مجلة البحوث الإعلامية

مجلة علمية محكمة تصدر عن جامعة الأزهر/كلية الإعلام

رئيس مجلس الإدارة: أ. د/ غانم السعيد - عميد الكلية.

رئيس التحرير: أ. د/ رضا عبدالواجد أمين - أستاذ الصحافة والنشر ووكيل الكلية.

مساعدو رئيس التحرير:

- أ. د/ عرفه عامر - الأستاذ بقسم الإذاعة والتليفزيون بالكلية
- أ. د/ فهد العسكر - وكيل جامعة الإمام محمد بن سعود للدراسات العليا والبحث العلمي (المملكة العربية السعودية)
- أ. د/ عبد الله الكندي - أستاذ الصحافة بجامعة السلطان قابوس (سلطنة عمان)
- أ. د/ جلال الدين الشيخ زيادة - عميد كلية الإعلام بالجامعة الإسلامية بأم درمان (جمهورية السودان)

مدير التحرير: د/ محمد فؤاد الدهراوي - مدرس العلاقات العامة والإعلان، ومدير وحدة الجودة بالكلية

سكرتيرو التحرير: د/ إبراهيم بسيونى - مدرس بقسم الصحافة والنشر بالكلية.
د/ مصطفى عبد الحى - مدرس بقسم الصحافة والنشر بالكلية.
د/ رامى جمال مهدي - مدرس بقسم الصحافة والنشر بالكلية.

مدقق اللغة العربية: أ/ عمر غنيم - مدرس مساعد بقسم الصحافة والنشر بالكلية.

سكرتير فني: أ/ محمد كامل - مدرس مساعد بقسم الصحافة والنشر بالكلية.

المراسلات:

- القاهرة- مدينة نصر - جامعة الأزهر - كلية الإعلام - ت: ٠٢٢٥١٠٨٢٥٦
- الموقع الإلكتروني للمجلة: http://jsb.journals.ekb.eg
- البريد الإلكتروني: mediajournal2020@azhar.edu.eg

- العدد السادس والخمسون - الجزء الثالث - جمادى الأول ١٤٤٢هـ - يناير ٢٠٢١ م
- رقم الإيداع بدار الكتب المصرية ٦٥٥٥
- الترقيم الدولي للنسخة الإلكترونية: ٢٦٨٢-٢٩٢ x
- الترقيم الدولي للنسخة الورقية: ٩٢٩٧-١١١٠

الهيئة الاستشارية للمجلة

١. أ.د/ على عجوة (مصر)

أستاذ العلاقات العامة وعميد كلية الإعلام الأسبق بجامعة القاهرة.

٢. أ.د/ محمد معوض. (مصر)

أستاذ الإذاعة والتليفزيون بجامعة عين شمس.

٣. أ.د/ حسين أمين (مصر)

أستاذ الصحافة والإعلام بالجامعة الأمريكية بالقاهرة.

٤. أ.د/ جمال النجار (مصر)

أستاذ الصحافة بجامعة الأزهر.

٥. أ.د/ مي العبدالله (لبنان)

أستاذ الإعلام بالجامعة اللبنانية، بيروت.

٦. أ.د/ وديع العزعزي (اليمن)

أستاذ الإذاعة والتليفزيون بجامعة أم القرى، مكة المكرمة.

٧. أ.د/ العربي بوعمامة (الجزائر)

أستاذ الإعلام بجامعة عبدالحميد، بجامعة عبد الحميد بن باديس بمستغانم، الجزائر.

٨. أ.د/ سامي الشريف (مصر)

أستاذ الإذاعة والتليفزيون وعميد كلية الإعلام، الجامعة الحديثة للتكنولوجيا والمعلومات.

٩. أ.د/ خالد صلاح الدين (مصر)

أستاذ الإذاعة والتليفزيون بكلية الإعلام -جامعة القاهرة.

١٠. أ.د/ محمد فياض (العراق)

أستاذ الإعلام بكلية الإمارات للتكنولوجيا.

١١. أ.د/ رزق سعد (مصر)

أستاذ العلاقات العامة (جامعة مصر الدولية).

قواعد النشر

تقوم المجلة بنشر البحوث والدراسات ومراجعات الكتب والتقارير والترجمات وفقًا للقواعد الآتية:

- **يعتمد النشر على رأي اثنين من المحكمين المتخصصين في تحديد صلاحية المادة للنشر.**
- **ألا يكون البحث قد سبق نشره في أي مجلة علمية محكمة أو مؤتمرًا علميًا.**
- **لا يقل البحث عن خمسة آلاف كلمة ولا يزيد عن عشرة آلاف كلمة ... وفي حالة الزيادة يتحمل الباحث فروق تكلفة النشر.**
- **يجب ألا يزيد عنوان البحث -الرئيسي والفرعي- عن ٢٠ كلمة.**
- **يرسل مع كل بحث ملخص باللغة العربية وآخر باللغة الانجليزية لا يزيد عن ٢٥٠ كلمة.**
- **يزود الباحث المجلة بثلاث نسخ من البحث مطبوعة بالكمبيوتر .. ونسخة على CD، على أن يكتب اسم الباحث وعنوان بحثه على غلاف مستقل ويشار إلى المراجع والهوامش في المتن بأرقام وترد قائمتها في نهاية البحث لا في أسفل الصفحة.**
- **لا ترد الأبحاث المنشورة إلى أصحابها .... وتحتفظ المجلة بكافة حقوق النشر، ويلزم الحصول على موافقة كتابية قبل إعادة نشر مادة نشرت فيها.**
- **تنشر الأبحاث بأسبقية قبولها للنشر .**
- **ترد الأبحاث التي لا تقبل النشر لأصحابها.**

محتويات العدد

- توظيف التسويق الحسي كأداة لتحفيز السلوك الشرائي وعلاقته بالولاء للعلامة التجارية - دراسة ميدانية على عملاء مطاعم الوجبات السريعة العالمية في مصر — أ.م.د. أماني ألبرت — ٩٧٥

- محددات المسئولية الجنائية لجرائم الاختراق والاعتراض والانتحال وآليات الضبط والردع في التشريعات العربية في العصر الرقمي: دراسة تحليلية مقارنة — أ.م.د. نرمين نبيل الأزرق — ١٠٤١

- اتصالات إدارة الأزمات وعلاقتها بالثقة التنظيمية للعاملين وسلوكياتهم للمواطنة التنظيمية - دراسة على عينة من الشركات الخاصة العائلية العاملة في مصر — أ.م.د. ريم أحمد عادل — ١٠٨١

- اتجاهات النخبة نحو دور المتحدث الرسمي لوزارة الصحة والسكان في إدارة أزمة كورونا: دراسة ميدانية — أ.م.د. مروى السعيد السيد — ١١٤٩

- مخاطر «الفبركة الرقمية» في الإعلام الجديد جائحة كورونا عبر وسائل التواصل الاجتماعي «نموذجًا» — د. استقلال دليل محمد العازمي — ١٢٠٧

- التعرض للمواقع الإلكترونية الإخبارية وعلاقته بحالة المزاج العام لدى الشباب الجامعي البحريني (دراسة حالة على خطة السلام الأمريكية) — د. محمد مصطفى رفعت محرم — ١٢٣١

- اتجاهات مستخدمي مواقع التواصل الاجتماعي نحو جائحة كورونا (كوفيد- 19): تحليل من المستوى الثاني لدراسات مدخل معالجة اللغة الطبيعية — د. ريهام سامي — ١٢٧٧

سمات خطاب تعليقات مستخدمي صفحات وزارة التربية والتعليم المصرية عبر مواقع التواصل الاجتماعي إزاء نظام التعليم عن بُعد
د. هبة مصطفى حسن مصطفى
١٣١٩

اعتماد طلاب أقسام الإعلام التربوي على صحافة الهاتف المحمول كمصدر للأخبار (دراسة ميدانية)
د. إيناس منصور كامل شرف
١٣٦١

دور صحافة الموبايل في تشكيل اتجاهات الجمهور المصري نحو الأحداث الجارية «دراسة ميدانية»
راشد صلاح الدين راشد
١٤١٩

م	القطاع	اسم المجلة	اسم الجهه / الجامعة	نقاط المجلة (مارس 2020)	نقاط المجلة (يوليو 2020)	ISSN-P	ISSN-O
1	الدراسات الإعلامية	مجلة البحوث الإعلامية	جامعة الأزهر	6.5	7	1110-9297	2682-292X
2	الدراسات الإعلامية	مجلة بحوث العلاقات العامة الشرق الأوسط	الجمعية المصرية للعلاقات العامة	6	7	2314-8721	2314-873X
3	الدراسات الإعلامية	المجلة العربية لبحوث الإعلام و الإتصال	جامعة الأهرام الكندية	5	5	2536-9393	
4	الدراسات الإعلامية	مجلة إتحاد الجامعات العربية لبحوث الإعلام و تكنولوجيا الإتصال	Cairo University	4	4	2356-9891	
5	الدراسات الإعلامية	المجلة العلمية لبحوث الإعلام و تكنولوجيا الإتصال	جامعة جنوب الوادى	3.5	3.5	2536-9237	
6	الدراسات الإعلامية	مجلة البحوث و الدراسات الإعلامية	اكاديمية الشروق	3.5	5.5	2357-0407	
7	الدراسات الإعلامية	المجلة العلمية لبحوث العلاقات العامة والإعلان	جامعة القاهرة – مركز بحوث الرأى العام	3	5.5	2356-9131	
8	الدراسات الإعلامية	المجلة العلمية لبحوث الإذاعة والتلفزيون	جامعة القاهرة – مركز بحوث الرأى العام	3	5.5	2356-914X	
9	الدراسات الإعلامية	المجلة العلمية لبحوث الصحافة	جامعة القاهرة – مركز بحوث الرأى العام	3	5.5	2356-9158	
10	الدراسات الإعلامية	المجلة المصرية لبحوث الإعلام	جامعة القاهرة – مركز بحوث الرأى العام	3	5.5	1110-5836	
11	الدراسات الإعلامية	المجلة المصرية لبحوث الرأى العام	Cairo University, Center of Public Opinion Research	3	6.5	1110-5844	

- يطبق تقييم مارس 2020 للمجلات على كل الأبحاث التى نشرت فيها قبل 1 يوليو 2020
- يطبق تقييم يوليو 2020 للمجلات على كل الأبحاث التى ستنشر فيها بدء من 1 يوليو 2020 و حتى صدور تقييم جديد في يوليو 2021
- المجلات التي لم تتقدم بطلب إعادة تقييم سيظل تقييم مارس ٢٠٢٠ مطبقا على كل الأبحاث التي ستنشر بها وذلك لحين صدور تقييم جديد في يوليو 2021
- يتم إعادة تقييم المجلات المحلية المصرية دورياً في شهر يوليو من كل عام ويكون التقييم الجديد سارياً للسنة التالية للنشر في هذه المجلات

حقوق الملكية الفكرية © 2020 محفوظة لوحدة نظم المعلومات الادارية ودعم اتخاذ القرار بمركز الخدمات الالكترونية والمعرفية -المجلس الأعلى للجامعات

محددات المسئولية الجنائية لجرائم الاختراق والاعتراض والانتحال وآليات الضبط والردع في التشريعات العربية في العصر الرقمي: دراسة تحليلية مقارنة

Criminal liability determinants of hacking, interception & plagiarism and ways of regulation and deterrence in Arab legislations in the digital age: Analytical comparative study

أ.م.د. نرمين نبيل الأزرق

أستاذ مساعد، كلية الإعلام، جامعة القاهرة

nermeenalazrak@hotmail.com

ملخص الدراسة

تتحدد مشكلة الدراسة في رصد وتوصيف محددات المسئولية الجنائية لجرائم الاختراق والاعتراض والانتحال وتحليلها كما وردت بالنصوص التشريعية في البلاد العربية، وكيفية مواجهة القوانين لتلك الجرائم، وتقييم الأطر التشريعية الضابطة في الدول العربية والمقارنة بينها من حيث شمول النصوص ووضوحها وآليات الردع ونوعية العقوبة، وما إذا كانت التشريعات تضع ظروفًا استثنائية، وماهية أوجه الشبه والاختلاف بين البلاد العربية محل الدراسة (مصر والإمارات والسودان والأردن) في هذه الأمور القانونية، وتأتي نظرية الردع Deterrence theory في هذا الإطار المتصل بمكافحة التهديدات والأفعال الإجرامية المختلفة ومنها الجرائم الإلكترونية بمعطياتها لتوضح كيف يكون القانون عاملًا مهمًا لمواجهة الجريمة وتحقيق الردع.

تعتمد الدراسة على المنهج الوصفي التحليلي، وكذا المنهج الاستقرائي، وتم استخدام أداة تحليل النصوص القانونية، كما اعتمت الدراسة أسلوب المقارنة المنهجية للمقارنة بين تلك النصوص القانونية في تشريعات الدول العربية محل الدراسة، ومن أهم النتائج: تميز القانون المصري بتوضيح حالات ارتكاب الجريمة الإلكترونية التي يترتب عليها المسئولية الجنائية لفاعلها بشكل أكبر من القوانين الأخرى، وبشكل عام فلقد خرجت التشريعات العربية محل الدراسة الخاصة بمكافحة جرائم تقنية المعلومات من عباءة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وجاءت نصوصها القانونية لتتسق إلى حد كبير مع أهداف هذه الاتفاقية، ويتضح من مجمل نتائج هذه الدراسة أن هناك توجهًا قويًا بالتشريعات العربية– محل الدراسة– بشكل عام لمكافحة الجرائم الإلكترونية ومنها جرائم الاختراق والاعتراض والانتحال بفعالية.

الكلمات المفتاحية: التشريعات العربية – الاختراق – الانتحال – الاعتراض – العصر الرقمي.

Abstract

The study aims at describing and analyzing the criminal liability determinants of hacking, interception & plagiarism as real dangerous crimes of cybercrimes. The study also seeks to analyze ways of regulation and deterrence in Arab legislations in the digital age. Regarding the deterrence theory and using document analysis method according to the methodology of legal research, the study compares the legislations in Egypt, Jordan, Sudan and United Arab Emirates, mainly focusing on specific laws for combating cybercrimes in these countries. The results revealed that there are differences in determining the criminal liability between the legislations in the four countries. The results demonstrated the efficiency in the Egyptian legal articles for combating cybercrimes (Hacking, interception & plagiarism) and clarifying some problematic issues related to such articles in the four countries. The results in general revealed that the articles under scrutiny attain the deterrence for such crimes.

Key words: Arab legislations– Hacking– Interception– plagiarism– digital age.

مقدمة:

في ظل الانتقال المتسارع لاستخدام تقنيات المعلومات والاتصالات والتحولات التكنولوجية المتعاظمة التي نشهدها يومًا بعد يوم، وتزايد أعداد مستخدمي الإنترنت ومواقع التواصل الاجتماعي، تسعى كافة الدول إلى العمل على صياغة أطر تشريعية متطورة لتواكب هذه التقنيات وإمكاناتها، ولتضبط استخدامات هذه التقنيات بحيث تدعم الحقوق والاستخدامات الإيجابية، وتواجه كافة أنواع التجاوزات والجرائم والتهديدات التي تنجم عنها.

