GARANTIES POUR LES PARTENARIATS PUBLICS-PRIVÉS EN MATIÈRE DE SURVEILLANCE

Décembre 2021

privacyinternational.org

À PROPOS DE PRIVACY INTERNATIONAL

Les gouvernements et les entreprises ont recours à 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

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, la tentation est grande de recourir aux services d'entreprises technologiques privées - par le biais de partenariats public-privé ("PPP"). La lutte contre la pandémie de COVID-19 et l'urgence de trouver des réponses et des solutions afin d'y répondre n'ont fait que renforcer l'impression des États qu'il est impératif de faire usage de technologies "innovantes" ainsi que de systèmes d'analyse de données développés par des prestataires externes. Mais ces PPP prennent de nouvelles formes qui s'écartent de la sphère des marchés publics traditionnels. Nous assistons en effet à une plus grande co-dépendance entre les parties. Aujourd'hui, l'État peut développer de nouveaux systèmes ou procédés entièrement dépendants des services d'une poignée d'entreprises voire d'une entreprise unique, celles-ci pouvant se voir conférer l'accès à des données ou à d'autres informations qu'elles seront en mesure d'exploiter afin de développer leurs propres services. Au-delà d'une simple relation commerciale "ponctuelle", ces partenariats se construisent souvent au fil de sollicitations des industriels, de promesses d'atteindre une compréhension parfaite de la réalité, et d'un accès toujours plus privatisé aux données - souvent au mépris des règles des marchés publics et des droits fondamentaux.

La privatisation de responsabilités relevant du secteur public peut s'avérer profondément problématique lorsqu'elle s'opère en l'absence de garanties essentielles pour s'assurer que les droits humains ne sont pas discrètement bafoués. Cela est particulièrement vrai lorsque les systèmes déployés sont utilisés à des fins de surveillance et de traitement en masse de données à caractère personnel. Les entreprises privées ont la réputation de jouer avec les limites de ce qui peut être fait légalement et éthiquement avec les identités et les données des individus, sans que le même niveau de responsabilité que celui exigé des autorités publiques ne leur soit imposé. Cela constitue un affront majeur aux droits fondamentaux lorsque ces mêmes entreprises sont mobilisées dans la fourniture de services publics.

Grâce à notre travail d'investigation et à celui de nos partenaires dans le monde entier, PI a identifié un certain nombre de problèmes communs aux PPP impliquant des technologies de surveillance et/ou des traitements de données en masse. Pour répondre à ces problèmes, nous avons défini un certain nombre de garanties dont nous recommandons la mise en œuvre tant par les autorités publiques que par les entreprises qui auraient l'intention de conclure de tels partenariats. Réparties entre des principes de Transparence, d'Attribution adéquate des marchés publics, de Responsabilité, de Légalité, de Nécessité et de Proportionnalité, de Contrôle et de Recours, ces garanties visent à faire respecter les droits humains et à rétablir la confiance dans les missions de l'État, celles-ci étant de plus en plus souvent confiées au secteur privé. Ces garanties ne tiennent pas compte des juridictions, afin qu'elles puissent s'appliquer aussi largement que possible dans le monde entier. Il s'agit d'un document évolutif, que nous mettons régulièrement à jour à l'aide de nouveaux exemples de violations commises dans le monde et de plaidoyers réussis contre les partenariats visant à instaurer la surveillance des individus.

Les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme (les "Principes directeurs de l'ONU")[1], approuvés à l'unanimité par les États lors de l'Assemblée générale de l'ONU en 2011[2], fournissent un mandat clair aux États et aux entreprises les invitant à renforcer les mesures visant à faire respecter, protéger et réaliser les droits de l'homme et les libertés fondamentales, et à étendre leurs responsabilités à cet égard, y compris dans l'industrie technologique[3]. Les garanties suivantes exposent ce que PI considère comme un cadre de protection adéquat pour faire appliquer ces responsabilités et garantir que les PPP n'entraînent pas de violations des droits humains. PI espère que ce document pourra aider la société civile à plaider en faveur d'un tel système face aux déploiements omniprésents de technologies.

[1] Haut-Commissariat des Nations unies aux droits de l'homme, Principes directeurs relatifs aux entreprises et aux droits de l'homme, 2011, disponible sur https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_fr.pdf.
[2] Résolution du Conseil des droits de l'homme de l'ONU sur les droits de l'homme et les sociétés transnationales et autres entreprises, Doc ONU A/HRC/RES/17/4, 6 juillet 2011, disponible sur https://undocs.org/en/A/HRC/RES/17/4.
[3] L'application des principes directeurs des Nations unies à l'industrie technologique a été réaffirmée par le Haut-Commissaire des Nations unies aux droits de l'homme dans le *B-Tech Foundational Paper on The UN Guiding Principles in the Age of Technology*, disponible à l'adresse https://www.ohchr.org/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf.

I. TRANSPARENCE

La transparence est un élément essentiel et une condition préalable à tout exercice et à toute protection des droits humains. En l'absence de transparence appropriée, l'exercice du pouvoir par l'État ne peut être soumis à l'examen de l'opinion publique. Le Rapporteur spécial des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a constaté que "[l]e principe de transparence et d'intégrité suppose l'ouverture et la communication au sujet des pratiques de surveillance". Le Rapporteur spécial a également noté que "[l]es techniques de surveillance doivent absolument faire l'objet d'un débat ouvert et d'un examen approfondi afin que le public en saisisse les avantages et les limites et en vienne à comprendre la nécessité et la légalité de la surveillance".[4]

Les PPP, et les relations commerciales continues qu'ils instaurent, souffrent souvent d'un manque de transparence. Les entreprises ont des intérêts commerciaux à préserver la confidentialité de leurs systèmes et de leurs algorithmes couverts par les secrets commerciaux. Nous avons régulièrement observé des États utiliser délibérément cette justification pour éviter d'avoir à communiquer autant d'informations que possible sur les détails d'une technologie de surveillance ou d'analyse de données. Mais comme tout processus de passation de marchés publics, les PPP appellent à respecter certaines exigences de transparence à chaque étape de leur déploiement : dès les procédures entourant les appels d'offres publics comme dans le cadre des conditions de déploiement des technologies, jusqu'à l'impact ou aux résultats des déploiements. Cela est essentiel pour que le public et la société civile puissent saisir l'étendue et les modalités de la surveillance d'État et de la gouvernance par les données.

[4] Rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, A/HRC/13/37, 28 décembre 2009 (" Rapport 2009 du Rapporteur spécial des Nations Unies sur la lutte antiterroriste "), paragraphes 55 et 56, disponible sur https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/178/05/PDF/G0917805.pdf?OpenElement; voir également *Escher et al. c. Brésil*, Cour interaméricaine des droits de l'homme, arrêt (sur les objections préliminaires, le fond, les réparations et les frais), opinion concordante du juge Sergio García Ramírez, série C n° 200, 6 juillet 2009, para. 6 ("Nous rejetons la furtivité avec laquelle le tyran dissimule son intolérable arbitraire. Nous condamnons le secret qui entoure les symboles de l'autoritarisme. Nous censurons l'opacité dans l'exercice de la puissance publique. Nous exigeons - et nous y parvenons, pas à pas, sur la base de l'argument des droits de l'homme - la transparence dans les actes du Gouvernement et dans la conduite de ceux qui nous gouvernent").

	v	Exemple(s)	Garantie(s)
1	Manque d'informations accessibles au public - les organisations de la société civile ("**OSC**") doivent déployer des efforts considérables pour obtenir des réponses limitées et restreintes aux demandes d'informations.	Palantir et le gouvernement britannique : les informations sur la collaboration de Palantir avec les services du gouvernement britannique ont été très limitées. PI et d'autres OSC ont tenté à plusieurs reprises d'obtenir des informations supplémentaires mais n'en ont reçu que très peu, celles-ci étant parfois contradictoires. [5]	**Tous les documents relatifs aux PPP doivent être mis à la disposition du public** - et en cas de préoccupations légitimes concernant la divulgation d'informations sensibles (tels que les secrets d'État ou les informations relatives à la sécurité nationale), ils doivent être mis à disposition, sur la base d'un accord de confidentialité, des organes de contrôle indépendants[6] (avec les autorisations/droits d'accès appropriés) pouvant évaluer leur conformité et exiger certains changements si nécessaire.[7] Toute expurgation de ces documents lorsqu'ils sont rendus publics doit être strictement justifiée et pouvoir être examinée si nécessaire par un organe de contrôle indépendant, et contestée. Les contrats de marchés publics doivent être

[5] Voir le rapport de PI et No Tech for Tyrant, *All Roads Lead to Palantir*, 29 octobre 2020, disponible sur https://privacyinternational.org/report/4271/all-roads-lead-palantir.

