مجلة كلية القانون والعلوم السياسية العدد (٢)

الجرائم الألكترونية
واقع وتحدي

أ.د . واثبة داود السعدي
أستاذة مادة العقوبات في جامعة بغداد، درست أيضاً في المعهد القضائي
عضوة في ديوان التدوين القانوني، والجامعة الأردنية، وجامعة اليرموك
مستشارة مؤتمر جنيف لحقوق الإنسان
مستشارة المؤسسة القطرية لحماية الطفولة والأمومة

المقدمة

مثلما قدم تسارع التقدم التكنولوجي خدمات جليلة للمجتمعات الانسانية عن طريق الفضاء الألكتروني ووسائل الاتصال الحديثة كالانترنيت وسائر صور الاتصال الالكتروني عبر الأقمار الصناعية ، أدى في الوقت ذاته الى ظهور أنماط اجرامية جديدة لم تكن معروفة سابقا ولم تعد مقتصرة على دولة معينة في مداها بل تجاوزت الحدود الدولية، فالجريمة الألكترونية جريمة مبتكرة تمثل ضربا من ضروب الذكاء والدهاء الاجرامي من الصعب ادراجها ضمن الأوصاف التقليدية للجرائم المعالجة في القوانين الداخلية والدولية ،كما لا يمكن لأنظمة الملاحقة التقليدية أن تؤدي الى تتبعها وكشف فاعلها ومحاسبته بنجاح ، لذا لابد من تشريع جديد يتمتع واضعيه ببنية تشريعية جنائية وتقنية تفوق دهاء وذكاء الفاعلين الجناة يعكس الدقة اللازمة على المستوى القانوني والتقني بما يضمن تكامل مبدأ الشرعية الموضوعية في التجريم والعقاب ومبدأ الشرعية الاجرائية في آن واحد ويأخذ دوره الفعلي في الاتفاقيات والمعاهدات الدولية .

أهمية الموضوع

تتمثل أهمية الموضوع في كون الجرائم الألكترونية تمس مصالح المجتمع مساسا مباشرا في كل صورها كالقرصنة والاختراق غير المشروع لأنظمة الحاسوب وبرامجه وتدميرها بواسطة الفيروسات وتقليد ونسخ برامج الغير بدون علمهم أو موافقتهم ، والسرقة والنصب والاحتيال ، وتسهيل الدعارة وعرض المواد الاباحية ،ونشر المعلومات المظللة والاعلانات الكاذبة ، وانتهاك حرمة الحياة الخاصة ، والاتجار بالبشر والاتجار بالأعضاء البشرية ، وعمليات الابتزاز التي تمارس ضد الأشخاص وضد الشركات والتهديدبافشاء الأسرار والخصوصيات ، وعمليات التجسس وعمليات الارهاب ، والسطو على البنوك والمؤسسات المالية من خلال التعامل الألكتروني والسحب من الأرصدة بواسطة البطاقة الممغنطة أو الدفع الألكتروني .

اشكالية البحث في الموضوع

ترجع اشكالية البحث في هذا الموضوع الى أن الجريمة الألكترونية جريمة ديناميكية متطورة تتميز بصفات فنية ومفردات ومصطلحات متجددة اضافة الى أن أغلب مستنداتها عبارة عن تسجيلات تتم وتنتشر بسرعة البرق عبر شبكات الاتصال المعلوماتي ، كما أن أغلب صورها عابرة للحدود وبذلك فهي تثير اشكالية في تحديد الاختصاص القانوني والاختصاص القضائي ، كما تثير اشكالية التكييف القانوني للفعل في مدار التمييز بين العمل التحضيري والشروع والجريمة التامة ،اضافة الى ان هذا النمط من الجرائم أضاف في مجال الاثبات الدليل الرقمي الى الدليل المستندي الورقي المعروف .

تمهيد

قبل الدخول في الموضوع لابد من الاشارة الى أهم الوسائل الألكترونية :-

الحاسوب (الكومبيوتر) :- وهو مجموعة من الأجهزة المترابطة والتي تعمل متكاملة مع بعضها بهدف تشغيل مجموعة البيانات الداخلة طبقا لبرنامج تم وضعه للحصول على نتائج معينة .

شبكة المعلومات (الأنترنيت) عبارة عن شبكة يمكن من خلالها تصفح صفحات متنوعة عن طريق وسائل متعددة مكتوبة أو مرسومة بالصوت والصورة من خلالها يمكن التواصل مع الآخرين عن طريق غرف المحادثة ،والوصول الى معلومات معينة أو التسوق أو المتاجرة والتعاقد والاعلان عن السلعة والترويج لها في كافة أنحاء العالم .

البريد الألكتروني (الايميل) وهو خط يمكن للمستخدم ارسال واستقبال الرسائل من خلاله في كافة انحاء العالم .

المجاميع الاخبارية ومواقع نقل الملفات وهي عبارة عن مساحات تغطي مواضيع علمية وثقافية وفنية وتاريخية واخبارية متنوعة أو بالأحرى كل ما يتعلق بالاهتمامات الانسانية .

ايجابيات استخدام الوسائل الألكترونية :-

استخدام الوسائل الألكترونية يساعد في تطوير ذهنية الأطفال والشباب وتوسيع مداركهم وتنمية روح الابداع والابتكار لديهم .

تساعد في تطوير العلاقات الانسانية وتسهل الاتصالات الهاتفية والاتصالات البريدية بازهد الاسعار .

تساعد في سرعة انتشار البحوث العلمية والبحوث الانسانية وسرعة تناقل الاخبار العالمية .

تساعد في سرعة انتشار اخبار البورصة وكافة التعاملات المالية والتجارية .

تسهل احيانا في القبض على المجرمين حيث يستخدم الحاسب الآلي في الكشف عن الجرائم والتعرف على مرتكبيها عن طريق بصمة الصوت أوبصمة العين كما يساعد في رصد سوابق الجناة وفي استقبال البلاغات وفي التواصل مع البوليس الدولي (الانتريول).

يمكن استخدامها في تنفيذ برنامج مراقبة المحكوم عليهم المفرج عنهم شرطيا حيث يوضع جهاز صغير في معصم المفرج عنه شخصيا يشير الى مكان تواجده .