وتتعدد أشكال الاستخدامات غير المشروعة في هذا الإطار، ومنها: اختراق الحساب الخاص بالبريد الإلكترونى، والتجسس واختراق الحياة الشخصية، والإساءة لشخصيات عامة بدون وثائق ومستندات، واستغلال الصور بشكل غير مشروع، واستغلال أسماء بشكل غير مشروع، وتغيير بعض الحقائق والصور ونشر الأخبار الزائفة، وكذلك القذف والسبُّ عبر مواقع التواصل الاجتماعى، ووضع فيديوهات مشوهة أو مبتورة، وتبادل أشكال الإساءة بين الأفراد والأشخاص الاعتبارية باستغلال وسائل التواصل الاجتماعى، واستخدام شخص لبيانات ومعلومات شخص آخر واستغلالها بشكل غير قانوني كسرقة الهوية والانتحال.

وتتعدد التصنيفات التي يضعها الباحثون للجرائم الإلكترونية بحسب استخدامات الكمبيوتر والإنترنت فيها والنتائج المترتبة عليها [1]، والبعض يرى التصنيفات بحسب مجال الاختراق والاعتراض إما سياسي أو بنكي أو خاص بالأطفال أو بالهوية [2]، كما تتعدد التصنيفات التي يضعها المشرِّعون لتلك الأفعال أو التجاوزات التي تدخل في دائرة التجريم، والتي ترتكب بواسطة مستخدمي مواقع التواصل الاجتماعي سواء الأشخاص الطبيعية أو الاعتبارية، ومن هذه التجاوزات ما يصنف باعتباره من **جرائم العدوان على الاعتبار**، مثل القذف والسبِّ واقتحام الخصوصية، ومنها ما يصنف باعتباره من **الجرائم الماسَّة بالأمن العام** كجرائم التحريض والإرهاب وإثارة الرأي العام وإثارة

الفتن، وقد تأتي هذه الأفعال ضمن **جرائم الاعتداء على الآداب العامة** مثل نشر المضامين الإباحية والمخلة بالآداب العامة، وهناك العديد من الجرائم الأخرى التي يمكن أن تقع عن طريق مواقع التواصل الاجتماعى والتى تصنف تحت **جرائم الاختراق والاعتراض**، مثل الدخول بأى طريقة غير مشروعة إلى نظام معلوماتى أو حاسب آلي أو شبكة معلوماتية أو مشاهدة البيانات دون وجه حق لأغراض متعددة، منها: سرقة البيانات والمعلومات أو سرقة الهوية أو بغرض التنصت أو بغرض تغيير المعلومات المتبادلة.

والجريمة الإليكترونية Digital crime/ Cyber crime بشكل عام تتكون من نفس عناصر الجريمة العادية– الضحية والجاني والفعل الإجرامي-، ولكنها تتم في بيئة مختلفة إذ قد لا يكون الجاني في نفس مكان أو بلد وقوع الجريمة وما يتبعها من تداعيات؛ ومن ثم فهي جريمة عابرة للقارات، كما أن تلك الجريمة تتم بأساليب تقنية حديثة باستخدام وسائل الاتصال الحديثة والشبكة المعلوماتية.

ويمكن المقارنة بين بعض نماذج الجريمة التقليدية Real-life crime مع الجريمة الإلكترونية Virtual crime لتوضيح كيف انتقلت الجريمة من الواقع المادي إلى الواقع الافتراضي في العصر الرقمي، فالاحتيال في الجريمة التقليدية أصبح الاحتيال على الشبكة، وكذلك الاحتيال بالمزاد الإلكتروني، والسطو كجريمة تقليدية أصبح القرصنة على الإنترنت والحرمان من الخدمة ومهاجمة النظام بالفيروسات، وتحولت الجرائم الجنسية وجرائم الشذوذ في العصر الرقمي إلى استمالة الضحايا عبر الإنترنت واستغلالهم عبر المواقع الإباحية، كما أن غسيل الأموال تحول لأنظمة الدفع عبر شبكة الإنترنت، وتحولت السرقة في العصر الرقمي إلى جرائم الهوية وسرقة الملكية والابتزاز الإلكتروني.

وتعد جرائم الاعتراض والاختراق والانتحال من أكثر الجرائم التي يمكن أن تؤثر تأثيرًا سلبيًا على الأشخاص والبنية المؤسسية، وتهدد أمن وسلامة واستقرار الضحية سواء كانت شخصًا طبيعيًا أو اعتباريًا؛ فردًا أو مؤسسة أو دولة، حيث إن "الاعتراض" Illegal interception يمكِّن الجاني بشكل غير قانوني من مشاهدة البيانات أو المعلومات أو الحصول عليها لأغراض متعددة منها التنصت أو التخزين أو تغيير المحتوى أو تعديل المسار، و"الاختراق" hacking / trespassing يمكِّن الجاني من التعدي على خصوصية أي شبكة أو نظام والحصول على ما تحتويه من بيانات ومعلومات؛ مما يؤدي لخسائر وتداعيات فادحة قد يكون من بينها تدمير النظام نفسه، و"سرقة الهوية

والانتحال" Identity theft and fraud/piracy يجعل الجاني وكأنه الشخص أو المؤسسة ذاتها التي قام بالاستيلاء على اسمها، بكل ما يترتب على ذلك من تداعيات خطيرة تضر بمصالح الضحية والمتعاملين معها.

وهي جرائم مترتبة على بعضها البعض فجرائم اختراق المواقع أو النظام أو الحاسوب تعد من أهم أسباب سرقة الهوية والانتحال، كما أن جرائم الاعتراض أيضًا قد تنبني على جرائم الاختراق؛ بل إنها توصف بكونها جرائم مكملة complementary crime لجريمة الاختراق [3]، وقد تكون سببًا من أسباب إفشاء الهوية وتدمير النظام ومن ثم تسهل جرائم سرقة الهوية والانتحال والاحتيال.

وفي ضوء تزايد الاستخدامات غير المشروعة وتزايد جرائم الاختراق والاعتراض والانتحال بكل ما لها من تأثيرات سلبية ومسيئة، سواء على مستوى الأفراد أو المؤسسات والمجتمعات والدول أصبح من الأهمية أن يتم رصد وتوصيف محددات المسئولية الجنائية عن جرائم الاختراق والاعتراض والانتحال، وكيفية مكافحتها، وهي من أبرز جرائم العصر الرقمي كما وردت بالنصوص التشريعية في البلاد العربية وبخاصة أولى البلاد العربية التي أصدرت قوانين لمكافحة الجرائم الإلكترونية (الإمارات والسودان والأردن ثم مصر)، وصدَّقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

والبحث يهتم بكيفية مواجهة تلك الجرائم وتحقيق الردع من خلال تحليل ما هو منصوص عليه في التشريعات العربية المختلفة، وتقييم الأطر التشريعية الضابطة في الدول العربية، والمقارنة بينها من حيث شمول النصوص ووضوحها وآليات الردع ونوعية العقوبة، وما إذا كانت التشريعات تضع ظروفًا استثنائية لتشديد العقوبة، وماهية أوجه الشبه والاختلاف بين البلاد العربية في هذه الأمور القانونية.

وتأتي نظرية الردع Deterrence theory في هذا الإطار المتصل بمكافحة التهديدات والأفعال الإجرامية المختلفة ومنها الجرائم الإلكترونية بمعطياتها؛ لتوضح كيف يكون القانون عاملًا مهمًا لمواجهة الجريمة وتحقيق الردع، فوفقا للنظرية فإن الردع بالقانون والعقوبات التي يتضمنها يعد ضرورة وأساس لمكافحة الهجمات الالكترونية ومرتكبيها وذلك عبر خطوات تصاعدية لتتوافق مع طبيعة الفعل الإجرامي والآثار المترتبة عليه [4]، ويتسق ذلك مع علم العقاب الذي يوضح كيفية وضع تشريعات لنصوص عقابية وحدودها وآلية تنفيذها؛ حتى تتحقق أغراض العقوبة لتحقيق الردع والأمان والعدالة، وهذا دور السياسة الجنائية التي تحدد المسئولية الجنائية وتبحث في أغراض الجزاء الجنائي، وتحدد أفضل أساليب تنفيذ هذا الجزاء لتحقق أغراضه [5].

ولقد أسهم المفكر Cesar Beccaria وكذلك Jeremy Benthman في وضع جذور وأسس نظرية الردع [6]، وأوضح Beccaria أن العقاب ضرورة لمنع تكرار الجريمة مرة أخرى وردع من يفكر في القيام بالجريمة، وربط ذلك بالطبيعة البشرية التي ترفض الألم والعزلة، والنظرية تقوم على مقومات ثلاثة وهي: اليقين أو القناعة بالجريمة والسرعة والصرامة في مواجهتها، ومن ثم فالعقاب المناسب دون غلظة يمنع الجريمة ويردع من يفكر في ارتكابها [7]، ويرى كثير من الباحثين بناء على فكرة العقاب وربطها بنظرية الردع أن استراتيجيات الردع المكثفة تؤثر بالفعل على منع الجريمة إذا وضع القانون الملائم [8]، وتعتمد الرؤية البحثية في هذا البحث في تحليل وتفنيد النص القانوني، والمقارنة بين قوانين مكافحة جرائم الاختراق والاعتراض والانتحال في بعض نماذج من البلاد العربية على تقييم مدى التكامل والشمول وتحقق آلية الردع بالنص القانوني.

الدراسات السابقة:

وفي إطار العمل على توصيف وتحليل محددات المسئولية الجنائية للتجاوزات والاستخدامات غير المشروعة عبر مواقع التواصل الاجتماعي وجرائم الاختراق والاعتراض والانتحال وآليات مواجهتها في التشريعات العربية **يمكن أن تقسم البحوث والدراسات السابقة إلى محورين رئيسين في هذا الصدد:**

المحور الأول: "الدراسات التي تهتم برصد وتحليل الجريمة الإلكترونية بشكل عام أو ببحث عدد من التجاوزات والجرائم الإلكترونية معا من زوايا متعددة": ومن ذلك: دراسة رغدة البهي (2018) [9] **حول "الردع السيبراني المفهوم والإشكاليات والمتطلبات"** ولقد سعت الدراسة للإجابة على مدى ملائمة نظرية الردع لمواجهة الهجمات السيبرانية، وبحثت الدراسة آليات الردع وفوائدها وكيفية مواجهتها للجريمة الإلكترونية، وانتهت الدراسة إلى أنه ينبغي أن يطبق الردع نهج whole of government، وعليه يجب دمج كل عناصر السلطة الدبلوماسية والاقتصادية والاستخباراتية إلى جانب السلطة القانونية، خاصة وأن الباحثة ترى أن العالم سيشهد مزيدًا من الهجمات السيبرانية في الأعوام القادمة.

ودراسة سورية ديش (2018) [10] والتي تناولت **"أنواع الجرائم الإلكترونية وإجراءات مكافحتها"** بالجزائر بالتركيز على القانون الجزائري ودستور الجزائر، واعتمدت الدراسة على المنهج الوصفي؛ لتوصيف كافة أنواع الجرائم الإلكترونية والمنهج التحليلي؛ لتقييم الأساليب القانونية لمكافحة الجرائم الإلكترونية، وأظهرت الدراسة بعد مسح كافة النصوص القانونية بقانون الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أنه على الرغم

من وجود عدد من النصوص القانونية، فإنها ليست كافية؛ وذلك لعدة صعوبات، منها: أن رجال العدالة لم يتعودوا على مثل هذه الجرائم، أو بسبب عدم وجود دليل مادي يثبت الجريمة التقنية أحيانًا، أو بسبب عدم القدرة على ملاحقة الجناة للطبيعة الخاصة للجريمة الإلكترونية.

ودراسة إيناس محي الدين (2017) [11] **حول "حدود المسئولية المدنية عبر وسائل النشر الإلكتروني"**، واستهدفت الدراسة تحديد طبيعة نظام المسئولية المدنية الخاص بالنشر بواسطة وسائل النشر الإلكتروني، وتوضيح الأحكام العامة ونظام المسئولية المطبق على وسائل النشر المكتوبة، وبيان مدى انطباق هذه الأحكام على النشر بواسطة وسائل النشر الإلكتروني، وبتحليل ذلك انتهت الدراسة إلى أن نظام المسئولية المدنية للمواقع الإلكترونية الإعلامية يعتمد على القواعد التقليدية للمسئولية المدنية، وطالبت بوضع قانون خاص ينظم النشر الإلكتروني يواكب أحدث التطورات التقنية، وأن تكون الجرائم التي ينص عليها القانون محددة بشكل واضح وصريح ولا تحتمل التأويل، وأن تكون العقوبات مدنية وليست جنائية.

ودراسة دينا عبدالعزيز فهمي (2017) [12] **حول "المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي"**، والتي سعت من خلالها لبحث جرائم النشر الإلكتروني عبر مواقع التواصل الاجتماعي، وبالاعتماد على تحليل النصوص القانونية قامت الدراسة بالمقارنة بين المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي والعقوبات المرتبطة بها في كل من الإمارات والسعودية والكويت، وأوضحت نتائج الدراسة أن السعودية قد اهتمت بتطوير نصوص قانونية لتحقيق الردع لمرتكبي الجريمة الإلكترونية وأن الإمارات والكويت والاتفاقية العربية لمكافحة جرائم تقنية المعلومات نصوا على تجريم كثير من صور الدخول إلى موقع إلكتروني أو نظام معلومات إلكتروني، مع تشديد العقوبة في حالات متعددة.

ودراسة سعيد الحديدي (2017) [13] **بعنوان "تحديات التنظيم القانوني لحرية الاتصال بالإنترنت: دراسة مقارنة"**، والتي هدفت إلى رصد التحديات التي توجه المنظومة التشريعية نتيجة للعديد من الممارسات عبر الإنترنت التي أدت إلى تعارض العديد من المصالح المشروعة مثل مقتضيات حرية الاتصال والتعبير، وحماية المصلحة العامة، واحترام الحق في الخصوصية، بالشكل الذي عجزت معه القواعد القانونية التقليدية القائمة في التصدي لهذه الإشكاليات، وخلصت الدراسة إلى ضرورة إعادة النظر واستحداث قواعد قانونية جديدة تعمل على التوازن بين مقتضيات حرية الاتصال

والتعبير عبر الإنترنت ومن جهة أخرى احترام الحق في الخصوصية وحماية المصلحة العامة والنظام العام.

ودراسة Kimberly Pavlik (2017) [14] التي اهتمت ببحث **أثر الجرائم الإلكترونية على تطور التشريعات؟**، والتي قارنت بين تطور الجرائم الإلكترونية وتطور التشريعات لمواجهتها في الولايات المتحدة، ووجدت الدراسة أن القوانين فرضت غرامات مختلفة خاصة بالجريمة الإلكترونية، وأن هناك قوانين استحدثها الكونجرس بالفعل لمكافحة الجريمة الإلكترونية مثل كود 18 قسم 1030 وقانون التزوير والانتحال (CFAA).

