تحتلّ قضيّة الخصوصيّة موقعًا خاصًّا في عصر وسائل التواصل الاجتماعيّ التي تقوم بصورة رئيسة على المشاركة الواسعة للمعلومات، وعلى قابليّة تداول المحتوى المنشور عليها بصور لا محدودة وفي سياقات متنوّعة، ومع جماهير تتّسم بالكثرة والتنوّع والسيولة. وقد فاقمت التطوّرات الكبيرة والمتلاحقة في مجال الذكاء الاصطناعيّ في السنوات القليلة الأخيرة من تعقيدات مفهوم الخصوصيّة، ومن تداعيات خرقها بغير صورة. فتقنيّات الذكاء الاصطناعيّ المستحدثة التي ترتكز على جمع كميّات هائلة من البيانات ودمجها وإعادة استخدامها لأغراض عدّة، مثل تشات جي بي تي (Chat GPT) وتقنية التزييف العميق (Deepfake)، تمثّل تحديًّا كبيرًا لخصوصيّة أصحاب البيانات، ولأمنهم وسلامتهم في بعض الأحيان.

في ضوء هذه التحديّات، ثمّة حاجة ملحّة إلى إعادة تأطير مفهوم الخصوصيّة بما يتناسب مع مرتكزات هذا العصر من مستجدّات تكنولوجيّة متواترة، ومن تغيّر في أنماط الاتصال والاجتماع الرقميّ. في هذا الصدد، يمثّل كتاب "الخصوصيّ سياسيّ: الخصوصيّة الشبكيّة ومواقع التواصل الاجتماعيّ"(1) إسهامًا مهمًّا، إذ يضطلع بالحفر في مفهوم عمل الخصوصيّة وديناميّاته، وتداعيات خرقها في ضوء العوامل السياسيّة والاجتماعيّة والتقنيّة ذات الصلة. تهدف مؤلفة الكتاب أليس مارويك، الأستاذة المشاركة في قسم الاتصال الجماهيريّ في جامعة نورث كارولينا في تشابيل هيل، إلى تبيان الحاجة إلى تجاوز المفهوم الكلاسيكيّ للخصوصيّة وتفكيك ما ارتبطت به من ثنائيّات ومفاهيم مغلوطة إلى إطار آخر يمكنه الإحاطة بتحديّات استخدام البيانات وشروطها في السياقات الرقميّة الراهنة.

النموذج الشبكيّ للخصوصيّة

تستهلّ مارويك كتابها بتبيان الطبيعة الشبكيّة للخصوصيّة في عصر مواقع التواصل الاجتماعيّ. ترتكز الـسوشال ميديا، بحكم كونها اجتماعيّة بالتعريف، على ربط المستخدمين ببعضهم وترسيم علاقاتهم وشبكاتهم الاجتماعيّة. بالإضافة إلى ذلك، فإنّ أحد خصائص التواصل عبر المنصّات الاجتماعيّة هو انهيار السياق، إذ إنّ المعلومات على هذه المنصّات كثيرًا ما تتجاوز سياقها الأصليّ وتتدفق عبر شبكات اجتماعيّة وتكنولوجيّة متعددة إلى سياقات أخرى. وكما تقوم مواقع التواصل الاجتماعيّ على تسهيل تشاركيّة المعلومات، فإنّها، بحسب مارويك، مُصمَّمة بحيث تسمح بتسريبها كذلك. فالقدرة على التقاط لقطات الشاشة، ونسخ الرسائل وإعادة توجيهها، على سبيل المثال، يعني ببساطة سهولة نقل

معلومات نشأت في الأصل في سياق تشاركيّ خاصّ بين صديقين على تطبيق مثل ميسنجر إلى جمهور وسياقات أوسع وأبعد. كما يمكن لممارسات رقميّة مثل الإشارة إلى شخص ما في صورة أو شريط فيديو، أو نشر الذكريات المشتركة على موقع إنستاجرام، أو حتّى خاصيّة تحديد أشخاص قد تعرفهم على موقع فيسبوك أن تكشف بيانات مهمّة عن مستخدمي الـسوشال ميديا، وتجعل شبكاتهم الاجتماعيّة مرئيّة للآخرين كذلك.