بعد الاطلاع على ايجابيات استخدام الوسائل الألكترونية استخداما مشروعا نستعرض الاستخدام غير المشروع للوسائل الالكترونية (الجرائم الألكترونية)

الفصل الأول ـ ماهية الجريمة الألكترونية

المطلب الأول – التعريف بالجريمة الألكترونية

وردت عدة تعاريف للجريمة الألكترونية منها التعاريف التالية :

عرف مكتب تقييم التقنية في الولايات المتحدة الجريمة الألكترونية بانها "الجرائم الي تقوم بها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي."(١)

وتعرف بانها "نشاط جنائي يمثل اعتداء على برامج وبيانات الحاسب الآلي ." (٢)

كما تعرف بانها "كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية ويهدف الى الاعتداء على أي مصلحة مشروعة سواء كانت مادية أو معنوية."(٣)

وتعرف ايضا بانها "عبارة عن افعال غبر مشروعة يكون الحاسب الآلي محلا لها أو وسيلة لارتكابها ."(٤)

ومنهم من عرفها بانها الجريمة ذات الطابع المادي، تتمثل في كل فعل أو سلوك غير مشروع مرتبط بأية وجهة أو بأي شكل بالحواسيب والشبكات الحاسوبية، يتسبب في تحميل أو إمكان تحميل المجني عليه خسارة، وحصول أو إمكان حصول مرتكبه على أي مكسب.. وغالبا ما تهدف هذه الجرائم إلى سرقة المعلومات الموجودة في الأجهزة الحاسوبية، أو تهدف على نحوٍ غير مباشر إلى الاساءة الى الأشخاص والجهات المعنية بتلك المعلومات. والجريمة من هذا النوع لها مسميات عدة، منها جرائم الحاسوب والإنترنت – جرائم التقنية العالية – الجريمة الإلكترونية– الجريمة السايْبِريّة – جرائم أصحاب الياقات البيضاء(٥)

كما تعرف بانها جريمة ذات طابع مادي تتمثل في كل فعل او سلوك غير مشروع ،من خلال استعمال الوسائط الألكترونية مثل الحواسيب ،اجهزة النقال ، شبكات الاتصال الهاتفية ، شبكات نقل المعلومات ، شبكة الانترنيت ، حيث تتسبب في تحميل او امكانية تحميل المجنى عليه خسارة وحصول او امكانية حصول مرتكبه على أي مكسب ، تهدف هذه الجرائم الى الوصول غير الشروع لبيانات سرية غير مسموح الاطلاع عليها ونقلها ونسخها او حذفها أو تهديد وابتزاز الأشخاص والجهات المعنية بتلك المعلومات أو تدمير بيانات وحواسيب الغير بواسطة فيروسات .(٦)

(١) د.مفتاح بو بكر الطردي المستشار بالمحكمة العليا الليبية/ الجريمة الألكترونية والتغلب على تحدياتها / ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية /جمهورية السودان في ٢٣ ---٢٥ /٩ /٢٠١٢

(٢) د.مفتاح بو بكر الطردي المستشار بالمحكمة العليا الليبية/ الجريمة الألكترونية والتغلب على تحدياتها / ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية /جمهورية السودان في ٢٣ ---٢٥ /٩ /٢٠١٢

(٣) د.مفتاح بو بكر الطردي المستشار بالمحكمة العليا الليبية/ الجريمة الألكترونية والتغلب على تحدياتها / ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية /جمهورية السودان في ٢٣ ---٢٥ /٩ /٢٠١٢

(٤) د.مفتاح بو بكر الطردي المستشار بالمحكمة العليا الليبية/ الجريمة الألكترونية والتغلب على تحدياتها / ورقة مقدمة الى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية /جمهورية السودان في ٢٣ ---٢٥ /٩ /٢٠١٢

(٥) مصطفى سمارة /مركز التميز لأمن المعلومات

(٦) منى شاكر فرج Assurance Center of Excellence in Information

اما المشرع القطري فقد عرفها في المادة الخامسة من قانون مكافحة الجريمة الالكتونية رقم ١٤ لسنة ٢٠١٤ بانها " أي فعل ينطوي على استخدام وسيلة تقنية المعلومات او نظام معلوماتي او الشبكة المعلوماتية بطريقة غير مشروعة بما يخالف القانون ."

ونرى بانها "كل فعل غير مشروع يوقع ضررا أو يمثل خطرا بشخص من الأشخاص الطبيعية أو المعنوية أو بأي كيان محلي أو دولي اداة ارتكابه الحاسوب أو أية وسيلة من الوسائل الألكترونية" .

المطلب الثاني – سمات الجرائم الألكترونية

تختلف الجرائم الألكترونية عن الجرائم العادية اختلافا كبيرا وأهم سماتها هي :--

١- انها جريمة تعتمد الذكاء والدهاء في ارتكابها وترتكز على التفكير العلمي المدروس حيث انها تتناسب في وجودها طرديا مع ذكاء ودهاء الفاعل وبذلك فهي لا تحتاج الى مجهود عضلي أو قوة بدنية لارتكابها كباقي أغلب الجرائم التقليدية .

٢- انها من الجرائم التي يصعب اكتشافها ومتابعتها واثباتها فهي تتناسب عكسيا في كشفها ومتابعتها واثباتها مع ذكاء ودهاء الفاعل حيث انها تمتاز بما يلي :

أ- انها جريمة لا تترك في الغالب أثرا بعد ارتكابها .

ب – صعوبة الاحتفاظ الفني باثارها ان وجدت .

ج – انها تحتاج الى خبرة فنية يصعب على أغلب المحققين التعامل معها .

٣ – انها في أغلب صورها جريمة عالمية عابرة للحدود ، حيث يمكن أن يكون احد اطرافها في بلد معين او قارة معينة والطرف الآخر في بلد آخر أوقارة أخرى .

المطلب الثالث – انواع الجرائم الألكترونية :

استأنسنا بتقسيم الجرائم الألكترونية بالتقسيم الوارد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٢ .

اولا – جريمة الدخول غير المشروع وتتحقق بـ:

الدخول أو البقاء او الاتصال غير المشروع مع كل اوجزء من تقنية المعلومات

محو او تعديل او تشويه او نسخ او نقل او تدمير للبيانات المحفوظة او للاجهزة والانظمة الالكترونية وشبكات الاتصال والحاق الضرر بالمستخدمين والمستفيدين .

الحصول على معلومات حكومية سرية .

ثانيا – جريمة الاعتراض غير المشروع وتتحقق بالاعتراض الغير مشروع والمتعمد لخط سير البيانات باي من الوسائل الفنية او بقطع بث او استقبال البيانات .

ثالثا – جريمة اساءة استخدام وسائل تقنية المعلومات وذلك بانتاج او بيع او شراء او استيراد او توزيع او توفير او حيازة اوراق او برامج مصممة لغاية ارتكاب جرائم الكترونية.

رابعا – جريمة الاعتداء على سلامة البيانات بتدمير او محو او اعاقة او تعديل

او حجب تقنية المعلومات قصدا وبدون وجه حق .

خامسا – جريمة التزوير باستخدام وسائل تقنية المعلومات من اجل تغيير الحقيقة في البيانات تغييرا من شأنه احداث ضرر وبنية استعمالها كبيانات صحيحة .