ودراسة بوقرين عبد الحليم (2016) [15] التي استهدفت "**البحث عن المسئولية الجزائية عن الاستخدام غير القانوني لمواقع التواصل الاجتماعي في التشريعين الجزائري والإماراتي**"، وإلى أي مدى تقتصر المسئولية على أصحاب مواقع التواصل الاجتماعي أم أنها تتعدى ذلك إلى مقدمي خدمات الإنترنت؟ واستهدفت الكشف عن صور الاستخدام غير المشروع لمواقع التواصل الاجتماعي، والتكييف القانوني للاستخدامات غير المشروعة لمواقع التواصل الاجتماعي، واعتمدت على المنهج التحليلي لتحليل النصوص القانونية، والمنهج الوصفي لوصف الظاهرة وبيان أبعادها، وتوصلت إلى أن ما أورده المشرِّع الإماراتي يعتبر النص المناسب بالفعل للمعاقبة على انتهاك الخصوصية، ولم تجد الدراسة نصًّا خاصًّا للعقاب على السَّبِّ والقذف الذي يقع عبر وسائل التواصل الاجتماعي في التشريع الجزائري، بحيث تكون العقوبة أكثر من عقوبة السَّبِّ والقذف العادي، وهو ما اهتم به المشرِّع الإماراتي.

ودراسة كيانوين وانج (2016) Qianyun Wang [16] التي سعى من خلالها للمقارنة بين **عقوبة الجرائم الإلكترونية في القانون الجنائي لكلٍّ من الصين والمجلس الأوروبي والولايات المتحدة الأمريكية وإنجلترا وسنغافورة**، وتوصلت الدراسة لأهمية وجود قانون محدد خاص بتلك الجرائم في كل بلد، وأن أحد المشكلات المتصلة بتشريعات مكافحة الجريمة الإلكترونية هو تجددها وتطورها بشكل دائم ومتلاحق.

ودراسة ريجنر سابيلون وآخرين (2016) Regner Sabillon & others [17] والتي سعت لتفصيل **أركان الجريمة الإلكترونية وعناصرها وتفنيد أنواعها** بالاستناد لكافة الجرائم التي تتم في الواقع، ومستويات تنفيذها ومداها في التأثير، وتوصيف وتصنيف كل نوع ومستوى خاص بالجرائم الإلكترونية.

ودراسة عبدالله دغش العجمي (2014) [18] بشأن "**المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة**" التي اهتمت بالمقارنة بين قوانين مكافحة الجريمة الإلكترونية

بشكل عام في كل من (الأردن والكويت) سواء قوانين التنظيم أو العقوبات ومنها قانون جرائم أنظمة المعلومات 2010 بالأردن وقانون الشركات الجديد رقم 25 لسنة 2012 بالكويت، وبالاعتماد على المنهج الوصفي التحليلي قام الباحث بتحليل النصوص القانونية في كل من البلدين، وأوضحت الدراسة عدة نتائج منها: أن القواعد الموجودة بالتشريع الجزائي الكويتي غير كافية لمواجهة تلك الجرائم؛ وأن المشرِّع الأردني أعطى اهتمامًا حقيقيًا لتلك النوعية من الجرائم، وسبق المشرِّع الكويتي في ذلك، وأن هناك إشكاليات خاصة بالتفتيش والملاحقة والضبط لم يتمكن المشرِّع من تنظيمها.

المحور الثاني: ويتصل بالدراسات التى يمكن تصنيف اهتمامها الموضوعى بأنه يركز على جزئية واحدة ومحددة فيما يتعلق بالجريمة الإلكترونية، ومن ذلك دراسة حسين ربيع وجمال زين العابدين أمين (2019) [19] **حول "إشكاليات التنظيم القانوني للمسئولية الجنائية عن النشر الصحفي الإلكتروني في مصر"**، والتي ركزت على بحث الثغرات القانونية بقانون تنظيم الصحافة والإعلام رقم 180 لسنة 2018 للكشف عن الإشكاليات التي تثيرها نصوص القانون فيما يتعلق بالتنظيم القانوني للمسئولية الجنائية عن جرائم النشر الصحفي الإلكتروني، مستعينة بالمنهج الوصفي التحليلي والاستقرائي، والتي أظهرت نتائجها أن هناك غموضًا في بعض النصوص؛ مما يؤدي لاختلاف تأويلها، وعدم وضوح في النصوص القانونية بين حق النقد من ناحية وبين جرائم السَّبِّ والقذف من ناحية أخرى، وأن القانون يوسع محظورات النشر.

ودراسة رائد محمد فليح النمر (2019) [20] التى اهتمت بتوصيف وتحليل **حماية الخصوصية لمستخدمى مواقع التواصل الاجتماعى** على ضوء تشريعات البحرين، وباستخدام المنهج التحليلى لتحليل النصوص القانونية ذات الصلة وبخاصة قانون حماية البيانات الشخصية البحرينى رقم 30 لسنة 2018؛ توصلت الدراسة إلى أن المشرِّع شدد العقوبة على سرقة البيانات الشخصية واستغلالها وذلك لأهمية حماية الحياة الخاصة.

ودراسة حمدي محمد محمود حسن (2018) [21] **التى ركزت على دراسة المسئولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي دراسة تحليلية مقارنة وتحديد قوانين جرائم الاعتداء على الحياة الخاصة والسَّبِّ والقذف والمساس بالقيم الدينية،** وبالاعتماد على تحليل قوانين مكافحة جرائم تقنية المعلومات أظهرت النتائج أن المشرِّع حرص- في كل من عمان والكويت وقطر والإمارات العربية المتحدة- على تجريم الآراء التي تؤدي إلى الفتنة بين أفراد المجتمع، أو التي تمس القيم الدينية أو النظام العام في

الدولة، كما جرم الاعتداء على الحياة الخاصة والسَّبِّ والقذف باستخدام وسائل التواصل الاجتماعي، ويتم ذلك من خلال قانون مكافحة جرائم تقنية المعلومات في كل بلد.

ودراسة محمد أحمد المعداوي (2018) [22] التي بحثت تحديدًا في كيفية "**توفير الحماية القانونية للخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي**" من خلال البحث عن النصوص والتشريعات العربية والأوروبية في هذا الإطار مع الاسترشاد بالأحكام القضائية الصادرة عن القضاء الفرنسي، وباستخدام المنهج التحليلي المقارن لتحليل النصوص القانونية المتعلقة بموضوع الدراسة وكذا استخدام المنهج المقارن للوقوف على موقف التشريعات المقارنة؛ توصلت نتائج الدراسة إلى أن مواقع التواصل تخترق خصوصية الأشخاص حينما تقوم باستغلال البيانات الشخصية في الأغراض التجارية؛ بل وأحيانًا استغلال بيانات مستخدم آخر حتى ولو لم يكن في قائمة الأصدقاء- كما هو عليه الحال في تويتر- من أجل استخدامها في أغراض غير مشروعة، ومن ثم تؤكد الدراسة على مسئولية الشخص المسئول عن معالجة البيانات.

ودراسة Asherry Brian Magalla (2018) [23] التي بحثت **قانون رقم** 13 **لسنة** 2015 **لمكافحة الجرائم الإلكترونية بتنزانيا** وفنَّدت نصوص القانون والمفاهيم الواردة به بشأن الجرائم الإلكترونية، وكيف يمكن مكافحة الجريمة، وتنفيذ الآليات العقابية المناسبة للحد من الجريمة بتنزانيا.

ودراسة Nazura Abdul Manap **&** others (2015) [24] التي بحثت **تطور قوانين سرقة الهوية والانتحال** في كل من بريطانيا وماليزيا وإيران، وإلى أي مدى تأثرت بتطور استخدامات الإنترنت؟ وباستخدام المنهج التحليلي والمقارنة توصلت الدراسة إلى غموض بعض القوانين والمفاهيم المتصلة بالانتحال؛ ولذا تحتاج إلى التطوير لتحقيق الردع المطلوب، وكذلك توحيد المفاهيم بما يحد من التحايل على القانون.

ودراسة خالد حامد مصطفى (2013) [25] **عن المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي** والتي سعت للإجابة عن التساؤل التالي: من المسؤول عن المعلومات الواردة على المحتوى الكائن على الموقع إذا صنفت كجريمة كما نص المشرِّع الإماراتي؟ وكيف واجه القانون ذلك؟ واعتمدت الدراسة على تحليل ما ورد بالمرسوم بقانون 5 لسنة 2012 لتحليل اتجاه المشرِّع في هذا الشأن، وتوصلت إلى أن هناك عدم شمول ترتب عليه عدم وضوح في تحديد المسؤول عن النشر، وفي تحديد عناصر الجريمة كاملة، وإلى أن المشرِّع أغفل الجوانب الإجرائية المتمثلة في

تحديد الالتزامات التي تقع على الناشر الإلكتروني ومزود خدمات الاستضافة؛ مما يترتب عليه خطورة كبيرة وبخاصة ما يمس أمن الدولة.

التعليق على الدراسات السابقة:

- على الرغم من اتجاه عدد غير قليل من الباحثين في العالم كله وخاصة في العقد الأخير لدراسة الجريمة الإلكترونية من جوانب متعددة، منها كيفية حدوث الجرائم الإلكترونية وتأثيراتها المتعددة على الصحافة والإعلام وأشكال الاعتداءات والجرائم، وكيفية التعامل مع تلك الاعتداءات **إلا أن المكتبة الأكاديمية العربية لا تزال في حاجة إلى مزيد من الدراسات التي تهتم ببحث وتفنيد وتحليل آليات الضبط والمواجهة التشريعية لمثل تلك النوعية من الجرائم– الجرائم الإلكترونية-** بغرض تقييم وتطوير تلك التشريعات المرتبطة بالجرائم الإلكترونية في ظل تزايد حجم التجاوزات والاعتداءات الإلكترونية المتكررة.
- سبقت الدراسات الأجنبية الدراسات العربية في كثافة الاهتمام بالقضايا والموضوعات المتصلة بجرائم تقنية المعلومات وتشريعات تنظيم استخدامات الإنترنت وتكنولوجيا الاتصال، وذلك يتسق مع طبيعة التطور التكنولوجي وتطور استخدامات الإنترنت والاختلاف بين الدول في ذلك، ومن الملاحظ **أن الدراسات الأجنبية الإعلامية مزجت إلى حد كبير وملاحظ بين المداخل والنظريات الخاصة بعلوم الإعلام إلى جانب علوم الحاسوب والهندسة وعلم النفس؛ لأهمية ذلك في هذا الحقل البحثي وهو ما يتفق مع كون علوم الإعلام تعد علوم بينية.**
- **أخذت الجرائم المتصلة بالخصوصية تحديدًا وانتهاك حرمة الحياة الخاصة وسرقة المعلومات والبيانات الشخصية اهتمامًا كبيرًا من الباحثين** كما اتضح للباحثة من خلال مسح الدراسات السابقة، ويرتبط ذلك بتزايد حالات الاعتداء على الحياة الخاصة باستغلال كل إمكانات التكنولوجيا الجديدة، ولكن في المقابل لا تزال أنواع الجرائم الأخرى في حاجة إلى مزيد من الاهتمام من الباحثين، مثل الجرائم الخاصة بإشاعة الفاحشة عبر الإنترنت أو جرائم التحريض وبث خطاب الكراهية، وجرائم انتهاك حقوق الملكية الفكرية، وكذلك الجرائم المتصلة بالاختراق والاعتراض والانتحال على أهميتها وخطورته، ومن هذا المنطلق جاء اهتمام الدراسة بهذه الجرائم تحديدًا لندرة الدراسات الخاصة بها ولخطورة تبعات هذه الجرائم.
- **جاء الاعتماد على تحليل النص القانوني وأسلوب المقارنة المنهجية بين التشريعات المختلفة سواء العربية أو الأجنبية في المرتبة الأولى** من الأدوات وأساليب البحث التي

اتبعها الباحثون، وذلك في إطار اهتمام دراسات التشريعات بالجوانب التحليلية والمقارنة بين النصوص التشريعية المتعددة في كل دولة أو بين الدول المختلفة.

مشكلة الدراسة:

تتبدى المشكلة البحثية في تحليل كيفية مواجهة التشريعات العربية لجرائم الاختراق والاعتراض والانتحال، وتقييم الأطر التشريعية الضابطة للمجال الإلكتروني في الدول العربية؛ لما له من أثر في سد الفجوة البحثية في هذا المجال، وتوفير الأساس العلمي لتطوير النص القانوني في ظل تسارع التطورات والتغيرات التكنولوجية والاتصالية في هذا المجال، وتتصل أيضًا مشكلة الدراسة بالمقارنة بين محددات المسئولية الجنائية لجرائم الاختراق والاعتراض والانتحال وتحليلها كما وردت بالنصوص التشريعية في البلاد العربية، وذلك من حيث شمول النصوص ووضوحها، وآليات الردع، ونوعية العقوبة وما إذا كانت التشريعات تضع ظروفًا استثنائية، وماهية أوجه الشبه والاختلاف بين البلاد العربية- محل الدراسة- (مصر والإمارات والسودان والأردن) في هذه الأمور القانونية.

أهمية الدراسة:

- التزايد المستمر لأشكال التجاوزات والجرائم المتصلة بالاختراق والاعتراض والانتحال في العصر الرقمي باستخدام مواقع التواصل الاجتماعي، خاصة أنها أصبحت وسيلة يعتمد عليها البعض لنشر الأخبار الزائفة ولتضليل الجمهور ولإثارة الفتن وزعزعة الاستقرار الأمني للدول، وهناك الكثير من الدراسات التى أشارت لضرورة الاهتمام بالجانب التشريعى لمواجهة تلك التجاوزات، ولقد تصدر اقتراح سن تشريعات وقوانين تنظم دور مواقع التواصل الاجتماعى ومضمونها المرتبة الأولى من إجمالى اقتراحات المبحوثين لتطوير دور مواقع التواصل في الحد من الجرائم الإلكترونية بنسبة 29.39٪ من دراسة أميرة محمد [26]، ومن ثم تأتى الدراسة لتفنِّد وتقيِّم وتقدِّم مقترحات تتصل بآليات مكافحة تلك الجرائم الخطيرة؛ جرائم الاختراق والاعتراض والانتحال، وبالتركيز عليها تحديدًا، مما يسمح بالتعمق والمقارنة على أساس دقيق بين نصوص القوانين العربية محل الدراسة، وهو ما يتسق مع متطلبات العصر الرقمى وإشكالياته.
- تعد الدراسة من أوائل الدراسات التى تهتم ببحث آليات الردع فيما يتصل بجرائم شديدة الخطورة ألا وهي الاختراق والاعتراض والانتحال، وتحلل وتقارن النصوص

القانونية التى تتصل بمحددات المسئولية الخاصة بهذه الجرائم، التي بات يطلق عليها جرائم العصر.

- تأتى الدراسة في ظل مطالبة الحكومة المصرية ببحث كل سبل مواجهة الجرائم الإلكترونية، ومطالب الهيئات الدولية بضرورة تضافر الجهود المحلية والإقليمية والدولية لبحث آليات التصدى الفاعل لتلك الجرائم، وتفنيد النص القانونى، ومراجعة التشريعات القائمة لمواجهة تلك الجرائم مواجهة قانونية ناجعة، والسعى الجاد من مختلف الجهات ومن الأكاديميين المسؤولين لدراسة وبحث آليات مواجهة تلك التجاوزات والجرائم للحد منها والتصدى لمخاطرها.
- مما يدعم أهمية الدراسة أن الرؤية المقارنة تفيد في رصد أوجه الشبه والاختلاف بين نصوص القوانين العربية المتصلة بجرائم الاختراق والاعتراض والانتحال، وهو ما يظهر جوانب الحسم والفعالية في بعض النصوص مقابل جوانب الضعف أو النقص في النصوص الأخرى، الأمر الذى يؤكد أهمية الدراسة في عملية تفنيد النصوص القانونية وتقييمها، والربط بين الردع والسياسة الجنائية والنصوص القانونية وتوضيح كيفية تطويرها.