[6] De nombreuses garanties recommandent de confier certaines responsabilités à un organe de contrôle indépendant. Le choix de l'organe de contrôle indépendant approprié dans chaque cas dépendra du contexte national et de la nature du partenariat concerné. Par exemple, un partenariat dans lequel l'État passerait un contrat avec une entreprise pour l'utilisation d'une technologie de surveillance des communications nécessitera le contrôle d'un organisme de réglementation habilité à contrôler les pouvoirs d'investigation de l'État. Si la technologie concernée implique un traitement en masse de données à caractère personnel, une autorité de protection des données devra nécessairement être impliquée.

[7] Pour un exemple argentin de la manière dont le droit d'accès à l'information publique interagit avec les exceptions pour des raisons de sécurité nationale, veuillez consulter les observations présentées par l'Asociación por los Derechos Civiles (ADC) au Bureau du rapporteur spécial pour la liberté d'expression (RELE) de la Commission interaméricaine des droits de l'homme (CIDH) (mai 2018), disponibles sur https://adc.org.ar/wp-content/uploads/2019/06/039-acceso-a-la-informacion-publica-y-excepciones-de-seguridad-nacional-en-argentina-05-2018.pdf.

	v	Exemple(s)	Garantie(s)
			rendus publics (c'est déjà une obligation dans de nombreuses juridictions). La documentation plus large sur les PPP doit fournir des informations significatives sur la substance du partenariat, afin de permettre la compréhension de l'impact sur le public et les droits fondamentaux des citoyens. **La documentation du PPP doit généralement comprendre les éléments suivants** (selon la nature de la technologie et des services fournis, certaines évaluations peuvent ou non être requises) : • Contrats, informations sur les marchés publics, protocoles d'accord (MoU) et tout autre document fournissant des détails sur le partenariat. • Accords de partage de données ("**APD**") ou Accords de traitement de données ("**ATD**") • Études d'impact sur les droits humains ("**EIDH**") • Analyses d'impact sur la protection des données ("**AIPD**") ou évaluations des facteurs relatifs à la vie privée ("**PIA**") • Analyses d'impact algorithmiques ("**AIA**") • Registre des activités de traitement

	v	Exemple(s)	Garantie(s)
			Les autorités doivent tenir à jour un **inventaire public des technologies de surveillance** utilisées ou déployées dans leur juridiction. Cet inventaire doit contenir les détails et les finalités de traitement des technologies, leur portée (géographique, temporelle), les risques identifiés pour les droits des individus et les mesures prises pour les atténuer.
2	Les intérêts commerciaux ou les droits de propriété intellectuelle empêchent la divulgation de détails sur le fonctionnement d'une technologie ou d'un système.	Amazon et le NHS britannique : le contrat obtenu a été largement expurgé pour des raisons propres à l'intérêt commercial d'Amazon[8]. Après la contestation de PI, l'autorité britannique de protection des données en a ordonné une divulgation partielle.[9] Vote électronique au Paraguay : les machines de vote ont été	Les entreprises impliquées dans les PPP devraient renoncer au secret des affaires et rendre leurs technologies **entièrement auditables** par tout tiers, afin de permettre de comprendre (1) à quelles données l'entreprise et sa technologie ont accès, (2) comment la technologie analyse les données et tire des conclusions (y compris via la révélation des paramètres algorithmiques), et (3) quel rôle la technologie joue dans le processus décisionnel de l'autorité publique. Ces informations doivent être mises à la disposition du public avant l'attribution du marché. Si certains détails liés au fonctionnement d'une technologie particulière ne peuvent être divulgués pour des raisons précises et valables de

[8] Privacy International, Alexa, que se cache-t-il derrière votre contrat avec le NHS ? ", 6 décembre 2019, disponible sur https://privacyinternational.org/node/3298.
[9] Privacy International, Amazon Alexa/NHS contract : ICO allows partial disclosure, 27 avril 2021, disponible sur https://privacyinternational.org/news-analysis/4486/amazon-alexanhs-contract-ico-allows-partial-disclosure.

	v	Exemple(s)	Garantie(s)
		mises à disposition pour un audit, mais ni le code source ni le matériel n'ont été fournis lors dudit audit[10].	risque de préjudice commercial grave pour l'entreprise, un **organe de contrôle indépendant lié par des obligations de confidentialité** devrait se voir accorder un accès complet à ces informations.
3	Manque de visibilité sur le traitement des données à caractère personnel.	Palantir et les services de l'immigration britanniques, utilisation d'un outil lors du franchissement des frontières (*Border Flow Tool*) : il a fallu des mois à PI ainsi que de multiples demandes d'accès (*Liberté d'information* ('**FOI**')) pour comprendre quel type de données personnelles Palantir allait traiter. En effet, le contrat public ne mentionnait qu'un traitement de données des	Lorsqu'il est envisagé de traiter des données à caractère personnel dans le cadre d'un PPP, toute documentation provisoire ou définitive doit inclure des **éléments sur les activités prospectives comme réelles de traitement** et intégrer au minimum : • Les catégories de personnes concernées (notez que l'utilisation de termes généraux tels que "membres du public" tend à démontrer que les autorités n'ont pas correctement réfléchi à l'impact du traitement) • Types de données à caractère personnel, avec les finalités du traitement pour chacun d'entre eux • Sources des données à caractère personnel (c'est-à-dire où les données seront obtenues) et base légale de traitement pour l'obtention des données via chacune de ces sources

[10] TEDIC, Voto electrónico : falta de claridad de parte del TSJE a pocos días hábiles del periodo de testeo, 9 mars 2020, disponible sur https://www.tedic.org/voto-electronico-falta-de-claridad-testeo-tsje/.

	v	Exemple(s)	Garantie(s)
		"membres du public"[11].	Ces informations doivent être publiées dans les politiques de respect de la vie privée destinées aux populations dont les données seront traitées.
4	Manque de visibilité sur le type et niveau d'accès aux données accordés à l'entreprise.	Palantir et le NHS : le contrat contredisait l'analyse d'impact sur la protection des données (AIPD) réalisée en ce qui concerne l'accès de Palantir aux données[12].	**Les contrats de PPP doivent donner des détails explicites sur l'accès de l'entreprise aux données** (que ce soit pour la maintenance du logiciel, l'assistance à la clientèle, les journaux d'audits ou les situations d'urgence), et prévoir des garanties correspondantes pour assurer la sécurité et la bonne gestion des données. Les AIPD doivent évaluer les risques de transfert des données des citoyens (celles-ci pouvant constituer dans certains cas des données très sensibles) vers des entités privées et examiner la pertinence des droits d'accès, des mesures de sécurité, de conservation et de suppression associés.
5	L'accès du public à l'information sur les PPP est souvent entravé par l'absence ou l'inadéquation d'un cadre juridique ou procédural entourant	Caméras de surveillance Huawei à Valenciennes : les nombreuses demandes de PI à la ville de	Une **législation garantissant un accès approprié aux informations d'intérêt public** doit exister ou être adoptée. La documentation relative aux PPP doit pouvoir être consultée par le public dans le cadre d'une telle

[11] Whatdotheyknow, Registre des demandes d'accès de Privacy International au Cabinet Office, du 18 septembre 2020 au 3 mars 2021, disponible sur https://www.whatdotheyknow.com/request/contracts_with_palantir#incoming-1737614.
[12] Privacy International, The Corona Contracts : Public-Private Partnerships and the Need for Transparency, 26 juin 2020, disponible sur https://privacyinternational.org/long-read/3977/corona-contracts-public-private-partnerships-and-need-transparency.

	v	Exemple(s)	Garantie(s)
	l'accès à l'information (par exemple, les lois sur l'accès aux documents administratifs).	Valenciennes sont restées sans réponse pendant de longs mois car aucune entité définie n'avait été désignée comme responsable pour répondre à nos demandes[13].	législation. Lorsqu'un PPP est mis en place, **une personne ou une entité au sein de l'autorité publique compétente doit être désignée comme responsable** de l'accès aux informations relatives au déploiement d'une technologie et aux services connexes, et ses coordonnées doivent être disponibles sur le site internet notifiant le déploiement de la technologie et au sein de la documentation publique du PPP.

