئولة عن الجرائم الإلكترونية في اليمن هو في جزء منه يندرج في إطار ما بات يُعرف بالإعلام الأمني، الذي يُعد من المصطلحات الحديثة التي ذاعت وانتشرت وتبوأت مكانتها بين مختلف أساليب الإعلام النوعي، وهو(كل ما تقوم به الجهات ذات العلاقة من أنشطة إعلامية ودعوية وتوعوية بهدف المحافظة

على أمن الأفراد والجماعة، وأمن الوطن ومكتسباته في ظل المقاصد والمصالح المعتبرة، فتنساب الرسائل الإعلامية بالأشكال والقوالب المناسبة بما يحقق التجاوب الجماهيري مع الرسائل التوعوية والأفكار الامنية المطروحة، ويستهدف تكوين رأي عام مستنير وواع بشأن القضايا المتعلقة بمكافحة الجريمة وإقرار الأمن، ويتطلب ذلك عملاً مخططاً وفقاً لمعايير احترافية)(الحاج، 2016، ص ص130-131) .

كما أن أعمال التثقيف والتوعية بمخاطر الجرائم الإلكترونية إنما يستهدف منع وقوع الجرائم الإلكترونية أصلاً والحد من تبعاتها ونتائجها الكارثية على الأفراد والمجتمعات، المثبتة في الكثير من الدراسات والتقارير الدولية.

وانطلاقاً من مهام أجهزة الإعلام في المجتمعات من أجل تهيئة المناخ المساعد على الاستقرار والتنمية، وبالنظر إلى ما يقرره فقهاء القانون والعلوم الأمنية أن (أية محاولة لحل مشكلة الجريمة دون الاعتماد على مشاركة الجمهور لا شك أنها محاولة عقيمة) (عدلي، 2011، ص505)؛ فإنه ينبثق عن ذلك أهمية اضطلاع إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجرائم الإلكترونية في اليمن بواجباتها في التوعية وتثقيف الجمهور اليمني من المستخدمين بمخاطر الجريمة الإلكترونية، التي ستخفف بالضرورة من الأعباء الملقاة على جهات التحقيق الشرطية والعدلية والقضائية.

أهمية النهج التوعوي الاستباقي في مواجهة الجريمة الإلكترونية في اليمن:

وفقاً لملاحظة الباحث واللقاءات التي أجراها مع عدد من المختصين في الجهات ذات العلاقة بالجرائم الإلكترونية، ومنها وزارة الداخلية أحد الجهات المسئولة الرئيسة عن الجرائم الإلكترونية، وجد الباحث اعتماد وزارة الداخلية بالعاصمة صنعاء ممثلةً بالإدارة العامة للبحث الجنائي والأجهزة الأمنية ذات العلاقة في تعاملها مع الجرائم الإلكترونية على (النهج الأمني التفاعلي) بعد وقوع الجرائم الإلكترونية في حالة ورود البلاغات بذلك الشأن، حيث يجرى التحقيق في تلك الجرائم بناءً على قانون العقوبات والجزاءات القديم المعمول به، ويرى الباحث أنه لا يجب الرهان والتعويل على (النهج الأمني التفاعلي) في التعامل مع الجرائم الإلكترونية على الرغم من أهميته ولزوميته، بل إن الأمر يجب أن يمتد ليشتمل على (النهج التوعوي الاستباقي) القائم على توعية الجماهير والأفراد من مستخدمي الإنترنت ومواقع التواصل الاجتماعي والتثقيف بطرق وأساليب الوقوع في شراك الجرائم الإلكترونية ومدى خطورتها على الفرد والمجتمع وكيفية الوقاية منها، وطرق التعامل معها والتبليغ عنها حال حدوثها، وبما يسهم في تجنب خسارة الأفراد لصحتهم النفسية ولأموالهم ومعلوماتهم وسلامتهم الشخصية، وهنا تتجسد أدوار إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجرائم الإلكترونية في أنشطتها وبرامجها وفعالياتها التوعوية والتثقيفية بمخاطر الجريمة الإلكترونية بما يعمل على تحصين الأفراد والمؤسسات والمجتمع من الوقوع في تلك الجرائم، وسينعكس ذلك الجهد إيجاباً على وعي المستخدمين بمن فيهم

قادة الرأي والسياسيين، بما يسهم في خلق وتكوين الإرادة السياسية اللازمة لسن القوانين والتشريعات المتعلقة بمكافحة الجرائم الإلكترونية.

ثانياً: محور الجرائم الإلكترونية وأمن المعلومات:

أنواع الجرائم الإلكترونية:

فيما يلي تصنيف أهم الجرائم الإلكترونية، بحسب علاقتها بالجرائم التقليدية:

1- جرائم إلكترونية ضد الأفراد: وهي الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق غير مشروعة، كحسابات البريد الإلكتروني وكلمات السر التي تخصهم، وقد يصل الأمر إلى انتحال شخصياتهم وأخذ الملفات والصور المهمة من أجهزتهم بهدف تهديدهم بها ليمتثلوا لأوامرهم.

2- جرائم إلكترونية ضد الملكية: تستهدف المؤسسات الشخصية والحكومية والخاصة، وتستهدف إتلاف الوثائق الهامة أو البرامج الخاصة، وتتم عن طريق نقل برامج ضارة لأجهزة هذه المؤسسات باستخدام الكثير من الطرق كالرسائل الإلكترونية.

3- الجرائم السياسية الإلكترونية: وهي جرائم تستهدف المواقع العسكرية للدول، من خلال سرقة معلومات تتعلق بالدولة وأمنها.

4- سرقة المعلومات: ويشتمل هذا النوع من الجرائم سرقة المعلومات المحفوظة إلكترونياً وتوزيعها بأساليب غير مشروعة (موقع موضوع، أنواع الجرائم الإلكترونية، 2020).

5- الإرهاب الإلكتروني: ويشتمل على اختراقات للأنظمة الأمنية الحيوية على مواقع الإنترنت، تكون جزءاً من مجهود منظم لمجموعة من الإرهابيين الإلكترونيين، وتعد مواقع التواصل الاجتماعي والإنترنت وسائل نموذجية للجماعات الإرهابية لبث الأفكار المتطرفة واستقطاب وتجنيد جهاديين جدد (الفقيه والصالحي، 2017، ص ص 273-320).

6- جرائم الاحتيال والاعتداء على الأموال: وتتم من خلال إدخال بيانات غير صحيحة أو تعليمات من غير المشروع التصريح بها، بغية السرقة من قبل موظفين فاسدين في الشركات والمؤسسات المالية، أو بحذف أو تعديل المعلومات المحفوظة، أو إساءة استخدام أدوات الأنظمة المتوافرة وحزم البرامج، أو من خلال التصيد الإلكتروني.

7- الجرائم الإلكترونية المتعلقة بالجنس: ومنها ما تعج به المواقع الإلكترونية من صور وأفلام إباحية، التي تعد من الجرائم التي تستهدف التحلل من الأخلاق والقيم، وتمتد لتشمل استغلال الأطفال والفتيات في مثل تلك الأعمال، التي هي مجرّمة في أغلب قوانين مكافحة الجرائم الإلكترونية على مستوى الدول.

8- جرائم الابتزاز الإلكتروني: وهي أن يتعرض نظام حاسوبي أو موقع إلكتروني ما لهجمات حرمان من خدمات معينة، حيث يشن هذه الهجمات ويكررها قراصنة محترفون؛ بهدف تحصيل مقابل مادي لوقف هذه الهجمات.

9- جرائم السب أو القذف أو التشهير: بغرض المساس بشرف الآخرين وسمعتهم، ويقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية، لتصل المعلومات المراد نشرها إلى

أعداد كبيرة من مستخدمي شبكة الإنترنت (البهي، 2018، ص 242).

10- المطاردة الإلكترونية: والمقصود بها الجرائم المتعلقة بتعقب أو مطاردة الأفراد عن طريق الوسائل الإلكترونية لغاية تعريضهم للمضايقات الشخصية أو الإحراج العام، أو السرقة المالية وتهديدهم بذلك.

طرق ارتكاب الجرائم الإلكترونية:

يتم ارتكاب الجرائم الإلكترونية من خلال عمليات القرصنة التي تصل إلى أنظمة الحواسيب، أو حسابات البريد الإلكتروني، أو مواقع الويب بطرق غير مصرَّحة، وكذلك الفيروسات والبرامج الضارة التي تضر البيانات، وتجعلها عرضة للسرقة، حيث يسرق المخترقون بيانات شخصية مثل أرقام بطاقات الائتمان، ومعلومات الحساب المصرفي، لهذا يجب الحماية من المخاطر باستخدام إجراءات أمان الإنترنت (موقع موضوع، الحماية من الجرائم الإلكترونية، 2020)، وقد يقع الأفراد ضحايا للجرائم الإلكترونية الناجمة عن الدخول في روابط مجهولة عن طريق الاستدراج بأساليب الهندسة الاجتماعية.

واقع الجريمة الإلكترونية في اليمن:

على الرغم من التطور الذي شهدته اليمن في مجال الاتصالات وتقنية المعلومات وإدخال خدمة الإنترنت في وقت مبكر عام 1996م، إلا أن مجال أمن المعلومات الإلكتروني في اليمن لم يحظ بالاهتمام اللائق من مختلف القطاعات (الحكومية والخاصة والمجتمع المدني)، الذي انعكس على هشاشة أمن المعلومات الأمر الذي جعل البلاد هدفاً للجرائم الإلكترونية بمختلف أشكالها ومصادرها، وقد بلغ عدد مستخدمي الإنترنت في اليمن في شهر يناير 2021م حوالي 8،06 مليون مستخدم (ذمران، 2021، ص ص1-2)، وقد حصلت اليمن في العام 2018م على تقييم دولي متدنٍ في الأمن الإلكتروني، حيث جاءت في الترتيب 172 من جملة 175 بلداً على مستوى دول العالم في مستوى الأمن الإلكتروني، بحسب تقرير الدليل العالمي للأمن السيبراني للاتحاد الدولي للاتصالات (ITU) عام 2018م، كما تعتبر اليمن من بين أكثر 10 دول عالمياً من حيث مشاركة البرمجيات الضارة (الوصابي، 2021، ص9)، ويرجع ضعف البنية المعلوماتية الاتصالية في اليمن وهشاشتها بدرجة أساسية إلى غياب التشريعات والقوانين المعززة للأمن الإلكتروني، خاصة في مجال مكافحة الجريمة الإلكترونية، إلى جانب غياب البرامج التوعوية والتثقيفية بمفهومها ومخاطرها، كما أن غياب برامج التوعية والتثقيف بمخاطر الجريمة الإلكترونية للجهات ذات العلاقة قد أثر أيضاً على ضعف الوعي لدى صانعي القرار السياسي والتشريعي بأهمية إقرار وإنفاذ قانون يعنى بمكافحة الجريمة الإلكترونية، حيث إن قانون مكافحة الجرائم الإلكترونية لم يراوح مكانه في أدراج بيروقراطية مجلس النواب اليمني منذ أواخر العام 2020م، الذي لم يقر حتى وقت إعداد هذه الدراسة.