أهداف الدراسة:

- الكشف عن توصيف النص القانوني لصور الاستخدام غير المشروع (تحديدًا فيما يتصل بالاختراق– الاعتراض– الانتحال) لمواقع التواصل الاجتماعي بتشريعات الدول العربية محل الدراسة.
- رصد التكييف القانوني لحالات الاستخدامات غير المشروعة فيما يتصل بالاختراق والاعتراض والانتحال باستغلال الإنترنت في تشريعات الدول العربية محل الدراسة.
- توصيف العقوبات الواردة بتشريعات البلاد العربية محل الدراسة في حالات الاختراق والاعتراض والانتحال باستغلال الإنترنت.
- توصيف مدى التغليظ أو التيسير في العقوبة في الحالات المختلفة لجرائم الاختراق والاعتراض والانتحال في البلاد العربية محل الدراسة.
- تحليل مدى شمول النصوص القانونية ووضوحها وآليات الردع ونوعية العقوبة في التشريعات المختلفة محل الدراسة.
- تحليل وتقييم واقع الاتساق بين النص القانوني الخاص بالاختراق والاعتراض والانتحال وبين معطيات العصر الرقمي والإشكاليات الواقعية الناجمة عنه في الاستخدامات غير المشروعة للإنترنت.

- المقارنة بين النصوص القانونية المتصلة بجرائم الاختراق والاعتراض والانتحال في التشريعات العربية المختلفة محل الدراسة.

تساؤلات الدراسة:

في ضوء أهداف الدراسة المحددة، تسعى الدراسة للإجابة عن التساؤلات التالية:

- ما هي صور الاستخدامات غير المشروعة وفقًا لتوصيف النص القانوني (تحديدًا فيما يتصل بالاختراق– الاعتراض– الانتحال) لمواقع التواصل الاجتماعي بتشريعات الدول العربية محل الدراسة؟
- كيف جاء التكييف القانوني لحالات الاستخدامات غير المشروعة فيما يتصل بالاختراق والاعتراض والانتحال باستغلال الإنترنت في تشريعات الدول العربية محل الدراسة؟
- ما هي العقوبات الواردة بتشريعات البلاد العربية محل الدراسة في حالات الاختراق والاعتراض والانتحال باستغلال الإنترنت؟
- كيف تراوح النص القانوني بين التغليظ أو التيسير في العقوبة في الحالات المختلفة لجرائم الاختراق والاعتراض والانتحال في البلاد العربية محل الدراسة؟
- إلى أي مدى يتحقق شمول النصوص القانونية ووضوحها وكفاية آليات الردع المتصلة بنوعية العقوبة في التشريعات المختلفة محل الدراسة؟
- إلى أي مدى يتحقق الاتساق بين النص القانوني الخاص بالاختراق والاعتراض والانتحال، وبين معطيات العصر الرقمي والإشكاليات الواقعية الناجمة عنه في الاستخدامات غير المشروعة للإنترنت؟
- ما أوجه الشبه والاختلاف بين النصوص القانونية المتصلة بجرائم الاختراق والاعتراض والانتحال في التشريعات العربية المختلفة محل الدراسة؟

نوع الدراسة:

تعتبر هذه الدراسة من الدراسات المتخصصة في فقه القانون Doctrinal research وهي تلك البحوث والدراسات التي تهتم برصد وتوصيف النصوص القانونية وتحليلها بالرجوع إلى القوانين ذاتها كمصادر أولية ورئيسة؛ لكشف الرؤية التشريعية التي صيغت وفقًا لها القوانين لمواجهة الجرائم [27]، وتأخذ الدراسة منحى الدراسات الوصفية التحليلية لكونها تهتم بتوصيف محددات المسئولية الجنائية والتكييف القانوني المتصل بجرائم الاختراق والاعتراض والانتحال كما وردت بكافة النصوص القانونية المنظمة لها في البلاد العربية محل الدراسة، وتهتم بتحليلها في ضوء الاتفاقية العربية لمكافحة جرائم

الإنترنت ومعطيات العصر الرقمي والتحديات المهنية وواقع الظروف المجتمعية؛ بل والمقارنة بين تلك النصوص القانونية وتوضيح أوجه الشبه والاختلاف ومدى الاتساق القانوني مع التطورات وواقع العصر الرقمي ومعطياته وإشكالياته.

منهج الدراسة وأدواتها:

وبغرض التوصل للنتائج المستهدفة تعتمد الدراسة على المنهج الوصفي التحليلي لوصف وتحليل النصوص القانونية المتصلة بمحددات المسؤولية الجنائية عن جرائم "الاختراق" و"الاعتراض" و"الانتحال"، وكذا المنهج الاستقرائي وذلك لاستقراء- وليس مجرد وصف- النصوص القانونية؛ بل ربطها بالهدف من القانون وبيان أبعادها، ولذا تم استخدام أداة تحليل النصوص القانونية أحد أهم الأدوات المستخدمة في بحوث القانون ودراساته سواء من جانب المشرِّعين أو المحامين أو الأكاديميين [28]، والتي يتم الاعتماد عليها في دراسات التشريعات بوصفها أداة التحليل الملائمة لتفنيد النصوص القانونية محل الدراسة، إذ يعد النص القانوني وحدة التحليل في هذه الدراسات، كما اعتمدت الدراسة أسلوب المقارنة المنهجية للمقارنة بين تلك النصوص القانونية في تشريعات الدول العربية محل الدراسة.

عينة الدراسة ومبررات اختيارها:

تركز الدراسة تحديدًا على النصوص القانونية المتصلة بالأفعال المجرَّمة التالية (الاختراق) و(الاعتراض) و(الانتحال) وذلك في كل من: **مصر** والتي وقعت فيها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010) وتستهدف متابعة وتطوير آليات مكافحة الجريمة الإلكترونية، وأصدرت مصر قانونًا مفصلًا عام 2018 لمكافحة جرائم تقنية المعلومات والذي جاء إجمالًا في 45 مادة، **والإمارات** التي كانت من أوائل الدول التي صدقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وأولى الدول العربية التي سنَّت قانونًا مخصصًا للجرائم الإلكترونية عام 2006 والذي تم إلغاؤه بعد ذلك وإصدار "المرسوم بقانون رقم 5 لسنة 2012 لمكافحة جرائم تقنية المعلومات"، وجاء إجمالًا في 51 مادة، وتعديلاته بالقانون 2018 مؤخرًا [29]، وجاءت كذلك وفقًا لتقرير التنافسية الرقمية العالمي (2019) الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية في المركز الأول عربيا و12 عالميا في مؤشر التنافسية الرقمية ،**والسودان** التي كانت من أوائل الدول العربية التي صدقت على الاتفاقية العربية وكذلك من أوائل الدول العربية في إصدار قانون مخصص للجريمة الإلكترونية وذلك عام 2007 [30] والذي اشتمل إجمالًا على 30 مادة، **والأردن** التي كانت من الدول المصدِّقة

على الاتفاقية العربية، وكانت من أولى البلاد العربية في سَنِّ قانون مخصص للجريمة الإلكترونية عام 2010 [31] والذي عدل بحسب "القانون رقم 27 لعام 2015" والذي اشتمل إجمالًا على 18 مادة وتعديلاته عام 2018.

وبالتالي جاء تحديد مقارنة التشريعات في مصر مع كل من الإمارات والسودان والأردن باعتبارها من أوائل الدول التي صدقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي سبقت غيرها كذلك في وضع وإصدار قانون مخصص للجريمة الإلكترونية.

ويركز البحث على قوانين محددة (اشتملت على 90 نصًا قانونيًا)؛ ففي **مصر** "القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات"، وتتركز محددات جرائم الاختراق والاعتراض والانتحال في اثنتين وثلاثين مادة من مواد القانون تتصل بالتعريفات والتكييف القانوني لتلك الجرائم، والمسئولية الجنائية لمرتكبي الجرائم، وأشكال العقوبة وحالات تخفيف أو تغليظ العقوبة، وفي **الإمارات** "المرسوم بقانون رقم 5 لسنة 2012 لمكافحة جرائم تقنية المعلومات"، وتتركز محددات جرائم الاختراق والاعتراض والانتحال في سبع وعشرين مادة من مواد القانون تتصل بالتعريفات والتكييف القانوني لتلك الجرائم، والمسئولية الجنائية لمرتكبي الجرائم وأشكال العقوبة، وحالات تخفيف أو تغليظ العقوبة، وفي **السودان** "قانون جرائم المعلوماتية" 2007 والذي تناول في ثماني عشرة مادة المحددات المتصلة بجرائم الاختراق والاعتراض والانتحال وما يتصل بالتكييف القانوني لتلك الجرائم، والمسئولية الجنائية وما يرتبط بها من عقوبات، وحالات تخفيف العقوبة وتغليظها، وفي **الأردن** "قانون رقم 27 لسنة 2015" وتعديلاته بقانون 2018 وذلك من خلال ثلاث عشرة مادة خصصت لتوضيح أحكام ومحددات جرائم الاختراق والاعتراض والانتحال، والتكييف القانوني لتلك الجرائم والمسئولية الجنائية عنها والعقوبات المتصلة بها.

وهكذا تحددت عينة المواد القانونية الخاضعة للتحليل في الدراسة في (90 مادة) إجمالًا، ويمكن تحديدها فيما يلي:

وفقًا للقانون المصري: 32 مادة تختص بالجرائم موضوع الدراسة وهي المواد (1: 6 – 12: 18 – 22: 24 - 27: 42).

وفقًا للقانون الإماراتي: 27 مادة تختص بالجرائم موضوع الدراسة وهي المواد (1: 11 – 14: 15 – 21: 22 – 27: 42).

وفقًا للقانون السوداني: 18 مادة تختص بالجرائم موضوع الدراسة وهي المواد (1 :9 – 11 – 23 :30).

ووفقًا للقانون الأردني: 13 مادة تختص بالجرائم موضوع الدراسة وهي المواد (1 :8 – 11 :13 – 16 :17).

مفاهيم الدراسة:

- **المسئولية الجنائية** Criminal responsibility: تعنى المسئولية بشكل عام: حالة الشخص إذا ما ارتكب شيئًا يستوجب المساءلة، والمسؤولية الجنائية تكون بقيام الشخص بأداء فعل مستوجب للعقوبة الجنائية بكل الأركان والعناصر التي يشترطها القانون في هذا الفعل، والمسئولية الجنائية تحقق العدالة لتحميلها الجاني مسئولية أفعاله [32].

وتعني المسئولية الجنائية مساءلة الشخص عن أعماله وتصرفاته التي يقوم بها باختياره، فيخالف بها القوانين، والسياسة الجنائية هي الخطوط العامة التي تحدد اتجاه المشرِّع والسلطات لتطبيق التشريع وتنفيذه بما يحقق الدفاع الاجتماعي [33].

- **جرائم الاختراق الإلكترونية** hacking/trespassingهي تلك الأفعال التي تعمد إلى الدخول بدون وجه حق أو سبب مشروع إلى نظام ما أو جهاز حاسوب.
- **جرائم الاعتراض الإلكترونية** Illegal interception هي أن يتمكن الجاني بشكل غير قانوني من مشاهدة البيانات أو المعلومات أو الحصول عليها لأغراض متعددة منها التنصت أو التخزين أو تغيير المحتوى أو تعديل المسار.
- **جرائم الانتحال الإلكترونية** Identity theft and plagiarism عبر الإنترنت وشبكات التواصل الاجتماعي هي ما يتعمد الفاعل القيام به دون وجه حق من استخدام هوية شخص آخر للإفادة من سمعته أو صلاحياته، وتتخذ جريمة انتحال الهوية عبر الإنترنت أحد وجهين: انتحال هوية الفرد أو انتحال هوية المواقع [34]، ووصفها المختصون بجريمة الألفية الجديدة نتيجة لسرعة تزايد وانتشار ارتكابها [35].

نتائج الدراسة:

بعد انتشار وتزايد استخدام تقنيات المعلومات والاتصالات على المستوى العربي وتعدد استعمالات أجهزة الاتصال ودخول الرقمنة إلى مختلف القطاعات استحدثت النصوص القانونية في مختلف البلاد؛ من أجل ضبط الاستخدامات ومنع التجاوزات ومكافحة الجرائم والأعمال غير القانونية التي يمارسها الأفراد أو الجهات، ومنها:

اختراق أنظمة المعلومات والاعتراض وسرقة الهوية والانتحال، وفي هذا الإطار سعت البلاد العربية لمواجهة تلك الجرائم الماسَّة بأمن الأفراد والمؤسسات والبلاد، ومن أوائل هذه البلاد الإمارات والسودان والأردن ثم مصر، ويتضح فيما يلي كيف تكافح كل دولة جرائم الاختراق والاعتراض والانتحال عبر قوانين مخصصة لذلك وما أوجه الشبه والاختلاف بين كل قانون من القوانين محل الدراسة:

أولًا: فيما يتصل بتحديد حالات ارتكاب الجريمة ومرتكبي الجريمة الإلكترونية الذين يتم مساءلتهم:

وفقًا للقانون المصري رقم 175 لسنة 2018 فإن المشرِّع وسَّع محددات المسئولية الجنائية، وهو ما يتسم- في رأينا- بالشمول في النص القانوني، إذ جاء النص ليشمل المصريين وغير المصريين مرتكبي الفعل المجرَّم وفقًا للقانون، طالما كان الفعل معاقَبًا عليه في الدولة التي وقع فيها تحت أي وصف قانوني في أحوال متعددة (6 أحوال محددة) أقرَّها القانون في مادته الثالثة (م.3 /1-6) وهي: إذا ارتكبت الجريمة على متن أي وسيلة نقل مسجلة على مصر أو تحمل علمها، وإذا كان من المجني عليهم مصريين، وإذا تم الإعداد للجريمة أو تمويلها في مصر، وإذا ارتكبت الجريمة بواسطة جماعة إجرامية تمارس نشاطها في أكثر من دولة منها مصر، وإذا كان من شأن الجريمة إلحاق ضرر بمصريين أو مقيمين في مصر أو بأمن البلاد، وإذا وجد مرتكب الجريمة في مصر ولم يتم تسليمه.

ووفقًا لقانون الإمارات المرسوم بقانون 5 لسنة 2012 بشأن جرائم تقنية المعلومات؛ فإن النص القانوني يشمل كذلك المصريين وغير المصريين مرتكبي الفعل المجرَّم كما هو الحال في القانون المصري؛ إلا أن المشرِّع لم يُفصِّل أحوال ارتكاب الأفعال غير المشروعة التي تحدد وقوع الجريمة وتحدد وقوع مرتكبها تحت طائلة القانون، غير أن القانون الإماراتي أكد في نص المادة 47 أن هذا القانون يطبق على كل من ارتكب إحدى الجرائم المنصوص عليها بالقانون خارج الدولة.

ووفقًا لقانون جرائم المعلوماتية لسنة 2007 بالسودان فإن النص القانوني أوضح أن أحكام القانون تطبق على الجرائم إذا ارتكبت داخل أو خارج السودان وامتد أثرها داخل السودان (م.2)، ولم يُفصِّل أكثر من ذلك في شأن حالات ارتكاب الجريمة، بينما في قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015 فإن المشرِّع نصَّ على تطبيق العقوبات المقررة حال وقوع الجريمة بالأردن أو ألحقت أضرارًا وترتبت آثارها في الأردن أو ارتكبت من شخص مقيم بها (م.17).