[13] Privacy International, Huawei à Valenciennes : une mauvaise romance (18 novembre 2021), disponible sur https://www.privacyinternational.org/long-read/4691/huawei-valenciennes-bad-romance.

II. ATTRIBUTION ADÉQUATE DES MARCHÉS PUBLICS

Les États doivent respecter certaines procédures officielles lors de l'attribution de marchés publics et de l'évaluation de services d'entreprises privées s'étant vues déléguer des prérogatives de puissance publique. Il s'agit là d'un principe fondamental des marchés publics, essentiel pour préserver l'intégrité de la dépense publique et la fourniture de services publics. Dans le cadre de ces procédures d'attribution de marchés, l'État et l'entreprise doivent exercer une diligence raisonnable l'un envers l'autre pour s'assurer que chacun respecte ses obligations respectives en matière de droits humains. En vertu des principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, les entreprises sont tenues "[d']éviter de porter atteinte aux droits de l'homme d'autrui et [de] remédier aux incidences négatives sur les droits de l'homme dans lesquelles elles ont une part", mais aussi de "connaître les droits de l'homme et montrer qu'elles les respectent dans la pratique", y compris dans le cadre de leurs relations commerciales[14].

Dans le contexte des PPP pour le déploiement de technologies ayant un impact potentiel sur l'exercice effectif des droits humains, les procédures d'attribution de marchés publics devraient être renforcées par certaines garanties et principes. Ceux-ci devraient permettre de s'assurer que des analyses d'impact appropriées ont été réalisées et qu'une technologie spécifique n'est pas déployée pour d'autres raisons que sa capacité à remplir un objectif de traitement approuvé et déclaré publiquement (et ce, entre autres, afin d'éviter des pratiques telles que la corruption, le lobbying abusif, le népotisme...). En exigeant des entreprises qu'elles respectent les obligations de diligence raisonnable en matière de droits humains ("DRDH"), les États peuvent également s'assurer qu'une technologie a été correctement évaluée lors de sa conception et de son développement, et non pas uniquement lors de son déploiement.

[14] Principe directeur 11 de l'ONU.

Quant à la phase dite de post-déploiement, les relations continues et de plus en plus interdépendantes entre les États et les entreprises dans le domaine des technologies de surveillance exigent des évaluations et des contrôles similaires, soutenus et approfondis tout au long du cycle de vie du partenariat.

	Problème	Exemple(s)	Garantie(s)
6	Absence ou non-respect d'une procédure officielle d'attribution de marchés publics et/ou exceptions à une telle procédure pour des raisons relatives à la sécurité nationale.	Au Pérou, l'utilisation d'une application de suivi de Covid-19 (*Peru En Tus Manos*) a été encouragée par le gouvernement, bien qu'aucune procédure officielle d'attribution de marché public n'ait été suivie[15]. Le contrat initial de Palantir avec le NHS pour la banque de données Covid, d'une valeur de 1 livre sterling, a été conclu sans examen approfondi ni respect des procédures	Lorsqu'ils attribuent un contrat à une entreprise, les pouvoirs publics doivent démontrer qu'ils respectent les **procédures officielles d'attribution de marchés publics** et doivent mettre en place une **documentation officielle** régissant ce type de partenariat. Toute exception à ce type de procédure (pour des raisons de sécurité nationale ou autres) doit être strictement encadrée et ne saurait servir à introduire une nouvelle technologie pour ensuite la réaffecter à des fins non autorisées en l'absence de procédure officielle d'attribution. Le niveau de contrôle requis dans un processus d'attribution de marché public ne devrait pas dépendre de la valeur du marché, mais plutôt des risques soulevés par le déploiement envisagé de la technologie.

[15] Hiperderecho, Liderazgo, estrategia, y donaciones privadas de tecnología frente al Covid-19, 6 juillet 2020, disponible sur https://hiperderecho.org/2020/07/liderazgo-estrategia-y-donaciones-privadas-de-tecnologia-frente-al-covid-19/. Pour la couverture de PI, voir Partenariats publics privés sur la technologie au Pérou : un gouvernement sans horizon, 17 septembre 2020, disponible sur https://privacyinternational.org/case-study/4167/public-private-partnerships-technology-peru-government-without-horizon.

	Problème	Exemple(s)	Garantie(s)
		d'attribution de marchés publics[16].	
7	Absence d'EIDH ou d'AIPD, ou absence de vigilance dans la réalisation de ces études.	Reconnaissance faciale en Argentine : le Rapporteur spécial de l'ONU sur le droit à la vie privée s'est dit préoccupé par le fait que deux villes avaient déployé des dispositifs de reconnaissance faciale et d'autres logiciels de surveillance sans effectuer de PIA, et que personne n'avait été en mesure d'expliquer la nécessité ou la proportionnalité	Les États et les entreprises contractantes doivent s'assurer que des processus de **diligence raisonnable en matière de droits humains** sont en place et témoignent d'une certaine robustesse. Ceux-ci doivent inclure dans leur champ d'application les premières étapes de la conception et du développement d'une technologie, ainsi que les étapes de déploiement et d'utilisation de celle-ci[19][20]. Les modalités des processus en place doivent être rendus publics et disponibles à la consultation. Lorsqu'un PPP est envisagé, des EIDH doivent être réalisées pour tout déploiement général ou spécifique d'une technologie[21]. Des AIPD doivent également être réalisées pour le déploiement de toute technologie impliquant un traitement de données

[16] The Bureau of Investigative Journalism, *Revealed : Data giant given 'emergency' Covid contract had been wooing NHS for months*, 24 février 2021, disponible sur https://www.thebureauinvestigates.com/stories/2021-02-24/revealed-data-giant-given-emergency-covid-contract-had-been-wooing-nhs-for-months.

[19] Le Haut-Commissariat des Nations unies aux droits de l'homme, B-Tech Foundational *Paper on Bridging Governance Gaps in the Age of Technology - Key Characteristics of the State Duty to Protect* (document de base sur la réduction des lacunes en matière de gouvernance à l'ère du numérique - caractéristiques clés de l'obligation de protection incombant à l'État), établit une "attente selon laquelle les entreprises doivent procéder à une diligence raisonnable en matière de droits de l'homme pour "connaître les droits de l'homme et montrer qu'elles les respectent dans la pratique" en indiquant comment elles traitent les impacts négatifs dans lesquels elles sont, ou pourraient être, impliquées, y compris en ce qui concerne la conception et l'utilisation de leurs produits et services, disponible à l'adresse https://www.ohchr.org/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf.

[20] Le Haut-Commissariat des Nations unies aux droits de l'homme a élaboré des lignes directrices sur l'exercice d'une diligence raisonnable en matière de droits de l'homme par les entreprises, disponibles sur https://www.ohchr.org/EN/Issues/Business/Pages/CorporateHRDueDiligence.aspx. Le Guide de l'OCDE sur le devoir de diligence pour un comportement responsable des entreprises fournit également des conseils pratiques et opérationnels pour la mise en œuvre du devoir de diligence en matière de droits de l'homme, disponible sur https://www.oecd.org/investment/due-diligence-guidance-for-responsible-business-conduct.htm.

[21] Pour des conseils pratiques sur la conduite des EIDH, voir par exemple l'Institut danois des droits de l'homme, Human rights impact assessment guidance and toolbox, 25 août 2020, disponible à l'adresse https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox.