وقد بلغ عدد الجرائم الإلكترونية المبلغ عنها بالبحث الجنائي في نطاق أمانة العاصمة صنعاء خلال عامين من تاريخ 1سبتمبر2018م حتى 1سبتمبر 2020م أكثر من (500) جريمة

إلكترونية، وهي تعد نسبة بسيطة من حجم الجرائم الإلكترونية الفعلية الواقعة على الأفراد والمؤسسات (سراج، 2021، ص ص 16-17)، نظراً لإحجام الكثير من الأفراد والمؤسسات عن التقدم بالإبلاغ لخشيتهم من الفضيحة أو لعدم ثقتهم في قدرة الأجهزة الأمنية على ضبط الجناة.

وتتم الإحالة بوقوع الجرائم الإلكترونية إلى الإدارة العامة للبحث الجنائي، في ظل عدم وجود قانون مكافحة جرائم تقنية المعلومات، وتتم الإحالة من البحث الجنائي بعد التحقيق إلى نيابة البحث الجنائي، التي تقوم بدورها بإحالة ملف القضية إلى المحكمة المختصة حسب الاختصاص المكاني للقضية فقط، حيث لا توجد نيابة متخصصة بالجرائم الإلكترونية، كما لا توجد محاكم متخصصة بالجرائم الإلكترونية حتى وقت إعداد هذا البحث (اليوسفي، 2021).

النتائج العامة للدراسة:

أولاً: نتائج الدراسة الميدانية والتحليل النوعي للمجموعات المركزة:

جدول رقم (1) توزيع الجمهور طبقاً لمعدل استخدامهم اليومي للإنترنت

م	التكرار والنسبة / مدى الاستخدام	التكرار	النسبة
.1	من يوم إلى يومين	63	15.7
.2	من ثلاثة أيام إلى أربعة أيام	43	10.8
.3	من خمسة أيام إلى سبعة أيام	294	73.5
الإجمالي		400	100

تشير بيانات الجدول السابق إلى ارتفاع معدل الاستخدام اليومي للمبحوثين للإنترنت من خمسة أيام إلى سبعة أيام، الذي جاء في المرتبة الأولى بنسبة (73.5%)، وجاء في المرتبة الثانية الاستخدام اليومي للإنترنت من يوم إلى يومين بنسبة (15.7%)، تلاه الاستخدام اليومي للإنترنت من ثلاثة أيام إلى أربعة أيام بنسبة (10.8%)، وهذا يشير إلى ما أصبح يمثله الإنترنت من وسيلة اتصال رقمي أحدث تحولات في المجتمع اليمني، ووفقاً لما أشارت إليه نتائج التحليل النوعي للمجموعات المركزة من أن الإنترنت أصبح معززاً للاتصال الإلكتروني وإمكانيات الوصول إلى الخدمات التجارية والعامة وتيسير بيئة التعليم الافتراضي والتعلم عن بعد واستخدامات الترفيه والتواصل الاجتماعي من خلال منصات الإنترنت، وسهولة الوصول إلى البيانات والمعلومات وتجاوز حدود الاتصال الزماني والمكاني، بالإضافة إلى أن الإنترنت أصبح يمثل قدرة الأفراد لصناعة المحتوى الإعلامي الشخصي والمؤسسي بعيداً عن (مقص الرقيب)، الأمر الذي انعكس على زيادة معدل الاستخدام اليومي للإنترنت.

وتتشابه هذه النتيجة مع دراسة (الحزورة وحيدر، 2020، ص 211)، التي توصلت نتائجها إلى ارتفاع معدل استخدام الشباب اليمني للإنترنت، كما تتشابه مع دراسة (محمد، 2017، ص 238)، التي توصلت إلى زيادة معدل استخدام الجمهور السوداني اليومي للإنترنت.

جدول رقم (2) توزيع المبحوثين طبقاً لعدد الساعات التي يستخدمون فيها الإنترنت:

م	التكرار والنسبة / مدى الاستخدام	التكرار	النسبة
.1	أقل من ساعتين	118	29.5
.2	من ساعتين إلى أقل من أربع ساعات	140	35
.3	أربع ساعات فأكثر	142	35.5
	الإجمالي	400	100

يتضح من خلال الجدول السابق زيادة حجم استخدام المبحوثين اليومي للإنترنت، حيث جاء في المرتبة الأولى الاستخدام الكثيف للجمهور عينة الدراسة (أربع ساعات فأكثر) بنسبة (35.5%) من إجمالي عينة الدراسة، وجاء في المرتبة الثانية الاستخدام المتوسط من (ساعتين إلى أقل من أربع ساعات) بنسبة (35%)، تلاه الاستخدام (أقل من ساعتين) بنسبة (29.5%)، وتعكس نتيجة الجدول السابق زيادة حجم اعتماد المبحوثين على الإنترنت؛ نظراً لكون خدمة الإنترنت أصبحت متوفرة سواءً من خلال الهاتف أو عبر شبكات الواي فاي الشخصية والعامة، مما أدى إلى كثافة استخدام الإنترنت كعادة يومية متكررة لدى الجمهور اليمني لدرجة تصل لدى البعض حد الإدمان، كما يجعل كثافة الاستخدام العالية للإنترنت لدى الجمهور اليمني؛ يجعلهم عرضة لكل تأثيراتها، بما في ذلك التأثيرات السلبية ومنها إمكانية تعرضهم للجرائم الإلكترونية.

وفي إطار تحليل إجابات المشاركين بالمجموعات المركزة أظهر التحليل النوعي إجماع المشاركين بالمجموعات المركزة على ارتفاع حجم وكثافة استخدام الجمهور اليمني للإنترنت، وفقاً لما عبرت عنه المشاركة (أ ش) بقولها: "تزايد إقبال المجتمع اليمني بصفة عامة والشباب بصفة خاصة على التعامل مع وسائل الإعلام الرقمي والإنترنت؛ نظراً لما وفرته من ميزات من حيث التكلفة وسرعة التدفق وسهولة الوصول إلى المستقبِل والتفاعلية وتوفير التسلية وتسيير الأعمال وكمصدر للأخبار والمعلومات"، فيما لفت المشارك (م س) بالمجموعات المركزة إلى ازدياد نسبة استخدام الإنترنت في اليمن في السنوات الأخيرة بسبب: "الرغبة في الهروب من الواقع والأوضاع المعيشية الصعبة، فأصبح الإنترنت يشكل نوع من السلوى والبحث عن أمل للكثيرين"، كما أشارت بيانات التحليل النوعي للمجموعات المركزة انتقال الجمهور من الوضع السلبي في علاقته بالوسائل الإعلامية الجماهيرية إلى المستخدم المنتج في علاقته بوسائل الإعلام الرقمي الجديدة والإنترنت، مظهراً قدرته على المشاركة وبناء وإنتاج معنى لما يتعرض له من مضامين إعلامية واتصالية، باستثناء بعض استخدامات الأفراد السلبية للإنترنت، وما قد ينجم عنها من مخاطر اجتماعية وصحية ونفسية وثقافية واقتصادية، منها إمكانية التعرض للجريمة الإلكترونية.

وتتشابه هذه النتيجة مع ما خلصت إليه دراسة (الحزورة وحيدر، 2020، ص 211) التي توصلت إلى زيادة حجم استخدام المبحوثين من الشباب اليمني للإنترنت، ودراسة (محمد، 2017، ص 238) التي توصلت إلى زيادة حجم استخدام المبحوثين من الجمهور السوداني للإنترنت لمدة تصل إلى أكثر من ثلاث ساعات في اليوم.

جدول رقم (3) توزيع المبحوثين (عينة الدراسة) طبقاً لتعرضهم لجريمة إلكترونية:

م	التكرار والنسبة / التعرض لجريمة	التكرار	النسبة
.1	نعم	188	47
.2	لا	212	53
	الإجمالي	400	100

تكشف بيانات الجدول السابق عن نسبة تعرض الجمهور عينة الدراسة للجرائم الإلكترونية، حيث يتضح أن نسبة (47%) من المبحوثين قد تعرضوا لنوع واحد على الأقل من الجرائم الإلكترونية، بتكرار بلغ (188).

ويعد الباحث أن ارتفاع نسبة تعرض الجمهور للجريمة الإلكترونية بنسبة تقارب (50%) مؤشر خطير يدل على تفاقم الجريمة الإلكترونية؛ بحيث أصبحت تشكل (ظاهرة)، لها دلالاتها وانعكاساتها السلبية على الأفراد والمجتمع اليمني وعلى الاقتصاد والتنمية في بلد يعاني أصلاً من شح الإمكانات والموارد المحدودة التي تضاف إلى الأوضاع الصعبة التي يعيشها اليمنيون.