ثانيًا: النصوص التشريعية المتصلة بالجهة المسؤولة قانونًا عن متابعة الاتصال والجرائم الإلكترونية:

يختص قانون تنظيم الاتصالات رقم١٠ لسنة٢٠٠٣ في مصر بتنظيم قطاع الاتصالات، بحيث تعتبر الجهة المسئولة عن قطاع الاتصالات في مصر هي الهيئة العامة للاتصالات وهي تابعة لوزارة الاتصالات، كما أوضح المشرِّع المصري في القانون رقم 175 لسنة 2018 المختص بتنظيم ومكافحة الجرائم الإلكترونية أن المسئول عن متابعة الاتفاقيات الدولية في شأن مكافحة الجرائم الإلكترونية هو المركز الفني للاستعداد لطوارئ الحاسب والشبكات بالجهاز القومي لتنظيم الاتصالات، كما أنه تم تخصيص إدارة خاصة بمكافحة جرائم شبكات المعلومات تابعة لوزارة الداخلية المصرية، ووفقًا لقانون الاتصالات الإماراتي رقم "5" لسنة 2012 لمكافحة جرائم تقنية المعلومات في الإمارات فإن الهيئة التي تختص بعملية التنظيم هي "الهيئة العامة لتنظيم قطاع الاتصالات"، ولقد تم إنشاء الهيئة الوطنية للأمن الإلكتروني سنة 2012 في الإمارات لمكافحة الجرائم الإلكترونية تحديدًا وفقًا للمرسوم بقانون اتحادي رقم 3 لسنة 2012.

بينما في السودان تم إصدار قانون الاتصالات لسنة 2001، وتختص وفقًا له الهيئة القومية للاتصالات والمنشأة بموجب أحكام المادة 6 من هذا القانون بتنظيم الاتصالات بالسودان، ولقد نصَّ قانون جرائم المعلوماتية (م.28)- وفقًا لقانون الهيئة القضائية لسنة 1986- على أن تكون هناك محكمة خاصة ونيابة متخصصة وشرطة متخصصة لجرائم المعلوماتية، ووفقًا لقانون الاتصالات الأردني رقم ١٣ لسنة ١٩٩٥ فقد اختص تنظيم قطاع الاتصالات- من خلال هيئة تنظيم قطاع الاتصالات- بعملية الضبط والتنظيم وذلك إضافة لموظفي الضابطة العدلية الذين يخول لهم قانون جرائم أنظمة المعلومات (م.12) مهام الاستدلال والتقصي والتفتيش.

ثالثًا: المحددات التشريعية المتصلة بجرائم الاختراق الإلكترونية:

تعتبر جرائم الاختراق الإلكترونية hacking/trespassing هي تلك الأفعال التي تعمد إلى الدخول بدون وجه حق أو سبب مشروع إلى نظام ما أو جهاز كمبيوتر، وذلك لأسباب متعددة منها: التجسس ومعرفة معلومات سرية معينة، أو تشويه موقع الكتروني أو شخص سواء شخص طبيعي أو اعتباري، أو بغرض تغيير بعض البيانات والمعلومات أو حذفها وغيرها من الأسباب، ويتم الاختراق عن طريق القراصنة (الهاكرز) الذين يستغلون ضعف الأنظمة التقنية لبعض مواقع التواصل الاجتماعي والمواقع الإلكترونية فيقومون باستغلال الثغرات الأمنية في مزودات الويب وأنظمة التشغيل.

ويتبادل القراصنة (الهاكرز) المعلومات في هذا الشأن بغرض الاطلاع على مواطن الضعف في الأنظمة المعلوماتية وتتم عملية تبادل المعلومات فيما بينهم بواسطة النشرات الإعلامية الإلكترونية؛ بل إنهم يعقدون المؤتمرات لكافة مخترقي الأنظمة المعلوماتية للتشاور حول وسائل الاختراق وآليات نجاحها، ويتبع المخترقون أساليب عدة في عمليات الاختراق وتختلف هذه الأساليب من موقع لآخر وفقًا لنوعية نظام التشغيل الخاص بالموقع [36].

ويشتغل المخترقون على الثغرات الموجودة في الأنظمة التقنية ويستغلونها في عمليات الاختراق إلى أن يتم التوصل إلى حلول لسد هذه الثغرات، وتظل بعض العيوب والثغرات لفترة طويلة حتى يتم اكتشافها أو إيجاد حلول لها، وذلك لأن أغلب الثغرات التي يكتشفها المخترقون لا يعلنون عنها ليتمكنوا من استغلالها فترة أطول [37].

وهناك عدة مواد تتصل بجريمة الاختراق أوردها المشرِّع في القوانين الخاصة بمكافحة جرائم تقنية المعلومات في الدول العربية محل الدراسة، وتتضح فيما يلي:

فيما يتصل بمفهوم الاختراق:

وهو كما أوضحه القانون المصرى رقم 175 لسنة 2018 ويعنى تحديدًا "الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بأى طريقة غير مشروعة إلى نظام معلوماتى أو حاسب آلى أو شبكة معلوماتية وما في حكمها"، أى أن المشرِّع المصرى أراد حماية الأنظمة المعلوماتية وخصوصيتها وخصوصية الحواسب الآلية وشبكات المعلومات من الدخول غير المشروع (الاختراق)؛ وذلك بغض النظر عن استغلال ذلك الاختراق في أي استخدامات غير مشروعة أو مضرة.

وبالمقارنة بين القوانين محل الدراسة، نجد أن المشرِّع لم يضع بقانون الإمارات تعريفًا لجريمة الاختراق في نص القانون؛ وكذلك فعل المشرِّع السوداني ومثله الأردني، وهو ما يميز القانون المصري في هذه الجزئية.

فيما يتصل بتوصيف جريمة الاختراق والعقوبات المترتبة عليها:

أوضح المشرِّع المصرى جريمة الاختراق بمستوياتها المتعددة والعقوبات المترتبة عليها وهو ما سيتم رصده وتوصيفه فيما يلي:

- جريمة تجاوز حدود الحق في الدخول unauthorized access إذ جرَّم المشرِّع المصري في قانون مكافحة جرائم تقنية المعلومات (م.15) كافة الجرائم التي يتجاوز من خلالها الشخص حدود الحق في الدخول، حيث عاقب المشرِّع المصري مرتكب تلك الجريمة بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 30 ألف جنيه ولا

تتجاوز 50 ألف جنيه، أو بإحدى هاتين العقوبتين، وذلك لكل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدمًا حقًا مخولًا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول، وهكذا رأى المشرِّع المصري خطورة التجاوز في حق الدخول باعتبارها جريمة اختراق.

وترى الباحثة أهمية تلك المادة التي تمنع الاستخدامات المتكررة لموقع أو حساب أو نظام معلوماتي دون أن يكون للمستخدم وجه حق في ذلك.

- **جريمة الدخول غير المشروع للمواقع**، إذ جرَّم المشرِّع المصري في قانون مكافحة جرائم تقنية المعلومات في المادة 15 كافة الجرائم التي يتم الدخول فيها للمواقع الإلكترونية بصورة غير مشروعة، فعاقب المشرِّع المصري مرتكب تلك الجريمة "بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن 50 ألفًا ولا تجاوز 100 ألف جنيه، أو إحدى هاتين العقوبتين، وذلك لكل من دخل عمدًا أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه".
- **ثم فرَّق المشرِّع المصري بين مجرد الدخول (الاختراق) كجريمة في حد ذاتها وبين ما يفعله الجاني مرتكب تلك الجريمة مما يترتب على فعل الاختراق**، فأوضح المشرِّع أنه "إذا نتج عن ذلك الدخول غير المشروع حدوث إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي؛ تكون العقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 ألف جنيه ولا تتجاوز 200 ألف أو بإحدى هاتين العقوبتين".
- **كما أوضح المشرِّع مزيدًا من المسئولية عن الجريمة في حال ارتباطها بمقدِّم الخدمة**، وذلك في المادة 31 من ذات القانون 175 لسنة 2018 أن هناك عقوبات لكل مقدِّم خدمة– على خلاف القانون- لم يحافظ على سرية البيانات ولم يحمِ البيانات من الاختراق والاعتراض.

ومما سبق يتضح أن القانون المصري فصَّل بوضوح ما يتصل بجريمة الاختراق من حيث تحديدها وفقًا للتعريف الذي أورده لها ثم تفصيل محددات المسئولية الجنائية لمرتكبي الجريمة في كافة أحوالها، ثم أيضًا التفصيل في حالات ارتكاب الجريمة والتفرقة بين الاختراق في حد ذاته والاختراق الذي ينتج عنه جرائم أخرى تضر بالمجني عليهم.

أمَّا وفقًا لقانون الإمارات المرسوم بقانون 5 لسنة 2012 بشأن جرائم تقنية المعلومات فإن القانون جرَّم الاختراق كجريمة في حد ذاته، دون النظر إلى ما يترتب عليه من أفعال- كما هو الحال في القانون المصري- ويمكن توضيح ذلك تفصيلًا كما يلي:

- عاقب القانون في مادته الثانية بالفقرة الأولى (2 -1) "بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة ".
- كما أشار المشرِّع في القانون الإماراتي عن عقوبة تجاوز حدود التصريح الخاص بالدخول، وهو ما يتشابه مع ما ورد بالقانون المصري في هذا الشأن (م.15).
- ولقد شدَّد العقوبة في الفقرة الثانية من ذات المادة في حالة وجود جرائم تترتب على جريمة أو فعل الاختراق، بحيث "تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسين ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة 1 من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات"، ثم غلَّظ المشرِّع العقوبة في حالة الاختراق والإتلاف لما يتصل تحديدًا بالبيانات أو المعلومات الشخصية (م.2 -3).
- ويعاقب القانون ليس فقط على الاختراق أو تجاوز مرات الدخول وإنما يعاقب "كل من حصل بدون تصريح على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات ، أو موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلوماتية أو معلومات الكترونية" (م.14).
- كما يعاقب القانون في الإمارات على ارتكاب الجريمة بسبب تأدية الشخص لعمله (م.3) وهو ذاته المبدأ المعمول به في القانون المصري.

أمَّا وفقًا لقانون جرائم المعلوماتية، القانون رقم 13 لعام 2007 بالسودان والمعدل بعام 2018:

- فإن جريمة "الاختراق" قانونًا وردت في نص المادة الرابعة، والتى نصت على" أن كل من يدخل موقعًا أو نظام معلومات دون أن يكون مصرحًا له ويقوم بالاطلاع عليه أو نسخه؛ يعاقب بالسجن مدة لا تجاوز سنتين أو بالغرامة أو بالعقوبتين معًا، وكذلك من يقوم بإلغاء بيانات أو معلومات ملكًا للغير أو حذفها أو تدميرها أو إفشائها أو

إتلافها أو تغييرها أو إعادة نشرها، أو تغيير تصاميم الموقع أو إلغائه أو شغل عنوانه يعاقب بالسجن مدة لا تجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معًا.

- وتم البتُّ فيها أيضًا ضمن نص المادة 7 والتى جاءت بعنوان "جريمة دخول المواقع عمدًا بقصد الحصول على بيانات أو معلومات أمنية"، ومن ثم فإن العنوان الذى وضع للجريمة جاء فيه تعريف محدد ووحيد للبيانات والمعلومات وهي كونها "أمنية" فقط.

ونص المشرع على أن كل من يدخل عمدًا موقعًا أو نظامًا مباشرة أو عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها بغرض:
(أ) الحصول على بيانات أو معلومات تمس الأمن القومى للبلاد أو الاقتصاد الوطنى يعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معًا.
(ب) إلغاء بيانات أو معلومات تمس الأمن القومى للبلاد أو الاقتصاد الوطنى أو حذفها أو تدميرها أو تغييرها يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معًا.

- وفي المادة 8 نص المشرِّع على أن كل من يدخل بأي وسيلة نظامًا أو وسائط أو شبكة معلومات وما في حكمها ويقوم عمدًا بإيقافها أو تعطيلها أو تدمير البرامج أو البيانات أو المعلومات أو مسحها أو حذفها أو إتلافها يعاقب بالسجن مدة لا تتجاوز ست سنوات أو بالغرامة أو بالعقوبتين معًا.
- كما أوضح المشرِّع مزيدًا من المسئولية عن الجريمة في حال ارتباطها بالموظف العام، وبالتالى غلَّظ المشرِّع العقوبة على الجرائم في هذه الحالة.

ووفقًا لما ورد بقانون الجرائم الإلكترونية رقم 27 لسنة 2015 بالأردن فقد:

- نص القانون في المادة (3-أ) على الاختراق كجريمة والدخول بما يجاوز التصريح الممنوح للمستخدم، ثم أشار في المادة (3-ب) للأفعال المجرمة التى تترتب على الاختراق وأوضح العقوبات الخاصة بتلك الجرائم والتي تتراوح بين الحبس والغرامة أو بهما معًا.

رابعًا: المحددات التشريعية فيما يتصل بجرائم الاعتراض الإلكترونية:

جرائم الاعتراض الإلكترونية هي: تلك الجرائم التي تعني العمل على تغيير مسار المعلومات المتداولة أو إخفائها أو تعطيلها وذلك لأسباب غير مشروعة، ولقد عرفت جريمة الاعتراض غير المشروع وفقًا لنص "الاتفاقية العربية لمكافحة جرائم تقنية

المعلومات" بأنها الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات (م.7).

مفهوم جرائم الاعتراض الإلكترونية:

عرف المشرِّع المصري الاعتراض في نص مادته الأولى بأنه "مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق".

وبالنظر إلى نصوص القانون الإماراتي والسوداني والأردني فإننا سنجد غيابًا لتعريف محدد لمفهوم الاعتراض وما المقصود به تحديدًا، وهو ما يميز القانون المصري.

فيما يتصل بتوصيف جريمة الاعتراض والعقوبات المترتبة عليها:

جرَّم المشرِّع المصري كافة أشكال الاعتراض التي تتم في مواجهة المعلومات والبيانات وكل ما هو متداول عبر مواقع التواصل الاجتماعي وكافة الموقع الإلكترونية، حيث:

- عاقب المشرِّع المصري مرتكبي جريمة "اعتراض المعلومات والبيانات وكل ما هو متداول عبر مواقع التواصل الاجتماعي وكافة المواقع الإلكترونية بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 250 ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعترض بدون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها" وذلك كما ورد بالمادة 16 من القانون المصري الخاص بمكافحة جرائم تقنية المعلومات.
- أيضًا أكد المشرِّع المصري على مقدم الخدمة (م.3/2) تأمين البيانات والمعلومات بما يحافظ على سريتها وعدم اعتراضها أو اختراقها أو تلفها.

ووفقًا لقانون الإمارات فإن نصوص مكافحة جريمة الاعتراض أوردت ما يلي:

- يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع إلكتروني أو نظام معلومات إلكتروني (م.8).
- يعاقب "بالحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من التقط أو اعترض عمدًا وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية" (م. 15).

وبالتالي فإن القانون الإماراتي جرَّم فعل الاعتراض في حد ذاته باعتباره جريمة دون النظر إلى أي من الأفعال المترتبة عليه، ثم أوضح القانون في المادة ذاتها أنه إذا "أفشى أي شخص المعلومات التي حصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق فإنه يعاقب بالحبس مدة لا تقل عن سنة واحدة " (م. 15).