وعلى مستوى أكبر، فإنّ تقنيّات البيانات الضخمة (Big data) التي تعتمد على جمع المعلومات وشرائها من مصادر متعددة، من بينها منصّات التواصل الاجتماعيّ، تُبرز أيضًا الطبيعة الاجتماعيّة والشبكيّة للمعلومات في العصر الرقميّ. فتقنيّات مثل الخوارزميّات التنبؤيّة (Predictive algorithms) واختبار الحمض النووي المتعلّق بالأسلاف (Genomic ancestry testing)، عادة ما تتعقّب شبكات كاملة من الأفراد، وقد تكشف من ثمّ عن معلومات خاصّة جدًّا. فإرسال شخص ما لمسحة شدقيّة إلى موقع 23andMe، على سبيل المثال، قد لا يترتبّ عليه الكشف عن علاقات عائليّة خفيّة فحسب، بل إنّ هذه المعلومات قد تستخدمها أطراف أخرى مثل أقسام الشرطة أو شركات الأدوية لأغراض حلّ الجرائم أو لتطوير أدوية جديدة وما إلى ذلك.

تُبيّن هذه الأمثلة مدى صعوبة تجنّب انتهاكات الخصوصيّة التي تتسبب فيها التقنيّات الشبكيّة من الـسوشال ميديا إلى تقنيّات البيانات الضخمة، إلى مراقبة الشركات الكبرى والحكومات وما قد يستتبع ذلك من تداعيات جمّة. رغم ذلك، لم تزل نماذج الخصوصيّة القائمة ترتكز على كونها مسؤولية فرديّة. فإذا تسرّبت بيانات من موقع لآخر، ومن سياق لسياق مغاير، فإنّ اللوم غالبًا ما يُوجَّه إلى الشخص الذي شارك المحتوى المعنيّ بدلًا من توجيه النقد إلى الأفراد أو الكيانات التي قامت باستخدامه دون إذن، أو التقنيّات الرقميّة التي تُيسّر هذا النوع من التسريبات. تنتقد مارويك هذا التوجّه النيوليبراليّ الذي يؤسّس للتصوّرات القانونيّة والتقنيّة للخصوصيّة في الولايات المتحدة. وقد رسّخت شركات التكنولوجيا هذا النموذج الفردانيّ فعليًّا بتوجيه سياسات الخصوصيّة إلى الأفراد، بالرغم ممّا لهذه السياسات من إشكاليّات، من بينها أنّ إعدادات الخصوصيّة تتغيّر باستمرار، وغالبًا ما تُكتب بلغة أكاديميّة تجعلها صعبة الفهم والتطبيق، والأهمّ أن عدم الموافقة على هذه السياسات لا يترك لمستخدمي المنصّات الاجتماعيّة خيارًا غير الخروج منها.

الخصوصيّة كشأن سياسيّ

في ضوء هذه المعطيات، تتبنّى مارويك نموذجًا شبكيًّا للخصوصيّة، لا لأنّ هذا المفهوم يناسب أنماط التواصل في عصر الشبكات الاجتماعيّة فحسب، بل لأنّه يساعد أيضًا على فهم الخصوصيّة باعتبارها مسألة سياسيّة تتأصّل في ممارسات بنيويّة وتعيد إنتاج الأنماط القائمة من اللامساواة العرقيّة، والطبقيّة، والجندريّة، والجنسانيّة، خاصّة مع تزايد أنظمة المراقبة والتنقيب عن البيانات على الإنترنت وتنوّعها. تتجذّر مثل هذه التفاوتات في ممارسات وتشريعات قديمة ومعاصرة ترتكز على منح الحقّ في الخصوصيّة لبعض الفئات وإنكاره على فئات أخرى. فثمّة، على سبيل المثال، تاريخ طويل من تعقّب المعلومات حول مجتمعات السود وملاحقتها وجمعها في الولايات المتحدة، وما يرتبط بتلك الممارسات من انتهاكات سافرة للخصوصيّة. ثمّة كذلك أنماط متنوّعة من رصد للعرب والمسلمين ومراقبة وتعقّب إلكترونيّ لهم في الولايات المتحدة منذ أحداث 11 سبتمبر. كما تتبدّى التحيّزات العرقيّة للتقنيّات الرقميّة المعاصرة مثلًا في تقنيّات التعرّف على الوجوه (Facial-recognition technology) التي تعتمد في تدريب خوارزميّاتها على الوجوه البيضاء فقط، ما يثير أسئلة مهمّة حول قدرتها على التعرّف بدقّة على وجوه الأفراد من مجموعات عرقيّة أخرى، مثل الأفارقة الأمريكيّين أو الآسيويّين(2).

