Global Network
on Extremism & Technology

بحوث المحتوى المتطرف على منصات التواصل الاجتماعي: حماية البيانات وأخلاقيات البحث بين التحديات والفرص

مانجانا سولد، جوليان جنك

مشروع GNET من المشرعات الخاصة التي يقدمها المركز الدولي لدراسة الراديكالية، كينجز كوليدج لندن.

هذا التقرير بقلم مانجانا سولد و جوليان جنك

الشبكة العالمية للتطرف والتكنولوجيا (GNET) مبادرة بحثية أكاديمية يدعمها منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT)، وهي مستقلة ولكن تمولها الصناعة من أجل فهم أفضل لاستخدام الإرهابيين للتكنولوجيا والتصدي لهم. ويقوم المركز الدولي لدراسة الراديكالية (ICSR) بتنظيم فعاليات الشبكة العالمية للتطرف والتكنولوجيا (GNET) والإشراف عليها، بصفته مركزًا بحثيًا أكاديميًا داخل قسم دراسات الحروب في كينجز كوليدج لندن. والآراء والاستنتاجات الواردة في هذه الوثيقة آراءُ المؤلفين، ولا تُفسر على أنها تمثل آراء منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT) ولا الشبكة العالمية للتطرف والتكنولوجيا (GNET) ولا المركز الدولي لدراسة الراديكالية (ICSR)، سواء كانت صريحة أو ضمنية.

بيانات الاتصال

لأي أسئلة أو استفسارات، أو للحصول على نسخ أخرى من هذا التقرير، يرجى التواصل مع:

ICSR
King's College London
Strand
London WC2R 2LS
المملكة المتحدة

هاتف: **+44 20 7848 2098**
بريد إلكتروني: **mail@gnet-research.org**

تويتر: **@GNET_research**

هذا التقرير، كغيره من منشورات الشبكة العالمية للتطرف والتكنولوجيا (GNET)، يمكن تنزيله مجانًا من موقع شبكة GNET على الإنترنت www.gnet-research.org.

الملخص التنفيذي

لم تحظ العلاقة بين الإرهاب والتكنولوجيا بهذا القدر من الأهمية على المستوى الاجتماعي والسياسي من قبل. ولا تكاد تجد عملية تعبئة أو عملية راديكالية أو هجومًا عنيفًا، وقع أو لم يقع، إلا وكان الإنترنت عنصرًا من بين عناصره. ويُعد تحليل هذه العمليات في البيئات التجريبية الصعبة عبر الإنترنت تحديًا يتصدى له الباحثون، لاسيما المعنيون بالشبكة العالمية للتطرف والتكنولوجيا (GNET). ونجد وفرة في البيانات التجريبية، حتى إذا وُضع في الاعتبار نزوع الأنظمة والسياسات إلى التغير باستمرار، فضلاً عن التحول نحو تزايد المساحات المغلقة والمشفرة. وفيما تتمخض هذه الوفرة عن تحديات وفرص،[1] يجد الباحث الذي يتناول المحتوى المتطرف عبر الإنترنت نفسه محاطًا بحدود صارمة ونطاقات رمادية تحيط بما يجوز له فعله وما لا يجوز، ما يفسح الطريق لاعتبارات الأخلاق وحماية البيانات. ودارت حول هذه الموضوعات مناقشات اكتسبت أهمية كبيرة في السنوات الأخيرة واحتدمت في منتديات البحوث الدولية.

يلخص هذا التقرير الصادر عن الشبكة العالمية للتطرف والتكنولوجيا (GNET) حالة المناقشات الدائرة حول الأخلاقيات والخصوصية، ويُبين للباحثين وشركات التكنولوجيا حدود البحوث والفرص المتاحة لها ويطرح التوصيات ذات الصلة. ويسير في خطوات ثلاث: أولاً، يلخص عددًا من الاعتبارات الأخلاقية الرئيسية التي ينبغي أن يضعها الباحث في هذا المجال الأكاديمي في الاعتبار؛ ثانيًا، يلقي نظرة عامة على مبادئ حماية البيانات الرئيسية التي يتعين مراعاتها ويسلط الضوء على الفرص المتاحة وموازنة الأعمال المطلوبة من الباحثين في هذا الصدد؛ ثالثًا، يناقش التفاعل بين الباحثين ومصادر البيانات وسياسات المنصات، ويلخص في هذا السياق بعض التوصيات الرئيسية للباحثين وشركات التكنولوجيا والجهات التنظيمية. أهم النقاط: أولاً، كلما تعددت قواعد البيانات ونقاط الوصول عبر المنصات كانت حافزًا للتوسع في هذا المجال البحثي وترويجه؛ ثانيًا، هناك حاجة ماسة للتعاون البحثي الدولي فيما يتعلق بتحليل المحتوى المتطرف عبر الإنترنت، بالاستناد إلى تعزيز التنسيق الدولي والتقارب فيما بين قواعد حماية البيانات؛ ثالثًا، ينبغي ألا يُنظر إلى أنظمة حماية البيانات على أنها مصدر إزعاج وإنما كوسيلة لتمكين البحوث العلمية عن طريق رسم خطوط أوضح لما يجوز وما لا يجوز؛ وأخيرًا، يتطلب المجال التجريبي الديناميكي وضع آليات متسقة لتعزيز التعاون بين شركات التكنولوجيا والباحثين والجهات التنظيمية لتكييف السياسات والأعراف المتبعة والأطر القانونية بطريقة توضح الأهمية الاجتماعية والسياسية للعلاقة بين التطرف والتكنولوجيا بكل إنصاف.

1 عبد الله الرحمون، شيراز ماهر، و تشارلي وينتر، تحليل شفرة الكراهية: استخدام التحليل التجريبي للنصوص في تصنيف المحتوى الإرهابي، المركز الدولي لدراسة الراديكالية (ICSR) كينجز كوليدج لندن (2020).

المحتويات

1 مقدمة

لعب الفضاء الرقمي دورًا رئيسًا في تعزيز راديكالية كثيرين من مرتكبي الهجمات السابقة:[1] لم يستغل المتطرفون، ومنهم أنيس عمري (برلين، ألمانيا)، برينتون تارانت (كرايستشيرش، نيوزيلندا) وستيفان بالييت (هالي، ألمانيا)، منصات التواصل الاجتماعي لجمع المعلومات وتوزيعها، وللتواصل والتجهيز لها فحسب، وإنما لتبادل الأفكار مع أصحاب الأفكار المماثلة أيضًا، بل وأحيانًا لمشاركة الهجمات مع آلاف المشاهدين مباشرة. ويمكننا تتبع التواصل بين مرتكبي العمليات الراديكالية أو المتطرفة لمعرفة الكثير عن العمليات الراديكالية التي تجري في العالم الافتراضي. وتكمن أهمية المحتوى وطريقة عرضه، وكذلك طريقة التواصل بين هذه الأطراف الفاعلة، في هذا الصدد، في أنها تُعد بمثابة خلفية يمكن أن توضع على أساسها أنسب التدابير للوقاية منهم وتشتيت شملهم.

في سياق هذا المجال البحثي، وبطبيعة الحال تزايدت أهمية البيانات المسترجعة من وسائل التواصل الاجتماعي.[2] ويتجلى ذلك في العديد من المنشورات العلمية المستندة إلى بيانات مستمدة من وسائل التواصل الاجتماعي: مثل فيسبوك[3] و تويتر[4] و يوتيوب[5] و انستغرام.[6] وأصبح من الممكن الوصول إلى كم هائل من هذه البيانات واستخدامها في طرح الفرضيات واختبارها.[7] ولا تخلو هذه الفرص من القيود والمزالق. ويتعلق هذا الأمر بالمتطلبات الأخلاقية وحماية البيانات المحتملة، ويلقي في طريق الباحثين تحديات، وفرصًا أيضًا، لا مفر منها. وفيما تُعد الشفافية ومبدأ "تعظيم الاستفادة وتقليل الضرر" ضروريْن على مدار عملية البحث بأكملها، هناك مبادئ وإرشادات أخرى ينبغي أن توضع في الاعتبار. نتناول في البابيْن الأوليْن موجزًا ثمة اعتبارات أخلاقية مهمة ينبغي أن تتضمنها عملية البحث في هذا المجال

1 بالغ الامتنان لما تفضل به سيباستيان جولد من تعليقات على إصدارات هذا التقرير السابقة وتوجيهات قانونية حاذقة في العديد من مساعينا البحثية في السنوات الماضية. نتوجه بالشكر أيضًا إلى كلارا أوغست سوس على تعليقاتها وليو باور و كلارا سينها على ما قدماه من دعم لإنهاء هذا التقرير.

2 Sebastian J. Golla, Henning Hofmann, and Matthias Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," Datenschutz und Datensicherheit – DuD 42, no. 2 (2018): 89, http://link.springer.com/10.1007/s11623-018-0900-x; Manjana Sold, Hande Abay Gaspar, and Julian Junk, Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities, 2020.

3 Agata Błachnio, Aneta Przepiórka, and Patrycja Rudnicka, "Psychological Determinants of Using Facebook: A Research Review," International Journal of Human-Computer Interaction 29 (2013), https://doi.org/10.1080/10447318.2013.780868; Ralf Caers et al., "Facebook: A Literature Review," New Media & Society 15 (2013), https://doi.org/10.1177/1461444813488061; Stefania Manca and Maria Ranieri, "Is It a Tool Suitable for Learning? A Critical Review of the Literature on Facebook as a Technology Enhanced Learning Environment," Journal of Computer Assisted Learning 29 (2013), https://doi.org/10.1111/jcal.12007; Ashwini Nadkarni and Stefan G. Hofmann, "Why do People Use Facebook?," Personality and Individual Differences 52, no. 3 (2012), https://doi.org/10.1016/j.paid.2011.11.007; Robert E. Wilson, Samuel D. Gosling, and Lindsay T. Graham, "A Review of Facebook Research in the Social Sciences," Perspectives on Psychological Science 7 (2012), https://doi.org/10.1177/1745691612442904.

4 Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," Studies in Conflict & Terrorism 38, no. 1 (2015); Amandeep Dhir, Khalid Buragga, and Abeer A. Boreqqah, "Tweeters on Campus: Twitter a Learning Tool in Classroom?," Journal of Universal Computer Science 19 (2013); Shirley Ann Williams, Melissa Terras, and Claire Warwick, "What Do People Study When They Study Twitter? Classifying Twitter Related Academic Papers," Journal of Documentation 69 (2013).

5 Chareen Snelson, "YouTube Across the Disciplines: A Review of the Literature," MERLOT Journal of Online Learning and Teaching Journal of Qualitative Methods 7, no. 14 (2011), http://jolt.merlot.org/vol7no1/snelson_0311.htm; Raphael Ottoni et al., "Analyzing Right-wing YouTube Channels: Hate, Violence and Discrimination," (2018); Kostantinos Papadamou et al., "Understanding the Incel Community on YouTube," (2020).

6 Tim Highfield and Tama Leaver, "A Methodology for Mapping Instagram Hashtags," First Monday 20, no. 1 (2015); Asuncion Bernardez-Rodal, Paula Requeijo Rey, and Yanna G. Franco, "Radical right parties and anti-feminist speech on Instagram: Vox and the 2019 Spanish general election," Party Politics (2020); Lena Frischlich, "#Dark inspiration: Eudaimonic entertainment in extremist Instagram posts," new media & society (2020).

7 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 89.

الأكاديمي، ونطرح رؤىً لما يجب مراعاته من مبادئ حماية البيانات الرئيسية.[8] ونسلط الضوء على الفرص المتاحة والموازنة بين التدابير المطلوبة من الباحثين في هذا الصدد. وفي الباب الثالث، نناقش مسألة التفاعل بين الباحثين ومصادر البيانات وسياسات المنصات، ونقدم بعض التوصيات المهمة.

8 In Sold, Abay Gaspar, and Junk, "Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities" نناقش عددًا من هذه العناصر باستفاضة، على غرار ما جاء في فصول De Koning et al. "On Speaking, Remaining Silent and Being Heard: Framing Research, Positionality and Publics in the Jihadi Field," in Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations, ed. Christoph Günther and Simone Pfeifer (Edinburgh: Edinburgh University Press, 2020) and "Ethics in Gender Online Research: A Facebook Case Study," in Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations, ed. Christoph Günther and Simone Pfeifer (Edinburgh: Edinburgh University Press, 2020) in the same volume by Günther and Pfeifer Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations (Edinburgh: Edinburgh University Press, 2020).

2 الاعتبارات الأخلاقية المحورية

تلعب الاعتبارات الأخلاقية دورًا في كل مشروع بحثي تقريبًا. ومن ثم فإن أخلاقيات البحث "لا تكفل الامتثال للقوانين فحسب وإنما تسعى إلى حماية المعنيين أيضًا".[9] وتنتشر البيانات الشخصية في كل مكان عند تحليل المحتوى المستمد من منصات التواصل الاجتماعي.[10] وكثيرًا ما يكون الوصول إلى هذا النوع من البيانات، مع شدة ضخامتها، سهلاً بعض الشيء، لكنه لا يثير قضايا أخلاقية مستجدة تمامًا ولا ينتهك[11] "المعايير والقيم المعترف بها في أخلاقيات البحث"، فضلاً عن أن التغير السريع في المنصات والسياقات والأحداث لا يجعل من توفير المساحة الكافية للاعتبارات الأخلاقية وتكييف هذه الاعتبارات مع المنصات والرؤى والسياسات المتغيرة ضرورةً فحسب، وإنما تحديًا كبيرًا أيضًا. لذا، كما هو الحال في أي مشروع بحثي، ينبغي أن نوازن بين المصلحة المجتمعية والعلمية وحق الفرد في الخصوصية. ومع ذلك، يثير استخدام البيانات المستمدة من وسائل التواصل الاجتماعي تحديات خاصة وقد "ينطوي على حقل ألغام محتمل".[12]

ومع أن المبادئ الأخلاقية ليس لها معيار مقبول عمومًا يوجب اعتبارها أمرًا إلزاميًا، هناك مباديء أخلاقية أكد كثيرون مرارًا وتكرارًا على اعتبارها ذات أهمية خاصة في هذه الأدبيات. تنقسم هذه المبادئ إلى ثلاث فئات: أولاً، ما يتعلق منها بالعلاقة بين الباحث وموضوعات البحث الفردية. ثانيًا، المبادئ المتعلقة بالبعد المجتمعي. ثالثًا وأخيرًا، ما يتجلى منها بذاته ويخص الباحثين أنفسهم. ونتناول هذه النتائج بإيجاز فيما يلي لتسهيل الوصول إليها خدمةً لما يُجرى من أبحاث في المستقبل حول التطرف والتكنولوجيا.

المبادئ الأخلاقية التي تتعلق بموضوع البحث الفردي

تتناول المبادئ التي تتعلق بموضوع البحث الفردي السرية أو احترام الأشخاص، و الإحسان. يعني ضمان السرية أن يتخذ الباحثون الذين يعرفون هوية موضوع البحث خطوات معينة لكي لا يكتشف الآخرون هوية الموضوع أو لا يُكشف عنها إليهم. وينبغي ألا تُستخدم بيانات أي شخص في أغراض بحثية إلا بموافقته كلما أمكن.[13] وتضمن الموافقة المستنيرة الحفاظ على حقوق الفرد الشخصية وحقه في تقرير مصيره عن علم. وبالتالي، على الباحث أن يتحلى بالشفافية ويتأكد من أن الشخص المعني على علم بخضوعه للبحث، وأنه على دراية بمشروع البحث القادم بأسلوب مفهوم، وأن الفرصة قد أتيحت له للموافقة على المشاركة فيه أو رفضها طواعيةً. ومع ذلك، فإن طلب الموافقة المستنيرة ليس بالأمر السهل عند التعامل مع المحتوى المتطرف، لأن السعي إلى الحصول على موافقة الأشخاص قيد البحث قد يعرض البحث للخطر: كثيرًا ما يتغير سلوك الفرد إذا علم أن بياناته محل اهتمام وقد تخضع للتحليل. وعلى سبيل المثال، إذا علم الفرد أنه (أو سلاسل رسائله ومشاركاته وتعليقاته عبر الإنترنت) قيد الملاحظة، فقد يسلك سلوكًا مختلفًا، ويتواصل مع الآخرين عبر قنوات أخرى، ويحجم عن إبداء آرائه أو يكيفها بطريقة أو بأخرى افتراضيًا.

9 NESH A Guide to Internet Research Ethics (2019), 3, https://www.forskningsetikk.no/en/guidelines/social-sciences-humanities-law-and-theology/a-guide-to-internet-research-ethics/.

10 يُقصد بالبيانات الشخصية أي معلومات تخص شخصًا طبيعيًا محددًا أو يمكن تحديده ("صاحب البيانات") انظر المادة 4 (1) من لائحة حماية البيانات العامة (GDPR).

11 اللجنة الوطنية لأخلاقيات البحث في العلوم الاجتماعية والإنسانية (NESH)، A Guide to Internet Research Ethics، 2.