وبينت نتائج التحليل النوعي للمجموعات المركزة وجود أكثر من وجهة نظر، حيث أشار فريق من المشاركين إلى أن ازدياد نسبة الأمية التكنولوجية وانخفاض الوعي بمخاطر الجريمة الإلكترونية وطرق التعامل معها من أهم العوامل المؤدية إلى تفشي الجرائم الإلكترونية بأنواعها ب(نسب كبيرة)، واتضح ذلك من خلال إفادة بعض المشارِكات بالمجموعات المركزة، حيث أشارت (ن س) إلى ذلك بقولها: "هناك الكثير من اليمنيين من الجنسين ممن ارتكبت جرائم إلكترونية بحقهم، يفضلون عدم الإفصاح عنها خشية الآثار الاجتماعية عليهم أو خوفاً من الفضيحة، وفي حالة كون الضحية بنوكًا أو مصارف فإنهم يفضلون الصمت وحل المشكلة بأنفسهم بصورة سرية؛ خشية اهتزاز سمعتهم، ومن ثَمّ فقدان ثقة العملاء بهم، ولذلك فالأرقام المصرح عنها في الجهات الشرطية هي أقل بكثير جداً من العدد الفعلي" .

أما الفريق الآخر رجح ازدياد نسبة احتمالات تعرض أجهزة المستخدمين في اليمن لجرائم إلكترونية، وعدم معرفة أغلبهم بتعرضهم لاختراق أجهزتهم وربما سحب بياناتهم الشخصية إلى أجهزة الجناة، وفقاً لإفادة أحد المشاركين الذي أشار إلى: "إمكانية تعرض الكثير من أجهزة المستخدمين للاختراق وسحب البيانات وقد لا يجد الجاني نقطة ضعف على المجني عليه أو ما يغريه بالابتزاز فيتركه مثلاً".

وتتشابه هذه النتيجة مع دراسة (فاريش وقاوش، 2018، ص 114) حيث أفاد ثلث المبحوثين من المراهقين الجزائريين أنهم وقعوا ضحايا الجريمة الإلكترونية، كما تتوافق مع دراسة (إبراهيم، 2016، ص 3)، التي توصلت إلى تنامي إحصاءات الأمن العام فيما يتعلق بجرائم الإنترنت في المجتمع المصري، وظهور أنماط جديدة من الجرائم ولدتها الثورة التكنولوجية عبر الإنترنت.

جدول رقم (4) توزيع المبحوثين طبقاً لنوع الجريمة التي تعرضوا لها:

	درجة الموافقة / نوع الجريمة	نعم				لا				المجموع		الترتيب
		التكرار		النسبة		التكرار		النسبة		التكرار	النسبة	
		ذكور	إناث	ذكور	إناث	ذكور	إناث	ذكور	إناث			
1	احتيال مالي إلكتروني.	12	10	6.4	5.3	92	73	48.9	38.8	188	100	السابع
2	ابتزاز وتهديد بنشر مقاطع مصورة بالجهاز.	5	12	2.6	6.4	99	72	52.7	38.3	188	100	السادس
3	سرقة حساب الواتس.	19	20	10.1	10.6	86	63	45.7	33.5	188	100	الخامس
4	سرقة حساب الفيسبوك.	29	16	15.4	8.5	75	68	39.9	36.2	188	100	الرابع
5	انتحال الشخصية على الإنترنت.	28	25	15	13.2	77	58	41	30.9	188	100	الثالث
6	سب وقذف وتهديد من خلال النت.	32	24	17	12.8	73	59	38.8	31.4	188	100	الثاني
7	تعطيل النظام المعلوماتي للجهاز بالبرامج الضارة.	34	22	18.1	11.7	71	61	37.8	32.4	188	100	الثاني
8	استغلال جنسي.	6	6	3.2	3.2	99	77	52.7	41	188	100	الثامن
9	تلقي رسائل إباحية.	60	48	31.9	25.5	45	35	23.9	18.6	188	100	الأول

ملاحظة: يحتمل الجدول السابق إفادة المبحوثين بتعرضهم لعدة أنواع من الجرائم الإلكترونية.

يحوي الجدول السابق إحصائية بأنواع الجرائم الإلكترونية التي تعرض لها الجمهور عينة الدراسة، التي أفاد الكثير منهم إلى تعرضهم إلى عدة أنواع من الجرائم الإلكترونية، وتكشف بيانات الجدول السابق نوعية الجرائم الإلكترونية التي تعرض لها المبحوثين عينة الدراسة، حيث جاء في مقدمة تلك الجرائم (تلقي رسائل إباحية) بنسبة بلغت (57.4%) من إجمالي مفردات من تعرضوا لمثل تلك الجرائم، موزعة بين (31.9%) ذكور مقابل (25.5%) إناث.

تلاها في الترتيب الثاني كل من الجريمتين (تعطيل النظام المعلوماتي للجهاز بالبرامج الضارة) و(السب والقذف والتهديد من خلال النت) حيث جاءت كلتا العبارتين بنفس النسبة (29.8%) من إجمالي مفردات عينة الدراسة ممن تعرضوا للجرائم الإلكترونية، موزعة بين نسبة (18.1%) من الذكور مقابل (11.7%) من الإناث ممن تعرضن لتلك الجريمة، وجاءت جريمة (انتحال الشخصية على الإنترنت) في الترتيب الثالث بإجمالي نسبة (28.2%) من إجمالي الجمهور عينة الدراسة، موزعة بين نسبة (15%) ذكور، بينما جاءت نسبة الإناث (13.2%).

تلاها بالترتيب الرابع (سرقة حساب الفيسبوك) حيث جاءت بنسبة (23.9%) من إجمالي مفردات من تعرضوا لتلك الجرائم، موزعة بين (15.4%) من إجمالي مفردات عينة الذكور، مقابل (8.5%) من إجمالي عينة الإناث، تلاها بالترتيب الخامس (سرقة حساب الواتس آب)، التي جاءت بنسبة (20.7%)، موزعة بين (10.1%) من إجمالي مفردات عينة الذكور مقابل (10.6%) من مفردات عينة الإناث.

وجاء (الابتزاز والتهديد بنشر مقاطع مصورة كانت بالجهاز) في الترتيب السادس بنسبة (9%)، موزعة بين (2.6) من إجمالي عينة الذكور مقابل (6.4%) من إجمالي مفردات عينة الإناث.

تلاها (الاحتيال المالي الإلكتروني) بالترتيب السابع بنسبة (11.7%)، موزعة بين (6.4%) من إجمالي عينة الذكور مقابل (5.3%) من إجمالي عينة الإناث.

وجاء في الترتيب الثامن والأخير جريمة (الاستغلال الجنسي) بنسبة (6.4%)، التي تقاسمها الذكور والإناث من الجمهور عينة الدراسة بنسبة متساوية بلغت (3.2%)، ويعد الباحث أن عاملي ضغط الأسرة وضغط المجتمع من أهم عوامل قوة المجرم الإلكتروني فيما يتعلق بجرائم الاستغلال الجنسي الذي قد تتعرض له الإناث في اليمن، ويبدأ هذا النوع من الجرائم على سبيل المثال من خلال حصول الجاني على صور فوتوغرافية أو فيديو غير محتشم للضحية الأنثى من خلال دخول الضحية الأنثى في روابط مجهولة أو فتح مرفقات غير معروفة المصدر، ينتهي بابتزازهن أو استغلالهن جنسياً، في حين لم يستثن الاستغلال الجنسي الذكور، إما جراء حصول المجرمين الإلكترونيين لصور خاصة للإناث من أقارب الضحية الذكر، مثل صورهن في حفل زفاف وما شابه، أو من خلال انخراط الذكر في علاقة مع نساء مجهولات من خلال تطبيقات المحادثات الفيديوية على الإنترنت ينتهي بالتقاط صور للذكر في وضع مخل أو متعري وابتزازه مالياً بتلك الصور، كما يعد الباحث أن انتشار أنواع الجرائم الإلكترونية في المجتمع اليمني بهذه النسب، يضع ضغطاً كبيراً على الموارد المالية والحاجة إلى الرعاية الصحية والخدمات القضائية والجنائية والاجتماعية، وسيؤدي ذلك إلى انخفاض الإنتاجية، سيما في ظل عدم وجود قانون في اليمن يعنى بمكافحة الجريمة الإلكترونية، وفي ظل ما توصلت إليه الدراسة من غياب برامج التوعية والتثقيف بمخاطر الجريمة الإلكترونية من الأجهزة ذات العلاقة.

واعتبرت المجموعات المركزة أن الجرائم الإلكترونية المتعلقة بالشرف والعرض هي الأكثر تفاعلاً وتأثيراً في أوساط المجتمع اليمني نظراً لحداثة هذه الجرائم الغير مألوفة على المجتمع، والمتعارضة تماماً مع المبادئ وقيم وأخلاق الشعب اليمني.

وتتفق أو تقترب هذه النتائج مع بعض نتائج الدراسات السابقة مع اختلاف مناهج الدراسات والجمهور الذي تم تطبيق الدراسة عليه، مثل:

- دراسة (الهادي، 2020، ص ص 868-869) التي خلصت إلى أن أكثر أنواع الجرائم الإلكترونية التي تعرض لها المراهقون المصريون هي على التوالي: الرسائل الضارة وسرقة بعض ملفات

الحاسوب وتلقي رسائل إباحية والتعرض للفيروسات وقرصنة البرامج.

- دراسة (سجية وآخرون، 2019، ص ص 40-41) التي توصلت إلى تعرض المبحوثين من الطلبة بالجزائر لأشكال متنوعة من الجرائم الإلكترونية، مثل الاستيلاء على المعلومات وجريمة نشر الصور والفيديوهات الخاصة، والتعدي على الملكية الفكرية، وجريمة نشر فيديوهات خاصة.
- دراسة (Khan)،2018، p6 ، الذي خلص إلى ظهور أشكال جديدة من الجرائم الإلكترونية مع النمو السريع للإنترنت وتكنولوجيا الحاسوب، ومن تلك الجرائم الاحتيال وانتحال الشخصيات والسطو على بطاقات الائتمان وتتبع كلمات المرور والوصول غير المصرح به للأجهزة.
- دراسة (نبيلة، 2014، ص45) التي توصلت إلى أن التطور المذهل في تكنولوجيا الاتصالات والمعلومات والإنترنت أدى إلى ظهور مجموعة جديدة من الجرائم الإلكترونية المستحدثة والفريدة والمغايرة لتلك الجرائم التي اعتاد رجال القانون والفقه الجنائي على التعامل معها ومكافحتها.

