ISSN-2032-2075 مجلة رسالة الحقوق
الإصدار (17) العدد الثاني
أبريل – مايو – يونيو 2025

المسؤولية الرقمية للشركات: دراسة تحليلية
Corporate Digital Responsibility: Analytical Study

بحث مقدم من قبل
أ.م. د عقيل كريم زغير
كلية القانون / جامعة كربلاء
Aqeel.k@uokerbala.edu.iq

الخلاصة:
برزت المسؤولية الرقمية للشركات كإطار مهم لضمان الاستخدام الأخلاقي والمسؤول للتكنولوجيات الرقمية من قبل الشركات. ومع تسارع التحول الرقمي على مستوى العالم، أصبحت الحاجة إلى أطر قانونية قوية لحكم سلوك الشركات في المجال الرقمي واضحة بشكل متزايد. يتناول هذا البحث الأسس القانونية للمسؤولية الرقمية للشركات، مع التركيز على مجالات رئيسية مثل خصوصية البيانات والمساءلة الخوارزمية والأمن السيبراني وحقوق أصحاب المصلحة. كما يستكشف هذا البحث دور المعايير الدولية واللوائح الوطنية وحوكمة الشركات في تشكيل ممارسات المسؤولية الرقمية للشركات. ومن خلال تحليل الأطر القانونية العامة، تسلط هذه الدراسة الضوء على التحديات والفرص في تنفيذ المسؤولية الرقمية للشركات وتقدم توصيات لصناع السياسات والشركات.
الكلمات المفتاحية: المسؤولية الرقمية، الاستخدام الأخلاقي للتكنلوجيا، الامن السيبراني، التكنلوجيا الرقمية.

Abstract:
Corporate digital responsibility has emerged as an important framework for ensuring the ethical and responsible use of digital technologies by corporations. As digital transformation accelerates globally, the need for robust legal frameworks to govern corporate behavior in the digital sphere has become increasingly evident. This article examines the legal foundations of corporate digital responsibility, focusing on key areas such as data privacy, algorithmic accountability, cybersecurity, and stakeholder rights. It also explores the role of international standards, national regulations, and corporate governance in shaping corporate digital responsibility practices. By analyzing general legal frameworks, this study highlights the challenges and opportunities in implementing corporate digital responsibility and provides recommendations for policymakers and companies.
Keywords: Digital Responsibility, Ethical use of Technology, Cybersecurity, Digital Technology.

المقدمة

في عصر حيث تعمل التحولات الرقمية على إعادة تشكيل الصناعات، برز مفهوم المسؤولية الرقمية للشركات (CDR) كإطار مهم لضمان ممارسات الأعمال الأخلاقية والمسؤولة في المجال الرقمي. ومع اعتماد الشركات بشكل متزايد على التقنيات القائمة على البيانات والذكاء الاصطناعي والمنصات الرقمية، أصبحت الحاجة إلى إطار قانوني قوي لحكم مسؤولياتها أمرًا بالغ الأهمية. يستكشف هذا البحث الأبعاد القانونية للمسؤولية الرقمية للشركات، ويفحص كيف تعالج القوانين واللوائح والسياسات الناشئة الحالية قضايا مثل خصوصية البيانات والشفافية الخوارزمية والأمن السيبراني والاستخدام الأخلاقي للتكنولوجيا. من خلال تحليل التفاعل بين المساءلة الشركاتية والامتثال القانوني، تهدف هذه الدراسة إلى تسليط الضوء على أهمية الإطار القانوني المنظم في تعزيز الثقة والاستدامة والابتكار في الاقتصاد الرقمي. عليه تناول هذا البحث دراسة مفهوم المسؤولية الرقمية للشركات والإطار القانوني لها ثم حوكمة المسؤولية الرقمية للشركات وتحديات تنفيذها مقسما على ثلاثة مباحث تناولناها تباعا بالآتي:

المبحث الأول: مفهوم المسؤولية الرقمية للشركات

نتناول في هذا المبحث تعريف المسؤولية الرقمية للشركات وعوامل ظهورها وعلاقتها بالمسؤولية الاجتماعية للشركات في ثلاثة مطالب بالآتي:

المطلب الاول: تعريف المسؤولية الرقمية للشركات

عرفت المسؤولية الرقمية للشركات بانها الاستخدام الأخلاقي والمسؤول للتكنولوجيات الرقمية من قبل الشركات لخلق تأثير اجتماعي إيجابي مع التخفيف من المخاطر والآثار الخارجية السلبية.[1] وذهب اخر الى انها الالتزامات والتعهدات التي تتحملها الشركات تجاه أصحاب المصلحة في المجال الرقمي. ويشمل ذلك ممارسات البيانات المسؤولة، وتطوير الذكاء الاصطناعي الأخلاقي، وتدابير الأمن السيبراني، وحماية الحقوق الرقمية.[2] أي ان مسؤولية الشركات الرقمية هي المبدأ الذي ينص على أن الشركات لديها واجب رعاية المجتمع عند تطوير ونشر وإدارة التقنيات الرقمية، وهذا ينطوي على إعطاء الأولوية للممارسات الأخلاقية والمستدامة والشاملة عبر سلسلة القيمة الرقمية.[3] وعرفها جانب اخر بانها دمج الاعتبارات الرقمية في استراتيجية المسؤولية الاجتماعية الشاملة للشركة، وهي تتطلب من الشركات مراعاة الآثار الاجتماعية والبيئية والحوكمة لمنتجاتها وخدماتها وعملياتها الرقمية.[4] ويرى جانب اخر بانها مجموعة المبادئ والممارسات التي توجه استخدام المؤسسة للتكنولوجيات الرقمية لخلق قيمة لأصحاب المصلحة مع الحفاظ على المصالح المجتمعية والمعايير الأخلاقية.[5] تسلط هذه التعريفات الضوء على الطبيعة المتعددة الجوانب للمسؤولية الرقمية للشركات، والتي تشمل إدارة البيانات وأخلاقيات الذكاء الاصطناعي والأمن السيبراني والحقوق الرقمية والتأثير المجتمعي الأوسع للتكنولوجيات الرقمية. وهي تؤكد على الحاجة إلى أن تتبنى الشركات نهجًا شاملاً يركز على أصحاب المصلحة في ممارساتها وابتكاراتها الرقمية. عليه يمكن تعريف المسؤولية الرقمية للشركات بانها مجموعة من الممارسات والمبادئ التي تُوجّه كيفية إدارة الشركات لأصولها الرقمية وبياناتها وابتكاراتها التكنولوجية بما يعود بالنفع على أصحاب المصلحة والمجتمع والبيئة.

المطلب الثاني: ظهور المسؤولية الرقمية للشركات

لقد تطور مفهوم مسؤولية الشركات بشكل كبير على مر السنين، حيث توسع من المسؤولية الاجتماعية للشركات التقليدية ليشمل الأبعاد الرقمية في إطار المسؤولية الرقمية للشركات. ومع ذلك، فقد أدى ظهور التقنيات الرقمية إلى إدخال تحديات جديدة، مما دفع إلى توسيع نطاق المسؤولية الاجتماعية للشركات لتشمل المسؤوليات الرقمية. ويعكس هذا التطور الاعتراف المتزايد بالدور الذي تلعبه الشركات في معالجة التحديات العالمية مثل عدم المساواة والتدهور البيئي وانتهاكات حقوق الإنسان. ويعزى هذا التطور الى عاملين موضوعيين هما:

1- التطور السريع للتكنلوجيا الرقمية

لقد أدى التقدم السريع للتكنولوجيات الرقمية إلى ظهور مجموعة من التحديات الناشئة، مما دفع الحاجة إلى اتباع نهج شامل للمسؤولية الرقمية للشركات. اذ ان النمو الهائل في توليد البيانات، إلى جانب صعود تحليلات البيانات المتطورة والتعلم الآلي، ادى إلى زيادة المخاوف بشأن خصوصية البيانات والتحيز الخوارزمي وإساءة استخدام المعلومات الشخصية. ولمواجهة هذه التحديات يتطلب من الشركات أن تتبنى ممارسة بيانات مسؤولة للتخفيف من المخاطر وبناء الثقة.[6] بالإضافة الى التأكيد على أهمية تطوير الذكاء الاصطناعي الأخلاقي، اذ أظهر النشر المتزايد لأنظمة الذكاء الاصطناعي عبر وظائف الأعمال قضايا مثل النتائج التمييزية والافتقار إلى الشفافية في اتخاذ القرارات الخوارزمية مما دفع الشركات والمؤسسات إلى تنفيذ أطر حوكمة قوية للذكاء الاصطناعي لضمان العدالة والمساءلة.[7] كما أن انتشار تقنيات إنترنت الأشياء والحجم المتزايد لبيانات المستشعرات أدى إلى ظهور ثغرات جديدة في الأمن السيبراني ومخاطر الخصوصية، مما جعل من الضروري للشركات إعطاء الأولوية للنشر الآمن والمسؤول لأنظمة إنترنت الأشياء لحماية أصول الشركة ومصالح المستهلكين.[8] بالإضافة إلى ذلك، أن صعود المنصات الرقمية والأسواق عبر الإنترنت أدى إلى تضخيم المخاوف بشأن تعديل المحتوى والحقوق الرقمية وإمكانية احتكار المنصات لقمع المنافسة والحد من اختيار المستهلك. وهذا ما اوجب على الشركات العاملة في هذه المساحات معالجة هذه التحديات للحفاظ على الثقة المجتمعية وضمان الممارسات العادلة.[9]

علاوة على ذلك، أثارت أتمتة المهام وتعطيل نماذج التوظيف التقليدية مخاوف بشأن تشريد الوظائف وحقوق العمال والحاجة إلى إعادة التدريب والارتقاء بالمهارات. ونتيجة لذلك، يُطلب من الشركات النظر في التأثير الاجتماعي لمبادرات التحول الرقمي وتطوير استراتيجيات لدعم قوتها العاملة.[10] وأخيرًا، أصبح التأثير البيئي للتكنولوجيات الرقمية، مثل استهلاك الطاقة في مراكز البيانات وتوليد النفايات الإلكترونية، قضية ملحة، ومن المتوقع الآن أن تعالج الشركات الاستدامة البيئية لعملياتها ومنتجاتها الرقمية للحد من بصمتها البيئية.[11]

2- توقعات أصحاب المصلحة والضغوط التنظيمية

لقد لعبت توقعات أصحاب المصلحة والضغوط التنظيمية دورًا محوريًا في تشكيل تطور المسؤولية الرقمية للشركات. حيث أصبحت الشركات مسؤولة بشكل متزايد امام أصحاب المصلحة المختلفين لإظهار الممارسات الأخلاقية والمسؤولة في عملياتها الرقمية. على سبيل المثال، أصبح العملاء أكثر وعيًا بقضايا خصوصية البيانات ويطالبون بمزيد من الشفافية والأمان في كيفية التعامل مع معلوماتهم الشخصية.[12] وبالمثل، يعرب الموظفون عن مخاوفهم بشأن تأثير التحول الرقمي على الأمن الوظيفي والتوازن بين العمل والحياة والحاجة إلى التعلم والتطوير المستمر. وقد أدى هذا إلى زيادة التوقعات للشركات لإعطاء الأولوية لرفاهية القوى العاملة والاستثمار في مبادرات إعادة التدريب.[13] كما لعب المستثمرون أيضًا دورًا رئيسيًا في دفع تبني المسؤولية الرقمية للشركات. وبإدراك المخاطر المالية والسمعية المرتبطة بالممارسات الرقمية غير المسؤولة، يدمج المستثمرون بشكل متزايد معايير البيئة والمجتمع والحوكمة (ESG)، بما في ذلك تدابير المسؤولية الرقمية، في عمليات صنع القرار الخاصة بهم.[14] وعلى الصعيد التنظيمي، تقدم الحكومات والهيئات الدولية قوانين وإرشادات أكثر صرامة لحكم الممارسات الرقمية للشركات. على سبيل المثال، وضعت اللائحة العامة لحماية البيانات (GDPR)للاتحاد الأوروبي وقانون الذكاء الاصطناعي المقترح معايير صارمة لحماية البيانات والاستخدام الأخلاقي للذكاء الاصطناعي.[15] حيث إن عدم الامتثال لهذه اللوائح يمكن أن يؤدي إلى عقوبات مالية كبيرة وعواقب قانونية وأضرار في السمعة، مما يجبر الشركات على إعطاء الأولوية للمسؤولية الرقمية للشركات.[16] بالتالي إن الشركات التي تفشل في تلبية توقعات أصحاب المصلحة والمتطلبات التنظيمية تخاطر بفقدان ثقة المستهلك، وتكافح من أجل جذب المواهب والاحتفاظ بها، وتعريض قدرتها على الاستمرار في العمل على المدى الطويل.[17] ولمعالجة هذه الضغوط، تعمل المؤسسات بشكل متزايد على دمج المسؤولية الرقمية في استراتيجياتها المؤسسية وأطر الحوكمة الخاصة بها، مع الاعتراف بها كمكون أساسي لمسؤوليتها الاجتماعية واستدامة أعمالها.[18] وقد كان الاتحاد الأوروبي في طليعة من عالج المسؤولية الرقمية للشركات من خلال الأطر التنظيمية الشاملة. وبإدراك التحديات التي تفرضها التقنيات الرقمية، طور الاتحاد الأوروبي مبادرات مثل قانون الخدمات الرقمية وقانون الأسواق الرقمية لتنظيم المنصات الرقمية وضمان تعديل المحتوى المسؤول.[19] وتهدف هذه المبادرات إلى مواءمة أنشطة الشركات الأوروبية مع التزام الاتحاد الأوروبي بحقوق الإنسان والشفافية والمساءلة. فقد تبنت الولايات المتحدة نهجًا أكثر لامركزية تجاه المسؤولية الرقمية، مع توزيع السلطة التنظيمية عبر وكالات فيدرالية متعددة. وتشمل الوكالات الرئيسية المشاركة في التنظيم الرقمي لجنة التجارة الفيدرالية (FTC)، ووزارة العدل(DOJ) ولجنة الاتصالات الفيدرالية (FCC)، ولكل وكالة تفويض محدد، مثل إنفاذ قوانين مكافحة الاحتكار، وحماية المستهلك، وتنظيم الاتصالات.[20] عليه فان تطور المسؤولية الرقمية للشركات يسلط الضوء على التحول التدريجي من التركيز الضيق على خصوصية البيانات والأمن السيبراني إلى فهم أكثر شمولاً للتأثيرات الأخلاقية والاجتماعيةوالبيئية للممارسات الرقمية للشركات، مما أدى في النهاية إلى ظهور مفهوم شامل للمسؤولية الرقمية للشركات.

