



Assemblée générale

Distr. générale
23 juillet 2021
Français
Original : anglais

Soixante-seizième session

Point 75 b) de l'ordre du jour provisoire*

**Promotion et protection des droits humains :
questions relatives aux droits humains, y compris
les divers moyens de mieux assurer l'exercice
effectif des droits humains et des libertés
fondamentales**

Droit à la vie privée

Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre à l'Assemblée générale le rapport établi par le Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci, en application de la résolution [28/16](#) du Conseil.

* [A/76/150](#).



Rapport du Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci

Résumé

Dans le présent rapport, le Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci, s'emploie à mieux faire connaître les divers moyens de gérer la pandémie au regard du droit à la vie privée. Cette étude, qui fait fond sur le rapport de 2020 du Rapporteur spécial à l'Assemblée générale (A/75/147), est plus aboutie que celle figurant dans ce document, dans la mesure où il existe à présent davantage d'éléments disponibles permettant d'analyser avec plus d'exactitude la pandémie de maladie à coronavirus 2019 (COVID-19). Le Rapporteur spécial, qui examine en particulier les effets de la lutte contre la COVID-19 sur la protection des données, la technologie et la surveillance, note que les mesures prises actuellement par les États pour juguler la propagation de la maladie continuent de porter atteinte à l'exercice du droit à la vie privée et à la personnalité, et à d'autres droits humains intimement liés entre eux. On trouvera dans le rapport des recommandations formulées à l'intention des États et des acteurs non étatiques, tendant à une meilleure prise en compte du droit à la vie privée et de la personnalité, à la préservation de l'accès des enfants à l'enseignement en ligne, à la protection du droit à la confidentialité de l'information et à l'application du principe de transparence et de critères mesurables.

I. Introduction

1. Bien que la pandémie de maladie à coronavirus 2019 (COVID-19) continue d'évoluer, un plus grand nombre de données sont à présent disponibles pour déterminer comment la gérer en prenant des mesures sanitaires efficaces tenant mieux compte du droit à la vie privée.
2. La question de savoir dans quelle mesure l'atteinte au droit à la vie privée résultant de la pandémie est légale, proportionnelle et nécessaire, soulevée dans le rapport de 2020 du Rapporteur spécial à l'Assemblée générale (A/75/147), vise à définir quelle est la meilleure démarche à adopter pour gérer l'actuelle pandémie et celles qui surviendront dans le futur. Elle demeure sans réponse faute de données précises pouvant être comparées, l'opacité dans ce domaine s'expliquant notamment par une mauvaise préparation des États à la pandémie et un manque de responsabilité effective des décideurs, associés à un contexte politique propre à chacun d'eux.
3. Quoiqu'il en soit, le présent rapport vise à mieux faire connaître les moyens de gérer la pandémie au regard du droit à la vie privée. Il repose en grande partie sur des consultations publiques axées sur la COVID-19, qui ont été organisées conjointement par le Rapporteur spécial, l'Assemblée mondiale pour la protection de la vie privée et l'Organisation de coopération et de développement économiques du 21 au 23 juin 2021¹, et sur d'autres travaux de recherche.

II. Vie privée, personnalité et maladie à coronavirus

4. De nombreuses mesures prises par les États pour juguler la propagation de la COVID-19 ont eu des effets négatifs sur l'exercice du droit à la vie privée et d'autres droits humains. Ces effets ont été amplifiés par des situations existantes d'inégalité structurelle, d'exclusion sociale et de privation. La crise sanitaire a révélé au grand jour l'interdépendance des États et du secteur des affaires, ainsi que les liens étroits unissant le genre, la race, l'ethnicité, le statut socioéconomique et les réalisations en matière de santé. Les mesures prises pour contrôler la propagation du virus ont entraîné une restriction des droits humains pour l'ensemble des citoyens mais ont eu des effets disproportionnés sur certains segments de la société².
5. Le Rapporteur spécial s'est employé à promouvoir le droit à la vie privée au sens large, c'est-à-dire au-delà du droit à la confidentialité de l'information³ et de la surveillance, en soulignant le caractère positif et favorable qu'il revêt concernant la dignité innée de la personne, sa contribution à l'exercice d'autres droits humains et son importance pour le développement de la personnalité de tout être humain. Cette vision relève d'une approche qui voit le droit à la vie privée non pas comme un droit humain hors de tout contexte mais en lien avec les autres droits, en particulier ceux sur lesquels il produit une action favorable ou qui ne pourraient s'exercer sans lui. Ainsi, le droit à la vie privée est un prérequis fondamental au droit à un développement sans entrave de la personnalité, qui est explicitement reconnu à l'article 22 de la Déclaration universelle des droits de l'homme de 1948 : « Toute personne... a droit... à obtenir la satisfaction des droits... indispensables à sa dignité

¹ La professeure Elizabeth M. Coombs, M. Ketan Modh et M. Halefom Abraha méritent une reconnaissance particulière pour leur aide dans l'élaboration et la révision du présent rapport.

² « Epidemics have gendered effects », Clare Wenham, professeure agrégée, enseignant la politique mondiale de la santé à la London School of Economics and Political Science, citée par Martha Henriques, 13 avril 2020. Voir à l'adresse suivante : www.bbc.com/future/article/20200409-why-covid-19-is-different-for-men-and-women.

³ Il n'est pas rare que ce terme soit utilisé à tort de manière interchangeable avec le terme qui désigne la sous-catégorie « confidentialité des données ».

et au libre développement de sa personnalité ». L'article 29 de la Déclaration protège également le droit de développer sa personnalité : « L'individu a des devoirs envers la communauté dans laquelle seule le libre et plein développement de sa personnalité est possible ». L'une des références les plus explicites au lien qui unit droit à la vie privée et droit à la personnalité qui puissent être trouvées dans le discours tenu à l'Organisation des Nations Unies depuis la publication de la Déclaration, figure dans la résolution 34/7 du Conseil des droits de l'homme sur le droit à la vie privée à l'ère du numérique, dans laquelle le Conseil se déclare conscient que le droit à la vie privée peut permettre l'exercice d'autres droits, contribuer au libre développement de la personnalité et de l'identité de chacun et faciliter la participation individuelle à la vie politique, économique, sociale et culturelle, et note avec préoccupation que les violations du droit à la vie privée et les atteintes à ce droit peuvent avoir des incidences sur la réalisation d'autres droits de l'homme, notamment le droit à la liberté d'expression et de ne pas être inquiété pour ses opinions et le droit à la liberté de réunion et d'association pacifiques. Afin que la lutte contre la COVID-19 soit menée à bien, il faut l'associer à des critères mesurables qui prennent en compte un certain nombre de droits inextricablement unis par des liens rendus de plus en plus complexes par certaines technologies, notamment l'Internet, la photographie et la téléphonie, dont la convergence ne peut mieux apparaître que dans l'utilisation du smartphone.

6. Comme il est souligné dans le document, le premier rapport du Rapporteur spécial sur la pandémie de COVID-19⁴, ne pouvait être, comme c'est le cas du présent document, qu'un rapport d'étape, et il s'est fondé uniquement sur des faits recueillis durant les quatre premiers mois de la pandémie. Il visait avant tout à définir quelles étaient les autorités compétentes et sur quelle base juridique les mesures sanitaires et le droit à la vie privée pouvaient reposer. Il n'a pas traité des effets de la pandémie sur tous les aspects de la vie privée ou des différents aspects que ces effets revêtaient selon les groupes sociaux, en particulier les personnes en situation de vulnérabilité ou marginalisées, des questions majeures qui reflètent l'état d'une société et de ses institutions publiques. Le fait d'intégrer d'une manière ou d'une autre tous les droits humains dans la gestion de pandémie renseigne sur cet état.

7. Le rapport de 2021 du Rapporteur spécial (A/HRC/46/37) a examiné la question des effets produits par la COVID-19 sur le respect de la vie privée des enfants. Environ 90 % d'entre eux ont été touchés par la fermeture des établissements scolaires. En 2020, le nombre d'applications éducatives téléchargées a augmenté de 90 % par rapport à la moyenne hebdomadaire enregistrée à la fin de 2019.

8. Le passage à l'éducation en ligne a accentué le déséquilibre des rapports de force entre les entreprises qui produisent des contenus pédagogiques numériques et les enfants, et entre les administrations et les enfants et leurs parents, plusieurs États ayant dérogé aux lois en vigueur sur la protection des données relatives aux enfants. Ailleurs, par exemple dans certains États australiens, le droit à la vie privée des enfants n'est pas protégé dans les écoles publiques, quand bien même des acteurs non gouvernementaux contrôlent régulièrement les dossiers éducatifs numériques des enfants. Ces dossiers contiennent, entre autres, les caractéristiques intellectuelles, l'orientation scolaire prévisible, les notes de participation, le temps de réaction, les pages lues et les vidéos visionnées.

9. On ne peut séparer la gestion de la pandémie de l'éducation, de même qu'on ne peut ignorer les liens existant entre éducation, respect de la vie privée et gestion de la pandémie. Lorsque la pandémie pousse l'éducation à être dispensée de plus en plus sous une forme numérique, les conséquences pour la vie privée, si elles ne sont pas

⁴ A/75/147.

toujours visibles, sont néanmoins considérables. C'est d'autant plus vrai que dans la plupart des pays, la scolarité est obligatoire dès le jeune âge et la majorité des enfants et des parents sont dans l'incapacité de remettre en cause les modalités de respect de la vie privée prévues par les entreprises produisant des contenus pédagogiques numériques ou refuser de fournir des données, cela en dépit de préoccupations légitimes. Ainsi, à la fin de 2020, une analyse de 496 applications éducatives utilisées dans 22 pays a révélé que nombre d'entre elles collectaient des éléments d'identification des appareils, 27 enregistraient les données de localisation et 79 des 123 applications testées manuellement communiquaient les données propres aux utilisateurs à des tiers, comme des partenaires publicitaires. Elle fournit des informations sur les risques liés à la sécurité des données. À titre d'exemple, entre le 24 août et le 24 septembre 2020, Microsoft a enregistré 5,7 millions d'incidents liés à des logiciels malveillants⁵ qui ont visé ses logiciels éducatifs.

10. De la même manière, les mesures prises pour enrayer la propagation du virus ont eu des conséquences involontaires, dont certaines concernent la protection du droit à la vie privée des personnes. Celle qui a consisté à fixer des jours durant lesquels les hommes et les femmes pouvaient alternativement sortir de leur domicile pour effectuer des tâches essentielles telles que se procurer des vivres ou consulter des services de soins⁶ a porté préjudice aux populations transgenres⁷. En mettant des restrictions à la liberté de circulation des personnes en fonction de leur genre, on accroît le risque pour les lesbiennes, gays, bisexuels, transgenres, queers et intersexes (LGBTQI) de voir leur genre révélé et d'être victimes d'atteintes lors des contrôles d'identité effectués par les forces de sécurité et la police. Depuis le début de la pandémie, de nombreux États ont également jugé « non essentiels » les soins vitaux prodigués en lien avec l'affirmation de genre.