جدول رقم (5) توزيع المبحوثين طبقاً للعبارات المتعلقة بالوعي بمفهوم الجريمة الإلكترونية

	العبارات	المتوسط الحسابي	الانحراف المعياري	الوزن المئوي	الترتيب
1.	الابتزاز والتهديد الإلكتروني بالتشهير بنشر مقاطع للضحية	2.82	0.542	%94	الأول
2.	سرقة بيانات الحاسوب والهواتف الذكية من خلال الإنترنت	2.81	0.562	%93.6	الثاني
3.	التجسس على الحاسوب والهواتف الذكية	2.80	0.565	%93.4	الثالث
4.	الاحتيال المالي الإلكتروني	2.76	0.604	%91.9	الرابع
5.	استغلال الأطفال جنسياً بالإنترنت	2.75	0.633	%91.5	الخامس
6.	استغلال المنظمات الإرهابية للإنترنت في التمويل لتجنيد إرهابيين	2.75	0.617	%91.5	الخامس
7.	الانتحال الإلكتروني للشخصية	2.74	0.631	%91.4	السادس
8.	جرائم التهديد من خلال الإنترنت	2.73	0.647	%91	السابع
9.	سحب بيانات الأجهزة الإلكترونية بالوصلات السلكية بدون الإذن من أصحابها	2.73	0.635	%91	السابع
10.	استهداف أمن المعلومات والمرافق والاتصالات في الدولة	2.72	0.647	%90.6	الثامن
11.	غسل الأموال وتجارة المخدرات عن طريق الإنترنت	2.70	0.662	%89.8	التاسع
12.	جرائم السب والقذف والتهديد بالإنترنت	2.64	0.690	%88.1	العاشر
13.	الترويج للمواقع والأفلام الإباحية	2.63	0.694	%87.9	حادي عشر
	المتوسط العام لجميع العبارات	2.73	0.625	%91.2	

توضح بيانات الجدول السابق موافقة أغلب المبحوثين على العبارات المتعلقة بمفاهيم الجريمة الإلكترونية، ويعكس ذلك معرفتهم (الجيدة) بمفاهيمها العامة، حيث جاء الوزن المئوي العام للعبارات (91.2%) بمتوسط حسابي عام (2.73) ، وقد جاءت في المرتبة الأولى عبارة (الابتزاز والتهديد الإلكتروني بنشر مقاطع مصورة للضحية) بمتوسط حسابي (2.82)، فيما جاءت عبارة (سرقة بيانات الحاسوب والهواتف الذكية من خلال الإنترنت) في المرتبة الثانية بمتوسط حسابي (2.81).

كما جاء في المرتبة الثالثة العبارة (التجسس على الحاسوب والهواتف الذكية) بمتوسط حسابي (2.80)، أما المرتبة الرابعة فحلت عبارة (الاحتيال المالي الإلكتروني) كمفهوم للجريمة إلكترونية لدى عينة الدراسة بمتوسط حسابي (2.76)، تلاها في المرتبة الخامسة العبارتين (استغلال الأطفال جنسياً من خلال الإنترنت) و(استغلال المنظمات الإرهابية للإنترنت في التمويل لتجنيد إرهابيين جدد) بمتوسط حسابي (2.75)، ثم في المرتبة السادسة (الانتحال الإلكتروني للشخصية) بمتوسط حسابي (2.74)، وجاء في المرتبة السابعة العبارتين (سحب بيانات الأجهزة الإلكترونية بالوصلات السلكية بدون إذن اصحابها) و(جرائم التهديد من خلال الإنترنت) بمتوسط حسابي (2.73)، تلى ذلك في المرتبة الثامنة عبارة (استهداف أمن المعلومات والمرافق والاتصالات في الدولة) بمتوسط حسابي (2.72)، كما جاءت عبارة (غسل الأموال وتجارة المخدرات عن طريق الإنترنت) في المرتبة التاسعة بمتوسط حسابي (2.70)، وفي المرتبة العاشرة جاءت العبارة (جرائم السب والقذف والتهديد بالإنترنت) بمتوسط حسابي (2.64)، وجاء في المرتبة الحادية عشرة والأخيرة العبارة (الترويج للمواقع والأفلام الإباحية) بمتوسط حسابي (2.63).

يتضح مما سبق أن وعي الجمهور بمفهوم الجريمة الإلكترونية جاء جيداً، وهذا ناجم عن انتشار الجريمة الإلكترونية في المجتمع اليمني، بحيث أصبح مفهومها معروفاً لدى الجمهور، على الرغم من أن أخبار الجريمة الإلكترونية لا تشكل حالياً أولوية في أجندة أخبار وسائل الإعلام الحديثة والتقليدية في اليمن.

وقد أظهر التحليل النوعي تحفظ المشاركين بالمجموعات المركزة تجاه معرفة الجمهور اليمني بمفهوم الجريمة الإلكترونية، فقد رأى بعض المشاركين أن الجمهور اليمني ضعيف المعرفة بمفهومها نتيجة لضعف برامج التوعية والتثقيف بهذا الشأن، وفقاً لما عبر عنه المشارك (ع ف) بقوله: "إن الجمهور اليمني غير مهتم بمعرفته بمفاهيم الجريمة الإلكترونية لعدم قيام الجهات الرسمية ذات العلاقة بتوعيته بتلك المفاهيم"، بينما رأى البعض الآخر بالمجموعات المركزة أن معرفة الجمهور اليمني بمفهوم الجريمة الإلكترونية (متوسطة) في أحسن الأحوال، وأضاف المشارك (م ث) أن: "معرفة الجمهور اليمني بمفهوم الجريمة الإلكترونية تكاد تنحصر في الجرائم المتعلقة بالجانب الأخلاقي والابتزاز بالصور مع ضعف كبير في معرفتهم بمفاهيم الجرائم الإلكترونية الأخرى" ، في حين رأى الفريق الآخر أن أغلب الأفراد المستخدمين للإنترنت لديهم مستويات معرفة (جيدة) بمفهوم الجريمة الإلكترونية وعن

وجودها كما توضح المشاركة (ل ي) أن: "أغلب الأفراد المستخدمين للإنترنت يعرفون مفهوم الجريمة الإلكترونية لكنهم ضعفاء في معرفة أساليب ارتكابها وفي اتخاذ طرق الوقاية منها"، كما أشار (ن م) إلى أن: " مفهوم الجريمة الإلكترونية أصبح منتشراً بصورة كبيرة في المجتمع اليمني من كثرة الجرائم التي تحصل في المجتمع، التي يعرف الناس عنها من خلال معرفتهم الشخصية بضحايا تلك الجرائم، أو من خلال ما يتم تداوله بوسائل الإعلام خصوصاً جرائم الابتزاز بالصور المرتبطة بالشرف".

وتختلف هذه النتائج مع دراسة (الخراساني، 2013، ص38) التي توصلت إلى أن أغلب المبحوثين في اليمن لا يعلمون مفهوم الجريمة الإلكترونية، وأفادوا بعدم وجود جرائم إلكترونية في اليمن، ويرجع سبب الاختلاف إلى حداثة عهد اليمنيين بالإنترنت آنذاك.

جدول رقم (6) توزيع المبحوثين طبقاً للعبارات المتعلقة بالوعي بأساليب الجريمة الإلكترونية:

	الأساليب	المتوسط الحسابي	الانحراف المعياري	الوزن المئوي	الترتيب
.1	الاحتفاظ بالصور الشخصية غير المحتشمة في الجهاز يسهل الابتزاز الإلكتروني	2.64	0.687	%88	الأول
.2	الاحتفاظ بأرقام الحسابات المصرفية في الجهاز يسهل الاحتيال المالي	2.48	0.772	%82.8	الثاني
.3	القيام بالمراسلات المالية من خلال مواقع التواصل الاجتماعي يسهل الاحتيال المالي	2.44	0.786	%81.4	الثالث
.4	إقامة صداقة مع غرباء في الإنترنت تسهل الجريمة الإلكترونية	2.35	0.796	%78.4	الرابع
.5	فتح مرفقات بريد إلكتروني وارد من مصادر مجهولة المصدر قد يتيح انتقال فيروسات للأجهزة	2.14	0.925	%71.3	الخامس
.6	فتح مرفقات بمواقع التواصل الاجتماعي دون التأكد من صحة محتواها يسهل عملية سرقة البيانات	2.11	0.934	%70.4	السادس
.7	الدخول في روابط مجهولة بالإنترنت تحت إغراء الفوز بجائزة أو ربح معين من أساليب الجريمة الإلكترونية	2.10	0.935	%70.1	السابع
	المتوسط العام لجميع العبارات	2.32	0.833	%77.5	

تكشف بيانات الجدول السابق معرفة المبحوثين (المتوسطة) بأساليب ارتكاب الجرائم الإلكترونية بوزن مئوي عام (77.5%) وقد جاء ترتيب تلك العبارات على النحو الآتي:

جاءت عبارة (الاحتفاظ بالصور الشخصية غير المحتشمة يسهل الابتزاز الإلكتروني) في المرتبة الأولى بمتوسط حسابي (2.64)، فيما جاء في المرتبة الثانية عبارة (الاحتفاظ بأرقام الحسابات

المصرفية في الجهاز يسهل الاحتيال المالي) بمتوسط حسابي (2.68)، أما في المرتبة الثالثة فقد حلت عبارة (القيام بالمراسلات المالية من خلال مواقع التواصل الاجتماعي) بمتوسط حسابي (2.44)، ويشير هذا إلى أن غالبية الجمهور موافق على هذه العبارة، أما عبارة (إقامة علاقة صداقة مع غرباء على الإنترنت) فقد احتلت الترتيب الرابع بمتوسط حسابي (2.35) حلت بعدها عبارة (فتح مرفقات بريد إلكتروني وارد من مصادر مجهولة المصدر) التي حلت خامساً بمتوسط حسابي (2.14)، وجاءت عبارتا (فتح مرفقات بمواقع التواصل الاجتماعي دون التأكد من صحة محتواها) و(الدخول في روابط مجهولة بالإنترنت تحت إغراء الفوز بجائزة أو ربح معين) في ترتيب متأخر بالمرتبة السادسة بمتوسط حسابي (2.11)، وفي المرتبة الأخيرة جاءت عبارة (الدخول في روابط مجهولة تحت إغراء الفوز بجائزة أو ربح معين) بمتوسط حسابي (2.10).