سادسا – جريمة الاحتيال بادخال او تعديل او محو او حجب للمعلومات او البيانات او بالتدخل في وظيفة انظمة التشغيل وانظمة الاتصالات او بمحاولة تعطيلها او تغييرهااو تعطيل الاجهزة والبرامج والمواقع الألكترونية .

سابعا – الجرائم الجنسية – وتتمثل بـ :

١– انتاج او عرض او توزيع او توفير او نشر او شراء او بيع او استيراد مواد اباحية او مخلة بالحياء بواسطة التقنية الألكترونية.

٢– التعري والممارسات اللاأخلاقية عبر الانترنيت .

٣– الاستغلال الجنسي بواسطة طرق الكترونية.

٤– تغير وتبديل في الصور والمعالم الشخصية بغية نشرهاباستخدام الوسائل الألكترونية والاساءة لاصحابها .

ثامنا – الجرائم المتعلقة بالتعدي على الملكية الفكرية وذلك بانتهاك حقوق المؤلف والحقوق المجاورة لحق المؤلف .

تاسعا – الاستخدام غير المشروع لادوات الدفع الالكتروني وذلك بـ:

١– تزوير او اصطناع او وضع اي اجهزة او مواد تساعد على تزوير او تقليداي اداة من ادوات الدفع الالكتروني باي وسيلة كانت .

٢ – الاستيلاء على بيانات اداة من ادوات الدفع الالكتروني او استعمالها او تقديمها للغير او تسهيل امر الاستيلاء عليها من قبل الغير .

٣ – استخدام الشبكة المعلوماتية او احدى وسائل تقنية المعلومات في الوصول بدون وجه حق الى ارقام او بيانات اي اداة من ادوات الدفع .

عاشرا – الجرائم المنظمة المرتكبة باستخدام طرق الكترونية ومنها :

١ – القيام بعمليات غسيل اموال او نشر طرق القيام بها باستخدام الطرق الألكترونية .

٢ – الترويج للمخدرات والمؤثرات العقلية او الاتجار بها باستخدام الطرق الألكترونية

٣ – الاتجار بالاشخاص باستخدام الطرق الألكترونية .

٤ – الاتجار بالاعضاء البشرية باستخدام الطرق الألكترونية .

٥ – الاتجار غير المشروع بالاسلحة باستخدام الطرق الألكترونية .

حادي عشر— الجرائم المتعلقة بالارهاب

١— نشر افكار ومبادئ جماعات ارهابية والدعوة لها باستخدام طرق الكترونية.

٢ – تمويل العمليات الارهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الارهابية باستخدام طرق الكترونية .

٣ – نشر طرق صناعة المتفجرات التي تستخدم في عمليات ارهابية بواسطة وسائل الكترونية .

٤ – نشر النعرات والفتن والاعتداء على الأديان والمعتقدات بواسطة وسائل الكترونية .

الفصل الثاني ـ الطبيعة القانونية للجريمة الألكترونية

المطلب الأول – الطبيعة القانونية لمحل الجريمة الألكترونية

لا تثور اية صعوبة أو جدل عندما يكون محل الجريمة مالا ماديا كأن يكون جهاز الحاسب الآلي بكامله أو مكوناته المادية كوحدات الادخال او الاخراج او وسائل التخزين المرنة اوالصلبة او الشاشة او الطابعة كونها مالا ماديا قابلا لأن يكون محلا لجرائم الأموال كالسرقة والاتلاف والتعطيل ولكن الصعوبة تثور عندما يكون المال المعلوماتي المعتدى عليه معنويا كالبيانات والمعلومات المخزنة داخل الحاسب فهناك من يرى بان الاشياء المادية وحدها هي التي تقبل الحيازة والاستحواذ وان الشئ موضوع السرقة او الاتلاف او التعطيل يجب ان يكون ماديا اي له كيان مادي ملموس كان تكون مسجلة على شريط او اسطوانة فاذا تمت سرقة او اتلاف احدى هاتين الدعامتين لا يثور اي اشكال في اعتبارها جريمة او اتلاف مال معلوماتي ، أما اذا كانت المعلومة لها طبيعة معنوية لا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ الاً في ضوء حقوق الملكية الفكرية . أما الاتجاه الثاني فيرى بان المعلومات ما هي الاً مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعاماتها المادية على اعتبار ان المعلومات لها قيمة اقتصادية قابلة لن تحاز حيازة مشروعة اوغير مشروعة كما هو الحال في الطاقة الكهربائية وباقي الطاقات التي يمكن ان تكون محلا للسرقة .حيث ان القول عكس ذلك يعني تجريد المال المعلوماتي من الحماية القانونية الجنائية ويفسح المجال واسعا امام قرصنة البرامج والمعلومات .

المطلب الثاني – التحديات والمواجهة

تتخذ الجرائم الألكترونية انماطا جديدة تمثل تحديا جديا في الوقت الحاضر، يتطلب تجاوزه التعرف على هذه التحديات وابراز جوانبها انطلاقا من خطورة هذه الجرائم وضرورة مكافحتها على صعيد التجريم والعقاب من ناحية ومن ناحية اخرى عن طريق الملاحقة القانونية وهذا يتطلب محاولة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة والنزول بقدر معين امام ضرورة التعاون القضائي الدولي الذي يتطلب تطوير البنية التشريعية الجنائية بذكاء تشريعي متواصل لسد الثغرات التي يمكن ان تمس الشرعية من جانب ومن جانب آخرى يمكن أن يفلت منها الجناة ، على أن يتكامل هذا التطور في الدور والهدف مع المعاهدات الدولية والعربية .

بما أن الجرائم الألكترونية في اغلب صورها جرائم عابرة للحدود فالتساؤل يثور حول كيفية اعمال مبدأ الأقليمية على الجرائم التي ترتكب بواسطة شبكة المعلومات الدولية (الأنترنيت) وكيف يمكن تحديد اقليم الدولة الذي وقعت عليه مثل هذه الجرائم بتعددها وتنوعها وتعقيدها ، والجواب على هذا التساؤل ان التقدم العلمي الراهن وتطور وسائل الاتصال الحديثة كالأنترنيت وسائر صور الاتصال الألكتروني عبر الأقمار الصناعية، اتاح فرصا كبيرة للخروج على مبدأ الاقليمية وتبني مدونة جديدة لفض مثل هذا التنازع أو على الأقل ترتيب معايير اخرى لأن معيار اقليمية القانون لم يعد هو المعيار الوحيد

