مجلة العلوم الاقتصادية والإدارية والقانونية
العدد الثاني ـ المجلد الثالث
فبراير 2019م
ISSN: 2522- 3372

المجلة العربية للعلوم و نشر الأبحاث
Arab Journal of Sciences & Research Publishing
AJSRP

الجريمة الإلكترونية في سلطنة عمان: التحديات والحلول القانونية

عبد الله بن علي بن سالم الشبلي
كلية القانون || جامعة صحار || سلطنة عمان

الملخص: هدف البحث إلى تحديد مفهوم الجريمة الإلكترونية وخصائصها، ودور التشريع العماني في إيجاد الحلول المناسبة لها؛ ومن أجل تحقيق هدف البحث الرئيس؛ فقد تم استخدام المنهج القانوني الوصفي. وتوصل البحث إلى أن المشرّع العماني استطاع مواكبة التقدم الحضاري من خلال تطوير القوانين التي تكافح الجرائم بصورة عامة، والجرائم الإلكترونية وتقنية المعلومات على وجه الخصوص من خلال منظومة قانونية متكاملة؛ إذ تتراوح تلك العقوبات بين الغرامة المالية والعقوبات السالبة للحرية. وتوصل البحث إلى جملة من التوصيات منها: أهمية القيام بدراسات معتمدة على المسوح الميدانية تتناول أنواع الجرائم الإلكترونية المرتكبة، وأعداد مرتكبيها، ودوافعهم الإجرامية، وجنسياتهم، وفئاتهم العمرية؛ من أجل تطوير القوانين المعمول بها حالياً في سلطنة عمان لتتواكب من القوانين العالمية الحديثة في ذات المجال، وتوعية المجتمع بخطورة الجرائم الإلكترونية، وأساليب ارتكابها، وتأثيرها الأخلاقي على الفرد والمجتمع، وطرق الوقاية منها.

الكلمات المفتاحية: الجريمة الإلكترونية، المشرع العماني.

المقدمة:

وفرت السهولة النسبية للبشرية في العالم المعاصر استخدام الإنترنت في مختلف المجالات، والحصول عليه على نحو متزايد وبأسعار معقولة، والحصول على أجهزة الحاسوب على اختلافها مع أجهزة المودم فائقة السرعة والمزودة للأنترنت؛ إذ أدى ذلك إلى إتاحة التواصل بين بني البشر في مختلف أنحاء العالم، إلى جانب توظيف هذه الشبكة في المجالات التجارية والتعليمية والصحية والترفيهية وفي مجال المال والأعمال، وغيرها من مجالات الحياة الإنسانية.

وبالمقابل فإن هناك من حاول الإفادة من هذا التطور المذهل في مجال التقانة والانتشار الواسع لشبكة المعلومات العالمية (الانترنت)؛ إلى ارتكاب الكثير من الجرائم التي تستخدم فيها وسائل التقانة الحديثة، والتي لم تكن معروفة من ذي قبل، والتي سميت فيما بعد بالجرائم الإلكترونية أو جرائم تقنية المعلومات؛ وذلك من خلال استغلال الجماعات الإجرامية المنظمة ما أتاحه العصر الجديد من إمكانات، وما وفره من أساليب ووسائل، وأجهزة وأدوات، لاستحداث الجرائم الإلكترونية المنظمة، والعابرة للحدود؛ فقد اتخذت أشكالاً عدة كان من بين أخطرها تنامي الإجرام الإلكتروني؛ الأمر الذي تسبب في بروز العديد من الأشكال الجديدة من الإجرام الإلكتروني كالاحتيال والغش، والتزييف، والسطو على الحسابات المصرفية، وغيرها من صور الجرائم ذات الطابع الإلكتروني، وهذا بدوره أدى إلى نشوء محاولات نشطة للبحث عن الوسائل والأساليب الكفيلة للحد من تلك الخروقات والاعتداءات من مختلف دول العالم بصورة عامة وسلطنة عمان على وجه الخصوص؛ حيث سعت سلطنة عمان إلى تطوير قوانينها كسائر دول العالم لتتواكب مع تلك التطورات التقنية، وما أفرزته من جرائم إلكترونية حديثة.

مشكلة البحث:

تتحدد مشكلة البحث الحالي في التساؤل الآتي: ما واقع الجريمة الإلكترونية في سلطنة عمان، والسبل الكفيلة لمعالجتها؟ من أجل معرفة واقع الجرائم الناشئة عن استخدام التقانة الإلكترونية، ومدى الحاجة إلى

تطويرها من عدمه. ومما يؤكد وجود هذه المشكلة البحثية ما أشار إليه الغافري (2010) في دراسته إلى أن سلطنة عمان تحاول جاهدة مواجهة الاستعمالات السيئة لشبكة الإنترنت، وما ينجم عنها من أضرار سواء بالنسبة للمجتمع أو الأفراد.

أسئلة البحث:

تتبلور أسئلة البحث الحالي في السؤال الرئيس الآتي: ما واقع الجريمة الإلكترونية في سلطنة عمان، والسبل الكفيلة لمعالجتها؟ ويتفرع عن هذا السؤال الأسئلة الفرعية الآتية:

1- ما تعريف الجرائم الإلكترونية من الناحية القانونية كما يراها المشرع العماني؟
2- ما هي خصائص الجريمة الإلكترونية؟
3- ما أنواع الجرائم الإلكترونية؟
4- ما هي الإجراءات القانونية التي اتخذتها سلطنة عمان من أجل مكافحة الجرائم الإلكترونية بغية القضاء عليها أو التحفيف من انتشارها؟

فرضيات البحث:

يمكن تحديد فرضيات البحث الحالي في الآتي:

1- عدم وجود تعريف قانوني يحدد مفهوم الجرائم الإلكترونية في التشريع العماني.
2- لا توجد تشريعات قانونية خاصة تعاقب مرتكب الجريمة الإلكترونية في سلطنة عمان.

أهداف البحث:

تتحدد أهداف البحث في الهدف الرئيس للبحث هو الوقوف على مدى كفاية النصوص القانونية التي تتصدى للجرائم الإلكترونية بسلطنة عمان، ويتفرع عن هذا الهدف الأهداف الفرعية الآتية:

1- تعريف الجرائم الإلكترونية من الناحية القانونية.
2- توضيح خصائص الجريمة الإلكترونية.
3- تحديد أنواع الجرائم الإلكترونية.
4- بيان الإجراءات القانونية التي اتخذتها سلطنة عمان من أجل مكافحة الجرائم الإلكترونية بغية القضاء عليها أو التحفيف من انتشارها.

أهمية البحث:

تكمن أهمية هذا البحث من خلال تسليط الضوء على دور المشرِّع العماني في مواكبة قوانينه لمكافحة الجرائم الإلكترونية على اختلاف أشكالها؛ باعتبارها أحد إفرازات التقانة الحديثة نتيجة لسوء استخدامها من قبل ذوي الميول الاجرامية، إلى جانب توضيح دور المشرِّع القانوني العماني من أجل التصدي لهذا النوع من الجرائم من أجل الحد منها أو القضاء عليها.

منهج البحث:

على الرغم من اتسام الجرائم الإلكترونية بالعمومية من ناحية، ووجود بحوث ودراسات تناولتها بالدراسة، والتحليل من ناحية أخرى؛ فقد اعتمد البحث الحالي على المنهج القانوني الوصفي القائم على وصف المشكلة؛ بهدف

معرفة أسبابها، والعوامل التي أفضت إليها؛ وصولاً إلى معرفة حلولها؛ وذلك من خلال تحليل آراء فقاء القانون حول الجرائم الإلكترونية بصورة عامة، وما توصل إليه المشرِّع العماني وطبقته المحاكم في أحكامها على وجه الخصوص.

