دور التشريع الجزائي في الحد من مخاطر الثورة الصناعية الرابعة في سلطنة عمان

الدكتورة/ صابرين جابر محمد أحمد*

الملخص:

لا يستطيع أحد أن ينكر النواحي الإيجابية للثورة الصناعية الرابعة حيث الإمكانات الهائلة في مجال تكنولوجيا المعلومات عن طريق تلك الوسائل الإلكترونية الذكية وغيرها من وسائل الذكاء الاصطناعي فقد سهلت الحصول على المعرفة وسرعة إنجاز المهام كما ساعدت على تعزيز سرعة التعلم بل اتخاذ القرار.

ورغم ذلك فقد أسفرت تلك الثورة عن العديد من المخاطر التي كان أهمها الجرائم الإلكترونية فلم تمنع أهميتها في مختلف النواحي الحياتية وقوع العديد من الأفعال الإجرامية نتيجة الاستخدام السيء للوسائل الإلكترونية والذكاء الاصطناعي حيث تزداد مخاطر الهجمات الإلكترونية مما يهدد المصالح العامة والخاصة بالخطر.

وكان من الضروري أن يكون هناك تدخلاً تشريعياً للحد من الأفعال الإجرامية التي تنتج عن سوء استخدام الوسائل التي أفرزتها الثورة الصناعية الرابعة.

وقد تدخل المشرع العماني بإصدار قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ١٢ لسنة ٢٠١١م، كما أصدر قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم ٦ لسنة ٢٠٢٢م.

وقد اتبعت في هذا البحث المنهج الوصفي والمنهج التحليلي لوصف تلك الثورة وبيان سياسة المشرع العماني في الحد منها، وتحليل النصوص الجزائية التي تواجه تلك المخاطر الناجمة عن سوء استخدام الوسائل الإلكترونية الحديثة.

ويحتوي هذا البحث على مبحثين المبحث الأول يدور حول ماهية الثورة الصناعية الرابعة والمخاطر الناجمة عنها أما المبحث الثاني فيتحدث عن الآليات الجنائية للحماية من سوء استخدام الوسائل الالكترونية.

الكلمات المفتاحية: الثورة الصناعية الرابعة – الذكاء الاصطناعي – الجرائم الإلكترونية – الوسائل الإلكترونية.

---

* أستاذ القانون الجنائي المساعد – كلية الحقوق – جامعة ظفار.

The Role of Penal Legislation in Reducing the Risks of the Fourth Industrial Revolution in Sultanate of Oman

Dr. Sabrine Jaber Mohammed Ahmed*

Abstract:
No one can deny the positive aspects of the Fourth Industrial Revolution, with its enormous potential in information technology through smart electronic devices and other artificial intelligence tools. It has facilitated access to knowledge, speeded up task completion, and helped to enhance the speed of learning and decision-making. However, this revolution has also resulted in many risks, the most important of which is electronic crime. Despite its importance in various aspects of life, many criminal acts have occurred due to the misuse of these means and artificial intelligence, with the increasing risk of cyber-attacks threatening public and private interests. Legislative intervention was necessary to limit criminal acts resulting from the misuse of the means produced by the Fourth Industrial Revolution. The Omani legislator intervened by issuing the Information Technology Crimes Law issued by Royal Decree No. 12 of 2011, as well as the Personal Data Protection Law issued by Royal Decree No. 6 of 2022.
This research used a descriptive and analytical approach to describe the Fourth Industrial Revolution and the Omani legislator's policy to limit its risks, as well as to analyze the criminal texts facing these risks resulting from the misuse of modern electronic means. This research consists of two sections: the first section discusses the nature of the Fourth Industrial Revolution and the risks resulting from it, while the second section talks about the criminal mechanisms for protection against the misuse of electronic means.

Keywords: Fourth Industrial Revolution - Artificial Intelligence - Electronic Crimes - Electronic Means.

---

*Assistant Professor of Criminal Law, College of Law, Dhofar University.

المقدمـــة

تمثل الثورة الصناعية الرابعة تطوراً غير مسبوق في مجال التكنولوجيا وتقنية المعلومات بصفة خاصة؛ حيث تعد استمراراً لسلسلة التطورات التكنولوجية التي حدثت بفضل الثورات الصناعية الثلاث التي سبقتها، لاسيما الثورة الصناعية الثالثة التي ظهر من خلالها الكمبيوتر، ودخل العالم الإنساني في إطار التكنولوجيا المعلوماتية حيث الحاسب والكمبيوتر والإنترنت.

إلا أن الثورة الصناعية الرابعة تعد تقدماً مذهلاً لم تشهده أي ثورة سابقة لها لما خلفته من تغير جذري في الوقت الحاضر أو بما هو محتمل مستقبلاً؛ حيث الابتكارات اللامحدودة التي نتجت عن تلك الثورة كالذكاء الاصطناعي، والروبوتات، وتطبيقات الهواتف الذكية، والهندسة الحيوية، وتقنية النانو، وإنترنت الأشياء وغيرها.

ورغم هذا التقدم الهائل في التكنولوجيا الصناعية وعلى رأسها تقنية المعلومات فقد أسفر عن العديد من المخاطر التي تمثلها تلك الثورة في حال إساءة استخدامها أهمها الجرائم الالكترونية؛ لذلك كان لابد من وجود آليات للحد من تلك المخاطر.

ومما لا شك فيه أن الآليات التشريعية من أهم الوسائل التي تتخذها الدول للحد من مخاطر الاستخدام السيء لمنتجات الثورة الصناعية؛ لذلك عمل المشرع العماني على مواجهة الجرائم الإلكترونية وسن التشريعات للحد منها فأصدر قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ١٢/ ٢٠١١، كما عمل على حماية البيانات الخاصة للفرد لما تمثله من أهمية في حياته فسن قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم ٦/٢٠٢٢.

إشكالية البحث:

تنطلق إشكالية البحث من ذلك التطور الهائل الذي خلفته الثورة الصناعية الرابعة في تقنية المعلومات، وما نتج عنها من وسائل التكنولوجيا الرقمية الحديثة، والتي أصبح لا

غنى عنها في معظم نواحي الحياة؛ إلا أن الإشكالية في حالة إساءة استخدام تلك الوسائل التكنولوجيا الحديثة في صناعة الآلة، واستخدامها فيما يضر الفرد والمجتمع بما يخلف جرائم إلكترونية.

فهل هناك آليات معينة انتهجها المشرع العماني للحد من تلك الانتهاكات الإجرامية بما يمثل جرائم إلكترونية؟ وهل تعد تلك الآليات كافية لذلك؟

تساؤلات البحث:

١- ما مدلول الثورة الصناعية؟

٢- ما هي مخاطر الثورة الصناعية؟

٣- كيف يمكن مواجهة المخاطر الناتجة عن الثورة الصناعية؟

٤- ما مفهوم الجريمة الإلكترونية وما مدى خطورتها كعائق للتقدم الذي أحدثته الثورة الصناعية؟

٥- هل هناك قصور تشريعي أم أن الآليات الجزائية التي ينتهجها المشرع العماني كافية لمنع الجريمة الإلكترونية أو على الأقل الحد منها؟

أهمية البحث:

من الأهمية أن يكون هناك العديد من الدراسات القانونية حول الثورة المعلوماتية، من حيث إلقاء الضوء على الدور الذي تلعبه في عصرنا المعاصر، وما تمثله للأجيال المقبلة في إطار قانوني حول مكافحة الجرائم الإلكترونية التي تنتج عن استخدام التكنولوجيا الرقمية الناتجة عن تلك الثورة.

أهداف البحث:

١- إلقاء الضوء على مدلول الثورة الصناعية الرابعة وأهميتها.

٢- بيان الوجوه السلبية لاستخدامات الثورة الصناعية الرابعة.

٣- دور المشرع في مواجهة الجريمة الإلكترونية كأحد مخاطر الثورة الصناعية الرابعة.

٤- بيان الآليات الجزائية للحد من مخاطر الجريمة الإلكترونية.

منهج البحث:

يتبع البحث المنهج الوصفي والمنهج التحليلي على النحو الآتي:

المنهج الوصفي: حيث يصف الثورة الصناعية الرابعة وسياسة المشرع العماني في وضع القواعد القانونية الجزائية للحد من الجرائم الإلكترونية التي تعد أخطر نتائج تلك الثورة.

المنهج التحليلي: يوضح تحليلاً لموقف المشرع العماني من التجريم والعقاب للجريمة الإلكترونية، ويحلل القواعد القانونية في مدى قدرتها وفاعليتها في الحد منها.

حدود البحث:

الحدود التشريعية: قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ٢٠١١/١٢، وقانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم ٢٠٢٢/٦.

الحدود الموضوعية: إلقاء الضوء على مدلول الثورة الصناعية الرابعة، وآليات مكافحة الجريمة الإلكترونية كأحد أهم المخاطر الناتجة عنها.