المطلب الثالث: المسؤولية الرقمية للشركات وعلاقتها بالمسؤولية الاجتماعية للشركات

المسؤولية الرقمية للشركات والمسؤولية الاجتماعية للشركات عبارة عن أطر مترابطة توجه الشركات في التعامل مع مسؤولياتها الأخلاقية والاجتماعية والبيئية. وفي حين ركزت المسؤولية الاجتماعية للشركات تقليديًا على التأثير الأوسع للشركةعلى المجتمع،فإن المسؤولية الرقمية للشركات تتناول على وجه التحديد الاستخدام الأخلاقي والمسؤول للتكنولوجيات الرقميةويمكن استكشاف العلاقة بين المسؤولية الرقمية والمسؤولية الاجتماعية للشركات من عدة جوانب هي:

1 .من حيث المفهوم

تشير المسؤولية الرقمية للشركات إلى التزام الشركة بالعمل بطريقة مستدامة اقتصاديًا واجتماعيًا وبيئيًا. وهي تشمل المبادرات التي تفيد المجتمع، مثل الحد من انبعاثات الكربون، وتعزيز ممارسات العمل العادلة، ودعم التنمية المجتمعية.[21] بينما تركز المسؤولية الرقمية للشركات على الاستخدام الأخلاقي والمسؤول للتكنولوجيات الرقمية، بما في ذلك خصوصية البيانات والأمن السيبراني والمساءلة الخوارزمية والتأثير المجتمعي للابتكارات الرقمية، حيث تضمن المسؤولية الرقمية للشركات معالجة الشركات للتحديات الفريدة التي يفرضها التحول الرقمي.[22]

2 .التطور من المسؤولية الاجتماعية للشركات إلى المسؤولية الرقمية للشركات

لقد أدى ظهور التقنيات الرقمية إلى توسيع نطاق المسؤولية الاجتماعية للشركات، مما أدى إلى ولادة المسؤولية الرقمية للشركات كمجال متخصص. في حين تعالج المسؤولية الاجتماعية للشركات القضايا الاجتماعية والبيئية التقليدية، تعالج المسؤولية الرقمية للشركات الآثار الأخلاقية للرقمنة، مثل: خصوصية البيانات والأمان (ضمان جمع وتخزين واستخدام البيانات الشخصية بشكل مسؤول).[23] المساءلة الخوارزمية (معالجة التحيزات وضمان الشفافية في اتخاذ القرارات القائمة على الذكاء الاصطناعي).[24] والإدماج الرقمي (تعزيز الوصول العادل إلى التقنيات الرقمية للمجتمعات المهمشة).[25]

وبالتالي، تمثل المسؤولية الرقمية للشركات تطورًا للمسؤولية الاجتماعية للشركات، حيث تتكيف مبادئها مع تحديات وفرص العصر الرقمي.

3 .مجالات التداخل الرئيسية بين المسؤولية الاجتماعية والرقمية للشركات

على الرغم من أن للمسؤولية الرقمية للشركات إطار عمل مميز، إلا أنها تشترك مع المسؤولية الاجتماعية للشركات في العديد من المبادئ الأساسية:

- إشراك أصحاب المصلحة: تؤكد كل من المسؤولية الاجتماعية للشركات والمسؤولية الرقمية للشركات على أهمية التواصل مع أصحاب المصلحة، بما في ذلك العملاء والموظفين والمجتمعات، لمعالجة مخاوفهم وتوقعاتهم.[26]
- الاستدامة: تركز المسؤولية الاجتماعية للشركات على الاستدامة البيئية، بينما تمتد المسؤولية الرقمية إلى استدامة العمليات الرقمية، مثل تقليل البصمة الكربونية لمراكز البيانات وإدارة النفايات الإلكترونية.[27]
- الممارسات الأخلاقية: يدعو كلا الإطارين إلى ممارسات الأعمال الأخلاقية، حيث تعالج المسؤولية الاجتماعية للشركات قضايا مثل ممارسات العمل العادلة وتركز المسؤولية الرقمية للشركات على الذكاء الاصطناعي الأخلاقي واستخدام البيانات.[28]

4 .تكامل المسؤولية الرقمية والاجتماعية للشركات

تكمل المسؤولية الرقمية للشركات المسؤولية الاجتماعية لها، وذلك من خلال معالجة التحديات المهمة للعصر الرقمي:

- الأخلاقيات الرقمية: توفر المسؤولية الرقمية للشركات إطارًا لمعالجة المعضلات الأخلاقية المتعلقة بالتقنيات الرقمية، مثل استخدام الذكاء الاصطناعي في التوظيف أو تأثير وسائل التواصل الاجتماعي على الصحة العقلية.[29]
- الامتثال التنظيمي: تضمن المسؤولية الرقمية امتثال الشركات للوائح الرقمية المحددة، مثل قوانين حماية البيانات على سبيل المثال (GDPR) وأطر حوكمة الذكاء الاصطناعي.[30]
- الابتكار والمسؤولية: تشجع المسؤولية الرقمية الشركات على الابتكار بمسؤولية، وموازنة التقدم التكنولوجي مع الرفاهية المجتمعية.[31]

5 .دور المسؤولية الرقمية للشركات في استراتيجيات المسؤولية الاجتماعية للشركات الحديثة

مع تزايد أهمية التقنيات الرقمية في العمليات التجارية، يُنظر إلى المسؤولية الرقمية للشركات بشكل متزايد باعتباره مكونًا أساسيًا لاستراتيجيات المسؤولية الاجتماعية للشركات. حيث يجب على الشركات دمج مبادئ المسؤولية الرقمية في أطر المسؤولية الاجتماعية للشركات الخاصة بها من أجل:

- بناء الثقة: تعمل الممارسات الرقمية الشفافة والأخلاقية على تعزيز ثقة أصحاب المصلحة وسمعة الشركة.[32]
- تخفيف المخاطر: إن معالجة المخاطر الرقمية، مثل خروقات البيانات والتحيزات الخوارزمية، تقلل من المسؤوليات القانونية والسمعة.[33]
- دفع الابتكار: تعمل الممارسات الرقمية المسؤولة على تعزيز الابتكار المستدام، ومواءمة التقدم التكنولوجي مع القيم المجتمعية.[34]

عليه فان المسؤولية الرقمية للشركات هي امتداد للمسؤولية الاجتماعية للشركات التي تعالج الآثار الأخلاقية والمجتمعية للتكنولوجيات الرقمية. ومن خلال دمج المسؤولية الرقمية للشركات في استراتيجيات المسؤولية الاجتماعية للشركات، يمكن للشركات ضمان أمن ممارساتها الرقمية.

المبحث الثاني: الإطار القانوني للمسؤولية الرقمية للشركات

يجب أن يشتمل الإطار القانوني للمسؤولية الرقمية للشركات على عدة عناصر رئيسية لمعالجة التحديات والتوقعات المختلفة المتعلقة بالممارسات الرقمية للشركات بشكل فعال. ومن خلال معالجة هذه العناصر الرئيسية، يمكن للإطار القانوني للمسؤولية الرقمية للشركات أن يوفر نهجًا شاملاً ومتكاملًا لتنظيم الممارسات الرقمية للشركات، وتعزيز الابتكار المسؤول والمستدام، والحفاظ على ثقة الجمهور في النظام البيئي الرقمي. في المطالب الاتية نتناول اهم عناصر الإطار القانوني للمسؤولية الرقمية للشركات:

المطلب الأول: الخصوصية وحماية البيانات في المسؤولية الرقمية للشركات

تعتبر الخصوصية وحماية البيانات من المكونات الأساسية للإطار القانوني للمسؤولية الرقمية للشركات. ومع نمو حجم وتعقيد جمع البيانات وتحليلها بشكل كبير، تواجه الشركات تدقيقًا متزايدًا لضمان الإدارة الأخلاقية والمسؤولة للمعلومات الشخصية. يحلل هذا المطلب العناصر الرئيسية للخصوصية وحماية البيانات وهي:

أولا: لوائح حوكمة البيانات والخصوصية

يجب أن ينشئ الإطار القانوني القوي للمسؤولية الرقمية للشركات لوائح حوكمة شاملة للبيانات لضمان الشفافية والمساءلة والامتثال في ممارسات البيانات للشركات. كما يجب أن تحدد هذه اللوائح متطلبات واضحة لجمع البيانات وتخزينها ومعالجتها ومشاركتها، مع التركيز على حماية حقوق الخصوصية الفردية.[35] وهذا يتطلب من الشركات الحصول على موافقة صريحة من الأفراد قبل جمع البيانات الشخصية وتوفير معلومات يمكن الوصول إليها حول كيفية استخدام البيانات وتأمينها. اذ إن الشفافية ضرورية لبناء الثقة العامة وضمان الامتثال لمعايير الخصوصية العالمية.[36]ان أمن البيانات يفرض اتخاذ تدابير قوية للحماية من الخروقات والوصول غير المصرح به. وتشمل هذه التدابير التشفير وضوابط الوصول

وبروتوكولات الاستجابة للحوادث لحماية المعلومات الحساسة.[37] كما يجب محاسبة الشركات على خروقات البيانات أو إساءة استخدام المعلومات الشخصية، مع فرض عقوبات صارمة ومتطلبات الإبلاغ الإلزامي لضمان الإخطار الفوري للأفراد المتضررين، وتعتبر آليات المساءلة هذه ضرورية للتخفيف من المخاطر والحفاظ على ثقة أصحاب المصلحة.[38] عليه فإن أحد الجوانب الرئيسية لخصوصية البيانات وحمايتها هو تمكين الأفراد من السيطرة على بياناتهم الشخصية، اذ يجب أن يمنح الإطار القانوني الأفراد الحق في الوصول إلى بياناتهم وتصحيحها وحذفها، والذي يشار إليه غالبًا باسم "الحق في النسيان".[39] حيث تمكن هذه الحقوق الأفراد من محاسبة الشركات على ممارساتها المتعلقة بالبيانات وضمان التعامل مع المعلومات الشخصية بمسؤولية. هذا المبدأ ذو أهمية خاصة في سياق التقنيات الناشئة، حيث أصبحت عملية جمع البيانات ومعالجتها منتشرة على نحو متزايد. علاوة على ذلك، ان ظهور الذكاء الاصطناعي وإنترنت الأشياء أدى إلى ظهور تحديات جديدة تتعلق بالخصوصية يجب معالجتها ضمن إطار المسؤولية الرقمية للشركات. اذ يجب أن يفرض الإطار القانوني تطوير أنظمة الذكاء الاصطناعي الأخلاقية التي تعطي الأولوية لخصوصية البيانات والعدالة والشفافية، مما يضمن عدم انتهاك عملية صنع القرار المدعومة بالذكاء الاصطناعي للحقوق الفردية.[40] وبالمثل، يجب أن يخضع نشر أجهزة إنترنت الأشياء وجمع بيانات المستشعرات لضمانات خصوصية صارمة لمنع الوصول غير المصرح به وإساءة استخدام معلومات المستهلك. ومن خلال إنشاء لوائح قوية لحماية وخصوصية البيانات، يمكن للإطار القانوني لحماية البيانات الشخصية أن يساعد في بناء الثقة العامة، وتخفيف مخاطر الأضرار المتعلقة بالبيانات، وضمان التزام الشركات بمسؤوليتها عن حماية المعلومات الشخصية لأصحاب المصلحة لديها.[41] وتمثل اللائحة العامة لحماية البيانات (GDPR)، التي تم سنها في عام 2016 ودخلت حيز التنفيذ في عام 2018، علامة فارقة في تنظيم خصوصية البيانات العالمية. الهدف الأساسي من اللائحة العامة لحماية البيانات هو تعزيز حقوق الأفراد فيما يتعلق بالبيانات الشخصية وإنشاء قواعد منسجمة لمعالجة البيانات في جميع أنحاء الاتحاد الأوروبي.[42] ان الأحكام الرئيسية التي تتضمنها هذه اللائحة هي:

- التعريف الموسع للبيانات الشخصية: تحدد اللائحة العامة لحماية البيانات، البيانات الشخصية على نطاق واسع، بما في ذلك أي معلومات يمكنها تحديد هوية الفرد بشكل مباشر أو غير مباشر، بما في ذلك معرفات الإنترنت مثل الأسماء وأرقام التعريف وبيانات الموقع والمعرفات عبر الإنترنت.[43]
- الموافقة والشفافية: يجب على الشركات الحصول على موافقة صريحة ومجانية من الأفراد وتقديم معلومات واضحة حول استخدام البيانات.[44]
- الحقوق الفردية: تمنح اللائحة العامة لحماية البيانات الأفراد الحق في الوصول إلى بياناتهم وتصحيحها وحذفها ونقلها، بالإضافة إلى الحق في الاعتراض على معالجة البيانات.
- مبادئ حماية البيانات: تفرض اللائحة العامة لحماية البيانات مبادئ مثل تقليل البيانات، والحد من الغرض، والحد من التخزين.[45]
- المساءلة والتنفيذ: يجب على الشركات تنفيذ التدابير الفنية والتنظيمية لضمان الامتثال، مع فرض غرامات تصل إلى 4٪ من الإيرادات السنوية العالمية أو 20 مليون يورو لعدم الامتثال.[46]

