تأثير التكنولوجيا على الحقوق والحريات في العصر الرقمي تحليل قانوني للتحديات والفرص في سلطنة عمان

The Impact of Technology on Rights and Freedoms in the Digital Age A Legal Analysis of Challenges and Opportunities in the Sultanate of Oman

أ.د. محمد عبد الله الشوابكة

رئيس قسم القانون العام
– كلية الحقوق
جامعة ظفار- سلطنة عُمان

الكلمات الافتتاحية:
تكنولوجيا، حقوق وحريات، تشريعات، جريمة إلكترونية، دستور.

Keywords:
Technology, Rights and freedoms, Legislation Cyber-crime, constitution

Abstract

The impact of technology on rights and freedoms in the digital age is an important topic at the present time, and the study addressed this important topic by studying the situation in the Sultanate of Oman, and this impact is especially evident with the technological progress and digital transformation that the country has recently witnessed. The study reviewed the challenges and opportunities posed by the use of technology in the field of human rights and fundamental freedoms, on the one hand advanced technology is capable of achieving positive developments in society, such as enhancing transparency and combating corruption, improving access to information and promoting freedom of expression, and on the other hand the misuse of technology can lead to violations of the rights of

individuals, such as violations of privacy and personal security. This study was addressed from several aspects that have an effective impact, such as digital technology crimes, which also pose a threat to national security and sovereignty, in addition to the negative effects on children and youth and the challenges of privacy rights. The study followed the descriptive, analytical and comparative approach and concluded several results, the most important of which are: Digital transformation can sometimes lead to digital violations and privacy breaches, which pose a direct threat to the rights of citizens. It also concluded with several recommendations, the most important of which are: Updating and strengthening legislation related to the protection of rights and freedoms in the digital age, especially the Basic Law, to be consistent with continuous technological developments.

الملخص

تأثير التكنولوجيا على الحقوق والحريات في العصر الرقمي يشكل موضوعاً هاماً في الوقت الراهن، وقد تناولت الدراسة هذا الموضوع الهام من خلال دراسة الوضع بسلطنة عمان، ويتجلى هذا التأثير بشكل خاص مع التقدم التكنولوجي والتحول الرقمي الذي شهدته البلاد مؤخراً. استعرضت الدراسة التحديات والفرص التي يطرحها استخدام التكنولوجيا في مجال حقوق الإنسان والحريات الأساسية، ومن جهة فإن التكنولوجيا المتقدمة قادرة على تحقيق تطورات إيجابية في المجتمع، مثل تعزيز الشفافية ومكافحة الفساد، وتحسين الوصول إلى المعلومات وتعزيز حرية التعبير، ومن جهة أخرى يمكن أن تؤدي سوء استخدام التكنولوجيا إلى انتهاكات لحقوق الأفراد، مثل انتهاكات الخصوصية والأمن الشخصي. هذا وقد تم تناول هذه الدراسة من عدة جوانب لها تأثيرها الفعال، مثل جرائم التكنولوجيا الرقمية التي تشكل أيضاً تهديداً للأمن والسيادة الوطنية، بالإضافة إلى الآثار السلبية على الأطفال والشباب وتحديات حقوق الخصوصية. وقد اتبع في الدراسة المنهج الوصفي والتحليلي والمقارن وخلصت الدراسة إلى عدد من النتائج، من أهمها: أن التحول الرقمي يمكن أن يؤدي في بعض الأحيان إلى انتهاكات رقمية واختراقات للخصوصية، مما يشكل

تهديدًا مباشرًا لحقوق المواطنين. كما خلصت إلى عدد من التوصيات، من أهمها: تحديث وتعزيز التشريعات المتعلقة بحماية الحقوق والحريات في العصر الرقمي وبالأخص النظام الأساسي، لتكون متسقة مع التطورات التكنولوجية المستمرة.

المقدمة

شهدت التكنولوجيا تقدماً ملحوظاً في الفترات الأخيرة، مما أحدث تحولات جوهرية في العديد من جوانب الحياة المتعددة، بما في ذلك جانب الحقوق والحريات. في عصر الرقمنة، أصبحت التكنولوجيا الحديثة جزءاً لا يتجزأ من أساسيات الحياة اليومية، إذ يتم الاعتماد عليها في مختلف المجالات مثل العمل، والتعليم، والتواصل الاجتماعي، والترفيه، وغيرها. هذا الاعتماد المتزايد على التكنولوجيا يجعل من الضروري حماية حقوق الأفراد وحرياتهم لما تنطوي عليها من أخطار في بعض الأحيان. تناولت هذه الدراسة مدى تأثير التكنولوجيا على الحقوق والحريات في العصر الراهن، مع التركيز على التحديات والفرص التي تواجهها سلطنة عمان في هذا الخصوص. تقدم التكنولوجيا في مجال تكنولوجيا المعلومات والاتصالات أحدث ثورة عالمية في هذا الميدان، مما جعلها تؤثر في جميع جوانب حياة البشر، سواء على المستوى المحلي أو العالمي. حيث أصبحت عملية تبادل المعلومات والمعرفة أسهل وأسرع، وتدفق المعلومات عبر وسائل الاتصال المختلفة قد سهل تبادل الأخبار والحوارات بشكل أكبر. مع ذلك، فإن هذا التطور أحدث أيضًا العديد من التحديات والمخاطر، خاصة مع ضعف الرقابة على التكنولوجيا. فقد ظهرت الجرائم المعلوماتية، وهي نوع جديد من الجرائم يعتمد على التكنولوجيا في ارتكابها، والتي تشكل تهديدًا للأمن والاستقرار وخطراً أيضاً على الحقوق والحريات، سواء على المستوى المحلي أو العالمي. إذ يمكن استخدامها لإثارة الفوضى والاضطرابات، وكذلك للوصول غير المشروع إلى المعلومات السرية أو لسرقة الأموال. بالإضافة إلى ذلك، تعتبر عائقًا أمام التنمية الاقتصادية والأمنية.

مشكلة البحث: في إطار التأثير الحادث من التكنولوجيا على مختلف حقوق الأفراد وحرياتهم في العصر الرقمي، نشهد تحولًا تاريخيًا وثقافيًا يتماشى مع التقدم

العلمي والتكنولوجي يُسهم في تبسيط الإجراءات وتعزيز فعالية الحياة الاجتماعية، مما ينعكس إيجابيًا في القانون الجزائي، إذ يصبح جزءًا من الأدوات الحديثة للسياسة الجنائية لتحقيق الأهداف الإيجابية. ومع ذلك، تكتسب التكنولوجيا الحديثة أيضًا جوانب سلبية، وذلك من خلال تطور جرائم التكنولوجيا الرقمية وانتهاكات حقوق الأفراد والسيادة الوطنية. من الناحية التشريعية، يسمح القانون الدولي والقانون الوطني بشأن حقوق الإنسان باستخدام تكنولوجيا المعلومات بحرية، وبتبادل البيانات والمعلومات عبر وسائل التواصل الاجتماعي، مع التشديد على أهمية وجود قواعد ونصوص قانونية تعمل على تنظيم تلك الحرية. وتشير التطورات التشريعية في السلطنة إلى اهتمام المشرع بمكافحة جرائم التكنولوجيا الحديثة، وتأتي هذه التشريعات لتلعب دورًا مهمًا في تنظيم توافر واستخدام الخدمات الحكومية، وتبرز أهمية سرعة سن النظم والقوانين المتعلقة بالمعاملات الإلكترونية في هذا السياق التقني الراهن.

ويمكن القول بأن الحقوق والحريات في العصر الرقمي تواجه تحديات مثل التجسس ومراقبة البيانات، والجرائم الإلكترونية الأكثر انتشارا والتي تشكل تهديداً للأفراد والمجتمعات، فضلاً عن تأثيراتها السلبية على الأطفال والشباب مثل التعرض للمحتوى غير الملائم واستغلالهم، وفي المقابل لا تخلوا من الإيجابيات الكثيرة.

أهداف البحث: يهدف البحث إلى التحليل المناسب للتحديات والفرص التي تواجه كلاً من حقوق الأفراد وحرياتهم في العصر الرقمي في السلطنة، واقتراح عددا من الحلول القانونية لمثل تلك التحديات.

منهج البحث: هذه الدراسة ستستخدم المنهج الوصفي والتحليلي والمقارن، حيث سيتم تحليل النصوص القانونية ذات الصلة ومقارنة التحديات والفرص في التشريعات المختلفة.

خطة البحث: سوف يتم تقسيم البحث إلى مبحث تمهيدي يتناول فيه الإطار النظري للدراسة، ومبحثين: الأول يتم فيه تناول التحديات التي تواجه الحقوق والحريات في العصر الرقمي، أما المبحث الثاني سيتم فيه تناول الفرص التي تفتحها التكنولوجيا

لحماية الحقوق والحريات في العصر الرقمي في سلطنة عمان.

