CONTESTER LES PARTENARIATS PUBLIC-PRIVÉ EN MATIÈRE DE SURVEILLANCE : Manuel pratique pour la société civile

Juin 2022

privacyinternational.org

À PROPOS DE PRIVACY INTERNATIONAL

Les gouvernements et les entreprises utilisent la technologie pour nous exploiter. Leurs abus de pouvoir menacent nos libertés et ce qui fait de nous des êtres humains. C'est pourquoi Privacy International milite afin d'obtenir le progrès que nous méritons toutes et tous. Notre mission est de préserver la démocratie, de défendre la dignité des personnes et de demander des comptes aux puissantes institutions qui sapent la confiance du public. Après tout, la vie privée est précieuse pour chacune et chacun d'entre nous, que l'on soit en train de demander l'asile, de lutter contre la corruption ou de rechercher des conseils de santé.

Rejoignez notre mouvement mondial dès aujourd'hui et prenez parti pour ce qui compte vraiment : notre liberté d'être humain.

Privacy International
62 Britton Street,
Londres EC1M 5UY, Royaume-Uni
Téléphone +44 (0)20 3422 4321
privacyinternational.org

Privacy International est une organisation caritative enregistrée (1147471), et une société à responsabilité limitée par garantie enregistrée en Angleterre et au Pays de Galles (04354366).

SOMMAIRE

REMERCIEMENTS

Nous remercions nos organisations partenaires : ADC, TEDIC, et une autre organisation qui souhaite rester anonyme, qui ont contribué à ce manuel.

- The Association of Technology, Education, Development, Research and Communication (TEDIC) est une ONG paraguayenne fondée en 2012 qui développe des technologies civiques ouvertes et défend les droits numériques pour une culture libre sur Internet.
- Asociación por los Derechos Civiles (ADC) est une organisation de la société civile basée en Argentine qui, depuis sa fondation en 1995, travaille à la défense et à la promotion des droits civils et humains en Argentine et en Amérique latine.

INTRODUCTION

Alors que les États du monde entier cherchent à étendre leurs capacités de surveillance tout en exploitant la puissance des données dans leurs offres de services publics, ils sont souvent tentés de recourir aux services d'entreprises technologiques privées, dans le cadre de partenariats public-privé (« PPP »). La lutte contre la pandémie de COVID-19 et l'urgence de trouver des réponses et des solutions qui en découlent n'ont fait qu'accroître la perception de la nécessité pour les États d'utiliser des technologies « innovantes » et des systèmes d'analyse de données volumineuses (big data) développés par des prestataires externes. Mais ces collaborations prennent une nouvelle forme, s'écartant des relations traditionnelles de marchés publics.

Nous observons en effet une plus grande co-dépendance entre les parties, l'État pouvant développer de nouveaux systèmes ou processus entièrement dépendants des services d'une entreprise ou d'une poignée d'entreprises, celles-ci recevant en contrepartie un accès à des données ou d'autres informations pour les utiliser dans le développement de ses propres services. Au-delà d'une simple relation commerciale « ponctuelle », ces partenariats se construisent souvent à force de démarchage, de promesses d'atteindre une vérité parfaite et de toujours plus d'accès aux données pour les acteurs privés, contournant souvent les règles des marchés publics et empiétant au passage sur les droits fondamentaux des individus.

La privatisation des responsabilités publiques exige plus que jamais un examen minutieux afin de garantir que les droits humains ne soient pas discrètement bafoués. Cela est particulièrement vrai lorsque les systèmes déployés sont utilisés pour la surveillance et le traitement de masse des données personnelles. Les entreprises privées sont connues pour tester les limites de la légalité et de l'éthique concernant l'utilisation des identités et des données des individus, tout en n'étant pas soumises au même niveau de responsabilité que celui exigé des autorités publiques. Cela représente une atteinte importante aux droits fondamentaux lorsque ces mêmes entreprises sont mobilisées dans la fourniture de services publics.

La société civile a le pouvoir d'exposer les risques et les problèmes qui émergent de ces partenariats par le biais d'enquêtes et de plaidoyers. Mais l'identification de risques

concrets et d'atteintes potentielles aux droits humains n'est pas une tâche aisée, car elle nécessite une compréhension à plusieurs niveaux de la technologie et des principes juridiques et de gouvernance concernés. En s'appuyant sur notre propre travail d'enquête et sur l'expertise de nos partenaires, Privacy International a conçu un manuel destiné aux organisations de la société civile, aux organisations non gouvernementales, aux universitaires et aux particuliers afin qu'ils puissent comprendre ces partenariats. Ce manuel fournit des clés pour obtenir des informations cruciales, comprendre la technologie en question et identifier les problèmes de protection des données et de gouvernance.

Ce manuel est divisé en quatre sections principales : la première section met en garde contre les divers risques de ce type d'enquêtes ; la deuxième section se concentre sur la collecte d'informations clés relatives au partenariat par divers moyens ; la troisième section se penche sur la technologie en question dans le partenariat, en adoptant une approche descendante, en commençant par les moyens d'établir une définition large de la technologie en question, et en terminant par les méthodes permettant de comprendre comment la technologie fonctionne réellement ; la quatrième section examine les préoccupations et les garanties en matière de gouvernance, y compris les bonnes pratiques internationales, les questions de protection des données et les garanties pertinentes.

Les checklists fournies à la fin de ce manuel peuvent être utilisées comme un aperçu des éléments clés à examiner et pour vous aider à suivre votre travail.

Ce manuel est donc destiné à vous aider à :

- enquêter sur un partenariat public-privé, à trouver des informations pertinentes ;
- poser les bonnes questions aux partenaires concernés (privés et publics) ;
- identifier les préoccupations liées à la technologie impliquée et à la gouvernance du partenariat.

Nous avons développé séparément un ensemble de garanties pour les partenariats de surveillance public-privé, que vous pouvez utiliser pour obtenir des idées de plaidoyer une fois que vous avez identifié les préoccupations grâce à ce manuel.

1. ÉVALUATION DES RISQUES

L'étude d'un partenariat public-privé s'accompagne d'un certain nombre de risques juridiques, techniques et humains qui doivent être évalués avant d'entreprendre toute action. Ces risques évoluent en fonction de votre cadre de recherche et du contexte plus large dans lequel le partenariat opère. Nous vous suggérons d'identifier et d'évaluer les risques liés à votre projet d'enquête avant toute autre chose. Pour vous aider dans cette tâche, vous pouvez vous référer aux listes non exhaustives ci-dessous.

A. RISQUES A EVALUER

- Diffamation : La loi sur la diffamation protège la réputation d'une personne physique ou morale contre toute ingérence injustifiée. Vous pouvez être poursuivi en justice pour diffamation par un acteur privé contre lequel vous faites des allégations. Les lois sur la diffamation diffèrent selon les juridictions et la charge de la preuve pourrait vous incomber entièrement.
- Obtention illégale d'informations : En fonction de votre juridiction, certains types d'enquêtes pourraient être en infraction avec la loi (comme la publication de fuites d'informations ou le piratage).
- Propriété intellectuelle : Les secrets commerciaux et les droits d'auteur sont deux exemples de droit de la propriété intellectuelle que vous pourriez enfreindre en menant ou publiant votre enquête.
- Risques pour les personnes (personnel, source, partenaires...) : Toute activité susceptible de mettre en danger la vie d'une personne impliquée ne doit pas être entreprise, à moins qu'il n'existe des mesures spécifiques à prendre pour atténuer les risques. Les risques peuvent inclure, entre autres : les dommages physiques, les dommages psychologiques, les dommages sociaux, les dommages économiques et les dommages juridiques.
- L'atteinte à la réputation : Risques pour l'objectivité, l'impartialité ou la crédibilité de votre organisation. Les risques peuvent inclure : des faits inexacts, des déclarations

insuffisamment étayées et l'exploitation de la surveillance des médias sociaux (SOCMINT) ainsi que d'autres sources ouvertes (OSINT) sans considération pour la vie privée, etc.

B. SUGGESTIONS DE MESURES DE GESTION DES RISQUES

Vous trouverez ci-dessous quelques suggestions d'atténuation de ces risques. Elles ne sont pas exhaustives, et peuvent ne pas, à elles seules, suffire à atténuer tous ces risques.

- Une solide méthodologie de recherche : Citer vos sources, évaluer la qualité de ces sources, prendre des photos, vidéos captures d'écran à chaque étape de votre enquête, utiliser un langage adéquat et non diffamatoire.
- Corroborer/recouper les informations : Corroborer plusieurs sources et témoignages pour assurer la validité de l'information.
- Expurger et nettoyer les documents : Expurger les données personnelles et supprimer les métadonnées des documents.
- Préparation avant une prise de parole en public ou une interview avec les médias pour adopter un langage adéquat.
- Conserver les sources originales et les stocker en toute sécurité.
- Réfléchir à la sécurité des personnes (consentement, anonymat et plus) avant d'entreprendre toute action.

2. RECHERCHE D'INFORMATIONS

Il est souvent difficile d'obtenir des informations adéquates sur un partenariat public-privé, en particulier lorsque des secteurs sensibles du gouvernement sont concernés, tels que les services de renseignement et les services de police. Les informations relatives à ces activités sont souvent volontairement cachées au public et protégées par des lois et des sanctions excessives.

Mais s'il est possible d'y accéder en toute sécurité, il existe de nombreuses méthodes et ressources qui peuvent vous aider. Nombre de ces sources sont déjà facilement accessibles en ligne, tandis que d'autres nécessitent un travail administratif et l'intervention de personnes susceptibles de vous aider.

Il n'est pas forcément sécuritaire d'accéder à ces sources de partout dans le monde : certains gouvernements sont connus pour punir les militants, les journalistes et autres personnes pour avoir exposé ou même cherché des informations sur de tels contrats, il faut donc évaluer et gérer les risques.

A. UTILISER LES LOIS SUR L'ACCÈS A L'INFORMATION

Une demande au titre du droit d'accès aux documents administratifs (FOI) ou d'autres lois sur l'accès à l'information (telles que les lois sur le droit à l'information) désigne une demande officielle que vous adressez à un organisme public (vos autorités locales, régionales ou municipales, la police, un ministère, etc.) afin d'accéder à des informations que le public est en droit de connaître. Vous pouvez essayer d'obtenir un contrat que les partenaires ont signé, une correspondance (e-mails ou lettres) entre les partenaires, des comptes rendus de réunions, des statistiques officielles, ou simplement une réponse à une question, voire d'autres documents tels qu'une présentation donnée à l'autorité publique par une entreprise, ou des matériaux de formation. Certaines lois précisent ce que vous pouvez et ne pouvez pas demander :

l'Ouganda, par exemple, exige que vous demandiez des documents spécifiques, ce qui signifie que vous ne pouvez pas poser de questions.

