La société et les droits fondamentaux aux risques du numérique en temps de crise

Poullet, Yves

Published in:
État de droit, état d'exception et libertés publiques

Publication date:
2022

Document Version
le PDF de l'éditeur

La société et les droits fondamentaux aux risques du numérique en temps de crise – Plaidoyer pour un régime légal strict de l'état d'exception[1]

Yves Poullet

Professeur émérite à la Faculté de droit de l'Université de Namur
et coprésident de l'institut NADI
Professeur associé à l'Université catholique de Lille
Membre de l'Académie royale de Belgique

1. En 2012, Jacques Larrieu introduisait un ouvrage intitulé *Crise(s) et droit*[2] par une définition de la crise. Il y voyait un « désordre » provoquant « la désintégration des normes qui règlent ordinairement la société », qui peut faire naître un « droit de circonstance » considéré comme dangereux, mais qui peut être aussi à l'origine d'un « progrès du droit » dès lors qu'il invite les spécialistes à concevoir un « droit nouveau qui tire les leçons de la crise ».

Inspirés de cette conception de l'interaction entre un phénomène de crise et le droit, nous devons bien constater que le numérique est souvent une manière de répondre aux crises et que son utilisation au service de la lutte contre la pandémie est un facteur majeur de bouleversement du fonctionnement de notre droit, sans doute plus insidieux que conscient.

Sans doute, ce bouleversement du droit par le numérique n'est pas propre aux temps de crise. En effet, le numérique envahit nos vies. Instrument de libéra-

---

1 Le présent texte a été rédigé en septembre 2021. Il n'a pu tenir compte des développements plus récents sur le Covid Safe Ticket et le contrôle de la vaccination à l'appui duquel les ressources de la technologie ont été sollicitées.

2 J. Larrieu, « Avant-propos », *in* J. Larrieu (dir.), *Crise(s) et droit*, Institut fédératif de recherche « Mutation des normes juridiques », Université de Toulouse I, 2012, pp. 9-12. On ajoutera dans le même sens les réflexions des auteurs d'un dossier thématique de la revue *Droit et Société* consacré à la crise Covid-19, qui concluent que si « la crise nie le droit », elle ne nie pas pour autant « la réflexion qui lui est propre ». Ces auteurs, et nous y reviendrons, conçoivent la crise comme un « moment où se révèle qu'une activité humaine peut endommager gravement, voire anéantir les conditions de sa propre continuation » et où se jouent simultanément trois types de dynamiques sociales : les « dynamiques de fonctionnement régulier » ainsi mises en lumière, les « versions modifiées des dynamiques de fonctionnement régulier » qui altèrent les conditions de ce fonctionnement et les « dynamiques de réaction » visant à faire face à ces altérations (S. Abitboul, A. Alemanno, E. Barbara, J. Cattan, Chr. Coslin, M. Delmas-Marty, J.-G. Flandrois, L. Kövesi, H.W. Micklitz, H. de Vauplane, J. Ziegler, « Ce que 2020 a fait au droit », *Le Grand Continent*, 4 janvier 2021, https://legrandcontinent.eu/fr/2021/01/04/ce-que-2020-a-fait-au-droit/).

tion et de développement de nos capacités, il constitue également un redoutable outil de contrôle, de surveillance de chacun d'entre nous et de prévisibilité de nos comportements dans le chef tant de nos autorités publiques que d'entreprises privées, en particulier des plateformes de communication et d'information.

Le développement d'outils autorisant la collecte d'informations au cœur de nos activités (l'internet des objets) joint au développement d'outils de capacité quasi infinie de transmission, de stockage et de traitement de l'information permet d'améliorer chaque jour ce suivi et ce contrôle.

Récemment, s'est ajouté l'emploi d'algorithmes et de technologies fondées sur l'apprentissage automatique (*machine learning*) dans le traitement des données collectées ou accessibles par les acteurs, offreurs de services ou de biens, présents sur la toile : classement et exploitation de l'information, reconnaissance faciale et profilage, etc.

Toutes ces transformations de notre rapport aux autres, des interactions possibles entre acteurs, bouleversent notre société et méritent que le droit les prenne en compte sous peine d'une perte de maîtrise de la puissance de cet objet technologique mis au service de certains. Ce qui sans doute est propre aux temps de crise, c'est que l'utilisation de l'outil trouve à l'occasion de ces périodes de troubles une légitimité qui fasse oublier au droit ses propres assises.

Faut-il pour autant renoncer à l'utilisation de tels outils efficaces ? Non, mais sans doute faut-il circonscrire par un régime juridique adapté à ces temps d'exception leur déploiement. Cette réflexion guide nos développements.

2. La réflexion croise deux domaines d'application. Le premier concerne les leçons prises à l'occasion de *la lutte contre la pandémie*[3]. Les mesures prises aujourd'hui ou envisagées pour demain, dans le cadre de la lutte contre cette pandémie ou d'autres, ont une portée restrictive des libertés, qui va plus loin que de simples limitations mais constituent une remise en cause de l'essence même de celles-ci.

Le numérique est omniprésent dans ces mesures : création de bases de données, qu'il s'agisse des personnes contaminées, vaccinées ou des soignants ; suivi des personnes, on songe ici aux systèmes mis en place dans nos téléphones mobiles chargés de détecter parmi notre entourage la présence ou non de personnes contaminées ; utilisation de systèmes d'intelligence artificielle tantôt pour la recherche, tantôt pour le repérage de *clusters*, tantôt pour la prévention ; utilisation de drones pour contrôler le respect des réglementations interdisant les déplacements, etc.

Pour ne reprendre qu'un exemple, le 12 janvier 2021, un simple arrêté de la ministre de l'Intérieur modifiait l'arrêté du 28 octobre 2020 qui organise les mesures d'urgence pour limiter la propagation du coronavirus Covid-19 pour confier à l'O.N.S.S. un pouvoir de profilage, de suivi et de surveillance de la population belge, et ce aux fins de faire respecter différents prescrits, par ailleurs insuffisamment précisés, de police administrative[4].

Le numérique, s'il fait l'objet de textes spécifiques, constitue surtout la condition même de l'effectivité des mesures réglementaires prises par nos gouvernants, et cette effectivité risque d'aboutir à la négation de certaines libertés.

Sans doute, ce qui est présenté abusivement comme la « guerre » à la Covid-19 peut justifier la prise de certaines décisions dans le cadre d'une « urgence » technologique justifiée elle-même par l'« urgence sanitaire », mais le souci du respect des libertés réclame qu'attention soit portée au respect de certains principes comme la proportionnalité, le contrôle démocratique et la limitation stricte dans le temps de cet état d'exception.

3. Le second domaine s'intéresse à l'utilisation du numérique dans la lutte contre la *criminalité*, et en particulier à l'utilisation par la police ou les services de renseignements des bases de données de communication que les opérateurs de communication seraient tenus de conserver. Sans doute, des outils en particulier s'appuyant sur l'intelligence artificielle sont désormais à la disposition des autorités policières et judiciaires : numérisation et impression 3D de scènes de crime, prédictions morphologiques, anticipation d'actes criminels, reconnaissance faciale, utilisation de drones…

Au-delà, les preuves numériques constituent désormais un instrument majeur de la solution d'un nombre croissant d'infractions. On citera ainsi la disposition de l'article 706-102-1 du Code de procédure pénale français[5] qui prévoit le

[3] Nous renvoyons à ce propos à nos études déjà publiées : Y. Poullet, « Pandémie, numérique et droits de l'homme – Un étrange cocktail », *J.D.E.*, 2020/6, n° 270, pp. 246-263 ; S. Parsa et Y. Poullet, « Les droits fondamentaux à l'épreuve du confinement et du déconfinement », *in* S. Parsa et M. Uyttendaele (coord.), *La pandémie de Covid-19 face au droit*, Limal, Anthemis, 2020, pp. 137 et s. ; Y. Poullet, « Covid et libertés – Quelques considérations », *in* D. Doat et Y. Poullet (dir.), *Actes du colloque organisé par l'UCLille du 4 février 2021 – Labo ETHICS – UCLille*, Paris, L'Harmattan, à paraître.

[4] L'article 8 de l'arrêté du 12 janvier autorisait en effet l'O.N.S.S. à utiliser la puissance de ses logiciels de *data mining* et de *data matching* – aptes à « collecter, combiner et traiter » toutes bases de données utiles (données de santé, de contact, d'identification, de travail et de résidence) sans que les finalités de ces traitements soient clairement identifiées par l'arrêté, comme l'avis de l'Autorité de protection des données (A.P.D.) du 3 février 2021, soit postérieurement à la publication de l'arrêté, le démontrait, ni que la proportionnalité de l'ingérence créée par cette mesure soit justifiée. L'arrêté a fait l'objet d'un recours en annulation devant le Conseil d'État, recours mené par l'A.P.D. et la Ligue belge des droits de l'homme.

