مواجهة الشراكات بين القطاعين العام والخاص في مجال المراقبة: دليل للمجتمع المدني

يونيو 2022

privacyinternational.org

نبذة عن برايفسي إنترناشيونال

الحكومات والشركات تستخدم التكنولوجيا لاستغلالنا, و تسيء استعمال سلطاتها على نحوٍ يهدد حرياتنا وكل شيء يميزنا كبشر. لذلك، فإن برايفسي إنترناشيونال تقوم بحملاتٍ تستهدف تحقيق التقدم الذي نستحقه جميعًا. نهدف إلى حماية الديمقراطية والدفاع عن كرامة الإنسان والمطالبة بمحاسبة المؤسسات ذات النفوذ التي تخون الثقة العامة. فإنّ الخصوصية تحظى بأهمية بالغة لدى كل واحد فينا، سواء كنت طالبًا للجوء أو مكافحًا للفساد أو باحثًا عن المشورة الصحية.

ومن ثم، ندعوك للانضمام إلى حركتنا العالمية اليوم والنضال في سبيل تحقيق الهدف الأهم؛ ألا وهو حريتنا الإنسانية.

برايفسي إنترناشيونال
62 Britton Street, London EC1M 5UY, United Kingdom
هاتف: 4321 3422 20(0) 44+
privacyinternational.org

برايفسي إنترناشيونال هي مؤسسة خيرية مسجلة برقم (1147471)، وهي شركة تضامن محدودة مسجلة في إنجلترا وويلز برقم (04354366).

المحتويات

شكر وعرفان

نتقدم بالشكر إلى المنظمات الشريكة لنا: ADC وTEDIC وغيرهما من المنظمات التي ترغب في عدم الكشف عن هويتها والتي أسهمت في إعداد هذا الدليل.

- جمعية التكنولوجيا والتعليم والتنمية والبحوث والاتصالات (TEDIC) هي منظمة غير حكومية في باراغواي تأسست عام 2012، ويتمثل عملها في تطوير تكنولوجيا مدنية مفتوحة المصدر والدفاع عن الحقوق الرقمية في سبيل تعزيز ثقافة حرة على الإنترنت.
- Asociación por los Derechos Civiles (ADC) هي منظمة مجتمع مدني في الأرجنتين تأسست عام 1995، وتعمل منذ تأسيسها على الترويج للحقوق المدنية والإنسانية والدفاع عنها في الأرجنتين وأمريكا اللاتينية.

مقدمة

تسعى الدول في جميع أنحاء العالم إلى تعزيز قدرات المراقبة لديها وتسخير قوة البيانات لتقديم الخدمات العامة؛ وفي ضوء ذلك، فإنها غالبًا ما تستعين بخدمات شركات التكنولوجيا الخاصة – وذلك من خلال الشراكات بين القطاعين العام والخاص (PPPs). كما أدت الجهود التي بُذلت في مكافحة جائحة كوفيد-19، وما صاحبها من رغبة ملحة في إيجاد أجوبةٍ وحلول مناسبة، إلى زيادة الحاجة المفترضة لدى الدول إلى استخدام التكنولوجيات "المبتكرة" وأنظمة تحليل البيانات الضخمة التي تطورها الشركات. لكن هذا التعاون بات يتخذ شكلاً جديدًا يختلف عن الشكل التقليدي لعلاقات المشتريات العامة.

نلاحظ أن الاعتماد المتبادل بين الأطراف باتت تتزايد، حيث يمكن للدولةِ أن تطور أنظمة أو عمليات جديدة تعتمد كليًا على خدمات شركة وحدة، وبموجب ذلك يمكن للشركة أن تصل إلى بيانات و معلومات لتطوير خدماتها الأخرى. تتجاوز هذه الشراكات الإطار البسيط للعلاقات التجارية "غير المتكررة"، إذ غالبًا ما تُبنى على المراودة، والوعود بالحصول على الحقيقة الكاملة، والوصول الخاص إلى البيانات - مع التحايل في كثير من الأحيان على قواعد المشتريات العامة، وإعاقة الحقوق الأساسية في سياق هذه العملية.

على أنّ خصخصة المسؤوليات العامة تتطلب تمحيصًا أكثر من أي وقت مضى لضمان عدم انتهاك حقوق الإنسان في الخفاء، وهذا هو الحال لا سيما في الحالات التي تُستخدم فيها الأنظمة المنتشرة لأغراض المراقبة والمعالجة الجماعية للبيانات الشخصية. وليس سرًا أنّ الشركات الخاصة تتلاعب بالحدود القانونية والأخلاقية التي تقيد التعامل مع هويات الأفراد وبياناتهم، دون أن تخضع للمساءلة بنفس القدر الذي تخضع له السلطات العامة - مما يشكل انتهاكًا كبيرًا للحقوق الأساسية عندما تُستخدم لتقديم خدمات عامة.

يمتلك المجتمع المدني القدرة على الكشف عن المخاطر والمشاكل التي تنشأ عن هذه الشراكات من خلال الاستقصاء والإبلاغ العام. بيْد أنّ تحديد المخاطر والانتهاكات المحتملة لحقوق الإنسان ليس بالمهمة السهلة، إذ يتطلب فهمًا متعدد المستويات لما يرتبط بذلك من تكنولوجيا وقانون وحوكمة. واستنادًا إلى أعمال الاستقصاء التي أجريناها، وبناءً على خبرات شركائنا، صممت برايفسي إنترناشيونال هذا الدليل لمنظمات المجتمع المدني والمنظمات غير الحكومية والمؤسسات الأكاديمية والأفراد لفهم والتحقق في هذه الشركات والتي تساعد الباحثين الحصول على معلومات مهمة، وفهم التكنولوجيا المعنية، وكذا تحديد المسائل المرتبطة بالخصوصية والحوكمة.

يهدف هذا الدليل إلى دعم أي شخص يحاول معرفة المزيد بشأن الشراكات بين القطاعين العام والخاص في مجال المراقبة وتحديد المخاطر والمشكلات الرئيسية المرتبطة بذلك. ولتحقيق هذا الهدف، تم تقسيم هذا الدليل إلى أربعة أقسام: يركز القسم الأول على تقييم المخاطر، والقسم الثاني يركز على جمع المعلومات الرئيسية المتعلقة بالشراكة عبر وسائل مختلفة؛ ويتطرق القسم الثالث بعمق إلى التكنولوجيا المستخدمة في الشراكة، مع استخدام مقاربة تنازلية من القمة إلى القاع تبدأ من الوسائل المستخدمة لوضع تعريف عام للتكنولوجيا، وتنتهي بأساليب فهم طريقة عمل التكنولوجيا في

الواقع؛ ويتناول القسم الرابع الشواغل والضمانات المتعلقة بالحوكمة والإدارة، بما في ذلك أفضل الممارسات الدولية ومشكلات حماية البيانات والضمانات ذات الصلة.

ويمكن استخدام القوائم المرجعية المتوفرة في نهاية هذا الدليل كعرض عام للأمور الرئيسية التي ينبغي دراستها، ولمساعدتك في تتبع ما تنجزه من أعمال.

يتمثل الغرض من هذا الدليل في مساعدتك على ما يلي:

- دراسة شراكة بين القطاعين العام والخاص، والحصول على المعلومات ذات الصلة
- طرح الأسئلة المناسبة على الشركاء المعنيين (من القطاعين العام والخاص)
- تحديد الشواغل المتعلقة بالتكنولوجيا المعنية وحوكمة الشراكة

أعددنا مجموعة من الضمانات الخاصة بالشراكات بين القطاعين العام والخاص في مجال المراقبة يمكنك استخدامها للحصول على أفكار بشأن المناصرة بمجرد تحديد الشواغل من خلال هذا الدليل.

1. تقييم المخاطر

إنّ دراسة أي شراكة بين القطاعين العام والخاص عادةً ما تكون مصحوبة بعدد من المخاطر القانونية والفنية والإنسانية التي يجب تقييمها قبل اتخاذ أي إجراء. وتتغير هذه المخاطر بتغير إطارك البحثي والسياق الأوسع الذي يكتنف الشراكة المعنية. نقترح عليك أن تقوم، أولاً وقبل كل شيء، بتحديد المخاطر المتعلقة بمشروعك الاستقصائي ومن ثم تقييمها. ولمساعدتك في هذه المهمة، يمكنك الرجوع إلى القوائم غير الشاملة أدناه.

أ. المخاطر التي ينبغي مراعاتها

- التشهير: يكفل قانون التشهير حماية سمعة الشخص من أي تدخل غير مبرر. لذلك، فقد تخضع للمقاضاة بتهمة التشهير من جانب جهة خاصة إذا قمت بتوجيه الادعاءات ضدها. ذلك مع العلم بأن قوانين التشهير تختلف باختلاف الولايات القضائية، وقد تتحمل أنت عبء الإثبات برمته.
- الحصول غير المشروع على المعلومات: ثمة أنواع معينة من أعمال الاستقصاء قد تكون مخالفة للقانون (مثل نشر المعلومات المسربة أو القرصنة) حسب الولاية القضائية التي تعمل في نطاقها.
- الملكية الفكرية: الأسرار التجارية وحقوق الطبع والنشر هما مثالان من الحقوق المحمية بموجب قوانين الملكية الفكرية الذي قد تنتهكه بينما تقوم بعملك الاستقصائي.
- المخاطر على الأشخاص (الموظفون والمصدر والشركاء...): لا ينبغي القيام بأي نشاط يمكن أن يعرض حياة شخص معني أو مشارك للخطر، ما لم تكن هناك إجراءات محددة يجب اتخاذها للحد من المخاطر. قد تشمل المخاطر، على سبيل المثال لا الحصر: الضرر الجسدي، والضرر النفسي، والضرر الاجتماعي، والضرر الاقتصادي، والضرر القانوني.
- الإضرار بالسمعة: المخاطر على موضوعية مؤسستك أو حيادها أو مصداقيتها. قد تشمل المخاطر: الحقائق غير الدقيقة والبيانات غير المدعومة بشكل كافٍ واستغلال رصد وسائل التواصل الاجتماعي (SOCMINT) والمصادر المفتوحة الأخرى (OSINT) دون مراعاة الخصوصية، وما إلى ذلك.

ب. إجراءات التخفيف المقترحة

فيما يلي بعض الإجراءات المقترحة للحد من هذه المخاطر. هذه الإجراءات ليست شاملة، وقد لا تكون كافية وحدها للحد من جميع المخاطر بنجاح.

- منهجية بحث قوية: الاستشهاد بالمصادر وتقييم جودة المصادر والتقاط الصور ومقاطع الفيديو واستخدام اللغة المناسبة.
- التثبت من المعلومات: التثبت من المصادر والشهادات المتعددة للتأكد من صحة المعلومات.
- تنقيح الوثائق وتنظيفها: تنقيح البيانات الشخصية وإزالة البيانات الوصفية من الوثائق.
- التحضير قبل التحدث للجمهور أو عمل لقاءات إعلامية لاستخدام لغة مناسبة.
- الاحتفاظ بالمصادر الأصلية وتخزينها بأمان.
- مراعاة سلامة الأشخاص (الموافقة وإخفاء الهوية وغير ذلك الكثير) قبل اتخاذ أي إجراء.

2. كشف المعلومات

ليس من السهل عادةً الحصول على معلومات كافية عن أي شراكة بين القطاعين العام والخاص، لا سيما عندما يتطلب الأمر مشاركة جهات حكومية حساسة، مثل أجهزة الاستخبارات ووكالات إنفاذ القانون. كما أنّ المعلومات المتعلقة بهذه الأنشطة غالبًا ما تكون محجوبة عن العامة بشكلٍ مقصود، وتكون أيضًا محمية بقوانين وعقوبات صارمة.

لكن يمكن الوصول إليها بشكل آمن، إذ ثمة وسائل وموارد عديدة يمكن أن تساعد في هذا الشأن. والعديد من هذه المصادر متاحة ويمكن الوصول إليها بسهولة عبر الإنترنت، بينما هناك مصادر أخرى تتطلب عملاً مكتبيًا ومشاركة أشخاص يمكنهم تقديم المساعدة.

غير أنّ هذه المصادر ليست جميعها متاحة للوصول بسهولة أو يمكن الوصول إليها بأمان من أي مكان: من المعروف أن الحكومات حول العالم تعاقب النشطاء والصحفيين وغيرهم بتهمة الكشف أو حتى البحث عن معلومات بشأن العقود بين الجهات والمؤسسات العامة والشركات الخاصة، بالتالي يكون من الضروري تقييم المخاطر والعمل على الحد منها.

أ. استخدام قوانين الوصول إلى المعلومات

إن طلبًا بموجب قانون حرية المعلومات أو غير ذلك من قوانين الوصول إلى المعلومات (مثل قوانين الحق في المعلومات) هو طلب رسمي تقدمه إلى هيئة عامة (السلطات المحلية أو الإقليمية أو البلدية أو الشرطة أو الوزارة أو ما إلى ذلك) من أجل الوصول إلى المعلومات التي يحق للجمهور معرفتها. فقد تحاول الحصول على عقد أبرمه الشركاء، أو بعض المراسلات (رسائل البريد الإلكتروني أو الخطابات) بين الشركاء أو بعض الإحصائيات الرسمية أو مجرد رد على سؤال أو حتى وثائق أخرى مثل العرض الذي قدمته الشركة إلى السلطة العامة. وهناك بعض القوانين التي تحدد ما يمكنك وما لا يمكنك طلبه - في أوغندا، مثلاً، يتعين عليك طلب وثائق معينة، مما يعني أنه لا يمكنك طرح الأسئلة.

