السياسة العقابية التي اتَّبعها المشرِّع العُماني في قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم 12 / 2011

The penal policy adopted by the Omani legislator in the Anti-Cyber and Information Technology Crimes Law issued by Royal Decree No. 12/2011

د. خليل بن حمد البوسعيدي: كلية الحقوق، جامعة الشرقية، سلطنة عمان

Dr. Khalil bin Hamad Al Busaidi: College of Law, Al Sharqiya University, Sultanate of Oman

Email: Khalilalbusaidi6866@hotmail.com

الملخص:

هدفت الدراسة للتعرف على السياسة العقابية التي اتَّبعها المشرِّع العُماني في تجريم الأفعال المرتكبة في إطار جرائم تقنية المعلومات، وكذلك استعراض ملامح هذه السياسة العقابية في سلطنة عمان، وتلمس الفلسفة العقابية التي اتَّبعها المشرِّع، وبيان أنواع الجرائم التي شملها القانون والعقوبات المقررة لها. ولتحقيق أهداف الدراسة فقد اعتمد الباحث على المنهج الوصفي المدعَّم بالجوانب التاريخية لصدور التشريعات في سلطنة عمان، مع استعراض النصوص القانونية الواردة في قانون مكافحة جرائم تقنية المعلومات بصفة خاصة. وخلصت الدراسة إلى مجموعة من النتائج أبرزها أن التجريم في أي دولة هو نتاج تفاعل الكثير من العناصر التي تشكِّل في مجملها التوجه العام للدولة في سياسة التجريم وسياسة العقاب على حد سواء، وقد خطَت سلطنة عمان خطواتٍ واسعةً في تجريم الأفعال التي تقع تحت مظلة قانون مكافحة جرائم تقنية المعلومات، ومن خلال هذه القوانين نلاحظ ملامح التشديد في العقوبة في تغليظ العقوبات السالبة للحرية ورفع العقوبات المالية والظروف المشددة للعقاب، وكذلك إضافة جرائم جديدة في التجريم، أما ملامح التخفيف فتمثلت في تخفيف مدة العقوبة السالبة للحرية والظروف المخففة والتخيير فيما بين الجمع بين العقوبات الحبسية والغرامات، وتخفيف العقوبة في حالة الإبلاغ عن الجريمة. وأوصت الدراسة بضرورة إضافة التدابير العقابية ضمن العقوبات الواردة في القانون، وكذلك مراجعة العقوبات بصورة دائمة ومستمرة لتتوافق مع واقع الجريمة وتنوعها وطنيًّا وعالميًّا.

الكلمات المفتاحية: السياسة العقابية، ملامح التشديد والتخفيف، جرائم تقنية المعلومات، الجرائم الإلكترونية.

Abstract:

The study aimed to identify the penal policy adopted by the Omani legislator in criminalizing acts committed in the context of information technology crimes. In addition to reviewing the features of this penal policy in the Sultanate of Oman, and handling the penal philosophy adopted by the legislator. Moreover, indicating the types of crimes in the law and the penalties determined for them. The researcher used the descriptive approach to achieve the objectives of the study, which supported by the historical aspects of the legislation issued in the Sultanate of Oman, with a review of the legal texts in the Anti-Cyber and Information Technology Crimes Law in particular. The study concluded with a set of results, the most important is that criminalization in any country comes as a result of the interaction of many elements that collectively constitute the general orientation of the state in both criminalization and punishment policy. The Sultanate of Oman has taken great steps in criminalizing acts that fall under the umbrella of the Anti-Cyber and Information Technology Crimes Law. Through these laws, the restriction features of the penalty is noted by increasing and aggravating of freedom deprivation penalties, increasing financial penalties and increasing punishment circumstances. as well as adding new types of crimes in criminalization. As for the features of abatement, they are represented in mitigating the duration of the freedom deprivation's penalty, the moderating circumstances and the preference, which is done by combining prison sentences and fines, and mitigating the penalty in the case of reporting the crime. The study recommended the necessity of adding penal processes within the penalties issued in the law, as well as permanently and continually reviewing the penalties to nationally and globally conform to the reality of crime and its diversity.

Keywords: penal policy, features of aggravation and mitigation, information technology crimes, electronic crimes.

الإطار المنهجي للدراسة

المقدمة:

تُعدُّ ثورة المعلومات والتكنولوجيا التي يشهدها العالم منذ فترة ليست بالطويلة ذات أبعاد إيجابية وسلبية على حد سواء، تنعكس على المجتمعات البشرية كافة، فالجانب الإيجابي يتمثل في التطور الحضاري والتقدم التقني والإلكتروني في شتي مجالات الحياة، ومع هذا الجانب الإيجابي كان هنالك جانب سلبي لهذا التطور يتمثل في ظهور الجرائم الإلكترونية، التي تؤدي إلى اختراق أجهزة الحاسب الآلي والهواتف والأنظمة الإلكترونية والأضرار بها، لذا تصدت كافة الدول لهذه الجرائم من خلال بسط حمايتها الفنية والقانونية، ومعاقبة مرتكبي هذه الجرائم، فأصدرت معظم الدول قوانين تتعلق بالأمن السيبراني، ومنها سلطنة عمان التي أصدرت قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2011/12).

اشتمل هذا المرسوم على الإجراءات القانونية الواجب اتخاذها في حالات التعدي على سلامة وسرية البيانات والمعلومات الإلكترونية والنظم المعلوماتية بكافة أشكالها وأنواعها، وإساءة استخدامها، وجرائم التزوير والاحتيال المعلوماتي، وجرائم المحتوى والتعدي على البطاقات الائتمانية، فالمشرِّع العماني قد اعتمد في تجريم هذه الأفعال وتحديد العقوبات المناسبة لها من خلال الاتفاقيات الدولية والصكوك العالمية، كاتفاقية "بودابست" لمكافحة الجرائم المعلوماتية، واستفاد كذلك من التجارب والممارسات العالمية والإقليمية في هذا الصدد، وأيضًا من خلال التجربة التي اكتسبتها السلطنة في مكافحة هذه الجرائم.

وكان لهذا التنوع، الذي اتَّبعه المشرِّع العماني عند وضع قانون مكافحة جرائم تقنية المعلومات معتمِدًا في ذلك على القوانين الدولية، الأثرُ الكبيرُ في تغيير السياسة العقابية التي اتَّبعها، من خلال تشديد العقوبات في بعض الجرائم وتخفيفها في جرائم أخرى، مع ما صاحب ذلك من تأثر بالتشريعات الأخرى في هذا الجانب.