[5] Le Code de procédure pénale français, par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (n° 2011-267, *J.O.*, 15 mars 2011), prévoyait déjà cette possibilité d'accès aux preuves numériques. La loi du 13 novembre 2014 (n° 2014-1353, *J.O.*, 14 novembre 2014) tendant à œuvrer au renforcement des dispositions relatives à la lutte contre le terrorisme a singulièrement élargi ce recours et une loi du 3 juin 2016 (n° 2016-731, *J.O.*, 4 juin 2016) a encore étendu ces possibilités d'accès en temps réel et à distance à l'ensemble des enquêtes de flagrance ou préliminaires pour les affaires de criminalité et de délinquances organisées sur autorisation du Juge des libertés et de la détention et sur requête du Procureur de la République. Un décret de 2019 (n° 2019-1602, *J.O.*, 31 décembre 2019) précise les contours de cette captation des preuves numériques. Ces textes ont fait

recours « à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques ».

L'utilisation des systèmes de *machine learning* (intelligence artificielle, I.A.) représente une opportunité indéniable pour les autorités policières[6]. Les capacités de traitement des ordinateurs permettent, face à des données de plus en plus nombreuses et collectées de manière de plus en plus ubiquitaire, de faciliter tant les tâches de prévention que de détection des infractions et de leurs auteurs. Prenons quelques exemples : détecter des messages racistes sur le Net ; analyser grâce à des systèmes d'analyse émotionnelle les réactions de suspects ou, grâce à la reconnaissance faciale, reconnaître dans la foule un criminel ou une personne suspectée de terrorisme ; grâce au croisement de données socio-économiques multiples, y compris de consommation, de mobilité, de dépenses, retrouver un criminel ou prédire la dangerosité d'une personne ; calculer la dangerosité future de personnes reconnues coupables[7]…

L'I.A. est considérée comme un gage d'optimisation ; elle l'est également en ce qui concerne l'objectivation des décisions prises. Optimisation dans la mesure où les capacités de la machine de traiter les informations sont sans commune mesure avec celles du cerveau humain. Objectivation dans la mesure où l'utilisateur est invité à se fier aux résultats des opérations d'intelligence artificielle, fruits d'une statistique apparemment neutre appliquée à des faits soi-disant objectifs, *data do not lie*. Ainsi, l'apparence d'objectivité rend difficile la contestation de ce qui apparaît être la vérité sortie des ordinateurs.

l'objet de sévères critiques de la C.N.I.L. dans ces délibérations (voy. en particulier l'avis du 26 septembre 2019). On note que l'Union européenne est sur le point d'adopter un règlement « relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale », qui a pour objectif d'adapter les mécanismes de coopération entre États membres au monde numérique en fournissant les outils judiciaires et répressifs nécessaires pour tenir compte des modes de communication actuels des criminels et pour simplifier l'obtention et la collecte, dans le cadre de procédures pénales, des preuves électroniques stockées ou détenues par des fournisseurs de services relevant d'un autre État (Proposition de règlement, COM(2018) 225 final, 17 avril 2018).

6 Ainsi, le Conseil d'État, dans la décision du 21 avril 2021 sur laquelle nous reviendrons (*infra*, n° 8), relève à la suite des arguments du gouvernement : « l'obligation pour le juge d'écarter les dispositions du droit national imposant une conservation généralisée et indifférenciée des données de connexion pour des finalités autres que de sauvegarde de la sécurité nationale priverait de garanties effectives les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment des atteintes à la sécurité des personnes et des biens, et de recherche des auteurs d'infractions pénales ».

7 Dans l'affaire *E. Loomis* (*State v. Loomis*, 881 N.W.2d 749 (Wis. 2016)), les tribunaux américains ont utilisé, lors de la détermination de la peine, un algorithme secret qui donnait une estimation d'une probabilité de récidive du prévenu. L'utilisation de cet algorithme a été très critiquée. Il s'agit plus précisément d'un logiciel d'intelligence artificielle nommé COMPAS proposé par la société Northpointe.

4. À propos de l'utilisation de la technologie dans la lutte contre la criminalité, y compris le terrorisme, nous nous limiterons comme annoncé (*supra*, n° 3) à un seul point, dans la mesure où il rejoint notre propos consacré selon le titre même de la contribution aux risques, encourus par nos libertés, liés à l'utilisation de la technologie dans le cadre de régime dit d'exception technologique, l'état d'exception et les libertés.

On connaît la possibilité pour les États de faire obligation aux opérateurs de communication de conserver les données de communication (mais non leur contenu) et, dès lors, de permettre aux autorités policières et judiciaires de même qu'aux services de renseignements d'accéder à de telles données. De telles prérogatives se justifient par l'article 15 de la directive ePrivacy[8].

Ce sont les contours de cette possibilité qui ont fait l'objet d'une décision récente de la Cour de justice de l'Union européenne (C.J.U.E.). Cette décision européenne, même si elle a été interprétée en sens divers tant par notre Cour constitutionnelle que par le Conseil d'État français, introduit l'idée que seul un état d'exception, par ailleurs défini strictement, peut justifier l'utilisation du recours à l'obligation de conservation par les opérateurs de communication des dérogations aux libertés, et ce au-delà des simples limitations qui, en temps normal, sont prévues par l'article 52 de la Charte des droits fondamentaux de l'Union européenne.

5. Que ce soit à propos de la pandémie ou de la recherche des auteurs d'infractions ou d'agents terroristes, demain de la lutte contre le réchauffement climatique ou d'une catastrophe naturelle, il est clair que l'appel aux ressources du numérique et aux développements d'applications toujours plus performantes constitue une tentation forte pour nos gouvernants, et ce dans l'idée d'une pleine efficacité des normes que requièrent les situations. La C.N.I.L.[9] parle à cet égard de « solutionnisme technologique »[10], c'est-à-dire le recours

8 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L 201, 31 juillet 2002, pp. 0037-0047. Cette directive a été revue à plusieurs reprises et fait l'objet actuellement de débats à l'occasion de sa transformation en règlement européen.

9 « Dans son avis, la C.N.I.L. rappelle que l'utilisation d'applications de recherche des contacts doit s'inscrire dans une stratégie sanitaire globale et appelle, sur ce point, à une vigilance particulière contre la tentation du "solutionnisme technologique". Elle souligne que son efficacité dépendra, notamment, de sa disponibilité dans les magasins d'application (*appstore*, *playstore*…), d'une large adoption par le public et d'un paramétrage adéquat » (C.N.I.L., « Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée "StopCovid" », www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid).

10 « Courant de pensée originaire de la Silicon Valley qui souligne la capacité des nouvelles technologies à résoudre les grands problèmes du monde, comme la maladie, la pollution, la faim ou la criminalité. Le solutionnisme est une idéologie portée par les grands groupes internet américains qui façonnent l'univers numérique. Lors de l'édition 2008 du festival South by Southwest, Mark Zuckerberg, fondateur de Facebook, déclarait : "Le monde étant confronté à de nombreux enjeux majeurs, ce que nous tentons de mettre en place en tant qu'entreprise, c'est une infrastructure sur laquelle s'appuyer pour en dénouer

facile à l'outil technologique pour répondre au défi posé par l'urgence des situations avec la croyance que ce recours permettra de résoudre le problème.

Par ailleurs, on ne s'étonnera pas du rapprochement de ces deux domaines : les mêmes technologies de surveillance et de contrôle ne sont-elles pas à l'œuvre dans les deux cas[11] et le raisonnement sur le privilège à accorder à l'utilisation à de telles technologies ne s'explique-t-elle pas par un raisonnement semblable, à savoir : vu l'état d'urgence et la gravité des situations, l'efficacité sans pareil de telles technologies doit être mise au service de la priorité donnée, sur les libertés individuelles, au droit à la santé, d'une part, au droit à la sécurité publique, d'autre part ?

L'objectif est donc à travers ces deux domaines de réfléchir aux limites qui pourraient être imposées à l'utilisation du numérique, aux hypothèses où ces limites pourraient être dépassées, de même qu'aux conditions de ce dépassement.

