مجلة الحكمة للدراسات والأبحاث المجلد 03 العدد 01 (11) 2023/03/30
ISSN print/ 2769-1926 ISSN online/ 2769-1934

دور الاتفاقيات الدولية والتشريعات الوطنية في مكافحة جرائم تقنية المعلومات

أ.م.د/علوي علي أحمد الشارفي*
أستاذ القانون الجنائي المشارك
أكاديمية الشرطة، اليمن
alawiali013@gmail.com

تاريخ الارسال: 2023/02/01 تاريخ القبول: 2023/03/05

ملخص:

تعتبر جرائم تقنية المعلومات من الجرائم المستحدثة التي تستهدف التطورات التكنولوجية، وتؤدي الى انتشار الشبكات الإرهابية في كثير من دول العالم باستغلال الوسائل الإلكترونية بكافة أنواعها والتي تشكل خطرًا على الاستقرار الداخلي وتهدد السلم والأمن الدوليين.

ولقد أثارت جرائم تقنية المعلومات بعض المشاكل القانونية بخصوص تطبيق نصوصها التقليدية على هذا النوع من الأفعال والتي تتطلب قوانين خاصة محلية واتفاقيات دولية للحد من هذه الجرائم المستحدثة.

وتهدف الدراسة الى معرفة تقنية المعلومات، وماهي ادواتها وخصائصها، وبيان دور الاتفاقيات الدولية والتشريعات العربية والغربية في مكافحة جرائم تقنية المعلومات، وقد توصلت الى بعض النتائج والتوصيات لمعالجة مشاكل جرائم تقنية المعلومات.

الكلمات المفتاحية: جرائم تقنية المعلومات– الاتفاقيات الدولية– التشريعات الوطنية– المنظمات الدولية– الإنترنت.

* **المؤلف المرسل:** أ.م.د/علوي علي أحمد الشارفي، **الايميل:** alawiali013@gmail.com

مقدمة:-

لقد شهد القرن الماضي تطوراً سريعاً في مجال تكنولوجيا المعلومات والاتصالات، وأصبحت أداة أساسية في الحياة اليومية وشاملة لأغلب القطاعات الطبية والتجارية والأمنية وغيرها من القطاعات، وعملت إضافة نوعية في التنمية الاقتصادية والاجتماعية للدول.

واصبح العالم يتواصل عبر شبكة اتصال عالمية تنقل الإنسان بجميع حواسة دون أن يتحرك من مكانة للتفاعل مع من يريد في أي بقعة من العالم، فقد برز عصر تقنية المعلومات في جميع مناحي الحياة السياسية والاجتماعية والاقتصادية وغيرها.

وقد تطورت المعلومات وتم ربطها بالأقمار الصناعية لسرعة بثها وإيصالها كمعلومة تقنية ملائمة وواضحة وشاملة للحدث وفي وقتها المناسب الى مستخدميها عبر مصادر التقنية الحديثة مثل الحاسب الآلي والإنترنت والبرامج التطبيقية والتشغيلية.

ومع هذا التطور المعلوماتي تعقدت الجريمة وظهرت جرائم مرتبطة بمصادر التقنية الحديثة تحت مسميات متعددة، مثل جرائم المعلومات أو جرائم تقنية المعلومات أو جرائم تكنولوجيا المعلومات وجرائم الإنترنت والجرائم السيبرانية والجرائم الإلكترونية، وجميعها أفعال إجرامية خطيرة تهدد السلم والاستقرار، يرتكبها أشخاص بدوافع مادية أو شخصية ضد أفراد أو أشخاص اعتبارية، بأدوات إلكترونية بكل سهولة ويسر وبعيدًا عن الرقابة الأمنية متجاوزًا الحدود الجغرافية.

ونظرًا لسرعة الوصول الإلكتروني الى جميع مجالات الحياة وفي كل دول العالم، فقد أثرت تأثيرًا مباشرًا على الأمم، واصبح من الضروري القيام بإعداد قوانين وقرارات عبر اتفاقيات دولية، تنظم تقنية المعلومات واعتماد استراتيجية على المستوى الدولي والإقليمي تشارك فيها المنظمات المتخصصة.

يجب على جميع الشعوب وضع قواعد تشريعية وطنية، تنظم التطور المتسارع في تقنية المعلومات وتحافظ على خصوصيات الأفراد والممتلكات العامة والخاصة، وتحقيق مبدأ العدالة والردع العقابي.

أولاً مشكلة الدراسة:-

أن التطور المتسارع في تكنولوجيا المعلومات فتح مجالات كثيرة للإبداع والابتكار، واوجد فرص للعمل في جميع مجالات الحياة، ومع هذا التطور لم تستطيع الاتفاقيات الدولية والتشريعات المحلية مواكبة ذلك ووضع ضوابط لاستخدام هذه التكنولوجيا وتوجيهها في الاتجاه الصحيح.

ثانيًا أهداف الدراسة:-

تهدف الدراسة الى معالجة المشكلة من خلال الاتي:

- ماهية تقنية المعلومات؛
- ماهي أدوات تقنية المعلومات؛
- توضيح خصائص وأنواع المعلومات؛
- بيان دور الاتفاقيات الدولية في مكافحة جرائم تقنية المعلومات؛
- إبراز دور التشريعات العربية والغربية في مكافحة جرائم تقنية المعلومات.

ثالثًا منهج الدراسة:-

أتبعنا في هذه الدراسة المنهج الوصفي التحليلي لأحكام الاتفاقيات الدولية والتشريعات المتعلقة بمكافحة جرائم تقنية المعلومات.

رابعًا خطة الدراسة:-

ستكون الدراسة على النحو التالي:

المبحث الأول: ماهية تقنية المعلومات

المطلب الأول: مفهوم وأدوات تقنية المعلومات

المطلب الثاني: خصائص وأنواع المعلومات

المبحث الثاني: دور الاتفاقيات الدولية والتشريعات الوطنية في مكافحة جرائم تقنية المعلومات

المطلب الأول: المنظمات والاتفاقيات الدولية

المطلب الثاني: التشريعات الوطنية

الخاتمة:

المبحث الأول

ماهية تقنية المعلومات

تمهيد:-

المعلومات هي علم التعامل المنطقي ولها قواعد ونظم، وتتميز بالمرونة يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة، فالمعلومات مصطلح استعمله لأول مرة لويس ميكالوف (**A.I.Mikhailov**) كأسم لعلم المعلومات العلمية. (هشام رستم، 1994م، ص27)

فهي مجموعة من الحقائق والرموز أو المفاهيم والتعليمات التي تصلح لأن تكون محلاً للتبادل والاتصال أو التفسير أو للمعالجة سواءً تم ذلك بواسطة الأفراد أو بالأنظمة الإلكترونية.

ويميز الباحثين بين المعلومات والبيانات، فالبيانات تعبر عن الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض ولم تخضع بعد للتفسير أو التجهيز أو الاستخدام والتي تخلو من المعنى الظاهر في أغلب الأحيان، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات. (نائلة فريد، 2005م، ص94)

المعلومات تتطلب تقنية لإعدادها وإخراجها بواسطة الحاسب الآلي وتتميز بخصائص ذات قيمة معرفية أو تطبيقية، وقد تكون معلومات عادية متاحة لعامة الناس أو معلومات سياسية أو عسكرية بدرجات متفاوتة من السرية.

المطلب الأول

مفهوم وأدوات تقنية المعلومات

المعلومات هي خلاصة بيانات أو ناتج تجميع أرقام وصور أو تحديد رموز مشفرة وإخراجها في صورة معلومة نهائية قد تكون معرفية أو تطبيقية، وتتميز المعلومات بقابليتها للدمج.

وتشمل المعلومات كل حقائق مدركة تتواجد معنويًا كقيمة معرفية وماديًا في شكل أرقام وأحرف ورسوم وصور وأصوات، ويتم جمعها ومعالجتها وحفظها وتبادلها بوسائط إلكترونية وورقية.

والمعلومات الإلكترونية هي: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والأصوات والأرقام والحروف والرموز والإشارات وغيرها. (حسني عبد السميع، 2011م، ص61)

الفرع الأول تعريف تقنية المعلومات:-

المعلومات قد تكون نوعًا من المعرفة أو تكون في شكل هندسي أو مجموعة من الإرشادات والأوامر، وقد تتعلق بأمور مالية أو فنية أو أدبية وهي تختلف فيما بينها من حيث نوعها وأهميتها، وقد تكون المعلومات مخزنة في الحاسب الآلي، ويجب توفير الحماية اللازمة لها وعدم التلاعب بها أو تغييرها.

وتُعرف المعلومات بأنها كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقلة أو مشاركته أو نسخة بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات وما في حكمها. (قانون مكافحة جرائم تقنية المعلومات المصري، رقم 175 لسنة 2018م)

وتُعرف تقنية المعلومات بأنها أي وسيلة مادية أو غير مادية أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقًا للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات في نظام معلوماتي أو شبكة مرتبطة بها سلكيًا أو لاسلكيًا. (مشروع قانون جرائم تقنية المعلومات اليمني، 2022م)

وقد صاغت الأكاديمية الفرنسية في عام 1967م تعريفًا لتقنية المعلومات بأنها(علم التعامل العقلاني على الأخص بواسطة آلات أتوماتيكية مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعمادًا للاتصالات في ميادين التقنية والاقتصاد والاجتماع). (محمد سكيكر، 2010م، ص14)

وعرفتها اليونسكو بأنها(الفروع العلمية والتقنية والهندسية وأساليب الإدارة الفنية المستخدمة في تداول ومعالجة المعلومات وتطبيقاتها، والمتعلقة كذلك بالحسابات وتفاعلها مع الإنسان والآلات وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية). (محمد سكيكر، 2010م، ص15)

ويقصد بتقنية المعلومات هي عملية تغذية ومعالجة وتخزين ثم بث وإستخدام المعلومات الرقمية والنصية والمصورة والصوتية عن طريق تقنيات الحاسب الآلي والاتصالات، وبالتالي فهي تتضمن توظيف أدوات وأساليب وتجهيزات متطورة لنقل المعلومات من المرسل الى المستقبل بأقل وقت وجهد وتكلفة وبأقصى قدر من الدقة. (الاتحاد الدولي للاتصالات، 2015م)

وقد عرف بعض الخبراء تقنية المعلومات بأنها(التزاوج والالتحام التقني بين الحاسبات والاتصالات والاستعمال المتزايد للإلكترونيات في العمليات الصناعية والتجارية ابتداءً بنظم البرمجيات بالحاسب حتى بطاقة الائتمان "الدفع الإلكتروني" التي يحتفظ بها الشخص معه). (هشام رستم، 1994م، ص28)

وتقنية المعلومات أو المعالجة الإلكترونية تتم كليًا أو جزئيًا لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل وكذلك استرجاع أو استنباط للبيانات والمعلومات الإلكترونية وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الإلكترونية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات ووسائط أخرى. (قانون مكافحة جرائم تقنية المعلومات المصري، رقم 175 لسنة 2018م)

وتكمن أهمية المعلومات في الآتي:-

1- تساعد في تحقيق الميزة التنافسية لإنتاج معلومات حقيقية؛

2- تعتبر المعلومات موردًا استراتيجيًا تعتمد علية الدول والمنظمات؛

3- المعلومات تحقق الضبط والانتظام الوظيفي؛

4- تشكل المعلومات قاعدة أساسية لحل المشكلات؛

5- تؤثر المعلومات في نوعية القرارات المتخذة.

