"علاقة الجرائم الإلكترونية بالأداء المهني للصحفيين المصريين"

أحمد جعفر أحمد محمد (*)

مقدمة:

يمكن تعريف الجرائم الإلكترونية بأنها الجرائم التي تستهدف الأجهزة الإلكترونية بجميع أنواعها، من خلال اختراق عبر شبكه الإنترنت بغرض إعاقتها عن العمل أو إغراقها بالفيروسات الضارة بهدف تدميرها كليا أو جزئيا أو سحب معلومات وبيانات شخصيه من محتواها ونشرها بهدف استخدامها بشكل غير مشروع يضر بالضحية، ومن أمثلة الجرائم الإلكترونية التي يتعرض الأفراد لها هي الابتزاز والاحتيال والتصيد والتنمر الإلكتروني، سرقة الأموال والحسابات كلمات السر وانتحال الشخصيات، والإرهاب الإلكتروني، والتجسس وتخريب وتعطيل الأجهزة.

وتتعرض المؤسسات الإعلامية مؤخراً لبعض أنواع الجرائم الإلكترونية، التي أدت إلى تعطيلها، وحجب موقعها على الإنترنت وصعوبة تصفح الجمهور لها، ونشر الأخبار الزائفة والإشاعات عليها، وإلحاق الضرر ببياناتها وأجهزتها واتصالاتها، وحذف أرشيفها الرقمي، وانتهاك حقوق الملكية الفكرية، بجانب تهديد وترهيب الصحفيين العاملين بها باختراقهم والتجسس عليهم.

وعلى سبيل المثال تعرضت صحف عالمية كثيرة لبعض الجرائم الإلكترونية، مثل "نيويورك تايمز" و"شارل إبدو" و"لوموند" كما تعرضت مؤسسات عربية لنفس الأمر مثل صحيفة "عكاظ السعودية" و"الأخبار اللبنانية" و"الوطن البحرينية"، وتعرضت صحف "المصري اليوم" و"الأهرام" و"وكالة أنباء الشرق الأوسط" و"الوطن" و"دار التحرير" و"الوفد".

وحسب موقع websiterating فإن هناك جريمة إلكترونية كل (١٠) ثوان، وهناك (٢,٢٤٤) هجومًا إلكترونيًا يوميًا، وأيضا ١ من أصل ٣٦ هاتفًا ذكيًا يعمل بنظام أندرويد به تطبيقات محفوفة بالمخاطر مثبتة، وبالنسبة للمؤسسات والشركات فهناك (٦٦%) منهم تعرضت للجرائم الإلكترونية في عام ٢٠٢٠.

(*) هذا البحث مستل من رسالة الماجستير الخاصة الباحث، وهي بعنوان: [الأمن الإلكتروني للصحفيين المصريين وعلاقته بالأداء المهني]، وتحت إشراف د. صابر حارص محمد – كلية الآداب – جامعة سوهاج & د. نها السيد عبد المعطي - كلية الآداب- جامعة سوهاج.

ومما تقدم يتبين أهمية الوعي بالجرائم الإلكترونية وسبل مكافحتها من جانب الصحفيين المصريين بشكل خاص، ونتيجة لغياب هذا الوعي أو انخفاض مستواه تعرضت الكثير من المؤسسات الصحفية والإعلامية إلى بعض أنواع الجرائم الإلكترونية، ومن هنا تأتي أهمية البحث الوقوف على الجرائم الإلكترونية التي تهدد الأداء المهني الصحفي، وكيفية الوقاية منها.

الجرائم الإلكترونية

تعددت المصطلحات والمسميات التي تعبر عن الجرائم المعلوماتية، فالبعض يطلق عليها الجرائم الإلكترونية، وجرائم الإنترنت أو جرائم الكمبيوتر والإنترنت، والبعض الآخر يطلق عليها الجرائم السيبرانية على اعتبار أن هذا المصطلح يضم جرائم الكمبيوتر وجرائم الشبكات، وجرائم تقنية المعلومات، والجرائم الذكية، وجرائم نظم المعلومات، وجرائم العصر وغيرها من المصطلحات والتي تعني الاستخدام غير المشروع للتقنية المعلوماتية، والاعتداء على أي كائن بشري أو مادي بصفة طبيعية أو اعتبارية. (غريب، ٢٠١٧، ص٢٢)

وتتكون الجرائم المعلوماتية أو الجرائم السيبرانية افتراضيا من مقطعين Cyber Crime +، المقطع الأول الجريمةcrime ، والإلكترونية cyber ويستخدم المقطع الأخير لوصف فكرة من عصر المعلوماتية، فالجرائم الإلكترونية تعرف قانونا بأنها " المخالفات التي ترتكب ضد الأفراد أو المجموعات بدافع، ويقصد منها إيذاء سمعة الضحية أو أي أذى مادي أو نفسي مباشر أو غير مباشر باستخدام شبكات الاتصالات والمعلومات"، وتعد الجرائم الإلكترونية ظاهرة اجتماعية متوافقة مع انتقال المجتمعات الي المجتمع الرقمي حيث ينتقل فيها نشاط الناس من الواقع الفعلي المادي إلى الواقع الافتراضي، وتعد عابرة للحدود الوطنية وتمتاز بسهولتها وانخفاض تكاليفها والسرعة في تنفيذها وتوظيف الاتصالات في ارتكابها. (العوادي، ٢٠١٦، ص١٠)

وتنصب الجرائم الإلكترونية على أحد العناصر الاتى بيانها إما منفردة، أو أنها تستهدف كل هذه العناصر:

1 - الأشخاص: تستهدف نسبة كبيرة من الجرائم الإلكترونية أشخاصاً أو جهات معينه بشكل مباشر من خلال استخدام التهديد، أو الابتزاز أو السرقة أو الابتزاز الأخلاقي، فمثالً قد يتم سرقة المال بواسطة الإنترنت، وذلك من خلال استخدام

أرقام بطاقات مصرفية تعود للغير، وكذلك استخدام الإنترانت لممارسة الفاحشة مع قاصر أو مع فتاة حتى وان كانت غير قاصر فيما بات يطلق عليه "الجنس الإلكتروني" أو الإرشادات التي تحمل في طياتها تعليمات إرهابية موجهة ضد شخص أو أشخاص أو جهات معينة بذاتها. (الجهيني، ٢٠٠٥، ص٧٦)

٢ -المعلومات: أصبحت المعلومات مصدر قوة وسلطة، حتى قيل أن المعرفة هي السلطة، وأن الحصول على المعرفة وحسن استخدامها عاملان أساسيان من عوامل التقدم، ولذلك فإن التكنولوجيا الحديثة تتعلق بالمعرفة، فالمعلومات اضحت قيمة اقتصادية كبيرة، وأصبحت أيضا مجالا خصبا للجرائم الإلكترونية من خلال القيام بسرقة المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر الإنترنت، فهذا النوع من الجرائم يستهدف سرقة المعلومات أو تغييرها أو حذفها. (حسنية، ٢٠١٧، ص١٢)