Les informations obtenues dans le cadre de ces demandes sont un outil inestimable pour les journalistes, les militants et le public : plus le public dispose d'informations, mieux nous sommes informés en tant que société et plus il est facile d'exiger des changements.

Cependant, bien que ces lois soient en apparence très en faveur du public et que plus de 90 pays disposent de législations obligeant les fonctionnaires à fournir des documents publics, dans la pratique, il n'est pas si simple d'obtenir les informations recherchées.

Lorsque vous soumettez de telles demandes, il est important de se rappeler quelques recommandations clés :

- Vérifiez que ce que vous cherchez n'est pas déjà librement accessible
- Sachez qui vous devez contacter (trouvez la bonne autorité contractante)
- Gardez vos demandes précises et contenues
- Parlez leur langue
- Soyez prêt à faire preuve de patience !

Privacy International propose un guide qui présente certaines des leçons que nous avons tirées du dépôt de telles demandes dans le monde entier.

Le Global Investigative Journalism Network dispose d'une excellente liste de ressources FOI disponibles dans de nombreux pays sur tous les continents. Nous vous recommandons vraiment d'y jeter un coup d'œil : beaucoup des guides FOI que nous aimons figurent dans ce référentiel.

Il est important de se rappeler que des documents publics utiles à vos recherches peuvent exister dans des juridictions insoupçonnées. Dans les cas où une société a son siège dans un pays mais exerce ses activités dans un autre, il peut être utile de soumettre des demandes dans l'une ou l'autre juridiction. Par exemple, des journalistes ont pu trouver plus d'informations sur la fourniture de technologies de surveillance à la Macédoine du Nord en soumettant des demandes aux autorités du Royaume-Uni qui

ont supervisé l'autorisation de l'exportation. Cependant, certains pays (par exemple l'Inde) n'autorisent que les demandes émanant de citoyens du pays.

Ce que disent nos partenaires :

Les lois sur l'accès à l'information peuvent être des outils utiles mais peuvent aussi s'avérer décevantes. Vous devez garder à l'esprit que votre demande peut rester sans réponse et prévoir en conséquence d'autres moyens d'obtenir des informations.

Certains de nos partenaires nous ont indiqué qu'ils trouvaient les demandes d'information plus utiles pour confirmer des choses qu'ils avaient déjà trouvées dans d'autres sources, tandis que d'autres les trouvaient plus utiles du point de vue de la communication publique ou pour en savoir plus sur la raison du rejet de la demande.

B. AUTRES SOURCES

i. Renseignement de sources ouvertes

Lorsque vous essayez de trouver plus d'informations sur les partenariats public-privé, il existe de nombreuses sources accessibles au public qui peuvent fournir des informations supplémentaires : la collecte et l'utilisation de ces informations sont parfois appelées Open Source Intelligence (OSINT) ou renseignement en libre accès.

Des organisations telles que Bellingcat ont largement utilisé l'OSINT pour découvrir les pratiques illégales des gouvernements et les violations des droits humains, y compris sur certaines des agences gouvernementales les mieux protégées et les plus secrètes du monde.

L'accès à des informations utiles dépend toutefois d'un certain nombre de facteurs, notamment le pays dans lequel le partenariat est basé, le type d'entreprise impliquée et le type de technologie ou de service qu'elle fournit.

Il existe de multiples ressources en ligne et dans des publications qui fournissent des informations sur la collecte d'OSINT, notamment :

- Bellingcat
- i-intelligence
- Le Tow Center for Digital Journalism
- OSINT Framework

De nombreuses techniques soulèvent toutefois d'importantes questions de sécurité, d'éthique et de droit qui doivent être prises en compte. Le Human Rights Center de la Berkeley School of Law et le Haut Commissariat des Nations unies aux droits de l'homme ont élaboré un guide sur l'utilisation des OSINT dans les enquêtes sur les violations du droit pénal international, des droits de l'homme et du droit humanitaire, qui fournit des indications sur ces considérations.

Par exemple, comme le note le guide, il pourrait être illégal dans certaines juridictions de déformer votre identité sur les réseaux sociaux. Même si ce n'est pas illégal, il peut s'agir d'une violation des conditions d'utilisation du réseau social ou du site, et si une fausse identité est utilisée pour accéder à ou solliciter des informations autrement inaccessibles d'un individu ou d'un groupe, cela peut violer des principes éthiques ou la loi.

Les sources ouvertes permettant d'accéder à des informations sur les partenariats public-privé comprennent :

- Les sites Web des entreprises, qui peuvent présenter leurs produits et parfois même publier des listes de clients.
- Les documents déposés par les entreprises auprès des autorités de réglementation, qui contiennent souvent des informations importantes comme leurs activités commerciales, leur structure et leurs revenus. Des chercheurs ont pu effectuer des analyses détaillées des structures d'entreprise des sociétés en utilisant ces informations. Ces informations sont disponibles sur des plateformes telles que OpenCorporates.
- Les offres d'emploi publiées sur des sites de recrutement et de réseaux sociaux communément accessibles, comme LinkedIn. Celles-ci fournissent souvent des indices ou des détails sur les activités commerciales d'une entreprise et leur localisation, ainsi que sur les innovations en préparation : par exemple, un journaliste britannique a pu accéder à des informations sur une « super base de données » secrète du gouvernement en utilisant les informations des offres d'emploi.
- Les données sur le commerce international, couramment mises à disposition par certains gouvernements et entreprises. Par exemple, les autorités indiennes publient des données sur les importations et les exportations, dont certaines sont ensuite accessibles sur des sites Web commerciaux. Cela peut être utilisé pour identifier certaines exportations : par exemple, Forensic News a identifié qu'une société israélienne de logiciels espions avait expédié des équipements à la police secrète d'Ouzbékistan en utilisant les données d'expédition.
- Données sur la transparence de l'aide gouvernementale. Cela peut souvent décrire les cas où les autorités gouvernementales ont fourni des équipements, des financements ou des formations à leurs homologues dans le monde entier et donc

fournir des informations sur les logiciels ou les équipements auxquels ils ont accès. Par exemple, en utilisant les données sur l'aide américaine, il est possible de cartographier les entreprises de surveillance dont les produits ont été fournis aux gouvernements d'Amérique centrale.

- Les réseaux sociaux, y compris par exemple les réseaux sociaux professionnels tels que LinkedIn. Il s'agit d'une source courante pour les journalistes et elle peut être utilisée pour identifier certaines informations concernant des personnes et des entreprises, mais elle doit être utilisée de manière éthique et légale (voir ci-dessus).

ii. Données sur les marchés publics

Les données sur les marchés publics sont l'une des meilleures sources ouvertes pour trouver des informations sur les partenariats public-privé. Les sites centralisés des marchés publics sont disponibles en plus de la documentation des appels d'offres sur les sites Web dédiés des agences, bien que les détails soient souvent limités.

Les informations accessibles au public sur les appels d'offres - annonces précisant qu'une autorité gouvernementale cherche à se procurer un service ou un produit auprès du secteur privé - peuvent fournir des informations précieuses. Souvent, l'appel d'offres ne fournit que des informations générales, mais il peut néanmoins servir de base à des recherches plus approfondies, par exemple en soumettant une demande d'accès à la liberté d'information (FOI).

Au Royaume-Uni, par exemple, il existe une plateforme centralisée, accessible au public, qui permet à quiconque de rechercher des appels d'offres lancés par des agences gouvernementales (bien qu'en pratique, de nombreux détails ne soient pas divulgués pour des raisons de sécurité nationale).

De même, les États-Unis, l'UE, la Russie et d'autres pays du monde entier publient des appels d'offres sur les sites web gouvernementaux.

En utilisant ces documents de marchés publics à l'approche des Jeux olympiques d'hiver de Sotchi en 2014, par exemple, des journalistes ont pu établir et cartographier la manière dont les services de sécurité russes prévoyaient de surveiller les communications téléphoniques et Internet tout au long des jeux.

Après avoir repéré un appel d'offres de Frontex (l'agence des frontières de l'UE) qui cherchait une société de surveillance pour suivre les personnes sur les réseaux sociaux, Privacy International a répondu par des questions détaillées sur la légalité du dispositif. Deux jours plus tard, Frontex a annulé l'appel d'offres.

Parfois, ces mêmes sites ou des sites similaires fournissent également des informations sur les contrats qui ont été attribués à telle ou telle entreprise. Par exemple, aux États-Unis, le site Web des marchés publics fédéraux fournit des données sur les entreprises qui ont obtenu des contrats. Ces sites sont régulièrement utilisés par les journalistes pour accéder à ces informations et en informer le public, bien que les détails soient là encore généralement minimes. Tech Inquiry fournit une plateforme consultable à travers laquelle il est possible de rechercher les contrats signalés par les autorités australiennes, canadiennes, américaines et britanniques.

Privacy International a également un guide destiné aux chercheurs et aux journalistes sur certaines sources ouvertes disponibles qui peuvent être utilisées pour identifier les exportations de surveillance.

Un cours en ligne gratuit pour en savoir plus sur la vie privée et la recherche sur les technologies de surveillance développé par Privacy International est disponible sur Advocacy Assembly.

iii. Parties concernées, une autre source d'information

En plus des recherches documentaires et des demandes formelles, entrer en contact avec des personnes impliquées dans un partenariat public-privé ou susceptibles d'en avoir connaissance peut donner accès à des informations ou à des perspectives cruciales pour votre travail.

Les universitaires, les membres du gouvernement, les personnes travaillant dans des entreprises privées similaires peuvent tous être des sources d'information utiles pour votre travail s'ils sont approchés correctement et si des pratiques de recherche adéquates sont mises en place (comme l'anonymisation).

Les journalistes qui ont couvert le partenariat sur lequel vous vous penchez peuvent également avoir eu accès à des sources importantes et être disposés à partager des détails supplémentaires avec vous si vous les contactez directement.

De même, d'autres organisations ou groupes peuvent se pencher sur le même partenariat. Essayez de vous coordonner avec ces groupes afin de partager des informations et éventuellement de renforcer votre plaidoyer par la suite.