خطة البحث:

يحتوي البحث على مبحثين، المبحث الأول يتناول ماهية الثورة الصناعية الرابعة؛ حيث ينقسم إلى مطلبين، المطلب الأول يتناول مفهوم الثورة الصناعية وخصائصها وتأثيرها على المجتمع العماني، بينما يتناول المطلب الثاني الجريمة الإلكترونية كأحد مخاطر الثورة الصناعية الرابعة، أما المبحث الثاني فيتناول دور المشرع العماني في مواجهة خطر الجرائم الإلكترونية، وينقسم إلى مطلبين، المطلب الأول يتناول مكافحة الجريمة الإلكترونية في ظل قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢، في حين يتناول المطلب الثاني مكافحة الجريمة الإلكترونية في ظل قانون حماية البيانات الشخصية رقم ٢٠٢٢/٦.

المبحث الأول

ماهية الثورة الصناعية الرابعة

تلعب الثورة الصناعية الرابعة دوراً غير محدود في تغيير كل معالم المجتمع الإنساني بجوانبه المختلفة؛ حيث تعد نتاجاً للتطورات الهائلة في عالم التكنولوجيا، والتقدم التقني.

ويتناول هذا المبحث التعرف على مفهوم الثورة الصناعية وخصائصها، كما يتناول التعرف على الجريمة الإلكترونية، من خلال التعرف على مفهومها وخصائصها، وانعكاساتها على المجتمع العماني، وذلك من خلال المطلبين التاليين:

المطلب الأول

مفهوم الثورة الصناعية وخصائصها وتأثيرها على المجتمع العماني

يتناول هذا المطلب التعرف على مفهوم الثورة الصناعية الرابعة، من خلال استعراض بعض التعريفات التي قيلت بشأنها، كما يوضح أهم خصائصها ومميزاتها وعيوبها، وكذلك أهم الآثار المترتبة على المجتمع العماني.

أولاً– مفهوم الثورة الصناعية الرابعة، وخصائصها:

تتعدد التعريفات التي قيلت بشأن الثورة الصناعية الرابعة، كما تتعدد خصائصها، وذلك على النحو الآتي:

- **تعريف الثورة الصناعية الرابعة:**

تعبر الثورة بصفة عامة عن التغيرات النوعية الجوهرية في بنية مادية أو اجتماعية أو فكرية فتغيرها تغيراً جذرياً كما هو الحال في مجال التكنولوجيا عبر الثورات الثلاثة السابقة على الثورة الرابعة[1].

---

[1] د. علي أسعد وطفة، الثورة الصناعية الرابعة تحديات أم فرص، جامعة الكويت، ٢٠١٩م، ص١.

يطلق العديد من المصطلحات على الثورة الصناعية الرابعة؛ مثل الثورة الصناعية الرقمية، ثورة الذكاء الاصطناعي، ثورة إنترنت الأشياء[٢].

ويستخدم مفهوم الثورة الصناعية انطلاقاً من المفهوم العام للثورة، والذي يقصد به التغير الجذري الذي يحدثه التطور التكنولوجي في بنية المجتمع اقتصادياً وسياسياً واجتماعياً[٣].

وقد عرفت الثورة الصناعية الرابعة بأنها: "منظومة من المخترعات العبقرية والابتكارات التكنولوجية الفائقة مثل الثورة الرقمية، والذكاء الاصطناعي، وتكنولوجيا النانو، وإنترنت الأشياء والهندسة الحيوية"[٤].

كما تعرف بأنها: "نتاج للتكامل والانصهار الرقمي بين مختلف الثورات العلمية والتكنولوجية الهائلة في الفضاء السيبراني".

كما عرفت بأنها: "انطلاق التقانات الذكية على نحو تتلاشى فيه الخطوط الفاصلة والحدود القائمة بين ما هو رقمي وتكنولوجي وفيزيائي وبيولوجي"[٥].

- **خصائص الثورة الصناعية الرابعة:**

أ- اندماج التكنولوجيا بالمجتمع لدرجة إنها تصبح وحدة واحدة، فلا تتضح الحدود بين العالم المادي والرقمي والبيولوجي[٦].

---

[٢] آسيا بعضي، الثورة الصناعية الرابعة، مجلة الاقتصاد والتنمية المستدامة، المجلد٥، العدد٢، ٢٠٢٢م، ص٥٤٦.

[٣] د. على أسعد، مرجع سابق، ص٢.

[٤] راجع في تعريف الثورة الصناعية الرابعة، كلاوس شواب، الثورة الصناعية الرابعة، كتاب منشور على الموقع التالي:
https://www.dohainstitute.org/ar/ResearchAndStudies/Pages/the-futures-of-arab-science-and-technology-in-the-fourth-industrial-revolution.aspx

[٥] علي أسعد وطفة، المرجع السابق، ص٥.

[٦] هيئة تحرير مجلة الإرشاد النفسي بجامعة عين شمس، تداعيات الثورة الصناعية الرابعة، العدد ٦٧، ٢٠٢١م، بدون رقم صفحة.

ب- التعلم المتعمق للآلة والأشكال الجديدة للذكاء الاصطناعي[٧].

ج- الاعتماد على الآلة وإحلالها كبديل الإنسان.

د- ارتباط حركة الفرد والمجتمع بالشبكة المعلوماتية والفضاء الخارجي[٨].

و- السرعة والتأثير الممتد والشامل لنواحي الحياة[٩].

ثانياً- مميزات وعيوب الثورة الصناعية الرابعة:

لا شك أن الثورة الصناعية الرابعة لها نواحي إيجابية، جعلتها تتسم بالعديد من المميزات التي تجعل لها أثراً إيجابياً على الحياة الإنسانية، بل تجعلها تتميز عن غيرها من الثورات السابقة عليها.

- **مميزات الثورة الصناعية الرابعة:**

أ- السرعة الفائقة: حيث أن انتشار التكنولوجيا الرقمية تنتشر بسرعة هائلة الأحداث عملية تغيير شاملة، تلك السرعة التي جعلت أي نوع من التقدم التكنولوجي السابق عليها يصبح متقادم نظراً لسرعة ما أحدثته الثورة الصناعية الرابعة من تغير[١٠].

ب- الشمولية: حيث يشمل التغير الذي تحدثه الثورة الصناعية الرابعة تغيرات جذرية في مختلف نواحي الحياة، مما يجعل التكنولوجيا سبباً في اندماج الحياة الاجتماعية بالنواحي الاقتصادية[١١].

ج- التطور التقني الهائل في العديد من المجالات المهمة للبشرية مثل تقنيات التعديل الجيني.

د- تحسين جودة الحياة وزيادة كفاءة المنتجات والخدمات.

---

[٧] المرجع السابق، ص٥.

[٨] المرجع السابق، بدون صفحة.

[٩] آسيا بعضي، مرجع سابق، ص٥٦٧.

[١٠] على أسعد وطفة، المرجع السابق، ص٧.

[١١] المرجع السابق، ص٨.

د- تحقيق راحة كبيرة للأفراد وقدر كبير من الرفاهية، وهو ما نتلمسه فيما نعيشه في الوقت الحالي من ذلك التقدم المذهل في التطبيقات الإلكترونية التي تمكن الفرد من إنجاز معاملاته إلكترونياً.

هـ- تقديم خدمات أوسع للأفراد.

و- فتح أسواق جديدة ودفع عجلة النمو الاقتصادي.

- **عيوب ومخاطر الثورة الصناعية الرابعة:**

تتعدد العيوب التي تنتج جراء استخدام التكنولوجيا المتطورة التي أرستها الثورة الصناعية الرابعة، نشير إليها في النقاط الآتية:

أ- إحلال الآلة محل الإنسان يؤدي إلى ارتفاع نسبة البطالة، حيث تصبح الآلة هي البديل الأسرع، حيث تقوم الثورة الصناعية الرابعة على فكرة تقليل الأيدي العاملة، والتشغيل الآلي للصناعة من خلال التغيير الرقمي الذي تحدثه هذه الثورة[١٢]

ب- زيادة الطلب على العمال ذوي الكفاءات والمهارات العالية في مجال التكنولوجيا الرقمية وتقنية المعلومات، وهو ما يؤدي إلى الاستغناء عن نسبة كبيرة من الأيدي العاملة[١٣].

ج- قد يقتصر الدور البشري على التدقيق والمراقبة، وهو ما يتطلب أيضاً كفاءات معينة وعلى قدر عال من الفهم بالآلة وتقنية المعلومات.

د- انتشار قنوات التواصل الاجتماعي لاسيما مع التطور التكنولوجي الهائل الذي خلفته الثورة الصناعية الرابعة إلى العديد من السلبيات التي تصل إلى حد نشر الجريمة.

هـ- أهم المخاطر التي تتولد عن التقنيات الحديثة في مجال تقنية المعلومات الهجمات السيبرانية التي تنال الدول والأفراد، وتهدد أمن المجتمع، والعديد من السلوكيات الإجرامية التي تتطور بتطور التكنولوجيا تحت ما يسمى بالجرائم الإلكترونية التي تشهد أشكالاً مختلفة، وبصورة متسارعة.

---

[١٢] أحمد حسن عمر، مفهوم الثورة الصناعية الرابعة، مجلة الاقتصاد والمحاسبة، العدد ٦٦٦، ٢٠١٧م، ص١٦-١٩.

