دور دولة الكويت ودول الخليج العربي في مكافحة الجرائم التقنية

أ. عبدالله مزيد سعد العازمي

د.نسيمة بنت حسين

قسم القانون- كلية أحمد إبراهيم للحقوق- الجامعة الإسلامية العالمية – ماليزيا

Role of Kuwait and Arab Gulf States in combating technical crimes

Mr. Abduallah Mazid Saad Alazmi

Dr. Nassima bint Hussein

Department of Law, Faculty of Ahmed Ibrahim for Law, International Islamic University, Malaysia

ملخص البحث:

يهدف هذا البحث إلى معرفة ما هو دور دولة الكويت اقليميا في مكافحة جرائم تقنية المعلومات وخصوصا جرائم التواصل الاجتماعي، وكذلك لمعرفة دور دول مجلس التعاون في مكافحة جرائم تقنية المعلومات وخصوصا جرائم التواصل الاجتماعي، من خلال استخدام المنهج الوصفي لوصف ظاهرة الجرائم التقنية والمنهج التحليل لتحليل تلك البيانات والمعلومات وتوصل الباحث إلى عدة نتائج من أهما: أن دول مجلس التعاون واجهت صعوبات في تعريف الجريمة وتكيفها وما هو القانون المناسب لها، وواجهت أيضا صعوبات في تطبيق التشريعات على الجرائم التقنية حيث هناك اختلاف في شكل الجريمة ونوعها، وأن دول مجلس التعاون ركزت على المواجهة الفكرية لهذه الجرائم.

الكلمات المفتاحية: الكويت، مجلس التعاون، مكافحة، الجرائم التقنية.

Abstract:

This article aims to get to know the national role of Kuwait and other Arab Gulf States in combating the technical and Information Technology (IT) crimes, especially those concerning social media. The study employs the descriptive approach to describe the phenomenon under study and the descriptive approach to analyze the data. The study concludes with a number of findings, the most important of which are: Arab Gulf States have faced difficulties in defining this type of crime and the type of the suitable law to deal with it. They have also faced difficulties in applying the regulations to IT crimes, as there is a difference in the form and type of this type of crime. Arab Gulf States focused on intellectual combating of these crimes.

Keywords: Kuwait, Arab Gulf States, IT crimes.

المقدمة:

تعد الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم، وتعتبر ثورة الاتصالات هي المحرك الأساسي في التطورات الحادثة في الوقت الحالي، إلا أنها ليست المحرك الوحيد في هذه التطورات، حيث أن التطور الكبير في تكنولوجيا الحاسبات قد أسهم بصورة كبيرة في تسارع معدلات التقدم في مجال الاتصالات والمعلومات.

إنّ الاستخدام الكبير لِلأنظمة التكنولوجية قاد إلى الكثير من المنافع والفوائد بجانب المشاكل والمِخاطر، وقدّم أصنافاً من الجرائم لم تكن مُتداولةً سابقاً، سُمّيت بالجرائم التقنية ، وتختلف هذه الجرائم باختلاف الهدف منها والمستهدف فيها وطرق استخدامها، والمكان والدولة التي تنطلق منها هذه الجرائم، وقد كان للدول المتقدمة قوانين واجراءات تحاول الحد من هذه الجرائم ومنعها ومعاقبة مرتكبيها، ومن هذه الدولة دول الخليج العربي الذي سعت إلى تعريف هذه الجرائم وسن القوانين والاجراءات للحد منها، ويحاول هذا البحث تسليط الضوء على دور دولة الكويت ودول الخليج العربي في مكافحة الجرائم التقنية.

مشكلة البحث:

تتمثل مشكلة البحث في عدم وجود رؤية واضحة لدى دولة الكويت و دول التعاون في مواجهة الجرائم التقنية، الواقعة بواسطة التواصل الاجتماعي، حيث لم يوجد تشريع قانوني في أي من تلك الدول يكافح تلك الجرائم التقنية اقليما مما حدا بالباحث القيام بها البحث محاولة منه لإجاد حل مناسب لتلك المشكلة.

هدف البحث :

يهدف الباحث في بحث إلى الآتي :

- معرفة ما هو دور دولة الكويت اقليميا في مكافحة جرائم تقنية المعلومات وخصوصا جرائم التواصل الاجتماعي.
- معرفة دور دول مجلس التعاون في مكافحة جرائم تقنية المعلومات وخصوصا جرائم التواصل الاجتماعي.

سبب اختيار البحث :

اختار الباحث بحثه بعنايه للأسباب التالية :

- ألتمس الباحث من خلال الواقع آثار تلك الجرائم التقنية وخصوصا جرائم تقنية المعلومات على الحكومات والأفراد.
- معرفة دور الدول في مكافحتها واختار دولة الكويت لأنها موطن الباحث.

- معرفة دور دولة الكويت في مكافحة تلك الجرائم اقليميا أي في دول المجلس التعاون لأنه يعتبر ذلك اقليم الباحث.
- معرفة دور دول مجلس التعاون في مكافحة هذه الجرائم.
- معرفة مدى التعاون الاقليمي من خلال تشريعاتهم لمكافحة جرائم تقنية المعلومات.

منهج البحث :

استخدم الباحث المنهج الوصفي في جمع البيانات والقوانين والمفاهيم النظرية وسعى إلى تحليلها ونقدها.

الدراسات السابقة :

- **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها:** إعداد مركز البحوث والدراسات سلطنة عُمان، أكاديمية السلطان قابوس لعلوم الشرطة، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥م، ٢٠١٦م.
- **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها،** مداوي القحطاني، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥م، دولة قطر، ٢٠١٦م.

اختلف بحث الباحث عن هذه **الدراسات (السابقة)** حيث كانت الدراسات السابقة كانت ذكر المعلومات و أغلبها سطحية دون التعمق فيها بينما **هذا البحث** تطرق لما تحتويه تلك الاستراتيجية وخصوصا استراتيجية دولة الكويت بتعمق مع الانتقاد احيانا والآراء ايضا.

خطة البحث :

اقتضت طبيعة البحث أن يشمل مقدمة وتمهيد ومبحثين وخاتمة.

المقدمة وفيها: مشكلة البحث، أهداف البحث، وأسباب اختيارها، ومنهج البحث، والدراسات السابقة.