11. L'intégrité physique et l'autonomie sont liées au droit à la vie privée. Le foyer est par nature le lieu de l'intimité mais être confiné dans un espace familial lors d'une pandémie peut poser un problème pour d'autres raisons. Lors des périodes de confinement, la violence familiale fondée sur le genre, exercée par les conjoints ou des membres de la famille, a augmenté⁸. Du fait de ces mesures, certains enfants ont couru un risque plus élevé de subir des violences physiques ou psychologiques dans leur foyer et n'ont eu que des possibilités limitées de contact avec certains adultes auxquels ils auraient pu confier ce qu'ils subissaient⁹.

12. Si les droits humains avaient fait l'objet d'évaluations avant et pendant la pandémie, les risques susmentionnés auraient été atténués ; ces évaluations constituent donc une composante essentielle de l'orientation générale qu'il faudra suivre à l'avenir.

⁵ Voir Quentin Palfrey *et al.*, « Privacy considerations as schools and parents expand utilization of Ed Tech apps during the COVID-19 pandemic », International Digital Accountability Council, 1^{er} septembre 2020. Disponible à l'adresse suivante : <https://digitalwatchdog.org/wp-content/uploads/2020/09/IDAC-Ed-Tech-Report-912020.pdf>.

⁶ Panama et le Pérou, entre autres. Voir à l'adresse suivante : www.reuters.com/article/us-health-cronavirus-peru-idUSKBN21K39N, avril 2020.

⁷ L'identité de genre relève de la vie privée, Voir Comité des droits de l'homme, *G. v. Australia*, (CCPR/C/119/D/2172/2012), par. 7.2 (2017).

⁸ Voir COVID-19 and increase in gender-based violence and discrimination against women, Joint call by the EDVAW Platform of independent United Nations and regional expert mechanisms on violence against women and women's rights on combating the pandemic of gender-based violence against women during the COVID-19 crisis, 20 juillet 2020. Disponible à l'adresse suivante : <https://rm.coe.int/edvaw-statement-covid-19-and-vaw-final/16809efd2c>.

⁹ A/HRC/46/19, par. 17.

III. Vie privée, autres droits humains et maladie à coronavirus

13. La pandémie a soulevé des questions relativement aux droits et à la place qu'ils occupent dans une démocratie. Dans 10 des 13 pays dans lesquels des enquêtes ont été conduites en 2020 et 2021, le sentiment de division sociale s'est considérablement accru depuis le début de la pandémie¹⁰. Ainsi, si les passeports vaccinaux visent à améliorer l'accès aux droits et à assouplir la restriction des déplacements, ils excluent ceux qui n'ont pas accès aux vaccins, ne peuvent pas être vaccinés pour des raisons médicales ou choisissent de ne pas l'être. À l'heure actuelle, la proportion cumulée de la population mondiale qui relève de ces catégories est très importante¹¹.

14. Partout dans le monde, les gens ont cédé à leur gouvernement des pans de leur vie privée et de leurs libertés pour juguler la maladie. Les mesures mises en place à l'échelle nationale ont nui à la liberté d'expression (57 pays) ; à la liberté de réunion (147 pays) ; au droit à la vie privée (60 pays)¹². La proportionnalité et la nécessité de ces atteintes auraient dû être évaluées depuis longtemps.

15. Les dispositifs de surveillance de la maladie restant en place voire étant étendus, les pouvoirs publics auront un accès accru aux données à caractère personnel relatives à la localisation, aux antécédents médicaux et à d'autres informations sensibles sur la vie et les moyens financiers de la population. Il semble que certains États soient réticents à renoncer à leurs nouveaux pouvoirs et aux outils de surveillance à grande échelle, une fois la crise sanitaire résorbée. En Chine, une application de suivi du coronavirus est en train d'être rendue pérenne dans certaines villes. Fait encore plus préoccupant, un nouveau système recourt à un logiciel pour imposer les quarantaines et il s'avère communiquer des données à caractère personnel à la police, ce qui représente un troublant précédent du contrôle social automatisé¹³. Ces risques seraient plus marqués en Asie, mais dans tous les pays, y compris dans les démocraties, les autorités peuvent exploiter des données à des fins politiques et causer ainsi la perte de droits humains¹⁴. Les mesures prises en urgence pour lutter contre la pandémie présentent des risques qui exigent une protection propre aux situations de crise¹⁵.

IV. Protection des données, technologie, surveillance et maladie à coronavirus

16. Les données liées à la COVID-19 sont des données relatives à la santé, qui constituent une catégorie de données à caractère personnel appelées à bénéficier à titre prioritaire de niveaux spéciaux de protection, comme le prévoient les législations internationales, régionales et nationales. Bien que des recommandations aient déjà été formulées en vue de l'instauration d'un cadre général de protection des données

¹⁰ Voir l'étude réalisée par Pew Research Center entre le 1^{er} février et le 26 mai 2021 sur un échantillon de 18 850 personnes vivant dans 17 économies avancées. Disponible en anglais à l'adresse suivante : www.pewresearch.org/fact-tank/2021/06/24/eu-seen-favorably-across-17-advanced-economies-but-views-vary-on-its-coronavirus-response/.

¹¹ Voir OCDE, « L'accès aux vaccins anti-COVID-19 dans un monde en crise : état des lieux et stratégies », Les réponses de l'OCDE face au coronavirus (COVID-19), 18 mars 2021.

¹² Voir International Center for Not-for-Profit Law, COVID-19 Civic Freedom Tracker. Disponible à l'adresse suivante : www.icnl.org/covid19tracker/?issue=5.

¹³ Paul Mozur, Raymond Zhong et Aaron Krolik, *In Coronavirus fight, China gives citizens a color code, with red flags*, The New York Times, 1^{er} mars 2020, mis à jour du 28 janvier 2021.

¹⁴ Voir Sofia Nazalya, « Human Rights Outlook 2020 », 30 septembre 2020.

¹⁵ Voir Graham Greenleaf, COVID-19: the available evidence...and a little bit of hindsight, 23 juin 2021.

relatives à la santé¹⁶ et que le Rapporteur spécial ait présenté un mémoire explicatif¹⁷ à l'Assemblée générale en octobre 2019, on estime que près de 75 % des États Membres de l'ONU sont bien en deçà des normes établies dans ces documents. Tous les éléments disponibles portent à croire que ces lacunes se sont creusées davantage sous l'effet de la pandémie de COVID-19.

17. Pour remédier efficacement aux crises sanitaires, la collecte et la gestion de données sensibles sont nécessaires mais requièrent de solides mesures de protection de la vie privée. Dans de nombreux cas, toutefois, les dispositifs propres à traiter les données strictement nécessaires à la réalisation des objectifs de santé fixés n'étaient pas en place et ne le sont toujours pas.

18. Dans un grand nombre de pays, les garanties de transparence en ce qui concerne le traitement des données et les mesures assurant réparation en cas d'atteinte à la confidentialité de ces données font défaut. Dans d'autres pays, les directives existantes en matière de protection des données n'ont pas été suivies ; ainsi, le certificat COVID numérique de l'Union européenne, proposé par la Commission européenne le 17 mars 2021, un an après le début de la pandémie en mars 2020, n'a pas été soumis à une étude d'impact : « compte tenu de l'urgence, la Commission n'a pas procédé à une analyse d'impact »¹⁸.

19. De telles défaillances nuisent à l'action de santé publique et à la confiance que la population place dans cette action. Ainsi, 60 % des Américains considèrent que si les pouvoirs publics mettaient en place un dispositif de suivi des personnes au moyen de leur téléphone portable, une telle mesure ne contribuerait guère à empêcher la propagation de la COVID-19¹⁹.

20. Les données étant au cœur des mesures de lutte contre la pandémie, la COVID-19 est aussi devenue, au fil du temps, une « crise des données ». Les données à caractère personnel et les données sanitaires qui sont traitées par les pouvoirs publics et les entreprises du secteur numérique soulèvent des questions quant à leur nécessité et à leur juste proportion, aux méthodes de leur collecte et aux garanties sécurité concernant leur utilisation première et secondaire²⁰. En ce qui concerne les lesbiennes, gays, bisexuels, transgenres, queers et intersexes²¹, le partage non consenti de leurs données sanitaires est particulièrement préoccupant. Près de la moitié des Australiens (48 %) se disent davantage préoccupés par la protection de leurs données de géolocalisation dans le contexte de la COVID-19 et les trois quarts d'entre eux (75 %) pensent que les entreprises et les autorités ne sont pas dispensées des obligations qui leur incombent en temps ordinaire au titre de la législation relative au respect de la vie privée²².

¹⁶ Voir à l'adresse suivante : www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.Pdf.

¹⁷ Voir à l'adresse suivante : www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf.

¹⁸ Voir partie 3 du mémoire explicatif relatif à la proposition de la Commission européenne. Disponible à l'adresse suivante : eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0130.

¹⁹ Voir l'enquête réalisée par Pew Research Center en avril 2020. Disponible en anglais à l'adresse suivante : www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/.

²⁰ *Ibid.*

²¹ A/HRC/40/63, par. 84 (2019).

²² Bureau du Commissariat australien à l'information (2020).

Technologie

21. Les technologies utilisées dans la gestion de la pandémie relèvent de quatre grands groupes :

- a) Outils de traçage des contacts et de distanciation physique reposant sur la localisation de proximité au moyen de Bluetooth ;
- b) Codes QR ou codes-barres utilisés pour avoir accès à certains lieux ;
- c) Accès aux données relatives à la géolocalisation par l'utilisation de l'historique contenu dans la station cellulaire ou par le Système mondial de localisation (GPS), en vue d'alerter les personnes susceptibles de se trouver à proximité d'autres personnes, dont le résultat du test de dépistage de la COVID-19 est positif ;
- d) Applications permettant l'inscription à la vaccination ou le téléchargement de certificats de vaccination.

22. Les données manquent pour ce qui est de juger de la précision de certaines technologies. Selon certaines indications, celles qui sont utilisées actuellement ne sont pas fiables. Par exemple, en Israël, la population a réussi à remettre en cause les mesures de quarantaine auxquelles elle était soumise au moyen de la triangulation téléphonique. Sur les 20 000 personnes ayant formé un recours contre leur prescription d'isolement, 54 % (soit 12 000 environ) ont obtenu gain de cause²³. Aux États-Unis d'Amérique, l'American Civil Liberties Union a indiqué que les données issues de la station cellulaire étaient imprécises²⁴.

23. Le suivi de proximité au moyen de l'application Bluetooth a également été jugé insuffisamment fiable. Selon une étude sur la mise en place d'un tel suivi dans les tramways, qui a été menée en Allemagne, en Italie et en Suisse, il est apparu que la fiabilité de la détection équivalait à un déclenchement aléatoire de notifications²⁵. La fiabilité est fonction de la force du signal, qui est elle-même soumise à des facteurs comme les différences entre les modèles/tailles de périphérique, les fluctuations liées à l'orientation des périphériques, l'absorption par le corps humain ou un contenant et la réflexion des ondes radio par les murs, les sols et le mobilier.

La surveillance de la pandémie grâce aux données

24. Le terme technique « surveillance » est utilisé dans les études épidémiologiques et en matière de contrôle de la propagation des maladies. Il peut également faire référence à des activités de sécurité liées, par exemple, à la collecte de renseignements ou à l'application de la loi. Que ce soit en matière de santé ou de sécurité, la surveillance doit être nécessaire et proportionnelle.