حدود البحث:

- الحدود الموضوعية: نظراً لتنوع الوسائل والأساليب المستخدمة في مجال الجرائم الإلكترونية، اقتصر البحث الحالي على الجرائم الناشئة نتيجة الاستخدام الجرمي لشبكة المعلومات العالمية (الانترنت) بصفة عامة دون الخوض في جرائم معينة بذاتها، أو التعرض لأركانها، لعدم القدرة على استيعابها في هذا البحث؛ مع توضيح دور المشرِّع القانوني العماني من أجل التصدي لهذا النوع من الجرائم بغية القضاء عليها، ومكافحتها للحيلولة دون انتشارها على نطاق واسع.
- الحدود المكانية: سوف يتم تناول الموضوع في حدود سلطنة عمان.
- الحدود الزمانية: سيقوم الباحث بدراسة الموضوع في إطار زمني يتناسب مع التشريعات القانونية ذات العلاقة بالجريمة الإلكترونية، والمعمول بها في سلطنة عمان.

الخطة، وهيكل البحث:

المبحث الأول: مفهوم جريمة الإلكترونية، وأنواعها.

المطلب الأول: مفهوم جريمة الإلكترونية.

المطلب الثاني: أنواع الجرائم الإلكترونية.

المطلب الثالث: خصائص الجرائم الإلكترونية، وسماتها.

المبحث الثاني: موقف المشرِّع العماني من الجرائم الإلكترونية، وكيفية علاجها.

المطلب الأول: موقف المشرِّع العماني من الجرائم الإلكترونية.

المطلب الثاني: تدرج المشرع العماني في العقوبة المتعلقة بالجريمة الإلكترونية.

المطلب الثالث: دور قانون جرائم تقنية المعلومات في مكافحة أنواع الجرائم الإلكترونية في سلطنة عمان.

المبحث الأول: مفهوم جريمة الإلكترونية، وأنواعها.

المطلب الأول: مفهوم جريمة الإلكترونية:

تعددت آراء فقهاء القانون حول تعريف الجريمة الإلكترونية تماماً كتعدد مسمياتها، فمنهم من يسميها "الجريمة الإلكترونية" ومنهم من يطلق عليها "الجريمة المعلوماتية" فيما ذهب فريق ثالث إلى تسميتها بـ "الجرائم السيبرانية"، ويتفق أغلب الباحثين على عدم توصل التشريعات الوطنية، والمؤسسات القانونية في العالم المعاصر لتعريف موحد للجريمة الإلكترونية؛ حيث تبنَّى كل رأي من المشرِّعين القانونيين تعريفاً خاصاً به بالنظر إلى الزاوية التي رآها، فقد جاءت بعض التعريفات من زاوية فنية، وأخرى قانونية ، وفريق ثالث يعرفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استناداً إلى معايير أخرى حسب القائلين بها، وهذا ما حدا بالأمم المتحدة إلى عدم التوصل لتعريف متفق عليه دولياً (حجازي، 2009).

وعرفت منظمة التعاون الاقتصادي والتنمية (OECD) كما ورد لدى الملط (2006: 87) الجريمة الإلكترونية بأنها: كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية.

كما عرَّف الشوا (1994: 7) الجرائم الإلكترونية بأنها: تلك الأفعال الإجرامية الناتجة من خلال أو بواسطة استخدام الشبكة المعلوماتية، والتقنية الحديثة المتمثلة في الكمبيوتر والمعالجة الآلية للبيانات، أو بنقلها.

وعرَّفها مصطفى، وآخرين (2011) بأنها: كل فعل ضار بالآخرين عبر استعمال الوسائط الإلكترونية مثل الحواسيب، وأجهزة الموبايل، وشبكات الاتصالات الهاتفية، وشبكات نقل المعلومات، وشبكة الانترنت أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموماً.

وعلى الرغم من صعوبة وضع تعريف محدد لظاهرة هذه الجريمة وحصرها في مجال ضيق، فإن البعض يعرفها على أنها " أي نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي"(البشري، 2000).

وبالمقابل فهناك من القانونيين لا يرون في التعريف السابق تعريفاً للجريمة الإلكترونية بقدر ما هو بيان للأسلوب الذي ترتكب به أو المحل الذي تقع عليه. وتتكون الجريمة الإلكترونية أو الافتراضية (Cyber Crime) من مقطعين هما الجريمة (Crime) والإلكترونية (Cyber). ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب الآلي أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية هي "المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت وغرف الدردشة، والبريد الإلكتروني (البداينة، 2014).

إن الجرائم الإلكترونية أصبحت أكثر تنظيماً؛ فظهر هناك ما يسمى بمصطلح "الجريمة المنظمة "إلى جماعات ترتكب أفعالا تخترق بها القانون للحصول على مساعدات مادية، كما تهتم بالابتزاز والخداع والإنتاج والتوزيع غير القانوني لإدمان المخدرات، والتعامل غير القانوني مع السلع الممنوعة مثل الأسلحة (تامي، 2015: 87).

وأكد ديش (2017) على أن التقدم التكنولوجي، وتكنولوجيا المعلومات والاتصالات أصبحت تأخذ حيزاً مهماً في التعاملات اليومية، وأصبح الكمبيوتر هو محور كل التعاملات بالنسبة للأشخاص، المؤسسات، الشركات ومختلف الإدارات. فقد اتسعت في الآونة الأخيرة دائرة استخدام الشبكات الإلكترونية للمعلومات، كوسيلة اتصال دولية في شتى مجالات الحياة، لتحقيق ما تصبو إليه الإنسانية من السرعة في إنجاز المشاريع، اختصار الوقت والمسافات وحتى الجهد البدني والذهني، وأضحت هذه الشبكات تحوي معلومات غير محصورة في مجال محدد، بل تتعلق بكافة ميادين الحياة الاجتماعية، الاقتصادية، العلمية وغيرها. إلا أن الاستخدام المتزايد لهذه الأنظمة المعلوماتية أدى إلى الكثير من المخاطر وأفرز أنواعاً من الجرائم، أصبح بما يعرف الجرائم الإلكترونية. لذا فإن من الصعوبة تحديد تعريفها في مجال واحد.

أما في سلطنة عمان فقد تم تحديد تعريف الجريمة الإلكترونية بصورة واضحة من خلال إصدار قانون مكافحة جرائم تقنية المعلومات رقم (2011/12)، ففي الفقرة (ب) من المادة الأولى منه حدد مفهوم تقنية المعلومات؛ إذ نصت الفقرة على تعريف تقنية المعلومات بأنها " الاستخدام العلمي للحوسبة، والإلكترونيات، والاتصالات لمعالجة، وتوزيع البيانات، والمعلومات بصيغها المختلفة". كما أشار المشرع العماني في الفقرة (ج) من ذات المادة على أن " جرائم تقنية المعلومات: الجرائم المنصوص عليها في هذا القانون".

لذا فإن المشرع العماني من خلال القانون – آنف الذكر – أكد على أهميته هذا القانون، وتماسه مع العديد مع التشريعات، وهو ما يتضح عند تصفح فصوله السبعة، والتي عالج الفصل الأول منها التعريفات والأحكام العامة، أما الثاني من القانون فتعلق بموضوع التعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية والنظم المعلوماتية، بينما اختص الفصل الثالث منه بموضوع إساءة استخدام وسائل تقنية المعلومات، وجاء

الفصل الرابع ليجرم التزوير والاحتيال المعلوماتي، أعقبه الفصل الخامس والذي خصص للجرائم الخاصة بالمحتوى، في حين أفرد الفصل السادس من القانون لموضوع التعدي على البطاقات المالية، وفي النهاية خصص الفصل السابع من القانون لبيان الأحكام الختامية.

وإجمالاً يمكن القول أن جوهر الجريمة الإلكترونية أبعد من تلك الأوصاف سالفة الذكر، ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية".