التمهيد : وفيه

- الاثار السلبية للجرائم التي تقع عبر وسائل التواصل الاجتماعي.
- الصعوبات التي واجهة دول مجلس التعاون لمكافحة جرائم تقنية المعلومات
- التحديات التي واجهة دول مجلس التعاون لمكافحة جرائم تقنية المعلومات

المبحث الأول: عقد المؤتمرات وإنشاء مراكز لمكافحة جرائم تقنية المعلومات والأمن السيبراني.

المطلب الأول: المؤتمرات.

المطلب الثاني: إنشاء المراكز الوطنية للأمن السيبراني.

المطلب الثالث : القوانين والتشريعات الخليجية في مكافحة الجرائم التقنية.

المبحث الثاني : استراتيجية دول مجلس التعاون في مكافحة جرائم التواصل الاجتماعي

المطلب الاول: إدارة الأزمات الأمنية.

المطلب الثاني: الاهتمام بالأمن الفكري.

الخاتمة وفيها النتائج والتوصيات.

التمهيد:

لدولة الكويت وكذلك دول مجلس التعاون الخليجي دوراً بارزا في مكافحة الجرائم التقنية، ويشمل ذلك الجرائم التي تقع عبر وسائل التواصل الاجتماعي، حيث إن هذه الوسائل لها تأثير ومساهمة في تفشي الفساد وخصوصا الأسري حيث كان لهذه الوسائل آثار سلبية منها:[١]

١. اختلاط الثقافات والقيم الأخلاقية.

٢. انتشار العولمة التقنية التي هي سبب رئيسي لهذه البرامج.

٣. صعوبة بل عدم القدرة على السيطرة على مستخدمي برامج التواصل الاجتماعي وهذا أثر عشناه في واقعنا وما زال بعض البلدان تعاني منه وهو ما عرف بالربيع العربي حيث صعب على الحكومات السيطرة على وسائل التواصل الاجتماعي التي تعتبر بؤرة التواصل بين المتظاهرين وقد استفادت القنوات الإخبارية بنشر أخبارها من تلك الوسائل، واستفادت من المعلومات التي ينشرها المستخدمون، فأصبحت الحكومات غير قادرة على ملاحقة الجميع وكان الحل الأمثل هو قطع هذه البرامج عن المتظاهرين، لكي توقف استخدام وسائل التواصل الاجتماعي[٢].

وقد واجهت دول مجلس التعاون الخليجي عدة صعوبات وتحديات لمكافحة هذه الجرائم وهي كالآتي:

أولاً: صعوبة تكييف هذه الجريمة ومدى تطبيق القانون عليها، حيث إن الدستور الكويتي نص في المادة ٣٢[٣] على أنه لا جريمة ولا عقوبة إلا بنص، أي أن المشرع قد أخذ بمبدأ المشروعية لجميع الأعمال، إذ إن الجرائم المستحدثة لا يتم معاقبة الفاعل إلا على نص يبين أنها جريمة ومعاقب عليها، لكن هذه الجرائم اقترنت بأفعال مطابقة للواقع كالقذف عبر وسائل التواصل الاجتماعي.

ثانياً: أن الجريمة الإلكترونية عابرة للحدود فمن المعروف أنها إذا وقعت الجريمة داخل إقليم الدولة يطبق عليها قانون تلك الدولة لكن لو كان الفعل بدولة ووقوع اثرها بدولة أخرى، فإنه يؤثر على اختصاص تطبيق القانون للدول.(٤)

ثالثاً: أن النصوص التشريعية الموجودة تعتبر غير كافية لهذه الجرائم؛ لأن هناك جرائم لم يتم النص عليها، كجريمة الدخول غير المشروع لموقع إلكتروني إضافة إلى ما يتم استخدامه كأداة للجريمة وهي الوسائل التقنية، إذ إن من يستخدمها عادة شخص ذو ذكاء أي أنه عالم بأنه مرتكب للجريمة.

رابعاً: أن النصوص التشريعية غير واضحة لمثل هذه الجرائم أي أنه لا بد من تكون هناك نصوص واضحة يستطيع القاضي أن يحكم عليها دون أن يكون فيها شك، فالشك غالباً ما يفسر لصالح المتهم.

ونعود إلى مشكلة الاختصاص، إذ إن جرائم التواصل الاجتماعي عابرة للحدود، إذ قد يكون هناك خطأ إجرائي قد يسبب ببطلان الحكم الجزائي للمجرم، فقوانين دول مجلس التعاون تنص على إقليم الجزاء للدولة لكن هناك جرائم قد نص بعض قوانينهم على أن يمتد الإقليم الجزائي في حال كانت هذه الجرائم تمس أمن الدولة، وهناك قوانين تنص على مبدأ الصلاحية الشخصية، أي يطبق القانون على كل من يحمل الجنسية إذا ارتكب فعلاً مجرماً ومعاقباً عليه، كما هناك مبدأ الصلاحية العالمية إذ يتم ملاحقة مجرمين المخدرات والاتجار بالبشر بناءاً عليه.

والحلول التشريعية التي قامت بها دول مجلس التعاون الخليجي لمكافحة الجرائم الإلكترونية كباقي الدول غير كافية لمكافحة الجرائم الإلكترونية، حيث تعد هذه الجرائم ذات تطور تقني وبصورة جديدة للواقعة عبر هذه الوسائل، حيث تمثلت هذه الحلول بوضع قوانين تشريعية وأيضاً إقامة مؤتمرات في مجال مكافحة جرائم تقنية المعلومات أو ما يسمى بالأمن السيبراني.

المبحث الاول: عقد المؤتمرات وإنشاء مراكز لمكافحة جرائم تقنية المعلومات والأمن السيبراني.

المطلب الاول: المؤتمرات:

عقدة عدة مؤتمرات في دول مجلس التعاون الخليجي ومنها:

١. مؤتمر أبوظبي العالمي للأمن السيبراني(٥) تحت عنوان " التهديدات الوطنية والمشتركة – الحماية والتعليم ٢٠١٤م، حيث عقد هذا المؤتمر في أبوظبي وكان بتمويل ومشاركة كل من الكلية العالمية للتكنولوجيا (أبوظبي) ومعهد نيويورك للتكنولوجيا، وناقش هذا المؤتمر التهديدات الإلكترونية في مجال

الاقتصاد والأمن والجانب الاجتماعي، ووسائل الحماية منها، كما استعرض الخبرات في هذه المجال والتدريب لمكافحة هذه الجرائم.