ويعد الباحث أن المعرفة المتوسطة للجمهور بأساليب الجريمة الإلكترونية يجعل استخدامهم للإنترنت مجازفة حقيقية بالخصوصية، وبسلامة البيانات التي تحتويها الأجهزة الذكية، الأمر الذي قد يشكل معه ضغطاً على موارد التنمية في بلد يعاني أصلاً من ضعف الاقتصاد.

وقد أكد المشاركون بالمجموعات المركزة على (تواضع) معرفة الجمهور اليمني بأساليب الجريمة الإلكترونية، حيث فسر المشارك (م د) ذلك بقوله: "إن معرفة الجمهور اليمني بأساليب ارتكاب الجرائم الإلكترونية ضعيفة، انعكاسا لضعف برامج التوعية والتثقيف للجهات ذات العلاقة بالقطاعين الرسمي والخاص المستثمر في تكنولوجيا الاتصالات والمعلوماتية".

جدول رقم (7) توزيع المبحوثين طبقاً للعبارات المتعلقة بالوعي بطرق الوقاية من الجريمة الإلكترونية:

	طرق الوقاية	المتوسط الحسابي	الانحراف المعياري	الوزن المئوي	الترتيب
.1	التمتع بالحذر أثناء استخدام الإنترنت	2.42	0.758	%80.6	الأول
.2	استخدام كلمة سر قوية للجهاز	2.32	0.684	%77.3	الثاني
.3	عدم إرسال المعلومات الشخصية أو البيانات الهامة عبر البريد الإلكتروني أو مواقع التواصل	2.315	0.814	%77.2	الثالث
.4	عدم فتح رسائل بريدية مجهولة المصدر	2.31	0.854	%76.9	الرابع
.5	عدم استقبال ملفات في الشات من أشخاص غير موثوق بهم	2.29	0.865	%76.3	الخامس
.6	عدم الاحتفاظ بمعلومات أو بيانات مهمة أو أرقام حسابات مصرفية أو صور خاصة في الجهاز	2.28	0.799	%76	السادس
.7	عدم الدخول في مواقع مشبوهة مثل مواقع تعليم التجسس واختراق أجهزة الأفراد	2.35	0.874	%75	السابع
.8	تجنب تحميل البرامج المهكرة مجاناً توفيراً للمال	2.21	0.848	%73.8	الثامن

.9	الاحتفاظ بالمعلومات الشخصية أو البيانات الهامة أو أرقام الحسابات المصرفية في ذواكر تخزين خارج الجهاز	2.22	0.845	%74	التاسع
.10	عدم الاستجابة للرسائل المغرية ورسائل الاستدراج، مثل: مبروك ربحت جائزة أو ربح	2.18	0.890	%72.6	العاشر
.11	استخدام نظام تشغيل وبرامج مرخصة	2.07	0.850	%72.4	حادي عشر
.12	عدم إقامة علاقات صداقة مع غرباء على الإنترنت	2.16	0.849	%72	ثاني عشر
.13	الاحتفاظ بالملفات والمواقع على النت بكلمة سر	2.14	0.871	%71.2	ثالث عشر
.14	عدم الدخول في روابط مجهولة بالإنترنت ومواقع التواصل الاجتماعي	2.11	0.917	%70.2	رابع عشر
.15	عدم فتح مرفقات بمواقع التواصل أو من مصادر غير آمنة دون التأكد من صحة محتواها	2.11	0.887	%70.1	خامس عشر
.16	تثقيف النفس بالفيروسات واختراق الأجهزة	2.07	0.832	%68.8	سادس عشر
.17	استخدام مكافح فيروسات في الجهاز	2.03	0.854	%67.6	سابع عشر
.18	القيام بتحديث نظام التشغيل للجهاز	2.03	0.810	%67.5	ثامن عشر
.19	الاحتفاظ بنسخة ورقية للأعمال على الإنترنت	1.84	0.843	%61.4	تاسع عشر
.20	القيام بتحديث مكافح الفيروسات بالجهاز باستمرار	1.82	0.845	%60.7	عشرون
.21	تغيير كلمة السر بالجهاز بصورة دورية	1.77	0.741	%58.9	واحد وعشرون
المتوسط العام لجميع العبارات		2.08	0.822	%69.3	

تكشف بيانات الجدول السابق عن (وعي ضعيف) للمبحوثين بالدراسة بطرق الوقاية من الجريمة الإلكترونية، حيث جاء الوزن المئوي العام (69.3%) وجاء ترتيب تلك العبارات كما يلي: جاء (التمتع بالحذر أثناء استخدام الإنترنت) في المرتبة الأولى بمتوسط حسابي (2.42)، فيما جاءت عبارة (استخدام كلمة سر قوية للجهاز) في المرتبة الثانية بمتوسط حسابي (2.32) وقد لاحظ الباحثان أن أغلب الجمهور اليمني يعتقدون أن استخدامهم لكلمة سر قد لا تتجاوز ستة أرقام تجعلهم في وقاية من تعرض أجهزتهم للاختراق وأعمال القرصنة ومن المعلوم في الأوساط البرمجية أن كلمة السر القوية للأجهزة تصل إلى ستة عشر رقماً تشتمل على الحروف الأبجدية والرموز، وجاء في المرتبة الثالثة (عدم إرسال معلومات شخصية أو بيانات هامة أو صور خاصة عبر البريد الإلكتروني أو مواقع التواصل) بمتوسط حسابي (2.315)، كما جاء في المرتبة الرابعة عبارة (عدم القيام بفتح رسائل بريدية مجهولة المصدر) بمتوسط حسابي (2.31)، وجاءت العبارة (عدم استقبال ملفات في الشات من أشخاص غير موثوق بهم) في المرتبة الخامسة بمتوسط حسابي (2.29)، ثم عبارة (عدم الاحتفاظ بالمعلومات أو البيانات الهامة أو أرقام الحسابات المصرفية أو الصور الخاصة في الجهاز) فقد جاءت في المرتبة السادسة بمتوسط حسابي

(2.42)، أما عبارة (عدم الدخول في المواقع المشبوهة) فقد جاءت في الترتيب الثامن بمتوسط حسابي (2.28)، بينما جاء في المرتبة السابعة عبارة (عدم الدخول في مواقع مشبوهة، مثل مواقع تعليم التجسس واختراق اجهزة الأفراد) بمتوسط حسابي (2.35)، تلا ذلك عبارة (تجنب تحميل البرامج المهكرة مجاناً توفيراً للمال) في المرتبة الثامنة بمتوسط حسابي (2.21)، كما جاء بعد ذلك (الاحتفاظ بالمعلومات الشخصية أو البيانات الهامة أو أرقام الحسابات المصرفية في ذواكر تخزين خارج الجهاز) في المرتبة التاسعة بمتوسط حسابي (2.22)، وجاءت العبارة (عدم الاستجابة للرسائل المغرية ورسائل الاستدراج مثل: مبروك ربحت جائزة أو ربح معين) في المرتبة العاشرة بمتوسط حسابي (2.18)، تلاها في المرتبة الحادية عشرة (استخدام نظام تشغيل وبرامج مرخصة) بمتوسط حسابي (2.07) تلى ذلك في المرتبة الثانية عشرة (عدم إقامة علاقة صداقة مع غرباء على الإنترنت) بمتوسط حسابي (2.16)، بينما جاء (الاحتفاظ بالملفات والمواقع على النت بكلمة سر) في المرتبة الثالثة عشرة بمتوسط حسابي (2.14) وفي المرتبة الرابعة عشرة جاء (عدم الدخول في روابط مجهولة بالإنترنت ومواقع التواصل الاجتماعي) بمتوسط حسابي (2.11)، وفي المرتبة الخامسة عشرة جاء (عدم فتح مرفقات بمواقع التواصل أو من مصادر غير آمنة دون التأكد من صحة محتواها) بمتوسط حسابي (2.11)، كما جاءت عبارة (تثقيف النفس فيما يتعلق بالفيروسات واختراق الأجهزة) في المرتبة السادسة عشرة بمتوسط حسابي (2.07)، ثم جاء في المرتبة السابعة عشرة عبارة (استخدام مكافح فيروسات في الجهاز) بمتوسط حسابي (2.03)، وجاء (القيام بتحديث نظام التشغيل للجهاز) في المرتبة الثامنة عشرة بمتوسط حسابي (2.03)، كما جاءت عبارة (الاحتفاظ بنسخة ورقية للأعمال على الإنترنت) في المرتبة التاسعة عشرة بمتوسط حسابي (1.84)، ثم جاءت عبارة (القيام بتحديث مكافح الفيروسات بالجهاز باستمرار) في المرتبة العشرين بمتوسط حسابي (1.82) .

ويسترعي الانتباه مجيء عبارة (القيام بتغيير كلمة السر بالجهاز بصورة دورية) في مرتبة متأخرة هي المرتبة الحادية والعشرين بمتوسط حسابي (1.77)، وهذا الأمر يجعل أجهزة المستخدمين عرضة لكشف كلمات سر المرور بأجهزتهم، ويعرض بياناتهم لأعمال القرصنة والاختراق.

ويعتبر الباحث أن ضعف وعي الجمهور اليمني بطرق الوقاية من الجريمة الإلكترونية، نتيجة طبيعية لضعف برامج التوعية والتثقيف بمخاطر الجريمة الإلكترونية، ونتيجة أيضاً لعدم وجود قانون لمكافحة الجريمة الإلكترونية في اليمن.