	Problème	Exemple(s)	Garantie(s)
		de ces déploiements[17]. Huawei à Côme : l'AIPD réalisé par la municipalité ne couvrait pas l'impact de la technologie de reconnaissance faciale (**'RF'**) et n'évaluait pas la précision des algorithmes de RF[18].	à caractère personnel, que le traitement soit considéré comme susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques ou non[22]. Lorsque des algorithmes sont utilisés pour prendre des décisions automatisées, des AIA doivent également être réalisées[23].
8	Les AIPD sont considérées comme un outil de mise en conformité ultérieur à l'attribution d'un contrat plutôt que comme des outils d'aide à la décision d'attribuer un marché public.	Huawei à Côme : AIPD réalisée seulement après l'attribution de l'appel d'offres à A2A Smart City[24].	Des AIPD individuelles doivent être réalisées au cours du processus d'attribution de marché lors de l'évaluation des différentes technologies et des services des entreprises, et les résultats de ces AIPD doivent être pris en compte dans la décision d'attribuer ou non un marché. **Les autorités publiques ne sauraient attribuer un contrat de PPP qu'*après* qu'une AIPD ait été réalisée, publiée et mise à la disposition** des organes de contrôle

[17] Haut-Commissariat des Nations unies aux droits de l'homme, Déclaration aux médias du rapporteur spécial des Nations unies sur le droit à la vie privée, à l'issue de sa visite officielle en Argentine, 17 mai 2019, disponible sur https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E).
[18] Voir Wired, *Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale*, 9 juin 2020, disponible sur https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/. PI a été actif sur le sujet, voir *How facial recognition is spreading in Italy : the case of Como*, 17 septembre 2020, disponible sur https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como.
[22] Pour des conseils pratiques sur la conduite des analyses d'impact sur la protection des données et un modèle type d'évaluation, voir par exemple Information Commissioner's Office, Data protection impact assessments, disponible à l'adresse https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.
[23] Pour des conseils pratiques sur la réalisation des EAI, voir par exemple AI Now Institute, Algorithmic Impact Assessments : A Practical Framework for Public Agency Accountability, avril 2018, disponible à l'adresse https://ainowinstitute.org/aiareport2018.pdf.
[24] Voir n 18.

	Problème	Exemple(s)	Garantie(s)
			indépendants comme du public pour consultation pendant une période déterminée.
9	Risque que les entreprises contribuent à la surveillance de masse et aux pratiques autoritaires d'un État en procédant au déploiement de leurs technologies dans le pays.	Huawei en Ouganda : Huawei aurait dispensé une formation sur la surveillance à des agents des services de renseignement, qui s'en seraient saisis afin d'espionner les opposants du régime ougandais[25]. Le PCN (Point de Contact National de l'OCDE) britannique a estimé que les politiques de RSE et les pratiques de vigilance en matière de droits de l'homme de l'entreprise Gamma International étaient insuffisantes[26].	Les autorités doivent évaluer les politiques et les antécédents des entreprises en matière de droits humains et n'accorder des contrats de PPP qu'aux entreprises qui, dans le cadre de leurs politiques en matière de droits humains ou d'autres codes d'éthique, **s'engagent à refuser toute demande d'assistance de la part d'États en vue de déployer des dispositifs de surveillance illégaux à l'encontre de groupes spécifiques ou lorsqu'il existe des risques importants pour le respect des droits humains**. L'implication antérieure d'une entreprise candidate à un marché public dans des violations de droits humains ayant eu lieu dans d'autres pays doit être un facteur conduisant au rejet de son offre.

[25] The Wall Street Journal, *Huawei Technicians Helped African Governments Spy on Political Opponents*, 15 août 2019, disponible sur https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.
[26] NCP britannique, Décision suite à la plainte de Privacy International à l'encontre de Gamma International UK Ltd, 26 février 2016, disponible sur https://www.gov.uk/government/publications/privacy-international-complaint-to-uk-ncp-about-gamma-international-uk-ltd.

	Problème	Exemple(s)	Garantie(s)
10	Les technologies déployées à des fins privées sont parfois récupérées par les autorités publiques dans leurs activités de maintien de l'ordre, en l'absence de toute procédure d'attribution de marché public et de garde fou.	Amazon Ring a conclu des accords avec des services de police dans le monde entier, leur donnant accès à des réseaux de surveillance privés[27]. L'entreprise britannique Facewatch qui commercialise des outils de surveillance dédiés aux commerces a proposé aux services de police d'accéder à ses dispositifs[28]. Reconnaissance faciale à la gare de King's Cross de Londres - La RF a été installée à des fins de sécurité privée, puis utilisée dans le cadre d'activités de	Par principe, les **autorités publiques ne sauraient systématiquement faire usage de systèmes de surveillance et de traitement en masse de données déployés dans les espaces privés et/ou exploiter les données dérivées de ces systèmes**. Toute utilisation de ces derniers doit se faire de manière ponctuelle, en cas de stricte nécessité, en suivant un cadre juridique approprié, et en respectant les mêmes normes minimales de transparence, de traitement et de procédure régulière que celles exigées pour tout PPP. Cela signifie, par exemple, que les autorités ne sauraient se voir accorder un accès général, privilégié et indifférencié à ces systèmes ou données, mais devraient plutôt demander des informations spécifiques lorsqu'elles en ont besoin - en suivant un cadre juridique approprié et une procédure prescrite.

[27] Privacy International, *One Ring to watch them all*, 25 juin 2020, disponible sur https://privacyinternational.org/long-read/3971/one-ring-watch-them-all.
[28] Voir la lettre de PI à Mark Smith, PDG de Southern Co-Operative, 1er décembre 2020, disponible sur https://privacyinternational.org/sites/default/files/2020-12/PI%20Letter%20to%20Co-Op%20re%20Facewatch.pdf.

	Problème	Exemple(s)	Garantie(s)
		maintien de l'ordre[29].	

[29] Privacy International, King's Cross vous a surveillé - et la police a contribué, 25 juin 2020, disponible sur https://privacyinternational.org/case-study/3973/kings-cross-has-been-watching-you-and-police-helped.

III. RESPONSABILITÉ

En matière de droits humains, la responsabilité désigne l'obligation pour les personnes en position d'autorité d'assumer *la responsabilité* de leurs actes, d'en *répondre* devant les personnes concernées sous peine de *sanction exécutoire* si leur conduite ou leur explication venait à être jugée insuffisante[30]. Il s'agit d'un principe fondamental qui permet à l'ensemble des autres principes de pleinement s'appliquer à l'encontre de toute "entité responsable". À cet égard, les États se doivent d'offrir un espace suffisant à la société civile pour qu'elle puisse critiquer, dénoncer et contester les utilisations de technologies qui violeraient ou risqueraient de violer les droits humains[31].

Dans le contexte des garanties indispensables dans le déploiement de PPP, cette définition de la responsabilité exige d'identifier les obligations, les devoirs et les normes qui seront imposées à chacun des acteurs de la relation partenariale - à-travers, par exemple, l'inclusion de références à des codes reconnus ou à des politiques conçues sur mesure. Le défi est de taille pour les PPP, car l'État s'en remet ici à des acteurs privés, qui, contrairement à lui ne sont généralement pas tenus d'agir dans l'intérêt général ou pour assurer une mission de service public. Les mécanismes de responsabilisation doivent donc être particulièrement robustes et définis *avant* le déploiement de tout PPP.

	Problème	Exemple(s)	Garantie(s)
11	Les autorités publiques sont	Les données de Thomson Reuters	Lorsqu'un PPP ayant un impact potentiel sur le respect ou l'exercice

[30] Haut-Commissariat des Nations unies aux droits de l'homme, Qui sera responsable? Les droits de l'homme et le programme de développement pour l'après-2015, résumé, 2015, disponible sur https://www.ohchr.org/Documents/Publications/WhoWillBeAccountable_summary_en.pdf.