المبحث التمهيدي : الإطار النظري للدراسة : تمثل التكنولوجيا تحولا جذريا من النظام التقليدي إلى النظام الرقمي معتمدة في ذلك على تقنيات المعلومات والاتصالات في مختلف مجالات العمل.[١] مما لا شك فيه أن هذا التحول يتطلب وضع التشريعات والنظم اللازمة لضمان توافر واستخدام التكنولوجيا بطريقة قانونية وآمنة[٢]، مع التأكيد على أهمية الجوانب التشريعية والقانونية في تقدم التكنولوجيا، حيث يصعب تحقيق التطور في هذا المجال دون التنظيم وتوجيه الاستخدام القانوني للتقنية. إذ ينبغي سن التشريعات والقوانين اللازمة لتنظيم وتوجيه استخدام التقنية الرقمية، حيث تختلف عن الخدمات التقليدية وتتطلب قوانين متخصصة[٣]، كما ينبغي وجود تنظيمات قانونية تتعلق بالمعاملات الإلكترونية في البيئة التقنية، تكون واضحة وشاملة لضمان الأمان والحماية للمستخدمين. تشير التكنولوجيات الحديثة التي غيّرت العالم وأحدثت تغييرات جذرية في السياسة الجزائية إلى أجهزة الحاسوب والذكاء الاصطناعي، ويمثل التحول الرقمي والمفاهيم الحديثة، مثل التحليل الجنائي الرقمي والتحقق من الهوية الرقمية وغيرها، أدواتً حيوية تُستخدم في مكافحة الجريمة وتحقيق العدالة، بالتالي، يعمل التفاعل بين التكنولوجيا والتشريعات القانونية على تحقيق الأهداف المشتركة، التي تركز على الأمان والحماية والعدالة في جميع المجالات، بما في ذلك المجال الجزائي[٤].

مصطلحات الدراسة:

أولا- مفهوم التكنولوجيا: التكنولوجيا تمثل التحول من الأنظمة التقليدية إلى الأنظمة الحديثة التي تعتمد على تقنيات المعلومات والاتصالات في العديد من مجالات العمل، وهذا يتطلب اتباع سلسلة من المتطلبات التنظيمية والقانونية[٥]. إذ تعرف التكنولوجيا بأنهما " الاستخدام الأمثل للتقنيات الرقمية والأدوات والموارد لتلبية احتياجات ورغبات الأفراد"[٦]، وتشمل مجالات مثل الحوسبة والاتصالات والطب والطاقة والنقل، والتي تتطور باستمرار لتلبية الاحتياجات الجديدة وحل المشكلات الحالية. وهذا التطور المتسارع يؤثر بشكل كبير على الحياة اليومية للأفراد، مما

يسهم في التطور الاقتصادي والاجتماعي والثقافي للمجتمعات[٧].أما التحول الرقمي فيشير إلى الاستفادة من تكنولوجيا الحاسوب والإنترنت لتعزيز عمليات إنشاء القيم بكفاءة وفعالية أكبر، ويتناول التغيرات الواسعة التي تنشأ نتيجة لتقنيات جديدة وتأثيرها على العمل والتفاعل بشكل عام.[٨] يُعرف التحول الرقمي بأنه عملية تحسين الخدمات وإنشاء وتقديم قيمة جديدة من خلال التكنولوجيا الحديثة، مثل تطبيق التكنولوجيا الذكية واستخدام مفهوم الواقع الافتراضي بحيث يُحدث تغييرات شاملة في الخدمات والشركات[٩]. في سلطنة عمان، يُعَتَبَر التحول الرقمي عملية شاملة تستهدف اعتماد التكنولوجيا الرقمية واستخدامها لتحسين الخدمات الحكومية وتعزيز التنمية الاقتصادية والاجتماعية. إذ يقوم على تحسين الاتصالات وتبسيط الإجراءات الحكومية، وتحسين جودة الخدمات العامة للمواطنين والمقيمين. كما يشمل تطوير البنية التحتية التقنية وتعزيز القدرات الرقمية للمؤسسات والأفراد في البلاد. حيث يُعَتَبَر التحول الرقمي جزءًا أساسيًا من رؤية السلطنة لتعزيز الاقتصاد الرقمي وتحقيق التنمية المستدامة[١٠]. ثانياً- مزايا التكنولوجيا: تظهر مزاياها الملموسة في عدة جوانب[١١]: تتمثل في تقليل التكاليف، مما يؤدي إلى تحقيق كفاءة أكبر في إدارة الأعمال، وفي المجال القانوني إلى توفير التكلفة للمتقاضين، وتطوير استراتيجيات محكمة أكثر فعالية، مما يخدم مصلحة المتقاضين، فضلاً عن إتاحة القدرة على تحليل البيانات القانونية بشكل فعال، مما يساعد في اتخاذ قرارات دقيقة ومستنيرة، بالإضافة إلى تحسين نظام القانون والقضاء ليصبح أكثر ذكاءً وفعالية، مما يحل محل الاعتماد على الأنظمة التقليدية.

ثالثاً: – متطلبات تطبيق التكنولوجيا: تحتوي تطبيقات التكنولوجيا على مجموعة من المتطلبات التي يجب تلبيتها لضمان فعالية وأمان الاستخدام[١٢]: منها تغيير أسلوب التعليم للعناصر البشرية القضائية والقانونية، بهدف تزويدهم بالمهارات الحديثة وتمكينهم من تحقيق الازدهار في المجتمع والبيئة الرقمية، وإنشاء بنية تحتية للاتصالات الرقمية بحيث يجب إقامة بنية تحتية فعّالة للاتصالات الرقمية في منظومة القانون والقضاء، مع الحفاظ على صيانتها وضمان إمكانية الوصول إليها، وتحقيق

التوازن بين تكاليف وجودة الخدمات القضائية، وتحقيق الشفافية وحماية البيانات داخل منظومتها ، وضمان استقلالية العمل القضائي، مع تعزيز الثقة وحماية البيانات الرقمية، وتيسير الوصول إلى الخدمات داخل تلك المنظومة من خلال تحسين الخدمة العامة ووضع آليات وضوابط لجودة الخدمات الرقمية، وتحسين الإطار التنظيمي لها، وتنفيذ نماذج مبتكرة وأساليب حديثة لخدمة المجتمع. في سلطنة عُمان، شهدت خدمات الحكومة الإلكترونية تطورًا ملحوظًا في السنوات الأخيرة بفضل التحول الرقمي الذي تشهده السلطنة.

يمكن القول: ملاحظة الزيادة في استخدام المواطنين للخدمات الحكومية الإلكترونية في مختلف المجالات مثل التعليم، والصحة، والمالية، والأعمال، وغيرها. إذ قامت الحكومة العمانية بتطوير البنية التحتية الرقمية وتقديم خدمات إلكترونية مبتكرة تلبي احتياجات المواطنين والمقيمين، مثل تسهيل إجراءات التسجيل وتقديم الطلبات والدفع الإلكتروني وتوفير المعلومات بشكل سريع وفعّال. كما تم توفير تطبيقات هاتف ذكي لتسهيل الوصول إلى الخدمات الحكومية بسهولة أكبر وفي أي وقت ومن أي مكان. يعزز هذا الاستخدام النشط للتكنولوجيا الرقمية فعالية الخدمات الحكومية ويسهم في تحقيق التواصل الفعال بين الحكومة والمواطنين. ومع ذلك، هناك تحديات ما زالت تواجه استخدام المواطنين للخدمات الحكومية الإلكترونية، مثل نقص الوعي التكنولوجي والقلق بشأن الأمان الرقمي وتحديات الوصول إلى الإنترنت في بعض المناطق النائية. لذلك، يتطلب دعم استخدام الخدمات الحكومية الإلكترونية جهود مستمرة لتوعية المواطنين وتحسين البنية التحتية الرقمية وتعزيز الأمان الرقمي[١٣]. ومقابل ذلك يكون هناك تحديات تواجه الأفراد في حقوقهم وحرياتهم في ظل العصر الرقمي هذا ما سوف يتم تناوله في المبحث الأول.

المبحث الأول : التحديات التي تواجه الحقوق والحريات في العصر الرقمي في سلطنة عمان

تمهيد وتقسيم:

في عصر تهيمن عليه التكنولوجيا وتطورات الإنترنت، تواجه الحقوق والحريات في

سلطنة عمان تحديات متزايدة نتيجة للتقدم الرقمي السريع، لما تشكله من انتهاكات للحقوق والحريات في بعض الأحيان، كاستخدامها لجرائم اختراق الخصوصية الشخصية ونشر المعلومات بطرق غير قانونية، مما يعرض الأفراد لخطر فقدان سيطرتهم على بياناتهم الشخصية، فضلاً عن الاحتيال الإلكتروني والتهديدات السيبرانية، الأمر الذي من شأنه التأثير بشكل مباشر على حقوق الأفراد وتعريض سلامة المعلومات للخطر. سيتم تناول ذلك في مطلبين، الأول لانتهاك الحق في الخصوصية، أما المطلب الثاني لانتهاكات الحق في الأمن.

المطلب الأول : انتهاك الحق في الخصوصية : التطور التكنولوجي الكبير وتقدم وسائل التواصل الاجتماعي والاتصالات المتعددة، جنبًا إلى جنب مع فتح العالم وتبادل البيانات والمعلومات عبر الإنترنت، أدى إلى جمع ومعالجة كميات هائلة من البيانات الشخصية. هذا يستدعي إنشاء نظام قانوني لحماية تلك البيانات لتفادي المخاطر المحتملة المترتبة على استخدامها، وذلك من خلال تحديد الإجراءات اللازمة والالتزامات الخاصة بعملية معالجة البيانات الشخصية، في هذه الحالة، يمكن تقليل أخطار انتهاك الخصوصية وتعزيز الثقة في النظام الرقمي[١٤]. لذلك، أصبح الحق في حماية البيانات الشخصية مسألة قانونية مهمة، حيث أقر المشرعون بحمايته وضمان الحماية الكافية له على المستويين الدولي والوطني. سيتم تناول ذلك في فرعين، الأول على المستوى الدولي، أما الفرع الثاني سيخصص على المستوى الوطني.