إشكالية الدراسة:

تتمثل إشكالية الدراسة في بيان مدى التطور التشريعي في العقوبات المحددة لجرائم تقنية المعلومات، والأسباب التي دعت المشرِّع إلى تشديد بعض العقوبات والتخفيف في بعضها الآخر، مع بيان توجه المشروع العماني مستقبلًا من خلال الإضافات التشريعية والتوسع في الأفعال المجرَّمة في مجال تقنية المعلومات، ومدى استفادة المشرِّع من الاتفاقيات الدولية والقوانين المقارنة في هذا الشأن.

تساؤلات الدراسة:

ستجيب هذه الدراسة على عدة تساؤلات هي:

- ما ملامح السياسة العقابية في قانون مكافحة جرائم تقنية المعلومات مقارنةً بالقوانين الجنائية السابقة التي تعرضت للجرائم الإلكترونية؟
- ما أوجه تشديد العقوبات في قانون مكافحة تقنية المعلومات؟
- ما أوجه تخفيف العقوبات في قانون مكافحة تقنية المعلومات؟

منهج الدراسة:

تعتمد هذه الدراسة المنهج الوصفي التحليلي المدعَّم بالجوانب التاريخية لصدور التشريعات في سلطنة عمان، مع استعراض النصوص القانونية الواردة في قانون مكافحة جرائم تقنية المعلومات بصفة خاصة، والنصوص القانونية في القوانين ذات العلاقة بالدراسة، وعمل المقارنات الإيضاحية للوصول إلى أهداف الدراسة والإجابة على تساؤلاتها.

أهداف الدراسة:

تهدف هذه الدراسة إلى بحث واستعراض ملامح السياسة العقابية في قانون مكافحة جرائم تقنية المعلومات في سلطنة عمان، وتلمس الفلسفة العقابية التي اتَّبعها المشرِّع، وبيان أنواع الجرائم التي شملها القانون والعقوبات المقررة لها ومقارنتها بالقوانين الجنائية الأخرى في ذات الإطار بحسب ما تتطلبه الدراسة، وتوضيح التدرج التشريعي الذي اتَّبعه المشرِّع العماني في وضع العقوبات لجرائم تقنية المعلومات والتغييرات التي طرأت في هذا الجانب ومقارنة ذلك مع التجارب التشريعية المقارنة.

أهمية الدراسة:

ستوضح هذه الدراسة السياسة والفلسفة العقابية التي اتَّبعها المشرِّع العماني عند إصداره لقانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2011/12)، مقارنةً بالسياسة العقابية التي اتَّبعها المشرِّع في القوانين الصادرة قبل هذا القانون في مجال مكافحة الجرائم الإلكترونية ذاته، وهي الفصل الثاني مكرر من الباب السابع من قانون الجزاء الصادر بالمرسوم السلطاني رقم (7 / 74)، وتلمس أوجه هذه السياسة العقابية من خلال الوقوف على غايات التشديد والتخفيف في العقوبات، بما يضمن تحقيق أهداف الردع والزجر لمرتكبي جرائم تقنية المعلومات، واستعراض النصوص القانونية العقابية في القانون، ومقارنتها مع التجارب التشريعية المقارنة.

وقد تكمن أهمية هذا الموضوع كذلك من خلال قلة الدراسات التي تسلط الضوء على السياسات العقابية في التشريعات العمانية بصفة عامة، وقلة الدراسات حول قانون مكافحة جرائم تقنية المعلومات في السلطنة بصفة خاصة.

الدراسات السابقة:

لم يقف الباحث على دراسات سابقة في ذات موضوع البحث بالتحديد، إذ إن أغلب الدراسات السابقة كانت تتحدث عن السياسة العقابية بصفة عامة من خلال النظريات العلمية والفلسفة القانونية في علم العقوبات، أما بعض الدراسات فكانت تتحدث عن السياسة العقابية في جرائم مختلفة عن جرائم تقنية المعلومات، والبعض الآخر يتحدث عن جرائم المعلومات في إطاره المحلي فقط، دون التطرق إلى قانون مكافحة جرائم تقنية المعلومات في السلطنة، وسنستعرض دراستين من الدراسات المذكورة:

1) المعمرى ومصطفى (2021م): دراسة موجزة حول الجرائم المعلوماتية وتعريفها وأهمية تجريمها مجتمعيًّا وعالميًّا

تتحدث هذه الدراسة عن قانون مكافحة جرائم تقنية المعلومات في السلطنة وفي العالم بصفة عامة، وتقييم دور المشرِّع العماني عند وضع قانون مكافحة جرائم تقنية المعلومات، إذ تشيد الدراسة بالتوجه الذي انتهجه المشرِّع في هذا القانون من حيث شمولية تعريف جرائم تقنية المعلومات، وأنه لا يغل يد الادعاء العام والمحكمة إذا ظهرت تقنيات جديدة ترتكب بواسطتها الأفعال المجرمة، بالتالي لن تجد أجهزة العدالة نفسها محصورة في تعريف محدود بوسائل معينة خاصة وأن التطور التقني في تجدد مستمر. ويلاحظ أن هذه الدراسة تناقش جرائم تقنية المعلومات من خلال وجه مختلف تمامًا عن الدراسة التي نحن بصددها، فالباحثان قد ركَّزا على مناقشة القانون والتعليق عليه بصورة مباشرة، أما دراستنا هنا فتركز على السياسة العقابية ومدى التطور الذي تم في تحديد العقوبات والتغييرات التي تمت في هذا الجانب.

2) دراسة الدسوقي (2005م): الحماية الجنائية لسرية المعلومات الإلكترونية (دراسة مقارنة).

تتحدث هذه الدراسة عن الجرائم الإلكترونية المستحدَثة، وكيفية مكافحة هذه الجرائم، وما يحتاجه المشرِّع عند وضع تنظيم قانوني لمكافحة جرائم تقنية المعلومات والجرائم الماسة بسرِّية المعلومات الإلكترونية على وجه التحديد، إذ ركَّز الباحث في دراسته على استعراض النظام القانوني البحريني في مواجهة الجرائم الماسة بسرِّية المعلومات الإلكترونية في حالة وقوعها بحالته التي هو عليها، ومدى حاجته إلى التطوير والتعديل وصور الأفعال الإجرامية لتلك الجرائم وسبل مكافحتها. ويتضح من خلال استعراض هذه الدراسة أنها ركزت على جانب معين من جرائم تقنية المعلومات،

وهي الجرائم المتعلقة بالسرّية الإلكترونية، كما أن الباحث قد ركز في دراسته على دولة البحرين ونظامها القانوني، وابتعدت الدراسة كثيرًا عن السياسة العقابية للجرائم المعلوماتية، ولذلك يتبين الفارق الكبير بين هذه الدراسة والدراسة التي نحن بصددها هنا.