[١٣] أحمد حسن عمر، المرجع السابق، ص١٦.

و- المخاطر البيئية التي تتسبب فيها الثورة الصناعية الرابعة، أولها الاحتباس الحراري، ومشاكل التنوع الحيوي، والكوراث الطبيعية، بل الكوارث البيئية التي هي من صنع الإنسان.

ثانياً- أثر الثورة الصناعية الرابعة على سلطنة عمان:

لقد كانت سلطنة عمان من أبرز الدول التي سعت إلى محاولة تحويل خدماتها التقليدية إلى خدمات إلكترونية، تماشياً مع ما أفرزته الثورة الصناعية الرابعة، وتحقيقاً لما ترنو إليه رؤية عمان٢٠٤٠ ، حيث وفرت سلطنة عمان بوابة رسمية للخدمات الحكومية، حيث بذلت هيئة تقنية المعلومات وجميع مؤسسات السلطنة جهوداً في إطار التحول الرقمي.

ومن خلال السعي الدائم لسلطنة عمان، وتحقيقاً لرؤية "عمان ٢٠٤٠" ، فهي تعمل على رفع الناتج المحلي من مساهمة الاقتصاد الرقمي إلى١٠%، ومساهمة تقنية المعلومات بين ٣٠% إلى٣٥%، وذلك من خلال التوجه الاستراتيجي الذي يهدف إلى تحقيق زيادة في المساهمة الاقتصادية تُقدر بنحو ٥٠% لكل ٥ سنوات، وبزيادة في حصة تقنية المعلومات تقدر بـ ٥% [١٤].

كما أحدثت تحولاً نوعياً، والذي يعد تأثراً، بل مواكبة لما يشهده العالم من تطور هائل في تقنية المعلومات من خلال "الاستراتيجية الوطنية لمجتمع عمان الرقمي والحكومة الإلكترونية" التي حددت خطط وآليات العمل لتحقيق هذا الهدف، وانطلاقاً من هذه الاستراتيجية ولدت مبادرة عمان الرقمية، التي تهدف إلى تفعيل تقنية المعلومات والاتصال؛ لتعزيز الخدمات الحكومية، وتمكين الأفراد من التعامل الرقمي؛ حيث تهدف تلك المبادرة إلى إيجاد بنية أساسية متكاملة؛ لتوفير الخدمات الإلكترونية، وكذلك سرعة إنجاز العمل في الجهات الحكومية وغير الحكومية[١٥].

---

(١٤) https://omannews.gov.om/topics/ar/3/show/409487/

(١٥) https://www.oman.om/home-page

كما جاء البرنامج الوطني للذكاء الاصطناعي والتقنيات المتقدمة في عام ٢٠٢٠م ضمن هيكلة وزارة النقل والاتصالات وتقنية المعلومات كأحد البرامج التنفيذية للبرنامج الوطني للاقتصاد الرقمي، والذي يعد التوجه الاستراتيجية للذكاء الاصطناعي والتقنيات المتقدمة في السلطنة، لتشجيع تبني الذكاء الاصطناعي، والتقنيات المتقدمة وتوطينها، بقياس التجارب الدولية، وتنسيق لقاءات وورش عمل مع الشركاء من القطاعين العام والخاص والأكاديميين ورواد الأعمال المختصين بتقنيات الذكاء الاصطناعي، والتقنيات المتقدمة.

وقد وضعت وزارة النقل والاتصالات أنظمة لمواكبة التطور الذي أفرزته الثورة الصناعية الرابعة؛ حيث وضعت تنظيماً لسياسة استخدام الذكاء الاصطناعي؛ لتشجيع الجهات الإدارية على استخدامه بطريقة آمنة[١٦].

ورغم ذلك؛ فإن خطر الجريمة الإلكترونية يزداد يوماً بعد يوم بتزايد التطور التقني، وهو ما يهدد أمن المجتمع؛ لذا كان لابد من وجود سياسات تشريعية للحد من تلك الجرائم، وهو ما نتناوله في المبحث الثاني من البحث.

المطلب الثاني

الجريمة الإلكترونية كأحد مخاطر الثورة الصناعية الرابعة

من أهم وأخطر التهديدات التي نتجت عن التطور التقني الهائل الذي أرسته الثورة الصناعية الرابعة الجريمة الإلكترونية؛ حيث تكثر مخاطر الهجمات الإلكترونية عبر الإنترنت، بل إن تقرير المخاطر العالمية ٢٠١٨م أعرب عن مخاوفه من قيام محترفي الجرائم الإلكترونية من القدرة على التسلل إلى مركباتنا وأعمالنا وبياناتنا[١٧].

---

(١٦) https://www.qscience.com/content/journals/10.5339/jist.2020.2?crawler=true

(١٧) علي أسعد وطفة، ص١١.
https://www.researchgate.net/publication/349105626_althwrt_alsnayt_alrabt_frs_wthdyat

أولاً- تعريف الجريمة الإلكترونية:

تعرف الجريمة الإلكترونية بأنها: "كل سلوك اجرامي يتم بمساعدة الحاسب الآلي، أو هي كل جريمة تتم في محيط الحاسبات الآلية" [١٨]، كما عرفت بأنها: "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسة"[١٩].

كما عرفت بأنها: "نشاط غير مشروع موجه لنسخ، أو تغيير، أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب والتي تحول عن طريقه"[٢٠]، أو هي: "مجموعة الأفعال غير المشروعة المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب"[٢١]، وعرفت كذلك بأنها: "أية جريمة تكون متطلب لاقترافها أن تتوفر لدى فاعلها معرفة تقنية الحاسب"[٢٢].

---

[١٨] مهند وليد إسماعيل، التنظيم القانوني للجريمة الإلكترونية، مجلة العلوم القانونية والسياسية، المجلد (١١)، العدد (١) السنة (٦)، ٢٠١٦م، ص١٧٢.

[١٩] رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الجديد، ٢٠١٣م، ص١٩، راجع في تعريف جرائم الإنترنت.

[٢٠] مهند وليد إسماعيل، المرجع السابق ص١٧٢.

[٢١] المرجع السابق ص٢١، ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دار الجامعة الجديدة، ٢٠١٢م، التعريف ص١١، ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، رسالة ماجيستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، ٢٠١٢م، ص٨، محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، المنصورة، مصر، ٢٠١٥م، ص١٤.

[٢٢] محمود أحمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة عمان، ٢٠٠٥م، ص١٥، نقلاً عن المرجع السابق، ص٢٠، وراجع في تعريف الجريمة الإلكترونية هدى حامد قشقوش: جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، ١٩٩٢م، ص٨، د. اسراء جبريل رشاد مرعي: الجرائم الإلكترونية، الأهداف – الأسباب – طرق الجريمة ومعالجتها، المركز العربي للدراسات الاستراتيجية والاقتصادية والسياسية، بحث منشور على الموقع الإلكتروني:
https://democraticac.de/?p=35426
ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية، دار الجامعة الجديدة، ٢٠١٢م، ص١١.
طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٩م، ص١٥٩، نقلاً عن المرجع السابق ص٢٤.

وهناك اتجاه جمع بين أكثر من معيار لتعريف الجريمة الإلكترونية، ومن ذلك تعريفها بأنها: "أي سلوك غير قانوني، أو غير أخلاقي، أو غير مفوض يتعلق بالنقل، أو المعالجة الآلية للبيانات يعد اعتداء على الكمبيوتر"[٢٣].

ومن مجمل التعريفات السابقة فالجريمة الإلكترونية تعد مختلفة عن الجريمة التقليدية في موضوعها ونهاية أو محلها وهو المعلومات أو البيانات الإلكترونية، وسواء كانت بجهاز الحاسوب أو أياً من الأجهزة الأخرى مثل الهواتف النقالة والذكية التي تخزن عليها المعلومات والبيانات.

لذلك يمكن تعريفها تعريف بأنها: "كل فعل يسلكه الجاني يمثل اعتداء على المعلومات أو البيانات الإلكترونية، ويمثل انتهاكاً يجرمه القانون، ويسن عليه جزاءً جنائياً".

ثانياً- خصائص الجريمة الإلكترونية:

هناك عدد من الخصائص التي تميز الجريمة الإلكترونية عن الجريمة التقليدية تتلخص في:

١- لا تعترف الجريمة الإلكترونية بحدود جغرافية أو زمنية؛ حيث ترتكب عن طريق استخدام شبكة الإنترنت، فطبيعتها متعدية للحدود، عابرة للدول بل القارات حتى صار العالم كله مسرحاً لارتكابها[٢٤].

٢- صعوبة الإثبات في الجرائم الإلكترونية؛ نظراً لطبيعة الوسائل التي يستخدمها الجاني، والتي تتميز بكونها وسائل تقنية حديثة ومتطورة، ومن الصعب في تلك الوسائل وجود أثر مادي ملموس[٢٥]؛ فقد يقوم الجاني بالتخلص منها أو إتلاف الوسيلة المستخدمة

---

[٢٣] في ذات المعنى عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، ٢٠٠٧م، ص١٥، نقلاً عن د. أحلام النهوي، المرجع السابق، ص٣.