المطلب الثاني: أنواع الجرائم الإلكترونية:

إن للجرائم الإلكترونية أنواعاً كثيرة؛ لا يمكن حصرها؛ إذ لم يوضع لها معايير محددة من أجل تصنيفها بصورة قاطعة، وهذا راجع إلى التطور المستمر لشبكة المعلومات العالمية، والخدمات التي تقدمها .وقد تضاربت آراء فقهاء القانون من أجل تحديد أنواع جرائم الانترنت، وتعددت التصنيفات؛ فهناك من عدَّدها بحسب موضوع الجريمة، وأخر قسمها بحسب طريقة ارتكابها.

ونتيجة لذلك الاختلاف القانوني بين فقهاء القانون حول العالم إلا أن هناك محاولات مستمرة من أجل تقسيمها بصورة إجرائية؛ ويمكن تقسيم الجريمة الإلكترونية في جانبها القانوني إلى نوعين (الدريبي، 2013)، و(الملط، 2006):

أولاً: الجرائم التي تستعمل فيها الوسائل التكنولوجية من أجل القيام بالفعل الإجرامي مثل: تزوير الأموال عن طريق الماسح الضوئي فهذا النوع له إطاره القانوني في معظم التشريعات العالمية.

ثانياً: الجرائم التي تستخدم التقانة الحديثة لارتكابها؛ وذلك عن طريق شبكة الانترنت كإنشاء مواقع إباحية، أو الانضمام إلى مجموعات إرهابية، أو المتاجرة بالسلاح أو المخدرات، أو المتاجرة بأسرار الناس عن طريق اختراق مواقعهم، أو أجهزة الكمبيوتر الشخصية، أو انتحال الشخصية باستخدام بطاقات الائتمان.

وهناك من فقهاء القانون من حاول تصنيف الجرائم الإلكترونية بحسب علاقتها بالجرائم التقليدية إلى خمسة أنواع أساسية (Smith, Urbas, and Grabosky, 2004):

الأول: يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال شبكة المعلومات العالمية.

الثاني: دعم الأنشطة الإجرامية: ويتعلق الأمر بما تلعبه الشبكة من دور في دعم جرائم غسيل الأموال، والمخدرات، والاتجار بالأسلحة، واستعمال الشبكة كسوق للترويج غير المشروع في المجالات غير المشروعة.

الثالث: جرائم الدخول في نظام المعالجة الآلية للمعطيات: وتقع الجريمة على البيانات والمعلومات المكونة للحاسوب، وتغييرها أو تعديلها، أو حذفها مما يغير مجرى عمل الحاسوب.

الرابع: جرائم الاتصال: وتشمل كل ما يرتبط بشبكات الهاتف، وما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الإنترنت.

الخامس: الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية: ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها بأي صورة طبقاً لقانون حماية الملكية الفكرية.

كما تم توظيف، واستغلال وسائل التواصل الاجتماعي المختلفة من قبل الجماعات الارهابية في ارتكاب مختلف الجرائم الإلكترونية على مستوى دول العالم؛ مما حدا بتلك الدول إلى استحداث قوانين تلزم مستخدمي تلك المواقع بضرورة الالتزام بها (Levinson, 2013:167).

وهناك من حصر الجرائم الإلكترونية في أربع قضايا وهي: الغش عبر الإنترنت، والسرقة، والقرصنة الإلكترونية، والجنس الجنائي(Sattar J. Aboud, 2011).

ويؤكد القحطاني (2016) على أهمية وضع استراتيجية شاملة لمكافحة الجريمة الإلكترونية في الدول الخليجية، وللوصول إلى هذه النتيجة بشكل منطقي وسليم، كما أن من الأهمية بمكان تحديد الأوجه المعاصرة التي أحاطت بالجرائم الإلكترونية، والتحديات التي تلقيها على الهيئات التشريعية والقضائية والتنفيذية في كافة جوانب الحياة، وخاصة المشكلات العملية التي تواجه هذه الأجهزة والسلطات، انطلاقاً من مبدأ المشروعية والتهديد الذي يحيق به جراء هذه الجرائم، فعناصر الجريمة مختلفة، ومتجددة، فهي غامضة أحياناً، وافتراضية غالباً، ولذلك فإن وجود النصوص المعاصرة التي تعالج هذه الأفعال المجَرَّمة أمر على غاية من الأهمية، ووجود الأجهزة القضائية والتنفيذية القادرة على التعامل مع هذه النصوص أمر لا يقل أهمية.

إن من بين أخطر الجرائم التي ترتكب باستخدام التقانة الحديثة ووسائل الاتصال المختلفة تلك المتعلقة باستخدام مواقع التواصل الاجتماعي التي غزت الأسر والبيوت، ولم تترك للخصوصية مكاناً، حتى وصلت إلى درجة يمكن من خلالها تهديد الأمن القومي، مما يوجب وضع القواعد القانونية التي تنظمها وتضبطها؛ بحيث توجد التوازن بين الحفاظ على حق الفرد بالتعبير عن نفسه وحماية خصوصيته، وبين حق المجتمع.

وسلطنة عمان كغيرها من دول العالم لم تسلم من الجرائم الإلكترونية بأنواعها المختلفة، ولعل جريمة الابتزاز الإلكتروني من بين الجرائم الأكثر ارتكاباً. كما أن من أنواع الجرائم الإلكترونية اختراق الحسابات المصرفية، وسرقة بياناتها، والعبث بها. وبحسب إحصاءات المركز الوطني للسلامة المعلوماتية رقم (12 /2014) تبيّن وقوع (80) ألف محاولة اختراق إلكتروني، و(2000) حالة أمنية معلوماتية، و(8) آلاف محاولة لنشر فيروسات إلكترونية خبيثة.

لذا فقد حرصت سلطنة عمان على تطوير قوانينها في مجال الجريمة الإلكترونية بما يكفل حفظ حقوق مستخدمي تلك الوسائل التقنية، وبالمقابل ردع كل من تسول له نفسه العبث بالأمن باستخدام تلك الوسائل الإلكترونية، وتوظيفها بصورة سيئة.

المطلب الثالث: خصائص الجرائم الإلكترونية، وسماتها:

تتميز الجرائم الإلكترونية التقليدية منها، والمستحدثة بخصائص معينة تنفرد بها عن غيرها من الجرائم وهي (عيد، 1419)، و(الجنبيهي، والجنبيهي، 2004: 13- 15)، و(www.arablaw.ne):

الأولى: الحاسب الآلي هو أداة ارتكاب الجريمة الإلكترونية: هذه الخاصية ليست مقتصرة على الجرائم المتعلقة بشبكة الإنترنت؛ فقد يكون الحاسب الآلي أداة لارتكاب هذا النوع من الجرائم فهو أيضاً أداة لارتكاب العديد من الجرائم المعلوماتية؛ كالتزوير المعلوماتي، وسرقة المعلومات المخزنة بالحاسب الآلي وغيرها، أضف إلى ذلك فإن ارتكاب جرائم الإنترنت لا تتم في جميع الأحوال بواسطة الحاسب الآلي فقط، وإنما قد تتم بواسطة أجهزة الهاتف النقال خاصة وأن الولوج إلى شبكة الإنترنت من الممكن أن يتم بواسطة هذه الهواتف المطورة، والأجهزة اللوحية.

الثانية: تُرتكب بواسطة شبكة الإنترنت: جرائم الإنترنت من الجرائم الحديثة التي تستخدم فيها شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها، وتعد شبكة الإنترنت حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم؛ كالبنوك والشركات بكافة أنواعها والأشخاص وغيرها، والتي غالباً ما تكون الضحية.