الفرع الثاني أدوات تقنية المعلومات:-

أولاً الحاسب الآلي "جهاز الكمبيوتر":

بدأ العمل على أول جهاز رقمي في العالم سنة 1937م بمعرفة عالم رياضي من جامعة هارفارد وهو (**Howard Aiken**) وقد أنتهى من إنجاز الجهاز في عام 1942م بمساعدة من شركة(**I B M**) التي كانت تقوم بإنتاج ماكينات الكروت المثقبة، وقد كان طول الجهاز خمسون قدمًا وارتفاعه ثمانية أقدام ويحتوي على حوالي سبعمائة وخمسون ألف جزئي يتم توصيلها بما يقارب من خمسمائة مفتاح كهروميكانيكي. (محمد سكيكر، 2010م، ص20)

وفي عام 1958م، حلت وحدات الترانزستور محل الصمام الإلكتروني ليصبح الجهاز أصغر حجمًا وأسرع وقتًا وأكفأ في العمل وأقل استهلاكًا للكهرباء، وفي عام 1964م أدخلت شريحة السيلكون(**Chip**) واندمجت بصورة مكثفة داخل البنية المبلورة لوحدات الترانزستور، واستخدمت في عام 1982م مواد جديدة ووسائل مبتكرة في تصنيع العناصر الإلكترونية ودمجها في رقائق سيلكون وضبط انتاجها. (السيد عاشور، 2000م، ص26)

وبعد هذه المرحلة حدث تطور تقني وفني بدمج شريحتي المعالج والذاكرة داخل شريحة واحدة بحجم وتكلفة أقل أدت إلى رفع قدرة وأداء الخلايا، ومع هذا التطور ظهرت شركات الكمبيوتر والتي استطاعت تصنيع الأجهزة المتعددة وإعداد وتنظيم وتصميم برامج حديثة.

فالحاسب الآلي "الكمبيوتر" هو جهاز أو منظومة لتنفيذ مجموعة من التعليمات المحددة بتسلسل سبق إعداده وتشمل عمليات حسابية ومنطقية أو عمليات نقل البيانات من أجزاء الحاسب وتخزينها أو استرجاعها. (محمد سكيكر، 2010م، ص21)

ويقصد بالحاسب الآلي "الكمبيوتر" طبقًا للموسوعة الشاملة (كل جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال أو إخراج معلومات وإجراء عمليات حسابية أو منطقية وذلك بأن يقوم الحاسب بالكتابة على أجهزة الإخراج أو التخزين، ويتم إدخال البيانات بواسطة مشغل الحاسوب عن طريق وحدات الإدخال أو استرجاعها من وحدة المعالجة المركزية فتتم كتابتها على أجهزة الإخراج). (محمد سكيكر، 2010م، ص22)

ويُعرف الحاسب الآلي بأنه (جهاز إلكتروني يستطيع القيام بأداء عمليات حسابية ومنطقية طبقًا للتعليمات المعطاة وله سرعة كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية من الدقة، ولديه القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة اليها). (محمد الرومي، 2004م، ص13)

الحاسب الآلي هو جهاز إلكتروني قادر على تخزين ومعالجة وتحليل واسترجاع البيانات والمعلومات بطريقة إلكترونية، وله برنامج عبارة عن مجموعة من الأوامر والتعليمات معبر عنها بأي لغة أو رموز أو إشارات، وتتخذ أي شكل من الأشكال ويمكن استخدامها بطريقة مباشرة أو غير مباشرة لإداء وظيفة أو تحقيق نتيجة.

والحاسب الآلي "الكمبيوتر" هو عبارة عن جهاز أو مجموعة من الأجهزة أو الأجزاء المرتبطة أو المتصلة مع بعضها أو ذات علاقة، والتي يقوم واحد منها أو أكثر وفقاً لبرنامج معين بوظيفة المعالجة الآلية للبيانات. (اتفاقية بودابست، لسنة2001م)

وتتم تقنية نظم المعلومات في نظم الحاسبات(**Computer Systems**) والتي هي كل مكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة إضافة إلى الأشخاص الذين يمكن بواسطتهم تحقيق وظيفة أو هدف محدد، ويتكون الحاسب الآلي من التالي:- (محمد سكيكر، 2010م، ص23)

1- المدخلات: وهي الوسائل التي تستخدم في إدخال البيانات والبرامج إلى وحدة التشغيل المركزية ومنها وحدة الإدخال في الحاسب وتستخدم في إدخال البيانات والأوامر ومفاتيحها تشبه مفاتيح الآلة الحاسبة، ويكون الإدخال بالآتي:

أ. شاشات اللمس وهي تسمح بإدخال بعض البيانات عن طريق لمس أماكن حساسة في الشاشة؛

ب. نظام الإدخال المرئي وتستخدم كاميرا فيديو لالتقاط صور وتحويلها إلى أرقام أو إشارات للمقارنة بالصورة المخزنة بالحاسب؛

ج. نظام الإدخال الصوتي يستخدم بواسطة ميكرفون أو تلفون لتحويل الصوت إلى إشارات كهربائية ترسل إلى الحاسب للمطابقة وتنفيذ المطلوب أدائه؛

د. نظام الفأرة حيث يحرك المؤشر إلى الأمر أو الرقم المطلوب فيضغط على المفتاح الموجود في الفأرة ويتم تنفيذ المطلوب؛

هـ. نظام القلم الضوئي وهو جهاز إلكتروني حساس للضوء يساعد على التمكن من الشاشة بتحريكها أو تغييرها وتنفيذ العمليات المطلوبة؛

و. نظام الاحزمة المغناطيسية وهو إدخال البيانات إلى جهاز الحاسوب بسرعة ودقة حيث يتم تسجيلها على كروت بها شفرة وبيانات محددة كرقم الحساب؛

ز. نظام شفرة الأعمدة وهو جهاز حساس للضوء يستخدم في المحلات التجارية لتعريف السلع وأسعارها.

2- وحدة الذاكرة الرئيسية: تستخدم لحفظ البيانات والمعلومات والبرامج وتتكون من نوعين:

أ- ذاكرة القراءة وتستخدم لتخزين البيانات والأوامر وتكون على الجهاز من الشركة المصنعة؛

ب- ذاكرة القراءة والكتابة وتستخدم في جميع أغراض التخزين أثناء تشغيل الحاسب.

3- **وحدة الحساب والمنطق**: وهي جزء من المعالجة المركزية وتقوم بمعالجة البيانات حسابيًا ومنطقيًا مثل عمليات الجمع والطرح والقسمة.

4- **وحدة التحكم**: وهي أساس وحدة المعالجة المركزية حيث تقوم بالتنسيق بين وحدات الحاسب وضبط جميع التعليمات.

5- **وحدة الإخراج**: وهي الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات ومنها:

أ. الشاشة وهي وحدة العرض المرئي ويتم عن طريقها استعراض أي بيانات أو معلومات؛

ب. الطابعة وهي جهاز يستخدم في إخراج نسخ مطبوعة من المعلومات؛

ج. المصغرات الفلميه لتسجيل المعلومات على فلم مصغر؛

د. الرسام ويستخدم في طباعة الرسوم بدرجات وضوح مختلفة.

6- **وحدات التخزين**: وهي تخزين البيانات والمعلومات داخل جهاز الحاسب الآلي.

ثانيًا نظام التشغيل:- (www.mawdoo3.com)

يُعرف نظام التشغيل (**System Operating**) ويرمز اختصارًا(**OS**) بأنه عبارة عن مجموعة من البرامج الأساسية التي تدير جهاز الحاسوب، وتنظم جميع المهام التي يقوم بها، وتسهل على المستخدم الاستفادة من الآلات والملحقات التي يتكون منها الجهاز، كما تمكنه من الاستفادة من البرامج التطبيقية المختلفة.

ويُعرف بأنه البرنامج الرئيسي لاي جهاز حاسوب، فهو المسؤول عن تشغيل الجهاز وعمل بقية البرامج بالشكل الصحيح.

وكذلك يُعرف بأنه برنامج ذات طابع خاص يعمل كواجهة للجهاز ويعتبر حلقة الوصل بين المستخدم والحاسب الآلي. (محمد سكيكر، 2010م، ص24)

وهو النظام الذي تعمل به جميع البرمجيات (**Software**) مثل متصفحات الإنترنت وبرامج الميديا وبرامج تحرير النصوص وغيرها، وتدير هذا النظام والعمليات التي تجري عليها ذاكرة أجهزة الحاسب الآلي، فمن دونها لن يكون للحاسوب أي فائدة اطلاقًا، ويتم تحميل نظام التشغيل على أي جهاز قبل شرائه، وقد شهدت أنظمة التشغيل تطورًا كبيرًا نتيجة الانفتاح المعلوماتي، وصدرت العديد من برامج التشغيل منها:

1- نظام التشغيل ويندوز (**Windows**) حيث يعد من أشهر أنظمة الحواسيب لان غالبية المستخدمين يتعاملون مع أجهزة ويندوز المتطورة وسهله الاستخدام، ظهر أول إصدار لهذا البرنامج في عام 1985م من قبل شركة مايكروسوفت العالمية وكان عبارة عن لوحة رسومية مساعدة لكتابة الأوامر في نظام دوس (**Dos**) وفي عام 1995م ظهر أول نظام مستقل لهذه الشركة بهدف التحكم التام في نظام تشغيل الكمبيوتر دون الحاجة للإدخال اليدوي لكل أمر وإضافة مزايا كتشغيل الفيديو وألعاب الفيديو وقد صدر العديد من النسخ المطورة من هذا النظام.

2- نظام لينكس(**Linux**) يعد هذا النظام من أكثر الأنظمة شهرة واستخدامًا بين أنظمة التشغيل، ويشبه في طريقة عمل الويندوز، ولكنة نظام مفتوح يسمح للمستخدمين بالوصول الى جميع تطبيقات أجهزة ونظام الحاسوب لتنفيذ العمليات والتعديل عليها، وهو صعب القرصنة ونقل الفيروسات اليه، ويستخدم بشكل خاص في اكتشاف أخطاء أجهزة الكمبيوتر ومحاولة إصلاحها وإنشاء خوادم الشبكة واستضافة مواقع الويب.

3- نظام أندرويد(**Android**) نظام تشغيل أصدر في عام 2008م من قبل شركة قوقل، وهو من أشهر أنظمة التشغيل للهواتف الذكية والحواسيب اللوحية، ويتحكم البرنامج بجميع أنظمة الهاتف التي تعمل بهذا النظام ومدعوم بأنظمة حماية وتشغيل من ذات الشركة، ولدية العديد من التطبيقات المجانية سهله التحميل.

4- نظام أي أو أس(**ios**) وهو نظام تشغيل محمول خاص يعمل على الأجهزة المحمولة أو أجهزة الكمبيوتر المكتبية والمحمولة واللوحية الخاصة بشركة آبل، وهو ثاني أكبر نظام تشغيل في العالم بعد نظام اندرويد، ويتميز بأنه نظام تشغيل آمن ومستقر وسهل الاستخدام ومتعدد اللغات.

مهام نظام التشغيل:-

نظام التشغيل يؤدي العديد من المهام التي تجعل استخدام الحاسوب ممكنًا بالنسبة للإنسان، نظرًا الى أن لغة الحاسوب لا تشبه لغة البشر والتعامل معها يحتاج الى لغة برمجية تؤدي دور الوسيط بين المستخدم والحاسب الآلي بمكوناته المختلفة.

وتختلف مهام كل نظام تشغيل باختلاف نوع جهاز الحاسوب، فالأجهزة الكبيرة التي يتطلب عملها الاتصال بأجهزة أخرى أو السماح لأكثر من شخص باستخدامها في وقت واحد تحتاج الى نظام تشغيل

يساعدها على التعامل مع وحدات الحاسوب وملحقاته، أما الحواسيب الشخصية فنظام تشغيلها يكون أكثر بساطة لأنها تتعامل مع مستخدم واحد وعمليات بسيطة.