25. Par souci de protéger la santé de leur population, des pays utilisent la surveillance à des fins de suivi de la propagation de la maladie, en recourant aux dispositifs suivants :

²³ « Over 12,000 mistakenly quarantined by phone tracking, Health Ministry admits », *The Times of Israel*, 14 juillet 2020.

²⁴ Voir Jay Stanley et Jennifer Stisa Granick, « The limits of location tracking in an epidemic » (8 avril 2020).

²⁵ Voir Douglas J Leith et Stephen Farrell, « Measurement-Based Evaluation of Google/Apple Exposure Notification application programme interface for Proximity Detection in a Light-Rail Tram » (2020) PLOS One, vol. 15, e0239943.

- a) Recherche physique des contacts, comme à Malte²⁶ ;
- b) Utilisation de Bluetooth, du GPS, du suivi par base cellulaire et de codes QR ou codes-barres téléchargés sur les téléphones portables, ainsi que de la technologie mettable incorporée à des systèmes spécialement conçus pour être utilisés en période d'épidémie, comme c'est le cas en République de Corée ;
- c) Utilisation de bases cellulaires et d'autres sources de données obtenues par triangulation, créées à l'origine pour lutter contre le terrorisme de manière souterraine et réaffectées à la pandémie, comme en Israël ;
- d) Enregistrement obligatoire par codes-barres ou codes QR, comme en Australie²⁷ ;
- e) Passeports vaccinaux, par exemple le règlement relatif au certificat COVID numérique de l'UE, entré en vigueur le 1^{er} juillet 2021²⁸.

26. La collecte et le traitement des données issues de ces sources ont varié d'un pays à l'autre pour ce qui est du type de données, de leur lieu de stockage, des personnes y ayant accès et de l'autonomie de ceux dont les données à caractère personnel ont été recueillies. La plupart de ces données ont été le produit de mesures appliquées au moyen de technologies en même temps qu'elles ont contribué à leur élaboration. Le dispositif technologique conditionne pour une grande part les possibilités qui sont laissées aux citoyens de contrôler certains aspects de leur droit à la vie privée.

27. Les applications de traçage des contacts offrent selon le cas une approche centralisée ou décentralisée de la collecte de données, que ce soit en matière de recherche de contacts ou d'inscription à la vaccination. Les deux approches se distinguent essentiellement par le lieu où les données sont stockées et par la manière dont celles-ci sont traitées. Dans le cadre de l'approche centralisée, quel que soit l'endroit où les données utilisateur sont produites, elles sont stockées et traitées sur un serveur central administré par les autorités sanitaires ou sur les serveurs d'une entreprise choisie par les pouvoirs publics.

28. Dans le cas du traçage des contacts, les serveurs calculent le niveau de risque actualisé de tous les utilisateurs et déterminent les utilisateurs à contacter. Dans le cas de l'inscription à la vaccination, les serveurs renferment, à des fins administratives, les données relatives aux dates de vaccination prévues, aux types de vaccins et au statut de chaque individu.

29. Du point de vue des autorités, les systèmes centralisés permettent, entre autres utilisations, l'analyse des données collectées en vue d'appréhender l'évolution de la pandémie, de cerner les zones les plus gravement touchées et d'évaluer la couverture vaccinale. L'allocation des ressources sur la base des priorités ainsi établies s'en trouve facilitée.

30. L'Australie s'est dotée de deux systèmes centralisés : une application de proximité Bluetooth (COVIDSafe) et un programme de suivi par code QR, utilisé pour l'accès à certaines manifestations. L'application COVIDSafe est entrée en vigueur après promulgation d'une loi ad hoc assortie de garanties en matière de

²⁶ Jessica Arena, « What is contact tracing and how is Malta doing it? », *Times of Malta*, 23 mars 2020.

²⁷ Voir par exemple, Gouvernement de l'État d'Australie méridionale, « COVID Safe Check-In » (voir à l'adresse suivante : www.covid-19.sa.gov.au/business-and-events/covid-safe-check-in) et Gouvernement de l'État de Nouvelle-Galles du Sud, « Setting up electronic check-in and QR codes » (voir à l'adresse suivante : www.nsw.gov.au/covid-19/covid-safe/customer-record-keeping/setting-up-electronic-check-and-qr-codes).

²⁸ Certificat COVID numérique de l'UE. Voir à l'adresse suivante : https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_fr.

respect de la vie privée. Le programme recourant au code QR, en revanche, n'a pas été adossé à une législation spécifique et repose sur d'anciens règlements sanitaires ainsi que sur la loi relative au respect de la vie privée de 1988. Cette absence pose un problème car l'Australie est dépourvue de garanties constitutionnelles pour ce qui est du droit à la vie privée.

31. Forte de son expérience acquise lors de l'épidémie de la maladie du syndrome respiratoire du Moyen-Orient (MERS) en 2015, la République de Corée a mis au point une approche centralisée qui passe par l'utilisation des documents détenus par les établissements médicaux, les données générées par le système GPS, les opérations commerciales par carte bancaire et la télévision en circuit fermé²⁹. Cette approche a permis de déterminer les itinéraires des patients, le risque d'exposition pour les personnes de leur entourage, de classer les contacts selon le degré de proximité et de les soumettre, le cas échéant, à des mesures de quarantaine.

32. Par une décision administrative en date du 23 mars 2020, l'Argentine a également créé une base de données centralisée en vue de recueillir les données générées par l'application Cuidar³⁰. Facultative pour les personnes vivant en Argentine, cette application a été rendue obligatoire pour les voyageurs en provenance de l'étranger, les autorités nationales et provinciales ayant eu accès aux données générées par Bluetooth.

33. Les dispositifs centralisés, dont ceux existant en Australie, en Israël et en République de Corée, suscitent des inquiétudes quant à la protection et au stockage d'informations sensibles, dont des données sanitaires, dans de bonnes conditions de sécurité, et par le fait que ces bases de données centralisées seront très probablement réutilisées par les pouvoirs publics et les entreprises à d'autres fins de surveillance, y compris politiques et commerciales.

34. Les citoyens nourrissent de la méfiance à l'égard des autorités qui mettent en place de vastes bases de données à leurs dépens. Ainsi, la majorité des Australiens (60 %) acceptent de faire quelques concessions en matière de protection de la vie privée, aux fins de la lutte contre la COVID-19 et au nom d'un intérêt supérieur, mais à titre temporaire. Il n'en reste pas moins que plus de la moitié d'entre eux (54 %) sont à présent davantage préoccupés par la protection de leurs données à caractère personnel, dans le cadre de la gestion de la pandémie, 26 % se déclarant même très préoccupés³¹.

35. Les applications décentralisées permettent aux utilisateurs de mieux contrôler leurs données à caractère personnel, qui sont stockées sur leurs téléphones et non dans une base centrale de données accessible aux pouvoirs publics et à d'autres entités. Parmi les dispositifs décentralisés les plus répandus, on peut citer le système de notification d'exposition Google-Apple, une interface de programmation d'applications, au moyen duquel les alertes ne passent pas par une base centrale de données mais sont déclenchées automatiquement et localement sur les téléphones des utilisateurs.

36. Certains pays ont eu recours aux deux types de dispositifs, centralisé et décentralisé. Singapour a mis au point des dispositifs de traçage mettables équipés de

²⁹ Voir « Contact transmission of COVID-19 in South Korea: novel investigation techniques for tracing contacts » *Osong Public Health and Research Perspectives*, vol. 11, n° 1 (2020), p. 60 à 63.

³⁰ Voir à l'adresse suivante (en espagnol) : www.boletinoficial.gob.ar/detalleAviso/primera/227116/20200324.

³¹ Voir 2020 Australian Community Attitudes to Privacy Survey. Disponible à l'adresse suivante : www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/.

Bluetooth afin d'enregistrer tous les échanges avec les dispositifs similaires se trouvant à proximité, les données ainsi produites ayant été conservées durant 25 jours avant d'être détruites³². Cette approche a conduit au développement d'applications pour téléphones portables qui ont servi à la recherche des contacts, à l'application de mesures de quarantaine, au suivi des symptômes et à la fourniture d'informations sur la pandémie, 46 applications de ce type ayant été répertoriées en août 2020³³.

37. Au croisement de ces sujets liés aux dispositifs techniques se pose la question de savoir si les technologies adoptées sont obligatoires ou facultatives. Une application peut être considérée comme facultative si un utilisateur a la possibilité de décider de ne pas s'en servir en choisissant de :

- a) Ne pas installer du tout l'application ;
- b) Désactiver la fonction Bluetooth/GPS ;
- c) Utiliser l'application mais refuser de communiquer l'information de diagnostic positif.

38. Alors qu'au départ, les réactions à l'égard de l'utilisation volontaire des applications de traçage des contacts ont été positives tant en Israël qu'en Australie, les personnes les ayant utilisées représentent en fin de compte un faible pourcentage de la population. En Australie, où en vertu de la loi de 2020 intitulée *Privacy Amendment (Public Health Contact Information) (COVIDSafe Act)*, rendre obligatoire l'utilisation de l'application COVIDSafe constitue un délit³⁴, le public a initialement bien accepté le dispositif avec 70 % d'opinions favorables, et pourtant l'application ne fait quasiment plus d'adeptes à l'heure actuelle³⁵. Les administrations des États fédérés australiens semblent se fier davantage aux contrôles effectués à l'entrée de certains lieux, dont l'accès est conditionné par la présentation d'un code QR. La République de Corée offre l'exemple d'une initiative politique qui a consisté à imposer un dispositif de géolocalisation conçu dans le pays, certains attribuant les bons résultats obtenus dans la lutte contre la pandémie au fait que les mesures adoptées ont revêtu un caractère obligatoire³⁶.

39. Donner son consentement et avoir la possibilité de le retirer font partie intégrante du droit à la vie privée. Or cette dernière possibilité n'existe pas si les applications de traçage des contacts sont rendues obligatoires. L'adoption de mesures contraignantes fait également courir le risque de voir les pouvoirs publics et les entreprises faire une mauvaise utilisation des données collectées, que ce soit dans le cadre d'une « dérive de la surveillance » ou de leur réaffectation, sans aucune possibilité laissée aux personnes de retirer les leurs des bases où elles sont stockées.

³² Voir « TraceTogether, safer together ». Disponible à l'adresse suivante : www.tracetogether.gov.sg/.

³³ Voir Hanson John Leon Singh, Danielle Couch et Kevin Yap, « Mobile health apps that help with COVID-19 management: scoping review », *JMIR Nursing*, vol. 3, n° 1 (2020), e20596.

³⁴ Voir la section 94H de la loi aux termes de laquelle :

- 1) Est coupable de délit une personne qui en oblige une autre à :
 - a) télécharger l'application COVIDSafe sur un dispositif de communication ; ou
 - b) activer ladite application sur un dispositif de communication ; ou
 - c) consentir au téléchargement de données générées par l'application sur un dispositif de communication, à l'intention de l'entité chargée d'administrer la base nationale de données COVIDSafe (National COVIDSafe Data Store).

Peine encourue : emprisonnement d'une durée de cinq ans ou amende de 300 unités de pénalité, ou les deux.

³⁵ Paul M. Garrett et Simon J. Dennis, « Australia has all but abandoned the COVIDSafe app in favour of QR codes (so make sure you check in) », *The Conversation*, 1^{er} juin 2021.