La proposition actuellement étudiée par notre Parlement est certes un premier pas dans cette direction. Au-delà, l'article 15 de la Convention européenne des droits de l'homme (ci-après, « C.E.D.H. ») constitue un guide précieux pour l'affirmation d'un cadre plus strict mais également plus général balisant cet état d'exception afin que les urgences qui fondent un tel état ne soient prétextes à la montée d'un état autoritaire.

Cette crainte d'une technologie vectrice d'un état, voire d'une société autoritaire, inspire certains prescrits de textes européens récents, en particulier la proposition de règlement sur l'intelligence artificielle. Elle introduit dans cette perspective des limites heureuses, voire des interdictions, aux développements de certaines applications de cette technologie nouvelle.

Les potentialités de l'outil numérique justifient pleinement l'angoisse des juges, des autorités de protection des données et des associations de libertés civiles face à ce qui peut être demain un outil banal aux mains des gouvernants, voire,

un certain nombre." Dans le même esprit, Eric Schmidt, président exécutif de Google, annonçait lors d'une conférence en 2012 : "Si nous nous y prenons bien, je pense que nous pouvons réparer tous les problèmes de monde." » (Fr. Laugée, « Solutionnisme », *La revue européenne des médias et du numérique*, 2014, n° 33, https://la-rem.eu/2015/04/solutionnisme/).

11 Dans le *Cahier de prospective* récemment publié par l'IWEPS et rédigé par Vincent Calay, l'auteur relève différentes technologies utilisées dans un premier temps pour la prévention du terrorisme et désormais employées dans le cadre de la lutte contre la pandémie : « Par exemple, le chien robot *Spot* conçu par Boston Dynamics pour évaluer à distance des situations à risque, notamment liées au terrorisme (comme la présence d'explosifs), a été introduit dans un parc de Singapour pour surveiller le respect, par les usagers du parc, des règles de distanciation sociale : par ses capteurs et caméras, le robot analyse le niveau de fréquentation du parc et diffuse, par haut-parleur, des messages rappelant les règles de distanciation sociale. » (V. Calay, « L'empire des logiciels, menace pour les démocraties ? », *Cahier de prospective de l'IWEPS*, juillet 2021, n° 5, p. 18.) Il renvoie également à l'ouvrage d'O. Tesquet, *État d'urgence technologique. Comment l'économie de la surveillance tire parti de la pandémie*, Paris, Premier Parallèle, 2021, pp. 48-52.

pire encore, de certaines entreprises privées au service d'un intérêt général mal compris ou d'intérêts privés. Tel est le fil rouge de notre réflexion.

6. Notre propos part donc de l'examen de *l'arrêt de la C.J.U.E. relatif à l'accès des autorités policières et judiciaires aux données de communication du 6 octobre 2020*, et ce dans le cadre de l'application de l'article 15 de la directive ePrivacy. Cette décision introduit la notion d'état d'exception comme fondement de la levée de certaines interdictions ou plutôt de l'élargissement de l'accès aux données par une obligation des opérateurs de communication de conserver les données dites de communication[12].

Le deuxième point étudie *l'article 15 de la Convention du Conseil de l'Europe* dont l'application a été recommandée aux États membres, à l'occasion de leur lutte contre la pandémie, et confronte la loi belge votée ce 15 juillet 2021 aux exigences de cet article.

Le troisième point élargit le propos, en s'appuyant sur *l'importance de limiter l'utilisation du numérique en dehors de cet état d'exception*, voire y compris de manière plus radicale encore.

Nos conclusions appellent nos législateurs à agir afin d'assurer une maîtrise collective et démocratique du développement d'un numérique au service des libertés, sans négliger l'intérêt général.

I. La décision européenne de la Cour de justice de Luxembourg du 6 octobre 2020 à propos de l'obligation de conservation généralisée des données de communication

7. Cette décision s'inscrit dans la droite ligne de décisions précédentes[13], qui, déjà, condamnaient l'obligation de conservation des données mise à charge

12 Le champ d'application des textes législatifs pris sur base de cet article 15 ne couvre que les fournisseurs de services traditionnels de communications électroniques au sens de la directive établissant le code européen des communications électroniques. Or, les particuliers et entreprises recourent de plus en plus, pour leurs communications interpersonnelles, à de nouveaux services sur l'internet, comme la voix sur IP, la messagerie instantanée et le courrier électronique web, en lieu et place des services de communication traditionnels. Ces services, ainsi que les réseaux sociaux tels Twitter et Facebook, sur lesquels les utilisateurs partagent du contenu, devraient donc aussi être couverts par le futur règlement ePrivacy.

13 Arrêt du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C-594/12, EU:C:2014:238 ; arrêt du 21 décembre 2016, *Tele2 Sverige*, C-203/15 et C-698/15, EU:C:2016:970 ; arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788. Le communiqué de presse paru à la suite de l'arrêt du 6 octobre 2020 confirme cette cohérence jurisprudentielle : « Ainsi, dans l'arrêt du 8 avril 2014, Digital Rights Ireland e.a (C-293/12 et C-594/12, EU:C:2014:238) (voir CP n° 54/14), la Cour a déclaré invalide la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public

systématiquement des opérateurs de communication par la directive de 2006[14] adoptée en son temps et annulée dès le premier des arrêts cités. Nonobstant cette annulation, certains législateurs avaient estimé pouvoir maintenir une obligation de conservation sur base de l'article 15 de la directive ePrivacy. L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, § 1er, de la directive ePrivacy, ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 du traité sur l'Union européenne ?

Cette obligation, pourtant légale au regard des ordres juridiques français et belge, est contestée. Les associations et sociétés requérantes, dont chez nous l'O.B.F.G., contestent en effet les dispositions réglementaires imposant aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenu de conserver de façon généralisée et indifférenciée, pour une durée d'un an, les données de trafic et de localisation de l'ensemble de leurs utilisateurs ainsi que leurs données d'identité civile et certaines données relatives à leurs comptes et aux paiements qu'ils effectuent en ligne.

Elles contestent également les dispositions réglementaires permettant aux services de renseignement de recueillir et d'opérer des traitements sur ces données.

ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54), au motif que l'ingérence dans les droits au respect de la vie privée et à la protection des données à caractère personnel, reconnus par la charte des droits fondamentaux de l'Union européenne [...], que comportait l'obligation générale de conservation des données relatives au trafic et à la localisation prévue par cette directive n'était pas limitée au strict nécessaire. Dans l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970) (voir CP n° 145/16), la Cour a ensuite interprété l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) [...]. Cet article habilite les États membres – pour des raisons de protection, entre autres, de la sécurité nationale – à adopter des "mesures législatives" afin de limiter la portée de certains droits et obligations prévus par la directive. Enfin, dans l'arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788) (voir CP n° 141/18), la Cour a interprété ce même article 15, paragraphe 1, dans une affaire qui concernait l'accès des autorités publiques aux données relatives à l'identité civile des utilisateurs des moyens de communications électroniques. »

14 Directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public et modifiant la directive 2002/58/CE. Cette directive a été annulée par l'arrêt *Digital Rights* du 8 avril 2014 déjà cité: « La directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, est invalide ».

La Cour de justice de Luxembourg tranche de la manière suivante :

> « En revanche, dans des situations dans lesquelles un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, celui-ci peut déroger à l'obligation d'assurer la confidentialité des données afférentes aux communications électroniques en imposant, par des mesures législatives, une conservation généralisée et indifférenciée de ces données pour une durée temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. S'agissant de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique, un État membre peut également prévoir la conservation ciblée desdites données ainsi que leur conservation rapide. Une telle ingérence dans les droits fondamentaux doit être assortie de garanties effectives et contrôlée par un juge ou une autorité administrative indépendante ».

Elle ajoute que l'injonction doit être proportionnée, prise pour une période temporellement limitée au strict nécessaire et faire l'objet d'un contrôle effectif, soit par une juridiction soit par une entité administrative indépendante dont la décision est dotée d'un effet contraignant, afin de vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties prévues. Ces conditions remplies, l'analyse automatisée des données, notamment celles relatives au trafic et à la localisation, de l'ensemble des utilisateurs de moyens de communications électroniques doit être permise.