٢. مؤتمر الأمن السيبراني في مسقط (عُمان) ٢٠١٤م عقد هذا المؤتمر وذلك لأهمية الأمن السيبراني ولتزايد مستخدمي تقنية المعلومات، حيث أصبح من الضروري مكافحة الجرائم الإلكترونية في المنطقة وطرق الحماية منها، ومن مخرجات هذا المؤتمر تكوين لجان ذات خبرة عالية في الأمن السيبراني من القطاعات الحكومية مثل وزارة الدفاع وغيرها من الإدارات وكان الغرض منها تحديد التحديات والتهديدات الأمنية وطرق مواجهة تلك التحديات والتهديدات.

٣. المؤتمر الإقليمي الثالث للأمن السيبراني مسقط (عُمان) ٢٠١٤م أقيم هذا المؤتمر تحت مظلة هيئة تقنية المعلومات العمانية، وكان بالتعاون مع الاتحاد الدولي للاتصالات وتم إدارة المؤتمر من قِبل المركز العماني الوطني للسلامة المعلوماتية، وتم مناقشة عدة أمور في هذا المؤتمر ومنها مجالات الأمن السيبراني، وطرق مواجهة التهديدات التي تمس القطاعات الإقليمية والعالمية.

٥. مؤتمر الأمن السيبراني الدوحة (قطر) ٢٠١٤م تم عقد المؤتمر في دولة قطر وكان تحت تنظيم شركة بريطانية (تانجينت لينك) وبرعاية شركة قطرية مزودة لخدمات التكنولوجيا في دولة قطر وكان المؤتمر يهدف إلى بيان أهمية مراقبة التهديدات الرقمية وكذلك تبني نهج استباقي لإدارة أهداف الأمن السيبراني وذلك للقطاعين العام والخاص، كما هدف إلى سبل حماية مالكي الأسهم في البيئة الرقمية عالمياً.

٥. المؤتمر الدولي الأول حول مكافحة جرائم الإنترنت الرياض (المملكة العربية السعودية)، ٢٠١٥م عقد هذا المؤتمر تحت رعاية خادم الحرمين الشريفين الملك عبدالله بن عبدالعزيز رحمة الله، وكان الهدف من هذا المؤتمر هو رفع مستوى مكافحة جرائم تقنية المعلومات، واشتمل هذا المؤتمر على عدة مواضيع، وهي:

أ. الآثار والخصائص والاتجاهات الحديثة لجرائم تقنية المعلومات.

ب. الوعي العام للجرائم التقنية.

ج. الجرائم التقنية والإرهاب.

د. ملامح مجرمي الجرائم التقنية.

هـ. مفاهيم جرائم تقنية المعلومات.

و. التحديات لجرائم تقنية المعلومات وطرق مواجهتها.

ز. قوانين جرائم تقنية المعلومات.

ح. تجارب الدول الأخرى لمكافحة جرائم تقنية المعلومات.

٦. المؤتمر والمعرض الخليجي الأول تحت عنوان (تحديات الأمن السيبراني للمعلومات والاتصالات – وكان شعار المؤتمر (بيئة معلوماتية ومالية آمنة) الكويت ٢٠١٨م،[٦] عقد هذا المؤتمر تحت رعاية نائب رئيس مجلس الوزراء ووزير الدولة لشؤون مجلس الوزراء وحظي بدعم من الجهاز المركزي لتكنولوجيا المعلومات، وشاركت فيه عدة جهات محلية وخليجية ودولية متخصصة بمجال الأمن السيبراني، ناقش هذا المؤتمر عدة أمور منها:

١) مواجهة الاختراقات التقنية التي لها تأثير على الاقتصاد والبنية التحتية والخدماتية وتكثيف الجهود لمواجهتها.

٢) الارتقاء لتطوير مستوى الأمن السيبراني.

٣) تعزيز التعاون بين البلدان وتسهيل إنشاء الفرق الوطنية لاستجابة للطوارئ المعلوماتية.

المطلب الثاني: إنشاء المراكز الوطنية للأمن السيبراني، ومنها:

١- مركز الاستجابة لطوارئ الحاسب الآلي في دولة الإمارات العربية المتحدة، أنشأ هذا المركز عام ٢٠٠٧م من قبل هيئة تنظيم الاتصالات وذلك ليحقق عدة أهداف، وهي:

أ. حماية البنية التحتية المعلوماتية، وحماية أمن المعلومات من المخاطر التي تهددها تقنياً كالاختراقات عبر الانترنت.

ب. تعزيز الوعي على جميع مستويات الدولة للأمن السيبراني.

ج. بناء خبرات وطنية متخصصة في إدارة المركز ويتحرى عن الأدلة المعلوماتية في الحسابات.

د. تسهيل للاتصال بين الدول للإبلاغ عن جرائم تقنية المعلومات.

هـ. تعزيز قانون مكافحة جرائم تقنية المعلومات والمساعدة على إحداث قوانين جديدة.

و. تسهيل التواصل بين كل من الفرق المحلية والدولية لحوادث أمن المعلومات في جميع القطاعات.

٢- في مملكة البحرين: أسست شركة (تحديث للاستشارات) وهي شركة خاصة مركزاً للاستجابة لطوارئ الحاسب الآلي في سنة ٢٠١٢م ويقوم هذا المركز بالأعمال التالية:

أ) يقدم خدمة للكشف عن البرامج الضارة ويحدد موقعها.

ب) يوفر تحذيرات بشكل مبرمج ومتعمق تفيد بتوفير القدرة وسرعة القرار.[٧]

٣- المركز الوطني الإرشادي لأمن المعلومات (فريق الاستجابة لطوارئ الحاسب الآلي) في المملكة العربية السعودية:

أنشأ هذا المركز بواسطة هيئة الاتصالات وتقنية المعلومات، ويهدف هذا المركز إلى الآتي:

أ. رفع مستوى الوعي للأمن المعلوماتي.