[٢٤] لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها، مجلة الميزان للدراسات الإسلامية والقانونية، ٢٠١٦/٢٠١٧م، ص٩.
https://portal.arid.my/Publications/e1788f58-0853-47.pdf

[٢٥] مهند وليد إسماعيل، المرجع السابق ص١٧٦، أمجد حسن مرشد الدعجة، استراتيجية مكافحة الجرائم المعلوماتية، رسالة ماجيستير، جامعة أم درمان الإسلامية، ٢٠١٤م.

في اقترافها، وبالتالي يصعب إيجاد الدليل كما يصعب تصور الاعتراف فيها، وشهادة الشهود، وهو ما يجعل التحري والتحقيق والمقاضاة أمراً يحيطه العديد من المعضلات والمشكلات الإدارية والقانونية، وباعتبارها متعدية الحدود ولا تعترف بمكان أو زمان، وهو ما يجعلنا نواجه مشكلة الاختصاص القضائي والقانون الواجب التطبيق، ويصعب معه التحقيق والملاحقة والضبط والتفتيش، ولعل كيانات الذكاء الاصطناعي بما لديها من إمكانات غير هائلة أصبحت قادرة على القيام بسلوكيات إجرامية بأشكال مختلفة لم تكن معروفة من ذي قبل.

٣- يستخدم غالباً الحاسب الآلي في ارتكاب الجرائم الإلكترونية، وكذلك الهواتف النقالة، بل قد يستخدم الحاسب الآلي في سرقة المعلومات أو التزوير المعلوماتي في الحالات التي لا تستلزم استخدام شبكة الإنترنت، بالإضافة إلى التقنيات العالية التي تتمثل في إنترنت الأشياء، والذكاء الاصطناعي، وغيرها التي تعد وسيلة لارتكاب العديد من الجرائم.

٤- يتميز المجرم الإلكتروني بصفات خاصة من الذكاء والمهارة لتنفيذ سلوكه الاجرامي، بل أن هذا المجرم يكون لديه من الخبرة والمهارة التي يكتسبها في كثير من الأحيان من دراسته في مجال تكنولوجيا المعلومات، فهو -غالباً- مجرم محترف، فالإجرام المعلوماتي هو إجرام يحتاج إلى الذكاء دون استخدام للعنف أو القوة، وهوما يقوم به المجرم المعلوماتي[٢٦]، وها هو عصرنا الحالي يشهد إجراما للآلة بأشكال مختلفة وبصورة متسارعة؛ فأصبح المجرم الإلكتروني رجل آلي حتى وإن سلمنا بأن من صنعه إنسان.

٥- تتعدد دوافع المجرم الإلكتروني؛ فقد تكون بدافع الحصول على الربح أو بدافع الحقد أو الكراهية أو الحصول على المعلومة في حد ذاتها[٢٧].

---

[٢٦] اسراء جبريل، المرجع السابق، بدون رقم صفحة، غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، المنصورة، مصر، ٢٠١٦-٢٠١٧م، ص١٣ في سمات المجرم المعلوماتي.

[٢٧] مهند وليد إسماعيل، المرجع السابق، ص١٧٧.

المبحث الثاني

دور المشرع العماني في مواجهة خطر الجرائم الإلكترونية

لا شك أن الثورة الصناعية الرابعة رغم أهميتها في الحياة المعاصرة بما تنتجه من تطور تكنولوجي يزداد يوما بعد يوم إلا أنها كذلك أفرزت العديد من الجرائم التي تستخدم فيها تقنية المعلومات؛ والتي تعد هي الأساس الذي ترتكز عليه تلك الثورة فها هي تقنية النانو، وإنترنت الأشياء، والذكاء الاصطناعي، والروبوتات وغيرها من نتاجات الثورة الصناعية الرابعة التي تعد بمنزلة الإنجازات البشرية غير المسبوقة، ورغم ذلك فالجانب المظلم لها هو خطورة الجرائم التي قد ترتكب من خلال استخدامها.

وقد سارع المشرع العماني بإصدار قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ١٢ لسنة ٢٠١١ لمواجهة خطر الجرائم الإلكترونية، وذلك بعد سلسلة من التشريعات السابقة، والتي كانت تواجه بعض التهديدات الإلكترونية؛ ليكون هذا القانون أكثر فعالية في مواجهة خطر الجرائم الإلكترونية[٢٨].

كما أصدر المشرع العماني قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم ٢٠٢٢/٦.

المطلب الأول

مكافحة الجريمة الإلكترونية

في ظل قانون مكافحة جرائم تقنية المعلومات

أصدر المشرع العماني قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢ لمكافحة الجرائم المعلوماتية، وقد انتهج المشرع العماني سياسة في التجريم والعقاب خلال هذا القانون.

---

[٢٨] إضافة فصل ثاني مكرر إلى الباب السابع من قانون الجزاء العماني (ملغي) رقم ٧٤/٧ بموجب التعديل بالمرسوم السلطاني رقم ٢٠٠١/٧٢، قانون الاتصالات الصادر بالمرسوم السلطاني رقم ٢٠٠٢/٣٠، قانون المعاملات الالكترونية الصادر بالمرسوم السلطاني رقم ٢٠٠٨/٦٩.

أولاً- أحكام التجريم في قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢:

نظم المشرع أحكام التجريم على الأفعال التي تمثل جرائم إلكترونية من خلال عدة فصول فبعد أن أوضح بالفصل الأول منه معاني بعض المصطلحات المتعلقة بتقنية المعلومات[٢٩]، تناول بالتوالي صور الانتهاكات التي تمثل جرائم إلكترونية بحيث يختص كل فصل ببيان نوع معين من تلك الجرائم، كما تناول بالفصل الثاني من القانون جرائم التعدي على سلامة وسرية وتوفر البيانات والتعاملات الإلكترونية والنظم المعلوماتية وذلك بالمواد من (٣) إلى (١٠)، ثم تناول بالفصل الثالث منه الأفعال التي تمثل إساءة استخدام لوسائل تقنية المعلومات سواء بإنتاج أو بيع أو شراء أو توزيع أو عرضها، وذلك لأغراض ارتكاب جرائم تقنية المعلومات، وذلك بالمادة (١١) منه، بينما بالفصل الرابع جرم المشرع الأفعال التي تستخدم بها وسائل تقنية المعلومات لتغيير الحقائق وتزويرها في البيانات أو المعلومات الإلكترونية بعنوان: التزوير والاحتيال الإلكتروني والذي يمثله الأفعال التي يستخدمها المجرم الإلكتروني للتحايل، وإلحاق الضرر بالمستخدمين وذلك بالمواد (١٢)، و(١٣)، وفي الفصل الخامس منه تناول المشرع جرائم المحتوى من المادة (١٤) إلى(٢٧) حيث تتنوع تلك الأفعال الإجرامية [٣٠] فجرم من خلالها الأفعال التي يكون القصد منها استخدام وسائل تقنية المعلومات لنشر الإباحية ما لم تكن لأغراض علمية أو في الفجور، والأفعال التي فيها تعدى على حرمة الحياة الخاصة، وانتهاك

---

[٢٩] عرف قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢ بالفقرة (ب) من المادة (١) يقصد بتقنية المعلومات الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة وتوزيع البيانات والمعلومات بصيغتها المختلفة.

كما عرفت الفقرة (و) من ذات المادة وسيلة تقنية المعلومات جهاز إلكتروني يستخدم لمعالجة البيانات والمعلومات الإلكترونية أو تخزينها أو إرسالها أو استقبالها كأجهزة الحاسب الآلي وأجهزة الاتصال.

وقد عرف الموقع الإلكتروني بالفقرة (ح) بأنه مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية من خلال عنوان محدد.

[٣٠] نصت المادة (٣) على أنه: "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد عن ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين".

خصوصيتها، والتي تتعدد صور الأفعال فيها من التقاط صور، ونشر أخبار، أو تسجيلات صوتية، أو مرئية سواء كانت صحيحة أو لا، وكذلك في السب والقذف، وغيرها من الأفعال التي تمثل جرائم إلكترونية.

ويعد التعدي على البطاقات المالية، والتي تناولها المشرع بالفصل السادس منه بموجب المادة (٢٨) منه من أخطر الجرائم التي عالجها المشرع العماني، وأخيراً أورد المشرع العماني بعض الأحكام الختامية التي تتعلق بالعقاب في حال ارتكاب الشخص الاعتباري للجرائم الإلكترونية، كما تناول كذلك أحكام الإعفاء من العقوبة في حال الإبلاغ عنها، وكذلك تناول العقوبات التكميلية التي يحكم بها في سبيل ذلك.

