التعدي الإلكتروني والأمن المعلوماتي في ظل قانون الجرائم الالكترونية الليبي رقم 5 لسنة 2022م دراسة مقارنة

نجاة سالم عبدالرحمن سعيد

كلية القانون جامعة الزيتونة

الملخص:

بتتبع السلسلة التاريخية للأنترنت سنجد أنه تطور عبر الزمن، حيث ظهر في بداية الأمر في شكل مراسلات، تطورت فيما بعد لتظهر في شكل بريد الكتروني الذي تطور بدوره ليتحول إلى شبكات ومحركات بحث ترعاها وتشرف عليها وتديرها شركات عالمية؛ الأمر الذي أدى إلى ظهور العالم المعلوماتي الموازي للعالم الذي نعيشه والذي لا يقل أهمية عنه وعلى ذلك، فليس بالأمر الغريب وقوع السلوكيات الإجرامية ضمن إطاره وذلك من خلال تعرض المعلومات الالكترونية من رسائل وصور واتصالات وبطاقات ائتمان وغيرها إلى مجموعة من المخاطر في مختلف مراحلها، ولم يقف الأمر عند هذا الحد بل تطور الأمر إلى مرحلة متقدمة من الاجرام حيثُ ظهر الابتزاز الالكتروني والقرصنة والنصب والاحتيال وغيرها من صور التعدي الالكتروني الذي بات يمثل الجانب السلبي والمظلم لتقنية المعلومات والتواصل؛ ذلك من زاوية ومن زاوية أخرى باتت هذه السلوكيات تهدد القيم والمصالح العليا في المجتمع وتمس بأمنه القومي، واستقراره المالي حيثُ تسبب في الخسائر الاقتصادية والأزمات المالية والأخلاقية في المجتمعات الإسلامية، كل ذلك لا يخرج عن كونه اختراق للخصوصية أي جرائم جنائية الأمر الذي يتطلب الحيلولة دون وقوعها، وذلك من خلال حزمة من الاجراءات الفنية والقانونية الجنائية ، لتقرير الحماية اللازمة للحياة الخاصة، والحيلولة دون هتك سترها، وبالتالي فأن السؤال الرئيس الذي يطرحه البحث هو: ماهي

أهم صور وسائل الحماية المتبعة لتأمين المعلومات الالكترونية سواء على الصعيد الفني بوصفها تمثل الجانب الوقائي أو على الصعيد التشريعي بوصفه يمثل الجانب العلاجي وما مدى فاعليتها أمام تزايد مخاطر الجرائم الالكترونية وقلة الدراسات السابقة، لحداثة طرح تفاصيل الموضوع على طاولة البحث خاصة في الدول العربية.

الكلمات المفتاحية:

التعدي ، الأمن ، الابتزاز الالكتروني، المشرع الليبي، الجرائم، القرصنة

المقدمة:

نظراً للأهمية التي تشكلها مواقع التواصل الاجتماعي بمختلف أنواعها، والتي فرضتها الثورة التقنية التي اكتسحت الوجود بفعل العولمة التكنولوجية، حيثُ أضخت تقنية المعلومات والاتصالات البشرية تقدم خدمات رئيسية في مختلف مجالات الحياة خاصة في مجال التجارة الاليكترونية فقد أضحى العالم في ظلها يبدوا وكأنه رقعة جغرافية واحدة واعتمدت عليها أغلب الدول، الأمر الذي نتج عنه تطوراً في نوع الإجرام والتعدي الجنائي، إذ لم يعد الأمر مقتصراً على الاعتداء الجسدي أو اللفظي أو المالي الملموس فحسب، بل امتد ليشمل الاعتداء الإلكتروني والمعلوماتي، والتعدي على الخصوصية كنسخ ولصق بعض المعلومات دون علم مصدريها وكذلك اختراق مواقع التواصل الاجتماعي والمساس بالعرض والآثار والأنفس وغيرها من المخاطر الالكترونية التي تتعرض لها المعلومات ، في جميع مراحلها والتي يصعب حصرها، فأصبحت بذلك الحاجة ملحة إلى تأمين الفضاء السيبراني وبالتالي فأن أهمية البحث تنبع من اعتبار العالم الافتراضي، عالمًا موازيًا للعالم الواقعي، تحدث فيه الجرائم شأنه شأن الأخير، وقد تكون في الأول أسوء وطأة ؛ باعتبارها تدل على أن مرتكبيها على درجة عالية من الخطورة الإجرامية، بوصفهم يرتكبون و ينفذون مشروعاتهم الإجرامية بواسطة التسلل إلى حسابات الغير سواء كانوا أشخاص طبيعيين أو اعتباريين، كالتسلل إلى المنظومات المعمول بها داخل مؤسسات الدولة ، و تتمحور بذلك إشكاليته التي تدور حول ضرورة تحصين المعلومات الإلكترونية ووضع أسوار من الحماية الجنائية لتطويق شبكة الاتصالات بأكملها بحيث تصبح محصنة فلا يمكن الوصول إليها و هتكها ،ومن أهم

التساؤلات التي طرحتها هذه الإشكالية: هل يمكن الاعتماد على الجانب الفني فقط لضمان هذا التحصين أم أنه لا بد من النظر إلى الوسائل التشريعية لمواجهة هذا التعدي، ومحاسبة كل من تسول له نفسه تجاوز حدود خصوصية الآخرين؟ وهل تبنى المشرع الجنائي الليبي سياسية جنائية موضوعية واجرائية ناجزة في مواجهة التعديات الالكترونية مقارنة بغيره من التشريعات العربية؟ وإلى أي حد كان موفق في مسلكه الذي تبناه؟ ومن خلال أهمية البحث وإشكاليته يمكن تحديد نطاقة، كما تم الاعتماد على المنهج التاريخي تارة والتحليلي تارة والنقدي تارة أخرى والمقارن كلما دعت الضرورة إلى ذلك، وكلما أمكن ذلك، حيثُ تم طرح تفاصيل البحث ضمن هيكلية ثنائية مقسمة كالتالي:

المطلب الأول: وسائل الحماية الوقائية.

المطلب الثاني: وسائل الحماية العلاجية.

المطلب الأول

تدابير الحماية الوقائية

تتعرض المعلومات الإلكترونية في مرحلة نشأتها وتكوينها الأول واسترجاعها وإلغائها وجمعها داخل النظام لمخاطر، كخرق الحماية المادية؛ المتمثلة في التفتيش في مخلفات التقنية كما تواجه خطر استراق الأمواج، ويتم ذلك باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم باختلاف أنواعها وكذلك إنكار أو إلغاء الخدمة ويقصد بذلك: الإضرار المادي بالنظام لمنع تقديم الخدمة، فضلاً عن ذلك قد يتم خرق الحماية المتعلقة بالأشخاص، ويتم ذلك بتخفي الفاعل عن طريق انتحاله لصلاحيات شخص مفوض؛ ويتم هذا من خلال الدخول غير المصرح به إلى النظام عبر استخدام وسائل التعريف الخاصة بمستخدم آخر مصرح له بالدخول إلى النظام الخاص، وقد يتم خرق الحماية بواسطة الهندسة الاجتماعية، ويتم الحصول على معلومات تهيئ الاقتحام من خلال علاقات اجتماعية، كما قد يلجأ المخترق إلى الإزعاج والتحرش الذي يكون في صورة تهديدات يندرج تحتها أنواعا عديدة من الاعتداءات والأساليب غير المشروعة، وقد يكون في صورة توجيه رسائل الإزعاج والتحرش، أو عن طريق فرصته البرمجيات التي تتحقق بواسطة نسخها دون تصريح

أو استغلالها على نحو مادي دون تخويل بهذا الاستغلال أو تقليدها ومحاكاتها والانتفاع المادي بها على نحو يخل بحقوق صاحبها. (العالم، جرائم نظم المعلومات، ص 15) .