Lorsque vous approchez des personnes directement impliquées dans le partenariat en question, vous devez vous assurer qu'elles se sentent en sécurité et que vous comprenez leur position. Il est essentiel d'être conciliant et d'éviter les accusations pour obtenir des informations importantes. Vous devez toujours être sensible aux préoccupations qu'elles peuvent avoir. En toutes circonstances, il est essentiel de discuter et de convenir à l'avance des conditions de cet échange d'informations. Demandez toujours de l'aide et des conseils si vous n'êtes pas sûr de la façon de traiter une source.

Avertissement : Avant d'entreprendre une interview, assurez-vous d'avoir procédé à une évaluation des risques adéquate et d'avoir sérieusement envisagé les risques pour votre organisation, ainsi que pour les personnes avec lesquelles vous vous entretenez. Vous devez vous assurer que vous pouvez fournir un niveau adéquat de confidentialité et de sécurité, et que vous comprenez les implications juridiques, avant de contacter des personnes susceptibles de se mettre en danger en partageant des informations.

Ce que disent nos partenaires :

Si le PPP que vous étudiez cible une région ou une zone spécifique, la consultation des journaux locaux, des groupes Facebook et des organisations locales peut révéler des informations importantes. Ces groupes peuvent avoir accès à des informations qui ne sont pas connues de tous ou être en contact avec des personnes clés impliquées dans le partenariat.

ADC, en Argentine, a déjà obtenu des informations clés en consultant un groupe Facebook d'habitants essayant de se mobiliser contre un projet dans leur région.

C. CHECKLIST – RECHERCHE D'INFORMATIONS

Pour vous aider dans vos recherches, vous pouvez utiliser cette checklist :

- ☐ Avez-vous envisagé les implications éthiques, juridiques et sécuritaires de l'accès aux et/ou du partage des informations que vous recherchez ?
- ☐ Avez-vous envisagé les risques possibles et les mesures de gestion des risques propres à votre contexte et à vos circonstances ?
- ☐ Les informations que vous recherchez sont-elles déjà facilement accessibles dans le domaine public ?
- ☐ La juridiction qui vous intéresse a-t-elle une loi sur la liberté d'information ou l'accès aux documents que vous pourriez utiliser ?
- ☐ Existe-t-il des guides ou des cours pertinents sur la manière de mener certaines techniques de recherche en libre accès qui pourraient vous aider à trouver ce que vous cherchez ?
- ☐ Existe-t-il des sources ouvertes auxquelles vous pourriez accéder dans votre pays pour trouver l'information ?
- ☐ Existe-t-il des sources ouvertes situées à l'étranger auxquelles vous pourriez accéder pour trouver l'information ?
- ☐ Existe-t-il des personnes ou des organisations qui pourraient vous aider à trouver l'information et que vous pouvez contacter en toute sécurité ?
- ☐ Vos sources vous ont-elles donné un consentement approprié et correctement informé ?
- ☐ Avez-vous réfléchi à la manière de traiter les informations que vous recevez de vos sources ?
    - ☐ Où allez-vous enregistrer ces informations ?
    - ☐ Avez-vous besoin de les rendre anonymes ? De les pseudonymiser ?
    - ☐ Devez-vous expurger des informations ? Comment allez-vous vous y prendre ?
    - ☐ Y a-t-il des détails contextuels dans l'information qui pourraient pointer vers votre source ou quelqu'un d'autre ?

3. IDENTIFIER ET COMPRENDRE LA TECHNOLOGIE CONCERNÉE

Les technologies au cœur d'un partenariat public-privé peuvent être entourées de secret et d'opacité, ce qui complique l'évaluation des risques par les acteurs externes. Qu'il s'agisse de mots à la mode ou d'une terminologie technique obscure, il n'est pas facile de se faire une idée réelle de la technologie en question et de ce qu'elle fait réellement. Cette section est conçue pour vous aider à trouver plus d'informations sur la technologie, à la comprendre et à identifier les failles potentielles.

A. IDENTIFIER LES COMPOSANTES DE LA TECHNOLOGIE EN QUESTION

La première étape de l'étude d'une technologie consiste à trouver des informations de base à son sujet, pour la définir et la catégoriser. Consulter la page Wikipedia d'une technologie donnée est souvent un bon point de départ et vous aidera à clarifier ce qui est implicite dans une technologie (par exemple pour la reconnaissance faciale). Cela est particulièrement utile lorsqu'aucune technologie spécifique n'est mentionnée dans le partenariat ou lorsque vous examinez un appel d'offres. Vous pouvez également consulter les documents marketing de l'entreprise pour vous faire une idée de sa spécialisation et du type de produit qu'elle propose.

Parfois, un partenariat impliquera plus d'une technologie, parfois plusieurs contrats et/ou partenariats : comme un système d'identification qui peut nécessiter un scanner d'empreintes digitales et une base de données, qui peuvent être fournis par différentes entreprises.

Avoir une idée générale de ce que vous recherchez est une étape simple mais très importante pour pouvoir aller de l'avant et identifier les risques. Votre objectif est de pouvoir donner une définition générale mais juste de la technologie en question dans le partenariat.

Exemples de descriptions générales d'une technologie :

- Système de reconnaissance faciale : un système capable de faire correspondre des visages identifiés dans une image ou une vidéo donnée avec un ensemble de données de visages humains précédemment identifiés.
- Bracelet électronique : un bracelet physique attaché à une personne, capable d'enregistrer et de transmettre sa géolocalisation ou sa proximité avec une station de base.
- Véhicule aérien sans pilote (« Drone ») : véhicule aérien autonome ou télécommandé capable d'effectuer des actions prédéfinies et de collecter, traiter et transmettre des données environnementales telles que des images, des températures et des sons.

Une fois cette première étape franchie, vous vous rendrez rapidement compte que les technologies reposent généralement sur de multiples éléments physiques et logiques pour fonctionner. La décomposition et l'identification de chaque couche est donc l'étape logique suivante pour comprendre comment la technologie fonctionne et quels sont les potentielles failles. Par exemple, un système de reconnaissance faciale capture, transmet, stocke et traite des données. Différents éléments jouent un rôle clé dans chacune de ces étapes.

Ces couches peuvent être du matériel, des logiciels ou une combinaison des deux. L'ensemble des technologies derrière un terme simple comme « une base de données » peut s'avérer complexe. Plus vous serez minutieux dans sa division en composantes, meilleure sera votre compréhension des enjeux et des risques qu'elle peut poser.

En utilisant une approche centrée sur les données, les différents éléments composant la technologie entreront généralement dans l'une des quatre catégories suivantes :

i. Système de collecte/capture des données (hardware/software)

La collecte de données revient à capturer des informations. Il peut s'agir d'un appareil photo prenant une photo, d'un capteur capturant des informations comme la

température, d'un logiciel enregistrant une action comme un clic sur un bouton ou d'un dispositif d'extraction de téléphone mobile saisissant les données d'un téléphone. Les systèmes de collecte de données peuvent être des dispositifs physiques (« hardware »), comme un satellite équipé de capteurs, ou virtuels (« software »), comme une application ou un scraper Web (un morceau de code qui parcourt Internet pour collecter des données).

Pourquoi est-ce important ?

Comprendre quelle partie de la technologie est chargée de la collecte des données vous permet de comprendre quelles sont les données collectées (images, sons, données saisies par l'utilisateur), d'où elles proviennent (capteurs, interactions avec l'utilisateur) et dans quelles circonstances elles sont collectées (à l'insu de la personne, à quelle fréquence, etc.). Cela vous permet d'identifier les problèmes potentiels concernant la légalité de la collecte ou l'exactitude des données recueillies.

Exemples de système de collecte de données :

- Un réseau de caméras dans une ville
- Un site Web permettant de s'inscrire à un événement public
- Un satellite équipé de divers capteurs prenant des photos d'une zone donnée
- Une machine à lire les empreintes digitales à l'aéroport

Risques potentiels de la collecte de données

Les données collectées peuvent être incorrectes, les capteurs peuvent être truqués, les données peuvent être collectées sans consentement ou autre base juridique, les capteurs physiques peuvent se dégrader avec le temps, la logique ou les instructions (pour un logiciel) peuvent être biaisées ou incorrectes, ou le dispositif peut être vulnérable à une attaque (surcharge, saisie d'informations incorrectes, etc.).

ii. Système de transmission de données (hardware/software)

Une fois les données collectées, elles peuvent être transmises à un autre système pour stockage ou traitement, par exemple un serveur. Les transmissions s'effectueront généralement par le biais de solutions existantes avec des protocoles bien définis tels que la suite de protocoles Internet (TCP/IP) pour la communication entre des dispositifs sur le même réseau (comme deux serveurs connectés à l'Internet ou une caméra intelligente et un ordinateur connecté à un réseau privé), mais l'innovation pourrait parfois être l'enjeu (par exemple, la proposition New IP faite par la Chine à l'Union internationale des télécommunications (UIT) ou 5G New Radio, la norme mondiale pour l'interface radio des réseaux 5G).

Pourquoi est-ce important ?

Comprendre si et comment les données sont transmises vous permet d'identifier les risques de sécurité potentiels (si la transmission n'est pas sécurisée, par exemple en utilisant un réseau Wi-Fi non sécurisé), les préoccupations existantes (si un protocole/réseau est obsolète et présente des vulnérabilités connues comme la 2G) ou les exigences techniques (par exemple la distance à laquelle le Bluetooth peut fonctionner pour transmettre des données de manière fiable) afin de mieux évaluer l'adéquation dans le contexte donné.

Exemples de systèmes de transmission de données :

- La suite des protocoles Internet (TCP/IP, le protocole sur lequel reposent la plupart des technologies Internet)
- Le système mondial de communications mobiles (GSM)
- Le Bluetooth
- Les satellites de télécommunications via des ondes radio à haute fréquence

Risques potentiels de la transmission de données

La technologie peut être peu sûre (niveau de cryptage faible ou insuffisant, vulnérabilités connues, etc.), les données peuvent être dégradées/perdues en transit, les données peuvent être interceptées/altérées, le système peut présenter des

menaces pour la santé, le système peut être interrompu par des facteurs externes (attaque par déni de service sur un réseau, destruction d'un émetteur/récepteur, etc.).

Remarque : Pour en savoir plus sur les protocoles, les normes et les organismes de normalisation, consultez la section « Note sur les protocoles techniques et les normes » à la fin de ce chapitre.

iii. Système de stockage des données (software/hardware)

Après la capture et la transmission des données, celles-ci peuvent être stockées quelque part à des fins de traitement ou d'archivage. Les systèmes de stockage s'appuient généralement sur une forme de dispositif de stockage tel qu'un disque dur, une carte SD, une clé USB, souvent dans le cadre d'un système plus important si un accès régulier est nécessaire (ordinateur portable, serveur...). La variété des logiciels chargés de stocker et d'accéder à ces données est massive, des logiciels de base de données tels que MySQL aux systèmes basés sur la blockchain qui offrent l'immuabilité des données.