الفرع الأول- حماية البيانات الشخصية على المستوى الدولي: تعمل المواثيق الدولية على توفير الضمانات اللازمة للبيانات الشخصية، وظهر هذا الاهتمام بشكل واضح على الصعيد الدولي من خلال تبني اللائحة الأوروبية لحماية البيانات العامة (GDBR) تمنح هذه اللائحة أهمية كبيرة لحماية الخصوصية وسرية البيانات الشخصية للأفراد، كجزء من الأمن القومي والداخلي للدول الأعضاء في الاتحاد الأوروبي. وبالتالي، تم تطبيق اللائحة الأوروبية لحماية البيانات العامة (GDBR) في ٢٥ مايو ٢٠١٨ على جميع الدول الأعضاء في الاتحاد الأوروبي[١٥]. في الوقت الحالي، يعتمد الكثير من تعاملات الأفراد على بياناتهم الشخصية، التي يتم تخزينها ومعالجتها بطريقة تجعلها سهلة

الوصول إليها، حيث تقوم العديد من الجهات والشركات بإنشاء قواعد بيانات لعملائها لتسهيل الوصول إليها عند الحاجة. ورغم وجود العديد من المزايا والآثار الإيجابية لهذه العملية، فإن التجارب أظهرت تعرض بعض هذه البيانات لانتهاكات واختراقات، سواء أثناء عملية المعالجة أو التخزين أو النقل. وبالتالي، أصبحت الخصوصية التي كان يتمتع بها الأفراد أكثر عرضة للمخاطر، مما يقلص نطاق الحماية الشخصية بسبب انتشار التكنولوجيا الحديثة. فوسائل تقنية المعلومات المستخدمة حاليًا تشكل خطرًا وتهديدًا كبيرًا على الحياة الشخصية وحريات الأفراد، حيث أثبتت قدرتها الفائقة على كشف تفاصيل حياة الفرد بشكل سريع، بعدما كانت محجوبة عن رؤية الآخرين[١٦]. مما لا شك فيه، أنها تشكل تهديدًا كبيرًا على خصوصية أصحاب هذه البيانات، حيث تُظهر نظرية التسويق المباشر الطريقة التي يُنشأ فيها إعلان مخصص لكل عميل بالإسناد إلى المعلومات المجمعة عنه، والتي تشمل البيانات الشخصية، وهو ما أدى إلى زيادة قيمة هذه البيانات وظهور تجارتها. وعندما يتم معالجة هذه البيانات أثناء جمعها أو تخزينها أو نقلها، تتعرض لمخاطر تنتهك خصوصيتها. هذا وقد ساهم انتشار الوسائل الإلكترونية في تسهيل ذلك مع ضعف الوازع الأخلاقي أو غياب القوانين التي تحمي تلك البيانات. ولذلك، تدخل المشرع في العديد من الدول ومنها سلطنة عمان لوضع إطار قانوني ينظم معالجة البيانات الشخصية، بحيث تكون هذه المعالجة شفافة وتُعلم بها الأشخاص المعنيون بهذه البيانات، بالإضافة إلى حقهم في الاعتراض عليها[١٧].

الفرع الثاني- على المستوى الوطني: تطورت البيانات الشخصية بمعدل يواكب التقدم الهائل في شبكة الإنترنت. لم تعد هذه البيانات تقتصر على المعلومات التقليدية مثل الاسم والعنوان، بل توسع نطاقها لتشمل الصور الشخصية ومقاطع الصوت، بالإضافة إلى مجموعة متنوعة من المعلومات الأخرى المتعلقة بالشخص، مثل وضعه المالي، وسلوكياته، وعاداته، واهتماماته. ومن بين هذه المعلومات، تبرز البيانات البيو مترية التي تتعلق بجسم الإنسان[١٨]. المشرع العماني في المادة الأولى من المرسوم السلطاني رقم ٦ / ٢٠٢٢ بشأن حماية البيانات الشخصية حدد

مفهوم المعالجة على النحو التالي: "هي العملية أو مجموعة من العمليات التي يتم تنفيذها على البيانات الشخصية، بما في ذلك جمعها، أو تسجيلها، أو تحليلها، أو تنظيمها، أو تخزينها، أو تعديلها، أو تحويرها، أو استرجاعها، أو مراجعتها، أو تنسيقها، أو دمج بعضها مع بعض، أو حذفها، أو إلغاؤها، أو الإفصاح عنها، سواء عبر الإرسال، أو التوزيع، أو النقل، أو التحويل، أو الإتاحة بوسائل أخرى."

بناءً على المفهوم المذكور، سيتم بيان أخطار معالجة البيانات الشخصية من خلال الآتي:

أولاً- المخاطر المتعلقة بتجميع البيانات الشخصية: يُفهم تجميع البيانات الشخصية على أنه عملية تضمن جمع وترتيب عناصر البيانات الشخصية لفرد معين، وإدراجها في بطاقة معلومات تتعلق بذلك الفرد، سواء كانت هذه البطاقة ورقية أو إلكترونية، وهذا يعتبر أمرًا ضروريًا لتنفيذ معالجة هذه البيانات، ومع ذلك، قد تتضمن معالجة البيانات الشخصية أخطار محتملة، مثل انتهاك حقوق وحريات الأفراد وانتهاك خصوصيتهم. يُلاحظ أن العديد من المؤسسات الحكومية والشركات الخاصة تقوم بجمع وتخزين بيانات شخصية مفصلة عن المتعاملين معها، وتشمل هذه البيانات الوضع المادي والصحي والتعليمي، والعائلي، والاتجاهات الاجتماعية، وغيرها. ومن الممكن أن يفتح ذلك الباب لسوء استخدام البيانات أو توجيهها بشكل خاطئ، أو لمراقبة الأفراد بطرق غير مشروعة والحكم عليهم من خلال تحليل سجلات البيانات الشخصية المخزنة[١٩]. إن توفر ربط الأجهزة الإلكترونية مع بعضها البعض عبر جهاز مركزي أو شبكات الاتصال العامة هي وسيلة لتبادل المعلومات والبيانات الشخصية بين الأنظمة المعلوماتية، مما يؤدي إلى إنتاج بيانات جديدة عن الأفراد[٢٠]. في الوقت الراهن، يمكن جمع البيانات الشخصية دون علم الأفراد المعنيين بها بسبب التطورات التكنولوجية، خاصة عبر الإنترنت، حيث يُمكن تجميع البيانات وتخزينها باستخدام ميزات مثل ملفات تعريف الارتباط.[٢١] المادة ٤٣ من قانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم ٦٩ لسنة ٢٠٠٨ العماني تنص على "أنه يُسمح لأي جهة حكومية أو مقدم خدمات تصديق بجمع البيانات الشخصية مباشرة من الشخص نفسه

أو من شخص آخر بعد الحصول على موافقته الصريحة، وذلك لأغراض إصدار شهادة أو المحافظة عليها أو تسهيل ذلك". وتنص المادة أيضًا على "أنه لا يجوز جمع البيانات أو معالجتها أو استخدامها لأي غرض آخر دون الحصول على موافقة صريحة من الشخص المعني بجمع البيانات".[٢٢] بالإضافة إلى جمع المعلومات من قبل الشبكات الخاصة بالتواصل الاجتماعي، حيث تُعتبر هذه الشبكات مخزنًا للبيانات، حيث يُقدم المستخدمون معلوماتهم الشخصية للتسجيل فيها وإنشاء حساباتهم الخاصة، وغالبًا ما يُترك المستخدمون دون قراءة السياسات الخصوصية، مما قد يؤدي إلى التنازل الصريح عن بياناتهم الشخصية. بالإضافة إلى ذلك، يقوم المستخدمون بمشاركة معلومات عن حياتهم اليومية وحالتهم المزاجية وآرائهم السياسية، وهذه المعلومات تُعد سرية ولا يجب أن يكون للآخرين الوصول إليها دون موافقة صاحبها. وعدم قراءة سياسات الخصوصية يمكن أن يؤدي إلى استغلال بيانات المستخدمين لأغراض غير مشروعة[٢٣].

ثانيا- المخاطر المتعلقة باستخدام ومعالجة البيانات الشخصية: يهدف استخدام البيانات الشخصية ومعالجتها إلى تحقيق أهداف المعالجة المحددة، مع التأكيد على عدم تجاوز حدود هذه الأهداف المعلنة[٢٤]. إلا أن هناك أخطار متعددة مرتبطة باستخدام البيانات الشخصية ومعالجتها لما يكتنفها من غموض حول الأهداف المراد بها، ويمكن لغموض أو اتساع أهداف معالجة البيانات من جانب المسؤول عنها على سبيل المثال، والذي يتعين عليه الإعلان عنها للجنة الوطنية للمعلوماتية والحريات، أن يمنحه مساحة واسعة للتلاعب. وعندما يكون هناك ربط لعملية المعالجة بعدة أهداف، فإنه يصعب تقدير مدى مشروعية تلك المعالجة، مما يعرض الأشخاص المعنيين ببياناتها لعدم اليقين بشأن حقوقهم الخاصة بالبيانات التي يتم معالجتها[٢٥].كما يمكن نتيجة تزايد تدفق المعلومات عبر الأنترنت أن تتزايد معها المخاطر وخاصة مع ظهور الملاجئ الآمنة التي لا تخضع لأي قيود على عمليات المعالجة، مما يسمح بجمع ومعالجة البيانات دون قيود، حيث يلجأ العديد من المؤسسات في عالم الإنترنت إلى هذه الملاجئ لتجنب القيود القانونية على معالجة البيانات الشخصية[٢٦].