وتعد أنظمة التشغيل مجموعة من البرمجيات عالية الجودة صُممت من قبل مخترعين وخبراء تتحكم في الأجهزة الإلكترونية، وتُسهل استخدام الأدوات المختلفة الموجودة فيها، فلا يمكن استخدام أي جهاز حاسوب أو هاتف دون وجود نظام التشغيل، ولا يمكن فتح واستخدام أي برنامج وتطبيق إلا باستخدام نظام التشغيل المناسب. (محمد سكيكر، 2010م، ص29)

ثالثًا الإنترنت:-

بدأت الإنترنت بالتشكل في أواخر الستينيات من القرن العشرين، وكانت وزارة الدفاع الأمريكية قلقة في ذلك الوقت بشأن إمكانية نشوب حرب نووية مدمرة؛ فبدأت في البحث عن وسائل لربط المنشآت الكمبيوترية معًا بطريقة تجعل قدرتها على الاتصال فيما بينها تصمد في مواجهة الحرب، وقد دشنت وزارة الدفاع وكالة أربا (ARPA) عام 1975م والتي أنشئت شبكة أربانت(**ARPA NET**) وهي شبكة من الحواسيب العسكرية والجامعية، ووضعت قواعد تشغيل الشبكة الأساس لتأمين اتصال سريع نسبيًا وخالٍ من الأخطاء بين كمبيوتر وأخر. (سمير الغزاوي، 2005م، ص9)

وظلت أربانت(**ARPA NET**) تنمو وتتطور طوال عقد السبعينات على نحو بطيء ولكنه مستمر، وبحلول عام 1983م(†)، قامت وزارة الدفاع بتقسيم الشبكة الى شبكتين احتفظت الشبكة الأولى باسمها الأساسي أربانت(**ARPA NET**) وغرضها في مجال الاستخدامات العسكرية، في حين سميت الشبكة الثانية باسم ميلانت (**MILNET**) وخصصت للاستخدامات المدنية أي تبادل المعلومات وتوصيل البريد الإلكتروني، ومنها ظهر مصطلح الإنترنت حيث أمكن تبادل المعلومات بين هاتين الشبكتين، وفي عام 1986م، أمكن ربط شبكات خمس مراكز للكمبيوترات العملاقة واطلق عليها أسم الانسفانت(**NSF NET**) والتي أصبحت فيما بعد العمود الفقري وحجر الأساس لنمو وازدهار الإنترنت في أمريكا ومن ثم دول العالم الأخرى. (سالم سليمان، 2014م، ص33)

وبدأت حواسيب من بلدان أخرى تنضم للشبكة، كما دخلت شبكات أخرى في الخدمة أيضاً مثل شبكة يو يو سي بي(**UUCP**) التي أنشئت لخدمة مستخدمي نظام التشغيل يونيكس، وشبكة

المستخدم(**يوزنت**) وهي وسيلة لنشر المقالات النصية حول العديد من الموضوعات. (الموسوعة العربية العالمية، 1425هـ، 2004م)

وبالتالي لا زال عدد المستخدمين لهذه الشبكة في ازدياد مستمر، ويمكن القول بالمقارنة مع عدد المستخدمين أنه ينضم أكثر من ستة وأربعين شخص كل دقيقة إلى شبكة الإنترنت على مستوى العالم، وفي تقرير نشرته شبكة(**NUA**) الأمريكية قدرت فيه أن عدد المستخدمين للإنترنت عام 2005م كان مائتين وخمسة وأربعين مليون شخص حول العالم، وفيما ذكرت قناة الجزيرة الوثائقية في برنامج بثته تحت إسم "حرب الإنترنت" إن عدد المشتركين في شبكة الإنترنت قد تجاوز المليار شخص في العام 2005م وذلك يدل على أن عدد مستخدمي شبكة الإنترنت حول العالم ينمو ويزيد بسرعة كبيرة من الصعب على البعض أحيانًا معرفتها أو حتى تقديرها. (منير، ممدوح الجنبيهي، 2006م، ص8)

الإنترنت(**Internet**) تعني الترابط بين الشبكات أو شبكة الشبكات، وهي اختصار للمصطلح الإنجليزي(**Interconnected Network**) وتتكون شبكة الإنترنت أو الشبكة العالمية من عدد مهول من أجهزة الحواسيب المرتبطة مع بعضها البعض تحت تنظيم بروتوكولات معينة تسمى ببروتوكولات تراسل الإنترنت، وتأتي تسمية شبكة المعلومات الدولية بالإنترنت تمييزًا لها عن غيرها من الشبكات كـ"الإنترانت" (**Intranet**) و"الإكسترانت" و"الاربانت" أو الانسفانت، رغم أن هاتين الأخيرتين تعتبران أساس ونواة قيام الإنترنت العالمية.

وتتكون شبكة الإنترنت من عشرات الملايين من شبكات الكمبيوتر الصغيرة تربط الكثير من المؤسسات التجارية والمعاهد والأفراد حول العالم، وبذا تمكن شبكة الإنترنت مستخدمي الكمبيوتر في جميع أرجاء العالم من استخدامها في أغراض الحياة المختلفة، وإرسال واستقبال الرسائل، وتبادل المعلومات بأشكالها المختلفة بل وممارسة الألعاب الإلكترونية وألعاب الكمبيوتر مع أناس يتصلون بالشبكة من أقاليم ودول أخرى.

وتتباين أجهزة الحواسيب الموصلة بشبكة الإنترنت بحسب استخدام هذه الحواسيب واستخدام الشبكة أيضًا، فتوجد الحواسيب البسيطة الرخيصة المعروفة غالبًا باسم الحواسيب الشخصية(**Personal computer**) وتوجد أيضًا الحواسيب الرئيسية الضخمة التي تستخدمها المؤسسات الحكومية، والمعاهد التعليمية والشركات التجارية، وغيرها من المؤسسات والشركات المختلفة الأخرى.

ويمكن تعريف الإنترنت بأنها مجموعة كبيرة من شبكات الحاسب المترابطة والمنتشرة في أنحاء كثيرة من العالم، ويمكن من خلالها تبادل الملفات والتقارير والبرامج والتطبيقات والبيانات والمعلومات. (إسماعيل حميد، 2021م، ص271)

وتقوم فكرة عمل الإنترنت على مشاركة المعلومات، بمعنى أن المعلومة المرفوعة على شبكة الإنترنت تصبح متاحة لمستخدمي الشبكة المتصلين بها، فعند الدخول إلى الشبكة عن طريق أحد متصفحات أو مستعرضات الشبكة المثبتة على جهاز الكمبيوتر وكتابة العنوان المقصود نرى عادة أن العنوان الإلكتروني للشركة يبدأ بالأحرف(**www**) وهذه الأحرف هي اختصار لعبارة(**World Wide Web**) وتعني أن المتصفح يريد دخول شبكة الإنترنت العالمية واستخدامها، وعند تشغيل المستعرض يمكن للمستخدم الوصول إلى ملايين المواقع حول العالم، ولكل موقع عنوانه الإلكتروني الخاص به الذي يشار إليه بالأحرف(**URL**) وهي اختصار لمصطلح "محدد موقع المعلومات" على شبكة الإنترنت (**Uniform Resource Locator**) وهناك أدلة لهذه العناوين تجري المحافظة عليها ويتم تحديثها بصورة مستمرة عبر الشبكة نفسها، وتنظم العناوين نفسها عن طريق تقسيمها إلى فئات عديدة مثل التعليمية والتجارية أو المنظمات، وفي حالة عناوين هذه الفئات قد يأخذ نوع المجال رموزًا عبارة عن أحرف لاحقة تدل على فئة الموقع مثل(.**edu**) وهي اختصار لكلمة تعليمية (**educational**) أو(.**com**) وهي اختصار لكلمة تجارية (**commercial**) أو(**tv**) وهي اختصار لكلمة تلفزيونية (**television**) وبإمكان المستخدم إرسال طلب عبر مقدم خدمة الإنترنت إلى الشبكة عن طريق كتابة العنوان المطلوب أو النقر بمؤشر الفأرة(**mouse**) على صورة أو كلمة مرتبطة إلكترونيًا بالعنوان وعندما يصل الطلب إلى وجهته يستجيب الكمبيوتر الملقم بإرسال المعلومات المطلوبة للمستخدم، وتأخذ هذه المعلومات في الغالب شكل صفحة بداية رئيسية تعرف باسم الصفحة الأم(**Home page**) وهي مماثلة لجدول المحتويات في كتاب أو مجلة، وانطلاقًا من الصفحة الأم يمكن للمستخدم البحث عن مزيد من المعلومات عن طريق الارتباطات التي تمكنه من الانتقال إلى صفحات أخرى في نفس موقع الويب، أو في مواقع الويب الأخرى، بالإضافة إلى ذلك فإن لغة البرمجة المستخدمة في الويب، أو لغة ترميز النص التشعبي والمعروفة بـ(**HTML**) اختصارًا لـ (**Hyper Text Markup Language**) تلعب دور الوسيط لعملية الربط بين المعلومات

الواردة من حواسيب موجودة حول العالم، وقد أدى هذا التطور إلى إيجاد دليل تفاعل يمكن المستخدمين من القفز بسهولة من محتويات أحد الحواسيب إلى محتويات كمبيوتر أخر متعقبين أثر المعلومات حول العالم.

وقد تطورت شبكة الإنترنت مؤخرًا حتى أصبح نظام طلب المعلومات عن طريق الشبكة من الشبكة نفسها، فبدلاً من أن كان دور شبكة الإنترنت يقتصر على تمثيل دور الوسيط بين طالب المعلومة والخادوم (عبدالحميد بسيوني، 2004م، ص10)، الموفر لها صار طلب المعلومات من الشبكة نفسها وتخزن المعلومات على شبكة الإنترنت نفسها وذلك عن طريق ما يسمى بـ "بروتوكول نقل النص التشعبي" **Hyper Text Transfer Protocol**) أو اختصارًا (**HTTP**) ويوفر هذا البروتوكول العديد من المزايا لاستخدام شبكة الإنترنت والحصول على المعلومات من الشبكة مباشرة مثل إتاحة المعلومات في أي وقت لطالبها، وتقليل التحكم وإدارة تلك المعلومات من قبل أصحابها والسرعة في الحصول على المعلومة نفسها.

خصائص شبكة الإنترنت:-

1- اللا مكان فإنها شبكة إلكترونية تتخطى كل الحواجز الجغرافية والمكانية؛

2- اللا زمان نظرًا للسرعة الكبيرة التي يتم بها نقل المعلومات عبر الشبكة تسقط عامل الزمن من الحسابات؛

3- التفاعلية فالفرد يستطيع أن يحدد ماذا ومتى يحصل على ما يريد من معلومات؛

4- المجانية فإن خدمات الإنترنت من الخدمات الأساسية في الحياة التي تتوفر بشكل شبة مجاني أو مجاني؛

5- الربط الدائم حيث أصبح بإمكان الفرد أن يتصل بالإنترنت من خلال طائفة متنوعة من الأوامر بواسطة الحاسب الآلي أو الهواتف النقالة وغيرها؛

6- السهولة يستطيع صغير السن أو الرجل الكبير أن يستخدم الإنترنت بسهولة ولايحتاج إلى تدريبات للبدء في استخدام الإنترنت بل يحتاج إلى توضيح بالمبادئ الأولية للاستخدام. (محمد سكيكر، 2010م، ص29)

المطلب الثاني

خصائص وأنواع المعلومات

المعلومات هي الحقائق والافكار والأخبار التي يتبادلها الناس في حياتهم العامة عبر وسائل الاتصالات المختلفة، والإنسان الذي يحتاج المعلومة ويستخدمها هو نفسة منتج لمعلومات أخرى وناقل لها عبر وسائل الاتصال.