فضلاً عن ذلك قد يمتد الاختراق المادي إلى الحماية المتعلقة بالاتصالات والمعطيات وذلك من خلال الهجوم على المعطيات ونسخها بشكلٍ غير مصرح به؛ وهي العملية الشائعة التي تتبع الدخول غير المصرح به للنظام، كالاختراق الذي يقصد به: الهجوم على المواقع الموجودة على شبكة الإنترنت، والذي يكون مبني بالدرجة الأولى على فكرة السيطرة عن بعد ،بالإضافة إلى المخاطر التي تهدد أمن المعلومات الإلكترونية سالفة الذكر توجد صور من خلالها يمكن للمعتدى أن ينفذ مشروعه الإجرامي ،عبر شبكات الإنترنت والتي تقع في مقدمتها الفيروسات، فالفايروس: عبارة عن برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، غير أنها مصممة بصورة تمكنها من التأثير على كافة البرامج الأخرى الموجودة على الحاسب الآلي، سواء بجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى على جهاز الحاسب الآلي، بالتالي تعطلها عن العمل، كل هذه المخاطر وغيرها من السلوكيات المجرمة أو التي ينبغي تجريمها بو صفها تمثل مساسًا غير مشروع بحقوق الأفراد والمجتمعات، تتطلب حماية وقائية وأخرى علاجية ، فأمام التغيرات والتطورات المتسارعة والمتفاوتة لا يمكن حصر موضوع الحماية في الجانب التشريعي فحسب، بل من الممكن استخدام وسائل أخرى لحماية الحقوق والحريات قبل اللجوء إلى السلطة التشريعية ومطالبتها بسن تشريعات تجرم الاعتداء على حق من الحقوق المعتبرة واللازم حمايتها ،فتمت وسائل يمكن تفعيلها لتحقيق الأمن المعلوماتي ، والتي تعرف بأدوات السياسة الوقائية، أي وسائل تحقيق أمن الشبكة الإلكترونية والمتمثلة في حزمة من الجدران الأمنية، كمجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته كخطوة لتحقيق الأمن المعلوماتي ، وتهدف هذه الوسائل إلى ضمان استخدام النظام من قبل الشخص المخول بهذا الاستخدام، بالإضافة إلى مجموعة الوسائل المتعلقة بالتحكم بالدخول، والنفاذ إلى الشبكة باعتبارها تساعد في التأكد من أمان الشبكة ومصادرها والتأكد من أنها استخدمت استخداماً مشروعاً وتتمثل في مجموعة الوسائل الهادفة إلى منع إفشاء المعلومات لغير المخولين بذلك ، وتهدف إلى تحقيق

سرية المعلومات وتشتمل هذه الوسائل: الآلية الفنية المتبعة في تشكيل جدار من الحماية الفنية والآلية التشريعية المتبعة في تشكيل أو صنع إطار الحماية الجنائية وصناعة طوقها اللازم لحماية الخصوصية وضمان عدم اختراقها، وتتمثل وسائل الحماية الوقائية، في مجموعة التدابير الفنية التي أعدها المخترعون لضمان أمان الشركة مثل: تقنيات تشفير المعطيات والملفات وإجراءات حماية حفظ النسخ، بالإضافة إلى الحماية المادية للأجهزة ومكونات الشبكات واستخدام الفلترات والموجهات فضلاً، عن مجموعة الوسائل الهادفة للحماية التكاملية (سلامة المحتوى)، وهى الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مصرح لها بذلك وتشمل من بين ما تشمل تقنيات الترميز والتوقعات الإلكترونية وبرمجيات تحرى الفيروسات، ومن أهم صور وسائل الحماية الفنية ما يعرف بالجدران النارية : وهى :- عبارة عن أدوات بسيطة تعمل كمنفذ للإنترنت؛ أي تعمل الحارس على الشبكة، حيث تقوم بتنظيم حركة البيانات، وتحافظ على أمن الشبكة، وهي عبارة عن موجهات تستخدم في تقسيم الشبكات وقد تم استخدام أول جدران نارية لتحقيق الأمن في أوائل التسعينات، وكانت في صورة موجهات لبروتوكول IP مع قوانين فلترة كانت تبدو كالتالي: - اسمح لفلان بالدخول والنفاذ للملف التالي - امنع فلان من الدخول (الجهيني، 2001، ص10).

وقد كانت هذه الجدران فعالة ولكنها محدودة؛ حيث كان من الصعب وضع قوانين فلترة البيانات وفي بعض الأحيان يصعب تحديد أجزاء التطبيقات المراد منعها من النفاذ إلى الشبكة، وفى أحيانا أخرى كانت عناصر الشبكة أعلى مثل الموظفين العاملين ضمنها قد يتغيرون فتتغير تبعاً لذلك القوانين، ولذلك كان. الجيل الثاني من الجدران النارية أكثر قدرة وأكثر مرونة للتعديل، فضلاً عن ذلك فأن الجدران النارية، كانت توضع على ما يعرف المستضيفات الحصينة، وأول جدار ناري من هذا النوع يستخدم الفلاتر وبوابات التطبيقات (البرمجيات الوسيطة) كان من شركة ديجيتال اكو يمنت، وكان يعتمد على الجدار الناري من شركة DC باعتبارها أول من وضعت الجدران النارية التي أنتجتها الشركة الذي تتكون من نظام خارجي يدعى بحارس البوابة، وهو النظام الوحيد الذى يمكنه مخاطبة الأنترنت، بالإضافة إلى قدرته على التحقق من هوية المستخدمين، وللتحقق

من الهوية لا بد من استخدام استراتيجية جيدة بشكل يتجاوز مجرد التحقق من اسم المستخدم والكلمات السرية التي لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين؛ وذلك لأنه عن طريق استخدام وصلة غير خاصة مثل وصلة غير مشفرة عبر الإنترنت، فإن أسماء المستخدمين وكلماتهم السرية يمكن نسخها وإعادة استخدامها، أما الأساليب القوية للتحقق من هوية المستخدمين ،فتستخدم أساليب التشفير مثل: الشهادات الرقمية التي يمكن من خلالها، تفادي هجمات إعادة الاستخدام حيث تم نسخ اسم المستخدم، وإعادة استخدامها ولتحقيق الحماية الالكترونية، لا بد من التعرف على طرق حية للتعامل مع الخطر الذي تتعرض له المعلومات، من خلال اختراق الحسابات الخاصة والعامة، والدخول غير المشروع إلى شبكات الإنترنت، والتي قسمها المختصون إلى مراحل يأتي في مقدمتها تصنيف المعلومات، ثم توثيقها لمعرفة المهام والواجبات الإدارية، المُلقى بها على عاتق المتصلين ومستخدمي الشبكات، سواء كانت هذه المهام شخصية أو إدارية وعلى ذلك فأن تصنيف المعلومات يعتبر عملية أساسية عند بناء أي نظام او في بيئة أي نشاط يتعلق بالمعلومات، وتختلف التصنيفات حسب المنشأة، فقد تصنف المعلومات الي معلومات متاحة وأخرى موثوقة وسرية للغاية، وقد تكون معلومات متاح الوصول إليها، وأخرى محظور الوصول إليها وهكذا، أما بالنسبة لمرحلة التوثيق فأهمية هذا الإجراء تتطلب اتباع نظام التوثيق الخطى لبناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها، وبشكل رئيس فأن نظام التعريف والتحويل وتصنيف المعلومات، يتطلب وجود استراتيجية أو سياسة الأمن موثقة ومكتوبة، وأن تكون إجراءاتها ومكوناتها كاملة، بالإضافة إلى خطط التعامل مع المخاطر والحوادث والجهات المسؤولة ومسؤولياتها وخطط التعافي، وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر، لأن مهام المتصلين بنظام أمن المعلومات تبدأ في الأساس من حسن اختيار الأفراد المؤهلين و عمق معارفهم النظرية والعملية، على أن يكون مدركاً أن التأهيل العلمي يتطلب تدريباً متواصلاً، ولا يقف عند حدود معرفة وخبرة هؤلاء عند تعيينهم، وبشكل رئيس فأن المهام الادارية أو التنظيمية تتكون من ستة عناصر هي: تحليل المخاطر ووضع السياسة الإدارية أو التنظيمية،