٣ - الأجهزة: في هذه الحالة تكون الأجهزة هي هدف هذه الجرائم، وذلك من خلال استخدام أساليب فنية لتدمير مكونات الحاسوب المعنوية، وذلك لتعطيلها أو تخريبها أو محو البيانات والمعلومات والبرامج المخزنة في نظام المعالجة للحاسوب، وأهم هذه الأساليب المستخدمة هي الفيروسات. (عرب، ٢٠٠١، ص٤٤٨)

- أسباب انتشار الجرائم الإلكترونية:

١ -سهولة الوصول: من المعروف أن أي شخص بالعالم يمكن أن يتصل بالإنترنت، يكفي أن تمتلك حاسوب واشتراك دوري، هذا ما خلق مشكلة حماية نظم الحاسوب ضد الوصول غير المصرح به، حيث توفر الإمكانات لانتهاك التكنولوجيا.

٢ -الإهمال: عبارة عن عدم الانتباه لحماية النظم المعلوماتية، ويعتبر إهمالا يسمح للمجرمين بالتحكم أو تدمير الحاسوب، ويمكن القول إن الإهمال هو اهم أسباب الجرائم الإلكترونية سواء من طرف الأفراد أو الشركات، فعدم تعيين برامج حماية الحاسوب ونظم التشغيل يؤدي إلى التعرض للهجمات الإلكترونية، وكذلك الشركات والمؤسسات التي تتقاعس عن اقتناء برامج الحماية، تخاطر بسرية وخصوصية معلومات زبائنها.

٣ -الانتقام أو التحفيز: المجرم المعلوماتي يسعى دائما لتحدي نفسه، ليتكون لديه نوع من الطمع الدائم في إتقان الأنظمة المعقدة لإلحاق الضرر والخسائر بالضحايا، خاصة الشباب منهم الذين تحركهم رغباتهم للحصول على عائدات

مالية بسرعة، تكون وجهتهم العبث بالبيانات خاصة في أعمال التجارة الإلكترونية والدفع الإلكتروني. (Maghu، ٢٠١٤، ص٨٥٣)
٤ -ضعف تنفيذ القوانين وفرضها.
٥ -جرائم الإنترنت بهدف الدعاية أو اكتساب الشهرة: اغلبها تتم من طرف شباب وهدفهم منها ملاحظتهم لكن دون الحاق الأذى بالآخرين .
٦ -الأسباب النفسية: كالإحباط والفراغ الذي يعاني منه بعض مستخدمي الإنترنت ما يؤدي بهم الي استكشاف طرق القرصنة تعلمها لملأ الفراغ وتحقيق الربح المادي .
٧- عدم وعي المستخدمين: خاصة مع إهمالهم لسبل الحماية اللزمة كتعيين نظم التشغيل وتثبيت برامج الأمن والحماية، كما يميلون لاستخدام المواقع غير الموثوقة التي تحتوي العديد من الثغرات المساعدة على عمليات القرصنة والتي تنشر الفيروسات. (شلبية، ٢٠١٩، ص١٤٧)

- **تصنيف الجرائم الإلكترونية وأشكالها:**

صنفت اللجنة الأوروبية الجريمة الإلكترونية في ثلاثة تصنيفات رئيسية وهي كالآتي:
أولاً - الجرائم الإنترنت التقليدية: مثل الغش والخداع وترويج للمنوعات والقرصنة والنصب الإلكتروني، وعدم تسليم الأشياء المباعة بعد الحصول على ثمنها، وتقليد الماركات وبيعها والاعتداء على الملكية الفكرية وبيع المسروقات .

ثانياً - جرائم نشر المحتوى غير المشروع: نشر المواد الإعلامية التي تساعد على انتشار الجريمة مثل صناعة القنابل والمواد الحارقة وإخفاء أدلة ارتكاب الجرائم والاعتداءات الجنسية، والتحريض على الانتحار، وتجنيد الإرهابيين وأعمال الشغب والعنف والتمييز العنصري .
ثالثاً - الجرائم الخاصة بتقنية الاتصالات والمعلومات: الاعتداء على الأنظمة المعلوماتية، بالتعطيل أو السرقة أو بالتخريب وحذف المحتوى وإنشاء الفيروسات ونشرها والاختراق للأنظمة والقرصنة الإلكترونية. (صائغ، ٢٠١٨، ص٤٤)

- **مكافحة الجرائم الإلكترونية: -**

١ -تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية وبرمجيات الفيروسات وبرامج التجسس (خبازي، ٢٠١٧، ص٣٧)
٢ -استخدام جدار الحماية وهو حاجز يوضع بين المستخدم وخادم شبكة الإنترنت، ومن أهم مهامه فحص المعلومات الداخلة والخارجة والسماح لها بالمرور في حالة مطابقتها للمواصفات و تقديم تقارير عن التحركات المشبوهة.
٣ -تشفير البيانات و هو تحويل المعلومة من نص واضح إلى آخر غير مفهوم، و قد أستحسن هذا النوع من النظام لنجاحه في عدم كشف المعلومات على شبكة الإنترنت. . (المنتشري، ٢٠٢٠، ص٤٦٧)
٤ -استخدام أحدث النسخ والإصدارات الخاصة بالمتصفحات لتجنب الثغرات الإلكترونية الموجودة في الإصدارات القديمة التي توفر بيئة خصبة للمخترقين.
٥ -مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.
٦ -استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات، وعدم أيقاف برامج مكافحة الفيروسات والجدار الناري.
٧ -الاحتفاظ بنسخ احتياطية لكل المعلومات الحساسة في أقراص إضافية ليست مرتبطة بالشبكة .
٨ -استخدام أنظمة كشف الاختراقات ووضع حلول للثغرات الأمنية. (رشاد، ٢٠١٨، ٤٤٦)
٩-اختيار كلمات مرور قوية، وعمليات تحقق أمنية لمواقع التواصل الاجتماعي، والبريد الإلكتروني، والحسابات الشخصية على الحاسوب أو الهواتف الذكية. (المنتشري، ٢٠٢٠، ص٤٦٧)
١٠ -تجنب تحميل برامج أو ملفات مجهولة المصدر أو غير الموثوقة، ويجب فحص الأقراص وشرائح الذاكرة والتأكد من خلوها من الفيروسات قبل استخدامها. (العوادي، ٢٠١٦، ص٢٣)
١١ -ضرورة التأكد من العناوين الإلكترونية التي تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب بنكي.
١٢ -عدم حفظ الصور الشخصية في الكمبيوت، وتجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب. (رشاد، ٢٠١٨، ٤٤٦)