تقسيمات الدراسة:

- المبحث الأول: التجريم والعقاب في جرائم تقنية المعلومات في السلطنة.
- المبحث الثاني: ملامح السياسة العقابية التي اتَّبعها المشرّع العماني في قانون مكافحة جرائم تقنية المعلومات.
- الخاتمة والتوصيات.

المبحث الأول: التجريم والعقاب في جرائم تقنية المعلومات في السلطنة

تُعدُّ الجريمة ظاهرةً اجتماعيةً يرتبط وجودها بوجود المجتمعات، فمتى وُجِدت المجتمعات وُجِد الأفراد برغباتهم وأهوائهم وأهدافهم المختلفة التي قد تتضارب وتتعارض أحيانًا، مما يجعل البعض يرى في الاعتداء على الآخرين سبيلًا لتحقيق أهدافه الخاصة، فالجريمة قديمةٌ قدم الوجود الإنساني، بالتالي تعرَّف الجريمة بأنها كل سلوك أو امتناع عن سلوك يُخالِف قاعدةً شرعيةً أو نظاميةً وُضِعت لتنظيم سلوك الإنسان في مجتمعه[1]، وعليه فإن فكرة الجريمة لا تتغير في جوهرها بل تتغير صورها وتتعدد بحسب المصدر الذي وضع الأوامر والأنظمة.

وفي المقابل تعرَّف العقوبة بأنها إجراء يستهدف إنزال آلام بالفرد من قبل السلطة المختصة بمناسبة ارتكاب جريمة[2]، بالتالي تتنوع العقوبات بحسب أنواع الجرائم، وهنالك العقوبات الأصلية مثل الإعدام والسجن والغرامة، والعقوبات التبعية مثل الحرمان من الحقوق المدنية ومنع مزاولة مهنة معينة وغيرها، وعليه سنتحدث في هذا المبحث عن مفهوم السياسة العقابية في المطلب الأول، وفي المطلب الثاني سنتحدث عن القوانين العمانية الصادرة في مجال مكافحة جرائم تقنية المعلومات والعقوبات الواردة فيها.

المطلب الأول: تعريف مصطلح السياسة العقابية:

دول العالم قاطبة تسعى إلى حماية نفسها من الجريمة، وتعمل بجهد كبير على الحد من انتشارها وذلك عبر سن القوانين والتشريعات، من خلال انتهاج سياسات تهدف إلى ردع كل ما من

[1] مصطفى البيطار (2016): أصول علمي الإجرام والعقاب، جدة: مكتبة القلم، ص11.
[2] هشام شحاته إمام (2007): دروس في علم العقاب، القاهرة: دار الفكر، ص 17.

شأنه أن يعكر صفو الأمن والأمان الذي تعيشه المجتمعات، كل ذلك يأتي في إطار سياسات عقابية مدروسة ومخطط لها بصورة واضحة تتفق مع واقع انتشار الجريمة ومكافحتها.

وعليه يمكن القول إن السياسة العقابية[1] بصورة عامة هي الكيفية التي ينبغي بها مواجهة الظاهرة الإجرامية وذلك بشكل يكفل حماية المجتمعات ومنع الجريمة أو الحد منها بصورة كبيرة، بالتالي فإن علم السياسة العقابية يسلِّم بحقيقة الظاهرة الإجرامية في المجتمع ويتناولها بالدراسة والتحليل، ومن ثم يضع الاستراتيجيات المناسبة للحد من الجريمة عن طريق الجزاء الجنائي.

وقد حَوَت الكتب والدراسات الكثير من التعريفات لمصطلح السياسة العقابية، منها أن هذه السياسة تبحث في أغراض الجزاء الجنائي، وتحدِّد أفضل الأساليب التي تنفي هذا الجزاء لتحقق أغراضه[2]، وأن السياسة العقابية تنصبُّ أساسًا على تنفيذ الجزاء الجنائي السالب للحرية، وأن تطبيقه قد يستغرق حياة المحكوم عليه، بهدف الردع العام والردع الخاص وبسط الأمن، ويكون ذلك من خلال دراسة الجزاء الذي يوقع على المحكوم عليهم والآثار المترتبة على هذا الجزاء، إلا أن هذا التعريف باقتصاره على الجزاء السالب للحرية قد أستبعد الأنواع الأخرى من الجزاءات والعقوبات المستحدَثة كالتدابير الاحترازية، فصور الجزاء منها ما هو تقليدي ومنها ما هو مستحدَث يتفق مع تطور المجتمع وتطور الفكر القانوني فيه[3].

ويرى بعض الباحثين أن السياسة العقابية مجموعة من القواعد تحدِّد أساليب تنفيذ العقوبات والتدابير الاحترازية على نحو من شأنه أن يحقق أغراضها، وهذا التعريف يشير إلى عنصرين: الأول أن السياسة العقابية تهتم بدراسة العقوبة والتدبير الاحترازي، والثاني أن السياسة العقابية تنفِّذ الجزاء الجنائي بشكل يكفل تحقيق أغراض العقوبة العامة والخاصة[4].

---

[1] "في الشريعة الإسلامية تُعرَّف السياسة العقابية أو السياسة الجنائية بأنها "القانون الموضوع لرعاية الآداب والمصالح وانتظام الأحوال". وكذلك "ما يفعله الحاكم لمصلحة العامة من غير ردود في الشرع". فهي لا تخرج عن تحقيق مقصدين: الأول جلب المصالح والثاني درء المفاسد"، فايزة رزوقي وبوراس عبد القادر(2021م): السياسة الجنائية المعاصرة بين أنسنة العقوبة وتطوير قواعد العدالة، الجزائر، جامعة ابن خلدون، بحث علمي منشور في مجلة الحقوق والعلوم الإنسانية، ص249.

[2] خوري عمر (2008م): السياسة العقابية في القانون الجزائري، جامعة الجزائر، رسالة دكتوراه، ص 9.

