تطبيق حماية البيانات على الوجه الصحيح في أبحاث العلم التشاركي

روبن بيرس، ماريانا إيفرام



الملخص:

يتناول هذا المقال حماية البيانات في مشروعات العلم التشاركي، منطلقًا من أن تزايد هذه المشروعات وأهميتها للسياسات سيُخضع طريقة إجرائها لتدقيق أكبر، وأن مشروعيتها العلمية والسياسية والقانونية مرهونة بالتعامل السليم مع البيانات، إذ إن الامتثال لقوانين حماية البيانات التزام قانوني قد يجر الإخلال به غرامات باهظة. ويعرض المقال، في صيغة أسئلة وأجوبة مستندة إلى اللائحة العامة لحماية البيانات، أبرز الاعتبارات في ثلاث مراحل: التخطيط، ويشمل تقليل البيانات وفئات البيانات الشخصية والحساسة والترميز بالأسماء المستعارة وتحديد المتحكم في البيانات ومعالجها؛ والاستقطاب والموافقة المستنيرة؛ والدراسة والتحليل، ويشمل نقل البيانات عبر الحدود وتقييد مدة التخزين والتعامل مع اختراق البيانات وانسحاب المشاركين. ويخلص إلى أن حماية البيانات جزء أصيل من المشروع لا يُترك للمحامين وحدهم، مع التوصية باستشارة خبير مختص.

الكلمات المفتاحية: حماية البيانات، العلم التشاركي، اللائحة العامة لحماية البيانات، الخصوصية في البحث العلمي، تقليل البيانات

مقدمة:

مع تزايد مشروعات العلم التشاركي عددًا[1] ونطاقًا وصلةً بالسياسات العامة، يُرجَّح أن تخضع طريقة إجراء البحوث التي تقوم عليها لتدقيق أكبر. وفضلًا عن ذلك، فإن جدوى العلم التشاركي لا تتوقف على جودة النتائج التي يقدمها وأهميتها فحسب، بل تتوقف بالقدر نفسه على العملية التي جرى بها الحصول على تلك النتائج. ومن أهم المجالات في هذا الصدد التعامل مع البيانات، ولا سيما في ضوء الاهتمام المتزايد بحقوق المواطنين في حماية البيانات. ويعرض هذا المقال بعض الاعتبارات الرئيسية لحماية البيانات التي تنشأ عادةً عند تنفيذ مشروع من مشروعات العلم التشاركي. وقد اخترنا بضع مسائل في مراحل مختلفة من مشروع العلم التشاركي لنبيّن أن حماية البيانات عملية مستمرة، تبدأ في مرحلة التخطيط قبل انطلاق المشروع، وتتواصل حتى بعد انتهائه. إن الجدوى

العلمية والسياسية والقانونية للعلم التشاركي مرهونة إلى حد كبير بتطبيق حماية البيانات على الوجه الصحيح. وانطلاقًا من المبادئ وصولًا إلى الممارسة، يوضح هذا المقال سبلًا للتعامل المسؤول مع البيانات من جانب الباحثين المواطنين (citizen scientists).

ومن الفوائد التي تُنسب إلى العلم التشاركي أنه يمكّن غير المتخصصين من الاضطلاع بدور فاعل في إنتاج المعرفة، فيُسهم بذلك في «دمقرطة» العلم، وهو نشاط ظل تقليديًا مغلقًا ومقصورًا على المتخصصين. غير أن هذا النهج الأكثر شمولًا في العلم يجلب معه مسؤوليات إضافية. فبحسب نوع العلم التشاركي، سواء أكان نابعًا من المجتمع (حيث تنبع الأسئلة والأهداف والمناهج من مجتمع من غير المتخصصين)، أم مشروعات تقودها المؤسسات وتستقطب غير المتخصصين لجمع البيانات أو الإسهام بها، أم مزيجًا ما بين هذين، قد يجد الباحثون المواطنون أنفسهم يتحملون بعض مسؤوليات الباحث الرئيسي المؤسسي أو كلها.[2] فالباحث المواطن، بمعنى ما، يضطلع بدور مزدوج هو دور «المشارك» ودور «الباحث» حين يؤدي دورًا فاعلًا في توجيه البحث. فهو الآن في موقع «المشارك المحمي» و«الباحث» المسؤول عن توفير تلك الحماية معًا. ومن أخطر المسؤوليات التي يجب أن يضطلع بها التعامل السليم مع البيانات.