١٣ -حماية المعلومات الشخصية ومنع الآخرين من الاطلاع عليها.
١٤ -عدم إرسال أي معلومات شخصية عبر البريد الإلكتروني، أو الإفصاح عن معلومات خاصة عبر مواقع التواصل الاجتماعي. (المنتشري، ٢٠٢٠، ص٤٦٧)
١٥- كسر حاجز الخوف وضرورة الإبلاغ عنها، إذ يعتبر مركز الشكاوى الخاص بالجرائم الإلكترونية في العالم من اهم الأطر المؤسسة لمكافحة هذا النوع من الجرائم. ،(فاريش، ٢٠١٨، ص٧٢)

- **تحديات تعوق مكافحة الجرائم الإلكترونية:**

أشارت دراسة (Henrichsen , 2019) أن عوائق تبني الصحفيين لأمن المعلومات هي- :
١ -عدم فهم الصحفيين للمخاطر والتهديدات الناتجة عن الجرائم الإلكترونية، وعدم الوعي بخطورة الاختراق والقرصنة الإلكترونية، والمراقبة والتجسس الإلكتروني على الصحفيين وممارساتهم المهنية.
٢ -تناقض اتجاهات الصحفيين نحو تقنيات الأمن الإلكتروني، وأيضا الصحفيين لديهم تناقض تجاه الأدوات والاستراتيجيات التي من شأنها حماية أجهزتهم وحساباتهم ومعلوماتهم وبياناتهم.
٣ -الافتقار إلى الثقافة الأمنية لدى المؤسسات، فالمؤسسات الإخبارية لا تولى اهتمام كافي لمسائل الأمن والحماية الإلكترونية.
٤- الاعتقاد بأن ممارسات أمن المعلومات مطلوبة فقط مع الصحفيين الذين يعملون مع مصادر سياسية حساسة، وأن الصحفيين الآخرين يعتقدون انهم لا يمكن أن يقعوا ضحايا للجرائم الإلكترونية كالتجسس والمراقبة، لأنهم يعملون في تغطية قضايا عامة غير حساسة.

الدراسات السابقة:

١) دراسة Tsui (٢٠٢١) بعنوان: وعى الصحفيين بالمخاطر التكنولوجية وآثارها على حرية الصحافة.

تهدف هذه الدراسة إلى التعرف على قياس خبرات الصحفيين في استخدام تقنيات أمن المعلومات، لمواجهة الجرائم الإلكترونية، وذلك من خلال دراسة وصفية، والمنهج المسحي، واعتمدت على أسلوب المقابلة لجمع البيانات من عينة عمدية قوامها ٢٠ صحفي في هونج كونج.

وتوصلت الدراسة الى: -

- أن الصحفيين ذوي الخبرات والمهارات الأمنية المتقدمة في مجال الأمن السيبراني، لديهم وعي أكثر لحماية أنفسهم من المخاطر والتهديدات كالجرائم الإلكترونية التي تجعل الصحفيين ضحايا لها، وهذا يمكنهم من التواصل بأمان مع مصادرهم وزملائهم، ولديهم القدرة في استمرار التعلم لتقنيات الأمن الإلكتروني.

- وتوجد هناك علاقة وثيقة بين ارتفاع مهارات الأمن الإلكتروني لدى الصحفيين (المعرفة بمفاهيم الأمن السيبراني، المعرفة بطرق مكافحة الجرائم الإلكترونية، المعرفة بمخاطر الجرائم الإلكترونية)، وبين حرية الممارسات الصحفية، وأن ذلك لا يعني التحرر من المراقبة والتجسس والاختراق الإلكتروني فقط، بل اختيار قصص صحفية حساسة لتغطيتها.

٢) دراسة أحمد (٢٠٢٠) بعنوان: إدراك الصحفيين للمخاطر الرقمية وإستراتيجيات تطبيقهم للأمن الرقمى فى عملهم المهنى.

تهدف هذه الدراسة إلى التعرف على المخاطر والتهديدات الرقمية التي تواجه الصحفيين، وذلك من خلال دراسة وصفية اعتمدت على المنهج المسحي وتم استخدام أداة الاستبيان لجمع البيانات من عينة متاحة قوامها ١٣٧ صحفي في مصر يعملون بصحف (أخبار اليوم، واليوم السابع، والوطن، والشروق، والوفد).

- وتوصلت الدراسة إلى:

- أن ٩٥% من الصحفيين يعتقدون بأنهم عرضة للهجمات الرقمية، وغالبية الصحفيين ليسوا على دراية بأدوات الأمن الرقمي مثل التشفير الإلكتروني، مما يدل على أهمية الحاجة لتوسيع مفهوم الوعي بالتهديدات الرقمية والأمن الرقمي

لديهم، حيث أفاد ٧١% من الصحفيين على ضرورة تبني استراتيجيات تنمي من الوعي بالأمن الرقمي للصحفيين.
- وجاءت أكثر مخاوف الصحفيين من التهديدات الرقمية هي (تسريب البيانات الشخصية، والخوف من انتهاك الخصوصية، وخسارة البيانات، والخوف على المصدر) (أحمد، ٢٠٢٠)

٣) دراسة الأزرق (٢٠٢٠) بعنوان: التهديدات الرقمية ضد الصحفيين المصريين ووعيهم بالآليات المستخدمة للحفاظ على سلامتهم.
تهدف هذه الدراسة إلى التعرف على اتجاهات الصحفيين نحو المخاطر الرقمية ومدى وعيهم بها، وذلك من خلال دراسة نوعية اعتمدت على المنهج المسحي، واستخدام المقابلة المتعمقة لجمع البيانات من ٦٠ صحفي يعملون بالصحف القومية والخاصة والحزبية المصرية، واعتمدت أيضاً على المنهج التحليلي لتحليل المستندات القانونية والإطار القانوني للجريمة الإلكترونية في مصر.
- وتوصلت الدراسة إلى:
- أن الصحفيين يعتمدون بشكل كبير على الإنترنت وخدماته المختلفة في ممارسة العمل الصحفي، وهم على وعي بحماية أنفسهم من مخاطر الإنترنت، وقد عرف الصحفيين التهديدات الرقمية على أنها (مصدر للتسريبات ونشر الشائعات والأخبار الكاذبة التي تدمر الأمن والسلام الاجتماعي، ويرى البعض أنها عبارة عن حملات التشهير على الإنترنت ، وانتهاك خصوصية الصحفيين ، والتصيد الاحتيالي ، والمراقبة عبر الإنترنت ، والقرصنة على الإنترنت ، والقرصنة على الحسابات ، بالإضافة إلى هجوم البرامج الضارة ، والتضليل ضد الصحفيين ، ومهاجمة أجهزة الكمبيوتر الشخصية والحسابات عن طريق الفيروسات، والتحرش الجنسي عبر الإنترنت)
- وأن ٢٢% من الصحفيين يعرفون كيفية حماية أنفسهم ويمكنهم استخدام التقنيات والبرامج المختلفة بشكل احترافي والتي تساعدهم على تجنب المخاطر الرقمية. (الأزرق، ٢٠٢٠)

