المراقبة التكنولوجية والتحكم السيبراني
مآلات الخصوصية في عصر الذكاء الاصطناعي

■ أ. أسماء عبدالحفيظ خميس نوير[1]

ملخّص

تُبَشِّرُ الظاهرةُ التي يُشارُ إليها الآنَ باسم البيانات الضخمة (Big Data) بآمال كبيرة وفرص واعدة؛ باعتبارها مصدرًا محتملًا لإيجاد حلول لعدّة مشكلات مجتمعيّة، مثل الإرهاب (Terrorism)، ولكنْ قدْ ينتهي الأمرُ أيضًا إلى أنْ تُصبحَ مظهرًا مُؤرقًا، ما يُتيحُ انتهاكَ الخصوصيّة وتقليصَ الحُريّات المدنيّة وزيادةَ سيطرة الدولة والشركات. بناءً على ذلك، تُعَدُّ الخصوصيّةُ من أكثر المفاهيم عُرضَةً للتغيّر في عصر الذكاء الاصطناعي؛ حيثُ لمْ تَعُدْ "المُراقبةُ" مجرّدَ أداة تُستخدمُ في حالات استثنائيّة، مثلَ الأزماتَ أو حالات الطوارئ، بلْ أصبحتْ عنصرًا رئيسًا في حياتنا اليوميّة. لقد اتَّسعَ المفهومُ ليشملَ "المُراقبةَ التكنولوجيّةَ" و"التحكُّمَ السيبرانيَّ"، وهي أشكالٌ دقيقةٌ من المُراقبة تعتمدُ على إعادة تشكيل السلوك والاختيارات من خلال الخوارزميّات. تُحاولُ الدراسةُ الإجابةَ عن كثير من التساؤلات المطروحة، مثل: كيفَ تُؤثّرُ أنظمةُ المُراقبة التكنولوجيّة والتحكُّم السيبرانيِّ على مفهوميْ الخصوصيّة والحُريّة في عصر الذكاء الاصطناعي؟ وهلْ يمكنُنا تطويرُ نماذجَ بديلة تُعزّزُ العدالةَ التكنولوجيّةَ؟

كما تعتمدُ الدراسةُ على المنهج التحليليِّ النقديِّ، وتُظهرُ النتائجُ الأوليّةُ أنَّ الخصوصيّةَ لمْ تَعُدْ حقًّا يُنتَهَكُ، بلْ أصبحتْ بنيةً تُصاغُ من الداخل، من خلال تقنيّات تُمارسُ "سلطةً ناعمةً" تُؤثّرُ على وعي الأفراد وسلوكياتهم.

الكلمات المفتاحية: الخصوصيّةُ الرقميّةُ، المُراقبةُ التكنولوجيّةُ، التحكُّمُ السيبرانيُّ، السيادةُ الخوارزميّةُ، العدالةُ التكنولوجيّةُ.

---

١ - باحثة دكتوراه في فلسفة العلوم بكلية الآداب، جامعة أسيوط بجمهورية مصر العربية، تخصص دقيق فلسفة الذكاء الاصطناعي وتكنولوجيا الروبوتات.

مقدمة

لقـد أتاحَت التكنولوجيا فرصًـا جديدةً هائلةً لمُقدِّمي المعلوماتِ ومُسـتخدميها على حدٍّ سواءٍ. فكلُّ مُنظَّمةٍ تمتلكُ مواردَ حاسوبيّةً هائلةً لمعالجةِ أنشطتِها الوظيفيّةِ المتعدِّدةِ. وبفضلِ ثـورةِ التكنولوجيا الرقميّةِ، أصبحتِ المعلوماتُ أكثرَ ديمومةً ومرونـةً وقابليّةً للتنقُّلِ. ويمكنُ تجميعُ أو إعادةُ دمجِ أجزاءِ المعلوماتِ بسـهولةٍ لإنشـاءِ ملفاتٍ تعريفيّةٍ كاشـفةٍ. وفي الوقتِ نفسه، تُتيحُ تقنيّاتُ المُراقبةِ وبنيةُ الإنترنتِ المفتوحةِ تتبُّعًا دقيقًا لحركاتِ الأشخاصِ في الفضاءِ الإلكترونيِّ وفي العالمِ الماديِّ. كما تُوفِّرُ تقنيّاتٌ مثلُ الهواتفِ المحمولةِ فُرصًا واسـعةً لمثلِ هـذهِالمُراقبـةِ.

لـذا، تُضعفُ التكنولوجيا الرقميّةُ الشـبكيّةُ خصوصيّتَنا الفعليّةَ بشـكلٍ ممنهجٍ، وتُقلِّلُ من توقُّعاتنا بشـأنِ مستوى الخصوصيّةِ الذي نشعرُ بأنّنا نستحقُّه. تُبطئُ الخلافاتُ العامّةُ أحيانًا هذا التوجُّهَ الحاسـمَ نحوَ جعلِ كلِّ شـخصٍ شـفافًا قدرَ الإمكانِ، لكنّ حقـوقَ الخصوصيّةِ القويّةَ تبدو غيرَ متوافقةٍ بشـكلٍ متزايدٍ مع هذهِ التقنيّاتِ. ويبرزُ بشكلٍ خاصٍّ التهديدُ الذي تتعرَّضُ لهُ خصوصيّةُ المعلوماتِ، والذي يتضمَّنُ سيطرةَ الشخصِ على تدفُّقِ معلوماتِه الشخصيّةِ.

يُمثِّـلُ الذكاءُ الاصطناعيُّ نقطةَ تحوُّلٍ إلى نظامٍ معرفيٍّ مسـتقلٍّ قادرٍ على التعمُّقِ في البنى الأساسِ للوعيِ البشريِّ وإعادةِ تشكيلِها من الداخلِ، وذلك في إطارِ ما يُعرفُ بنموذجِ «التحكُّمِ السـيبرانيِّ». في هذا السياقِ، لمْ تَعُدِ الخصوصيّةُ حقًّا فرديًّا فحسب، بلْ أصبحتْ ساحةً لصراعٍ مُعقَّـدٍ بين الأنظمـةِ التقنيّةِ والهويّاتِ الرقميّةِ والبنى السياسـيّةِ التي تُعيـدُ تعريفَ الحدودِ بين العامِّ والخاصِّ. لقد أصبحتِ القضايا المتعلِّقـةُ بالخصوصيّةِ تمسُّ جوهرَ التوازنِ بين الحريّةِ والمُراقبـةِ، وبين الأمـنِ والانتهاكِ، وبين ما يُصرَّحُ بهِ طوعًا وما يُسـتخلصُ ضمنيًّا نتيجةَ التتبُّعِ الخفيِّ.

أولًا: تحولات الخصوصية في العصر الرقمي

تُعدُّ الخصوصيّةُ وحمايةُ البياناتِ من أبرزِ الجوانبِ التي تشــهدُ تغيُّراتٍ جوهريّةً نتيجةَ هذا التطوُّرِ التكنولوجيِّ؛ إذ يفرضُ كلُّ تطوّرٍ تكنولوجيٍّ تأثيرَه على طبيعةِ حياةِ الإنســانِ وقيمه، إلى الحدِّ الذي قد يؤدي إلى تغيّرِ ما كان يُعدُّ ثابتًا ومستقرًّا في حياتهم، خاصّةً إذا استمرَّ هذا الثباتُ لفترةٍ طويلة، ما يولِّدُ شعورَ الاعتيادِ والاعتقادِ بأنّه أصلٌ ثابتٌ لا يقبلُ التغيير[١].

تتباينُ الآراءُ وتختلفُ في وضعِ تعريفٍ جامعٍ مانعٍ للخصوصيّة، فنجدُ معانٍ متعددةً تعكسُ تحديــاتٍ كبيرةً في تحقيقِهــا، خاصّةً في ظلِّ التطــوّراتِ التكنولوجيّةِ والاعتــمادِ على البياناتِ الضخمةِ في العصرِ الحاليِّ، من بينِ هذه المعاني[٢]:

- الحقُّ في وضعِ حدودٍ للتدخّلِ في الذاتِ، أي القدرةُ على حمايةِ النفسِ من أيِّ تدخّلٍ غيرِ مرغوبٍ فيه.
- الحقُّ في السريّة، الذي يشيرُ إلى حقِّ الفردِ في التحفّظِ على بعضِ الأمورِ عن الآخرين.
- الحقُّ في التحكمِ في المعلوماتِ الشــخصيّة، ويعني قدرةَ الشخصِ على التحكمِ في البياناتِ التي يعرفُها الآخرونَ عنه.

تميّــزَ أيضًــا (جوديــث ديكــو- Judith DeCew)، في مقالِها في موســوعةِ ســتانفورد حول "الخصوصيّة" بين أربعةِ حقوقِ خصوصيّةٍ على النحوِ الآتي: [٣]

١. التطفّلُ على عزلةِ الشخصِ أو انفرادِه، أو في شؤونِه الخاصة.
٢. الكشفُ العلنيُّ عن حقائقَ خاصةٍ محرجةٍ عن الفردِ.
٣. الدعايةُ التي تضعُ الشخصَ في ضوءٍ زائفٍ في نظرِ الجمهور.
٤. الاستيلاءُ على صورةِ الشخصِ لصالحِ شخصٍ آخرَ.

وفقًا لـ (هيلين نيسينباوم - Helen Nissenbaum)، من المستحيلِ تعريفُ الخصوصيّةِ بشكلٍ مجردٍ أو في ســياقِ الفردِ البحتِ. ولكن يجب تعريفُها على أنّهــا التحكمُ في تدفّقِ المعلوماتِ

---

١ - بهاء درويش: أخلاقيات العلم والتكنولوجيا وتطبيقاتها في الواقع المعاصر، ص١٠٠.

٢ - وائل أحمد عبد الله صبره: التحديات الأخلاقية التي تواجه العلم والتكنولوجيا في عصر البيانات الضخمة، ص٥٨١.