يهدف هذا المقال إلى أن يكون نقطة انطلاق للتفكير في جوانب حماية البيانات في مشروع من مشروعات العلم التشاركي. وترمي المسائل المختارة إلى بيان كيف تُترجَم مبادئ حماية البيانات ولوائحها إلى تطبيقات في الواقع. وبطبيعة الحال، لا بديل عن استشارة خبير في حماية البيانات بشأن احتياجات مشروع بعينه واعتباراته في ولاية قضائية بعينها. ومع ذلك، يفيد الباحثون المواطنون أنفسهم ومشروعاتهم حين يمتلكون قدرًا من الفهم لما يتطلبه إعداد مشروع مسؤول تجاه البيانات.

التخطيط: قبل استقطاب المشاركين:

كيف أقرر ما البيانات التي أجمعها؟:

قد تبدو فكرة أن «المزيد من البيانات أفضل» أمرًا طبيعيًا في نظر الباحث. غير أن اللائحة العامة لحماية البيانات (General Data Protection Regulation: GDPR) تنص على مبدأ «تقليل البيانات» (data minimization)، الذي يوفر أساسًا مهمًا للإجابة عن هذا السؤال. وينص مبدأ تقليل البيانات على أن يكون جمع البيانات «كافيًا وذا صلة ومقتصرًا على ما هو ضروري فيما يتعلق بالأغراض التي تُعالَج من أجلها».[3] لذلك، عند تقرير البيانات التي ستُجمع، من الضروري تحديد البيانات التي تحتاج إليها فعلًا في بحثك، وسبب ذلك. فقد تكون بعض البيانات المتعلقة بالمشاركين ضرورية للإجابة عن السؤال، كالجنس والأصل العرقي والعمر، إذا كانت الدراسة تسعى إلى فهم أنماط أو مشكلات أو تحديدها مما قد تكون له آثار على السياسات تتعلق بهذه السمات من حيث صلتها بالموضوع قيد الدراسة. وإن لم يكن الأمر كذلك، فينبغي تطبيق مبدأ تقليل البيانات.

هل توجد فئات مختلفة من البيانات؟:

نعم. فالهدف العام لقانون حماية البيانات هو توفير حماية واسعة للأفراد عبر حماية بياناتهم الشخصية (أي معلومات تتعلق بشخص يمكن تحديد هويته[4]). لذلك يصبح السؤال عمّا إذا كانت البيانات قادرة على تحديد هويتك اعتبارًا حاسمًا. فإذا كان من المرجح أن تحدد المعلومات هويتك، فإنها تندرج ضمن فئة «البيانات الشخصية» وستحتاج إلى الحماية. ومن المعلومات التي قد تشكّل بيانات شخصية الاسم وعنوان البريد الإلكتروني، بل حتى

السمات الأقل مباشرة، مثل الهوية الجسدية أو النفسية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية.[5] وقد يجمع مشروع العلم التشاركي أنواعًا كثيرة من البيانات. فعلى سبيل المثال، يُعد عدد المشاة الذين يعبرون جسرًا في ساعة الذروة بيانات غير شخصية، في حين تُعد أسماء الأشخاص الذين يملؤون استبانة عن عبور الجسر أو عناوينهم بيانات شخصية. وإذا احتاج المشروع إلى مراسلة المشاركين، أو تقديم التدريب لهم، أو تتبّع مدخلات شخص ما على مدى الزمن، فسوف ينطوي ذلك على معالجة البيانات الشخصية لأولئك المشاركين، وستنطبق أحكام حماية البيانات.