ب. تعزيز ورفع مستوى الثقة للتعاملات الإلكترونية.

ج. يقدم النصائح والمشورة للأفراد وكذلك المؤسسات في كل ما يخص أمن المعلومات.(٨)

رؤية المركز: أن تكون المرجعية موثقة ومفوضة بشأن أمن المعلومات في المملكة العربية السعودية.(٩)

٤- دولة الكويت: لدى الدولة إستراتيجية لحماية ومراقبة الأصول والبنى التحتية الحيوية والمعلومات الوطنية وشبكة المعلومات الكويتية، ومن تلك المبادرات:

أ- إنشاء مركز الأمن الوطني السيبراني والجهة المسئولة: الهيئة العامة للاتصالات وتقنية المعلومات.

ب- إنشاء مراكز عمليات الأمن السيبراني والجهة المسئولة: وزارة الدفاع ووزارة الداخلية وقطاعات أخرى حيوية.

ج- تطوير التشريعات والقوانين المتعلقة بالجرائم الإلكترونية والأمن السيبراني لمواكبة التطور التكنولوجي والجهة المسئولة: وزارة الداخلية ووزارة العدل ووزارة الإعلام والجهاز المركزي لتكنولوجيا المعلومات والهيئة العامة للاتصالات وتقنية المعلومات (مركز الأمن الوطني السيبراني).(١٠)

تهدف مراكز عمليات الأمن السيبراني إلى توفير المراقبة المستمرة لأحداث الأمن السيبراني وتوفير وسائل الاستجابة المناسبة.

أما مركز الأمن الوطني السيبراني دولة الكويت: فيهدف إلى تعزيز الوعي الوطني للأمن السيبراني، حيث يكون هذا التعزيز لجميع فئات المجتمع، إذ إن المركز يشجع على استخدام وسائل الحماية وحلول الأمن لتجنب المخاطر الإلكترونية، ومن ضمن وسائل التوعية ما يقوم به المركز بالتعاون مع وزارات الدولة كوزارة التربية والمؤسسات التابعة لها لتثقيف المجتمع وذلك عبر تطوير مناهج أكاديمية متعلقة بهذا المجال.

ومن مهام المركز:

أ- يعمل مع القطاع الخاص ومزودين خدمات الاتصالات والانترنت لضمان الحماية اللازمة للبيانات المتبادلة وتحسين مستوى الأمن السيبراني.

ب- يعزز الوعي للمجتمع بجميع فئاته لمخاطر وتهديدات الفضاء الإلكتروني.

ج- تطوير التشريعات والقوانين المتعلقة بالجرائم الإلكترونية والأمن السيبراني لمواكبة التطور التكنولوجي.

د- يشجع على استعمال التطبيقات الآمنة وأفضل سبل الحماية الإلكترونية.

ويضم المركز عدة أقسام داخلية، وهي:

أ- مركز عمليات الأمن السيبراني.

ب- فريق الاستجابة لطوارئ الحاسب.[١١]

مسؤولية الأمن السيبراني تقع على القطاعات الحكومية كما تقعل على جهات أخرى كالقطاع الخاص والمؤسسات وأفراد المجتمع فمسئولية الأمن السبراني مسئولية مشتركة.[١٢]

ويرى الباحث أنه من المفترض أن تكون تلك المراكز منفصلة عن وزارات الدولة وتكون كهيئة مستقلة.

كما من المفترض أن يختص أحد المراكز بالإثبات الإلكتروني لأي فعل تقني سواء كان جريمة أو لم تكن.

المطلب الثالث : القوانين والتشريعات الخليجية في مكافحة الجرائم التقنية:

لم تكن القوانين الخاصة بالعقاب كقانون الجرائم وغيرها من قوانين باختلاف اسمائها كافية لمواجهة هذه الجرائم فتعمد المشرع الى سن قوانين مستحدثه لمكافحة هذه الجرائم[١٣]، وكانت جهود دول مجلس التعاون الخليجي في التصدي للجرائم الإلكترونية واضحه وسباقه في هذا المجال سوف نستعرض أهم القوانين التي أصدرتها دول مجلس التعاون الخليجي لمكافحة الجرائم الإلكترونية [١٤]، حيث أصدرت الإمارات العربية المتحدة عدداً من القوانين منها[١٥]:

١. القانون الاتحادي رقم ٣ لسنة ٢٠٠٣م بشأن تنظيم قطاع الاتصالات والقوانين المعدلة له.
٢. القانون الاتحادي رقم ١ لسنة ٢٠٠٦م بشأن المعاملات والتجارة الإلكترونية.
٣. القانون الاتحادي رقم ٢ لسنة ٢٠٠٦م بشأن مكافحة جرائم تقنية المعلومات.
٤. القانون الاتحادي رقم ٣ لسنة ٢٠١٢م بإنشاء الهيئة الوطنية للأمن الإلكتروني.
٥. القانون رقم ٥ لسنة ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات.

الذي ألغى القانون رقم ٢ لسنة ٢٠٠٦م بخصوص جرائم تقنيه المعلومات وكل قانون يخالفه.

ويرى الباحث أن القانون الإماراتي قد توسع كثيرا في تصنيف الجرائم وتنوعها ودقه عرضها وشدد في العقوبات.

ويعد هذا من خصائص القانون الإماراتي حيث تناول جميع جوانب الجرائم الإلكترونية من دخول غير مشروع الى موقع أو نظام أو شبكه معلوماتية أو افشاء أو تدمير أو تغيير أي معلومات فيه.

والتزوير الإلكتروني أو إدخال معلومات الى موقع أو شبكة أو نظام معلومات تهدف إلى الإضرار فيه أو التوصل إلى معلومات مهمة خاصة مثل أرقام البطاقة الائتمانية ونحوها.

أما في سلطنة عمان فقد صدر قانون عام سنة ٢٠١١م والذي يتميز بمساواة الفعل مع العقوبة بعكس الإماراتي الذي شدد بالعقوبات.

أما القانون السعودي قد أخذ بين تغليظ العقوبة وبين مساواة الفعل بالعقوبة.