The Private Is Political
Networked Privacy and Social Media
Alice E. Marwick

تبعًا لذلك، تستند مارويك في ما تقترحه من إطار شبكيّ لتصوّر الخصوصيّة الرقميّة إلى نظرية هيلين نيسنباوم حول التكامل السياقيّ (Contextual integrity) التي ترتكز على نقض التصوّرات الثنائيّة التي ترى المعلومات إمّا عامّة أو خاصّة. على النقيض من ذلك، تطرح نظريّة التكامل السياقيّ الخصوصيّة لا باعتبارها سمة متأصّلة في المعلومات ذاتها، بل في السياق الذي يجري فيه تشارك المعلومات. من ثمّ تستحيل الخصوصيّة وفقًا لهذا الإطار، وخلافًا للتصوّرات القانونيّة التي تراها أمرًا متماثلًا في كلّ المواقف، إلى أمر سياقيّ في المقام الأوّل؛ إذ تتعلّق الخصوصيّة بصورة جوهريّة بالسياقات التي تتدفّق فيها المعلومات وبما يتصل بهذه السياقات من قيم وأعراف مختلفة، ومن علاقات قوّة كذلك. وعليه تدعو مارويك إلى التفكير في الخصوصيّة الرقميّة بعيدًا عن ثنائيّة العام والخاصّ؛ إذ يمكن عوضًا عن ذلك النظر إلى المعلومات من حيث موقعها على امتداد طيف من المرئيّة (Visibility).

ولفهم كيف يشتبك الأشخاص من مختلف الانتماءات والتوجّهات بصورة فعليّة مع الخصوصيّة، وكيف يجري التعاطى معها ومعاينة تداعيات انتهاكها في ظلّ هذا الواقع الرقميّ المعقّد، تعتمد مارويك في هذا الكتاب على مقابلات مطوّلة ومجموعات نقاش بؤريّة، أجرتها بين عامي 2014 و2019، مع 128 مشاركًا ومشاركة من الولايات المتحدة، ينتمون إلى مجموعات ديموغرافيّة متنوّعة. تسعى مارويك من خلال هذه الدراسة إلى مخالفة النهج السائد لدراسة الخصوصيّة، وذلك بوضع أصوات الأقليّات والفئات الأكثر هشاشة وخبراتهم في المركز، بدلًا من التركيز على تأطير الخصوصيّة من منظور أصحاب شركات التكنولوجيا أو الدول وصنّاع السياسات.

"شغل الخصوصيّة"

وفقًا للإطار الذي تطرحه مارويك لفهم الخصوصيّة وأشكلتها في سياقنا المعاصر، تطوّر المؤلفة مفهوم شغل الخصوصيّة (Privacy work)، وهو يشير إلى ما يقوم به الناس من ممارسات، وما يتخذونه من قرارات في إطار محاولاتهم للحفاظ على القدر المناسب من الخصوصيّة في مواجهة انتهاكات التقنيّات الرقميّة الشبكيّة. تُموضع مارويك حماية الخصوصيّة في إطار نسويّ، وتبني مفهوم شغل الخصوصيّة على فكرة شغل الأمان (Safety work) التي طوّرتها عالمة الاجتماع النسويّة ليز كيلي، للتعبير عن الجهود والاستراتيجيّات التي تتّبعها النساء لتجنّب عنف الرجال، وهو شغل غير مرئيّ وغير مأجور، تمامًا كما "شغل الخصوصيّة" الذي تجادل مارويك بعدم جدواه في أغلب

الأحيان. تدحض مارويك بهذا المفهوم أحد الاعتقادات المغلوطة الشائعة، حتّى في أوساط التقنيّين والأكاديميّين، أنّ الناس، خاصّة الأجيال الشابّة، لا تأبه بالخصوصيّة، وذلك من خلال توضيح كمّ الجهد اللامتناهي ونوعه الذي ينخرط فيه الأفراد للحفاظ على خصوصيّتهم قدر الإمكان.