ومن الممارسات الشائعة «ترميز» هوية المشارك، باستخدام اسم مستعار أو رقم أو طريقة أخرى لوسم البيانات، مع إتاحة إعادة تحديد الهوية في الوقت نفسه لمن يصل إلى مفتاح يربط الاسم المستعار بالاسم الحقيقي. فعلى سبيل المثال، قد توفر كتابة «المشارك (AB12495)» في استبانة بدلًا من «جون سميث»، مع الاحتفاظ بمفتاح منفصل، مستوى أعلى من الحماية لهوية جون سميث، ولكن بشرط أن يُخزَّن المفتاح ويُتعامَل معه بطريقة آمنة. وهذه العملية، المسماة الترميز بالأسماء المستعارة (pseudonymization)، لا تزال تنطوي على التعامل مع بيانات شخصية، وتنطبق عليها قوانين حماية البيانات. وإضافة إلى ذلك، ثمة أحكام أخرى كثيرة واجبة التطبيق، منها توفير السبل التي تمكّن الأشخاص من الوصول إلى بياناتهم، وتصحيحها في حال عدم دقتها.[6] وهكذا يجب على الباحثين المواطنين، في دورهم المزدوج بوصفهم باحثين ومشاركين، أن يقرروا البيانات الضرورية للمشروع، وهل هذه البيانات شخصية (قابلة لتحديد الهوية)، وكيف ستُجمع وتُخزَّن بأمان.

هل توجد بيانات لا ينبغي لنا جمعها، أو بيانات يجب التعامل معها بطريقة مختلفة؟:

ثمة «فئات خاصة» من البيانات الشخصية ينبغي التعامل معها بطريقة مختلفة. وتستدعي «البيانات الحساسة» عناية خاصة لأنها قد تكشف معلومات يمكن أن تجعل الشخص عرضة للأذى أو أن تُستخدم ضده بطريقة ما. ويَعُدّ القانون هذه البيانات محتاجة إلى مستوى مشدد من الحماية. فعلى سبيل المثال، تشمل «البيانات الحساسة» الآراء السياسية، والدين، والأصل العرقي أو الإثني، والعضوية في النقابات العمالية، والبيانات المتعلقة بصحة الفرد أو حياته الجنسية أو ميوله الجنسية.[7] لذلك ينبغي للعالم المواطن، بوصفه باحثًا ومشاركًا، أن يقرر هل البيانات الحساسة ضرورية للدراسة، وإن كانت كذلك، فكيف يضمن حمايتها الكافية.

وإذا وجدت أن المشروع يحتاج إلى جمع «بيانات حساسة»، فيجب عليك الحصول على الموافقة الصريحة من المشارك، إما ببيان مكتوب وإما بالبريد الإلكتروني. ومرة أخرى، ينبغي أن يحكم مبدأُ تقليل البيانات تقريرَ ما إذا كنت تحتاج إلى جمع «بيانات حساسة».

من المسؤول عمّا يحدث للبيانات؟:

يُعد تحديد الأشخاص المسؤولين في أي مشروع جزءًا رئيسيًا من التخطيط. ففي مشروعات العلم التشاركي التي لا تديرها المؤسسات في المقام الأول، يصبح الباحثون المواطنون في جوهر الأمر هم الأطراف المسؤولة. وحين تدخل المؤسسات والمواطنون في شراكة بحثية، قد يكون من المناسب إبرام اتفاقات مكتوبة بشأن المسؤوليات.[8] ويطرح تدفق البيانات تحديات كثيرة تتعلق بالجمع والوصول والتخزين، على سبيل المثال. ويُوصى بشدة بتعيين شخص لتنسيق هذه العملية وإدارتها. وثمة دوران يتعلقان بحماية البيانات ينبغي للباحثين المواطنين أن يكونوا على دراية بهما منذ بداية المشروع، هما «المتحكم في البيانات» (data controller) و«معالج البيانات» (data processor). فالمتحكم في البيانات هو الشخص أو الأشخاص أو المنظمة المسؤولة في نهاية المطاف والمكلفة

بالامتثال للالتزامات القانونية لحماية البيانات.[9] وتمتد هذه المسؤولية طوال المشروع،[10] وتشمل تحديد غرض الجمع وتحديد المخولين بمعالجة البيانات أو التعامل معها، فضلًا عن ضمان الامتثال في أثناء المشروع وتحديد مدة التخزين وطريقته في نهايته. وقد يتقاسم هذه المسؤولية جميع الشركاء الذين يشتركون في تحديد الغرض ويسهمون في اتخاذ القرار. أما معالج البيانات، من ناحية أخرى، فيشير إلى أي شخص يعالج البيانات نيابةً عن المشروع. وهكذا قد يكون كل فريق في مشروع العلم التشاركي، على سبيل المثال، معالجًا للبيانات إذا كان يجمع البيانات ويحللها.