ولا حتى المعيار الأكثر قبولا في بعض الجرائم بل زادت اهمية معايير اخرى كانت فيما مضى تعد احتياطية كمعيار العينية ومعيارالعالمية كما شهد مبدأ الاقليمية تطورا في مفهومه فلم يعد ملازما لوقوع فعل مادي أو حتى احد العناصر المكونه له بل بلغ الامر حد نزع الصفة المادية كليا عن هذا الفعل حيث اعتبر مجرد مكالمة هاتفية مع شخص في دولة اخرى مبررا لاعتبار الجريمة قد وقعت فوق اقليمها. فاعتبار الجريمة الألكترونية من الجرائم العالمية العابرة للحدود يفوت الفرصة على الجاني في التهرب من المسؤولية ومن العقاب ، وفي حالة تنازع القوانين فيتقدم مبدأ الاقليمية باعتبار في الغالب فيه متحصلات الجريمة ومن ثم مبدأ الشصية على ان يشمل كل الجنسيات التي يتمتع فيها الفاعل فالدولة التي يتمتع بجنسيتها وتواجد على اقليمها تكون صاحبة الاختصاص سواء كانت الدولة الأم أم لا وفي هذه الحالة لا يمكنه الافلات من المسؤولية ولا من تنفيذ العقاب . وفي كل الأحوال اعتماد قواعد تسليم المجرمين سواء بالنص عليها في القوانين الداخلية أم في المعاهدت الدولية او العربية او الثنائية هو الطريق الامثل لملاحقة الجناة مرتكبي الجرائم الألكترونية .

هذا وقد يؤدي تطبيق القواعد التقليدية في المساهمة الجنائية وما يتبعها من قواعد تحدد مدد التقادم في الدول التي تعتمد تشريعاتها قواعد تقادم الجرائم وتقادم الأحكام الى افلات الفاعل من المثول امام القضاء أو من تنفيذ الحكم الصادر بحقه لذا فاعتبار الجرائم الألكترونية من الجرائم المستمرة هو الحل الأمثل .

وفي مجال الاثبات يجب اعتماد الدليل الرقمي الى جانب الدليل المادي ,والدليل الرقمي هو الدليل المأخوذ من اجهزة الحاسب الآلي في شكل مجالات ونبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة.(٧)

والدليل الرقمي هو مكون رقمي لتقديم المعلومات في اشكال متنوعة مثل الرموز او النصوص المكتوبة او الصور او الأصوات او الأشكال والرسوم يعبر عن فكر وقول يطلق عليه الكتابة الرقمية بالمعنى الواسع ، التي لا تشمل الكتابة التقليدية على الورق فحسب بل تشمل الكتابة التي تتم عن طريق وسائل الاتصال الحديثة (شبكة المعلومات الدولية وما في حكمها) مهما كانت الدعامة المستخدمة في تثبيتها .(٨)

ويتمتع الدليل الرقمي بخصائص معينة هي :-

١ – الدليل الرقمي دليل غير ملموس .

٢ – الدليل الرقمي دليل فني أو علمي مستمد من الآلة .

٣ – يعتمد فهم مضمون الدليل الرقمي على استخدام اجهزة وتجميع وتحليل فحواه ليكون دليلا في الاثبات .

(٧) ممدوح عبد المجيد عبد المطلب \ استخدام بروتوكول Tcp\ip بحث وتحقيق الجرائم على الكومبيوتر منشور على الأنترنيت .

(٨) لمزيد في الاطلاع انظر د . مفتاح بو بكر \ مصدر سابق ص ٣٨ وما يليها

انواع الدليل الرقمي :--

١ – المخرجات ذات الطبيعة الورقية .

٢ – المخرجات ذات الطبيعة الألكترونية.

٣ – المخرجات المرئية المعروضة بواسطة شاشة الحاسب الآلي الخاصة به .

وقد قسمت وزارة العدل الأمريكية عام ٢٠٠٢ الدليل الرقمي الى ثلاثة اقسام :-

١ – السجلات المحفوظة في الحاسب الآلي .

٢ – السجلات التي يتم انشاؤها بواسطة الحاسب ومخرجات برامجه التي لم يساهم الانسان في انشائها كسجلات الهاتف وتوفير اجهزة الحاسب الآلي .

٣ – السجلات التي تم حفظ جزء منها بالادخال والجزء الآخر تم انشاءه بواسطة الحاسب الآلي ومن امثلة ذلك البيانات التي تم ادخالها الى الجهاز وتتم معالجتها من خلال برنامج خاص كاجراء العمليات الحسابية على تلك البيانات .

الدليل الرقمي كدليل اثبات يمكن تقسيمه الى :-

١ – ادلة اعدت لتكون وسيلة اثبات كالسجلات التي تم انشاءها بواسطة الآلة تلقائيا وكذلك السجلات التي جزء منها تم حفظه بالادخال وجزء تم انشاءه بواسطة الآلة .

٢ – ادلة لم تعد لتكون وسيلة اثبات وهذا النوع من الأدلة الرقمية ينشا دون ارادة الشخص اي انه اثر يتركه الفاعل دون ان يكون راغبا في وجوده .

هذا وقد تم الاعتراف بالدليل الرقمي كوسيلة اثبات في بعض التشريعات الاوربية والعربية منها المادة "١٣٠٦"من القانون المدني الفرنسي والتي تنص على" تقبل الكتابة في شكل الكتروني كدليل في الاثبات مثلها في ذلك مثل الكتابة على دعامة ورقية مادام الشخص المنسوب اليه هذه الكتابة قد تم تحديده على وجه صحيح وقد تم اثبات هذه الكتابة والاحتفاظ بها في ظروف من شأنها ان تحفظ سلامتها ."

والى مثل ذلك نحا المشرع القطري حيث نص في المادتين ١٥ و١٦ من القانون رقم ١٤ لسنة ٢٠١٤ على ما يلي : "م ١٥ لا يجوز استبعاد اي دليل ناتج عن وسيلة من وسائل تقنية المعلومات او انظمة المعلومات او شبكات المعلومات او المواقع الالكترونية او البيانات والمعلومات الالكترونية بسبب طبيعة ذلك الدليل ." "وم ١٦ لا يجوز استبعاد اي من الأدلة المتحصل عليها بمعرفة الجهة المختصة او جهات التحقيق من دول اخرى لمجرد ذلك السبب طالما ان الحصول عليها قد تم وفقا للاجراءات القانونية والقضائية للتعاون الدولي ".

الفصل الثالث :ـ الجهود الدولية والداخلية لمكافحة الجريمة الألكترونية

المطلب الأول :- الجهود الدولية لمكافحة الجريمة الألكترونية

تكاتفت الجهود الدولية على الصعيدين الدولي والعربي لمكافحة الجرائم الألكترونية ومنها :-

اولا :- ركز المؤتمران السابع و الثامن الخاصان بمكافحة الجريمة ومعاملة المجرمين على الجرائم الألكترونية وما تفرزه من صعوبات باعتبارها من الجرائم العابرة للحدود ذات الطابع الاقتصادي.