المعلومة قد تكون نوعًا من المعرفة وقد تكون في شكل هندسي، وقد تكون مجموعة من الإرشادات والأوامر، وقد تتعلق بأمور مالية أو فنية أو أدبية وهي تختلف فيما بينها من حيث أهميتها ونوعها.

الفرع الأول خصائص المعلومات:-

بمجرد استكمال المعلومة يتم التعبير عنها بواسطة الإنسان بطريقة مباشرة أو عبر وسيط إلكتروني، وقد تكون المعلومة معرفية أو مهارية أو رقمية وحسابية وغيرها.

ولكي تكون المعلومات ذات قيمة يجب أن تتوفر فيها مجموعة من الخصائص نذكر منها:-

1- الملائمة وهو المعيار الأساسي لقيمة المعلومة حيث تتلاءم المعلومات مع الغرض الذي أُعدت من أجله، ويمكن الحكم على مدى الملائمة بكيفية التأثير على سلوك المستخدمين؛

2- الوضوح وهي أن تغطي المعلومات الهدف المراد لها وخالية من الغموض؛

3- الموضوعية وهي أن تتصف بعدم التحيز وتكون حقيقية؛

4- الوقتية أن تقدم المعلومات في الوقت المناسب وتكون مفيدة ومؤثرة؛

5- الشمول وهو أن تكون المعلومات كاملة في شكلها النهائي. (محمد سكيكر، 2010م، ص32)

الفرع الثاني انواع المعلومات:- (محمد سكيكر، 2010م، ص33)

المعلومات هي الأساس في البناء والتطور والإبداع، وهي عبارة عن مجموعة بيانات لها مدلول معين تستخدم في العديد من المجالات الصحية والاقتصادية والسياسية والاجتماعية وكذلك في المجال العسكري والأمني ومنها:-

1- المعلومات التطويرية وهي التي يمكن الحصول عليها من خلال القراءة والاطلاع على الكتب أو المقالات وتنمي القدرات المعرفية؛

2- المعلومات الفكرية وهي معلومات نابعة عن فكر الإنسان نتيجة تعليمه وقراءته فهي تخرج على شكل نظريات وحقائق علمية؛

3- المعلومات التعليمية عبارة عن تلقين وتعليم الشخص لهذه المعلومات؛

4- المعلومات النظامية وهي جمع البيانات والنظريات من أجل القيام ببحث علمي؛

5- المعلومات البحثية عبارة عن النتائج والفرضيات التي يصل اليها الباحث أو بعد إجراء التجارب العلمية؛

6- المعلومات الإخبارية يستطيع الفرد الحصول عليها من أجل الوصول لقرار أو تحقيق هدف؛

7- المعلومات السرية وهي معلومات قد تكون ذات سرية مرتفعة أو متوسطة وقد تكون رموز أو إشارات أو شفرات رقمية يصعب الوصول اليها.

المبحث الثاني

دور الاتفاقيات الدولية والتشريعات الوطنية في مكافحة جرائم تقنية المعلومات

تمهيد:-

إن التطور الكبير لتكنولوجيا المعلومات لم يكن مصحوبًا بقواعد قانونية واضحة، الأمر الذي أثار عددًا من المخاوف المتعلقة بجرائم تقنية المعلومات وخصوصيات الأفراد وحدود الرقابة والثغرات الأخرى.

وقد استحوذ الخطر المتزايد بهذه الجرائم على اهتمام منظمة الأمم المتحدة والوكالات التابعة لها الخاصة بتقنية المعلومات، أصدرت العديد من القرارات الدولية.

وللحفاظ على الأمن المعلوماتي يتم إبرام بعض الاتفاقيات الدولية التي تشكل نوعًا من الاطار القانوني واعتماد إستراتيجية استرشادية على المستوى الدولي والإقليمي.

ولكن في الواقع إن القوانين الداخلية القائمة للدول لاتزال متأخرة في تنظيم تقنية المعلومات، مما يجبر الأشخاص الطبيعية والأشخاص الاعتبارية على اتخاذ تدابير تقنية محدودة لحماية مصالحها.

وأمام هذا الوضع الذي يتخطى الحدود الجغرافية، حاولت عددًا من الدول وضع قواعد قانونية تحد من ارتكاب جرائم تقنية المعلومات عبر الاسترشاد بالقرارات والاتفاقيات الدولية في قوانينها الداخلية والخاصة بتقنية المعلومات.

المطلب الأول

دور المنظمات والاتفاقيات الدولية في مكافحة جرائم تقنية المعلومات

من المؤكد إن الجرائم الإلكترونية تنمو عن طريق استغلال الانتشار الواسع لتكنولوجيا المعلومات والاتصالات ووصولها الى مستخدمين غير مدركين مخاطر أفعالهم الإجرامية على الأفراد والمجتمعات لتحقيق اغراضهم والتي تسبب خسائر مالية ودمار إلكتروني وتعدي على خصوصيات الأفراد.

إن سرعة التطور التكنولوجي تجعل وسائل الدفاع والوقاية في أمن المعلومات بطيئة وغير ملائمة نظرًا لسرعة التغيير والابتكار، وزيادة الانفتاح والربط بين الشبكات المعلوماتية العالمية.

ولسلامة استخدام التكنولوجيا المتطورة وشبكات المعلومات، ولحماية حقوق الإنسان في الحصول على المعلومات، وفرض التعايش السلمي بين شعوب العالم، تعمل منظمة الأمم المتحدة والمنظمات التابعة لها، على إصدار قرارات دولية تحرم التعدي على هذه الحقوق وتضع معايير ملزمة للحماية.

وللحد من انتشار جرائم تقنية المعلومات، تسعى العديد من الدول لإبرام اتفاقيات جماعية في اطار جغرافي لتحسين القدرات في التحقيق وتبادل المعلومات.

الفرع الأول دور المنظمات الدولية في مكافحة جرائم تقنية المعلومات:-

تعمل منظمة الأمم المتحدة منذ فترة طويلة في مجال تأمين سلامة استخدام التكنولوجيا وشبكات المعلومات، وتشارك وكالات الأمم المتحدة المختلفة في مختلف المفاوضات لإيجاد توافق في الآراء بشأن عدد من القضايا، بما في ذلك وضع معايير توفير الحماية لشبكات المعلومات.

أولاً قرارات الجمعية العامة للأمم المتحدة هي:- (www.un.orq)

1- القرار(121/45) لعام 1990م بمنع جرائم الكمبيوتر؛

2- القرار(63/55) بتاريخ 4 ديسمبر 2000م، بخصوص الجرائم السيبرانيه أو المعلوماتية، بأن تُضمن الدول في قوانينها وممارستها إلغاء أية ملاذات آمنة لكل من يسئ استخدام تكنولوجيا المعلومات، وأن تحمي سرية المعلومات وأنظمة الحاسوب وسلامتها من الاعتداء غير المشروع وأن تجرم الأفعال الإجرامية الإلكترونية؛

3- القرار(199/58) في يناير 2004م، بشأن "إنشاء ثقافة عالمية للأمن السيبراني" والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني؛

4– القرار(177/60) لسنة 2005م، بخصوص التعاون لمكافحة الجرائم السيبرانيه حيث يشجع الدول في مكافحة الجرائم السيبرانيه وتقديم المساعدة للدول الأعضاء؛

5– القرار(211/64) لسنة 2010م، بتحديث القوانين، الذي يدعو الدول الى تحديث قوانينها في مجال الجرائم السيبرانيه والبيانات الشخصية والتجارة والتواقيع الإلكترونية.

ثانيًا جهات تابعة للأمم المتحدة:–

هناك العديد من القرارات الصادرة عن جهات تابعة للأمم المتحدة في مجموعة من المجالات ذات الصلة بأمن الفضاء الإلكتروني مثل:–

1– قرار المجلس الاقتصادي والاجتماعي(E/20) بتاريخ 2007/7/26م، بشأن التعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية؛

2– قرار لجنة مكافحة المخدرات(5/48) تاريخ 2005/12/1م، حول تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات؛

3– التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات(INCB) التي نُشرت في عام 2005م، للحد من انتشار المبيعات غير المشروعة من المستحضرات الصيدلانية عبر الإنترنت. (www.un.orq)

وتدعو الأمم المتحدة في قراراتها المختلفة دائمًا الدول الأعضاء عند وضع القوانين الوطنية والسياسة العامة لمكافحة سوء استخدام تكنولوجيا المعلومات، أن تأخذ بعين الاعتبار قراراتها، وتوصيات اللجان الخاصة بمنع الجريمة، وكذلك المؤتمرات واللقاءات المخصصة لهذه الجرائم العابرة للحدود الجغرافية، والمهددة للأمن والاستقرار والرفاه في العالم.

ثالثًا الوكالات المتخصصة:–

الاتحاد الدولي للاتصالات، هو وكالة تتبع الأمم المتحدة، ومجال العمل هو مسائل تكنولوجيا المعلومات والاتصالات، ويعتبر النقطة المركزية الأولى للحكومات وللقطاع الخاص في مساعدة العالم على الاتصال، ويضم ثلاث قطاعات رئيسية هي قطاع الاتصالات الراديوية، وقطاع تقييس الاتصالات، وقطاع تنمية الاتصالات. (ويكيبيديا، وقت الدخول 9 pm، 8 نوفمبر 2022م)

ويوفّر الاتحاد الدولي للاتصالات الذي يضم في عضويته 192دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية منبرًا إستراتيجيًا للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة، ويعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات، وقد وضع الاتحاد الدولي للاتصالات مخططًا لتعزيز الأمن السيبراني العالمي يتكون من سبعة أهداف رئيسية هي:

1– وضع إستراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة؛

2– وضع إستراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلقة بجرائم الإنترنت؛

3– وضع إستراتيجية لتحديد الحد الأدنى المقبول عالميًا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة؛

4– وضع إستراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود؛

5– وضع إستراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية؛

6– تطوير إستراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية؛

7– تقديم المشورة بشأن إمكانية اعتماد إطار إستراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها. (الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانيه في المنطقة العربية، 2015، ص9)

الفرع الثاني دور الاتفاقيات الدولية في مكافحة جرائم تقنية المعلومات:–

تم إبرام العديد من الاتفاقيات بخصوص أمن المعلومات في اطار الاتحاد الأوروبي والاتحاد الأفريقي، لغرض معالجة الجرائم الإلكترونية المتطورة وحماية الحقوق الأساسية للإنسان، ومؤامة التشريعات الوطنية مع إستراتيجية الاتفاقيات في الحد من جرائم تقنية المعلومات.

وقد سعت الدول العربية الى تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، ولحاجتها الماسة الى تبني سياسة جنائية مشتركة تهدف الى حماية المجتمع العربي ضد جرائم تقنية المعلومات من خلال عقد الاتفاقيات التي تراعي النظام الداخلي لكل دولة، وتلتزم بالمعاهدات والاتفاقيات الدولية المتعلقة بحقوق الإنسان وحمايتها.