والمعلومات التي يتم الحصول عليها من خلال هذه الطلبات هي أداة مهمة وقيمة بالنسبة للصحفيين والنشطاء والجمهور: كلما زادت المعلومات المتاحة للجمهور، زادت معرفتنا كمجتمع وكان من الأسهل المطالبة بالتغييرات.

ومع ذلك، فعلى الرغم من أنّ هذه القوانين عادةً ما تعد بالكثير، وأنّ أكثر من 90 دولة لديها قوانين تقتضي من المسؤولين تقديم السجلات العامة، فإنّ حملهم على إتباع القانون والقيام بذلك ليس بهذه البساطة من الناحية العملية.

وعند تقديم مثل هذه الطلبات، من المهم ألا تنسى بعض التوصيات المهمة:

- تأكد من أنّ ما تبحث عنه ليس متاحًا بالفعل
- اعرف الجهة التي تراسلها

- اجعل الطلب محددًا!
- تحدث بلغتهم
- تحلّ بالصبر!

لدى برايفسي إنترناشيونال دليل يحدد بعض الدروس التي تعلمناها من تعبئة مثل هذه الطلبات حول العالم.

لدى الشبكة العالمية للصحافة الاستقصائية قائمة ممتازة لموارد حرية المعلومات المتاحة في العديد من الدول على مستوى كل قارة. ونحن نوصيك بالاطلاع عليها - تتضمن هذه القائمة العديد من أدلة حرية المعلومات التي نعتمد عليها في عمانا.

من المهم ألا تنسى أن السجلات العامة قد تكون موجودة في ولايات قضائية أخرى وقد تكون مفيدة جداً للكشف عن معلومات مهمة. وفي حال كان مقر الشركة في دولة ولكنها تزاول نشاطها في دولةٍ أخرى، فقد يكون من المفيد تقديم الطلبات في أي من أو كلا من الدولتين. على سبيل المثال، استطاع بعض الصحفيون الحصول على مزيد من المعلومات حول توفير تكنولوجيا المراقبة إلى مقدونيا الشمالية عن طريق تقديم طلبات إلى السلطات في المملكة المتحدة التي أشرفت على إذن التصدير. وعلى الرغم من ذلك، فإن بعض الدول (مثل الهند) لا تسمح إلا بطلبات المواطنين.

ماذا يقول شركاؤنا:

على الرغم من أنّ قوانين الوصول إلى المعلومات قد تعتبر أدوات مفيدة، إلا أنها قد تكون مخيبة للآمال أيضًا. لذلك، ينبغي أن تضع في اعتبارك أنّ طلبك قد لا يتلقى ردًا، ومن ثم عليك أن تخطط لاستخدام وسائل أخرى للحصول على المعلومات.

أخبرنا بعض شركائنا أنهم وجدوا طلبات المعلومات مفيدة للغاية في تأكيد الأشياء التي حصلوا عليها بالفعل من مصادر أخرى، بينما وجدها آخرون أشد فائدة من منظور الاتصالات العامة أو من حيث إنها تسمح بمعرفة المزيد من سبب رفض الطلب.

ب. المصادر الأخرى

1) المعلومات المستمدة من مصادر علنية

عند محاولة الحصول على مزيد من المعلومات حول الشراكات بين القطاعين العام والخاص، يكون هناك الكثير من المصادر المتاحة للعامة التي يمكن أن توفر معلومات إضافية - يُشار أحيانًا إلى عملية جمع هذه المعلومات واستخدامها باسم "المعلومات المستمدة من مصادر علنية".

توسعت منظمات مثل Bellingcat في استخدام المعلومات المستمدة من مصادر علنية للكشف عن الممارسات الحكومية غير القانونية وانتهاكات حقوق الإنسان - يشمل ذلك بعض الوكالات الحكومية الأشد حماية وسرية في جميع أنحاء العالم.

على أنّ الوصول إلى معلومات مفيدة إنّما يعتمد على عدد من العوامل، منها البلد محل الشراكة، ونوع الشركة الضالعة في الشراكة، ونوع التكنولوجيا أو الخدمة التي تقدمها.

ثمة موارد متعددة عبر الإنترنت وعبر المنشورات توفر معلومات حول جمع المعلومات المستمدة من مصادر علنية، منها ما يلي:

- Bellingcat
- i-intelligence
- مركز تاو للصحافة الرقمية
- إطار المعلومات المستمدة من مصادر علنية

هناك العديد من الأساليب التي تثير مسائل أمنية وأخلاقية وقانونية يجب أخذها في الاعتبار. اشترك مركز حقوق الإنسان في كلية الحقوق في بيركلي مع مكتب المفوض السامي للأمم المتحدة لحقوق الإنسان في إعداد دليل استخدام المعلومات المستمدة من مصادر علنية في التحقيق في انتهاكات القانون الجنائي الدولي وقانون حقوق الإنسان والقانون الإنساني الدولي، حيث توجد بعض الإرشادات بشأن هذه الاعتبارات.

فعلى سبيل المثال، يذكر الدليل أنّ تزييف هويتك على وسائل التواصل الاجتماعي قد يكون غير قانوني في بعض الولايات القضائية. وحتى لو لم يكن كذلك، فربما يظل يشكل انتهاكًا لشروط الخدمة الخاصة بشركات وسائل التواصل الاجتماعي، إذ في حالة استخدام هوية مزيفة للوصول إلى معلومات يتعذر الوصول إليها أو التماسها بطريقة أخرى من قبل فرد أو مجموعة، فقد يمثل ذلك مخالفةً للمبادئ الأخلاقية أو القانون.

تشمل المصادر العلنية للبيانات ذات الصلة بالوصول إلى المعلومات المتعلقة بالشراكات بين القطاعين العام والخاص ما يلي:

- المواقع الإلكترونية للشركة، حيث يمكنها تقديم معلومات عامة عن منتجاتها ونشر قوائم عملائها في بعض الأحيان.
- ملفات الشركة المقدمة للجهات التنظيمية التي غالبًا ما تتضمن معلومات مهمة مثل الأنشطة التجارية والهيكل التنظيمي والإيرادات. وقد تمكن الباحثون من إجراء تحليلات مفصلة للهياكل المؤسسية للشركات باستخدام مثل هذه المعلومات. وهذه المعلومات متاحة على منصات مثل .OpenCorporates
- إعلانات الوظائف المنشورة على مواقع التوظيف ومواقع التواصل الاجتماعي التي يسهل الوصول إليها عادةً مثل LinkedIn. وغالبًا ما تقدم هذه الإعلانات قرائن أو تفاصيل حول الأنشطة التجارية التي تزاولها الشركة ومكان هذه الأنشطة، وماهية الابتكارات التي في طور الإعداد: على سبيل المثال، فقد تمكن صحفي بريطاني من الوصول إلى معلومات على "قاعدة بيانات فائقة" حكومية سرية باستخدام المعلومات المتاحة في إعلانات الوظائف.
- بيانات الشحن والتجارة المتاحة للعامة من قبل بعض الحكومات والشركات. على سبيل المثال، تنشر السلطات الهندية بيانات الشحن المتعلقة بالواردات والصادرات، وهذه البيانات يمكن الوصول إلى بعضها بعد ذلك عبر المواقع التجارية على الإنترنت. ويمكن استخدام هذه البيانات لمعرفة صادرات معينة: على سبيل المثال، استطاعت Forensic News أن تعرف من خلال بيانات الشحن أنّ شركة برمجيات تجسس إسرائيلية قد شحنت معدات إلى الشرطة السرية في أوزبكستان.
- بيانات شفافية المساعدات الحكومية. غالبًا ما توضح هذه البيانات الحالات التي عمدت فيها السلطات الحكومية إلى تقديم معدات أو تمويل أو تدريب لنظرائها في جميع أنحاء العالم، وبالتالي توفر معلومات حول البرمجيات أو المعدات التي يمكنهم الوصول إليها. على سبيل المثال، فقد أمكن باستخدام بيانات المساعدات الأمريكية تحديد شركات المراقبة التي قُدمت منتجاتها إلى الحكومات في أمريكا الوسطى.
- وسائل التواصل الاجتماعي، ومنها على سبيل المثال الشبكات الاجتماعية المهنية مثل LinkedIn. تُعد هذه الوسائل مصدرًا شائعًا يمكن للصحفيين استخدامه للوصول إلى معلومات معينة عن الأفراد والشركات، ولكن يجب استخدامها بشكل أخلاقي وقانوني (انظر أعلاه).

2) بيانات متعلقة بالمشتريات

تُعد بيانات المشتريات الحكومية من أفضل المصادر العلنية للعثور على معلومات حول الشراكات بين القطاعين العام والخاص، إذ تتوافر مواقع المشتريات الحكومية المركزية بالإضافة إلى وثائق المناقصات على مواقع الوكالات الحكومية المخصصة لهذا الغرض، على أنّ التفاصيل المتعمقة غالبًا ما تكون مقيدة.

كما يمكن الحصول على معلومات قيمة من المعلومات المتاحة للجميع عن المناقصات - الإخطارات التي توضح أن هيئة حكومية تسعى للحصول على خدمة أو منتج من القطاع الخاص. وعلى الرغم من أن المناقصات توفر معلومات عامة فقط، لكن يمكن استخدامها أيضًا كأساس لإجراء المزيد من البحوث، بما في ذلك عن طريق تقديم طلب حرية الوصول إلى المعلومات.

على سبيل المثال، توجد في المملكة المتحدة منصة مركزية متاحة للجمهور وقابلة للبحث فيها تتيح لأي شخص البحث عن مناقصات الوكالات الحكومية (على أنّ كثيرًا من التفاصيل تُحجب في الواقع لأسباب تتعلق بالأمن القومي).

وعلى نحو مماثل، تعمد الولايات المتحدة والاتحاد الأوروبي وروسيا ودول أخرى حول العالم إلى نشر المناقصات على المواقع الحكومية.

على سبيل المثال، تمكن الصحفيون، باستخدام وثائق المشتريات الحكومية هذه في الفترة التي سبقت دورة الألعاب الأولمبية الشتوية في سوتشي عام 2014، من تحديد الكيفية التي كانت تخطط بها الأجهزة الأمنية الروسية لمراقبة اتصالات الهاتف والإنترنت خلال فعاليات الألعاب.

ومثال آخر، بعد أن نمى إلى علمها طرح Frontex (الوكالة الحدودية التابعة للاتحاد الأوروبي) مناقصة للبحث عن شركة مراقبة لتعقب الأشخاص على وسائل التواصل الاجتماعي، ردت برايفسي إنترناشيونال بطرح أسئلة مفصلة بشأن قانونية الخطة. وبعد يومين ألغت Frontex المناقصة.

إضافة إلى ذلك، فإنّ هذه المواقع نفسها أو ما شابهها توفر في بعض الأحيان معلومات بشأن ماهية العقود التي تمت ترسيتها وماهية الشركات التي وقعت عليها الترسية. على سبيل المثال، توفر مواقع المشتريات الفيدرالية في الولايات المتحدة بيانات عن ماهية الشركات التي حصلت على عقود. ويستخدم الصحفيون هذه المواقع عادةً للوصول إلى مثل هذه المعلومات والإبلاغ بها، على الرغم من أن التفاصيل عادةً ما تكون ضئيلة. ويوفر موقع Tech Inquiry منصة قابلة للبحث فيها يمكن من خلالها البحث عن العقود التي أبلغت بها السلطات الأسترالية والكندية والأمريكية والبريطانية.

لدى برايفسي إنترناشيونال أيضًا دليل موجه للباحثين والصحفيين بشأن بعض المصادر العلنية المتاحة التي يمكن استخدامها لتحديد الصادرات في مجال المراقبة.

تتوفر دورة مجانية عبر الإنترنت لمعرفة المزيد حول الخصوصية والبحث في تكنولوجيا المراقبة أعدتها برايفسي إنترناشيونال على .Advocacy Assembly

3) أصحاب المصلحة كمصادر للمعلومات

إضافة إلى البحوث المكتبية والطلبات الرسمية، فإن التواصل مع الأشخاص المنخرطين في الشراكات بين القطاعين العام والخاص أو الذين قد تتوافر لديهم معرفة بشأن هذه الشراكات يمكن أن يساعد في الوصول إلى معلومات أو وجهات نظر تكون ذات أهمية كبيرة بالنسبة لعملك.

كما يمكن الاستفادة من الأكاديميين وأعضاء الحكومة والأشخاص العاملين في شركات خاصة مماثلة كمصادر للمعلومات المفيدة لعملك، بشرط التواصل معهم بشكل مناسب مع تطبيق ممارسات بحثية مناسبة (مثل إخفاء الهوية).

ولعل الصحفيين الذين غطوا الشراكة التي تبحث بشأنها قد تمكنوا أيضًا من الوصول إلى مصادر مهمة ويكون لديهم استعداد لتزويدك بتفاصيل إضافية عند الاتصال بهم مباشرة.

بالمثل، فقد تكون هناك منظمات أو مجموعات أخرى تبحث بشأن الشراكة نفسها؛ لذلك، حاول التنسيق مع هذه المجموعات لتبادل المعلومات وربما لتعزيز المناصرة لاحقًا.

عند التواصل مع الأشخاص الضالعين مباشرة في الشراكة المعنية، يجب عليك التأكد من أنهم يشعرون بالأمان وأنك تتفهم موقفهم، ذلك أنّ استيعاب الآخرين وتجنب الاتهامات هما عاملان أساسيان للحصول على المعلومات المهمة، ومن ثم ينبغي أن تكون دائمًا مراعيًا لشواغلهم. ومن المهم في جميع الأحوال أن تناقش شروط هذا التبادل للمعلومات وأن تتفق على هذه الشروط مسبقًا. ولا تتردد أبدًا في طلب المساعدة والمشورة إذا كنت محتارًا بشأن كيفية التعامل مع المصدر.