12 Sold, Abay Gaspar, and Junk, Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities, 52; see also: Farina Madita Dobrick et al., Research Ethics in the Digital Age: Ethics for the Social Sciences and Humanities in Times of Mediatization and Digitization, ed. Farina Madita Dobrick, Jana Fischer, and Lutz M. Hagen (Wiesbaden: Springer VS, 2018), 1.

13 NESH, A Guide to Internet Research Ethics, 2.

وتنشأ مشاكل أخرى عند استخدام بيانات مستمدة من أشخاص عديدين مختلفين لأغراض بحثية.[14] مثلاً، من الصعب أن نضمن قيام 100,000 مستخدم من أصحاب الحسابات على Twitter، على سبيل المثال، بمنح بياناتهم للباحثين ليستخدموها في الوقت المناسب. وفي هذه الحالات، قد يعرض الباحثون على الأفراد خيار إلغاء اشتراكاتهم، ما يسمح لهم بسحب موافقتهم وقتما شاءوا أثناء المشروع البحثي. ويمتاز هذا النهج بأن الباحث لا يضطر إلى الحصول على موافقة جميع الأفراد مسبقًا. ويُستعان بهذا الخيار أيضًا إذا كانت كمية البيانات الشخصية صغيرة نسبيًا أو إذا كانت البيانات مجهولة المصدر. وينبغي أن يتعامل الباحثون دائمًا مع بيانات جُمعت أثناء إجراء دراسة ما وبعد الانتهاء منها بسرية تامة. ولا قيمة لموافقة الأفراد على تحليل بياناتهم أو رفضهم. وينبغي أن يضع الباحث اسمًا مستعارًا للبيانات أو يجعلها مجهولة الاسم في جميع الحالات. ومع ذلك، كثيرًا ما يصعب إخفاء هوية أصحاب البيانات[15] ومن الممكن اكتشافها حتى بعد إخفائها.[16] لذا يجب أن يسأل الباحثُ نفسه أين يخزن البيانات وكيف، وهل البرنامج المستخدم جدير بالثقة، ومدى شمولية سياسة خصوصية بائع البرمجيات، وهل هناك حاجة، مثلاً، إلى برنامج تشفير.

هذا فضلاً عن تطبيق مبدأ الإحسان: على الباحث أن يضمن عدم إلحاق أي ضرر بالمشاركين وتعظيم الاستفادة من الدراسة. ولنفترض أن باحثًا يجري دراسة عن المقاتلين الأجانب، مثلاً، فيجب عليه أن يضمن إخفاء هوية صاحب البيانات بحيث لا يمكن كشفها، مخافة أن يتعرض لملاحقة قضائية أو إدانة عامة. وإذا تعذر ضمان إخفاء الهوية (بسبب خضوع الباحث للمراقبة المستمرة أثناء اجتماعاته مع المشارك أو لأن حذف بيانات المشارك الشخصية يحول دون طرح فرضيات معينة مثلاً)، فقد يتعين إيقاف الدراسة أو إعادة تصميمها.

وبقدر ما يتعلق الأمر بتعظيم الاستفادة وتقليل المخاطر، فليس من السهل تقليل المخاطر في حد ذاته.[17] ومع ذلك، يمكننا تعظيم الاستفادة من البيانات التي جُمعت عبر الإنترنت بأقل جهد أثناء البحث في الموضوعات الرقمية. ومن أسباب ذلك ضعف الاحتمالات القائمة لتوفير البيانات وأكواد إمكانية الاستنساخ (على سبيل المثال، Harvard Dataverse أو GitHub) أو الدوريات العالية الجودة ذات الوصول المفتوح التي تصل إلى شريحة عريضة من الجمهور (مثل Global Studies Quarterly التي أنشأتها رابطة ISA مؤخرًا أو دورية Texas National Security Review الصادرة عن جامعة تكساس في أوستن (UT Austin)).

المبادئ الأخلاقية التي تتعلق بالبعد المجتمعي

تشير المبادئ المتعلقة بالبعد المجتمعي لأي مشروع بحثي إلى العدل و واحترام القانون والمصلحة العامة. ويشير مبدأ العدل إلى أن العلماء يجب أن يضمنوا الموازنة بين التكاليف والمزايا لمختلف الفئات الاجتماعية التي يتناولها مشروع بحثي معين. ويجب ألا تتحمل الأقلياتُ والفئاتُ المستضعفةُ التكاليفَ بينما تتمتع الأغلبية والفئات الثرية في الوقت ذاته بالمزايا.[18]

وينص مبدأ احترام القانون والمصلحة العامة على وجوب مراعاة القوانين وسياسات المواقع ذات الصلة بالبحث (شركات وسائل التواصل الاجتماعي مثلاً) عمومًا.[19] ينطوي البحث الرقمي على مشكلة محورية وهي كثرة المسؤوليات التي يجب مراعاتها وتنوعها، عند جمع بيانات عن المتطرفين السياسيين في بلدان مختلفة مثلاً. ومع ذلك، قد تُنتهك أيضًا شروط الاستخدام في حالات نادرة جدًا. وعلى سبيل المثال، اتخذت جامعة نيويورك قرارًا واعيًا بانتهاك شروط استخدام فيسبوك لجمع البيانات

14 Elizabeth Buchanan, "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL," PLoS ONE 12, no. 12 (2017): 2, https://doi.org/10.1371/journal.pone.0187155.

15 Buchanan, "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL," 4.

16 Matthew J. Salganik, Bit by Bit. Social Research in the Digital Age (New Jersey: Princeton University Press, 2018), 40. والأفضل واللؤلي، ووفقًا للائحة GDPR Recital 26، إخفاء هوية الأشخاص تمامًا.

17 Salganik, Bit by Bit. Social Research in the Digital Age, 298.

18 Salganik, Bit by Bit. Social Research in the Digital Age, 298; NESHA Guide to Internet Research Ethics, 5–6; British Psychological Society, Ethics Guidelines for Internet-mediated Research (2017), 17, www.bps.org.uk/publications/policy-and-guidelines/research-guidelines-policy-documents/research-guidelines-poli.

19 Salganik, Bit by Bit. Social Research in the Digital Age, 300.

حول إستراتيجية الدعاية السياسية على فيسبوك، ربما لأن فيسبوك يواصل منع إمداد الباحثين بالبيانات المطلوبة.[20] وقد تُنتهك شروط الاستخدام التي وضعتها الشركة في هذه الحالة لأن الدعاية السياسية والمعلومات الخاطئة في المجال الرقمي من القضايا المهمة لنزاهة الانتخابات والنهوض بالديمقراطية، وينبغي أن تُستخدم البيانات للصالح العام حصريًا. هذا فضلاً عن أن المصلحة العامة تقتضي أن يناقش الباحثون قراراتهم بشفافية وعلانية.[21] وعندها فقط يصبح الجمهور قادرًا على إجراء مناظرات أخلاقية حول ما يفعله العلماء، ولا مانع من الاستعانة بالآراء المطروحة في هذه المناقشات في تصاميم الأبحاث لتعزيز الشعور بالمسؤولية في المشاريع البحثية وزيادة تركيزها على المحتوى. يُقصد بالشفافية الإفصاح عن مشروع البحث وشرحه للمشاركين في البحث والمصارحة بشأن بطرق جمع البيانات ومعالجتها عند عرض نتائج البحث أو نشرها.

المبادئ الأخلاقية التي تتعلق بالباحثين أنفسهم

من الواضح أن الباحثين جزء من عملية البحث ذاتها؛ لذا يجب أن يهتم الأكاديميون والدوائر الرسمية برفاهيتهم. وهذا الأمر يتعلق بأمن الباحث و/أو سلامته. ويجب أن يُصمَّم البحث تصميمًا يحمي الباحثين أنفسهم، لاسيما إذا كان موضوع البحث حساسًا كالراديكالية. وقد تترتب عليه ثمة مخاطر منها التهديد الجسدي والترهيب بالآخرين، ويجب أن تتضمن سلامة الباحث تقديم الدعم النفسي له أيضًا، لأن التعامل مع المحتوى الترويعي يخضع لحدود معينة. ويجب أن تؤخذ هذه الجوانب في الاعتبار قبل بدء المشروع، وكثيرًا ما تغفل عنها المؤسسات المشاركة في البحث أو لا تضمنها بالكامل.

هناك مسألة أخرى تتعلق بالثقة، وتعمل من منظور الباحث والمبحوث. فمثلاً، على الباحث أن يتساءل إن كان ملف التعريف زائفًا أو لا. وهناك حدود لما يمكن التحقق منه، وكذلك لشفافية هوية المرء (قد يعني الأمن والأمان إخفاء هوية المرء). ويتخذ أكثر المستخدمين أسماءً وهميةً أو يقدمون معلومات خاطئة عن مواقعهم أو يختارون لغات غير لغتهم. وكثيرًا ما يستعين المستخدمون باللغة الإنجليزية، ما يجعل تحديد جنسياتهم أمرًا صعبًا.

وبالإضافة إلى ذلك، يواجه الباحثون تحديات التنقل بين المنصات عند ربط خيط أحد الموضوعات على منصة ما بخيط موضوع آخر على منصة أخرى. هذا فضلاً عن مواجهة تحديات الاختصارات، والتعبيرات المستحدثة، والخلط بين لغات مختلفة وبنية الجُمل المنقوصة التي أضحت سمة مميزة لمحادثات الإنترنت.[22] وأصبح تحليل المحتوى باستخدام برامج التحليل الآلي أشد صعوبة ويطرح تحديات أخرى.[23] وهي تحديات معقدة لن نتغلب عليها إلا بالبحوث المدمجة. وقد يترتب على الدور الذي يتبناه الباحثون في عملية جمع البيانات، سواءً كان فاعلاً أو غير فاعل، عواقب وخيمة تنال من صلاحية تصميم البحث الداخلية وتثير عددًا من الأسئلة الأخلاقية الفرعية. إذا تولى الباحثون دورًا غير فاعل/رقابيًا تمامًا في عملية جمع البيانات في جميع الأوقات، فمن المفترض ألا يكون لهم تأثير على عمليات التواصل المراقبة – وقد يكون هذا الأمر بالغ الأهمية لصحة نتائج البحث. ومع ذلك، كثيرًا ما تكون هناك حدود لأدوار الملاحظة (بتوجيه أسئلة إلى ملف تعريف الباحث مثلاً) وهناك خط رفيع بين الملاحظة بتطفل والملاحظة بدون تطفل.

ولو نظرنا من منظور أخلاقي لرأينا العلاقة التي تربط بين إعدادات الخصوصية وتنفيذ أي مشروع بحثي أيضًا. وإذا اخترنا إعدادات تجعل المحتوى قابلاً للعرض علنًا، فسوف يُعتبر تحليل الباحث لهذه البيانات أقل انتهاكًا لخصوصية الموضوع مما لو تبادل الأصدقاء هذه البيانات فيما بينهم فقط أو حتى مجموعة أصغر منتقاة من بعض

20 "Facebook to researchers: Stop using our data," 2020, https://edition.cnn.com/2020/10/24/tech/facebook-nyu-political-ad-data/index.html.

21 Salganik, Bit by Bit. Social Research in the Digital Age, 300–01.

22 Albert Bifet and Eibe Frank, "Sentiment knowledge discovery in Twitter streaming data," in Discovery Science, ed. Bernhard Pfahringer, Geoff Holmes, and Achim Hoffmann, Lecture Notes in Computer Science (Heidelberg: Springer VS, 2010); Simon Carter, Wouter Weerkamp, and Manos Tsagkias, "Microblog language identification. Overcoming the limitations of short, unedited and idiomatic text," Language Resources and Evaluation 47, no. 1 (2013).

23 انظر عبد الله الرحمون، ماهر، و وينتر، تحليل شفرة الكراهية: استخدام التحليل التجريبي للنصوص في تصنيف المحتوى الإرهابي.

الأشخاص يحددها المستخدم. وعند إجراء البحث ببيانات مستقاة من وسائل التواصل الاجتماعي تظهر الأسئلة الأخلاقية مصحوبة بأسئلة قانونية. ولأننا لا نستطيع تلافي الضرر المحتمل تمامًا ولا توقعه عمومًا، فإن الهدف من التفكير الأخلاقي وتلبية المتطلبات القانونية هو إقامة علاقة متوازنة بين الفوائد المنشودة من البحث والالتزام بالخصوصية.[24] وإذا كان هناك ترابط بين المتطلبات القانونية والاعتبارات الأخلاقية ولا يمكن فهمه إلا إذا جُمعا معًا في حزمة واحدة، يحتاج الباحث إلى تناولهما كلٌ على حدة. ونتناول فيما يلي التوصيات القانونية التي استخلصناها من الأدبيات.

24 Anne Lauber-Rönsberg, "Data Protection Laws, Research Ethics and Social Sciences," in Research Ethics in the Digital Age. Ethics for the Social Sciences and Humanities in Times of Mediatization and Digitization, ed. Farina M. Dobrick, Jana Fischer, and Lutz M. Hagen (Wiesbaden: Springer VS, 2018), 41.

3 مبادئ حماية البيانات المركزية – الباحثون بين الحدود القانونية والتحديات والفرص

تزخر وسائل التواصل الاجتماعي عمومًا، والشبكات الاجتماعية خصوصًا، بأفراد (وجماعات) كثيرًا ما يكشفون قدرًا كبيرًا من المعلومات عن أنفسهم. ومن المعلومات الشخصية التي قد يقدمونها أصلهم العرقي، وآراؤهم السياسية، ومعتقداتهم الدينية والأيديولوجية، وعاداتهم الجنسية، وتوجهاتهم الجنسية، وصحتهم وانتماءاتهم، كعضويتهم في نقابات عمالية معينة، مثلاً. ومن بين هذه المعلومات الشخصية ما قد يثير اهتمام الباحثين الذين يجرون دراسات في مجالات مختلفة. ويجب مراعاة لوائح حماية البيانات عند جمع البيانات الشخصية أو استخدامها، في أي سياق كان. وفيما يلي، نلقي نظرة عامة على الإطار القانوني لحماية البيانات عند إجراء البحوث الاجتماعية التجريبية القائمة على الملاحظة في وسائل التواصل الاجتماعي بناءً على اللائحة العامة لحماية البيانات (GDPR).[25]

وتورد هذه اللائحة العديد من الامتيازات المهمة للبحث العلمي، لكنها لا تقدم أي مبررات معينة لمعالجة البيانات. وكثيرًا ما تُقيَّم شرعية المعالجة التي تخدم الأغراض البحثية على أساس توازن المصالح في كل حالة على حدة. ومن البيانات الشخصية ما يتسم بحساسية خاصة، ومن ثم فإنها تخضع للحماية أكثر من غيرها (مثل المعتقدات الدينية أو الآراء السياسية التي تمثل أهمية كبيرة لفحص المحتوى المتطرف على منصات التواصل الاجتماعي). وقد يأتي مشروع البحث مثقلاً بالقيود أو محملاً بالتحديات والفرص للباحثين. وسوف نناقش فيما يلي مسألة الحصول على الموافقة أو عدم الحصول عليها لما لها من أهمية كبيرة.

اللوائح القانونية التي تنظم البحث في البيانات الشخصية بموافقة أصحابها

تزخر وسائل التواصل الاجتماعي بالكثير من البيانات الشخصية. وإذا كان الوصول إلى هذه المعلومات ممكنًا دون عوائق كبيرة، وتعمَّد الأفرادُ المعنيون نشرها، فما زالت اللائحة العامة لحماية البيانات (GDPR) تحميها باعتبارها بيانات شخصية. ولا مفر من جمع البيانات الشخصية وتحليلها في كثير من المشروعات البحثية. وتورد هذه اللائحة الحماية القانونية المفروضة على هذه المعلومات الشخصية، في الاتحاد الأوروبي.[26] ولا تنص اللائحة العامة لحماية البيانات (GDPR) على تصريح معين لمعالجة البيانات الشخصية لأغراض البحث العلمي، ولكن المواد 5 و 6 و 9 تحديدًا تنظم جواز معالجة البيانات. ووفقًا للائحة العامة لحماية البيانات (GDPR)، يُحظر عمومًا معالجة البيانات الشخصية إلا بنص قانوني صريح يجيزها أو بموافقة الشخص المعني.

ولكل شخص أن يقرر الكشف عن بياناته الشخصية واستخدامها إن شاء، إما بالقبول أو الرفض. ويجب أن يُمنح، في كل حالة على حدة، فرصة ليقرر جواز معالجة بياناته أو لا وشروط معالجتها. ولضمان ذلك، فإن لوائح حماية البيانات التي تتناول الموافقة

25 تسري اللائحة العامة لحماية البيانات (GDPR) اعتبارًا من 25 مايو 2018 في جميع الدول الأعضاء في الاتحاد الأوروبي. والهدف منها هو التوفيق بين قوانين خصوصية البيانات في جميع أنحاء أوروبا.

26 ويشمل نطاق تطبيق اللائحة "التعامل مع" البيانات بجميع أنواعها وصورها، ومن ثم جمعها وتخزينها وهيكلتها وما إلى ذلك. انظر المادة 4 (2) من اللائحة العامة لحماية البيانات (GDPR).