[31] Le document de base B-Tech du Haut-Commissaire des Nations unies aux droits de l'homme intitulé "Combler les lacunes de la gouvernance à l'ère de la technologie - Caractéristiques essentielles du devoir de protection de l'État" indique qu'"il est impératif que les États ne se servent pas de leurs obligations de protection contre les atteintes aux droits de l'homme pour façonner les pratiques, les produits et les services des entreprises de manière à provoquer des violations des droits de l'homme ou à y contribuer. À cet égard, toutes les parties prenantes - notamment la société civile et les organisations de défense des droits de l'homme - ont un rôle crucial à jouer pour repérer ces risques, les dénoncer et travailler dur pour y remédier. " Disponible sur https://www.ohchr.org/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf.

	Problème	Exemple(s)	Garantie(s)
	souvent tenues par des lois ou des codes spécifiques qui imposent à l'État de respecter certaines obligations en matière de droits humains, tandis que les entreprises privées ne sont pas toujours liées par ces mêmes textes.	ont été vendues aux services d'immigration et de douane des États Unis (ICE), une agence américaine qui aurait séparé des enfants de leurs parents et les aurait détenus dans des conditions déplorables. L'entreprise Thomson Reuters s'est contentée d'invoquer ses *"principes de confiance"* pour démontrer son engagement de ne pas contribuer à des violations de droits humains, en lieu et place d'un engagement clair à respecter la législation en vigueur relative aux droits humains dans	des droits humains est conclu, les obligations de l'État en matière de protection contre de telles atteintes doivent également s'appliquer pleinement à l'entreprise. Il doit en effet exister un mécanisme permettant de tenir l'entreprise responsable de toute violation de droits humains facilitée par sa technologie et/ou ses services. Les États doivent donc veiller à ce que les entreprises auxquelles ils attribuent des marchés publics dans le cadre de PPP **respectent les dispositions de toutes les lois, lignes directrices ou codes applicables que l'autorité publique signataire est tenue de respecter**[33]. Ce point doit être explicitement prévu dans la documentation qui régit le partenariat[34].

[33] Au Royaume-Uni, c'est ce qu'a recommandé le *Surveillance Camera Commissioner* pour le déploiement de la reconnaissance faciale par les forces de police, dans son rapport *Facing the Camera, Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales*, novembre 2020, paragraphe 4.73 : "Lorsque l'exploitation par un tiers d'un système de caméras de surveillance est confiée à un prestataire de services du secteur privé, la police doit veiller à ce que tout contrat relatif à l'exploitation de ce système impose au fournisseur l'obligation contractuelle d'agir conformément aux dispositions du Code [des caméras de surveillance] et aux dispositions légales applicables chaque fois que ce système est exploité en partenariat avec la police ou à sa demande." Disponible sur https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf.

[34] Le principe directeur de l'ONU dispose que "Comme étape nécessaire, les contrats de service pertinents ou la législation d'habilitation devraient clarifier les attentes de l'État quant au respect des droits de l'homme par ces entreprises. Les États devraient s'assurer qu'ils peuvent effectivement superviser les activités des entreprises, notamment en prévoyant des mécanismes indépendants adéquats de surveillance et de responsabilité. "

	Problème	Exemple(s)	Garantie(s)
		le cadre de ses services[32].	
12	Des technologies développées dans un certain pays sont fournies à un autre dont les normes en matière de droits humains sont différentes.	Le gouvernement chinois collabore avec des entreprises de surveillance chinoises afin de développer des normes technologiques de reconnaissance faciale considérées comme répressives (en intégrant, par exemple, le suivi des individus en fonction de leur origine ethnique) - ces mêmes technologies sont ensuite exportées[35]. Des opérateurs télécom fournissent des infrastructures permettant l'interception légale de télécommunications développées pour les normes de l'UE à des régimes dont la	Les États doivent **contrôler les exportations** de technologies de surveillance en évaluant le potentiel de leur utilisation à des fins de violations de droits humains. Les documents relatifs aux PPP doivent annexer **un ou plusieurs cadres de référence convenus en matière de droits de l'homme** qui régiront le partenariat et seront utilisés tout au long du cycle de vie de celui-ci afin de vérifier la conformité aux droits humains de la technologie en tant que telle, de son utilisation par l'État, ainsi que de tout service que l'entreprise privée serait amenée à fournir ultérieurement. Les entreprises doivent refuser de fournir leurs produits ou services à un État dont elles savent qu'il ne respecte pas les normes internationales en matière de droits humains[37].

[32] Sam Biddle, Thomson Reuters défend son travail pour l'ICE, en fournissant " l'identification et la localisation des étrangers ", The Intercept, 27 juin 2018, disponible sur https://theintercept.com/2018/06/27/thomson-reuters-defends-its-work-for-ice/.
[35] Avi Asher-Schapiro, *China found using surveillance firms to help write ethnic-tracking specs*, Reuters, 30 mars 2021, disponible sur https://www.reuters.com/article/us-china-tech-surveillance-trfn-idUSKBN2BM1EE.
[37] Les principes directeurs des Nations unies exigent des entreprises qu'elles prennent en compte l'utilisation potentielle de leurs produits dans le cadre de leur devoir de vigilance en matière de droits de l'homme.

	Problème	Exemple(s)	Garantie(s)
		législation en matière de droits humains est différente voire inexistante[36].	
13	Détournement de finalité (*function creep*) - les utilisations d'une technologie évoluent au fil du temps sans que de nouvelles procédures de validation et de contrôle ne soient respectées.	Caméras de vidéosurveillance utilisées pendant la pandémie de Covid-19 pour surveiller le respect de l'obligation de port du masque et de distanciation sociale sur la voie publique[38].	Une fois l'emploi d'une technologie approuvé, une **politique d'utilisation de technologie** doit être élaborée afin d'encadrer son usage par l'autorité publique. Cette politique doit définir des limites claires quant aux modalités d'utilisation et de finalité de traitement de la technologie, avec une liste exhaustive des usages autorisés et une liste non-exhaustive des usages interdits[39]. Toute utilisation de la technologie qui contreviendrait à la politique d'utilisation doit faire l'objet d'une nouvelle procédure de validation déterminant si la nouvelle utilisation est légale et conforme aux autres garanties. La politique d'utilisation de la technologie doit alors être amendée pour refléter cette nouvelle pratique. Toute utilisation projetée de la technologie qui serait totalement incompatible avec la finalité initiale du déploiement doit être rejetée.

[36] Voir par exemple Christopher Rhoads et Loretta Chao, *Iran's Web Spying Aided By Western Technology*, The Wall Street Journal, 22 juin 2009, disponible sur https://www.wsj.com/articles/SB124562668777335653.

[38] Voir l'avis de la CNIL sur l'utilisation de la "vidéo intelligente" pour mesurer le taux de port du masque dans les transports en commun : CNIL, *La CNIL publie son avis sur le décret relatif à l'utilisation de la vidéo intelligente pour mesurer le port du masque dans les transports*, publié le 12 mars 2021, disponible sur https://www.cnil.fr/fr/avis-sur-le-decret-video-intelligente-port-du-masque.

[39] Cela serait essentiel, par exemple, pour se conformer au principe de "limitation des finalités" du RGPD de l'UE, qui exige que les données à caractère personnel soient "collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités" (article 5, paragraphe 1, point b)). Ce principe de limitation des finalités doit être appliqué plus largement à toute utilisation d'une technologie qui affecte le bon respect des droits humains.