تمثل اللائحة العامة لحماية البيانات تحولاً كبيرًا في حماية البيانات، مع التأكيد على الحقوق الفردية وأمن البيانات. إنها تتطلب من المؤسسات اعتماد أطر حوكمة شاملة للبيانات وقد وضعت معيارًا عالميًا لمعايير خصوصية البيانات. وفي حين أنها تفرض تحديات، فإنها توفر أيضًا فرصًا للشركات لبناء الثقة مع المستهلكين من خلال ممارسات حماية البيانات المحسنة. الا ان الشركات تواجه تحديات كبيرة في التكيف مع متطلبات اللائحة العامة لحماية البيانات، بما في ذلك الحاجة إلى موارد مالية وبشرية كبيرة لضمان الامتثال. ويشمل ذلك تدريب الموظفين وتحديث ممارسات إدارة البيانات.[47]

ان اللائحة العامة لحماية البيانات لها تأثير خارج الحدود الإقليمية، حيث تنطبق اللائحة على أي مؤسسة تعالج البيانات الشخصية لمواطني الاتحاد الأوروبي، بغض النظر عن الموقع، مما يتطلب منهم الالتزام بمعايير حماية البيانات في الاتحاد الأوروبي.[48] مما يضع بالتالي معيارًا عالميًا لحماية البيانات.[49] كما أثرت اللائحة العامة لحماية البيانات بشكل كبير على قوانين حماية البيانات العالمية، مما ألهم لوائح مماثلة في جميع أنحاء العالم. هذا التأثير واضح في سن قوانين مثل قانون خصوصية المستهلك في كاليفورنيا (CCPA) في الولايات المتحدة،[50] وقانون حماية المعلومات الشخصية في الصين (PIPL)،[51] وقانون حماية البيانات العامة في البرازيل (LGPD)، وقانون حماية المعلومات الشخصية (APPI) في اليابان.[52]

ثانيا: الامن السيبراني وإدارة المخاطر الفعالة

الأمن السيبراني وإدارة المخاطر الفعّالة من المكونات التي لا غنى عنها في المسؤولية الرقمية للشركات. ومع اعتماد الشركات بشكل متزايد على التقنيات الرقمية وجمع كميات هائلة من البيانات، أصبح تنفيذ تدابير الأمن السيبراني القوية واستراتيجيات إدارة المخاطر الاستباقية أمرًا ضروريًا لحماية الأصول الرقمية والحفاظ على ثقة أصحاب المصلحة. ان دور الأمن السيبراني وإدارة المخاطر كعنصر من عناصر الاطار القانوني للمسؤولية الرقمية للشركات يتمثل بالاتي:

1. الأمن السيبراني في المسؤولية الرقمية للشركات

يركز الأمن السيبراني على حماية الأصول الرقمية للمؤسسات، بما في ذلك الشبكات والأنظمة والتطبيقات والبيانات، من الوصول غير المصرح به وإساءة الاستخدام والتعطيل.[53] ويشمل ذلك نشر مجموعة شاملة من عناصر التحكم الأمنية،

مثل جدران الحماية وأنظمة الكشف عن الاختراق والوقاية منه والتشفير وبروتوكولات إدارة الوصول، للتخفيف من التهديدات السيبرانية.[54] إن التكرار المتزايد وتعقيد الهجمات الإلكترونية، مثل برامج الفدية والتصيد الاحتيالي، يؤكدان على الحاجة إلى إعطاء الشركات الأولوية للأمن السيبراني كجزء من إطار عمل المسؤولية الرقمية الخاص بها. كما يجب أن يأخذ النهج الشامل للأمن السيبراني في الاعتبار العوامل التكنولوجية والبشرية. على سبيل المثال، يجب على الشركات توفير برامج تدريب وتوعية شاملة بالأمن السيبراني للموظفين لتقليل نقاط الضعف الناشئة عن الخطأ البشري.[55] بالإضافة إلى إن تعزيز ثقافة الأمن داخل الشركة والتعاون مع أصحاب المصلحة الخارجيين، مثل الوكالات الحكومية والشركاء الصناعيين، يمكن أن يعزز تبادل معلومات التهديد ويحسن المرونة الشاملة.[56]

2. إدارة المخاطر في المسؤولية الرقمية للشركات

تعد إدارة المخاطر بالغة الأهمية بشكل خاص في سياق التحول الرقمي، حيث يمكن أن يؤدي التبني السريع للتكنولوجيات الجديدة إلى إدخال نقاط ضعف غير متوقعة. ان إدارة المخاطر الفعّالة هي عملية تحديد المخاطر وتقييمها والاستجابة لها، بما في ذلك تلك المتعلقة بالأمن السيبراني.[57] يجب أن تتضمن استراتيجية إدارة المخاطر الاستباقية ما يلي:

- تحديد المخاطر: تحديد التهديدات المحتملة، مثل خروقات البيانات، وإصابات البرامج الضارة، والتهديدات الداخلية.
- تقييم المخاطر: تقييم احتمالية وتأثير المخاطر المحددة.
- تخفيف المخاطر: تنفيذ الضوابط للحد من احتمالية أو تأثير المخاطر.
- المراقبة والمراجعة: مراقبة المخاطر بشكل مستمر وتحديث استراتيجيات التخفيف لمعالجة التهديدات الناشئة.[58]

من خلال دمج إدارة المخاطر في إطار المسؤولية الرقمية للشركات الخاص بها، يمكن للشركات حماية نفسها وأصحاب المصلحة من العواقب المالية والسمعة والمسؤولية القانونية للحوادث الإلكترونية.

3. الاستجابة للحوادث وإخطار الخروقات

تعتبر الاستجابة للحوادث وإخطار الخروقات من المكونات الأساسية لاستراتيجية إدارة المخاطر والأمن السيبراني في الشركة. تشير الاستجابة للحوادث إلى الطريق المنهجي المتبع لمعالجة وإدارة عواقب حادث أمني، مثل خرق البيانات أو الإصابة بالبرامج الضارة.[59] يجب أن تتضمن خطة الاستجابة للحوادث الفعّالة العناصر الرئيسية التالية:

- تحديد الحوادث وتصنيفها: اكتشاف الحوادث وتصنيفها بناءً على نوعها وشدتها.
- الاحتواء والتخفيف: اتخاذ إجراءات فورية للحد من تأثير الحادث ومنع المزيد من الضرر.
- التحقيق والتحليل: إجراء تحقيق شامل لتحديد السبب الجذري ونطاق الحادث.
- الإصلاح والتعافي: تنفيذ تدابير لاستعادة العمليات الطبيعية ومنع تكرارها.
- مراجعة ما بعد الحادث: تقييم فعالية الاستجابة ودمج الدروس المستفادة لتحسين الاستعداد المستقبلي.[60]

من ناحية أخرى، يشير إشعار الاختراق إلى الالتزام القانوني والأخلاقي للشركات بإبلاغ الأفراد المتضررين والسلطات التنظيمية وأصحاب المصلحة الآخرين عندما يؤدي خرق البيانات إلى المساس بالمعلومات الشخصية أو الحساسة.[61] يعد إشعار الاختراق في الوقت المناسب والشفاف أمرًا ضروريًا للحفاظ على الثقة والامتثال للوائح حماية البيانات والتخفيف من الضرر الذي يلحق بالأفراد المتضررين. يجب على الشركات إنشاء بروتوكولات إشعار بالاختراق محددة جيدًا، بما في ذلك معايير الإبلاغ عن الخروقات وإطارات زمنية للإخطار وقنوات الاتصال، لضمان الامتثال للمتطلبات القانونية المتطورة.

4. الامتثال لمعايير الأمن السيبراني

الامتثال لمعايير الأمن السيبراني هو حجر الزاوية في المسؤولية الرقمية للشركات، حيث يوفر للمؤسسات إطارًا منظمًا لحماية الأصول الرقمية والمعلومات الحساسة. تشمل معايير الأمن السيبراني الرئيسية ما يلي:

1- معيار أنظمة ادارة امن المعلومات ISO/IEC 27001 Information security management systems

أحد أكثر معايير الأمن السيبراني المعترف بها على نطاق واسع هو معيار ISO/IEC 27001، الذي طورته المنظمة الدولية للمعايير (ISO) واللجنة الكهروتقنية الدولية (IEC). يحدد هذا المعيار المتطلبات اللازمة لإنشاء نظام إدارة أمن المعلومات (ISMS) الخاص بالشركة وتنفيذه وصيانته وتحسينه باستمرار. من خلال الحصول على شهادة ISO/IEC 27001، تثبت الشركات التزامها بتنفيذ مجموعة قوية من ضوابط الأمان، بما في ذلك إدارة الوصول والاستجابة للحوادث وتخطيط استمرارية الأعمال ومراقبة الامتثال، مما يساعد المؤسسات على إثبات التزامها بالأمن السيبراني.[62]

بالإضافة الى ان الحصول على شهادة ISO/IEC 27001 يُظهر التزام الشركة بأمن المعلومات، فانه يساعد في التخفيف من مخاطر وتأثيرات خروقات الأمن، ويقلل من العقوبات من الجهات التنظيمية، ويوفر التحقق المستقل من قبل طرف ثالث لنظام إدارة أمن المعلومات الخاص بالشركة ISMS.[63]

2- معيار إطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتكنولوجيا

يوفر هذا الإطار، الذي طوره المعهد الوطني للمعايير والتكنولوجيا، لغة مشتركة لتحديد وتقييم وإدارة مخاطر الأمن السيبراني. وتمكن وظائفه الأساسية الخمس - تحديد وحماية واكتشاف والاستجابة والتعافي - المؤسسات من تطوير استراتيجية شاملة لإدارة الأمن السيبراني.[64]

- تحديد: تتضمن هذه الوظيفة فهم بيئة الشركة لإدارة مخاطر الأمن السيبراني على الأنظمة والأصول والبيانات والقدرات. وهي تساعد في تطوير فهم الشركة لإدارة مخاطر الأمن السيبراني على الأنظمة والأشخاص والأصول والبيانات والقدرات.
- الحماية: تحدد هذه الوظيفة الضمانات المناسبة لضمان تقديم خدمات البنية التحتية الحرجة. وهي تدعم القدرة على الحد من تأثير حدث الأمن السيبراني المحتمل أو احتواءه.
- الكشف: تحدد هذه الوظيفة الأنشطة لتحديد وقوع حدث الأمن السيبراني. وهي تمكن من اكتشاف أحداث الأمن السيبراني في الوقت المناسب.
- الاستجابة: تتضمن هذه الوظيفة الأنشطة المناسبة لاتخاذ إجراء بشأن حادث الأمن السيبراني المكتشف. وهي تدعم القدرة على احتواء تأثير حادث الأمن السيبراني المحتمل.
- الاسترداد: تحدد هذه الوظيفة الأنشطة المناسبة للحفاظ على خطط المرونة واستعادة أي قدرات أو خدمات تضررت بسبب حادث الأمن السيبراني.[65]

3- معيار امان بيانات بطاقات الدفع PCI DSS

يعد معيار أمان بيانات صناعة بطاقات الدفع (PCI DSS) إطارًا بالغ الأهمية للمؤسسات التي تتعامل مع بيانات بطاقات الدفع، ويهدف إلى تقليل مخاطر اختراق البيانات والاحتيال المالي. ويضع متطلبات أمنية شاملة لمعالجة وتخزين ونقل معلومات بطاقات الائتمان.[66]

تم إنشاء PCI DSS للتخفيف من خروقات الأمن والخسائر المالية المرتبطة ببيانات بطاقات الدفع. وهو يوفر إرشادات لمقدمي الخدمات والتجار لتنفيذ بنى تحتية أمنية قوية. حيث يتكون المعيار من اثني عشر متطلبًا أمنيًا تغطي تصميم السياسات، وأمان البيانات، وهندسة الشبكة، وتصميم البرامج، والتشفير. يتم تقييم الامتثال من قبل مقيمي الأمن المؤهلين PCI (QSAs).[67]

4- معيار اللائحة العامة لحماية البيانات GDPR

اللائحة العامة لحماية البيانات (GDPR)، هي قانون شامل لحماية البيانات أقره الاتحاد الأوروبي، ودخلت حيز التنفيذ في مايو 2018. وهي تنطبق على أي شركة تتعامل مع البيانات الشخصية لمواطني الاتحاد الأوروبي، بغض النظر عن موقع الشركة، ولها آثار عالمية كبيرة. تضع اللائحة العامة لحماية البيانات متطلبات صارمة للتعامل مع البيانات الشخصية وحمايتها، بما في ذلك إخطار خرق البيانات الإلزامي، وحقوق موضوع البيانات، وتدابير المساءلة. يعد الامتثال للائحة العامة لحماية البيانات أمرًا ضروريًا للشركات العاملة داخل الاتحاد الأوروبي أو التي تخدم العملاء فيه، حيث يمكن أن يؤدي عدم الامتثال إلى غرامات كبيرة وضرر سمعة. لقد أدى قانون حماية البيانات العامة إلى تغييرات كبيرة في سياسات الخصوصية في جميع أنحاء العالم، حيث قامت الشركات بمراجعة سياساتها للامتثال لمتطلبات قانون حماية البيانات العامة. ويشمل ذلك تحسينات في الشفافية وحقوق المستخدم، على الرغم من أن العديد من السياسات لا تزال غير متوافقة تمامًا.[68]

ثالثا: الذكاء الاصطناعي الأخلاقي والمساءلة الخوارزمية

لقد أدى دمج الذكاء الاصطناعي وأنظمة اتخاذ القرار الخوارزمية في العمليات المؤسسية إلى زيادة أهمية الذكاء الاصطناعي الأخلاقي والشفافية والعدالة باعتبارها حجر الزاوية للمسؤولية الرقمية للشركات. هذه المبادئ ضرورية لضمان تطوير التقنيات الرقمية ونشرها بشكل مسؤول، وتقليل الضرر وتعزيز النتائج العادلة. ونتناول تلك المبادئ بالآتي:

1. المساءلة الخوارزمية

غالبًا ما تواجه أنظمة الذكاء الاصطناعي التدقيق بحثًا عن التحيزات المحتملة وقضايا العدالة. اذ ان ضمان العدالة يتضمن التخفيف من التحيزات التي قد تؤدي إلى التمييز وعدم المساواة. حيث ان تقنيات معالجة البيانات مسبقًا والتدقيق الخوارزمي ضرورية لمعالجة هذه المخاوف وتعزيز النتائج العادلة.[69] تعد المساءلة في أنظمة الذكاء الاصطناعي أمرًا بالغ الأهمية، خاصة وأن هذه الأنظمة تستخدم في مجالات عالية المخاطر مثل الخدمات العامة والرعاية الصحية وصنع القرار المالي. اذ وضع إرشادات واضحة وهياكل حوكمة يمكن أن يساعد في الحفاظ على المساءلة والثقة العامة.[70] ولتفعيل الذكاء الاصطناعي الأخلاقي والمساءلة الخوارزمية، يجب على الشركات اعتماد أطر شاملة تتضمن:

- المبادئ والإرشادات الأخلاقية: وضع مبادئ أخلاقية واضحة لتطوير الذكاء الاصطناعي ونشره، بما يتماشى مع أفضل ممارسات الصناعة والمتطلبات التنظيمية.
- هياكل الحوكمة: إنشاء لجان أخلاقية للذكاء الاصطناعي للإشراف على الاستخدام المسؤول للذكاء الاصطناعي وتحديد المخاطر والأضرار المحتملة.
- حوكمة البيانات: ضمان جودة البيانات المستخدمة لتدريب نماذج الذكاء الاصطناعي وإنصافها وخصوصيتها، حيث يمكن أن تؤدي البيانات المتحيزة أو غير المكتملة إلى نتائج تمييزية.[71]

فمن خلال إعطاء الأولوية للذكاء الاصطناعي الأخلاقي والمساءلة الخوارزمية، يمكن للشركات بناء الثقة مع أصحاب المصلحة، وتخفيف المخاطر، والمساهمة في نظام بيئي رقمي أكثر إنصافًا.