الاستقطاب:

ما الذي يحتاج المشاركون المحتملون إلى معرفته عمّا يحدث لبياناتهم؟:

من أهم جوانب إعداد مشروع بحثي الحصول على الموافقة المستنيرة (informed consent) من المشاركين. ومن المعلومات الأساسية التي يجب أن تتضمنها الموافقة الغرضُ الذي تُعالَج البيانات من أجله، وبيانات الاتصال بالمتحكم في البيانات، ومدة معالجة البيانات وتخزينها، وغير ذلك. وعليه، فلكي يقدم المشاركون موافقة مستنيرة سليمة، يجب تزويدهم بمعلومات عمّا سيحدث لبياناتهم.[11]

الدراسة والتحليل:

هل يمكننا تداول البيانات بين فرق المشروع المختلفة في بلدان مختلفة؟:

لبعض مشروعات العلم التشاركي شركاء متعددون يوجدون في بلدان مختلفة. ونتيجة لذلك، قد يرغب شركاء المشروع في نقل البيانات عبر بلدان مختلفة لأغراض التحليل. وتتوقف إمكانية هذا النقل على عوامل كثيرة، منها هل البيانات مجهّلة الهوية (anonymized) أم قابلة لتحديد الهوية، وما البلدان المعنية.

فعلى سبيل المثال، قد تكون المشروعات التي يقع جميع شركائها في الاتحاد الأوروبي أقل تعقيدًا، لأن كل بلد يخضع للائحة العامة لحماية البيانات. أما إذا كان الشركاء يقعون خارج الاتحاد الأوروبي، فستكون هناك مسؤوليات واشتراطات إضافية قبل إمكان مشاركة البيانات، لضمان «الحماية الكافية»، إما بصدور قرار كفاية (adequacy decision) من المفوضية الأوروبية، وإما بتطبيق مجموعة من البنود التعاقدية النموذجية (Standard Contractual Clauses: SCC) (المتاحة للجمهور على موقع المفوضية الأوروبية).[12] وقد تحاول بعض مشروعات العلم التشاركي تقليل العوامل المعقِّدة في عمليات النقل الدولي إما باستخدام بيانات مجهّلة الهوية وإما بإجراء جميع عمليات المعالجة داخل البلد.

هل توجد اعتبارات خاصة بتخزين البيانات؟:

إن تحديد إطار زمني واضح لتخزين البيانات أمر مهم، لأنه كلما طالت مدة الاحتفاظ بالبيانات ارتفع خطر تسريبها أو إساءة استخدامها بطرق تضر بحقوق المشاركين أو مصالحهم. ويمكن لمبدأ «تقييد مدة التخزين» (storage limitation) في اللائحة العامة لحماية البيانات أن يوضح كيفية التعامل مع هذه المسألة. فهو ينص على أن تُحفظ البيانات «في صورة تتيح تحديد هوية أصحاب البيانات مدةً لا تتجاوز ما هو ضروري للأغراض التي تُعالَج من أجلها البيانات الشخصية».[13]

وبطبيعة الحال، كلما كانت فئات البيانات المخزنة أكثر حساسية، كالبيانات الصحية مثلًا، وجب أن تكون التدابير الأمنية أشد. ومن ثم، يجب استخدام تدابير تقنية وتنظيمية لمنع الوصول غير المصرح به إلى البيانات أو فقدانها أو تغييرها.[14] ومن المهم ملاحظة أن الباحثين المواطنين يظلون مسؤولين عن التعامل مع البيانات الشخصية وتخزينها حتى بعد انتهاء المشروع. وفي نهاية المشروع ينبغي حذف البيانات أو تجهيل هويتها. ولا ينطبق قانون حماية البيانات على البيانات المجهّلة الهوية.

ماذا علينا أن نفعل إذا وقع حادث أمني أو اختراق للبيانات؟:

حتى مع بذل أفضل الجهود، قد يقع اختراق للبيانات (data breach)، ويجب أن يكون المشروع مستعدًا للتعامل مع ذلك بسرعة وعلى النحو المناسب. ففي البحث التقليدي الذي تقوده المؤسسات، يكون موظفون مؤسسيون معيّنون مسؤولين عن إخطار السلطات المختصة في حال وقوع اختراق للبيانات. أما في مشروعات العلم التشاركي التي تكون المسؤولية فيها مشتركة، فمن المفيد تعيين شخص محدد للقيام بهذه الإجراءات، لأن المشروع سيكون مسؤولًا عن الإخطار السريع لسلطة الإشراف الإقليمية، وإخطار أي أفراد اخترقت بياناتهم في ظروف معينة.[15]