ويلاحظ ان خبر ما فعل المشرع العماني حين انتهج تعريف تقنية المعلومات بانها (الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات؛ لمعالجة وتوزيع البيانات والمعلومات بصيغها المختلفة) حيث وسع من وسائل ارتكابها فلم يحصرها في وسائل معينة وهو ما يجعل سلطة الاتهام الممثلة في الادعاء العام وكذلك المحكمة غير مقيدة، لا سيما مع ما تفرزه الثورة الصناعية الرابعة يوماً بعد يوم من تقدم غير مسبوق في المجال الإلكتروني وبالتالي يشمل هذا القانون تجريم أي أفعال تستخدم بأي تقنيات حديثة حتى لو لم تكن موجودة وقت إصدار القانون والعمل به[٣١].

ومن خلال ما سبق يكون المشرع العماني قد أعد الجرائم الإلكترونية ما بين الجنح والجنايات.

وعلى سبيل التمثيل يعد من الجرائم الإلكترونية التي أعدها المشرع العماني جنح ما ورد بالمواد من (٣)، (٤)، (٥)، (٦)، (٧).

وكذلك يعد من الجرائم التي أعدها المشرع في مصاف الجنايات ما ورد بالمادة (٢٠) والمتعلقة بالإرهاب الإلكتروني، والمادة (٢٥) المتعلقة بتجريم الاتجار بالمخدرات

---

[٣١] دراسة علمية حول مكافحة الجرائم المعلوماتية والتقنية في السلطنة – الموقع الرسمي لجريدة عمان (omandaily.om).

وترويجها إلكترونياً، كما اعتد بأحكام الشروع، وهو ما أورده بنص المادة (٣٠) من القانون السابق الإشارة إليه.

ثانياً- أحكام العقاب ف قانون مكافحة جرائم تقنية المعلومات رقم٢٠١١/١٢:

اعتد المشرع العماني في تنظيمه لأحكام العقاب على الجرائم الإلكترونية بالعقوبات الأصلية والتكميلية، وعن العقوبات الأصلية فقد تراوحت ما بين الإعدام كما في الأفعال الاجرامية التي تناولها المشرع بالمادة (٢٥) منه والخاصة بالاتجار وترويج المخدرات.

كما اعتد بالسجن، والغرامة كعقوبة أصلية على بعض الجرائم[٣٢]، فنجده في المادة (٣) منه قد جرم ثلاثة أفعال حيث تناولت المادة (٣) الدخول غير المشروع إلى المواقع الإلكترونية أو النظم المعلوماتية تدخلاً مقصوداً حيث اعد السجن من عقوباتها الأصلية، كما شدد العقوبة على تلك الأفعال الواردة في الفقرة الأولى لتصبح العقوبة السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة، وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى العقوبتين.

وقد شدد المشرع العقوبة لنفس الحالات التي وردت بالفقرة الأولى إذا كانت البيانات التي تم انتهاكها شخصية؛ حيث جعلها السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات، وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين

ورغم أن المشرع قد شدد العقوبة في الحالتين السابقتين؛ إلا أن العقوبة ما زالت لا تتناسب مع حجم الجرم المرتكب؛ فالمعلومات التي قد يتسبب الجاني بفعله العمدي في انتهاكها قد يتسبب عنها خسائر مادية ومعنوية فادحة، لاسيما إذا كانت شخصية.

ونلاحظ أن هذا ما فعله المشرع بالمادة (٤)؛ حيث شدد عقوبة الجرائم الواردة بالمادة (٣) لتصبح السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات، وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني إذا ارتكبت أثناء أو بمناسبة

---

[٣٢] أشرف بن عبد الله الضويحي، المساهمة في الجرائم المعلوماتية المتعلقة بالاعتداء الشخصي، رسالة ماجيستير، لجنة ملخصات الأبحاث القضائية بالجمعية العلمية القضائية السعودية، العدد الثالث، ١٤٢٨-١٤٢٩هـ، ص١٠٩.

عمله بمعني أن الجاني في هذه الحالة يعمل في الجهة التي قام بالتعدي على معلوماتها أو بياناتها بالصور

وقد تناول المشرع الأفعال الإجرامية في هذا القانون التي يستخدم في ارتكابها الحاسوب كأداة أو الإنترنت، وعليه يجب التفرقة بين هذه الحالة وبين الحالة التي ترتكب فيها الجريمة وتقع على الحواسيب نفسها كمحل لها ككيانات مادية؛ ففي الحالة الأولى تعد جريمة إلكترونية، بينما في الحالة الثانية لا تنطبق الجرائم المعلوماتية؛ فعند سرقة جهاز الحاسوب أو إتلافه أو تملكه بأي فعل مجرَم مثل الاحتيال أو النهب أو الابتزاز أو التملك الجنائي، فهنا ينطبق قانون الجزاء رقم ٢٠١٨/٧ على هذه الأفعال. أما في الحالة الثانية وهي حالة ارتكاب الجريمة بواسطة هذه الأجهزة فيطبق قانون مكافحة جرائم تقنية المعلومات لسنة ٢٠١١م.

والملاحظ هنا أن العقوبة في هذه الحالة هي ذات العقوبة التي أوردها المشرع في الفقرة الثانية من المادة الثالثة إذا كان الانتهاك على بيانات شخصية، ورغم أن الجاني المقصود بالمادة الرابعة يعد موظف في هذه الجهة، وهو ما يجعل خطورته أشد من المجرم في الحالة الأخرى؛ إلا أن العقوبة ظلت كما هي وهو ما ستوجب تشديدها.

ومن نص المادة (٤) نلاحظ أن المشرع جعل العقوبة السجن والغرامة كعقوبة أصلية وحسناً فعل المشرع؛ حيث جعل السجن والغرامة عقوبة إلزامية، ورغم ذلك فيلاحظ ضآلة العقوبة المقررة لهذه الجريمة؛ لذا من الضروري تغليظها لتتناسب مع حجم الفعل الإجرامي.

وعن المادة (٥)؛ فقد جرمت الأفعال التي تمثل دخول غير مشروع والتعدي بالإتلاف أو التغيير أو التعديل المتعمد باستخدام وسائل تقنية المعلومات بالسجن الذي لا يقل عن شهر ولا يزيد على ثلاث سنوات، وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على عشرة آلاف ريال عماني.

أما المادة (٦)؛ فقد جرم المشرع الدخول غير المشروع للحصول على معلومات أو بيانات حكومية سرية، وجعل في حكمها البيانات والمعلومات السرية الخاصة بالمصارف والمؤسسات المالية؛ حيث يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات،

وبغرامة لا تقل عن ألف ريال عماني ولا تزيد ثلاثة آلاف ريال عماني، أو بإحدى هاتين العقوبتين، وشدد العقوبة في حالة إذا ترتب على فعله إلغاء أو تغيير أو تعديل أو إتلاف أو نسخ أو تدمير أو نشر لتلك البيانات بالسجن مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات، وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف عماني، ونلاحظ أيضاً أن المشرع في هذه الصورة جعل السجن والغرامة عقوبة أصلية وجوبية.

ثم تناول المشرع بالمادة (٨) تجريم استخدام وسائل تقنية المعلومات لإعاقة وصول البيانات والمعلومات الإلكترونية المرسلة عبر وسائل تقنية المعلومات أو الشبكة المعلوماتية بالسجن مدة لا تقل عن شهر ولا تزيد على سنة، وبغرامة لا تقل عن خمسمائة ريال عماني، أو بإحدى هاتين العقوبتين.

أما المادة (٩) فجرمت الأفعال التي من شأنها إيقاف الشبكة أو تدميرها أو تعطيلها بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاثة سنوات، وبغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني، أو إحدى هاتين العقوبتين.

كذلك جرمت المادة (١٠) الأفعال التي تعوق الخدمة الإلكترونية من الوصول؛ حيث تكون عقوبتها السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، وبغرامة لا تقل خمسمائة ريال عماني ولا تزيد على ألفي ريال عماني.

أما الفصل الثالث؛ فقد تناول المشرع من خلاله الجرائم المتعلقة بإساءة استخدام وسائل تقنية المعلومات، وذلك بالمادة (١١) منه؛ حيث عاقب المشرع بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على ثلاثة سنوات، وبغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على خمسة عشر ألف ريال عماني، أو بإحدى هاتين العقوبتين العديد من أوجه التعامل بالشبكة الإلكترونية لإنتاج وسائل إلكترونية لأغراض ارتكاب الجرائم الإلكترونية.

ثم تناول المشرع في الفصل الرابع جرائم التزوير والاحتيال الإلكتروني بالمواد (١٢)، (١٣)؛ حيث جرم في المادة (١٢) الأفعال التي تستخدم فيها وسائل تقنية المعلومات لتزوير البيانات أو المعلومات الإلكترونية والتعامل بها على أنها صحيحة بالسجن مدة لا تقل عن سنة ولا تزيد عن ثلاث سنوات، وبغرامة لا تقل عن ألف ريال عماني ولا تزيد

على ثلاثة آلاف ريال عماني، أو بإحدى هاتين العقوبتين، ثم عاد ليشدد العقوبة في حالتين هما إذا كان من شأن ذلك تحقيق مصلحه لنفس أو الغير أو احداث ضرر بالغير، وكذلك تشدد عقوبة المستعمل إذا استعملها وهو يعلم أنها مزورة لتصبح العقوبة السجن المؤقت مدة لا تقل عن ثلاث سنوات ولا تزيد على خمس عشرة سنة وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد عن خمسين ألف ريال عماني.