2. الشفافية والقدرة على التفسير

إن الشفافية والقدرة على التفسير تعتبر من المكونات الأساسية للمسؤولية الرقمية للشركات. ومع قيام الشركات بدمج المزيد من التقنيات الرقمية، فإن الطلب على الممارسات الشفافة والقابلة للتفسير يصبح أمرًا بالغ الأهمية لضمان المساءلة والثقة بين أصحاب المصلحة.[72] فالشفافية عنصر ذو أهمية كبيرة في المسؤولية الرقمية للشركات، حيث إنها تسمح لأصحاب المصلحة بفهم وتقييم تصرفات وقرارات الشركة. والشفافية هي المدى الذي يرى فيه أصحاب المصلحة أن المؤسسة توفر فرص التعلم عن نفسها، مما قد يعزز الثقة والمساءلة. أدى استخدام تكنولوجيا المعلومات والاتصالات إلى تطوير "الشفافية الديناميكية"، والتي تنطوي على تبادل ثنائي الاتجاه للمعلومات بين الشركات وأصحاب المصلحة، مما يعزز بيئة أكثر تعاونًا.[73] اما القدرة على التفسير في الأنظمة الرقمية فهي متطلب غير وظيفي يعالج الحاجة إلى أن تكون أنظمة البرمجيات مفهومة للمستخدمين. وهي مرتبطة ارتباطًا وثيقًا بالشفافية، حيث تساعد في التخفيف من غموض النظام من خلال تزويد المستخدمين بتفسيرات مفهومة لسلوك البرمجيات. فالذكاء الاصطناعي القابل للتفسير له أهمية خاصة في المجالات ذات المخاطر العالية، حيث تعد الشفافية أمرًا بالغ الأهمية لتطوير الذكاء الاصطناعي المسؤول.[74] ومع ذلك، قد لا تكفي القدرة على التفسير وحدها للمستخدمين العاديين، الذين غالبًا ما يحتاجون إلى معلومات خلفية إضافية لبناء الثقة في أنظمة الذكاء الاصطناعي.[75] الا انه على الرغم من الأهمية الكبيرة للشفافية والقدرة على التفسير، تظل التحديات قائمة في تنفيذها. فلا تزال العديد من الأساليب الرقمية للشفافية في مرحلة التجربة وتقدم حلولاً محدودة. بالإضافة إلى ذلك، هناك حاجة إلى مواءمة تقنيات التفسير الفني مع متطلبات السياسة والقانون لضمان تلبية الاحتياجات المتنوعة لأصحاب المصلحة. لذا فتحسين الشفافية والقدرة على التفسير يتطلب وضع إرشادات واضحة ودمج ملاحظات المستخدم لمعالجة متطلبات المستخدمين غير الخبراء بشكل أفضل.[76]

3 .عدم التمييز والإنصاف

المسؤولية الرقمية للشركات هي إطار عمل يوجه الشركات في إدارة التقنيات والبيانات الرقمية بشكل أخلاقي وعادل. فهي تضع معايير للاستخدام الأخلاقي والعادل للبيانات والتكنولوجيا، وحماية خصوصية العملاء، وضمان ديناميكيات القوة العادلة بين الشركات وشركائها. حيث يعد ضمان عدم تمييز الخوارزميات وعمليات البيانات ضد الأفراد بناءً على الخصائص الشخصية مبدأً أساسيًا للمسؤولية الرقمية للشركات. يتضمن هذا الحصول على البيانات وحمايتها وصيانتها بشكل غير متحيز، بالإضافة إلى تفسير البيانات واتخاذ القرارات بشكل موضوعي.[77] لذا يُنظر إلى المسؤولية الرقمية للشركات على أنها امتداد للمسؤولية الاجتماعية للشركات، مع التركيز على الجوانب الرقمية للمسؤولية الاجتماعية للشركات. وهي تنطوي على استخدام التقنيات الرقمية بشكل مسؤول لتحسين النتائج الاجتماعية والاقتصادية والبيئية.[78]

اما بالنسبة للعدالة في الأنظمة الرقمية هي مفهوم متعدد الأوجه يهدف إلى ضمان التوزيع العادل لفوائد وأعباء التقنيات الرقمية، وتجنب التأثيرات المتباينة على المجتمعات الضعيفة أو المهمشة.[79] اذ انه في عالم التعلم الآلي، غالبًا ما يتم تعريف العدالة رياضيًا، مع وجود عائلتين رئيسيتين من التعريفات: تلك التي تقيد التفاوتات في القرار وتلك التي تحد من تأثير الخصائص المحمية مثل العرق والجنس. ومع ذلك، يمكن أن تؤدي هذه التعريفات في بعض الأحيان إلى سياسات اتخاذ قرار لا تفيد المجموعات المقصودة، مما يشير إلى أن العدالة في الخوارزميات يجب أن تأخذ في الاعتبار العواقب الخاصة بالسياق.[80] بالإضافة إلى ذلك، فإن الطبيعة الذاتية للعدالة تعني أن المعتقدات الفردية حول العدالة يمكن أن تختلف، مما يستلزم وجود أطر لقياس هذه المعتقدات وتجميعها من أجل تصميم أفضل للسياسة والنظم.[81]

بالتالي يواجه مجال التعلم الآلي العادل العديد من التحديات، بما في ذلك الحاجة إلى مواءمة الخوارزميات مع أهداف السياسة ومعالجة المقايضات بين معايير العدالة المختلفة. يقدم مفهوم العدالة الأساسية، الذي يأخذ في الاعتبار تأثير القرارات على الأفراد، حلاً محتملاً من خلال ضمان عدم تأثير السمات المحمية بشكل مباشر على النتائج.[82] علاوة على ذلك، يهدف تطوير أطر مثل FAIR-Frame إلى نمذجة العدالة عبر سمات محمية متعددة، ومعالجة الأضرار التمثيلية والتخصيصية في تطبيقات التعلم الآلي.[83] من خلال إعطاء الأولوية لعدم التمييز والإنصاف، يمكن للشركات إثبات التزامها بالتحول الرقمي العادل والمساهمة في نظام بيئي رقمي أكثر شمولاً.

رابعا: الحقوق الرقمية والاستخدام المسؤول للتكنولوجيا

لقد استلزم المشهد الرقمي المتطور دمج الحقوق الرقمية وحماية المستهلك وحقوق الموظفين في إطار المسؤولية الرقمية للشركات. وتعتبر هذه العناصر بالغة الأهمية لضمان التزام الشركات بالمعايير الأخلاقية وحماية مصالح أصحاب المصلحة والمساهمة في نظام بيئي رقمي مستدام وعادل. نتناول في هذه الفقرة فحصًا تحليليًا لهذه المكونات كما يلي:

1 .الحقوق الرقمية

تشمل الحقوق الرقمية حقوق الإنسان والحريات الأساسية في المجال الرقمي، مثل الحق في الخصوصية وحرية التعبير والوصول إلى المعلومات.[84] يشير الاستخدام المسؤول للتكنولوجيا إلى النشر الأخلاقي والمستدام للتكنولوجيات الرقمية التي تحترم هذه الحقوق مع تقليل التأثيرات السلبية على المجتمع والبيئة. ولدمج الحقوق الرقمية والاستخدام المسؤول للتكنولوجيا في إطار المسؤولية الرقمية للشركات الخاص بها، يجب على الشركات، تنفيذ سياسات حوكمة البيانات القوية لضمان الشفافية والامتثال لقواعد الخصوصية، مثل اللائحة العامة لحماية البيانات، وتزويد الأفراد بمعلومات واضحة حول جمع البيانات واستخدامها، وتمكينهم من ممارسة حقوقهم في الوصول إلى بياناتهم أو تصحيحها أو حذفها.[85]كما يجب ضمان حرية التعبير والوصول إلى المعلومات عن طريق عدم قيام المنصات الرقمية بتقييد التعبير المشروع بشكل غير

ملائم أثناء معالجة التحديات مثل المعلومات المضللة والمحتوى الضار، وتعزيز الوصول الشامل إلى الخدمات الرقمية، وخاصة للمجتمعات المهمشة أو المحرومة.[86] بالإضافة الى ذلك دعم الاستدامة البيئية من خلال اعتماد ممارسات مستدامة، مثل مراكز البيانات الموفرة للطاقة وإدارة النفايات الإلكترونية المسؤولة، لتقليل التأثير البيئي للتكنولوجيات الرقمية.[87]

2. حماية المستهلك في العصر الرقمي

تشير حماية المستهلك إلى القوانين واللوائح والممارسات التي تحمي حقوق المستهلك ومصالحه في السوق في العصر الرقمي، تشمل حماية المستهلك، الشفافية والإفصاح من خلال توفير معلومات واضحة ودقيقة حول المنتجات والخدمات الرقمية، بما في ذلك شروط الاستخدام وممارسات جمع البيانات، والحصول على موافقة مستنيرة لاستخدام البيانات لضمان وعي المستهلك وسيطرته.[88] كذلك تعزيز خصوصية البيانات والأمان وتنفيذ تدابير حماية البيانات القوية لمنع الوصول غير المصرح به أو إساءة استخدام معلومات المستهلك، كما يجب إخطار المستهلكين على الفور في حالة حدوث خروقات للبيانات أو حوادث أمنية.[89] علاوة على ذلك يجب على الشركات الالتزام بالتسويق العادل والأخلاقي من خلال تجنب تكتيكات التسويق الخادعة أو التلاعبية، مثل الأنماط المظلمة، التي تستغل نقاط ضعف المستهلك، وضمان عدم انتهاك ممارسات الإعلان الرقمي لحقوق المستهلك أو التسبب في ضرر.[90]

3. حقوق الموظفين والمراقبة في مكان العمل الرقمي

مع اعتماد الشركات بشكل متزايد على التقنيات الرقمية، أصبحت حماية حقوق الموظفين في مكان العمل الرقمي جانبًا بالغ الأهمية من المسؤولية الرقمية للشركات. تشمل الاعتبارات الرئيسية في الخصوصية وحماية البيانات من خلال وضع سياسات واضحة لجمع وتخزين واستخدام البيانات الشخصية للموظفين، وضمان الامتثال لقوانين وأنظمة العمل. كما يجب تقييد مراقبة الموظفين بما هو ضروري ومتناسب لأغراض العمل المشروعة.[91] كما ان من الأمور الرئيسة احترام حقوق الموظفين في حرية التعبير وتكوين الجمعيات، حتى في الفضاءات الرقمية، لتحقيق الموازنة بين هذه الحقوق والحاجة إلى الحفاظ على بيئة عمل مهنية وشاملة.[92] وان على الشركات ضمان عدم تسبب التقنيات الرقمية والأنظمة الخوارزمية المستخدمة في إدارة الموارد البشرية في ممارسات متحيزة أو تمييزية وتنفيذ الضمانات اللازمة لمنع تضخيم أوجه عدم المساواة في التوظيف أو الترقية أو تقييم الأداء.[93] اما من ناحية الصحة والسلامة المهنية، فعلى الشركات مسؤولية معالجة التأثيرات الجسدية والعقلية والعاطفية للتكنولوجيات الرقمية، مثل وقت الشاشة المطول والإجهاد الرقمي، ووضع سياسات لدعم رفاهية الموظفين وإنتاجيتهم وتوازن العمل والحياة.[94] فمن خلال تضمين حقوق الموظفين ومراقبتهم في إطار عمل المسؤولية الرقمية للشركات الخاص بهم، يمكن للشركات إنشاء بيئة عمل رقمية عادلة وشاملة ومُمكِّنة، وتعزيز الثقة والاستدامة طويلة الأجل.