3 - Sherali Zeadally and Mohamad Badra ,Privacy in a Digital, Networked World: Technologies, Implications and Solutions, p.293.

في سـياقاتٍ اجتماعيةٍ تقنيـةٍ معيّنة. نقترحُ في هذه الورقة البحثيّة ضرورةَ التمييز بين السـياقات المختلفة من حيثُ مدى ارتباطها بالذات والعوامل الاجتماعية المؤسسية التي قد تؤثّرُ عليها أو تشوّهها، وذلك لأسبابٍ عمليةٍ ولإظهار التطوّر التاريخيِّ لمفهوم الخصوصيّة.

في ضـوءِ هذا التوضيـحِ لمفهوم الخصوصيّة، يمكننا ملاحظةُ أنّهـا تنطوي على علاقةٍ بين عدة أشـخاصٍ أو فاعلين، سـواء أكانوا أفـرادًا أم شركاتٍ تنظيمية. ومـن الناحية الاصطلاحيّة، للخصوصيّة (مدلولاً سـلبيًّا - Negative Sense)، فهي مشتقةٌ من كلمة (Privo) اللاتينية تعني السـلبَ أو الإفسادَ أو نزعَ السريّة عن شخصٍ ما. وبهذا المعنى، تصبحُ الخصوصيّةُ موضوعيّةً؛ لأنَّ أحدَ الفاعلينَ لديه مصلحةٌ في شيءٍ ما يكون لدى وكيلٍ آخرَ مصلحةٌ في حجبه عنه. مضافًا إلى ذلـك، يمكن تعريفُ الخصوصيّة أيضًـا بوصفها حقًّا للفردِ في عدمِ سـلبِ شيءٍ ما يملكهُ الفردُ بحقٍّ[1].

يُعـدُّ التحدّي المتمثّلُ في التوفيق بين الخصوصيّة واسـتخدام تقنيـات الذكاء الاصطناعيِّ أمرًا بالغَ الأهميّة. لذا، يجب التعاملُ بحذرٍ مع التقنيات القائمة على الذكاء الاصطناعيِّ، خاصّةً عندما يتعلّقُ الأمرُ بالخصوصيّة التي قد يتنازلُ الأفرادُ عنها عند اسـتخدام التكنولوجيا الحديثة. فأنظمةُ الذكاء الاصطناعيِّ، خاصّةً تطبيقاتُ تعلّم الآلة، تعتمد بشـكلٍ كبيرٍ على جمع البيانات ومعالجتها ومشاركتها، غالبًا دون علم المستخدمينَ أو موافقتهم الكليّة[2].

تمثّلُ الخصوصيّةُ أمرًا ضروريًا لأنّها تحمينا من الأذى، وتمنحنا الاحترامَ ككائناتٍ مسـتقلة تسعى إلى السيطرة على حياتها وحماية مساحتها الشخصيّة وكرامتها. وهذا يُبرزُ دورَ الخصوصيّة في تعزيز الاستقلاليّة الشـخصيّة. ومع ذلك، غالبًا ما تُعدُّ تكنولوجيا المعلومات تهديدًا مباشرًا للخصوصيّـة؛ حيث تثيرُ الروبوتاتُ المزوّدةَ بأجهزة استشـعار وكاميرات مخاوفَ جديّةً بشـأن انتهاك الخصوصيّة وجمع البيانات الشخصيّة دون إذن أو إساءة استخدامها[3].

عـلى وجه الخصوص، تمثّلُ الروبوتاتُ الشـخصيّةُ خطرًا إضافيًـا؛ حيث يمكنُ أن تتحوّل

1 - Michael Steinmann et al., «Embedding Privacy and Ethical Values in Big Data Technology», pp. 277–301.

2 - Ilse Oosterlaken , The Capability Approach, Technology and Design, p.82.

3 - Bernd Carsten Stahl, Ethics of Artificial Intelligence: Case Studies and Options for Addressing Ethical Challenges, p.39.

إلى أدوات تدعم ما يُعرف بـ رأسمالية المراقبة (Surveillance Capitalism) الذي عبّرت عنها الخبيرةُ الاقتصاديةُ (شوشانا زوبوف-Shoshana Zuboff)، وهو نموذجٌ جديدٌ من القمع الاجتماعي والاقتصادي يعتمدُ على مراقبة المستخدمين. في هذا السياق، تُجمعُ بياناتُ الأفراد وتُباعُ لتحقيق أرباح، ما يشكل تهديدًا كبيرًا لاستقلاليتهم وخصوصيّتهم، ويضع ضرورةً مُلحةً لمعالجة هذه التحديات الخُلُقيّة بشكل فعّال[1].

إذن ما هي البيانات التي يجمعُها الروبوتُ؟ وكيف يجري تخزينُها؟ وما المخاطرُ المحتملةُ لانتهاك البيانات أو الوصول غير المصرَّح به؟

تُثيرُ الروبوتاتُ المزوّدةَ بالميكروفونات والكاميرات قلقًا بشأن الخصوصية؛ حيث يمكنُها تسجيلُ الصوت والفيديو أثناءَ تفاعلها مع المستخدمينَ. تُعرَّضُ هذه التسجيلاتُ الخصوصيةَ للخطر إذا جرى تخزينُها أو الوصولُ إليها أو مشاركتُها دونَ موافقة المستخدم. مضافًا إلى ذلكَ، قد تخزنُ الروبوتاتُ بياناتٍ شخصيةً مثلَ الأسماء، وتعبيرات الوجه، والأصوات، والمحادثات، والتفضيلات، سواءً في ذاكرتها الداخلية أم في قواعد بيانات متصلة بالإنترنت. في حال عدم تأمين هذه البيانات بشكل كاف، تصبحُ عرضةً للاختراق أو الوصول غير المصرَّح به، ما يسلّطُ الضوءَ على ضرورة وضع أنظمة صارمة لحماية البيانات وضمان استخدام آمن[2].

نجدُ على سبيل المثال، الروبوتات الاجتماعية التي لديها القدرةُ على مراقبة سلوك المستخدمينَ وحركاتهم وتفاعلاتهم بمرور الوقت، بهدف التعلُّم وتكييف استجاباتها وفقًا للبيانات المجمعة. ومع ذلكَ، تثيرُ هذه المراقبةُ المستمرةُ مخاوفَ جديةً بشأن الخصوصية، مثلَ المراقبة التدخلية واحتمال إساءة استخدام البيانات أو تصنيفها بطرق غير مشروعة. غالبًا ما تتصلُ هذه الروبوتاتُ بخوادمَ خارجية أو خدمات سحابية لمعالجة البيانات أو تحديث البرامج أو الوصول إلى معلومات إضافية، ما يزيدُ من خطر انتهاك الخصوصية، خاصّةً إذا لم تُتخذْ تدابيرُ صارمةٌ لحماية البيانات[3].

1 - Tulika Singh, AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy, pp. 703-704.

2 - Oliver Korn, Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction, p.206.

3 -Ibid, p.209.

مضافًا إلى ذلكَ، قد لا يكونُ المستخدمونَ دائمًا على درايةٍ بجمعِ البياناتِ أو الأغراضِ التي تُستخدمُ من أجلها معلوماتُهم الشخصيةُ، ما يُضعفُ استقلاليتهم وسيطرتهم على بياناتهم. من هنا، يُعدُّ استخدامُ الروبوتاتِ الشخصيةِ على أنّهم مساعدين منزليينَ مصدرًا متزايدًا للقلق؛ حيث تعرضُ الأفرادَ لشكلٍ من أشكالِ المراقبةِ، فضلاً عن التهديداتِ المحتملةِ التي قد تشكّلها على الخصوصيةِ، ما يتطلّبُ المزيدَ من التدقيقِ والضوابطِ لضمانِ الاستخدامِ الخُلُقيّ والمسؤولِ لها.

على سبيلِ المثالِ، يمكنُ الإشارةُ إلى الروبوتِ «جيبو» (Jibo)، الذي طورته الباحثةُ الأمريكيةُ (سينثيا بريزيل- Cynthia Breazeal)، وهي واحدةٌ من أبرزِ روادِ مجالِ الروبوتاتِ الاجتماعيةِ.

يُعدُّ "جيبو" أولَ روبوتٍ اجتماعيٍّ مخصصٍ للاستخدامِ المنزليِّ في العالمِ. يتميّزُ هذا الروبوتُ الصغيرُ بقدرتهِ على التفاعلِ مع بيئتهِ باستخدامِ حواسٍ شبيهةٍ بالسمعِ والبصرِ واللمسِ، ما يتيحُ له التفاعلَ مع البشرِ بشكلٍ طبيعيٍّ ومساعدةَ الأسرةِ في إنجازِ مجموعةٍ متنوعةٍ من المهامِّ. من بينِ وظائفهِ تشغيلُ الموسيقى والقصصِ الصوتيةِ، فضلاً عن تذكيرِ المستخدمينَ بالمواعيدِ والمهامِّ، مما يجعلهُ أشبهَ بفردٍ من أفرادِ الأسرةِ[1].

«الخصوصية محكومٌ عليها بالفشل». بهذا العنوانِ، وصفتْ مجلةُ الإيكونوميستْ بدقةٍ قبلَ أكثرَ من ٢٠ عامًا تطورًا يُعرفُ بعصرِ ما بعدَ الخصوصيةِ. ولا تفتقرُ الساحةُ إلى الإخفاقاتِ التي تؤكّدُ هذا التحولَ؛ ففي قضيةِ «كامبريدج أناليتيكا»، قامتِ الشركةُ بتحليلٍ غيرِ قانونيٍّ لما يصلُ إلى ٨٧ مليون ملفٍّ شخصيّ لمستخدمي فيسبوك. استخدمت كامبريدج أناليتيكا هذه البياناتِ لإنشاءِ ملفاتٍ تعريفيةٍ استُغلتْ في الحملةِ الانتخابيةِ الأمريكيةِ وفي استفتاءِ خروجِ بريطانيا من الاتحادِ الأوروبي.