Pourquoi est-ce important ?

Identifier où et comment les données sont stockées vous permet de mieux comprendre les implications (le logiciel/méthode utilisé peut être sujet à des vulnérabilités de sécurité ou fréquemment visé par des attaques comme une base de données ElasticSearch ou un produit Bucket similaire), la rétention (le système peut permettre de stocker les données seulement pendant un certain temps ou, au contraire, stocker les données indéfiniment comme un système blockchain), le contrôle d'accès (un système trop permissif peut permettre un accès non autorisé) et la durabilité (la durée de vie attendue d'une carte SD est plus faible que celle d'un SSD par exemple). Le système de stockage de données choisi est-il adapté à l'objectif qu'il entend atteindre ? Savoir où se trouve un système de stockage, à quoi il est connecté et qui y a accès donne également des clés pour mieux évaluer les risques.

Exemples de systèmes de transmission de données :

- Un disque dur/une clé USB avec un système de fichiers donné (NTFS, exfat, ext4...)
- Une base de données SQL (une base de données logicielle conçue pour être accessible à l'aide du langage SQL)
- Une blockchain dupliquée sur plusieurs clients
- Un CD non réinscriptible (CDR-R)
- Un logiciel de tableur tel que Microsoft Excel

Risques potentiels liés au stockage des données

Une mauvaise gestion des autorisations permettant un accès non autorisé aux données, la faillibilité du stockage matériel physique (par exemple, un disque peut tomber en panne et perdre les données qu'il stockait), des capacités de rétention des données inadéquates (par exemple, une blockchain stockant des données qui devraient être effacées), un espace de stockage inadéquat (par exemple, qui ne peut pas stocker de nouvelles données parce qu'il est plein), une mauvaise durée de vie (par exemple, choisir une gestion logicielle de base de données qui n'est pas prise en charge par son fabricant et qui ne reçoit pas ou ne recevra bientôt plus de mises à jour de sécurité), etc.

iv. Système de traitement des données (software)

Lors de la capture ou après le stockage, les données peuvent être traitées pour produire de nouvelles informations. Il peut s'agir d'un logiciel d'analyse d'images définissant les objets visibles dans une image capturée, d'un algorithme donnant la solution d'un problème mathématique, ou d'un programme prédisant des températures sur la base de données collectées précédemment. Les systèmes de traitement des données peuvent soit traiter les données à la volée (sans les stocker dans des étapes intermédiaires), soit utiliser des données stockées. Ces systèmes sont généralement des logiciels développés à l'aide d'un ensemble de langages de programmation (Java, Python, Go...) et peuvent fonctionner en liaison avec le système de stockage des données. Ils peuvent fonctionner sur de nombreux dispositifs allant d'un serveur à un smartphone ou un microcontrôleur monocarte. Certains systèmes, comme l'intelligence

artificielle basée sur les réseaux neuronaux, disposent de performances différentes selon les données qu'ils traitent, mais aussi selon les données sur lesquelles ils ont été entraînés. Dans ce cas, il peut être intéressant de considérer l'ensemble de données d'entraînement pour le système d'IA comme une composante distincte dans la catégorie Collecte/capture de données. Mieux vous séparerez les différents composants, mieux vous comprendrez ce qui est en jeu.

Pourquoi est-ce important ?

Les systèmes de traitement des données peuvent produire des informations biaisées et inexactes, que ce soit à cause des données introduites dans le système (incomplètes, inexactes, non représentatives...) ou à cause de défauts de logique (quelque chose de non pris en compte dans la logique de l'algorithme). Comprendre ce que le traitement est censé faire, quelles données sont traitées et quel type d'information il produit peut vous permettre de repérer d'éventuelles failles dans la logique du code, des variables manquantes ou d'évaluer dans quelle mesure un système est approprié pour prendre une décision.

Exemples de systèmes de traitement de données :

- Un logiciel de reconnaissance faciale traitant des photos prises par des caméras publiques
- Un logiciel de détection des mouvements de bateaux utilisant l'IA et l'imagerie satellite
- Un système publicitaire qui déduit vos traits de personnalité à partir de données collectées en ligne
- Un assistant virtuel tel que Siri/Google/Alexa

Risques potentiels du traitement des données

Défauts dans la logique de l'algorithme (quelque chose qui n'a pas été pris en compte ou une erreur humaine qui fausse les résultats), mauvaise prise en charge du fabricant (le logiciel/programme n'est plus pris en charge après un certain temps, ce qui rend le développement futur et les corrections compliquées ou impossibles pour l'acheteur), faible transparence/responsabilité due à la licence (les logiciels propriétaires rendent le

processus d'audit compliqué ou impossible), biais dû à l'ensemble de données sur lequel il a été entraîné ou aux données qui ont été incluses, faille de sécurité (accès non autorisé, piratage...) etc.

v. Note sur la hiérarchisation des composantes technologiques

Si vous vous intéressez à une entreprise ou à un contrat spécifique, vous pouvez utiliser cette structure et ces informations pour vous concentrer sur les couches dans lesquelles l'entreprise est principalement impliquée. Si vous vous intéressez à une entreprise spécialisée dans le traitement des données (comme Palantir), vous savez que cette couche sera probablement la plus importante.

Cela ne signifie pas que vous devez négliger les autres couches de la technologie déployée, au contraire. Ces éléments, parce qu'ils ne font pas nécessairement partie de l'expertise de l'entreprise ou de l'organisme public pourraient finir par être négligés et mal gérés. Par exemple, le Royaume-Uni a stocké et finalement perdu des données relatives à la COVID dans un fichier Excel, ce qui montre à quel point le système de stockage des données n'a pas été pris en compte, surtout par rapport aux efforts déployés pour collecter ces données.

B. ÉVALUER LA NOUVEAUTÉ/LE CARACTÈRE INNOVANT

Les partenariats public-privé peuvent très bien impliquer une technologie bien connue et déjà largement déployée dans d'autres contextes, mais ils peuvent aussi être un terrain d'innovation et de nouveauté.

Nous pouvons identifier deux principaux types d'innovation :

1. Technologie entièrement nouvelle : Une nouvelle technologie qui n'est pas largement utilisée ou qui n'a pas été déployée dans un contexte réel (en dehors d'un laboratoire ou d'un article de recherche) ;

2. Nouvelles fonctions/capacités : Un nouvel ensemble de caractéristiques ajoutées à une technologie existante qui étendent considérablement ses performances et ses capacités.

Un autre type d'« innovation » peut consister à déployer des technologies existantes dans de nouveaux contextes. L'évaluation de ces déploiements nécessitera principalement l'identification des usages et des problèmes de gouvernance (section 4 ci-dessous).

i. Technologie entièrement nouvelle

Dans le cas d'une technologie entièrement nouvelle, le facteur de nouveauté est généralement évident car la technologie en question est probablement peu connue. Les nouvelles technologies de pointe sont rares et présentent plusieurs risques, car elles n'ont pas nécessairement été testées correctement ou peuvent avoir des effets secondaires inattendus. L'approche d'une technologie entièrement nouvelle est difficile pour les acteurs externes et il peut être difficile de recueillir des informations pertinentes. Néanmoins, il existe plusieurs risques communs qui accompagnent l'innovation et qui pourraient valoir la peine d'être explorés :

- Les disparités entre l'environnement de test et le monde réel ayant un impact sur l'efficacité de la technologie ;
- Des tests insuffisants, ce qui signifie que la population pour laquelle elle est déployée est en fait un cobaye ;
- Une surestimation des capacités et de la précision de la technologie : la technologie ne fonctionne pas, produit trop d'erreurs ;
- La génération de nouveaux problèmes a été négligée : il peut s'agir du coût de la maintenance, de la viabilité du projet dans le temps, des problèmes découlant des cas frontières ou du fait que l'organisme public est prisonnier d'un contrat pour un service que personne d'autre ne peut fournir ;
- Le détournement d'usage, la technologie pouvant être utilisée à d'autres fins que celles pour lesquelles elle a été initialement conçue ;
- Un manque de transparence/responsabilité si la technologie est protégée par des secrets commerciaux et/ou par des licences exclusives.

ii. Nouvelles fonctions/capacités

Dans le cas d'une technologie existante dotée de nouvelles fonctionnalités ou capacités, l'innovation peut être plus difficile à repérer mais peut avoir un impact important sur l'utilisation de la technologie. Les nouvelles fonctions et capacités peuvent résulter d'un saut technologique au niveau du matériel ou du logiciel. Il peut s'agir, par exemple, de nouveaux processeurs (CPU) beaucoup plus puissants que la génération précédente, ou de nouveaux développements techniques tels que l'informatique quantique. Du côté logiciel, il peut s'agir du développement de nouvelles techniques de traitement, comme l'essor de l'apprentissage de réseaux de neurones profonds et de solutions d'IA équivalentes.

Ces innovations peuvent aussi être simplement l'ajout d'une technologie existante sur une solution, par exemple en montant des capteurs à fréquence Radion sur une multitude de petits satellites (tels que CubeSat), une innovation rendue possible par le faible prix de ces satellites. Les risques qui découlent de l'ajout de nouvelles fonctionnalités ou capacités sont plus spécifiques et devraient être plus faciles à identifier. Voici quelques-uns des risques qui découlent de telles innovations :

- Les capacités ajoutées peuvent être inutiles pour que la technologie remplisse sa fonction initiale (par exemple, équiper les caméras portées sur le corps de capteurs de température) ;
- La capacité ajoutée n'a pas été correctement testée pour l'environnement dans lequel elle est déployée et pourrait donner des résultats inappropriés (par exemple, le déploiement d'un algorithme de réseau neuronal pour le système judiciaire) ;
- La nouvelle fonctionnalité/capacité donne à la technologie une portée beaucoup plus intrusive (par exemple, l'amélioration de la qualité d'image des caméras de vidéosurveillance) ;
- Une nouvelle fonctionnalité/capacité rend la technologie beaucoup plus efficace et permet une application de masse (par exemple, l'interception et le traitement de masse des données d'Internet).

iii. Note sur les protocoles et normes techniques

Comme mentionné dans la section Système de transmission de données, les protocoles et normes techniques peuvent être un élément intéressant à examiner et à comprendre lorsqu'on essaie de disséquer une technologie. Cela peut fournir des informations sur le fait que le déploiement de la technologie a lieu dans un environnement déjà développé et standardisé, ou qu'il tente de définir de nouvelles normes. Voici quelques définitions utiles et des organismes de normalisation qui pourraient être pertinents :

Définitions :

- Protocole : un protocole est un langage convenu qui permet à différents éléments de communiquer. L'un des protocoles les plus connus est la suite de protocoles Internet, également connue sous le nom de TCP/IP. Les protocoles sont généralement standardisés et répondent à un ensemble de règles spécifiques. Ils permettent à tout nouvel acteur sur un marché de développer facilement un produit qui sera capable d'utiliser l'infrastructure existante et de communiquer avec d'autres produits. Par exemple, avec TCP/IP, n'importe qui peut créer un appareil connecté à Internet qui communiquera avec un serveur ou des appareils similaires dans le monde entier.
- Norme technique : norme ou exigence pour l'exploitation d'une tâche technique. Les normes techniques sont plus abstraites que les protocoles dans la mesure où elles n'offrent pas de règles concrètement définies pour un langage de programmation ou une technologie donnée. Elles établissent des principes, des méthodes et des processus uniformes qui doivent être suivis lors du développement d'une technologie. L'objectif est de garantir l'interopérabilité entre les dispositifs et les systèmes (par exemple, s'assurer qu'un disque dur externe d'une société autre que le fabricant de votre ordinateur fonctionnera dans n'importe quel ordinateur). Les normes peuvent être élaborées de manière privée ou unilatérale par des organismes de normalisation. Exemple : le « Universal Serial Bus » (USB).