وقد توافقت بيانات التحليل النوعي للمجموعات المركزة من ناحية ترجيحها لضعف وعي الجمهور اليمني بطرق الوقاية من الجريمة الإلكترونية، وقد عبر (ح س) المشارك بالمجموعات المركزة عن اعتقاده بأن: "اغلب الأفراد المستخدمين للإنترنت في اليمن لا يهتمون بإجراءات الحماية من الجرائم الإلكترونية، وفي أحسن الأحوال يكتفي العدد الكبير من المستخدمين بكلمة سر دخول للجهاز قد لا تتجاوز 9 أرقام في أحسن الأحوال، والكثير يحبذون كلمات سر سهلة الاختراق مثل رقم الجوال

أو تاريخ الميلاد وغيرها من أرقام يسهل تخمينها"، فيما أشارت المشاركة (أ ش) بالمجموعات المركزة إلى: "أن اهتمام إدارات أمن المعلومات بالجهات ذات العلاقة بأعمال التوعية بهذا الشأن؛ ينحصر في توعية التقنيين والمهندسين والمبرمجين والخبراء بالمؤسسات المالية والجهات الحكومية بطرق الوقاية من الجريمة الإلكترونية، ويبدو أنها غير معنية بتعميم إجراءات الاستخدام الآمن للإنترنت للجمهور العام" .

وتتفق هذه النتائج في مجملها مع عدد من الدراسات مثل دراسة (Khan، 2018، p6) التي توصلت إلى أن 33% من عينة دراسته بالهند لا يغيرون كلمة المرور مطلقاً، و62% لا يعلمون المقصود بكلمة المرور القوية.

كما تتشابه هذه النتيجة مع دراسة (محمد، 2017، ص 238) التي توصلت إلى أن هناك نسبة مقدرة من أفراد المجتمع السوداني تعلم أهمية حفظ نسخ ورقية من أعمالهم على الإنترنت وتقوم بحفظها ورقياً، ويحفظ البعض ملفاتهم بكلمات سر يسهل تخمينها واختراقها.

جدول رقم (8) توزيع المبحوثين طبقاً للجهات التي تلقوا من خلالها توعية بمخاطر الجرائم الإلكترونية

	درجة الموافقة / الجهة	نعم		لا		المجموع		الترتيب
		التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	
1	الإعلام الأمني بوزارة الداخلية	100	25	300	75	400	100	الثالث
2	المؤسسة العامة للاتصالات	111	27.8	289	72.2	400	100	الثاني
3	وزارة العدل	18	4.5	382	95.5	400	100	السادس
4	شركة تيليمن	53	13.3	347	86.7	400	100	الخامس
5	شركة يمن نت	95	23.8	305	76.2	400	100	الرابع
6	رسائل SMS لشركات الهاتف المحمول	207	51.8	193	48.2	400	100	الأول

تكشف بيانات الجدول السابق – بشكل عام – ضعف إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجرائم الإلكترونية (وزارة الاتصالات وتقنية المعلومات، المؤسسة العامة للاتصالات، مشغلي الإنترنت تيليمن ويمن نت، وزارة الداخلية، وزارة العدل) في أعمال توعية وتثقيف الجمهور اليمني بمخاطر الجريمة الإلكترونية، حيث أشار المبحوثون عينة الدراسة إلى أنهم تلقوا توعية بمخاطر الجرائم الإلكترونية من خلال رسائل sms بنسبة بلغت (51.8%) فقط بالترتيب الأول، كما تظهر بيانات الجدول السابق تلقي المبحوثين لتوعية بمخاطر الجريمة الإلكترونية في الترتيب الثاني من المؤسسة العامة للاتصالات السلكية واللاسلكية بنسبة ضعيفة هي (27.8%)، وجاء في الترتيب الثالث تلقي الجمهور توعية من الإعلام الأمني بوزارة الداخلية بنسبة ضعيفة (25%)، ثم في الترتيب الرابع أفاد المبحوثون بتلقيهم توعية بمخاطر الجريمة الإلكترونية من شركة يمن نت بنسبة ضعيفة بلغت (23.8%)،

ثم في الترتيب الخامس أفاد المبحوثون عينة الدراسة بتلقيهم توعية بخطر الجريمة الإلكترونية من شركة تيليمن بنسبة (13.3%) بينما جاء في الترتيب السادس والأخير تلقي المبحوثين توعية بمخاطر الجريمة الإلكترونية من وزارة العدل بنسبة ضعيفة جداً (4.5%)، ويعتبر الباحث أن ضعف برامج التوعية والتثقيف الإعلامي بمخاطر الجريمة الإلكترونية لإدارات الإعلام والعلاقات العامة بالمؤسسات المسئولة عن الجريمة الإلكترونية، يقذف بمستخدمي الإنترنت في اليمن إلى المجهول ويُسهل وقوعهم كضحايا محتملين للجريمة الإلكترونية بأنواعها، حيث يؤدي ذلك القصور إلى ضعف وعي مستخدمي الإنترنت في اليمن بخطورة الجرائم الإلكترونية وطرق تجنبها والوقاية منها، الأمر الذي ينعكس سلباً على التنمية والجوانب المالية والاقتصادية والنفسية والصحية للأفراد والمجتمع، كما يعتبر ذلك القصور في أداء أعمال التوعية بمخاطر الجريمة الإلكترونية لتلك الإدارات المعنية؛ أحد نتائج القصور في التشريعات المجرمة والرادعة للجريمة الإلكترونية.

وقد أظهر التحليل النوعي للمجموعات المركزة الضعف الكبير في جهود الجهات المسئولة عن الجريمة الإلكترونية من ناحية توعية الجمهور اليمني بمخاطر الجريمة الإلكترونية، وأرجع عدد من المشاركين بالمجموعات المركزة السبب الرئيسي لذلك إلى عدم وجود قانون لمكافحة الجريمة الإلكترونية، وعبرت المشاركة (ج س) عن ذلك بقولها: "انعكس تلكؤ مجلس النواب في إقرار قانون مكافحة جرائم تقنية المعلومات، والمحال إليه مشروع القانون منذ أواخر عام 2020م، على ضعف جهود التوعية بمخاطر الجريمة الإلكترونية، ويوضح ذلك بجلاء ركاكة الأداء الحكومي والتشريعي في هذا الجانب"، وأفادت عدد من المشاركات بالمجموعات المركزة بأن الدور التوعوي للجهات المسئولة عن الجريمة الإلكترونية يأخذ شكلاً مناسباتياً عند حدوث المشكلة، وفقاً لما عبرت عنه المشاركة (ي ي):"أن جهود الجهات ذات العلاقة في التوعية بمخاطر الجريمة الإلكترونية سواءً الإعلام الأمني أو هيئات وزارة الاتصالات تحدث في حالة وقوع الجرائم الإلكترونية التي تؤثر في المجتمع أو الاقتصاد مثلاً، ويعيبها أنها جهود نادرة وغير منتظمة" ، فيما عبرت المشاركة (ل ي) بقولها:" إن أي جهود توعية للجهات ذات العلاقة في هذا الاتجاه يجب أن تشتمل على شرح للحيل التي يتبعها مرتكبو الجرائم الإلكترونية".

كما أرجع عدد آخر من المشاركين بالمجموعات المركزة ذلك الضعف إلى أسباب متعددة وفقاً لما عبر عنه المشارك (م أ) بقوله: "جهود التوعية الإعلامية والتكنولوجية بمخاطر الجريمة الإلكترونية ضعيفة ومتواضعة جداً لعدة أسباب تختلف بحسب الجهة المسئولة، سواء من ناحية الاختصاصات أو الإمكانيات أو الأفكار أو الوسائل المتاحة"، وهذا برأي الباحث يتفق مع نتائج التحليل النوعي للمقابلات المعمقة التي أجريت مع المدراء والمسئولين بإدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية، التي سيلي التطرق اليها.

وتتشابه هذه النتائج مع دراسة (بيت المال، 2014، ص (17-18) الذي توصل إلى أهمية

اهتمام المؤسسات الأمنية في الأردن بحملات التوعية العامة بمخاطر سوء استخدام وسائل التواصل الاجتماعي المؤدية للجريمة الإلكترونية، وحضورها على الوسائل الاجتماعية.

كما تختلف النتائج في الجدول السابق مع دراسة (محمد، 2017، ص 237) حيث توصلت إلى أن إدارات العلاقات العامة والإعلام بالمؤسسات المسئولة عن الجريمة الإلكترونية بالسودان (نجحت) في تأسيس شراكات فاعلة واتفاقات فيما بينها بخصوص التوعية بمخاطر الجرائم الإلكترونية بناءً على معرفتهم الجيدة بمخاطرها، وبوجود باتفاقيات دولية قيد التنفيذ، وكانت أكثر الوسائل التي استخدمت لأعمال التوعية هي الصحف والتلفزيون، لكنها لم تهتم باستخدام الإعلام الرقمي في التوعية.

ثانياً: نتائج التحليل الكيفي للمقابلات المعمقة مع المدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية:

تتوافق النتائج السابقة بالدراسة مع النتيجة العامة بالتحليل النوعي الكيفي للمقابلات المعمقة التي أجراها الباحث مع مدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية، وفقاً للمحاور الآتية:

1- مدى معرفة القائمين على الاتصال بمخاطر الجرائم الإلكترونية:

أظهر التحليل النوعي (المعرفة المتوسطة) بمخاطر الجريمة الإلكترونية لدى مدراء ومسئولي تلك الإدارات بكل من إدارتي تيليمن ووزارة العدل، كما أظهر (المعرفة المرتفعة) بتلك المخاطر لدى بقية المدراء والمسئولين بتلك الإدارات المعنية.

2- وجود لوائح منظمة بالإدارات فيما يتعلق بواجباتها تجاه التوعية بمخاطر الجريمة الإلكترونية:

أقر جميع مدراء ومسئولي إدارات الإعلام والعلاقات العامة بعدم وجود (لوائح منظمة في إداراتهم خاصة بتوعية وتثقيف الجمهور اليمني بمخاطر الجريمة الإلكترونية)؛ الأمر الذي يعكس ضعف الأداء الرسمي الحكومي التوعوي في هذا الاتجاه.