٤) دراسة العشري (٢٠٢٠) بعنوان: اتجاهات الصحفيين نحو قانون مكافحه جرائم تقنيه المعلومات رقم ١٧٥ لسنه ٢٠١٨ والممارسات الصحفية المتصلة بها.
تهدف هذه الدراسة إلى التعرف على اتجاهات الصحفيين حول طبيعة العمل الصحفي والممارسات المهنية المتصل بها، واتجاهاتهم نحو الإيجابيات

والسلبيات القانون، وذلك من خلال دراسة وصفية اعتمدت على المنهج المسحي باستخدام الاستبيان لجمع البيانات من عينه متاحة مكونة من ١٨٨صحفي.
- وتوصلت الدراسة إلى:
١- جاءت آراء الصحفيين حول مدى رضائهم عن تطبيق قانون مكافحه جرائم تقنيه المعلومات بأن ٩٥% غير راضٍ تماما، و٠% راضٍ جدا.
2- وجاءت إيجابيات وسلبيات القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، فكانت الإيجابيات مرتبة كالتالي (يحمي المصادر، حماية المجتمع من الأخبار الكاذبة، حماية المادة العلمية، حماية جريمة الانتفاع بدون حق بخدمات الاتصالات، حماية الحريات الشخصية، حماية الأمن القومي، حماية الدخول غير المشروع على المواقع، حماية تجاوز حدود الحق في الدخول على المواقع والشبكات، حماية الملكية الفكرية، وأخيرا القانون يحمي الصحفيين).
٣- وبخصوص سلبيات القانون جاءت مرتبة كالتالي (صياغة بعض المواد الغامضة تحتاج الى تفسير، المواد القانونية لا تحمي الصحفيين، عرقلة الصحفيين في حجب المعلومات، عرقلة الصحفيين في النشر). (العشري، ٢٠٢٠)

٥) دراسة Christofoletti (٢٠١٨) بعنوان: <u>الهجمات والتهديدات الرقمية وانعكاساتها كمخاطر مهنية لدى الصحفيين.</u>
تهدف هذه الدراسة إلى معرفة المخاطر والتهديدات التي يتعرض لها الصحفيون، سواء كانت مخاطر جسدية، أو أخلاقية، أو قانونية، أو سياسية، أو رقمية، وأثرها على الممارسات الصحفية، وذلك من خلال دراسة تحليلية، استخدمت هذه الدراسة تحليل تقارير صادرة عن المنظمات غير الحكومية الوطنية والدولية من سنة ٢٠٠١ الي سنة ٢٠١٦ وتحليل نحو ٨٠ تقرير من ٩ منظمات مختلفة.
<u>- وتوصلت الدراسة إلى:</u>
١- بينت الدراسة أن الهدف من الهجمات الإلكترونية هو الاعتراض، أو المراقبة، أو التضليل، أو الإتلاف، أو الكشف غير مصرح به عن المعلومات والهويات والمواقع الجغرافية والبيانات الحساسة لدى الصحفيين، مما تؤدي الى حدوث مخاطر جسدية أو أضرار معنوية أو مادية، وذكرت الدراسة بأن مخاطر الجرائم الإلكترونية هي نتاج تفاعل واستخدام الصحفيين لتكنولوجيا المعلومات والاتصال أثناء الممارسات الصحفية اليومية.

٢- وجاءت الجرائم الإلكترونية التي يتعرض لها الصحفيون هي (مراقبة التنقل والموقع الجغرافي، انتهـــاك واعتراض الرسائل الفورية، تهديدات البريد الإلكتروني، تثبيت وتنشيط فيروسات وبرامج خبيثة لجمـــــــع وتدمير الملفات، انتهاك الحسابات الشخصية على الإنترنت، تهديدات الرسائل القصيرة، اختراق غـــــرف الأخبار، سرقة كلمات المرور من خلال التصيد الاحتيالي، سرقة المعلومات أو فقدها، حالات التنصت على الهاتف). (٢٠١٨، Christofoletti)

مشكلة الدراسة:

على الرغم من المخاطر والأضرار التي يمكن أن تسببها تكنولوجيا الاتصال والمعلومات على العمل الصحفي عامة والأداء المهني للصحفيين خاصة إلا أن الدراسات العلمية في هذا الصدد اتجهت إلى دراسة الآثار والتداعيات الإيجابية التي تنعكس في سرعة أداء العمل الصحفي ودقته.
فضلاً عن أن هناك قصور شديد في مكافحة الجريمة الإلكترونية، لأنها تتسم بالخفاء وتجاوز الحدود والسرعة في حدوثها وصعوبة اكتشافها، وأصبحت التشريعات والقوانين غير كافية لمواجهتها، مما أدى إلى استمرار انتشار الجرائم الإلكترونية في البيئة الرقمية، واستخدامها كأداة للحروب في العصر الحالي، انتقلت بطبيعة الحال إلى العمل الصحفي والإعلامي.
ومما تقدم يتضح أن ثمة تهديدات وجرائم إلكترونية تحدث في البيئة الصحفية العربية والأجنبية على سواء، وتترك آثارها على الممارسات الصحفية بشكل فردي ومؤسسي، في حين لم تتصدى الدراسات العربية لذلك بالقدر الكافي الذي يوفر للصحفيين بيئة آمنة تقلل من المخاطر وتحافظ على جودة الممارسات المهنية، وهو ما يمكن بلورته في التساؤل الرئيسي (أثر الجرائم الإلكترونية على الممارسات المهنية للصحفيين المصريين).

أهمية الدراسة:

- تزويد الصحفيين بالوعي اللازم لتجنب الوقوع كضحايا للجرائم الإلكترونية ومقومات ممارسة المهنة في ظل بيئة آمنة تحميهم وتحمي مؤسساتهم التي يعملون بها من أعمال القرصنة والاختراق، إضافة إلى إكسابهم طرق التعامل حال وقوع هذه التهديدات والتقليل من مخاطرها.

- معالجة القصور في دراسة الظواهر المهنية التي تركت فيها التكنولوجيا آثاراً خطيرة على العمل الصحفي والإعلامي عامة نتيجة لندرة الدراسات السابقة العربية في هذا الصدد.
- دعم الدراسة نقابة الصحفيين والمؤسسات الإعلامية والصحفية وهيئات الإعلام بالدولة بأهمية توفير الأمن الإلكتروني للصحفيين، حتى يتسنى لهم الاستقرار المهني.