تحديد المعاملة أو الاستراتيجية ووضع خطة الأمن ووضع البناء الأمني، وتوظيف الأجهزة والمعدات والوسائل، وتنفيذ الخطط والسياسات.

ومن المهم أن ندرك أن نجاح الواجبات الإدارية يتوقف على درجة ادراك كل المعنيين في الإدارة بمهامهم التقنية والإدارية والمالية على اعتبار أن مسائل الأمن يدركها الكافة، ويمكن للكل التعامل مع ما يخص واجباتهم من بين عناصر الأمن، وكذلك على المستوى الشخصي أو على مستوى المستخدمين فأنه على المؤسسة أن تضع التوجيهات الكافية لضمان وعى عام ودقيق بمسائل الأمن، لبناء ثقافة الأمن لدى العاملين، والتي تتوزع بين وجوب مراعاة اخلاقيات استخدام التقنية وبين الإجراءات المطلوبة من الكل عند ملاحظة أي خلل على كل مستخدم أن يعلم ما له وما عليه عند استخدامه لوسائل التقنية المعلوماتية، من وسائل الأمن الفنية التي يجب اتباعها لمنع الاختراق أو التعدي على الخصوصية التي من الممكن استخدامها في بيئة الانترنت والأجهزة التي تمكنا منه، بالإضافة إلى الجدران النارية والتشفير ونظام التحكم في الدخول ونظام تحرى الاختراق وبرمجيات مقاومة الفيروسات، توجد وسيلة مهمة جداً، والمتمثلة في ضرورة التعرف على المستخدمين ووضع حدود الاستخدام، لأن الدخول إلى أنظمة الكمبيوتر وقواعد البيانات ومواقع المعلوماتية عموما يمكن تقييده بالعديد من الوسائل مثل: التعرف على شخصية المستخدم وتحديد نطاق الاستخدام، وهو ما يعرف بأنظمة التعرف علي المستخدمين، ووضع حدود لصلاحيات الاستخدام والتحويل، وتتكون هذه الأنظمة من خطوتين أساسيتين هما : وسيلة التعرف على شخص المستخدم قبول وسيلة التعرف ،وهو ما يسمى بالتوثيق من صحة الهوية المقدمة وتختلف وسائل التعريف باختلاف التقنية المستخدمة وهي نفسها وسائل أمن الوصول إلى المعلومات، أو الخدمات في قطاعات استخدام النظم أو قطاعات الأعمال الإلكترونية، وبشكل عام فإن هذه الوسائل تتوزع إلى ثلاثة أنواع:

1- شيء ما يملكه الشخص مثل البطاقة البلاستيكية أو غير ذلك.

2- شيء ما يعرفه الشخص مثل كلمات السر أو الرمز أو الرقم الشخصي أو غير ذلك.

3- شيء ما يرتبط بذات الشخص موجود فيه مثل: بصمة الأصبع أو بصمة العين وغيرها. (الهاجري، 2002، ص16)

وتعد وسائل التعريف والتوثيق الأقوى من بين تلك الوسائل على نحو لا يؤثر على سهولة التعريف، وفعاليته في ذات الوقت، وفي جميع الأحوال أيا كانت وسيلة التعريف التي سيتم اتباعها، يجب أن تخضع لنظام أمن وارشادات أمنية يتعين مراعاتها فكلمات السر مثلاً: وهي الأكثر شيوعاً من غيرها من النظم التي تتطلب أن تخضع لسياسة مدروسة من حيث طولها أو مكوناتها، والابتعاد عن تلك الكلمات التي يسهل تخمينها أو تحريها، وكذلك خضوع الاستخدام لقواعد عدم الاطلاع وعدم الإفشاء والحفاظ عليها، ومتى ما استخدمت وسائل تعريف ملائمة لإتاحة الوصول للنظام، ومتى ما تحققت عملية التوثق والمطابقة والتأكد من صحة التعريف (الهوية) فإن المرحلة التي تلي ذلك هي: تحديد نطاق الاستخدام، وهو ما يعرف بالتحويل أو التصريح باستخدام قطاع ما، وهذه المسألة تتصل بالتحكم بالدخول، أو التحكم بالوصول إلى المعلومات أو أجزاء النظام، وسجلات الأداء أيضًا بدورها تعتبر صورة من صور الأمن المعلوماتي، حيث تحتوى مختلف أنواع الكمبيوترات وما في حكمها على نوع من السجلات التي تكشف استخدامات الجهاز وبرمجياته، وآلية النفاذ إليه، وفي حالة تعدد المستخدمين ؛أي حالة شبكات الكمبيوتر التي يستخدم مكوناتها أكثر من شخص فنى، وعليه فإن هناك أكثر من نوع من أنواع سجلات الأداء وتوثيق الاستخدامات، كما أن سجلات الأداء تتباين من حيث نوعها وطبيعتها وعرضها، فهناك سجلات تاريخية وأخرى مؤقتة وثالثة للتبادل وسجلات للنظام، وعلي رأس الهرم سجلات الأمن، وبشكل عام فإن سجلات الأداء منوط بها أن تحدد شخص المستخدم ووقت الاستخدام ومكانه، وطبيعته ومحتواه وإلى معلومات أخرى تتبع النظام نفسه ومن وسائل الأمن التقنية أيضاً، عملية الحفظ المتمثلة في عمل نسخة إضافية من المواد المخزنة على إحدى وسائط متحركة التخزين، سواء داخل النظام أو خارجه، وتخضع عمليات الحفظ إلى قواعد يتعين أن تكون محددة سلفاً، وموثقة ومكتوبة، ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية كما يمثل وقت الحفظ وحماية النسخة الاحتياطية ونظام الترقيم والتبويب، وآلية الاسترجاع والاستخدام ومكان