المبحث الثالث: حوكمة المسؤولية الرقمية للشركات وتحديات تنفيذها

نتناول في هذا المبحث حوكمة المسؤولية الرقمية للشركات، والتحديات والاعتبارات في تنفيذ المسؤولية الرقمية للشركات في مطلبين كالاتي:

المطلب الأول: حوكمة المسؤولية الرقمية للشركات

تعتبر حوكمة المسؤولية الرقمية للشركات جانبًا بالغ الأهمية لضمان عمل الشركات بشكل أخلاقي ومسؤول في العصر الرقمي. ومع تزايد دمج التقنيات الرقمية في العمليات التجارية، يتعين على الشركات اعتماد أطر حوكمة قوية لمعالجة الآثار الأخلاقية والاجتماعية والبيئية لممارساتها الرقمية. نقدم في هذا المطلب تحليلاً معمقًا للمكونات الرئيسية لحوكمة المسؤولية الرقمية للشركات بالآتي:

أولا: موثوقية الأنظمة

تعتبر موثوقية الأنظمة الرقمية عنصرًا أساسيًا في حوكمة المسؤولية الرقمية للشركات. اذ ان الأنظمة الموثوقة تضمن عمل التقنيات الرقمية على النحو المقصود، مما يقلل من مخاطر الفشل التي قد تؤدي إلى عواقب مالية وسمعة وتشغيلية كبيرة. تشمل الموثوقية استقرار ودقة ومرونة الأنظمة الرقمية، وخاصة في التطبيقات عالية المخاطر مثل الرعاية الصحية والتمويل والمركبات ذاتية القيادة.[95] ولضمان موثوقية النظام، يجب على الشركات تنفيذ عمليات اختبار صارمة وضمان الجودة أثناء تطوير ونشر الأنظمة الرقمية، واعتماد آليات التكرار والسلامة من الفشل لمنع فشل النظام وضمان استمرارية العمليات. بالإضافة الى تحديث وصيانة الأنظمة بانتظام لمعالجة نقاط الضعف والتكيف مع المبادئ التكنولوجية المتطورة.[96] ان موثوقية الأنظمة ذات أهمية بالغة في سياق الذكاء الاصطناعي والتعلم الآلي، حيث يمكن أن تؤدي الأخطاء أو التحيزات الخوارزمية إلى عواقب بعيدة المدى. على سبيل المثال، يمكن أن تؤدي أنظمة الذكاء الاصطناعي غير الموثوقة في الرعاية الصحية إلى تشخيصات أو توصيات علاجية غير صحيحة، مما يشكل مخاطر جسيمة على سلامة المرضى.[97] لذلك، يجب على الشركات إعطاء الأولوية للموثوقية باعتبارها عنصرًا أساسيًا في إطار حوكمة المسؤولية الرقمية للشركات الخاصة بها.

ثانيا: شفافية البيانات

تشير شفافية البيانات إلى الانفتاح والوضوح في ممارسات البيانات، بما في ذلك كيفية جمع البيانات ومعالجتها واستخدامها. تعد ممارسات البيانات الشفافة ضرورية لبناء الثقة مع أصحاب المصلحة، وضمان المساءلة، والامتثال للمتطلبات التنظيمية.[98] وتتحقق الشفافية في البيانات من خلال الإفصاح عن مصادر البيانات، أي تحديد مصادر البيانات المستخدمة

في الأنظمة الرقمية وعمليات صنع القرار بوضوح. وتزويد أصحاب المصلحة بمعلومات يمكن الوصول إليها حول كيفية استخدام بياناتهم ولأية أغراض. بالإضافة الى التواصل المفتوح بين الشركات وأصحاب المصلحة من خلال إنشاء قنوات لأصحاب المصلحة لإثارة المخاوف وطلب التوضيح حول ممارسات البيانات.[99] تعد الشفافية مهمة بشكل خاص في سياق الذكاء الاصطناعي واتخاذ القرارات الخوارزمية، حيث يمكن أن يؤدي الافتقار إلى الشفافية إلى انعدام الثقة والمخاوف الأخلاقية. على سبيل المثال، يمكن للخوارزميات الغامضة المستخدمة في قرارات التوظيف أو الإقراض أن تديم التحيزات والتمييز، وتقوض العدالة والإنصاف.[100] من خلال إعطاء الأولوية لشفافية البيانات، يمكن للشركات تعزيز ثقة أصحاب المصلحة وإظهار التزامها بالممارسات الرقمية الأخلاقية.

ثالثا: جمع البيانات وتخزينها

يعد جمع البيانات وتخزينها أمرًا أساسيًا في حوكمة المسؤولية الرقمية للشركات، حيث يؤثران بشكل مباشر على الخصوصية والأمان والاعتبارات الأخلاقية. اذ يجب على الشركات وضع سياسات وممارسات واضحة لجمع البيانات وتخزينها لضمان الامتثال للمعايير القانونية والأخلاقية.[101] ويتم ذلك من خلال تقليل البيانات وجمع البيانات الضرورية فقط لأغراض محددة، بما يتماشى مع مبادئ مثل متطلبات تقليل البيانات في اللائحة العامة لحماية البيانات.[102] ومن ثم التخزين الآمن لهذه البيانات عن طريق تنفيذ تدابير أمنية قوية، مثل التشفير وضوابط الوصول، لحماية البيانات المخزنة من الوصول غير المصرح به أو الخروقات.[103] كما ينبغي مراعاة سياسات الاحتفاظ بالبيانات ووضع إرشادات واضحة حول المدة التي يتم الاحتفاظ بالبيانات فيها ومتى يجب حذفها لتقليل مخاطر سوء الاستخدام أو الخروقات.[104] كما يجب على الشركات أيضًا مراعاة الآثار الأخلاقية لجمع البيانات، وخاصة في الحالات التي تنطوي على بيانات حساسة أو شخصية. على سبيل المثال، يثير جمع البيانات البيومترية لتقنيات التعرف على الوجه مخاوف كبيرة بشأن الخصوصية ويتطلب دراسة أخلاقية دقيقة.[105]

رابعا: ملكية البيانات والخصوصية

تعتبر ملكية البيانات والخصوصية من المكونات الأساسية لحوكمة المسؤولية الرقمية للشركات، حيث تحدد من لديه السيطرة على البيانات وكيفية استخدامها. إن مفهوم ملكية البيانات معقد، حيث غالبًا ما تنطوي البيانات على العديد من أصحاب المصلحة، بما في ذلك الأفراد والشركات والحكومات.[106] تتضمن المبادئ الأساسية لملكية البيانات والخصوصية ما يلي:

- الحقوق الفردية:منح الأفرادالسيطرةعلى بياناتهم الشخصية،بمافي ذلك الحق في الوصول إلى بياناتهم وتصحيحها وحذفها.
- المسؤولية المؤسسية: ضمان تعامل الشركات مع البيانات بمسؤولية وشفافية، مع وجود سياسات واضحة لاستخدام البيانات ومشاركتها.
- الامتثال التنظيمي: الالتزام بلوائح حماية البيانات، مثل اللائحة العامة لحماية البيانات، التي تضع متطلبات صارمة لخصوصية البيانات والمساءلة.

إن حماية خصوصية البيانات مهمة بشكل خاص في سياق التقنيات الناشئة، مثل إنترنت الأشياء والذكاء الاصطناعي، حيث غالبًا ما يكون جمع البيانات منتشرًا وغير شفاف. على سبيل المثال، تجمع أجهزة إنترنت الأشياء كميات هائلة من بيانات الاستشعار، مما يثير المخاوف بشأن كيفية استخدام هذه البيانات ومن لديه حق الوصول إليها.[107]

خامسا: مسؤولية البيانات وإدارتها

تشير مسؤولية البيانات وإدارتها إلى الإدارة الأخلاقية والمسؤولة للبيانات طوال دورة حياتها. ويشمل هذا ضمان استخدام البيانات بطرق تتوافق مع القيم المجتمعية ولا تسبب ضررًا.[108] ويتم ذلك عن طريق الاستخدام الأخلاقي للبيانات وضمان استخدام البيانات بطرق تحترم الحقوق الفردية وتعزز الرفاهية المجتمعية. لذلك يجب انشاء آليات مساءلة واضحة لممارسات البيانات، بما في ذلك عمليات الرقابة والتدقيق. بالإضافة الى إشراك أصحاب المصلحة من خلال التواصل معهم لفهم مخاوفهم وتوقعاتهم فيما يتعلق باستخدام البيانات.[109] تعتبر إدارة البيانات مهمة بشكل خاص في سياق الذكاء الاصطناعي، حيث يمكن أن يؤدي إساءة استخدام البيانات إلى نتائج متحيزة أو تمييزية. على سبيل المثال، يمكن أن تؤدي بيانات التدريب المتحيزة إلى أنظمة الذكاء الاصطناعي التي تديم أوجه عدم المساواة القائمة، مثل التحيزات العنصرية أو الجنسانية.[110]

سادسا: أمن البيانات

يعد أمن البيانات حجر الزاوية في حوكمة المسؤولية الرقمية للشركات، لأنه يحمي الأصول الرقمية والمعلومات الحساسة من الوصول غير المصرح به والانتهاكات وإساءة الاستخدام. إن تدابير أمن البيانات الفعّالة ضرورية للحفاظ على ثقة أصحاب المصلحة والامتثال للمتطلبات التنظيمية.[111] ويتم ضمان امن البيانات من خلال استخدام التشفير لحماية البيانات أثناء النقل وفي حالة السكون. وتنفيذ ضوابط وصول صارمة لضمان وصول الأفراد المصرح لهم فقط إلى البيانات الحساسة. بالإضافة الى الاستجابة للحوادث عن طريق وضع بروتوكولات للاستجابة لانتهاكات البيانات وحوادث الأمن، بما في ذلك الإخطار في الوقت المناسب لأصحاب المصلحة المتضررين.[112] يعد أمن البيانات أمرًا بالغ الأهمية بشكل خاص في الصناعات مثل الرعاية الصحية والتمويل، حيث يمكن أن يكون للانتهاكات عواقب وخيمة على الأفراد

والمؤسسات. على سبيل المثال، يمكن أن يؤدي خرق البيانات في مؤسسة رعاية صحية إلى الكشف عن معلومات حساسة للمريض، مما يؤدي إلى سرقة الهوية أو أضرار أخرى.[113] من خلال مراعاة أمن البيانات، يمكن للشركات التخفيف من المخاطر وحماية مصالح أصحاب المصلحة.

سابعا: استخدام البيانات وإمكانية الوصول إليها

يشير استخدام البيانات وإمكانية الوصول إليها إلى كيفية استخدام البيانات ومن لديه حق الوصول إليها. يضمن الاستخدام الأخلاقي للبيانات استخدام البيانات بطرق تتوافق مع القيم المجتمعية ولا تسبب ضررًا، في حين تضمن إمكانية الوصول أن البيانات متاحة لمن يحتاجون إليها.[114] لذا يجب تقييد الغرض لضمان استخدام البيانات فقط للأغراض التي تم جمعها من أجلها. وتعزيز الوصول العادل والشامل إلى البيانات، وخاصة للمجتمعات المهمشة أو المحرومة. ويجب مراعاة الشفافية عن طريق تقديم معلومات واضحة حول كيفية استخدام البيانات ومن لديه حق الوصول إليها.[115] تعتبر إمكانية الوصول إلى البيانات مهمة بشكل خاص في سياق مبادرات البيانات المفتوحة، حيث تجعل الحكومات والشركات البيانات متاحة للجمهور لتعزيز الابتكار والشفافية. ومع ذلك، يجب موازنة إمكانية الوصول مع اعتبارات الخصوصية والأمان لضمان عدم إساءة استخدام البيانات الحساسة.[116]

ثامنا: أخلاقيات الروبوت

تشير أخلاقيات الروبوت إلى الاعتبارات الأخلاقية المحيطة بتطوير واستخدام الروبوتات والأنظمة المستقلة. ومع تزايد دمج الروبوتات في المجتمع، يجب على الشركات معالجة القضايا الأخلاقية مثل المساءلة والسلامة والتأثير على العمالة.[117] وتتضمن المبادئ الأساسية لأخلاقيات الروبوت:

- المساءلة: ضمان وجود آليات واضحة لمحاسبة الأفراد أو الشركات عن تصرفات الروبوتات.
- السلامة: تصميم الروبوتات للعمل بأمان وتقليل المخاطر على البشر والبيئة.
- التأثير الاجتماعي: النظر في الآثار الاجتماعية الأوسع للروبوتات، مثل التأثير على العمالة والكرامة الإنسانية.[118]

إن أخلاقيات الروبوتات ذات أهمية خاصة في التصنيع والرعاية الصحية والنقل، حيث يتم استخدام الروبوتات بشكل متزايد لأداء المهام التي يقوم بها البشر تقليديًا. على سبيل المثال، يثير استخدام المركبات ذاتية القيادة أسئلة أخلاقية حول كيفية اتخاذ القرارات في المواقف التي تهدد الحياة.[119] من خلال إعطاء الأولوية لأخلاقيات الروبوتات، يمكن للشركات ضمان أن استخدامها للروبوتات يتماشى مع المبادئ الأخلاقية والقيم المجتمعية. من كل ما تقدم نخلص الى إن حوكمة المسؤولية الرقمية للشركات هي تحدٍ متعدد الأوجه يتطلب من الشركات معالجة مجموعة واسعة من الاعتبارات الأخلاقية والاجتماعية والبيئية، والتي بدورها تمكن الشركات من بناء الثقة مع أصحاب المصلحة والامتثال للمتطلبات التنظيمية والمساهمة في نظام بيئي رقمي مستدام وعادل. كما لا تعمل هذه الجهود على تعزيز سمعة الشركة فحسب، بل تضمن أيضًا استدامة الأعمال التجارية على المدى الطويل في العصر الرقمي.