	Problème	Exemple(s)	Garantie(s)
14	Les entreprises s'appuient sur des organes internes de "conseil en matière de droits humains" pour démontrer leur conformité aux cadres de protection des droits humains, mais le fonctionnement de ces organismes n'est pas transparent et ceux-ci sont soumis à des obligations de confidentialité.	L'entreprise Palantir a créé le *Palantir Council of Advisors on Privacy and Civil Liberties* (PCAP) pour l'aider à "naviguer dans le paysage européen et plus largement international de la confidentialité des données"[40]. Le PCAP est uniquement consultatif, ses membres sont rémunérés pour leur temps et ses discussions sont confidentielles[41]. L'entreprise NSO s'était précédemment engagée à consulter des experts en droits humains sur ses pratiques, mais l'identité des experts et le contenu des conseils reçus n'ont jamais été rendus publics[42].	Si les entreprises parties à un PPP souhaitent s'appuyer sur les conseils d'organes internes privés pour démontrer qu'elles font preuve de vigilance, qu'elles tiennent compte des droits humains et qu'elles respectent la législation applicable en la matière, les **délibérations, conclusions et décisions de ces organes internes doivent être rendues publiques**. Ceux-ci doivent également choisir les cadres de protection des droits de l'homme nationaux, régionaux ou internationaux spécifiques auxquels ils adhèrent et indiquer quels cadres ont été choisis pour quels technologies ou déploiements. Des audits réguliers évaluant la conformité des produits et services de l'entreprise avec ces cadres doivent être réalisés et leurs résultats publiés.

[40] Palantir, *Privacy & Civil Liberties Engineering*, disponible sur https://www.palantir.com/pcl/.
[41] Ibid.
[42] Voir la lettre de plusieurs ONGs au groupe NSO, *NSO Group continue à ne pas respecter les droits de l'homme*, 27 avril 2021, disponible sur https://www.accessnow.org/cms/assets/uploads/2021/04/Rights-groups_NSO-Group-continues-to-fail-in-human-rights-compliance_27-April-2021.pdf.

	Problème	Exemple(s)	Garantie(s)
15	Il a été démontré que l'utilisation de technologies algorithmiques fondées sur l'exploitation de données peut avoir pour effet d'ancrer les inégalités, les discriminations et les injustices, sans permettre aux personnes concernées de remettre en question les décisions prises par ou à l'aide de ces technologies.	Un algorithme développé par l'entreprise Palantir a été utilisé pour distribuer les vaccins de Covid-19 aux États-Unis, créant des disparités et des inégalités inexplicables dans la répartition des doses entre les différents États[43].	Les algorithmes et autres dispositifs de prise de décision automatisés déployés dans le cadre de PPP doivent **pouvoir être contrôlés et remis en question** - en étant vérifiables (comme l'exige la garantie n° 21 ci-dessous). La capacité d'auditer les technologies est particulièrement essentielle pour assurer un contrôle et un droit de recours adéquats (par exemple, si une technologie a conduit à un résultat qui est ensuite contesté devant un tribunal ou utilisé comme preuve, la bonne administration de la justice exige que la technologie soit entièrement vérifiable). Dans le cadre de la procédure d'attribution de marché public, l'évaluation des différents systèmes devrait **comparer leurs niveaux de biais discriminatoires**. Si un biais discriminatoire est identifié, il doit être rectifié, et s'il ne peut l'être, la technologie ne saurait être déployée.

[43] The New York Times, *Where Do Vaccine Doses Go, and Who Gets Them ? The Algorithms Decide*, 7 février 2021, disponible à l'adresse https://www.nytimes.com/2021/02/07/technology/vaccine-algorithms.html?referringSource=articleShare.

IV. LÉGALITÉ, NÉCESSITÉ ET PROPORTIONNALITÉ

L'utilisation d'une technologie ou d'un système pour assurer une mission de service public ne peut être légitime que si elle est légale, c'est-à-dire si elle s'inscrit dans un cadre juridique approprié autorisant l'utilisation de cette technologie pour ces objectifs spécifiques. Il s'agit du principe de légalité, un principe fondamental du droit international des droits humains qui exige que toute ingérence dans les droits humains soit "prévue par la loi"[44]. En outre, le droit international des droits humains exige que toute ingérence dans le droit au respect de la vie privée soit nécessaire et proportionnée[45]. Aussi, lorsqu'un Etat déploie une technologie susceptible d'avoir un impact pour le respect de la vie privée de ses citoyens, il doit être en mesure de démontrer de manière "spécifique et individualisée la nature précise de la menace" à laquelle cette technologie cherche à répondre[46]. Le principe de proportionnalité exige que l'ingérence dans la vie privée soit à la fois "proportionnée [à l'objectif recherché] et qu'elle constitue l'option la moins intrusive possible"[47].

Dans le contexte des PPP, des évaluations de la légalité, de la nécessité et de la proportionnalité doivent être effectuées *avant* toute attribution de marchés publics à des entreprises privées, ainsi que *pendant* la passation de marché et ce avant tout déploiement de la technologie.

---

[44] Voir les articles 8 à 11 de la Convention européenne des droits de l'homme, les articles 12 et 17 à 22 du Pacte international relatif aux droits civils et politiques, et les articles 11 à 13, 15 et 16 de la Convention interaméricaine des droits de l'homme.
[45] Voir Comité des droits de l'homme des Nations unies, *Toonen c. Australie*, Comm. No. 488/1992, Doc ONU CCPR/C/50/D/488/1992, 31 mars 1994, para 8.3 ("Toute ingérence dans la vie privée doit être proportionnelle au but recherché et être nécessaire dans les circonstances de l'espèce.") ; Haut-Commissariat des Nations unies aux droits de l'homme, Le droit à la vie privée à l'ère numérique, Doc ONU. A/HRC/27/37, 30 juin 2014). (" Rapport du HCDH sur le droit à la vie privée à l'ère numérique "), paragraphe 23 (" Ces sources faisant autorité [les Observations générales 16, 27, 29, 31 et 34 du Comité des droits de l'homme de l'ONU et les Principes de Syracuse] soulignent les principes primordiaux de légalité, de nécessité et de proportionnalité [...] ").
[46] Comité des droits de l'homme des Nations unies, Observation générale n° 34 (article 19 du PIDCP), 12 septembre 2011, paragraphe 35.
[47] Rapport du HCDH sur le droit à la vie privée à l'ère numérique (n 45), paragraphe 10.

	Problème	Exemple(s)	Garantie(s)
16	Des technologies portant atteinte à la vie privée sont déployées en l'absence de cadre juridique approprié autorisant et régissant leur utilisation.	La technologie d'extraction des données des téléphones portables (**MPE**) est déployée par les services de police du Royaume-Uni depuis des années en l'absence de cadre juridique approprié[48]. Huawei à Valenciennes : Huawei a déployé des caméras de surveillance équipées de technologies de reconnaissance faciale dans la ville de Valenciennes, alors que la RF n'est pas légalement autorisée en France[49].	Lorsqu'il examine le besoin d'avoir recours au déploiement d'une technologie pour répondre à un besoin public ou assurer une mission de service public, l'État doit se demander si **un cadre juridique approprié prévoit l'utilisation de cette technologie pour l'objectif visé**. La technologie ne doit pas être expérimentée ni déployée avant l'adoption d'une loi adaptée (et non d'un règlement). Une telle loi ne sera considérée comme appropriée que si elle autorise l'utilisation d'une technologie spécifique, par des autorités spécifiques, dans un objectif précis - un texte d'application générale (par exemple, l'octroi de pouvoirs discrétionnaires généraux et indifférenciés aux services de police) ne sera pas suffisant. Un cadre juridique adapté devra également contenir des politiques et des orientations spécifiques régissant l'utilisation de la technologie (telles que la politique d'utilisation de la technologie présentée dans la garantie n°13).
17	Les technologies déployées dans le cadre de PPP ne sont pas	Huawei à Belgrade : l'AIPD n'a pas établi que l'utilisation de la	Dans le cadre d'une AIPD et/ou d'une EIDH adéquate, une **évaluation de la nécessité** doit être menée pour démontrer clairement

[48] Privacy International, *Digital Stop and Search : how the UK police can secretly download everything from your mobile phone*, mars 2018, disponible à l'adresse https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.
[49] Privacy International, *Huawei à Valenciennes : une mauvaise romance* (18 novembre 2021), disponible sur https://www.privacyinternational.org/long-read/4691/huawei-valenciennes-bad-romance.