الحفظ، وأمنه وتشفير النسخ التي تحتوي على معطيات خاصة وسرية مسائل رئيسية يتعين اتخاذ معايير واضحة ومحددة بشأنها، وفي جميع الأحوال وبغض النظر عن حجم وسائل الأمن التقنية المستخدمة، ومعايير الأمن وإجراءاته المتبعة، فإنه لا بد من نظام متكامل للتعامل مع المخاطر والحوادث والاعتداءات الإلكترونية المختلفة، والتي يأتي في مقدمتها اختراق الخصوصية ويأتي في مقدمة أدوات السياسة الجنائية الوقائية الهادفة إلى الحيلولة دون وقوع الجرائم الالكترونية ومواجهتها ومكافحتها الصك الدولي ذو الطابع العالمي متمثلاً في اتفاقية الأمم المتحدة لمكافحة الفساد لعام 2003م، والتي تعتبر ليبيا من الدول الأطراف فيها، ونتيجة لعدم قابلية نفاذ هذا النص بشكل مباشر، الأمر الذي دفع المشرع الجنائي الليبي إلى تشريع القانون رقم 5 لسنة 2022م بشأن الجرائم الاقتصادية، والتي احتوت على ايحاءات تشير بطريقة غير مباشرة إلى ضرورة تجريم التعديات الالكترونية؛ وذلك من خلال حثها الدول الأطراف على تعزيز الشفافية والمساءلة وضرورة استخدام التكنولوجيا الحديثة؛ لمنع الفساد مما يشمل الأدوات الرقمية والأنظمة الالكترونية وإذا كانت هذه المواجهة تشكل منظومة الأمن التقني والفني أو الإلكتروني، فما هي محتويات المنظومة الأمنية التشريعية، سواء على المستوى الدولي أو الوطني، هذا ما سنسلط عليه الأضواء في التالي:

المطلب الثاني

تدابير الحماية العلاجية

ثمة مجهودات دولية بذلت في سبيل تحقيق الأمن المعلوماتي، وحماية الخصوصية المعلوماتية ، يأتي في مقدمتها، المجهودات التي بذلتها منظمة التعاون الاقتصادي والتنمية التي تضم في عضويتها حوالي 29 دولة، وغرضها الرئيسي هو تحقيق أعلى مستويات النمو الاقتصادي لأعضائها وتناغم التطور الاقتصادي مع التنمية الاجتماعية، حيثُ وضعت هذه المنظمة أدلة وقواعد إرشادية بشأن حماية الخصوصية، ونقل البيانات، وقد تم تبنى هذه القواعد من قبل مجلس المنظمة، مع التوصية للأعضاء بالالتزام بها، وتغطي هذه القواعد الأشخاص الطبيعيين فقط، وتتضمن التوجيهات هذه المبادئ الرئيسية لحماية الخصوصية، وحماية البيانات الخاصة، كما نصت الاتفاقية الأوروبية لحقوق الانسان والحريات على وجوب حماية الحياة الخاصة للأفراد من

التدخل والاعتداء، ونصت أيضًا على وجوب حماية الحقوق المعلوماتية وذلك من خلال توفير القدر اللازم من الحماية القانونية الكفيلة بذلك (المادة الثامنة والعاشرة من الاتفاقية المذكورة التي ابرمت بموجب اتفاق عالمي بشأن حماية الخصوصية عن طريق مجلس أوروبا عام 1950م).

كما تم تكليف لجنة وزراء من المجلس نفسه، مهمتها معالجة موضوع الخصوصية المتعلقة بحماية الأفراد في نطاق المعالجة الآلية للبيانات الشخصية، وقررت هذه الاتفاقية عشر مبادئ، تمثل الحد الأدنى لمعايير حماية الخصوصية، وهذه والمبادئ متقاربة جداً مع المبادئ التي أقرتها منظمة التعاون الاقتصادي والتنمية مع مزيداً من التفصيلات، وفي عام 1989م تبنت الأمم المتحدة دليلاً يتعلق باستخدام الحسابات في عملية تدقيق البيانات الشخصية وفي عام 1995م تبنت الهيئة العامة دليل استخدام المعالجة الآلية للبيانات الشخصية، وفي سبيل حماية الخصوصية، والحيلولة دون انتهاكها بدلت العديد من الجهود من قبل لجنة حقوق الانسان لدى الامم المتحدة كما أطلقت مجموعة الدول الثمانية، مجموعة توصيات لحماية الخصوصية ضمن مؤتمرها الذي عقد حول مجتمع المعلومات عام 1999م، ومن المجهودات المبذولة في سبيل حماية الأمن المعلوماتي أيضًا مناقشة منظمة التجارة العالمية مسائل الخصوصية، فيما يتعلق بحرية انتقال المعلومات وقد أقرت المنظمة بأن الخصوصية قيد عادل على عملية انتقال البيانات، وأصدرت الولايات الأمريكية المتحدة عام 1986م قانوناً لمعاقبة الهاكرز بالسجن، وهذا القانون لا يطال الأحداث، فقد قام روبرت. موريس وهو طالب متخرج من الجامعة، بإطلاق أول دودة ذات نسخ ذاتي، على نظام يونكس بغرض التحريك و الاختبار، وكان ذلك على شركة الحكومة الأمريكية ARPA NET ولكن فقد السيطرة على الدودة لتنتقل إلى حوالى 6000 كمبيوتر، على نفس الشبكة ليوضع روبرت تحت الملاحظة والمراقبة لمدة ثلاث سنوات وغرامة عشرة الآلاف دولار، أما أول قضية دولية من هذا الشأن، فكانت من نصيب ألمانيا الغربية عام 1989م بعد اتهام أربعة من الهاكرز الألمان باختراق أجهزة حكومية أمريكية وسرقة المصدر البرمجي لنظام التشغيل وبيعه للاتحاد السوفيتي، وقد برزت مجموعات من الهاكرز بعد ذلك، وبدأ التنافس بين تلك المجموعات في اختراق كافة أنواع أجهزة الحاسبات، ففي عام 1995م تم اعتقال أشهر هاكر في العالم. كيفن ميك ، حيثُ بقي

أربع سنوات دون محاكمة في السجن، وفى الوقت نفسه استطاع هاكرز من دولة روسيا سرقة عشرة ملايين دولار من سيتي بنك أكبر بنك تجاري في العالم (في الولايات المتحدة الأمريكية) كما شهدت الساحة الدولية أحكاماً بالسجن على مرتكي حملات الأعراف التي نجحت في تعطيل مواقع ياهو، وشهد عام 2000م اختراقات DNS التي استطاع من خلالها حجب موقع شركة ميلر مايكروسوفت عن ملايين المستخدمين لمدة يومين.(عبد النبي ، 1999م، ص20).

وشهد العالم ثورة تشريعية في مجال تأمين الخصوصية ومنع انتهاكها ففي أمريكا صدر قانون خصوصية الاتصالات الإلكترونية عام 1987م وفي ألمانيا صدر قانون حماية المعطيات 1977م، بالإضافة إلى قانون حماية البيانات الصادر عام 2000م، وفي فرنسا صدر قانون لمعالجة آلية المعطيات عام 1978م وجرت عليه عدة تعديلات، كما نجد أن الاتحاد الأوروبي منذ بداية التسعينات أخذ يصدر توجيهاته الملزمة لبلدان الاتحاد عند إصدارها لتشريعات الحماية المعلوماتية، والتي كان من بينها التوجيهات المتعلقة بالتجارة الالكترونية والتوقيع الالكتروني، وحماية المستهلك الكترونيًا ، وبلغ التعاون الدولي مداه حين أقبلت بلدان أوروبا على عقد اتفاقية موحدة لمواجهة جرائم الانترنت عام 2001م، والتي هدفت إلى حل إشكاليات الاختصاص القضائي والقانون الواجب التطبيق في شأن جرائم الأنترنت (حجازي، 2007م، ص8).