إخلاء المسؤولية: قبل إجراء أي مقابلة، تأكد من أنك أجريت تقييمًا مناسبًا للمخاطر ودرست بجدية المخاطر التي تتعرض لها مؤسستك، وكذا الأشخاص الذين تتحدث معهم. عليك أن تتأكد من قدرتك على توفير مستوى مناسب من الخصوصية والأمان، وأنك مدرك للعواقب القانونية، قبل التعامل مع الأشخاص الذين قد يعرضون أنفسهم للخطر من خلال تبادل المعلومات.

ماذا يقول شركاؤنا:

إذا كانت الشراكة بين القطاعين العام والخاص التي تبحث بشأنها تستهدف مكانًا معينًا أو منطقة معينة، فإنّ البحث في الصحف المحلية ومجموعات Facebook والمنظمات المحلية يمكن أن يكشف عن معلومات مهمة. فهذه المجموعات ربما تكون قد وصلت إلى معلومات غير معروفة على نطاق واسع أو ربما تكون متصلة بأشخاص رئيسيين ضالعين في الشراكة.

ذات مرة، حصلت ADC في الأرجنتين على معلومات مهمة عن طريق البحث في مجموعة على Facebook لمواطنين يحاولون الاحتشاد ضد مشروع يجري تنفيذه في منطقتهم.

وقد وجد شريكنا، الذي يفضل عدم ذكر هويته، أن إجراء مقابلات مع أصحاب مصلحة غادروا مؤسسة ما مؤخرًا يمكن أن يساعدك مثلاً على فهم المواضع التي لا تعبر بدقة عن الواقع.

قائمة مرجعية

ج. قائمة مرجعية - كشف المعلومات

لمساعدتك في بحثك، ربما عليك استخدام القائمة المرجعية هذه:

- هل راعيت العواقب الأخلاقية والقانونية والأمنية للوصول إلى و/ أو تبادل المعلومات التي تبحث عنها؟
- هل راعيت المخاطر المحتملة وعمليات التخفيف الخاصة بسياق وظروف عملك؟
- هل المعلومات التي تبحث عنها يسهل الوصول إليها بالفعل في المجال العام؟
- هل يوجد في الولاية القضائية التي تهتم بها قانون لحرية المعلومات أو قانون للوصول إلى الوثائق يمكنك استخدامه؟
- هل توجد أدلة أو دورات ذات صلة متاحة حول كيفية استخدام بعض أساليب البحث في المصادر العلنية التي قد تساعدك في العثور على ما تبحث عنه؟
- هل هناك أي مصادر علنية يمكنك الوصول إليها في بلدك للعثور على المعلومات؟
- هل هناك أي مصادر علنية يمكنك الوصول إليها في الخارج للعثور على المعلومات؟
- هل هناك أي أفراد أو منظمات يمكنهم مساعدتك في العثور على المعلومات ويمكنك التعامل معهم بأمان؟
- هل منحتك مصادرك الموافقة المناسبة عن علم؟
- هل نظرت في كيفية التعامل مع المعلومات التي تتلقاها من مصادرك؟
  - أين ستحفظ المعلومات؟
  - هل تحتاج إلى إخفاء هويتها؟ أو إعطائها اسمًا مستعارًا؟
  - هل تحتاج إلى تنقيح المعلومات؟ كيف ستفعل ذلك بدقة؟
  - هل توجد أي تفاصيل سياقية في المعلومات قد تشير إلى مصدرك أو أي شخص آخر؟

3. كشف التكنولوجيا الأساسية وفهمها

إنّ التكنولوجيات التي تتمحور حولها الشراكة بين القطاعين العام والخاص قد تكون محاطة بالسرية والغموض على نحوٍ يجعل من الصعب على الجهات الخارجية تقييم المخاطر. وهذا يتمثل في أمورٍ عدة بدءًا من استخدام الكلمات الطنانة وصولاً إلى استخدام المصطلحات التقنية الغامضة، وبالتالي فإنّ الحصول على فهم حقيقي لماهية التكنولوجيا وما تقوم به في الواقع ليس بالمهمة السهلة. لذلك، فإنّ هذا القسم مصمم لتزويدك بإرشادات تساعدك في العثور على مزيد من المعلومات عن التكنولوجيا، فضلاً عن فهمها وتحديد العيوب المحتملة المرتبطة بها.

أ. تحديد مكونات التكنولوجيا

عند دراسة أي تكنولوجيا، فإنّ الخطوة الأولى تتمثل في البحث عن معلومات أساسية عنها - لتعريفها وتصنيفها. ولعل استعراض صفحة ويكيبيديا الخاصة بالتكنولوجيا المعنية غالبًا ما يكون نقطة انطلاق جيدة من شأنها مساعدتك في استيضاح ما تنطوي عليه هذه التكنولوجيا (مثل التعرف على الوجه). وهذا مفيد بشكل خاص عندما لا تكون هناك تكنولوجيا محددة مذكورة في الشراكة أو عندما تبحث في مناقصةٍ ما. وربما عليك أيضًا أن تراجع المواد التسويقية للشركة للتعرف على تخصصها ونوع المنتج الذي تقدمه.

تنطوي الشراكة أحيانًا على أكثر من تكنولوجيا، عبر عقود و/أو شراكات متعددة أحيانًا - مثل نظام هوية قد يتطلب ماسحًا ضوئيًا لبصمات الأصابع وقاعدة بيانات قد توفرها شركات مختلفة.

أن تحصل على فهم عام لما تبحث عنه، فهذه خطوة بسيطة ولكن مهمة لكي تتمكن من المضي قدمًا وتحديد المخاطر. فهدفك هو أن تكون قادرًا على تقديم تعريف واسع ودقيق رفيع المستوى لماهية التكنولوجيا في الشراكة.

فيما يلي أمثلة لتوصيفات رفيعة المستوى للتكنولوجيا:

- نظام التعرف على الوجه - نظام قادر على مطابقة وجوه محددة في صورة أو مقطع فيديو مع مجموعة بيانات لوجوه بشرية جرى تحديدها مسبقًا.
- سوار التعقب المثبت في الكاحل - سوار مادي مثبت في طرف شخص ما قادر على تسجيل وإرسال معلومات الموقع الجغرافي أو الجوار بعلامة أساسية.
- الطائرة المسيّرة - طائرة ذاتية التحكم أو مسيّرة عن بعد قادرة على اتخاذ إجراءات محددة مسبقًا وجمع البيانات البيئية مثل الصور ودرجات الحرارة والأصوات ثم معالجة هذه البيانات ونقلها.

بمجرد الانتهاء من تنفيذ الخطوة الأولى، فلن تلبث حتى تدرك أن التكنولوجيات تعتمد عادةً على عدة عناصر مادية ومنطقية لتؤدي وظائفها. بالتالي، فإن تقسيمها وتحديد كل طبقة منها هو الخطوة المنطقية التالية لفهم الكيفية التي تعمل

بها التكنولوجيا وتحديد نقاط الفشل المحتملة. على سبيل المثال، يقوم نظام التعرف على الوجه باستخراج البيانات ونقلها وتخزينها ومعالجتها، وفي كل خطوة من هذه الخطوات، هناك عناصر مختلفة تلعب دورًا رئيسيًا.

قد تكون هذه الطبقات عبارة عن جهاز أو برنامج أو مزيج من الاثنين. غير أنّ جمع التكنولوجيات خلف مصطلح بسيط مثل "قاعدة بيانات" قد يكون مسألة معقدة. وبالتالي، كلما كنت أدق في تقسيمها إلى مكونات، كان لديك فهم أفضل لماهية التكنولوجيا وطبيعة مخاطرها المحتملة.

وباستخدام مقاربة متمحورة حول البيانات، سنجد أنّ العناصر المختلفة المكونة للتكنولوجيا عادةً ما تندرج ضمن إحدى الفئات الأربع التالية:

1) طريقة جمع/ استخراج البيانات (الأجهزة/ البرمجيات)

جمع البيانات هو عملية تُستخدم لاستخراج المعلومات. قد يتمثل ذلك في كاميرا تلتقط صورة، أو مستشعر يستقي معلومات مثل درجة الحرارة، أو برمجيات تسجل إجراءً مثل النقر على زر أو أحد أجهزة استخراج بيانات الهاتف محمول يستخرج البيانات من الهاتف. وأنظمة جمع البيانات هذه قد تكون أجهزة مادية، مثل قمر صناعي مزود بمستشعرات، أو وسائل افتراضية، مثل تطبيق أو تقنية تجريف الويب (تقنية كودية يتمثل عملها في الزحف عبر الإنترنت لجمع البيانات).

سبب الأهمية

أن تفهم جزء التكنولوجيا المسؤول عن جمع البيانات، فهذا يجعلك تفهم ماهية البيانات المُجمّعة (صور، صوت، بيانات أدخلها المستخدم)، ومصدر هذه البيانات (مستشعرات، تفاعلات المستخدم) وطبيعة الظروف التي تكتنف عملية جمعها (بمعرفة الشخص أو دون معرفته، كم مرة، وما إلى ذلك). وهذا يسمح لك بتحديد المشكلات المحتملة المتعلقة بقانونية عملية الجمع أو دقة البيانات المُجمّعة.

أمثلة لنظام جمع البيانات:

- شبكة من الكاميرات في المدينة
- موقع إلكتروني للتسجيل في فعالية عامة
- قمر صناعي مزود بمجموعة متنوعة من المستشعرات يلتقط صورًا لمنطقة معينة
- آلة قراءة بصمات الأصابع في المطار

المخاطر المحتملة في جمع البيانات

قد تكون البيانات المجمّعة غير صحيحة، وقد تتعرض المستشعرات للتلاعب، وقد تُجمع البيانات من دون موافقة أو أي أساس قانوني آخر، وقد تتدهور المستشعرات المادية بمرور الزمن، وقد تكون الأسس المنطقية أو مجموعة التعليمات (بالنسبة لبرمجيات معينة) متحيزة أو غير صحيحة، وقد يكون الجهاز معرضًا للهجوم (يتعرض لحمل زائد، ويُزود بمعلومات خاطئة، وما إلى ذلك).

2) طريقة نقل البيانات (الأجهزة/ البرمجيات)

من الممكن أن تُنقل البيانات، بمجرد جمعها، إلى نظام آخر لأغراض التخزين أو المعالجة، كالخادم على سبيل المثال. تحدث عمليات النقل هذه في العادة عبر الحلول القائمة ذات البروتوكولات المحددة جيدًا مثل حزمة بروتوكولات الإنترنت ((TCP/IP) للاتصال بين الأجهزة على نفس الشبكة (مثل خادمين متصلين بالإنترنت أو كاميرا ذكية وجهاز كمبيوتر متصلين بشبكة خاصة)، ولكن قد يُستخدم أحيانًا ابتكار محفوف بالمخاطر (ومثال على ذلك هو اقتراح IP الجديد الذي قدمته الصين في الاتحاد الدولي للاتصالات (ITU) أو تقنية 5G New Radio، المعيار العالمي للواجهة الهوائية لشبكات الجيل الخامس).

سبب الأهمية

أن تدرك ما إذا كانت البيانات تُنقل وتفهم الكيفية التي تُنقل بها، فهذا يسمح لك بتحديد المخاطر الأمنية المحتملة (إذا لم يكن النقل مؤمّنًا، على سبيل المثال باستخدام شبكة Wi-Fi غير آمنة)، أو الشواغل القائمة (إذا كان البروتوكول قديمًا/ الشبكة قديمة وتنطوي على ثغرات أمنية معروفة مثل شبكات الجيل الثاني)، أو المتطلبات التقنية (بما في ذلك المسافة التي تعمل عليها تقنية بلوتوث لنقل البيانات بشكل موثوق) لتقييم الملاءمة بشكل أفضل في سياق معين.

أمثلة لأنظمة نقل البيانات:

- حزمة بروتوكولات الإنترنت (TCP/IP، البروتوكول الذي تُبنى عليه معظم تكنولوجيات الإنترنت)
- النظام العالمي للاتصالات المتنقلة (GSM)
- بلوتوث
- اتصالات الأقمار الصناعية عبر موجات الراديو العالية التردد

المخاطر المحتملة في نقل البيانات

قد تكون التكنولوجيا غير آمنة (أن يكون مستوى التشفير ضعيفًا أو منخفضًا، وأن تكون هناك ثغرات معروفة، وما إلى ذلك)، وقد تتدهور البيانات/ تُفقد أثناء عملية النقل، وقد تتعرض البيانات للاعتراض/ التلاعب، وقد يشكل النظام تهديدات

صحية، وقد يتعطل النظام بفعل عوامل خارجية (تعرض الشبكة لهجوم رفض الخدمة، وتدمير جهاز الإرسال/ الاستقبال، وما إلى ذلك).

ملحوظة: لمعرفة المزيد عن البروتوكولات والمعايير وهيئات المعايرة، انظر "ملحوظة بشأن البروتوكولات والمعايير الفنية" في نهاية هذا الفصل.

3) طريقة تخزين البيانات (الأجهزة/ البرمجيات)

بعد استخراج البيانات ونقلها، فقد يتم تخزينها في مكان ما لأغراض المعالجة والأرشفة. عادةً ما تعتمد أنظمة التخزين على شكل من أشكال أجهزة التخزين مثل محرك الأقراص الثابتة، وبطاقة SD، ووحدة USB، وغالبًا ما يكون ذلك في إطار نظام أكبر إذا الأمر يستلزم وصولاً منتظمًا (كمبيوتر محمول، خادم ...). وثمة تنوع هائل في البرمجيات المسؤولة عن تخزين هذه البيانات والوصول إليها، بدءًا من برمجيات قواعد البيانات مثل MySQL وصولاً إلى الأنظمة المستندة إلى سلسلة الكتل التي توفر الثبات.