أما في الكويت فقد صدر القانون الكويتي رقم ٦٣ لسنة ٢٠١٥م بشأن مكافحة جرائم تكنولوجيا المعلومات، والمعروف باسم قانون الجرائم الإلكترونية، وهو قانون يتعلق بمختلف الجرائم المعلوماتية. دخل حيز التنفيذ في ١٢ يناير ٢٠١٦م(١٦).

وانتقد القانون من قبل العديد من المنظمات الدولية لحقوق الإنسان بسبب القيود المفروضة على حرية التعبير وحرية الصحافة.

ولكن نلاحظ أن تلك القوانين في دول مجلس التعاون الخليجي -السابق ذكرها- بما فيها دولة الكويت لم يتم وضع إجراءات خاصة لقانون الجرائم الإلكترونية بل اعتمدت على نفس الإجراءات المتبعة في القانون الجزائي بعكس القانون القطري والقانون البحريني الذي وضعا إجراءات مختلفة وذلك باختلاف الفعل الإلكتروني عن الفعل الواقعي.

المبحث الثاني: استراتيجية دول مجلس التعاون في مكافحة جرائم التواصل الاجتماعي

إن مواقع التواصل الاجتماعي قد فرضت نفسها لدى جميع المجتمعات خصوصاً مجتمعنا العربي، وسبب ذلك سهولة التواصل بين الأفراد، فجعلت المستخدم يتلقى المعلومات منها بدل الإعلام التقليدي، ودائماً المستخدم يتلقى الأخبار الجديدة وما يدور في الساحة أولاً بأول، فكان لزاماً على الدول أن توجد استراتيجية لاحتواء هذه المواقع والبرامج.(١٧)، وذلك من خلال محورين أساسيين، هما: محور إدارة الأزمات الأمنية، ومحور الاهتمام بالأمن الفكري وبيان ذلك في المطلبين الآتيين:

المطلب الأول: إدارة الأزمات الأمنية:

إن إدارة الأزمات الأمنية تتطلب من الحكومات أن تقوم بعدة مهام وهي: حيث إن الحرب الإلكترونية في وسائل التواصل الاجتماعي لها أبعاداً خاصة فهي تركز على عقول وقلوب المستخدمين، ومكافحة تلك التأثيرات كالإشاعات وغيرها من أخبار لابد أن تكون بدعاية مضادة، وحيث إن وسائل التواصل الاجتماعي تعتبر سهلة المنال، ومن خلال أدوات رخيصة يستطيع المستخدم أن ينشر ما يريد من أفكار للغير بهذه الوسائل، فقد قامت دول مجلس التعاون الخليجي بملاحقة مروجين الإشاعات قضائياً كما قامت بإنشاء حسابات رسمية في هذه البرامج لكي تستطيع أن تواجه الإشاعات، ومثال ذلك: حسابات الجهات الرسمية للدولة (وزارة الداخلية في الانستاغرام: moi_kuw، وزارة الأشغال العامة mpw_kw).

ولا شك أن وسائل التواصل الاجتماعي أتاحت المجال لدى المستخدمين ليعبروا عن أفكارهم، ومن المعروف أن الإنسان اجتماعي بطبيعة حاله، يحب التواصل لا يمكن أن يعيش بمفرده.

ولمواقع التواصل الاجتماعي أهمية كبيرة في وقتنا الحاضر، حيث يتواصل المستخدمون فيما بينهم وينتشر الخبر بسرعة كبيرة، مما يصعب مكافحته بسهولة ولهذا لا بد من مواجهة ذلك من خلال عدة أمور، منها:

١) **الإعلام المضاد:** وهو نفي الخبر إذا كان غير صحيح، أو إصدار بيان حول الخبر.

٢) **الإعلام الوقائي:** من المعروف أن الوقاية عبارة عن الحيلولة دون وقوع الشيء فإذا قام الإنسان بعمل وقاية من شيء فالقصد منه تجنب حدوث هذا الشيء، وحيث إن وسائل التواصل الاجتماعي لها تأثير كبير على المجتمع وجب على الحكومات والجهات المعنية الأخرى القيام بعمل إعلام وقائي، فالجهات المسئولة تتجه إلى الوقاية من وقوع الجريمة بما يسمى بالأمن الوقائي، ويعرفّ بأنه الحيلولة دون وقوع الجريمة، أي لا يتم الانتظار لكي تقع الجريمة فتتحرك وتكافحها بل تستخدم أساليب ترمي إلى التضييق ووضع عراقيل على المنحرفين والمجرمين لكي لا يرتكبوا جرائمهم.(١٨)

ج) **التوعية الأمنية:** يعتبر الإعلام في عصرنا الحديث من أهم وسائل التوعية سواء كان من قبيل التثقيف أو التوجيه أو الإرشاد، والإعلام الأمني له أهمية في استقرار المجتمعات، فالتوعية الأمنية يعتمد عليها المجتمع والجهات المسئولة في مواجهة الظواهر السلبية والإجرامية كسبب من أسباب منع وقوع الجرائم، وهي تعمل على تغيير السلوك السلبي إلى السلوك الإيجابي بما يتوافق مع الإجراءات الأمنية وبما يصب في صالح أمن المجتمع والمواطنين، فمبدأ العقاب غير كاف لردع المجرمين، بل لا بد من أن يتم الاهتمام بالوسائل الأخرى كالإعلام،(١٩) والتوعية الأمنية قد يقوم بها مستخدموا برامج التواصل الاجتماعي من خلال نشر أو إعادة نشر المحتوى الإعلامي.

٤) **تطبيق أساليب أمنية علمية لإدارة الأزمات:** حيث إن علم إدارة الأزمات من العلوم الإنسانية الحديثة، ولما لها من أهمية في وقتنا الراهن وازداد الاهتمام بها لما نشاهده من متغيرات محلية وإقليمية، وتعرف الأزمة الأمنية بأنها "الحالة التي يستفحل فيها الحدث الأمني وتتصاعد الأعمال المكونة له إلى مستوى التأزم الذي تتشابك فيه الأمور ويتعقد فيه الوضع إلى الحد الذي يتطلب معه ضرورة تكاتف جهود العديد من الجهات الأمنية وغير الأمنية لمواجهتها بحكمة وخبرة وقدرة على احتمال ما يترتب عليه من أضرار والحيلولة دون استفحالها، وذلك من أجل الوصول إلى تحقيق الهدف المنشود والمتمثل في أقل قدر من الخسائر بأقل جهد وأقل تكلفة ممكنة وضبط الجناة للاستفادة منهم في إمكان التعرف على الأبعاد الحقيقة لتلك الأزمة منعا لتكرارها ودرءاً لانتشارها".(٢٠)

وللأزمة الأمنية عدة خصائص، منها:

أ) عدم وضوح الهدف.