³⁶ Voir Kyung Sin Park, « Korea's COVID-19 success and mandatory phone tracking » (opennet, 20 octobre 2020).

Une limite franchie ?

40. De nombreux pays se sont retrouvés peu préparés à faire face à un nombre croissant de cas d'infection et de décès. Un certain nombre d'entre eux ont ressenti le besoin impératif de trouver des solutions pour protéger la santé et la vie de leur population, en utilisant tous les moyens disponibles. Que ce soit sciemment ou non, dans certains pays, l'action des pouvoirs publics a franchi une limite en termes de droit des droits humains et a pris une forme qui ne sied pas aux sociétés démocratiques et n'est pas acceptable dans ce type de société.

41. Les moyens de surveillance disponibles à des fins sanitaires et à des fins de renseignement et de sécurité n'ont parfois plus été distingués les uns des autres, ce qui a effacé des frontières et des distinctions essentielles. Dans les cas d'adoption de solutions facultatives auxquelles la population a adhéré, le mode d'agir des États est révélateur de la manière dont le droit à la vie privée et l'autonomie des citoyens peuvent être contournés.

Israël

42. Le cas d'Israël, dont le Gouvernement a déclaré l'état d'urgence le 19 mars 2020 en vertu de l'Ordonnance de santé publique datant de 1940³⁷, illustre une tentative de contournement des droits. Le Ministère de la santé a mis en vigueur une application dénommée HaMagen, grâce à laquelle des informations sur les déplacements et la localisation de ses utilisateurs ont été collectées puis stockées dans la mémoire interne de leur téléphone portable ou, en fonction du choix de ceux-ci, envoyés au Ministère et mis à la disposition des employés, représentants et prestataires de services. Cette application est ainsi à la fois décentralisée et centralisée (à titre facultatif).

43. Parallèlement à cet aménagement, le Gouvernement israélien a autorisé l'Agence israélienne de sécurité à demander des données provenant de stations cellulaires à des prestataires de services téléphoniques, voire à les collecter sans le consentement des personnes impliquées. Lesdits prestataires ont été contraints de suivre les déplacements des personnes infectées en s'appuyant sur les données enregistrées dans leur téléphone, en vertu de deux décrets adoptés d'urgence coup sur coup à la mi-mars 2020, qui autorisaient la police à requérir ces données à des fins de localisation des malades et de contrôle aléatoire des personnes placées en quarantaine avec recherche rétroactive de leurs déplacements durant les 14 derniers jours³⁸. Cette méthode de surveillance a ensuite été invalidée par la Cour suprême israélienne en avril 2020, ce qui a obligé le Gouvernement à adopter une nouvelle loi visant à autoriser l'Agence à continuer ses activités de recherche sur une base légale acceptable. En juillet 2020, une loi temporaire portant autorisation de la mission confiée à l'Agence israélienne de sécurité a été promulguée.

44. Au début de 2021, un amendement temporaire à l'Ordonnance de santé publique de 1940 a autorisé le transfert des données à caractère personnel relatives à des personnes non vaccinées aux municipalités et aux fonctionnaires de l'éducation et des services sociaux. Au début de mars 2021, la Cour suprême du pays a interdit le recours à la loi susmentionnée à des fins de surveillance massive puis elle a suspendu l'application de l'amendement.

45. En outre, des informations indiquent que les données vaccinales ont été utilisées aux fins suivantes : vastes recherches menées sur la population sans consentement ; publication d'informations sur les voies de transmission du virus ; utilisation de

³⁷ Greenleaf, « COVID-19: the available evidence ... and a little bit of hindsight » (voir note 15).

³⁸ David M. Halbfinger, Isabel Kershner et Ronen Bergman, « To track Coronavirus, Israel moves to tap secret trove of cellphone data », *The New York Times*, 16 mars 2020.

drones dans le cadre du suivi des quarantaines à domicile ; recours à des sociétés spécialisées dans les données génétiques pour les tests de dépistage de la COVID-19 et divulgation d'un projet de loi relatif à la communication de données épidémiologiques à la police³⁹.

46. L'application décentralisée HaMagen mise en service par le Ministère de la santé, bien accueillie au départ, a permis de dépister 30 % des premiers cas de la maladie mais son utilisation s'est effondrée en raison d'une défiance du public à l'égard des garanties qu'elle offrait en matière de respect de la vie privée⁴⁰. Il apparaîtrait que l'action de traçage des contacts menée par l'Agence ait eu une utilité limitée en raison :

- a) de l'absence de données claires sur les avantages du programme, en termes absolus et comparatifs ;
- b) de la tendance observée à obtenir des résultats faussement positifs.

47. Le système utilisé en Israël est inspiré des technologies mises en œuvre dans la lutte antiterroriste et fait usage de celles-ci. Selon certaines sources, depuis la mi-mars 2020, l'Agence israélienne de sécurité aide le Gouvernement israélien à mener des enquêtes épidémiologiques en fournissant au Ministère de la Santé les itinéraires des personnes contaminées par le coronavirus et les listes de celles avec lesquelles elles ont été en contact étroit. Ces informations sont disponibles dans la base de données renfermant les métadonnées de communication de l'Agence. Depuis mars, le Gouvernement israélien a essayé de faire une plus grande place au contrôle parlementaire dans ses opérations de renseignement. Contrairement à la France, aux Pays-Bas et au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Israël n'est pas doté d'un organe d'experts indépendant régi par la loi, habilité à agir en tant qu'autorité de contrôle autonome en complément de la commission parlementaire ; de ce fait, la question de savoir si un service de renseignement a la capacité de procéder à un contrôle minutieux et efficace dans ce domaine demeure une préoccupation majeure. Environ un an après le déploiement de technologies porteuses de telles violations du droit à la vie privée aux fins de la lutte contre la pandémie, Israël a été définitivement condamné par la Cour suprême, le 1^{er} mars 2021, pour avoir franchi une limite et a été frappé de l'interdiction d'utiliser à grande échelle les téléphones portables pour rechercher les personnes contaminées par le coronavirus, la Cour ayant qualifié cette mesure d'infraction grave aux libertés civiles⁴¹. Le Rapporteur spécial note que selon certaines informations, ces actions menées par Israël ont également freiné le développement d'applications respectueuses de la vie privée et la conduite d'enquêtes épidémiologiques, et il considère que le recours à des moyens de lutte antiterroriste dans un contexte purement sanitaire est contraire au droit international des droits humains et établit un dangereux précédent.

République de Corée

48. Dans d'autres pays, comme la République de Corée, les autorités ont également imposé aux prestataires de services téléphoniques d'assurer le traçage des déplacements des personnes contaminées⁴². La surveillance s'est exercée au moyen

³⁹ Prof. Yuval Shany, Israel's response to the COVID-19 pandemic: Right to Privacy Aspects, Federmann Cyber Security Research Centre, Hebrew University of Jerusalem, « COVID-19: the available evidence...and a little bit of hindsight » (voir note 15).

⁴⁰ Voir, par exemple, Mitnick J, « How Israel's COVID contact tracing app rollout went wildly astray » (CIO, 7 novembre 2020).

⁴¹ Voir Maayan Lubell, *Israeli Supreme Court bans unlimited COVID-19 mobile phone tracking*. Disponible à l'adresse suivante : www.reuters.com/article/us-health-coronavirus-israel-surveillance-idUSKCN2AT279.

⁴² Voir Kyung Sin Park, « Korea's COVID-19 success and mandatory phone tracking » (voir note 36).

d'une application téléchargeable sur smartphone, rassemblant des technologies traditionnellement utilisées dans les domaines de la répression et de la lutte contre le terrorisme, et combinant plusieurs sources de données à caractère personnel pour dresser un tableau des déplacements d'une personne, notamment :

- a) Les opérations effectuées par carte de crédit ou carte de débit, qui donnent à voir où une personne a fait ses achats et pris un repas, et comment elle a utilisé le réseau des transports ;
- b) Les fichiers-journaux de localisation téléphonique obtenus auprès des opérateurs de téléphonie mobile – qui donnent une idée approximative du quartier dans lequel se trouve une personne lors de la connexion à différentes antennes-relais ;
- c) Les informations capturées par le vaste réseau des caméras de surveillance.

49. Il convient tout d'abord de préciser que dans la plupart des cas observés, les mesures intrusives au regard de la vie privée, qui ont été prises en République de Corée pour lutter contre la pandémie de COVID-19, avaient une base légale et étaient encadrées par la loi. Les questions qui n'ont pas encore reçu de réponse restent les mêmes : ces mesures étaient-elles/sont-elles nécessaires et ont-elles répondu/répondent-elles au principe de proportionnalité dans une société démocratique ?

50. Afin de répondre avec exactitude à cette question, il importe d'examiner en détail ce qui s'est réellement passé en République de Corée. Les technologies employées semblent à l'évidence avoir porté leurs fruits en permettant de trouver en un temps record le lieu de l'infection et la façon dont celle-ci s'était propagée.

51. Au moment où la COVID-19 commençait de se propager, le Gouvernement de la République de Corée a transformé la plateforme de données Smart City, en cours de développement, en un outil de suivi sanitaire. L'Agence de prévention et de lutte contre les maladies a mis au point un dispositif de soutien aux enquêtes épidémiologiques, une plateforme permettant aux autorités sanitaires de collecter et d'analyser rapidement des données aux fins du suivi des cas confirmés de COVID-19. Ce système a commencé d'être opérationnel le 26 mars 2020, soit juste deux mois après que le premier cas de COVID-19 a été confirmé dans le pays. Une fois un cas de COVID-19 confirmé, des enquêteurs habilités demandent à connaître chacune des données relatives à la localisation de la personne infectée, lesquelles sont versées dans les systèmes par les entités concernées, en application de la loi relative à la prévention et à la lutte contre les maladies infectieuses. Le système procède alors en temps réel à une analyse du suivi, laquelle, associée aux entretiens classiques menés par des chercheurs de sujets contacts, permet à la fois un traçage rapide des contacts et la détection de points chauds. Il a permis de suivre des personnes et d'enquêter en moins de 10 minutes pour confirmer des cas de COVID-19, alors qu'un jour ou plus était nécessaire auparavant. La confidentialité et la sécurité des données sont assurées par le fait que seuls les enquêteurs de l'Agence sont habilités légalement à accéder au système et chaque accès au système requiert de s'identifier pour des raisons de sécurité. Afin de réduire au maximum la collecte d'informations personnelles, la période maximale durant laquelle cette collecte s'effectue a été fixée à 14 jours, soit la période d'incubation de la maladie. Ce système est en outre temporaire, toutes les données à caractère personnel étant appelées à être détruites à la fin de la pandémie de COVID-19⁴³.

52. Le dispositif de soutien aux enquêtes épidémiologiques décrit ci-dessus a constitué la première des mesures reposant sur la technologie prises par le

⁴³ Voir Jiyeon Kim et Neil Richards « South Korea's COVID success stems from an earlier infectious disease failure », 29 janvier 2021. Disponible à l'adresse suivante : <https://slate.com/technology/2021/01/south-korea-mers-covid-united-states-democracy.html>.