8. On connaît la lecture différente de cette décision par les hautes juridictions française et belge. En *France*, le Conseil d'État[15] donne à la situation exceptionnelle à laquelle les juges européens lient la possibilité d'une conservation générale des données de communication une interprétation large, en estimant que la menace terroriste existe au regard d'événements récents :

> « la France est confrontée à une menace pour sa sécurité nationale, appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure [...] qui, par son intensité, revêt un caractère grave et réel. Cette menace est, à la date de la présente décision, non seulement prévisible mais aussi actuelle. Cette menace procède d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés. Deux nouveaux attentats ont déjà été déjoués en 2021. Le plan Vigipirate a été mis en œuvre au niveau "Urgence attentat" entre le 29 octobre 2020 et le 4 mars 2021 puis au niveau "Sécurité renforcée – risque attentat" depuis le 5 mars 2021, attestant d'un niveau de menace terroriste durablement élevé sur le territoire. Par ailleurs, la France est particulièrement exposée au risque d'espionnage et d'ingérence étrangère, en raison notamment de ses capacités et de ses engagements militaires et de son potentiel technologique et économique »[16].

15 C.E. fr., 21 avril 2021, *French Data network e.a.*, nos 393099, 394922, 397844, 397851, 424717 et 424718.

16 Le Conseil d'État ajoute pour justifier le maintien d'une obligation de conservation généralisée: « La France est également confrontée à des menaces graves pour la paix publique, liées à une augmentation

Sans doute, le Conseil d'État français exige une réévaluation de ces circonstances exceptionnelles légitimant la conservation généralisée mais ne précise pas la procédure à suivre, les critères selon lesquels la gravité de la menace est appréciée, ni l'autorité compétente qui aura à prendre cette décision.

La Cour constitutionnelle *belge* s'en tient à une interprétation stricte[17]. Elle relève à la suite de la jurisprudence européenne que la mesure de conservation généralisée constitue une menace pour la vie privée et la liberté d'expression bien plus importante que toute autre mesure d'accès limité à des données[18]. Elle souligne que la conservation ne s'entend que de menaces graves à la sécurité nationale et non à ces objectifs de sécurité publique comme la criminalité grave :

> « Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme »[19].

La haute Cour belge estime dès lors que « [p]our satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère

de l'activité de groupes radicaux et extrémistes. Ces menaces sont de nature à justifier l'obligation de conservation généralisée et indifférenciée des données de connexion. »

17 C.C., 22 avril 2021, *O.B.F.G. e.a.*, n° 57/2021, R.G. n^{os} 6590, 6597, 6599 et 6601.

18 *Ibid.*, § 117 : « Cette conclusion apparaît d'autant plus justifiée que les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 27, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 99). »

19 C.J.U.E., 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, § 135. Elle continue au § 136 : « Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, mêmes graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs. »

personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire »[20]. Sur cette base, la Cour estime qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données soit l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues[21].

9. Sans doute, ce qui frappe dans les décisions tant européennes que belges, c'est la mise en évidence, pour apprécier les risques encourus par nos libertés, de l'importance de l'utilisation du numérique dans la mise en œuvre des dispositions réglementaires. C'est en considérant ces nouveaux risques liés en particulier aux perspectives à large échelle de profilage, de détection automatisée de données sensibles, de géolocalisation, mais également aux risques d'utilisations illicites liées à l'accès aux données de communication, que se justifient l'annulation des dispositions nationales qui autorisent la conservation généralisée des données de communication et la prohibition en principe de tout instrument de surveillance de masse[22].

La prise en considération de tels risques justifie par ailleurs les précisions que la décision européenne apporte aux autres mesures susceptibles d'être adoptées cette fois de manière non exceptionnelle par les autorités policières[23]. Sans

20 C.C., 22 avril 2021, *O.B.F.G. e.a.*, *op. cit.*, § 132.

21 *Ibid.*, § 139.

22 La décision *Schrems II* a déclaré invalide l'accord dit « Privacy Shields ». Cet accord avait été pris par la Commission européenne avec le gouvernement américain afin d'encadrer les flux transfrontières vers les États-Unis. Il a été considéré comme ne satisfaisant pas aux exigences d'adéquation imposées par le Règlement général sur la protection des données (R.G.P.D.).

23 Nous n'étudierons pas les balises mises à ces autres mesures. Ainsi, en fonction de la gravité des risques de telles mesures d'utilisation des techniques modernes, la Cour précise que sont légitimes 1. les dispositions réglementaires : « prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la *criminalité grave* et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ; prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la *lutte contre la criminalité grave et de menaces graves* à la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ; prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, 2. l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingé-

doute, si, comme le constate la juridiction française, les développements du numérique permettent une effectivité des législations pénales sans commune mesure avec celle des outils traditionnels de recherche policière et judiciaire, voire des services de renseignements, les atteintes à nos libertés tant individuelles que collectives exigent des limites à leur adoption.

Comme le note la Cour constitutionnelle belge, « l'arrêt de la Cour de justice du 6 octobre 2020 impose un changement de perspective par rapport au choix que le législateur a effectué : l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. La réglementation prévoyant une telle obligation doit par ailleurs être soumise à des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales (point 133). Cette réglementation doit garantir que l'ingérence se limite au strict nécessaire et doit toujours "répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi" (points 132 et 133) »[24].

Pour revenir à notre sujet, à savoir le régime d'exception justifié par des impératifs de sécurité nationale, en l'occurrence les dispositions réglementaires prescrivant aux opérateurs de communication la conservation généralisée des données de communication et l'accès à celles-ci par les autorités policières et judiciaires ainsi que par les services de renseignement, sans doute serait-il utile de prolonger la réflexion sur la façon dont se définit et s'édicte ce régime d'exception. À cet égard, nous proposons de tirer quelques enseignements de l'article 15 de la Convention européenne des droits de l'homme qui prévoit précisément, de manière inchoative certes, le cadre de ces régimes d'exception. Le recours à cet article a été invoqué récemment à propos de l'adoption des mesures contre la pandémie.

rence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte des droits fondamentaux de l'Union européenne, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave (C.J.U.E., 2 octobre 2018, *Ministerio fiscal*, C-207/16) et permettant, aux fins de la lutte *contre la criminalité grave* et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services » (C.J.U.E., 6 octobre 2020, *La Quadrature du Net e.a.*, *op. cit.*, dispositif. Nous soulignons). L'arrêt européen précise : « Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données » (arrêt, n° 68).

24 C.C., 22 avril 2021, *O.B.F.G. e.a.*, *op. cit.*, point B.18.

II. L'article 15 de la C.E.D.H. – fondement des régimes d'exception – vers une traduction belge ?

A. La lutte contre la pandémie, autre cas d'état d'exception

10. La résolution du Parlement européen du 13 novembre 2020 sur la pandémie et l'État de droit résume bien le propos ci-dessus tenu sur l'importance du numérique dans la lutte contre la Covid et les risques y liés :

> « Considérant que, dans le cadre de la lutte contre la pandémie, les mesures restrictives des droits relatifs au respect de la vie privée et à la protection des données devraient revêtir un caractère essentiel, proportionné et temporaire ; que les nouvelles technologies ont joué un rôle important face à la pandémie, mais qu'elles posent de nouveaux défis et ont soulevé des inquiétudes ; que les gouvernements de certains États membres ont recouru à une surveillance extrême de leurs citoyens : utilisation de drones[25], surveillance au moyen de véhicules de police équipés de caméras, traçage grâce aux données de localisation des prestataires de services de télécommunications, patrouilles de police et militaires, suivis de quarantaines obligatoires par des appels de la police au domicile ou obligations de déclaration au moyen d'applications ; que certains États membres ont introduit des applications de traçage des contacts, bien qu'il n'existe pas de consensus quant à leur efficacité et que le système décentralisé, pourtant le plus respectueux de la vie privée, n'est pas toujours utilisé que, dans certains États membres, la réouverture des espaces publics est allée de pair avec la collecte de données à partir des contrôles de température obligatoires et de questionnaires et l'obligation de communiquer des informations sur les contacts, parfois au mépris des obligations découlant du règlement général sur la protection des données »[26].

À propos de la lutte contre la pandémie, aujourd'hui, il est temps de mesurer l'ampleur des dégâts faits à nos libertés. Les droits à l'éducation, au rassemblement, à l'exercice du culte, à la libre expression et à la libre entreprise, à la mobilité, à la vie privée se trouvent tous limités ou suspendus et, en tout cas, sacrifiés au « tout sanitaire ». Comme l'écrit Garapon, « les mesures adoptées dans l'urgence s'apparentent à une immense prescription médicale généralisée à l'ensemble de la population, plus qu'à du droit ».