الثالثة: مرتكب الجريمة ذو خبرة في الحاسب الآلي والإنترنت: إن الخبرة الكبيرة والدراية الفائقة بكل ما يتعلق بالحاسب الآلي وشبكة الإنترنت هي ما تميز مرتكب الجريمة المعلوماتية بشكل عام، ولا يقتصر الأمر على جرائم الإنترنت فهذه الخاصية مشتركة بين جميع الجرائم المعلوماتية ومن بينها جرائم الإنترنت.

الرابعة: لا حدود جغرافية أو زمنية لها: إن أهم ما يميز شبكة الإنترنت عالميتها، وكونها تربط بين الدول فلا تحدها حدود الطبيعة أو حدود السياسة، وتسمح لمستخدميها بالتنقل المعنوي أو الافتراضي بين الدول والقارات بدون تعقيدات أو صعوبات أو عوائق؛ فهي عالم ضخم متنوع متجدد خالي من الحدود والعوائق.

الخامسة: تتسم بالخطورة البالغة: فالجرائم المتعلقة بشبكة الإنترنت تتسم بالخطورة البالغة من عدة نواحي: فمن ناحية أولى يلاحظ أن الخسائر الناجمة عنها كبيرة جداً قياساً بالجرائم التقليدية خاصة جرائم الأموال، ومن ناحية ثانية فإنها ترتكب من فئات متعددة تجعل من التنبؤ بالمشتبه فيه أمراً صعباً. ومن ناحية ثالثة تنطوي على سلوكيات غير مألوفة؛ وهذا ما حدا بمكتب التحقيقات الفيدرالية الأمريكي "FBI" أن يطلق عليها وصف الوباء " Epidemic.

السادسة: صعوبة التحقيق والتحري والمقاضاة: إن جرائم الإنترنت تتسم بالغموض حيث يصعب إثباتها فالتحري عنها والتحقيق فيها، والمقاضاة في نطاقها ينطوي على العديد من المشكلات والتحديات الإدارية والقانونية، والتي تتصل ابتداءً من عملية ملاحقة الجناة، فإن تحققت مكنت الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة، أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم. وكون هذه الجرائم لا تحدها حدود وتعد من الجرائم العابرة للحدود فهذا بحد ذاته يثير تحديات ومعوقات في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق، والملاحقة والضبط والتفتيش، وبالتالي فإن الوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى، هذا من ناحية وضرورة تكاتف جميع دول العالم في مكافحتها من ناحية أخرى (Barbara,2000).

ويؤكد بونعارة (2016) على أن الجريمة الإلكترونية، من بين الجرائم التي استحضرتها الممارسة السيئة لثورة التكنولوجيا المعلوماتية، تختلف كثيراً عن الجريمة التقليدية، في طبيعتها، ومضمونها، ونطاقها، وتأثيراتها، وأنواعها، ووسائلها وأدواتها، وحتى في خصوصية وتميز مرتكبيها، وقد ساهمت عوامل التحضر السريع، والرغبة بتحقيق الثراء، وتوافر الفرص لارتكابها في انتشارها، وارتفاع نسبة ضحاياها، خاصة مع قصور وسائل الرقابة، وضعف التشريعات القانونية، وفرض العقوبات لتحجيم تأثيرات هذا النوع من الجرائم المستحدثة، التي تستهدف الأفراد والبيانات والدول، وترهق كاهلها بالخسائر الفادحة في مختلف قطاعات الحياة، فهي تمثل حقيقة "الاستعمار الإلكتروني" في أبشع صوره.

إن الجرائم الإلكترونية الحديثة، لم تقتصر على نوع من الجرائم بعينها، بل تعددت أنواعها لتشمل كل جوانب الحياة الإنسانية السياسية، والاقتصادية، والاجتماعية؛ مما حدا بجميع دول العالم إلى أن تكثف جهودها من أجل التصدي لهذا النوع من الجرائم التي عرفها العصر الحديث (Emma Kosian, 2016) .

لقد عكفت مختلف دول العالم وعلى رأسها الولايات المتحدة الأمريكية، والدول الأوروبية على تطوير قوانينها المتعلقة بالجرائم من خلال سن التشريعات الإلكترونية، وتجريبها لقياس مدى فاعليتها في التحكم في الجرائم الإلكترونية، ومراجعة العوامل التي تؤثر في مكافحة الجريمة السيبرانية، وذلك لعدة أسباب من بينها: التعقيد في الجريمة السيبرانية، والأعداد المتزايدة من الجرائم هي السبب الرئيسي الذي يواجه تنسيق التشريعات على الإنترنت؛ حيث يعمل الاتحاد الأوروبي على التنسيق العالمي للجريمة السيبرانية، ولكن مثل هذا الهدف هو هدف طويل المدى للغاية، وانضمت الولايات المتحدة إلى الاتحاد الأوروبي في جهد مشترك، وهي فرصة أفضل لتحديد دورها في مكافحة الجريمة السيبرانية (Mike Redford, 2011).

وإجمالاً يمكن القول أن هذا النوع من الجرائم لا تحدها حدود ولا تعترف بعنصر المكان أو الزمان حيث يلعب البعد الزماني والمتعلق اختلاف المواقيت بين دول العالم، والمكاني المتعلق إمكانية تنفيذ الجريمة عن بعد،

والقانوني المتعلق بأي قانون يطبق؟؛ دوراً مهماً في تشتيت جهود التحري والتنسيق الدولي لتعقبها، ومحاسبة مرتكبيها. فالجرائم هنا لن تكون مقتصرة على دولة بعينها، وإنما سيكون العالم كله مسرحاً لها؛ حيث يمكن للمجرم ارتكاب جريمته من أي مكان في العالم وفي أي زمان دونما عوائق على اختلافها؛ مما يسهل عليه ارتكابها، والتواري عن الملاحقة القانونية.

لذا فإن الحل الأمثل لمواجهة تلك الجرائم لا يقتصر على الحلول القانونية فحسب بل لابد من الجانب الوقائي من خلال تكاتف جميع منظمات المجتمع المدني لإقامة المعارض والندوات لتوعية المجتمع والقطاع الخاص للتعريف بهذه الجرائم ومخاطرها، وكيفية استخدام مواقع التواصل الاجتماعي بصورة آمنة، وممارسة الحريات والحقوق في الحدود القانونية والدستورية (محمود، وكاظم ،2015).

المبحث الثاني: موقف المشرّع العماني من الجرائم الإلكترونية، وكيفية علاجها:

المطلب الأول: موقف المشرِّع العماني من الجرائم الإلكترونية:

كما هو معلوم من الناحية القانونية فإن المقصود من نطاق تطبيق القانون: انبساط سلطته على الوقائع والأشخاص المخاطبين بأحكامه وقواعده.

وفي الحقيقة هناك مذهبان يحددان نطاق تطبيق القانون على مستوى العالم المعاصر؛ فبعض الدول تأخذ بمبدأ إقليمية القوانين ويقصد به: أن قانون دولة ما يطبق ويسري على جميع ما يقع على إقليمها من وقائع، وعلى كافة الأشخاص المقيمين في هذه الدولة أياً كانت جنسيتهم، بمعنى آخر أكانوا وطنيين أم أجانب، وسواء أكانت إقامة هؤلاء الآخرين إقامة دائمة أم إقامة مؤقتة؛ فالدول التي تأخذ بهذا المبدأ إنما تطبق فكرة سيادة الدولة بالمعنى الواسع لهذا الأخير.

وبالمقابل فهناك من الدول التي تأخذ بمبدأ شخصية القوانين ويقصد به: أن قانون الدولة يطبق فقط على رعاياها، وسواء أكانوا مقيمين على إقليمها أم رحلوا للإقامة خارج إقليم تلك الدولة، والدول التي تأخذ وتتبنى هذا المبدأ إنما تقرر مبدأ سيادة الدولة على رعاياها.