ب) سرعة الانتشار.

ج) خطورة للتبعات.

د) تعدي القصد.

هـ) الصعوبة في السيطرة.

وهناك عدة أساليب استراتيجية تستخدم لمواجهة هذه الأزمات، وهي:[٢١]

١. استراتيجية استخدام العنف للتعامل مع هذا الأزمة، وهو عبارة عن مجموعة تحركات وإجراءات عسكرية وتكون بكل حزم وقوة لتتصدى لتلك الأزمة مع احتمالية وقوع خسائر قد تطول الأرواح.

٢. استراتيجية وقف النمو، وهي عبارة عن قبول الأمر الواقع مع بذل الجهد لكي تمنع تدهور الوضع وليضمن عدم وصولها لمرحلة أكبر، ويتم التعامل معها بحرص مع القوى كتلبية بعض المتطلبات وتقديم بعض التنازلات، والقيام بالتوجيه والإرشاد، وذلك للحد من الأزمة إلى أن يمكن دراسة العوامل المسببة لها.

٣. استراتيجية التجزئة، وهي عبارة عن دراسات وتحاليل يعتمد عليها لمعرفة العوامل المكونة لتلك الأزمة والقوى المؤثرة عليها والعلاقة الارتباطية بينهما.

٤. استراتيجية إجهاض الفكر الصانع للأزمة، وفيها يتم معرفة ما هو الفكر الواقف وراء هذه الأزمة؟ وما هي الاتجاهات والقيم المؤثرة عليها؟ ومن هنا تستخدم سياسة إضعاف وإجهاض الفكر المؤثر على هذه الأزمة.

المطلب الثاني: الاهتمام بالأمن الفكري:

تقوم الجهات المعنية بالاهتمام بالأمن الفكري لأفراد المجتمع لما له من خطر في حدوث تخريب مادي وضياع الشخصية وذوبانها في الإطار الإجرامي، فتحصين الفكر واجب ضد التيارات الفكرية المنحرفة، وخصوصاً أفراد الجهات الموكل لها الاهتمام بالجانب الأمني للمجتمع كأفراد الشرطة وغيرهم من مسئولين على هذا الجانب، فتحصين هؤلاء يساعد على مكافحة الأفكار الإجرامية والمنحرفة وهناك عدة خطوات يجب إتباعها لكي يتحقق تحصين أفكار الأفراد المسئولين خصوصاً أفراد الشرطة، وهي:[٢٢]

١) اختيار أفراد الشرطة بشروط ومواصفات خاصة محددة ومنضبطة.

٢) رفع كفاءة أفراد الشرطة في مستوى فكرهم وأخلاقهم وسلوكهم ويكون ذلك من خلال الثقافة التخصصية والعامة وجعلهم يكتسبون المهارات المعرفية.

٣) تنمية الحس الأمني لدى أفراد الشرطة ويكون ذلك من خلال التحقيق بالظواهر الإجرامية والسلبية وخصوصاً ما يمس الفكر وبشكل تحليلي، وفي حال وقوع حدث إجرامي فيجب عدم نشر أي معلومة عن ذلك لكي يتم تحقيق جزء من المكافحة.

٤) تنمية روح المواطنة لدى أفراد الأمن.

٥) تنمية الوازع الديني لرجال الأمن؛ لأن الوازع الديني يرسخ القيم الأخلاقية والاجتماعية والإنسانية.

ويرى الباحث أن بعض هذه الخطوات يجب أن تدرس في المدارس والجامعات فالوسيلة التربوية والتعليمية من أهم الوسائل للقضاء على الجانب الفكري الإجرامي.

وأما الجانب الرقابي فيتم من خلال الخطوات الآتية:[٢٣]

١. الدعاية المضادة: تعتبر المعركة الإلكترونية من المعارك الحديثة في عصرنا الراهن، وهي معركة مستحدثة وسلاح الدفاع هو عبارة عن إصدار بيان أو عمل توضيحي أو نفي الخبر أو توجيه وإرشاد ضد الشائعات والأفكار الإجرامية، ويكون ذلك بالحسابات الرسمية لمؤسسات الدولة وأيضاً حسابات الأفراد.

٢. الرصد والمراقبة: وهي سياسة تتبعها الأجهزة الأمنية برصد الأفكار والأفعال المخالفة للقانون واللوائح والأدب والنظام العام من خلال الفضاء الإلكتروني وخصوصاً برامج التواصل الاجتماعي، ومن ثم تقوم بعمل الإجراءات القانونية لذلك كاستدعاء وتحقيق وإحالته للجهات المختصة وغالباً ما يصل بهم الأمر إلى محاكمتهم.

ويرى الباحث أن الرصد والمراقبة أصبح بيد المواطن أكثر من الدولة، إذ بعض الأحيان يكون بسبب الرأي العام تتحرك أجهزة الدولة.

٣. سحب المحتوى الرقمي: إن إدارات برامج التواصل الاجتماعي جعلت لمستخدميها فضاءً إلكترونياً أكثر حرية وقليل القيود، فضغط الحكومات عليها بالتعاون معها لمكافحة جرائم التواصل الاجتماعي ضعيف جداً لكن هناك حالات تنظر لها دون تدخل الحكومات وهي الاستغلال الجنسي للأطفال، وهناك بعض الحالات التي تستجيب تلك المواقع لها، فغالباً إدارات تلك البرامج غير متعاونة لكي ترضي مستخدميها وتعطيهم حرية أكثر، وهذا عقبة للجهات الأمنية وخصوصاً الحسابات الوهمية والأسماء المستعارة.

ويرى الباحث أن سحب المحتوى الرقمي كاقتلاع الورم السلطاني قد يكون له بقايا وقد لا يكون له بقايا.