على معالجة البيانات الشخصية تُقصر الموافقة على محتوى معين وبمتطلبات رسمية محددة. وهي على سبيل التحديد، وحسب اللائحة العامة لحماية البيانات (GDPR)، تعيين وتحديد الغرض المقصود من استخدام البيانات، وإمداد صاحب البيانات بمعلومات كافية عن معالجة بياناته، والتأكيد على طوعية الموافقة وإمكانية الرجوع فيها في أي وقت أثناء عملية البحث.

ويُضاف إلى إقرار الشخص بالموافقة جواز قيام الباحثين باستخدام البيانات إذا كان الشخص موضوع البيانات قد نشر بيانات حساسة عن وعي بحساسيتها. وفي هذه الحالة، ترفع المادة 9 (2) (هـ) من اللائحة حظر المعالجة المقرر بموجب الفقرة 1 وتزول عن الشخص موضوع البيانات أي ضرورة خاصة توجب الحماية. وعندئذ يمكن اعتبار قيام الشخص موضوع البيانات بنشر البيانات عن وعي نوعًا من التنازل عن الحماية الخاصة المنصوص عليها في المادة 9. ومع ذلك، وحتى إذا نشر الشخص المعني البيانات، فلن تزول عن البيانات بأكملها الحماية التي تكفها اللائحة العامة لحماية البيانات (GDPR).[27] وفيما تسري المادة 6، على وجه الخصوص، تبقى الحاجة إلى أساس قانوني لمعالجة البيانات قائمة، حتى وإن عُطلت المادة 9 (1).[28]

وهذا يقودنا إلى سؤال: ما المقصود "بنشر" البيانات؟ تعتبر البيانات منشورة إذا أتاحها للجمهور عددٌ من الأشخاص غير محدد دون عائق ملموس يحول دون الوصول إليها. وبالتالي، فيما يخص متطلبات حماية البيانات، هناك جانب محوري آخر يتعلق بنوع وسائل التواصل الاجتماعي التي استُقيت منها البيانات. هل (فروع) وسائل التواصل الاجتماعي التي استُمدت منها مفتوحة أم مغلقة، أم أنها جاءت من وسائل للتواصل الاجتماعي أعدت خصيصًا للأغراض البحثية؟ والمعيار الأساسي الفاصل هنا هو "تقييد الوصول إليها بفتح الحساب وتسجيل بيانات الدخول".[29] ويتمتع المستخدمون، حسب المنصة ذاتها، بإمكانية تحديد الفئة التي يخاطبونها بالمحتوى. ومن بين وسائل التواصل الاجتماعي وسائلٌ أعدت خصيصًا للأغراض البحثية، حيث أثبتت موافقة المستخدم على معالجة بياناته الشخصية أنها حل عملي، ولكن الأمر مختلف في وسائل التواصل الاجتماعي الأخرى. وهنا تكمن أهمية تلبية المتطلبات القانونية قبل معالجة البيانات الشخصية. وهذا ينطبق أيضًا إذا كانت البيانات قد جُمعت من مصادر متاحة للجمهور.[30] علاوة على ذلك، "قد تدخل المعلومات العامة في نطاق الحياة الخاصة حيث تُجمع وتُخزن بطريقة منهجية في ملفات تحتفظ بها السلطات".[31] ويُضاف إلى هذا أن الأفراد يتمتعون أيضًا بحقهم في الخصوصية وإن دخلوا الساحة العامة بكامل إرادتهم. وإن البيانات المستقاة من ساحات التواصل شبه العامة أو حتى المغلقة تحتاج إلى الحماية بقدر أكبر من البيانات المستقاة من الساحات العامة.

ومع ذلك، كما ذكرنا أعلاه، قد يتعرض البحث للخطر في كثير من الأحيان لضرورة الحصول على الموافقة، أو قد يكون الحصول عليها بكل بساطة أمرًا محالاً لكثرة من يجب الحصول على موافقتهم. وهذا الوضع لا يقتصر على الأبحاث التي تتناول الأفراد أو الجماعات الراديكالية أو المتطرفة فحسب، وإنما في العديد من المجالات البحثية الحساسة الأخرى. لهذا السبب، نلجأ إلى اللوائح القانونية التي تنظم البحث في البيانات الشخصية دون موافقة أصحابها.

---

27 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 92.

28 في هذه المرحلة، تجدر الإشارة إلى أن المادة 6 من اللائحة العامة لحماية البيانات (GDPR) يمكن تطبيقها أيضًا في الوقت ذاته مع المادة 9 من اللائحة ذاتها. وتقومان جنبًا إلى جنب معًا ويجب الالتزام بهما.

29 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 96.

30 Ian Brown and Josh Cowls, Check the Web. Assessing the Ethics and Politics of Policing the Internet for Extremist Material, Oxford Internet Institute (2015), 46. تمتاز الساحات العامة بإمكانية الوصول إلى أي شيء دون قيود، لأنها ملتقى الغرباء من كل حدب وصوب. أما "الساحات الخاصة فتتسم بفرض قيود معينة على إمكانية الوصول ... وغياب الغرباء" Anne Nassauer و Nicolas Legewie. "YouTube, Google, Facebook: 21st Century Online Video Research and Research Ethics," Forum: Qualitative Social Research 19, 32, no. 3 (2018).

31 European Court of Human Rights Application, "Rotaru v Romania no. 28341/95," (2000): § 43.

اللوائح القانونية التي تنظم البحث في البيانات الشخصية دون موافقة أصحابها

كثيرًا ما يعتمد البحث على البيانات الشخصية لتحقيق الأهداف البحثية المنشودة، ولهذا وضع المشرعون معايير معينة تحدد الأهلية لإجراء البحوث. وهذا يسمح بفرض قيود على الحق في تقرير المصير المفيد لأغراض البحث العلمي. وإذا استُخدمت البيانات في إجراء تحريات لا تندرج ضمن الفئات المحددة للمادة 9 من اللائحة العامة لحماية البيانات (GDPR)، فإن المادة 6 دون غيرها هي التي تنظم مشروعية معالجتها حصريًا. ولهذا، عند معالجة البيانات الشخصية، يجب أن تطبَّق قاعدة واحدة على الأقل من القواعد المنصوص عليها في هذه المادة. وبالتالي، لا يُسمح بمعالجة البيانات الشخصية دون موافقة صاحبها إلا في ظروف محدودة: على سبيل المثال، إذا لم يكن لها تأثير على المصالح المشروعة للشخص موضوع البيانات على الإطلاق أو إذا كان تنفيذ مشروع البحث ينطوي على مصلحة عامة تفوق المصالح المشروعة للشخص موضوع البيانات ولن يتحقق الغرض من البحث إلا بها أو بمشقة وعناء. وإذا استُوفي هذا الشرط، جاز إجراء البحث دون موافقة الشخص المعني. وكثيرًا ما تعتمد قانونية المعالجة بدون موافقة على الموازنة بين الحق في الخصوصية والفوائد المنشودة من البحث. وعلى أي حال، من الضروري أن نوازن بين المصلحة المرجوة من البحث والمصالح المشروعة لصاحب البيانات.

ووفقًا للمادة 9 (2) (ي) من اللائحة العامة لحماية البيانات (GDPR)، توجد أيضًا أحكام قانونية لمعالجة فئات خاصة من البيانات الشخصية لخدمة أغراض البحث: أولاً، وجود سؤال بحثي مع مفهوم محدد. ويوجب الغرضُ من البحث العلمي على الباحثين أن يثبتوا أنَّ المشروع البحثي المعني يلبي المتطلبات العلمية من حيث بنيته ومحتواه. ثانيًا، على الباحثين أن يثبتوا عدم جدوى المشروع بدون بيانات شخصية ملموسة. لذا ينبغي أن يتوسع الباحثون في تعليل الأسباب الموجبة لجمع البيانات الشخصية اللازمة لمشروع البحث. وعلى سبيل المثال، ينبغي أن يتسأل العلماء في قرارة أنفسهم ما إذا كان إجراءُ البحث ممكنًا ببيانات أقل أو بأنواع أخرى من البيانات. ثالثًا، يجب الموازنة بين المصالح مرة أخرى، مثل كمية البيانات والظروف الخاصة المحيطة بأصحابها. وبالتالي، يجب إيضاح العلة من وراء ترجيح مصلحة البحث (إلى حد كبير) على مصلحة صاحب البيانات في حماية بياناته، لإضفاء الشرعية على معالجة البيانات لصالح أغراض البحث دون موافقة صاحبها.

وتقتضي هذه الغاية مراعاة مبادئ الضرورة والملاءمة والتناسب في معالجة البيانات الشخصية وإقرار لوائح لتنظيم الوصول وضمان استخدام البيانات الشخصية وفقًا للوائح حماية البيانات: أولاً، يجب على الباحثين إثبات أن المشروع يسعى إلى تحقيق غرض مشروع. وصحيحٌ أن البحث قد يُعتبر غرضًا مشروعًا في ذاته عمومًا.[32] ومع ذلك، ينبغي عدم اللجوء إلى معالجة البيانات الشخصية لمشروع بحثي دون موافقة أصحاب البيانات إلا إذا تعذر تحقيق الغرض من البحث بوسائل أخرى.[33] وينبغي أن تُعتبر الضرورةشرطًا آخر من شروط التناسب المسبقة. وإذا تعذر تحقيق الهدف ذاته بإجراء ألطف – أي أقل تعديًا – فمن الضروري اتخاذ إجراء آخر. وينبغي أن يُعتبر اختبار الضرورة الخطوة الأولى التي يجب أن يمتثل لها أي إجراء مقترح لمعالجة البيانات الشخصية. وإذا لم يجتز الإجراء المعني اختبار الضرورة، فلا داعي لفحص مدى تناسبه. وإن ثبت أن الإجراء غير ضروري، وجب تعديله ليلبي متطلبات الضرورة.

يجب أن تكون معالجة البيانات المستقاة عبر الإنترنت دون موافقة صاحبها ملائمة أيضًا. ويتطلب مبدأ الملاءمة ألا يتجاوز المحتوى وشكل العمل المستوى اللازم لتحقيق الأهداف. ولتحديد مدى ملاءمة التدخل، يجب أن يوازن الباحثون بين المبررات القانونية للتدخل (وهذا يعتمد على الفائدة المجتمعية المتوقعة من البحث في الغالب)

32 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 90.

33 Sold, Abay Gaspar, and Junk, Designing Research on Radicalisation using Social Media Content: لوائح حماية البيانات بين التحديات والفرص، 62–63.

وبين التزامهم بحماية من تُنتهك خصوصيته بهذا التدخل. وما أن يوضع هذا الأمر في الاعتبار، يجب أن يثبت الباحثون أيضًا احترامهم تدابير وضمانات حماية أصحاب البيانات، كاستخدام الأسماء المستعارة مثلاً، وفقًا للمادة 89 من اللائحة العامة لحماية البيانات (GDPR).

وعند النظر إلى مشروع البحث من منظور حماية البيانات، نرى جانبًا آخر مهمًا يشير إلى فاعلية الباحث أو سلبيته. ومن الأمور التي تؤثر على متطلبات حماية البيانات مسألة ما إذا كان الباحثون عند جمع البيانات مجرد مراقبين سلبيين – أي ما إذا كانوا قد آثروا عدم التفاعل في جمع البيانات – أم لا. وفي هذه الحالة، لا يقوم الباحث بدورٍ فاعل في أي وقت ولا يدخل في الحديث. ومع أن هذا الدور السلبي في المراقبة يستبعد أيضًا الحصول على الموافقة من البداية،[34] يظل مستوى التدخل متدنيًا دون إحداث أي تأثير على ما يُعلّق عليه أو يُنشر. وفي الوقت ذاته، يعني الانخراط في البحث باتباع نهجٍ فاعل أن الحصول على موافقة لجمع البيانات الشخصية وتحليلها أمرٌ ممكنٌ، ولكنه يخاطر بإنتاج محتوى متداخلاً، (بل) واستباق الحديث أو احتمال التأثير على سلوك الآخرين في النشر.

وينبغي توفير المزيد من الحماية لمن تعذر الحصول على موافقتهم. ووفقًا للمادة 89 (1) من اللائحة العامة لحماية البيانات (GDPR)، يجب اتخاذ تدابير فنية وتنظيمية تكفل احترام مبدأ اقتصاد البيانات على وجه الخصوص. ومن الجوانب المهمة في هذا الصدد الاقتصاد في كمية البيانات التي تُجمع وحصر معالجتها في نطاق القدر اللازم للغرض منها فحسب، وتحديد فترة تخزينها، ووضع لائحة تنظم إمكانية الوصول إليها. وهذا هو الوضع المنشود حسب ما تنص عليه الجملتان 3 و 4 من المادة 89 (1) من اللائحة العامة لحماية البيانات (GDPR)، بقدر ما تستطيع البيانات المجهولة المصدر أو المستعارة تحقيق الأغراض المرجوة منها. وبقدر ما يتعلق الأمر بأرشفة البيانات، تفرض مفاهيم الأدوار وحلول الوصول الآمن نفسها بكل وضوح.[35]

علاوة على ذلك، حتى إذا كانت معالجة البيانات الشخصية (بموجب موافقة أو نص قانوني) ممكنة، يجب اتخاذ التدابير الفنية والتنظيمية التي تكفل تحقيق الغرض من حماية البيانات. ويمكن تحقيق ذلك بتخزين المعرِّفات والبيانات في أماكن منفصلة على سبيل المثال. وبالإضافة إلى ذلك، يجب تخصيص البيانات لغرض محدد. وسوف يُحتفظ بالمعلومات وتُفحص ملائمتها للغرض الذي جمعت من أجله.

34 Kerstin Eppert et al., Navigating a Rugged Coastline: Ethics in Empirical (De-)Radicalization Research, core-nrw Netzwerk für Extremismusforschung in Nordrhein-Westfalen (Bonn, 2020), 9, https://www.bicc.de/fileadmin/Dateien/Publications/other_publications/Core-Forschungsbericht_1/CoRE_FP_1_2020.pdf.

35 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 94.

4 نظرة عامة على مصادر البيانات وسياسات المنصات ودور الباحثين – التفاعل والتوصيات

يجب على المستخدمين والباحثين أن يمتثلوا للاتفاقات القانونية الخاصة بالمنصة المعنية وأن يضعوها في الاعتبار، فضلاً عن المبادئ الأخلاقية ولوائح حماية البيانات، وكذلك القيود الفردية الأخرى عند استخدام برامج الغير. وفي واقع الأمر، تستعين المنصات الرائدة بسياسات مختلفة، هذا من ناحية، ومن ناحية أخرى كثيرًا ما تكون هذه السياسات طويلة أو يصعب فهمها، وتشكل بذاتها تحديًا آخر. وفيما يلي نقدم لمحة موجزة عن أهم السياسات لشركات التكنولوجيا الرائدة، ونستخلص منها بعض التوصيات العامة.

تويتر

عززت تويتر قدرة مستخدميها على التحكم في بياناتهم من خلال سياسة خصوصيتها الجديدة التي تتوافق مع اللائحة العامة لحماية البيانات (GDPR)، ودخلت حيز التنفيذ في مايو 2018. وحيث أنها تسري على جميع المستخدمين أيًا كانت مواقعهم، يبدو أن الحماية التي تكفلها اللائحة العامة لحماية البيانات (GDPR) سوف تمتد لجميع المستخدمين في كافة أنحاء العالم. وما أن يبدأ المستخدمون مطالعة التغريدات، تجمع تويتر منهم معلومات عن عنوان الآي بي (IP) ونوع الجهاز المستخدم. وبطبيعة الحال، تُستخلص البيانات وتُجمع عندما يرسل المستخدم تغريداته، ويتفاعل مع المستخدمين الآخرين، ويعيد تغريداته، وإعجاباته وما إلى ذلك. ووفقًا لسياسة خصوصية تويتر، يُستبعد محتوى المراسلات المباشرة من جمع البيانات ومعالجتها. وتُستخدم البيانات التي جُمعت في اقتراح التغريدات وتتبع الحسابات وتوجيه الدعاية. وتوفر تويتر لمستخدميها عناصر التحكم، إلى حد ما، في أنواع البيانات التي يُسمح بجمعها. وعلى سبيل المثال، يستطيع المستخدمون تحويل حساباتهم إلى عامة أو خاصة وتشغيل وسم الآخرين للصور أو إيقافه. ويستطيع المستخدمون أيضًا تنزيل المعلومات التي شاركها المستخدم على تويتر. مثلاً، يتمتع المستخدمون بفرصة "التواصل على تويتر أيضًا، باستخدام طرق عامة، من خلال تغريدات محمية ورسائل مباشرة"، بالإضافة إلى التغريدات العامة التي "يستطيع أي شخص في أي مكان في العالم مشاهدتها والبحث فيها فورًا".[36] ويمكن أيضًا استخدام تويتر تحت اسم مستعار ثم "تُحفظ البيانات لحوالي 18 شهرًا، أو حتى يُحذف الحساب".[37] ومع إطلاق API v2 في أغسطس 2020، "يسهل تويتر على الشركات والأكاديميين ومطوري برامج الغير إمكانية البناء على منصته":[38] ويوفر لمطوري الغير إمكانية الوصول إلى ميزات طالما افتقدها عملاؤه، بما في ذلك "سلاسل المحادثات، وإدراج نتائج الاستطلاع في التغريدات، وتثبيت التغريدات في ملفات التعريف، وتصفية الرسائل غير المرغوب فيها، وتعزيز إمكانات التصفية الشاملة وتعيين لغة الاستعلام البحثي".[39] هذا بالإضافة إلى إمكانية الوصول في الوقت الفعلي إلى دفق التغريدات.