لذا فإن المشرع العماني- كما هو الشأن في القوانين الحديثة عموماً- أخذ بصفة عامة أو أصلية بمبدأ إقليمية القوانين، وذلك يعني أن التشريعات العمانية تطبق على كل ما يقع من وقائع وأحداث في إقليم السلطنة، وسواء وقع من قبل عمانيين أم من قبل أجانب. والمقابل فإن المشرع العماني يأخذ بمبدأ شخصية القوانين، ولكن في حالات استثنائية محددة؛ كتلك الاستثناءات الخاصة بالحقوق والواجبات المنصوص عليها في النظام الأساسي للدولة في سلطنة عمان، وهي بطبيعة الحال مقررة للعمانيين دون الأجانب، وسواء أكان هؤلاء العمانيون إقامتهم داخل السلطنة أم كانوا خارجها. أو بعض الاستثناءات التي نص عليها قانون الجزاء العماني، وكذلك ما يقرره القانون الدولي العام من حصانة عامة لرؤساء الدول الأجنبية، وكذلك أفراد أسرهم، والسفراء وأعضاء البعثات الدبلوماسية وغيرهم. فجميع هؤلاء لا يخضعون حال ارتكابهم لجريمة ما لقانون الدولة التي يتواجدون فيها طالما وقعت الجريمة أثناء ممارستهم لوظيفتهم أو بمناسبة ممارستهم إياها أم لا. وقد أخذ المشرع العماني بهذه الأحكام.

ومن الاستثناءات القانونية كذلك قواعد القانون الدولي الخاص؛ فهذه القواعد التي تعين القانون الواجب التطبيق في العلاقات التي يتوافر فيها العنصر الأجنبي، ومن الأمثلة التطبيقية ما نصت عليه المادة (12) من قانون المعاملات المدنية العماني؛ إذ تنص المادة على أنه "يسري قانون الدولة التي ينتمي إليها الزوج على الآثار التي يرتبها عقد الزواج على أنه إذا اتحدت جنسية الزوجين بعد الزواج يطبق قانون جنسيتهما على آثار الزواج".

وإجمالاً يمكن القول أن سلطنة عمان قد شهدت في الفترة الأخيرة طفرة تشريعية في مختلف المجالات، وكان للفضاء السيبراني نصيباً منها، حيث سعى المشرع العماني إلى مكافحة الجرائم الإلكترونية بشكل مرحلي، وتعد السلطنة من أوائل الدول العربية التي تضمنت قوانينها الجرائم الإلكترونية، ويمكن إبراز ملامح مكافحة الجرائم الإلكترونية في السلطنة على النحو التالي (البقمي، 2008)، و(الغافري، http://hussain- alghafri.blogspot.com، تاريخ الزيارة 2018/10/25).

المطلب الثاني: تدرج المشرع العماني في العقوبة المتعلقة بالجريمة الإلكترونية:

حاول المشرِّع العماني مواكبة التقدم التكنولوجي، من خلال تحديث القوانين التي تجرّم الاستخدام غير المشروع لوسائل التقانة الحديثة، وكذلك شبكة المعلومات العالمية (الانترنت)؛ ويمكن إجمال المراحل القانونية التي مر بها المشرع العماني من أجل تطوير القوانين ذلك العلاقة بالجريمة الإلكترونية على النحو الآتي:

أولاً: قانون الجزاء العماني: لم يشتمل قانون الجزاء العماني الذي صدر في عام 1974م على نصوص تجرم الانتهاكات ذات الصلة بتقنية المعلومات، وهذا يعطي مؤشراً بأن الوضع الجرمي في السلطنة لم يكن يستدعي وجود مثل هذه النصوص. إلا أن العولمة لم تبق الوضع على حاله كثيراً، إذ اضطر المشرع العماني في عام 2001م – أي بعد قضية سرقة الشفرات الخاصة بشبكة المعلومات العالمية عام 1997م حيث تعرّضت مجموعة من حسابات المُشتركين للاختراق، ممّا كبّد أصحابها مبالغ طائلة – إلى التدخل بإجراء تعديل في القانون، وذلك بإضافة فصل في الباب السابع منه تحت عنوان "جرائم الحاسب الآلي" بموجب المرسوم السلطاني رقم (2001/72). اشتمل هذا الفصل على خمس مواد (المواد 276 مكرراً و276 مكرراً 1 و276 مكرراً 2 و276 مكرراً 3 و 276 مكرراً 4). إذ عبرت تلك النصوص القانونية عن إرادة المشرع العماني ورغبته في مواكبة التطور السريع لتقنية المعلومات وشبكات الاتصال.

إن المادة القانونية- سالفة الذكر- والتي تمت إضافتها عدَّدت الصور الإجرامية التي يعاقب عليها قانون الجزاء العماني؛ إذ جرمت المادة 276 مكرراً ؛ عشر صور جرمية وهي: الالتقاط غير المشروع للمعلومات أو البيانات، والدخول غير المشروع على أنظمة الحاسب الآلي، والتجسس والتصنت على البيانات والمعلومات، وانتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم، وتزوير بيانات أو وثائق مبرمجة أيًا كان شكلها، وإتلاف وتغيير ومحو البيانات والمعلومات، وجمع المعلومات والبيانات وإعادة استخدامها، وتسريب المعلومات والبيانات، والتعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع، ونشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكًا لقوانين حقوق الملكية والأسرار التجارية.

أما المادة 276 مكرراً 1 فقد نصت على تجريم صورة اضافية وهي: الاستيلاء على البيانات، تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات، وجاءت العقوبة "بالسجن مدة لا تقل عن ستة أشهر ولا تزيد عن سنتين وبغرامة لا تقل عن خمسمائة ريال أو بإحدى هاتين العقوبتين"، لكنها لم تنص على سرقة الكمبيوتر أو أي صور أخرى متصلة بتعطيل عمل الأنظمة الإلكترونية، كما لم تتضمن النصوص ولم تتعرض لجرائم الاحتيال باستخدام الحاسب الآلي وإن كانت النصوص تضمنت بعض صوره من الناحة الفنية.

أما المادة 276 مكرراً 3 فقد نصت على أنه "يعاقب بالسجن مدة لا تزيد عن خمس سنوات وبغرامة لا تجاوز ألف ريال كل من:

1. قام بتقليد أو تزوير بطاقة الوفاء أو السحب.
2. استعمال البطاقة المقلدة أو المزورة مع العلم بذلك.

3. قبول الدفع ببطاقة الوفاء المقلدة أو المزورة مع العلم بذلك.

كما عالجت المادة 276 مكرراً 4 ثلاث صور من صور استخدام بطاقات الوفاء الإلكترونية، ونصت على أنه " يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تجاوز خمسمائة ريال كل من:

1. استخدم البطاقة كوسيلة للوفاء مع علمه بعدم وجود رصيد له.
2. استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو عالم بذلك.
3. استعمل بطاقة الغير بدون علمه.

قانون تنظيم الاتصالات: رغبة من المشرِّع العماني في إيجاد إطار قانوني فعال لتنظيم قطاع الاتصالات بالسلطنة ولتشجيع المنافسة، وإيجاد بيئة مستقرة تتسم بالشفافية وتعزز ثقة المستثمرين في هذا المجال فقد المرسوم السلطاني رقم (2002/30). أعقبه صدور لائحته التنفيذية بموجب القرار رقم 2008/144؛ بالإضافة إلى مجموعة من القرارات التنظيمية ذات الصلة.