- ولكن المشرِّع في القانون الإماراتي ميَّز بين المعلومات والبيانات الشخصية وغير الشخصية، ثم ميَّز تحديدًا المعلومات والبيانات الطبية عن غيرها؛ فشدد العقوبة على تغيير أو نسخ أو الإتلاف بأي طريقة للمعلومات والبيانات الشخصية (م.2/فقرة 3)، ثم غلظ العقوبة لدرجة أكبر في حال كانت هذه البيانات والمعلومات تتعلق بتشخيص طبي وسجلات طبية (م.7)، وهو ما لم يرد تفصيلًا في القانون المصري.

ووفقًا لقانون جرائم المعلوماتية بالسودان جاء الاعتراض مجرَّمًا بنص مباشر بالقانون كما يلي:

- كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمها أو يلتقطها أو يعترضها دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معًا (م.6 من قانون جرائم المعلوماتية).

وبالتالي فإن القانون السوداني جرَّم فعل الاعتراض في حد ذاته باعتباره جريمة دون النظر إلى أي من الأفعال المترتبة عليه على عكس جريمة الاختراق التي وردت كجريمة بوجود أفعال أخرى مصاحبة لها في نصوص القانون السوداني.

- ثم ورد في المادتين 8 و9 من القانون السوداني تجريمًا للأفعال المتصلة بالاعتراض والناشئة عنه مع النص على العقوبات المقررة لتلك الأفعال المجرمة وهي إيقاف أو تعطيل أو إتلاف البرامج أو البيانات أو المعلومات أو مسحها وحذفها (نص م.8) وعقوبتها السجن مدة لا تتجاوز ست سنوات أو الغرامة أو العقوبتين معًا، وكذلك إعاقة أو تشويش أو تعطيل الوصول للخدمة (نص م.9) وجاءت عقوبتها مدة لا تتجاوز سنتين أو الغرامة أو بالعقوبتين معًا.

أما القانون الأردني فلقد جرم الاعتراض وفقا لنص المادة (5) التي أقرت الحبس والغرامة لكل من قام باعتراض ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلوماتي.

خامسًا: المحددات التشريعية فيما يتصل بجرائم الانتحال الإلكترونية:

جرائم الانتحال الإلكترونية- كما ذكرنا آنفًا- هي جرائم الانتحال عبر الإنترنت وشبكات التواصل الاجتماعي وهي ما يتعمد الفاعل القيام به دون وجه حق من استخدام هوية شخص آخر للإفادة من سمعته أو صلاحياته، وتتخذ جريمة انتحال الهوية عبر الإنترنت أحد وجهين: انتحال هوية الفرد أو انتحال هوية المواقع، ووصفها المختصون بجريمة الألفية الجديدة نتيجة لسرعة تزايد وانتشار ارتكابها، ولكن لم يرد أي نص صريح بشأن مفهوم جرائم الانتحال في أي من القوانين محل الدراسة.

إلا أن المشرِّع المصري أثبت اهتمامه بجريمة الانتحال وأفرد لذلك نصًّا خاصًّا به، إذ أوجب في قانون مكافحة جرائم تقنية المعلومات (م.2/2-3) أنه يجب على مقدم الخدمة المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها المستخدمون، أو الأشخاص والجهات التي يتواصلون معها، كما أوجب القانون أيضًا ضرورة القيام بتأمين المعلومات والبيانات بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها.

ووفقًا لقانون الإمارات فإنه "يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات" (م.11).

كما أن المادة 9 التي استبدلت بالمادة 1 في القانون الاتحادي رقم 12 لسنة 2016 أوضحت عقوبة شديدة الغلظة تصل إلى مليوني درهم لكل من استغل عنوانًا عائدًا للغير- وهو ما يتسق مع معنى الانتحال- بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها (راجع نص المادة 1 من القانون الاتحادي رقم 12 لسنة 2016).

وهكذا ربط المشرِّع في القانون الإماراتي بين الجرائم المترتبة على الانتحال، في معرض نصه في المادة 11 والمادة 1 لتعديل المادة 9، والانتحال في حد ذاته كفعل غير مشروع، أي أنه عاقب على ما ترتب على جريمة الانتحال وليس الانتحال في حد ذاته باعتباره جريمة في حد ذاتها.

وفي قانون جرائم المعلوماتية السوداني أشارت المادة 11 إلى الانتحال، وجاءت المادة تحت عنوان "الاحتيال أو انتحال صفة غير صحيحة"، ونصت على أن كل من يتواصل عن طريق شبكة المعلومات عن طريق الانتحال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة بغرض الاستيلاء على مال أو سند أو توقيع للسند يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معًا.

وكما هو واضح من خلال استقراء وتحليل هذا النص المتصل بالانتحال وسرقة الهوية يتضح أن الفعل المجرَّم هنا والعقوبة المتصلة به ترتبط بالاستيلاء على المال أو السند أو التوقيع، وكان حريٌّ بالمشرِّع أن يوسع من صلاحيات هذا النص فلا يربطه فقط بهذه الأمور المحددة.

ووفقًا لما ورد بالقانون الأردني فإن المادة (3-ج) تُجرِّم الدخول إلى الموقع لانتحال صفته أو انتحال شخصية مالكه وتعاقب على ذلك بالحبس والغرامة معًا، كما تُجرِّم المادة (4) كل من استخدم برنامجًا أو نظامًا معلوماتيًا لانتحال صفة الموقع أو شخصية المالك.

سادسًا: حدود القانون فيما يتصل بالتصالح والإعفاء وتخفيف العقوبة:

أجاز المشرِّع المصرى التصالح وفقًا للقانون رقم 175 لسنة 2018، ولكنه أفرد لذلك شروطًا وإجراءات محددة، فالمشرِّع في القانون المصرى يجيز في مادته رقم (42) للمتهم في أية حالة كانت عليها الدعوى الجنائية وقبل صيرورة الحكم باتًّا إثبات الصلح مع المجنى عليه أو وكيله الخاص أو خلفه العام أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال وذلك في الجنح المنصوص عليها في المواد 15، 16، 17، 18، 19، 20، 24، 27، 29، 31، 32، ولا ينتج إقرار المجنى عليه بالصلح المنصوص عليه أثره إلا باعتماده من الجهاز بالنسبة للجنح المنصوص عليها بالمواد 15، 18، 19، 24 من هذا القانون، وأوضح المشرِّع أن التصالح لا يتم إلا بدفع الجانى ضعف مبلغ الحد الأقصى للغرامة المقررة نصًّا في القانون، أما بالنسبة للشروع في ارتكاب الجريمة فإن عقوبتها هى نصف العقوبة المقررة للجريمة (م.40) ويعفى من العقوبة كل من بادر بالإبلاغ عن الجريمة قبل البدء في تنفيذها وقبل كشفها (م.41).

وكذلك نجد أن المشرِّع بالقانون الإماراتى أقر أيضًا بتخفيف العقوبة لتصل إلى النصف في حال الشروع في الارتكاب فقط دون أن يتم الجانى ارتكاب الجريمة فعليًّا (م.40 من المرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات)، كما أن المشرِّع نصَّ في المادة 45 أن النائب العام له أن يطلب تخفيف العقوبة أو الإعفاء منها إذا تم الإدلاء بمعلومات متى أدى ذلك إلى الكشف عن الجريمة، وكذلك فإن المشرِّع السوداني

نصَّ على تخفيف العقوبة في حال الشروع في الجريمة كما ورد بنص المادة 24 بينما لم يشر المشرِّع الأردنى إطلاقًا لحالات تخفيف العقوبة.

سابعًا: الرؤية التشريعية فيما يتصل بالظروف المشددة في الجرائم الإلكترونية:

المواد من 34 إلى 37 من القانون المصرى لمكافحة جرائم الإنترنت تولَّى من خلالها المشرِّع تفصيل حالات تشديد العقوبة ثم تحديد المادتين 38 و39 للعقوبات التبعية، ووفقًا للقانون فإن تشديد العقوبة جاء في أربع حالات:

- إذا وقعت الجريمة بغرض الإخلال بالنظام أو الأمن العام أو اللوائح والدستور (م.34).
- وإذا وقعت الجريمة ولم يبلغ عنها مسؤول الموقع وقت علمه بها، فهنا يعاقب عقابًا مشددًا (م.35).
- وإذا كان المسؤول عن إدارة الموقع على علم بالجريمة أو سهَّل للجاني القيام بها (م.36).
- وأكد القانون (م.37) أن ذلك العقاب المشدد لمسؤول الموقع لا يترتب عليه استبعاد المسئولية الجنائية عن الجانى الأصلى، ثم حدد القانون في مادتيه 38 و39 مصادرة الأجهزة التى تم من خلالها ارتكاب الجريمة، وكذلك عزل الموظف العمومي الذي تمت الجريمة أثناء أو بسبب وظيفته.

ولقد شدد المشرع الإماراتى العقوبة في حال ارتكاب الجريمة بمناسبة أو بسبب تأدية الشخص لعمله (م.3)، كما شدد القانون العقوبة في حالة الاختراق بقصد الحصول على بيانات حكومية أو معلومات سرية لمنشآت اقتصادية، وغلظ العقوبة أكثر في حال إتلاف تلك البيانات (م.4).

أما المشرع السودانى فقد شدد العقوبة في حالة قيام الموظف العام بجريمة الاختراق أو بتسهيلها لشخص ما (م.5) وسار المشرع الأردنى على نفس النهج، فقد شدد العقوبة في حال ارتكابها بسبب العمل (م.8)، واهتم كذلك بمضاعفة العقوبة في حال ارتبطت تلك الجرائم الخاصة بالاختراق والاعتراض والانتحال بالمعاملات المالية والخدمات المصرفية (م.7)، أو إذا كانت تمس الأمن الوطنى أو العلاقات الخارجية للدولة والاقتصاد الوطنى وغير متاحة للجمهور، أو إذا تم تعديلها أو إتلافها أو إفشاءها (م.12أ، ب، ج، د)، كما أشار القانون لمضاعفة العقوبة في حال تكرار الجُرم.

ثامنًا: بعض الإشكاليات المتصلة بتحديد المسئولية في الجرائم الإلكترونية:

هناك بعض الإشكاليات التي يمكن مناقشتها وتوضيحها في ضوء ما تم التعرض له من النصوص القانونية والتشريعات محل الدراسة، إذ اتضح أن المشرع أحيانًا قد يربط بين الفعل الإجرامي وبعض الآثار المتصلة به لوضع عقوبة عليه؛ ففي صياغة محددات الانتحال وسرقة الهوية يتضح أن الفعل المجرَّم والعقوبة المتصلة به ترتبط بالاستيلاء على المال أو السند أو التوقيع، كما هو الحال في جرائم المعلوماتية السوداني (المادة 11)، وهذا من الأمور التي تحتاج لمراجعة؛ إذ كان حريٌّ بالمشرع أن يوسع من صلاحيات هذا النص فلا يربطه فقط بهذه الأمور المحددة. وبشكل عام يجب توقيع العقوبة حال تكييفها باعتبارها فعلًا غير قانوني وليس بربطها بآثار معينة تنشأ عن ارتكابها.

كما يمكن النظر إلى تضييق محددات الفعل الإجرامي وربطه بنمط محدد من الأفعال غير القانونية باعتباره إشكالية تستلزم المراجعة والبحث فيها، ومما تبدى في هذا الإطار، في حدود الدراسة، تركيز المشرع السوداني العقوبة في جرائم الاختراق على المساس بالمعلومات الأمنية والاقتصادية (مادة 7/ أ-ب)، ولم يشر إلى أي شكل آخر من أشكال البيانات والمعلومات. إن الإشكالية في هذا الصدد تكمن في فتح المجال لارتكاب بعض الجرائم المتصلة بالاختراق دون مساس بمرتكب الجريمة طالما خرجت عن نطاق ما تم تحديده، على حين تتطلب الجرائم الإلكترونية بكافة أشكالها ومستوياتها مواجهة حاسمة وناجزة وهذا يرتبط بنص قانوني حاسم وناجز يحقق الردع المطلوب في مثل هذه الجرائم الخطيرة.

هناك إشكالية خطيرة تتصل بالتكييف القانوني للجرائم وما يتصل به من تشديد للعقوبات، كما هو الحال عند الجمع بين جريمتين خاصة مع ما لهما من آثار شديدة الخطورة على الدول والمجتمعات، ومن ذلك أن جريمة انتحال الهوية عبر الإنترنت تتخذ أحد وجهين: انتحال هوية الفرد أو انتحال هوية المواقع، وقد يتم الجمع بينهما، وكذلك جريمة اختراق البيانات الشخصية والبيانات الحكومية، فقد يكون الشخص الطبيعي له بيانات شخصية ولكنها جزء من منظومة بيانات حكومية لما له من صفة اعتبارية في نفس الوقت، وهنا أيضًا تعتبر الجريمة جريمة مركبة، وهو الأمر الذي يستلزم اهتمام المشرع وتشديد العقوبة لمثل هذه الجرائم المركبة.

إن جرائم الاختراق والاعتراض والانتحال مثلها مثل باقي الجرائم الإلكترونية، تتخذ أنماطًا جديدة يومًا بعد يوم، وتتنوع آليات تنفيذها، وهذا يمثل إشكالية في كيفية تطوير

النص القانوني والصياغات القانونية المتصلة به بما يتماشى مع التطور الرقمي والذكاء الاصطناعي والقدرة على الاستعانة بهم في هذا المجال.

هناك إشكالية ترتبط بتحديد المفاهيم تحديدًا يحُول دون توسيع أو تضييق دائرة التجريم دون سند قانوني واضح، وبالنظر إلى نصوص القانون الإماراتي والسوداني والأردني فإننا سنجد غيابًا لتعريف محدد لمفهوم الاعتراض وما المقصود به تحديدا، وهو ما يميز القانون المصري، وبالمقارنة بين القوانين محل الدراسة نجد كذلك أن المشرع لم يضع بقانون الإمارات تعريفًا لجريمة الاختراق في نص القانون وكذلك فعل المشرع السوداني ومثله الأردني، وهو ما يميز القانون المصري في هذه الجزئية.

الخلاصة

- هناك نصوص قانونية متعددة وواضحة في التشريعات العربية في الدول محل الدراسة (مصر، الإمارات، السودان، الأردن) تتصل بمكافحة جرائم الاختراق والاعتراض والانتحال وتضعها بالفعل كأولى الجرائم التي تعمل على تحديد أركانها ومكافحتها، وذلك لخطورتها ولكونها من أهم الجرائم التي قد ينبني عليها في كثير من الأحوال باقي أشكال جرائم تقنية المعلومات، وإن كانت هناك بعض الاختلافات بين تلك النصوص بحسب رؤية المشرع في كل بلد، **ومما سبق وأوضحته النتائج تفصيلًا يمكن تلخيصه في رؤية تحليلية مقارنة كما يلي:**

- جريمة تجاوز حدود الحق في الدخول هي جريمة مهمة وموجودة في القوانين: المصري والإماراتي والأردني، وهي تعد نوعًا من أنواع الاختراق لتعديها الحدود الشرعية، ويتسق ذلك مع نص المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تنص على أن الدخول أو البقاء أو الاتصال غير المشروع هو جريمة في حد ذاتها، أما في القانون السوداني فلم يضمِّنها المشرع في القانون.
- يتميز القانون المصري بتوضيح حالات ارتكاب الجريمة الإلكترونية التي يترتب عليها المسئولية الجنائية لفاعلها بشكل أكبر من القوانين الأخرى؛ السوداني والإماراتي والأردني، ويتيح ذلك إمكانية أكبر لتضييق فرص الإفلات من الجريمة، وهو المطلوب من النص القانوني.
- وباستقراء وتحليل ما سبق يتضح أن القانون السوداني لم يجرِّم فعل الاختراق والدخول غير المصرح به وغير المشروع كفعل غير قانوني في حد ذاته- كما فعل المشرع في كل من القانون المصري والأردني والإماراتي- وإنما ربط المشرع العقوبة بالقيام بأفعال محددة.