36 Twitter, Twitter Privacy Policy (2020), https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-june-18th-2020/Twitter_Privacy_Policy_EN.pdf.

37 Identity Guard, "What You Need to Know About Twitter's Privacy Policy," (2018), https://www.identityguard.com/news/twitter-privacy-policy.

38 "Twitter launches new API as it tries to make amends with third-party developers," 2020, https://www.theverge.com/2020/8/12/21364644/twitter-api-v2-new-access-tiers-developer-portal-support-developers.

39 "Twitter ändert API zugunsten von Third-Party-Entwicklern," 2020, https://onlinemarketing.de/technologie/twitter-api-third-party-entwicklern.

وأعادت تويتر تنظيم الوصول إلى واجهة برمجة التطبيقات (API) على ثلاثة مستويات: كان "الاستماع إلى المحادثة العامة وتحليلها" ممكنًا خلال فترة الوصول المبكر.[40] ولكنها لم تطلق إلا مستوى الوصول الأساسي المجاني فقط، ما يقيد عدد مرات استدعاء المطورين لواجهة برمجة التطبيق (API)، ويبقى أن نرى ما يظهر للباحثين من تغييرات وفرص. ويُعد التواصل المفتوح ميزة أساسية يمتاز بها تويتر على غيره من الشبكات الاجتماعية. ويستطيع من شاء أن يبحث عن التغريدات الفردية والمحادثات الكاملة ويعرضها، سواءً كان مستخدمًا أو لديه متابعة متبادلة مع الشخص المعني على تويتر. وبالتالي، لا يتمتع الباحثون بإمكانية الوصول إلى البيانات الشاملة وغير المفلترة فحسب ولكن إلى حماية البيانات أيضًا. ومن شروط البحث في تويتر ألا يضر استخدامُ البيانات بمصالحه الاقتصادية. ويحظر استغلال التغريدات في إنشاء قواعد البيانات الكبيرة وإثرائها وتوزيعها، ولو كان لأغراض غير تجارية.[41] ولا يمكن وزن النتائج أو مقارنتها لافتقار الباحثين للمعلومات عن أنشطة تويتر ككل.

فيسبوك

لم يقتصر فيسبوك على تغيير سياسته في حماية البيانات وفقًا للائحة العامة لحماية البيانات (GDPR) فحسب، على غرار تويتر، وإنما طبقها على جميع عملائه في كافة أنحاء العالم. ويجمع فيسبوك وانستغرام وماسنجر وغيرهم من المنتجات والميزات الأخرى التي يوفرها فيسبوك أنواعًا مختلفة من المعلومات بناءً على تفاعل المستخدم مع منتجات فيسبوك. ومن بينها المعلومات والمحتوى المُحمَّل، وبيانات شبكات المستخدم الاجتماعية (كالحسابات، والمجموعات، والهاشتاجات وغير ذلك مما يتفاعل معه المستخدم)، ومعلومات الاستخدام وبيانات عن مشتريات المنصة الداخلية، وكذلك بيانات عن تفاعل المستخدمين الآخرين مع محتوى المستخدم وملفات تعريفه. هذا فضلاً عن جمع بيانات عن الأجهزة المتصلة بفيسبوك أو انستغرام، بما في ذلك سمات الأجهزة وحركات المؤشر وموفري خدمة الإنترنت وشركات الهاتف وإعدادات الأجهزة. ويستخدم فيسبوك هذه البيانات لتحسين منتجاته وتوجيه المحتوى وتقديم توصيات بشأن الحسابات. ويجعل هذه البيانات متاحة لعملاء الغير. ولا تتم مشاركة هذه البيانات مع المعلنين فحسب، ولكن أيضًا مع الغير الذي يشغل تطبيقاته على فيسبوك أو يستخدم خدماته. وكما هو الحال في منصات التواصل الاجتماعي الأخرى، يستطيع المستخدمون ضبط إعداداتهم على تقييد جمع البيانات، وتنزيل ما جُمع عنهم من بيانات والوصول إليها. وتخضع بعض البيانات لمستويات خاصة من الحماية: يستطيع المستخدمون أن يختاروا تقديم معلومات على فيسبوك حول آرائهم الدينية أو السياسية أو صحتهم أو أصولهم العرقية أو الإثنية أو معتقداتهم الفلسفية أو عضويتهم النقابية.[42] ومع أن فيسبوك قد أدخل بعض التحسينات على الخصوصية مؤخرًا،[43] لا تزال واجهة المستخدم غير شفافة بدرجة كافية. هذا فضلاً عن أن المستخدمين يمكنهم بالكاد أن يحدوا من جمع البيانات، على عكس الدعاية المخصصة. ويتيح فيسبوك لمستخدميه إمكانية الوصول إلى معلوماتهم على فيسبوك، بما فيها صورهم ومنشوراتهم وردود أفعالهم وتعليقاتهم باستخدام ما يسمى بأداة "الوصول إلى معلوماتك". وبالإضافة إلى ذلك، يستطيع المستخدمون تنزيل نسخة من المعلومات الخاصة بهم من على فيسبوك باستخدام أداة "تنزيل معلوماتك".

ويوفر فيسبوك للباحثين والأكاديميين المعلومات والمحتوى اللازميْن لإجراء بحوثهم.[44] ورداً على فضيحة Cambridge Analytica في عام 2018، وعد فيسبوك بإطلاق مبادرة بحثية لمنح الأكاديميين إمكانية الوصول إلى بياناته دون مساس بخصوصية معلومات المستخدمين. وعلى الرغم من إطلاق مركز جديد للوصول

40 "Twitter API v2: Early Access," 2020, https://developer.twitter.com/en/docs/twitter-api/early-access.

41 Michael Beurskens, "Legal questions of Twitter research. Twitter and society," in Digital Formations, ed. Katrin Weller (New York et al.: Peter Lang, 2014).

42 "Data Policy," 2020, https://www.facebook.com/policy.php.

43 "Mit mehr Kontrolle über die eigene Privatsphäre ins neue Jahrzehnt," 2020, https://about.fb.com/de/news/2020/01/mehr-kontrolle-uber-die-eigene-privatsphare/.

44 "Facebook Research. Supporting exciting and innovative research through meaningful engagements," 2020 لمزيد من التفاصيل انظر.

إلى البيانات يمنح الباحثين فرصة الاطلاع على جميع مجموعات البيانات المتاحة على فيسبوك، لم يسلم فيسبوك من الانتقاد بعد لإخفاقه في إمداد الباحثين بالدعم الكافي.[45]

Google

يبدو أن غوغل، على عكس فيسبوك وتويتر، تمتنع حتى الآن عن تطبيق سياسة خصوصيتها المنقحة، التي تتماشى مع اللائحة العامة لحماية البيانات (GDPR)، على الأقاليم الواقعة خارج الاتحاد الأوروبي. وعلى سبيل المثال، ظهرت تقارير أن المستخدمين في المملكة المتحدة سوف يُحرمون من الحماية التي تكفلها اللائحة العامة لحماية البيانات (GDPR) وعليهم الآن أن يقبلوا تخزين بياناتهم، على عكس الاتحاد الأوروبي، في الولايات المتحدة الأمريكية إذا اقتضت الضرورة تخزينها على خوادم وفقًا لقواعد اللائحة العامة لحماية البيانات (GDPR)، ما يعني أن مستويات حماية البيانات تختلف باختلاف التوجيهات التي يضعها مقدمو الخدمة أنفسهم عمومًا. وحيث أن يوتيوب مجرد ركن من أركان إمبراطورية غوغل التي تتألف من عشرات التطبيقات والخدمات ونظام لتشغيل الهاتف المحمول، فمن المرجح أن تقوم الشركة بجمع بيانات عن مستخدميها أكثر من تويتر أو فيسبوك مثلاً. ومن بين الأشياء التي تجمعها يوتيوب بيانات عن تفاعل المستخدمين وتعليقاتهم وتحميلات الفيديوهات ومعدلات مشاهدة الفيديوهات وغير ذلك الكثير. وبينما يشارك يوتيوب بيانات المستخدمين بالفعل مع الغير ممن ينشرون إعلانات على الموقع ويوفر واجهة لبرمجة التطبيقات (API)، ظهرت تأكيدات صريحة أن يوتيوب لا يبيع البيانات للغير، مثل شركات التواصل الاجتماعي الأخرى. ويوفر يوتيوب للمستخدمين الراغبين في الوصول إلى بياناتهم خيارات عديدة لمراجعة بياناتهم، بل وحذفها أيضًا.

تيك توك

أما TikTok فإنها، بخلاف العديد من شركات التواصل الاجتماعي الكبيرة، تتعامل مع سياسة الخصوصية في إطار نهج يقوم على التصنيف الإقليمي. فيما يخص أوروبا، على سبيل المثال، هناك توجيهات بوضع متطلبات معينة من اللائحة العامة لحماية البيانات (GDPR) في الاعتبار. أما الولايات المتحدة الأمريكية والبلدان الأخرى، فلها توجيهات أخرى. ويُجمع المحتوى ويُحلّل، بالإضافة إلى نقاط البيانات المعتادة (أنشطة الاستخدام، ومعلومات الأجهزة، وبيانات الموقع، ودليل الهاتف عند الوصول إليه، ومعلومات عن محتوى الغير المشترك على المنصة). ويبدو أن TikTok لا توفر للباحثين إمكانية الوصول إلى واجهة برمجة التطبيقات (API) ولا أي وسيلة أخرى لجمع البيانات بطريقة قانونية. ولكن وجد متخصصو تكنولوجيا المعلومات طرقًا بديلة لإنشاء واجهات غير رسمية لبرمجة التطبيقات وجمع بيانات عن المستخدمين وآرائهم وتفاعلاتهم.[46]

تليغرام

وتحتفظ تليغرام، على غرار TikTok، بسياسة مستقلة لخصوصية المستخدمين الأوروبيين. وتقوم تليغرام، كمنصة للاتصالات، بتخزين المعلومات الأساسية فقط عن المستخدمين (رقم الهاتف، وعنوان البريد الإلكتروني، واسم المستخدم، وما إلى ذلك). وتُخزَّن الدردشات العادية (التي تسمى "بالمحادثات السحابية") أيضًا بين المستخدمين والمحادثات الجماعية. ويقال إن الدردشات السرية مشفرة بالكامل، ولا يراها إلا المستخدمون المشاركون فيها. ولا توفر تليغرام للباحثين أية وسائل لجمع البيانات وتحليلها، مثل واجهة برمجة التطبيقات (API). ومع ذلك، أنشأ الباحثون كاشطة خاصة بهم للوصول إلى القنوات العامة والتفاعلات والرسائل لخدمة الأغراض

45 انظر على سبيل المثال "Facebook needs to share more with researchers," World View, 2020, https://www.nature.com/articles/d41586-020-00828-5.

46 "How to Collect Data from TikTok," 2020, https://towardsdatascience.com/how-to-collect-data-from-tiktok-tutorial-ab848b40d191.

البحثية.[47] وفيما يُعد الكشط أداة جذابة لتقييم الشبكات الاجتماعية لخدمة الأغراض البحثية، فإنه محل خلاف شديد، من حيث الجوانب القانونية والاعتبارات الأخلاقية، كوسيلة لاسترجاع البيانات.[48]

توصيات عامة

من هذا المنظور العام نرى صورة متشعبة في أفضل أحوالها: تختلف كمية البيانات المتاحة للباحثين باختلاف المنصة. وعمومًا، تحتفظ المنصات بالحق في البيانات، وفي معالجتها أو نقلها. ومع ذلك، فإن بعض المنصات، وليس كلها، حددت نقاط الوصول والاختصاصات للاستخدام العلمي بوضوح. وسيكون انفتاح العديد من شركات التكنولوجيا على العلم أمرًا مرغوبًا أيضًا باستخدام واجهات لبرمجة التطبيقات (APIs) تتسم بالوضوح والاستدامة والاتساق ومن حيث عمليات البحث (عن مجموعات البيانات التي تم إنشاؤها باستخدام مصطلح بحثي مثلاً) أيضًا. وعلى تويتر، مثلاً، لا تُدرج التغريدات المرتبطة بالردود في نتائج البحث. و Data Grants (منح البيانات)[49] برنامج تجريبي لمنح الباحثين إمكانية الوصول إلى البيانات العامة والتاريخية، لكن تقتصر إمكانية الوصول هذه على عدد قليل من المشاريع التي يختارها تويتر.

تحتل البحوث والتحقيقات التي تتناول التطرف السياسي العنيف على الإنترنت في كثير من الأحيان مكانة مميزة في جداول أعمال مختلف المؤسسات السياسية والمجتمعية وكذلك شركات التكنولوجيا. وتخضع قواعد البيانات التي تحتوي على بيانات المستخدمين، كما ناقشنا في هذا التقرير من قبل، للوائح حماية البيانات في الدولة المعنية. وتحد من مشاركة البيانات الحالية، لأسباب وجيهة، مع علماء آخرين محليًا، وعلى وجه الخصوص دوليًا. وفي هذا السياق، حري بنا أن نتساءل عن إمكانية استخدام الباحثين للبيانات التي جُمعت بهدف إجراء المزيد من التحليلات والمشاريع. وفيما تنطبق اللائحة العامة لحماية البيانات (GDPR) على جميع الدول الأعضاء في الاتحاد الأوروبي، تفتقر قواعد التعاون مع الشركاء الخارجيين إلى الوضوح، على الرغم من تعزيز التقارب بين المعايير في مختلف أنحاء العالم وأن شركات التكنولوجيا مثل فيسبوك تطبق القواعد العالمية وتروج لها.

وهو اتجاه واعد في خضم القيود المفروضة عليها. وعلاوة على ذلك، معظم لوائح حماية البيانات، بما فيها اللائحة العامة لحماية البيانات (GDPR)، تغدق امتيازات معينة على الباحثين. وإذا توازنت بعض المبادئ في استراتيجيات حماية البيانات بطريقة منهجية وشفافة من أجل مشاريع بحثية معينة وفي إطار مناقشة جادة مع مسؤولي حماية البيانات (ومع المنصات، في بعض الحالات)، أصبحت التحليلات اللازمة وإمكانية الوصول إلى النتائج لخدمة المزيد من الباحثين ممكنة في جميع الحالات تقريبًا. ومع ذلك، تُفرض قيود على استنساخ النتائج إذا استُرجعت البيانات من ساحات مشفرة وفي ظل استخدام هويات مستعارة أو مخفية. ويتفاقم الأمر مع الإسراع بحذف المحتوى المتطرف أكثر فأكثر. ولو استُضيف المحتوى المتطرف المحذوف في مكان آمن، فربما وجد الباحثون الذين يمكنهم الوصول إلى هذا المحتوى أنفسهم قادرين على طرح تحليلات أعم وأشمل. وكثير من الأمور ينبغي مناقشتها، في هذا الصدد، مع جهات النشر الأكاديمي والنشر على الإنترنت، ومنها ما يتعلق، مثلاً، بضمان درجة عالية من الصلاحية الخارجية لأي دراسة منشورة دون تقديم دوافع تحفز على انتهاك متطلبات حماية البيانات وأخلاقيات البحث. وإن لم يتحقق هذا التوازن، ضعُفت وتضاءلت النتائج المرجوة من البحث.

والتعاون الوثيق بين شركات التكنولوجيا والباحثين في تبادل المعرفة والتعاون التقني والبحوث المشتركة مربحٌ لكل منهما. ويستطيع الباحثون أن يعظموا استفادتهم كثيرًا من الإبلاغ، مثلاً، عن المحتوى المُشكِل، ولكن ينبغي أن يتعاملوا بحسم مع الآثار المترتبة على الإبلاغ عن هذا المحتوى وفقًا للمعايير الأخلاقية الموضحة أعلاه. وعلى الشركات التقنية أن تطبق آليات شفافة في التعامل مع المحتوى المبلغ عنه وأن

47 Jason Baumgartner et al., The Pushshift Telegram Dataset (2020).

48 Sebastian J. Golla and Max von Schönfeld, „Kratzen und Schürfen im Datenmilieu – Web Scraping in sozialen Netzwerken zu wissenschaftlichen Forschungszwecken," Kommunikation und Recht (2019).

49 انظر "Introducing Twitter Data Grants," 2014, https://blog.twitter.com/engineering/en_us/a/2014/introducing-twitter-data-grants.html.