[3] السنيدي، عبد العزيز سالم(2018م): السياسة العقابية للمشرِّع الإماراتي في مواجهة الجرائم المعلوماتية، جامعة الامارات، رسالة ماجستير غير منشورة، ص 7.

[4] محمود نجيب حسني (1976): علم العقاب، ط1976، القاهرة: دار النهضة العربية، القاهرة، ص 2.

وفي نظر الباحث أن هذا التعريف هو الأرجح، وذلك على أساس أن السياسة العقابية تهتم بدراسة العقوبة دونما إغفال للتدابير الاحترازية، وفلسفة علم الجريمة والعقاب، فالعقوبة بذلك تشمل الردع العام والخاص الذين يتطلب توفرهما في العقوبة المحددة للفعل الإجرامي[1].

المطلب الثاني: القوانين العمانية الصادرة في مجال مكافحة جرائم تقنية المعلومات والعقوبات الواردة فيها

تشهد السلطنة ثورة هائلة في نظم المعلومات، إذ تتوسع هذه النظم وتتشكل بصورة دائمة ومستمرة، وبالتأكيد مع هذا الانتشار الواسع تظهر الجريمة الإلكترونية، التي تتطلب إصدار قوانين تكافح الجريمة الإلكترونية وتحمي الأفراد وبياناتهم و أجهزتهم الإلكترونية والنظم التقنية والتطبيقات والبرمجيات من أي اختراقات، وتحمي بذلك المجتمع وأفراده من انتهاك الخصوصية أو الاستغلال، وهذا ما يضمنه المرسوم السلطاني رقم (2011/12) الذي يقضي بأن يُصدر قانون مكافحة جرائم تقنية المعلومات، ويتضمن خطوات تُتَّخَذ وفق القانون في حال:

- حدوث تَعَدٍّ على خصوصية البيانات الإلكترونية والأنظمة التقنية وسرِّيَّتها بصورها كافة.
- أن يُساء استعمال الأجهزة الإلكترونية والأنظمة التقنية والنظم المعلوماتية.
- أن تُرتَكَب عمليات احتيالية أو عمليات تزوير متعلقة بالبيانات والمعلومات الإلكترونية
- أن تُرتَكَب جريمة متعلقة بمحتوى إلكتروني.
- حدوث تَعَدٍّ على بطاقات الائتمان.

وقد اعتمد المشرِّع العماني عند إصداره لهذا القانون على اتفاقية الجرائم الحاسوبية، والمعروفة أيضًا بِاسم اتفاقية "بودابست" بشأن جرائم الإنترنت أو اتفاقية "بودابست"[2]، وكذلك اعتمد على التشريعات والقوانين الاسترشادية عالميًّا وعربيًّا فيما يتعلق بمجال الجرائم الإلكترونية وجرائم الإنترنت، إيمانًا منه بامتلاك المواطنين العُمانيين كافةً حق استعمال الحواسيب الآلية والإنترنت والأجهزة التقنية والنظم المعلوماتية استعمالًا سليمًا آمنًا، وكي يعمل على تشكيل سلسلة تتكامل عالميًّا وبقية دول العالَم في مجال مكافحة الجريمة الإلكترونية، وعلى تعزيز التعاون في هذا المجال على صعيد الدول،

[1] السنيدي، مرجع سابق، ص 8.

2 صدرت اتفاقية "بودابست" في 23 نوفمبر 2021م، وهذه الاتفاقية تُعَدُّ أول معاهدة دولية بشأن الجرائم المرتكبة عبر الإنترنت وشبكات الكمبيوتر الأخرى، وهدفها الرئيس، المنصوص عليه في الديباجة، هو اتباع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من الجرائم الإلكترونية، لا سيما من خلال اعتماد التشريعات المناسبة وتعزيز التعاون الدولي. انظر الرابط التالي: https://cutt.us/xnS4H

من أجل خَفض نسب الجريمة الإلكترونية في عُمان، ولفتح باب أكثر اتساعًا للاستعمالات التقنية والتعامل الآمن مع الأجهزة المرتبطة بالشبكة العالمية للمعلومات (الإنترنت)[1].

كما أن السلطنة لديها استراتيجية طويلة المدى تتعلق بتحسين بيئة الأعمال الإلكترونية، إذ تتضمن هذه الاستراتيجية مجموعةً من التوجيهات والإجراءات والممارسات المتعلقة بالمجال الإلكتروني، بالإضافة إلى معايير نظام إدارة أمن المعلومات، ويسعى هذا الإطار إلى حماية المعلومات والإشراف عليها وفق إجراءات معينة يمكن للجهات الحكومية تنفيذها[2].

ويهدف أمن المعلومات إلى حماية أصول المعلومات من الدخول غير المصرح به والتغيير ما فيها، سواء أكان ذلك في مرحلة تخزين البيانات أو خلال معالجتها أو نقلها، كما يشكِّل هذا الإطار مرجِعًا أساسيًّا لوضع الخطط من أجل أن يضمن أن تستمر الأعمال المرتبطة بأمن البيانات والمعلومات الإلكترونية وتقييم ما تواجهه مؤسسات الدولة الحكومية من مخاطر ووضع حلول لها، ويقدِّم هذا الإطار العديد من الخدمات للقطاع العام والخاص، مثل خلق بيئة آمنة عن طريق حماية البيانات والمعلومات من الاختراق، وتقليل عدد المخاطر والتهديدات الداخلية والخارجية، وبناء الثقة بين كل من الموظفين والعملاء في المعاملات التجارية والوقاية، والحد من الحوادث والتهديدات المتعلقة بأمن المعلومات، وإيجاد حلول للمشاكل والحوادث المتعلقة بأمن المعلومات، وتبني التطوير المستمر في إجراءات أمن المعلومات لضمان الدخول الآمن للمستخدمين للاستفادة من الخدمات الحكومية الإلكترونية [3].