ثانيا :- حرص مجلس الاتحاد الأوربي على التصدي للجرائم الألكترونية مما أدى الى ابرام الاتفاقية الأوروبية لجرائم الحاسب الآلي والإنترنت المسماة باتفاقية بودابست بشأن الإجرام الألكتروني، الموقعة في ١١/٢٣ /٢٠٠١ على خمسة عناوين، الأول تناول أربعة أنواع من الجرائم هي: الجرائم التي تمس سرية وأمن وسلامة توفير بيانات الحاسب ومنظوماته وهي تضم (الدخول غير المشروع – والإعتراض غير المشروع – والتدخل في البيانات – والتدخل غير المشروع في المنظومة – وإساءة استخدام الأجهزة)، والثاني تناول الجرائم المتصلة بالحاسب الآلي وتضم (جريمة التزوير المتعلقة بالحاسب – وجريمة التدليس المتعلقة بالحاسب)، والثالث تناول الجرائم المتصلة بالمواد الإباحية للأطفال (الإنتاج أو النشر غير المشروع للمواد الإباحية وصور الأطفال الفاضحة)، والرابع تناول الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المرتبطة بها (الطبع والنشر) ؛ والعنوان الخامس خصص للمسؤولية وللجزاءات ، وهو يشتمل على بنود إضافية يشان الشروع و الاشتراك ، وأيضا الجزاءات أو التدبير وذلك طبقا للاتفاقيات أو المعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية .

ثالثا :- اصدر مجلس وزراء العدل العرب في دورته التاسعة عشر عام ٢٠٠٣ قرارا بشأن مشروع قانون عربي استرشادي لمكافحة جرائم تقنية وانظمة المعلومات يحتوي على ٢٧ مادة رسمت القواعد الأساسية كدليل تستعين به الدول العربية عند وضع قوانينها لمكافحة الجرائم الألكترونية .

رابعا :- مصادقة مجلس وزراء الداخلية العرب في دورته الحادية والعشرين عام ٢٠٠٤ على مشروع القانون الاسترشادي الذي اصدره مجلس وزراء العدل العرب .

خامسا :- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٢ وتحتوي على ٤٣ مادة في اربعة فصول خصص الأول للهدف من الاتفاقية والثاني للتجريم في المواد من ٥ ---٢١ والثالث لنطاق تطبيق الاحكام الاجرائية والرابع للاختصاص

سادسا :- في ١٤ نوفمبر ٢٠١٣ اعلنت شركة "مايكروسوفت " عن انشاء مركز لمكافحة الجريمة الألكترونية يضم اعضاء منها ، وشركات تعمل في مجال التكنولوجيا وبعض جهات تنفيذ القانون وتوظف " مايكروسوفت "حوالي ١٠٠ محام ومحقق وخبير تقني لمكافحة البرامج المزيفة ، والتصدي لانتشار المواد الاباحية الخاصة بالاطفال

على الأنترنيت ، ولعمليات الاحتيال الألكتروني وغيرها من المخاطر التي يتعرض لها مستخدموا الأنترنيت . ويرى الخبراء ان اقامة هذا المركز داخل مقر شركة "ميكروسوفت " هو رسالة رسمية من الشركة تعبر عن التزامها بالمساعدة في حل هذه المشكلة ومن بين التقنيات التي ستستخدم في مكافحة الجريمة الألكترونية تقنية " سايت برينت " التي تسمح بوضع خريطة لشبكات الجريمة المنظمة على الأنترنيت ، وتقنية " فوتو دي ان ايه " وهي تكنولوجيا متقدمة لمكافحة المواد الاباحية الخاصة بالأطفال بالاضافة الى تقنيات الطب الشرعي الألكتروني التي تستخدم في رصد الجرائم الألكترونية على مستوى العالم بما في ذلك اعمال النصب والاحتيال وانتحال الشخصية على الشبكة الألكترونية .

سابعا :- مقترح انشاء مركز لمكافحة الجريمة الألكترونية الذي قدمته المفوضية الأوربية /الجهاز التنفيذي للاتحاد الأوربي ، يهدف للمساهمة في حماية المواطنين الأوربيين والشركات من التهديدات المتزايدة التي يتعرض لها كل مستعمل لشبكة الأنترنيت وسيكون مقر المركز الجديد لمكافحة الجريمة الألكترونية في مكتب الشرطة الأوربية "يوروبول" في لاهاي / هولندا ، باشر عمله نهاية عام ٢٠١٣ .ومن الجرائم الالكترونية التي كشفها وتابعها والمنشورة على الانترنيت الآتي :

"مائة وثمانية عشر شخصا في ثمانين مطارا بخمسة وأربعين بلدا تم توقيفهم من طرف رجال الأمن في إطار مداهمات بشأن المتاجرة بتذاكر غير قانونية لرحلات جوية عبْر مختلف بقاع العالم تقوم بها شبكات إجرام منظَّم تسرق التذاكر على الإنترنت.

العملية التي أشرفت عليها ونسقتها الشرطة الأوروبية "يوروبول" استهدفت عمليات سرقة تُكلِّف شركات النقل الجوي المدني مليار دولار سنويا.

ويل فان جيميرت الناطق باسم مؤسسة الشرطة الأوروبية يوروبول يقول:

"في غالب الأحيان، الأمر لا يتعلق بأناس يحاولون قضاء عطلة بكلفة منخفضة بل بالإجرام المنظَّم. كما لاحظنا أن هذه المخالفات قد تكون مرتبطة بجرائم أخرى كتجارة المخدرات والهجرة السرية، بمعنى أن الأمر يتعلق بمجرمين يستخدمون هذا النظام".

هذه الجرائم تتم ايضا عبْر سرقة بطاقات الائتمان، غير أن الشرطة الأوروبية تقول إنها عازمة على محاربتها من خلال التنسيق بينها وبين أجهزة الشرطة العالمية وشركات الملاحة الجوية ومؤسسات البطاقات الائتمانية "[٩]

المطلب الثاني : - الجهود الداخلية لمكافحة الجرائم الألكترونية

جاءت معالجات كافة الدول متفرقة ومبتسرة بقوانين تعالج جانب او اكثر واغلب المعالجات كانت لحماية الملكية الفكرية والتوقيع الألكتروني وفي اغلب صورها تتسم بالتبعية للقوانين العقابية للجرائم التقليدية :

اولا : - الدول الأوربية والولايات المتحدة الامريكية : بادرت السويد لاصدار قانون بشأن حماية المعلومات الشخصية المخزنة في الحاسب الآلي والأنترنيت عام ١٩٧٣ المعدل عام ١٩٨٢ تلتها الولايات المتحدة الأمريكية حيث اصدرت عام ١٩٧٦ قانون

(٩) euronews 2015 © Copyright

خاص بحماية الحاسب الآلي وفي عام ١٩٨٤ اصدرت قانونا متعلقا بالتحليل المعلوماتي عدل في ١٩٨٦ وفي عام ٢٠٠٢ اصدرت قانون المعاملات التجارية الرقمية . اما فرنسا فبعد مد جزر حول دستورية القوانين المتعلقة بالجرائم الألكترونية أصدرت في نهاية القرن الماضي قانونا متعلقا ببعض الجرائم الألكترونية وفي عام ٢٠٠٠اصدرت القانون رقم ٢٣٠ بخصوص الاثبات والتوقيع الألكتروني .هذا وسارت الدول الأوربية تباعا في نفس الاتجاه للتصدي للجرائم الألكترونية .