تكون على دراية بما يواجه الباحثين من تحديات أخلاقية وعملية في هذا الشأن. ومن الحلول الممكنة توفير خيار يمكِّن الباحثين من التعامل مع المحتوى المبلغ عنه بطريقة مختلفة عن غيره: ليس هناك ما يمنع الشركات من مراقبة هذا المحتوى عن كثب دون حذفه. ومن أمثلة التعاون الناجح بين شركات التكنولوجيا والباحثين منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT). ومن أهم أهداف منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT) "تمكين الباحثين من دراسة الإرهاب ومكافحة الإرهاب، بما في ذلك طرح وتقييم أفضل الممارسات للتعاون بين أصحاب المصلحة المتعددين ومنع إساءة استخدام المنصات الرقمية".[50] ويقوم منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT) بتمويل الشبكة العالمية للتطرف والتكنولوجيا (GNET) لعقد حوارات – مفتوحة وبالغة الأهمية – عظيمة القيمة، وينبغي أن تستمر دون انقطاع لتعزيزها.

وهناك أدوات عديدة أو على الأقل مبادرات تُطلَق عبر المنصات تهم الباحثين الذين يتعاملون مع المحتوى العام من وسائل التواصل الاجتماعي. ومن بين هذه الأدوات CrowdTangle[51]، التي تسمح بتحليل المحتوى العام في وسائل التواصل الاجتماعي وتجميعه في صورة تقارير. وتتيح CrowdTangle إمكانية الوصول إلى توقيت المنشور ونوع المساهمة (فيديو، صورة، نص) ومعلومات عن الصفحة أو الحساب العام أو المجموعة العامة التي نُشرت فيها وعدد التفاعلات (على سبيل المثال، معلومات عن "الإعجاب"، وردود الفعل، والتعليقات، وعدد مرات مشاركة المساهمة) أو مشاهدات الفيديو التي حققتها، فضلاً عن الصفحات العامة أو الحسابات التي شاركتها. وهي بداية جيدة، لكنها تنتظر المزيد من التطوير والتوسع. ومن الانتقادات التي وُجهت إلى CrowdTangle أنها لا تفيد الباحثين أكثر من غيرهم لصعوبة رصدها الأنماط التي لم تُحدد مسبقًا.[52] وعلاوة على ذلك أن العديد من المشاريع البحثية يحتاج إلى بيانات غير عامة على وجه التحديد. والباب مفتوح للمزيد من المبادرات، إلى جانب CrowdTangle أو إصداراتها المعدلة المحتملة. وفيما يتنقل المستخدمون من منصة إلى أخرى، وتتوسع الشبكات المتطرفة عبر منصات عديدة ويتزايد انتشار المحتوى عبر مختلف المنصات، تُعد الأدوات الشاملة بمثابة دفعة لمزيد من البحث، وتفسح المجال أمام تخصصات أخرى وعلماء آخرين لتحليل مختلف التحديات الاجتماعية والسياسية التي تولد من رحم ديناميكيات التطرف على الإنترنت: ننتظر المزيد من هذه المبادرات بكل الترحاب.

50 "Global Internet Forum to Counter Terrorism: Evolving an Institution," 2020, https://www.gifct.org/about/.

51 ولا تُتاح إمكانية الوصول الشامل إلى CrowdTangle إلا لشركات ومؤسسات معينة تفي بالمتطلبات اللازمة. ولكن امتداد CrowdTangle Link Checker Chrome Extension متاح لجميع الأطراف المعنية. ويظهر الامتداد عدد مرات مشاركة عنوان URL والصفحات العامة أو الحسابات التي شاركت عنوان URL وبيانات التفاعل مع هذه المنشورات.

52 Hegelich, "Facebook needs to share more with researchers".

5 ملاحظات ختامية

من الباحثين مَن يتجنب التعامل مع بيانات مستمدة من وسائل التواصل الاجتماعي أو يشرع في مشاريع بحثية دون اهتمام كافٍ بأمور حماية البيانات والمبادئ الأخلاقية – وربما لا يهتم بها أصلاً. ودفعًا للحيرة التي يقع فيها الباحثون، طرحنا في هذا التقرير رؤى حول أهم الاعتبارات الأخلاقية ومتطلبات حماية البيانات التي يواجهها العلماء عند التعامل مع البيانات الشخصية المستقاة من وسائل التواصل الاجتماعي، وتناولنا التحديات والقيود التي يفرضها هذا العمل. وبالرغم من هذه العقبات، لا يمكننا وما كان لنا أن نتجنب تحليل البيانات المستقاة من العالم الرقمي. وطالما كانت الصلة بين عالم الانترنت ودنيا الواقع وثيقة. ولن نفهم ما يطرأ على هذين العالمين من ظواهر إلا إذا جمعنا بينهما. وهدفنا هو تشجيع غيرنا من الباحثين على التعامل مع البيانات المستقاة من وسائل التواصل الاجتماعي. وأشار التقرير أيضًا إلى الفرص المتاحة لتحقيق هذا الهدف.

ويجب على الباحثين، كلما أمكن، أن يقوموا بواجباتهم ومسؤولياتهم وتخفيف المخاطر التي تواجه موضوعاتهم البحثية. وينبغي أن يحصل الباحثون أيضًا على الموافقة المستنيرة كلما أمكن، وأن يحذفوا المعلومات التي يسهل تحديدها بسهولة ويحتفظوا بمعلومات الحصول على الموافقة حتى نشر المشروع. ويجب أن يضع الباحثون في اعتبارهم المتطلبات الأخلاقية ومتطلبات حماية البيانات في جميع مراحل المشروع البحثي (من بدايته حتى نشر نتائجه ومعالجة البيانات بعد الانتهاء من المشروع).

وتثير البيانات المستقاة من منصات مختلفة فضول الباحثين. وتختلف سياسات الخصوصية التي تطبقها كل شركة من شركات التكنولوجيا باختلاف المنصات ذاتها. ومثلما نرى بعض التداخل – على سبيل المثال، تطبق فيسبوك وتويتر متطلبات اللائحة العامة لحماية البيانات (GDPR) على مستخدميهما على مستوى العالم – ترى بعض الاختلافات أيضًا، وقد ناقشنا بعضها في هذه المقالة. ومع أن السنوات الأخيرة شهدت اهتمامًا متزايدًا بوضع سياسات سهلة الاستخدام، لأسباب أهمها زيادة المتطلبات والضغط على مشغلي المنصة، كثيرًا ما لا تظهر الفرص المتاحة للباحثين بوضوح. وهناك حاجة ملحة للمزيد من التطوير فيما يتعلق بالحقوق ومنح الباحثين إمكانية الوصول عبر المنصات. وإن كانت هناك تطورات إيجابية، نحتاج من شركات التكنولوجيا أن تقدم للباحثين المزيد من التنازلات. وينبغي في الوقت ذاته أن يعظم الباحثون استفادتهم من العروض الحالية التي تقدمها شركات التكنولوجيا؛ وذلك وفقًا للمبادئ الأخلاقية والقانونية الأساسية التي تناولها هذا التقرير وتُستخدم استخدامًا صحيحًا في تصميمات البحث، وهذه القيود أضعف من عوامل التمكين.

المشهد السياسي

هذا القسم بقلم أرميدا ڤان ريج و لوسي توماس، وهما باحثتان مشاركتان في معهد السياسات في كينجز كوليدج لندن. ويلقي نظرة عامة على المشهد السياسي وعلاقته بهذا التقرير.

مقدمة

أثار البحث عن المحتوى الإرهابي و/أو المتطرف على مدى عقود طويلة أسئلةً صعبةً حول الجوانب القانونية والأخلاقية والعملية للباحثين والحكومات والنشطاء ووكالات إنفاذ القانون على حد سواء. ومن ناحية، هناك تشريعات لحماية البيانات، فضلاً عن القيود التي يجب على الباحثين الالتزام بها عند التعامل مع البيانات الشخصية. ومن ناحية أخرى، هناك تشريعات تتعلق بمكافحة الإرهاب وطرق استخدام البيانات الإرهابية والمتطرفة في خدمة أغراض البحث. وهذا الأمر يدفع الباحثين لخوض غمار مجال شائك يعرضهم وغيرهم للخطر.

وسوف نسلك، في هذا التقرير، نهجًا مغايرًا لما عهدناه في تقارير سابقة، حيث نتناول المشهد السياسي بشأن حماية البيانات الشخصية في ثمانية من البلدان التسعة أولاً. ثم يلقي التقرير نظرة عامة متعمقة على مشهد مكافحة الإرهاب في الدولة التاسعة، وهي المملكة المتحدة، وسوف يتناول بعض الأسئلة الصعبة التي قد تواجه الباحثين المهتمين بالبحث في موضوع الإرهاب.

حماية البيانات في منصات التواصل الاجتماعي: مواجهة التحديات وتقييم التطورات الجديدة

كندا

يتولى مكتب مفوض الخصوصية الكندي (OPC) المسؤولية عن حماية حقوق خصوصية بيانات الأفراد وتعزيزها. ومن اختصاصات مكتب مفوض الخصوصية الكندي (OPC) فرض الامتثال لقانون الخصوصية (Privacy Act) الذي ينظم طريقة تعامل الوكالات الحكومية الفيدرالية مع البيانات الشخصية، ولقانون حماية المعلومات الشخصية والوثائق الإلكترونية (PIPEDA) الذي يتناول القطاع الخاص. وقانون حماية المعلومات الشخصية والوثائق الإلكترونية (PIPEDA) قانون فيدرالي، أما مقاطعات ألبرتا وكولومبيا البريطانية وكيبيك فلديها قوانين مستقلة لخصوصية البيانات تتشابه في جوهرها.[53]

وعمومًا، يُلزم قانون حماية المعلومات الشخصية والوثائق الإلكترونية (PIPEDA) المؤسسات الخاصة بـ "الحصول على موافقة الشخص عند جمع معلوماته الشخصية أو استخدامها أو الكشف عنها" والامتثال للمتطلبات التشريعية لحماية تلك البيانات. وبموجب قانون حماية المعلومات الشخصية والوثائق الإلكترونية (PIPEDA)، يجب أن تلتزم الشركات بعشرة "مبادئ عادلة للمعلومات" تضمن حماية حقوق بيانات الأفراد، بما فيها المساءلة والموافقة وتقييد جمعها وتقييد استخدامها والكشف عنها والاحتفاظ بها ودقتها وضمانات حمايتها.[54]

53 'PIPEDA in brief,' Office of the Privacy Commissioner of Canada. حاليًا: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

54 المرجع نفسه.

وبالإضافة إلى بحوث مسح الأفاق وتحديد نطاق التقنيات الجديدة وتأثيرها على حقوق بيانات الكنديين،[55] فإن قانون حماية المعلومات الشخصية والوثائق الإلكترونية (PIPEDA) يخول مكتبَ مفوض الخصوصية الكندي (OPC) صلاحيات تنفيذية لمواجهة خروقات حماية البيانات. وتشمل هذه الصلاحيات التنفيذية صلاحيات إجراء تحقيقات وغرامات مالية – يمكن فرض غرامات تبلغ 100,000 دولار على الشركات التي لا تبلغ مكتب مفوض الخصوصية الكندي (OPC) بانتهاكات البيانات. وبالمثل في نيوزيلندا، نجد هذه الغرامة أقل كثيرًا من نظيرتها في القطاعات الأخرى، مثل مبلغ اللائحة العامة لحماية البيانات (GDPR) البالغ 20,000,000 يورو (أو نحو 4٪ من إجمالي أعمالها السنوية).

وفي نوفمبر 2020، اقترح وزير الابتكار والعلوم والصناعة الكندي تشريعًا جديدًا لحماية البيانات الشخصية. وأشارت الوزارة، في بيان صحفي، إلى جائحة فيروس كورونا كسياق يستدعي تحديث قوانين الخصوصية وتطويرها، لأن التكنولوجيا يستخدمها كثيرون للتواصل فيما بينهم.[56]

وسوف يضع التشريع المقترح، قانون تنفيذ الميثاق الرقمي (DCIA)، قانونًا جديدًا للخصوصية للقطاع الخاص بما في ذلك منصات وسائل التواصل الاجتماعي. وسوف يطرح قانون تنفيذ الميثاق الرقمي (DCIA) صلاحيات رقابية وتنفيذية أقوى كثيرًا للتعامل مع الانتهاكات – تبلغ 5٪ من الإيرادات أو 25 مليون دولار – بالإضافة إلى فرض الالتزام بالشفافية على الشركات المعنية باستخدامها للخوارزميات والذكاء الاصطناعي. ويعني قانون تنفيذ الميثاق الرقمي (DCIA) أن "الشركات عليها أن تلتزم بالشفافية بشأن كيفية استخدام هذه الأنظمة في طرح تنبؤات أو توصيات أو قرارات مهمة بشأن الأفراد. وسوف يتمتع الأفراد أيضًا بحقهم في مطالبة الشركات بشرح كيفية قيام نظامها الآلي باتخاذ القرارات أو طرح التنبؤات أو التوصيات وشرح كيفية حصولها على المعلومات."[57] وفي قانون غانا لحماية البيانات لعام 2012 بندٌ مماثل (انظر أدناه).

المفوضية الأوروبية

ركزت المفوضية الأوروبية على تنظيم الجوانب العديدة للخدمات الرقمية، في إطار مبادرة المفوضية الأوروبية "لتهيئة أوروبا للعصر الرقمي". وهذا يشمل حماية البيانات الشخصية والخصوصية. وخصوصية البيانات في الاتحاد الأوروبي تنظمها اللائحة العامة لحماية البيانات (GDPR). ودخلت اللائحة العامة لحماية البيانات (GDPR) حيز التنفيذ في عام 2016. وتعمل على "حماية حق المواطنين الأساسي في حماية بياناتهم كلما استخدمت سلطات إنفاذ القانون الجنائي بياناتهم الشخصية في إنفاذ القانون" و "سوف تضمن على وجه الخصوص حماية البيانات الشخصية للضحايا والشهود والمشتبه باقترافهم جرائم على النحو الواجب وسوف تسهل التعاون عبر الحدود في مكافحة الجريمة والإرهاب".[58]وتُطبَّق، بحزم، على الشركات العاملة في السوق الأوروبية، بغض النظر عن مقراتها. وهذا يعني أن الشركات مثل غوغل عليها أيضًا الالتزام بمبادئ اللائحة العامة لحماية البيانات (GDPR) وإلا فسوف تتعرض للغرامة و/أو المقاضاة.

وإلى جانب اللائحة العامة لحماية البيانات (GDPR)، أنشئت أيضًا هيئة European Data Protection Supervisor للإشراف على حماية البيانات. وهي هيئة مستقلة تابعة للاتحاد الأوروبي، ومكلفة بضمان الامتثال والتعامل مع الشكاوى بموجب اللائحة العامة لحماية البيانات (GDPR).[59]

---

55 'Research,' Office of the Privacy Commissioner of Canada. حاتم: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/

56 'New proposed law to better protect Canadians' privacy and increase their control over their data and personal information,' Government of Canada، 17 نوفمبر 2020. متاح: https://www.canada.ca/en/innovation-science-economic-development/news/2020/11/new-proposed-law-to-better-protect-canadians-privacy-and-increase-their-control-over-their-data-and-personal-information.html

57 'Fact Sheet: قانون تنفيذ الميثاق الرقمي، 2020' Government of Canada. متاح: https://www.ic.gc.ca/eic/site/062.nsf/eng/00119.html

58 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

59 انظر https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

بصرف النظر عن حماية حقوق المواطنين، منحت اللائحة العامة لحماية البيانات (GDPR) أيضًا السلطات المعنية الأدوات اللازمة لضمان الامتثال وتعزيز المساءلة لمن يتعاملون مع البيانات الشخصية. ومنذ عام 2018، عندما احتاجت جميع الدول الأعضاء في الاتحاد الأوروبي إلى تفعيل اللائحة العامة لحماية البيانات (GDPR)، قُدمت آلاف الشكاوى، وصدرت مئات الغرامات بسبب انتهاك اللائحة. وربما كان من أشهرها تغريم فرنسا شركة غوغل بسبب "انعدام الشفافية وعدم كفاية المعلومات وعدم صدور موافقة سليمة فيما يتعلق بتخصيص الإعلانات" وإصدار غرامة بلغت 50,000,000 يورو.[60]

وبالإضافة إلى اللائحة العامة لحماية البيانات (GDPR)، يوجد أيضًا توجيه Data Protection Law Enforcement Directive لإنفاذ قانون حماية البيانات. ويتعلق التوجيه 680/2016 بمعالجة البيانات الشخصية من قبل جهات إنفاذ القانون إذا كان الشخص مشتبهًا بارتكاب جريمة أو شاهدًا أو ضحية لجريمة.[61] ولكن، لا يمكن الفصل بوضوح بين اللائحة العامة لحماية البيانات (GDPR) والتوجيه 680/2016 في نطاقات تطبيقهما، وخطورة هذا الأمر أن إحدى عمليات معالجة البيانات قد تندرج تحت اللائحة العامة لحماية البيانات (GDPR) في الدول الأعضاء في الاتحاد الأوروبي، بينما تندرج تحت هذا التوجيه في أخرى.[62]

وأخيرًا، لا ننسى توجيه الاتحاد الأوروبي بشأن أمن الشبكات وأنظمة المعلومات (NIS) الذي يطرح تدابير قانونية لتعزيز الأمن السيبراني.[63]وهذا الأمر يتعلق تحديدًا بالآتي: تعزيز استعداد الدول الأعضاء؛ وزيادة التعاون بين الدول الأعضاء؛ وتحسين البنية التحتية الحيوية عبر الاتحاد الأوروبي.[64]

وفيما يخضع تنظيم خصوصية البيانات، إلى حد ما، لحدود الاختصاص القضائي، تسعى المفوضية الأوروبية أيضًا إلى تنفيذ لائحة الخصوصية الإلكترونية (لتحل محل توجيه الخصوصية الإلكترونية).[65] وتسعى هذه اللائحة بدورها إلى حماية خصوصية المواطنين على منصات الإنترنت، مثل تطبيقات المراسلة. وفيما اعتمد البرلمان الأوروبي لائحة الخصوصية الإلكترونية، توقفت المناقشات على مستوى المجلس الأوروبي.[66] وذهب البعض إلى أن هذا التركيز على حماية البيانات يتعارض مع تشريعات الاتحاد الأوروبي لمكافحة الإرهاب.[67]

فرنسا

طبقت فرنسا، كدولة عضو في الاتحاد الأوروبي، اللائحة العامة لحماية البيانات (GDPR) في مايو 2018 وتوجيه أمن الشبكات وأنظمة المعلومات (NIS) في عام 2019. وما أن ينتهي المجلس الأوروبي من المفاوضات الجارية بخصوص توجيه الخصوصية الإلكترونية، على نحو ما ناقشنا أعلاه، فسوف ينظم هذا التوجيه حماية بيانات المواطنين جنبًا إلى جنب مع اللائحة العامة لحماية البيانات (GDPR) وتوجيه أمن الشبكات وأنظمة المعلومات (NIS).