25 Sur l'utilisation de drones à des fins de lutte contre la pandémie, notons que, par une ordonnance de référé rendue le 18 mai 2020, le Conseil d'État français a enjoint à « l'État de cesser, sans délai, de procéder aux mesures de surveillance par drone, du respect, à Paris, des règles de sécurité sanitaire applicables à la période de déconfinement ». Le Conseil d'État a estimé que, du fait de la possibilité de zoomer et d'identifier des personnes physiques, les dispositifs utilisés par la préfecture de police de Paris étaient soumis aux règles protégeant les données personnelles. Il a jugé que ces drones étaient utilisés en dehors du cadre prévu par la loi « Informatique et Libertés » et portaient une atteinte « grave et manifestement illégale au droit au respect de la vie privée » (C.E. fr., Juge des référés, 18 mai 2020, n° 440442, inédit au *Rec. Lebon*, § 18, www.legifrance.gouv.fr/ceta/id/CETATEXT000041897158/).

26 Résolution du Parlement européen du 13 novembre 2020 sur l'incidence des mesures relatives à la Covid-19 sur la démocratie, l'état de droit et les droits fondamentaux, 2020/2790(RSP), www.europarl.europa.eu/doceo/document/TA-9-2020-0307_FR.html, point AA.

Mieux, les rhétoriques du temps de guerre[27], de l'état de nécessité et de la défense de la Nation sont évoquées à l'appui de mesures qui se succèdent avec comme seul guide les chiffres… ceux d'hospitalisations pour des lits trop peu nombreux, ceux des morts qu'on n'aime pas compter, ceux de la vaccination que certains gouvernements rendent obligatoire, pour certaines professions du moins.

Dans le même temps, nous inquiètent plus encore les risques que le déluge de mesures masque : ceux d'un État de droit et d'une démocratie qui peu à peu s'évanouissent. La résolution du Parlement européen citée en exergue de ce point fait écho à l'inquiétude :

> « Ces mesures ont une incidence sur la démocratie, l'état de droit et les droits fondamentaux étant donné qu'ils influent sur l'exercice des libertés et droits individuels, tels que la liberté de circulation, la liberté de réunion et d'association, la liberté d'expression et d'information, la liberté de religion, le droit à la vie de famille, le droit d'asile, le principe d'égalité et de non-discrimination, le droit à la vie privée et à la protection des données, le droit à l'éducation et le droit de travailler »[28].

Nous voilà avertis mais la parole européenne, fût-elle celle de nos représentants élus, semble avoir des difficultés à se faire entendre de nos gouvernants, pressés d'agir sous la pression du public qui ne sait plus à quel saint se vouer et aime qu'un pouvoir fort le rassure.

11. À l'appui de telles mesures, on note la multiplication des traitements informatiques et bases de données créés en ces temps de Covid, pour tracer, traquer la maladie et donc les individus porteurs ou susceptibles de porter le virus, et c'est sans doute à propos de ces mesures que les débats se sont les plus focalisés avec une belle résistance, celle en particulier menée par les autorités de protection des données, garantes de la protection de nos libertés individuelles[29].

27 Nous faisons allusion notamment aux déclarations du président Macron le 16 mars 2020, où il annonce aux Français que des mesures de confinement sont nécessaires pour freiner la propagation de la Covid-19, et déclare sur un ton grave : « Nous sommes en guerre » (A. Lemarié et C. Pietralunga, « "Nous sommes en guerre" : face au coronavirus, Emmanuel Macron sonne la "mobilisation générale" », *Le Monde*, 17 mars 2020, www.lemonde.fr/politique/article/2020/03/17/nous-sommes-en-guerre-face-au-coronavirus-emmanuel-macron-sonne-la-mobilisation-generale_6033338_823448.html). En France, le fondement légal du confinement s'inspire de deux origines militaires, de sorte que la référence à la guerre est bien plus qu'une métaphore. Ainsi, le premier décret du 16 mars 2020 en appelait à la théorie des circonstances exceptionnelles, remontant à la Première Guerre mondiale.

28 Résolution du Parlement européen du 13 novembre 2020, *op. cit.*, point D. La résolution s'appuie notamment sur la communication de la Commission du 30 septembre 2020 intitulée « Rapport 2020 – La situation de l'État de droit dans l'Union européenne » (COM(2020)0580) et les 27 chapitres par pays qui l'accompagnent sur l'État de droit dans les États membres (SWD(2020)0300-0326), qui traitent de l'incidence des mesures relatives à la Covid-19 prises par les États membres sur la démocratie, l'État de droit et les droits fondamentaux.

29 Le lecteur trouvera la liste complète et impressionnante des avis, opinions, déclarations, etc. des autorités de protection des données et autres organes nationaux et internationaux de protection des données sur le site https://globalprivacyassembly.org/covid19/. Voy. également le site très nourri de l'équipe

Les mesures proposées sont-elles de simples limitations de nos libertés ou s'agit-il plus radicalement d'une suspension, voire d'une atteinte à l'essence même de celles-ci, ce que l'article 52 de notre Charte européenne des droits fondamentaux proscrit ? L'article 52 de la Charte européenne consacre à la fois la possibilité de limitation des droits fondamentaux énoncée dans la Charte, en même temps qu'elle assigne des balises à cette limitation : « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être *prévue par la loi* et *respecter le contenu essentiel* desdits droits et libertés. Dans le respect du *principe de proportionnalité*, des limitations ne peuvent être apportées que si elles sont *nécessaires et répondent effectivement à des objectifs d'intérêt général* reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui » (nous soulignons).

Où trouver le fondement d'une mise entre parenthèses des libertés et droits fondamentaux, à l'heure même où le numérique donne aux prescrits réglementaires, parfois de simple police administrative, une portée bien plus prégnante sur nos libertés ? La liberté de réunion, y compris syndicale, est-elle encore possible lorsque des drones surveillent les rassemblements et ont un effet dissuasif sur la population ? La vaccination même affichée comme une ardente « obligation » morale s'impose au citoyen, qui se sait « traqué » par une base de données largement accessible, y compris lorsqu'il s'adresse à un pharmacien pour l'obtention d'un simple médicament sans lien avec la Covid ou souhaite s'asseoir à la table d'un restaurant[30] ou participe à un événement dit de masse.

de recherche L.S.T.S. de la V.U.B. (Bruxelles) : « Data Protection Law & Covid-19 : An Observatory », https://lsts.research.vub.be/en/data-driven-approaches-to-covid-19-data-protection-law-dpl-x-covid-19.

30 Il ne nous revient pas de discuter de l'opportunité de la vaccination obligatoire (sur ce point, voy. les réflexions récentes de X. Bioy, « Vers la vaccination obligatoire contre la Covid ? Que dit le droit de la santé ? Que répondent les droits fondamentaux ? », *Le club des juristes*, 8 juillet 2021) mais de noter que même si celle-ci existe pour d'autres maladies, l'instrument qui la constate ne fait pas l'objet d'une information centralisée accessible largement. Dans les autres cas, l'instrument qui constate la vaccination est un document porté par le citoyen qui garde la maîtrise de le communiquer aux personnes habilitées à la recevoir. La création d'une base de données modifie complètement le risque encouru par le nombre de personnes qui peuvent avoir accès réglementairement à cette information, sans compter les risques d'accès illicite à la base de données. Sur ce point, voy. l'avis récent de l'A.P.D. concernant un projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement des données liées au certificat Covid numérique de l'U.E. et au Covid Safe Ticket, le P.L.F. et le traitement des données à caractère personnel des travailleurs salariés et des travailleurs indépendants vivant ou résidant à l'étranger qui effectuent des activités en Belgique et un projet d'accord de coopération d'exécution entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française concernant le traitement des données liées au certificat Covid numérique de l'U.E. et au Covid Safe Ticket, le P.L.F. et le traitement des données à caractère personnel des travailleurs salariés et des travailleurs indépendants vivant ou résidant à l'étranger qui effectuent des activités en Belgique (CO-A-2021-139 & CO-A-2021-140) du 12 juillet 2021, n° 124/2021 : « l'Autorité souligne le caractère particulièrement sensible et inédit du Covid Safe Ticket qui est un dispositif de contrôle visant à conditionner l'accès à certains lieux ou événements à la présentation

12. La limitation des droits fondamentaux ne doit donc pas être confondue avec la dérogation ou suspension de ces droits. Les dérogations mettent « entre parenthèses » les libertés fondamentales pour une période donnée, dans des circonstances exceptionnelles données, telles que l'état d'urgence sanitaire, les atteintes terroristes, l'état de guerre[31]. Il s'ensuit que les États ne sont plus alors contraints de satisfaire aux conditions de justification imposées pour les restrictions aux droits fondamentaux lorsqu'ils se trouvent dans ces circonstances spécifiques de dérogation[32].