ومن المهم إدراك أن أنواعًا متعددة من الحوادث قد تؤدي إلى اختراق للبيانات، مثل:

- فقدان أو سرقة حاسوب محمول يتضمن بيانات الباحثين المواطنين
- رسالة بريد إلكتروني أُرسلت إلى غير وجهتها
- الوصول غير المصرح به (مثل شخص من منظمتك غير مصرح له بالتعامل مع بيانات العلم التشاركي).

ماذا نفعل (بالبيانات) إذا انسحب أحد من الدراسة؟:

لنتأمل موقفًا يقرر فيه بضعة علماء مواطنين، بعد أشهر قليلة من بدء مشروعك، أنهم لم يعودوا يرغبون في المشاركة. ينبغي للمشروع أن يبيّن بطريقة معقولة وفي الوقت المناسب أن بإمكان المشارك الانسحاب.[16] فعلى سبيل المثال، يمكن لرابط إلغاء الاشتراك (opt-out) في أسفل صفحة الويب ذات الصلة أن يوفر هذا الخيار. وبعد أن يسحب الفرد موافقته، لا يمكن عمومًا استخدام بيانات ذلك الشخص في الدراسة اعتبارًا من تاريخ الانسحاب.

أفكار ختامية:

ينبغي أن يكون واضحًا أن حماية البيانات ليست أمرًا يُترك للمحامين (وإن كنا نوصي بشدة باستشارة خبير في حماية البيانات). فحماية البيانات جزء لا يتجزأ من مشروع العلم التشاركي. ويهدف هذا العرض الموجز، من خلال أسئلة شائعة توضح حضور حماية البيانات في جميع مراحل العلم التشاركي، إلى تنبيه المنخرطين في العلم التشاركي إلى مركزية هذه المجموعة من الحقوق والمصالح. وفضلًا عن ذلك، فبالتعرف على مبادئ حماية البيانات، وهي المساءلة، والدقة، وتقليل البيانات، وتقييد الغرض، والمشروعية، والشفافية، والسلامة والسرية، وتقييد مدة التخزين، المنصوص عليها في المادة 5 من اللائحة العامة لحماية البيانات، يمكن للباحثين المواطنين أن يتعلموا كيف يفكرون في الصورة التي يكون عليها العلم التشاركي المسؤول تجاه البيانات. والقصد من الأسئلة والأجوبة توضيح كيفية عمل بعض هذه المبادئ في الممارسة. إن حماية البيانات مجال شديد التفصيل، لكن كلما زاد وعيك بما تعنيه حماية البيانات لمشروعك، كنت في موقع أفضل لفهم متطلبات القانون وتطبيقها.

المراجع:

1. Lea Den Broeder et al., "Citizen Science for public health," Health Promotion International, 33, no. 3, (2018): 505-514, DOI: https://doi.org/10.1093/heapro/daw086 (accessed 11 November 2021).
2. Alena Buyx et al., "Every participant is a PI. Citizen science and participatory governance in population studies," International Journal of Epidemiology, 46, no. 2, (April 2017): 377-384, DOI: https://doi.org/10.1093/ije/dyw204 (accessed 11 November 2021).
3. "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," European Union, April 27, 2016, Article 5(c), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed 12 November 2021).
4. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Recital 26.
5. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Article 4.1.
6. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Article 15-16.
7. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Article 9.
8. David B. Resnik, Kevin C. Elliott, and Aubrey K. Miller, "A framework for addressing ethical issues in citizen science," Environmental Science & Policy, 54, (2015): 475-481. DOI: https://doi.org/10.1016/j.envsci.2015.05.008 (accessed 11 November 2021).
9. European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Article 4.7, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (accessed 23 November 2021).
10. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Article 24.
11. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Article 7.
12. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Chapter 5.
13. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Article 5(e).

14. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Article 32.

15. European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," Article 33

16. "Guidelines 05/2020 on consent under Regulation 2016/679," Article 7.3, European Data Protection Board, adopted May 4, 2020, edpb_guidelines_202005_consent_en.pdf (europa.eu), (accessed 11 November 2021).