أما على مستوى الدول العربية فقد كان الحراك التشريعي جدا ضعيف وبطيء إلى حد كبير في مجال ضبط المعاملات الالكترونية وتأمين الفضاء السيبراني فقد كان المشرع التونسي سباق في هذا المجال، حيثُ أصدر قانون التجارة والمبادلات الالكترونية عام 2000م، والذي عالج فيه أحكام العقد والمعاملات الالكترونية، كما عالج الجرائم التي تقع ويكون موضوعها التجارة المذكورة، كما أصدرت إمارة دبي قانونها في نفس الشأن رقم 2 لعام 2002م، والذي يهدف إلى ضبط المعاملات الالكترونية والتوقيع الالكتروني والحماية القانونية، وبذلك تكون دولة تونس ودولة الامارات العربية المتحدة صاحبتا المبادرة الأولى في هذا المجال، حيثُ بادرت دولة الامارات العربية إلى وضع مشروع قانون اتحادي لمكافحة جرائم الكمبيوتر عقب صدور القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، ويعتبر هذا القانون استرشادي،

حيثُ وضع القواعد الأساسية التي يتعين على المشرع العربي اللجوء إليها عند سن قانون وطني يهدف إلى مواجهة أو مكافحة الجرائم الإلكترونية، سواء كان هذا القانون مستحدثًا أو تعديلاً لقانون العقوبات الساري المفعول فيها في أي دولة عربية ،وقد حدد هذا القانون جرائم الانترنت بشكلٍ عام، وحدد عقوباتها، وأعطى مساحة للمشرع الوطني في تحديد أركانها وتحديد الآثار الجنائية المترتبة عنها، وقد جاء هذا القانون كثمرة عمل بين وزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية، حيثُ قدم كل منهما مشروعًا في هذا الخصوص في عام 2003م، وتم اعتماد مشروع قانون مشترك وبعد اقراره لم يعد هناك أي عذر لأي مشرع عربي في التقاعس عن المبادرة بإصدار قانون يصب في نفس الاتجاه أيًا كان نصيب الدول من استعمال الحاسب الآلي، وعلى إثر ذلك صدر في مصر صدر قانون التوقيع الاليكتروني رقم 15 لسنة 2004م، والذي قرر فيه المشرع المصري الحماية الجنائية للتوقيع الالكتروني كما أصدر المشرع المصري القانون رقم 175 لسنة2018م للجرائم الالكترونية، وفي الأردن صدر قانون الجرائم الإلكترونية السنة 2002 وبدأت تطبيقه 2023/9/12م (أبو الليل، 2001م، ص 22).

الأمر الذي ترتب عليه عدم وجود أحكاماً جنائية قاطعة وفقا لأحكام هذا القانون، وفي المقابل لجأت بعض الدول العربية إلى إدخال بعض التعديلات على تشريعاتها الجنائية لمواجهة جرائم الأنترنت، وبتتبع التطور التشريعي في ليبيا عبر الزمن سنجد أن تشريعاتنا الجنائية الصادرة مذ 1951م جاءت خالية من أي إشارة ولو كانت عابرة لتقنين الجرائم الالكترونية حتى عام 2022م عندما صدر القانون رقم 5 بشأن الجرائم الالكترونية، على الرغم من معرفتها الأنترنت والتواصل الاجتماعي قبل ذلك بفترة لابأس بها، وعلى الرغم من تأخر الحركة التشريعية في ليبيا وتخلفها عن تجريم الاعتداءات الالكترونية وتأخرها عن القانون العربي النموذجي المذكور الذي أكد على الجريمة المعلوماتية تقع بكافة أنواعها، والتي تتدرج من جرائم غش الحاسب الآلي عن طريق اختراقه، وسرقة المعلومات المخزنة عليه أو اتلافها وتدميرها إلى جرائم أشد خطورة مثل التزوير الالكتروني وسرقة الأموال بوسائط الكترونية، والاتجار بالبشر وجرائم العرض، وجرائم الآثار وغيرها

من صور الاجرام المستحدث التي يمكن ارتكابها بواسطة الانترنت أن التشريع المذكور يبدو وكأنه جاء في عجالة، حيثُ أنه لم يتدارك ما تخلف عنه ولم يحتوي الموقف كما ينبغي حيث تناول في مادته الأولى تعريفات لبعض المصطلحات المتداولة في الفضاء الإلكتروني، والمتمثلة في تعريفه للجريمة الالكترونية: على أنها: (كل فعل يرتكب من خلال استخدام أنظمة الحاسب الآلي أو شبكة المعلومات الدولية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون) ما يمكن ملاحظته في هذا الشأن أن هذا القانون بتعريفه للجريمة الالكترونية يكون المشرع الجنائي قد اقتحم مجال يخرج عن دائرة اختصاصه فليس من وظيفته التعريف، بل اعتدنا على أنه يترك مجال التعريف بالمصطلحات للفقه وبذلك يكون المشرع وضع قيد على سلطة القضاء في تحديد مفهوم الجريمة الالكترونية خارج حدود تعريفه لها، وإن كان ذلك يصب في اتجاه مخالف للعدالة أو يساعد بعض الجناة على الإفلات من العقاب، كما أن تعريفه للجريمة الالكترونية جاء مبتور حيث حصرها في ارتكابها بالطريق الإيجابي أي عن طريق الفعل وأنكر ارتكابها بالامتناع أي سلباً، على الرغم من إمكانية تصور ذلك وعدم استحالته، أما عن باقي المصطلحات فلم يضبطها من الناحية القانونية كمصطلح الاختراق كان الأجدر أن يترك أمر تعريفه للفقه الجنائي، كما يمكن ملاحظة عدم انسجام أهدافه مع محتواه، فالأولى تلوح في أفق يبعد كثيرًا عن الأخيرة، وفي المادة الثالثة تناول حدود سريان هذا القانون حيثُ ركز على الفعل وأهمل الفاعل ولم يتعرض لجنسية مرتكبه، كما أنه قرر قاعدة مبدأ الأثر الفوري لنصوصه دون الإشارة إلى إمكانية تطبيق أحكامه بأثر رجعي إذا كان أصلح للمتهم والعكس بالعكس، وفي المادة الرابعة الاستخدام المشروع الوسائل التقنية وفي المادة الخامسة خصوصية المواقع الإلكترونية وفي المادة السادسة الأعمال الأدبية والفنية أو العلمية، وفي المادة السابعة مراقبة ما ينشر عبر وسائل التقنية الحديثة، وفى المادة الثامنة حجب المواقع الإباحية أو المخلة بالآداب العامة وفي المادة التاسعة حيازة وسائل التشفير وفي المادة العاشرة التأثير في النظام الإلكتروني وفي المادة الحادية عشر الدخول غير المشروع، وفي المادة الثانية عشر قرر العقوبات المترتبة على مخالفة أحكام المادة الحادية عشر. وفي المادة الثالثة عشره تناول الاعتراض والتعرض، ويلاحظ على المادة الثالثة عشر أن عنوانها غير