أولاً الاتفاقية المتعلقة بالجريمة الإلكترونية "بودابست" 2001م:-

تعتبر من أهم الاتفاقيات الإقليمية التي ساهمت في معالجة الجرائم المعلوماتية، وفرض التزامات محددة على الدول الأطراف فيها لتحسين القدرات الوطنية للتحقيق في هذه الجرائم والتعاون الدولي وتسليم المجرمين، وإن اتفاقية المجلس الأوروبي تحتوي على(**48 مادة**) تسعى من خلالها الى معالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر المؤامة بين القوانين الوطنية وقوانين الدول الأخرى وتهدف الى:-

1- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية؛

2- توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونيًا؛

3- تعيين نظام سريع وفعال للتعاون الدولي؛

4- الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر؛

5- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها؛

6- المساعدة المتبادلة في جمع حركة المعلومات واعتراضها؛

7- تسهيل الإجراءات المتعلقة بطلبات المساعدة المتبادلة؛

8- التعاون الدولي في تسليم المجرمين والإنابة القضائية الدولية. (اتفاقية بودابست، 2001م)

وغرض الاتفاقية هو احترام حقوق الإنسان وحرياته الشخصية، والحد من تلك الجرائم التي قد يتعرض لها، وقد صنّفت الاتفاقية هذه الجرائم بأربعة أنواع مختلفة هي:-

- **الجرائم ضد سلامة المعلومات وخصوصيتها:**

وتتمثل في النفاذ الكامل أو الجزئي الى نظام الكمبيوتر، بشكل متعمد بغرض الحصول على بيانات أو معلومات للاستفادة وتحقيق الاضرار بالغير ومنها:- (المواد 2، 3، 4، 5، 6)

1- الدخول غير المشروع؛

2- الاعتراض غير القانوني؛

3– التجسس على البيانات والمعلومات؛

4– التدخل في البيانات والمعلومات؛

5– التدخل في أنظمة الكمبيوتر وبرامجه.

- **الجرائم المتصلة بالكمبيوتر:**

وهي عبارة عن أفعال مجرمة ترتكب بصفة عمدية للحصول بدون وجه حق على منفعة اقتصادية ذاتية أو لفائدة شخص أخر طبيعي أو شخص اعتباري وتشمل:- (المادتان7، 8)

1– استخدام الكمبيوتر للتزوير؛

2– النصب والاحتيال الإلكتروني؛

3– سرقة البيانات الشخصية.

- **الجرائم المتصلة بالمحتوى:**

يقصد بها الجرائم ذات الصلة بالأشخاص الطبيعية أو الأشخاص الاعتبارية، حيث تعرض بشكل مرئي أو بواسطة وسائل تقنية المعلومات، لتعود بالفائدة المادية أو المعنوية للمجرم أو لصالح شخص أخر طبيعي أو شخص اعتباري وهي:- (المادة 9)

1– التشهير والمعلومات الكاذبة؛

2– وجود مضمون جنسي أو إباحي؛

3– مواد إباحية ذات علاقة بالأطفال؛

4– العاب القمار والألعاب غير المشروعة على الإنترنت؛

5– بيانات التحريض على العنصرية والكراهية وتمجيد العنف؛

6– التعرّض للأديان؛

7– البريد المزعج؛

8– أي مواد أخرى.

- **الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة:**

وهي كل الأفعال التي ترتكب عمدًا أو بالمساعدة أو بالتحريض على كافة حقوق النشر والتأليف والحقوق المصاحبة على نطاق تجاري بواسطة وسائل تقنية المعلومات، لمصلحة أفراد أو جماعات أو منظمات أو دول ومنها:- (المادة 10)

1- تبادل الأغاني والملفات والبرامج المحمية في حقوق التأليف والنشر من خلال برامج تبادل المعلومات؛

2- استخدام العلامات التجارية في أنشطة إجرامية بهدف التضليل؛

3- التحايل على نظم إدارة الحقوق الرقمية؛

4- الجرائم ذات الصلة باسم المواقع الإلكترونية.

ثانيًا أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي2014م:- (اتفاقية الاتحاد الأفريقي)

تعتبر اتفاقية ذات طابع إقليمي تضم دول الاتحاد الأفريقي، لغرض تدارك انتشار الجرائم الإلكترونية التي تشكل تهديدًا حقيقيًا لأمن الاتحاد، وتهدف الى تحديد الأهداف والتوجهات الرئيسية لمجتمع المعلومات في أفريقيا وتعزيز التشريعات والأنظمة الحالية الخاصة بتكنولوجيا المعلومات والاتصال للدول الأعضاء والمجموعة الاقتصادية الدولية وكفالة الأمن المعلوماتي والإطار القانوني الضروري لظهور اقتصاد المعرفة في أفريقيا، وتهدف كذلك الى تحديث القوانين الجنائية في قمع الجريمة الإلكترونية من خلال وضع سياسات لاعتماد جرائم جديدة خاصة بتكنولوجيا المعلومات والاتصالات ومواءمة نظام العقوبات الموجود فعليًا في الدول الأعضاء مع المناخ التكنولوجي الحديث، وتأخذ في الاعتبار تطبيق قانون الإجراءات الجزائية في تحديد الشروط الخاصة بالجرائم الإلكترونية. (المواد 24، 25، 26)

وتؤكد تمسك الدول الأعضاء بالحريات الأساسية وحقوق الإنسان والشعوب المكفولة بموجب القوانين الداخلية للدول الأعضاء، والواردة في الإعلانات والاتفاقيات الدولية، والصكوك في إطار الاتحاد الأفريقي والأمم المتحدة. (المواد 26، 27)

وتتطلع الى الاستجابة للاحتياجات المتمثلة في وضع تشريعات متناسقة في مجال الأمن الإلكتروني بالدول الأعضاء لمكافحة انتهاكات البيانات ذات الطابع الشخصي، وتتكون الاتفاقية من(**38 مادة**).

وقد وضحت الاتفاقية التعريف بالبيانات ذات الطابع الشخصي بأنها (أي معلومات متصلة بشخص طبيعي محدد أو قابل للتحديد بشكل مباشر أو غير مباشر بالإشارة الى رقم هويته أو الى عامل واحد أو أكثر محدد لهويته الطبيعية أو السيكولوجية أو الذهنية أو الاقتصادية أو الثقافية أو الاجتماعية)، وإن معالجة البيانات ذات الطابع الشخصي تعني (أي عملية أو مجموعة عمليات تجري على بيانات شخصية بمساعدة أو بدون مساعدة طرف آلية، مثل جمع وتسجيل وتنظيم وحفظ وتكييف وتعديل واستخلاص وحماية ونسخ والكشف من خلال الإرسال ونشر أو أي شكل أخر من أشكال الإتاحة عن طريق القفل أو الرابط بالإضافة الى تشفير وحذف وإتلاف بيانات شخصية). (المادة الأولى)

وقد حددت الاتفاقية الجرائم الخاصة بتقنية المعلومات على النحو التالي:- (المادة 29)

- **الهجمات على أنظمة الكمبيوتر:**

أ. وصول أو محاولة الوصول الغير مصرح به الى أجزاء أو كل نظام الحاسب الآلي أو تجاوز الوصول المسموح به؛

ب. وصول أو محاولة الوصول غير المصرح به الى أجزاء أو كل نظام الحاسب الآلي أو تجاوز الوصول المسموح به، بقصد ارتكاب جريمة أخرى أو تسهيل ارتكاب جريمة؛

ج. البقاء أو محاولة البقاء عن طريق الاحتيال في كل أو جزء من نظام الحاسب الآلي؛

د. إعاقة وتشوية أو محاولة لإعاقة أو تشوية أداء نظام الحاسب الآلي؛

هـ. إدخال أو محاولة إدخال البيانات عن طريق الاحتيال في نظام الحاسوب؛

و. إتلاف أو محاولة إتلاف وحذف أو محاولة حذف أو إفساد أو محاولة إفساد أو تغيير أو محاولة تغيير أو تعديل أو محاولة تعديل لبيانات الكمبيوتر عن طريق الاحتيال.

- **الخروقات على البيانات المحوسبة:**

أ. اعتراض أو محاولة لاعتراض البيانات المحوسبة عن طريق الاحتيال بواسطة الوسائل التقنية أو تجاوز الصلاحية أو إتلاف سرية المعلومات أثناء الأرسال وأثناء انتقال البيانات من والى أو داخل منظومة الحاسب الآلي؛

ب. التعمد في إدخال أو تغيير أو حذف بيانات الحاسب الآلي؛

ج. استخدام البيانات التي تم الحصول عليها من نظام الحاسب الآلي عن طريق الاحتيال مع العلم بذلك؛

د. شراء عن طريق الاحتيال لمصلحته شخصيًا أو لمصلحة شخص أخر أي فائدة من خلال إدخال أو تعديل أو حذف أو إخفاء بيانات محوسبة أو أي شكل أخر من أشكال التدخل في أداء الحاسب الآلي؛

هـ. أية معالجة أو السماح لمعالجة بيانات ذات طابع شخصي؛

و. المشاركة في تشكيل جماعة بهدف إعداد أو ارتكاب جريمة أو أكثر من الجرائم المنصوص عليها بهذه الاتفاقية.

- **الجرائم ذات الصلة بالمحتوى:**

أ. إنتاج وتسجيل أو عرض أو تصنيع أو توفير أو نشر أو نقل صورة أو تمثيل المواد الإباحية الخاصة بالأطفال أو أي انتاج من المواد الإباحية الخاصة بالأطفال عن طريق جهاز الحاسب الآلي؛

ب. الشراء للحيازة أو لصالح شخص أخر أو الشروع في الاستيراد أو التصدير لصورة أو تمثيل من المواد الإباحية الخاصة بالأطفال؛

ج. امتلاك صورة أو تمثيل المواد الإباحية الخاصة بالأطفال؛

د. تسهيل أو منح حق الوصول الى الصور والوثائق والاصوات أو أي تمثيل مواد إباحية لقاصر؛

هـ. إنتاج أو تحميل ونشر أو إتاحة بأي شكل من الأشكال كالكتابات والرسائل والصور والرسومات أو أي تمثيل أخر للأفكار أو النظريات العنصرية أو المتعلقة بكراهية الأجانب؛

و. التهديد من خلال نظام الحاسب الآلي بقصد اركاب جريمة جنائية ضد أي شخص لأسباب تتعلق بانتمائه الى مجموعة عرقية أو اللون أو النسب أو الأصل القومي أو الديني؛

ز. إهانة بواسطة الحاسب الآلي لاي أشخاص لأسباب تتعلق بانتمائهم الى مجموعة عرقية أو اللون أو النسب أو الأصل القومي أو الاثني أو الديني أو الرأي السياسي؛

ح. الإنكار المتعمد أو الموافقة أو تبرير الأفعال التي تعتبر إبادة جماعية أو جرائم ضد الإنسانية من خلال الحاسب الآلي.

- **الجرائم المتعلقة بإجراءات تأمين الرسائل الإلكترونية:**

حيث تلتزم الدول الأعضاء باتخاذ ما يجب من تدابير تشريعية أو تنظيمية لضمان المحافظة على أدلة الإثبات الرقمية في القضايا الجنائية.

واضافة المادة (30) مواءمة جرائم معينة(جرائم الممتلكات) الى تكنولوجيا المعلومات والاتصالات، منها جرائم السرقة الإلكترونية وجرائم الابتزاز المالي، وجرائم غسل الأموال وجريمة الإرهاب الإلكتروني، والجرائم المتعلقة بالأمن القومي.