- جاء التمييز للمعلومات أو البيانات الشخصية وتغليظ العقوبة في حال اختراقها وإتلافها رادعًا ومميزًا للقانون الاتحادي الإماراتي عن باقي القوانين التي لم تميز اختراق البيانات الشخصية بعقوبة خاصة بنص القانون.
- القوانين في كل من مصر والإمارات والأردن والسودان اهتمت بتجريم من يمتلك الأجهزة التي من خلالها يتم ارتكاب الجرائم وهو ما يعد إساءة استخدام لوسائل تقنية المعلومات، وذلك بما يتفق مع المادة التاسعة من الاتفاقية العربية لمكافحة تقنية المعلومات والتي تجرِّم حيازة أو إنتاج أو شراء أو استيراد أية أدوات أو برامج بغرض ارتكاب الجرائم الإلكترونية.
- القانون السوداني يركز العقوبة في جرائم الاختراق على المساس بالمعلومات الأمنية والاقتصادية ولم يشر إلى أي شكل آخر من أشكال البيانات والمعلومات، وهو في رأيي قصور في التشريع لأنه لا يعاقب على باقي أنواع البيانات التي يتم الحصول عليها بدون وجه حق أو تعطيلها وإفسادها، وكذلك اقتصر المشرع في جريمة الانتحال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة بربطها بغرض الاستيلاء على مال أو سند أو توقيع للسند، وكان حريٌّ به أن يعاقب عليها دون ربطها بأمر محدد فقط، وهو ما تفاداه المشرع في القوانين الأخرى.
- يعاقب القانون عقوبات مشددة في كل من مصر (م.31) والإمارات (م.3) والسودان (م.5) والأردن (م.8) على ارتكاب الجريمة بسبب تأدية الشخص لعمله، وهو بالتالي مبدأ معمول به في مختلف قوانين مكافحة جرائم تقنية المعلومات في الدول العربية محل الدراسة، وهو يتسق مع نظرية الردع والتي ترى بضرورة تدرج العقوبة مع طبيعة الجُرم وطبيعة مرتكبه.
- جاء التمييز للمعلومات أو البيانات الشخصية وتغليظ العقوبة في حال اختراقها وإتلافها مميزًا للقانون الاتحادي الإماراتي عن غيره، كما جاءت جريمة الحصول بدون تصريح على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات أو موقع أو غيره كجريمة غير متكررة في قوانين أخرى وتميز القانون الإماراتي وتحقق مزيدًا من الردع في مكافحة جرائم تقنية المعلومات.
  - من حيث شمول النص القانوني، فلقد جاءت النصوص القانونية- في تشريعات البلاد العربية محل الدراسة- شاملة ومستوفاة للأغلب الأعم من محددات كل جريمة من جرائم الاختراق والاعتراض والانتحال، إلا أن عدم وضع تعريف محدد جامع مانع للجرائم في قوانين الإمارات والسودان والأردن هو أمر يحتاج

لإعادة نظر من المشرع؛ إذ إنه من المعروف دومًا أن وضع التعريف المحدد والدقيق للجريمة يمنع إمكانية التحايل عليها أو الإفلات من العقوبة، وكذلك يؤدي إلى تيسير فهم الأفراد لسمات ومحددات الفعل الإجرامي بما يمنع وقوعهم في دائرة الجريمة عن غير فهم أحيانًا، كما أن القصور في توسيع بعض الجرائم وربطها فقط بأفعال محددة– كما سبقت الإشارة- يحتاج لإعادة نظر من المشرع حتى يتحقق الشمول المطلوب.

- من حيث وضوح النص القانوني، جاءت النصوص في التشريعات العربية محل الدراسة فيما يتصل بجرائم الاختراق والاعتراض والانتحال واضحة بدون غموض أو ألفاظ تحتمل دلالات مختلفة، وهو أمر شديد الأهمية، حتى لا يسمح بتحميل المعنى المقصود بالقانون معاني أخرى مما يسلبه قيمته وتأثيره المطلوب في مكافحة تلك الجرائم الخطيرة التي تهدد الفرد والمجتمع والوطن كله.
- آليات الردع من حيث صرامة العقوبات وتدرجها في الشدة في نصوص القوانين العربية، جاءت حاسمة ورادعة إلى حد كبير، وهو ما يتسق مع معطيات نظرية الردع وأسس علم العقاب، ولكن يمكن التفكير في تغليظ العقوبات أي تشديدها في حالة جرائم الانتحال في مختلف القوانين محل الدراسة خاصة أن تلك النوعية من الجرائم لها آثار شديدة الضرر والخطورة، فانتحال موقع رسمي لجهة حكومية أو جريدة معروفة أو منظمة دولية ووضع بيانات سرية عليها أو معلومات كاذبة أو أخبار ملفقة قد يحدث حالة من الفوضى أو الذعر، أو يؤدي لإثارة الرأي العام وقد يحدث صراعًا أو فتنًا بين الأفراد والمجتمعات والدول.
- نوع العقوبة كما جاءت في القوانين، ينحصر بشكل عام بين الحبس والسجن والغرامة؛ وبالتالي هي عقوبات متعددة ورادعة لتواجه مستويات الجريمة المتعددة لكل من جريمة الاختراق وجريمة الاعتراض وجريمة الانتحال، إلا أن المشرع السوداني لم يضع نصًّا صريحًا بمبلغ الغرامة في أي من النصوص المتصلة بالعقوبات المقررة وفقًا للقانون على ارتكاب الجرائم على عكس باقي القوانين.

مناقشة نتائج الدراسة:

- بشكل عام، خرجت التشريعات العربية محل الدراسة الخاصة بمكافحة جرائم تقنية المعلومات من عباءة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وجاءت نصوصها القانونية لتتسق إلى حد كبير مع نصوص هذه الاتفاقية، ويتضح من مجمل نتائج هذه الدراسة أن هناك توجهًا قويًا بالتشريعات العربية– محل الدراسة– بشكل عام لمكافحة الجرائم الإلكترونية، ومنها جرائم الاختراق والاعتراض والانتحال بفعالية.
- تحظى جرائم الاختراق والاعتراض والانتحال على وجه التحديد بالفعل باهتمام المشرع العربي، وهو ما يتسق مع خطورة هذه الجرائم ومع ما يترتب عليها من تبعات مدمرة وخطيرة ومع التوجه العالمي المستحدث في كل بلاد العالم؛ لضبط محددات تلك الجرائم ومكافحتها بنصوص قانونية حاسمة وواضحة.
- وكما أوضحت النتائج التحليلية والمقارنة لقوانين البلاد العربية فيما يتصل بعقوبات جرائم الاختراق والاعتراض والانتحال وغيرها من جرائم تقنية المعلومات، فلقد دلت النصوص القانونية المخصصة للعفو وتخفيف العقوبة على اهتمام المشرع بعدم التعسف في الحالات التي لا تتطلب تشديدًا أو تعسفًا مثل الاعتراف من قبل مرتكب الجريمة أو عدم وقوع الجريمة فعليًا، وهذا الأمر كما ترى الباحثة يعد من باب السياسة الجنائية غير المتشددة، وهو أمر يشجع على التراجع عن إتمام الجريمة والتفكير في الإبلاغ عن أي جريمة ومرتكبيها بما يسهم في الحد من تلك الجرائم فعليًا.
- المساهمة الجنائية (بمعنى اشتراك أكثر من فرد في أكثر من عمل متصل بإتمام الجريمة الإلكترونية) كانت أحد أهم توجهات المشرع الواضحة في صياغة الجريمة والعقوبة في كل القوانين محل الدراسة، وهو أمر مهم فيما يتصل بمواجهة ومكافحة مثل تلك الجرائم؛ لأنه لا يعفي أحدًا من فعل أسهم به في أن تتم الجريمة بالفعل حتى لا يفلت أحد من الجريمة.
- تتسق التشريعات الخاصة بجرائم الاختراق والاعتراض والانتحال في البلاد العربية وما ورد بشأنها في الاتفاقية العربية مع التطور في ما يتعلق باتفاقيات تنظيم الإجرام المعلوماتى، ومن ذلك اتفاقية بودابست Convention sur la cyber criminalite, Budapest والتى جاءت (2001) كرد فعل من المجلس الأوروبي إزاء الإجرام المعلوماتي والاستخدامات غير المشروعة لشبكات

المعلومات، ولمواجهة التغيرات التى حدثت بسبب التوجه الحديث نحو الرقمنة، وتُلزم مواد تلك الاتفاقية الدول الأعضاء باتخاذ الإجراءات اللازمة لمواجهة جرائم المعلومات والاستخدامات غير المشروعة لشبكات المعلومات، وذلك على النحو التالى:

- الدخول غير القانونى المتعمد إلى أى نظام معلوماتى.
- التدخل المتعمد في المعطيات بتدميرها أو حذفها أو إفسادها أو تشويشها أو تعديلها.
- الاعتراض غير القانونى المتعمد بواسطة وسائل تكنولوجية للبيانات المرسلة.
- التدخل المتعمد في الأنظمة لتعطيل أداء وعمل الأنظمة.
- إساءة استخدام الأجهزة.
- التزوير المتعمد باستخدام الحاسوب بإدخال أو حذف أو إخفاء بيانات الحاسوب.
- الاحتيال المتعمد باستخدام الحاسوب على نحو يسبب خسارة الغير لممتلكاته.
- الجرائم المرتبطة بحق المؤلف.

- هناك خلاف بين بعض الدراسات فيما يتصل بالعقوبات المتصلة بجرائم الاختراق والاعتراض والانتحال، فهناك من يرى أهمية العقوبات المشددة ومن ثم يطالبون بمزيد من القيود والعقوبات المغلظة ومزيد من النصوص القانونية التى توضح الجريمة وتشرح كافة عناصرها وآليات الضبط والمكافحة، ومن ذلك دراسة رغدة البهى (2018) ودراسة عبدالله داغش العجمى (2014)، في مقابل الرأى الآخر والذى يرى ضرورة التوجه نحو عدم تشديد العقوبات ومن ثم يطالبون بمزيد من تخفيف القيود مثل دراسة سعيد الحديدى (2017) ودراسة إيناس محيى الدين (2017)، **والباحثة ترى** أن القانون فيما يتعلق بتشديد العقوبات في بعض الحالات هو الأنسب؛ لأنه يوضح كيف أن بعض الحالات يجب أن تكون سببًا لتشديد العقوبة وهذا من باب الردع المطلوب أمام مثل تلك الأفعال.

حدود الدراسة وما تثيره من أفكار بحثية:

اهتمت هذه الدراسة بموضوع محدد ومهم في عصر التحول الرقمي وما نشهده حاليًا من التطورات التكنولوجية وإساءة استخداماتها أحيانًا ألا وهو "محددات المسئولية الجنائية عن جرائم الاختراق والاعتراض والانتحال كما وردت بالنصوص التشريعية في البلاد العربية"، وكيفية مواجهة تلك الجرائم كما ورد بنصوص التشريعات العربية المختلفة محل الدراسة، وتقييم الأطر التشريعية الضابطة في الدول العربية والمقارنة بينها من حيث شمول النصوص ووضوحها وآليات الردع ونوعية العقوبة، وما إذا كانت التشريعات تضع ظروفًا استثنائية وماهية أوجه الشبه والاختلاف بين البلاد العربية محل الدراسة (مصر، والإمارات والأردن والسودان) في هذه الأمور القانونية.

وفي ضوء البحث المتواصل في الاستخدامات غير المشروعة لمواقع التواصل الاجتماعي والقوانين المتصلة بها بشكل عام لمكافحتها يتضح أيضًا أن هناك أفكارًا بحثية مهمة وجديرة كذلك بالبحث والدراسة في السياقات المتصلة بالجريمة الإلكترونية، ومن ذلك:

- دراسة كل ما يتصل بجريمة إنشاء المواقع الإباحية وارتكاب جرائم الآداب العامة بواسطة مواقع التواصل الاجتماعي، باعتبارها من أخطر الجرائم الإلكترونية، ومدى استخدامها بين الجمهور ومستخدمي مواقع التواصل الاجتماعي، وتأثيراتها على المجتمعات العربية والشباب والعقوبات المتصلة بها في القوانين العربية ومقارنتها بغيرها من القوانين في أنظمة قانونية مختلفة بالعالم.
- بحث الجرائم المتصلة بإثارة الفتن وتأليب الرأي العام والتحريض، واستخدام خطاب الكراهية ضمن الخطاب المتبادل، وماهية التشريعات الضابطة لذلك سواء في بلادنا العربية أو في البلاد الأجنبية المختلفة.
- إجراء بحوث تتعلق بكيفية ضبط التشريعات المتصلة بأشكال اختراق الخصوصية ورصد وتوصيف محددات تلك الجريمة في التشريعات المختلفة، ويمكن إجراء دراسات تتبعية طولية أي ترصد وتوصف اختلافات ومحددات وعقوبات تلك الجريمة عبر الفترات الزمنية المختلفة، وكذلك إجراء دراسات مقارنة في نفس الفترة الزمنية بين أكثر من دولة.
- يمكن أيضًا في هذا الصدد التفكير في دراسات وبحوث تتصل تحديدًا بالخبراء والمشرِّعين والقائم بالاتصال في البلاد العربية؛ من أجل تقييم النص القانوني وتطويره وفقًا لواقع الممارسات المهنية وواقع التطورات التكنولوجية وتطور الاستخدامات غير المشروعة للمواقع الإلكترونية ومواقع التواصل الاجتماعي.