منسجم مع مضمونها حيثُ عُنونت بالاعتراض أو التعرض وعاقب كل من اعترض حيثُ يُفهم بأن العقوبة يستحقها كل من اعترض عن نظامًا معلوماتيًا لا من تعرض له أو اعترضه، ويستشف من ذلك سوء الصياغة وعدم الفلاح في انتقاء الألفاظ والمباني المعبرة عن المعاني ، والمادة الرابعة عشر تناول حيازة برامج في فك الترميز واستعمالها، وفي المادة الخامسة عشر تناول التعدي على عمل نظام معلوماتي للحصول على منفعة مادية وفي المادة السادسة عشر تعرض إلى التعدي على عمل نظام معلوماتي و استعمال مخرجاته، وفي المادة السابعة عشر الترويح السلع غير مرغوب فيها، وفى المادة الثامنة عشر تناول الاستلاء على أدوات التعريف والهوية واستخدامها، وفي المادة التاسعة عشر تناول إنتاج المواد الإباحية وترويجها والمادة العشرون تناولت التحريض على الدعارة، وفى المادة الواحد والعشرون تناول مزج أو تركيب الصوت والصور وفي المادة 22 تعرض لمضايقة الغير وفي المادة الثالثة والعشرون تعرض إلى استغلال القصر أو المعوقين نفسيا أو عقلياً في أعمال إباحية وفي المادة الرابعة والعشرون تناول التعدي على حقوق التأليف وفى المادة الخامسة والعشرون تقليد الأعمال الرقمية والبرامج التقنية وفي المادة السادسة والعشرون تناول بيع الأعمال الرقمية المقلدة وفي المادة السابعة والعشرون الإتجار في الآثار والتحف التاريخية، وفي المادة 29 تناول إثارة النعرات العنصرية أو الجهوية، وفي المادة 30 تناول التعدي على الأشخاص بسبب انتماءهم وفي المادة 31 تناول المقامرة وفى المادة 32 الترويج للخمور والمسكرات، وفي المادة 33 تناول الترويج المخدرات والمؤثرات العقلية وفى المادة 34 تناول تعطيل الأحكام الحكومية، وفي المادة 35 تناول الامتناع عن التبليغ، وفي المادة 36 تناول ائتلاف الأدلة القضائية الرقمية، وفي المادة 37 تناول تهديد الأمن أو السلامة العامة وفي المادة 38 تناول التحريض على القتل أو الانتحار، وفي المادة 39 تناول عقوبة حيازة وسائل التشفير واستعمالها، وتناول في المادة 40 إتلاف نتائج الفحوص الطبية، وتناول في المادة 41 الحصول على الخدمات التي تقدمها البطاقات الإلكترونية دون وجه حق وفي المادة 42 تناول الإساءة إلى المقدسات والشعائر الدينية وتناولت المادة 43 الإتجار بالأشخاص وتعرض في المادة 4 إلى غسل الأموال عبر مواقع التواصل الاجتماعي وتناولت المادة 45 مساعدة الجماعات الارهابية، وتعرضت المادة

46 إلى استخدام علامة تجارية مسجلة في الدولة، والمادة 48 تعرضت لمسؤولية الشخص المعنوي، والمادة 49 تبادل فيها تطبيق قانون والقوانين المكملة، وتناول في المادة 50 تبادل المصادرة وتناول إبعاد الأجنبي في المادة 51 وفي المادة 52 تناول مأموري الضبط القضائي في (الجريدة الرسمية لسنة 2023م العدد 1 السنة الأولى).

من خلال استعراض مواقف بعض التشريعات الجنائية بما في ذلك التشريع الجنائي الليبي اتضح أن التشريعات استخدمت سبل مختلفة لحماية الخصوصية والحيلولة دون اختراقها أو التعدي عليها كما لاحظنا تأخر المجتمعات العربية في سلوك طريق هذه الحماية ربما يكون ذلك مرهونا بتصنيفها من ضمن دول العالم والثالث بينما لدول الغربية فكانت السباقة لذلك بحكم طبيعة هذه المجتمعات وعلاقتها بالوسائل التقنية، باستقراء نصوص القانون المذكور يمكن الوصول إلى أن المشرع الجنائي الليبي ، تبنى سياسة عقابية جدا هشة وضعيفة ،لا تصلح لمواجهة التعدي الالكتروني ولا يمكن أن تحقق الأمن المعلوماتي المنشود، فعلى الصعيد الموضوعي ، مازال المشرع الجنائي الليبي في اتجاه تبني العقوبات السالبة للحرية على الرغم من أن الواقع العملي ، اثبت مساوئها وعدم فلاحها في تحقيق الردع العام والخاص ، كما أنها مناهضة لفكرة الاقتصاد الجنائي في جانب الجزاء حيثُ تساهم في إثقال كاهل الدولة بالنفقات على المحكوم عليهم ، فكان الأجدر به تبني عقوبات مالية رادعة خاصة على الأشخاص المعنوية ، حيثُ تساهم في إدخال إيرادات لخزانة الدولة وتحقق الردع الخاص والعام ، كما أنه جاء خاليًا من حكم الشروع في ارتكاب الجرائم المنصوص عليها ضمن أحكامه ، على الرغم من أن جانب من الفقه يرى أن عقوبة الشروع الواردة في القانون المذكور كانت ضعيفة ، كما أن أحكامه جاءت خالية من التفريد القضائي للعقوبات حيث جاءت العقوبات الواردة فيه محددة نوعا وكما ومقدارًا ، حيثُ جاءت في شكل حبس محدد المدة إجباريًا وغرامة محددة المقدار وسجن محدد المدة، ولم يقرر عقوبة الغرامة الرادعة لبعض الجنايات الخطيرة الواردة فيه، كجريمة الاتجار في الآثار والتحف التاريخية (المادة 27) من القانون المذكور والذي يكون غرض الجاني من ارتكابها الحصول على كسب مالي غير مشروع ، وكذلك لم يتعرض لجريمة إخفاء الأموال المتحصلة من الجرائم الالكترونية، ولم ينص على عقوبة حل الشخص

المعنوي إلا في حالة واحدة ،إذا كان الغرض من انشاءه ارتكاب الجرائم الإلكترونية المنصوص عليها ضمن أحكامه ،كما أنه جاء خاليًا من النص على الظروف التي تستوجب تشديد العقوبة التي تساهم بشكل فعال في تفريد العقوبة والتي تعتبر من أهم أدوات القضاء الجنائي في تقدير العقوبة، والتي أخذت بها العديد من التشريعات المقارنة (كالتشريع الأردني في المادة 14 من القانون رقم 27 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات و قانون جرائم المعلوماتية في السودان لسنة 2007م، والمادة 31 من المرسوم السلطاني رقم 11 لسنة 2011م بشأن مكافحة جرائم تقنية المعلومات في سلطنة عمان، وكذلك المادة 49 من القانون رقم 14 لسنة 2014م بشأن إصدار قانون مكافحة الجرائم الاليكترونية في قطر والقانون الفلسطيني رقم 10 بشأن الجرائم الالكترونية لسنة 2018 في مادته 28 و29)، فقد أغفل المشرع الجنائي الليبي وضع ظروف مشددة عامة للعقوبات المقررة في قانون الجرائم الالكترونية المذكور بالنظر إلى وصف الجر يمة أو محلها أو صفة الجاني وذلك على خلاف الوضع في التشريع المقارن الذي شدد العقوبات في المجال نفسة بالنظر إلى صفة مرتكبها أو لحساب أو لمصلحة من أُرتكبت كأن تكون ارتكبت لمصلحة دولة أجنبية أو أي جماعة معادية أو إرهابية، أو تنظيم غير مشروع كما في التشريع الإماراتي الذي أعتبر هذا النوع من الجرائم الالكترونية من جرائم أمن الدولة، كما جعلت ارتكاب الجرائم الالكترونية لمصلحة دولة أجنبية ظرفًا مشدداً بموجب أحكام المادة 60 من القانون الاتحادي رقم 34 لسنة 2021م بشأن مكافحة الشائعات والجرائم الالكترونية بدولة الامارات العربية وجعلت الجريمة المذكورة من جرائم أمن الدولة بموجب المادة 70 من القانون المذكور، كما أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م أكدت على وجوب تشديد العقوبات التقليدية الواردة في قوانين العقوبات الوطنية إذا ارتكبت بطريقة الكترونية وأكدت على ذلك أيضًا اتفاقية الاتحاد الأفريقي للأمن السيبراني وحماية البيانات الشخصية لعام 2014م، وعلى هذا النهج سارت العديد من التشريعات العربية كالتشريع الاماراتي ، و لم يتناول القانون الليبي المعني أحكام العود ، ولم يتصدى لفكرة المساهمة الجنائية ولم يحدد حكم الشريك ،كما قرر العقوبة نفسها الواردة في قانون العقوبات لأي جريمة تقليدية منصوص عليها فيه إذا ارتكبت بطريقة ذكية أو اليكترونية ،