في عامِ ٢٠١٣، كشفَ (إدوارد سنودن-Edward Snowden) عن أن وكالةَ الأمنِ القومي الأمريكيةِ (NSA) كانت تراقبُ اتصالاتِ الإنترنت العالميةِ دونَ أي قيودٍ. مضافًا إلى ذلكَ، قامتِ الحكومةُ البريطانيةُ بمراقبةِ سياسيينَ من دولٍ أخرى بشكلٍ منهجيٍّ من خلالِ التجسسِ على رسائلِ البريدِ الإلكتروني وأجهزةِ الكمبيوترِ الخاصةِ بهم خلالَ قمةِ مجموعةِ العشرين.

1 - Mark Coeckelbergh et al, Envisioning Robots in Society – Power, Politics, and Public Space: Proceedings of Robophilosophy, p.12.

لقد أصبحنا معتادينَ على تقاريرَ تتعلقُ بسرقةِ البياناتِ أو الكشـفِ غيرِ المصرَّحِ بها، خاصّةً من قبل شركاتٍ أخرى.

في نهايةِ عام ٢٠١٨، واجهت الشركةُ المصنعةُ للروبوت تحدياتٍ كبيرةً في عمليةِ تسـويقه وبيعه؛ حيث لم تتمكن من تحقيقِ النجـاحِ التجاريِّ المتوقعِ. أدى ذلك إلى اتخاذِ قرارٍ بإغلاقِ خوادمِ الروبوت، ما جعله غيرَ قابلٍ للاسـتخدامِ بشكلٍ فعّالٍ. وفي النهايةِ، اضطرت الشركةُ إلى بيعِ ملكيتِها الفكريةِ لشركةٍ "فينتشر بارتنرز" (Venture Partners) (SQN) لإنهاء نشاطِها المرتبطِ بالروبوت[1].

يترتّـبُ على ذلك الانتقالُ من مفهومِ الخصوصية بوصفـه حقًّا (Privacy as a Right) إلى الخصوصية بوصفها خدمةً (Privacy as a Service)، كما يكشفُ هذا التحولُ عن صعودِ نموذجٍ اقتصاديٍّ خفيٍّ، تندرجُ فيه الخصوصية بوصفها جزءًا من السوق الرقميةِ. مضافًا إلى ذلك، ترتبطُ تحـولاتُ الخصوصية ارتباطًا وثيقًا بتحولِ معنى "الذاتيـة". أي لم تعد الذاتُ في البيئة الرقمية تُعرفُ على أسـاسِ الحريةِ في الاختيارِ، بل وفقًا لمجموعةٍ من الأنماطِ السلوكيةِ التي تستنتجها الخوارزمياتُ من التفاعلاتِ اليومية.

يمكنُ استخدامُ أربعةِ مبادئَ خُلُقيةٍ لتحديدِ المعنى الخُلُقيِّ للخصوصية، وهي[2]:

١. عدمُ الإيذاء: (Nonmaleficence) يشيرُ إلى الضررِ الذي يمكنُ أن يتعرّضَ لهُ فردٌ أو مجموعةٌ من الأفرادِ. وفي سـياقِ البياناتِ الضخمةِ، يجبُ أن يُفهَم "الضرر" على أنه ضررٌ مباشرٌ (جسديٌّ أو نفسيٌّ أو اجتماعيٌّ أو اقتصاديٌّ، وما إلى ذلك) بعد استخدامِ البياناتِ الشخصيةِ.

٢. العدالةُ: (Justice) تشيرُ إلى توزيعِ الفرصِ والحقوقِ والسلعِ بين الأفرادِ أو مجموعاتِ الأفرادِ المستهدفين من أنشطةِ التنقيبِ عن البياناتِ (Data Mining).

٣. الاستقلاليةُ: (Autonomy)تشـيرُ إلى قدرةِ الأفرادِ أو مجموعاتِ الأفرادِ على اتخاذِ القـراراتِ. وفي حـينِ أن مبدأَ اللا ضررِ يصوّرُ الوكلاءَ أشـياء أو أهدافًا لممارسـاتِ

1 - Oliver Korn , Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction, p.208.

2 - Bernd Carsten Stahl et al, ibid, pp.60-63.

التنقيب عن البيانات، فإن مبدأ الاستقلالية يصوّرُهم أشخاصًا.

٤. الثقةُ: (Trust) تشيرُ إلى العلاقة بين مصادر البيانات والوكلاء المهتمين بالتنقيب عن بياناتهم. وهي تشـملُ جميعَ العلاقات، أي الوكلاء في ممارسـاتهم المشتركة بشكلٍ عام.

يتبـيّنُ من ذلك أن تحـولات الخصوصية لا تعكسُ فقط صراعًا بين المسـتخدمينَ من جهة والـشركات أو الحكومات من جهة أخرى، بل تثيرُ أيضًا تسـاؤلات عن إعادة تعريف الإنسـان في البيئـة الرقمية. هل لا يزالُ الفردُ هو من يحدّدُ هويتهُ، أم أنّ مجموعتَه الرقميةَ أصبحت تؤدّي دورًا أكبرَ في تشـكيل هويته ووجوده؟ في هذا السياق، لم تعد الخصوصية مجرد قضية قانونية، بل أصبحت إشكاليةً فلسفيةً وسياسيةً تتداخلُ فيها تقنياتُ الذكاء الاصطناعي مع أعمقِ الأسئلة المتعلقة بالحرية والوجود والكرامة.

ثانيًا: المراقبة التكنولوجية وإعادة برمجة الوعي في البيئة الرقمية

في عالَمنـا الرَّقميِّ، لا خيارَ أمامَنا إلا مشـاركة بياناتنا الشـخصيَّة مـعَ شركات التِّكنولوجيا الكبرى؛ حيث

تسـتخدمُها هذه الشركاتُ لتوجيه وعْينا نحوَها، ما يُتيحُ لهـا جنيَ الأرباح منَ الإعلانات في مجتمعٍ يُسـمَّى «مجتمعَ المراقبة»، نُواجهُ علاقةَ قُـوَّة غير متكافئة معَ هذه الشركات (وأحيانًا معَ الحكومات)، ولا نملكُ سيطرةً تُذكرُ على ما يحدُثُ لبياناتنا.

يتزايـدُ اعتمادُنا على هذه العلاقات غير المتكافئة معَ اسـتخدام شركات التكنولوجيا الكبرى للمعلومات التي تجمعُها عنَّا لتلبية عاداتنا ورغباتنا الشخصيَّة [1].

يُعرفُ هـذا أيضًا بمفهوم «المراقبـة التكنولوجيَّة»، مفـادُه: عمليَّةٌ ترتكزُ عـلى أنظمة الذَّكاء الاصطناعيِّ، وتعلُّم الآلة، وتحليل السلوك.

لا تكتفـي هذه الأنظمـةُ بجمع البيانات، بـل تُعالجُها وفقَ نمـاذجَ خوارزميَّـة متقدِّمة تقومُ بتكوينملفّات شخصيَّة دقيقة للأفراد، تستندُ إلى عاداتهم، وميولهم، وتوقيت تصفُّحهم، وأنماط استجابتهم، واختياراتهم المتكرِّرة.

1 - Roos Slegers. Privacy and Surveillance, p.177.

وبناءً على ذلك، لا يجري تعقُّبُ المستخدم فقط، بل يُعادُ توجيهُ وعْيه تدريجيًّا نحوَ خيارات محدَّدة، واستبعادِ بدائلَ أُخرى من دونِ أنْ يعيَ ذلك؛ حيث تُصبحُ الخوارزميَّاتُ هنا وسيلةً للتحكُّم[1].

يُؤكِّدُ الفيلسوفُ الفرنسيُّ (بيير ليفي- Pierre Lévy) على أنَّ المعرفةَ في العصرِ الرَّقميِّ لم تعُدْ تقتصرُ على الأفراد، بل تُوزَّعُ من خلال أنظمة ذكاء اصطناعيٍّ تمُارسُ نوعًا من "أتمتة الذكاء الجمعيِّ".

يتغيَّرُ الوعيُ تدريجيًّا بفعلِ هذا التوزيعِ ليُعادَ تشكيلُه وفقًا لواجهاتِ منصاتِ التواصُلِ الاجتماعيِّ، لا من خلال إدراكِ الإنسانِ المباشرِ للواقع.

فالمستخدمُ لا يعودُ يرى العالمَ كما هو، بل كما تُريه إيَّاه الخوارزميَّاتُ.

نتيجةً لذلك، تظهرُ ظاهرةٌ مستعصيةٌ تُعرفُ بـ"إعادةِ برمجةِ الوعي"، حيثُ تتداخلُ فيها ثلاثُ قُوى، وهي: السوقُ، والتقنيَّةُ، والسُّلطةُ.

فالمراقبةُ التكنولوجيَّةُ لا تقتصرُ على جمعِ البياناتِ عن الوعي، بل تهدفُ أيضًا إلى تحسينِ هذا الوعي بما يتَّفقُ معَ مصالحِ الشركاتِ أو المنصاتِ.

المثالُ الأبرزُ على ذلك هو التلاعبُ بالمحتوى الإخباريِّ أو الترفيهيِّ، كما في (يوتيوب - YouTube)، و(نتفليكس - Netflix)، و(إنستغرام - Instagram)؛ حيث يُعادُ تشكيلُ إدراكِ المستخدمِ للعالَمِ من خلالِ المحتوى الذي يُقترَحُ عليه باستمرارٍ، بناءً على تفاعلاته السابقة، من خلال عمليَّة "التحيُّز" المدعوم تقنيًّا[2].