ثم تأتي المادة (١٣) لتعاقب بالسجن الذي لا تزيد مدته عن سنة ولا تزيد على ثلاثة سنوات، وبغرامة لا تقل عن ألف ريال عماني، أو بإحدى هاتين العقوبتين في حالة الاحتيال الإلكتروني؛ حيث جرمت صور الأفعال التي تمثل اعتداء على البيانات أو المعلومات الإلكترونية بالتعديل أو التغيير أو الإتلاف أو التشويه، ثم عادت لتشدد العقوبة إذا كان النظام المعلوماتي الذي تم الاعتداء عليه خاصاً بجهة حكومية أو مصرفية أو مؤسسة مالية تصبح العقوبة السجن الذي لا تقل مدته عن ثلاث سنوات ولا تزيد على خمس عشرة سنة، وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرين ألف ريال عماني.

وتعد جريمة الاحتيال الإلكتروني من أخطر الجرائم وأبرزها في إطار الجرائم الإلكترونية؛ لذا لابد من تغليظ العقوبة برفع حديها الأدنى والأقصى، سواء عقوبة السجن أو الغرامة مع الجمع بينهما على سبيل الوجوب والإلزام.

أما الفصل الخامس؛ فقد تناول المشرع من خلاله الجرائم الواقعة على المحتوى، وبموجب المادة (١٤) منه عاقب المشرع بالسجن مدة لا تقل عن شهر ولا تزيد على سنة، وغرامة لا تقل عن مائة ريال ولا تزيد عن ألف ريال عماني، أو بإحدى هاتين العقوبتين، وذلك في حالة الاستخدام غير المشروع للشبكة المعلوماتية في أوجه متعددة للتعامل بغرض الإباحية، ثم يعود المشرع ليشدد العقوبة على هذه الصور من التعامل غير المشروع من خلال استخدام الشبكة المعلوماتية لتصبح العقوبة السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات، والغرامة التي لا تقل عن ألف ريال ولا تزيد عن خمسة آلاف ريال عماني، إذا كان محل المحتوى أو موضوعه يتعلق بالأحداث، ثم عاد المشرع ليشدد العقوبة مرة أخرى بالمادة (١٥) لتصل إلى السجن الذي لا تقل مدته عن

ثلاث سنوات ولا تزيد على خمس سنوات، وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على خمسة آلاف ريال عماني في حالة الاستخدام غير المشروع للتحريض أو المساعدة على الفجور، وإذا وقعت الجريمة على حدث تشدد العقوبة للسجن الذي لا تقل مدته عن خمس سنوات ولا تزيد على عشر سنوات، ثم تناول المشرع تجريم استخدام غير المشروع للشبكة المعلوماتية أو الوسائل الأخرى كالهواتف النقالة في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد ليصبح السجن مدة لا تقل عن سنة ولا تزيد على ثلاثة سنوات، وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على خمسة آلاف ريال عماني، أو بإحدى هاتين العقوبتين بالمادة (١٦)، بينما المادة (١٧) جرم المشرع من خلالها الاستخدام غير المشروع للشبكة المعلوماتية الذي يتعلق بالمساس بالآداب العامة بالسجن مدة لا تقل عن شهر ولا تزيد عن ثلاث سنوات وبغرامة لا تقل عن مائة ريال عماني، أو بإحدى هاتين العقوبتين، وبالمادة (١٨) تناول المشرع تجريم الأفعال التي يقصد بها الابتزاز والتهديد للقيام بعمل أو الامتناع عن عمل لتصبح السجن من شهر ولا تزيد عن ثلاث سنوات، وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني، أو بإحدى هاتين العقوبتين، وتشدد العقوبة لتصبح السجن لا يقل عن ثلاث سنوات ولا يزيد عن عشر سنوات، وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد عن عشرة آلاف ريال عماني، إذا كان التهديد بارتكاب جناية أو جريمة مخلة بالشرف والاعتبار.

والمتأمل في مثل هذه الجريمة يجد أنها من الخطورة التي تهدد المجتمع بأسره، بل تؤدي أحياناً إلى الانتحار في الوقت الذي تتسم فيه العقوبة عليها بالضآلة التي لا تتناسب مطلقاً مع مثل هذا النوع من الجرائم؛ لذا من الضروري تغليظ عقوبتي السجن الغرامة والجمع بينهما.

وبالمادة (٢٠) من القانون عاقب المشرع بالسجن المطلق، وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على مائتي ريال عماني على إنشاء مواقع إلكترونية لأغراض إرهابية، ووصل الأمر بالمشرع العماني إلى حد تشديد العقاب لتصلح العقوبة الإعدام أو السجن المطلق، والغرامة التي لا تقل عن خمسة وعشرين ألف ريال عماني ولا تزيد على مائة ألف ريال عماني للجاني الذي ينشئ موقع إلكتروني للاتجار أو الترويج لبعض

المواد من المخدرات والمؤثرات العقلية المنصوص عليها في الجداول ١،٢،٣،٤ والجدول ١ من المجموعة الثانية، وخفف العقوبة لتصبح السجن المؤقت مدة لا تقل عن عشر سنوات ولا تزيد على خمسة عشرة سنة، وغرامة لا تقل عن عشرة آلاف ريال عماني ولا تزيد على خمسة عشر آلاف ريال عماني، إذا كان القصد هو التعاطي أو تسهيل التعامل فيها في غير الأحوال المصرح بها قانوناً.

وعن العقوبات التكميلية والمتمثلة في المصادرة والغلق؛ فقد نص المشرع على عقوبة المصادرة للأشياء المستخدمة، والأموال المتحصلة من هذه الجريمة بالمادة (٣٢) فقرة أ، وعقوبة غلق الموقع الالكتروني بالفقرة ب من المادة ذاتها[٣٣].

واستمراراً في تنظيم أحكام التجريم في مكافحة الجرائم الإلكترونية؛ فقد عد المشرع العماني أن الإبلاغ عنها من أحد الجناة أو شركائهم للسلطات المختصة قبل الكشف عنها مانعاً من العقاب، بحيث تؤدي هذه المعلومات للكشف عن هذه الجريمة، وذلك تشجيعاً للإبلاغ عن هذه الجرائم، فإذا وقع الإبلاغ عن هذه الجرائم بعد الكشف عنها جاز للمحكمة أن تعفي من العقاب من أبلغ السلطات المختصة منهم إذا أدى هذا الإبلاغ إلى ضبط باقي الجناة[٣٤].

---

[٣٣] نصت المادة (٣٢) "دون الاخلال بحقوق الغير حسن النية على المحكمة ان تحكم في جميع الأحوال بالآتي:

١-مصادرة جميع الأجهزة والأدوات والبرامج وغيرها من الأشياء التي استعملت في ارتكاب جريمة تقنية المعلومات وكذلك الأموال المتحصلة منها.

٢- غلق الموقع الإلكتروني والمحل الذي ارتكبت فيه جريمة تقنية المعلومات او الشروع فيها إذا كانت الجريمة قد ارتكبت بعلم مالكه وعدم اعتراضه ويكون الغلق دائما او مؤقتا المدة التي تقدرها المحكمة في ضوء ظروف وملابسات الجريمة.

٣-طرد الأجنبي المحكوم عليه بعقوبة إرهابية او بعقوبة تأديبية إذا كانت الجريمة شائنة.

[٣٤] نصت المادة (٣٣) على: "يعفى من العقاب كل من بادر من الجناة أو شركائهم إلى إبلاغ السلطات المختصة بمعلومات عن جريمة وقعت بالمخالفة لأحكام هذا القانون قبل الكشف عنها، فاذا تم الادلاء بتلك المعلومات بعد الكشف عنها جاز للمحكمة إعفاؤه من العقاب شريطة أن يترتب على الادلاء بالشهادة ضبط باقي الجناة".

المطلب الثاني

مكافحة الجريمة الإلكترونية

في ظل قانون حماية البيانات الشخصية رقم ٢٠٢٢/٦

تمثل البيانات الشخصية أهمية بالغة في حياة كل فرد من أفراد المجتمع؛ فهي حق لصيق به، أقرته الدساتير والمواثيق الدولية، وأكده النظام الأساسي لسلطنة عمان الصادر بالمرسوم السلطاني رقم ٢٠٢١/٦، فلا شك أن حمايتها يضمن الحفاظ على كرامة الانسان وخصوصيته.

وعدم حماية تلك البيانات التي تمثل للفرد معلومات شخصية قد تعرضه للابتزاز والاحتيال، والعديد من الأفعال الإجرامية التي يمكن أن تقع عليه.

وقد انتهج المشرع العماني سياسة تشريعية في التجريم والعقاب بموجب أحكام هذا القانون.