	Problème	Exemple(s)	Garantie(s)
	toujours nécessaires pour atteindre les objectifs fixés.	vidéosurveillance "intelligente" était nécessaire pour la sécurité publique car elle a surestimé ses effets positifs sur la réduction de la criminalité[50].	que le recours à une technologie ou à un système d'analyse de données particulier est nécessaire pour atteindre des objectifs précisément définis. Celui-ci ne saurait constituer un simple avantage. Dans le cadre de cette évaluation, tout effet positif anticipé de la technologie doit être interrogé à l'aide d'un ensemble de sources indépendantes et de pratiques comparatives.
18	Les technologies déployées dans le cadre de PPP ont souvent un impact sur les droits humains disproportionné par rapport à leur objectif.	Huawei à Côme : la nécessité d'un système de reconnaissance faciale a été justifiée dans la documentation officielle par un incident isolé survenu des années auparavant[51].	Dans le cadre d'une AIPD et/ou d'une EIDH appropriée, une **évaluation de la proportionnalité** doit être réalisée pour mesurer l'impact négatif sur les droits et libertés des individus et démontrer qu'il est justifié par un impact positif correspondant sur leur bien-être. Ces évaluations doivent tenir compte des effets dissuasifs (*chilling effects*) potentiels sur l'exercice d'autres droits, tels que les droits à la liberté d'expression et à la liberté de réunion, qui peuvent être affectés par les systèmes de surveillance et de traitement de données d'une manière pouvant être difficile à anticiper et à mesurer.

[50] SHARE, *"Thousands of Cameras"* - une réponse citoyenne à la surveillance biométrique de masse, 25 juin 2020, disponible sur https://privacyinternational.org/case-study/3967/thousands-cameras-citizen-response-mass-biometric-surveillance.
[51] Voir Wired et Privacy International (n 18).

V. CONTRÔLE

Les principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme exigent que les États exercent "un contrôle adéquat afin de satisfaire à leurs obligations internationales en matière de droits de l'homme lorsqu'ils s'assurent par contrat auprès d'entreprises de services qui peuvent avoir une incidence sur l'exercice des droits de l'homme, ou s'ils légifèrent en la matière".[52]

Le contrôle continu du déploiement et des performances d'une technologie est essentiel pour veiller au respect de mécanismes de responsabilisation permettant de garantir qu'une technologie est utilisée conformément à son objectif déclaré, de détecter de potentiels abus ou dommages et de garantir un droit de recours. Le rapporteur spécial des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a expliqué que "les systèmes de surveillance doivent faire l'objet d'une supervision efficace afin de minimiser les préjudices et les abus". Le rapporteur spécial a recommandé que "[d]es instances de contrôle indépendantes, dotées de mandats robustes, doivent être créées pour examiner les politiques et les pratiques, afin de permettre un contrôle strict de l'utilisation de procédés de surveillance intrusifs et du traitement des informations à caractère personnel"[53]. Les garanties présentées dans cette section préconisent donc des mesures concrètes afin d'établir des mécanismes de contrôle adaptés tenant compte des préjudices potentiels que peut causer le déploiement de technologies privées aux personnes ou communautés qui y sont confrontées.

[52] Principe directeur 5 de l'ONU.
[53] Rapport 2009 du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Martin Scheinin, (n 4), paragraphe 62.

	Problème	Exemple(s)	Garantie(s)
19	Absence d'entité indépendante chargée de superviser le partenariat et ses obligations envers le public.	Technologie d'extraction des données des téléphones portables au Royaume Uni : l'utilisation de cette technologie par les forces de l'ordre au Royaume-Uni a duré des années d'une manière que l'autorité de protection des données britannique (l'ICO) a par la suite jugée irrégulière et illégale[54].	Lorsqu'un nouveau PPP est déployé, **établir ou désigner une instance de contrôle indépendante** (en fonction de la technologie et de l'autorité concernée, il peut s'agir de l'autorité de protection des données du pays, s'il en existe une, ou d'une autorité de supervision des pouvoirs de surveillance) chargée (1) d'examiner, d'approuver ou de rejeter les nouvelles propositions d'utilisation de la technologie ou du système déployé dans le cadre du PPP, (2) de procéder à des audits réguliers du déploiement de la technologie, y compris à travers des consultations publiques portant sur l'impact de la technologie sur les droits des populations et sur l'atteinte des objectifs visés, et (3) de recevoir des plaintes et des griefs et de servir de médiateur entre le public et les entités utilisant la technologie[55]. Cette instance de contrôle indépendante doit être dotée de moyens suffisants (humains et financiers) pour être en mesure d'exercer ses fonctions.
20	Manque de consultation des populations affectées par le	Amazon Ring a conclu des accords avec des services de police,	Lorsqu'une technologie est susceptible d'affecter certaines populations de manière disproportionnée, il est recommandé

[54] Voir les recommandations concernant la surveillance sur Information Commissioner's Office (ICO), *Mobile phone data extraction by police forces in England and Wales - Investigative Report*, juin 2020, disponible sur https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf.

[55] Au Royaume-Uni, par exemple, le Commissaire chargé des caméras de surveillance recommande que "lorsque les forces de police envisagent d'utiliser des technologies de reconnaissance faciale en temps réel (LFR), elles doivent mettre en place des mécanismes permettant une "surveillance éthique" significative et indépendante de leur prise de décision et de leur conduite opérationnelle. Ces considérations devraient être appliquées dans le cadre des processus de planification initiale de la police et être établies avant le début de toute activité opérationnelle". (Facing the Camera, n 33, paragraphe 2.26).

	Problème	Exemple(s)	Garantie(s)
	déploiement des technologies.	leur donnant accès à des réseaux de surveillance privés en l'absence de consultation des populations[56].	d'**instituer un "conseil civil de contrôle"** composé de personnes directement affectées par la technologie et en particulier de celles qui risquent d'être victimes de discrimination. Ce conseil de contrôle doit être consulté avant tout déploiement de la technologie, il doit être en charge de recueillir le consentement de la population concernée et être en mesure de recevoir et de faire entendre les doléances relatives à l'impact de la technologie sur les droits des individus dans toutes les phases de déploiement de celle-ci.
21	Absence d'évaluations d'impact continues.	Aux États-Unis, les services de police n'enregistrent pas les erreurs ou les résultats erronés des technologies de reconnaissance faciale (RF) qu'ils mobilisent, ce qui donne une vision unilatérale et exclusivement positive de la RF[57].	Tout au long du déploiement d'une technologie dans le cadre d'un PPP, les autorités publiques doivent enregistrer certains indicateurs de performance de cette technologie tels que les taux de vrais positifs, de vrais négatifs, de faux négatifs et de faux positifs, les niveaux de précision, l'objectif visé par le déploiement et les résultats dans les faits[58]. Par l'intermédiaire d'une instance de contrôle indépendante, et en collaboration avec un conseil civil de contrôle, les autorités publiques doivent effectuer des **audits réguliers** de la technologie et des **mises à jour adéquates des EIDH**. Ces audits doivent inclure des

[56] Voir Privacy International (n 27).
[57] Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, 12 janvier 2020, The New York Times, disponible sur https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.
[58] Des indicateurs de performance similaires ont été recommandés par le Commissaire aux caméras de surveillance pour être développés par le Conseil national des chefs de police du Royaume-Uni afin d'évaluer l'impact des opérations de reconnaissance faciale en temps réel (Facing the Camera, n 33, paragraphe 6.10).

	Problème	Exemple(s)	Garantie(s)
			consultations régulières avec les groupes et les individus concernés par la technologie (en particulier ceux qui risquent d'être victimes de discrimination) et avec les OSC, afin d'évaluer les impacts actuels ou potentiels de la technologie de manière holistique. Un **audit "rétrospectif"** doit également être réalisé après la fin de la relation contractuelle, car les impacts d'une technologie sur les droits humains peuvent parfois être différés dans le temps. Les conclusions de cet audit doivent être publiées et servir de base aux évaluations de tout futur PPP.

VI. DROIT AU RECOURS

Le déploiement de technologies privées aux fins d'assurer des missions de service public peut être source de nombreux dysfonctionnements et entraîner de graves répercussions pour le respect des droits humains. Lorsque des violations ont lieu, le droit international des droits humains impose aux États de garantir le "droit à un recours effectif" à toute personne dont les droits auraient été violés[59]. Les États ont pour obligation légale de fournir des mesures réparatrices efficaces visant notamment à indemniser "les préjudices aux droits de l'homme liés aux entreprises, tout comme les préjudices aux droits de l'homme associés au développement et à l'utilisation de technologies numériques par les entreprises."[60].