ومن متطلبات توجيه أمن الشبكات وأنظمة المعلومات (NIS) إنشاء هيئة لحماية البيانات. وهي اللجنة الوطنية للمعلوماتية والحريات (CNIL) في فرنسا. وأصدرت اللجنة الوطنية للمعلوماتية والحريات (CNIL) حتى الآن غرامات على غوغل وغيرها لانتهاك اللائحة العامة لحماية البيانات (GDPR).

60 انظر https://www.bbc.co.uk/news/technology-46944696
61 انظر https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
62 انظر https://www.tandfonline.com/doi/pdf/10.1080/13600869.2017.1370224?needAccess=true، p.253
63 انظر https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
64 المرجع نفسه.
65 انظر https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0568:FIN:EN:PDF
66 انظر https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform
67 انظر https://www.coe.int/en/web/commissioner/-/human-rights-in-europe-should-not-buckle-under-mass-surveillance

غانا

قننت غانا تشريعات خصوصية البيانات الرئيسية وأدرجتها في قانون حماية البيانات الذي تم إقراره في عام 2012. وأنشئت بموجب هذا القانون، على غرار دول أخرى مثل كندا ونيوزيلندا، لجنة حماية البيانات (DPC) التي تتمتع بصلاحيات رقابية وتنفيذية لضمان الامتثال للمسؤوليات المقررة بموجب القانون.[68]

ويتناول قانون حماية البيانات لعام 2012 مراقبي البيانات في القطاعين العام والخاص، ويلزمهم بالالتزام بثمانية مبادئ لحماية البيانات، منها المساءلة وتحديد الغرض منها والمصارحة.[69] وتتمتع لجنة حماية البيانات (DPC)، على غرار البلدان الأخرى، بصلاحية فرض غرامات على مراقبي البيانات الذين ينتهكون المسؤوليات المنصوص عليها في هذا القانون.

من أبرز الجوانب المبتكرة في قانون حماية البيانات في غانا، لا سيما أن إقراره يعود إلى عام 2012، بندٌ يمنح الأفراد الحق في التحرر من اتخاذ القرارات المؤتمتة. ويعني هذا البند أن "ما يتعلق بك من قرارات مهمة بناءً على بياناتك الشخصية ينبغي أن يكون لها مدخلات بشرية ويجب ألا تُستخرج بطريقة آلية، ما لم توافق أنت على ذلك."[70] وهذا النموذج حديث ويعتمد على موافقتك على معالجة البيانات بطريقة آلية وخوارزمية، ولكن تترتب عليه عواقب بعيدة المدى فيما يتعلق بطرق وصول الباحثين إلى بيانات التواصل الاجتماعي ومعالجتها باستخدام البرامج المختلفة. ومع أن هذا البند يتعلق حاليًا بالمعلومات التي "تؤثر إلى حد كبير على الفرد"،[71] إذا تحركت الحكومة الغانية لتعزيز هذه الفقرة، فهذا قد يعني أن الباحثين سيواجهون صعوبة في استخدام برامج كشط البيانات الآلية.

ولكن قانون حماية البيانات لعام 2012 يقوض حاليًا حقوق بيانات المواطنين ببندٍ ينص على أن "البيانات الشخصية التي تُعالَج لأغراض البحث ... يجوز الاحتفاظ بها إلى أجل غير مسمى."[72] وعلاوة على ذلك، إذا "تمت معالجة البيانات وفقًا للشروط ذات الصلة"، فإن "البيانات الشخصية التي تُعالَج لأغراض البحث فقط تُعفى من أحكام هذا القانون."[73] وهذا يعرض الحقوق المكفولة لبيانات الأفراد لخطر شديد لأن الباحثين يمكنهم استيفاء الحد الأدنى من متطلبات حماية البيانات ومعالجة البيانات بطريقة غير أخلاقية. ويعني هذا التعريف الغامض والفضفاض لكلمة "بحث" أن حقوق بيانات الأفراد قد تتعرض للخطر بسهولة نسبية.

اليابان

ينص قانون حماية المعلومات الشخصية لعام 2003 (APPI) على الأحكام المتعلقة بحماية البيانات في اليابان. وتقع مسؤولية فرض الامتثال لقانون حماية المعلومات الشخصية (APPI) على لجنة حماية المعلومات الشخصية (PPC) التي تأسست في عام 2016 لتعزيز مركزية السلطات التنظيمية المنفصلة سابقًا.

وتتمتع لجنة حماية المعلومات الشخصية (PPC) بمستوى من الصلاحيات الرقابية والتنفيذية أقل من المتوسط: قد تفضي انتهاكات البيانات إلى الغرامات والسجن. ومع ذلك، نجد أن غرامات هذه الانتهاكات منخفضة للغاية – تصل إلى 300,000 ين ياباني (أعلى قليلاً من 2,000 جنيه إسترليني، أو حوالي 2,800 دولار).[74] ولا يشدد قانون حماية المعلومات الشخصية (APPI) أيضًا على فرض أي التزامات مباشرة على الكيانات التي تعالج البيانات الشخصية، وإنما يوفّع تدابير إشرافية وإرشادية خفيفة.

---

68 انظر https://www.dataprotection.org.gh/

69 'The Data Protection Principles,' Data Protection Commission. متاح: https://www.dataprotection.org.gh/data-protection/data-protection-principles

70 'Data Protection for Individuals,' Data Protection Commission. متاح: https://www.dataprotection.org.gh/data-protection/data-protection-for-individuals

71 Data Protection Act 2012, s.41. متاح: https://www.dataprotection.org.gh/index.php/resources/downloads/data-protection-act/38-data-protection-act-2012-act-843

72 البند نفسه، s.65.

73 المرجع نفسه.

74 قانون حماية المعلومات الشخصية 2003، s.56. متاح: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

وهذا مهم لاسيما للبحوث الأكاديمية، لأن النطاق الإقليمي لقانون حماية المعلومات الشخصية (APPI) يمتد إلى خارج اليابان، حيث يُلزم كل من يتعامل مع بيانات تتعلق بأفراد يابانيين – حتى لو كان هذا التعامل معها من خارج اليابان – بالالتزام بهذه التدابير الخفيفة فقط.

وفي عام 2020، تمت مراجعة وتعديل قانون حماية المعلومات الشخصية (APPI)، وترتبت على ذلك عواقب مهمة. وعلى عكس الاتجاه العالمي العام نحو تعزيز الحقوق المكفولة لبيانات المواطنين، تخفف تعديلات عام 2020 كثيرًا من الالتزامات الواقعة على الجهة التي تعالج البيانات. وفيما يخص المعلومات التي تمت معالجتها بطريقة مستعارة، فقد يتغير الغرض من استخدام البيانات في غير نطاق استخدامها الأصلي، ولم يعد يسري الالتزام بإخطار لجنة حماية المعلومات الشخصية (PPC) بانتهاك البيانات ولم يعد للأفراد حق الوصول إلى بياناتهم أو تصحيحها أو طلب وقفها.[75]

وفي انتكاسة أخرى لحقوق بيانات الأفراد، تم إعفاء الباحثين أيضًا من قانون حماية المعلومات الشخصية (APPI)، لأنه "لا يسري إلا على الأشخاص أو الكيانات التي تتعامل مع المعلومات الشخصية في سياق أعمالها."[76] وهذا يعني، في واقع الأمر، أن المواطنين اليابانيين ممن تُتاح بياناتهم للباحثين ليعالجوها ليس لديهم من الحقوق إلا القليل جدًا.

نيوزيلندا

أما في نيوزيلندا، فيتولى مكتب مفوض الخصوصية (OPC) مسؤولية حماية المعلومات والبيانات الشخصية. وأنشيء المكتب في عام 1993 في إطار قانون الخصوصية للعام نفسه، وهو أول تشريع فعلي ينظم البيانات الشخصية في نيوزيلندا. ويتحكم هذا التشريع في كيفية "جمع المعلومات الشخصية واستخدامها والكشف عنها وتخزينها ومنح حق الوصول إليها".[77] ومهام مكتب مفوض الخصوصية (OPC) تفاعلية واستباقية: لا يحقق في الشكاوى المتعلقة بانتهاكات الخصوصية ولا يفرض الامتثال لقانون الخصوصية فحسب، وإنما يقوم المفوض بمراقبة تطورات التقنيات الناشئة لاستقراء تأثيرها المحتمل على خصوصية الأفراد أيضًا.[78]

في ديسمبر 2020، دخل تشريع جديد حيز التنفيذ في نيوزيلندا يحمي المعلومات الشخصية: قانون الخصوصية لعام 2020. واقتُرح هذا القانون الجديد "ردًا على الطريقة التي أحدثت بها التكنولوجيا ثورة في التعامل مع البيانات الشخصية"،[79] حيث طرأ على طبيعة البيانات الشخصية وحجمها تغيير لا نكاد نستوعبه منذ عام 1993. ولو وضعنا ما سبق في الاعتبار، وجدنا أن التغيرات التي طرأت على قانون 1993 قليلة إلى حد ملحوظ؛ وهذا مَردُّه، في رأي المفوض الحالي، إلى "أن قانون الخصوصية تشريع محايد من الناحية التكنولوجية ويسلك نهجًا قائمًا على المبادئ لتعزيز مرونته في مواجهة التغيرات التكنولوجية".[80]

إن التغيير الرئيسي في القانون الجديد حماية البيانات الشخصية لمواطني نيوزيلندا في الخارج: لا يمكن الآن "الكشف عن المعلومات في الخارج ما لم تكن هناك ضمانات مماثلة للقانون النيوزيلندي".[81] ولقانون عام 2020 "تأثير خارج الحدود

75 'Japan – Data Protection Overview,' Data Guidance. متاح: https://www.dataguidance.com/notes/japan-data-protection-overview

76 المرجع نفسه.

77 'What is personal information and the Privacy Act?,' Data.govt.nz. متاح: https://www.data.govt.nz/manage-data/privacy-and-security/what-is-personal-identifiable-information-and-the-privacy-act/

78 'What we do,' Office of the Privacy Commissioner. متاح: https://www.privacy.org.nz/about-us/what-we-do/

79 'Input of the New Zealand Human Rights Commission: OHCHR Report on the Right to Privacy in the Digital Age,' United Nations Human Rights Office of the High Commissioner، 10 ابريل 2018. متاح: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/HRC_NewZealand.pdf

80 'Media Release: Privacy Act turns 25,' Office of the Privacy Commissioner، 19 فبراير 2018. متاح: https://www.privacy.org.nz/assets/Uploads/2018-02-19.pdf

81 'Privacy Act 2020: One Small Step for New Zealand, but No Giant Leaps in Sight,' Equal Justice Project، 31 أغسطس 2020. متاح: https://www.equaljusticeproject.co.nz/articles/37tbkho3ex74g87sw2n6yz6beyso4a2020

الإقليمية" مدرج فيه بوضوح، لتخضع أي شركة تعمل في نيوزيلندا لالتزامات حماية البيانات، ولو لم يكن لها وجود مادي هناك.[82] ونقاط الاختصاص القضائي هذه مثيرة للاهتمام، حيث إن العديد من شركات التكنولوجيا ووسائل التواصل الاجتماعي الكبرى مقراتها في الخارج، لا سيما في الولايات المتحدة الأمريكية حيث قوانين حماية البيانات فيها أضعف. وفيما تتبنى العديد من الدول تشريعات مماثلة، يزداد الضغط الدولي على الولايات المتحدة الأمريكية لتشديد قوانين خصوصية بياناتها لمواكبة الالتزامات الخارجية.

ويمنح قانون خصوصية عام 2020 أيضًا مكتب مفوض الخصوصية (OPC) صلاحيات تنفيذية أوسع، بما فيها زيادة حد الغرامة الأقصى الموقَّع على انتهاك مبادئ الخصوصية من 2,000 دولار إلى 10,000 دولار. أما في السياق الدولي، فنجد هذه الغرامة أقل كثيرًا من نظيرتها في القطاعات الأخرى، مثل مبلغ اللائحة العامة لحماية البيانات (GDPR) البالغ 20,000,000 يورو (أو نحو 4٪ من إجمالي أعمالها السنوية)، أو 10,000,000 دولار كحد أقصى في أستراليا. ويُضاف إلى هذا أن القانون النيوزيلندي الجديد أخفق في مراعاة "حق النسيان" الوارد في اللائحة العامة لحماية البيانات (GDPR)، والذي يجوز للأفراد بموجبه أن يطلبوا حذف المعلومات الشخصية.[83] وهذا الحق مهم لاسيما إذا وضعنا في اعتبارنا العلاقة بين أخلاقيات البيانات وبين البحوث، إذ يحق للمستخدمين الذين ينشرون محتوى متطرفًا على منصات وسائل التواصل الاجتماعي – المحتوى الذي يمكن استخدامه في أغراض البحث – حذف هذا المحتوى.

المديرية التنفيذية للجنة الأمم المتحدة لمكافحة الإرهاب

أما داخل منظومة الأمم المتحدة، فتندرج حماية البيانات في نطاق عمل مؤتمر الأمم المتحدة للتجارة والتنمية (أونكتاد). ولقد ناقش أونكتاد الحاجة إلى الموازنة بين حماية البيانات والمراقبة وما يترتب عليها من تحديات. وطرح توصيفًا للوضع الراهن، عقب إحالة قضية كبرى إلى محكمة العدل الأوروبية، وظهور "اتجاه إلى فرض شروط وقيود على عملية المراقبة في أي نظام لحماية البيانات في أوروبا، وقد يخلّف هذا الأمر آثارًا جانبيةً على السلطات القضائية التي تلتزم التزامًا تامًا بالقانون الأوروبي".[84]

ولا عجب أن الاختصاص القضائي مجال بالغ الصعوبة، لا سيما إذا تعلق الأمر بحماية البيانات عبر الإنترنت. وأشار مؤتمر أونكتاد إلى أن اللائحة العامة لحماية البيانات (GDPR) بها بند، في المادة 3، يتجاوز الحدود الإقليمية، ويسعى في واقع الأمر إلى ضمان "حماية البيانات المحلية" التي تستهدف السكان المحليين، بغض النظر عن موقع الشركة.[85]

الولايات المتحدة

ليس للولايات المتحدة الأمريكية قانون فيدرالي محوري للخصوصية، بخلاف غيرها من البلدان. وإنما لديها العديد من قوانين خصوصية البيانات التي تركز على جوانب منفصلة من خصوصية البيانات – على سبيل المثال، تتمتع البيانات الصحية بحماية يكفلها قانون Health Insurance Portability and Accountability Act (نقل التأمين الصحي والمساءلة) لعام 1996، وتخضع البيانات الشخصية التي تحتفظ بها الحكومة لقانون الخصوصية (US Privacy Act) الأمريكي لعام 1974.

82 'Privacy 2.0: Key changes in the Privacy Act 2020,' Office of the Privacy Commissioner, 16 يونيو 2020. متاح: https://www.privacy.org.nz/blog/key-changes-in-the-privacy-act-2020/

83 'Privacy Act 2020,' Equal Justice Project، 31 أغسطس 2020. متاح: https://www.equaljusticeproject.co.nz/articles/37t bkho3ex74g87sw2n6yz6beyso4a2020

84 انظر https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf، p.16.

85 المرجع نفسه، p.20.

وليس لخصوصية البيانات الشخصية ولا البيانات على الإنترنت لائحة فيدرالية تنظمها بحزم في الولايات المتحدة الأمريكية. وفي الولايات المتحدة، يعد الإنترنت نوعًا ما من الغرب المتوحش التنظيمي، حيث يستطيع الأفراد والجماعات والمنظمات والشركات الوصول إلى البيانات ومعالجتها دون تنظيم محدد لحقوق البيانات.