أولاً- أحكام التجريم في ظل قانون حماية البيانات الشخصية:

عرف المشرع العماني البيانات الشخصية بموجب نص المادة (١) من قانون حماية البيانات الشخصية بأنها: "البيانات التي تجعل شخصاً طبيعياً معرفاً، أو قابلاً للتعريف بطريقة مباشرة، أو غير مباشرة، وذلك بالرجوع إلى معرف أو أكثر، كالاسم أو الرقم المدني أو بيانات المعرفات الإلكترونية أو البيانات المكانية، أو بالرجوع إلى عامل أو أكثر خاص بالهوية الجينية أو الجسدية أو العقلية أو النفسية أو الاجتماعية أو الثقافية أو الاقتصادية".

وفي سبيل حماية تلك البيانات؛ فقد اتبع المشرع العماني سياستي الإلزام والحظر في قانون حماية البيانات الشخصية، وفي حال الإخلال بهما تقع العقوبة على من خالف أحكامه، وذلك على النحو الآتي:

نص المشرع العماني في المادة (٥) من هذا القانون على أن: "يحظر معالجة البيانات الشخصية للطفل إلا بموافقة ولي أمره، ما لم تكن تلك المعالجة لمصلحة الطفل الفضلى، وذلك وفقاً للضوابط والإجراءات التي تحددها اللائحة"[٣٥].

وهو حظر نسبي يتوقف على موافقة ولي الأمر، وذلك للحفاظ على مصلحة الطفل الأولى بالرعاية، والتي لا شك أن الأولى برعايتها ولي أمره.

وفي إطار المحافظة على حق الفرد في الحفاظ على بياناته الشخصية؛ فقد حظر المشرع بموجب المادة (١٠) المساس بالبيانات الشخصية للفرد؛ إلا بموجب موافقة صريحة لصاحب تلك البيانات[٣٦].

---

[٣٥] إلا أن المشرع قد استثنى معالجة بعض البيانات كما في المادة (٣) من القانون لا تسري أحكام هذا القانون على معالجة البيانات الشخصية التي تتم في الأحوال الآتية:

أ – حماية الأمن الوطني، أو المصلحة العامة.

ب – تنفيذ وحدات الجهاز الإداري للدولة وغيرها من الأشخاص الاعتبارية العامة للاختصاصات المقررة لها قانونًا.

ج – تنفيذ التزام قانوني ملقى على عاتق المتحكم بموجب أي قانون أو حكم أو قرار من المحكمة.

د – حماية المصالح الاقتصادية، والمالية للدولة.

هـ – حماية مصلحة حيوية لصاحب البيانات الشخصية.

و – كشف أو منع أي جريمة جزائية بناء على طلب رسمي مكتوب من جهات التحقيق.

ز – تنفيذ عقد يكون صاحب البيانات الشخصية طرفا فيه.

ح – إذا كانت المعالجة في إطار شخصي، أو أسري.

ط – أغراض البحوث التاريخية أو الإحصائية أو العلمية أو الأدبية أو الاقتصادية، وذلك من قبل الجهات المصرح لها القيام بهذه الأعمال، شريطة عدم استخدام أي دلالة أو إشارة تتعلق بصاحب البيانات الشخصية فيما تنشره من بحوث وإحصائيات، لضمان عدم نسب البيانات الشخصية إلى شخص طبيعي معرف، أو قابل للتعريف.

ي – إذا كانت البيانات متاحة للجمهور وبما لا يخالف أحكام هذا القانون.

[٣٦] "لا يجوز معالجة البيانات الشخصية إلا في إطار الشفافية والأمانة، واحترام كرامة الإنسان، وبعد الموافقة الصريحة لصاحب البيانات الشخصية على ذلك".

كما أعطى المشرع صاحب البيانات الشخصية في حال وجود أي مخالفة في معالجة بياناته الشخصية الحق في التقدم بشكوى إلى الجهة المسؤولة بموجب المادة (١٢)[٣٧].

وعن سياسة الإلزام؛ فقد ألزم المشرع العماني بموجب المادة (٢٢) منه المتحكم بالحصول على الموافقة الكتابية لصاحب البيانات الشخصية قبل إرسال أي مادة إعلانية أو تسويقية وذات أغراض تجارية إليه، وذلك على النحو الذي تحدده اللائحة.

كذلك ألزم المشرع المتحكم والمعالج بموجب المادة (١٣) ببعض الضوابط والإجراءات التي يجب الالتزام بها عند معالجة البيانات الشخصية؛ لتحديد المخاطر التي من الممكن أن تقع على صاحب البيانات[٣٨].

بل إن هناك إلزاما وجوبياً على المعالج قبل البدء في معالجة أي بيانات شخصية بأن يخطر صاحبها ببعض البيانات، وذلك بموجب المادة (١٤)، حتى يتمكن الشخص من معرفة المعالج والمتحكم في تلك البيانات، وكذلك ليتمكن من التواصل مع المسؤول عن حماية بياناته الشخصية[٣٩].

---

[٣٧] على أنه: "يجوز لصاحب البيانات الشخصية التقدم بشكوى إلى الوزارة إذا رأى أو اعد أن معالجة بياناته الشخصية لا تتوافق مع أحكام هذا القانون، وذلك طبقا للضوابط والإجراءات التي تحددها اللائحة".

[٣٨] المادة (١٣): "يلتزم المتحكم بوضع الضوابط والإجراءات الواجب الالتزام بها عند معالجة البيانات الشخصية، ويجب أن تشتمل على وجه الخصوص الآتي:

أ – تحديد المخاطر التي قد تقع على صاحب البيانات الشخصية جراء المعالجة.

ب – إجراءات وضوابط نقل وتحويل البيانات الشخصية.

ج – التدابير الفنية والإجرائية لضمان تنفيذ المعالجة وفقا لأحكام هذا القانون.

د – أي ضوابط أو إجراءات أخرى تحددها اللائحة".

[٣٩] المادة (١٤): "يلتزم المتحكم قبل البدء في معالجة أي بيانات شخصية أن يخطر صاحب البيانات الشخصية كتابة بما يأتي:

أ – بيانات المتحكم، والمعالج.

ب – بيانات التواصل مع مسؤول حماية البيانات الشخصية.

ج – الغرض من معالجة البيانات الشخصية، والمصدر الذي جمعت منه.

وكذلك اتبع المشرع سياسة الإلزام كما في المادة (١٥)؛ حيث ألزمت المتحكم والمعالج بالضوابط التي تقررها الوزارة، وكذلك ألزمتهم المادة (١٦) بتعيين مدقق خارجي لمعالجة البيانات بناء على طلب الوزارة.

وكذلك المادة (١٩)؛ حيث جاء فيها ما نصه: "يلتزم المتحكم، عند حدوث اختراق للبيانات الشخصية، يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية، بإبلاغ الوزارة وصاحب البيانات الشخصية عن الاختراق، وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة".

كما ألزمت المادة (٢١) المتحكم بسرية البيانات الشخصية، وعدم نشرها إلا بموافقة مسبقة من صاحب البيانات الشخصية، كما ألزمت المادة (٢٢) المتحكم بالحصول على موافقة كتابية قبل الإعلان أو التسويق.

ثانياً- أحكام العقاب في ظل قانون حماية البيانات الشخصية:

أوضح القانون أنه مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون الجزاء أو أي قانون آخر، يعاقب على الجرائم المبيّنة في هذا القانون بالعقوبات المنصوص عليها فيه، حيث عاقب بموجب نص المادة (٢٥) بغرامة لا تقل عن ٥٠٠ ريال ولا تزيد على ألفي ريال عماني، كل من يخالف أحكام المادة (١٤) من هذا القانون، ويعاقب بغرامة لا تقل عن ألف ريال، ولا تزيد على ٥ آلاف ريال عماني، كل من يخالف أحكام المواد (١٥)، و(١٦)، و(١٧)، و(١٨)، و(٢٠)، و(٢٢) من هذا القانون وذلك بموجب نص المادة (٢٦).

ويعاقب بغرامة لا تقل عن ٥ آلاف ريال، ولا تزيد على ١٠ آلاف ريال عماني، كل من يخالف أحكام المادة (١٣) من هذا القانون وذلك بموجب نص المادة (٢٧)، ويعاقب بغرامة لا تقل عن ١٠ ألف ريال، ولا تزيد على ٢٠ ألف ريال عماني، كل من

د – الوصف الشامل والدقيق للمعالجة وإجراءاتها، ودرجات الإفصاح عن البيانات الشخصية.

هـ – حقوق صاحب البيانات الشخصية بما في ذلك حق الوصول إلى البيانات، وتصحيحها، ونقلها، وتحديثها.

و – أي معلومات أخرى قد تكون ضرورية لاستيفاء شروط المعالجة".

يخالف أحكام المواد (٥)، و(٦)، و(١٩)، و(٢١) من هذا القانون، وذلك بموجب نص المادة (٢٨). ويعاقب بغرامة لا تقل عن ١٠٠ ألف ريال، ولا تزيد على ٥٠٠ ألف ريال عماني، كل من يخالف أحكام المادة (٢٣) من هذا القانون، وذلك بموجب نص المادة (٢٩).