يتنوّع شغل الخصوصيّة، ويعتمد جزء منه على بعض الخاصيّات والمحدّدات التكنولوجيّة، مثل إغلاق إعدادات تحديد المواقع، أو حظر بعض الأفراد كليّة، أو فقط حظر وصول محتوى معيّن لهم، أو تغيير الحسابات من عامّة إلى خاصّة على المواقع التي تسمح بذلك، أو استخدام التصفّح المُجهّل (Incognito browsing) عند زيارة بعض المواقع، أو استخدام تقنيّات تعزيز الخصوصيّة، مثل الشبكات الافتراضيّة الخاصّة (VPNs).

كما يلجأ مستخدمو السوشال ميديا إلى توظيف استراتيجيّات أخرى مبتكرة لحماية الخصوصيّة، منها ما يُعرف بالتقسيم الاجتماعيّ (Social segmentation)، ويتضمّن تقسيم الجمهور باستخدام مواقع وتطبيقات مختلفة، وأحيانًا بإنشاء حسابات مختلفة على نفس التطبيق، وذلك للتحكّم في نوع المعلومات التي يجري مشاركتها مع أنواع مختلفة من الجماهير. وثمّة استراتيجيّة أخرى لحماية الخصوصيّة، تسمّيها الأكاديميّة والباحثة الأمريكيّة دانا بويد إخفاء البيانات (Social steganography) التي تعتمد على الإبهام أو كتابة المحتوى بشكل غامض للحدّ من فهمه، إذ يكون المحتوى المعنيّ في هذه الحالة متاحًا بشكل كبير، لكنّه يكون مفهومًا لبعض المطّلعين عليه فقط. وتشمل أنواع شغل الخصوصيّة أيضًا الرقابة الذاتيّة، والمشاركة المحدودة، وكذلك الخروج التام من مواقع التواصل الاجتماعيّ.

تُبيّن مارويك من خلال هذا المفهوم أنّ الخصوصيّة ليست حالة جامدة، بل عمليّة مستمرّة ومجموعة قرارات وممارسات غالبًا ما ينخرط فيها مستخدمو الشبكات الاجتماعيّة لإدارة تدفّق المعلومات الخاصّة بهم. كما أنّ هذا المفهوم يبرز التفاوتات في توزيع الخصوصية؛ إذ إنّ الجهد الذي يحتاج الفرد أن يبذله، ومدى نجاحه في حماية خصوصيّته في الفضاء الرقميّ، يعتمد على ما لديه من سلطة وامتيازات؛ فالفئات المهمّشة تبذل جهدًا أكبر بكثير من الأثرياء وذوي النفوذ لحماية أنفسهم من المراقبة الإلكترونيّة وغيرها من انتهاكات الخصوصيّة. بالإضافة إلى ذلك، تشير مارويك إلى أنّ الحكومات والشركات الكبرى تستفيد من عدم نجاح شغل الخصوصيّة في أغلب الأحيان؛ إذ تبقى المعلومات متاحة أمام سماسرة البيانات وغيرهم من الكيانات التي تتربّح من جمع البيانات من المنصّات الرقميّة.

لذلك، فتأطير حماية الخصوصيّة بوصفه عملًا غير مرئيّ وغير مدفوع الأجر يضيء على تداعيات توزيعه بشكل غير متكافئ لصالح تفاوتات القوّة القائمة.

الخصوصيّة والهويّات الاجتماعيّة

بما أنّ الخصوصيّة مسألة سياسيّة، فإنها بالطبع تتأثّر بالقيم والأعراف الاجتماعيّة السائدة، وبتفاوتات القوّة كذلك. فالتعاطي مع المعلومات في الفضاء الرقميّ وتحديد ما يمكن أن "يُكشَف" وما "يجب" أن يُخفَى من معلومات يتأثر بالنظم البنيويّة، مثل العنصريّة والميسوجينيّة ورهاب المثليّة. على سبيل المثال، تؤثر الأعراف الجندريّة السائدة على التعاطي مع النساء على مواقع التواصل الاجتماعيّ؛ فالنساء أكثر عرضة بصورة كبيرة لأنماط معيّنة من التحرّش والوصم والانتقام على الإنترنت. فإلى جانب استخدام اللغة التحقيريّة والإهانات والشتائم الجنسيّة ضدهنّ، تتخذ انتهاكات الخصوصيّة المُمكَّنة بالتكنولوجيا الرقميّة أشكالًا عدّة، من بينها استقاء المعلومات الشخصيّة (Doxing)، الذي يعني إفشاء معلومات شخصيّة مثل العنوان أو رقم الهاتف أو الاسم الحقيقيّ لشخص ما دون إذنه، والانتقام الإباحيّ (Revenge porn)، ويتضمّن نشر محتوى ذا طابع جنسيّ دون موافقة الشخص المعنيّ، والتحشيد (Dogpiling) الذي يقوم على شنّ هجمات جماعيّة مُنسّقة على شخص ما.