ومنا خلال ما سبق يتضح لنا أن دولة الكويت وغيرها من دول مجلس التعاون لديها قوانين تكافح جرائم تقنية المعلومات لكنها بحاجة إلى تعديلات وكذلك تفتقر إلى التعاون الدولي المشترك حيث قوانينها عبارة عن حماية داخليها وليس دولية و دولة الكويت نموذجا.

مثلا قانون مكافحة جرائم تقنية المعلومات ٢٠١٥/٦٣م[٢٤] ملخص هذا القانون :

المادة ١ عدة تعريفات .

المادة ٢ وحتى المادة ١٠ افعال تقع من خلال العالم التقني وخصوصا وسائل التواصل الاجتماعي إلا انها يحتاج لبعض التعديلات وابسطها عدم ذكر فعل **البقاء** حيث هناك من علق صراحة على قصور القانون وعدم ذكره لفعل البقاء [٢٥] وأيضا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث نصت على هذا الفعل في المادة ٦ في الفقرة ١[٢٦].

أما باقي المواد نصت على فعل التشديد والاختصاص والتقادم وغيرها من أمور.

ويرى الباحث أن القانون يفتقر إلى التعاون الدولي إذ لا بد من تعديله وإضافة مواد تختص بالتعاون الدولي وذلك لمكافحة جرائم تقنية المعلومات.

الخاتمة: إن الجرائم التقنية تعتبر جرائم حديثة فلابد أن يتم مواجهتها بالطرق الحديثة وأن ما قامت به دول مجلس التعاون عبارة عن قوانين لمواجهة الجرائم ذات الطابع التقني، وقد توصل الباحث إلى عدة نتائج من أهما:

النتائج :

١. إن قوانين دول مجلس التعاون أغلبها بل جلها تنظم شأنها الداخلي ولا تكافح تلك الجرائم التقنية سواء إقليميا أو دوليا.

٢. بطئ بعض الدول بإنشاء بعض المراكز التي تم إقرارها بالمؤتمرات.

٣. أهمية التعاون الاقليمي، فالاتفاقية العربية أشمل من اجتهادات دول مجلس التعاون من ناحية التشريع وليس الإجراء الميداني حيث استراتيجيات دول مجلس التعاون ممتازة جدا لكن ننتظر تفعيلها.

٤. ليس كل قوانين دول مجلس التعاون نصت على إجراءات خاصة بجرائم تقنية المعلومات فالدول التي نصت على ذلك هي دولة قطر ومملكة البحرين، وأما باقي الدول فتستعين في ذلك بقوانين الإجراءات التقليدية.

التوصيات :

١. أن المواجهة الفكرية لا تكفي في حال عدم تشريع قانون رادع .

٢. أن جرائم تقنية المعلومات وخصوصا الواقعة عبر وسائل التواصل الاجتماعي لا بد أن يكافحها قانون مختص.

٣. أوصي بإضافة مواد خاصة بالإجراءات لمكافحة جرائم تقنية المعلومات وعدم الاعتماد على القوانين التقليدية كقانون أصول المحاكمات الجزائية.

هوامش البحث:

(١) إعداد مركز البحوث، والدراسات، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، (سلطنة عُمان، أكاديمية السلطان قابوس لعلوم الشرطة، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥م، ٢٠١٦م)، ص٥٥.

(٢) سارة رمضان، ومُحَمَّد ناجي، **عُزلة عن قطع الاتصالات أثناء ثورة يناير ٢٠١١م** (مؤسسة حرية الفكر والتعبير، ب.ط، ب.ت)، ص١٠.

(٣) **دستور دولة الكويت لسنة (١٩٦٢)**،المادة (٣٢).

(٤) مداوي القحطاني، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، (مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥، دولة قطر، ٢٠١٦)، ص٣٤.

(٥) إعداد مجمع البحوث والدراسات، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، (سلطنة عُمان، أكاديمية السلطان قابوس لعلوم الشرطة، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥م، ٢٠١٦م)، ص٧٥.

(٦) **وكالة الأنباء الكويتية– كونا**، تاريخ ٢٠١٨/١٠/٢١ بعنوان (هيئة الاتصالات) الكويتية: إنشاء مركز وطني للأمن السيبراني يعزز قدرات البنى التحتية للمؤسسات، ينظر الرابط، آخر زيارة ١٥ أكتوبر ٢٠١٨م:
https://www.kuna.net.kw/ArticleDetails.aspx?id=2753988

(٧) إعداد مجمع البحوث والدراسات، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، (سلطنة عُمان، أكاديمية السلطان قابوس لعلوم الشرطة، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥م، ٢٠١٦م)، ص٨٢.

(٨) الموقع الإلكتروني للمركز الوطني الإرشادي لأمن المعلومات http://www.cert.gov.sa/.

(٩) إعداد مجمع البحوث والدراسات، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، ص٨٣.

(١٠) **الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت**، (٢٠١٧ – ٢٠٢٠)، ص٢٢.

(١١) **الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت**، ٢٠١٧ – ٢٠٢٠، ص١٧.

(١٢) **الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت**، نفس المرجع، ص٢٥.

(١٣) أمير فرج يوسف، **جرائم تقنية المعلومات بدول الخليج** العربي، دار الكتب والدراسات العربية، ٢١٠٢، ص ١٢١.

(١٤) – نظام مكافحة جرائم المعلوماتية السعودي مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨

– مرسوم سلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات (عمان)

– مرسوم رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات الإماراتي

– قانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات الكويتي

– قانون رقم ٦٠ لسنة ٢٠١٤ بشأن مكافحة جرائم تقنية المعلومات البحريني.

– قانون رقم ١٤ لسنة ٢٠١٤ بشأن مكافحة جرائم تقنية المعلومات القطري.

(١٥) **السياسة العقابية للمشرع الاماراتي في مواجهة الجرائم المعلوماتية في ظل المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات**، عبدالعزيز السنيدي، اطروحة دكتوراه، جامعة الامارات العربية المتحدة، كلية القانون، ٢٠١٨، ص ٣٦.