كما عاقب المشرع العماني بموجب نص المادة (٣٠) الشخص الاعتباري بغرامة لا تزيد تقل عن ٥٠٠٠ ولا تزيد على ١٠٠٠٠٠ في حال ارتكاب الجريمة باسمه أو حسابه أو لحساب أحد أعضاء مجلس إدارته أو غيره مما عددتهم المادة إذا تم ذلك بموافقة الشخص الاعتباري أو بتستر منه أو إهمال جسيم.

ويتضح من ذلك أن المشرع قد انتهج سياسة معينة، وهي اعتبار الغرامة هي العقوبة الأصلية الوحيدة التي تطبق على الجاني في حال مخالفته لنصوص قانون حماية البيانات الشخصية، كما أجاز له الحكم بعقوبة تكميلية تتمثل في مصادرة الأدوات المستخدمة في ارتكاب الجريمة، بالإضافة إلى عقوبة الغرامة، وذلك بموجب المادة (٣١).

وقد أعطى المشرع للوزارة الحق في فرض جزاءات إدارية على المخالفات التي يتم ارتكابها بمخالفة أحكام هذا القانون، على ألا تزيد الغرامة الإدارية على ٢٠٠٠ ريال وذلك بموجب المادة (٣٢).

وباستعراض العقوبات السابقة، والتي تعد العقوبة الجزائية الأصلية الوحيدة بها هي الغرامة التي اكتفى بها المشرع؛ إلا أنها تختلف في مقدارها من حيث الحد الأدنى والحد الأقصى بحجم المخالفة التي ارتكبها الجاني لأحكام قانون حماية البيانات الشخصية.

كما يتضح أن المشرع قد أضاف عقوبة تكميلية هي المصادرة للأدوات المستخدمة لارتكاب الجريمة، والملاحظ أن المشرع اعتبرها جوازية وليست وجوبية، وربما كان ذلك على اعتبار أن الجهاز المستخدم أو الأدوات المستخدمة لارتكاب الجريمة ليست ملكاً لمرتكب الفعل، وذلك في الغالب.

ورغم أن صدور قانون حماية البيانات الشخصية كان ضرورة ملحة؛ وحسناً فعل المشرع العماني؛ إلا ان خطورة المعلومات والبيانات الشخصية تستوجب وجود عقوبة السجن كعقوبة رادعة، بالإضافة إلى عقوبة الغرامة، فربما عقوبة الغرامة حتى لو كان المبلغ

المحكوم به يمثل مبلغاً كبيراً؛ إلا أن بعض الأشخاص قد لا يشعر بها لارتفاع مستواه المادي.

لذا نأمل أن تضاف عقوبة السجن في تعديل تشريعي سريع، حتى يحقق الردع الكافي لمن تسول له نفسه، ممن ينطبق عليهم القانون، التعدي على البيانات الشخصية للفرد، وانتهاك خصوصيتها.

ورغم أهمية التشريعات السابق الإشارة إليها في مكافحة الجرائم الإلكترونية؛ إلا أنه وفقاً لمجريات الأمور من انتشار أدوات ووسائل للإجرام الإلكتروني بسرعة متناهية فإننا نأمل سن تشريعات جديدة لاسيما بعد انتشار جرائم الذكاء الاصطناعي، والتي تصل إلى حد ارتكاب الآلة للجريمة، وهو ما يتعين أن يكون هناك تصوراً للمسؤولية الجزائية، وكذلك الإجراءات الجزائية التي من الممكن أن تتخذ في هذه الحالات.

الخاتمـــة

تناول البحث إلقاء الضوء على مدلول الثورة الصناعية، حتى يمكن الوصول إلى أهم المخاطر التي تمثل تحدياً للاستفادة من تلك الثورة؛ حيث تعد الجريمة الإلكترونية أهم المخاطر التي تعد نتاجاً لما أفرزته الثورة الصناعية من تقدم، وقد خرج البحث بمجموعة من النتائج والتوصيات.

أولاً- النتائج:

١- للثورة الصناعية إنجازات تمثل نواحي إيجابية وأخرى تمثل خطراً على المجتمع الإنساني.

٢- للثورة الصناعية الرابعة خصائص تميزها عن الثورات الصناعية الثلاث التي تسبقها.

٣- الجريمة الإلكترونية تعد أخطر الآثار التي ترتبت على الانتشار الواسع لما أنتجته الثورة الصناعية الرابعة.

٤- تدخل المشرع العماني لمكافحة الجريمة الإلكترونية بإصدار قانون مكافحة جرائم تقنية المعلومات رقم ٢٠١١/١٢.

٥- تدخل المشرع العماني بالحفاظ على البيانات الشخصية للفرد، حتى لا يتعرض للانتهاكات التي تمسه في معلوماته الشخصية وخصوصيته بقانون حماية البيانات الشخصية، الصادر بالمرسوم السلطاني رقم ٦/ ٢٠٢٢.

٦- عدم كفاية التشريعات الحالية لمواجهة خطر الجرائم الإلكترونية، لاسيما بعد توجه السلطنة للتحول الرقمي، واستخدام الذكاء الاصطناعي في بعض الجوانب الحياتية.

ثانياً- التوصيات:

١- نوصي بضرورة تعديل تشريعي يتناسب مع التطور السريع في أشكال وحجم الجرائم الإلكترونية التي أصبحت أكثر خطراً من ذي قبل لا سيما ما يتعلق بجرائم الذكاء الاصطناعي.

٢- نوصي بزيادة الوعي بمخاطر الجرائم الإلكترونية عن طريق نشر الثقافة القانونية.

٣- تعديل بعض النصوص القانونية بقانون مكافحة جرائم تقنية المعلومات لعدم تناسب عقوبتها مع حجم الجرم المرتكب كما في المادة (١٨) الخاصة بالابتزاز الإلكتروني.

٤- اعتبار السجن عقوبة أصلية لبعض جرائم انتهاك قانون حماية البيانات الشخصية.

٥- تشديد عقوبة الموظف الذي يرتكب جريمة الابتزاز الإلكتروني عن الشخص العادي.

٦- تزويد المناهج الدراسية بمناهج حديثة لنشر الثقافة الإلكترونية، ليس كمعلومات فقط في مقرر للحاسوب بل تعليم الطلاب وتدريبهم على كيفية التعامل مع بعض البرامج الذكية، حتى لا يقعوا فريسة لأي جريمة إلكترونية.

المراجـــع

أولاً- الكتب العامة:

- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الجديد، ٢٠١٣م.
- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، المنصورة، مصر، ٢٠١٥م.
- محمود أحمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة عمان، ٢٠٠٥م.
- هدى حامد قشقوش: جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، ١٩٩٢م.
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٩م.
- ناير نبيل عمر، الحماية الجنائية للمحل الالكتروني في الجرائم المعلوماتية، دار الجامعة الجديدة، ٢٠١٢م.
- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، ٢٠٠٧م.

ثانياً- الرسائل العلمية:

- أشرف بن عبد الله الضويحي، المساهمة في الجرائم المعلوماتية المتعلقة بالاعتداء الشخصي، رسالة ماجيستير، لجنة ملخصات الأبحاث القضائية بالجمعية العلمية القضائية السعودية، العدد الثالث، ١٤٢٨-١٤٢٩هـ.
- أمجد حسن مرشد الدعجة، استراتيجية مكافحة الجرائم المعلوماتية، رسالة ماجيستير، جامعة ام درمان الإسلامية، ٢٠١٤م.
- ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، رسالة ماجيستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، ٢٠١٢م.

ثالثاً- الدوريات والأبحاث العلمية:

- آسيا بعضي، الثورة الصناعية الرابعة، مجلة الاقتصاد والتنمية المستدامة، المجلد٥، العدد٢، ٢٠٢٢م.
- اسراء جبريل رشاد مرعي: الجرائم الإلكترونية، الأهداف – الأسباب – طرق الجريمة ومعالجتها، المركز العربي للدراسات الاستراتيجية والاقتصادية والسياسية، بحث منشور على الموقع الإلكتروني:

https://democraticac.de/?p=35426

- علي أسعد وطفة، الثورة الصناعية الرابعة تحديات أم فرص، جامعة الكويت، ٢٠١٩م.
- هيئة تحرير مجلة الارشاد النفسي بجامعة عين شمس، تداعيات الثورة الصناعية الرابعة، العدد ٦٧، ٢٠٢١م.
- لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها والية مكافحتها، مجلة الميزان للدراسات الإسلامية والقانونية، ٢٠١٦/٢٠١٧م.

https://portal.arid.my/Publications/e1788f58-0853-47.pdf

- مهند وليد إسماعيل، التنظيم القانوني للجريمة الإلكترونية، مجلة العلوم القانونية والسياسية، المجلد (١١)، العدد (١) السنة (٦)، ٢٠١٦م.

رابعاً- المواقع الالكترونية:

- https://www.oman.om/home-page
- https://www.qscience.com/content/journals/10.5339/jist.2020.2?crawler=true
- https://www.researchgate.net/publication/349105626_althwrt_alsnayt_alrabt_frs_wthdyat
- https://www.omandaily.om
- https://omannews.gov.om/topics/ar/3/show/409487/