Bref, il appert, au vu de l'ampleur des restrictions apportées par les lois et ordonnances, voire décrets de toutes natures pris par l'autorité publique, que celle-ci aurait dû se référer à l'article 15 de la Convention du Conseil de l'Europe pour les justifier[33]. Sans doute, dans le cas de telles suspensions ou dérogations des libertés fondamentales, l'article 52 n'interdit pas de recourir à l'article 15 de la C.E.D.H., nous dit l'interprète autorisé de la Charte, à savoir

de la preuve de l'état de santé des personnes » (§ 39) et plus loin « En outre, pour que l'ingérence dans les droits fondamentaux générée par l'introduction du Covid Safe Ticket soit admissible, il faut que les auteurs du projet démontrent, à l'aide d'éléments factuels et concrets, (1) que le Covid Safe Ticket permet effectivement d'atteindre cet objectif, (2) qu'il n'y a pas de moyens moins intrusifs permettant de l'atteindre et (3) que les avantages apportés par ce dispositif dépassent les inconvénients et les risques (y compris le risque d'accoutumance et de normalisation sociale des comportements qui portent atteinte aux droits fondamentaux ainsi que le risque de "glisser" vers une société de surveillance) qu'il introduit. Actuellement, cette démonstration fait défaut » (§ 43).

31 S.U. Colella, « Chapitre 1 – L'acception des notions de restriction, limitation et dérogation », *in La restriction des droits fondamentaux dans l'Union européenne*, Bruxelles, Bruylant, 2018, p. 126.

32 O. de Schutter, *International Human Rights Law. Cases, Materials, Commentary*, 2e éd., Cambridge, Cambridge University Press, 2014, p. 585. *Cf.* également, l'affirmation forte de la Secrétaire générale du Conseil de l'Europe, Marija Pejčinović Burić, lors de la publication le 7 avril 2020, de la boîte à outils à l'intention de l'ensemble des gouvernements européens sur le respect des droits de l'homme, de la démocratie et de l'État de droit pendant la crise du Covid-19 (disponible à l'adresse: https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40): « While some restrictive measures adopted by member states may be justified on the ground of the usual provisions of the European Convention on Human Rights (Convention) relating to the protection of health (see Article 5 paragraph 1e, paragraph 2 of Articles 8 to 11 of the Convention and Article 2 paragraph 3 of Protocol No 4 to the Convention), measures of exceptional nature may require derogations from the states' obligations under the Convention ».

33 Le droit constitutionnel belge soulève une difficulté supplémentaire dans la mesure où l'article 187 de la Constitution semble interdire, sauf argument tiré de la primauté du droit international et donc l'obligation de s'en référer à l'article 15 de la C.E.D.H., toute dérogation aux libertés au-delà de simples limitations: « En Belgique, de telles suspensions ne sont pas autorisées par la Constitution. En effet, adopté en 1831, l'article 187 de la Constitution dispose que "la Constitution ne peut être suspendue en tout ni en partie". Cette interdiction proscrit formellement, l'instauration d'un "état d'urgence" ou d'un "état d'exception", sauf en temps de guerre, en application de l'arrêté-loi du 11 octobre 1916 relatif à l'état de guerre et à l'état de siège. L'esprit du Constituant de 1831 est clair, sa volonté était d'empêcher la mise en place de régimes d'exception où les droits fondamentaux sont suspendus, même au nom de l'intérêt de la nation... La formule de l'article 187 implique que "les pouvoirs doivent continuer à être exercés même dans des circonstances de crise et de transition" car "même en pareilles circonstances, l'autorité doit défendre l'intérêt général et rencontrer les besoins collectifs" » (S. Parsa et Y. Poullet, « Les droits fondamentaux à l'épreuve du confinement et du déconfinement », *op. cit.*, p. 146).

l'Agence des droits fondamentaux de l'Union européenne (*Fundamental Rights Agency*, ci-après FRA):

> « La Charte n'empêche pas les États membres de se prévaloir de l'article 15 de la C.E.D.H., qui autorise des dérogations aux droits prévus par cette dernière en cas de guerre ou d'autre danger public menaçant la vie de la nation, lorsqu'ils prennent des mesures dans les domaines de la défense nationale en cas de guerre et du maintien de l'ordre, conformément à leurs responsabilités reconnues dans l'article 4, paragraphe 1, du traité sur l'Union européenne et dans les articles 72 et 347 du traité sur le fonctionnement de l'Union européenne »[34].

L'intérêt de ce recours à l'article 15 s'explique par le fait qu'il instaure un régime d'exception qui, tout en autorisant des restrictions importantes aux libertés au nom d'intérêts généraux supérieurs bien spécifiés, se voit balisé afin de maintenir un État de droit[35]. Des auteurs constitutionnalistes tant français que belges ont à juste titre regretté que la mise en œuvre de cet article n'ait pas été opérée par les gouvernements de ces deux pays à l'occasion de la prise de mesures pour lutter contre la pandémie[36].

B. Le régime de l'article 15 de la C.E.D.H.

13. Venons-en précisément à cet article 15 que, contrairement à la France et la Belgique, pas moins de dix pays signataires de la Convention[37] ont souhaité

34 FRA, « Article 52 – Portée et interprétation des droits et principes », https://fra.europa.eu/fr/eu-charter/article/52-portee-et-interpretation-des-droits-et-des-principes.

35 Sur la dérive totalitaire que facilitent les états dits d'exception, voy. l'ouvrage de M.-L. Basilien-Gainche, *État de droit et états d'exception, une conception de l'État*, coll. Fondements de la politique, Paris, P.U.F., 2013: « L'État de droit renvoie au droit et à la norme, à la normalité et à l'ordinaire: il est une finalité politique de l'État, un horizon de perfection nourri de séparation des pouvoirs et de garantie des droits. Quant aux états d'exception, ils évoquent le dérèglement et l'extraordinaire, la concentration des pouvoirs et la restriction des droits ». À noter la réflexion de B. Rappin (« Algorithme, management, crise: le triptyque cybernétique du gouvernement de l'exception permanente », *Quaderni*, 2018/2, n° 96, pp. 103-114), qui voit dans la cybernétique le risque d'une consolidation des états d'exception: « la cybernétique constitue la matrice du gouvernement contemporain de l'exception permanente ». Nous reviendrons sur les réflexions de cet auteur inspirées des écrits de Naomi Klein (*infra*, n° 26).

36 Ainsi, notamment en France, Fr. Sudre, « La mise en quarantaine de la Convention européenne des droits de l'homme », *Le club des juristes*, 20 avril 2020; J.-P. Costa, « Le recours à l'article 15 de la Convention européenne des droits de l'homme », *Le club des juristes*, 27 avril 2020; en Belgique, Fr. Ost, « Nécessité fait loi? La santé n'a pas de prix? Ce que le Covid fait au droit », *in* S. Parsa et M. Uyttendaele (coord.), *La pandémie de Covid-19 face au droit*, *op. cit.*, pp. 17 et s., en particulier pp. 26 et 27; M. Verdussen, « Droits humains et crise sanitaire: l'État mis au défi », *La Libre Belgique*, 19 juillet 2020.

37 Il est intéressant de noter que si la France comme la Belgique n'ont pas (encore) utilisé cette exception à l'occasion de la pandémie, d'autres pays ont démarré les procédures depuis la mi-mars. Selon la Commission de Venise (Rapport intérimaire sur les mesures prises dans les États membres de l'U.E. à la suite de la crise de la Covid-19 et leur incidence sur la démocratie, l'État de droit et les droits fondamentaux, 8 octobre 2020, Avis n° 995/2020, CDL-AD(2020)018, § 35, www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2020)018-f): « Au plus fort de la crise de la Covid-19 en Europe au printemps 2020, neuf États membres de l'U.E. avaient déclaré l'état d'urgence, quelle que soit sa formulation juridique, en vertu des dispositions pertinentes de leur Constitution: Bulgarie, Espagne, Estonie, Finlande, Hongrie, Luxembourg, Portugal, République tchèque et Roumanie ». Voy. également Conseil de l'Europe,

mettre en branle à l'occasion de la pandémie et que, curieusement, la France avait déjà invoqué trois fois et pour la dernière lors des attentats terroristes de 2015[38]. L'article 15 de la C.E.D.H.[39] autorise, moyennant préalable information du Secrétaire général de la Convention, des dérogations à l'application des droits et libertés en cas d'état urgence : « En cas de guerre ou en cas d'autre danger public menaçant la vie de la nation, toute Haute Partie contractante peut prendre des mesures dérogeant aux obligations prévues par la présente Convention, dans la stricte mesure où la situation l'exige et à la condition que ces mesures ne soient pas en contradiction avec les autres obligations découlant du droit international ».