سبب الأهمية

أن تتعرف على مكان تخزين البيانات وطريقة تخزينها، فهذا يمكّنك من تحقيق فهم أفضل للتداعيات (قد تكون البرمجيات/ الطريقة المستخدمة عرضة للثغرات الأمنية أو الاستهداف المتكرر بالهجمات مثل قاعدة بيانات ElasticSearch أو غير ذلك من منتجات التخزين Bucket المشابهة)، والاحتفاظ (قد يسمح النظام بتخزين البيانات لفترة معينة من الوقت فقط أو، على العكس من ذلك، قد يسمح بتخزين البيانات إلى أجل غير مسمى مثل نظام سلسلة الكتل)، ومراقبة الوصول (يمكن للنظام الذي يطبق نهجًا فضفاضًا بشكل مفرط لمنح الأذونات أن يسمح بوصول غير مصرح به) والاستدامة (العمر المتوقع لبطاقة SD أقل من عمر SSD على سبيل المثال). فهل نظام تخزين البيانات المختار مناسب للغرض المتوخى؟ كما أنّ معرفة مكان نظام التخزين وما الذي يتصل به ومن الذي يتمتع بالوصول إليه تمنحك مفاتيحًا مهمة يمكن استخدامها لإجراء تقييمًا أفضل للمخاطر.

أمثلة لأنظمة نقل البيانات:

- محرك أقراص ثابت/ وحدة USBبنظام ملفات محدد (NTFS, exfat, ext4…)
- قاعدة بيانات SQL (قاعدة بيانات برمجية مصممة للوصول إليها باستخدام لغة SQL)
- نسخ سلسلة كتل عبر عدة وحدات تابعة
- قرص مدمج غير قابل لإعادة الكتابة عليه (CDR-R)
- برمجيات جدول البيانات مثل Microsoft Excel

المخاطر المحتملة في تخزين البيانات

سوء إدارة الأذونات مما يسمح بالوصول غير المصرح له للبيانات، وقابلية حدوث خطأ عند التخزين المادي على الأجهزة (على سبيل المثال، يمكن أن يفشل القرص وبالتالي تُفقد البيانات المخزنة عليه)، وعدم توافر ما يكفي من قدرات الاحتفاظ بالبيانات (على سبيل المثال، تقوم سلسلة الكتل بتخزين بيانات يتعين محوها)، وعدم توافر مساحة كافية للتخزين (على سبيل المثال، تعذر تخزين بيانات جديدة لعدم وجود مساحة)، وانخفاض متوسط العمر المتوقع (على سبيل المثال، اختيار إدارة لبرمجيات قواعد البيانات لا تدعمها الشركة المصنعة ولا تتلقى تحديثات الأمان المناسبة أو لن تتلقاها قريبًا) وما إلى ذلك.

4) طريقة معالجة البيانات (البرمجيات)

بمجرد استخراج البيانات أو بعد تخزينها، يمكن معالجتها لإنتاج معلومات جديدة. وقد يتمثل ذلك في صورة برمجيات تحليلية تحدد ماهية الأشياء المرئية في صورةٍ ملتقطة، أو خوارزمية تعطي الحل لمشكلة رياضية أو برنامج يتنبأ بدرجات الحرارة بناءً على بيانات مجمّعة مسبقًا. ويمكن لأنظمة معالجة البيانات إما معالجة البيانات آليًا (بدون تخزين البيانات في خطوات وسيطة) أو استخدام البيانات المخزنة. وهذه الأنظمة في العادة عبارة عن برمجيات مطورة باستخدام مجموعة من لغات البرمجة (Java وPython وGo ...) وقد تؤدي وظيفتها عبر اتصال بنظام تخزين البيانات. كما يمكن تشغيلها على مجموعة متنوعة من الأجهزة بدءًا من الخادم ووصولاً إلى الهاتف الذكي أو وحدة التحكم الدقيقة ذات اللوحة الواحدة. وثمة أنظمة معينة، مثل الذكاء الاصطناعي المعتمد على الشبكات العصبية، سوف تؤدي وظيفتها بشكل مختلف بناء على البيانات التي تعالجها، ليس هذا فحسب، ولكن أيضًا بناء على البيانات التي دُربت عليها. وفي هذه الحالة، قد يكون من المفيد التعامل مع مجموعة بيانات تدريب نظام الذكاء الاصطناعي كمكون منفصل ضمن فئة جمع/ استخراج البيانات. إذ كلما قمت بفصل المكونات المختلفة بشكل أفضل، كان لديك فهم أفضل لماهية المكون المحفوف بالمخاطر.

سبب الأهمية

قد تنتج أنظمة معالجة البيانات معلومات متحيزة وغير دقيقة، سواء بسبب البيانات المُدخلة في النظام (كأن تكون غير مكتملة أو غير دقيقة أو غير تمثيلية ...) أو بسبب عيوب منطقية (شيء غير معروف في منطق الخوارزمية). لذلك، فإنّ فهم الغرض من تصميم المعالجة، وماهية البيانات الخاضعة للمعالجة، ونوع المعلومات الناتجة عن المعالجة، يمكن أن يسمح لك باكتشاف العيوب المحتملة في منطق الكود أو المتغيرات المفقودة أو تقييم مدى ملاءمة النظام لاتخاذ القرار.

أمثلة لأنظمة معالجة البيانات:

- برمجيات للتعرف على الوجه تعالج صورًا التقطتها الكاميرات العامة
- برمجيات لاكتشاف حركة القوارب باستخدام الذكاء الاصطناعي وصور الأقمار الصناعية

- نظام إعلان يستنتج سمات شخصيتك بناءً على بيانات جُمعت عبر الإنترنت
- مساعد افتراضي مثل Siri/Google/Alexa

المخاطر المحتملة في معالجة البيانات

عيوب في منطق الخوارزمية (شيء غير محسوب أو خطأ بشري يجعل النتائج خاطئة)، وضعف الدعم من الشركة المصنعة (تفقد البرمجيات الدعم بعد وقت معين مما يجعل التطوير والإصلاحات المستقبلية معقدة أو مستحيلة بالنسبة للمشتري)، وضعف الشفافية/ المساءلة بسبب الترخيص (تجعل البرمجيات الاحتكارية عملية التدقيق معقدة أو مستحيلة)، والتحيز بسبب مجموعة البيانات التي جرى التدريب عليها أو البيانات التي جرى إدراجها, والثغرة الأمنية (الوصول غير المصرح به، والاختراق ...) وما إلى ذلك.

5) ملحوظة عن ترتيب مكونات التكنولوجيا من حيث الأولوية

إذا كنت تقوم بالبحث بشأن شركة معينة أو عقد معين، فيمكنك استخدام هذه التفاصيل والمعلومات للتركيز على الطبقات التي تشارك فيها الشركة بشكل أساسي. وإذا كنت تقوم بالبحث بشأن شركة متخصصة في معالجة البرمجيات والبيانات (مثل Palantir)، فأنت تعلم أنه من المحتمل أن تكون هذه هي الطبقة الرئيسية.

لا يعني هذا أنه يجب عليك إهمال الطبقات الأخرى للتكنولوجيا المنشورة، بل على العكس، هذه العناصر قد تُغفل أو يُساء إدارتها في النهاية نظرًا لأنها لا تكون بالضرورة جزءًا من خبرة الشركة أو الهيئة العامة. على سبيل المثال، قامت المملكة المتحدة بتخزين البيانات المتعلقة بجائحة كوفيد في ملف Excel ولكنها فقدته في نهاية المطاف، مما كشف عن ضعف الاهتمام باستخدام نظام تخزين البيانات، لا سيما بالمقارنة مع الجهد المبذول في جمع هذه البيانات.

ب. تقييم الحداثة/ الابتكار

قد تنطوي الشراكات بين القطاعين العام والخاص على تكنولوجيا معروفة جيدًا وواسعة الانتشار بالفعل في سياقات أخرى، إلا أنها قد تشكل أيضًا أساسًا للابتكار والحداثة.

وفي هذا الصدد، يمكننا تحديد نوعين رئيسيين من الابتكار:

1. تكنولوجيا جديدة لم تُستخدم على نطاق واسع أو لم تُنشر في سياق العالم الحقيقي (خارج المختبرات أو الأوراق البحثية)؛
2. إضافة مجموعة جديدة من الخصائص إلى تكنولوجيا قائمة يكون الهدف منها هو توسيع نطاق أدائها وقدراتها بشكل كبير.

وثمة أنواع أخرى من "الابتكار" قد تشمل نشر تكنولوجيا قائمة في سياقات جديدة. ولتقييم هذه الاستخدامات، سيستلزم هذا تحديد الشواغل المرتبطة بالحوكمة (القسم 4 أدناه).

1) تكنولوجيا جديدة كليًا

في حالة التكنولوجيا الجديدة كليًا، يكون عامل الحداثة واضحًا لأنّ التكنولوجيا تكون غير معروفة جيدًا. كما أنّ التكنولوجيات الرائدة نادرة، وتفرض مخاطر متعددة لأنها لم تخضع بالضرورة للاختبارات المناسبة أو قد تنطوي على آثار جانبية غير متوقعة. لذلك، فإنّ الجهات الفاعلة الخارجية قد تجد من الصعوبة بمكان الاقتراب من أي تكنولوجيا جديدة كليًا، وقد يكون من الصعب أيضًا جمع المعلومات ذات الصلة بها. ومع ذلك، هناك العديد من المخاطر الشائعة التي تكون مصاحبة للابتكار وقد تكون جديرة بالاستكشاف:

- الفوارق بين بيئة الاختبار والعالم الحقيقي، مما يؤثر على كفاءة التكنولوجيا
- عدم خضوع التكنولوجيا لاختبارات كافية، ما يعني أنّ العينة التي نُشرت التكنولوجيا على أساسها هي التي تنفذ عمليًا الاختبار الأولي لها
- المبالغة في تقدير إمكانات التكنولوجيا ودقتها - لا تؤدي التكنولوجيا إلى أخطاء كثيرة جدًا
- التغاضي عن ظهور مشكلات جديدة - قد ينتج ذلك عن تكلفة الصيانة، أو استدامة المشروع ضمن الإطار الزمني المناسب، أو المشكلات الناشئة عن حالات الاستخدام في الظروف القصوى، أو أن الهيئة العامة ملتزمة بعقد لا يمكن لأي جهة أخرى الإيفاء به
- اتساع نطاق الاستخدام، حيث يمكن استخدام التكنولوجيا لأغراض تزيد على الغرض الأولي لتصميمها
- الافتقار إلى الشفافية/ المساءلة إذا كانت التكنولوجيا محمية بأسرار تجارية و/أو بموجب ترخيص الملكية

2) خصائص/ قدرات جديدة

في حالة التكنولوجيا القائمة ذات الخصائص أو القدرات الجديدة، قد يكون من الصعب تحديد الابتكار، ولكنه يمكن أن يؤثر تأثيرًا مهمًا على أوجه الاستفادة من التكنولوجيا. وقد تأتي الخصائص أو القدرات الجديدة نتيجة قفزة تكنولوجية على مستوى الأجهزة أو البرمجيات، بما في ذلك، على سبيل المثال، وحدات معالجة مركزية جديدة (CPUs) أقوى بكثير من الجيل السابق، أو تطورات تقنية جديدة مثل الحوسبة الكمومية. وبالنسبة للبرمجيات، فقد تتمثل القفزة التكنولوجية في تطوير تقنيات معالجة جديدة مثل ظهور التعلم العميق وحلول الذكاء الاصطناعي المكافئة.

وقد تتمثل هذه الابتكارات أيضًا في مجرد إضافة تكنولوجيا موجودة إلى أحد الحلول، بما في ذلك عن طريق تركيب مستشعرات تردد الراديو في العديد من الأقمار الصناعية الصغيرة (مثل CubeSat)، وهو ابتكار أصبح ممكنًا بفضل السعر الرخيص لهذه الأقمار الصناعية. وتتسم المخاطر التي تنشأ عن إضافة خصائص أو قدرات جديدة بأنها أكثر تميزًا وبالتالي ينبغي تحديدها بشكل أكثر سهولة. فيما يلي بعض المخاطر التي تنشأ عن مثل هذه الابتكارات:

- قد تكون القدرات المضافة غير ضرورية للتكنولوجيا كي تؤدي وظيفتها الأولية (على سبيل المثال، تجهيز الكاميرات القابلة للارتداء بمستشعرات لدرجة الحرارة)
- عدم إخضاع القدرات المضافة لاختبارات مناسبة للبيئة التي ستُستخدم فيها، مما قد يسفر عن نتائج غير مناسبة (على سبيل المثال، استخدام خوارزمية الشبكة العصبية للنظام القضائي)
- أن تتسبب الخاصية/ القدرة الجديدة في جعل التكنولوجيا أكثر تطفلاً (مثل تحسين جودة الصورة لكاميرات المراقبة المرئية)
- تؤدي الخاصية/ القدرة الجديدة إلى تعزيز كفاءة التكنولوجيا والسماح بالاستخدام الجمعي لها (على سبيل المثال اعتراض بيانات الإنترنت ومعالجتها بشكل جمعي)

3) ملحوظة بشأن البروتوكولات والمعايير الفنية

كما هو مذكور في قسم نظام نقل البيانات، تُعدُ البروتوكولات والمعايير من الأمور المثيرة للاهتمام التي ينبغي النظر فيها وفهمها عند تحليل تكنولوجيا ما؛ إذ يمكن الحصول من خلالها على معلومات عما إذا كانت التكنولوجيا تُنشر في بيئةٍ مطورة وموحدة بالفعل أم أنها تحاول تحديد معايير جديدة. وفيما يلي بعض التعريفات المفيدة وبعض المعلومات حول هيئات المعايرة التي قد تكون ذات صلة:

التعريفات:

- البروتوكول: البروتوكول هو لغة متفق عليها تسمح للعناصر المختلفة بالتواصل. وثمة العديد من البروتوكولات المستخدمة لعل أشهرها هو حزمة بروتوكولات الإنترنت، المعروفة أيضًا باسم TCP/IP. هذه البروتوكولات عادةً ما تكون موحدة وخاضعة لمجموعة معينة من القواعد. ومن خلال هذه البروتوكولات، تستطيع أي جهة فاعلة جديدة في السوق أن تطور بسهولة منتجًا قادرًا على استخدام البنية التحتية القائمة والاتصال بالمنتجات الأخرى. فعلى سبيل المثال، يمكن لأي شخص أن ينشئ باستخدام TCP/IP جهازًا متصلاً بالإنترنت من شأنه الاتصال بخادم أو أجهزة مماثلة حول العالم.
- المعيار الفني: المعيار الفني عبارة عن قاعدة أو شرط يخضع له تشغيل مهمة فنية. والمعايير الفنية أكثر تجردًا من البروتوكولات من حيث إنها لا تقدم قواعد قاطعة للغة برمجة أو تكنولوجيا معينة، وإنما تحدد مبادئ وطرقًا وعمليات موحدة ينبغي اتباعها عند تطوير التكنولوجيا. ويتمثل هدفها في ضمان قابلية التشغيل البيني بين الأجهزة والأنظمة (بما في ذلك، على سبيل المثال، التأكد من أن محرك أقراص ثابت خارجي من شركة أخرى غير الشركة المصنعة لجهاز الكمبيوتر الخاص بك سيعمل في أي جهاز كمبيوتر). ويمكن تطوير المعايير بصفة أحادية أو خاصة من قبل مؤسسات المعايرة. على سبيل المثال: الناقل التسلسلي العالمي (USB).