ثالثا- المخاطر المتعلقة بحوسبة البيانات الشخصية: تحويل المعلومات والبيانات الشخصية إلى صيغ إلكترونية يُعرف عمومًا بحوسبة البيانات، يتم ذلك عن طريق تسجيل البيانات على وسائط إلكترونية، مثل الأقراص الممغنطة، بتمثيلها في صورة نبضات كهربائية، حيث يسمح هذا النهج باستخدام الحاسوب لقراءة البيانات ومعالجتها، مما يتيح تخزينها ونقلها ودمجها بسهولة، ويفتح الأبواب أمام استخدامات جديدة قد لا تكون معروفة بعد، ويسهل بالتالي عملية معالجتها وتحسينها إذا لزم الأمر[٢٧]. ويشير ما سبق إلى أن الإنسان كان يقوم بجمع ومعالجة البيانات الشخصية قبل ظهور التقنيات الحديثة لحوسبة البيانات. ومع ذلك، كانت هذه الممارسات تقتصر عادةً على نطاق محدود للغاية. بالنظر إلى استخدام أجهزة الحاسب في معالجتها يزيد من حجم هذه المخاطر بشكل كبير، وبالتالي يتعرض الأشخاص المعنيون بهذه البيانات لمخاطر متزايدة نظرًا لقدرة الحواسيب الهائلة على جمع البيانات ومعالجتها بسرعة وكفاءة، بالإضافة إلى سهولة نقلها عبر الشبكات المركزية أو شبكة الإنترنت[٢٨]. بالإضافة إلى ذلك، يجب الاعتراف بأن تأمين النظام المعلوماتي ليس معافًى من المخاطر، حيث إن الهجمات المستهدفة التي تستهدف النظام لاستهداف البيانات وتقويض الأمن ليست مستبعدة، تلك الهجمات قد تشكل تهديدًا جسيمًا للأنظمة المعلوماتية بأكملها، خاصة مع سهولة التسلل إلى هذه الأنظمة أو استغلال الثغرات الأمنية بهدف الوصول غير المشروع إلى البيانات. أضف إلى ذلك، عدم كفاءة أو انعدام نظم تأمين البيانات يمكن أن يؤدي إلى انتهاك حقوق الأفراد المتضمنة في البيانات المخزنة في هذه الأنظمة، فإذا ما تم اختراق النظام المعلوماتي، فإن ذلك يتيح للمخترق الوصول إلى البيانات وإمكانية تعديلها أو حذفها أو نسخها لاستخدامها بشكل غير مشروع، وبالتالي تزداد خطورة الوضع إذا تضمنت البيانات المعرضة للخطر معلومات حساسة والتي يجب الحصول على موافقة صريحة من الأشخاص المعنيين قبل جمعها أو معالجتها[٢٩].

أما في سلطنة عُمان، فتجميع المعلومات يمكن أن ينطوي على مجموعة من المخاطر التي يجب مراعاتها، بما في ذلك انتهاك الخصوصية والاستخدام غير المشروع لها،

كما يمكن أن يؤدي إلى انتهاك خصوصية الأفراد وتعريضهم لمخاطر مثل الاحتيال والتسويق غير المرغوب فيه، بالإضافة إلى ذلك، قد يشكل هدفًا للمتسللين السيبرانيين، مما يهدد أمانها وسلامتها، ويمكن أيضاً استخدام البيانات للتعديل أو التشويه بشكل غير مصرح به. كما قد يتم تبادل البيانات بين الجهات المختلفة بشكل غير آمن، مما يعرضها للخطر. ويمكن القول، بأن المشرع العماني قد تعامل مع تلك المسألة ووفر لها الحماية الدستورية والقانونية، وعلى الأفراد أن يكونوا حذرين وملتزمين بمشاركة معلوماتهم الشخصية فقط مع الجهات الموثوق بها، وأن يتبعوا الممارسات الأمنية عند التعامل مع البيانات الشخصية عبر الإنترنت[٣٠]. ففي النظام الدستوري العُماني، قد نص على حماية الحياة الخاصة والخصوصية وفقًا للمادة ٣٦ من النظام الأساسي للدولة رقم ٦ لسنة ٢٠٢١. وهذا يعني أن الخصوصية تُعَدّ حقًا دستوريًا في عُمان. بالإضافة إلى ذلك، تشمل القوانين مثل قانون الجزاء وقانون مكافحة جرائم تقنية المعلومات عقوبات على الأفعال التي تنتهك حرمة الحياة الخاصة. وهذا يعزز حماية الخصوصية ويوفر إطارًا قانونيًا لتحقيق العدالة في حالات الانتهاكات، فالمادة المادة (١٤) من المرسوم السلطاني رقم ٦ / ٢٠٢٢، المتعلق بقانون حماية البيانات الشخصية، تلزم المتحكمين بالبيانات باتخاذ إجراءات محددة قبل بدء معالجة أي بيانات شخصية. إذ تتضمن هذه الإجراءات "إشعار صاحب البيانات الشخصية كتابيا بعدة معلومات، مثل بيانات المتحكم والمعالج وبيانات الاتصال بمسؤول حماية البيانات الشخصية، والغرض من معالجة البيانات الشخصية، ووصف شامل لعملية المعالجة وإجراءاتها، وحقوق صاحب البيانات الشخصية مثل حق الوصول إلى البيانات وتصحيحها ونقلها وتحديثها، بالإضافة إلى أي معلومات أخرى قد تكون ضرورية لاستيفاء شروط المعالجة". أيضاً المادة (١٩) من ذات القانون، تلزم المتحكم في البيانات بالإبلاغ عن أي اختراق للبيانات الشخصية للوزارة، وصاحب البيانات الشخصية وفقًا للضوابط والإجراءات المحددة في اللائحة. يهدف هذا الإجراء إلى ضمان التعامل القانوني مع حالات اختراق البيانات وفقًا للقوانين واللوائح السارية.

المطلب الثاني : انتهاك الحق في الأمن : شهد العالم في السنوات المعاصرة تقدمًا

هائلًا في المجال التكنولوجي، الأمر الذي أحدث تحولات جذرية في مختلف جوانب الحياة، بما في ذلك المجال الجزائي. نتيجة لهذا التطور، ظهرت جرائم جديدة تعرف بالجرائم الرقمية، وهي الجرائم التي يتم ارتكابها باستخدام وسائل التكنولوجيا الحديثة، مثل الإنترنت والهواتف المحمولة. وسوف يتم تناول ذلك في فرعين، الأول يتناول الجرائم الرقمية، أما الفرع الثاني سيتم فيه تناول موقف المشرع العماني منها.

الفرع الأول- الجرائم الرقمية: تواجه الأمان الرقمي للأفراد والمؤسسات تحديات كبيرة، وتأتي جرائم الإنترنت والإرهاب الإلكتروني في مقدمة هذه التحديات. فقد يستغل الخارجين على القانون وسائل الإنترنت والتكنولوجيا لتبادل المعلومات، وتنظيم الأعمال غير المشروعة لتحقيق أغراضهم غير القانونية التي تشكل خطراً على الحقوق والحريات والمصالح العامة والخاصة، فضلاً عن ترهيبهم، حيث يعد الإرهاب الإلكتروني جزءًا لا يتجزأ من الجرائم الحديثة، إذ يهدف إلى تحقيق أهداف إرهابية باستخدام التكنولوجيا ووسائل الإنترنت. وقد استخدم "باري كولن Barry Collin "مصطلح "الإرهاب الإلكتروني" خلال فترة الثمانينات من القرن الماضي، ويُعد هذا المصطلح جزءًا من صور الجريمة المنظمة عبر الحدود الوطنية، التي تناولتها المادة الثالثة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة في عام ٢٠٠٠، وبروتوكولها الصادر في عام ٢٠٠٥[٣١].

في مجال الإرهاب الإلكتروني، يُلاحظ وجود مكاسب مالية وإغراءات تدفع ببعض الأفراد إلى القيام بأعمال القرصنة واختراق الحسابات المصرفية، ففي خلال السنوات الأخيرة، شهد العالم دخول عدد من القراصنة إلى نظام البورصة الأمريكية وقاموا بتزوير البيانات بهدف المضاربة الوهمية في السوق، فعلى سبيل المثال، في عام ٢٠١٣، قام قراصنة بقرصنة حساب وكالة الأنباء الأسوشيتيد برس على تويتر، ونشروا تقارير زائفة عن وقوع هجوم على البيت الأبيض، هذه الأنباء المزيفة أدت إلى خسائر سوقية تقدر ب ١٣٦ مليار دولار عندما تم تداولها على برامج تشغيل البورصة التي تستخدم الذكاء الاصطناعي[٣٢]. هناك عدة أسباب أدت إلى استخدام الإنترنت لأغراض غير

مشروعة، وأهم هذه الأسباب هو أن الإنترنت يوفر مجالًا واسعًا للتواصل والدعاية عن بعد لأية أغراض غير مشروعة بغض النظر عن البعد الجغرافي.