توصيات الدراسة:

- من الأهمية بمكان رفع مستوى وعي المستخدمين لوسائل التواصل الاجتماعي حتى لا يتحولوا إلى مرتكبي جرائم أو ضحايا لجرائم إلكترونية دون علمهم بذلك، وهو ما يتطلب مزيدًا من الاهتمام في كافة المدارس والجامعات وجهات العمل المتعددة بعمل دورات تدريبية أو ورش عمل لشرح وتوضيح كل ما يتصل بالجرائم الإلكترونية.
- ويرتبط بما سبق **ضرورة الاتجاه نحو تعميم تدريس التربية الرقمية** للأطفال والشباب، والعمل على نشر التربية الرقمية كمنهج يتسق مع التطورات التكنولوجية وواقع الظروف الحالية في الألفية الثالثة؛ وذلك لتفادي الوقوع تحت طائلة التجريم.
- الانتباه إلى ضرورة تدريس مواد تكنولوجيا الاتصال وأسس البرمجة والجرائم الإلكترونية إلى كل طلاب الإعلام والشرطة والحقوق والهندسة؛ لأنها أصبحت ضرورة ملحة في ظل تزايد الجرائم الإلكترونية، وأهمية رفع الوعي وتنمية المهارات الخاصة بالتعامل مع تلك الجرائم الإلكترونية لكل الجهات التي تعمل بمجال الاتصالات وما قد ينجم عنه من جرائم.
- من المهم وجود نص بكافة تشريعات مكافحة الجرائم الإلكترونية يلزم مديري تحرير المواقع بإبلاغ مزودي خدمات الاستضافة بعناوين المستخدمين والأسماء الخاصة بالبريد الإلكتروني عند فتح الصفحة الشخصية لهم، وتعهد المستخدم بصحة هذه البيانات وتحذيره رسميًا بأن استخدام اسم غير حقيقي أو هوية مزورة (الانتحال) يعرضه للمساءلة القانونية والعقاب، وهذا من شأنه الحد من جريمة الانتحال بما يترتب عليها من تبعات خطيرة على الفرد والمؤسسات والدولة.
- من الضروري إضافة التعريف الجامع المانع للجرائم بالقوانين التي لا تتضمن تعريفًا واضحًا ومحددًا لهما، الأمر الذي يمنع الوقوع في الخلط بين كل جريمة والأخرى، وبما يوضح محددات كل جريمة حتى لا يقع فيها بعض الأفراد عن جهل بها.
- من الأهمية بمكان التفكير الجمعي بشكل دائم بين البلاد العربية فيما يتصل بتوحيد التجريم والعقاب وآليات المتابعة القانونية لمثل هذه الجرائم الإلكترونية، والاستمرار في ذلك بناء على ما ورد بنص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات؛ وذلك من أجل ضبط استخدام الإنترنت ووقف كافة أشكال التجاوزات والجرائم الإلكترونية الموجودة حاليًا وما يستجد منها، وذلك يحتاج لمناقشات ومؤتمرات واجتماعات تتم بين ممثلين عن كافة الدول العربية من القانونيين وخبراء التكنولوجيا.

- نحتاج إلى مزيد من الدراسات في هذا المجال تهتم ببحث كافة أشكال الجريمة الإلكترونية وتبعات ارتكابها وآليات المواجهة، بحيث لا يكون ذلك على مستوى بلادنا العربية؛ وإنما في ضوء مقارنات مع عدد من الدول الأجنبية المختلفة بحيث تتحقق أقصى إفادة من رؤية ومعرفة نصوص القوانين المختلفة، وبناء عليه يسهل اكتشاف ومتابعة الجرائم الإلكترونية والحد من آثارها السلبية على الأفراد والمجتمعات والأوطان.
- أقترح أن تكون مادة الجريمة الإلكترونية أو جرائم تقنية المعلومات أحد المواد الأساسية بالجامعات المصرية لأهميتها؛ ولأنها ليست فقط من اختصاص طلاب كليات الإعلام والحقوق والشرطة؛ بل إن من حق كل طالب من الطلاب أن يعي أركان تلك الجرائم، وكيف يحمي نفسه من الوقوع فيها، وعقوباتها المقررة وفقًا للقوانين وكيفية مكافحتها.

قائمة المصادر والمراجع:

أولًا: المصادر:

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشئون القانونية، 2010.
- قانون مكافحة جرائم تقنية المعلومات "القانون رقم 175 لسنة 2018" (جمهورية مصر العربية)، الجريدة الرسمية، العدد 23 مكرر (ج)، السنة الحادية والستون،3 ذي الحجة سنة 1439ه، الموافق 14 أغسطس سنة 2018م.
- مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات (الإمارات العربية المتحدة)، الجريدة الرسمية، العدد 540، ملحق السنة الثانية والأربعون، 26 أغسطس 2012.
- قانون اتحادي رقم 12 لسنة 2016 بتعديل المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن جرائم تقنية المعلومات،23 مايو 2016، البوابة الرسمية لحكومة الإمارات العربية المتحدة.
file:///C:/Users/Dell/Downloads/Cyber%20Law.pdf
- المرسوم بقانون اتحادي رقم 2 لسنة 2018 الخاص باستبدال نصوص المواد (26) و(28) و(42) من المرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد 633، السنة 48،31 يوليو 2018.
- قانون جرائم المعلوماتية رقم 13 لسنة 2007 (السودان)، وزارة العدل، جمهورية السودان.
- https://www.moj.gov.sd/sudanlaws/#/reader/chapter/266
- قانون الاتصالات لسنة 2001 (جمهورية السودان).
- قانون الجرائم الإلكترونية رقم 27 لسنة 2015، الأردن، الجريدة الرسمية، 4 مايو 2015.

ثانيًا: الهوامش

(1) Russell G. Smith, Peter Grabosky, and Gregor Urbas, Cyber Criminals on Trial, Cambridge University Press, 2004, p. 7.

(2) Weiping Chang, Wingyan Chung, Hsinchun Chen and Shichieh Chou, 'An International Perspective on Fighting Cybercrime', Intelligence and Security Informatics Lecture Notes in Computer Science, vol. 26 (2003): p.p. 379-384.

(3) Liviu- Cosmin Vasilescu, Illegal interception of computer data transmission in the regulation of the New Romanian criminal code, Journal of law and administrative science, No.3, 2015, p.230.

(4) Annegret Bendiek &Tobiaz Metzger ,Deterrence theory in the cyber-century , Research Division EU/Europe Stiftung Wissenschaft und Politik German Institute for International and Security Affairs ,p. 3 ,2015.

(5) فوزية عبد الستار، مبادئ علم العقاب، (دار النهضة العربية، القاهرة ،1992)، ص 3.

(6) Cesar Beccaria, on crimes and punishments (Henry Paolucci trans., Macmillan 1986 (1764), taken from Raymond Paternoster, how much do we really know about criminal deterrence, Journal of Criminal law and criminology, vol.100, issue3, Summer 2010, p.p.765- 824.

(7) David Maimon, Deterrence in cyberspace: An interdisciplinary review of the empirical literature ,2020. In: Holt T., Bossler A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham.

(8) Anthony A.Braga , and L. Weisburd David. "The effects of focused deterrence strategies on crime: A systematic review and meta-analysis of the empirical evidence." Journal of Research in Crime and Delinquency 49, no. 3 (2012): 323-358.

(9) رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018، ص ص 201- 234.

(10) سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018، ص ص 235-258.

(11) إيناس محيي الدين عبد المعطي، حدود المسؤولية المدنية عبر وسائل النشر الإلكتروني، بحث مقدم إلى مؤتمر "القانون والإعلام"، كلية الحقوق، جامعة طنطا، 23-24 أبريل 2017.

(12) دينا عبد العزيز فهمي، المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، بحث قدم إلى المؤتمر العلمي الرابع بعنوان "القانون والإعلام"، كلية الحقوق، جامعة طنطا، 23-24 أبريل 2017.

(13) سعيد حموده الحديدي، تحديات التنظيم القانوني لحرية الاتصال بالإنترنت: دراسة مقارنة، بحث مقدم إلى مؤتمر "القانون والإعلام"، كلية الحقوق، جامعة طنطا، 23-24 أبريل 2017.

(14) Kimberly Pavlik, Cybercrime, Hacking, And Legislation, Journal of Cyber security Research, Vol. 1, N. 1, p.p. 13-16, 2017.

(15) بوقرين عبد الحليم، المسئولية الجنائية عن الاستخدام غير المشروع لمواقع التواصل الاجتماعي: دراسة مقارنة، مجلة جامعة الشارقة للعلوم القانونية، المجلد 16، العدد1، يونيو2014، ص ص 373-403.

(16) Qiwanyun Wang, A comparative study of cybercrime in criminal law: China, US, England, Singapore and the council of Europe, Erasmus Rotterdam University, PhD, 2016.

(17) Renger Sabillon , Jeimy Cano ,Victor Cavaller ,Jordi Serpa, Cybercrime and cybercriminals: A comprehensive study, International Journal of computer networks and Communication security, Vol. 4, no. 6, June 2016, p.p.165–176.

(18) عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2014.

(19) حسين ربيع وجمال زين العابدين أمين، إشكاليات التنظيم القانوني للمسئولية الجنائية عن النشر الإلكتروني في مصر، المجلة المصرية لبحوث الرأي العام، كلية الإعلام، جامعة القاهرة، المجلد 18، العدد4، الخريف 2019، ص ص119-163.

(20) رائد محمد فليح النمر، حماية خصوصية مستخدمي مواقع التواصل الاجتماعي على ضوء التشريعات في مملكة البحرين، مركز جيل البحث العلمي، سلسلة كتاب أعمال المؤتمرات، عدد خاص بالملتقى الدولي (الخصوصية في مجتمع المعلوماتية– لبنان)، العام السابع، العدد 26، يوليو 2019، ص ص 87-107.

(21) حمدي محمد محمود حسين، المسئولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، برلين، المجلد 2، العدد 8- أبريل نيسان، 2018، ص ص 1-33.

(22) محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، مجلة كلية الحقوق، جامعة بنها، العدد الثالث والثلاثون– الجزء الرابع، 2018، ص ص 1926-2057.

(23) Asherry Magalla, Prevention and detection of cybercrimes in Tanzania as described by the Cyber Crime Act, No. 13 of 2015, SSRN Electronic Journal ,2018.

(24) Nazura Abdul Manap & Others, Cyberspace identity: An overview, Mediterranean Journal of social sciences, vol.6, n.4 ,2015, p.p. 290-299.

(25) خالد حامد مصطفى، المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي، مجلة رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، المجلد 1، العدد2، مارس ٢٠١٣، ص ص8-45.

(26) انظر في ذلك (على سبيل المثال):
- إيمان محمد حسني عبد الله، آليات التضليل الإعلامي في الخطاب الخبري للصفحات الزائفة المنتحلة لأسماء الصحف المصرية على شبكة الفيسبوك، دراسة حالة على صفحتي اليوم السابع والبوابة الزائفتين، المجلة المصرية لبحوث الرأي العام، 2019، العدد18، الإصدار 1، ص ص 1-50.
- أميرة محمد، اتجاهات النخبة نحو تأثير مواقع التواصل الاجتماعي على الأمن القومي المصري، رسالة دكتوراه، كلية الآداب، جامعة دمياط، 2016.

(27) Mike Mc Conville & Wing Hong Chui, Research methods for law, Edinburgh, Edinburgh University press, 2007, p.p.18-19.

(28) Philip Langbroek and others, Methodology of legal research: Challenges and opportunities, Utrecht law review, Volume 13, Issue 3, 2017, p.2.

(29) أصدرت الإمارات أول قانون مخصص لجرائم تقنية المعلومات في عام 2006 ثم تم تعديله وتطويره ثلاث مرات في أعوام 2012 و2016 و2018 (القانون رقم 5 لسنة 2018 لمكافحة جرائم تقنية المعلومات) المعمول به حاليًا.

(30) أصدرت السودان أول قانون مخصص لمكافحة جرائم تقنية المعلومات في عام 2007 ثم تم إضافة بعض التعديلات له في العام 2018.

(31) أصدرت الأردن قانون لمواجهة جرائم المعلومات عام 2010 وكان قانونًا مؤقتًا تم تحويله ليصبح قانونًا دائمًا عام 2015.

(32) راجع ذلك في:
- عبد الواحد كرم، معجم المصطلحات القانونية، ط1، (القاهرة، دار الكتب القانونية ،1995)، ص 445.
- محمود نجيب حسني، علم العقاب، (دار النهضة العربية، القاهرة ،1966).
-أحمد فتحي سرور، أصول السياسة الجنائية، (دار النهضة العربية ،1972).

(33) أحمد فتحي سرور، السياسة الجنائية (فكرتها ومذاهبها وتخطيطها)، د. ن ،1969، ص ص6-7.

(34) أحمد حسن عبد العليم، الجرائم المعلوماتية الواقعة عبر مواقع التواصل الاجتماعي، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، برلين، العدد 6، تشرين الأول- أكتوبر، 2019، ص ص 109-129.

(35) عمرو عيسي الفقي، الجرائم المعلوماتية- جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، 2006، ص 102.

(36) صغير يوسف، الجريمة الإلكترونية عبر الإنترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص ص 31-32.

(37) عمر بن محمد العتيني، الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية، رسالة دكتوراه، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، الرياض، 2010، ص ص 49-50.

Journal of Mass Communication Research «J M C R»

A scientific journal issued by Al-Azhar University, Faculty of Mass Communication

Chairman: Prof.Ghanem Alsaaed

Dean of the Faculty of Mass Communication, Al-Azhar University

Editor-in-chief:Prof. Reda Abdelwaged Amin

Vice Dean, Faculty of Mass Communication, Al-Azhar University

Assistants Editor in Chief:

Prof. Arafa Amer

- Professor of Radio,Television, Faculty of Mass Communication, Al-Azhar University

Prof.Fahd Al-Askar

- Vice-President of Imam Muhammad bin Saud University for Graduate Studies and Scientific Research (Kingdom of Saudi Arabia)

Prof.Abdullah Al-Kindi

- Professor of Journalism at Sultan Qaboos University (Sultanate of Oman)

Prof.Jalaluddin Sheikh Ziyada

- Dean of the Faculty of Mass Communication, Islamic University of Omdurman (Sudan)

Managing Editor: Dr.Mohamed Fouad El Dahrawy

Lecturer at Public Relations and Advertising Department, **Faculty of Mass Communication, Al-Azhar University**

Editorial Secretaries:

Dr. Ibrahim Bassyouni: Lecturer at Faculty of Mass Communication, Al-Azhar University

Dr. Mustafa Abdel-Hay: Lecturer at Faculty of Mass Communication, Al-Azhar University

Dr. Ramy Gamal: Lecturer at Faculty of Mass Communication, Al-Azhar University

Arabic Language Editor : Omar Ghonem: Assistant Lecturer at Faculty of Mass Communication, Al-Azhar University

Designed by: Mohammed Kamel - Assistant Lecturer at Faculty of Mass Communication, Al-Azhar University

Correspondences

- Al-Azhar University- Faculty of Mass Communication.
- Telephone Number: 0225108256
- Our website: http://jsb.journals.ekb.eg
- E-mail: mediajournal2020@azhar.edu.eg

Issue 56 January 2021 - part 3

Deposit - registration number at Darelkotob almasrya /6555

International Standard Book Number "Electronic Edition" 2682- 292X

International Standard Book Number «Paper Edition»9297- 1110

Rules of Publishing

Our Journal Publishes Researches, Studies, Book Reviews, Reports, and Translations according to these rules:

- Publication is subject to approval by two specialized referees.
- The Journal accepts only original work; it shouldn›t be previously published before in a refereed scientific journal or a scientific conference.
- The length of submitted papers shouldn›t be less than 5000 words and shouldn›t exceed 10000 words. In the case of excess the researcher should pay the cost of publishing.
- Research Title whether main or major, shouldn›t exceed 20 words.
- Submitted papers should be accompanied by two abstracts in Arabic and English. Abstract shouldn›t exceed 250 words.
- Authors should provide our journal with 3 copies of their papers together with the computer diskette. The Name of the author and the title of his paper should be written on a separate page. Footnotes and references should be numbered and included in the end of the text.
- Manuscripts which are accepted for publication are not returned to authors. It is a condition of publication in the journal the authors assign copyrights to the journal. It is prohibited to republish any material included in the journal without prior written permission from the editor.
- Papers are published according to the priority of their acceptance.
- Manuscripts which are not accepted for publication are returned to authors.