3- قيام الإدارات بجهود في توعية المستخدمين بمخاطر الجرائم الإلكترونية:

أظهر التحليل النوعي للمقابلات مع المدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية عدم قيام تلك الإدارات بأي حملات لتوعية الجمهور اليمني بمخاطر الجريمة الإلكترونية، باستثناء شركة تيليمن التي قامت بعدة حملات (محدودة) لتوعية الجمهور بتلك المخاطر، التي ركزت من خلالها على تحذير المواطنين من التعامل مع المكالمات الدولية المهربة من داخل الوطن إلى خارجه أو العكس، التي تتم بواسطة تقنيات متطورة وأجهزة اتصالات حديثة عبر برتوكولات الإنترنت، وقد امتدت الحملات التي رعتها تيليمن لتوعية الجمهور اليمني بمخاطر الجرائم الإلكترونية من خلال المواقع الإلكترونية للشركة عبر الإنترنت والفيسبوك ومواقع التواصل الاجتماعي، وبرامج إذاعية وتلفزيونية بصورة محدودة.

4- مقدار رضا القائمين بالاتصال عن الأدوار التي يقدونه في مجال توعية الجمهور بمخاطر الجرائم الإلكترونية:

أظهر التحليل النوعي للمقابلات مع المدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية (إجماعهم) على عدم رضاهم عن مستوى الجهود التوعوية التي تقوم بها إداراتهم حيال الأعمال المتعلقة بتوعية وتثقيف الجمهور اليمني بمخاطر الجريمة الإلكترونية، ويتماشى هذا مع نتائج الدراسة الكمية والتحليل الكيفي للمجموعات المركزة من ناحية ضعف تلقي الجمهور لتوعية مسبقة بمخاطر الجريمة الإلكترونية من الجهات ذات العلاقة.

5- إدراك الجمهور اليمني لمخاطر الجريمة الإلكترونية من وجهة نظر القائم بالاتصال:

كما أظهر تحليل نتائج المقابلات المعمقة مع مدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجرائم الإلكترونية اعتقادهم (بعدم معرفة الجمهور اليمني بمخاطر الجريمة الإلكترونية وعدم تمتعهم بالوعي الكافي بطرق الوقاية منها وأساليب تجنبها)، ويعتبر الباحث أن ذلك يضع الجهات ذات العلاقة أمام مسئولية أخلاقية ومجافاة للمسئولية الوطنية الجسيمة المناطة بهم تجاه الآثار الكارثية لنتائج الجرائم الإلكترونية، التي أصبحت تهدد كيان الأسرة اليمنية ورفاه المجتمع .

6- مدى تحمل الجهات ذات العلاقة بالجرائم الإلكترونية المسئولية المباشرة عن ضعف توعية وتثقيف الجمهور اليمني بمخاطر الجرائم الإلكترونية:

(اتفق) مدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية على (تحملهم مسئولية مباشرة) في ضعف توعية وتثقيف الجمهور العام بمخاطر الجريمة الإلكترونية، إلا أن عدد منهم قام بتحميل المسئولية على جهات أخرى ذات علاقة، مثل مدير الإعلام الأمني بوزارة الداخلية ومدير الإعلام بالمؤسسة العامة للاتصالات، اللذان أقرّا بمسئولية إدارتيهما مسئولية مباشرة في ضعف وتوعية الجمهور اليمني بمخاطر الجريمة الإلكترونية، وحمّلا المسئولية أيضاً على جميع الجهات ذات العلاقة في ظل غياب الأنظمة والقوانين ذات العلاقة .

في حين حمّل مسئول إدارة العلاقات والتوعية القضائية بوزارة العدل المسئولية أيضاً على مشغلي الإنترنت (تيليمن ويمن نت) بصفة أساسية كونهما المشغلين الحصريين للإنترنت في اليمن، أما مسئول إدارة التسويق وعلاقات شركة يمن نت المملوكة لوزارة الاتصالات وتقنية المعلومات فقد قام بتحميل المسئولية على وزارة الاتصالات كونها – وفقاً لتفسيره – هي المسئولة عن السياسات العامة التوعوية، في حين تتحمل شركة يمن نت الركن المادي والخبرات الفنية لتنفيذ (السياسات التوعوية) بذلك الشأن، ويختلف هذا الرأي مع رأي مدير إدارة التسويق بشركة تيليمن، الذي ألقى المسئولية أيضاً على المؤسسة العامة للاتصالات كونها – حد وصفه – هي التي تبيع خدمة الإنترنت مباشرة للجمهور، وقد اختلفت الرؤى السابقة مع ما ذهب إليه مدير العلاقات العامة بديوان وزارة الاتصالات وتقنية المعلومات الذي حمّل المسئولية أيضاً عن ضعف برامج التوعية وتثقيف الجمهور اليمني بمخاطر الجريمة الإلكترونية على وزارة الإعلام نظراً – وفقاً لتعبيره

– لمطالباتهم بمبالغ مالية فلكية لقاء مساحات برامج وفلاشات إعلامية بوسائل الإعلام الرسمية للتوعية والإرشاد بمخاطر الجريمة الإلكترونية تنتجها وزارة الاتصالات وتقنية المعلومات، في حين لم يحمل مدير الوعي التكنولوجي الرقمي بالمؤسسة العامة للاتصالات إدارته أي مسئولية حيال ضعف أعمال توعية الجمهور بمخاطر الجريمة الإلكترونية، كون إدارته أنشئت عام 2022م واعتبر المدة القصيرة لإنشائها غير كافية لتحميلها مثل هذه المسئولية، وتقتصر حالياً أعمال هذه الإدارة على التوعية التكنولوجية الرقمية المحدودة لكوادر ومنتسبي المؤسسة العامة للاتصالات والوزارة.

7- المعوقات والصعوبات التي تحول دون قيام الجهات ذات العلاقة بأدوارها المطلوبة في التوعية بمخاطر الجرائم الإلكترونية:

كشف التحليل النوعي أهم الصعوبات والمعوقات التي تحول دون قيام تلك الإدارات بأدوارها المطلوبة في أعمال التوعية والتثقيف بمخاطر الجريمة الإلكترونية، التي جاءت بناء على وجهة نظر القائمين على الاتصال وفقاً للترتيب الآتي:

1- عدم وجود قانون لمكافحة الجريمة الإلكترونية.
2- ضعف التنسيق مع منظمات المجتمع المدني المحلية ذات العلاقة.
3- غياب التنسيق مع القطاع المستثمر في قطاع المعلوماتية.
4- غياب التنسيق مع الجهات المناظرة المسئولة عن الجريمة الإلكترونية.
5- الافتقار للخبرات الإعلامية من الباحثين في هذا المجال.
6- عدم وجود تدريب للموظفين بالجهة في هذا الاتجاه.
7- الموضوع غير مدرج في البرامج والخطط السنوية للجهة.
8- ضعف الإمكانات المادية وشحة الموارد المالية.

ويرى الباحث أن تهاون إدارات العلاقات العامة والإعلام بالجهات ذات العلاقة بالجريمة الإلكترونية بجهود توعية وتثقيف الجمهور بمخاطر الجريمة الإلكترونية قد انعكس على فقدان وعي النخبة السياسية والمشرع اليمني بأهمية وجود (قانون يعنى بمكافحة الجريمة الإلكترونية)؛ الأمر الذي أدى إلى عدم إقرار مجلس النواب للقانون المعني حتى وقت إعداد هذه الدراسة، وأصبحت بذلك اليمن هي الدولة العربية الوحيدة التي لا يوجد فيها قانون يكافح الجريمة الإلكترونية، وقد لاحظ الباحث انشغال تلك الإدارات بالأعمال النمطية وروتين البيروقراطية الإدارية الموروثة من عهود سابقة .

خاتمة:

سعت الدراسة للإلمام بالمشكلة البحثية من جميع أبعادها باستخدام المقاييس الكمية والكيفية المناسبة والاستفادة من التراث العلمي الذي تضمن التجارب الدولية في هذا المجال، وامتد ليشتمل على النزول الميداني للجهات ذات العلاقة، الذي تم من خلاله أيضاً إجراء المقابلات المعمقة مع المختصين في الجهات ذات العلاقة والحصول على البيانات والمعلومات المتاحة، الذي ساعد في استجلاء

الظاهرة موضوع الدراسة بصورة علمية تمخضت عن بلورة نتائج هذا البحث، والوصول إلى الخلاصة المتمثلة في عدد من التوصيات ومقترحات الدراسة.

وقد استهدف البحث معرفة أدوار الجهات ذات العلاقة بالجريمة الإلكترونية في اليمن في توعية الجمهور بمخاطر الجريمة الإلكترونية، وتضمن واقع الجرائم الإلكترونية في المجتمع اليمني، وقد خلص البحث إلى النتائج والتوصيات الآتية، التي يُطمح أن يستفيد منها صناع القرار في الجهات ذات العلاقة، بما يخدم مكافحة الجرائم الإلكترونية:

أولاً: النتائج:

أظهرت الدراسة انتشار الجريمة الإلكترونية في المجتمع اليمني، الذي يقابله ضعف أداء إدارات العلاقات العامة والإعلام بالجهات المسئولة عن التوعية بمخاطر الجريمة الإلكترونية في القيام بأدوارها التثقيفية والتوعوية المتعلقة بمواجهة مخاطر الجرائم الإلكترونية، والتعريف بأساليب الوقاية منها وفقاً لرؤية استراتيجية متكاملة، كما أن عدم صدور قانون مكافحة جرائم تقنية المعلومات في اليمن حتى يومنا هذا؛ يعكس كل ذلك ركاكة الأداء الحكومي والتشريعي في هذا الاتجاه، التي تعزى إلى غياب برامج التوعية والتثقيف بمخاطر الجرائم الإلكترونية ما انعكس على غياب أولوية ذلك الشأن عند صناع القرار، وإلى تفشي الجريمة الإلكترونية في المجتمع اليمني.

ثانياً: التوصيات والمقترحات:

1- سرعة إصدار قانون مكافحة جرائم تقنية المعلومات يعاقب مرتكبي جرائم الإنترنت في اليمن، ويحدد المسئولية والعقاب ويعرف الجرائم الإلكترونية وعناصرها وأركانها وكيفية القصد الجنائي فيها، إن التلكؤ في إقرار قانون مكافحة الجريمة الإلكترونية حتى يومنا هذا، يساعد بصورة مباشرة في انتشار الجرائم الإلكترونية بأنواعها في اليمن.