أهداف الدراسة:

١- التعرف على درجة وعي الصحفيين بالجرائم الإلكترونية.
٢- الكشف عن تأثير الجرائم الإلكترونية على الصحفيين المصريين.
٣- استطلاع مقترحات الصحفيين المصريين لمكافحة الجرائم الإلكترونية.

تساؤلات الدراسة:

١- ما درجة وعي الصحفيين بالجرائم الإلكترونية؟

٢- ما تأثير الجرائم الإلكترونية على الصحفيين المصريين؟

٣- ما مقترحات الصحفيين المصريين لمكافحة الجرائم الإلكترونية؟

نوع الدراسة:

تنتمي هذه الدراسة إلى الدراسات الوصفية التي تهتم بدراسة واقع الأحداث والظواهر والمواقف وتحليلها وتفسيرها، فيما يتعلق برصد الجرائم الإلكترونية التي يتعرض لها الصحفيون المصريون وتأثيراتها المهنية وطرق مكافحتها.

منهج الدراسة:

وتعتمد هذه الدراسة على منهج المسح الإعلامي "مسح القائم بالاتصال " لعينة من الصحفيين المصريين، بهدف جمع البيانات المتصلة بتعرض الصحفيين للجرائم الإلكترونية، وتأثيراتها المهنية، والسبل المقترحة لبيئة صحفية آمنة.

مجتمع الدراسة:

يتمثل مجتمع الدراسة في الصحفيين المصريين، الذين يعملون في الصحف المصرية (القومية والخاصة والحزبية)، وذلك لتمثيل كافة التيارات الصحفية في مصر.

عينة الدراسة :

تم تطبيق الاستبيان الإلكتروني على عدد ٩ مؤسسات صحفية، تمثل كافة التيارات الصحفية بمصر (القومي، والحزبي، والخاص)، على النحو التالي:
أولاً عينة التيار القومي : (الأهرام، أخبار اليوم، الجمهورية، روز اليوسف)
ثانياً عينة التيار الخاص : (اليوم السابع، المصري اليوم، الشروق، الوطن)
ثالثاً عينة التيار الحزبي : (الوفد)
وذلك باعتبار أن عدد هذه المؤسسات كافية لتمثيل التيارات الثلاث وتم اختيار ٢٥ صحفي من كل جريدة بالعينة المتاحة، بإجمالي ٢٢٥ صحفياً باعتبار أن حجم العينة هذا يناسب دراسات القائم بالاتصال

أداة جمع البيانات:

استخدم الباحث أداة الاستبيان لجمع البيانات من الصحفيين حول أثر الجرائم الإلكترونية على الممارسات الصحفية للصحفيين المصريين.

التعريفات الإجرائية للدراسة:

الجرائم الإلكترونية: وهي مجموعة من التهديدات الرقمية التي تسبب مخاطر للصحفيين على أجهزتهم الإلكترونية واتصالاتهم ومعلوماتهم وبياناتهم وحساباتهم الرقمية، مثل (التجسس والمراقبة الإلكترونية، وضياع وتلف الملفات واختراق البيانات، والابتزاز والتنمر الإلكتروني، وتعطيل الأجهزة الإلكترونية وقرصنتها، والأشكال الأخرى للجرائم الإلكترونية).

الصحفيون: وهم جميع الصحفيين الذين يعملون في الصحف المصرية بكافة أشكالها (القومية، والخاصة، والحزبية)، ويعتمدون على تكنولوجيا المعلومات والاتصال في ممارساتهم الصحفية اليومية، ويستخدمونها في كافة مراحل الأداء الصحفي.

نـتائج الدراسة:

المعرفة بـمفهوم الجرائم الإلكترونـية	ك	٪
نـعم	١٩٣	٪٨٥.٨
لا	٣٢	٪١٤.٢
الإجمالي	٢٢٥	٪١٠٠

معرفة الصحفيين بالجرائم الإلكترونية.

يهدف هذا الجدول للتعرف على نسبة الصحفيين المصريين الذين لديهم معرفة بمفاهيم الجرائم الإلكترونية، فجاءت نسبة الصحفيين الذين لديهم معرفة ٨٥%، بينما ١٤% من الصحفيين ليس لديهم أي معرفة، وهؤلاء يمكن أن تتأثر حياتهم الشخصية والمهنية بشكل كبير إذا لم يثقفوا أنفسهم ويأهلوا خبراتهم التكنولوجية لمستوى أفضل في مواجهة الجرائم الإلكترونية.

تعرض الصحفيين للجرائم الإلكترونية من قبل.

هل تعرضت للجرائم الإلكترونـية من قبل؟	ك	٪
نـعم	١٤٨	٪٦٥.٨
لا	٧٧	٪٣٤.٢
الإجمالي	٢٢٥	٪١٠٠

يجيب هذا الجدول على تعرض الصحفيين للجرائم الإلكترونية مثل (انتهاك خصوصيتهم، والتجسس والتنصت، والتصيد والابتزاز الإلكتروني، وتهديدهم، وقرصنة أجهزتهم واختراق حساباتهم على الإنترنت ...إلخ)، فذكر نسبة ٦٥.٨% من الصحفيين أنهم تعرضوا للجرائم الإلكترونية من قبل، بينما ذكر ٣٤,٢% من الصحفيين بأنهم لم يتعرضوا لأي جرائم إلكترونية من قبل، ويمكن القول أم التعرض لمثل هذه الجرائم تهدد استقرار العمل الإعلامي، لأن الصحفيين يتسم أدائهم بالاعتماد الكلي على تكنولوجيا الاتصال والمعلومات، وكذلك تعتمد المؤسسة الصحفية على بنية تحتية تكنولوجية كي تؤدي أعمالها

ومهامها، وهذه البنية التحتية التكنولوجية يمكن أن تتعرض للتدمير والتخريب وفقدان كامل معلوماتها وبياناتها إذا تعرضت المؤسسة للجرائم الإلكترونية.