هيئات المعايرة:

- الاتحاد الدولي للاتصالات (ITU): الاتحاد الدولي للاتصالات هو مؤسسة تابعة للأمم المتحدة مسؤولة عن الاتصالات والمعايرة الراديوية. وهو يعمل على ضمان اتفاق الدول والجهات الفاعلة الخاصة على المعايير والبروتوكولات اللازمة لتجنب التعارض وتعزيز التطور. ويُشار إلى المعايير التي يضعها الاتحاد الدولي للاتصالات باسم التوصيات. فيما يلي بعض الأمثلة على أعماله:
  - إدارة استخدام طيف الترددات الراديوية (تحديد أي جزء من الطيف يمكن استخدامه والهدف من هذا الاستخدام والجهة التي يمكنها استخدام ذلك الجزء، على سبيل المثال، تعمل شبكة Wifi وبلوتوث على تردد من 2400 إلى 2500 ميغا هرتز)؛
  - تطوير تنسيق المستندات المفتوحة والحفاظ عليه، وهو مثال على تنسيق ملف مستند مجاني ومفتوح المصدر يمكن لأي مطور برمجيات استخدامه لمعالجة الكلمات؛
  - نشر التوصيات المتعلقة بتدريع الكابلات للحد من التداخل؛
  - تضع فرق العمل توصيات حول موضوعات مثل تكنولوجيات المعلومات الكمية للشبكات والذكاء الاصطناعي للقيادة بمساعدة والقيادة الذاتية.
- فرقة العمل المعنية بهندسة الإنترنت (IETF): هي مؤسسة للمعايير المفتوحة معنية بتطوير معايير الإنترنت الطوعية والترويج لها، وبخاصة المعايير التي تشكل حزمة بروتوكولات الإنترنت (TCP/IP).
- المنظمة الدولية لتوحيد المقاييس (ISO): هي هيئة معنية بوضع المعايير تتألف من ممثلين لمختلف منظمات المعايير الوطنية، وهي تنشر المعايير الفنية والصناعية والتجارية في جميع أنحاء العالم. ومن أمثلة المعايير: المعيار ISO 80601 الذي يضمن معايرة موازين الحرارة بنفس الطريقة في المستشفيات المختلفة.
- W3C: منظمة المعايير لشبكة الويب العالمية.

إنّ هيئات المعايرة التي تجري مناقشات مفتوحة حول المعايير هي أماكن مثيرة للاهتمام للبحث عن جماعات الضغط والتأثير (وإنْ كان من الصعب اختراقها في كثير من الأحيان). فقد تستخدمها الشركات الخاصة أو الدول كمنافذ لدعم حل تقني قد ينطوي على عواقب سياسية. على سبيل المثال، خصصت W3C في عام 2021 فريق عمل كان معنيًا بـ"تحسين الإعلانات عبر الويب" حيث اقترحت Google بديلاً لملفات تعريف الارتباط الخاصة بأطراف خارجية التي لا تزال تتيح التتبع والاستهداف.

ج. فهم طريقة عمل التكنولوجيا المعنية

فيما يلي نحدد ثلاث طرق رئيسية يمكن من خلالها الوصول إلى فهم أفضل لطريقة عمل التكنولوجيا:

1) مراجعة الأدبيات المضافة
2) استخدام البدائل الحالية واختبارها
3) طرح الأسئلة على الخبراء

1) مراجعة الأدبيات

ثمة العديد من الموارد المتاحة التي تعمل على تبسيط التكنولوجيات المعقدة وتعميمها، بدايةً من ويكيبيديا. كما أن هناك موارد أخرى يمكن أن تكون مفيدة بشكل كبير حتى ولو كانت خلفيتها التقنية ضئيلة أو منعدمة، مثل الصحافة شبه المتخصصة. انظر على سبيل المثال:

- MIT Technology Review (على سبيل المثال، الحوسبة الكمومية)
- ArsTechnica (على سبيل المثال، ما يتعلق بـ NFTS)
- PC Mag (على سبيل المثال، ما يتعلق بـ 5G Mag)

الأوراق البحثية الأكاديمية هي أيضًا وسيلة للعثور على المعلومات على الرغم من صعوبة فهم اللغة دون معرفة تقنية مسبقة. ومع ذلك، يجدر بك البحث في الباحث العلمي من Google وغير ذلك من الموارد للعثور على أوراق بحثية عن التكنولوجيا التي تبحث عنها، وينبغي من الناحية المثالية أن يكون البحث في سياق مشابه لسياقك أو التركيز على شواغل مشابهة.

وهناك أيضًا بعض المنظمات غير الحكومية التي تتمتع بموارد تقنية وتنشر موادًا يمكن أن تسترشد بها في فهم الكيفية التي تؤدي بها تكنولوجيا معينة وظيفتها والكيفية التي يمكن بها استخدامها في سياقات معينة، على سبيل المثال:

- برايفسي إنترناشيونال (كتيب أولي بشأن بلوتوث، GPS)
- مؤسسة التخوم الإلكترونية EFF (مقال توضيحي بشأن Amazon Sidewalk وIMSI catchers)
- Citizen Lab (تحليل برمجيات تصفية المحتوى على التطبيق الصيني الشهير YY)

قد تحتوي المواقع الإلكترونية للشركات المصنعة على معلومات مفيدة - إلى حد ما - عن التكنولوجيا التي تبحث بشأنها والكيفية التي تؤدي بها وظيفتها. كما أنّ الوثائق الفنية أو الترويجية للمنتجات التي تصنعها هذه الشركات قد تكون أدوات رائعة لفهم مواصفات تكنولوجيا معينة والحصول على معلومات قيّمة حول كيفية عملها. وقد ترغب في استخدام وسائل مثل Google Dorking للعثور على الكتيبات الرسمية للشركات وغيرها من الوثائق التي من شأنها مساعدتك في مسعاك.

وكما هو الحال في أي عملية بحثية، تُعد الإحالة المرجعية لما تجده والتحقق من صحته من خلال أكثر من مصدر من الأمور المهمة لتجنب المعلومات الخاطئة!

2) استخدام واختبار البدائل الحالية

أن تحاول العثور على أنظمة مكافئة ميسورة التكلفة، وتدرس كيفية عمل هذه الأنظمة، فهذا يمكن أن يمنحك معلومات أفضل عما يجري داخل النظام الذي تقوم بتحليله. على سبيل المثال، إذا كنت تبحث بشأن أنظمة التعرف على الوجه، فقد يكون من المفيد البحث عن مشاريع من مصادر علنية يمكنك تحليلها بحرية مثل هذا المشروع.

على أنّ استخدام هذه البدائل قد يتطلب بعض المعرفة التقنية ولا يمكن للجميع الوصول إليها بسهولة. ومع ذلك، هناك مصادر تعليمية وأدلة للمبتدئين يمكنك استخدامها لتثبيت هذه الأنظمة واختبارها، وينبغي اعتبارها طريقة أسهل للتعامل مع هذه الاستراتيجية. بالمثل، فإن هناك بعض الدورات التدريبية عبر الإنترنت حول "كيفية البدء بـ س" يمكن أن تساعدك في الحصول على فهم أوضح للكيفية التي تؤدي بها التكنولوجيا وظيفتها. على سبيل المثال، من شأن الفصول التمهيدية في كتاب D2L بشأن التعلم العميق أن تساعدك على فهم مختلف العناصر الفاعلة في تكنولوجيا الذكاء الاصطناعي.

إضافة إلى ذلك، فإنّ المؤسسات ذات الخبرة التقنية يمكنها أيضًا نشر أدلة ووثائق ومنهجيات بشأن استخدام الأنظمة التي تستعملها في أعمالها. على سبيل المثال، لدى برايفسي إنترناشيونال بيئة اعتراض بيانات لتحليل الحركة من تطبيقات Android وأتاحتها للاستخدام من قبل أي شخص.

لعله من الجدير بك أن تبحث عن أشخاص آخرين سبق لهم أن أجروا مثل هذا الاختبار من قبل، مثل الخبراء الذين يحاولون الكشف عن العيوب أو إثبات التحيز في تكنولوجيا معينة. ومن الأمثلة الجيدة على الخبراء الذي أجروا اختبارًا لجزء من تكنولوجيا للكشف عن نقاط الضعف فيها العمل الذي قام به جوي بولامويني حول أنظمة التعرف على الوجه العنصرية.

3) طرح الأسئلة على الخبراء

بعد أن تنتهي من بحثك، قد تجد أن ثمة أسئلة ظلت دون إجابة، أو نقاطًا تحتار في كيفية الربط بينها، أو مجرد أشياء لا تتمتع بالخلفية التقنية لفهمها. وفي هذه الحالة، قد يكون من المفيد لك أن تتواصل مع خبراء أكاديميين أو مؤسسات صحفية أو منظمات مجتمع مدني متخصصة للحصول على المساعدة.

عند القيام بذلك، نقترح عليك أن توضح قدر الإمكان طبيعة العمل الذي تحاول القيام به، وما هو الغرض منه، وما الذي فهمته حتى الأن، وأن تطرح أسئلة دقيقة قدر الإمكان، ذلك أنّ الخبراء في هذا المجال قد لا يهتمون بإعطاء درسًا حول تكنولوجيا معينة بقدر اهتمامهم بمساعدتك على فهم استخدامها في سياق معين. بالتالي، يجب عليك كتابة قائمة تحتوي

على أسئلة دقيقة مع تفاصيل خاصة بالسياق، فهذا من شأنه تعظيم فرص الحصول على رد من خبير أو إجراء مكالمة معه.

فيما يتعلق بالشخص الذي يجب عليك التواصل معه، فربما ينبغي لك البدء بالأكاديميين الذين كتبوا أوراقًا بحثية حول التكنولوجيا التي تبحث بشأنها - وبخاصة، إذا كانت أبحاثهم تتمحور حول أحد المخاطر الرئيسية التي حددتها. وكخيار بديل، يمكنك مراسلة المهنيين الذين يستخدمون التكنولوجيا المعنية في أعمالهم إذ سيكون لديهم عادةً الكثير من الخبرة العملية حول كيفية استخدامها. كما أنّ البحث عن أشخاص في فرق العمل ومجموعات التبادل ومجموعات تبادل المعرفة يُعد خطوة أولى جيدة، إذ إنها تعبر عن إرادة للمشاركة والتعلم، مما يزيد من فرصك في العثور على شخص على استعداد لمساعدتك. إضافة إلى ذلك، يمكنك أيضًا الحصول على معلومات مناسبة عن طريق طرح الأسئلة على المجتمعات المتخصصة عبر الإنترنت مثل StackOverflow أو .Reddit

ثمة منظمات معينة مثل برايفسي إنترناشيونال لديها أيضًا خبراء تكنولوجيون يمكنك محاولة التواصل معهم. وإذا كانوا لا يتمتعون بالخبرة في التكنولوجيا التي تبحث بشأنها، فإنهم - على الرغم من ذلك - يمكنهم توجيهك إلى الموارد المناسبة أو إلى أشخاص آخرين يمكنك التحدث معهم.

ماذا يقول شركاؤنا:

أن تتوصل إلى فهمٍ تامٍ للتكنولوجيا التي تبحث بشأنها، فهذا هدف يصعب تحقيقه. تقترح ADC قبول أنه لا يمكنك بالضرورة معرفة الكيفية التي تؤدي بها كافة العناصر المعنية وظيفتها، وأن تحاول إخضاع عملك لمراجعة أقران للتأكد من أنك لا تقدم معلومات خاطئة تمامًا. ذلك أنّ التأكد من صحة الأساسيات وأن تحليلك يستند إلى معلومات جرى التحقق من صحتها لهو أهم من محاولة فهم كل شيء والتركيز على التفاصيل التي ربما تكون قد أسأت تفسيرها. وبوضع ذلك في الاعتبار، توصي ADC بأن تقصر نطاق عملك على أشياء قليلة وتركز عليها.