لا تُمارَسُ المراقبةُ من خلالِ كاميراتِ الفيديو أو أدواتِ الرصدِ فقط، بل تشملُ الخوارزميَّاتِ التي تتحكَّمُ بشكلٍ مستقلٍّ في مجموعةٍ متنوِّعةٍ منَ المجالاتِ عبرَ الإنترنتِ والمجالاتِ الرقميَّةِ البحتة، مثلَ الروبوتاتِ التي تتحكَّمُ في البرامجِ مفتوحةِ المصدرِ أو المجتمعاتِ عبرَ الإنترنتِ.

ونظرًا لأنَّ المعالجاتِ الرقميَّةَ يُمكنُها اتِّخاذُ قراراتِها الخاصَّةِ بناءً على تحليلِ هذهِ البياناتِ، فإنَّها تتولَّى دورَ المُراقبِ.

1 - Julia van Hee et al., The Surveillance Society: Which Factors Form Public Acceptance of Surveillance Technologies? p.170.

2 - Pradip Kumar Das et al, Privacy and Security Issues in Big Data: An Analytical View on Business Intelligence, p.19.

تشتهرُ شركةُ (أوبر - Uber) بمراقبةِ السائقينَ والتحكُّمِ في الطُّرقِ خوارزميًّا، وتَحلُّ الدفعاتُ الرقميَّةُ بشكلٍ متزايدٍ محلَّ التحكُّمِ العلنيِّ[1].

يُمكنُنا بسهولةٍ تصوُّرُ المواقفِ التي يجري فيها الاستفادةُ منَ المعلوماتِ الجوهريَّةِ للأنشطةِ التوليديَّةِ، وذلكَ في ظلِّ التطوُّراتِ التي طرأتْ على مجالِ الذكاءِ الاصطناعيِّ التوليديِّ.

وبذلك، يُصبحُ منَ الصعبِ على المستخدمينَ إدراكُ أنَّهم تحتَ المراقبةِ معَ تزايدِ ذكاءِ الأنظمةِ.

وقد أشارَ الفيلسوفُ الألمانيُّ (بيونج-تشول هان-Byung-Chul Han) إلى هذا المفهومِ بـ"القوَّةِ النَّاعمةِ الرقميَّةِ"، الذي يُعبِّرُ عن استخدامِ الأدواتِ والتقنيَّاتِ الرقميَّةِ، مثلَ وسائلِ التواصلِ الاجتماعيِّ والمنصاتِ الإلكترونيَّةِ، لتعزيزِ السَّيطرةِ والتأثيرِ على الأفرادِ والدُّولِ والمنظَّماتِ.

وتعتمدُ هذهِ القوَّةُ على الامتثالِ الطوعيِّ أو الإقناعِ بدلاً منَ الإكراهِ لتحقيقِ الأهدافِ المرجوَّةِ[2].

وعليه، لا تستهدفُ هذهِ المراقبةُ الأفرادَ فقط، بل تمتدُّ لتشكيلِ الوعيِ الجمعيِّ، خاصَّةً في أوقاتِ الأزماتِ أو الانتخاباتِ أو النِّزاعاتِ.

كما يُمكنُ لمنصَّاتِ التواصُلِ الاجتماعيِّ من خلالِ تحليلِ الرأيِ العامِّ أنْ تُعيدَ برمجةَ الوعيِ، وفقًا لما تقتضيهِ المصالحُ التجاريَّةُ أو السياسيَّةُ.

وهكذا، تتحوَّلُ المراقبةُ إلى أداةٍ سياديَّةٍ جديدةٍ تُمارسُ الحُكمَ من خلالِ جمعِ بياناتِ الأفرادِ بدلاً منَ القانونِ أو الخطابِ.

في هذا السِّياقِ، تتغيَّرُ طبيعةُ الفردِ في البيئةِ الرقميَّةِ، فلم يَعدْ مجرَّدَ مستخدمٍ حرٍّ، بل أصبحَ مادَّةً تتشكَّلُ وتُدارُ بواسطةِ الخوارزميَّاتِ.

بمعنى آخر، يجري إعادةُ تشكيلِ اختياراتِه وأحكامِه، وحتَّى وعيِه بذاتِه، من خلالِ مجموعةٍ منَ الرموزِ والبياناتِ التي تحملُ في طيَّاتِها توجيهًا سُلطويًّا خفيًّا.

إنَّ فهمَ المراقبةِ التكنولوجيَّةِ بوصفِها عمليَّةً لإعادةِ برمجةِ الوعيِ يدفعُنا إلى تجاوزِ المقارباتِ القانونيَّةِ الضيِّقةِ التي تركِّزُ على الانتهاكاتِ أو التجسُّسِ، نحوَ تحليلٍ أعمقَ يتناولُ الجوانبَ الأنثروبولوجيَّةَ والوجوديَّةَ لهذهِ الظاهرةِ.

---

1 - Sasmita Mohapatra, «Surveillance with Smart Spherical Robot», p.175.

2 - Roos Slegers, Ibid, p.180.

لا تقتصرُ الإشكاليَّةُ على «مَن يقومُ بالمراقبة»، بل تتعلَّقُ بكيفيَّة تشكيلِ الوعي نفسه.
وهذا يُثيرُ سؤالاً جوهريًّا: ما الذي يتبقَّى منْ حرِّيَّة الإنسانِ عندما يُعادُ تشكيلُ وعيه وفقَ منطقٍ لمْ يعرفْه، ولا يتحكَّمْ فيه، ولا يُدركْ حدودَه بدقَّةٍ؟

ثالثًا: السيادة الخوارزمية نحو فهم جديد للهيمنة الرقمية

لقد أدَّت الثورةُ الرقميَّةُ، خاصَّـةً في مجالاتِ الذكاء الاصطناعيِّ وتحليلِ البيانات الضخمة، إلى نشوءِ ما يُطلقُ عليه «بالسيادة الخوارزميَّة»، وهي تُشيرُ إلى قدرة الأنظمة التقنيَّة ـ وليسَ الدُّول أو الأفـراد ـ على اتخاذ قرارات تتعلَّقُ بحياة المسـتخدمينَ، مثلَ ما يُعـرضُ عليهم، وما يُحظَرُ، ومَن يُراقبُ. لم تَعُـد الخوارزميَّاتُ مجرَّدَ أدوات تقنيَّة حياديَّة، بـل أصبحتْ «كيانات تنظيميَّةً» (Regulatory Entities) تُمـارسُ ما يُشـبهُ التشريعَ والتنفيذَ، في غياب الشـفافيَّة والمسـاءلة، كـما نجدُها في البيئات الرقميَّة، مثلَ منصَّات (جوجل - Google)، و(فيسـبوك - Facebook)، و(أمازون - Amazon) [1].

تُعدُّ الخوارزميَّاتُ أشـبهَ بالصندوق الخفيِّ أو الصندوق السـحريِّ الذي يقفُ المستخدمونَ للإنترنت أمامَهُ بينَ الإعجاب الشديد بإمكانيَّات هذا العلم في التنبؤ بالمستقبل، والاتِّهام بالتحكُّم بآرائهم وخياراتهم، كما يَفتقدُ كثيرونَ الوعيَ بدورها الفاعل في توجيه ما يَطلِّعونَ عليه من خلال مواقـع التواصل الاجتماعيِّ ومحـركات البحث. فالخوارزميَّاتُ هي مَن تُحـدِّدُ نوعَ المقالات التي نقرؤُها، والصورَ التي نُشـاهدُها، والإعلانات التي تظهرُ لنا. وبغضِّ النظر عن ذلك، يَبقَى المسـتخدمُ للعالم الافتراضيِّ عاجزًا ومُستسـلمًا لهذه القوى التي تتحكَّمُ في تدفُّق المعلومات وتوجيهها، وتُقرِّرُ ما يتمُّ عرضُهُ وما يتمُّ إخفاؤُهُ [2].

كما يُمكنُ للخوارزميَّات النشطة على وسائل التواصل الاجتماعيِّ أن تُنشرَ معلومات مضلِّلةً. على سبيل المثال، يُمكنُ (للروبوتات السياسيَّة) (political bots) أن تتنكَّرَ باعتبارهم أشخاصًا حقيقيِّينَ، وتُنشرَ محتوىً سياسـيًّا. من الأمثلة على ذلك (تشـات بوت مايكروسـوفت "تاي" -

1 - Bernd Carsten Stahl et al., ibid, p.40.

2 - Georgy Ishmaev, « Sovereignty, privacy, and ethics in blockchain-based identity management systems», pp.239–252.

Microsoft chatbot Tay)، الـذي أُطلقَ في عام ٢٠١٦ لإجـراء محادثات مرحة على (تويتر) (Twitter)، ولكنَّـهُ بدأ في تغريد محتوىً عنصريٍّ بمجرَّد أن أصبحَ أكثرَ ذكاءً. علاوةً على ذلك، يُمكنُ لبعض خوارزميَّات الذكاء الاصطناعيِّ إنشاءُ مقاطع فيديو مزيفة، مثلَ الفيديو الذي جرى تعديلُهُ ليُظهرَ خطابًا للرئيس الأمريكيّ السابق (باراك أوباما- Barack Obama)، ما يعكسُ القدرةَ على التلاعب بالصورة والرسائل[1].