أكثر الجرائم الإلكترونية التي تحدث في المؤسسات الصحفية

الجرائم الإلكترونية التي تتعرض لها المؤسسات الصحفية	ك	%
انتحال شخصية الصحفيين على مواقع التواصل الاجتماعي	١٦٤	%٧٢.٩
التصيد والخداع للحصول على معلومات وبيانات وصور	١٤٥	%٦٤.٤
الابتزاز الإلكتروني والتهديد والتخويف بنشر الفضائح	١٥٢	%٦٧.٦
سرقة الموضوعات الصحفية ونشرها على مواقع أخرى	٢٢٠	%٩٧.٨
التلاعب بالمحتوى والمعلومات والأرقام والصور المضللة	١٣٨	%٦١.٣
نشر الفيروسات وتدمير البيانات على الأجهزة	١٠٣	%٤٥.٧
اختراق المواقع الإخبارية لنشر الشائعات والأخبار الزائفة	٢٠٧	%٩٢
اختراق حسابات الصحفيين على مواقع الإنترنت	٢٠٤	%٩٠.٧
التجسس والتنصت ومراقبة المكالمات الهاتفية	١٦٧	%٧٤.٢
انتهاك خصوصية الصحفيين وتعرضهم للسب والتشهير	١٨٨	%٨٣.٦

يوضح هذا الجدول الجرائم الإلكترونية التي يقع فيها الصحفيين ضحايا لها، والتي تهدد المؤسسات الصحفية، فقد جاءت أكثر الجرائم انتشارا في العمل الصحفي هي (سرقة الموضوعات والتحقيقات الصحفية ونشرها على مواقع أخرى بنسبة ٩٧.٨%، اختراق المواقع الإخبارية لنشر الشائعات والأخبار الزائفة بنسبة ٩٢%، اختراق حسابات الصحفيين على مواقع الإنترنت بنسبة ٩٠.٧%)

بعد ذلك جاءت الجرائم متوسطة الانتشار بين الصحفيين هي (التجسس والتنصت ومراقبة المكالمات الهاتفية وسرقة المحادثات الإلكترونية بنسبة

٧٤.٢%، انتحال شخصية الصحفيين على مواقع التواصل الاجتماعي بنسبة ٧٢.٩%، الابتزاز الإلكتروني والتهديد والتخويف بنشر الفضائح بنسبة ٦٧.٦%، التصيد والخداع للحصول على معلومات وبيانات وصور بنسبة ٦٤.٤%،التلاعب بالمحتوى والمعلومات والأرقام والصور المضللة بنسبة ٦١.٣%)

ومن السابق نلاحظ أن الجرائم الإلكترونية لا تهدد الصحفيين فقط، بل يتعرض الصحفيين لجرائم تضر بالاتي (جرائم تضر بالأجهزة كالحاسوب والهواتف الذكية، جرائم تضر بالبيانات والمعلومات، جرائم تضر بالخصوصية الشخصية للصحفيين، جرائم تضر بشبكة الانترنت)، لذا يجب على الصحفيين الاهتمام بالأمن الإلكتروني بكافة مكوناته سواء كان أمن المعلومات، أو أمن الشبكات، أو أمن التطبيقات، أو أمن الأجهزة التكنولوجية، وتأتي أسباب تعرض الصحفيين لمثل هذه الجرائم، عدم وجود وعي كافي لدى الصحفيين لصد الجرائم الإلكترونية، وإهمال تثبيت أدوات لضمان الأمان من تلك الجرائم على الأجهزة، وضعف تطبيق التشريعات الإلكترونية وجهل الأفراد بها، واستخدام نظم تشغيل وبرامج غير أصلية، وعدم اهتمام المؤسسة بتوعية وتدريب الأفراد بمسائل الأمن الإلكتروني، وعدم وجود سياسة أمنية تضمن حماية المؤسسة وأجهزتها وشبكاتها وافرادها من مخاطر التهديدات الرقمية.

حجم تأثير الجرائم الإلكترونية على المهام الصحفية اليومية

حجم التأثير	ك	%
تتأثر بشكل كبير	١٣٦	٦٠.٤٤%
تتأثر شكل ضعيف	٦١	٢٧.١١%
لا تتأثر	٢٨	١٢.٤٤%
الإجمالي	٢٢٥	١٠٠%

يهدف هذا الجدول لمعرفة حجم التأثير الذي يمكن أن تسببها الجرائم الإلكترونية مثل (انتهاك خصوصيتهم، والتجسس والتنصت، والتصيد والابتزاز الإلكتروني، وتهديدهم، وقرصنة أجهزتهم واختراق حساباتهم على الإنترنت ...إلخ) على المهام والممارسات الصحفية التي يقوم بها الصحفي، فقد ذكر عدد كبير من أفراد العينة ما نسبته ٦٠.٤% من الصحفيين أن المهام تتأثر بشكل كبير

بالجرائم الإلكترونية، وذكر نسبة ٢٧.١% من الصحفيين أن مهامهم تتأثر بشكل ضعيف، وأخيراً أكد عدد قليل من الصحفيين نسبتهم ١٢.٤% أن مهامهم لا تتأثر بالجرائم الإلكترونية.

وهذا بسبب أن تلك الجرائم تؤثر على جميع مراحل العمل الصحفي، وكذلك أصبحت مراحل العمل الصحفي تتم في بيئة رقمية، تعتمد على تكنولوجيا الاتصال والمعلومات، ونرى أن تلك التقنيات التكنولوجية عرضة للاختراق والقرصنة وإصابتها بالفيروسات، وأيضا عرضة للمراقبة والتجسس، لذلك يرى هؤلاء الصحفيين أنهم لا يستطيعون الاستغناء عن التقنيات الحديثة سواء في عملية جمع المعلومات من الميدان والمصادر، أو عملية تحرير الموضوعات ومعالجة الصور والفيديوهات، أو عملية النشر الصحفي للموضوعات على الإنترنت ومواقع التواصل الاجتماعي، ففي جميع هذه المراحل يعتمد الصحفي على الكمبيوتر ونظم التشغيل والبرامج، والهاتف الذكي، والإنترنت وخدماته من بريد إلكتروني وتخزين سحابي ومواقع التواصل الاجتماعي بشكل كبير وواسع، وهنا نرى أن الجرائم الإلكترونية تؤثر بشكل كبير على الأداء المهني للصحفيين.