لقد تطرق القانون – آنف الذكر- إلى الجرائم المتعلقة بشبكة الإنترنت؛ فقد جرَّم مجموعة من الأفعال ذات العلاقة بقطاع الاتصالات، والتي من الممكن أن ترتكب على شبكة الإنترنت أو بواسطتها. فقد نصت المادة 61 منه على أنه "يعاقب بالسجن مدة لا تزيد على سنة، وبغرامة لا تزيد على ألف ريال عماني، أو بإحدى هاتين العقوبتين كل من:

1. يستخدم نظام أو أجهزة أو وسائل الاتصالات بقصد توجيه رسالة مع علمه بأنها غير صحيحة أو بأنها تتسبب في الإضرار بسلامة أي شخص أو بكفاءة أية خدمة.
2. يستخدم أجهزة أو وسائل الاتصالات في غير الحالات المصرح بها من الهيئة أو في حالات تأدية مهام وظيفية لدى المرخص له بقصد:

أ. الحصول على معلومات عن مضمون الرسالة أو مرسلها أو المرسل إليه إذا كان من يستخدم هذه الوسائل أو تلك الأجهزة أو من ينوب عنه غير مصرح له من الهيئة – لأسباب تشغيلية – بالحصول على تلك المعلومات

ب. إفشاء سرية أية بيانات متعلقة بمضمون الرسالة أو بمرسلها أو بالمرسلة إليه تكون قد وصلت إلى علمه بسبب استخدام هذه الوسائل أو تلك الأجهزة سواء من قبله أو من قبل أي شخص آخر وذلك باستثناء الحالات التي يجوز فيها إفشاء سرية تلك البيانات بالتطبيق لأحكام هذا القانون أو أي قانون آخر.

3- كل من يرسل بواسطة نظام أو أجهزة أو وسائل الاتصالات رسالة مخالفة للنظام العام أو الآداب العامة مع علمه بذلك.

4- كل شخص طبيعي أو معنوي صاحب موقع أو مدير له أو المشرف عليه إذا حرض أو وافق على نشر الرسائل الواردة بالبند (3) من هذه المادة عن طريق شبكة الاتصالات أو ساعد عليه بعمل إيجابي أو سلبي.

ج. قانون المعاملات الإلكترونية: تماشياً مع الاستراتيجية الوطنية لمجتمع عمان الرقمي والحكومة الإلكترونية المنبثقة من الرؤية المستقبلية للاقتصاد العماني 2020، والتي أخذت هيئة تقنية المعلومات على عاتقها تنفيذها، فظهرت الحاجة إلى وجود تشريع قانوني متكامل يُعنى بتنظيم التعاملات التي تتم في العالم الافتراضي من حيث تحريرها وحفظها وتبادلها وتوفير الحماية التقنية لها وإضفاء الحجة القانونية لها؛ فكان صدور قانون المعاملات الإلكترونية ليشكل نقلة نوعية في البنية التشريعية القانونية التي تشهدها سلطنة عمان؛ حيث صدر هذا القانون بموجب المرسوم السلطاني رقم (2008/69) ، وقد وضع بعد دراسة ومقارنة أهم التجارب العالمية التي شملت قوانين التجارة الإلكترونية (الأونسترال، ,الولايات المتحدة الأمريكية، وفرنسا، وتونس). وهو يعد أول تشريع متكامل يعنى بتنظيم التعاملات التي تتم في العالم الافتراضي من حيث تحريرها وحفظها وتبادلها وتوفير

التقنية لها وإضفاء الحجية القانونية لها. وقد اشتمل على 54 مادة مقسمة إلى تسعة أبواب، ويشمل نطاق لقانون المعاملات التي يمكن إتمامها إلكترونيا سواء أكانت مدنية أو إدارية ومن أهم ملامحه المراسلات الإلكترونية وتنظيم مسألة التواقيع الإلكترونية وخدمات التصديق الإلكتروني والخصوصية المعلوماتية وتوفير الحماية الجنائية للتعاملات الإلكترونية (الغافري، 2010: 19).

وقد نص المشرع العماني في الباب التاسع من هذا القانون على تجريم (18) فعلاً إجرامياً يتعلق بتقنية المعلومات على النحو التالي:

1. المادة (52) جرمت (15) فعلاً إجرامياً وقضت بمعاقبة الجاني بعقوبتين الأولى سالبة للحرية (السجن بحد أقصى سنتين)، والثانية مالية (الغرامة بحد أقصى 5000 ريال عماني) هذه الأفعال يمكن ردها إلى الصور التالية:
   - أ- الاعتداء على البرامج والنظم المعلوماتية .
   - ب- الاختراق المعلوماتي.
   - ج- الاعتداء على المواقع الإلكترونية.
   - د- الاعتداء على البيانات والمعلومات المشفرة.
   - هـ- الاعتداء على منظومة التوقيع الإلكتروني.
   - و- التزوير المعلوماتي.
   - ز- الغش المعلوماتي .
   - ح- ممارسة نشاط مقدم خدمات التصديق الإلكتروني بدون ترخيص.
2. المادة (53) جرمت صوراً إضافية خاصة بالتوقيع الإلكتروني وفرضت على الفاعل عقوبة سالبة للحرية (السجن لمدة لا تزيد على سنة واحدة) وعقوبة مالية) الغرامة بحد أقصى 1500ريال) هي:
   - أ- صناعة أو حيازة نظام أو برنامج معلوماتي لإنشاء توقيع إلكتروني بدون موافقة صاحب التوقيع .
   - ب- عدم التعاون مع السلطات المختصة.

د. قانون مكافحة جرائم تقنية المعلومات: أتت فكرة القانون من منطلق رغبة المشرع العماني في سد النقص التشريعي في هذا المجال، وكون النصوص الواردة في سلسلة التشريعات- السالف ذكرها- لم تعد كافية لمواجهة هذه النوعية من الجرائم؛ نتيجة للتقدم المتسارع للتقانة فقد صدور المرسوم السلطاني رقم (2011/12).

المطلب الثالث: دور قانون جرائم تقنية المعلومات في مكافحة أنواع الجرائم الإلكترونية في سلطنة عمان:

يعتبر قانون مكافحة جرائم تقنية المعلومات في سلطنة عمان الأحدث في مجال مكافحة جرائم تقنية المعلومات من بين القوانين العربية القليلة الخاصة بمكافحة جرائم تقنية المعلومات، وقد استطاع سد معظم أوجه القصور في هذا الجانب. وسعى المشرع العماني من خلال هذا القانون إلى معالجة الكثير من المشكلات التي تواجه مكافحة هذا النوع من الجرائم وذلك من خلال التحديد الدقيق لمصطلح تقنية المعلومات، والبيانات والمعلومات الإلكترونية الحكومية، ووسيلة تقنية المعلومات، والشبكة المعلوماتية، والموقع الإلكتروني، والبرنامج المعلوماتي، والنظام المعلوماتي، ومزود الخدمة، والتقاط المعلومات، ومحتوى المعلومات، والمواد الاباحية. إلا أنه رغم ذلك لم يعرف الجريمة الإلكترونية، بل اكتفى بالإشارة إلى أن جرائم تقنية المعلومات هي الجرائم المنصوص عليها في هذا القانون (المقبالي، 2013)، و(البقمي، 2008).

لقد حاول المشرع العماني حصر أنواع الجرائم الإلكترونية من خلال تقسيمها إلى عدة تقسيمات؛ فقد جرَّم التعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية وذلك بتجريم:

1. الدخول غير المشروع إلى المواقع الإلكترونية والنظم المعلوماتية كلها أو جزء منها والبقاء فيها بعد علمه بواقعة الدخول غير المشروع.
2. التغيير والتعديل والاتلاف العمدي دون وجه حق، وباستخدام وسائل تقنية المعلومات، وبيانات أو معلومات فحص أو تشخيص أو علاج أو رعاية طبية.
3. الدخول غير المشروع بقصد الحصول على معلومات أو بيانات إلكترونية حكومية.
4. الدخول غير المشروع إلى أي موقع إلكتروني بقصد تغيير تصميمه أو تعديله أو إتلافه أو الغاؤه أو شغل عنوانه.
5. اعتراض البيانات أو المعلومات عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو التنصت عليها.
6. ايقاف أي نظام معلوماتي أو شبكة معلوماتية أو وسائل تقنية المعلومات أو تعطيلها.
7. اعاقة أو تعطيل حق الوصول إلى خدمات مزود الخدمة، أو الدخول إلى نظام معلوماتي أو وسائل تقنية المعلومات.