حقيقة الأمر إن الجرائم الرقمية تشكل أخطار جسيمة على حقوق وحريات الأفراد فضلاً عن المصالح العامة والخاصة، الأمر الذي يعتبر تحدياً أمام المشرعين لمواجهتها، فكان للمشرع العماني دوراً بارزاً للتصدي لها، وهذا ما سوف يتم تناوله في الفرع الثاني.

الفرع الثاني- موقف المشرع العماني من الجرائم الرقمية: في النظام الدستوري العُماني، يكفل النظام الأساسي في السلطنة رقم ٦ لسنة ٢٠٢١، الحق في الأمن وفقًا للمادة ٢٢ منه التي تنص على أن "الحياة الآمنة حق لكل إنسان، وتلتزم الدولة بتوفير الأمن والطمأنينة لمواطنيها ولكل مقيم على أراضيها." مما يعني أن سلطنة عمان تعبّر عن التزامها بحماية حقوق وحريات الإنسان من خلال نصوصها الدستورية وتشريعاتها الوطنية المعمول بها، فضلاً عن انضمامها إلى الميثاق العربي لحقوق الإنسان بموجب المرسوم السلطاني رقم ١٦ / ٢٠٢٣. حيث أكد الميثاق في المادة (٢/٣٥) على "عدم جواز فرض أي قيود على تلك الحقوق والحريات إلا بما ينص عليه التشريع المعمول به والضروري لصون الأمن القومي، أو السلامة العامة، أو النظام العام، أو لحماية الصحة العامة، أو الآداب العامة، أو لحماية حقوق الآخرين وحرياتهم".

أيضاً المشرع العماني في سبيل مواجهة كافة الجرائم، وتحقيق دولة القانون والمؤسسات واستتباب الأمن وحماية الحقوق والحريات خاصة من الجرائم الإلكترونية، أصدر المرسوم السلطاني رقم ١٢ لسنة ٢٠١١، بشأن قانون مكافحة جرائم تقنية المعلومات، حيث في المادة الأولى منه بين مفهوم تلك الجرائم بالنص على أنها " الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة، وتوزيع البيانات، والمعلومات بصيغتها المختلفة". إذ استخدام مثل هذه التقنيات التي تحتوي على كم هائل من المعلومات والبيانات الشخصية بالطرق غير المشروعة، يؤدي إلى انتهاك خصوصية الأشخاص أو التهديد بذلك، وربما استخدام تلك البيانات والمعلومات لغايات ارتكاب أفعال جرمية[٣٣]. تُظهر هذه الإجراءات الرؤية الحازمة للحكومة العمانية في التصدي للتحديات التي تتعلق بالأمان الرقمي ومواجهة سوء استخدام التكنولوجيا،

مما يعكس التزامها الراسخ بحماية أمن المجتمع والحفاظ على النظام.

المبحث الثاني : الفرص التي تفتحها التكنولوجيا لحماية الحقوق والحريات في سلطنة عمان

تمهيد وتقسيم: تعد التقنيات جزءًا أساسيًا من حياة الأفراد، وتأثيرها يمتد إلى مختلف المجالات الحياتية، وأصبحت ذات تأثير على الحقوق والحريات، حيث تسعى سلطنة عمان بشكل جدي للاستفادة من التكنولوجيا في تحقيق التقدم وحماية حقوق مواطنيها. التكنولوجيا الحديثة تعد أداة حيوية في تعزيز الأمان وحماية حقوق الأفراد وحرياتهم في المجتمعات المعاصرة، وفي سلطنة عمان، تشهد الجهود المستمرة لاستخدام التكنولوجيا في العديد من المجالات، وخاصة في المجال الأمني والقانوني، لتعزيز الأمان وصون حقوق الأفراد وحرياتهم. بالرغم من أن هناك اعتراضات تثار بخصوص استخدام التكنولوجيا القانونية كأداة للتنبؤ بنتائج القضايا بدلاً من دور القاضي في عملية اتخاذ القرارات، حيث تم ذكر هذا النقاش في قضية إريك لوميس، الذي وُجِّهت إليه خمس تهم جنائية في حادث إطلاق نار من سيارة على أخرى في عام ٢٠١٣، وعند صدور حكم المحكمة، أشار القاضي فيها إلى نتيجة تقييم برنامج "The COMPAS"فقط. وعند الاستئناف، قررت المحكمة العليا في ولاية ويسكونسن أن القاضي الذي يعتمد على برمجيات تقييم النصوص ذات المصدر المفتوح لإصدار الأحكام لا ينتهك بالضرورة المبادئ الدستورية المتعلقة بحقوق الإجراءات القانونية الواجبة وحق المتهم في المحاكمة العادلة، حتى لو لم يتم الكشف عن المنهجية المستخدمة في إنتاج التقييم للمحكمة أو للمتهم. ومع ذلك، ينبغي على القاضي ألا يعتمد بشكل حصري على تقييم البرنامج لدرجة الخطورة دون النظر إلى الأدلة الأخرى التي قد تؤكد على احتمالية عودة المتهم لارتكاب الجريمة[٣٤].

رفضت المحكمة العليا في الولايات المتحدة سماع القضية في يونيو ٢٠١٧[٣٥]، ويمكن أن يكون لهذا القرار عواقب وخيمة. فإذا بدأ القضاة تدريجيًا في اعتماد أساليب أنظمة الذكاء الاصطناعي، فإن ذلك قد يقوض مبادئ العدالة، بينما يمنح مبدأ الحق في المحاكمة العادلة المدعى عليه حقوقًا معينة، مثل معرفة الاتهامات الموجهة إليه

والأدلة المقدمة ضده، يمكن أن تكون الحقوق الفردية مهددة عندما تعتمد المحاكم أو السلطات الأخرى أحكامها جزئيًا أو كليًا على خوارزميات سرية، على الرغم من أنه قد يكون من المفيد أن يستفيد القضاة من الخوارزميات لتحسين جودة قراراتهم وتوحيدها، إلا أنهم لا ينبغي أبدًا أن يسمحوا للخوارزميات باتخاذ القرارات بدلاً منهم. وعلى ذلك، سوف يتناول هذا المبحث فيما يمكن أن تحدثه تقنيات الذكاء الاصطناعي من تأثير على الحق في الخصوصية في المطلب الأول، والحق في عدم التمييز في المطلب الثاني.

المطلب الأول : استخدام التكنولوجيا لدعم الحق في الخصوصية : يعالج الحق في الخصوصية الحرية الشخصية والاختيار الذاتي والاستقلال، إذ يتضمن هذا الحق القدرة على تحديد ما يُخفيه الفرد، وكيفية ومتى يتم الكشف عنه، ولمن يُكشف عن هذه المعلومات الخاصة بالأفراد[٣٦]. غالبًا ما يُستخدم مصطلحات مثل "الخصوصية" و"خصوصية المعلومات" و"خصوصية البيانات" و"حماية البيانات" بشكل مترادف للتأكيد على الحق في السيطرة على جمع ومعالجة البيانات الشخصية من قِبل الحكومات والكيانات الخاصة، سيتم تناول مفهوم الحياة الخاصة في الفرع الأول أما الفرع الثاني سيتم تخصيصه لموقف المشرع العماني من حماية الحياة الخاصة

الفرع الأول- مفهوم الحياة الخاصة وحمايتها: تناول الفقه العديد من المفاهيم لحق الحياة الخاصة أو الخصوصية، ومنهم من يعرفه بأنه "حق الإنسان في أن يترك وشأنه أو حقه في أن يترك في عزلته وممارسة حياته بعيدًا عن أي تلصص أو تطفل"، كما يُفهم الحق في الحياة الخاصة بما يتعلق بالحياة العائلية وأوقات الفراغ والحالة الصحية[٣٧]. ومما لا شك فيه أن الخصوصية في ظل الشبكة المعلوماتية مرتبطة بضرورة احترام سرية خصوصية الأفراد من مستخدمي تلك المواقع، سواء كانت هذه الخصوصية متعلقة بالبيانات أو الوقائع المخزنة في الحاسب الآلي للفرد أو الهاتف الذكي أو المواقع التي تم تخزينها عليها عبر مواقع التواصل الاجتماعي. ويُعتبر اختراق هذه الخصوصية عبر Facebook أو البريد الإلكتروني، والتجسس الإلكتروني، وإفشاء الأسرار الخاصة بالرسائل البريدية انتهاكًا للخصوصية. المشرع الأمريكي تصدى لحماية

الخصوصية للأفراد وأقر بهذه الحماية، حيث تم تكريس ذلك في الدساتير الأمريكية بأن "للإنسان الحق بالحياة والسعادة، وتوفير حياة آمنة، وأنه من غير الممكن تحققها إلا إذا تم منع الغير من التدخل في خصوصيات الأفراد".[٣٨]

الفرع الثاني- موقف المشرع العماني من حماية الحياة الخاصة:

الحق في الخصوصية يعد من الحقوق الأساسية للإنسان، لا يجوز التعرض له أو النيل منه، وقد نصت على حمايته كافة المواثيق والاتفاقيات الدولة، إذ في القرار الذي أصدرته الجمعية العامة للأمم المتحدة رقم ١٦٧/٦٨ الصادر في العام ٢٠١٣، والخاص بالحق في الخصوصية في العصر الرقمي قد دفع بالمفوض السامي لحقوق الإنسان في العام ٢٠١٤ إلى إصدار تقريره الخاص بالحق في الخصوصية في العصر الرقمي.[٣٩]

نظراً لخطورة جرائم تقنية المعلومات باعتبارها تمس حياة الإنسان الخاصة، فضلاً عن المؤسسات المالية والاقتصادية والأمنية، وما ترتبه من آثار خطيرة، كان لا بد للمشرع العماني أن يتصدى لها بالحماية، حيث صدر المرسوم السلطاني رقم ١٢لسنة ٢٠١١ بشأن قانون مكافحة جرائم تقنية المعلومات، الذي بين فيه صور الجرائم التقنية، وبذات الوقت حدد العقوبة الجزائية المقررة لكل صورة منها في المواد من ٣-٢٩ من القانون. وذلك امتثالاً للقواعد الدستورية التي وفرت تلك الحماية لحقوق الإنسان.