تَرتَّبَ على ذلك، صعـودُ الخوارزميَّات بوصفها قوةً حاكمةً، وأدَّى ذلك إلى ما يُعرَفُ بأنظمة (الصندوق الأسـود) (black-box systems)، أي الأنظمة التي تَفتقـرُ إلى رؤًى عن الآليَّات أو القواعد الداخليَّة وعمليَّات اتخاذ القرار في إدارة البيانات. ويمُكنُ التمييزُ بينَ أربعة أنواع مختلفة منها مـن حيثُ قابليَّة فحص الأنظمة المُعتمة، وذلكَ بنـاءً على المعرفة بمدخلات ومخرجات النظام، وهي[2]:

١. أنظمةُ الصندوق الأسود التي لا يُمكنُ فيها ملاحظةُ إلا الناتج.
٢. أنظمةُ الصندوق الأسـود التي تَتمكَّنُ من ملاحظة بعض المدخلات فقط، والتلاعب بها، على سبيل المثال أثناءَ الاختبار، ولكنْ بعضُ المدخلات غيرُ معروفة ولا يُمكنُ التلاعبُ بها.
٣. أنظمةُ الصندوق الأسود التي يُمكنُ من خلالها ملاحظةُ جميع المدخلات والمخرجات الناتجة.
٤. أنظمةٌ شفافةٌ من حيثُ المبدأ، ولكنَّها معقَّدةٌ للغاية بحيثُ لا يُمكنُ للبشر فهمُها.

يُدلِّلُ على ذلك، الفيلسوفُ الفرنسيُّ (أنطوان فيتكين-(Antoine Vitkine)، عندما أكَّدَ على أنَّ العالمَ يَعيشُ لحظةً خوارزميَّةً تُشكِّلُ فيها الخوارزميَّاتُ السلوكَ السياسيَّ والدينيَّ والثقافيَّ والرأيَ العامَّ، بالرغم من عدم وجود آليَّات فعَّالة تكشـفُ هذا التأثيرَ أو تُقاومُهُ. من الأمثلة البارزة على ذلك، أنظمةُ التصنيف الائتمانيِّ في (الصين)، ومنها نظامُ الائتمان الاجتماعيِّ (Social Credit System)، الذي يَعتَمدُ على الخوارزميَّات في إنشاء شبكة من قواعد بيانات السجلات الإداريَّة، وتصنيف درجات المواطنينَ، مكانتهم في المجتمع، وتحديد مَن يَسـتحقُّ الثقةَ أو العقابَ، بناءً

1 - Julia van Hee et al, Ibid, p.190.

2 - Tobias D. Krafft et al., «Black-Box Testing and Auditing of Bias in ADM Systems», p. 15.

على أفعاله، وشبكات علاقاته، ونشاطه الرقميِّ[1].

يَقودُ هذا الشكلُ من السيادة إلى نشوء «نظام تحكُّم خوارزميٍّ»، تختلفُ آليَّاتُهُ عن النُّظُم السلطويَّة التقليديَّة؛ لأنَّهُ لا يَعتَمِدُ على الإكراه أو العنف، بل على برمجيَّات تُقرِّرُ ما الذي يُعدُّ حقيقيًّا أو جديرًا بالظهور. فحين تُقرِّرُ خوارزميَّاتُ (يوتيوب) (YouTube) أو (تيك توك) (TikTok) أيَّ محتوى يُعرَضُ أوَّلًا، أو حين تُصنَّفُ نتائجُ البحث في (جوجل) (Google)، فإنَّها لا تَعرِضُ الواقعَ، بل تُعيدُ صياغتَهُ وفقًا لمصالح تجاريَّة أو أيديولوجيَّة غالبًا ما تكونُ غيرَ مُعلَنة.

نَستنتجُ ما سبقَ ذكرُه، إنَّ السيادةَ الخوارزميَّةَ لا تُطبَّقُ فقط على مستوى الأفراد، بل على مستوى البنى السياسيَّة ذاتها. فقد تَعتَمِدُ بعضُ الحُكومات والدُّول على أدوات تحليل البيانات الضخمة (Big Data Analytics) وأنظمة الذكاء الاصطناعيِّ في إدارة شؤونها، ما يجعلُها خاضعةً جزئيًّا لسلطة الشركات التكنولوجيَّة الكبرى. يُعرَفُ هذا بـ "الاستعمار الرقميِّ الجديد" (New Digital Colonialism)؛ حيث تُمارِسُ شركاتُ تكنولوجيا المعلومات سلطةً تتجاوزُ الحدودَ القوميَّةَ، وتُعيدُ رسمَ الخرائطِ السياديَّة وفقَ منطق السوق لا السياسة.

رابعًا: الأمن السيبراني، استراتيجيات التحكّم عبر سياسات الأمان في الأنظمة الذكية.

يُعَدُّ مفهومُ الأمن السيبرانيِّ(Cybersecurity) آليةً للحماية والتحكُّم، وأداةً لتنظيم العلاقات بينَ الدولة والمواطن والتكنولوجيا. فهو لم يَعُدْ مجردَ سياسة تقنية تهدفُ إلى حماية الأنظمة منَ الاختراقات، بل أصبحَ بنيةً رقميةً معقدةً للهيمنة تُدارُ من خلال سياسات الأمان فيما يُعرفُ بالأنظمة الذكية (Smart Systems). في هذا السياق، ترتبطُ المراقبةُ بالحماية، ويجري إعادةُ تفسير المخاطر وفقَ منطق خوارزميٍّ يتجاوزُ التحكُّمَ البشريَّ[2].

يشملُ الأمنُ السيبرانيُّ تقنياتٍ لحماية الأنظمة والشبكات والأجهزة والبرامج والبيانات

1 - Elena Consiglio and Giovanni Sartor, «A New Form of Socio-technical Control: The Case of China's Social Credit System», p.131.

2 - Hamid Jahankhani, Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, p.241.

الإلكترونيــة والتحكُّم فيها منَ الوصول غير المصرح بــه. ويُعَدُّ تطويرُ آلية دفاعية فعالة ومبتكرة مطلبًــا مُلحًّا؛ إذ أصبحــتْ حلولُ الأمن الســيبرانيِّ التقليديةُ غيرَ كافية لحمايــة المعلومات منَ التهديدات الإلكترونية. وهناكَ حاجةٌ إلى أســاليبَ أمن ســيبرانيٍّ قادرة عــلى اتخاذ قرارات آنية والاستجابة للهجمات الإلكترونية[٣].

بنــاءً على ذلك، أصبحــت المنظماتُ تعتمدُ على تقنيــات الذكاء الاصطناعــيِّ؛ لأنها تُؤدِّي دورًا فعالاً في مكافحة الجرائم الإلكترونية، مع تحسُّــن كبير في كشــف التســلُّل غير الطبيعيِّ. فهي تقنيةٌ يمكنُها تحليلُ ملايين البيانات لتتبُّع التهديدات الإلكترونية ومنع انتهاكات البيانات. وقد اســتُخدمتْ أيضًا في مجالات تطبيقية مثلَ التصنيع، والرعاية الصحية، والتعليم، والزراعة، والأمن السيبرانيِّ. كما تستطيعُ خوارزمياتُ الذكاء الاصطناعيِّ التنبؤَ بالهجمات التي شوهدتْ ســابقًا وغير المرئية، وقد أثبتتْ فعاليتَها في اكتشاف الهجمات السيبرانية بمعدل إنذارات كاذبة منخفض.

سُرعانَ ما أصبحَ الذكاءُ الاصطناعيُّ أداةً لأتمتة اكتشــاف التهديدات والاســتجابة لها بشكلٍ فعّال، مقارنةً بالطرق التقليدية التي يقودُها الإنســانُ والتي لا تستطيعُ مواكبةَ أحجام الفيروسات التي يجري إنشــاؤها يوميًّا. يُؤدِّي الذكاءُ الاصطناعيُّ دورًا فعالاً في كشف التهديدات، وكشف التســلُّل، والاحتيال، والأمن الســيبرانيِّ، ما يزيدُ من دقة الاستجابة السيبرانية وسرعتها. وتشملُ التخصصاتُ الرئيســةُ في الذكاء الاصطناعيِّ معالجةَ اللغــات الطبيعية، والتعلُّمَ العميقَ، وتعلُّمَ الآلة، والروبوتات، والرؤيةَ الحاسوبيةَ[٤].

تتضمَّنُ تقنياتُ الذكاء الاصطناعيِّ الهجوميةُ مجموعةً متنوعةً منَ الأساليب التي يستخدمُها المهاجمــونَ لاســتغلال نقاط ضعــف الشــبكات والتهرُّب من أنظمة الكشــف، ما يُعــزّزُ تأثيرَ الهجمات الإلكترونية. تشــملُ هذه الممارســات البُنى التحتيةَ للقرصنــة الذاتية، والتعلُّمَ الآليَّ العدائيَّ، والتطبيقات الخبيثةَ المدعومةَ بالذكاء الاصطناعيِّ. على ســبيل المثال، تســتخدمُ أطرُ القرصنة الذاتية التشغيلَ خوارزمياتِ الذكاء الاصطناعيِّ لتحديد نقاط ضعف البرامج ومتابعتها

3 - Ibid, p.246.

4 - Tuomo Sipola et al, Artificial Intelligence for Security: Enhancing Protection in a Changing World, p.31.

على نطاقٍ واسـعٍ، بينما تُسـتخدمُ تقنياتُ التعلُّمِ الآليِّ العدائيِّ لإنتـاجِ بياناتٍ مضللةٍ يمكنُ أنْ تكشفَ عن أنظمةِ الأمانِ المعتمدةِ على الذكاءِ الاصطناعيِّ[1].

علاوةً على ذلك، تدمجُ البرمجيَّاتُ الضَّارةُ المدعومةُ بالذكاءِ الاصطناعيِّ تقنياتِ التعلُّمِ الآليِّ لتفادي أنظمةِ الكشفِ التقليديةِ والتكيُّفِ مع تدابيرِ الحمايةِ التي تعتمدُها الجهاتُ المستهدفةُ. من بينِ أطـرِ القرصنةِ التي تعتمدُ على الذكاءِ الاصطناعيِّ، نجـدُ (ديب لوكر - DeepLocker) الذي يستخدمُ التعلُّمَ العميقَ لإخفاءِ الحمولاتِ الضارةِ، و(أوتو سبلوت) (AutoSploit)، وهي أداةٌ آليةٌ تُحدِّدُ نقاطَ الضعفِ وتسـتغلُّها بشـكلٍ مسـتقلٍّ. كما يقومُ (ديب فِش) (DeepPhish) بإنشاءِ هجماتٍ مخصصةٍ للغايةِ ومقنعةٍ. تُوضِّحُ هذه الأطرُ كيفَ يمكنُ للذكاءِ الاصطناعيِّ تعزيزُ قدراتِ المجرمينَ الإلكترونيينَ من خلالِ أتمتةِ وتحسينِ أساليبِ الاستغلالِ[2].