د. قائمة مرجعية - فهم التكنولوجيا

هذه القائمة المرجعية لمساعدتك على التأكد من أنك قد حددت بشكل مناسب الشواغل المرتبطة بالتكنولوجيا التي تبحث بشأنها:

- هل يمكنك وضع تعريف عام للتكنولوجيا وما طبيعة وظيفتها؟
- ما هو دور البيانات في التكنولوجيا ؟ (نظام جمع البيانات، نظام نقل البيانات، نظام تخزين البيانات، نظام معالجة البيانات)
- ما هي المخاطر المرتبطة بهذه التكنولوجيا فيما يتعلق بكل نظام معين؟
- إلى أي مدى تُعتبر هذه التكنولوجيا مبتكرة ورائدة؟
  - [اختياري] ما هي المخاطر المرتبطة بعامل الابتكار؟
- هل يمكنك شرح الكيفية التي تؤدي بها التكنولوجيا وظيفتها عمليًا؟
  - [اختياري] ما هي المخاطر المرتبطة بالكيفية التي تؤدي بها التكنولوجيا وظيفتها تحديدًا؟

4. مسائل تتعلق بالإدارة والحكم السليم

من خلال عملنا الاستقصائي والعمل الذي قام به شركاؤنا حول العالم، حددنا عددًا من مشكلات الحوكمة المتكررة والشائعة في الشراكات بين القطاعين العام والخاص. وقد أوردنا تفاصيل كل شاغل من شواغلنا والضمانات ذات الصلة بها هنا. نقدم في هذا القسم بعض الإرشادات الرفيعة المستوى بشأن كيفية تحديد أنواع الشواغل هذه.

أ. مبادئ الأمم المتحدة التوجيهية بشأن الأعمال التجارية وحقوق الإنسان

طبقًا لمبادئ الأمم المتحدة التوجيهية بشأن الأعمال التجارية وحقوق الإنسان (يُشار إليها هنا باسم "مبادئ الأمم المتحدة التوجيهية")، يتعين على الشركات احترام حقوق الإنسان، وهذا يعني عدم جواز تعديها على حقوق الإنسان للآخرين ووجوب تصديها لما تخلفه من آثار ضارة بحقوق الإنسان (المبدأ رقم 11 من مبادئ الأمم المتحدة التوجيهية).

مبادئ الأمم المتحدة التوجيهية عبارة عن مجموعة من المبادئ التوجيهية للدول والشركات لمنع انتهاكات حقوق الإنسان المرتكبة في العمليات التجارية والتصدي لهذه الانتهاكات وجبرها. وقد صادق مجلس حقوق الإنسان التابع للأمم المتحدة بالإجماع على مبادئ الأمم المتحدة التوجيهية في قراره رقم 4/17 بتاريخ 16 يونيو 2011.

تقدم مبادئ الأمم المتحدة التوجيهية معيارًا عالميًا ذا حجية للإجراءات التي تُتخذ لحماية حقوق الإنسان في سياق الأعمال. وبالتالي، يمكن استخدام هذه المبادئ في سياق العمل الاستقصائي لتقييم امتثال الشراكة بين القطاعين العام والخاص لمعايير حقوق الإنسان. كما يمكن استخدامها كمورد لمناصرة الإجراءات المحددة التي يتعين على الشركات والحكومات اتخاذها. في هذا القسم، نسلط الضوء على المسؤوليات الرئيسية للشركات المستمدة من مبادئ الأمم المتحدة التوجيهية، كما نوضح كيف أصبحت، رغم طابعها غير الملزم، هي القاعدة في تقييم المسؤوليات تجاه حقوق الإنسان في العمليات التجارية.

1) مبادئ الأمم المتحدة التوجيهية كمعيار سلوكي للشركات

تحتوي المبادئ التوجيهية على ثلاثة فصول أو ثلاث ركائز: الحماية والاحترام والانتصاف. يحدد كل فصل من هذه الفصول عددًا من الإجراءات والخطوات الملموسة التي يتيعن على الحكومات والشركات اتخاذها للإيفاء بواجباتها

ومسؤولياتها ذات الصلة لمنع انتهاكات حقوق الإنسان في سياق عمليات الشركة وتوفير سبل الانتصاف في حال حدوث مثل هذه الانتهاكات.

يتوقع من الشركات اتخاذ عددًا من الإجراءات، منها ما يلي:

- تبني التزام سياساتي عام وصريح بالإيفاء بمسؤولياتها تجاه احترام حقوق الإنسان (الالتزامات السياساتية بحقوق الإنسان)؛
- إجراء تقييمات للمخاطر لدراسة ما تنطوي عليه الأدوات والخدمات المقترحة من آثار فعلية ومحتملة على حقوق الإنسان (العناية الواجبة بشأن حقوق الإنسان وتقييم الآثار - HRDD)؛
- وضع آلية مساءلة داخلية لتنفيذ سياسات حقوق الإنسان وتطبيق ما يلزم من عمليات للتأكد من أنها توفر سبل انتصاف فعالة (آليات التظلم).

تتضمن إجراءات العناية الواجبة بشأن حقوق الإنسان أربعة عناصر رئيسية: تحديد أي أثر سلبي حقيقي أو محتمل على حقوق الإنسان قد تتسبب فيه الشركة أو تسهم فيه أو تكون متصلة به مباشرةً، ثم تقييم هذا الأثر؛ واتخاذ الإجراءات المناسبة وإدراج النتائج الصادرة عن تقييمات الأثر على مستوى عمليات الشركة ذات الصلة؛ وتعقب فعالية التدابير من أجل تقييم مدى نجاحها؛ والتواصل مع أصحاب المصلحةِ بشأن كيفية معالجة الآثار والتأكيد لأصحاب المصلحةِ بأنّ هناك سياسات وإجراءات مناسبة مطبقة.

2) شركات التكنولوجيا ومبادئ الأمم المتحدة التوجيهية

تنطبق مبادئ الأمم المتحدة التوجيهية على جميع الشركات، وبالتالي فإنها تنطبق على قطاع التكنولوجيا. ومع ذلك، لم تخضع شركات التكنولوجيا لنفس القدر من التمحيص كغيرها من القطاعات، والسبب الواضح في ذلك هو الطابع المعقد لمنتجاتها وخدماتها، بالإضافة إلى حداثة التأثيرات المجتمعية التي تتسبب فيها. يوفر مشروع الأعمال التجارية وحقوق الإنسان والتكنولوجيا الموارد والمبادئ التوجيهية الموثوقة بهدف تنفيذ المبادئ التوجيهية للأمم المتّحدة بشأن الأعمال التجارية وحقوق الإنسان في مجال التكنولوجيا. وقد تم إطلاق هذا المشروع في عام 2019 بقيادة مفوضيّة الأمم المتّحدة السامية لحقوق الإنسان (مكتب مفوضيّة الأمم المتّحدة السامية لحقوق الإنسان). انظر على سبيل المثال "مقدمة لمبادئ الأمم المتحدة التوجيهية في عصر التكنولوجيا".

إضافة إلى ذلك، توفر الإجراءات الخاصة للأمم المتحدة، وغيرها من هيئات حقوق الإنسان، إرشادات بشكل متزايد حول تطبيق مبادئ الأمم المتحدة التوجيهية في قطاع التكنولوجيا. ثمة موارد عديدة يمكنك النظر فيها، ومنها التقرير الذي أعدته الدكتورة كريستينا هوستي أوربان والبروفيسور فيونوالا ني أولين تحت إشراف ولاية المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب بشأن "استخدام بيانات المعلومات الحياتية (البيومترية) لتحديد هوية الإرهابيين: أفضل الممارسات أم الأعمال المحفوفة بالمخاطر؟". كما أنّ التقرير الصادر سنة 2019 عن المقرر الخاص المعني بالحق في حرية الرأي والتعبير بشأن "المراقبة وحقوق

الإنسان" يستخدم أيضًا مبادئ الأمم المتحدة التوجيهية كنقطة انطلاق عند دراسة مسؤولية الشركات (A/HRC/41/35).

3) مبادئ الأمم المتحدة التوجيهية كمعيار عالمية

في عام 2011، صادق مجلس حقوق الإنسان بالإجماع على مبادئ الأمم المتحدة التوجيهية (القرار رقم 4/17)، وهي معترف بها اليوم كمعيار عالمي ذي حجية بشأن مسؤولية الشركات تجاه احترام حقوق الإنسان. وعلى الرغم من أنّ مبادئ الأمم المتحدة التوجيهية ليست ملزمة قانونًا بصفة رسمية، فإنها باتت المعيار الذي ينظم عمليات الشركات من خلال التشريعات الوطنية الجديدة ومبادرات المستثمرين التي تتضمنها.

1) أساس التشريعات الوطنية: شكلت مبادئ الأمم المتحدة التوجيهية الأساس لوضع تشريعات وطنية جديدة بشأن مسؤولية الشركات في عدة بلدانٍ. على سبيل المثال، فقد اعتمد البرلمان الفرنسي عام 2017 قانونًا جديدًا يفرض واجب الحرص على الشركات المتعددة الجنسيات لمنع الانتهاكات الجسيمة لحقوق الإنسان على مستوى جميع شركاتها التابعة وسلاسل الإمداد الخاصة بها (loi de vigilance). وتعمد بلدان أخرى إلى إعداد مبادرات تشريعية مماثلة. وبالمثل، فقد مرر البرلمان الألماني في 11 يونيو 2021 "قانون العناية الواجبة للشركات في سلاسل الإمداد" (قانون العناية الواجبة في سلاسل الإمداد - "القانون" أو "LkSG"). وفي 23 فبراير 2022، اعتمدت المفوضية الأوروبية اقتراحًا لإعداد توجيه حول العناية الواجبة بشأن استدامة الشركات، يستند جزئيًا إلى مبادئ الأمم المتحدة التوجيهية.

عمدت ولايات وبلدان أخرى إلى تطبيق تشريعات العناية الواجبة فيما يتعلق بحقوق الإنسان - منها على سبيل المثال أستراليا وكاليفورنيا والمملكة المتحدة بشأن العبودية الحديثة وهولندا بشأن تشغيل الأطفال. انظر لمحة عامة حول آخر التطورات في مركز موارد الأعمال وحقوق الإنسان.

هناك بلدان عديدة أيضًا، منها تشيلي وكولومبيا والدنمارك وفنلندا وألمانيا وهولندا والنرويج وإيطاليا وإسبانيا وسويسرا وتنزانيا وتايلاند وكينيا وأوغندا والمملكة المتحدة والولايات المتحدة، أدرجت مبادئ الأمم المتحدة التوجيهية في خطط العمل الوطنية الخاصة بها. وخطة العمل الوطنية بشأن الأعمال وحقوق الإنسان هي استراتيجية سياساتية الهدف منها هو التأكد من أن الدول توفر الحماية المناسبة ضد الآثار السلبية على حقوق الإنسان بالنسبة للأفراد العاملين في الشركات.

في كثير من الأحيان، يمتد تطبيق التشريعات الوطنية ليشمل العمليات التجارية خارج أراضي الدول المشرعة. وعلى سبيل المثال، يهدف توجيه الاتحاد الأوروبي إلى ضمان احترام حقوق الإنسان والبيئة على نطاق سلسلة الإمداد بأكملها.

2) الاستثمار المسؤول: من المتفاهم عليه أيضًا أنّ مبادئ الأمم المتحدة توفر إرشادات بشأن الاستثمار المسؤول. في العام 2018، صدر تقرير عن الفريق العامل المعني بالأعمال التجارية وحقوق الإنسان التابع للأمم المتحدة يدعو المستثمرين تحديدًا إلى اتخاذ العناية الواجبة بحقوق الإنسان في إطار مسؤوليتها الخاصة بموجب المبادئ التوجيهية، والعمل بصورة أكثر منهجية على مطالبة الشركات التي يستثمرون فيها باتخاذ العناية الواجبة بحقوق الإنسان بفعالية، والتنسيق مع المنظمات والمنصات الأخرى لضمان التوافق والمشاركة الهادفة مع الشركات. ويضطلع المزيد والمزيد من المستثمرين بهذه المسؤولية، بدعمٍ من مبادراتٍ مثل تحالف المستثمرين من أجل حقوق الإنسان ومبادئ الاستثمار المسؤول.

ب. الشواغل المتعلقة بحماية البيانات/ الخصوصية

بمجرد وصولك إلى فهم جيد للطريقة التي تؤدي بها التكنولوجيا وظيفتها، فقد يتعين عليك عندئذ تقييم آثارها المختلفة على الخصوصية وحماية البيانات. وللقيام بذلك، حددنا أدناه بعض الجوانب العامة لعملية معالجة البيانات التي يمكنك مراجعتها لتحديد أية شواغل.

ليس هناك معايير لحماية البيانات معترف بها عالميًا، ولكن الهيئات الإقليمية والدولية وضعت مدونات وممارسات وقرارات وتوصيات وأدوات سياساتية متفق عليها دوليًا. وأهم هذه الأدوات هي:

- اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية المعتمدة من مجلس أوروبا (رقم 108)، سنة 1981 بصيغتها المعدلة سنة 2018؛
- المبادئ التوجيهية المتعلقة بحماية الخصوصيات وتدفقات البيانات الشخصية عبر الحدود المعتمدة من منظمة التعاون الاقتصادي والتنمية (1980) بصيغتها المعدلة سنة 2013؛
- المبادئ التوجيهية لتنظيم ملفات البيانات الشخصية المحوسبة (قرار الجمعية العامة رقم 95/45 و E/CN.4/1990/72).