كما أن المشرع أوضح صراحة في القانون- آنف الذكر- النصوص القانونية التي تجرَّم استخدام الشبكة المعلوماتية ووسائل تقنية المعلومات في انتاج أو حيازة أو بيع أو شراء أو استيراد أو توزيع أو عرض أو اتاحة برامج أو أدوات أو أجهزة مكيفة لأغراض ارتكاب جرائم تقنية المعلومات، والتزوير والاحتيال المعلوماتي، وجرائم المحتوى الموجود في شبكة المعلومات؛ حيث جرم القانون: استخدام الشبكة المعلوماتية وتقنية المعلومات في التعامل مع المواد الإباحية، واستخدام الشبكة المعلوماتية وتقنية المعلومات في الحض على الفجور أو الدعارة، والتعدي على حرمة الحياة الخاصة، والمقامرة الإلكترونية، والاخلال بالآداب العامة أو الترويج للبرامج المخصصة لذلك، والتهديد والابتزاز الإلكتروني، واستخدام الشبكة المعلوماتية وتقنية المعلومات في المساس بالقيم الدينية أو النظام العام، والارهاب الإلكتروني، وغسل الاموال الإلكتروني، والاتجار بالبشر الإلكتروني، والاتجار الإلكتروني بالأعضاء البشرية، والاتجار الإلكتروني بالأسلحة، والاتجار غير المشروع بالمخدرات، والتعدي على حقوق المؤلف والحقوق المجاورة، والاتجار الإلكتروني غير المشروع بالأثار والتحف الفنية. كما أوضح القانون تجريم التعدي على البطاقات المالية، والنص على مسؤولية الشخص المعنوي.

وبمقارنة القانون العماني- السالف الذكر- مع النصوص الدولية ذات الصلة بمكافحة الجرائم السيبرانية، يلاحظ أنه قابل للتطبيق على جميع الجرائم المتعلقة بشبكة المعلومات العالمية، وجميع وسائل التقانة الحديثة التي يمكن أن تساهم في ارتكاب الجرائم الإلكترونية؛ آخذاً في الاعتبار معظم الأفعال الإجرامية الواردة في النموذج المقترح من قبل (الاسكوا)، كما وأنه استفاض في تحديد أوجه التعدي على أنظمة المعلومات والبيانات وشبكات الاتصال، تمامًا كما ورد في الاتفاقية الأوروبية حول جرائم السيبرانية (بودابست 2001/10/23) المواد (5، 6، 7 و 8) منها. إلا أن القانون لم يرد فيه أي مواد تتعلق بتجريم الأعمال العنصرية وكره الأجانب؛ والمرتكبة بواسطة استخدام الشبكة المعلوماتية العالمية أو إحدى وسائل تقنية المعلومات، على غرار ما ورد في البروتوكول الإضافي للاتفاقية الاوروبية حول جرائم الحاسوب، وحول تجريم الأعمال العنصرية وكره الاجانب المرتكبة بواسطة الحاسوب.

الخاتمة:

تناول البحث الحالي الجريمة الإلكترونية في سلطنة عمان؛ باعتبارها ظاهرة بالغة الخطورة على مستوى الأفراد والمؤسسات والدول، إذ أن حجم الجريمة الإلكترونية في تزايد مستمر، وعمق تأثيرها السلبي على الفرد والمجتمع في تزايد مستمر؛ مما دفع الدول إلى بذل المزيد من الجهود الرامية على مكافحة هذا النوع من الجرائم؛ مع التأكيد على أهمية مكافحة هذه الجرائم بصورة تكاملية بين مختلف دول العالم؛ ذلك أن هذا النوع من الجرائم لا يقتصر على بلد دون غيره؛ نظراً لجسامة أخطارها وخسائرها الفادحة وسرعة انتشارها؛ حيث أصبح التعامل مع صور هذه الجرائم موضع اهتمام الجميع.

لقد حاول المشرِّع العماني جاهداً إيجاد النصوص القانونية الكفيلة بمكافحة هذا النوع من الجرائم إلا أن الجرائم الإلكترونية في تطور مستمر؛ وبالتالي أضحى ذلك عبأً إضافياً، وتحدياً لرجال القانون من أجل مواكبة القوانين لمختلف تلك الجرائم وخاصة الحديثة منها؛ إلى جانب التدريب المستمر لمكافحة تلك الجرائم لمختلف الوظائف القضائية والتشريعية والرقابية، والتي تساهم في التصدي لها ومعالجتها.

كما أن البحث الحالي أكد على وجود تعريف قانوني يحدد مفهوم الجرائم الإلكترونية في التشريع العماني من خلال قانون مكافحة جرائم تقنية المعلومات، وهو ما يدحض فرضية "عدم وجود تعريف قانوني يحدد مفهوم الجرائم الإلكترونية في التشريع العماني. كما أن ذات القانون أكد على وجود تشريعات قانونية خاصة تعاقب مرتكب الجريمة الإلكترونية في سلطنة عمان، وهو ما يدحض الفرضية الثانية لهذا البحث والتي تنص على " لا توجد تشريعات قانونية خاصة تعاقب مرتكب الجريمة الإلكترونية في سلطنة عمان ".

وإجمالاً يمكن القول أن المشرع العماني قد حاول التصدي للجريمة الإلكترونية منذ بدايات ظهور التقانة، وما صاحبها من تطوير في مجال شبكة الانترنت، وتوظيفها في شتى المجالات؛ إلى جانب حماية الفرد والمجتمع من تلك الجرائم، وخاصة تلك الجرائم المتعلقة بانتهاك الحياة الشخصية؛ من أجل حمايتهم من التأثيرات غير الأخلاقية لتلك الطفرة التكنولوجية، ومن افرزته من جرائم لمن تكن موجودة في المجتمع العماني، وهو ما يعني قدرة المشرع العماني على مواكبة التقدم الحضاري والتقني الذي يشهده العالم المعاصر؛ من خلال تشريع القوانين الكفيلة لمكافحة مختلف الأنواع من الجرائم الإلكترونية وحماية المصالح العامة والشخصية من خطر تلك الجرائم، وقد توصل البحث إلى جملة من النتائج، والتوصيات على النحو الآتي:

أولاً: النتائج الرئيسة:

خلص البحث الحالي إلى جملة من النتائج على النحو الآتي:

1. تدرج المشرِّع العماني في العقوبات التي تجرم مختلف الجرائم الإلكترونية من أجل القضاء عليها أو التخفيف من آثارها على الفرد والمجتمع.
2. تنوع العقوبات المتمثلة في مكافحة الجرائم في سلطنة عمان بين الغرامة المالية والعقوبات السالبة للحرية.
3. التناغم بين مختلف مؤسسات الدولة في مكافحة الجرائم الإلكترونية على اختلافها.
4. صعوبة إثبات الجرائم الإلكترونية؛ بسبب صعوبة الاحتفاظ الفني بآثارها – إن وجدت- والحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها، وهذه الجرائم تعد من التحديات التي يواجهها رجال القانون أثناء التحقيق مع المتهمين في ارتكابها.
5. تعد الجريمة الإلكترونية من الجرائم العابرة للحدود؛ وهو ما يعني سهولة ارتكابها، وبالتالي الإفلات من العقوبة.