تتضحُ هذه التحولاتُ في سياسـاتِ تصميمِ منصاتٍ رقميةٍ آمنةٍ، تُبنى على أسـاسِ مجموعةٍ منْ فرضياتِ التهديدِ، وتعملُ على تقييدِ حريةِ التنقُّلِ الرقميِّ، وتفرضُ على المسـتخدمِ شروطَ وصولٍ صارمةٍ، تُحدِّدُ سلوكَه ضمنَ بيئةٍ مقيَّدةٍ أمنيًّا، دونَ أنْ يكونَ واعيًا بذلك. وعليه، فإنَّ الأمنَ السيبرانيَّ هنا لا يحمي منَ الهجماتِ فقط؛ بل يُحدِّدُ المسموحَ والممنوعَ.

يشيرُ الفيلسوفُ الفرنسيُّ (إريك سادين-Éric Sadin) إلى مفهومِ "الأمنِ بوصفِه إيديولوجيا" (Security as Ideology)، مؤكدًا أنَّ مصطلحاتِ الأمانِ والحمايةِ تُسـتخدمُ لتبريرِ توسُّعِ نطاقِ التدخلِ التكنولوجيِّ في الحياةِ الشخصيةِ. يجري ذلك من خلالِ أنظمةٍ تتدخلُ في المراسلاتِ، والمواقعِ، وأنماطِ الشراءِ، والسلوكِ اليوميِّ، تحتَ شعارِ "حمايةِ المواطنِ منَ الخطرِ". ومعَ ذلك، لا يُمنحُ المواطنُ حقَّ المعرفةِ أو المساءلةِ، بل يُطلَبُ منهُ الثقةُ بأنَّ "الأنظمةَ تعرفُ أفضلَ"[3].

يتقاطـعُ مفهـومُ الأمنِ السـيبرانيِّ مع مفهـومِ السـيادةِ الرقميـةِ (Digital Sovereignty)؛ حيثُ تسـعى الدولُ إلى حمايةِ بياناتِها والتحكُّمِ في بنيتِها التحتيـةِ الرقميةِ، مع تجنُّبِ الاعتمادِ

1 - Thammisetty Swetha et al, «Leveraging AI for enhanced cybersecurity: a comprehensive review», p.8.

2 - Nachaat Mohamed, «Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms», p.5.

3 - Kodi A. Cochran, Cybersecurity Essentials: Practical Tools for Today›s Digital Defenders, p.135.

التكنولوجيِّ على الآخرين. ومعَ ذلك، قد يتحولُ هذا السباقُ نحوَ الأمنِ إلى سباقٍ نحوَ المركزية، ما يُؤدِّي إلى توسيعِ صلاحياتِ الرقابةِ وتقييدِ الفضاءِ الرقميِّ تحتَ ذريعةِ الحمايةِ منَ التهديداتِ السيبرانية. وهكذا، تظهرُ مفارقةٌ: كلما زادتْ سياساتُ الأمانِ، زادتْ احتمالاتُ تقييدِ الحرياتِ.

يُجادلُ الفيلسوفُ الإيطاليُّ (لوتشيانو فلوريدي- Luciano Floridi) بأنَّ السيادةَ الرقميةَ تُطبَّقُ بفعاليةٍ أكبرَ على مستوى الاتحادِ الأوروبيِّ، ممتدةً إلى سيادةِ الذكاءِ الاصطناعيِّ وشبكاتِ الجيلِ الخامسِ، مُغطيةً جوانبَ مختلفةً منَ التقنياتِ الأوروبية. يُكمِّلُ هذا النهجُ السيادةَ الوطنيةَ من خلالِ إنشاءِ إطارِ عملٍ فوقَ وطنيٍّ، يُتيحُ التناغمَ والتكاملَ، ويُوازنُ الشركاتِ متعددةَ الجنسيات. تظلُّ السيادةُ الشعبيةُ المصدرَ النهائيَّ للشرعية، لكنْ توَسُّعَها لدعمِ السيادةِ فوقَ الوطنيةِ يتطلَّبُ آلياتٍ مبتكرةً[1].

تنبعُ السيادةُ الرقميةُ، في نقاشِ الجهاتِ الفاعلةِ الحكومية، من منظورِ الولايةِ القضائيةِ للدولة، مقترنةً بأفكارِ الدولِ التي تحمي استقلاليتَها الاستراتيجيةَ معَ مراعاةِ نفوذِ الدولِ الأخرى والشركاتِ الخاصة. في حالةِ الشعوبِ الأصلية، تنبعُ السيادةُ الرقميةُ من حقِّ الشعوبِ الأصليةِ الأساسِ في تقريرِ المصيرِ في التعاملِ معَ المعلوماتِ المتعلقةِ بهم وبأراضيهم.

كما تُشدِّدُ السيادةُ الرقميةُ على حوكمةٍ وطنيةٍ أو فوقَ وطنيةٍ للبيانات، بينما تُقدِّمُ سيادةُ البياناتِ للشعوبِ الأصليةِ مطالباتِها بإدارةِ جمعِ البياناتِ والوصولِ إليها واستخدامِها لضمانِ توافقِها معَ قيمِها وهياكلِ الحوكمةِ ومبادئِها ونماذجِها؛ ما يمنحُ الشعوبَ الأصليةَ حقَّ تقريرِ المصيرِ في الفضاءِ الإلكترونيِّ[2].

لذلك، تتجاوزُ سياساتُ الأمنِ في الأنظمةِ الذكيةِ مجردَ حمايةِ الكودِ البرمجيِّ؛ إذْ تتعلقُ أيضًا بإعادةِ تشكيلِ السلوكِ البشريِّ. فعلى سبيلِ المثال، عندما تُحذِّرُ الهواتفُ الذكيةُ المستخدمينَ منْ «مواقعَ غيرِ آمنة» أو تمنعُ تحميلَ تطبيقاتٍ «مشبوهة»، فإنَّها تتولى دورَ الحارسِ الخفيِّ الذي يتخذُ قراراتٍ بدلاً منَ الإنسان. وغالبًا لا يجري مناقشةُ هذا النوعِ منَ التحكُّمِ المُقنَّعِ؛ لأنه يُعرَضُ

1 - Jason Edwards, Mastering Cybersecurity: Strategies, Technologies, and Best Practices, p.19.

2 - Huw Roberts et al, «Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance», p.51.

باعتباره خدمةً بدلاً من كونه سلطةً.

ومنْ أخطرِ مظاهرِ هذا الاتجاه هو أنَّ الأمنَ أصبحَ يُعَدُّ سلعةً تُباعُ وتُشترى. فشركاتُ الأمنِ السيبرانيِّ العالميةِ لا تُقدِّمُ منتجاتٍ فحسب، بل تبيعُ أيضًا شعورَ الطمأنينة، وتبني سرديات الخوفِ والتهديدِ لترويجِ أدواتها. مضافًا إلى ذلك، ترتبطُ بعضُ هذه الشركاتِ بعقودٍ مع الحكوماتِ تمنحُها سلطاتٍ واسعةً على البياناتِ والمراقبة، ما يُعيدُ إنتاجَ موازينِ قوةٍ غيرِ متكافئةٍ تحتَ مظلةِ الشراكة[1].

يمكنُنا أنْ نستنتجَ ممّا سبقَ أنَّ استراتيجياتِ التحكُّمِ في الأمنِ السيبرانيِّ، من خلالِ السياساتِ الأمنيةِ المعتمدةِ في الأنظمةِ الذكية، ليستْ مجردَ أدواتٍ تقنيةٍ محايدة، بل تعكسُ بشكلٍ مباشرٍ فلسفاتِ حوكمةِ المعلوماتِ وتوزيعِ السلطةِ في البيئاتِ الرقمية. وعلى الرغمِ منَ الإمكانياتِ الهائلةِ التي توفِّرُها هذه السياساتُ في مجالاتِ المراقبةِ والأمانِ والتحكُّم، فإنها تُثيرُ تحدياتٍ خُلُقيةً تتعلَّقُ بمفهومِ الخصوصيةِ وحدودِها، وإمكانيةِ التلاعبِ بأنظمةِ اتخاذِ القرارِ الذكيِّ.

تظهرُ الحاجةُ الملحَّةُ لإعادةِ تقويمِ هذه الاستراتيجيات، ليس فقط باعتبارها وسائلَ للحماية؛ بل أنظمةً تُعيدُ تشكيلَ العلاقةِ بينَ الإنسانِ والتكنولوجيا، وتطرحُ من جديدٍ مسألةَ السيادةِ الفرديةِ والجماعيةِ في ظلِّ هيمنةِ الخوارزميات. لا يمكنُ لأيِّ رؤيةٍ مستقبليةٍ للأمنِ السيبرانيِّ أنْ تكتملَ دونَ اتباعِ مقاربةٍ نقديةٍ تُوازنُ بينَ الكفاءةِ التقنيةِ والاعتباراتِ الحقوقية، وتُعزِّزُ من أهميةِ الشفافيةِ والمساءلةِ في تصميمِ وتشغيلِ الأنظمةِ الذكية.