وضمن الإجراءات التي تتخذها عُمان من أجل مكافحة الجرائم المعلوماتية وجرائم أمن البيانات الإلكترونية، جرى تجريم الأفعال الجرمية المتعلقة بالبيانات والمعلومات والأنظمة الإلكترونية من خلال أحد الفصول الذي جرت إضافته لقانون الجزاء الخاص بسلطنة عمان الذي صدر بحسب المرسوم السلطاني رقم (74/72)، إذ أضيف الفصل رقم (2) مكرر من الباب رقم (7) من قانون الجزاء العماني الخاص بمكافحة جريمة الحواسيب الآلية، ويُعَدُّ ذلك الفصل بمثابة التشريع العربي الأول من نوعه في مجال التصدي لظواهر الجريمة المعلوماتية[4]، إذ تضمن ذلك التشريع على 5 مواد: (276 مكرر)، و(276 مكرر/1)، و(276 مكرر/2)، و(276 مكرر/3)، و(276 مكرر/4)، تضمنت تجريم الاختراق الإلكتروني والتجسس الإلكتروني والاعتداء على الخصوصية الإلكترونية

1 محمد ناصر الهزاني (2018): المسؤولية الجنائية عن انتهاك الفضاء السيبراني، الرياض، جامعة نايف للعلوم الأمنية، رسالة ماجستير غير منشورة، ص 90.

2 موقع (عماننا) البوابة الإلكترونية للخدمات الحكومية الإلكترونية، انظر الرابط التالي: https://cutt.us/VNdtS

3 المرجع السابق.

4 الموقع الإلكتروني الخاص بهيئة تقنية المعلومات، انظر الرابط التالي: https://2u.pw/Wp6W1

والتزوير الإلكتروني والإتلاف المعلوماتي، والاعتداء على البرامج الحاسوبية والاعتداء على البيانات المرسلة عبر الشبكة وتزوير البطاقات الإلكترونية واستعمالها وقبول التعامل بها، والتعامل مع البطاقات مع العلم بعدم وجود رصيد فيها واستعمالها بعد انتهاء صلاحيتها واستعمال الغير لها، وفي عام 2011 ونتيجة لصدور قانون مكافحة جرائم تقنية المعلومات ألغي هذا الفصل من قانون الجزاء.

بعد ذلك تم إصدار تشريع خاص بمكافحة جريمة المعلومات الإلكترونية بحسب المرسوم السلطاني رقم (2011/12)، وقد تم فيه إفراد قانون خاص لجريمة التقنية والمعلومات ومستقل عن قانون الجزاء، تضمن (35) مادة اشتملت على توسع كبير في الأفعال الجرمية الإلكترونية، وقسم القانون إلى سبعة فصول، جاء الفصل الأول متضمنًا التعريفات والأحكام العامة، وجاء الفصل الثاني مخصصًا للجرائم المتعلقة بحدوث تَعَدٍّ على البيانات والمعلومات الموجودة إلكترونيًّا أو على أنظمة المعلومات وعلى سريتها وسلامتها، وقد جاء الفصل الثالث مخصَّصًا للجرائم التي تحدث عندما يُساء استعمال أدوات وأجهزة وأنظمة المعلومات الإلكترونية، وقد جاء الفصل الرابع مخصَّصًا لجرائم الاحتيال والتزوير الإلكتروني، وقد جاي الفصل الخامس مخصَّصًا للجرائم المتعلقة بمحتوى إلكتروني، وقد جاء الفصل السادس مخصَّصًا للجرائم المتعلقة بأن يحدث تَعَدٍّ على بطاقات الائتمان، والفصل السابع تضمن أحكامًا ختامية.

المبحث الثاني: ملامح السياسة العقابية التي اتَّبعها المشرِّع العماني في قانون مكافحة جرائم تقنية المعلومات:

نَصَّ التشريع الخاص بمكافحة جرائم تقنية المعلومات الذي صدر بحسب المرسوم السلطاني رقم (2011/12) على عديد من السلوكيات التي تتعلق بالمعلومات الإلكترونية والتطبيقات التقنية البرمجية، وكان ذلك التشريع تشريعًا شاملًا اتسع ليشمل الجريمة الإلكترونية وتفاصيلها كافة بشكل جيد، إذ إنه قد استوعب أغلب الأفعال الجرمية التي تعرضت لها القوانين العالمية، فجرَّم أفعال التعدي على سلامة نظم المعلومات التقنية والبيانات الإلكترونية وتوفيرها وسلامتها في 7 مواد شاملة متسعة، إلى جانب أنه نصَّ على تجريم السلوكيات الجرمية المرتبطة باستخدام وسائل تقنية المعلومات في مادة واحدة، ومن ثم تطرَّق القانون إلى جرائم التزوير والاحتيال الإلكتروني، ونظَّم هذا الجانب في مادتين شاملتين، وخصَّص بعد ذلك ثلاثة عشر مادةً لجرائم المحتوى، وفي الأخير تطرَّق إلى جرائم التعدي على البطاقات المالية في مادة واحدة فقط، وعليه فإن القانون قد تضمَّن خمسة وثلاثين مادةً في مكافحة جرائم تقنية المعلومات.

وأغلب هذه المواد تضمنت عقوبات مختلفة ومتفاوتة القوة، فمن حيث أنواع العقوبات التي تضمنها القانون فكانت لا تخرج عن السجن أو الغرامة أو الإعدام، إذ إن القانون لم يتضمن بصورة

خاصة العقوبات التبعية أو التدابير الاحترازية مثل الحرمان من الحقوق المدنية، وغيرها من أنواع العقوبات التبعية.

ومن الملاحظ أن غالبية المواد الواردة في التشريع السابق تكون بدايتها بلفظ "يعاقب"، مما يبيّن المنهاج البيّن المباشر المتَّبع من قبل تشريع سلطنة عمان في سياساته العقابية في عذا التشريع، وإن أخفَّ العقوبات التي وردت في هذا التشريع ما ورد في مادته الثالثة التي تنص على أنه "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على أشهر وبغرامة لا تقل عن 100 ريال عماني ولا تزيد على 500 ريال عماني أو بإحدى هاتين العقوبتين"[1]، وأيضًا ما ورد في المادة رقم (28) من هذا التشريع من أنه "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على 6 أشهر وبغرامة لا تقل عن 500 ريال عماني ولا تزيد على 1000 ريال عماني أو بإحدى هاتين العقوبتين"[2].

وإن أشد العقوبات التي وردت في نضوض هذا التشريع كانت في المادة رقم (25) وجاء فيها أنه "يعاقب بالإعدام أو بالسجن المطلق وبغرامة لا تقل عن 25,000 ريال عماني ولا تزيد على 100,000 ريال عماني"، وفي المادة رقم (20) المتعلقة بأن يُسجَن المجرم سجنًا مطلقًا وجاء فيها أنه "يعاقب بالسجن المطلق وبغرامة لا تقل عن 100,000 ريال عماني ولا تزيد على 100,000 ريال عماني"[3]. وبذلك يمكننا ملاحظة الفرق الشاسع بين العقوبتين الأخف والأعلى الواردة في التشريع العماني وذلك بناءً على نوع الفعل الذي يقع في إطار الجرائم الإلكترونية.