Quelques organismes de standardisation :

- Union internationale des télécommunications (UIT) : l'UIT est une agence des Nations unies chargée des radiocommunications et de la normalisation. Elle œuvre

pour que les pays et les acteurs privés s'accordent sur des normes et des protocoles afin d'éviter les conflits et de favoriser le développement. Les normes élaborées par l'UIT sont appelées Recommandations. Quelques exemples :

- Gérer le spectre des fréquences radio (définit quelle partie du spectre peut être utilisée pour quoi, et par qui, par exemple, les technologies Wi-Fi et Bluetooth fonctionnent entre 2 400 et 2 500 MHz) ;
- Développer et maintenir l'Open Document Architecture, un exemple de format de fichier de document standard libre et gratuit que tout développeur de logiciel peut utiliser pour le traitement de texte ;
- Publier des recommandations concernant le blindage des câbles pour limiter les interférences ;
- Des groupes de travail élaborent des recommandations sur des sujets tels que les technologies d'information quantique pour les réseaux et l'intelligence artificielle pour la conduite assistée et autonome.

- Internet Engineering Task Force (IETF) : un organisme de standardisation ouvert, qui élabore et promeut des standards Internet volontaires, en particulier les standards de la suite de protocoles Internet (TCP/IP).
- Organisation internationale de normalisation (ISO) : organisme de normalisation composé de représentants de divers organismes nationaux de normalisation qui publie des normes techniques, industrielles et commerciales dans le monde entier. Exemple de norme : ISO 80601, qui garantit que les thermomètres sont étalonnés de la même façon dans différents hôpitaux.
- W3C : organisme de standardisation pour le World Wide Web.

Les organismes de standardisation qui tiennent des discussions ouvertes sur les normes sont des lieux intéressants (bien que souvent difficiles d'accès) où rechercher le lobbying et les exercices d'influence. Des entreprises privées ou des pays pourraient les utiliser comme passerelles pour promouvoir une solution technique susceptible d'avoir des conséquences politiques. Par exemple, en 2021, le W3C dispose d'un groupe d'activité « amélioration de la publicité sur le Web » dans lequel Google a suggéré un remplacement des cookies tiers qui permettent toujours le suivi et le ciblage des internautes.

C. COMPRENDRE LE FONCTIONNEMENT DE LA TECHNOLOGIE EN QUESTION

Nous identifions ici trois principaux moyens de mieux comprendre le fonctionnement d'une technologie :

i. Analyse documentaire
ii. Utiliser et tester les alternatives existantes
iii. Interroger des experts

i. Analyse documentaire

Il existe plusieurs ressources qui simplifient et vulgarisent les technologies complexes, à commencer par Wikipedia. D'autres ressources peuvent être extrêmement utiles même avec peu ou pas de connaissances techniques, comme la presse semi-spécialisée. Voir par exemple :

- MIT Technology review (par exemple, sur l'informatique quantique)
- ArsTechnica, (par exemple, sur les NFT)
- PC Mag (par exemple, sur la 5G)

Les articles académiques sont également une avenue pour trouver des informations, bien que le langage puisse être moins accessible sans connaissances techniques préalables. Néanmoins, il vaut la peine de faire des recherches sur Google Scholar et d'autres ressources pour trouver des articles sur la technologie que vous étudiez, idéalement dans un contexte similaire au vôtre ou se concentrant sur des préoccupations similaires.

Certaines ONG disposant de ressources techniques publient également des documents qui peuvent vous aider à comprendre le fonctionnement d'une technologie particulière et la manière dont elle peut être utilisée dans des contextes spécifiques, par exemple :

- Privacy International (abécédaire technologique du Bluetooth, du GPS)

- EFF (explications sur Amazon Sidewalk et les capteurs IMSI)
- Citizen Lab (Analyse du logiciel de filtrage de contenu sur l'application chinoise populaire YY)

Dans une certaine mesure, les sites Web des fabricants peuvent fournir des indications utiles sur la technologie que vous examinez et sur la façon dont elle pourrait fonctionner. La documentation technique ou promotionnelle des produits fabriqués par ces entreprises peut être un excellent outil pour comprendre les spécifications d'une technologie donnée et donner un aperçu de son fonctionnement. Vous pouvez utiliser des méthodes telles que Google Dorking pour trouver les brochures officielles des entreprises et d'autres documents qui vous aideront dans votre quête. Enfin, les bases de données de brevets (qui sont toujours publiques et accessibles en ligne, en général gratuitement – comme celle de l'OMPI) peuvent aussi fournir de précieuses informations détaillées sur les technologies qui ont été brevetées.

Comme pour toute recherche, le recoupement de ce que vous trouvez et la vérification auprès de plus d'une source sont essentiels pour éviter la désinformation !

ii. Utiliser et tester des alternatives

La recherche de systèmes équivalents abordables et l'étude de leur fonctionnement peuvent vous donner une meilleure idée de ce qui se passe dans le système que vous cherchez à analyser. Si vous vous intéressez aux systèmes de reconnaissance faciale par exemple, il peut être utile de rechercher des projets en libre accès que vous pouvez librement disséquer comme celui-ci.

L'utilisation de ces alternatives pourrait nécessiter certaines connaissances techniques et ne pas être facilement accessible à tous. Les tutoriels et les guides pour débutants peuvent vous aider à configurer et à tester ces systèmes et devraient être considérés comme une façon plus facile d'aborder cette stratégie. De même, certains cours en ligne sur du type « comment démarrer avec X » peuvent vous aider à mieux comprendre le fonctionnement d'une technologie. Les chapitres d'introduction du livre D2L sur l'apprentissage profond, par exemple, vous aideront à comprendre les différents éléments en jeu dans la technologie de l'IA.

Les organisations disposant d'une expertise technique pourraient également partager des guides, de la documentation et des méthodologies pour utiliser les systèmes dont elles se servent dans leur travail. Par exemple, Privacy International dispose d'un environnement d'interception des données pour analyser le trafic des applications Android et l'a mis à la disposition de tous.

Il peut être intéressant de chercher d'autres personnes qui ont déjà effectué ce genre de tests, comme des experts qui tentent de trouver des failles ou de démontrer des biais dans une technologie donnée. Le travail de Joy Buolamwini sur les systèmes de reconnaissance faciale racistes est un bon exemple d'expert testant une technologie pour en exposer les faiblesses.

iii. Interroger des experts

Après avoir effectué vos recherches, il se peut que certaines questions restent sans réponse, que vous n'arriviez pas à faire certains liens, ou tout simplement que vous n'ayez pas le bagage technique pour les comprendre. Dans ce cas, il peut être utile de s'adresser à des experts du monde universitaire, de la presse spécialisée ou des organisations de la société civile.

Dans ce cas, nous vous conseillons d'expliquer aussi clairement que possible ce que vous essayez de faire, dans quel but, ce que vous avez compris jusqu'à présent et de poser des questions aussi précises que possible. Les experts dans le domaine seront généralement moins intéressés par le fait de faire un cours sur une technologie donnée plutôt que de vous aider à comprendre son application dans un contexte spécifique. En rédigeant une liste de vos questions précises, assortie de détails sur le contexte, vous maximiserez vos chances d'obtenir une réponse ou un appel avec un expert.

Pour ce qui est des personnes à contacter, vous pouvez commencer par vous adresser aux universitaires qui ont rédigé des articles sur la technologie que vous étudiez, en particulier si leurs recherches portent sur l'un des principaux risques que vous avez identifiés. Vous pouvez également écrire aux professionnels qui travaillent avec la technologie en question, car ils ont généralement une grande expérience pratique de son utilisation. Chercher des personnes dans des groupes de travail, des groupes

d'échange et des groupes de partage des connaissances est une bonne première étape, car cela indique une volonté de partager et d'apprendre, ce qui augmente vos chances de trouver quelqu'un prêt à vous aider. Poser des questions sur des communautés en ligne spécialisées telles que StackOverflow ou Reddit peut également vous permettre d'obtenir des informations très pertinentes.

Certaines organisations, comme PI, disposent également de technologues auxquels vous pouvez essayer de vous adresser. Il se peut qu'ils n'aient pas d'expertise sur la technologie qui vous intéresse, mais ils pourraient éventuellement vous indiquer des ressources ou d'autres personnes à qui parler.

Ce que disent nos partenaires :

Il est difficile de comprendre totalement la technologie que vous étudiez. ADC suggère d'accepter que vous ne pouvez pas nécessairement savoir comment toutes les composantes impliquées fonctionnent et d'essayer de soumettre votre travail à des pairs pour vous assurer que vous ne dites pas quelque chose de manifestement faux. Il est plus important de s'assurer que vous avez les bonnes bases et que votre analyse est fondée sur des informations vérifiées que d'essayer de tout comprendre et de se concentrer sur des détails que vous pourriez avoir mal interprétés. Dans cette optique, ADC recommande de limiter la portée de votre travail à quelques éléments et de vous concentrer sur ceux-ci.