خامسًا: العدالة التكنولوجية والحق في الحرية الرقمية

نحو نموذج بديل للحوكمة الخوارزمية

تُعَدُّ مسألةُ العدالةِ التكنولوجيَّةِ (Technological Justice) من أكثرِ القضايا تعقيدًا وإلحاحًا، خاصَّةً في ظلِّ استخدامِ الذكاءِ الاصطناعيِّ وهيمنةِ الحوكمةِ الخوارزميَّة (Algorithmic Governance) على مختلفِ جوانبِ الحياةِ العامَّةِ والخاصَّة. لم يَعُدِ السؤالُ المطروحُ هو كيفيَّةَ استخدامِ التكنولوجيا، بل لِمَنْ تُصمَّم، وما المعاييرُ التي تُنظَّمُ بها، ومَنْ همُ المستفيدونَ والمتُضرِّرونَ من نتائجها. في هذهِ المرحلةِ، يجري إعادةُ صياغةِ مفاهيمِ العدالةِ والمواطنةِ

1 - Jason Edwards, Ibid, p.22.

والحرِّيَّة وفقَ أنماطٍ جديدةٍ من السلطةِ والإقصاءِ، التي تتغلغلُ في البنى الخفيَّةِ للقرارِ والتحكُّمِ والمعرفةِ[1].

مع ذلكَ، أَعربَ بعضُ العلماءِ عن مخاوفِهم بشـأنِ استخدامِ الذكاءِ الاصطناعيِّ في مجالِ العدالةِ. وبالتالي، فإنَّ اسـتخدامَهُ يقتضي ضمانَ الوصولِ إلى البياناتِ الحسَّاسـةِ، بما في ذلكَ البياناتِ الشخصيَّةِ. في الوقتِ ذاته، لا يستطيعُ أيُّ نظامٍ اليومَ ضمانَ أمنِ البياناتِ عند استخدامِ تقنياتِ الذكاءِ الاصطناعيِّ. ويُقترحُ أيضًا أنَّ اتخاذَ قرارٍ يعتمدُ فقط على تقييمٍ خوارزميٍّ للظروفِ والأدلَّةِ سـيؤدِّي إلى انتهاكِ الحقوقِ الدسـتوريَّةِ للمواطنينَ في محاكمةٍ عادلـةٍ. ومع ذلكَ، لا يمكنُ الموافقةُ على هـذا الموقفِ إلَّا إذا حُرِمَ الأطرافُ، أوَّلًا، من فرصةِ إثارةِ الاعتراضاتِ على استنتاجاتِ الذكاءِ الاصطناعيِّ، وثانيًا، إذا كانَ القرارُ المتَّخذُ غيرَ قابلٍ للاستئنافِ[2].

تعتمدُ أنظمةُ الحوكمةِ الخوارزميَّةِ على مجموعةٍ من القواعدِ الحسـابيَّةِ والبرمجيَّاتِ الذكيَّةِ التي تُحدِّدُ كيفيَّةَ اتخاذِ القراراتِ وتوزيعِ الموارِدِ والفُرَصِ والمخاطرِ. تُستخدمُ هذه الخوارزميَّاتُ في مجالاتٍ مثلِ التوظيفِ، وتوزيعِ القـروضِ، والتنبؤِ بالجريمةِ، وتحديدِ الأولويَّاتِ الصحيَّةِ، مـا يجعلُها قوَّةً تنظيميَّةً جديدةً تُعيدُ تشـكيلَ المجـالِ العامِّ بطرقٍ غالبًا ما تفتقرُ إلى المسـاءلةِ الديمقراطيَّةِ. كما وصفَها الفيلسوفُ الألمانيُّ (فيرنر شميدت- Werner Schmidt)، بأنَّها تُمثِّلُ "بيروقراطيَّةً غيرَ مرئيَّةٍ" تُمارسُ سلطتَها ليسَ من خلالِ القانونِ، بل من خلالِ الترميزِ[3].

تُطرَحُ هنا أسئلةٌ جوهريَّةٌ: هل تعملُ الخوارزميَّاتُ بشكلٍ محايدٍ، أم أنَّها تُعيدُ إنتاجَ التحيُّزاتِ التي يحملُها مُصمِّموها؟ تُشـيرُ كثيرٌ من الدراسـاتِ إلى أنَّ هذه الأنظمةَ الذكيَّةَ غالبًا ما تعكسُ وتُعزِّزُ التحيُّزاتِ الطبقيَّةَ والعرقيَّةَ والجندريَّةَ، نتيجةً للبياناتِ المُستخدَمةِ في تدريبِها التي تستندُ إلى تاريخٍ غيرِ عادلٍ. فعلى سـبيلِ المثـالِ، إذا جرى تدريبُ خوارزميَّاتِ التوظيفِ باسـتخدامِ بياناتٍ تُفضِّلُ الذكورَ البيضَ، فإنَّها سـتقومُ بشـكلٍ تلقائيٍّ برفضِ السيرِ الذاتيَّةِ للنساءِ أو الأفرادِ من خلفيَّاتٍ عِرقيَّةٍ متنوِّعةٍ، حتَّى في غيابِ أيِّ نيَّةٍ مباشرةٍ لذلكَ[4].

1 - Martin Sand, Technological Utopianism and the Idea of Justice, p.131.

2 - Vasiliy A. Laptev and Daria R. Feyzrakhmanova, «Application of Artificial Intelligence in Justice: Current Trends and Future Prospects», pp.394–405.

3 - Ibid, p.400.

4 - Huw Roberts et al, Ibid, p.56.

في هـذا السـياق، تمُـارَسُ الحرِّيَّةُ الرقميَّةُ ضمنَ حـدودٍ ضيِّقة ومشـوَّهَة؛ حيث يُطلبُ من المسـتخدمينَ قبولُ الشروطِ دونَ أن يكـونَ لديهم وعيٌ حقيقيٌّ لتأثيراتهـا على خصوصيَّتهم. وهكـذا، تتلاشى فكـرةُ الحرِّيَّة من المجالَيْنِ السـياسيِّ والقانونيِّ، في الوقت الذي تسـعى فيه الشركاتُ التكنولوجيَّةُ لجمعِ البيانات وتحليلها واسـتخدامها لأغراضٍ تجاريَّة أو سياسيَّة، وكلُّ ذلكَ دونَ أن يكونَ هناكَ رادعٌ أو رقابةٌ كافيةٌ. إنَّ هذه الحرِّيَّةَ الشـكليَّةَ لا تسـتطيعُ الصمودَ أمامَ الهيمنة الخوارزميَّة التي تُعيدُ تشكيلَ السلوكِ والتفضيلات والتوجُّهات بشكلٍ غيرِ واعٍ؛ ما يؤدِّي إلى نمطٍ من «التحكُّم الرقميِّ»؛ حيث يعتقدُ المستخدمُ أنَّه يختارُ، بينما هو في الواقعِ تحتَ تأثيرِ نماذجَ تنبُّؤيَّة معقَّدة[1].

نجدُ أنَّ هناكَ كثيراً من الدعواتِ لتطويرِ نموذجٍ مختلفٍ للحوكمة الخوارزميَّة يعتمدُ على أُسسِ العدالة التشاركيَّة، والشفافيَّة، والمساءلة. يسعى هذا النموذجُ إلى تمكينِ المواطنينَ والمجتمعات المحليَّة من المشـاركة في تصميمِ وتقييمِ الأنظمة التقنيَّة، مع السـعي إلى تفكيكِ نهجِ المركزيَّة الـذي يُتيحُ للشركاتِ الكبرى الهيمنةَ على الفضاءِ الرقميِّ على المسـتوى العالميِّ. كما يتطلَّبُ الأمرُ تطويرَ أُطرٍ قانونيَّة جديدة تُعرِّفُ «التحيُّزَ الخوارزميَّ» بوصفه نوعًا من التمييز.

يُعَدُّ نموذجُ «حوكمةِ الذكاءِ الاصطناعيِّ من الأسفلِ» (Bottom-Up AI Governance) من الاتِّجاهات الواعـدة في هذا المجال؛ حيث يجري تزويدُ المجتمعات المُهمَّشـة بأدوات تقنيَّة ومعرفيَّة تُساعدُها على فهمِ الأنظمةِ التي تُسهمُ في التحيُّزِ الرقميِّ ضدَّها. مضافًا إلى ذلكَ، تمُثِّلُ مبادراتُ "البيانات حقًّا عامًّا" (Data as a Public Good) محاولةً لتقويضِ احتكارِ البيانات من قِبَلِ شركاتِ التكنولوجيا، وإعادةِ هذه البياناتِ إلى المواطنينَ بوصفهم المالكينَ الفعليِّينَ لها[2].

إنَّ الإخفاقَ في معالجةِ قضايا العدالة التكنولوجيَّة قد يؤدِّي إلى تفاقمِ الفجواتِ الاجتماعيَّة وظهورِ أشـكالٍ جديدة من «التمييزِ الخوارزميِّ»؛ حيث تتحوَّلُ الخوارزميَّاتُ إلى أداةٍ للوصولِ إلى الحقوق، ما يزيدُ من الفقرِ والتهميشِ والعنفِ الرمزيِّ. في المقابلِ، يمكنُ أن يُساعِدَ التركيزُ على العدالةِ الرقميَّة والحوكمةِ التشـاركيَّة في بناءِ مسـتقبلٍ رقميٍّ أكثرَ ديمقراطيَّةً، بحيث تُصبحُ

1 - Linda Mulcahy and Anna Tsalapatanis, Digital Justice: Engineering Disadvantage?, p. 21.

2 - Federico Pierucci, «Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace», p.27.

التكنولوجيا وسيلةً لتعزيز التمكين[1].

يمكنُ تخيُّلُ فضاءٍ إلكترونيٍّ يُدارُ وفقًا لمعاييرِ الكفاءة والسرعة، ويعتمدُ على مبادئ الكرامة وحقوق البشر، استنادًا إلى مفاهيم العدالة الخوارزميَّة وخُلُقيَّات الذكاء الاصطناعيِّ. يتطلَّبُ هذا التغييرُ تحوُّلًا جذريًّا في تصوُّرنا للتكنولوجيا؛ حيث ينبغي علينا أن ننظرَ إليها على أنّها أدوات غير محايدة، بل نُظُم سياسيَّة وخُلُقيَّة تحتاجُ إلى المراقبة والنقد والمساءلة.