المطلب الثاني: تحديات تنفيذ المسؤولية الرقمية للشركات

إن دمج المسؤولية الرقمية للشركات في ممارسات الشركات محفوف بالتحديات القانونية التي تتطلب الملاحظة الدقيقة. ومع اعتماد الشركات بشكل متزايد على التقنيات الرقمية، واتخاذ القرارات القائمة على البيانات، والابتكارات الناشئة مثل الذكاء الاصطناعي والأتمتة، يجب عليها معالجة شبكة معقدة من الاعتبارات القانونية وهي:

أولا: الامتثال التنظيمي

الامتثال التنظيمي هو حجر الزاوية في المسؤولية الرقمية للشركات، حيث يجب على الشركات الالتزام بمشهد سريع التطور للقوانين واللوائح التي تحكم الممارسات الرقمية. تشمل مجالات الاهتمام الرئيسية خصوصية البيانات وحوكمة الذكاء الاصطناعي والأمن السيبراني. على سبيل المثال، وضع قانون حماية البيانات العامة في الاتحاد الأوروبي وقانون خصوصية المستهلك في كاليفورنيا في الولايات المتحدة معايير صارمة لحماية البيانات والخصوصية. تتطلب هذه اللوائح من الشركات تنفيذ أطر حوكمة بيانات قوية، بما في ذلك تقليل البيانات، والحد من الغرض، وآليات إخطار الاختراق.[120]

إن التقنيات الناشئة مثل الذكاء الاصطناعي تزيد من تعقيد الامتثال. على سبيل المثال، يفرض قانون الذكاء الاصطناعي المقترح من الاتحاد الأوروبي الشفافية وعدم التمييز والإشراف البشري في أنظمة الذكاء الاصطناعي.[121] اذ يجب على الشركات أن تتماشى مبادرات الذكاء الاصطناعي الخاصة بها مع هذه المتطلبات لتجنب العواقب القانونية. بالإضافة إلى ذلك، يضيف الامتثال لقانون المنافسة وحقوق الملكية الفكرية ولوائح العمل طبقات من التعقيد إلى تنفيذ المسؤولية الرقمية للشركات.[122] ولمعالجة هذه التحديات، ينبغي للشركات الحفاظ على فهم عميق للقوانين واللوائح ذات الصلة، وتنفيذ أطر الامتثال القوية، بما في ذلك تقييمات المخاطر والتدقيق المنتظمة. علاوة على الاستثمار في الخبرة القانونية للموائمة مع المشهد التنظيمي المتطور.[123]

ثانيا: المسؤولية وإدارة المخاطر

يؤدي استخدام التقنيات الرقمية إلى تعريض الشركات لمخاطر المسؤولية الجديدة، مثل التحيز الخوارزمي، وانتهاكات البيانات، والعواقب غير المقصودة للأنظمة الآلية. ويثير اتخاذ القرارات الخوارزمية، على وجه الخصوص، مخاوف بشأن المساءلة، حيث أن تعقيد هذه الأنظمة يجعل من الصعب تتبع الأخطاء أو الأعطال.[124] كما تشكل انتهاكات البيانات مخاطر مالية وسمعة كبيرة، حيث بلغ متوسط تكلفة الاختراق في الولايات المتحدة 8.64 مليون دولار في عام 2020.[125]

للتخفيف من هذه المخاطر، يجب على الشركات تطوير استراتيجيات شاملة لتقييم المخاطر والتخفيف منها. وتأمين تغطية تأمينية مناسبة وصياغة اتفاقيات تعاقدية واضحة لتخصيص المسؤولية.[126] بالإضافة الى تنفيذ تدابير أمنية قوية للبيانات، مثل التشفير وضوابط الوصول، لمنع الخروقات.[127]

ثالثا: الملكية الفكرية وملكية البيانات

لقد أدى صعود التقنيات الرقمية إلى تحويل مشهد الملكية الفكرية، مما خلق تحديات حول ملكية الأصول الرقمية والتحكم فيها مثل الخوارزميات ومجموعات البيانات والبرامج. إن عدم ملموسية هذه الأصول وقابليتها للتكرار تعقد أطر الملكية الفكرية التقليدية.[128] بالإضافة إلى ذلك، فإن استخدام عملية اتخاذ القرار القائمة على البيانات يثير تساؤلات حول ملكية مجموعات البيانات الأساسية وحقوق الأفراد الذين تُستخدم بياناتهم.[129] يتعين على الشركات تطوير أطر قوية لإدارة الملكية الفكرية لحماية الأصول الرقمية، والتنقل بين ترتيبات مشاركة البيانات وضمان الامتثال لقواعد الخصوصية.[130] بالإضافة الى تعزيز ثقافة التعاون الرقمي مع حماية المزايا التنافسية.[131]

رابعا: قانون العمل والتوظيف

إن التحول الرقمي لمكان العمل يطرح تحديات قانونية تتعلق بخصوصية الموظفين ومراقبة البيانات والمعاملة العادلة. على سبيل المثال، يمكن أن تؤدي أنظمة الإدارة الخوارزمية إلى اتخاذ قرارات غير شفافة وتمييز محتمل.[132] إن التحول إلى العمل عن بعد، الذي تسارع بسبب جائحة كوفيد-19، يزيد من تعقيد الامتثال لقوانين العمل واتفاقيات المساومة الجماعية.[133] ولمعالجة هذه القضايا، ينبغي للشركات وضع سياسات تتماشى مع ممارسات مكان العمل الرقمي مع قوانين العمل، وتعزيز التواصل المفتوح مع الموظفين لمعالجة المخاوف بشأن التقنيات الرقمية.[134] بالإضافة الى الاستثمار في الخبرة القانونية للتماشي مع مشهد العمل المتطور.

خامسا: قانون مكافحة الاحتكار والمنافسة

إن تركيز القوة السوقية في المنصات الرقمية واستخدام الخوارزميات يثيران المخاوف بشأن الممارسات المناهضة للمنافسة. إن قدرة المنصات على تجميع كميات كبيرة من البيانات ونشر خوارزميات متطورة يمكن أن تخنق المنافسة والابتكار.[135] ان التواطؤ الخوارزمي، حيث تسهل الخوارزميات السلوك المناهض للمنافسة، هو مصدر قلق ناشئ آخر.[136] يتعين على الشركات تنفيذ أطر الامتثال للمنافسة لضمان الالتزام بقوانين مكافحة الاحتكار، وتعزيز قابلية نقل البيانات والتشغيل البيني لتعزيز المنافسة[137] ، وضمان الشفافية الخوارزمية لمنع التأثيرات المناهضة للمنافسة.[138]

سادسا: حوكمة الشركات والواجبات الائتمانية

إن دمج مبادئ المسؤولية الرقمية في عملية صنع القرار في الشركات له آثار على حوكمة الشركات والواجبات الائتمانية. يجب على المديرين والمسؤولين التأكد من أن الممارسات الرقمية تتماشى مع التزاماتهم القانونية تجاه أصحاب المصلحة.[139] الطبيعة الغامضة للأنظمة الخوارزمية تعقد الرقابة والمساءلة، مما يجعل من الصعب الوفاء بواجبات الرعاية والولاء.[140] وللتعامل مع هذه التحديات، يجب على الشركات تطوير أطر حوكمة قوية للإشراف على المبادرات الرقمية، وتعزيز مساءلة المديرين والمسؤولين من خلال سياسات واضحة ومراقبة الأداء.[141] علاوة على تعزيز ثقافة اتخاذ القرار الأخلاقي والمسؤولية الرقمية.[142]

الخاتمة

نخلص مما تقدم ان التقدم السريع للتقنيات الرقمية قد أحدث تحولاً جذرياً في المشهد المؤسسي، مما أتاح فرصاً وتحديات للشركات. وفي هذا السياق، برز مفهوم المسؤولية الرقمية للشركات كإطار عمل أساسي للمؤسسات لإدارة التطوير والنشر المسؤول للتقنيات الرقمية. وقد أكد هذا البحث ان الإطار القانوني للمسؤولية الرقمية للشركات يمثل أساسًا حيويًا لمعالجة التحديات المعقدة التي يفرضها العصر الرقمي. اذ من خلال تطبيق أطر حوكمة متينة للمسؤولية الرقمية للشركات، يمكن للشركات ضمان موثوقية وشفافية أنظمتها الرقمية، والإدارة المسؤولة للبيانات، والاستخدام الأخلاقي للتقنيات الناشئة، وحماية حقوق ومصالح أصحاب المصلحة. هذا النهج الشامل يُمكّن الشركات من التعامل مع المشهد الرقمي المعقد، وتعزيز الابتكار، والمساهمة في التحول الرقمي المستدام والشامل للمجتمع. ومع ذلك، فإن دمج المسؤولية الرقمية للشركات في استراتيجية الشركة وعملياتها لا يخلو من التحديات، وللتغلب على هذه التحديات يوصي الباحث:

1- تطوير أطر حوكمة شاملة: ينبغي على الشركات وضع سياسات وإجراءات وآليات مساءلة واضحة لضمان التطوير والنشر المسؤول للتقنيات الرقمية، مع التركيز على إدارة البيانات، والذكاء الاصطناعي الأخلاقي، وحقوق أصحاب المصلحة.

2- تعزيز التعاون بين الوظائف: يتطلب التنفيذ الفعال لإدارة المسؤولية والمخاطر تعاونًا وثيقًا بين الفرق القانونية، وتكنولوجيا المعلومات، وإدارة المخاطر، والفرق الأخرى ذات الصلة لضمان نهج شامل ومتسق للمسؤولية الرقمية.

3- الاستثمار في الخبرة القانونية والمهارات المتخصصة: يُمكن أن يُوفر توظيف متخصصين ذوي خبرة في التقنيات الناشئة، وخصوصية البيانات، وإدارة المسؤولية، إرشادات ودعمًا قيّمين في مواجهة التحديات القانونية والتنظيمية المتعلقة بحل النزاعات الرقمية.

4- ندعو المشرع العراقي الى تشريع القوانين ووضع السياسات التي تُعالج التحديات الفريدة التي يُشكلها الاقتصاد الرقمي، اذ ان تطوير أطر قانونية شاملة وقابلة للتكيف أمرًا بالغ الأهمية في تمكين الشركات من الوفاء بمسؤولياتها الرقمية.

5- تعزيز ثقافة المسؤولية الرقمية: يُعدّ ترسيخ ثقافة مؤسسية تُعطي الأولوية للاستخدام الأخلاقي والمستدام للتقنيات الرقمية، وتُمكّن الموظفين، وتُعزز ثقة أصحاب المصلحة، أمرًا أساسيًا لنجاح تنفيذ حل النزاعات الرقمية.

من خلال تنفيذ هذه التوصيات ومعالجة التحديات القانونية المُحددة، يُمكن للشركات إثبات التزامها بالمسؤولية الرقمية للشركات، وتعزيز استدامتها ومرونتها على المدى الطويل، والمساهمة في تطوير نظام بيئي رقمي أكثر إنصافًا وجدارة بالثقة.

الهوامش

(1) Lobschat, Lara, Benjamin Mueller, Felix Eggers, Laura Brandimarte, Sarah Diefenbach, Mirja Kroschke, and Jochen Wirtz. "Corporate digital responsibility." *Journal of Business Research* 122 (2021), p. 875.

(2) Floridi, Luciano, and Andrew Strait. "Ethical foresight analysis: What it is and why it is needed?." *The 2020 Yearbook of the Digital Ethics Lab* (2021), p. 182.

(3) Stahl, Bernd Carsten, Andreas Andreou, Philip Brey, Tally Hatzakis, Alexey Kirichenko, Kevin Macnish, S. Laulhé Shaelou, Andrew Patel, Mark Ryan, and David Wright. "Artificial intelligence for human flourishing–Beyond principles for machine learning." *Journal of Business Research* 124 (2021), p. 377.

(4) Wang, Mansi, Renmiao Yuan, Xin Guan, Zeyu Wang, Yanzhao Zeng, and Tao Liu. "The influence of digital platform on the implementation of corporate social responsibility: from the perspective of environmental science development to explore its potential role in public health." *Frontiers in Public Health* 12 (2024): 1343546.

(5) Kietzmann, Jan, Jeannette Paschen, and Emily Treen. "Artificial intelligence in advertising: How marketers can leverage artificial intelligence along the consumer journey." *Journal of Advertising Research* 58, no. 3 (2018), p. 263-267.

(6) Zuboff, Shoshana. "The age of surveillance capitalism." In *Social theory re-wired*, Routledge, 2023, p, 78; Taddeo, Mariarosaria, and Luciano Floridi. "How AI can be a force for good." *Science* 361, no. 6404 (2018), p. 751-752.

(7) Jobin, Anna, Marcello Ienca, and Effy Vayena. "The global landscape of AI ethics guidelines." *Nature machine intelligence* 1, no. 9 (2019): 389; Cath, Corinne. "Governing artificial intelligence: ethical, legal and technical opportunities and challenges." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018): 20180080, p. 5.

(8) Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." *Computer networks* 57, no. 10 (2013), p. 2266-2279; Schneier, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company, 2015, p. 45.

(9) Srnicek, N. "Platform Capitalism. Polity Press, Cambridge Malden, MA." (2017), p, 43; van Dijck, Jose. "The platform society: Public values in a connective world." (2018), p, 12.

(10) Manyika, J. "Jobs lost, jobs gained: Workforce transitions in a time of automation." *McKinsey Global Institute* 150 (2017); Autor, David H. "Why are there still so many jobs? The history and future of workplace automation." *Journal of economic perspectives* 29, no. 3 (2015), p. 5.

(11) Bieser, Jan CT, and Lorenz M. Hilty. "Assessing indirect environmental effects of information and communication technology (ICT): A systematic literature review." *Sustainability* 10, no. 8 (2018): 2662, p, 2; Freitag, Charlotte, Mike Berners-Lee, Kelly Widdicks, Bran Knowles, Gordon S. Blair, and Adrian Friday. "The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations." *Patterns* 2, no. 9 (2021), p, 8.

(12) Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The economics of privacy." *Journal of economic Literature* 54, no. 2 (2016), p. 442.

(13) West, Darrell M. *The future of work: Robots, AI, and automation*. Brookings Institution Press, 2018, p. 23; Bessen, James. *AI and jobs: The role of demand*. No. w24235. National Bureau of Economic Research, 2018, p. 10.

(14) Eccles, Robert G., and Svetlana Klimenko. "The investor revolution." *Harvard Business Review* 97, no. 3 (2019): 106-116.