D. CHECKLIST – COMPRENDRE LA TECHNOLOGIE

Cette checklist est là pour vous aider à vous assurer que vous avez bien identifié les préoccupations liées à la technologie sur laquelle vous enquêtez :

- ☐ Pouvez-vous définir de manière générale la technologie en question et ce qu'elle fait ?
- ☐ Quel est le rôle des données dans la technologie en question ? (système de collecte de données, système de transmission de données, système de stockage de données, système de traitement de données)
- ☐ Quels sont les risques associés à cette technologie pour chaque système particulier ?
- ☐ Dans quelle mesure cette technologie est-elle innovante et révolutionnaire ?
    - ☐ [Facultatif] Quels sont les risques associés au facteur innovation ?
- ☐ Pouvez-vous expliquer comment la technologie fonctionne dans la pratique ?
    - ☐ [Facultatif] Quels sont les risques associés au fonctionnement concret de la technologie ?

4. PRÉOCCUPATIONS EN MATIÈRE DE GOUVERNANCE

Grâce à notre travail d'enquête et à celui de nos partenaires dans le monde entier, nous avons identifié un certain nombre de problèmes de gouvernance persistants communs aux partenariats public-privé. Nous avons détaillé chacune de nos préoccupations, et les mesures de protection correspondantes pertinentes, ici. Dans cette section, nous fournissons quelques conseils généraux sur la façon d'identifier ces types de préoccupations.

A. PRINCIPES DIRECTEURS DES NATIONS UNIES RELATIFS AUX ENTREPRISES ET AUX DROITS HUMAINS (UNGP)

Selon les principes directeurs des Nations Unies relatifs aux entreprises et aux droits humains (UNGP), les entreprises sont tenues responsables de respecter les droits humains, ce qui signifie qu'elles doivent éviter de porter atteinte aux droits d'autrui et qu'elles doivent remédier aux effets néfastes sur les droits humains dans lesquels elles sont impliquées (UNGP 11).

Les UNGP sont un ensemble de lignes directrices destinées aux États et aux entreprises pour prévenir, traiter et remédier aux violations des droits humains commises dans le cadre d'activités commerciales. Le Conseil des droits de l'homme des Nations Unies a approuvé les UNGP à l'unanimité dans sa résolution 17/4 du 16 juin 2011.

Les UNGP constituent la norme mondiale faisant autorité en matière d'action pour la protection des droits humains dans un contexte commercial. En tant que tels, au cours d'une enquête, ils peuvent être utilisés pour évaluer la conformité d'un partenariat public-privé aux normes en matière de droits humains. Ils peuvent également être utilisés comme

une ressource pour plaider en faveur d'actions spécifiques que les entreprises et les gouvernements doivent mettre en place. Dans cette section, nous présentons les principales responsabilités des entreprises découlant des UNGP et expliquons comment, malgré leur caractère non contraignant, ils sont devenus la norme pour évaluer les responsabilités en matière de droits humains dans les opérations commerciales.

i. Les Principes directeurs de l'ONU, norme de conduite pour les entreprises

Les UNGP contiennent trois chapitres, ou piliers : protéger, respecter et réparer. Chacun d'entre eux définit des mesures concrètes permettant aux gouvernements et aux entreprises de s'acquitter de leurs obligations et de leurs responsabilités respectives en matière de prévention des atteintes aux droits humains dans le cadre des activités des entreprises et de réparation si de telles atteintes ont lieu.

Entre autres considérations, les entreprises doivent :

- adopter une politique explicite et publique de responsabilité de respecter les droits humains ;
- procéder à des évaluations des risques en examinant les impacts réels et potentiels sur les droits humains des outils et services proposés (diligence raisonnable et évaluation d'impact en matière de droits humains) ; et
- mettre en place des mécanismes internes de responsabilité pour la mise en œuvre des politiques en matière de droits humains et disposer d'un processus permettant d'y remédier (mécanismes de réclamation).

Le processus de diligence raisonnable comprend quatre éléments essentiels : l'identification et l'évaluation des impacts négatifs réels ou potentiels sur les droits humains que l'entreprise peut causer, auxquels elle peut contribuer ou auxquels elle peut être directement liée ; la prise de mesures appropriées et l'intégration des résultats des évaluations d'impact dans les processus pertinents de l'entreprise ; le suivi de l'efficacité des mesures afin d'évaluer si elles fonctionnent ; et la communication avec les parties

prenantes sur la manière dont les impacts sont traités et la démonstration aux acteurs concernés que des politiques et des processus adéquats sont en place.

ii. Entreprises technologiques et Principes directeurs de l'ONU

Les Principes directeurs de l'ONU s'appliquent à toutes les entreprises, et s'appliquent donc au secteur technologique. Cependant, les entreprises technologiques n'ont pas fait l'objet du même niveau d'examen que les autres secteurs, notamment en raison de la complexité inhérente de leurs produits et services, et de la nouveauté des effets sociétaux qu'elles provoquent. Le projet UN B-Tech fournit des conseils et des ressources faisant autorité pour la mise en œuvre des UNGP dans le secteur de la technologie. Il a été lancé en 2019 et est dirigé par le Haut-Commissariat des Nations Unies aux droits de l'homme. Voir par exemple "The UN Guiding Principles in the Age of Technology".

En outre, les procédures spéciales de l'ONU et d'autres organismes de défense des droits humains offrent de plus en plus de conseils concernant l'application des UNGP dans le secteur de la technologie. Voir entre autres le rapport préparé sous l'égide du mandat de la Rapporteuse spéciale sur les droits de l'homme et la lutte antiterroriste, par Dr Krisztina Huszti-Orbán et Prof. Fionnuala Ní Aoláin, sur "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?". De même, le rapport 2019 du Rapporteur spécial sur la liberté d'opinion et d'expression sur « Surveillance et droits de l'homme » utilise les UNGP comme point de départ pour examiner la responsabilité des entreprises.

iii. Les Principes directeurs de l'ONU, norme mondiale

Les UNGP sont reconnus aujourd'hui comme la norme mondiale faisant autorité en matière de responsabilité des entreprises de respecter les droits humains, approuvée à l'unanimité par le Conseil des droits de l'homme de l'ONU en 2011 (Résolution 17/4). Bien que les UNGP ne soient pas formellement contraignants sur le plan juridique, ils sont en train de devenir la norme régissant les activités des entreprises à travers le monde, grâce aux nouvelles législations nationales et régionales, et aux initiatives des investisseurs.

1) Base de la législation nationale : Les UNGP ont servi de base à l'élaboration de nouvelles législations nationales sur la responsabilité des entreprises dans divers pays. En 2017, par exemple, le Parlement français a adopté une nouvelle loi imposant aux multinationales un devoir de vigilance pour prévenir les violations graves des droits humains dans toutes leurs filiales et chaînes d'approvisionnement (loi de vigilance). D'autres pays préparent des initiatives législatives similaires. De même, le 11 juin 2021, le Parlement allemand a adopté la « Loi sur la diligence raisonnable des entreprises dans les chaînes d'approvisionnement » (Loi sur la diligence raisonnable des chaînes d'approvisionnement - « Loi » ou « LkSG »). Le 23 février 2022, la Commission européenne a adopté une proposition de directive sur le devoir de vigilance des entreprises en matière de durabilité, fondée en partie sur les principes directeurs des Nations Unies.

D'autres pays et États ont mis en œuvre une législation sur la diligence raisonnable portant sur des droits humains spécifiques, par exemple l'Australie, la Californie et le Royaume-Uni sur l'esclavage moderne et les Pays-Bas sur le travail des enfants. Voir un aperçu des développements récents au Centre de Ressources sur les Entreprises et les Droits de l'Homme.

En outre, plusieurs pays, dont le Chili, la Colombie, le Danemark, la Finlande, l'Allemagne, les Pays-Bas, la Norvège, l'Italie, l'Espagne, la Suisse, la Tanzanie, la Thaïlande, le Kenya, l'Ouganda, le Royaume-Uni et les États-Unis, ont intégré les principes directeurs des Nations Unies dans leurs plans d'action nationaux respectifs. Un plan d'action national sur les entreprises et les droits de l'homme est une stratégie politique visant à garantir que les États se protègent de manière adéquate contre les conséquences négatives des entreprises commerciales sur les humains des personnes.

Très souvent, l'application de la législation nationale s'étend aux opérations commerciales au-delà du territoire des États législateurs. Par exemple, le projet de directive européenne vise à garantir le respect des droits humains et de l'environnement tout au long de la chaîne d'approvisionnement, que ses éléments se trouvent en Union européenne ou ailleurs.

2) Investissement responsable : Les UNGP ont également été compris comme fournissant des orientations pour l'investissement responsable. En 2018, un rapport du Groupe de travail des Nations Unies sur les entreprises et les droits de l'homme a spécifiquement appelé les investisseurs à mettre en œuvre une diligence raisonnable en matière de droits humains dans le cadre de leur propre responsabilité au titre des UNGP, à exiger plus systématiquement une diligence raisonnable effective en matière de droits humains de la part des entreprises dans lesquelles ils investissent, et à se coordonner avec d'autres organisations et plateformes pour assurer un alignement et un engagement significatif avec les entreprises. De plus en plus d'investisseurs assument cette responsabilité, soutenus par des initiatives telles que l'Alliance des investisseurs pour les droits de l'homme et les Principes pour l'investissement responsable.

B. PRÉOCCUPATIONS RELATIVES A LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

Une fois que vous avez bien compris le fonctionnement d'une technologie, vous devrez peut-être évaluer ses diverses implications en matière de protection des données et de la vie privée. Pour ce faire, nous avons décrit ici certains aspects généraux du traitement des données que vous pouvez passer en revue pour identifier toute préoccupation.

Il n'existe pas de normes universellement reconnues en matière de protection des données, mais des organismes régionaux et internationaux ont créé des codes, des pratiques, des décisions, des recommandations et des instruments politiques qui font l'objet d'un accord international. Les instruments les plus importants sont les suivants :

- La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (n° 108), 1981, telle que modifiée en 2018 ;
- Les Lignes directrices de l'Organisation de coopération et de développement économiques sur la protection de la vie privée et les flux transfrontières de données à caractère personnel (1980), telles que modifiées en 2013 ;

- Les Lignes directrices pour la réglementation des fichiers informatisés de données à caractère personnel (résolution 45/95 de l'Assemblée générale et E/CN.4/1990/72).

D'autres cadres régionaux existent également, notamment le cadre de protection de la vie privée de l'APEC – Coopération économique pour l'Asie-Pacifique. Certaines lois sur la protection des données ont aussi une portée extraterritoriale. Par exemple, le règlement général sur la protection des données (RGPD) de l'Union européenne s'applique aux responsables du traitement et aux sous-traitants qui ne sont pas basés dans l'UE, pour autant qu'ils traitent les données de personnes qui se trouvent dans l'UE et que ce traitement soit lié à l'offre de biens ou de services dans l'UE ou qu'il soit lié au suivi de leur comportement.