تمثّل هذه الممارسات الرقميّة الشبكيّة نوعًا من الشهرة القسريّة، وتُعدّ انتهاكًا صارخًا للخصوصيّة، إذ لا تكشف عن معلومات شخصيّة فحسب، بل تدفع بالضحيّة إلى مركز الضوء رغمًا عنها، بغرض التنمّر أو الوصم أو الإسكات، ما قد يترتب عليه تداعيات فعليّة جسيمة قد تمسّ الحياة العائليّة أو المهنيّة، أو حتّى سلامة الضحيّة. وفي هذا الصدد، تستعير مارويك من مجال الأمن السيبرانيّ مفهوم ناقلات الهجوم (Attack vectors)، وهي عبارة عن ثغرات أو مواضع هشاشة يمكن استغلالها للهجوم على شخص ما، لتبيان كيف تُعدّ الهويّة الجندريّة والتوجّه الجنسانيّ والعرق وغيرها ناقلات هجوم تسوّغ التحرّش والتشهير في الفضاءات الرقميّة.

ترصد مارويك أيضًا من خلال تجارب المشاركات في دراستها سيادة وجهات النظر الذكوريّة في مجال الألعاب الإلكترونيّة (Gaming)، ومن ثمّ انخراط النساء اللاتي ينضممن إلى هذا العالم عادة في شغل خصوصيّة (وهو ما يُعتبر شغل أمان كذلك) متنوّع ومكثف لحماية أنفسهنّ من التحرّش، إذ قد تستخدم اللاعبات استراتيجيّات من قبيل إخفاء

نوعهنّ الاجتماعيّ خلال اللعب باستخدام أسماء مستعارة وأفاتارات محايدة جندريًّا، بالإضافة إلى تفادي الدردشة الصوتيّة قدر الإمكان، والاستعاضة عنها بالدردشة النصيّة.

وكما في حالة انتهاكات الخصوصيّة الرقميّة بناءً على النوع الاجتماعيّ، يُعاين الأفراد الذين ينتمون لطبقات اجتماعيّة مختلفة مستويات مختلفة من انتهاك الخصوصيّة؛ فالمراقبة المكثفة وما تستتبعه من انتهاكات للخصوصيّة كانت دائمًا من نصيب الفقراء والأحياء الفقيرة في الولايات المتحدة. فالأفراد من مجتمعات السود واللاتينيّين والمهاجرين غير المسجّلين الذين يعانونًا اقتصاديّة متزعزعة يخضعون بصفة عامة لمراقبة واسعة من قبل مؤسسات عدّة، تشمل الشرطة، والعدالة الجنائيّة، والتوظيف، والتعليم، والرعاية الاجتماعيّة، إذ تضطلع هذه الكيانات عادة بجمع كميّات هائلة من البيانات حول الأشخاص المعنيّين من سماسرة البيانات والسوشال ميديا وغيرها من مصادر، ليجري تغديتها لاحقًا في أنظمة القرار الآليّ المؤتمت (Automated decision systems). تقوم هذه النظم بمهمات تتضمّن تصنيف المستفيدين المحتملين من الخدمات الحكوميّة إلى فئات، وتخصيص الاستحقاقات، والتنبؤ بالسلوك الإجراميّ. تنتقد مارويك الاعتماد المتزايد على هذه الأدوات، لما لها من تحيّزات وإشكاليّات عدّة، تتضمّن عدم دقتها، وأنّها تعمل دون محاسبة، بالإضافة إلى ما تتسبّب فيه من انتهاكات صارخة للخصوصيّة.