(١٦) القانون الكويتي رقم (٦٣) لعام ٢٠١٥م، بشأن مكافحة جرائم تقنية المعلومات، البوابة الإلكترونية الكويتية. https://www.e.gov.kw/ .اطلع عليه في ٢٣ نوفمبر / ٢٠٢٠م.

(١٧) دينا عبد العزيز فهمي، **الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي**(مصر: دار النهضة العلمية، الإمارات: دار النهضة العربية، ب.ط، ٢٠١٨)، ص٣٧.

(١٨) مُحَمَّد سيف الدين ويسرا حسني، **المحددات النظرية والعلمية للإعلام الأمني الوقائي**(الرياض: جامعة نايف العربية للعلوم الأمنية، جامعة نايف للنشر، ب.ط، ٢٠١٦)، ص٣٣.

(١٩) جوزيف مسلم، **برامج الإعلام الأمني بين الواقع والتطلعات**(الرياض: جامعة نايف للعلوم الأمنية، ط١، ٢٠١٢)، ص٢١٣.

(٢٠) عمر حسن، وأحمد ضياء الدين، **إدارة الأزمة الأمنية، دراسة تطبيقية لإدارة الأزمة الأمنية في مواجهة الكوارث والإرهاب** (القاهرة،ب.ن، ب.ط، ١٩٩٧)، ص٢٣.

(٢١) **المجالس القومية المتخصصة**، جمهورية مصر العربية، موسوعة المجالس القومية المتخصصة(المجلد ٢٤، ١٩٧٤–١٩٩٨)، ص٢٨٤.

(٢٢) المتول والعنزي، **مواقع التواصل الاجتماعي والانحراف الفكري في المجتمع الخليجي**، ص٢٨٣.

(٢٣) المتولي والعنزي، **مواقع التواصل الاجتماعي والانحراف الفكري في المجتمع الخليجي**، نفس المرجع، ص٢٩٠.

(٢٤) **قانون مكافحة جرائم تقنية المعلومات** ٢٠١٥/٦٣ الكويتي.

(٢٥) عبدالحليم، بوقرين. "**قانون مكافحة جرائم تقنية المعلومات الكويتي؛ دراسة مقارنة**"، مجلة كلية القانون الكويتية العالمية، العدد ٤، السنة الخامسة، العدد التسلسلي ٢٠، الكويت (ديسمبر ٢٠١٧م)، ص٢٩٤.

(٢٦) **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** في القاهرة وذلك من خلال انعقادها في مقر الأمانة العامة لجامعة الدول العربية بتاريخ ٢٠١٠/١٢/٢١.

قائمة المراجع :

١. إعداد مركز البحوث والدراسات، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، سلطنة عُمان، أكاديمية السلطان قابوس لعلوم الشرطة، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥م، ٢٠١٦م).

٢. سارة رمضان، ومُحَمَّدناجي، **عُزلة عن قطع الاتصالات أثناء ثورة يناير ٢٠١١م**(مؤسسة حرية الفكر والتعبير، ب.ط، ب.ت).

٣. **دستور دولة الكويت لسنة(١٩٦٢)**،المادة (٣٢).

٤. مداوي القحطاني، **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، (مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥، دولة قطر، ٢٠١٦)، ص٣٤.

وكالة الأنباء الكويتية– كونا، تاريخ ٢٠١٨/١٠/٢١ بعنوان (هيئة الاتصالات) الكويتية: إنشاء مركز وطني للأمنالسيبراني يعزز قدرات البنى التحتية للمؤسسات، ينظر الرابط، آخر زيارة ١٥ أكتوبر ٢٠١٨م.

٥. https://www.kuna.net.kw/ArticleDetails.aspx?id=2753988.

٦. الموقع الإلكتروني للمركز الوطني الإرشادي لأمن المعلومات http://www.cert.gov.sa/

٧. **الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت**، (٢٠١٧ – ٢٠٢٠).

٨. أمير فرج يوسف ، **جرائم تقنية المعلومات بدول الخليج** العربي، دار الكتب والدراسات العربية، ٢١٠٢.

٩. **السياسة العقابية للمشرع الاماراتي في مواجهة الجرائم المعلوماتية في ظل المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات**، عبدالعزيز السنيدي، اطروحة دكتوراه، جامعة الامارات العربية المتحدة، كلية القانون، ٢٠١٨.

١٠. دينا عبد العزيز فهمي، **الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي**(مصر: دار النهضة العلمية، الإمارات: دار النهضة العربية، ب.ط، ٢٠١٨).

١١. مُحَمَّد سيف الدين، ويسراحسني، **المحددات النظرية والعلمية للإعلام الأمني الوقائي**(الرياض: جامعة نايف العربية للعلوم الأمنية، جامعة نايف للنشر، ب.ط، ٢٠١٦).

١٢. جوزيف مسلم،**برامج الإعلام الأمني بين الواقع والتطلعات**(الرياض: جامعة نايف للعلوم الأمنية، ط١، ٢٠١٢).

١٣. مُحَمَّد المتولي، وعبد الرحمن العنزي، **مواقع التواصل الاجتماعي والانحراف الفكري في المجتمع الخليجي** (دار الإيمان للطباعة، ط١، ٢٠١٨).

١٤. عمر حسن، وأحمد ضياء الدين، **إدارة الأزمة الأمنية، دراسة تطبيقية لإدارة الأزمة الأمنية في مواجهة الكوارث والإرهاب**(القاهرة، ب.ن، ب.ط، ١٩٩٧).

١٥. **المجالس القومية المتخصصة**، جمهورية مصر العربية، موسوعة المجالس القومية المتخصصة (المجلد ٢٤، ١٩٧٤– ١٩٩٨).

١٦. **قانون مكافحة جرائم تقنية المعلومات** ٢٠١٥/٦٣ الكويتي.

١٧. عبدالحليم، بوقرين. "**قانون مكافحة جرائم تقنية المعلومات الكويتي؛ دراسة مقارنة**"، مجلة كلية القانون الكويتية العالمية، العدد ٤، السنة الخامسة، العدد التسلسلي ٢٠، الكويت (ديسمبر ٢٠١٧م).

١٨. **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** في القاهرة وذلك من خلال انعقادها في مقر الأمانة العامة لجامعة الدول العربية بتاريخ ٢٠١٠/١٢/٢١.