Lorsqu'il existe une loi complète sur la protection des données, les organisations (publiques ou privées) qui collectent et utilisent des données à caractère personnel ont l'obligation de traiter ces données conformément à cette loi. Vous devrez donc toujours vous référer aux lois de votre propre juridiction, mais cette section donne un aperçu des différents éléments à identifier. Cependant, il ne s'agit pas d'une liste exhaustive de toutes les préoccupations potentielles en matière de protection des données ; pour obtenir des conseils plus complets sur la protection des données, veuillez consulter notre guide complet.

i. Sources des données

La toute première étape de l'évaluation du traitement des données par une technologie consiste à comprendre où les données sont collectées, c'est-à-dire d'où elles proviennent. Vous l'avez peut-être identifié au stade de l'évaluation du système de collecte/capture des données de la technologie (voir la section 3 ci-dessus), mais vous pouvez compléter cette analyse par toute documentation relative à la technologie ou au partenariat (par exemple, contrats, protocoles d'entente, études d'impact sur la protection des données, contrats de traitement de données...), et étudier :

- Les ensembles de données/bases de données qui alimenteront la technologie ;

- Les listes de personnes concernées ou de catégories de personnes concernées dont les données seront traitées (par exemple, les membres du public, les suspects, les victimes ou les témoins d'actes criminels, les personnes qui vivent dans la région X...) ;
- Les sources des données (par exemple, les données proviendront-elles de bases de données existantes, ou de services gouvernementaux particuliers ou d'autorités ?).

Une fois que vous avez compris d'où proviennent les données, vous devez évaluer si la collecte ou le partage des données est légal (c'est-à-dire s'il est autorisé par une base légale telle que le consentement de la personne concernée ou une obligation légale de partager ces données), et si cette base légale est explicitement indiquée dans la documentation. La légalité de la collecte des données dépendra de la juridiction à laquelle le partenariat ou la technologie est soumis.

ii. Licéité et loyauté

Les données personnelles doivent être traitées de manière licite, équitable et transparente. Ce principe est essentiel pour lutter contre des pratiques telles que la vente et/ou le transfert de données personnelles obtenues par négligence ou frauduleusement.

La licéité signifie que les données doivent être traitées d'une manière qui répond à base légale de traitement. Vous devez évaluer la licéité du traitement pour chaque type ou catégorie de données qui seront traitées par la technologie, et pour chaque finalité du traitement. Par exemple, si les données d'une base de données de visages de membres du public seront traitées pour être recoupées avec une base de données de photos d'identité judiciaire, vous devez évaluer (1) si chaque base de données a été compilée avec base légale de traitement – notez que cela nécessite non seulement de s'assurer que l'autorité publique dispose d'une base légale pour collecter les visages en premier lieu (comme abordé par la section précédente) et construire la base de données, mais aussi de s'assurer que si les bases de données ont été compilées par une société privée, celle-ci

disposait également d'une base légale pour collecter les données en premier lieu, et (2) si le processus de recoupement repose sur une base légale de traitement.

Les bases légales de traitement que l'on trouve le plus souvent dans les lois sur la protection des données sont :

- le consentement de la personne concernée ;
- la nécessité du traitement à l'exécution d'un contrat avec la personne concernée ou à l'exécution de mesures précontractuelles ;
- la nécessité du traitement au respect d'une obligation légale ;
- la nécessité du traitement à la sauvegarde des intérêts vitaux d'une personne concernée ou d'une autre personne ;
- la nécessité du traitement à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- la nécessité du traitement aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, sauf si les intérêts, droits ou libertés de la personne concernée prévalent sur ces intérêts.

Pour plus de détails sur ces motifs de traitement, veuillez vous référer à cette section de notre guide de protection des données sur les motifs de traitement des données personnelles.

La loyauté exige que les données soient uniquement utilisées d'une manière à laquelle les personnes concernées s'attendent raisonnablement, ni d'une manière qui aurait des « effets négatifs injustifiés sur elles ».

Il s'agit d'un principe général qui doit régir tous les aspects du traitement : la collecte des données, la finalité du traitement et les conséquences du traitement. Pour évaluer l'équité, vous devez déterminer si le responsable de traitement a tenu compte des attentes raisonnables des personnes concernées à la lumière du contexte et de la finalité du traitement, des risques pour leurs droits et libertés fondamentaux, et de la relation générale entre le responsable du traitement et les personnes concernées (par exemple, existe-t-il un

lien ou des relations entre les deux qui feraient que les personnes concernées s'attendent à ce qu'un tel traitement ait lieu).

iii. Transparence et droit à l'information

Le caractère équitable du traitement dépendra aussi en grande partie de la transparence dont bénéficient les personnes concernées par le traitement. Les personnes doivent être informées lorsque leurs données personnelles sont collectées, et elles doivent pouvoir obtenir des informations sur leur traitement. Lorsque vous évaluez le déploiement d'une technologie, vous devez identifier si et par quels mécanismes les personnes concernées sont informées du traitement de leurs données.

Au moment de la collecte des données, et chaque fois que les données seront traitées pour une finalité non envisagée au moment de la collecte, les personnes concernées devraient recevoir au moins les informations suivantes (tant lorsqu'elles ont fourni les données directement au responsable du traitement que lorsque celui-ci les a obtenues d'une autre source) :

- Des informations sur l'identité du responsable du traitement (et ses coordonnées) ;
- Les finalités du traitement ;
- La(es) bases légales du traitement ;
- Les catégories de données à caractère personnel qui seront traitées ;
- Les destinataires des données à caractère personnel ;
- Si le responsable du traitement a l'intention de transférer des données à caractère personnel vers un pays tiers et quelles sont les garanties prévues pour ce transfert ;
- La période pendant laquelle les données à caractère personnel seront conservées ;
- Les droits de la personne concernée (tels que le droit d'accès, le droit d'opposition, les droits de rectification, de verrouillage et d'effacement, les droits liés au profilage et à la prise de décision automatisée, le droit à la portabilité des données) ;
- Le droit de déposer une plainte auprès de l'autorité de contrôle compétente ;
- L'existence d'un profilage, y compris la base légale, l'importance et la conséquence envisagée de ce traitement pour la personne concernée ;

- L'existence d'une prise de décision automatisée et, à tout le moins, des informations significatives sur la logique utilisée, l'importance et les conséquences envisagées de ce traitement pour la personne concernée ;
- La source des données à caractère personnel (si elles ne sont pas collectées auprès de la personne concernée) ;
- Le caractère obligatoire ou facultatif de la collecte des données ;
- Les conséquences d'un refus de fournir les données ;
- Si les personnes ne sont pas informées, vous devez déterminer si une exemption au droit d'information s'applique. Cela pourrait être le cas, par exemple, si le refus du droit d'information est nécessaire et proportionné pour prévenir ou détecter une infraction, pour préserver la sécurité nationale ou à des fins sanitaires, sociales ou éducatives. Cependant, toute exemption à ce droit doit être prévue par la loi, et doit être justifiée et soutenue par une évaluation de sa nécessité et de sa proportionnalité. Pour plus de détails sur les exemptions, veuillez consulter la section de notre guide de la protection des données consacrée aux dispositions générales, aux définitions et au champ d'application.

iv. Stockage des données et contrôles d'accès

Une fois que vous êtes convaincu.e (ou non !) que les données seront traitées de manière légale, équitable et transparente, vous devez vous demander où et pendant combien de temps elles seront stockées. La première question à se poser est de savoir si les données seront stockées sur des serveurs détenus par l'autorité publique, ou par l'entreprise, ou un autre tiers (par exemple, un sous-traitant). Vous avez peut-être identifié cela lors de l'évaluation du système de stockage des données de la technologie (voir la section 3 ci-dessus). Cela aura une incidence sur la répartition des responsabilités en matière de sécurité des données et de gestion des contrôles d'accès.

Les données personnelles, au repos et en transit, ainsi que l'infrastructure sur laquelle repose le traitement, doivent être protégées par des mesures de sécurité contre des risques tels que l'accès, l'utilisation et la divulgation illicites ou non autorisés, ainsi que la perte, la destruction ou les dommages. Voir la section 3 ci-dessus pour plus de détails sur les points à étudier. Les garanties de sécurité doivent être détaillées dans la documentation entourant le partenariat, avec une attribution claire des responsabilités entre l'autorité publique contractante, l'entreprise et toute tierce partie.

Pour évaluer la pertinence des contrôles d'accès, vous devez vous demander quel type d'accès aux données sera accordé à l'entreprise. En particulier, si les données sont stockées sur les serveurs de l'entreprise, vous devez vérifier si l'entreprise aura un accès complet aux données, ou si son accès sera restreint de sorte que seule l'autorité publique y ait accès. Même si les données sont stockées sur les serveurs du gouvernement ou de l'autorité, l'entreprise peut être autorisée à y accéder. Les règles relatives aux contrôles d'accès doivent être prévues dans la documentation du partenariat, avec des exceptions claires et strictes pour, par exemple, l'accès en cas d'urgence, l'accès pour la maintenance et autres.

Les contrats accordent parfois aux entreprises l'accès aux données pour des raisons telles que « l'amélioration de leurs services », « l'analyse des performances de leurs produits », etc. Il faut s'en méfier et se demander exactement quelle forme prendra l'accès de l'entreprise, et si elle bénéficiera effectivement d'un accès à la base de données d'une autorité publique afin de développer ses propres services, et ainsi profiter du partenariat au-delà de la valeur monétaire du contrat.

Pour obtenir plus de détails sur les exemptions, veuillez consulter la section de notre guide de la protection des données consacrée aux principes de protection des données.

v. Transferts internationaux de données

Vous devez évaluer si le stockage des données, l'accès ou d'autres dispositions de transfert impliqueront le transfert de données vers un autre pays (par exemple, si la société

contractante stocke ses données aux États-Unis). Le principe de base est que tout transfert de données personnelles vers un pays tiers ne doit pas abaisser le niveau de protection du droit à la vie privée des personnes. Les différentes juridictions ont des lois différentes régissant la manière dont un transfert vers un pays tiers peut être garanti comme étant « adéquat » en termes de protection des droits, mais vous devriez généralement vérifier les points suivants :

- Votre pays/juridiction a-t-il estimé que le territoire où les données seront transférées offre une protection « adéquate » des droits des personnes (c'est-à-dire qu'il existe ce que l'on appelle souvent une « décision d'adéquation ») ?
- Le transfert spécifique a-t-il été examiné et autorisé par une autorité de contrôle ?
- Existe-t-il un accord comportant des clauses types de protection des données approuvées par une autorité de contrôle ?