وعليه سنتطرق الآن للحديث عن ملامح التشديد وملامح التخفيف في العقوبات الواردة في قانون مكافحة جرائم تقنية المعلومات، وذلك في مطلبين: المطلب الأول حول ملامح التشديد في العقوبات، والمطلب الثاني حول ملامح التخفيف في العقوبات.

المطلب الأول: ملامح التشديد في العقوبات:

إن المطَّلِع على قانون مكافحة جرائم تقنية المعلومات يلاحظ مباشرةً صفة التشديد التي سادت القانون في تحديد العقوبات، إذ إن القانون قد توسَّع في إدراج الأفعال الجرمية بصورة جيدة تعطي نوعًا من المرونة والسهولة للمتعاملين مع القانون، وتعطي مجالًا واسعًا للمستقبل في دخول الكثير من الأفعال الجرمية ضمن نطاق القانون، فالمشرِّع العماني انتهج منهج التشديد في العقوبات في الكثير من المواد القانونية، وذلك عند مقارنتها بالعقوبات التي تضمَّنها الفصل الثاني مكرر من الباب

[1] المادة (3) من قانون مكافحة جرائم تقنية المعلومات.
[2] المادة (28) من قانون مكافحة جرائم تقنية المعلومات.
[3] المادة (20) من قانون مكافحة جرائم تقنية المعلومات.

السابع من قانون الجزاء الصادر بالمرسوم السلطاني رقم (47/7)، وتتمثل صفة التشديد في كثير من الجرائم.

أولًا: تغليظ العقوبات السالبة للحرية (الحبس):

ورد في المادة رقم (276 مكرَّر) من الفصل الثاني مكرَّر من الباب التاسع من قانون الجزاء الخاص بسلطنة عُمان نصًّا بأنه يُعاقَب بالحبس بما لا يقلُّ عن 3 أشهر ولا يزيد على عامين وبدفع غرامة ما بين 100 ريال عماني إلى 500 ريال عماني أو بعقوبة واحدة منهما في كلٍّ من الجرائم التالية: جرائم الاعتداء على التطبيقات البرمجية المحوسبة، وجرائم إتلاف البيانات والمعلومات، وجرائم التجسس الإلكتروني، وجرائم الاختراق الإلكتروني.

ومن الملاحظ أن قانون مكافحة الجرائم المتعلقة بتقنية المعلومات وضع العقوبات في تجريمه لعدد من السلوكيات السابقة بالحبس بما لا يقلُّ عن شهر واحد ولا يزيد على عام واحد وبدفع غرامة لا تقلُّ عن 500 ريال عماني ولا تزيد على 2,000 ريال عماني أو بعقوبة واحدة منهما[1]، إلى جانب أنه وضع عقوبة على جرائم التجسس الإلكتروني إذ إنه يُعاقَب بالحبس بما لا يقلُّ عن عام واحد ولا يزيد على 3 أعوام وبدفع غرامة لا تقلُّ عن 1,000 ريال عماني ولا تزيد على 3,000 ريال عماني أو بعقوبة واحدة منهما.

وقد أورَدَ التشريع عقوبة تتعلق بارتكاب جرائم الاعتداء على الخصوصيات الإلكترونية، ناصًّا على أنه يُعاقب من يرتكب تلك الجرائم بالحبس بما لا يقلُّ عن عام واحد ولا يزيد على 3 أعوام وبغرامة ما بين 1,000 ريال عماني إلى 3,000 ريال عماني أو بعقوبة واحدة منهما[2]، وفيما يتعلق بجرائم التزوير الإلكتروني فإن التشريع قد أورَدَ عقوبة تلك الجرائم ناصًّا على أنه يعاقَب من يرتكبها بالحبس بما لا يقلُّ عن شهر واحد ولا يزيد على 3 أعوام وبدفع غرامة لا تقلُّ عن 1,000 ريال عماني ولا يزيد على 10,000 ريال عماني أو بعقوبة واحدة منهما[3].

وفيما يتعلق بجرائم إتلاف البيانات والمعلومات ومحوها فقد أورَدَ التشريع عقوبة تلك الجرائم ناصًّا على أنه يعاقَب من يرتكبها بالحبس بما لا يقلُّ عن 6 أشهر ولا يزيد على عام واحد وبدفع غرامة لا تقلُّ عن 500 ريال عماني ولا تزيد على 1,000 ريال عماني أو بعقوبة واحدة منهما[4].

[1] المادة (8) من قانون مكافحة جرائم تقنية المعلومات.
[2] المادة (6) من قانون مكافحة جرائم تقنية المعلومات.
[3] المادة (5) من قانون مكافحة جرائم تقنية المعلومات.
[4] المادة (7) من قانون مكافحة جرائم تقنية المعلومات.

وعليه فإن سمة التشديد في العقوبة واضحة في كافة الأفعال المجرمة، وذلك بزيادة مدة السجن ورفع قيمة الغرامة المالية.

ثانيًا: رفع العقوبات المالية (الغرامة):

ورَدَ في المادة رقم (276 مكرَّر/1) أنه يُعاقَب بالحبس بما لا يقلُّ عن 6 أشهر ولا يزيد على عامين اثنين وبدفع غرامة لا تقلُّ عن 100 ريال عماني ولا تزيد على 500 ريال عماني أو بعقوبة واحدة منهما كل من يرتكب جريمة الاستيلاء أو الحصول بطريقة غير مشروعة على بيانات خاصة بالغير تكون منقولةً أو مختزنةً أو معالجةً من خلال نظم المعالجة البرمجية، وبتتبُّع أحكام التشريع المتعلق بقانون مكافحة جرائم تقنية المعلومات فإننا نجد أن التشريع وضع العقوبة لذلك الجرم بالحبس بما لا يقلُّ عن عام ولا يزيد على 3 أعوام وبدفع غرامة لا تقلُّ عن 1,000 ريال عماني ولا تزيد على 3,000 ريال عماني أو بعقوبة واحدة منهما وذلك في حال كون المعلومات والبيانات الواردة في نص الفقرة الثانية من المادة رقم (3) معلومات أو بيانات شخصية.