والطريقة الوحيدة لحماية حقوق بيانات الأفراد على منصات التواصل الاجتماعي، في الوقت الحالي، عبر مفوضية التجارة الفيدرالية (FTC). وفي عام 2019، مثلاً، تمكنت مفوضية التجارة الفيدرالية (FTC) من توقيع غرامة ضخمة بلغت 5,000,000,000 دولار أمريكي على فيسبوك لانتهاكها الخصوصية في إطار فضيحة Cambridge Analytica.[86] وحققت مفوضية التجارة الفيدرالية (FTC) مع فيسبوك وفرضت عليها غرامة بموجب صلاحياتها المنصوص عليها في المادة 5، والتي تتعلق "بالأفعال أو الممارسات الجائرة أو الخادعة". وشارك فيسبوك معلومات المستخدمين الشخصية مع تطبيقات الغير التي نزَّلها "أصدقاء" المستخدمين، ونظرًا لأن العديد من المستخدمين لم يكونوا على دراية بهذه الممارسات ولم يلجأوا إلى التراجع عنها، كان الأمر بمثابة فعل جائر أو مخادع.[87] وهذه نقطة قانونية مهمة، لأنها تعني أن الشركة إذا لم تكشف عن معلومات حول معالجة بياناتها أو معالجتها، فلا يمكن تحميلها المسؤولية تجاه بند "الأفعال أو الممارسات الجائرة أو الخادعة".

أقرت بضع ولايات، وأهمها كاليفورنيا، تشريعات لحماية خصوصية بيانات المستهلكين. ويحظى تنظيم حماية البيانات في كاليفورنيا بأهمية كبيرة لأنها مقر العديد من وسائل التواصل الاجتماعي وشركات التكنولوجيا الكبرى. وكان قانون California Online Privacy Protection Act (حماية الخصوصية على الإنترنت في كاليفورنيا) لعام 2004 أول قانون يطالب مواقع الويب بنشر سياسات خصوصيتها، ويمتد بحسم إلى أي موقع ويب يستطيع سكان كاليفورنيا الوصول إليه، ما يُلزم جميع مواقع الويب الأمريكية تقريبًا بالامتثال.

دخل قانون كاليفورنيا لخصوصية المستهلك (CCPA) حيز التنفيذ في 1 يناير 2020. ويُعد قانون كاليفورنيا لخصوصية المستهلك (CCPA) علامة فارقة لحماية البيانات في الولايات المتحدة الأمريكية كونه يسري على "الشركات الربحية التي تمارس نشاطًا تجاريًا في كاليفورنيا" أو تلبي المتطلبات الأخرى المتعلقة بالإيرادات وبيانات أهل كاليفورنيا. وهذا يعني، من الناحية العملية، أن كبرى شركات التكنولوجيا ووسائل التواصل الاجتماعي تندرج في نطاق قانون كاليفورنيا لخصوصية المستهلك (CCPA). ويكفل قانون كاليفورنيا لخصوصية المستهلك (CCPA) للأفراد حقهم في معرفة المعلومات الشخصية التي تُجمع عنهم، وحقهم في حذف هذه المعلومات، وحقهم في التراجع عن بيع معلوماتهم الشخصية. وعلى الشركات إخطار المستهلكين بشرح ممارسات خصوصيتها.[88]

ويشير إقرار قانون كاليفورنيا لخصوصية المستهلك (CCPA) والغرامة التي وقعتها مفوضية التجارة الفيدرالية (FTC) على فيسبوك إلى رغبة سياسية في الولايات المتحدة الأمريكية لحماية حقوق بيانات الأفراد. وفي فبراير 2020، اقترحت السناتور كيرستن جيليبراند قانونًا شاملاً لحماية البيانات قد ينتهي إلى إنشاء وكالة تنفيذية فيدرالية مستقلة.[89] وهذا لا يرقى إلى مستوى ضمان حقوق والتزامات معينة تعزز خصوصية جميع الأمريكيين، ولكنه يشير إلى أن الولايات المتحدة الأمريكية قد تتحرك نحو إقرار تشريعات فيدرالية.

86 Julia Carrie Wong, 'Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports,' The Guardian، 12 يوليو 2019. متاح: https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations

87 'FTC Imposes $5 Billion and Sweeping New Privacy Restrictions on Facebook,' Federal Trade Commission، 24 يوليو 2019. متاح: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

88 'California Consumer Privacy Act,' State of California Department of Justice. متاح: https://oag.ca.gov/privacy/ccpa

89 'A run-down of US Sen. Gillibrand's proposed Data Protection Act,' International Association of Privacy Professionals، 21 فبراير 2020. متاح: https://iapp.org/news/a/an-run-down-of-sen-gillibrands-proposed-data-protection-act/

البحث في المحتوى المتطرف في المملكة المتحدة: استراتيجية Prevent وتشريعات مكافحة الإرهاب والتطورات السياسية

في أعقاب الهجمات الإرهابية في 11 سبتمبر 2001 في مدينة نيويورك والبنتاغون في الولايات المتحدة الأمريكية، شددت دول غربية عديدة إجراءاتها الأمنية الداخلية سعيًا لمنع وقوع أي هجمات على ترابها. وازداد اهتمام سياسة مكافحة الإرهاب في الغرب بمفهوم الراديكالية – أن يميل الأفراد شيئًا فشيئًا نحو القيم الإرهابية، ثم ينتهي بهم المطاف إلى تبنيها بل وتنفيذ هجمات عنيفة لأسباب إرهابية. وتُعزى هذه الراديكالية إلى مجموعة واسعة من العوامل الاجتماعية والفردية: التعرض للأيديولوجيات، والتضحية، والعزلة، والتنشئة الاجتماعية، والشبكات الاجتماعية، والإنترنت، وأوجه القصور في الروابط الأسرية، والصدمات، والحرمان الاجتماعي والاقتصادي النسبي، و "ثقافات العنف".[90] وبالنظر إلى العدد الهائل من "الطرق المؤدية إلى التطرف" المحتملة، أضحت الحكومات "تعتقد أنها تستطيع استباق الهجمات الإرهابية في المستقبل من خلال مجموعة من التدخلات في الحياة اليومية."[91]

وفي عام 2003، أطلقت وزارة الداخلية البريطانية استراتيجية Prevent ضمن إستراتيجيتها الأوسع لمكافحة الإرهاب، CONTEST. وبعد مراجعة Prevent أعيد إطلاقها في عام 2011، لاستهداف الأفراد "المعرضين" للراديكالية،[92] لا سيما داخل المؤسسات المدنية مثل المدارس ومقدمي رعاية الأطفال المسجلين والجامعات والكليات والسجون ودوائر مراقبة السلوك والرعاية الصحية والخدمات الاجتماعية وإنفاذ قوانين الهجرة. وتحتل استراتيجية Prevent "مساحة ما قبل الجريمة"[93] – لأنها تتدخل قبل حدوث أي نشاط إجرامي على أمل عرقلة مسار الراديكالية.[94]

وتركز استراتيجية Prevent على "تقديم الدعم وإعادة التوجيه للأفراد المعرضين لخطر، أو في طور الإعداد/التهيؤ لنشاط راديكالي إرهابي قبل ارتكاب أي جريمة".[95] ومن خلال تأطير استراتيجية Prevent باعتبارها إجراءً وقائيًا وليست عملاً تجريميًا، وضعت هذه الاستراتيجية كبرنامج وقائي وليس قمعي. ويترتب على تأطيرها بهذه الطريقة تأثيرٌ يؤدي إلى وضع مسؤولية تفعيل استراتيجية Prevent على عاتق المؤسسات المدنية. وهذه المؤسسات، شأنها شأن الجامعات، ملزمة بتوقع حالات الراديكالية المحتملة ومتابعتها والتدخل فيها ضمن واجبات الرعاية التي تنهض بها. وهذا يعني أيضًا أن الموظفين وأرباب العمل يبحثون عن عدد هائل ومعقد ومبهم من المؤشرات التي تشير إلى أن شخص ما عرضة للراديكالية. ولا عجب أن تتخذ المؤسسات نهجًا شديد الحذر في هذه البيئة.

وركزت استراتيجية Prevent، في سنواتها الأولى، في الجامعات على المجتمعات الطلابية، وخاصة الطلاب البريطانيين المسلمين. وبدأت المؤسسات في التدقيق في المحاضرات والفعاليات العامة وفعاليات المجتمع الطلابي للامتثال لاستراتيجية Prevent وتجنب أي غموض حول أي مظاهر لتمجيد المعتقدات المتطرفة في الحرم الجامعي. وهناك أمثلة لا حصر لها من الطلاب المسلمين الذين استُهدفوا واستُجوبوا بطريقة جائرة في الحرم الجامعي تحت رعاية استراتيجية Prevent،[96] ومنهم طالبٌ أحيلَ إلى فريق الأمن في جامعة ستافوردشاير لأنه قرأ كتابًا في إطار برنامج

90 Katherine E. Brown & Tania Saeed (2015), 'Radicalization and counter-radicalization at British universities: Muslim encounters and alternatives,' Ethnic and Racial Studies, vol. 38 no. 11, pp.1952–68.

91 المرجع نفسه.

92 HM Government 'Prevent Strategy'، يونيو 2011. متاح: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

93 David Goldberg, Sushrut Jadhav & Tarek Younis (2017), 'Prevent: What is Pre-Criminal Space?', British Journal of Psychology Bulletin, vol. 41 no. 4, pp.208–11.

94 والعجيب أن مصطلح "ما قبل الجريمة" صاغه فيليب ك. ديك، مؤلف قصة الخيال العلمي القصيرة Minority Report. انظر: Goldberg, Jadhav & Younis, pp.208–11.

95 Charlotte Heath-Kelly and Erzsébet Strausz, 'Counter-terrorism in the NHS: Evaluating Prevent Duty Safeguarding in the NHS,' University of Warwick. متاح: https://warwick.ac.uk/fac/soc/pais/research/researchcentres/irs/counterterrorisminthenhs/project_report_60pp.pdf

96 'The Impact of Prevent on Muslim Communities: A Briefing to the Labour Party on how British Muslim Communities are Affected by Counter-Extremism Policies,' The Muslim Council of Britain، فبراير 2016. متاح: http://archive.mcb.org.uk/wp-content/uploads/2016/12/MCB-CT-Briefing2.pdf;
Barbara Cohen and Waqas Tufail, 'Prevent and the normalization of Islamophobia,' Islamophobia: Still a challenge for us all, Runnymede Trust. متاح: https://core.ac.uk/download/pdf/161895664.pdf

دراسته العليا عن الإرهاب والجريمة والأمن العالمي.[97] وتم إلغاء أو تعديل ما يقرب من 2,500 فعالية في حوالي 300 جامعة (وهناك متحدثون ألغيت دعوتهم، مثلاً) في 2017-2018.

والصورة معقدة إذا تعلق الأمر بالباحثين الأكاديميين الذين يدرسون التطرف والإرهاب. ويظهر التعرض للمحتوى والقيم المتطرفة والإرهابية مباشرًا وأشد وضوحًا، لأن البحث غالبًا ما يتضمن الوصول إلى المحتوى الإرهابي والمتطرف وجمعه، مثل البيانات الرسمية الصادرة عن الجماعات الإرهابية، والدعاية الإرهابية (بما فيها الوسائط المرئية)، ومنشورات وسائل التواصل الاجتماعي التي تدعم وجهات النظر المتطرفة ولوحات الرسائل عبر الإنترنت وما إلى ذلك. ولاسيما أن البحث الذي يركز على جمع البيانات "من الميدان"، مثل المقابلات الشخصية مع الإرهابيين المدانين أو الأفراد الراديكاليين، يعني أن الباحث على اتصال مستمر مع من تبين أن لديهم معتقدات متطرفة أو إرهابية.

وهذا يفتح بابًا لأسئلة مثيرة للاهتمام عن طبيعة المخاطرة في البحث: هل لنا أو علينا أن نفهم أن الباحثين الأكاديميين عرضة للراديكالية؟ ما الآثار المترتبة على ذلك من منظور قانوني وسياسي؟ ما تأثير هذا على البحث والباحثين؟

أهم تشريعات المملكة المتحدة لمكافحة الإرهاب، لصلتها بالبحث في التطرف، هي قوانين الإرهاب Terrorism Acts لعامي 2000 و 2006. تنص المادتان 57 و 58 من قانون عام 2000 على حيازة المواد التي "تثير شكوكًا معقولة بأن حيازته [هكذا] كانت لغرض مرتبط بارتكاب عمل إرهابي أو التحضير له أو التحريض عليه"،[98] أو أن تلك المعلومات "من المحتمل أن تكون مفيدة لشخص يرتكب أو يعد لعمل إرهابي".[99] وبعبارة أخرى، تعتبر حيازة أي معلومات أو مواد تتعلق بالتطرف أو الإرهاب جريمة، لا سيما إذا كانت هذه المعلومات يمكنها أن تساعد الأفراد أو الجماعات في تجنيد الآخرين أو جعلهم راديكاليين، أو تنفيذ هجمات عنيفة.

ويقوم قانون الإرهاب (Terrorism Act) لعام 2006 على جرائم الحيازة المنصوص عليها في قانون عام 2000 ويتوسع فيها الآن لتشمل نشر هذه المواد (المادة 1) أيضًا ويجرم تمجيد الإرهاب (بما في ذلك بحيازة هذه المواد ونشرها؛ المادة 2). وتشير المادة الأولى إلى الأفراد أو الجماعات الذين يعتزمون "بطريقة مباشرة أو غير مباشرة تشجيع [الآخرين] أو تحريضهم بطريقة أخرى على ارتكاب أعمال إرهابية أو التحضير لها أو التحريض عليها"،[100] بما فيها إصدار بيانات "تمجد ارتكاب أو التحضير ... لتلك الأعمال".[101] ويُضاف إلى هذا أن أي مواطن بريطاني، والباحثين أيضًا، عرضة لهذه المخالفات حتى في الخارج.[102] وبعبارة أخرى، وجود الباحث خارج بلاده في بعثة بحثية أو عمل ميداني لا يحول دون اتهامه بموجب قانون المملكة المتحدة بتشجيع الإرهاب. وتتناول المادة الثانية نشر المنشورات الإرهابية. ويجرم على وجه التحديد توزيع المنشورات الإرهابية أو تداولها أو منحها أو بيعها أو إقراضها أو عرضها أو إرسالها إلكترونيًا أو تقديم خدمات للآخرين تمكنهم من الحصول عليها أو قراءتها أو الاستماع إليها أو الاطلاع عليها أو حيازتها أو شرائها أو اقتراضها.[103]

ويثير هذا الوضع مشكلات واضحة للأكاديميين الذين يدرّسون ويجرون أبحاثًا عن التطرف والإرهاب. وقد يُقال، مثلاً، إن المحاضر الذي يعرض على طلابه في حلقة بحثية مقطعًا من فيديو دعائي لتنظيم داعش، قد ارتكب مخالفات عديدة: حيازة

97 Randeep Ramesh & Josh Halliday, 'Student accused of being a terrorist for reading book on terrorism,' The Guardian، 24 سبتمبر 2015. متاح: http://www.theguardian.com/education/2015/sep/24/student-accused-being-terrorist-reading-book-terrorism

98 Terrorism Act 2000, s.57. متاح: https://www.legislation.gov.uk/ukpga/2000/11/section/57

99 المرجع نفسه، s.58.

100 Terrorism Act 2006, s.1.2 (b)(i). متاح: https://www.legislation.gov.uk/ukpga/2006/11/section/1

101 المرجع نفسه، s.1.3 (a).

102 المرجع نفسه، s.17.

103 المرجع نفسه، s.2.

مواد إرهابية، وتشجيع الآخرين بطريقة غير مباشرة على ارتكاب أعمال إرهابية، ونشر منشورات إرهابية.