مقترحات الصحفيين لمكافحة الجرائم الإلكترونية

مقترحات الصحفيين لمكافحة الجرائم الإلكترونية	ك	%
باستخدام برامج مكافحة الفيروسات وجدران الحماية والبرامج الأصلية وسد الثغرات	53	٢٣.٥%
عدم إفشاء كلمة المرور والحفاظ على سرية الصور والبيانات، وعدم الوثوق بأي شخص مجهول	15	١١.١%
التدريب والتأهيل بتكثيف الدورات التدريبية	90	٤٠%

أن تكون ضمن أولويات الجاهات المختصة كالدولة والجهات الأمنية والمؤسسات المعنية بتوفير الأمن الإلكتروني	11	٤.٨%
ضرورة سن تشريعات وقوانين للحد من الجرائم الإلكترونية وردع المجرمين	46	٢٠.٤%
أن توفر المؤسسة الصحفية بيئة تحتية تكنولوجية آمنة تضمن حمايتها	30	١٣.٣%
توفير خبير تكنولوجي بكل مؤسسة، ورسم سياسات وإجراءات آمنة بالمؤسسة	43	١٩.١%
زيادة الوعي بأهمية تعلم إجراءات الأمن الإلكتروني وصد الجرائم الإلكترونية	47	٢٠.٨%
توفير مستوى عالي من الأمان والحماية عند استخدام الأجهزة والبرامج ونظم التشغيل وشبكة الإنترنت	14	١٧.٣%
عدم فتح الروابط مجهولة المصدر من الرسائل أو المواقع	15	٦.٦%
سرعة إبلاغ المختص التكنولوجي، أو المؤسسة، أو النقابة، أو الجهات الأمنية عند التعرض للجرائم الإلكترونية لمعالجة مخاطرها	9	٤%

يقدم هذا الجدول مقترحات الصحفيين لزيادة وعيهم بمسائل الأمن الإلكتروني، ومكافحة الجرائم الإلكترونية، حيث قدموا مجموعة حلول لحماية أنفسهم تتمثل في التالي:

جاء أكبر سبب منفرداً بنسبة كبيرة تم الاتفاق عليه بين الصحفيين بأن أهم مقترح لزيادة وعي الأمن الإلكتروني، ومكافحة الجرائم الإلكترونية هي (التدريب والتأهيل بتكثيف الدورات التدريبية بنسبة ٤٠%)

وبعد ذلك طرح الصحفيون مجموعة مقترحات جاءت بمستوى متوسط الانتشار بين الصحفيين تتمثل في التالي: (باستخدام برامج مكافحة الفيروسات وجدران الحماية والبرامج الأصلية وسد الثغرات بنسبة ٢٣.٥%، زيادة الوعي بأهمية تعلم إجراءات الأمن الإلكتروني وصد الجرائم الإلكترونية بنسبة ٢٠.٨%، وضرورة سن تشريعات وقوانين للحد من الجرائم الإلكترونية وردع المجرمين بنسبة ٢٠.٤%، وتوفير خبير تكنولوجي بكل مؤسسة، ورسم سياسات وإجراءات آمنة بالمؤسسة بنسبة ١٩.١%، وتوفير مستوى عالي من الأمان والحماية عند استخدام الأجهزة والبرامج ونظم التشغيل وشبكة الإنترنت بنسبة

١٧.٣%)

وجاءت أقل المقترحات التي قدمها الصحفيون لزيادة الوعي بالأمن الإلكتروني هي (أن توفر المؤسسة الصحفية بيئة تحتية تكنولوجية آمنة تضمن حمايتها ١٣.٣%، وعدم إفشاء كلمة المرور والحفاظ على سرية الصور والبيانات، وعدم الوثوق بأي شخص مجهول بنسبة ١١.١%، وعدم فتح الروابط مجهولة المصدر من الرسائل أو المواقع بنسبة ٦.٦%، وأن تكون ضمن أولويات الجاهات المختصة كالدولة والجهات الأمنية والمؤسسات المعنية بتوفير الأمن الإلكتروني بنسبة ٤,٨%، وسرعة إبلاغ المختص التكنولوجي، أو المؤسسة، أو النقابة، أو الجهات الأمنية عند التعرض للجرائم الإلكترونية لمعالجة مخاطرها بنسبة ٤%)

وتؤكد دراستنا أن وجود خبير تكنولوجي، ووحدة معلوماتية تقنية بكل مؤسسة أمر ضروري وهام جدا، لأن هذه الوحدة تمتلك فريق تقني ذو مهارة تكنولوجية مرتفعة، يستطيع تأمين كافة الأجهزة التي تستخدمها المؤسسة وكذا تأمين شبكة الإنترنت، وسد أي ثغرات بالمؤسسة، تمكن المجرمين من شن هجوم رقمي عليها، وكذا سيتمكن هذا الفريق من زيادة تأمين أجهزة الصحفيين أنفسهم، ومعالجة أي هجوم قد أصابهم، والعمل على التقليل من مخاطر الجرائم الإلكترونية، فالمؤسسة يجب أن تولي اهتمام كبير بهذا المجال، ومحاولة فرضه على جميع العاملين بها، لأن اختراق صحفي واحد يمكن أن يسبب اختراق لكافة المؤسسة ككل، وأيضا ضرورة تشجيع الصحفيين على الاهتمام بهذا المجال، ويجب أيضا أن توفر المؤسسة الصحفية بنية تكنولوجية تحتية آمنة تضمن حماية الآخرين، وأن تقوم بتحديثها باستمرار.

وإذا كان لمؤسسات الدولة والمؤسسات الصحفية دور بالغ الأهمية في الحد من الجرائم الإلكترونية، فللصحفي نفسه دور أكثر أهمية في حماية نفسه وحماية المؤسسة الصحفية، فيجب على الصحفيين عدم إفشاء كلمات المرور، وتثبيت برامج مكافحة الفيروسات، وعدم فتح الروابط المجهولة المصدر، وعدم إفشاء أي بيانات وصور ومعلومات سرية، واستخدام التصفح الخفي، والتقليل من إذونات التطبيقات غير الموثوقة المصدر على الهاتف الذكي

النتائج العامة للدراسة:

١- ذكر الصحفيين محل الدراسة أن نسبة ٦٥% منهم قد تعرضوا للجرائم الإلكترونية من قبل، وأجابوا بأن أكثر الجرائم الإلكترونية التي تحدث

للمؤسسات الصحفي هي (سرقة الموضوعات والتحقيقات الصحفية ونشرها على مواقع أخرى، اختراق المواقع الإخبارية لنشر الشائعات والأخبار الزائفة ، اختراق حسابات الصحفيين الإنترنت).

٢- أثبتت نتائج الدراسة هناك أسباب تجعل الصحفي يقع ضحية للجرائم الإلكترونية، مما يترتب عليه تأثيرات سلبية على ممارساتهم الصحفية، فقد ذكر ٦٠% من الصحفيين عينة الدراسة أن الجرائم الإلكترونية تؤثر على المهام الصحفية اليومية بشكل كبير، ومن أكثر أسباب وقوع الصحفيين ضحية للجرائم الإلكترونية هي ضعف الوعي والمعرفة بأبعاد الجريمة الإلكترونية، وإهمال مكافحتها.