Gouvernement. Par ailleurs, la République de Corée utilise une application téléchargeable sur smartphone pour contrôler le respect des mesures imposées aux personnes soumises à l'isolement ou en quarantaine, à celles ayant reçu confirmation qu'elles avaient contracté la COVID-19, à celles en contact étroit avec une personne dont la contamination a été confirmée et aux voyageurs internationaux. Depuis le début de la pandémie, la République de Corée n'a jamais fermé ses frontières à un seul voyageur étranger qui souhaitait entrer dans le pays. Le pays a choisi de mettre en place des modalités spéciales qui prévoient une quarantaine de 14 jours à l'entrée dans le pays et un test de dépistage de la COVID-19 gratuit, l'objectif étant d'empêcher la propagation de la maladie. L'application utilisée pour l'isolement volontaire (Self-Quarantine Safety Protection App) présente deux volets : l'un permet à la personne en quarantaine de communiquer des informations sur son état de santé (ses symptômes), l'autre permet à l'agent traitant de contrôler le respect des mesures d'isolement au moyen de données de localisation générées par GPS, avec le consentement de la personne concernée. Si l'activation de cette deuxième fonction est fortement recommandée, elle n'est pas obligatoire. Les personnes qui ne possèdent pas de smartphone ou celles qui souhaitent ne pas adhérer à cette solution peuvent être suivies par la méthode traditionnelle, à savoir recevoir des appels de l'agent traitant. Il n'en reste pas moins que l'application avait été adoptée par 91,8 % de la population au 1^{er} septembre, les citoyens de la République de Corée comme les voyageurs étant rassurés de savoir que les personnes risquant de propager la COVID-19 respectent les mesures d'isolement volontaire⁴⁴.

53. On trouvera dans le résumé ci-après quelques-unes des raisons pour lesquelles le Rapporteur spécial considère qu'un volume important de données collectées au nom de la lutte contre la pandémie de COVID-19 durant certaines périodes, en particulier entre janvier et juin 2020, ne revêt aucun caractère de nécessité ni de proportionnalité :

Le partage des données relatives au traçage des contacts (c'est-à-dire « où, quand et pour combien de temps ») aide les gens à déterminer par eux-mêmes s'ils ont pu se trouver en contact étroit avec des personnes dont l'infection par le virus a été confirmée. Néanmoins, la divulgation des données de localisation peut présenter des risques du fait de la possibilité d'en déduire quels sont les lieux fréquentés par une personne et ses comportements routiniers. Les risques d'atteinte à la vie privée dépendent pour beaucoup des habitudes de déplacement de cette personne, qui seront fonction de plusieurs facteurs régionaux et des mesures de politique générale (par exemple, type de résidence, services de proximité et prescriptions de distanciation physique). En outre, les résultats indiquent que parmi les données relatives au traçage des contacts divulgués en République de Corée, on trouve des informations superflues telles que des détails démographiques (âge, genre, nationalité), des indications sur les liens sociaux (par exemple, domicile des parents) et des informations concernant le lieu de travail (nom de l'entreprise). Le partage des données relatives à des personnes dont l'identité est déjà connue n'est pas forcément utile au traçage des contacts, qui vise à localiser des personnes non identifiées qui auraient pu côtoyer de près des personnes dont l'état d'infection a été confirmé. En d'autres termes, à des fins de traçage des contacts, il serait moins utile de divulguer les caractéristiques personnelles et les liens sociaux (famille ou connaissances). L'adresse détaillée du lieu de travail pourrait ne pas être mentionnée dans la mesure où le plus souvent, il est aisé d'entrer en contact avec les membres du personnel d'une entité au moyen de ses réseaux internes de communication. On pourrait faire une exception à cette règle lorsqu'on soupçonne la possible infection d'un groupe qui

⁴⁴ *Ibid.*

aurait lui-même contaminé d'autres personnes. De la même façon, il n'est pas nécessaire de révéler des informations détaillées se rapportant au voyage de personnes arrivant de l'étranger (non communiquées au titre des principaux résultats), telles que le numéro du vol, le but ou la durée du voyage⁴⁵.

54. Tout en condamnant ce qui précède, à savoir la collecte à première vue non nécessaire et disproportionnée de données à caractère personnel, le Rapporteur spécial appelle également l'attention sur le fait que le Gouvernement et les institutions de la République de Corée tentent de manière ininterrompue et systématique d'accroître la protection de la vie privée face aux mesures de lutte contre la COVID-19, comme le montrent, entre autres, les faits suivants :

a) En juin et octobre 2020, le Centre de prévention et de lutte contre les maladies a publié des directives visant à la non-divulgaration de l'âge, du sexe, de la nationalité, du lieu de travail des personnes contaminées, ou encore de l'historique de leur voyage ou de leur lieu de résidence ; malgré cela, certaines administrations locales continuent de communiquer des informations liées au voyage de ces personnes. Des préoccupations demeurent quant à la collecte et au traitement de données à caractère personnel sensibles, susceptibles de mettre au jour des éléments relevant de l'intimité, tels que l'orientation sexuelle d'une personne ou ses relations privées.

b) En mars 2021, à des fins de protection de la vie privée et dans le cadre des mesures visant à prévenir la propagation de la COVID-19, le Gouvernement de la République de Corée a demandé au public d'utiliser le numéro personnel codé à la place du numéro de téléphone, dans les restaurants, cafés et autres lieux où il est demandé de présenter un code QR d'accès. Durant le mois de février 2021, les autorités avaient mis en vigueur une nouvelle mesure de protection de la vie privée, qui permet l'utilisation de numéros privés codés lors de visites de certains lieux ; un numéro codé est composé de quatre chiffres et de deux lettres et ne peut servir à passer un appel téléphonique ou à envoyer un texto. Seules les autorités sont habilitées à le convertir en cas de besoin urgent de contacter le détenteur de ce numéro pour des raisons liées à la COVID-19.

55. Le Rapporteur spécial conclut que dans le cadre de l'action menée pour tenter de lutter contre la COVID-19, la République de Corée a pris un certain nombre de mesures portant atteinte au droit à la vie privée, qui, dans certains cas, n'étaient ni nécessaires ni proportionnelles. Toutefois, dans la plupart de ces cas, si ce n'est dans tous, le Gouvernement a pris conscience de son erreur et s'est efforcé de prendre des mesures correctives (voir exemples susmentionnés).

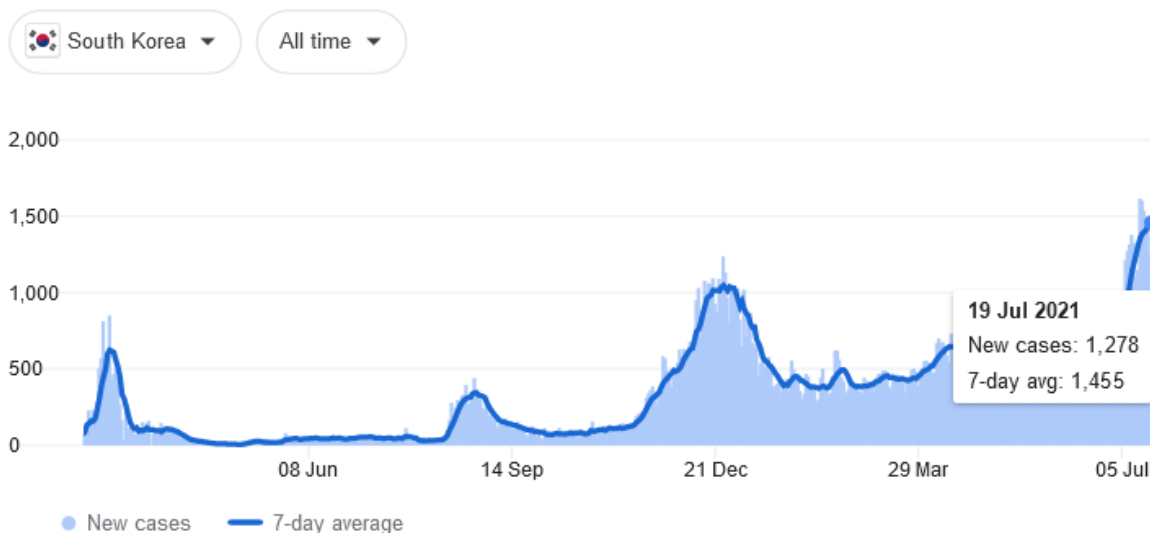
56. La figure ci-dessous montre l'évolution des trois vagues épidémiques survenues durant la pandémie de COVID-19 en République de Corée, de mars 2020 au 19 juillet 2021.

⁴⁵ Voir Gyuwon Jung *et al.*, « Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea », *Frontiers in Public Health*, 18 juin 2020. Disponible à l'adresse suivante : www.ncbi.nlm.nih.gov/pmc/articles/PMC7314957/ et www.frontiersin.org/articles/10.3389/fpubh.2020.00305/full.

Statistiques

New cases Deaths Vaccinations Tests

From JHU CSSE COVID-19 Data · Last updated: 1 day ago



Each day shows new cases reported since the previous day · [About this data](#)

Source : Université Johns Hopkins.

57. La figure montre que si le nombre de contaminations a considérablement baissé après la troisième vague survenue en janvier 2021, en mars et avril 2021, il était au même niveau que lors du pic atteint durant la première vague survenue en mars 2020, soit environ 530 nouveaux cas par jour. Au 19 juillet 2021, il avait atteint un niveau record avec quelque 1 300 nouvelles contaminations par jour. Au moment de la présentation du présent rapport (20 juillet 2021), on ne savait toujours pas expliquer précisément pourquoi un tel niveau avait été atteint en dépit de toutes les protections mises en place au détriment du droit à la vie privée. À ce stade, on ne peut que formuler des constatations préliminaires, les conclusions définitives nécessitant, pour être établies, qu'un plus grand nombre de données aient été traitées sur une plus longue période. On ne saurait donc se prononcer d'ores et déjà sur la question de savoir quelles mesures prises par le Gouvernement de la République de Corée pour lutter contre la pandémie de COVID-19 ont été nécessaires et proportionnelles. Il est donc difficile de mettre en évidence les bonnes pratiques, à supposer qu'elles existent, qui auraient pu gouverner la démarche officielle de protection de la vie privée dans le contexte de la pandémie, à l'exception de celles relatives à la limitation de la collecte des données à caractère personnel, mesure corrective introduite tout au long de 2020 et de 2021.

58. Au Nigéria, les mesures de confinement imposées dans tout le pays se sont accompagnées d'actions répressives et de violations des droits humains ayant entraîné la mort, les atteintes à la vie privée ayant probablement constitué les moins meurtriers des dommages majeurs causés par ailleurs. Outre les restrictions mises à la liberté de circulation, des informations ont fait état d'arrestations et de détentions arbitraires par les forces de sécurité nigérianes, qui auraient extorqué, saisi et confisqué des biens⁴⁶.