وهذا توجه يتعارض والعدالة الجنائية الناجزة حيثُ ارتكابها في الوسط السيبراني سيكون بوسيلة أسهل ويدل على خطورة الجاني، ومن هنا كان الأجدر بالمشع الليبي تشديد العقوبة الذي قد يكون في حالات معينة أكثر خطورة من الفاعل الأصلي كالوسيط في جرائم الإتجار بالبشر، ولم يتصوره إلا في مسألة التحريض على الانتحار في حين إمكانية تصوره في كل صورة من صور الجرائم الواردة فيه، كما يؤخذ عليه أيضاً عدم اتباعه للسياسة الوقائية وعدم محاولته الحيلولة دون وقوع الجرائم التي يحتويها، فضلا عن ضرورة تشديده لمسؤولية الشخص المعنوي ، أما على الصعيد الإجرائي، فلم يبين المشرع الوسائل التي من الممكن إثبات الجرائم الواردة فيه بواسطتها، على الرغم من أنه تعرض إلى ضرورة المحافظة على الدليل، ومعاقبة كل من تسول له نفسه إتلافه، فلما كانت الجرائم الالكترونية غالبًا ما ترتكب من قبل صغار السن ومن الذين ليس لديهم سوابق جنائية ويكون في الغالب ارتكب الجريمة نتيجة استعراض قدراته الالكترونية، فكان الأجدر بالمشرع هنا أن يأخذ ذلك في الاعتبار وان يمنح القاضي السلطة التقديرية اللازمة كما في التشريع المقارن الذي وسع السلطة التقديرية للقاضي ، لتقدير العقوبة بالنظر إلى كل واقعة على حدى (الزوي، 2023،497)،هذا فيما يتعلق بجنح الجرائم الالكترونية، أما بالنسبة لجنايات الجرائم الالكترونية، يمكن ملاحظة أن المشرع الليبي في القانون المذكور يعاقب على كل الجنايات بالجمع بين السجن والغرامة، على الرغم من أن عقوبة الغرامة ليست من العقوبات الأصلية ولا التبعية في الجنايات(دبارة، عقوبة الغرامة ومدى إمكانية الحكم بها في أحوال الشروع في الجنايات ص214).

ولم يحدد المشرع الجنائي الليبي في القانون المعني حدود مسؤولية الشخص المعنوي عن الجرائم الالكترونية حيثُ لم يفصل في أحكام هذه المسؤولية ولم يميز بين الحالات التي ترتكب فيها الجرائم الواردة فيه باسم الشخص المعنوي وبصفته ، وبين الحالات التي يرتب أيضاً من لك الجرائم موظف من العاملين في المؤسسة الموصوفة بالشخص المعنوي باسمه الشخصي وصفته الشخصية، كما يمكن ملاحظة استبعاد المشرع لوصف المخالفات عن الجرائم الاليكترونية، في حين كان يفترض عدم استبعادها على أن تقرر لها عقوبة مالية تساهم في الاقتصاد في العقوبات الجنائية والحيلولة دون الاسراف في العقوبات السالبة للحرية، كما أنه أغفل النص على أي ظرف مخفف للعقوبة

أو يؤدي إلى الإعفاء منها ، على خلاف التشريع الاماراتي (المادة 61 من القانون أو المرسوم الاماراتي المذكور)، كما أغفل وجوب الحكم بمحو البيانات وإتلاف البرامج التي استخدمها الجاني إضراراً بالمجني عليه للحيلولة دون رجوعه إليها واستخدامها ضد المجني عليه مرة أخرى، حيث تعتبر من متحصلات الجريمة وبعض التشريعات المقارنة نصت على ذلك كما في المادة 38 من القانون رقم 7 لسنة 2006 بشأن الجرائم السيبرانية في موريتانيا(الزوي، 2022م، ص497).

كما كان ينبغي على المشرع الليبي أن يعطي الشروع في الجرائم الاليكترونية حكما خاصًا ؛بحيثُ يأخذ عقوبة الجريمة التامة، ولا يخفف العقاب كما هو وارد في المادة 59 من قانون العقوبات الليبي لخصوصيته في الفضاء المعلوماتي، كما يلاحظ إغفال المشرع الليبي عن تنظيم التدابير الوقائية في مجال الجرائم الاليكترونية على خلاف التشريع المقارن الذي قررها، كما في التشريع الإماراتي المذكور، في حين كان يتعين عليه تقريرها؛ لما لها من أهمية، فمن المتصور ارتكاب الجرائم الواردة فيه من قبل القصر أو الذين لا تتناسب العقوبات الجنائية مع أوضاعهم ، كما أن القانون المذكور جاء خالياً من أي إشارة لقواعد الإثبات التي يفترض أن تحكم الجرائم الواردة فيه.

الخاتمة

النتائج:

1- فرض التطور التكنولوجي ، ظهور العالم الافتراضي العالم الموازي للواقع الأمر الذي أدى إلى ظهور نوع آخر من الجرائم وانتهاك نوع آخر من الحقوق ،الأمر الذي يفرض ضمان الأمن السيبراني وحفظه من الانتهاكات والاختراقات ، لضمان نجاح المعاملات الالكترونية التي تتم من خلاله.

2- كما أن تعدد الجماعات البشرية، دعا إلى ضرورة وجود التشريعات الجنائية لحماية الحقوق والحريات أدت الثورة التقنية إلى ضرورة وجود أسوار جنائية متينة لتحقيق الحماية الإلكترونية الأمن المعلوماتي .

3- أثبت الواقع العملي أن الجرائم الإلكترونية أكثر خطورة من الجرائم العادية، الاختلاف طبيعة كل منهما عن الأخرى فالجرائم إلكترونية تنتهك حق غير ملموس ويمكن ارتكابها في برهة

زمنية جدا قصيرة فبكبسة زر يمكن سرقة موقع أو انتهاك خصوصية أو تشويه سمعة أو احتراق منظومة أو تهكير حساب.

4- الضرر الناشئ عن الجرائم الإلكترونية يستحيل جبره فهي جرائم سهلة الارتكاب وبالغة الخطورة.

5- أن قانون الجرائم الإلكترونية الليبي رقم 5 لسنة 2022، قانون معيب سواء من حيث الصياغة أو المبالغة في تشديد العقوبات الواردة فيه واغفاله للعديد من الاحكام العامة والخاصة من الناحية الموضوعية كعدم توسيع السلطة القضائية التقديرية في تقرير العقوبات وتعديل موقفه بشأن تشديد وتخفيف العقوبة والإعفاء منها كذلك حكم الشروع والشريك بالتسبيب والتفصيل في مسؤولية الشخص المعنوي وقواعد الإثبات أيضاً، والتي حرصت عليها التشريعات المقارنة الأمر الذي أدى إلى بروز مواطن الخلل والنقص فيه إلا أنه يبقى الإرهاصة الأولى لمواجهة عواصف الانتهاكات التي انتابت عالم الاتصالات الإلكترونية عبر مواقع التواصل الاجتماعي ولا ضير في ذلك من الناحية النظرية ولكن الواقع العملي يوجب خلاف ذلك.