6. سهولة إخفاء أدلة ارتكابها، مع إمكانية التخلص منها، كما يمكن ارتكابها في وقت قصير مقارنة مع الجرائم التقليدية.

ثانياً: التوصيات والمقترحات:

1- أهمية القيام بدراسات مماثلة تتناول القيام بمسوح ميدانية تتعلق بأنواع الجرائم الإلكترونية المرتكبة، وأعداد مرتكبيها، ودوافعهم الإجرامية، وجنسياتهم، وفئاتهم العمرية، ومستواهم التعليمي؛ من أجل تطوير القوانين المعمول بها حالياً في سلطنة عمان؛ لتتواكب مع القوانين العالمية الحديثة في ذات المجال. وأهمية توعية المجتمع بخطورة الجرائم الإلكترونية، وأساليب ارتكابها.

2- إيجاد قضاء متخصص مدّرب للنظر في الجرائم الإلكترونية على اختلافها؛ إذ يحتاج هذا النوع من الجرائم إلى دراية تامة من الخبرة العملية في المجال التقني وطرق التعامل مع مختلف المكونات المتعلقة بالجرائم الإلكترونية، وأساليب الكشف عنها، وطرق التحقيق مع مرتكبيها، وهذا لا يتوفر لدى القضاء العادي.

3- التأكيد على أهمية التعاون المستمر بين مختلف الأجهزة للتصدي لهذا النوع من الجرائم؛ لما يمثله من خطورة بالغة على أمن وسلامة الفرد والمجتمع والدولة، وما ينتجه من آثار اقتصادية، واجتماعية، وأخلاقية، وقيمية على الفرد والمجتمع.

4- الاستمرار في حملات التوعية الإعلامية المجتمعية بخطورة الجرائم الإلكترونية؛ مع التركيز على الفئات العمرية الصغيرة على مستوى المدارس والجامعات، والكليات والمعاهد المختلفة؛ من أجل الوقاية من خطورة الجرائم الإلكترونية وآثارها السلبية التي تخلفها على الفرد والمجتمع على حد سواء، مع تبصير الفرد والمجتمع من خطورة توظيف التقانة في غير المجالات التي صنعت من أجلها.

5- التدريب المستمر لجميع منسوبي السلطة القضائية لتدريبهم على أحدث المستجدات التقنية في ارتكاب الجريمة الإلكترونية، وكيفية الكشف عنها.

المراجع:

أولاً: المراجع العربية:

- البداينة، ذياب موسى (2014). الجرائم الإلكترونية: المفهوم والأسباب، ورقة عمل في الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية 2- 4 سبتمبر 2014، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية.
- البشري، محمد أمين (2000). لتحقيق في جرائم الحاسب الآلي، بحوث مؤتمر القانون والكمبيوتر 1- 3 مايو 2000، جامعة الامارات العربية المتحدة المجلد الثالث، الطبعة الثالثة.
- البقمي، ناصر بن محمد (2008). مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية: أبو ظبي.
- بونعارة، ياسمينة (2016). الجريمة الإلكترونية، جامعة الأمير عبد القادر للعلوم الإسلامية: الجزائر.
- تامي، تامي (2015). الإعلام الفضائي والإرهاب، ط1، دار أسامة للنشر والتوزيع: الأردن.
- الجنبيهي، منير محمد و الجنبيهي، ممدوح محمد (2004). جرائم الإنترنت والحاسب الآلي، دار الفكر الجامعي ، الإسكندرية، جمهورية مصر العربية.
- حجازي، عبدالفتاح بيومي (2009). الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت.

- الدريبي، عبد العال (2013). الجريمة الإلكترونية بين التشريع والقضاء في الدول الغربية، المركز العربي لأبحاث القضاء الإلكتروني، الكويت.
- ديش، سورية (2017). الجرائم الإلكترونية، مجلة العلوم السياسية والقانون، جامعة جيلالي ليابس سيدي بلعباس: الجزائر.
- الشوا، محمد (1994). ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية: القاهرة.
- عبدالرحمن، محمد حسن قدري (2011). جرائم الاحتيال الإلكتروني، الفكر الشرطي، المجلد 20، العدد(79): الإمارات.
- عرب، يونس. جرائم الكمبيوتر والإنترنت، بحث منشور على شبكة الإنترنت من خلال الموقع www.arablaw.net
- عيد، محمد فتحي (1998). الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية الرياض، المملكة العربية السعودية.
- الغافري، حسين بن سعيد (2010). وضع التشريعات السيبرانية في سلطنة عمان، ودولة الامارات العربية المتحدة، ودولة قطر، اللجنة الاقتصادية والاجتماعية لغربي اسيا (الاسكوا)، ادارة تكنولوجيا المعلومات والاتصالات: بيروت.
- الغافري، حسين بن سعيد (2011). جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الإنترنت http://hussain- alghafri.blogspot.com، (تاريخ الزيارة 2018/10/25).
- الغافري، حسين بن سعيد (2011). الإطار القانوني لحماية الأطفال من مخاطر شبكة الانترنت ، قراءة في قانون مكافحة جرائم تقنية المعلومات. ورشة العمل الإقليمية في مجال السياسات وبناء القدرات في مجال حماية الأطفال على الانترنت. مسقط 30- 31 أكتوبر: سلطنة عمان.
- القحطاني، مداوي سعيد مداوي (2016). الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية. الأمانة العامة: الرياض.
- محمود، رعد سعدون، وكاظم، حسن جلوب (2015). الجرائم الإلكترونية، مجلة الدراسات المالية والمصرفية: بغداد.
- مصطفى، سمير سعدون، وآخرين (2011). الجريمة الإلكترونية عبر الانترنت، وأثرها، مجلة الدراسات المالية والمصرفية: بغداد.
- المقبالي، سعيد محمد (2013). الجريمة الإلكترونية في التشريع العماني، مقدمة من الادعاء العام بسلطنة عمان، الاجتماع الثاني للخبراء الإلكترونيين في جرائم الانترنت، فيينا.
- الملط، أحمد خليفة (2006). الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، القاهرة.

ثانياً: المراجع الأجنبية:

- Aboud, Sattar., J.2011. An Overview of Cybercrime in Iraq. The research Bulletin of Jordan ACM.Vol. pp131- 134.
- Barbara A. Bardes et al, (2000), "American Government and Politics To Today: the Essentials. United States: Wadsworth, Thomson arming.

- Kosian, Emma. 2016. Crisis and Security Management. Master Dissertation. Universiteit Leiden. Netherlands.
- Levinson, Paul (2013). New Media, international edition, 2nd edition, New York.
- Redford, Mike. 2011 European Intelligence and Security Informatics Conference. U.S. AND EU LEGISLATION ON CYBERCRIME.
- Smith, Russell, Peter Grabosky, and Gregor Urbas, (2004). Cyber Criminals on Trial. West Nyack, NY, USA: Cambridge University Press.

Electronic Crime in the Sultanate of Oman: Challenges and legal solutions

Abstract: The purpose of the research was to identify the concept of cybercrime and its Characteristics, the role of the Omani Legislator to find the appropriate solutions towards this problem. The researcher used the descriptive approach to achieve the research objectives. The research results showed that the Omani Legislator was able to deal with new civilization development and challenges by updating Laws and Rules that combat all criminal types and especially the electronic and informational crimes. The cybercrimes punishments are ranging from financial fines to freedom- related penalties. The research has reached a number of recommendations, including: The importance of conducting studies based on the surveys field that deal with the types of electronic crimes committed such as: the number of perpetrators, their criminal motives, their nationalities and age groups in order to develop the laws currently in force in the Sultanate of Oman to cope with modern international laws at the same criteria. It's very important to raise the awareness of society about the seriousness of electronic crimes, methods of committing them, its moral effectiveness and methods of prevention.

Keywords: Electronic Crime, Omani Legislator.