⁴⁶ Voir Simisola Akintoye, « Privacy implications of national responses to COVID 19 in Nigeria »,

59. Singapour illustre un cas de franchissement inutile d'une limite, donnant un exemple particulièrement spectaculaire du problème que représente la déviation progressive de fonction. Selon des informations parues dans les médias, l'adhésion populaire a considérablement faibli après que les autorités ont fait savoir, en janvier 2021, que la police avait utilisé les données générées par une application aux fins d'une enquête menée à propos d'un meurtre, alors que quelques mois plus tôt à peine, le ministre habilité avait fait le serment de n'utiliser de telles données qu'aux fins de la lutte contre la COVID-19. Fait rare, le Gouvernement a présenté des excuses. Pourtant, loin de faire marche arrière, il prévoit d'officialiser la capacité de la police d'accéder à de telles données dans des cas précis, et a déposé à cet effet un projet de loi devant le parlement⁴⁷. En vertu des nouvelles modifications de la loi relative à la COVID-19 (mesures temporaires) de 2020, votées par le Parlement de Singapour en février 2021, les données à caractère personnel collectées au moyen de programmes numériques de traçage des contacts durant la pandémie ne peuvent être utilisées qu'à cette fin, à moins qu'elles ne soient requises par les forces de l'ordre pour les besoins d'une enquête portant sur des délits graves⁴⁸.

Qui est responsable ?

60. En avril 2020, Google et Apple ont fait part d'efforts conjoints visant à aider les pouvoirs publics et les institutions sanitaires à contenir la propagation du virus à l'aide de la technologie Bluetooth. La solution a consisté à utiliser des interfaces de programmation d'applications et des technologies fonctionnant en système, permettant un plus grand respect de la vie privée de l'utilisateur grâce à une formule décentralisée⁴⁹. Avec la notification d'exposition, une initiative lancée par Google et Apple, les approches décentralisées du traçage numérique des contacts au moyen des téléphones portables sont devenues le mot d'ordre, étant donné la position dominante des deux entreprises sur le marché du smartphone. Cette technologie a été utilisée partout dans le monde, y compris en Australie, dans de nombreux États des États-Unis d'Amérique et dans la plupart des États membres de l'Union européenne. En juin 2020, le Gouvernement britannique a été contraint de changer radicalement d'orientation et de renoncer au mode de fonctionnement de l'application de traçage alors en vigueur dans le pays, pour passer à une formule reposant sur la technologie mise au point par Apple et Google.

61. En avril 2021, une mise à jour de l'application de traçage des contacts a été bloquée en Angleterre et au Pays de Galles car elle contrevenait aux dispositions de l'accord conclu avec Apple et Google⁵⁰. Cet accord, que toutes les autorités sanitaires avaient signé pour pouvoir utiliser la technologie de traçage des contacts respectueuse de la vie privée mise au point par les deux entreprises du numérique, stipulait que les données de localisation ne pouvaient pas être collectées au moyen de ce logiciel. Dans la mise à jour proposée, toutefois, il avait été demandé aux utilisateurs, dont le résultat

De Montfort University; Greenleaf, COVID-19: the available evidence...and a little bit of hindsight, 23 juin 2021 ; « Coronavirus: security forces kill more Nigerians than COVID-19 », BBC News, avril 2020.

⁴⁷ Voir Jamie Tarabay et Bloomberg, « Countries vowed to restrict use of COVID-19 data. For one Government, the temptation was too great », *Fortune*, 1^{er} février 2021.

⁴⁸ Voir Kirsten Han, COVID app triggers overdue debate on privacy in Singapore, *Al Jazeera*, 10 février 2021.

⁴⁹ Voir à l'adresse suivante: www.apple.com/mt/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

⁵⁰ Voir « Apple and Google block NHS Covid app update over privacy breaches », *The Guardian*, 20 avril 2021.

du test de dépistage du coronavirus était positif, de télécharger le fichier journal des lieux fréquentés (scans de codes-barres).

62. Ces incidents ont jeté une lumière crue sur le pouvoir que détiennent les entreprises du numérique. Indépendamment des aspects juridiques entrant ici en ligne de compte et des questions qui se posent quant à savoir lequel des protagonistes a adopté la position la plus respectueuse de la vie privée, un débat doit avoir lieu pour déterminer s'il est opportun que les pouvoirs publics soient dépendants du secteur privé pour fournir à leur population des outils de santé publique, et s'il est acceptable que ce secteur ait le pouvoir de dicter ses conditions dans de telles circonstances. De son côté, la France a prouvé qu'elle pouvait parfaitement se débrouiller seule en lançant, en juin 2020, une application qui avait été téléchargée par 25 % de la population française en mai 2021⁵¹.

V. Raccourcis et autres mécanismes relatifs à la pandémie

63. De nombreux pays n'étaient pas préparés à mettre en place des mesures sanitaires telles que la distanciation physique, la restriction des déplacements et le port du masque à bref délai. Des raccourcis ont été pris sous différentes formes et ont entraîné diverses conséquences.

64. Premièrement, on trouve, au nombre des mécanismes, la déclaration d'état d'urgence. À ce jour, 108 pays ont déclaré l'état d'urgence⁵² pour pouvoir, entre autres, lancer des actions imposant le traçage des contacts. Ainsi, l'Afrique du Sud a décrété l'état d'urgence en vertu de sa loi sur la gestion des catastrophes de 2002.

65. Deuxièmement, des règles ont été créées pour contourner la protection et la sécurité des données. En Autriche, en mars 2020, la loi sur la télématique sanitaire de 2012 a été modifiée pour permettre aux professionnels de la santé de transmettre des données sanitaires et génétiques par des moyens peu sûrs tels que le fax ou la messagerie électronique⁵³.

66. Troisièmement, de nouvelles lois ont été introduites. Le Danemark a adopté la loi relative à l'épidémie en mars 2020, ce qui a limité :

a) Le droit de réunion du fait de l'imposition de couvre-feux, de la restriction d'accès à certaines zones et de l'interdiction des regroupements et rassemblements de plus de 10 personnes du 18 mars au 8 juin 2020 ;

b) Le droit à la liberté individuelle du fait de l'hospitalisation, de l'isolement et de la vaccination obligatoires, et du fait de la détention de personnes sans confirmation de leur infection par le coronavirus ;

c) Le droit à la vie privée du fait de l'introduction d'applications numériques de traçage des contacts, assortie d'obligations faites aux personnes, aux entreprises et aux pouvoirs publics de fournir des données relatives à la COVID-19, et de solutions reposant sur les données à des fins de contrôle des déplacements, notamment ceux des citoyens.

67. La loi relative à l'épidémie a été amendée en février 2021 en vue de permettre l'introduction de processus et de mécanismes de contrôle parlementaires applicables

⁵¹ Voir Reuters, « French COVID tracing app downloaded by 25 per cent of the population – minister », 23 mai 2021.

⁵² Au 14 juillet 2021, International Center for Not-for-Profit Law. « COVID-19 Civic Freedom Tracker » (voir note 12).

⁵³ Voir à l'adresse suivante : www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120.

en cas d'adoption de règles et mesures intrusives ; pour accroître la transparence et réduire l'arbitraire du pouvoir ; pour limiter l'adoption de mesures contraignantes imposées aux personnes, par exemple en décrétant la vaccination facultative ; pour exercer un contrôle judiciaire sur les mesures contraignantes pouvant conduire à des peines de prison.

68. Quatrièmement, dans d'autres pays, les forces de l'ordre et des entités civiles ont été chargées de la mise en œuvre des règles sanitaires. À Malte, en avril 2021, en vertu de la loi sur la santé publique, le Commissaire à la santé a habilité les entités ci-après à faire appliquer les mesures relatives à la lutte contre la pandémie :

- a) La police et l'organisme chargé du dispositif d'application de la loi au niveau local ;
- b) Les forces armées de Malte ;
- c) Le réseau de transports *Transport Malta* ;
- d) L'Autorité maltaise du tourisme ;
- e) La Direction de la santé environnementale.

69. Les fonctionnaires appartenant à ces entités ont été autorisés à pénétrer dans les foyers pour y mener des inspections sur la base d'une information ou d'un soupçon donnant raisonnablement à penser que des réunions de personnes s'y tenaient en violation des règles en vigueur. Ces mesures dépourvues des garanties requises ont en outre mis à mal les principes de nécessité et de proportionnalité. D'ordinaire, un mandat judiciaire est nécessaire pour entrer dans le domicile d'un particulier, cet exemple mettant en lumière l'étendue considérable des pouvoirs exceptionnels conférés en matière sanitaire.

70. La nécessité de traiter de la question des rôles et responsabilités incombant aux secteurs respectifs de la santé et de l'application des lois se justifie également par le fait que dans certains pays comme le Royaume-Uni, les forces de l'ordre réclament d'être habilitées à pénétrer dans le domicile des personnes suspectées de ne pas respecter les règles de confinement, considérant que ce serait un bon moyen de faire appliquer les mesures correspondantes⁵⁴.

VI. Considérations diverses

71. La pandémie de COVID-19 suit son cours et le débat s'adaptera à son évolution. Actuellement, il s'agit d'examiner, entre autres, la position adoptée au regard des droits humains par l'Union européenne concernant le respect de la vie privée, par rapport notamment à la démarche de protection du consommateur qui est celle des États-Unis et, dans une certaine mesure, de l'Australie. Aux États-Unis, la Commission fédérale du commerce a récemment appelé l'attention sur le respect de la vie privée lors de la tenue de visioconférences et de l'utilisation de la technologie dans les domaines de la santé et de l'éducation, par des lettres d'avertissement et des alertes à l'escroquerie touchant au vol d'identité, à la suite de l'évolution vers le télétravail et l'enseignement en ligne⁵⁵.

72. Les précédentes crises sanitaires ont influencé la manière dont les pays ont géré la présente pandémie. Ainsi, si la République de Corée a rendu obligatoires les

⁵⁴ Voir « Police Chief calls for power of entry into homes of suspected lockdown breakers », Vikram Dodd, *The Guardian*, 5 janvier 2021.

⁵⁵ Voir Commission fédérale du commerce, « One year into COVID-19 pandemic, new Federal Trade Commission staff report highlights agency's ongoing efforts to protect consumers » (19 avril 2021).

mécanismes centralisés de traçage des contacts, c'est parce qu'une épidémie de la maladie provoquée par le coronavirus du MERS a frappé le pays en 2015. Se fondant sur son expérience, elle a revu sa loi sur la prévention des maladies infectieuses et la lutte contre elles afin d'empêcher la divulgation des variables liées au sexe, à l'âge, à l'éducation et à la nationalité, mais a établi l'obligation de révéler le statut sérologique.

73. La taille géographique d'un pays n'est pas sans influencer sur le caractère plus ou moins protecteur de certaines mesures au regard de la vie privée. Les pays les moins étendus ont été avantagés dans la gestion de certains aspects de la pandémie : ainsi, en dépit d'une forte densité de population, Singapour a été à même de remettre aux habitants de petites unités périphériques (*token*), un moyen qui est venu s'ajouter à l'application TraceTogether pour ceux qui n'avaient pas la possibilité d'utiliser cet outil numérique⁵⁶. Par ailleurs, dans des pays tels que l'Inde, à la fois vastes et densément peuplés, les autorités ont mis en place des moyens numériques d'inscription à la vaccination, en ligne ou sur téléphone portable via l'application CoWIN (reliée au numéro de téléphone de l'utilisateur), mais n'ont prévu aucun dispositif pour les personnes ne disposant ni d'un téléphone portable ni d'accès à Internet. La fourniture de petites unités périphériques (d'une autre solution ou d'un moyen anonyme d'inscription) aurait impliqué de les produire par millions mais ne pas l'avoir fait a été discriminatoire.