يعد هذا القانون نقلة نوعية شاملة تبين تحديات المشرع العماني في مواجهة الجرائم الناتجة عن التكنولوجيا، بعد أن كانت هناك تشريعات متفرقة في مواجهتها، إذ كان قبل ذلك قانون الجزاء العماني رقم ٧ لسنة ١٩٧٤، والمعدل بموجب المرسوم السلطاني رقم ٧٢ لسنة ٢٠٠١، حيث أضيف إليه فصل مكرر تحت عنوان " جرائم الحاسب الآلي" يجرم فيه الأفعال التي تعد جرائم إلكترونية وعلى الأخص منها انتهاك خصوصيات الغير أو التعدي على مكنونات أسرارهم، علماً بأنه كان أول قانون عربي يواجه تلك الجرائم، ثم تلا ذلك مع التطور والتحديث والمواجهة، صدر قانون الاتصالات رقم ٣٠ لسنة٢٠٠٢، الذي جرم بعض صور الجرائم الإلكترونية الخاصة بالتعدي على الخصوصية والسرية، ومع ذلك لم يرى المشرع العماني كفاية تلك النصوص القانونية، وأمام تطور الجرائم الإلكترونية والمواجهة والتحديات الحثيثة أصدر قانون مكافحة

جرائم تقنية المعلومات المشار إليه كتشريع خاص يعالج تلك الجرائم التكنولوجية المستحدثة، وذلك تماشياً وتطبيقاً للقواعد الدستورية. فالنظام الأساسي للدولة رقم ٦ لسنة ٢٠٢١، قد نص حماية حق الإنسان في حياته وكرامته وخصوصيته، فنجده في المادة ١٨ منه تنص على " الحياة والكرامة حق لكل إنسان، وتلتزم الدولة باحترامهما وحمايتهما وفقاً للقانون"، وفي المادة ٢٢ منه تنص على " الحياة الآمنة حق لكل إنسان، وتلتزم الدولة بتوفير الأمن والطمأنينة لمواطنيها ولك مقيم على أراضيها"، وفي المادة ٣٦ منه تنص على " للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات الإلكترونية بكافة أنواعها، والمراسلات الهاتفية، والبرقية، والبريدية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، فلا يجوز مراقبتها، أو تفتيشها، أو الاطلاع عليها، أو إفشاء سريتها، أو تأخيرها، أو مصادرتها، إلا في الأحوال التي يبينها القانون، ووفقاً للإجراءات المحددة فيه".

المطلب الثاني : استخدام التكنولوجيا لدعم الحق في عدم التمييز : تعتمد البرامج التكنولوجية على الخوارزميات التي قد تعمل على تعميق وتسريع عمليات فرز وتصنيف الأشخاص، أي التمييز، دون أي إمكانية للسيطرة على تأثيراتها على أولئك الذين قد يتأثرون بها. عليه سيتم تناول حق عدم التمييز في الإطار الدولي في الفرع الأول، أما الفرع الثاني سيتم تناول موقف المشرع العماني من حق عدم التمييز.

الفرع الأول- عدم التمييز في الإطار الدولي: هناك من يعرِف التمييز على أنه "أي معاملة غير عادلة للفرد بسبب عضويته في مجموعة معينة، مثل العرق أو الجنس أو اللون"، وما إلى ذلك[٤٠]. على سبيل المثال ومن خلال دراسة اللوغاريتمات التي تم تغذية الحاسوب الآلي بها في إدارة شرطة أوكلاند، بولاية "كاليفورنيا"، التي كان يقطنها نسبة عالية من السود والأمريكيين من أصول دول أمريكا اللاتينية، بشأن جريمة تعاطى المخدرات، وجدت الدراسة أن هذه الجريمة منتشرة بين السود والأمريكيين من أصول لاتينية، بينما أظهرت الإحصاءات في إدارة السجون أن جريمة تعاطى المخدرات منتشرة بين الأمريكيين في هذه المنطقة ككل، دون أن ترتبط بجماعة عرقية معينة، كما أظهرتها نتائج برامج الشرطة التنبؤية[٤١]. إذ أوضح "لاري

كرسنر"، المدعي العام في مقاطعة فيلادلفيا، أن النتائج التي أسفرت عنها برامج الشرطة التنبؤية في المقاطعة كانت متحيزة، حيث استبعدت العديد من المؤشرات الهامة مثل المستوى التعليمي والوضع الاقتصادي والوظيفي. وهذا يجعل من تلك النتائج غير موثوقة، وبالتالي يقلل من قدرتها على أن تكون أساسًا لاتخاذ القرارات الشرطية[٤٢].

لذلك، حق عدم التمييز يقتضي المساواة للجميع أمام القانون الذي يمنع التمييز القائم على أسس من "العرق أو الجنس أو الدين أو اللغة أو الأصل أو اللون وخلافه"، وهذا ما نصت عليه المواثيق الدولية، منها "العهد الدولي الخاص بالحقوق المدنية والسياسية في المادة ٢٦ منه" أيضاً " العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية في المادة الثالثة منه" ثم تم تكريسه بشكل واضح في الإطار المعياري للاتحاد الأوروبي، حسبما هو مبين في المادة ٢١ من لائحة "الرموز الفيدرالية"[٤٣]، والمادة ١٤ من "الاتفاقية الأوروبية لحقوق الإنسان"، بالإضافة إلى المواد ١-٢٥ من معاهدة "عمل الإتحاد الأوروبي"[٤٤]. إذا تم قياس هذه المعايير وتطبيقها، قد يُعتبر استخدام التقنية القانونية بطريقة معينة تمييزًا طبيعيًا لها[٤٥]. على سبيل المثال، في استخدام الشرطة للتنبؤات الجنائية، وجدت دراسة أن نظام COMPAS يتوقع أن يكون للمدعى عليه من البشرة السوداء تقييم أعلى للخطورة مما ينطبق عليه في الواقع، في حين أن المدعى عليه من البشرة البيضاء يظهر لديه معدلات أقل مما يتوقعه النظام[٤٦]. وبالرغم من أن البيانات المستخدمة في نظام COMPASلا تشمل معلومات عن جنس الفرد، إلا أن الجوانب الأخرى من البيانات المستخدمة قد تكون مرتبطة بالعرق، مما يمكن أن يؤدي إلى تباينات عنصرية في التنبؤات[٤٧]. هذا يطرح السؤال عن الإجراءات الضرورية لمعالجة هذه المسألة، والإجابة تكمن فيما اقترحه ألكسندر تيشبيريك؛ حيث يجب "أن تسير التقنية القانونية والذكاء الاصطناعي جنبًا إلى جنب مع حماية مبدأ عدم التمييز ضد الأشكال الجديدة للتمييز الاجتماعي في العصر الرقمي"[٤٨].

الفرع الثاني- موقف المشرع العماني من حق عدم التمييز : المشرع الدستوري

العماني وفقًا للمادة (٢١) من النظام الأساسي للدولة رقم ٦/ ٢٠٢١، أكد فيها على "المساواة بين جميع المواطنين أمام القانون، وتكافؤهم في الحقوق والواجبات العامة دون أي تمييز بسبب الجنس، أو الأصل، أو اللون، أو اللغة، أو الدين، أو المذهب أو الموطن أو المركز الاجتماعي". تأكيداً لالتزام السلطنة بحقوق وحريات الإنسان المنصوص عليها في النظام الأساسي، قامت السلطنة بالانضمام إلى الميثاق العربي لحقوق الإنسان بالمرسوم السلطاني رقم ١٦ / ٢٠٢٣، حيث يؤكد الميثاق في المادة (٣) على "حق كل فرد في التمتع بالحقوق والحريات المنصوص عليها فيه دون أي تمييز بسبب العرق، أو اللون، أو الجنس، أو اللغة، أو المعتقد الديني، أو الرأي، أو الفكر، أو الأصل الوطني، أو الاجتماعي، أو الثروة، أو الميلاد، أو الإعاقة البدنية، أو العقلية". وتتعهد الدول الأطراف في الميثاق باتخاذ التدابير اللازمة لضمان تكافؤ الفرص والمساواة الفعلية بين النساء والرجال في التمتع بجميع الحقوق المنصوص عليها فيه. يُمكن القول إن أنظمة الذكاء الاصطناعي قد تنتهك حق عدم التمييز، وبالتالي يتطلب وضع إطار تشريعي يضمن حماية تلك الحقوق والحريات الشخصية من المعالجة الآلية التي تعتمد على قواعد تمييزية، خاصة في مجال القرارات الإدارية المؤتمتة. عليه، التحديات والمعالجات التشريعية لمخاطر التكنولوجيا على الحقوق والحريات الفردية حثيثة من قبل المشرع العماني، والفرص متاحة لكل ما هو جديد في سبيل تحقيق الضمانات الدستورية والقانونية للحقوق والحريات الفردية.