هناك أطر إقليمية أيضًا، مثل إطار الخصوصية لرابطة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC). وثمة قوانين معنية بحماية البيانات خارجة عن نطاق الولاية الوطنية؛ على سبيل المثال، ينطبق النظام الأوروبي العام لحماية البيانات على جهات الرقابة والمعالجة غير الموجودة في الاتحاد الأوروبي طالما كانت تعالج بيانات أشخاص مقيمين قي الاتحاد الأوروبي، وأنّ هذه المعالجة متعلقة بعرض سلع أو خدمات في الاتحاد الأوروبي، أو أنّها ترقى إلى مراقبة سلوكهم.

وفي حال كان هناك قانون شامل لحماية البيانات، عندئذ تكون المؤسسات (العامة أو الخاصة) التي تجمع البيانات الشخصية وتستخدمها ملزمة بالتعامل مع هذه البيانات طبقًا لهذا القانون. وبالتالي، يُرجى الرجوع إلى القوانين المطبقة في الولاية القضائية التي تتبعها، غير أنّ هذا القسم يقدم لمحة عامة عن الأشياء المختلفة التي ينبغي

استكشافها. ومع ذلك، فهذه ليست قائمة شاملة لجميع الشواغل المحتملة المتعلقة بحماية البيانات - للاطلاع على دليل أشمل حول حماية البيانات، يُرجى الرجوع إلى دليلنا الشامل.

1) مصادر البيانات

تتمثل الخطوة الأولى لتقييم معالجة البيانات من خلال تكنولوجيا ما في فهم من أين تُجمع هذه البيانات، أو بمعنى آخر مصدر هذه البيانات. ولعلك تكون قد حددت ذلك في مرحلة تقييم نظام جمع/ استخراج البيانات الخاص بالتكنولوجيا (انظر الاستقصاء التقني أعلاه)، لكن يمكنك تعزيز هذا التحليل بوثائق حول التكنولوجيا أو الشراكة (مثل العقود، ومذكرات التفاهم، وتقييمات الأثر على حماية البيانات، واتفاقيات معالجة البيانات ...)، ثم تدرس:

- أي مجموعات بيانات/ قواعد بيانات تفيد التكنولوجيا
- أي قوائم بأصحاب البيانات أو فئات أصحاب البيانات التي ستخضع بياناتها للمعالجة (بما في ذلك أفراد من عامة الناس أو المشتبه بهم في جريمة أو ضحايا هذه الجريمة أو الشهود على هذه الجريمة أو الأفراد الذين يعيشون في المنطقة "س" ...)
- أي مصادر للبيانات (على سبيل المثال، هل تأتي البيانات من أي قواعد بيانات موجودة، أو من دوائر أو سلطات حكومية معينة؟)

بمجرد أن تفهم مصدر البيانات، يجب عليك أن تقيم مدى شرعية جمع أو تبادل هذه البيانات (بمعنى، هل هو مصرح به بناءً على أساس قانوني مثل موافقة صاحب البيانات، أو التزام قانوني بتبادل هذه البيانات) وما إذا كان هذا الأساس القانوني مذكورًا صراحةً في الوثائق. ذلك مع العلم بأن شرعية جمع البيانات تستند إلى الولاية القضائية الخاضعة لها الشراكة أو التكنولوجيا.

2) الشرعية والعدالة

يجب معالجة البيانات الشخصية على نحو شرعي وعادل وشفاف. وهذا المبدأ أساسي في التعاطي مع ممارسات مثل بيع و/أو نقل البيانات الشخصية التي يتم الحصول عليها بشكل مهمل أو احتيالي.

الشرعية معناها أنّه يجب معالجة البيانات على نحو يفي بالأسس القانونية للمعالجة. فيجب عليك تقييم شرعية المعالجة بالنسبة لكل نوع أو فئة من البيانات التي ستضخع للمعالجة بواسطة التكنولوجيا، ولكل غرض من أغراض المعالجة. على سبيل المثال، إذا كانت البيانات المأخوذة من قاعدة بيانات لوجوه أفراد من عامة الناس سوف تخضع للمعالجة للتحقق منها بمقارنتها مع إحدى قواعد البيانات الخاصة بالتصوير الجنائي التعريفي، عندئذ يتعين عليك تقييم (1) ما إذا كانت كل قاعدة بيانات قد جُمعت بناء على سبب قانوني للمعالجة (اعلم أن هذا لا يتطلب فقط التأكد من أن

السلطة العامة تستند إلى سبب قانوني لجمع صور الوجوه في المقام الأول (كما هو موضح في القسم السابق) ومن ثم بناء قاعدة البيانات، ولكن أيضًا ضمان أنه، في حالة جمع قواعد البيانات من قبل شركة خاصة، أن تكون هذه الشركة الخاصة تستند أيضًا إلى سبب قانوني لجمع البيانات في المقام الأول)، و(2) ما إذا كانت عملية التحقق تستند إلى سبب قانوني للمعالجة.

أسباب المعالجة الأكثر شيوعًا في قوانين حماية البيانات هي كالتالي:

- موافقة صاحب البيانات
- ضرورة المعالجة لتنفيذ عقد مع صاحب البيانات أو اتخاذ خطوات لإبرام عقد
- ضرورة المعالجة للامتثال لالتزام قانوني
- ضرورة المعالجة لحماية المصالح الحيوية لصاحب البيانات أو أي شخص آخر
- ضرورة المعالجة لأداء مهمة الغرض من تنفيذها هو تحقيق المصلحة العامة أو ممارسة السلطة الرسمية المخولة للمراقب
- ضرورة المعالجة لأغراض المصالح المشروعة التي يسعى إلى تحقيقها المراقب أو طرف ثالث، إلا إذا كانت هذه المصالح تتجاوزها مصالح أو حقوق أو حريات صاحب البيانات

لمزيد من التفاصيل حول أسباب المعالجة، يُرجى الرجوع إلى هذا القسم من دليل حماية البيانات الخاص بنا حول أسباب معالجة البيانات الشخصية.

تقتضي العدالة عدم استخدام البيانات بطرق لا يتوقعها أصحاب البيانات بشكل معقول، ولا بطرق قد تعرضهم "لآثار سلبية دون مبرر".

هذا مبدأ عام ينبغي أن ينظم جميع جوانب المعالجة - جمع البيانات والغرض من المعالجة وعواقب المعالجة. ولتقييم العدالة، يجب عليك أن تقيم ما إذا كانت السلطة التي تراقب عملية المعالجة قد راعت التوقعات المعقولة لأصحاب البيانات في ضوء سياق المعالجة والغرض منها، والمخاطر على حقوقهم وحرياتهم الأساسية، والعلاقة العامة بين المراقب وأصحاب البيانات (على سبيل المثال هناك بعض الروابط أو العلاقات بين الطرفين من شأنها أن تجعل أصحاب البيانات يتوقعون حدوث مثل هذه المعالجة).

3) الشفافية والحق في الحصول على المعلومات

إنّ تحديد عدالة المعالجة من عدمها إنما يعتمد بشكل كبير أيضًا على مقدار الشفافية التي حظى بها أصحاب البيانات حول عملية المعالجة، إذ ينبغي للأفراد أن يحصلوا على ما يكفي من معلومات عند جمع بياناتهم الشخصية، بالإضافة إلى ما يكفي من معلومات بشأن معالجة هذه البيانات. وعند تقييم نشر تكنولوجيا ما، يجب عليك أن تقيم مقدار

المعلومات التي حصل عليها أصحاب البيانات بشأن معالجة بياناتهم والآليات التي استُخدمت لتزويدهم بمثل هذه المعلومات.

وفي مرحلة جمع البيانات، وفي كل مرة تخضع فيها البيانات للمعالجة لغرض لم يكن متوخى أثناء عملية الجمع، ينبغي تزويد أصحاب البيانات بالمعلومات التالية على الأقل (سواء عندما يقدمون البيانات إلى المراقب مباشرة، أو عندما يحصل المراقب عليها من مصدر آخر):

- معلومات عن هوية المراقب (وبيانات الاتصال)
- الغرض من المعالجة
- السبب القانوني (أو الأسباب القانونية) للمعالجة
- فئات البيانات الشخصية التي ستخضع للمعالجة
- مستلمو البيانات الشخصية
- ما إذا كان المراقب يعتزم نقل البيانات الشخصية إلى دولة ثالثة وما هي الضمانات المقدمة للنقل
- مدة تخزين البيانات الشخصية
- حقوق صاحب البيانات (مثل حق الوصول، والحق في الاعتراض، وحقوق التصحيح والحظر والمسح، والحقوق المتعلقة بالتنميط واتخاذ القرار آليًا، والحق في إمكانية نقل البيانات)
- الحق في تقديم شكوى إلى السلطة الإشرافية
- وجود التنميط، بما في ذلك الأساس القانوني، وأهمية هذه المعالجة وعواقبها المتوقعة على صاحب البيانات
- وجود آلية لاتخاذ القرار آليًا وعلى الأقل معلومات مناسبة بشأن الأساس المنطقي لهذه المعالجة وأهميتها وعواقبها المتوقعة على صاحب البيانات
- مصدر البيانات الشخصية (إذا لم يتم الحصول عليها من صاحب البيانات)
- ما إذا كان تقديم البيانات إجباريًا أو اختياريًا
- عواقب عدم تقديم البيانات
- في حالة عدم حصول الأفراد على المعلومات، يجب عليك أن تقيم ما إذا كان هناك استثناء من الحق في الحصول على المعلومات مطبقًا. وقد يحدث ذلك مثلاً إذا كان الحرمان من الحق في الحصول على المعلومات ضروريًا ومتناسبًا لمنع جريمة أو الكشف عن جريمة، أو لحماية الأمن القومي، أو لأغراض الصحة أو العمل الاجتماعي أو التعليم. ومع ذلك، فإن أي استثناء من هذا الحق يجب أن ينص عليه القانون، ويجب أن يكون مبررًا ومدعومًا بتقييم الضرورة والتناسب. لمزيد من التفاصيل عن الاستثناءات، يرجى الرجوع إلى هذا القسم من دليل حماية البيانات الخاص بنا حول الأحكام العامة والتعاريف والنطاق

4) تخزين البيانات وضوابط الوصول

بمجرد أن ترتضي (أو لا ترتضي!) بأنّ البيانات سوف تخضع للمعالجة بشكل قانوني ومنصف وشفاف، عندئذ يتعين عليك دراسة المكان الذي ستُخزَّن فيه البيانات ومدة هذا التخزين. السؤال الأول الذي ينبغي طرحه هو عما إذا كانت البيانات سوف تُخزَّن على خوادم تحتفظ بها السلطة العامة أم الشركة أم طرف ثالث آخر (كجهة المعالجة على سبيل المثال). ولعلك تكون قد حددت ذلك في مرحلة تقييم نظام تخزين البيانات الخاص بالتكنولوجيا (انظر قسم الاستقصاء التقني أعلاه). ذلك أنّ هذه المسألة من شأنها أن تؤثر على توزيع المسؤوليات لضمان أمن البيانات وإدارة ضوابط الوصول.

ينبغي حماية البيانات الشخصية، سواء المخزنة والمنقولة، فضلاً عن البنية التحتية المستخدمة في المعالجة، بضمانات أمنية ضد مخاطر مثل الوصول والاستخدام والإفصاح غير القانوني أو غير المصرح به، وكذلك الفقد أو التدمير أو التلف. يُرجى الرجوع إلى القسم التقني من هذا الدليل للحصول على مزيد من التفاصيل حول ما ينبغي البحث عنه. ويجب أن تكون الضمانات الأمنية مفصلة في الوثائق المحيطة بالشراكة، مع توزيع واضح للمسؤوليات بين السلطة العامة والشركة وأي طرف ثالث.

لتقييم مدى ملاءمة ضوابط الوصول، ينبغي أن تدرس نوع الوصول إلى البيانات الذي ستحضى به الشركة. وعلى وجه الخصوص، في حالة تخزين البيانات على خوادم الشركة، يجب عليك التحقق مما إذا كانت الشركة ستتمتع بحق الوصول الكامل إلى البيانات، أم أنّ وصولها سيكون مقيدًا بحيث يقتصر الوصول إلى البيانات على السلطة العامة فقط. وعلى الرغم من أنه حتى لو كانت البيانات ستُخزن على خوادم الحكومة أو السلطة، فربما تحصل الشركة على حق الوصول، ومن ثم ينبغي أن تتحقق من كافة التفاصيل الدقيقة. كما ينبغي أن تتضمن وثائق الشراكة قواعد حول ضوابط الوصول، مع بيان الاستثناءات بشكل واضح ودقيق، بما في ذلك، على سبيل المثال، الوصول في حالات الطوارئ والوصول لأغراض الصيانة وغيرهما.

في بعض الأحيان، تسمح العقود للشركات بالوصول إلى البيانات لأغراضٍ مثل "تحسين خدماتها" و"إجراء تحليلات على أداء منتجاتها"، وما إلى ذلك. وبالتالي، ينبغي أن تنتبه إلى هذه الأمور وتتساءل بالضبط عن الشكل الذي سيكون عليه وصول الشركة، ومدى فعالية الاستفادة التي ستحققها الشركة من الوصول إلى قاعدة بيانات السلطة العامة من أجل تطوير خدماتها الخاصة، وبالتالي الاستفادة من الشراكة بما يتجاوز القيمة النقدية للعقد.

لمزيد من التفاصيل عن الاستثناءات، يرجى الرجوع إلى هذا القسم من دليل حماية البيانات الخاص بنا حول مبادئ حماية البيانات.