(15) Veale, M., & Zuiderveen Borgesius, F. Demystifying the draft EU Artificial Intelligence Act. *Computer Law & Security Review*, *42. 2021,* P. 1.
(16) Tankard, Colin. "What the GDPR means for businesses." *Network Security* 2016, no. 6 (2016), p. 7.
(17) Holdings, Daniel J. Edelman. *Inc. Edelman Trust Barometer*,2021 p. 14.
(18) UN Global Compact. *Uniting Business in the Decade of Action.2020,* p. 15.
(19) European Commission, 2021, p. 3.
(20) Khan, Lina M. "Amazon's antitrust paradox." *Yale lJ* 126 (2016): 712.
(21) Carroll, Archie B. "The Pyramid of Corporate Social Responsibility: Toward the Moral Management of Organizational Stakeholders." *Business Horizons* (1991), p. 40.
(22) Lobschat, Lara, Benjamin Mueller, Felix Eggers, Laura Brandimarte, Sarah Diefenbach, Mirja Kroschke, and Jochen Wirtz. "Corporate digital responsibility." *Journal of Business Research* 122 (2021): p. 875.
(23) GDPR, 2016, Art. 5.
(24) Floridi et al., 2018, p. 689.
(25) van Dijk, J. A. G. M. The digital divide. Polity Press, 2020, p. 2.
(26) Freeman, R. Edward. *Strategic management: A stakeholder approach*. Cambridge university press, 2010, p. 25.
(27) Hilty, Lorenz M., and Bernard Aebischer. "ICT for sustainability: An emerging research field." *ICT innovations for Sustainability* (2015): p. 10.
(28) Lobschat et al., 2021, p. 880.
(29) Floridi, 2019, p. 12.
(30) European Commission, 2021, p. 3.
(31) Lobschat et al., 2021, p. 890
(32) Lobschat et al., 2021, p. 890
(33)Hildebrandt, Mireille. "Algorithmic regulation and the rule of law." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (2018): 20170355, p. 17.
(34) Floridi, 2019, p. 15.
(35) Cath, Corinne. "Governing artificial intelligence: ethical, legal and technical opportunities and challenges." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018): 20180080., p. 189.
(36) Park, Hyojin, Hyeontaek Oh, and Jun Kyun Choi. "A Consent-Based Privacy-Compliant Personal Data-Sharing System." *IEEE Access* 11 (2023): 95912-95927.
(37) Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP* 4162018 (2018): p, 6.
(38) Purwoto, Purwoto, Mujiono Hafidh Prasetyo, Aditya Yuli Sulistyawan, and Kadek Cahya Susila Wibawa. "Corporate Responsibility For Personal Data Breach Cases." *International Journal of Multidisciplinary Research and Analysis* 6 (2023): 2757-60.
(39) Lynskey, Orla. *The Foundations of EU Data Protection Law*. Oxford University Press, 2015, p. 101.
(40) Floridi, Luciano. "The ethics of artificial intelligence: Principles, challenges, and opportunities." (2023).
(41) Cheryl, Barr-Kumarakulasinghe, and Boon-Kwee Ng. "Protecting the unprotected consumer data in internet of things: Current scenario of data governance in Malaysia." *Sustainability* 14, no. 16 (2022): 9893.
(42) European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L119*, 2016, 1–88.
(43) Article 4/1 stated: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or

indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

(44) Article 7: Conditions for consent

1- Where processing is based on consent, the controller shall be able to demonstrate that the data subject has

consented to processing of his or her personal data.

2- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3- The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the

performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

(45) See: CHAPTER III Rights of the data subject

(46) Article 83/6 stated: Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

(47) Tikkinen-Piri, Christina, Anna Rohunen, and Jouni Markkula. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies." *Computer Law & Security Review* 34, no. 1 (2018): 134-153.

(48) Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." *A practical guide, 1st ed., Cham: Springer International Publishing* 10, no. 3152676 (2017): 10-5555.

(49) Hu, Ivy Yihui. "The Global Diffusion of the 'General Data Protection Regulation'(GDPR)." *Edited by KH Stapelbroek and S. Grand. Erasmus School of Social and Behavioural Sciences* (2019).

(50) Bakare, Seun Solomon, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh. "Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations." *Computer Science & IT Research Journal* 5, no. 3 (2024): 528-543.

(51) Bolatbekkyzy, Gulbakyt. "Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation." *Groningen Journal of International Law* 11, no. 1.

(52) Bakare et al., 2024, p. 534.

(53) NIST, 2018, p. 1

(54) Dunn Cavelty, Myriam. "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities." *Science and engineering ethics* 20 (2014): p. 707.

(55) Ibid, 710.

(56) Floridi, Luciano. *The Fourth Revolution: How the infosphere is reshaping human reality*. Oxford University Press, 2014, p. 18.

(57) NIST, 2018, p. 4.

(58) Renn, Ortwin. *Risk governance: coping with uncertainty in a complex world*. Routledge, 2017, p. 9.

(59) NIST, 2018, p. 24.

(60) Ibid.

(61) GDPR, 2016, Art. 33–34.

(62) International Organization for Standardization. *ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements*. International

Organization for Standardization, 2013, p. 1; Humphreys, Edward. *Implementing the ISO/IEC 27001 information security management system standard*. Artech House, Inc., 2007.

(63) Disterer, Georg. "ISO/IEC 27000, 27001 and 27002 for information security management." *Journal of Information Security* 4, no. 2 (2013).

(64) NIST, 2018, p. 1.

(65) White, Gregory B., and Natalie Sjelin, eds. *Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM)*. IGI Global, 2020.

(66) DSS, WHAT IS PCI. "Payment Card Industry Data Security Standard (PCI DSS) 3.2." (2010). PCI Security Standards Council. (2018). *Payment Card Industry Data Security Standard (PCI DSS)*, p. 5.

(67) Liu, Jing, Yang Xiao, Hui Chen, Suat Ozdemir, Srinivas Dodle, and Vikas Singh. "A survey of payment card industry data security standard." *IEEE Communications Surveys & Tutorials* 12, no. 3 (2010): 287-303.

(68) Zaeem, Razieh Nokhbeh, and K. Suzanne Barber. "The effect of the GDPR on privacy policies: Recent progress and future promise." *ACM Transactions on Management Information Systems (TMIS)* 12, no. 1 (2020): 1-20.

(69) Floridi, Luciano. "The ethics of artificial intelligence: Principles, challenges, and opportunities." (2023); Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic impact assessments: a practical Framework for Public Agency." *AI Now* 9 (2018), p. 4.

(70) Busuioc, Madalina. "Accountable artificial intelligence: Holding algorithms to account." *Public administration review* 81, no. 5 (2021): 825-836.

(71) Barocas, Solon, and Andrew D. Selbst. "Big data's disparate impact." *Calif. L. Rev.* 104 (2016): p. 671.

(72) Samek, W. "Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models." *arXiv preprint arXiv:1708.08296* (2017), p. 1.

(73) Vaccaro, Antonino, and Peter Madsen. "Corporate dynamic transparency: the new ICT-driven ethics?." *Ethics and information technology* 11 (2009): 113-122.

(74) DeSimone, Hanna, and Maikel Leon-Espinosa. "Explainable ai: The quest for transparency in business and beyond." In *2024 7th International Conference on Information and Computer Technologies (ICICT)*, pp. 532-538. IEEE, 2024.

(75) Werz, Johanna M., Esther Borowski, and Ingrid Isenhardt. "Explainability as a Means for Transparency? Lay Users' Requirements Towards Transparent AI." *Cognitive Computing and Internet of Things* 124, no. 124 (2024).

(76) O'Shaughnessy, Matthew. "Five policy uses of algorithmic transparency and explainability." *arXiv preprint arXiv:2302.03080* (2023).

(77) Kunz, Werner H., and Jochen Wirtz. "Corporate digital responsibility (CDR) in the age of AI: implications for interactive marketing." *Journal of Research in Interactive Marketing* 18, no. 1 (2024): 31-37.

(78) Kong, Dongmin, and Boyang Liu. "Digital technology and corporate social responsibility: evidence from China." *Emerging Markets Finance and Trade* 59, no. 9 (2023): 2967-2993.

(79) Friedman, Batya, and Helen Nissenbaum. "Bias in computer systems." *ACM Transactions on information systems (TOIS)* 14, no. 3 (1996): p. 332.

(80) Corbett-Davies, Sam, Johann D. Gaebler, Hamed Nilforoshan, Ravi Shroff, and Sharad Goel. "The measure and mismeasure of fairness." *Journal of Machine Learning Research* 24, no. 312 (2023): 1-117.

(81) Zhang, Chenglong, Varghese S. Jacob, and Young U. Ryu. "Modeling individual fairness beliefs and its applications." *ACM Transactions on Management Information Systems* 15, no. 3 (2024): 1-26.

(82) Imai, Kosuke, and Zhichao Jiang. "Principal fairness for human and algorithmic decision-making." *Statistical Science* 38, no. 2 (2023): 317-328.

(83) Lalor, John P., Ahmed Abbasi, Kezia Oketch, Yi Yang, and Nicole Forsgren. "Should fairness be a metric or a model? A model-based framework for assessing bias in machine learning pipelines." *ACM Transactions on Information Systems* 42, no. 4 (2024): 1-41.

[84]Loader, Brian D., and Dan Mercea. "Networking democracy? Social media innovations and participatory politics." *Information, communication & society* 14, no. 6 (2013): p. 760.
[85] European Parliament, 2016, p. 36.
[86]Calderaro & Kavada, 2013, p. 3.
[87] Hilty, Lorenz M., and Bernard Aebischer. "ICT for sustainability: An emerging research field." *ICT innovations for Sustainability* (2015): p. 10.
[88] European Parliament, 2016, p. 36.
[89] Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." *URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP* 4162018 (2018): p. 6.
[90] Howells, 2005, p. 348.
[91] Lynskey, 2017, p. 101.
[92] Calderaro & Kavada, 2013, p. 3
[93] Barocas & Selbst, 2016, p. 674
[94] Hilty, Lorenz M., and Bernard Aebischer. "ICT for sustainability: An emerging research field." *ICT innovations for Sustainability* (2015): p, 10.
[95] Leveson, Nancy G. *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016, p. 45.
[96] Ibid, 47.
[97] Topol, Eric. *Deep medicine: how artificial intelligence can make healthcare human again*. Hachette UK, 2019, p. 23.
[98] Floridi, 2014, p. 18.
[99] Ibid, p. 20.
[100] Barocas & Selbst, 2016, p. 674.
[101]Cath, Corinne. "Governing artificial intelligence: ethical, legal and technical opportunities and challenges." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018): 20180080, p. 189.
[102] European Parliament, 2016, p. 35.
[103] NIST, 2018, p. 6.
[104] Cath, 2018, p. 190.
[105] Zuboff, 2019, p. 78.
[106] Lynskey, 2017, p. 101.
[107] Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. "Context aware computing for the internet of things: A survey." *IEEE communications surveys & tutorials* 16, no. 1 (2013): 414-454.
[108] Floridi et al., 2018, p. 689.
[109] Ibid, p. 690.
[110] Barocas & Selbst, 2016, p. 674.
[111] NIST, 2018, p. 1.
[112] Ibid, p. 6.
[113] Dunn Cavelty, Myriam. "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities." *Science and engineering ethics* 20 (2014): p, 707.
[114] Floridi, 2014, p. 18.
[115] Ibid, p, 20.
[116] Loader, Brian D., and Dan Mercea. "Networking Democracy?: Social Media Innovations in Participatory Politics." In *Social media and democracy*, pp. 1-10. Routledge, 2012, p. 3.
[117] Lin, Patrick, Keith Abney, and George Bekey. "Robot ethics: Mapping the issues for a mechanized world." *Artificial intelligence* 175, no. 5-6 (2011): p. 942.
[118] Ibid. p. 943.
[119] Ibid. p. 945.
[120] Lukács, Adrienn, and Szilvia Váradi. "GDPR-compliant AI-based automated decision-making in the world of work." *Computer Law & Security Review* 50 (2023): 105848.

(121) Justo-Hanani, Ronit. "The politics of Artificial Intelligence regulation and governance reform in the European Union." *Policy Sciences* 55, no. 1 (2022): 137-159.
(122) Cath, Corinne, Sandra Wachter, Brent Mittelstadt, Mariarosaria Taddeo, and Luciano Floridi. "Artificial intelligence and the 'good society': the US, EU, and UK approach." *Science and engineering ethics* 24 (2018): p. 511.
(123) Folorunso, Adebola, Temitope Adewumi, Adeola Adewa, Roy Okonkwo, and Tayo Nathaniel Olawumi. "Impact of AI on cybersecurity and security compliance." *Global Journal of Engineering and Technology Advances* 21, no. 01 (2024): 167-184.
(124) Hildebrandt, Mireille. "Algorithmic regulation and the rule of law." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (2018): 20170355, p. 17.
(125) Ponemon Institute. Cost of a data breach report. IBM Security, 2020, p. 6.
(126) Schuett, Jonas. "Risk management in the artificial intelligence act." *European Journal of Risk Regulation* 15, no. 2 (2024): 367-385.
(127) Ponemon Institute, 2020, p. 6.
(128) Ciuriak, Dan. "Intellectual Property and the Digital Economy: Five Issues for International Norms and Trade Rules." *Available at SSRN 3923127* (2021).
(129) Alejandre, Gemma Minero. "Ownership of databases: Personal data protection and intellectual property rights on databases." *European Review of Private Law* 29, no. 5 (2021).
(130) Samuelson, Pamela, and Suzanne Scotchmer. "The law and economics of reverse engineering." *Yale LJ* 111 (2001): 1575.
(131) Chen, Wen, and Ying Wu. "Does intellectual property protection stimulate digital economy development?." *Journal of Applied Economics* 25, no. 1 (2022): 723-730.
(132) Rosenblat, Alex, and Luke Stark. "Algorithmic labor and information asymmetries: A case study of Uber's drivers." *International journal of communication* 10 (2016): p. 27.
(133) Mehra, Salil K. "Remote Work and Development–A Law-and-Economics Perspective." *Law and Development Review* 0 (2024).
(134) Horváth, István, Daniel Pérez del Prado, Zoltán Petrovics, and Andrea Sitzia. "The Role of Digitisation in Employment and Its New Challenges for Labour Law Regulation." *ELTE LJ* (2021): 101.
(135) Hennemann, Moritz. "Artificial Intelligence and Competition Law." *Regulating Artificial Intelligence* (2020): 361-388.
(136) Mehra, Salil K. "Antitrust and the robo-seller: Competition in the time of algorithms." *Minn. L. Rev.* 100 (2015): 1313.
(137) Furman, Jason. "Unlocking digital competition: Report of the Digital Competition Expert Panel." (2019), p. 12.
(138) Hennemann, 2020, p. 372.
(139) Malukani, Bharti, Ashima Joshi, and Satnam Ubeja. "Corporate Governance in the Digital Age: Insights and Recommendations." *IUP Journal of Corporate Governance* 23, no. 3 (2024): 50-58.
(140) Stilgoe, Jack. "Machine learning, social learning and the governance of self-driving cars." *Social studies of science* 48, no. 1 (2018): p. 141.
(141) Rubinstein, Ira S. "Big data: The end of privacy or a new beginning?." *Int'l Data Priv. L.* 3 (2013): p. 13.
(142) Stilgoe, 2018, p. 155.