الخاتمة

التكنولوجيا وتطورها المتزايد في العصر الرقمي، لها تأثيرها على الحقوق والحريات سواء إيجاباً أم سلبا، لا يمكن تجاهلها، وهي بحد ذاتها تحديات تواجه المجتمعات الإنسانية، حيث قدمت هذه الدراسة لبيان تلك التحديات والفرص التي تنشأ عن تأثيرها. وقد خلصت إلى النتائج والتوصيات الآتية:

أهم النتائج:

١. أظهر البحث أن التحول الرقمي يمكن أن يؤدي في بعض الأحيان إلى انتهاكات رقمية واختراقات للخصوصية، مما يشكل تهديدًا مباشرًا لحقوق المواطنين وحرياتهم.
٢. أوضح البحث أن التكنولوجيا تفتح أبوابًا أمام الجرائم الإلكترونية بكافة أشكالها بشكل متطور ومتزايد.
٣. كشفت البحث عن وجود فرص كبيرة يفتحها النقاش حول التكنولوجيا في دعم الحق في الخصوصية وحق عدم التمييز، مما يسهم في تعزيز حماية حقوق وحريات المواطنين.
٤. أظهر البحث تصدي التشريعات العمانية لحماية الحقوق والحريات دستورياً وقانوناً من تأثيرات التكنولوجيا عليها.

التوصيات:

١. يؤمل التحديث المستمر وتعزيز التشريعات المتعلقة بحماية الحقوق والحريات في العصر الرقمي وبالأخص النظام الأساسي، لتكون متسقة مع التطورات التكنولوجية المستمرة.
٢. تعزيز الوعي بين المواطنين حول التهديدات الرقمية وكيفية حماية خصوصيتهم وحقوقهم الرقمية، من خلال حملات توعية وبرامج تثقيفية.

قائمة المراجع

أولا: قائمة المراجع باللغة العربية:

- باسم محمد فاضل مدبولي، المسئولية المدنية عن أضرار معالجة البيانات الرقمية، دراسة مقارنه، في ضوء اللائحة الأوروبية العامة (٦٧٩) لسنة ٢٠١٦ والقانون المصري ١٥١ لسنة ٢٠٢٠، دار الفكر الجامعي، الإسكندرية، ٢٠٢٣.
- بارق منتظر لامي، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، ٢٠١٧.
- جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، الأحكام الموضوعية

المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠١٠.

- حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة – الحق في الخصوصية – دراسة مقارنة، دار النهضة العربية للطبع والنشر والتوزيع، بدون سنة نشر.
- حسين سليم محمد سليم، الحماية الجنائية للبيانات الشخصية المعالجة آليا: دراسة مقارنة، مجلة العلوم القانونية الاقتصادية، جامعة عين شمس – كلية الحقوق، ٢٠٢٠.
- خالد عطوي، أثر الثورة التكنولوجية على حقوق الإنسان، مجلة الدراسات القانونية والسياسية، المجلد٨، العدد١ ، جانفي، ٢٠٢٢.
- دينا عبد العزيز فهمي، المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مجلة كلية الحقوق، جامعة طنطا، ٢٠١٧.
- دونا إبراهيم جلال، تقنية الذكاء الاصطناعي، رسالة ماجستير، كلية الحقوق، الجامعة اللبنانية، بيروت، لبنان، ٢٠٢١.
- رقية بنت خلفان بن ناصر العبدلية، حوكمة البيانات وفاعلية تطبيقها في المؤسسات الحكومية في سلطنة عمان، رسالة ماجستير، كلية الآداب والعلوم الاجتماعية – جامعة السلطان قابوس، ٢٠٢٢.
- سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية، المجلد ٣، العدد ٩، ٢٠١٥.
- سيف بن عبد االله الجبري، المكتبة الرقمية ودورها في بناء وتطوير مجتمع المعرفة التحدياتً الاجتماعية والثقافية واللغوية في العالم حاضرا ومستقبلا، المؤتمر العلمي لكلية الآداب والعلوم الاجتماعية، ٢٠٠٧.
- علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص

والحكومة- دراسة مقارنة، منشورات زين الحقوقية، بيروت، ٢٠١٣.

- عمر محمد سالم، مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي، المراقبة الإلكترونية والتحقيق الجنائي عن بعد، دار النهضة العربية، القاهرة، ٢٠١٣م.
- عمرو طه بدوي محمد، التنظيم القانوني لمعالجة البيانات الشخصية، دراسة تطبيقية على معالجة تسجيلات المراقبة البصرية، دار النهضة العربية، القاهرة، ٢٠٢٠.
- غيث محمد عاطف، قاموس علم الاجتماع، دار المعرفة الجامعية، الإسكندرية، ١٩٩٩.
- فتحي محمد عبد السلام الفقي، معالجة البيانات الشخصية عبر المواقع الإلكترونية والعلاقة التعاقدية الناشئة عنها، ط١، دراسة مقارنه، دار مصر، القاهرة، ٢٠٢٣.
- فضيل دليو، تكنولوجيا الإعلام والاتصال الجديدة بعض تطبيقاتها التقنية، دار هومة للطباعة والنشر، الجزائر، ٢٠١٢.
- محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنه، مجلة كلية الشريعة والقانون، جزء٤، طنطا، العدد ٣٣.
- محمد موسي على شحاته، انعكاسات تفعيل آليات التحول الرقمي في ضوء مبادرات الشمول المالي على تطبيقات الحكومة الإلكترونية بجمهورية مصر العربية ، مجلة الدراسات المعاصرة، العدد٩ ، ٢٠٢٠.
- محمود إبراهيم الغازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، ٢٠١٤.
- محمود عبد الرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية "الحق في الخصوصية المعلوماتية" مجلة كلية القانون الكويتية العالمية، العدد التاسع السنة

الثالثة، مارس ٢٠١٥.

- مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية، الجيزة، ٢٠١٦.
- مصطفى أحمد أمين، التحول الرقمي في الجامعات المصرية، كمتطلب لتحقيق مجتمع المعرفة، مجلة الإدارة التربوية، العدد١٩، ٢٠١٨.
- منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة، مجلة كلية بغداد للعلوم الاقتصادية، ٢٠١٣.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨.
- نوال بنت علي بن عبد الله البلوشية، التحول الرقمي في سلطنة عمان والعوامل المؤثرة في من وجهة نظر متخذي القرار في سلطنة عمان، رسالة ماجستير، كلية الآداب والعلوم الاجتماعية، جامعة السلطان قابوس، ٢٠١٩.
- نوال بنت علي بن عبد الله البلوشية، العوامل المساعدة على التحول الرقمي في سلطنة عمان، الاتحاد العربي للمكتبات والمعلومات، العدد٢٦، ٢٠٢٠.
- هدى حامد قشقوش، جرائم الحاسب الآلي الإلكترونية في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢.
- هشام محمد رستم، جرائم الحاسب المستحدثة، دار الكتب القانونية، القاهرة، ١٩٩٩.
- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ١٩٩٢.

ثانيا: قائمة المراجع باللغة الأجنبية:

- Aaron Shapiro, Comment, Reform Predictive Policing, Nature, Vol. 541, 2017.
- Bryce Goodman, Seth Flaxman, European Union regulations on algorithmic decision-making and a 'Right to Explanation'. AI Magazine, Vol. 38 No. 3, 2017.
- Gabriele Buchholtz, Artificial Intelligence and Legal Tech: Challenges to the Rule of Law, THE IRISH TIMES, Springer Nature Switzerland AG 2020, 2018.
- Horst Eide Mueller, The rise of robots and the law of humans, FACULTY OF LAW BLOGS, UNIVERSITY OF OXFORD, 2017.
- Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, Machine bias. ProPublica, New York, 2016,
- Julia Dressel, Hany Farid, "The accuracy, fairness, and limits of predicting recidivism, Science Advances, Vol. 4, no. 1, eaao5580, 2018.
- Nadia Rossbach, Innocent until predicted guilty: how premature predictive policing can lead to a self-fulfilling prophecy of juvenile delinquency, *Florida Law Review*, Vol. 75,
- Nadiah Kerisha Kadir and Judhariksawan, Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes, Fiat Justisia Jurnal Ilmu Hukum, Vol. 13 (4), 2019.

. Tom C.W. Lin, Artificial Intelligence, Finance, and the Law Artificial Intelligence, Finance, and the Law, *Fordham L. Rev.*, Vol. 88(2), 2019.

الهوامش

[1] د. هشام محمد رستم، جرائم الحاسب المستحدثة، دار الكتب القانونية، القاهرة، ١٩٩٩، ص ١٠٩.

[2] د. هدى حامد قشقوش، جرائم الحاسب الآلي الإلكترونية في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢، ص ١٠.

[3] د. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الأحكام الموضوعية المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٦.