في النهاية، تُعَدُّ العدالةُ التكنولوجيَّةُ ضرورةً على الصعيدَيْنِ السياسيِّ والخُلُقيِّ؛ لضمان ألَّا يتحوَّلَ الفضاءُ الرقميُّ إلى وسيلة جديدة للإقصاء، بل يجبُ أن يكونَ منصَّةً للعدالة والحرِّيَّة والاحترامِ للكرامة الإنسانيَّة في عالمٍ يُشكِّلُ فيه كلُّ شيءٍ بواسطة الخوارزميَّات.

خاتمة

تُظهرُ الدِّراسةُ مجموعةً من النَّتائج الَّتي توضِّحُ تداعيات المُراقبة التِّكنولوجيَّة والتَّحكُّم السِّبرانيِّ على الخُصوصيَّة في عصر الذَّكاء الاصطناعيِّ، من بينها الآتي:

١. تكشفُ الدِّراسةُ أنَّ انتشارَ أدوات المُراقبة التِّكنولوجيَّة وتَطويرَ أنظمة الذَّكاء الاصطناعيِّ قد أحدثَ تَحوُّلًا جذريًّا في مفهوم السِّيادة على البيانات؛ فقد أصبحت البياناتُ الشخصيَّةُ أكثرَ عُرضةً للاستغلال التِّجاريِّ والسِّياسيِّ تحتَ ذريعة الأمن والكفاءة، وهذا الأمرُ يُهدِّدُ بتقويض الثِّقة الرَّقميَّة ويَخلُقُ حالةً منَ الاغتراب التِّكنولوجيِّ.

٢. تَبرُزُ مشكلةُ التَّحيُّز الخوارزميِّ بوصفها واحدةً من أخطر تداعيات هذه الأنظمة؛ حيث تُسهمُ الخوارزمياتُ في إنتاج أشكال جديدة منَ التَّحيُّز، وتَعكسُ معاييرُ التَّصنيف والتَّقييم الَّتي تَعتَمِدُها أنظمةُ الذَّكاء الاصطناعيِّ تحيُّزاتٍ تمَّ بَرمجتُها مُسبقًا، ما يُؤدِّي

1 - Linda Mulcahy and Anna Tsalapatanis, Ibid, p.30.

إلى ظُهور أشكال جديدة منَ اللامُساواة الاجتماعيَّة.

٣. يُعـاني الإطارُ التَّشريعيُّ والرَّقابيُّ الحاليُّ من قُصور بالـغ في مُواكبة هذه التَّحوُّلات؛ حيث تَظهَرُ الفجوةُ بين سُرعة التَّطوُّر التِّكنولوجيِّ وبُطء الاستجابة القانونيَّة؛ فمعظمُ التَّشريعات الحاليَّة تَعتَمدُ منطقَ العلاج الجُزئيِّ للمشـكلات بدلاً منَ التَّأسيس لرؤية استباقيَّة شاملة، ما يجعلُها عاجزةً عن مُواجهة التَّحدِّيات الجديدة الَّتي يَفرضُها عصرُ التَّحوُّل الرَّقميِّ.

٤. أَظهَرَت الدِّراسـةُ أنَّ تَطويرَ أنظمة التَّحكُّم السِّـبرانيِّ يَخلُقُ تناقضًـا بين تَعزيز الأمن الرَّقمـيِّ من جهة، وتقويـض الحُريَّات الفرديَّة من جهة أُخـرى، في ظلِّ الافتقار إلى تَشريعات شاملة وفعَّالة لشفافيَّة استخدام البيانات.

٥. ينبغـي تَعزيزُ حُقـوق الخُصوصيَّـة وحمايتُها بالقانـون، خاصَّةً عندمـا يَتعلَّقُ الأمرُ بمعلومـات مثل البيانـات الشـخصيَّة أو الماليَّة؛ ومع ذلك، يجبُ إيـلاءُ المزيد منَ الاهتمام للسِّـياق ولإعـادة اسـتخدام المعلومات العامَّـة غير الخاضعـة للضَّوابط التَّنظيميَّة. كما أنَّ الأدوات التِّكنولوجيَّةَ المُتاحةَ للمُسـتخدم تُؤدِّي دورًا هامًّا؛ فمَنحُ المُستخدم بعضَ الحُريَّة، مَدعومًا بالتَّثقيف والتَّصميم التِّكنولوجيِّ المُناسب، سوف يُسـاعدُ على تَحقيق التَّوازن بين الحِفـاظ على حُقوق الخُصوصيَّـة وإنترنت مَفتوح الوُصول.

المصادر والمراجع

- بهاء درويش: أخلاقيات العلم والتكنولوجيا وتطبيقاتها في الواقع المعاصر، الإسـكندرية، دار الوفاء،، ط١، ٢٠٢١.
- وائـل أحمد عبد الله صبره: التحديات الأخلاقية التـي تواجه العلم والتكنولوجيا في عصر البيانات الضخمة، مجلة كلية الآداب، جامعة سوهاج، ط١، العدد الثالث والخمسون، الجزء الأول، أكتوبر ٢٠١٩.

- Bernd Carsten Stahl et al. Ethics of Artificial Intelligence: Case Studies and Options for Addressing Ethical Challenges, Cham: Springer, 2023, 1st edition.
- Elena Consiglio and Giovanni Sartor. "A New Form of Socio-technical Control: The Case of China's Social Credit System", in: Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China, Cham: Springer, 2023. https://doi.org/10.10078_1-41566-031-3-978/
- Federico Pierucci. «Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace», Digit. Soc. 4, 27 (2025). https://doi.org/10.1007/s442064-00189-025-
- Georgy Ishmaev. «Sovereignty, privacy, and ethics in blockchain-based identity management systems», Ethics Inf Technol 23, 239–252 (2021). https://doi.org/10.1007/s1067609563--020-x
- Hamid Jahankhani. Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022, Cham: Springer, 2023, 1st edition.
- Huw Roberts et al. "Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance", in: Quo Vadis, Sovereignty?

Philosophical Studies Series, vol 154. Cham: Springer, 2024. https://doi.org/10.10074_1-41566-031-3-978/

- Ilse Oosterlaken and Jeroen van den Hoven (eds). The Capability Approach, Technology and Design, Philosophy of Engineering and Technology 5, New York; Springer, 2012, 1st edition.
- Jason Edwards. Mastering Cybersecurity: Strategies, Technologies, and Best Practices, Apress Berkeley, CA, 2024, 1st edition.
- Julia van Hee et al. The Surveillance Society: Which Factors Form Public Acceptance of Surveillance Technologies? Cham: Springer, 2017, 1st edition.
- Kodi A. Cochran. Cybersecurity Essentials: Practical Tools for Today's Digital Defenders, Apress Berkeley, CA, 2024, 1st edition.
- Linda Mulcahy and Anna Tsalapatanis. Digital Justice: Engineering Disadvantage?, Cham: Palgrave Macmillan, 2024, 1st edition.
- Mark Coeckelbergh et al (Eds.). Envisioning Robots in Society – Power, Politics, and Public Space: Proceedings of Robophilosophy2018/ TRANSOR 2018 February 14–17, University of Vienna, Austria, Amsterdam: IOS Press, 2018, 1st edition.
- Martin Sand. Technological Utopianism and the Idea of Justice, Cham: Palgrave Macmillan, 2025, 1st edition.
- Michael Steinmann et al. "Embedding Privacy and Ethical Values in Big Data Technology", In Matei, S., Russell, M., Bertino, E. (eds) Transparency in social media. Computational Social Sciences. Springer, Cham, 2015, pp 277–301. https://doi.org/10.100715_1-18552-319-3-978/.
- Nachaat Mohamed. "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future

paradigms", Knowl Inf Syst, 2025. https://doi.org/10.1007/s10115-025-02429-y

- Oliver Korn. Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction, Cham: Springer, 2019, 1st edition.
- Pradip Kumar Das et al (eds). Privacy and Security Issues in Big Data: An Analytical View on Business Intelligence, Singapore: Springer, 2021, 1st edition.
- Roos Slegers. Privacy and Surveillance: In Business Ethics. Springer, Cham. 2023. https://doi.org/10.100710_1-37932-031-3-978/
- Sasmita Mohapatra. "Surveillance with Smart Spherical Robot", in ICT: Innovation and Computing. ICTCS 2023. Lecture Notes in Networks and Systems, vol 879. Singapore; Springer, 2024. https://doi.org/10.1007-978/14_1-9486-99-981
- Sherali Zeadally and Mohamad Badra. Privacy in a Digital, Networked World: Technologies, Implications and Solutions, Cham: Springer, 2015, 1st edition.
- Thammisetty Swetha et al. "Leveraging AI for enhanced cybersecurity: a comprehensive review", Discov Appl Sci 7, 584 (2025). https://doi.org/10.1007/s424520-06773-025-
- Tobias D. Krafft et al. «Black-Box Testing and Auditing of Bias in ADM Systems», Minds & Machines 34, 15 (2024). https://doi.org/10.1007/s11023-0-09666-024
- Tulika Singh. AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy, Singapore: Springer, 2024, 1st edition.
- Tuomo Sipola et al (eds). Artificial Intelligence for Security: Enhancing Protection in a Changing World, Cham: Springer, 2024, 1st edition.

- Vasiliy A. Laptev and Daria R. Feyzrakhmanova. "Application of Artificial Intelligence in Justice: Current Trends and Future Prospects", Hum-Cent Intell Syst 4, (2024), pp.394–405. https://doi.org/10.1007/s442302-00074-024-