المصادر

1. Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The economics of privacy." Journal of economic Literature 54, no. 2 (2016).
2. Alejandre, Gemma Minero. "Ownership of databases: Personal data protection and intellectual property rights on databases." European Review of Private Law 29, no. 5 (2021).
3. Autor, David H. "Why are there still so many jobs? The history and future of workplace automation." Journal of economic perspectives 29, no. 3 (2015).

4. Bakare, Seun Solomon, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh. "Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations." Computer Science & IT Research Journal 5, no. 3 (2024).
5. Barocas, Solon, and Andrew D. Selbst. "Big data's disparate impact." Calif. L. Rev. 104 (2016).
6. Bessen, James. AI and jobs: The role of demand. No. w24235. National Bureau of Economic Research, 2018.
7. Bieser, Jan CT, and Lorenz M. Hilty. "Assessing indirect environmental effects of information and communication technology (ICT): A systematic literature review." Sustainability 10, no. 8 (2018): 2662.
8. Bolatbekkyzy, Gulbakyt. "Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation." Groningen Journal of International Law 11, no. 1.
9. Busuioc, Madalina. "Accountable artificial intelligence: Holding algorithms to account." Public administration review 81, no. 5 (2021): 825-836.
10. Carroll, Archie B. "The Pyramid of Corporate Social Responsibility: Toward the Moral Management of Organizational Stakeholders." Business Horizons (1991).
11. Cath, Corinne, Sandra Wachter, Brent Mittelstadt, Mariarosaria Taddeo, and Luciano Floridi. "Artificial intelligence and the 'good society': the US, EU, and UK approach." Science and engineering ethics 24 (2018).
12. Cath, Corinne. "Governing artificial intelligence: ethical, legal and technical opportunities and challenges." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 376, no. 2133 (2018): 20180080.
13. Chen, Wen, and Ying Wu. "Does intellectual property protection stimulate digital economy development?." Journal of Applied Economics 25, no. 1 (2022): 723-730.
14. Cheryl, Barr-Kumarakulasinghe, and Boon-Kwee Ng. "Protecting the unprotected consumer data in internet of things: Current scenario of data governance in Malaysia." Sustainability 14, no. 16 (2022): 9893.
15. Ciuriak, Dan. "Intellectual Property and the Digital Economy: Five Issues for International Norms and Trade Rules." Available at SSRN 3923127 (2021).
16. Corbett-Davies, Sam, Johann D. Gaebler, Hamed Nilforoshan, Ravi Shroff, and Sharad Goel. "The measure and mismeasure of fairness." Journal of Machine Learning Research 24, no. 312 (2023).
17. Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP 4162018 (2018).
18. DeSimone, Hanna, and Maikel Leon-Espinosa. "Explainable ai: The quest for transparency in business and beyond." In 2024 7th International Conference on Information and Computer Technologies (ICICT), pp. 532-538. IEEE, 2024.
19. Disterer, Georg. "ISO/IEC 27000, 27001 and 27002 for information security management." Journal of Information Security 4, no. 2 (2013).
20. DSS, WHAT IS PCI. "Payment Card Industry Data Security Standard (PCI DSS) 3.2." (2010). PCI Security Standards Council. (2018). Payment Card Industry Data Security Standard (PCI DSS).
21. Dunn Cavelty, Myriam. "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities." Science and engineering ethics 20 (2014).
22. Eccles, Robert G., and Svetlana Klimenko. "The investor revolution." Harvard Business Review 97, no. 3 (2019): 106-116.
23. European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 2016.
24. Floridi, Luciano, and Andrew Strait. "Ethical foresight analysis: What it is and why it is needed?." The 2020 Yearbook of the Digital Ethics Lab (2021).
25. Floridi, Luciano. "The ethics of artificial intelligence: Principles, challenges, and opportunities." (2023).
26. Floridi, Luciano. The Fourth Revolution: How the infosphere is reshaping human reality. Oxford University Press, 2014, p. 18.
27. Folorunso, Adebola, Temitope Adewumi, Adeola Adewa, Roy Okonkwo, and Tayo Nathaniel Olawumi. "Impact of AI on cybersecurity and security compliance." Global Journal of Engineering and Technology Advances 21, no. 01 (2024).
28. Freeman, R. Edward. Strategic management: A stakeholder approach. Cambridge university press, 2010.
29. Freitag, Charlotte, Mike Berners-Lee, Kelly Widdicks, Bran Knowles, Gordon S. Blair, and Adrian Friday. "The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations." Patterns 2, no. 9 (2021).
30. Friedman, Batya, and Helen Nissenbaum. "Bias in computer systems." ACM Transactions on information systems (TOIS) 14, no. 3 (1996).
31. Furman, Jason. "Unlocking digital competition: Report of the Digital Competition Expert Panel." (2019).

32. Hennemann, Moritz. "Artificial Intelligence and Competition Law." Regulating Artificial Intelligence (2020): 361-388.
33. Hildebrandt, Mireille. "Algorithmic regulation and the rule of law." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 376, no. 2128 (2018): 20170355.
34. Hilty, Lorenz M., and Bernard Aebischer. "ICT for sustainability: An emerging research field." ICT innovations for Sustainability (2015).
35. Horváth, István, Daniel Pérez del Prado, Zoltán Petrovics, and Andrea Sitzia. "The Role of Digitisation in Employment and Its New Challenges for Labour Law Regulation." ELTE LJ (2021).
36. Hu, Ivy Yihui. "The Global Diffusion of the 'General Data Protection Regulation'(GDPR)." Edited by KH Stapelbroek and S. Grand. Erasmus School of Social and Behavioural Sciences (2019).
37. Imai, Kosuke, and Zhichao Jiang. "Principal fairness for human and algorithmic decision-making." Statistical Science 38, no. 2 (2023): 317-328.
38. Jobin, Anna, Marcello Ienca, and Effy Vayena. "The global landscape of AI ethics guidelines." Nature machine intelligence 1, no. 9 (2019).
39. Justo-Hanani, Ronit. "The politics of Artificial Intelligence regulation and governance reform in the European Union." Policy Sciences 55, no. 1 (2022): 137-159.
40. Khan, Lina M. "Amazon's antitrust paradox." Yale lJ 126 (2016).
41. Kietzmann, Jan, Jeannette Paschen, and Emily Treen. "Artificial intelligence in advertising: How marketers can leverage artificial intelligence along the consumer journey." Journal of Advertising Research 58, no. 3 (2018).
42. Kong, Dongmin, and Boyang Liu. "Digital technology and corporate social responsibility: evidence from China." Emerging Markets Finance and Trade 59, no. 9 (2023).
43. Kunz, Werner H., and Jochen Wirtz. "Corporate digital responsibility (CDR) in the age of AI: implications for interactive marketing." Journal of Research in Interactive Marketing 18, no. 1 (2024).
44. Lalor, John P., Ahmed Abbasi, Kezia Oketch, Yi Yang, and Nicole Forsgren. "Should fairness be a metric or a model? A model-based framework for assessing bias in machine learning pipelines." ACM Transactions on Information Systems 42, no. 4 (2024).
45. Leveson, Nancy G. Engineering a safer world: Systems thinking applied to safety. The MIT Press, 2016.
46. Lin, Patrick, Keith Abney, and George Bekey. "Robot ethics: Mapping the issues for a mechanized world." Artificial intelligence 175, no. 5-6 (2011).
47. Liu, Jing, Yang Xiao, Hui Chen, Suat Ozdemir, Srinivas Dodle, and Vikas Singh. "A survey of payment card industry data security standard." IEEE Communications Surveys & Tutorials 12, no. 3 (2010): 287-303.
48. Loader, Brian D., and Dan Mercea. "Networking democracy? Social media innovations and participatory politics." Information, communication & society 14, no. 6 (2013).
49. Lobschat, Lara, Benjamin Mueller, Felix Eggers, Laura Brandimarte, Sarah Diefenbach, Mirja Kroschke, and Jochen Wirtz. "Corporate digital responsibility." Journal of Business Research 122 (2021).
50. Lukács, Adrienn, and Szilvia Váradi. "GDPR-compliant AI-based automated decision-making in the world of work." Computer Law & Security Review 50 (2023): 105848.
51. Lynskey, Orla. The Foundations of EU Data Protection Law. Oxford University Press, 2015.
52. Malukani, Bharti, Ashima Joshi, and Satnam Ubeja. "Corporate Governance in the Digital Age: Insights and Recommendations." IUP Journal of Corporate Governance 23, no. 3 (2024).
53. Manyika, J. "Jobs lost, jobs gained: Workforce transitions in a time of automation." McKinsey Global Institute 150 (2017).
54. Mehra, Salil K. "Antitrust and the robo-seller: Competition in the time of algorithms." Minn. L. Rev. 100 (2015): 1313.
55. Mehra, Salil K. "Remote Work and Development–A Law-and-Economics Perspective." Law and Development Review 0 (2024).
56. O'Shaughnessy, Matthew. "Five policy uses of algorithmic transparency and explainability." arXiv preprint arXiv:2302.03080 (2023).
57. Park, Hyojin, Hyeontaek Oh, and Jun Kyun Choi. "A Consent-Based Privacy-Compliant Personal Data-Sharing System." IEEE Access 11 (2023): 95912-95927.
58. Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. "Context aware computing for the internet of things: A survey." IEEE communications surveys & tutorials 16, no. 1 (2013): 414-454.
59. Ponemon Institute. Cost of a data breach report. IBM Security, 2020.
60. Purwoto, Purwoto, Mujiono Hafidh Prasetyo, Aditya Yuli Sulistyawan, and Kadek Cahya Susila Wibawa. "Corporate Responsibility For Personal Data Breach Cases." International Journal of Multidisciplinary Research and Analysis 6 (2023): 2757-60.

61. Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic impact assessments: a practical Framework for Public Agency." AI Now 9 (2018).
62. Renn, Ortwin. Risk governance: coping with uncertainty in a complex world. Routledge, 2017.
63. Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." Computer networks 57, no. 10 (2013), p. 2266-2279.
64. Rosenblat, Alex, and Luke Stark. "Algorithmic labor and information asymmetries: A case study of Uber's drivers." International journal of communication 10 (2016): p. 27.
65. Rubinstein, Ira S. "Big data: The end of privacy or a new beginning?." Int'l Data Priv. L. 3 (2013).
66. Samek, W. "Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models." arXiv preprint arXiv:1708.08296 (2017).
67. Samuelson, Pamela, and Suzanne Scotchmer. "The law and economics of reverse engineering." Yale LJ 111 (2001).
68. Schneier, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2015.
69. Schuett, Jonas. "Risk management in the artificial intelligence act." European Journal of Risk Regulation 15, no. 2 (2024): 367-385.
70. Srnicek, N. "Platform Capitalism. Polity Press, Cambridge Malden, MA." (2017).
71. Stahl, Bernd Carsten, Andreas Andreou, Philip Brey, Tally Hatzakis, Alexey Kirichenko, Kevin Macnish, S. Laulhé Shaelou, Andrew Patel, Mark Ryan, and David Wright. "Artificial intelligence for human flourishing–Beyond principles for machine learning." Journal of Business Research 124 (2021), p. 377.
72. Stilgoe, Jack. "Machine learning, social learning and the governance of self-driving cars." Social studies of science 48, no. 1 (2018).
73. Taddeo, Mariarosaria, and Luciano Floridi. "How AI can be a force for good." Science 361, no. 6404 (2018).
74. Tankard, Colin. "What the GDPR means for businesses." Network Security 2016, no. 6 (2016).
75. Tikkinen-Piri, Christina, Anna Rohunen, and Jouni Markkula. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies." Computer Law & Security Review 34, no. 1 (2018): 134-153.
76. Topol, Eric. Deep medicine: how artificial intelligence can make healthcare human again. Hachette UK, 2019.
77. UN Global Compact. Uniting Business in the Decade of Action.2020.
78. Vaccaro, Antonino, and Peter Madsen. "Corporate dynamic transparency: the new ICT-driven ethics?." Ethics and information technology 11 (2009): 113-122.
79. van Dijck, Jose. "The platform society: Public values in a connective world." (2018).
80. van Dijk, J. A. G. M. The digital divide. Polity Press, 2020.
81. Veale, M., & Zuiderveen Borgesius, F. Demystifying the draft EU Artificial Intelligence Act. Computer Law & Security Review, 42. 2021, P. 1.
82. Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." A practical guide, 1st ed., Cham: Springer International Publishing 10, no. 3152676 (2017): 10-5555.
83. Wang, Mansi, Renmiao Yuan, Xin Guan, Zeyu Wang, Yanzhao Zeng, and Tao Liu. "The influence of digital platform on the implementation of corporate social responsibility: from the perspective of environmental science development to explore its potential role in public health." Frontiers in Public Health 12 (2024): 1343546.
84. Werz, Johanna M., Esther Borowski, and Ingrid Isenhardt. "Explainability as a Means for Transparency? Lay Users' Requirements Towards Transparent AI." Cognitive Computing and Internet of Things 124, no. 124 (2024).
85. West, Darrell M. The future of work: Robots, AI, and automation. Brookings Institution Press, 2018.
86. White, Gregory B., and Natalie Sjelin, eds. Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM). IGI Global, 2020.
87. Zaeem, Razieh Nokhbeh, and K. Suzanne Barber. "The effect of the GDPR on privacy policies: Recent progress and future promise." ACM Transactions on Management Information Systems (TMIS) 12, no. 1 (2020).
88. Zhang, Chenglong, Varghese S. Jacob, and Young U. Ryu. "Modeling individual fairness beliefs and its applications." ACM Transactions on Management Information Systems 15, no. 3 (2024).
89. Zuboff, Shoshana. "The age of surveillance capitalism." In Social theory re-wired, Routledge, 2023.
90. Zuboff, Shoshana. "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, edn." PublicAffairs, New York (2019).