74. Avec d'autres régions et pays du monde, l'Afrique, l'Amérique latine, l'Australie et l'Inde sont connues pour n'être dotées ni de protections constitutionnelles ni de solides lois nationales de protection des données ni de mécanismes de contrôle, ce manque ayant nui aux efforts déployés par les pouvoirs publics pour faire en sorte que la population accorde sa confiance aux mesures de santé publique.

75. Dans d'autres régions du monde, le lancement d'initiatives concernant la recherche des contacts ou l'inscription à la vaccination est encadré par de solides lois nationales de protection de données, des autorités compétentes en la matière, puissantes et indépendantes, et d'autres organes de contrôle, ce qui permet de prendre dûment en compte la nécessité d'une telle protection et de sensibiliser la collectivité à cet égard.

76. De nombreuses mesures conduisent à la collecte d'un très grand nombre de données sensibles, l'une des difficultés consistant à juger du caractère proportionnel de cette collecte. Même les principales législations reconnues dans ce domaine, comme le Règlement général sur la protection des données de l'Union européenne, requièrent l'élaboration de nombreuses prescriptions techniques et orientations lorsqu'elles s'appliquent dans un contexte de santé publique.

77. De nouveaux systèmes se sont superposés à des infrastructures informatiques complexes qui leur préexistaient. Dans de nombreux pays, les autorités chargées de la protection des données se sont avérées incapables d'évaluer sur le plan technique ces systèmes, accompagnés de longs descriptifs très techniques, faute de disposer du temps, des ressources et des connaissances spécialisées voulus, comme l'a noté, en Autriche, le Datenschutzrat (Comité de protection des données) dans son analyse de l'initiative régionale⁵⁷.

78. En général, les stratégies mises en œuvre dans les pays du monde entier ont conduit inévitablement à suspendre les libertés et les droits humains fondamentaux. Dans le cadre des mesures d'urgence, des solutions ont pu être trouvées rapidement

⁵⁶ « Token Go Where ». Voir à l'adresse suivante : <https://token.gowhere.gov.sg/>.

⁵⁷ Voir à l'adresse suivante : www.bmj.gv.at/dam/jcr:c4b7569c-46c3-4772-bb07-9085f61412a8/Stellungnahme_des_Datenschutzrates_Epidemiegesetz.pdf.

mais n'ont pas été analysées sous tous leurs aspects. Les applications téléchargeables sur smartphone et les autres formes de surveillance auraient dû être légalement recevables, fiables sur le plan technique et faire l'objet d'un consensus social, de même qu'elles auraient dû être soumises à une évaluation au regard des droits humains, qui a brillé par son absence durant la période considérée.

79. La confiance publique conditionne l'efficacité des mesures de lutte contre la pandémie. Si cette confiance contribue à la réussite de toute initiative gouvernementale, elle est plus que jamais nécessaire dans des circonstances extraordinaires telles que celles créées par la pandémie de COVID-19. C'est particulièrement vrai pour les mesures dont l'efficacité repose sur la participation volontaire des citoyens.

80. Les mesures portant atteinte à la vie privée se sont heurtées à une résistance. Aux États-Unis, les outils de localisation et les systèmes centralisés ont été fermement rejetés ; en juillet 2021, seuls deux États avaient mis en place des passeports vaccinaux et nombre d'autres les avaient interdits⁵⁸. Les gens redoutent que les mesures prises durant la pandémie ne soient pas abrogées. À cet égard, la majorité des Australiens (60 %) disent accepter de faire quelques concessions en matière de protection de la vie privée aux fins de la lutte contre la COVID-19 et au nom d'un intérêt supérieur, mais à titre temporaire⁵⁹.

81. La technologie joue un rôle primordial dans la gestion des questions sanitaires par les pouvoirs publics. Son utilisation peut toutefois conduire à normaliser la surveillance après la pandémie. Ainsi, les applications de traçage des contacts prescrites par les autorités pourraient être utilisées pour accéder aux données à caractère personnel et servir d'outils de surveillance publique. La normalisation de technologies intrusives trace la voie vers d'autres mesures portant atteinte à la vie privée. Les entreprises, par exemple, ont étendu leur surveillance sur les employés sous le prétexte de mettre en place des applications et des unités périphériques de suivi des mesures de distanciation physique.

82. La réticence ou l'incapacité des pouvoirs publics à déterminer la proportionnalité et la nécessité des mesures adoptées peut être liée à la déviation progressive du rôle de la technologie et des données collectées ou bien à l'inefficacité de tels outils.

83. Jusqu'à présent, la pandémie a engendré des problèmes imprévus résultant d'une évolution vers des environnements de travail hybrides, dans lesquels les employés ont été collectivement contrôlés par les employeurs. Les mesures prises par ceux-ci pour mettre en œuvre la distanciation physique a porté atteinte à la vie privée des employés. Si de nombreuses entreprises ont suspendu leur activité, d'autres ont contourné le problème en demandant à leur personnel de porter des dispositifs d'alerte sur la proximité physique. Nombre d'entre elles manifestent à présent un intérêt à contrôler le travail à domicile par des logiciels permettant l'enregistrement de la frappe, de captures d'écran et d'autres activités résultant de l'utilisation d'un ordinateur. Ces technologies risquent d'induire une déviation de la surveillance, tandis que d'autres dévient de leur mission en ne stockant plus localement les données générées par les dispositifs de contrôle mettables mais en les versant, sans raison valable, dans une base centrale de données.

84. La pandémie de COVID-19 a mis au jour les lacunes que présentaient les lois de protection des données existantes pour ce qui est de prendre en compte ces risques émergents eu égard aux données à caractère personnel et à la vie privée. Le Règlement

⁵⁸ Voir Elliott Davis, « Which States Have Banned Vaccine Passports? », *US News*, 1^{er} juin 2021.

⁵⁹ Bureau du Commissariat australien à l'information.

général sur la protection des données, qui par ailleurs fixe le niveau d'exigence requis en termes de protection des données partout dans le monde, ne donne pas la possibilité de déposer des plaintes collectives car il traite avant tout des droits individuels⁶⁰.

VII. Conclusions

85. C'est dans les situations d'urgence que se révèlent les qualités véritables des États et des acteurs des secteurs public et privé, y compris de chaque individu.

86. Les traités internationaux et la plupart des constitutions nationales permettent aux États d'accroître leurs pouvoirs à titre temporaire pour faire face à une situation de crise telle que celle résultant de la pandémie de COVID-19. Celle-ci a imbriqué santé, surveillance et conséquences personnelles, et exige donc une gestion conforme aux paramètres fixés dans chacun de ces domaines.

87. Du point de vue du droit à la vie privée, la pandémie a permis aux pouvoirs publics et aux entreprises une plus grande intrusion dans la vie personnelle, ce qui a donné lieu à des violations de ce droit. Bien qu'on puisse s'attendre à ce qu'une pandémie entraîne certaines atteintes à des fins de protection de la santé publique, il s'est avéré impossible à ce jour de juger dans quelle mesure elles ont été nécessaires et proportionnelles.

88. Malheureusement, de nombreux États ont conçu la protection de la vie privée comme opposée aux mesures requises pour sauver des vies. C'est une vue simpliste qui ne tient pas compte de l'importance que revêtent aux yeux des personnes le respect de leur intimité et les limites mises aux incursions indésirables des pouvoirs publics et du secteur commercial dans leur vie, d'où la résistance aux efforts déployés par les autorités pour gérer la pandémie.

89. Partout dans le monde, des raccourcis ont été empruntés pour mettre en œuvre les stratégies nationales de santé publique. Certains gouvernements ont eu recours à des lois instaurant l'état d'urgence pour faire adopter des mesures de traçage des contacts à caractère contraignant ; d'autres ont profité de l'absence d'un solide cadre législatif de protection des données pour se hâter de mettre en place des mesures telles que le traçage des contacts et l'inscription à la vaccination sans tenir compte du droit à la vie privée et d'autres droits humains. Les réponses apportées à la crise, celles du type « impulsives », ont consisté, entre autres, à exploiter les lois d'urgence et les faiblesses de la législation relative à la protection des données voire son inexistence. Pour un certain nombre d'États et de gouvernements, le caractère imminent de consultations électorales a visiblement constitué et continue de représenter un facteur clé⁶¹.

90. Les États Membres ont utilisé des outils technologiques pour suivre les cas d'infection, faire appliquer les mesures de quarantaine, maintenir les règles de distanciation physique et contrôler l'administration des vaccins, ces outils ayant été mis au point par des organismes publics et des entreprises.

91. Dans ce contexte, les pays étaient mal préparés face aux entreprises du numérique qui ont exercé leur indépendance et leur pouvoir, ce qu'illustre l'attitude d'Apple et de Google à l'égard du respect de la vie privée des utilisateurs d'applications de traçage des contacts. Il importe de reconnaître en parallèle que ces deux entreprises ont adopté une démarche raisonnable en matière de protection de la

⁶⁰ Voir Andrew Pakes, « High Visibility and COVID-19: returning to the post-lockdown workplace » (Ada Lovelace Institute, 19 mai 2020).

⁶¹ Voir à l'adresse suivante : www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections.

vie privée, qui dans certains cas, a été plus raisonnable que celle des États désireux d'utiliser les données collectées.

92. La pandémie suivant son cours, il faut que les organes compétents continuent de suivre de près la promotion et la protection du droit à la vie privée et des droits connexes et communiquent des informations à ce sujet au public, à l'échelle internationale, régionale et nationale.

93. Les approches centralisées, dont celles adoptées en Australie, en Israël et en République de Corée, présentent des risques pour la vie privée, liés à la protection et au stockage d'informations sensibles, dont les données sanitaires, au fait qu'il est très probable que ces bases de données centralisées soient réutilisées par les pouvoirs publics et les entreprises, ainsi qu'à un haut niveau de rétention de ces données. Les applications décentralisées offrent à leurs utilisateurs plus de contrôle sur leurs données à caractère personnel dans la mesure où toutes les informations relatives à leurs contacts sont stockées dans leurs téléphones portables et qu'il n'existe pas de base centrale de données accessible aux pouvoirs publics ou aux autorités.

94. Les applications obligatoires de traçage des contacts ont des incidences évidentes sur le droit à la vie privée ; le consentement de l'utilisateur et la possibilité laissée à celui-ci de le retirer ont été légalement reconnus comme faisant partie intégrante de ce droit dans de nombreux cas mais pas dans tous. L'adoption de mesures contraignantes fait également courir le risque de voir les pouvoirs publics et les sociétés faire une mauvaise utilisation des données sensibles collectées aux fins de la lutte contre la pandémie, que ce soit dans le cadre d'une « déviation de la surveillance » ou d'une réutilisation de ces données sans aucune possibilité laissée aux personnes de les retirer des bases dans lesquelles elles sont stockées. Les applications facultatives de traçage des contacts ont pâti d'une faible adhésion, généralement due à un manque de confiance du public dans la capacité des autorités d'assurer la sécurité de leurs données et à les protéger.

95. La technologie pose de nombreux problèmes de mise en œuvre, notamment l'absence de données sur la fiabilité de certains systèmes. La plupart des mesures susmentionnées conduisent à la collecte d'un très grand nombre de données sensibles, l'une des difficultés consistant à juger du caractère proportionnel de cette collecte. La technologie joue certes un rôle essentiel dans la gestion de la pandémie mais elle pourrait induire une normalisation de la surveillance dans le futur. La surveillance technologique intensive et omniprésente est loin d'être la panacée en cas de pandémies telles que celle engendrée par la COVID-19.