ولا أدَل على ذلك، في الواقع، من قضية "نوتنغهام 2". في مايو 2008، كان رضوان صابر، طالب ماجستير في جامعة نوتنغهام، يرسل بريدًا إلكترونيًا إلى مستشاره الأكاديمي، هشام يزة، لإعداد مقترحه البحثي لرسالة الدكتوراه حول الإرهاب الإسلامي. وكان صابر قد تصفح موقع وزارة العدل الأمريكية ونزَّل وثيقة حكومية بعنوان "دراسات عسكرية في الجهاد ضد الطغاة: دليل تدريب القاعدة" (التي استُخدمت في محاكمة قانونية لجماعة مسؤولة عن التفجيرات في شرق أفريقيا).[104] وكانت هذه الوثيقة متاحة مجانًا من خلال نظام المكتبات الجامعية ومعروضة للبيع في مكتبات بيع الكتب في الشوارع الرئيسية في المملكة المتحدة، مثل Waterstones.[105] ورأى زميله الوثيقة على حاسوب يزة؛ فأبلغ الجامعة، ثم أخطرت الجامعة الشرطة. واعتُقل صابر و يزة بدون أمر قضائي بموجب قانون الإرهاب لعام 2000. واحتُجز صابر سبعة أيام في حبس انفرادي.[106]

وبمرور الوقت، أجرِيت تعديلات على قانون عام 2000 استجابة لتحولات سياسية واجتماعية مختلفة. وأجْرِي التطوير الرئيسي الأول في عام 2015 مقترنًا بإقرار قانون Counter-Terrorism and Security Act (قانون مكافحة الإرهاب والأمن)، الذي عزز إلزام المؤسسات بالامتثال لاستراتيجية Prevent. وأصبح لدى الجامعات الآن واجب قانوني محدد، وهو "أن تولي الاعتبار الواجب للحاجة إلى منع الناس من الانجراف إلى الإرهاب"[107] ويُلزمها بوضع سياسات وإجراءات واضحة للباحثين العاملين في هذا المجال. ويستند قانون 2015 إلى نهج قائم على المخاطر، أي أن المؤسسات يجب عليها مراقبة وتقييم الأنشطة البحثية باستمرار والعمل على تخفيف ما تشكله من مخاطر. أما من الناحية العملية، فقد أدرجت جامعات عديدة الآن تقييم المخاطر ضمن استراتيجية Prevent في إجراءاتها المتبعة لتعزيز الأخلاقيات في البحث العلمي.[108] وتشير الخبرات المكتسبة من هذه الإجراءات إلى أن مجالس مراجعة الأخلاقيات طرحت نطاقًا أوسع لرؤية المخاطر يجعل سمعة المؤسسة على رأس اهتماماتها. وقد يُنظر إلى استراتيجية Prevent على أنها مكَّنت مجالس المراجعات المؤسسية من إقحام تطبيقات أخلاقيات البحث العلمي – فيما يخص "البحوث الخطرة، والحساسة سياسيًا" بجميع أنواعها[109] – في متاهة البيروقراطية بعراقيلها وتعقيداتها على أمل "إحباط التهديدات المحتملة وردعها خشية أن تنال من سمعة المؤسسة."[110] ولقد أثار هذا الأمر مخاوفَ جديةً بشأن الحرية الأكاديمية.

وظهر تحولٌ رئيسيٌ ثان ودخل حيز التنفيذ في أبريل 2019 مع إقرار قانون Counter-Terrorism and Border Security Act (قانون مكافحة الإرهاب وأمن الحدود). وأفضى هذا القانون إلى التوسع في الأحكام الجنائية الموجودة حينئذ لتشمل جميع المخالفات المبينة أعلاه في قانوني الإرهاب لعام 2000 وعام 2006؛ وزادت العقوبة القصوى الموقعة على نشر المنشورات الإرهابية، مثلاً، لأكثر من الضعف، أي زادت عقوبة السجن من سبع سنوات إلى 15 سنة.[111]

---

104 Rizwaan Sabir, 'Damages for my unjust "terror" arrest,' Al Jazeera، 21 سبتمبر 2011. متاح: https://www.aljazeera.com/opinions/2011/9/21/damages-for-my-unjust-terror-arrest/

105 انظر https://www.waterstones.com/book/military-studies-in-the-jihad-against-the-tyrants/anonymous/9781907521249

106 وأفرِج عن رضوان صابر وهشام يزة دون توجيه تهمة إليهما. وفي عام 2011، رفع صابر دعوى قضائية ضد شُرطة نوتنغهامشير واتهمها بالسجن الباطل والتمييز العنصري، وتمت تسويتها خارج المحكمة. انظر 'Sabir, 'Damages for my unjust "terror" arrest.

107 'Statutory guidance: Revised Prevent duty guidance for England and Wales,' UK Home Office، تحديث 10 ابريل 2019. متاح: https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales#c-a-risk-based-approach-to-the-prevent-duty

108 انظر، على سبيل المثال، 'Oversight of security-sensitive research material in UK universities,' Universities UK، نوفمبر 2019. متاح: https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/Oversight-security-sensitive-research-material-guidance-3.pdf

109 Adam Hedgecoe (2015), 'Reputational Risk, Academic Freedom and Research Ethics Review,' Sociology, vol. 50 no. 3, p.495.

110 المرجع نفسه.

111 Counter-Terrorism and Border Security Act 2019, s.7. متاح: https://www.legislation.gov.uk/ukpga/2019/3/section/7

ويتضمن قانون عام 2019 أربعة إجراءات جديدة تؤثر تأثيرًا بالغًا على البحوث الأكاديمية التي تتناول التطرف والإرهاب:

1. القانون يجرِّم الحصول على المواد الإرهابية أو الاطلاع عليها عبر الإنترنت؛[112]
2. يستثني صراحة من يؤدون عملاً صحفيًا أو يجرون بحثًا أكاديميًا من مخالفة جمع المعلومات (بما في ذلك عبر الإنترنت) (المادة 58 من قانون الإرهاب لعام 2000)؛[113]
3. يُجرّم دخول المواطنين أو بقاءهم في "منطقة محددة" خارج المملكة المتحدة.[114] يتمتع وزير الخارجية بسلطة تحديد تلك المنطقة في كل حالة على حدة، "بغرض حماية أفراد الشعب من خطر الإرهاب"؛[115]
4. يتوسع في مادة من مواد قانون الإرهاب لعام 2006 ليشمل نشر المنشورات الإرهابية كجريمة خارج المملكة المتحدة (بعد أن كان يتناول في السابق تمجيد الإرهاب فقط).

النقطة 2 أعلاه – يبدو استثناء الأكاديميين من جمع المواد الإرهابية (بما فيها على الإنترنت) – للوهلة الأولى كأنه تطورٌ محمودٌ يعيد الحرية الأكاديمية إلى بحوث الإرهاب والتطرف دون خوف من التداعيات القانونية. ومع ذلك، فالنقطة الحاسمة هي أن الباحثين الأكاديميين مع أنهم مستثنون الآن صراحة من المادة 58 من قانون الإرهاب لعام 2000 (حيازة مواد إرهابية)، فلا توجد حماية قانونية صريحة للأكاديميين من المادتين 1 (تمجيد الإرهاب) أو 2 (نشر المواد الإرهابية) من قانون الإرهاب لعام 2006.[116]

ومعنى هذا من الناحية العملية أن الأكاديميين الذين يصلون إلى المواد المتطرفة ويجمعونها عبر الإنترنت لخدمة أغراض البحث أو التدريس سوف يتحصنون بدفاع قانوني واضح. ولكن، إذا اقتطفوا هذه المواد في مقالات صحفية أو كتب أكاديمية، أو عرضوها في حجرة الدرس كأمثلة على الدعاية المتطرفة دون إدانة صريحة لهذه الجماعات، فقد يجد الباحث نفسه في وضع قانوني مريب. وعلاوة على ذلك، يعني قانون الإرهاب لعام 2000 إمكانية اعتقال الباحثين دون أمر قضائي واحتجازهم لمدة 28 يومًا ريثما تُوجَّه التهم إليهم، كما حدث مع رضوان صابر وهشام يزة.

وبالمثل، فقد يجد الباحثون الذين يقومون بعمل ميداني أو بجمع بيانات في الخارج أنفسهم تحت طائلة هذا التشريع الجديد. وإذا كان أحد الأكاديميين يقوم بعمل ميداني في الخارج، أو يعتزم القيام بذلك، في منطقة أعلن وزير الخارجية أنها "منطقة محددة"، فسوف يكون دخولها أو البقاء فيها جريمة.

وعمومًا، فإن الصورة القانونية للباحثين في الإرهاب غير واضحة. ومع أن تشريعات العام الماضي تشير إلى تفهم الحكومة أن الباحثين سوف تقع بحوزتهم مواد مريبة، لا تزال هناك تشريعات للكتب التي يظل الأكاديميون عرضة لها بشدة. وتبرز التشريعات والسياسات والأوساط الأكاديمية المناخ السياسي الحالي وترسخه؛ وفيما يشهد عصرنا هذا ارتفاعًا في نبرة الإسلاموفوبيا ودعمًا واسعًا للمتابعة الاستباقية والمراقبة البوليسية، تعبر استراتيجية Prevent وقوانين الإرهاب تعبيرًا بليغًا عن هاتين الظاهرتين.

---

112 المرجع نفسه، s.3.
113 المرجع نفسه، s.7.
114 Terrorism Act 2000, s.58(b). متاح: https://www.legislation.gov.uk/ukpga/2000/11/section/58B
115 'Counter-Terrorism and Border Security Bill: Supplementary Delegated Powers Memorandum,' UK Home Office، 5 سبتمبر 2018. متاح: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/739267/Supplementary-Delegated-Powers-Memo-designated-area-offence.pdf
116 "Sections 2 and 3 of the Terrorism Act 2006 also outlaw the dissemination of terrorist publications, including by electronic means, and give a very wide definition of 'terrorist publication' and 'statements' that could be construed as encouraging or inducing the commission preparation or instigation of acts of terrorism. Academic research is not a defence under the Terrorism Act 2006 [emphasis mine]." 'Oversight of security-sensitive research material in UK universities,' Universities UK, November 2019. متاح: https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/Oversight-security-sensitive-research-material-guidance-3.pdf

ومن العوامل المهمة التي يجب أن نضعها نصب أعيننا ونحن نقيِّم احتمالية تأثر الباحثين بحوكمة مكافحة الإرهاب في حكومة المملكة المتحدة (مثل استراتيجية Prevent) والتشريعات، تأثيرها الجائر على المسلمين. ويشكل "التطرف الإسلامي" 65٪ من مجموع الإحالات إلى استراتيجية Prevent، ما يعني أن "احتمالية إحالة المسلمين إلى استراتيجية Prevent العام الماضي هي 1 إلى 500 تقريبًا، أي أكثر من غير المسلمين بنحو 40 مرة. وبالمثل، فإن أكثر من نصف (54٪) الاعتقالات المتعلقة بالإرهاب التي شهدتها المملكة المتحدة في عام 2017 كانت لمن اعتُقد أن "هيئتهم العرقية آسيوية".[117] ويشير الواقع الإحصائي إلى أن الطلاب والباحثين الذين صُنِّفوا عرقيًا واستُضعفوا كمسلمين كانوا أشد عرضة بكثير لخطر الاستغلال – سواء أحيلوا إلى استراتيجية Prevent، أو حتى جُرِّموا – من قبل المنطقة الرمادية القانونية.

ومازلنا نرى تشريعات مكافحة الإرهاب في الحرم الجامعي تستهدف المسلمين ظلمًا حتى الآن. ومع ذلك، شهد شهر نوفمبر 2020 أكبر عدد من الإحالات المتعلقة بالتطرف اليميني المتشدد: 43٪ مقارنة بـ 30٪ للتطرف الإسلامي.[118] ويطرح هذا التطور أسئلة مثيرة للاهتمام حول التنميط العنصري والبحث في التطرف والإرهاب: هل سيُفهم الباحثون غير المسلمين على أنهم "مستضعفون" و "معرضون لخطر الراديكالية" من أجل البحث في إرهاب التفوق الأبيض؟ إذا كان الأمر كذلك، فما هي ردود الفعل الاجتماعية والسياسية التي قد يستثيرها هذا الوضع؟ يرى نقادٌ كثيرون أن استراتيجية Prevent وتشريعات مكافحة الإرهاب بمثابة آلية لمراقبة المجتمعات الإسلامية والسيطرة عليها داخل الحرم الجامعي وخارجه.[119] فإذا ترسخت هذه المهمة الآن، إذًا فما هي مهمة استراتيجية Prevent؛ إن كان لها مهمة أصلاً؟

ملاحظات ختامية: مشهدٌ عالميٌ متغير

تتنوع وتتعقد القضايا الأخلاقية والقانونية التي تواجه الباحثين الساعين للوصول إلى بيانات الأفراد ومعالجتها. وتتسم الآفاق العالمية المتوقعة للباحثين العاملين في مجاليْ التطرف والإرهاب بالتغير وعدم اليقين، في مواجهة التغيرات القانونية والسياسية سريعة الخطى على الصعيدين الوطني والدولي.

وفيما يخص الوصول إلى البيانات لخدمة الأغراض البحثية، هناك اتجاه عالمي عام نحو تعزيز تشريعات حماية البيانات لحماية حقوق بيانات الأفراد بصورة أفضل (مع بعض الاستثناءات، مثل اليابان أعلاه). وهذا يعني احتمالاً أن يكون الباحثون أكثر تقيدًا في المستقبل فيما يخص البيانات المتاحة لهم وطرق معالجتهم هذه البيانات واستخدامها. وبينما تسعى الشركات إلى مواكبة مزيج من التشريعات الوطنية وعبر الوطنية، تحتاج منصات وسائل التواصل الاجتماعي إلى تحديث سياسات خصوصيتها وتعديلها باستمرار. ولأن عواقب عدم القيام بذلك – كما رأينا، على سبيل المثال، في غرامة الـ 5,000,000,000 دولار التي وقعتها مفوضية التجارة الفيدرالية الأمريكية على فيسبوك – أصبحت أخطر من أي وقت مضى، فمن الممكن أن تتبنى المنصات نهجًا أكثر تحفظًا في سياسات خصوصيتها لضمان أمنها المالي وحسن سمعتها.

وفي الوقت ذاته، تتسم الآفاق القانونية والسياسية المتوقعة للباحثين العاملين في مجاليْ التطرف والإرهاب بعدم اليقين أيضًا. في المملكة المتحدة، أدى مناخ العمل البوليسي الاستباقي الذي يُبرَّر بتهديدات الأمن القومي إلى خلق بيئة سياسية يتعرض فيها الباحثون لخطر التجريم لاقترابهم من مواد معينة. ومع تقدم "الحرب على الإرهاب" في العقد الأول من القرن الحادي والعشرين، تميز السياق التشريعي

117 'Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, financial year ending 31 March 2017,' UK Home Office، يونيو 2017. متاح: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619016/police-powers-terrorism-mar2017-hosb0817.pdf

118 Jamie Grierson & Dan Sabbagh, 'Largest number of Prevent referrals related to far-right extremism,' The Guardian، 26 نوفمبر 2020. متاح: https://www.theguardian.com/uk-news/2020/nov/26/just-one-in-10-prevent-referrals-found-at-risk-of-radicalisation

119 Fahid Qurashi (2018), 'The Prevent strategy and the UK "war on terror": embedding infrastructures of surveillance in Muslim communities,' Palgrave Communications, vol. 4 no. 17 (2018); 'Liberty's written evidence to the JCHR's Inquiry on Freedom of Expression in Universities,' Liberty، ديسمبر 2017. متاح: https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Libertys-Evidence-to-the-JCHRs-Inquiry-into-Freedom-of-Expression-in-Universities-Dec-2017.pdf

للمملكة المتحدة بنهج قائم على القانون والنظام في مكافحة الإرهاب، ما أدى إلى العديد من التطورات القانونية التي تقيد المواد التي يستطيع الأكاديميون الوصول إليها والتحدث عنها والكتابة عنها وتدريسها ونشرها. ومع ذلك، بينما يتحول الاهتمام العالمي بعيدًا عن ما يسمى بـ "التهديد الإسلامي" نحو الوعي بالتفوق الأبيض العنيف، تطرح السياسات والأطر القانونية الحالية التي صُمِّمت لاستهداف إحدى الأقليات مشكلات صعبة. ولقد اعتمدت آليات الاستنكار الحالية التي يتبناها الزملاء والأقران في الجامعات على التنميط العنصري إلى حد كبير؛ هل ستصلح تلك النُهج مع الباحثين الغربيين العاملين في مجالات التفوق الأبيض.

وقد تتغير طبيعة البحث ونطاق تطبيقه في مجاليْ التطرف والإرهاب في الغرب إلى حد كبير في ضوء تغير السياق العالمي في السنوات المقبلة. وقد يصبح من الصعب، مثلاً، إجراء تحليل كمي واسع النطاق إذا تعززت قوانين خصوصية البيانات وسياسات خصوصية الشركات، أو الوصول إلى المتورطين مع الجماعات الإرهابية أو في الأعمال الإرهابية. وهذا قد يعني تغيُّر المنهجيات المتاحة للباحثين في موضوع التطرف، وربما تصبح أشد تركيزًا على الجانب النوعي، أو أضيق نطاقًا، أو أشد تأكيدًا على الإثنوغرافيا الرقمية.[120] ومع أنها تحولات مقلقة، فقد نجني من ورائها الكثير: مواجهات أقرب وأدق مع التطرف والإرهاب تظهر ذوي المعتقدات المتطرفة على الإنترنت وتعقيداتهم وتناقضاتهم بصورة أوضح.

120 انظر، على سبيل المثال: Sarah Pink et al. (eds.), Digital Ethnography: Principles and Practice (2015), SAGE Publications Ltd.

Global Network
on Extremism & Technology

بيانات الاتصال

لأي أسئلة أو استفسارات، أو للحصول على نسخ أخرى من هذا التقرير، يرجى التواصل مع:

ICSR
King's College London
Strand
London WC2R 2LS
المملكة المتحدة

هاتف: +44 20 7848 2098
بريد إلكتروني: mail@gnet-research.org

تويتر: @GNET_research

هذا التقرير، كغيره من منشورات الشبكة العالمية للتطرف والتكنولوجيا (GNET)، يمكن تنزيله مجانًا من موقع شبكة GNET على الإنترنت www.gnet-research.org.