إذ صاحب التشديد في العقوبة الحبسية كذلك رفع قيمة الغرامات المالية، وهو ما يتضح من خلال الأمثلة التي أوضحناها سالفًا.

ثالثًا: الظروف المشددة للعقاب:

من مظاهر التشديد في التشريع العماني أن القانون شدد في مادته رقم (4) ناصًّا على العقوبة بالحبس بما لا يقلُّ عن عام ولا يزيد عن 3 أعوام وبدفع غرامة لا تقلُّ عن 1,000 ريال عماني ولا تزيد على 3,000 ريال عماني أو بعقوبة واحدة منهما وذلك لكل من يرتكب واحدة من الجرائم التي نصَّت عليها المادة رقم (3) من ذلك القانون في خلال أو بمناسبة تأدية عمله[1]، فإن من يرتكب تلك الجريمة بمناسبة عمله تكون عقوبته مشددةً وذلك ردعًا له عن ارتكابها.

أما المادة رقم (29) من ذلك التشريع فقد نصت على أنه يُعاقَب الشخص الاعتباري بدفع غرامة تعادل ضعف الحد الأعلى لعقوبة دفع الغرامة التي قررها القانون للجرائم، في حال كانت الجريمة مرتَكَبةً بِاسم الشخص الاعتباري ذاك أو لحسابه من قبل رئيس أو عضو مجلس إدارته أو مديره أو أحد المسؤولين الآخرين الذي يتصرف بتلك الصفة أو بموافقته أو بتستره أو بإهمال جسيم منه، فإن التعامل مع الشخص الاعتباري مختلف عن التعامل مع الشخص الطبيعي في التشريعات،

[1] المادة (4) من قانون مكافحة جرائم تقنية المعلومات.

إذ تتضاعف الغرامات على الأشخاص الاعتباريين في حال ثبت ارتكاب أحدهم لجريمة بِاسمه أو لحسابه [1].

رابعًا: إضافة جرائم جديدة في التجريم:

تضمَّن قانون مكافحة جرائم تقنية المعلومات جرائم مختلفة ومتنوعة مقارنةً بما تضمَّنه الفصل الثاني مكرر من الباب السابع من قانون الجزاء الصادر بالمرسوم السلطاني رقم (7 / 74)، ويُعَدُّ هذا التوسع في الأفعال المجرَّمة دليلًا على مواكبة المشرِّع العماني للواقع المحلي والعالمي في مكافحة جرائم تقنية المعلومات، ودليل على التطور التشريعي في مكافحة الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة.

المطلب الثاني: ملامح التخفيف في العقوبات:

مع وجود السمة البارزة للتشديد في العقوبات التي نص عليها قانون مكافحة جرائم تقنية المعلومات، نجد أن القانون كذلك قد خفف في بعض الحالات مراعاة لأسباب مكافحة الجريمة الإلكترونية، وبما يتوافق مع واقع وانتشار الجرائم، فالتخفيف يرجع إلى انحسار الجرائم المخفف في عقوباتها، وكذلك من باب تشجيع الأشخاص على الإبلاغ عن الجرائم، ويمكن حصر حالات التخفيف فيما يلي:

أولا: تخفيف مدة العقوبة السالبة للحرية:

لقد نصت المادة رقم (276 مكرَّر/3) على تجريم سلوكيات تزوير بطاقات الوفاء واستخدامها وقبول التعامل معها، إذ ورَدَ فيها أنه يُعاقَب بالحبس بما لا يزيد على 5 أعوام وبدفع غرامة لا تتعدى 1000 ريال عماني كل من قلَّد أو زوَّر بطاقة وفاء أو سحب أو استخدم أو حاول استخدام بطاقة مقلدة أو مزورة مع علمه بذلك أو قبل الدفع ببطاقة الوفاء المقلدة أو المزورة مع علمه بذلك، ومن الملاحظ أن التشريع اللخاص بمكافحة جرائم تقنية المعلومات وضَعَ عقوباتٍ مخفَّفةً لتلك الجرائم فأنقص العقوبة عليها، إذ ورَدَ في القانون المتعلق بمكافحة الجرائم التقنية أنه يُعاقَب بالحبس بما لا يقلُّ عن شهر واحد ولا يزيد على 6 أشهر وبدفع غرامة لا تقلُّ عن 500 ريال عماني ولا تزيد على 1000 ريال عماني أو بعقوبة واحدة منهما[2].

وقد ورَدَ في المادة رقم (276 مكرَّر/4) أنه يُعاقَب بالحبس بما لا يزيد على 3 أعوام وبدفع غرامة لا تتعدى 500 ريال عماني كل من استعمل البطاقة كطريقة للوفاء مع العلم بعدم وجود رصيد

[1] المادة (29) من قانون مكافحة جرائم تقنية المعلومات.

[2] المادة (28) من قانون مكافحة جرائم تقنية المعلومات.

له أو استخدم البطاقة بعد نهاية صلاحيتها أو إلغائها وهو يعلم ذلك أو استخدم بطاقة غيره دون علمه، وقد عاقب القانون بالحبس بما لا يقلُّ عن شهر واحد ولا يزيد على 6 أشهر وبدفع غرامة لا تقل عن 500 ريال عماني ولا تزيد على 1000 ريال عماني أو بعقبة واحدة منهما، وفي الجرائم المتعلقة بقبول الدفع ببطاقة الوفاء المقلدة أو المزورة مع علم الشخص بذلك فقد نَصَّ التشريع على تجريم تلك الجرائم بالحبس بما لا يقلُّ عن 6 أشهر ولا يزيد على عام واحد وبدفع غرامة لا تقل عن 1000 ريال عماني ولا تزيد على 5000 ريال عماني أو بعقوبة واحدة منهما[1].

ويتضح من ذلك منهج التخفيف الذي اتَّبعه المشرِّع في هذه الجرائم نظرًا لانحسارها بصورة كبيرة، وكذلك تظهر بطاقات الوفاء بحيث يصعب تزويرها أو استخدامها بصورة مخالفة للقانون.

ثانيًا: الظروف المخففة (الشروع في الجريمة وعدم تحقق النتيجة):

خفَّف القانون العقوبة في حالة الشروع مفرِّقًا بينها وبين حالة ارتكاب الجريمة، إذ نصت المادة (30) يعاقب بنصف الحد الأعلى للعقوبة المقررة قانونًا للجرمية على الشروع في ارتكاب إحدى الجرائم المنصوص عليها في هذا القانون.