وفي مواجهة الأشخاص الاعتبارية (تلتزم الدول الأطراف باتخاذ ما يجب من التدابير التشريعية اللازمة لضمان أن تتحمل الأشخاص الاعتبارية غير الدولة، المجتمعات المحلية والمؤسسات العامة، المسؤولية عن الجرائم المنصوص عليها في هذه الاتفاقية، التي ترتكب نيابة عنها من قبل أعضائها أو ممثليها، إن مسؤولية الأشخاص الاعتباريين لا تستبعد مسؤولية الأشخاص الطبيعيين الذين هم مرتكبي أو شركاء في نفس الجرائم). (المادة 2/30)

ثالثًا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010م:-

تسعى الدول العربية الى مواكبة تطور تكنولوجيا المعلومات من خلال إصدار الارشادات للتعامل مع أدوات تقنية المعلومات، ونظرًا الى ارتفاع مؤشر جرائم تقنية المعلومات وتطور أساليبها وأنواعها، حرصت الدول العربية على مكافحة هذه الجرائم من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لسنة 2010م)

وقد أخذت بالمبادئ الدينية والأخلاقية السامية والالتزام بأحكام الشريعة الإسلامية مع مراعاة النظام الداخلي لكل دولة، وتعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، والالتزام بالمعاهدات والمواثيق الدولية المتعلقة بحقوق الإنسان، وتتكون الاتفاقية من(**43 مادة**) موزعة الى خمسة فصول، ورد في الفصل الأول تعزيز التعاون بين الدول العربية، وتعريف بالمصطلحات المرتبطة بالاتفاقية، ومجال تطبيق الاتفاقية على جرائم تقنية المعلومات، وفي الفصل الثاني نص بدعوة الدول الأطراف الى تجريم الأفعال المذكورة ضمن قوانينها الوطنية، وذكر في الفصل الثالث كل ما يتعلق بالأحكام الإجرائية من حيث نطاق تطبيقها والتحفظ على البيانات والتفتيش وغيرها، وبالفصل الرابع تم تخصيصه للتعاون القانوني

والقضائي للحد من ارتكاب جرائم تقنية المعلومات، وورد في الفصل الخامس أحكام ختامية، وقد تضمنت الاتفاقية الأفعال الإجرامية التالية:-

1- جريمة الدخول غير المشروع (المادة 6)؛

2- جريمة الاعتراض غير المشروع (المادة 7)؛

3- جريمة الاعتداء على سلامة البيانات (المادة 8)؛

4- جريمة إساءة استخدام وسائل تقنية المعلومات (المادة 9)؛

5- جريمة التزوير باستخدام وسائل التقنية المعلوماتية (المادة 10)؛

6- جريمة الاحتيال الإلكتروني (المادة 11) ؛

7- الجرائم الإباحية باستعمال أدوات تقنية المعلومات (المادة 12)؛

8- جريمة القمار والاستغلال الجنسي (المادة 13)؛

9- جريمة الاعتداء على حرمة الحياة الخاصة (المادة 14)؛

10- جرائم الإرهاب الإلكتروني (المادة 15) ؛

11- الجرائم المنظمة عبر الوطنية (المادة 16)؛

12- الجرائم المتعلقة بانتهاك حق المؤلف (المادة 17)؛

13- جرائم الاستخدام غير المشروع لأدوات الدفع الإلكترونية (المادة 181).

وحددت الاتفاقية المسؤولية الجنائية للأشخاص الطبيعية والمعنوية، حيث نصت المادة (20) على (أن تلتزم كل دولة طرف مع مراعاة قانونها الداخلي بترتيب المسؤولية الجزائية للأشخاص المعنوية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيًا).

رابعًا وثيقة الرياض 2012م:-

هي وثيقة للنظام "القانون" الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية، وتتكون من(**39 مادة**) عرفت النظام المعلوماتي ووسائل تقنية المعلومات، وأوجبت التعاون الدولي في تسليم المجرمين بين دول مجلس التعاون الخليجي مع عدم الاخلال بالاتفاقيات الدولية، وتهدف الى منع إساءة استخدام تقنية المعلومات، وشملت صور جرائم تقنية المعلومات بالاتي:

1- الدخول غير المشروع أو تجاوز الدخول المصرح به (المادة 3)؛
2- سرقة البيانات والمعلومات الشخصية (المادة 5)؛
3- التزوير الإلكتروني (المادة 7) ؛
4- التدخل في أنظمة الكمبيوتر وبرامجه (المادة 8)؛
5- إعاقة أو تعطيل الوصول الى الخدمات الإلكترونية(المادة 9)؛
6- التنصت أو الاعتراض لما هو مرسل عبر الشبكة المعلوماتية (المادة 11)؛
7- التهديد والابتزاز (المادة 13) ؛
8- الاحتيال المعلوماتي (المادة 14) ؛
9- التقاط خدمات الاتصالات أو قنوات البث المرئية والمسموعة بوسائل التقنية (المادة 18)؛
10- استغلال وسائل تقنية المعلومات في مواد إباحية أو أنشطة للقمار (المادة 20)؛
11- تحريض أو إغواء ذكرًا أو انثى لارتكاب الدعارة أو الفجور (المادة 21)؛
12- الإساءة الى المقدسات والشعائر والأديان السماوية (المادة 22)؛
13- الاعتداء على المبادئ والقيم الاسرية (المادة 23)؛
14- جرائم القذف والتشهير الإلكتروني (المادة 24)؛
15- جرائم الاتجار في الأشخاص، أو الاتجار بالأعضاء البشرية بالوسائل الإلكترونية (المادة 25)؛
16- الاتجار أو الترويج أو التعاطي للمخدرات أو المؤثرات العقلية (المادة 26)؛
17- جرائم غسل الأموال (المادة 27) ؛
18- جرائم الاخلال بالنظام والآداب العامة (المادة 28)؛
19- الإرهاب الإلكتروني (المادة 29) ؛
20- إنشاء موقع إلكتروني أو نشر معلومات عن الاتجار بالآثار أو التحف الفنية غير المصرح بها قانونًا. (المادة 30)

ونصت المادة (33) على(... يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكب أي من الجرائم المنصوص عليها في هذا النظام "القانون" أو الأموال المتحصلة منها،

كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم إغلاقًا كليًا أو للمدة التي تقدرها المحكمة إذا كانت الجريمة قد ارتكبت بعلم مالكها).

المطلب الثاني

دور التشريعات الوطنية في مكافحة جرائم تقنية المعلومات

تجريم الأفعال والعقاب عليها تعد من أخطر الأمور التشريعية التي تتصل بحرية المواطنين نتيجة ما تخلفه من الآثار التي تترتب عليه، ولذلك فان النصوص التشريعية الصادرة يجب أن تكون وفقًا لمبدأ الشرعية القانونية، وتختص السلطة التشريعية بتحديد الجرائم والعقوبات، وتلتزم عند وضعها للنصوص الجنائية أن تحدد المصالح الأساسية للأمة التي يقوم عليها بنيان المجتمع ويجب حمايتها، وأن تكون صياغة النصوص واضحة ومحددة لا خفاء فيها ولا غموض، وتحقق مبدأ العدالة والردع العقابي.

وبما أن العالم أصبح قرية واحدة إلكترونيًا وأصبحت وسائل الاتصالات في متناول غالبية المجتمعات، وبما أن جرائم تقنية المعلومات تجاوزت الحدود الجغرافية، وأصبحت تهدد أمن ورفاهية العالم فيجب وضع نصوص قانونية داخلية تتوافق مع الاتفاقيات الدولية للحد من ارتكاب جرائم تقنية المعلومات.

الفرع الأول دور التشريعات العربية في مكافحة جرائم تقنية المعلومات:-

حال التشريعات في الدول العربية متفاوت بين دولة وأخرى، فبعض الدول قد سعت ولكن بخطوات بطيئة في معالجة جرائم تقنية المعلومات، وذلك لبعدها عن التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي، وبما أن العديد من الدول أخذت بالسير في وضع التشريعات القانونية اللازمة لمكافحة هذه الجرائم، والبعض الأخر لا زال لم يحرك ساكنًا ويعتمد على تطبيق القانون الجنائي التقليدي على هذه الجرائم، والتي تفرض نوعًا من الحماية الجنائية ضد الأفعال المشابهة بالأفعال المكونة لأركان جرائم تقنية المعلومات، وقد اعتمد قانون براءات الاختراع بالتطبيق في بعض الدول العربية على الجانب المادي في نظام المعالجة الآلية للمعلومات، كما تم تصور نصوص قانون حماية الحياة الخاصة وقانون تحريم إفشاء الأسرار، بحيث يمكن تطبيقها على بعض جرائم تقنية المعلومات وأوكل الى القضاء الجزائي النظر في القضايا التي ترتكب بواسطة وسائل تقنية المعلومات.

- **المشرع الكويتي 2015م: -**

صدرت بعض القوانين بالمعاملات الإلكترونية ومنها:

1– القانون رقم(20) لسنة 2014م في شأن المعاملات الإلكترونية؛

2– القانون رقم(37) لسنة 2014م بأنشاء هيئة تنظيم الاتصالات وتقنية المعلومات؛

3– القانون رقم(63) لسنة 2015م بشأن مكافحة جرائم تقنية المعلومات، ويتكون من(**21 مادة**) شملت مصطلحات تعريفية بالبيانات الإلكترونية والنظام الإلكتروني، وعرف الجريمة الإلكترونية "بأنها كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة". (قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (63) ، لسنة 2015م)

وعدد جرائم تقنية المعلومات والعقوبات المقررة لها في حدها الأدنى والأعلى ومنها:

أ. الدخول غير المشروع الى جهاز آلي أو نظام معلوماتي أو موقع إلكتروني حيث شدد العقوبة في حال الحصول على معلومات حكومية سرية (المادة 2)؛

ب. التزوير والابتزاز الإلكتروني (المادة 3) ؛

ج. التشهير والمساس بالكرامة الشخصية (المادة 4)؛

د. الاحتيال الإلكتروني (المادة 3/5) ؛

هـ. الاعتراض غير القانوني (المادة 4) ؛

و. أعمال الدعارة والفجور (المادة 4/5) ؛

ز. السرقة الإلكترونية (المادة 5) ؛

ح. الاتجار بالبشر أو ترويج المخدرات والمؤثرات العقلية (المادة 8)؛

ط. غسل الأموال (المادة 9) ؛

ي. الإرهاب الإلكتروني (المادة 10) ؛

وفي المسؤولية الجنائية جاء في نص المادة (14) "مع عدم الإخلال بالمسؤولية الجزائية الشخصية لمرتكب الجريمة، يعاقب الممثل القانوني للشخص الاعتباري بذات العقوبات المالية المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا ثبت إن إخلاله بواجبات وضيفته أسهم في وقوع الجريمة مع علمة بذلك، ويكون الشخص الاعتباري مسؤولاً عما يحكم به من عقوبات مالية أو تعويضات إذا أُرتكبت الجريمة لحسابة أو باسمة أو لصالحة".

- **النظام السعودي2007م:-** (نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428هـ)

عرف النظام المعلوماتي بأنه (مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية). (المادة 2/1)

عرف الجريمة المعلوماتية بأنها(أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية المخالفة لأحكام هذا النظام). (المادة 8/1)

يهدف هذا النظام الى الحد من وقوع جرائم المعلوماتية وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها وبما يؤدي الى:-

أولاً المساعدة على تحقيق الأمن المعلوماتي:

حيث تنص المادة الثالثة "يعاقب بالسجن مدة لا تزيد عن سنتين وبغرامة لا تزيد عن خمسمائة ألف ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم المعلوماتية الأتية:

1- التنصت على ما هو مرسل عن طريق شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح أو التقاطه أو اعتراضه؛

2- الدخول غير المشروع لتهديد شخص أو ابتزازه لحملة على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا؛

3- الدخول غير المشروع الى موقع إلكتروني أو الدخول الى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه؛

4- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو مافي حكمها؛

5- التشهير بالأخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.

ثانيًا حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية:

نصت المادة الرابعة "يعاقب السجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًا من الجرائم المعلوماتية الاتية:

1- الاستيلاء لنفسة أو لغيرة على مال منقول أو على سند أو توقيع هذا السند وذلك عن طريق الاحتيال أو اتخاذ أسم كاذب أو انتحال صفة غير صحيحة؛

2– الوصول دون مسوغ نظامي صحيح الى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات.