٣- وأوضحت نتائج الدراسة بأن هناك مقترحات لمكافحة الجرائم الإلكترونية، وقدم الصحفيين مجموعة حلول لحماية أنفسهم تتمثل في التالي: (التدريب والتأهيل بتكثيف الدورات التدريبية، واستخدام برامج مكافحة الفيروسات وجدران الحماية والبرامج الأصلية لسد الثغرات، وتوفير خبير تكنولوجي بكل مؤسسة، ورسم سياسات وإجراءات تضمن وجود بيئة تكنولوجية آمنة بالمؤسسة الصحفية، وعدم إفشاء كلمات المرور والحفاظ على سرية الصور والبيانات، وعدم الوثوق بأي شخص مجهول على الإنترنت، وعدم فتح الروابط مجهولة المصدر من الرسائل أو المواقع، وسرعة إبلاغ المختص التكنولوجي، أو المؤسسة، أو النقابة، أو الجهات الأمنية عند التعرض للجرائم الإلكترونية لمعالجة مخاطرها).

التوصيات:

- توصي الدراسة بضرورة اهتمام الصحفيين بالأمن الإلكتروني وتوظيفه في الوقاية من مخاطر الجرائم الإلكترونية على حياتهم الشخصية والمهنية، وذلك من خلال أخذ دورات تدريبية مستمرة في مجال التكنولوجيا والأمن الإلكتروني.

- ضرورة أن توفر المؤسسة الصحفية بنية تحتية تكنولوجية آمنة متحدثة باستمرار، ووحدة تضم عدد من خبراء الأمن الإلكتروني يكون مهمتهم الحفاظ الدائم على أمن الصحفيين والمؤسسة.

- ضرورة أن تضع نقابة الصحفيين الأمن الإلكتروني ضمن معايير إنشاء الصحف، والتحاق الصحفيين بها، وأن تنشئ خط ساخن لدعم الصحفيين للإبلاغ

عن الهجمات والتهديدات التي تسببها الجرائم الإلكترونية، وضرورة وضع سياسات إلزامية قانونية على الصحفيين لحماية أنفسهم وسلامتهم الرقمية.

- ضرورة سن قوانين صارمة ورادعة لحماية حقوق الملكية الفكرية الإعلامية وحماية خصوصية الصحفيين الرقمية، وردع أي مجرم يخترق القانون، وذلك من خلال قوانين أكثر تفصيلاً ووضوحاً ينظم العمل الإعلامي.

مراجع الدراسة:

الكتب:

- الجهيني، منير محمد. وآخرون.(٢٠٠٤).جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها.د-ط. الإسكندرية:دار الفكر الجامعي.
- العوادي، أوس نجيب غالب.(٢٠١٦).الأمن المعلوماتي السيبراني.بغداد:سلسلة إصدارات مركز البيان للدراسات والتخطيط.
- عرب، يونس.(٢٠٠١).جرائم الكمبيوتر والإنترنت.بيروت: اتحاد المصارف العربية.

الدراسات:

- فاريش، رشيدة. ونوره قاوش.(٢٠١٨).تأثير مواقع التواصل الاجتماعي في انتشار الجريمة الإلكترونية في وسط المراهقين- دراسة ميدانية.رسالة ماجستير غير منشورة، قسم العلوم الإنسانية، تخصص الاتصال، كلية العلوم الإنسانية والاجتماعية، جامعة اكلي منحد والحاج البويرة.

المجلات:

- أحمد، وسام محمد.(٢٠٢٠).إدراك الصحفيين للمخاطر الرقمية وإستراتيجيات تطبيقهم للأمن الرقمي في عملهم المهني.المجلة العربية لبحوث الإعلام والاتصال، العدد ٣١، أكتوبر/ديسمبر، ص٤٥٠:ص٥٤٧
- الأزرق، نرمين نبيل.(٢٠٢٠).التهديدات الرقمية ضد الصحفيين المصريين ووعيهم بالآليات المستخدمة للحفاظ على سلامتهم-دراسة كيفية.مجلة البحوث الإعلامية، جامعة الأزهر، العدد ٥٤، الجزء ٦،يوليو،ص٤٢٩٩:ص٤٣٣٨.
- العشري، وائل.(٢٠٢٠).رؤية الصحفيين المصريين للضوابط المهنية والأخلاقية المنظمة لاستخدامات شبكات التواصل الاجتماعي في العمل الصحفي

وعلاقتها بأساليب الممارسة السائدة. المجلة العربية لبحوث الإعلام والاتصال، جامعة الأهرام الكندية، العدد ٢٨، ص ٨٦-٢٠٥.
- المنتشري، فاطمة يوسف.(٢٠٢٠).دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للعلوم التربوية والنفسية، السعودية، المجلد ٤، العدد ١٧، يوليو، ص. ٤٥٧-٤٨٤.
- حسنية، أحمد أسامة.(٢٠١٧).الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية. مجلة جامعة الأزهر، عدد خاص بمؤتمر كلية الحقوق الخامس المحَّكم، غزة، المجلد ٩١، ص١-٤١.
- رشاد، إسراء جميل.(٢٠١٨).الجرائم الإلكترونية (الأهداف – الأسباب - طرق الجريمة والمعالجة).مجلة الدراسات الاعلامية، المركز الديمقراطي العربي، العدد ١، يناير، ص٤٢٠-٤٥٤.
- شليبة، مقدم.(٢٠١٩).تأثير الجريمة الإلكترونية على المعلومات الرقمية.المجلة الجزائرية للأبحاث والدراسات، جامعة عبدالحميد مهري قسنطينة، المجلد ٣،العدد٩، ديسمبر،ص ١٣٧-١٥٩.
- صائغ، وفاء بنت حسن.(٢٠١٨). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية.المجلة العربية للعلوم الاجتماعية،المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية،المجلد٣، العدد ١٤، يوليو، ص، ٧٠:١٨.
- غريب، ماجده.(٢٠١٧).مدي الوعي لدى الفئة العمرية الشابة بنظام عقوبات الجرائم المعلوماتية السعودي. المجلة العربية الدولية للمعلوماتية، جامعة نايف العربية للعلوم الأمنية، السعودية، المجلد ٥، العدد ٩،ص١٧-٣٢.
المؤتمرات:
- خبازي، فاطمة الزهرة.(٢٠١٧).جرائم الدفع الإلكتروني وسبل مكافحتها.أعمال الملتقي الوطني: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر، ٢٩ مارس.

المراجع الأجنبية:

الكتب:

-Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2019). Building digital safety for journalism: A survey of selected issues. UNESCO Publishing.

المجلات:

-Maghu, S., Sehra, S., & Bhardawaj, A. (2014). Inside of cyber crimes and information security: Threats and solutions. International journal of information & computation technology, vol.4 (.8), 835-840

-Tsui, L., & Lee, F. (2021). How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. Journalism, 22(6), 1317-1339 .

-Christofoletti, R., & Torres, R. J. (2018). Journalists exposed and vulnerable: digital attacks as a form of professional risk/Jornalistas expostos e vulneraveis: ataques digitais como modalidade de risco profissional. Revista Famecos-Midia, Cultura e Tecnologia, 25(3), NA-NA .