Les dispositions de cet article de la Convention visent à introduire la théorie de l'état de nécessité pour justifier les exceptions[40], tout en imposant aux États membres des conditions strictes en vue d'encadrer l'exercice de telles dérogations. S'il est clair qu'il peut être invoqué vis-à-vis de situations de troubles à l'ordre public comme la guerre ou les menaces terroristes, l'article 15 peut-il être appliqué à des situations comme une pandémie ? L'interprétation des mots « en cas d'autre danger public menaçant la vie de la nation » autorise, selon la jurisprudence de la Cour européenne des droits de l'homme[41], cette extension. Celle-ci est d'ailleurs approuvée par le Conseil de l'Europe par le fait même de sa publication de la « boîte à outils » d'utilisation de l'article 15, en 2020.

14. Parmi les conditions fixées au régime des dérogations de la Convention, on distingue trois conditions matérielles[42] : premièrement, la survenance de

« Fiche thématique : Dérogation en cas d'état d'urgence », septembre 2020, p. 2, www.echr.coe.int/documents/fs_derogation_fra.pdf ; et pour des informations détaillées s'agissant du contexte dans lequel ces dérogations ont été formulées, la page internet de renvoi au Bureau des Traités du Conseil de l'Europe.

38 À la suite des attentats du 13 novembre 2015, après la déclaration de l'état d'urgence, la France a notifié au Conseil de l'Europe qu'elle risquait de déroger à la convention. Ces notifications ont pris fin le 1er novembre 2017 après la fin de l'état d'urgence. Voy. également les proclamations d'état d'exception en 1985 à propos des incidents en Nouvelle-Calédonie et, en 2005, à propos des violences urbaines. Il est donc étonnant que lors de sa décision analysée plus tôt à propos de la contestation par la C.J.U.E. de l'obligation de conservation généralisée des données de communication, le Conseil d'État n'ait plus mentionné ces procédures pourtant utilisées et jugées alors nécessaires.

39 À propos de cet article invoqué par quelques pays membres du Conseil de l'Europe à d'autres occasions que la pandémie et souvent pour des raisons de lutte contre le terrorisme, voy., notamment, J.-Fr. Renucci, *Droit européen des droits de l'homme*, 6e éd., Paris, L.G.D.J., 2015, pp. 33-35.

40 À noter en outre que l'article 17 de cette même Convention énonce de manière plus générale le principe d'interdiction d'abus, en particulier de la part des autorités publiques : « Aucune des dispositions de la présente Convention ne peut être interprétée comme impliquant pour un État, un groupement ou un individu, un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Convention ou à des limitations plus amples de ces droits et libertés que celles prévues à ladite Convention ».

41 On cite en ce sens, l'arrêt *Lawless c. Irlande*, 1er juillet 1961, n° 332/57, § 28, où la Cour a jugé que les termes de l'article 15 désignent « une situation de crise ou de danger exceptionnel et imminent qui affecte l'ensemble de la population et constitue une menace pour la vie organisée de la communauté composant l'État » ; et l'arrêt *Irlande c. Royaume-Uni*, 18 janvier 1978, n° 5310/71, § 207, qui laisse aux États une large marge de manœuvre dans l'interprétation des concepts de l'article 15.

42 Conseil de l'Europe, *Guide sur l'article 15 de la Convention européenne des droits de l'homme – Dérogation en cas d'état d'urgence*, mis à jour le 30 avril 2021, https://echr.coe.int/Documents/Guide_Art_15_FRA.pdf.

circonstances graves telles qu'une guerre ou d'autres dangers publics menaçant la vie de la nation ; deuxièmement, une nécessité absolue ; troisièmement, le respect des autres obligations découlant du droit international. À ces conditions de fond, il faut rajouter une condition de forme, à savoir la notification au Secrétaire général du Conseil de l'Europe tant des mesures prises que des motifs qui les ont inspirés, conformément au troisième paragraphe de l'article 15[43]. Les États doivent également informer le Secrétaire général du Conseil de l'Europe de la date à laquelle « les dispositions de la Convention reçoivent de nouveau pleine application ». Enfin, la Secrétaire générale, lors de la publication, le 7 avril 2020, de la boîte à outils sur l'utilisation de l'article 15 à l'occasion de la pandémie du coronavirus, rappelle que les dérogations doivent être proportionnées, encadrées si possible par des mesures législatives, « respecter les principes de l'État de droit (nécessité ne fait pas loi) et les principes démocratiques en cas d'état d'urgence, respecter les normes fondamentales en matière de droits de l'homme, notamment en ce qui concerne la liberté d'expression, la vie privée et la protection des données, la protection des groupes vulnérables contre la discrimination et le droit à l'éducation ; enfin, assurer une protection contre le crime et les victimes du crime, en particulier concernant la violence fondée sur le genre »[44]. Ainsi, cet état de nécessité ne dispense pas d'établir la légalité et la proportionnalité des mesures restrictives proposées[45].

15. Trois arguments plaident en faveur du passage par la procédure et les conditions de l'article 15 de la C.E.D.H. :

– la franchise : l'article 15 exige la transparence et la légitimité tant des mesures que des motifs ;

43 « Toute Haute Partie contractante qui exerce ce droit de dérogation tient le Secrétaire général du Conseil de l'Europe pleinement informé des mesures prises et des motifs qui les ont inspirées. Elle doit également informer le Secrétaire général du Conseil de l'Europe de la date à laquelle ces mesures ont cessé d'être en vigueur et les dispositions de la Convention reçoivent de nouveau pleine application. »

44 Boîte à outils à l'intention de l'ensemble des gouvernements européens sur le respect des droits de l'homme, de la démocratie et de l'État de droit pendant la crise du Covid-19, *op. cit.*

45 « At the same time, any derogation must have a clear basis in domestic law in order to protect against arbitrariness and must be strictly necessary to fighting against the public emergency. States must bear in mind that any measures taken should seek to protect the democratic order from the threats to it, and every effort should be made to safeguard the values of a democratic society, such as pluralism, tolerance and broadmindedness. While derogations have been accepted by the Court to justify some exceptions to the Convention standards, they can never justify any action that goes against the paramount Convention requirements of lawfulness and proportionality. » À propos de cet article, voy. les commentaires de la Commission de Venise du Conseil de l'Europe dans son Rapport intérimaire sur les mesures prises dans les États membres de l'U.E. à la suite de la crise de la Covid-19, *op. cit.*, § 15 : « Le troisième instrument est la dérogation aux droits de l'homme, à savoir, la suspension temporaire de certaines garanties des droits de l'homme, [...] auxquelles il est possible d'avoir recours en cas d'état d'urgence. Les dérogations sont des mesures plus radicales que les exceptions et les limitations et elles ne peuvent être utilisées que dans des circonstances exceptionnelles de "guerre ou en cas d'autre danger public menaçant la vie de la nation" (article 15.1 de la C.E.D.H.). Les dérogations sont soumises aux conditions de nécessité, de proportionnalité et de caractère temporaire. Elles impliquent également des obligations procédurales (déclaration de l'état d'urgence, notification en vertu des traités sur les droits de l'homme) qui rendent la surveillance plus facile et plus solide. Là encore, il existe une riche jurisprudence relative aux dérogations au niveau international et national ».

- le contrôle par les pairs et le Conseil de l'Europe : la communication envers le Conseil de l'Europe des mesures prises ou envisagées permet un *benchmarking* des décisions par rapport à celles d'autres États et cela sous l'œil vigilant des organes du Conseil de l'Europe, qui peuvent sur cette base comparative interroger les États sur la proportionnalité des mesures ;
- la nécessité d'une délibération démocratique parlementaire, dans la mesure où le Conseil de l'Europe sera saisi d'un texte ayant reçu l'assentiment du législatif au terme d'une procédure complète[46].

On ajoute d'autres avantages : en particulier, l'obligation de fixer aux mesures d'exception une durée ne dépassant pas l'urgence sanitaire. La fixation d'une date déterminée n'est pas obligatoire, mais notons que cette fixation n'empêche pas la prorogation, simplement elle oblige à justifier celle-ci et à passer par une procédure d'information du Conseil de l'Europe. Ensuite, elle exige que les mesures prises soient nécessaires, adéquates et strictement proportionnées[47]. Enfin, elle invite à réfléchir sur les limites fixées par l'exigence de respecter l'« essence » des libertés et droits, notion dont on regrette qu'elle n'ait fait l'objet jusqu'ici que de peu de commentaires. Cette notion invite à prendre en considération non seulement le contenu des prescrits mais aussi les mesures d'effectivité de tels prescrits, en particulier celles consistant en l'utilisation des technologies du numérique. Il est certain qu'au nom de l'état d'exception, le gouvernement a adopté des mesures qui allaient au-delà de la simple limitation des libertés et s'apparentaient à de véritables mises entre parenthèses de celles-ci[48].