ثانيا : – الدول العربية : اصدرت الجزائر مرسوم تنفيذي رقم ٢٠٧ لعام ٢٠٠٠ بشأن ضوابط وشروط كيفية اقامة خدمات الأنترنيت واستغلالها ، كما اصدرت تونس قانون رقم ٨٣ لسنة ٢٠٠٠ بشأن المبادلات والتجارة الألكترونية تلتها الأردن بالقانون المؤقت رقم ٨٣ لسنة ٢٠٠١ والذي اصبح نهائيا عام ٢٠١٠ ، ثم اصدرت دبي قانون رقم ٢ لعام ٢٠٠٢ بشأن المعاملات والتحارة الألكترونية ، واصدرت البحرين مرسوم بقانون رقم ٢٨ لعام ٢٠٠٢ المعدل عام ٢٠٠٦ بشأن المعاملات الألكترونية .أما مصر فقد اصدرت قانون رقم١٥ لعام ٢٠٠٤ بشأن المعاملات الألكترونية ، هذا واصدرت الامارات قانون رقم ٢ لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات ، كما اصدرت اليمن القانون ٤٠ لعام ٢٠٠٦ بشأن انظمة الدفع والعمليات المالية والمصرفية الألكترونية ،واصدرت المغرب قانون رقم ٢٠٠٧/٥٣/٠٥ المتعلق بالتبادل الألكتروني للمعطيات القانونية ، واصدرت عمان مرسوم سلطاني رقم ٦٩ لعام ٢٠٠٨ بشأن اللائحة التنفيذية لنظام التعاملات الألكترونية . أما قطر فقد اصدرت مرسوم بقانون رقم ١٦ لسنة ٢٠١٠ بشأن المعاملات والتجارة الألكترونية وفي١٦ ديسمبر ٢٠١٣ تمت احالة اصدار قانون مكافحة الجرائم الألكترونية الى لجنة الداخلية والخارجية لدراسته وابداء الرأي حوله , وفي الخامس عشر من سبتمبر عام ٢٠١٤ صدر القانون رقم ١٤ (قانون مكافحة الجرائم الألكترونية) .

وفي العراق لا يزال مشروع قانون جرائم المعلوماتية امام البرلمان حيث انهى قراءته الأولى في يناير ٢٠١٩ على ان يمضي في قراءته في الجلسات اللاحقة .

المطلب الثالث – قانون مكافحة الجرائم الألكترونية القطري رقم ١٤ لسنة٢٠١٤

يحتوي القانون على خمسة ابواب خصص الباب الأول للتعاريف حيث عرف وبدقة كل المصطلحات المتعلقة بالعملية الالكترونية وحدد في الباب الثاني الجرائم وفي الباب الثالث الاجراءات وفي الباب الرابع تناول التعاون الدولي ونص على الأحكام العامة في الباب الخامس .

اولا– التعاريف

١. تقنية المعلومات : اي وسيلة مادية او غير مادية أو مجموعة وسائل مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ,ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا او لاسلكيا في نظام معلوماتي او شبكة

معلوماتية .
٢. البيانات والمعلومات الآلكترونية : كل ما يمكن تخزينه او معالجته أو انشاؤه أو نقله باستخدام وسيلة تقنية المعلومات , وبوجه خاص الكتابة او الصور أو الصوت او الأرقام او الحروف أو الرموز أو الاشارات وغيرها .
٣. الشبكة المعلوماتية : ارتباط بين أكثر من وسيلة لتقنية المعلومات , للحصول على المعلومات وتبادلها , بما في ذلك الشبكات الخاصة والعامة والشبكة العالمية "الانترنيت" .
٤. نظام معلوماتي : مجموعة برامج واجهزة تستخدم لانشاء او استخراج المعلومات او ارسالها او استلامها او عرضها او معالجتها او تخزينها.
٥. البرنامج المعلوماتي : مجموعة من البيانات أو الأوامر القابلة للتنفيذ باستخدام وسيلة تقنية المعلومات والمعدة لانجاز مهمة ما .
٦. معالجة المعلومات : اجراء او تنفيذ عملية او مجموعة عمليات على البيانات او المعلومات سواء تعلقت بافراداو خلافه بما في ذلك جمع واستلام وتسجيل وتخزين وتعديل ونقل واسترجاع ومحو تلك المعلومات .
٧. بيانات المرور : اية بيانات او معلومات الكترونية تنشأ عن طريق احدى وسائل تقنية المعلومات توضح مصدر الاتصال والوجهة المرسلة اليها والطريق الذي تسلكه ووقت وتاريخ وحجم ومدة ونوع الخدمة .
٨. المحرر الالكتروني الرسمي : المحرر الرسمي الذي يصدر عن الجهات الحكومية او الهيئات او المؤسسات العامة باستخدام احدى وسائل تقنية المعلومات .
٩. الموقع الالكتروني : مكان اتاحة او معالجة البيانات او المعلومات الالكترونية على الشبكة المعلوماتية من خلال عنوان محدد .
١٠. الجريمة الالكترونية : اي فعل ينطوي على استخدام وسيلة تقنية المعلومات او نظام معلوماتي او الشبكة المعلوماتية بطريقة غير مشروعة بما يخالف احكام القانون .
١١. الالتقاط : مشاهدة البيانات او المعلومات الالكترونية او الحصول عليها .
١٢. بطاقة التعامل الالكتروني : البطاقة الالكترونية التي تحتوي على شريط ممغنط او شريحة ذكية او غبرها من وسائل تقنية المعلومات والتي تحتوي على بيانات او معلومات والتي تصدرها الجهات المرخص لها بذلك .

ثانيا – الأنماط الجرمية

قسم المشرع القطري الجرائم الالكترونية الى خمسة انواع وكالآتي :

١ – جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الالكترونية وقسمها الى :

أ – الدخول بغير وجه حق عن طريق الشبكة المعلوماتية أو باحدى وسائل تقنية

المعلومات الى موقع الكتروني او نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها .

وتضاعف العقوبة اذا ترتب على الدخول الحصول على بيانات او معلومات الكترونية او الحصول على بيانات او معلومات تمس الأمن الداخلي او الخارجي للدولة او اقتصادها الوطني اواية بيانات حكومية سرية بطبيعتها او بمقتضى تعليمات صادرة بذلك او الغاء تلك البيانات والمعلومات الالكترونية او اتلافها او تدميرها او نشرها او الحاق الضرر بالمستفيدين او المستخدمين او الحصول على اموال او خدمات او مزايا غير مستحقة .