Des exceptions aux restrictions sur les transferts internationaux de données peuvent s'appliquer. Si une exception est censée s'appliquer, elle doit être prévue par la loi et faire l'objet d'un examen attentif afin qu'elle ne soit pas interprétée de manière trop large ou qu'elle ne donne pas lieu à des abus, et que le transfert reste conforme aux normes relatives aux droits humains.

Vous pouvez envisager d'autres questions en rapport avec les transferts internationaux de données. Par exemple, si les données qui seront transférées sont très sensibles ou concernent des populations très vulnérables, même si une décision d'adéquation ou d'autres garanties sont en place, vous pouvez vous demander si le pays destinataire dispose de lois ou de pratiques qui lui permettent de demander les données, et donc s'il existe un préjudice potentiel pour les personnes si ces données se retrouvent entre les mains du gouvernement du pays destinataire.

Pour obtenir plus de détails sur les exemptions, veuillez vous reporter à la section de notre guide de la protection des données consacrée aux obligations des responsables du traitement et des sous-traitants.

C. RESPONSABILITÉ ET CONTRÔLE

Un autre aspect important de l'évaluation de la gouvernance d'un partenariat public-privé nécessite d'analyser tout mécanisme de responsabilité et de surveillance en place, y compris les mécanismes par lesquels le partenariat a été initialement établi (par exemple, les processus de marchés publics).

Vous devez vérifier que certains documents et processus sont en place afin que l'État contractant et l'entreprise soient responsables, qu'il y ait des contrôles appropriés et des mécanismes de recours adéquats. Notez que vous devez tenir compte de l'ensemble du cycle de vie du partenariat. Tout d'abord, au stade de la passation des marchés, le processus de passation de ce contrat a-t-il respecté les règles locales ou internationales en la matière ? Et ces règles de passation de marchés sont-elles adéquates ? Y a-t-il eu une transparence adéquate tout au long de la procédure de passation de marché ?

Les évaluations d'impact et de risque en matière de droits humains et/ou les évaluations d'impact sur la protection des données/de la vie privée doivent normalement être réalisées avant l'attribution de tout contrat. Elles doivent être réalisées avec diligence, en suivant des modèles appropriés approuvés dans votre juridiction ou autrement reconnus par la société civile mondiale. Un exemple serait le guide et la boîte à outils pour l'évaluation de l'impact sur les droits de l'homme de l'Institut danois des droits de l'homme. Une étude d'impact correcte doit (en particulier, mais entre autres) effectuer une évaluation de la nécessité et de la proportionnalité qui tient compte des risques pour les droits des individus.

Vous devez ensuite vous demander s'il existe un mécanisme de contrôle indépendant, qui permettrait de s'assurer que le partenariat reste circonscrit à son objectif déclaré, de détecter les abus ou les préjudices qui en résultent, et d'exiger des réparations. Où et comment cela est-il défini et établi ?

Lorsqu'un partenariat public-privé est déployé, un organisme de contrôle indépendant (par exemple une autorité de contrôle de la protection des données, un organe de contrôle des techniques de renseignement...) devrait être désigné, afin d'être chargé (1) d'examiner, d'approuver ou de rejeter les nouvelles propositions d'utilisation de la technologie ou du

système déployé dans le cadre du partenariat, (2) d'entreprendre des audits réguliers du déploiement de la technologie, y compris des consultations publiques sur l'impact d'une technologie sur les droits des civils et la réalisation de son ou ses objectifs prévus, et (3) de recevoir les griefs et d'assurer la médiation entre le public et les entités utilisant la technologie. Cet organe de contrôle indépendant devrait être doté de ressources appropriées (humaines et financières) pour être en mesure de remplir ses fonctions.

Si ces documents et processus ont été mis en place, ils vous aideront à déterminer si le déploiement de la technologie est légal, nécessaire et s'il constitue une réponse proportionnée au problème qu'il est censé résoudre. Si ce n'est pas le cas, efforcez-vous de déterminer si la solution est appropriée ou si elle est excessive. Vous pouvez, entre autres, écrire à l'autorité publique concernée pour lui demander de mettre en place ces documents ou processus.

Ensuite, vous devez déterminer si le partenariat est régi par certaines normes de transparence ou exigences légales. Si tel est le cas, sont-elles adéquates ?

Vous pouvez ensuite examiner comment les partenaires impliqués seront tenus responsables des conséquences du déploiement de la technologie. La responsabilité exige que les devoirs, les rôles et les normes soient définis, appropriés et attribués aux parties concernées. Existe-t-il des mécanismes appropriés permettant à des tiers d'examiner et de contester les conséquences ?

Tout partenariat public-privé devrait être régi par des politiques appropriées régissant et documentant les diverses exigences mentionnées ci-dessus, telles que les données qui seront traitées, les personnes qui ont accès aux données et dans quelles conditions, les garanties qui doivent être mises en place pour atténuer les risques pour les personnes, l'organisme indépendant qui sera chargé de superviser le déploiement, etc. Ces politiques doivent également régir l'utilisation de la technologie par l'autorité publique et définir des limites claires pour la finalité et l'utilisation de la technologie, avec une liste exhaustive des utilisations autorisées et une liste non exhaustive des utilisations interdites. Elles doivent également prévoir des mécanismes de recours, en décrivant les processus de traitement

des plaintes et d'application des sanctions en cas de violation des politiques, et en attribuant les responsabilités et les obligations de recours à l'État et à l'entreprise.

Les garanties que nous avons décrites ci-dessus constituent, selon nous, un cadre raisonnable de protections pour faire respecter les responsabilités énoncées dans les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (UNGP), et garantir que les partenariats de surveillance public-privé n'entraînent pas de violations des droits humains.

Pour plus d'informations sur les différentes garanties qui doivent régir les partenariats public-privé de surveillance, veuillez vous référer aux garanties PPP de Privacy International.

D. CHECKLIST – GOUVERNANCE

Protection des données et de la vie privée

- ☐ Une fois que vous avez identifié la source des données, avez-vous évalué si la collecte ou le partage des données est licite ?
    - ☐ La base légale est-elle explicitement indiquée dans la documentation du partenariat ?
- ☐ Les données sont-elles collectées d'une manière à laquelle les gens peuvent raisonnablement s'attendre ?
- ☐ Les responsables du traitement des données ont-ils envisagé les risques pour les droits et libertés fondamentaux des personnes dont les données seront collectées ?
- ☐ Quelles seront les conséquences du traitement des données des personnes de cette manière ?
- ☐ Les personnes seront-elles informées lorsque leurs données personnelles sont collectées ?
    - ☐ Par le biais de quels mécanismes ?
    - ☐ Existe-t-il une exemption dans ce cas ? Est-elle justifiée ? Est-elle étayée par une évaluation de la nécessité et de la proportionnalité ?
- ☐ Les particuliers sont-ils en mesure d'obtenir des informations sur le traitement des données ?
    - ☐ Par le biais de quels mécanismes ?
- ☐ Combien de temps les données seront-elles conservées ?
- ☐ Qui hébergera les données ?
- ☐ Existe-t-il des garanties appropriées protégeant les données au repos et en transit ?
    - ☐ Sont-elles détaillées dans la documentation entourant le partenariat ?
    - ☐ Existe-t-il une répartition claire des responsabilités entre les parties contractantes ?
- ☐ Quel type d'accès aux données sera donné à l'entreprise ?
- ☐ Les données seront-elles transférées au-delà des frontières ?

- Dans l'affirmative, le pays vers lequel elles seront transférées offre-t-il un niveau de protection des droits de l'individu inférieur, supérieur ou identique ?
- Votre pays/juridiction a-t-il estimé que le territoire où les données seront transférées offre une protection « adéquate » des droits des personnes (c'est-à-dire qu'il existe ce que l'on appelle souvent une « décision d'adéquation ») ?
- Le transfert spécifique a-t-il été examiné et autorisé par une autorité de contrôle ?
- Existe-t-il un accord comportant des clauses types de protection des données approuvées par une autorité de contrôle ?
- Si non : le contrat s'appuie-t-il sur une exemption ? Cette exemption est-elle prévue par la loi ? Ce transfert est-il conforme aux normes en matière de droits de l'homme ?

Responsabilité et contrôle

- Le processus de passation de ce contrat a-t-il suivi un cadre de passation approprié ?
- Le contrat passé avec l'entreprise est-il conforme aux normes nationales et internationales ?
- La solution technologique est-elle nécessaire et constitue-t-elle une réponse proportionnée au problème qu'elle est censée résoudre ?
- La ou les entreprises impliquées dans le contrat ont-elles adopté un engagement politique explicite et public pour assumer leur responsabilité en matière de respect des droits humains ?
- Les parties ont-elles réalisé des évaluations de risques examinant les impacts réels et potentiels sur les droits de l'homme des outils et services proposés (diligence raisonnable et études d'impact sur les droits humains) avant l'attribution du contrat, et les ont-elles tenues à jour pendant le déploiement ?
- La documentation du partenariat prévoit-elle un contrôle indépendant ?
    - Où et comment celui-ci est-il défini ?

    - L'organe de surveillance dispose-t-il des ressources appropriées pour remplir son rôle ?
- Existe-t-il des normes ou des exigences légales en matière de transparence ?
    - Ces normes/exigences sont-elles adéquates ?
    - Ces normes/exigences sont-elles respectées ?
- Existe-t-il des mécanismes de responsabilité pour l'organisme public impliqué dans ce contrat ?
- Existe-t-il des mécanismes de responsabilité pour l'organisme privé impliqué dans ce contrat ?
    - L'organisme privé a-t-il mis en place des mécanismes internes de responsabilité pour la mise en œuvre des politiques en matière de droits humains ?
    - A-t-il mis en place des procédures de recours ?
- Des tiers peuvent-ils examiner et contester ces mécanismes de responsabilité ou leurs conséquences ?
- Quelles sont, le cas échéant, les politiques qui régissent et documentent ces exigences ?
- Comprennent-elles des règles concernant l'utilisation de la technologie par l'autorité publique, avec des limites claires quant à l'objectif et à l'utilisation de la technologie ?
- Le contrat prévoit-il des mécanismes de recours en cas de violation de ces politiques ? Comprennent-ils des sanctions adéquates et l'application de ces sanctions

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org