التوصيات

1- كما جاء قانون الجرائم الاليكترونية ،مواكبًا للتطور التقني يجب على السلطة التشريعية تنقيحه وإعادة النظر فيه والتركيز على الأحكام الموضوعية التي أغفلها كالسلطة التقديرية للقاضي الجنائي وضرورة التوسع فيها ,ضرورة إعادة النظر في أحكام الشروع ، وتشديد وتخفيف العقوبات المترتبة على الجرائم الواردة فيه وإعادة النظر في أحكام المساهمة الجنائية، والتفصيل في مسؤولية الشخص المعنوي، و ذلك من خلال الاسترشاد بالقانون العربي النموذجي لمكافحة الجرائم الكمبيوتر والانترنت، وكذلك بالتوجيهات الدولية الواردة في نفس النطاق وبالتشريعات العربية المقارنة التي تجاوزت العيوب المنطوي عليها وكذلك إعادة النظر في الإثبات الجنائي وتطويره بما يتماشى مع طبيعة الجرائم الإلكترونية وطبيعتها.

2- إعادة النظر في القانون رقم 5 لسنة 2020م بشأن الجرائم الإلكترونية ليس لأنه يقيد حرية التعبير، لأن الحرية يجب ان لا تكون مطلقة حتى في القضاء الإلكتروني لابد من تقييدها تشريعياً ويجب أن يفهم كل فرد من أفراد المجتمع أن حريته تنتهي عند بداية حرية الآخرين.

3- عدم الاعتماد على التشريع فحسب لتحقيق، الأمن المعلوماتي لأن الإسراف في التحريم كعدمه بل لابد من تبني سياسات وقائية للحيلولة دون وقوع هذا النوع من الجرائم التي تنتهك الخصوصية وذلك بالاعتماد على الوسائل الفنية والتكنلوجية الموجودة في أجهزة ووسائل التواصل الإلكتروني.

4) فيما يتعلق بحماية الأشخاص المعنوية كالمصارف ومنظومة الرقم الوطني أو السجل العقاري أو المدني وغيره لابد من تأهيل القائمين عليها للإلمام بالتعامل معها وحماية المعلومات الحساسة من أي ضرر قد يقع عليها وقد يكلف المجتمع ثمناً باهظاً.

قائمة المراجع

أولاً : الكتب

1- داود حسن الطاهر، جرائم نظم المعلومات ،الرياض، أكاديمية نايف العربية للعلوم الأمنية، سنة 2002م.

2- طه ياسين عبد النبي، الأمن الإلكتروني، العراق، سنة 1999م.

3- عز الدين أحمد جلال، أساليب التعاون العربي في محال التخطيط لمواجهة جرائم الانترنت، الرياض، أكاديمية نايف العربية " للعلوم الجنائية، سنة 2002م.

4- على عبد القادر قهوجى، الجرائم المتعلقة باستخدام البطاقات الممغنطة، مصر/ القاهرة، سنة 2000م.

5- محمد عادل ريان، جرائم الحاسب الآلي وآلية البيانات ،دار الثقافة العربية ،الأردن، سنة 2002م.

6- ممدوح محمد الجهيني، التبادل الإلكتروني للبيانات EDI ،دار الفكر الجامعي الإسكندرية.

7- ممدوح و منير محمد الجهني، دار الفكر الجامعي الإسكندرية، سنة 2000م.

8- ممدوح الجهيني ، التعاون الدولي في حماية حقوق الملكية الفكرية، منشورات دار النهضة العربية، مصر، سنة 2001م.

9- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي دراسة قانونية معمقة في القانون المعلوماتي، دار الكتب القانونية، مصر، سنة 2007م.

ثانياً/ الرسائل والأطروحات العلمية:

1- عبدالرحمن محمد السويلم ،المساهمة في الجريمة المعلوماتية في النظام السعودي ، دراسة مقارنة بالقانون الأردني، رسالة ماجستير، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الامنية، الرياض/السعودية.

ثالثاً/ البحوث والمقالات المنشورة:

1- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت ، بحث منشور لدى مركز المنشاوي للدراسات والبحوث ، سنة **2007**م.

2- مصطفى مصباح دبارة، عقوبة الغرامة ومدى إمكانية الحكم بها في أحوال الشروع في الجنايات، بحث منشور في مجلة الدراسات القانونية، جامعة بنغازي ، المجموعة 15 ،السنة 16، سنة 1998م.

3- ما شاء الله عثمان علي الزوي، السياسة العقابية للمشرع الليبي في قانون مكافحة الجرائم الالكترونية رقم 5 لسنة 2022م دراسة مقارنة مع التشريعين المصري والاماراتي، بحث منشور في مجلة كلية القانون الكويتية العالمية، السنة الحادية عشر العدد الرابع سبتمبر 2023م.

4- نبيلة صدراني ، السلطة التقديرية للقاضي الجزائي في إيقاف وتنفيذ العقوبة ، بحث منشور في مجلة العلوم الإنسانية، جامعة محمد خيضر ،بسكرة ، الجزائر، المجموعة 28، العدد الرابع، ديسمبر 2017م.

5- إبراهيم الدسوقي أبو الليل، الجوانب القانونية عبر وسائل الاتصال الحديثة، بحث مقدم الى مؤتمر القانون والكمبيوتر والانترنت، جامعة الامارات، سنة 2001م.

رابعاً/ التشريعات:

1- القانون رقم (5) لسنة 2020م بشأن الجرائم الإلكترونية.

2- قانون الجرائم المصري رقم 175 لسنة 2018م بشأن الجرائم الالكترونية.

3- القانون المصري رقم 15 لسنة 2004م بشأن الحماية الجنائية للتوقيع الالكتروني.

4- القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لسنة 2003 م.

5- قانون الجرائم الإلكترونية الأردني لسنة 2002 والقانون الاردني رقم 27 لسنة 2015م بشأن مكافحة جرائم تقنية المعلومات.

6- القانون الفرنسي لمعالجة آلية المعطيات، لسنة 1978م.

7- القانون رقم 7 لسنة 2006م، بشأن الجرائم السيبرانية في موريتانيا

8- القانون رقم 14لسنة 2014م بشأن مكافحة الجرائم الالكترونية في قطر

9- الاتفاقية الأوروبية الموحد لسنة 2001م لمواجهة جرائم الأنترنت

10-قانون الجرائم الالكترونية الفلسطيني رقم 10 لسنة 2018م.

11-قانون الجرائم المعلوماتية السوداني لسنة 2007م.

12-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، لسنة 2010م.

13-اتفاقية الاتحاد الافريقي للأمن السيبراني، وحماية البيانات الشخصية، سنة 2014م.

14-قانون خصوصية الاتصالات الالكترونية الأميركي، سنة 1987م.

خامساً/ الوثائق:

1- موسوعة القانون وتقنية المعلومات – الخصوصية وحماية البيانات في العصر الرقمي من مستورات اتحاد المصارف العربية 2002م.

2- إصدارات الامم المتحدة، الجمعية العامة لجنة الأمم المتحدة للقانون – الدورة الثالثة والثلاثون – نيويورك 2000م.

3- تقرير the Electronic Privacy Information Center للأعوام من 1998 – 2000 المنشور على الموقع: http://www.privacxinternational.org/

2014