وجاء في نص المادة الخامسة "يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًا من الجرائم المعلوماتية الاتية:

1– الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو اتلافها أو تغييرها أو إعادة نشرها؛

2– إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها أو حذفها أو تسريبها أو اتلافها أو تعديلها؛

3– إعاقة الوصول الى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت.

ثالثًا حماية المصلحة العامة والاخلاق والآداب العامة:

تنص المادة السادسة "يعاقب السجن مدة لا تزيد عن خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًا من الجرائم المعلوماتية الاتية:

1– إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي؛

2– إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشرة للاتجار في الجنس البشري أو تسهيل التعامل به؛

3– إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها؛

4– إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشرة للاتجار بالمخدرات أو المؤثرات العقلية أو ترويجها أو طرق تعاطيها أو تسهيل التعامل بها.

رابعًا حماية الاقتصاد الوطني:

نصت المادة السابعة "يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم المعلوماتية الاتية:

1- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشرة لتسهيل الاتصال بقيادات تلك المنظمات أو أي من أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أداة تستخدم في الاعمال الإرهابية؛

2- الدخول غير المشروع الى موقع إلكتروني أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو أحد اجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.

- **المشرع المصري 2018م:-** (قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018م)

صدر قانون مكافحة جرائم تقنية المعلومات في 14 أغسطس 2018م، ويتكون من(**45 مادة**)، عرف في الباب الأول تقنية المعلومات ووسائلها، والتزامات وواجبات مقدم الخدمة، وتطبيق القانون من حيث المكان (المادة 3)، والتعاون الدولي في مجال مكافحة جرائم تقنية المعلومات، وفي الباب الثاني بين الأحكام والقواعد الإجرائية لمأمور الضبط القضائي وتعيين الخبراء، وكذلك حجية الأدلة الرقمية في الإثبات الجنائي، وفي الباب الثالث أنزل العقوبات قرين كل جريمة معلوماتية على النحو التالي:-

1- جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها (المادة 13)؛

2- جريمة الدخول غير المشروع (المادة 14)؛

3- جريمة تجاوز حدود الحق في الدخول (المادة 15)؛

4- جريمة الاعتراض غير المشروع (المادة 16)؛

5- جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية (المادة 17)؛

6- جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة (المادة 18)؛

7- جريمة الاعتداء على تصميم موقع (المادة 19)؛

8- جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة (المادة 20)؛

9- جريمة الاعتداء على سلامة الشبكة المعلوماتية (المادة 21)؛

10- جرائم الاحتيال والاعتداء على بطاقات البنوك وأدوات الدفع الإلكتروني (المادة 23)؛

11- الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني (المادة 24)؛

12- الاعتداء على حرمة الحياة الخاصة. (المادة 25)

وفي تقرير المسؤولية الجنائية، فقد نصت المادة(36) على إنه "في الأحوال التي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون، باسم ولحساب الشخص الاعتباري، يعاقب المسؤول عن الإدارة الفعلية إذا ثبت علمة بالجريمة أو سهل ارتكابها تحقيقًا لمصلحة له أو لغيرة بذات عقوبة الفاعل الأصلي، وللمحكمة أن تقضي بإيقاف تراخيص مزاولة الشخص الاعتباري للنشاط مدة لاتزيد على سنة، ولها في حالة العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري".

- **القانون السوداني2007م:-** (قانون جرائم المعلوماتية لسنة 2007م)

فسر قانون جرائم المعلوماتية البيانات أو المعلومات بأنه (الأرقام والحروف والرموز وكل ما يمكن تخزينه ومعالجته وتوليده وإنتاجه ونقلة بالحاسوب أو أي وسائط إلكترونية أخرى). (المادة 3)

وقد نظم الجرائم المعلوماتية وحدد عقوبة السجن المناسبة وترك تحديد الغرامة لسلطة القاضي التقديرية على النحو التالي:-

أولاً جرائم نظم ووسائط وشبكات المعلومات

حدد الجرائم ووضع لها عقوبة السجن في حدها الأدنى سنتين والحد الأعلى عشر سنوات كالاتي:

1- دخول المواقع وأنظمة المعلومات المملوكة للغير (المادة 4)؛

2- دخول المواقع وأنظمة المعلومات من موظف عام (المادة 5)؛

3- التنصت أو التقاط أو اعتراض الرسائل (المادة 6)؛

4- دخول المواقع عمدًا بقصد الحصول على بيانات أو معلومات أمنية (المادة 7)؛

5- إيقاف أو تعطيل أو اتلاف البرامج أو البيانات أو المعلومات (المادة 8)؛

6- إعاقة أو تشويش أو تعطيل الوصول للخدمة. (المادة 9)

ثانيًا الجرائم الواقعة على الأموال والبيانات والاتصالات

وضح القانون السوداني هذه الجرائم وحدد لكل جريمة عقوبة أقلها سنتين وأعلاها خمس سنوات وهي:

1- التهديد أو الابتزاز (المادة 10) ؛

2- الاحتيال أو انتحال صفة غير صحيحة (المادة 11)؛

3- الحصول على ارقام أو بيانات بطاقات الائتمان (المادة 12)؛

4– الانتفاع دون وجه حق بخدمات الاتصال. (المادة 13)

ثالثًا جرائم النظام العام والآداب

1– الاخلال بالنظام العام والآداب (المادة 14/1)؛

2– إنشاء أو نشر المواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام والآداب (المادة 15)؛

3– انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة (المادة 16)؛

4– اشانه السمعة. (المادة 17)

رابعًا جرائم الإرهاب والملكية الفكرية

وهو كل من أنشاء أو نشر أو استخدم موقعًا على شبكة المعلومات أو أحد أجهزة الحاسب الآلي وما في حكمها لجماعة إرهابية لتسهيل الاتصال والترويج لأفكارها أو تمويلها، وكذلك نشر مصنفات فكرية دون وجه حق ومنها:–

1– إنشاء أو نشر المواقع للجماعات الإرهابية (المادة 18)؛

2– جريمة نشر المصنفات الفكرية. (المادة 19)

خامسًا جرائم الاتجار في الجنس البشري والمخدرات وغسل الأموال

شدد القانون السوداني العقوبة على هذه الجرائم، في ادناها عشر سنوات واعلاها عشرين سنة كالتالي:

1– الاتجار في الجنس البشري (المادة 20)؛

2– الاتجار أو الترويج للمخدرات (المادة 21)؛

3– غسل الأموال. (المادة 22)

الفرع الثاني دور التشريعات الغربية في مكافحة جرائم تقنية المعلومات:–

اتجهت الدول المتقدمة الى استخدام نصوص قانونية جديدة تحرم جرائم تقنية المعلومات باعتبارها جرائم جديدة على قوانينها التقليدية، وعليه فقد صاغت نصوص قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة والمتطورة.

- **دولة السويد: –**

تعتبر دولة السويد من أوائل الدول التي اتجهت الى سن تشريعات قانونية جديدة خاصة بجرائم الإنترنت والحاسب الآلي لتستطيع أن تعاقب المتهمين بارتكاب الجرائم الإلكترونية، إذ صدر أول قانون خاص باسم

"قانون البيانات" في عام 1973م، وقد عالج هذا القانون قضايا الاحتيال عن طريق الإنترنت، بالإضافة الى كونه يشتمل على فقرات عامة من نصوصه لتشمل جرائم الدخول غير المشروع على البيانات الإلكترونية أو تزوير المعلومات الإلكترونية أو تحويلها أو الحصول غير المشروع عليها. (الجنبيهي، 2006م، ص79)

- **الولايات المتحدة الأمريكية: –**

هي الدولة الثانية التي تبعت السويد في إصدار قوانين خاصة بها تجرم الجرائم الإلكترونية اذ شرعت قانونًا خاصًا بحماية أنظمة الحاسب الآلي عام 1976م وفي عام 1985م حدد معهد العدالة القومي الأمريكي خمسة أنواع رئيسية للجرائم وهي:

1. جرائم الحاسب الآلي الداخلي؛
2. جرائم الاستخدام غير المشروع عن بعد؛
3. جرائم التلاعب بالحاسب الآلي؛
4. جرائم التعاملات الإجرامية؛
5. سرقة البرامج الجاهزة والمكونات المادية للحاسب الآلي. (عوض ، 1990م، ص35)

وفي عام 1986م صدر قانون رقم(1213) عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية، كما وضعت المتطلبات الضرورية اللازمة لتطبيقها، وعلى آثر ذلك قامت الولايات الداخلية بإصدار التشريعات الخاصة بكل منها على حده للتعامل مع تلك الجرائم الإلكترونية ومن تلك القوانين، القانون الخاص بولاية تكساس لجرائم الحاسب الآلي، فقد خولت وزارة العدل الأمريكية عام 2000م خمس جهات حكومية للتعامل مع جرائم الإنترنت والحاسب الآلي، منها مكتب التحقيقات الفدرالي"**FBI**". (عوض، 1990م، ص37)

- **بريطانيا: –**

فهي ثالث دولة تسن قانون خاص بجرائم الإنترنت والحاسب الآلي، إذ أقرت قانون لمكافحة التزوير والتزييف عام 1981م والذي شمل تعريف أداة التزوير، وسائط التخزين المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواًء بالطرق الإلكترونية أو التقليدية أو أي طرف أخر. (عوض، 1990م، ص39)

- **كندا: –**

فهي تطبق قوانين متخصصة ومنفصلة للتعامل مع جرائم الإنترنت، اذ عدلت في عام 1985م قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسوب والإنترنت، كما شمل القانون الجديد تحديد العقوبات المطبقة على المخالفات الحاسوبية وجرائم التدمير وجرائم الدخول غير المشروع على المعلومات الإلكترونية، كما وضع القانون صلاحيات جهات التحقيق، كما جاء في "قانون المنافسة" الذي يخول لمأمور القبض القضائي متى حصل على أمر قضائي حق التفتيش على أنظمة الحاسب الآلي والعامل معها وضبطها. (الجنبيهي، 2006م، ص20)

- **اليابان: –**

فقد قامت بتعديل قوانينها الجنائية لتستوعب المستجدات الإجرامية المتمثلة في جرائم الإنترنت والحاسب الآلي، وقد نصت على أنه لا يلزم مالك الحاسب المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمة السر التي يستخدمها إذا ما كان ذلك سيؤدي الى إدانته، كما أقرت قانون خاص في عام 1991م أجازت التنصت على شبكات الحاسب الآلي فقط إذا ما كان ذلك في مجال البحث عن الأدلة الخاصة بإحدى الجرائم الإلكترونية. (الجنبيهي، 2006م، ص22)

الخاتمة:–

في ختام هذه الدراسة توصلنا الى بعض النتائج والتوصيات على النحو الاتي:–

أولاً النتائج:

1. **–** المعلومات هي كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو نقلة أو مشاركته أو نسخة، كالشفرات والاكواد والحروف والرموز والاشارات والصور والاصوات وما في حكمها؛
2. **–** تقنية المعلومات تتم كليًا أو جزئيًا بكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو تركيب، باستخدام أي وسيط من الوسائط أو الحاسبات الإلكترونية؛
3. **–** تستخدم المعلومات في جميع مجالات الحياة؛
4. **–** تتعدد وتتطور جرائم تقنية المعلومات؛

5– للحفاظ على الأمن المعلوماتي تم إبرام بعض الاتفاقيات الدولية التي تشكل نوعًا من الاطار القانوني لاستخدام تقنية المعلومات؛

6– تعمل الأمم المتحدة والمنظمات والوكالات الدولية على تأمين سلامة استخدام التكنولوجيا وشبكات المعلومات بإصدار قرارات دولية تجرم التعدي عليها وتحمي مستخدميها من الأشخاص الطبيعيين والأشخاص الاعتبارية؛

7– للحد من انتشار جرائم تقنية المعلومات تسعى العديد من الدول في التعاون وعقد اتفاقيات جماعية في إطار جغرافي محدد؛

8– الجمهورية اليمنية وبعض الدول لا يوجد لديها قانون خاص بمكافحة جرائم تقنية المعلومات وإنما تطبق النصوص العقابية القائمة على مثل هذه الجرائم؛

9– دول لديها قانون مكافحة جرائم تقنية المعلومات ولكنها جامدة؛

10– العديد من تشريعات الدول تواكب تطور جرائم تقنية المعلومات وتحدث تشريعاتها الخاصة.