Dans le contexte des technologies de surveillance et du traitement de données à caractère personnel, le secret entourant les technologies utilisées rend la réparation des préjudices particulièrement difficile à obtenir. Tout en reconnaissant qu'une "notification préalable ou concomitante pourrait compromettre l'efficacité de la surveillance", le rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression a souligné que "les individus devraient néanmoins être avisés une fois la

[59] Voir la Déclaration universelle des droits de l'homme, Résolution 217 (III) A de l'Assemblée générale des Nations Unies, 10 déc. 1948, Art. 8 ("Toute personne a droit à un recours effectif devant les juridictions nationales compétentes contre les actes violant les droits fondamentaux qui lui sont reconnus par la constitution ou par la loi ; Art. 2(3), Pacte international relatif aux droits civils et politiques ("Les Etats parties au présent Pacte s'engagent à: a) Garantir que toute personne dont les droits et libertés reconnus dans le présent Pacte auront été violés disposera d'un recours utile, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles") ; Art. 25, CADH ("1. Toute personne a droit à un recours simple et rapide, ou à tout autre recours effectif devant les juges et tribunaux compétents, destiné à la protéger contre tous actes violant ses droits fondamentaux reconnus par la Constitution, par la loi ou par la présente Convention, lors même que ces violations auraient été commises par des personnes agissant dans l'exercice de fonctions officielles".) ; article 13, CEDH ("Toute personne dont les droits et libertés reconnus dans la présente Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles"). Voir également les Principes fondamentaux et directives concernant le droit au recours et à l'indemnisation des victimes de violations flagrantes du droit international des droits de l'homme et de violations graves du droit international humanitaire, résolution 60/147 de l'Assemblée générale des Nations Unies, 16 décembre 2005.

[60] Bureau du Haut Commissaire aux droits de l'homme des Nations Unies, B-Tech Foundational Paper, Access to remedy and the technology sector : basic concepts and principles. Citant le principe directeur 25 de l'ONU, disponible sur https://www.ohchr.org/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf.

surveillance achevée et avoir la possibilité de chercher réparation eu égard aux retombées de l'utilisation de mesures de surveillance des communications"[61].

Dans le contexte des PPP, l'absence récurrente d'informations due aux restrictions de confidentialité peut affecter la possibilité de chercher réparation. Le droit au recours doit être justifié, conçu et attribué d'une manière qui corresponde à la façon dont une technologie fonctionne et est utilisée - d'où la nécessité que les autres principes soient dûment respectés, en particulier le principe de transparence, de responsabilité et de contrôle.

De même, les États doivent être en mesure d'engager des poursuites à l'encontre des entreprises qui ne respectent pas les conditions de leurs accords de PPP ou qui sont tenues responsables de faciliter des violations de droits humains. Cela est essentiel pour que les États puissent s'acquitter de leurs obligations envers leurs citoyens lorsque la faute incombe entièrement ou partiellement à l'entreprise à laquelle ils ont attribué un marché.

	Problème	Exemple(s)	Garantie(s)
22	Absence de voies de recours en cas d'utilisation abusive d'une technologie	Un logiciel malveillant (*malware*) de l'entreprise NSO a été utilisé pour cibler des avocats de victimes au Mexique. Une fois découvert, NSO n'a pas contribué aux efforts visant à demander des comptes et à	Porter une action devant les tribunaux ou d'autres systèmes judiciaires n'est souvent pas une option viable pour les personnes affectées par des utilisations isolées d'une technologie, surtout si l'on considère que l'abus peut être difficile à établir par le biais de voies de recours traditionnelles. La politique d'utilisation de la technologie recommandée par la garantie n°13 doit inclure des **dispositions introduisant des voies de recours** en indiquant les mécanismes et entités existants, ou en en créant de nouveaux, pour le

[61] Rapport du rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression, UN Doc. A/HRC/23/40, 17 avril 2013, para 82, disponible sur https://undocs.org/fr/A/HRC/23/40 .

	Problème	Exemple(s)	Garantie(s)
		obtenir réparation[62].	traitement des plaintes et l'application de sanctions en cas de violation de cette politique (notamment en désignant un organisme de contrôle indépendant adéquat, à même d'enquêter et d'offrir des possibilités de recours). Ces voies de recours et les organismes chargés de leur bonne administration doivent être adaptés à la nature de la technologie, à son objectif et à ses effets identifiés. Ils doivent attribuer des responsabilités et des obligations de réparation tant à l'État qu'à l'entreprise concernée, et doivent respecter les huit "critères d'efficacité" énoncés dans le principe directeur 31 des Nations unies. Pour autant, les dispositions en matière de voies de recours ne doivent pas empêcher l'accès aux tribunaux ou à d'autres mécanismes judiciaires établis. Elles doivent trouver un juste équilibre entre l'effectivité des recours et le respect de l'État de droit. L'État doit également s'assurer que l'entreprise à laquelle il attribue un marché public dispose d'un mécanisme de réclamation[63] permettant de signaler les éventuels effets négatifs de technologies pour le bon respect des droits humains et d'y remédier rapidement.

[62] Citizen Lab, Reckless IV - *Les avocats des familles de femmes mexicaines assassinées ciblés par les logiciels espions de l'entreprise NSO*, 2 août 2017, disponible sur https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/

[63] Ceci est requis par le principe directeur 29 des Nations unies.

	Problème	Exemple(s)	Garantie(s)
23	Les contrats de PPP ont tendance à enfermer les autorités et les entreprises publiques dans le partenariat par le biais de clauses de modification ou de résiliation très coûteuses.	L'Agence des frontières du Royaume-Uni (*UK Border Agency*) est poursuivie en justice par l'entreprise Raytheon Systems Limited pour résiliation abusive d'un contrat de fourniture d'un système informatique de gestion de flux migratoires[64]. L'entreprise Palantir et les services de police de la ville de New York : à la fin du contrat, Palantir a refusé de produire l'analyse générée par son logiciel pour qu'elle soit transférée vers un nouveau système non affilié à	Les contrats de PPP doivent inclure des **clauses de résiliation** permettant (1) à l'entreprise de résilier le contrat si elle apprend que sa technologie a été utilisée ou est destinée à être utilisée pour des activités non conformes au cadre de référence convenu en matière de droits de l'homme, et (2) à l'État de résilier le contrat s'il apprend que l'un des produits de l'entreprise a été utilisé dans le cadre de violations de droits humains par d'autres États (que le produit en question soit ou non celui qui fait l'objet du contrat), ou s'il apparaît que certaines dispositions du contrat empêchent l'État d'agir dans l'intérêt général. Les contrats de PPP doivent également intégrer des **clauses strictes d'interopérabilité et de transférabilité**. L'interopérabilité et la transférabilité sont essentielles dans le domaine des marchés publics, car tout État est tenu de fournir des services conformément à certaines exigences et en respectant une procédure précise. Si une entreprise avec laquelle un contrat a été conclu modifie le fonctionnement de son ou de ses services ou ses modalités d'utilisation les rendant incompatibles avec les obligations de l'État, ce dernier doit être entièrement libre de

[64] Voir Computer Weekly, *Le gouvernement britannique paie 150 millions de livres sterling à Raytheon pour régler le différend sur les frontières électroniques*, 27 mars 2015, disponible à l'adresse https://www.computerweekly.com/news/4500243244/UK-government-pays-150m-to-Raytheon-to-settle-e-Borders-dispute.

	Problème	Exemple(s)	Garantie(s)
		l'entreprise Palantir[65].	se retirer de ce partenariat et d'en conclure un autre, sans que l'entreprise ne thésaurise des données ou des informations ni que le changement de fournisseur n'entraîne des coûts "punitifs" ou indus pesant sur la dépense publique.

[65] Voir Buzzfeed News, *There's A Fight Brewing Between The NYPD And Silicon Valley's Palantir*, 28 juin 2018, disponible sur https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org