ب – الدخول عمدا بغير وجه حق باي وسيلة موقعا الكترونيا او نظاما معلوماتيا او شبكة معلومات او جزء منها او تجاوز الدخول المصرح به او استمر في التواجد بها بعد علمه بذلك .

وتضاعف العقوبة اذا ترتب على الدخول الغاء او حذف او اضافة او افشاء او اتلاف او تغيير او نقل او التقاط او نسخ او نشر اصداراعادة نشر بيانات او معلومات الكترونية مخزنة في النظام المعلوماتي او الشبكة المعلوماتية او تغيير الموقع الالكتروني او الغائه او تعديل محتوياته اوتصميماته او طريقة استخدامه او انتحال شخصية مالكه او القائم على ادارته .

ج– التقاط او اعتراض او التنصت عمدا ودون وجه حق على اية بيانات مرسلة عبر الشبكة المعلوماتية او احدى وسائل تقنية المعلومات او على بيانات المرور .

٢ – جرائم المحتوى

أ– انشاء او ادارة موقعا لجماعة او تنظيم ارهابي على الشبكة المعلوماتية او احدى وسائل تقنية المعلومات او سهل الاتصال بقيادات تلك الجماعات او اي من اعضائها او الترويج لأفكارها او تمويلها او نشر كيفية تصنيع الأجهزة الحارقة او المتفجرة او اي اداة تستخدم في الأعمال الارهابية .

ب – انشاء او ادارة موقعا الكترونيا عن طريق الشبكة المعلوماتية او احدى وسائل تقنية المعلومات لنشر اخبار غير صحيحة بقصد تعريض سلامة الدولة او نظامها العام او امنها الداخلي او الخارجي للخطر .

ج – ترويج او بث او نشر بأي وسيلة اخبارا غير صحيحة بقصد تعريض سلامة الدولة او نظامها العام او امنها الداخلي او الخارجي للخطر .

د – انتاج مادة اباحية عن طفل بواسطة وسائل تقنية المعلومات او استورد او باع او عرض للبيع او الاستخدام او تداول او نقل او وزع او ارسل او نشر او اتاح او بث مادة اباحية عن طفل بواسطة وسائل تقنية المعلومات . كما وتعتبر حيازة مادة اباحية عن طفل جريمة بحكم القانون . هذا ولا يعتد في هذه الجرائم برضا الطفل ويعتبر طفلا في حكم هذه المادة كل من لم يتم من العمر ثماني عشرة سنة ميلادية كاملة .

هـ – استخدام الشبكة المعلوماتية او احدى وسائل تقنية المعلومات في تهديد او ابتزاز شخص لحمله على القيام بعمل او الامتناع عنه .

٣ – جرائم التزوير والاحتيال الالكتروني :

أ – تزوير المحررات الالكترونية الرسمية أوغير الرسمية او استعمالها مع العلم بانها مزورة .

ب – استخدام الشبكة المعلوماتية او احدى وسائل تقنية المعلومات في انتحال هوية شخص طبيعي او معنوي .

ج – استيلاء الشخص لنفسه او لغيره على مال منقول اوسند او التوقيع عليه بطريق الاحتيال او باتخاذ اسم كاذب او بانتحال صفة غير صحيحة .

د – استيلاء الشخص لنفسه او لغيره على مال منقول او على سند او التوقيع عليه بطريق الاحتيال او باتخاذ اسم كاذب او بانتحال صفة غير صحيحة .

٤ – جرائم بطاقة التعامل الالكتروني :

أ – الاستخدام اوالحصول او تسهيل الحصول دون وجه حق على ارقام او بيانات بطاقة تعامل الكتروني عن طريق الشبكة المعلوماتية او احدى وسائل تقنية المعلومات .

ب – تزوير بطاقة تعامل الكتروني باي وسيلة كانت .

ج – صنع او حيازة بدون ترخيص اجهزة او مواد تستخدم في اصدار او تزوير بطاقات التعامل الالكتروني .

د – استخدام او تسهيل استخدام بطاقة تعامل الكتروني مزورة مع علمه بذلك .

هـ – قبول بطاقة تعامل الكتروني غير سارية او مزورة او مسروقة مع علمه بذلك .

٥ – جرائم التعدي على حقوق الملكية الفكرية :

استخدام الشبكة المعلوماتية او احدى وسائل تقنية المعلومات في التعدي او تسهيل التعدي باي وسيلة وفي اي صورة على حقوق المؤلف او الحقوق المجاورة او براءات الاختراع اوالاسرار التجارية اوالعلامات التجارية او البيانات التجارية او الاسماء التجارية او المؤشرات الجغرافية او الرسوم والنماذج الصناعية او تصاميم الدوائر المتكاملة المحمية وفقا للقانون .

هذا كما نص القانون على جملة من الأحكام العامة حدد فيها صلاحيات والتزامات النيابة ومزودي الخدمة وأجهزة الدولة، وبين ضوابط لآليات المساعدة القانونية مع الدول الأجنبية للتحقيق في القضايا، وحدد حالات معينة لرفض تسليم المجرمين، وحدد عقوبات لإفشاء سرية الإجراءات بالقانون، كما نص على اعفاء الجناة من العقوبة في حالة ابلاغهم عن الجريمة والمشتركين فيها.قبل علم السلطات بها وقبل وقوع الضرر واجاز للمحكمة ان تقضي بوقف تنفيذ العقوبة اذا حصل الابلاغ بعد علم السلطات بها وادى الى ضبط باقي الجناة .

تقييم القانون رقم ١٤ لسنة ٢٠١٤

تختلف وجهات النظر في كل الأمور أو أغلبها ومنها القوانين لذا سنعرض بعضا منها :

– قالت منظمة العفو الدولية إن قانون مكافحة الجرائم الإلكترونية الجديد، والمثير للجدل، الذي يجرم نشر "أخبار غير صحيحة" على شبكة الإنترنت يشكل تهديداً جديا لحرية التعبير عن الرأي في قطر.

ووفق أحكام القانون الجديد، يجوز للسلطات حظر المواقع الإلكترونية التي ترى فيها تهديدا "لسلامة" البلاد، وتعاقب كل من ينشر أو يتبادل محتويات رقمية "تقوض" من "القيم الاجتماعية" في قطر أو "النظام العام فيها" على الرغم من أن القانون يسكت عن تعريف مثل هذه العبارات والمصطلحات.

وفي معرض تعليقه على الموضوع، قال نائب مدير برنامج الشرق الأوسط وشمال إفريقيا بمنظمة العفو الدولية، سعيد بومدوحة: "يُعد قانون مكافحة الجرائم الإلكترونية الجديد بمثابة انتكاسة لحرية التعبير عن الرأي في قطر".