96. Au nombre des problèmes connexes, on trouve l'égalité et la protection de la vie privée au travail. Les lois de protection des données, y compris le Règlement général sur la protection des données, présentent des lacunes. Il est nécessaire de mieux encadrer leur interprétation et la modification de leurs dispositions. Ces lois ne traitent généralement que des droits individuels et n'abordent pas les droits collectifs en matière de vie privée, qui prendront de l'importance au fur et à mesure des avancées de l'intelligence artificielle et de l'évolution vers un environnement de travail hybride.

97. Il est urgent de définir des principes communs relatifs à la confidentialité des données, qui pourront être appliqués à toute loi régissant la collecte de données dans le contexte de la pandémie. Ces principes communs normatifs devront être interopérables et utilisables dans les circonstances actuelles comme dans de futures occasions. Graham Greenleaf en a proposé une série, qui a été adaptée et axée sur une confidentialité programmée⁶².

⁶² Voir Greenleaf, « COVID-19: the available evidence ... and a little bit of hindsight » (voir note 15).

98. Il n'est pas de meilleur moment que le moment présent pour se préparer à faire face à une future pandémie⁶³. Les enseignements que l'on peut tirer ne concernent pas seulement la COVID-19 mais toute autre maladie à déclaration obligatoire ou pandémie qui pourrait survenir dans le futur.

VIII. Recommandations

99. Les recommandations ci-après visent à faire en sorte que chacun puisse exercer son droit à la vie privée au cours de l'actuelle pandémie et de futures crises sanitaires, sans immixtion arbitraire, comme stipulé dans la Déclaration universelle des droits de l'homme (art. 12), le Pacte international relatif aux droits civils et politiques (art. 17) et les conclusions formulées par les organes conventionnels.

100. Les recommandations ci-après visent à la fois les États et les acteurs non étatiques.

Vie privée et personnalité

101. **Les États et les acteurs non étatiques devraient appliquer les Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, ainsi que les orientations connexes pour la prise en compte des questions de genre (A/HRC/17/31, annexe).**

102. **Adopter les recommandations du Rapporteur spécial sur le droit à la vie privée visant à protéger contre les atteintes à la vie privée fondées sur le genre (A/HRC/43/52, par. 33 et 34).**

103. **Encourager les partenariats avec la société civile et le secteur industriel en vue de l'élaboration conjointe de stratégies et de solutions technologiques.**

104. **Assurer la participation de groupes sociaux particulièrement exposés aux consultations portant sur les mesures sanitaires spécifiques.**

105. **Limiter les atteintes à la vie privée induites par la lutte contre la pandémie en menant du point de vue des droits humains et compte tenu des questions de genre, des études d'impact sur la vie privée, préalablement à l'adoption de toute mesure, stratégie ou loi.**

106. **Évaluer régulièrement l'efficacité des mesures prises afin d'inclure les personnes vulnérables et marginalisées dans les interventions et l'action de relèvement.**

Enfants

107. **Élaborer des plans d'action détaillés concernant l'éducation en ligne, sur la base de l'article 29 1) de la Convention relative aux droits de l'enfant et des directives du Conseil de l'Europe sur la protection des données à caractère personnel des enfants dans le contexte scolaire.**

108. **S'assurer de l'établissement et du maintien des cadres législatifs requis pour l'éducation en ligne.**

109. **Créer une infrastructure publique afin d'aménager des espaces éducatifs non commerciaux et sociaux.**

⁶³ Voir « The best time to prevent the next pandemic is now: countries join voices for better emergency preparedness » (OMS, 1^{er} octobre 2020).

110. Faire en sorte que les données à caractère personnel des enfants soient traitées équitablement et de manière fiable et sûre, sur la base d'un fondement juridique légitime, tel que le Règlement général sur la protection des données et la Convention 108+, et en recourant à des dispositifs de protection des données conformes aux bonnes pratiques.

Confidentialité de l'information

111. Intégrer les droits humains dans la conception, la création et la mise en service de stratégies technologiques de lutte contre la pandémie.

112. Mettre en place, pour tous les types de mesures sanitaires prises dans le contexte d'une pandémie, des protections législatives reposant sur des principes communs, assorties de directives prévues pour les situations particulières. Le Rapporteur spécial recommande d'utiliser les 11 principes communs⁶⁴ propres aux systèmes de surveillance sanitaire centralisés et décentralisés, de prendre des dispositions législatives relatives aux maladies transmissibles et de s'y référer pour évaluer les politiques de prévention des pandémies partout dans le monde :

a) Établir une confidentialité programmée ou une confidentialité par défaut dès le départ, en intégrant à l'élaboration des mesures sanitaires axées sur la lutte contre les pandémies et les épidémies une évaluation globale de la situation relative aux droits humains et à la protection des données⁶⁵ ;

b) Prendre en compte la question de la confidentialité dès le début de l'action de lutte contre une épidémie ou une pandémie. Il est évident que la pierre angulaire de toute stratégie nationale devrait être la définition des moyens de lutter contre une épidémie, une tâche qui devrait faire l'objet d'une réflexion approfondie des années à l'avance et être intégrée à l'évaluation globale de la situation relative aux droits humains susmentionnée ;

c) Prévoir des contrôles précis et détaillés dans la législation relative à la confidentialité des données d'une région ou d'un pays ;

d) Pourvoir au besoin de clarté et de fondement juridique plus efficacement que par des actes ou règlements délégués, et faire en sorte de rendre la juridiction plus uniforme ;

e) Garantir l'accès aux lieux, manifestations, établissements, à l'éducation, etc., de sorte à éviter la discrimination ;

f) Protéger à titre vital les groupes vulnérables qui subissent plus particulièrement les effets négatifs des mesures de surveillance de la pandémie ;

g) Réduire au minimum et définir les utilisations autorisées des données relatives à la COVID-19, afin que ces données ne soient pas utilisées à d'autres fins une fois collectées ;

h) Spécifier les finalités en s'inspirant des nombreuses lois de protection des données existantes ;

i) Réduire au minimum la collecte de données ;

j) Afin d'assurer la proportionnalité de la collecte des données, établir une démarche de gestion des risques généralement acceptée et faire en sorte de

⁶⁴ Disponibles en anglais à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875920.

⁶⁵ Voir Conseil de l'Europe, Des solutions numériques contre la pandémie de COVID-19 – le rapport du Conseil de l'Europe sur la protection des données en 2020. Disponible à l'adresse suivante : <https://www.coe.int/fr/web/data-protection/-/digital-solutions-to-fight-covid-19-council-of-europe-report-on-data-protection-2020>.

limiter les dommages causés par les atteintes à la confidentialité des données, les cyberincidents et la déviation progressive de fonction ;

k) Établir des dispositions anticoercition : l'obligation d'utiliser ou de donner une preuve d'utilisation devrait être évitée ou strictement définie et encadrée par la loi. Toute demande de présentation d'un certificat d'utilisation devrait être exclue par la qualification de délit au regard du droit d'une telle attitude. Il est nécessaire de faire appliquer la loi mais aussi d'offrir des recours ;

l) Empêcher la déviation de la surveillance : éviter de suivre l'exemple de Singapour qui, après avoir promis en 2020 de s'en tenir à la recherche des contacts, a repris sa parole en 2021, autorisant l'utilisation des données à des fins d'enquêtes judiciaires ;

m) Gagner la confiance du public pour favoriser la participation volontaire, qui est nécessaire à l'application de la plupart des mesures de prévention d'une pandémie. Il faut déclarer contraire à la loi le fait d'étendre ce dispositif en tant que mesure de surveillance à d'autres domaines comme les enquêtes judiciaires, pour permettre d'instaurer cette confiance ;

n) Élaborer et inscrire dans la loi un programme de destruction en continu de toutes les données collectées, dans un bref laps de temps après leur collecte, qui peut être soit la durée d'incubation soit toute autre période définie sur la base d'éléments scientifiques ;

o) Instaurer, inscrire dans la loi et faire strictement appliquer une clause d'extinction de l'ensemble du système et la vérification obligatoire, conduite de manière indépendante, de la clôture de tous les systèmes de données épidémiques. Établir un délai certain ou un examen indépendant concernant la nécessité de veiller à la mise hors de service des systèmes de surveillance de la pandémie, avec vérification par voie réglementaire que cette mise hors de service a bien eu lieu ;

p) Assurer la supervision des systèmes de surveillance, qui doit être exercée de l'extérieur et de manière indépendante, et la communication régulière d'informations par un organe indépendant chargé de la protection des données ;

q) Définir les conditions requises en matière de transparence en consultation avec des experts et la société civile. Il peut s'agir de publier le code de la source utilisé pour la mise en place des systèmes de surveillance (applications de traçage des contacts), de mener des études générales d'impact sur la protection des données, et de publier des données sur l'efficacité des techniques utilisées pour surveiller la pandémie ;

113. Un dialogue suivi avec les grandes entreprises du numérique devrait compléter des débats publics, officiels ou informels, sur les attributions qui sont les leurs en matière de protection de la confidentialité en temps de pandémie.

Transparence et critères mesurables

114. Les pouvoirs exceptionnels conférés dans le domaine sanitaire doivent être évalués du point de vue de leur nécessité et de leur proportionnalité. Dans le cadre de ces évaluations périodiques et systématiques :

a) Le Rapporteur spécial sur le droit à la vie privée, seul et avec d'autres titulaires de mandat, devrait réexaminer la situation concernant les maladies à déclaration obligatoire et les maladies transmissibles en s'attachant particulièrement à la COVID-19 mais sans s'y limiter, au minimum tous les 24 à 36 mois, de sorte à mettre en évidence les risques existants et émergents, et à appréhender les mesures de politique générale les plus efficaces et

respectueuses de la vie privée qui pourraient être mises en œuvre pour se préparer à la survenue d'une pandémie, dans le cadre d'une approche intégrée de la protection des droits humains ;

b) Si un État décide que la surveillance technologique est nécessaire à la lutte contre la pandémie de COVID-19, il doit faire la preuve à la fois de la nécessité et de la proportionnalité de cette mesure, et élaborer une loi prévoyant explicitement la mise en œuvre de mesures de surveillance, qui seront obligatoirement assorties de garanties clairement définies ;

c) Les États et les sociétés devraient intégrer les droits humains dans la conception, la création et la mise en service des stratégies technologiques de lutte contre la pandémie, en raison des incidences majeures du numérique sur une large gamme de droits, en particulier le droit à la vie privée⁶⁶ ;

d) Les États et les sociétés devraient adopter des formes technologiques axées sur l'utilisateur et respectueuses des droits permettant, comme dans le cas des passeports vaccinaux, de porter ses données sur soi et de les présenter sur demande ;

e) Les mesures de lutte contre la pandémie prises par les États doivent être soumises à un examen externe et la manière dont ceux-ci gèrent la pandémie devrait être évaluée, de même que les autres responsabilités qui leur incombent en matière de droits humains à l'échelle nationale, dans le cadre de leur examen périodique conduit au niveau du système des Nations Unies.

⁶⁶ Voir [A/HRC/46/19](#).