5) عمليات نقل البيانات دوليًا

يجب عليك أن تقيم ما إذا كان تخزين البيانات أو الوصول إليها أو غير ذلك من ترتيبات النقل سوف تشمل نقل البيانات إلى دولة أخرى (على سبيل المثال، إذا كانت الشركة المتعاقدة موجودة في الولايات المتحدة). والمبدأ الأساسي في هذا الإطار هو أن أي نقل للبيانات الشخصية إلى دولة ثالثة لا ينبغي أن يحد من مستوى حماية حقوق الخصوصية للأفراد. وتوجد في الولايات القضائية المختلفة قوانين مختلفة تنظم عمليات النقل إلى دولةٍ ثالثة ويمكن الاعتماد عليها كضمانة "كافية" فيما يتعلق بحماية الحقوق، لكن عادةً ما يجب عليك التحقق مما يلي:

- هل تأكدت الدولة/ الولاية القضائية التي تقيم فيها من أن الإقليم الذي ستُنقل إليه البيانات يوفر حماية "كافية" لحقوق الأفراد (أو بمعنى آخر، هل يوجد ما يُسمى غالبًا بـ "قرار الكفاية")؟
- هل خضعت عملية النقل المعنية للمراجعة والمصادقة من قبل سلطة إشرافية؟
- هل ثمة اتفاق سارٍ ومعتمد من سلطة إشرافية يتضمن بنودًا نموذجية لحماية البيانات؟

يمكن أن تكون هناك استثناءات مطبقة للقيود المفروضة على عمليات نقل البيانات. وفي حالة الزعم بوجود استثناءات مطبقة، فمن المفترض أن تكون هذه الاستثناءات منصوصًا عليها في القانون، وأن تخضع لمراجعة دقيقة بحيث لا يتسع نطاق تفسيرها أو تكون عرضة لإساءة الاستخدام، ولكي تظل عملية النقل متوافقة مع معايير حقوق الإنسان.

يمكن لك أيضًا النظر في مسائل أخرى فيما يتصل بعمليات نقل البيانات دوليًا. فعلى سبيل المثال، إذا كانت البيانات التي ستُنقل حساسة للغاية أو تتعلق بفئات ضعيفة للغاية، حتى في حال وجود قرار كفاية أو ضمانات أخرى مطبقة، فقد يتعين عليك التحقق مما إذا كانت الدولة المستقبلة تطبق قوانين أو ممارسات تسمح لها بطلب البيانات - ومن ثم التحقق مما إذا كان من المحتمل أن يتعرض الأفراد للضرر إذا انتهى الأمر بهذه البيانات في أيدي حكومة الدولة المستقبلة.

لمزيد من التفاصيل عن الاستثناءات، يرجى الرجوع إلى هذا القسم من دليل حماية البيانات الخاص بنا حول التزامات الجهات المعنية بمراقبة البيانات ومعالجتها.

ج. المساءلة والرقابة

ينطوي تقييم أي شراكة بين القطاعين العام والخاص على جانب آخر مهم يتطلب تحليل آليات المساءلة والرقابة المعمول بها، بما في ذلك الآليات التي تأسست من خلالها الشراكة لأول مرة (مثل عمليات المشتريات العامة).

لذلك، يجب عليك التحقق من توافر وثائق وعمليات معينة تضمن خضوع الدولة المتعاقدة والشركة للمساءلة، فضلاً عن توافر القدر المناسب من آليات الرقابة والانتصاف. وتجدر الإشارة إلى أنّه يجب عليك دراسة عمر الشراكة بأكملها، وذلك بدءًا من مرحلة المشتريات بأن تطرح السؤال التالي: هل التزمت عملية المشتريات لهذا العقد بقواعد المشتريات المحلية أو الدولية؟ وهل قواعد المشتريات هذه كافية؟ وهل كان هناك قدر كافٍ من الشفافية خلال عملية المشتريات؟

عادةً ما يجب إجراء تقييمات المخاطر والآثار على حقوق الإنسان و/ أو تقييمات الآثار على حماية البيانات/ الخصوصية قبل ترسية أي عقد. يجب أن تُجرى هذه التقييمات بجدية وباستخدام النماذج المناسبة المعتمدة في الولاية القضائية التي تقيم فيها فيها أو المعترف بها من قبل المجتمع المدني على الصعيد العالمي. مثال على ذلك الإرشادات ومجموعة الأدوات الخاصة بتقييم الآثار على حقوق الإنسان الصادرة عن المعهد الدانمركي لحقوق الإنسان. ولكي يكون تقييم الآثار مناسبًا، فإنه يجب (على وجه الخصوص ولكن ضمن جملة أمور أخرى) أن يتضمن تقييم الضرورة والتناسب الذي يراعي على النحو الواجب المخاطر التي تتعرض لها حقوق الأفراد.

بعد ذلك، يجب عليك النظر فيما إذا كان هناك أي رقابة مستقلة من شأنها أن تضمن بقاء الشراكة منحصرة ضمن إطار غرضها المعلن، وذلك لاكتشاف ما ينشأ من انتهاكات وأضرار وكذا لطلب الانتصاف. أين وكيف يتحدد ويتأكد ذلك؟

عند تفعيل شراكة بين القطاعين العام والخاص، ينبغي تعيين هيئة رقابة مستقلة (مثل هيئة إشرافية لحماية البيانات أو هيئة إشرافية لها سلطات تحقيقية...) لتكون مسؤولة عن (1) مراجعة أو اعتماد أو رفض العروض الجديدة لاستخدام التكنولوجيا المنشورة أو النظام المنشور في إطار الشراكة، (2) إجراء عمليات تدقيق منتظمة لنشر التكنولوجيا بما في ذلك إجراء مشاورات عامة حول تأثير التكنولوجيا على حقوق المدنيين وتحقيق الهدف المنشود (أو الأهداف المنشودة)، و(3) تلقي التظلمات والتوسط بين الجمهور والجهات التي تستخدم التكنولوجيا. وينبغي تزويد هيئة الرقابة المستقلة هذه بالموارد المناسبة (البشرية والمالية) لتتمكن من أداء واجباتها.

في حالة توافر هذه الوثائق والعمليات، فإنّ ذلك سيساعدك في تحديد مدى قانونية نشر التكنولوجيا ومدى الحاجة إلى هذا النشر، وما إذا كانت هذه التكنولوجيا تُعتبر استجابة مناسبة للمشكلة التي تستهدف حلها. وإذا لم تكن متوافرة، فمن المهم أن تحاول تحديد ما إذا كان الحل مناسبًا أم أنه مكبل أو متجاوز لصلاحياته - يمكنك، من جملة أمور أخرى، مخاطبة السلطة العامة المعنية لطلب توفير هذه الوثائق أو العمليات.

بعد ذلك، يجب عليك أن تنظر فيما إذا كانت الشراكة خاضعة لمعايير شفافية أو متطلبات قانونية معينة. فإذا كانت كذلك، فهل هي كافية؟

يمكنك بعدئذ التفكير في كيفية مساءلة الشركاء المعنيين فيما يتعلق بعواقب نشر التكنولوجيا. تقتضي المسائلة أن تكون الواجبات والمسؤوليات والمعايير محددة وملائمة وأن تكون موزعة بين الأطراف المعنية. فهل توجد آليات مناسبة تسمح للأطراف الثالثة بدراسة العواقب والتصدي لها؟

ينبغي أن تكون أي شراكة بين القطاعين العام والخاص خاضعة لسياسات مناسبة لتنظيم المتطلبات المختلفة المذكورة أعلاه وتوثيقها، بما في ذلك، على سبيل المثال، ماهية البيانات التي ستخضع للمعالجة، والطرف الذي يحق له الوصول إلى البيانات تحت أي ظروف، وماهية الضمانات التي يجب وضعها لتخفيف المخاطر التي تهدد الأفراد، وماهية الهيئة المستقلة المسؤولة عن ممارسة الرقابة على النشر، وما إلى ذلك. كما يجب أن تنظم هذه السياسات استخدام السلطة العامة للتكنولوجيا ووضع حدود واضحة لغرض التكنولوجيا واستخدامها، مع وضع قائمة شاملة بالاستخدامات المصرح بها وقائمة غير شاملة بالاستخدامات المحظورة. وهي إلى ذلك ينبغي أن توفر أيضًا آليات الانتصاف عن طريق تحديد عمليات التعامل مع الشكاوى وإنفاذ العقوبات المفروضة بسبب انتهاكات السياسات، وتوزيع المسؤوليات والتزامات الانتصاف بين كل من الدولة والشركة.

إنّ الضمانات المحددة أعلاه تمثل - حسب اعتقادنا - إطارًا معقولاً للحماية من أجل تنفيذ المسؤوليات المحددة في مبادئ الأمم المتحدة التوجيهية بشأن الأعمال التجارية وحقوق الإنسان، وضمان ألا تؤدي الشراكات بين القطاعين العام والخاص في مجال المراقبة إلى انتهاكات لحقوق الإنسان.

لمزيد من الإرشادات حول الضمانات المختلفة التي ينبغي أن تنظم الشراكات بين القطاعين العام والخاص في مجال المراقبة، يُرجى الرجوع إلى ضمانات الشراكة بين القطاعين العام والخاص الصادرة عن برايفسي إنترناشيونال.

د. قائمة مرجعية - الحوكمة

حماية البيانات والخصوصية

- بمجرد انتهائك من تقييم مصدر البيانات، هل قيّمت مدى قانونية جمع البيانات أو تبادلها؟
  - هل هذا الأساس القانوني منصوص عليه صراحة في وثائق الشراكة؟
- هل يجري جمع البيانات بوسائل يمكن أن يتوقعها الأشخاص بشكل معقول؟
- هل راعى مراقبو البيانات المخاطر التي تتعرض لها الحقوق والحريات الأساسية للأشخاص الذين سوف تُجمع بياناتهم؟
- ماذا ستكون عواقب معالجة بيانات الأشخاص بهذه الطريقة؟
- هل سيتم إعلام الأفراد عند جمع بياناتهم الشخصية؟

- ومن خلال أي آلية؟
- هل يوجد استثناء في هذه الحالة؟ وهل هذا الاستثناء مبرر؟ وهل يدعمه تقييم الضرورة والتناسب؟

- هل الأفراد قادرون على الحصول على معلومات حول معالجة البيانات؟
  - ومن خلال أي آلية؟
- إلى متى سيتم تخزين البيانات؟
- من سيستضيف البيانات؟
- هل توجد ضمانات مناسبة تحمي البيانات في حالة التخزين والنقل؟
  - هل هذه الضمانات مفصلة في الوثائق المحيطة بالشراكة؟
  - هل هناك توزيع واضح للمسؤوليات بين الأطراف المتعاقدة؟
- ما نوع الوصول إلى البيانات الذي ستحضى به الشركة (أو الشركات)؟
- هل ستُنقل البيانات عبر الحدود؟
  - في حالة الإجابة بـ"نعم": هل مستوى حماية حقوق الأفراد في الدولة التي يجري نقل البيانات إليها أقل أم أعلى أم مكافئ؟
  - هل تأكدت الدولة/ الولاية القضائية التي تقيم فيها من أن الإقليم الذي ستُنقل إليه البيانات يوفر حماية "كافية" لحقوق الأفراد (أو بمعنى آخر، هل يوجد ما يُسمى غالبًا بـ "قرار الكفاية")؟
  - هل خضعت عملية النقل المعنية للمراجعة والمصادقة من قبل سلطة إشرافية؟
  - هل ثمة اتفاق سارٍ ومعتمد من سلطة إشرافية يتضمن بنودًا نموذجية لحماية البيانات؟
  - في حالة الإجابة بـ"لا": فهل هل يعتمد العقد على استثناء؟ هل ذلك الاستثناء منصوصًا عليه في القانون؟ هل عملية النقل هذه متوافقة مع معايير حقوق الإنسان؟

المساءلة والرقابة

- هل التزمت عملية المشتريات لهذا العقد بإطار مشتريات مناسب؟
- هل العقد المبرم مع الشركة مطابق للمعايير الوطنية والدولية؟
- هل الحل التكنولوجي ضروري، وهل يمثل استجابة مناسبة للمشكلة التي يستهدف حلها؟
- هل تبنت الشركة (أو الشركات) في العقد التزامًا صريحًا بالسياسة العامة للوفاء بمسؤوليتها إزاء احترام حقوق الإنسان؟
- هل أجرت الأطراف تقييمات للمخاطر لدراسة ما تنطوي عليه الأدوات والخدمات المقترحة من آثار فعلية ومحتملة على حقوق الإنسان (العناية الواجبة بشأن حقوق الإنسان وتقييم الآثار) قبل ترسية العقد، وهل حافظت على تحديث هذه التقييمات أثناء النشر؟
- هل تنص وثائق الشراكة على أي رقابة مستقلة؟
  - أين وكيف يتحدد ذلك؟

- هل تمتلك هيئة الرقابة الموارد المناسبة لأداء دورها؟

- هل هناك معايير أو متطلبات قانونية حول الشفافية؟
  - هل هذه المعايير/ المتطلبات كافية؟
  - هل يتم الإيفاء بهذه المعايير/ المتطلبات؟
- هل توجد آليات مساءلة للهيئة العامة الضالعة في هذا العقد؟
- هل توجد آليات مساءلة للهيئة الخاصة الضالعة في هذا العقد؟
  - هل وضعت الهيئة الخاصة آليات مساءلة داخلية لتنفيذ سياسات حقوق الإنسان؟
  - هل لديها عمليات قائمة لتوفير الانتصاف؟
- هل يمكن لأطراف ثالثة أن تدرس وتعارض آليات المساءلة هذه أو عواقبها؟
- ما هي السياسات التي تنظم أيًا من هذه المتطلبات وتوثقها، إن وجدت؟
- هل تتضمن قواعد تتعلق باستخدام السلطة العامة للتكنولوجيا، مع وضع حدودًا واضحة للغرض من التكنولوجيا واستخدامها؟
- هل هناك أي آليات انتصاف محددة في العقد فيما يتعلق بانتهاكات هذه السياسات؟ هل تتضمن عقوبات مناسبة بالإضافة إلى كيفية إنفاذ تلك العقوبات؟

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org