من جهة أخرى، تكشف تجارب بعض الأفراد من مجتمع الميم-عين الذين التقتهم مارويك لاستقصاء تجاربهم مع إشكاليّات الخصوصيّة الشبكيّة وكيفيّة تعاطيهم وتفاوضهم معها عن صعوبة رسم حدود صارمة بين الخاصّ والعام. على سبيل المثال، في ما يخصّ الإعلان عن هويّاتهم بوصفهم مثليّين أو أشخاصًا ترانس، كشف بعض هؤلاء الأشخاص أنّهم يستطيعون الإفصاح عن هذه الهويّات في أماكن عملهم أو في المقهى الذي يرتادونه باستمرار، أو حتّى على بعض مواقع التواصل الاجتماعيّ، بينما يخفونها عن عائلاتهم خوفًا من عواقب الوصم وفقد الاحترام. وفي ذلك قلب للتصوّر الكلاسيكيّ للمساحات العامة والخاصّة، وتشويش واضح لحدودها، إذ يمكن في مثل هذه الحالات أن يختبر الفرد الوصم والتهميش داخل ما يُفترض أنّها مساحة خاصّة مثل البيت، وأن يكون في المقابل مرتاحًا بشكل أكبر للكشف عن هويّة موصومة اجتماعيًّا في مساحة عامّة، مثل مكان العمل أو إحدى منصّات التواصل الاجتماعيّ.

لذلك، فإنّ هؤلاء الأشخاص لا يعايشون العام والخاصّ فكرةً ثنائيّة، بل طيفًا أو شبكةً من العلاقات والمواقف

والسياقات التي تتكشّف فيها المعلومات وتُعطى معنًى كذلك؛ فتجارب المشاركين في دراسة مارويك تبيّن أنّ الخروج من "الخزانة" أو البقاء فيها لا يحدث بشكل كامل وحدّي بالضرورة، إذ إنّهم قد يؤدّون هويّات مختلفة في السياقات المختلفة، ما يؤكّد أنّ مشاركة المعلومات حول الهويّات اللامعياريّة ليست أمرًا ثنائيًّا وجامدًا، بل سياقيّ في المقام الأوّل، ويعتمد على معايير معقّدة؛ شخصيّة واجتماعيّة وسياسيّة.

تخلص مؤلّفة هذا الكتاب المهمّ، بناءً على ما تطرحه من مقدّمات، إلى أنّ انتهاكات الخصوصيّة الشبكيّة، بما هي مسألة سياسيّة وبنيويّة في الأساس، تتطلّب معالجات بنيويّة. تُنبّه مارويك من ثمّ إلى الحاجة إلى إصلاح تشريعيّ شامل لضمان حماية البيانات وحماية خصوصيّات الأفراد بما يتماشى مع الطبيعة الشبكيّة للخصوصيّة الرقميّة، وتأمل أن تحفّز دراستها هذه تغييرًا في المفاهيم الاجتماعيّة حول الخصوصيّة، وأن تمثّل خطوة في اتّجاه رفض النموذج القائم على المسؤوليّة الفرديّة الكاملة عن انتهاكات الخصوصيّة، ومن ثمّ محاولة الدفع بكلّ الطرق في اتجاه وضع شركات التكنولوجيا وسماسرة البيانات والحكومات والدول أمام مسؤوليّاتها تجاه الانتهاكات الواسعة والخطيرة لخصوصيّات الأفراد في الفضاء الرقميّ.

1. Marwick, A. E. (2023). *The Private is political: Networked privacy and social media*. Yale University Press.
2. من الجدير بالذكر أنّ هذا الكتاب نُشر قبل بدء حرب الإبادة على غزّة بأشهر، وهو إذ يتناول الخصوصيّة شأنًا سياسيًّا بامتياز، حتّى على مستوى استخدام الأفراد اليوميّ للتقنيّات الرقميّة الشبكيّة، وما يكشف عنه من مثالب لهذه التقنيّات، فإنّ ذلك يدعونا إلى النظر مليًّا إلى تعقيدات مسألة الخصوصيّة في ظلّ استمرار الحرب الإسرائيليّة الجارية على المنطقة وتوسّعها، وموقع الخصوصيّة والشبكات الرقميّة منها، وما يطرحه السياق السياسيّ الراهن من أسئلة مهمّة حول هذا الموضوع.

الكاتب: أميرة عكارة