[4] د. عمر محمد سالم، مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي، المراقبة الإلكترونية والتحقيق الجنائي عن بعد، دار النهضة العربية ، القاهرة، ٢٠١٣م، ص ٢٧.

[5] د. هشام محمد رستم، مرجع سابق ص ١٠٩.

[6] د. فضيل دليو، تكنولوجيا الإعلام والاتصال الجديدة بعض تطبيقاتها التقنية، دار هومة للطباعة والنشر، الجزائر، ٢٠١٢، ص ٢٠.

[7] د. غيث محمد عاطف، قاموس علم الاجتماع، دار المعرفة الجامعية، الإسكندرية، ١٩٩٩، ص ٢٦٥.

[8] د. سيف بن عبد الله الجبري، المكتبة الرقمية ودورها في بناء وتطوير مجتمع المعرفة التحديات الاجتماعية والثقافية واللغوية في العالم حاضرا ومستقبلا، المؤتمر العلمي لكلية الآداب والعلوم الاجتماعية، ٢٠٠٧، ص ١٥.

[9] د. مصطفي أحمد أمين، التحول الرقمي في الجامعات المصرية، كمتطلب لتحقيق مجتمع المعرفة، مجلة الإدارة التربوية، العدد ١٩، ٢٠١٨، ص ٢١.

[10] نوال بنت علي بن عبد الله البلوشية، التحول الرقمي في سلطنة عمان والعوامل المؤثرة في من وجهة نظر متخذي القرار في سلطنة عمان، رسالة ماجستير، كلية الآداب والعلوم الاجتماعية، جامعة السلطان قابوس، ٢٠١٩، ص ١١.

[11] د. مصطفي أحمد أمين، التحول الرقمي في الجامعات المصرية، كمتطلب لتحقيق مجتمع المعرفة، مجلة الإدارة التربوية، العدد ١٩، ٢٠١٨، ص ١٩.

[12] د. محمد موسي على شحاته، انعكاسات تفعيل آليات التحول الرقمي في ضوء مبادرات الشمول المالي على تطبيقات الحكومة الإلكترونية بجمهورية مصر العربية، مجلة الدراسات المعاصرة، العدد ٩، ٢٠٢٠ ص ٢٠٦.

[13] نوال بنت علي بن عبدالله البلوشية، مرجع سابق ص ٤٨.

[14] د. فتحي محمد عبد السلام الفقي، معالجة البيانات الشخصية عبر المواقع الإلكترونية والعلاقة التعاقدية الناشئة عنها دراسة مقارنه، دار مصر، القاهرة، ٢٠٢٣، الطبعة الأولى، ص ٧.

[15] د. باسم محمد فاضل مدبولي، المسئولية المدنية عن أضرار معالجة البيانات الرقمية، دراسة مقارنه، في ضوء اللائحة الأوروبية العامة (٦٧٩) لسنة ٢٠١٦ والقانون المصري ١٥١ لسنة ٢٠٢٠، دار الفكر الجامعي، الإسكندرية، ٢٠٢٣، ص٩.

[16] د. عمرو طه بدوي محمد، التنظيم القانوني لمعالجة البيانات الشخصية، دراسة تطبيقية علي معالجة تسجيلات المراقبة البصرية، دار النهضة العربية، القاهرة، ٢٠٢٠، ص ١٠

[17] د. سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية، المجلد ٣، العدد ٩، ٢٠١٥، ص ٣٩٨.

[18] د. باسم محمد فاضل مدبولي، المسئولية المدنية عن أضرار معالجة البيانات الرقمية، دراسة مقارنه، في ضوء اللائحة الأوروبية العامة (٦٧٩) لسنة ٢٠١٦ والقانون المصري ١٥١ لسنة ٢٠٢٠، دار الفكر الجامعي، الإسكندرية، ٢٠٢٣، ص ٢٣.

[19] د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ١٩٩٢، ص١٧٩ وما بعدها.

[20] د. محمود عبد الرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية "الحق في الخصوصية المعلوماتية" مجلة كلية القانون الكويتية العالمية، العدد التاسع السنة الثالثة، مارس ٢٠١٥، ص١٠٩؛

[21] الكوكيز عبارة عن ملفات نصية تضعها معظم مواقع الويب على القرص الصلب في الخاص بالمتصفح (الزائر)، عند زيارته لهذه المواقع، بغرض جمع بعض المعلومات عن المستخدم، تتيح للموقع الذي أودعها أن يسترجعها عند الحاجة اليها، ومكمن الخطورة في هذه الملفات انه من الممكن استغلالها في انتهاك خصوصية المستخدمين وجمع معلومات عنهم خلال تصفحهم لمواقع الويب المختلفة.

[22] المرسوم السلطاني رقم ٦٩ لسنة ٢٠٠٨ بشأن صدور قانون المعاملات الإلكترونية، نشر في الجريدة الرسمية العدد ٨٦٤ بتاريخ ١ / ٦ / ٢٠٠٨م.

[23] د. دينا عبد العزيز فهمي، المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مجلة كلية الحقوق، جامعة طنطا، ٢٠١٧، ص ١٥.

[24] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨، ص ١٦٧.

[25] د. محمود إبراهيم الغازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية، ٢٠١٤، ص ٢٠، ٢١.

[26] د. مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية، الجيزة، ٢٠١٦، ص٣٢٣.

[27] د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة- دراسة مقارنة، منشورات زين الحقوقية، بيروت، ٢٠١٣، ص ٤٠٨ وما بعدها.

[28] د. منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة، مجلة كلية بغداد للعلوم الاقتصادية، ٢٠١٣، ص ١٠.

[29] د. حسين سليم محمد سليم، الحماية الجنائية للبيانات الشخصية المعالجة آليا: دراسة مقارنة، مجلة العلوم القانونية الاقتصادية، جامعة عين شمس – كلية الحقوق، ٢٠٢٠، ص ٤٥.

[30] أنظر رقية بنت خلفان بن ناصر العبدلية، حوكمة البيانات وفاعلية تطبيقها في المؤسسات الحكومية في سلطنة عمان، رسالة ماجستير، كلية الآداب والعلوم الاجتماعية – جامعة السلطان قابوس، ٢٠٢٢، ص ٨٥ وما بعدها.

[31] Nadiah Khaeriah Kadir and Judhariksawan, Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes, Fiat Justisia Jurnal Ilmu Hukum, Vol. 13 (4), 2019, p.335.

[32] Tom C.W. Lin, Artificial Intelligence, Finance, and the Law Artificial Intelligence, Finance, and the Law, Fordham L. Rev., Vol. 88(2), 2019, p. 541.

[٣٣] دونا إبراهيم جلال، تقنية الذكاء الاصطناعي، رسالة ماجستير، كلية الحقوق، الجامعة اللبنانية، بيروت، لبنان، ٢٠٢١، ص٢٢.

[34] State of Wisconsin v. Eric Loomis, 7. 881 N.W.2d 749 (Wis. 2016).

[35] Eric Loomis v. State of Wisconsin No. 16-6387.

[٣٦] د. حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة – الحق في الخصوصية – دراسة مقارنة، دار النهضة العربية للطبع والنشر والتوزيع، بدون سنة نشر، ص ٧٦ وما بعدها

[٣٧] د. محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنه، مجلة كلية الشريعة والقانون بطنطا، العدد ٣٣، الجزء الرابع، ص ٢٠٠١.

[٣٨] بارق منتظر لامي، جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، ٢٠١٧، ص٨٥-٨٦.

[٣٩] خالد عطوي، أثر الثورة التكنولوجية على حقوق الإنسان، مجلة الدراسات القانونية والسياسية، المجلد٨، العدد٠١، جانفي، ٢٠٢٢، ص٧٦.

[40] Andrew Altman, Discrimination, In: Zalta EN (ed) The Stanford encyclopedia of philosophy. Stanford University, Stanford. Winter 2016 edn, 2015. plato.stanford.edu/archives/win2016/entries/ discrimination. Accessed 4 March 2020.

[41] Aaron Shapiro, Comment, Reform Predictive Policing, Nature, Vol. 541, 2017, pp. 458- 460.

[42] Nadia Rossbach, Innocent until predicted guilty: how premature predictive policing can lead to a self-fulfilling prophecy of juvenile delinquency, *Florida Law Review*, Vol. 75, 2023, p.181,

[٤٣] وهو قانون اللوائح الفدرالية وىقصد بها القواعد واللوائح العامة والدائمة المنشورة في السجل الفيدرالي من قبل الإدارات والوكالات التنفيذية للحكومة الفيدرالية للولايات المتحدة. ويتم تقسيمه إلى ٥٠ مادة.

[44] Bryce Goodman, Seth Flaxman, European Union regulations on algorithmic decision-making and a 'Right to Explanation'. AI Magazine, Vol. 38 No. 3, 2017, p. 53.

[45] Gabriele Buchholtz, Artificial Intelligence and Legal Tech: Challenges to the Rule of Law, THE IRISH TIMES, Springer Nature Switzerland AG 2020, 2018, p. 189.

[46] Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, Machine bias. ProPublica, New York, 2016,

[47] Julia Dressel, Hany Farid, The accuracy, fairness, and limits of predicting recidivism, Science Advances, Vol. 4, no. 1, eaao5580, 2018, p. 2.

[48] Horst Eidenmueller, The rise of robots and the law of humans, FACULTY OF LAW BLOGS, UNIVERSITY OF OXFORD, 2017, p. 76.