ثانيًا التوصيات:

1– نوصي المشرع اليمني بأصدر قانون خاص بمكافحة جرائم تقنية المعلومات وأن يواكب تطورات هذه الجرائم؛

2– إقامة المؤتمرات والندوات الخاصة بتقنية المعلومات وتطورها ودراسة الثغرات والاعداد الأمني والقانوني لها؛

3– نوصي بالتعاون الدولي المعلوماتي والرد السريع بين دول العالم؛

4– تبني سياسة جنائية مشتركة تهدف الى حماية المجتمع العالمي ضد جرائم تقنية المعلومات؛

5– تنفيذ استراتيجيات الاتحاد الدولي للاتصالات لتعزيز أمن المعلومات العالمي؛

6– الاسترشاد بقرارات منظمة الأمم المتحدة في وضع القوانين الخاصة بمكافحة جرائم تقنية المعلومات.

ISSN print/ 2769-1926 ISSN online/ 2769-1934

CONCLUSION

At the end of this study we have mentioned some results and recommendations as following*;*

First results :

1) Information is what can be created, stored, processed, transferred, shared or copied as codes, letters, symbols, signals, sounds or images.
2) Information technology is partly or totally by writing, collecting, recording, saving, merging, showing, sending, receiving, or editing or deleting by using any tools or meditation of electronic devices.
3) Information can be used in all of life's aspects.
4) technology crimes varied and developed.
5) To protect information many of related conversations has been made.
6) United nation and international agencies are endeavoring to secure using of information and information networks by making international decisions protect information and criminalizing any act may cause injury for information either by natural or jurisdiction person.
7) To reduce speeding of information technology crimes nations, endeavor to cooperate by held conventions with certain geographical scope.
8) Yemen as many other countries hasn't any code to cope information technology crimes and the only applied are general provisions in other laws.
9) Many states have cybercrime laws but they haven't be updated.
10) Many states have updated cybercrime laws.

Recommendations

We recommend;

1) Yemeni legislature to promulgate cybercrime law and be in updating.
2) Holding conferences and seminars on information technology and its development, focusing on all details of its aspects.
3) International cooperation on information technology field.
4) Adopt a common criminal policy aimed at protecting international community against cybercrimes.
5) Implementation of International Telecommunication Union strategies to enhance international information security.

6) Consideration of United nation guidelines on cybercrime laws.

قائمة المراجع:-

الكتب والمراجع القانونية:-

1. الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانيه في المنطقة العربية، اللجنة الاقتصادية والاجتماعية لغربي آسيا(الإسكوا)، (2015م)، الأمم المتحدة، نيويورك.
2. إسماعيل حسن عبدالله حميد، (2021)، الأمن السيبراني، الجيل الجديد ناشرون، صنعاء.
3. السيد عاشور، (2000م)، ثورة الإدارة العلمية والمعلوماتية، القاهرة.
4. حسني عبد السميع إبراهيم، (2011م)، الجرائم المستحدثة عن طريق الإنترنت، دار النهضة العربية.
5. عبدالحميد بسيوني، (2004م)، طرق وبرامج الهاكرز وقرصنة المعلومات، دار الكتب العلمية للنشر والتوزيع.
6. عوض محمد عوض، (1990م)، قانون الإجراءات الجنائية، دار المطبوعات الجامعية.
7. محمد أمين الرومي، (2004م)، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية.
8. محمد علي سكيكر، (2010م)، الجريمة المعلوماتية وكيفية التصدي لها، القاهرة.
9. منير، ممدوح الجنبيهي، (2006م)، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية.
10. نائلة عادل محمد فريد قورة، (2005م)، جرائم الحاسب الاقتصادية، منشورات الحلبي القانونية
11. هشام محمد فريد رستم، (1994م)، قانون العقوبات ومخاطر تقنية المعلومات.

الرسائل العلمية:-

12. سالم سليمان عبدالجبوري، (2014م)، جريمة الاحتيال الإلكتروني، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة النهرين، العراق.
13. سمير إبراهيم جميل الغزاوي، (2005م)، المسؤولية الجنائية الناشئة عن استخدام الإنترنت، رسالة ماجستير، كلية القانون، جامعة بغداد.

القوانين والتشريعات:-

14. قانون الجرائم والعقوبات اليمني، رقم (12) لسنة1994م.
15. قانون الإجراءات الجزائية اليمني، رقم (13) لسنة 1994م.
16. قانون رقم (1) لسنة2010م، بشأن مكافحة جرائم غسل الأموال وتمويل الإرهاب اليمني.
17. قانون رقم (40) لسنة2006م، أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية اليمني.
18. قانون رقم (13) لسنة2012م، بشأن حق الحصول على المعلومات اليمني.
19. قانون رقم (15) لسنة2012م، بشأن حماية حق المؤلف والحقوق المجاورة.

20. قانون رقم (46) لسنة2008م، بشأن حماية المستهلك اليمني.
21. قانون رقم (8) لسنة1997م، بشأن الآثار اليمني.
22. قانون مكافحة جرائم تقنية المعلومات الكويتي، رقم 63 لسنة 2015م.
23. قانون مكافحة جرائم تقنية المعلومات المصري، رقم 175 لسنة 2018م.
24. نظام مكافحة جرائم تقنية المعلومات السعودي، مرسوم ملكي رقم(17) لسنة 1428هـ/2007م.
25. قانون جرائم المعلوماتية السوداني، لسنة 2007م.
26. مشروع قانون مكافحة جرائم تقنية المعلومات اليمني لعام 2020م.

الاتفاقيات والتقارير الدولية:-

27. الاتفاقية المتعلقة بالجريمة الإلكترونية "بودابست"، 2001م.
28. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لسنة 2010م.
29. النظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون، لدول الخليج العربي، 2012م.
30. اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، 2014م.
31. الموسوعة العربية العالمية، الرياض، 1425هـ/ 2004م.
32. تقرير الاتحاد الدولي للاتصالات بشأن الإطار القانوني لحماية الأطفال من مخاطر الشبكة المعلوماتية ووسائل تقنية المعلومات وبخاصة الجرائم الإلكترونية، (2015م).

المواقع الإلكترونية:-

33. www.un.orq
34. www.mawdoo3.com

References

Law references ;

1. Abdulhameed Basyoni (2004) Methods and programs of hackers, Dar Alkootob Al-elmia for publishing.
2. Awadh Muhammad Awadh, (1990), Criminal Procedure law, University Press
3. Hisham Mohamed Farid Rostom, (1994), Penal Code and Information Technology Risks.
4. Housni Abdulsamee Ibrahim (2011), recent crimes by internet, Dar Al-nahdha'a Al-Arabia.
5. Ismail Abdullah Humaid. (2021), Cybersecurity, Al-Geel Al-Gadeed, Publisher, Sana'a.

ISSN print/ 2769-1926 ISSN online/ 2769-1934

6. Mohamed Ali Skiker, (2010), Cybercrime and how to cope it, Cairo.
7. Mohammed Amin Al-Roumi, (2004), Computer and Internet Crimes, University Press.
8. Mounir, Mamdouh Al-Janbihi, (2006), Internet and Computer Crimes and Means of Combatting Them, Dar Al-Fikr Al-Jamia, Alexandria.
9. Naila Adel Mohammed Farid Qurah, (2005), Economic Computer Crimes, Al-Halabi Legal Publications
10. Said Ashoor, (2000), Scientific management& information revolution, Cairo.
11. Security in Cyberspace and Combatting Cybercrime in Arab Region, Economic and Social Commission for Western Asia (ESCWA), (2015), United Nations, New York.

Theses : -

12. Samir Ibrahim Jamil Al-Ghazzawi, (2005), Criminal Responsibility Arising from the Use of the Internet, Master's Thesis, College of Law, University of Baghdad.
13. Salem Suleiman Abdul Jubouri, (2014), The Crime of Electronic Fraud, Master's Thesis in Public Law, College of Law, Al-Nahrain University, Iraq.

Laws and Legislations :

14. Egyptian Law, No. 175 of 2018 on combatting Cybercrime.
15. Kuwait's Law, No. 63 of 2015 on combatting Cybercrime.
16. Saudi, Royal Decree No. (17) of 1428 AH / 2007 AD on combatting Cybercrime.
17. Sudanese Law of 2007 on Information Crimes.
18. Yemeni Code of Criminal Procedure, No. 13 of 1994.
19. Yemeni Law No. (1) of 2010 on combating money laundering and financing crimes of terrorism.
20. Yemeni Law No. (40) of 2006, on Payment Systems and Electronic Financial and Banking Operations.
21. Yemeni Law No. (13) of 2012 on the right of access to information.
22. Yemeni Law No. (15) of 2012 on the protection of copyright and related rights.

ISSN print/ 2769-1926 ISSN online/ 2769-1934

23. Yemeni Law No. (46) of 2008 on protection of Yemeni consumers.
24. Yemeni Law No. (8) of 1997 on Antiquities.
25. Yemen's draft law on combatting information technology crimes of 2020.
26. Yemeni Penal Code, No. 12 of 1994

International Conventions and Reports :

27. African Union Convention on Cybersecurity and Protection of Personal Data, 2014.
28. Arab Convention on Combatting Information Technology Crimes, 2010.
29. Budapest Convention on Cybercrime, 2001.
30. The Unified regulation for Combatting Information Technology Crimes for the GCC States, 2012.
31. International Arabic Encyclopedia, Riyadh, 1425 AH / 2004 AD.
32. ITU Report on the Legal Framework for the Protection of Children from the Dangers related with Information Network and Information Technology Means, Especially Cybercrime, A Model Regional Legal Framework on Child Online Protection, (2015), A Guide for Arab Region.

Websites : -

33. www.un.orq
34. www.mawdoo3.com

مجلة الحكمة للدراسات والأبحاث المجلد 03 العدد 01 (11) 2023/03/30
ISSN print/ 2769-1926 ISSN online/ 2769-1934

Role of international agreements and municipal legislations in combatting information technology crimes,

Alawi Ali Ahmed Al_sharefi
Associated criminal law professor
Police Academy, Yemen
alawiali013@gmail.com

Abstract:

Cybercrimes can consider as recent crimes that attack technology development and lead to speeding of terrorist networks over many countries exploiting all of electronic tools, they constitute dangerous upon national stability and threat international peace and security.

Cybercrimes raised a legal problem related with applying of classic act's provisions over this kind of crimes which require special domestic and international laws to reduce speeding of these crimes.

This study aims at discussing information technology and its characteristics and tools, and also to explain the role of international treaties & Arab and western countries in combatting these crimes.

Study ended to some of results and recommendations that conductive combatting cybercrimes.

Keywords: information technology crimes - international agreements - national legislation - international organizations - the Internet.