وأردف بومدوحة قائلاً: "يتضمن القانون الجديد أحكاماً فضفاضة ومبهمة الصياغة تناقض المعايير الدولية بشكل صارخ. إذ تنص فعلياً على منح الحكومة صلاحيات واسعة لمعاقبة كل من يقوم بنشر أو تبادل محتوى رقمي يعتبره المسؤولون ضاراً بقيم قطر الاجتماعية أو مصالحها الوطنية."

وأضاف بومدوحة: "ثمة خطر حقيقي بأن يقوض القانون الجديد من التعبير السلمي والمشروع عن الرأي من خلال تيسير القمع التعسفي للمعارضة السلمية".

ويتناول القانون مسائل من قبيل سرقة المعلومات وتزويرها وحقوق الملكية، وغير ذلك من الأفعال التي تُعتبر جرائم في عرف القانون الدولي، ولكنه يشترط أيضاً على مزودي خدمات الاتصالات القيام بحجب المواقع الإلكترونية، أو تزويد السلطات بأدلة أو سجلات بناء على طلبها. وتخضع حرية التعبير عن الرأي في قطر للرقابة الصارمة، وغالبا ما تمارس الصحافة المحلية الرقابة الذاتية على عملها [١٠]

– كما طالبت لجنة حماية الصحافيين باعادة النظر في القانون حيث بين منسقها في الشرق الأوسط بان "هذا القانون يهدف ظاهريا الى وقف الجرائم الالكترونية ولكنه يحد في مادتين على الاقل بشكل كبير من حرية التعبير وهي ليست جريمة وهما المادة السادسة والتي تنص على السجن ثلاثة اعوام والتغريم نصف مليون ريال لاقامة او ادارة موقع الكتروني يقوم بنشر اخبار خاطئة بهدف تهديد امن الدولة ".والمادة الثامنة التي تنص على السجن ثلاثة اعوام والتغريم مئة الف ريال لأي انتهاك للقيم الاجتماعية او نشر اخبار او صور او تسجيلات صوتية او مصورة تتعلق بالحياة الشخصية والعائلية للافراد حتى ولو كانت صحيحة " .[١١]

الا اننا نرى بان الصدق والمعلومة الصحيحة قيم اساسية في بناء كل مجتمع

(١٠) منظمة العفو الدولية /١٩ /٢٠١٤/٩ شبكة الاعلام العربية moheet .com

(١١) صحيفة الوسط البحرينية العدد ٤٣٩٥ الجمعة ١٩ سبتمبر ٢٠١٤.

والانسان مسؤول عن ما يصدر عنه من اقوال وكتابات ورسوم وغيرها من الأفعال مسؤولية يحتمها عليه احترامه لنفسه ولمجتمعه هذا من ناحية ومن ناحية اخرى ان حرمة الحياة الشخصية مصانة في الدساتير والقوانين ومنها القطرية .ومن ناحية ثالثة ما جاءت به الطفرة التكنولوجية من اساليب تخدم المجتمع وتطوره وتنوره وفي نفس الوقت تهده وتخربه بما تنقله من معلومات تغذي الكذب والنفاق والاستهتار والارهاب وما الى ذلك اوجبت تشريع قوانين كالقانون القطري رقم ١٤ لسنة ٢٠١٤ لمكافحة الجريمة الالكترونية ليواكب مستجدات التحولات التي يشهدها المجتمع القطري كباقي المجتمعات ويجسد حصانة قانونية ضرورية تواكب الطفرة التكنولوجية .

ان وجود تشريعات قانونية في هذا المجال مع ضمان توظيفها بمسؤولية الحرص على احترام روح النص القانوني والنظر الى ما وراء هذا النص من حماية للكيان الاجتماعي للفرد والأسرة والمجتمع ومؤسسات الدولة ونظامها السياسي بما يضمن الحد المطلوب من حرية الرأي وحرية التعبير فاحترام حرية الرأي وحرية التعبير حقوق يكفلها الدستور والكفالة هذه غير مطلقة حيث انها كباقي الحقوق مقيدة باحترام حقوق الآخروبضمان سلامة المجتمع وقيمه .

ان قانون مكافحة الجرائم الالكترونية يتسم بالمرونة الكافية بما يضمن حرية التعبير والتمكين من الوصول الى المعلومة الصحيحة من ناحية ومن ناحية اخرى ان الاطلاع عليه بامعان وتثقيف المواطنين والمقيمين به يوسع من دائرة الاستعمال الصحيح لوسائل التواصل الاجتماعي بما يكفل تعزيز ثقافة الكترونية تحترم المعلومة وقيم المجتمع وتوظف تكنولوجيا المعلومات التوظيف الأمثل .

الخاتمة

لابد لنا في ختام الموضوع ان نخلص الى توصيات معينة نلخصها بما يلي :--

١- التوعية اللازمة باهمية الوسائل الألكترونية وبايجابياتها وبالطرق الصحيحة لاستخدامها باعتبارها وسيلة وجدت لخدمة البشرية .

٢- التوعية بمضار الاستخدام غير الصحيح لوسائل الاتصال الألكتروني كاعطاء تفاصيل دقيقة عن الشخصية او الحساب المصرفي دون التأكد من شخصية المقابل ،أواستقبال ايميلات من جهات مجهولة قد تحمل فيروسات ،أوتصديق المغريات بالحصول على جائزة أو ارث أو اقامة واعطاء المعلومات الدقيقة التي قد تستخدم في سحب الأرصدة أو في عمليات الاحتيال .

٣ – التوعية بمضار التواصل مع المواقع السيئة كالمواقع الاباحية أو التي تساهم في انحراف السلوك .

٤- سد الفراغ التشريعي واعتماد الأسس القانونية المتطورة في النظرة الى الجرائم الألكترونية .ومنها :-

أ – اعتماد معيار المال المعنوي الى جانب المال المادي محلا للجريمة .

ب – اعتبار الجريمة الألكترونية من الجرائم المستمرة .

ج – اعتبار الجريمة الألكترونية من الجرائم العابرة للحدود يطبق عليها معيار العالمية في الاختصاص وعند النظر في تنازع الاختصاص عكس المعطيات التالية ،وهي الأولوية للاختصاص الاقليمي للدولة التي توجد متحصلات الجريمة على اقليمها ثم الاختصاص الشخصي للدولة التي يحمل جنسيتها بحيث ينعقد اختصاص كافة الدول التي يحمل جنسياتها في حالة تعدد جنسياته .

د – اعتماد الدليل الرقمي في الاثبات واعطاءه نفس اهمية الدليل الكتابي الورقي .

هـ – الاهتمام بالتعاون الدولي في مجال مكافحة الجريمة الألكترونية بعقد معاهدات دولية من بنودها التسليم والمحاكمة وتطبيق احكام المحاكم الأجنبية .