كما أن القانون قد عاقب بنصف الحد الأقصى للعقوبة في حالة عدم تحقق نتيجة الجريمة، إذ نصت المادة (31) يعاقب بذات العقوبة المقررة لمرتكب جريمة تقنية المعلومات كل من حرض أو ساعد الغير أو اتفق معه على ارتكابها، فإذا لم تتحقق النتيجة الإجرامية عوقب بنصف الحد الأقصى للعقوبة المقررة قانونًا للجرمية.

ثالثًا: التخيير بين الجمع بين العقوبات الحبسية والغرامات:

تتردد في القانون دائمًا عبارة "أو بإحدى هاتين العقوبتين"، وفي هذا التوجه تخفيف في العقوبة، وكذلك إعطاء مرونة كبيرة للقضاة بتخفيف العقوبة وفقًا للواقعة وما تصاحبها من ظروف سواء أكانت ظروف مشددة أو ظروف مخففة.

رابعًا: تخفيف العقوبة في حالة الإبلاغ عن الجريمة:

يعفي القانون من العقوبة كلُّ جانٍ أو شريكٍ لِجانٍ يبادر بإبلاغ السلطات المختصة بمعلومة حول جرم حدث بالمخالفة لأحكام القانون قبل أن تكشف السلطات عن ذلك الجرم من تلقاء نفسها،

[1] المادة (28) من قانون مكافحة جرائم تقنية المعلومات.

ففي حال إدلائه بالمعلومة بعد أن تكون السلطات قد كشفت عنها يجوز أن تعفي عنه[1] المحكمة من العقوبة شرط أن يترتب على إدلائه بالمعلومة ضبط بقية الأشخاص الجناة[2].

الخاتمة:

في ختام هذه الدراسة يتضح لنا التوجه الذي اتَّبعه المشرِّع العماني في السياسة العقابية في قانون مكافحة جرائم تقنية المعلومات، إذ إن السياسة العقابية بمفهومها العام هي الكيفية التي ينبغي بها مواجهة الظاهرة الإجرامية، وذلك بشكل يكفل حماية المجتمعات ومنع الجريمة أو الحد منها بصورة كبيرة، بالتالي تتأثر السياسة العقابية بواقع انتشار الجريمة هادفةً من ذلك تحقق الردع العام والردع الخاص على حد سواء، وقد تطورت التشريعات التي تنظم جرائم تقنية المعلومات في السلطنة، بدءًا بالفصل الثاني مكرر من الباب السابع من قانون الجزاء لمكافحة جرائم الحاسب الآلي في قانون الجزاء العماني الصادر بالمرسوم السلطاني رقم (74/7)، ثم المرسوم السلطاني رقم (2011/12) الذي أُصدِرَ بحسبه قانون مكافحة جرائم تقنية المعلومات الذي توسَّع في التجريم والعقوبات، ومن خلال هذا القانون تبينت ملامح التشديد في العقوبة في تغليظ العقوبات السالبة للحرية ورفع العقوبات المالية والظروف المشددة للعقاب وإضافة جرائم جديدة في التجريم، أما ملامح التخفيف فتمثلت في تخفيف مدة العقوبة السالبة للحرية والظروف المخففة والتخيير فيما بين الجمع بين العقوبات الحبسية والغرامات وتخفيف العقوبة في حالة الإبلاغ عن الجريمة.

ويمكن النظر في التوصيات التالية كمقترحات مستقبلية لتطوير قانون مكافحة جرائم تقنية المعلومات:

1. إضافة التدابير العقابية ضمن العقوبات الواردة في القانون، خاصةً أن قانون الجزاء الجديد قد تضمَّن مثل هذه التدابير العقابية.
2. إيجاد مركز علاجي لمرتكبي جرائم تقنية المعلومات، إذ أن الحاجة باتت كبيرة لمثل هذه المراكز العلاجية في ظل انتشار الجريمة الإلكترونية.
3. إعادة النظر في العقوبات السالبة للحرية والغرامات بما يتناسب مع تطور الجرائم الإلكترونية ومدى انتشارها وذلك بصورة مستمرة ودائمة.

---

[1] المادة (33) من قانون مكافحة جرائم تقنية المعلومات.

2 جاء في المرسوم الاتحادي للإمارات رقم 5 / 2012 في المادة (45) أنه (تقضي المحكمة، بناءً على طلب من النائب العام، بتخفيف العقوبة أو بالإعفاء منها، عمَّن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقًا لأحكام هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم".

قائمة المصادر والمراجع:

أولًا: القوانين:

- قانون الجزاء الجزاء العماني الصادر بالمرسوم السلطاني رقم (47/7).
- قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2011/12).

ثانيًا: الكتب والدراسات العلمية:

- حسني، محمود نجيب: علم العقاب، ط 1976، القاهرة: دار النهضة العربية.
- خوري عمر (2008م): السياسة العقابية في القانون الجزائري، جامعة الجزائر، رسالة دكتوراه.
- عبد العزيز سالم السنيدي (2018م): السياسة العقابية للمشرِّع الإماراتي في مواجهة الجرائم المعلوماتية، جامعة الإمارات، رسالة ماجستير غير منشورة.
- فايزة رزوقي وبوراس عبد القادر (2021م): السياسة الجنائية المعاصرة، الجزائر، جامعة ابن خلدون، بحث علمي منشور في مجلة الحقوق والعلوم الإنسانية.
- محمد ناصر الهزاني (2018): المسؤولية الجنائية عن انتهاك الفضاء السيبراني، الرياض، جامعة نايف للعلوم الأمنية، رسالة ماجستير غير منشورة.
- مصطفى البيطار (2016): أصول علمي الإجرام والعقاب، جدة: مكتبة القلم.
- هشام شحاته إمام (2007م): دروس في علم العقاب، القاهرة: دار الفكر.

ثالثًا: المواقع الإلكترونية:

- موقع (عماننا) البوابة الإلكترونية للخدمات الحكومية الإلكترونية، انظر الرابط التالي: https://omanportal.gov.om/wps/portal/index/aboutportal
- الموقع الإلكتروني الخاص بهيئة تقنية المعلومات، انظر الرابط التالي: https://2u.pw/Wp6W1
- الموقع الإلكتروني https://stringfixer.com/ar/Convention_on_Cybercrime.