2- إدراج اللوائح المتعلقة بالتوعية من مخاطر الجرائم الإلكترونية في برامج وخطط إدارات العلاقات العامة والإعلام بالجهات ذات العلاقة، وإعطاءها الاهتمام اللائق في توعية المواطنين بمخاطرها، وإقامة شراكات فيما بينها من جهة، وفيما بينها والقطاع المستثمر في تكنولوجيا المعلومات والاتصالات والإنترنت من جهة أخرى.

3- إدراج تعليمات الوقاية من الجرائم الإلكترونية ضمن منهج دراسي (للتربية الإعلامية) لطلبة المدارس والجامعات، يتناول فيه طرق الاستخدام الآمن للإنترنت وطرق الوقاية من الجرائم الإلكترونية.

قائمة المراجع

[1] إبراهيم، رانيا. (2016)، جرائم الإنترنت في المجتمع المصري، رسالة دكتوراه، كلية البنات للآداب والعلوم والتربية، قسم اجتماع، جامعة عين شمس، القاهرة

[2] اسعيداني، سلامي. (2006)، استراتيجية الإعلام في مكافحة الجريمة ومظاهر العنف نحو استراتيجية عربية لتفعيل الإعلام الأمني، جامعة المسيلة، *مجلة العلوم الإنسانية والاجتماعية*، الجزائر.

[3] الأطرش، عصام وعساف، محمد محي الدين. (يونيو 2019م)، معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية، جامعة الشارقة، *مجلة جامعة الشارقة للعلوم القانونية*، مج 16، ع1.

[4] البهي، رغدة. (2018، يناير)، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، المركز الديمقراطي العربي، *مجلة الدراسات الإعلامية*، ع 1، برلين

[5] بيت المال، حمزة أحمد. (2014) الإعلام ودوره في التوعية بالجرائم عبر وسائل التواصل الاجتماعي، ورقة علمية مقدمة للملتقى العلمي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان.

[6] الجوهري، محمود. (1997)، اتجاهات حديثة في العلاقات العامة، مكتبة الأنجلو المصرية، القاهرة

[7] حجاب، محمد منير ووهبي، سحر محمد. (بدون تاريخ)، المداخل الأساسية للعلاقات العامة، دار الفجر للنشر والتوزيع، الجيزة.

[8] الحزورة، نوال وحيدر، مهدي. (2020، سبتمبر)، استخدام الشباب اليمني للإنترنت وعلاقته بمستوى وعيهم بالشائعات الإلكترونية حول الأحداث الجارية، *مجلة الإعلام العربي والمجتمع*، مركز كمال أدهم للصحافة التلفزيونية والرقمية، كلية الشئون الدولية والسياسات العامة، الجامعة الأمريكية بالقاهرة، ع 29، القاهرة.

[9] الحاج، آمال. (2016، سبتمبر) دور الإعلام الأمني في نشر الوعي الاجتماعي ومكافحة الجريمة، *مجلة السودان*، ع 7، السودان.

[10]الحديدي، منى سعد. (2004)، الإعلام والمجتمع، ط1، الدار المصرية اللبنانية، القاهرة.

[11]الخراساني، سبأ. (2013)، الأبعاد الاجتماعية للجريمة الإلكترونية، رسالة ماجستير، غير منشورة، كلية الآداب والعلوم الإنسانية، قسم علم الاجتماع، جامعة صنعاء، اليمن.

[12]خيرالدين، حسن. (1986)، العلاقات العامة المبادئ والتطبيق، دارعين شمس للنشر، القاهرة.

[13]الفقيه، محمد والصالحي، حاتم. (2017، مايو) دور شبكات التواصل الاجتماعي في إمداد الشباب العربي بالمعلومات والأخبار حول ظاهرة الإرهاب، *المجلة العربية للإعلام والاتصال*، ع 17، السعودية

[14]كافي، مصطفى يوسف. (2015)، تخطيط الحملات الإعلامية والإعلانية، ط1، دار الحامد للنشر والتوزيع، عمان.

[15]الدحلة، محمود. (2018)، دور صفحة وحدة مكافحة الجرائم الإلكترونية على موقع الفيسبوك في التوعية الأمنية، رسالة ماجستير، غير منشورة، كلية الإعلام، قسم الصحافة والإعلام، جامعة الشرق الأوسط، الأردن.

[16] الزبن، غدير والخرابشة، عبد الكريم. (2021)، الجرائم الإلكترونية ومستوى الوعي بخطورتها، *مجلة الجامعة الإسلامية للدراسات الإنسانية*، ع 29، الأردن.

[17]الهادي، هيام. (2020، صيف)، تعرض المراهقين للجرائم الإلكترونية عبر وسائل الإعلام الرقمي وتأثيرها على إدراكهم للأمن الاجتماعي المصري، جامعة الأهرام الكندية، كلية الإعلام، *المجلة العربية لعلوم الإعلام والاتصال*، ع 30، القاهرة.

[18]الوصابي، علي حميد. (يونيو 2021م)، تحديات الأمن السيبراني على مستوى الهاتف النقال وشبكات المنظمات، وزارة الاتصالات وتقنية المعلومات، ورقة عمل مقدمة للمؤتمر الوطني الأول للأمن السيبراني، صنعاء.

[19]اليوسفي، عبدالإله. (2020، يوليو، 4، 14) مقابلة الباحث مع مدير الشئون القانونية في البحث الجنائي، صنعاء.

[20]بيت المال، حمزة. (2014، سبتمبر) الإعلام ودوره في التوعية بالجرائم عبر وسائل التواصل الاجتماعي، كلية العلوم الاستراتيجية، بحث مقدم إلى الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، الأردن

[21]جريمة الحاسوب: وكيبيديا .

[22]ذمران، عبدالفتاح محمد نقلاً عن GLOBAL DIGITAL HEADLINES. (يونيو 2021م)، الإجراءات الفنية لحماية أمن المعلومات في شبكة الاتصالات الوطنية، وزارة الاتصالات وتقنية

المعلومات، ورقة عمل مقدمة إلى المؤتمر الوطني الأول للأمن السيبراني، صنعاء.

[23]سجية، مرسيس وخيرة، بحاش وزهرة، بن نخلة وشيماء، سعيد. (2019) أثر استخدام مواقع التواصل الاجتماعي في انتشار الجريمة الإلكترونية، بحث تخرج ليسانس، كلية العلوم الإنسانية والاجتماعية، قسم علوم الإعلام والاتصال، جامعة محمد بو ضياف المسيلة، الجزائر.

[24]سراج، أحمد. (2021، يونيو)، التحديات الأمنية في مكافحة الجريمة الإلكترونية، ورقة عمل وزارة الداخلية مقدمة لاجتماع لجنة الدفاع والأمن واللجان ذات العلاقة بمجلس الشورى الجمهورية اليمنية، صنعاء

[25]سراج، أحمد والعبالي، وسيم. (2022، سبتمبر)، الجريمة الإلكترونية وأضرارها على الفرد والمجتمع، وزارة الدفاع، محاضرات بالكلية الحربية، صنعاء

[26]سعيد، محمد سعيد. (2013)، العلاقات العامة نشأتها وتطورها، محمد إبراهيم للطباعة والنشر، السودان، الخرطوم.

[27]سوير، سفيان. (2011)، جرائم المعلوماتية، رسالة ماجستير، غير منشورة، جامعة تلمسان، الجزائر.

[28]عدلي، عصمت. (2011)، الإعلام الأمني بين النظرية والتطبيق، دار الجامعة الجديدة، الإسكندرية

[29]فارش، رشيدة وقاوش نورة. (2018)، تأثير مواقع التواصل الاجتماعي في انتشار الجريمة الإلكترونية في وسط المراهقين، رسالة ماستر، كلية العلوم الإنسانية والاجتماعية، قسم علوم إنسانية، تخصص علوم الإعلام والاتصال، جامعة أكلي والحاج بويرة، الجزائر

[30]محمد، ميادة بشير. (2017)توظيف برامج العلاقات العامة في التوعية بمخاطر الجرائم الإلكترونية، رسالة ماجستير، غير منشورة، قسم علوم الاتصال تخصص العلاقات العامة والإعلان، جامعة السودان للعلوم والتكنولوجيا، السودان.

[31]نبيلة، هروال. (2014)، جرائم الإنترنت، دراسة مقارنة، أطروحة دكتوراه، غير منشورة، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، الجزائر.

[32]يوسف، صغيري. (2013)، الجريمة المرتكبة عبر الإنترنت، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، الجزائر.

[33]أساسيات الإنترنت

https://mawdouaa.com Online25/7/2021

[34]أنواع الجرائم الإلكترونية

https//:mawdoo3.com Online25/7/2021

[35] Hollis Stambaugh ، David S.Beupre ، David J. Lcove ، Richaveed Baker ، Wayne Cassaday and Wayne P. Williams، Electronic Crime Needs Assessment for State and Local Law Enforcement، U.S.Department of Justice ، Office of Justive Programs، National Institute of Justive https://www.ncjrs.gov/pdffiles1/nij/186276.pdf Online 4/6/2021

[36] Khan ،Afrozulla. (2018، May)، Cybercrime Awareness among Msw Students، School Of Social Work، Mangaluru، India، Department of Criminology and Forensic Science ، School of Social Work، Journal of Forenisic Scieences and Criminal Investigation ، Research Articale ، Volume 9 ، Issue 2

[37] https://juniperpublishers.com/jfsci/pdf /JFSCI.MS.ID.555757.pdf Online17/6/2021

[38] Otter ،Stephen and Others. (2015، December)، Real Lives،real crimes، study of digital crime and policing، UK ،London ،HMIC، Inspecting Policing in the police interest https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf Online17/6/2021

[39]Rahmi، Tariq and Hussain، Mumtaz، social media-Related Cybercrims and Techniques for Their Prevention، College of Computer Science & Information Systems ، Institute of Business Management ، Sciendo ، Riga Technical University ، Applied Computer System، 2019-May Vol.20. no.1، Pakistan،Karatchi https://www.researchgate.net/publication/333944511_Social_Media-Related_Cybercrimes_and_Techniques_for_Their_Preventiononline 17/6/2020