La restriction « essentielle » et la suspension des droits et libertés doivent faire l'objet d'une analyse de proportionnalité et d'une motivation plus soignées encore que les simples limites, dans la mesure où elles doivent présenter un caractère exceptionnel pour une situation jugée démocratiquement comme mettant en péril la sauvegarde de la nation[49]. Elle invite en tout cas à distinguer,

46 Commission de Venise, rapport intérimaire sur les mesures prises dans les États membres de l'U.E. à la suite de la crise de la Covid-19, *op. cit.*, § 34 : « L'état d'urgence peut être déclaré par le Parlement ou par l'exécutif. Idéalement, elle devrait être déclarée par le Parlement ou par l'exécutif, sous réserve de l'approbation immédiate du Parlement. En cas d'urgence, une entrée en vigueur immédiate pourrait être autorisée – cependant, la déclaration devrait être immédiatement soumise au Parlement, qui peut la confirmer ou l'abroger ». La Commission de Venise est, notons-le, un organe créé par le Conseil de l'Europe sur la situation de l'État de droit dans nos différents pays.

47 Sur les exigences liées à ces concepts, voy. nos réflexions *infra*, n° 22.

48 Sur ce point, voy. notre contribution dans les Actes du colloque de Lille (Y. POULLET, « Covid et libertés – Quelques considérations », *op. cit.*), en particulier les discussions en ce qui concerne les libertés de réunion syndicales, de religion, de déplacement,

49 En ce sens, la déclaration nette du Conseil d'État français : « Le caractère nécessaire, proportionné et approprié d'une telle mesure ne saurait être regardé comme exclu dans la perspective, qui est celle du projet de loi, de disposer de moyens juridiques pérennes de réponse à des catastrophes sanitaires dont la gravité ne peut être anticipée. Elle peut permettre, par elle-même, de concilier, dans les hypothèses d'épidémie d'une particulière gravité, l'exercice effectif de certaines libertés avec l'objectif de protection de la

comme le faisait le projet de loi français[50] à propos des mesures prises pour enrayer la pandémie, celles justifiées par la situation de crise « en cas de menaces et situation sanitaires graves » de celles nécessitées par l'état d'urgence sanitaire, qui requiert une déclaration « en cas de catastrophe sanitaire mettant en péril, par sa nature et sa gravité, la santé de la population ». C'est dans ce second cas seulement que l'état d'exception qui justifie des restrictions aux libertés et non de simples limitations devrait s'appliquer conformément aux prescrits de l'article 15 de la C.E.D.H.

On retrouve ici l'interprétation restrictive en ce qui concerne les situations d'exception, interprétation développée par la Cour de justice européenne à propos de l'obligation de conservation généralisée des données de communication (*supra*, n^os^ 6 et s.).

C. *L'analyse de la loi dite « pandémie »*

16. La réponse belge que constitue la loi dite « pandémie »[51] est-elle adéquate ? Sans aucun doute, non. D'abord, elle ne contient aucune référence à la procédure de l'article 15 de la C.E.D.H. Ensuite, elle est partielle, ne visant que l'urgence sanitaire. Ne fallait-il pas, au-delà de dispositions relatives à la pandémie, envisager un régime général de l'état d'exception, auquel invitait la Cour de justice européenne en ouvrant le débat relatif à cet autre sujet qu'est la conservation généralisée des données de communication ?

Le fondement de l'état d'exception dans les deux cas est semblable : dans le cas de l'obligation de conservation, on met en avant le droit à la sécurité comme justifiant des restrictions à nos libertés et au nom de l'efficacité la remise en cause des processus démocratiques ; dans le second, c'est le droit à la santé qui justifie ce même mouvement.

Enfin, cette réponse nous paraît manquer le sujet principal, celui du maintien de l'État de droit dans un contexte d'état d'exception. En particulier sur ce

santé publique, en lieu et place de mesures plus généralisées ou plus restrictives des libertés en cause, notamment de la liberté d'aller et venir et de la liberté d'entreprendre. » (C.E. fr., Avis sur un projet de loi instituant un régime pérenne de gestion des urgences sanitaires, 21 décembre 2020) ; et l'avis récent de l'A.P.D. à propos du contrôle de la vaccination (n° 124/2021, *op. cit.*).

50 On sait que ce projet a été finalement retiré par le gouvernement français à la suite des critiques du Conseil d'État et des sénateurs, dans la mesure où les régimes prévus ne permettaient pas un contrôle suffisant par le Parlement. H. BERKAOUI, « Urgences sanitaires : le gouvernement retire un projet de loi controversé », *Public Sénat*, 23 décembre 2020, www.publicsenat.fr/article/parlementaire/urgences-sanitaires-le-gouvernement-retire-un-projet-de-loi-controverse-186392 : « "On ne peut pas inscrire des mesures privatives de libertés uniquement sur des bases réglementaires", tonnait François-Noël Buffet en soulignant que ce texte faisait très peu de cas du contrôle du Parlement. Et, de fait, ce projet de loi visait à créer deux régimes d'exception – "l'état de crise sanitaire" et "l'état d'urgence sanitaire" – mobilisables par décret. Le Parlement, lui, se serait simplement vu informé par la remise d'un rapport en cas de mise en œuvre de l'état de crise sanitaire pendant plus de six mois ».

51 Loi du 14 août 2021 relative aux mesures de police administrative lors d'une situation d'urgence épidémique, *M.B.*, 20 août 2021, p. 90047.

dernier point, elle prend insuffisamment en compte le fait « numérique » dont la prise en considération est essentielle dans le cadre de ce maintien de l'État de droit. Ces deux dernières critiques sont développées ci-après.

17. Les réflexions qui précèdent invitent en effet à s'interroger sur les risques encourus par le fonctionnement de nos États de droit, dans le cadre de régimes d'exception. Dans le contexte d'état d'exception, il est étonnant que dans le débat présent, la question des libertés, certes centrale, n'ait pas conduit à s'interroger sur ce qui constitue la condition même et la garantie de ces dernières, à savoir le respect de l'État de droit.

À cet égard, attention eut dû être portée sur un texte passé inaperçu, du moins dans notre pays : la résolution du Parlement européen du 13 novembre 2020 sur l'incidence des mesures relatives à la Covid-19 sur la démocratie, l'État de droit et les droits fondamentaux[52].

La résolution souligne :

> « considérant que le fonctionnement des démocraties et le système de contre-pouvoirs, qui les encadre, sont perturbés lorsqu'une situation d'urgence sanitaire contribue à modifier la répartition des pouvoirs ; qu'il en est notamment ainsi lorsque le pouvoir exécutif peut acquérir de nouveaux pouvoirs qui lui permettent de limiter les droits individuels et d'exercer des compétences généralement réservées au pouvoir législatif et aux autorités locales, tandis que le rôle des parlements, du pouvoir judiciaire, de la société, ainsi que les activités et la participation des citoyens sont frappés par des restrictions ; que dans la plupart des États membres, le pouvoir judiciaire s'exerce sans restrictions spécifiques, mais qu'il est quasiment impossible aux tribunaux de fonctionner de manière normale en raison des mesures de confinement ».

Telle est bien la situation lorsque les juridictions ne peuvent plus se réunir ou hésitent à se prononcer dans les cas d'urgence[53] et que les organismes de contrôle de la légalité ou de la constitutionnalité ne peuvent se prononcer dans la mesure où les normes prises par l'exécutif échappent à leur contrôle ; telle est bien la situation au moment où les associations ne peuvent plus s'exprimer dans la rue, et où même les médias accueillent difficilement les détracteurs des mesures anti-Covid, au nom d'une conception élargie de la désinformation, bien loin du principe de la liberté d'expression affirmé notamment par le Conseil de l'Europe[54].

52 Résolution du Parlement européen du 13 novembre 2020, *op. cit.*

53 À cet égard, il serait utile que le recours en cas de violation de libertés soit d'office considéré comme fondé sur une situation d'urgence et que celle-ci ne se limite pas aux seules constatations de dommages matériels ou physiques.

54 Voy. le célèbre attendu de la Cour de Strasbourg dans l'affaire *Handyside c. Royaume-Uni* (7 décembre 1976, n° 5493/72, § 49) : la liberté d'expression « vaut non seulement pour les "informations" ou "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'État ou une fraction quelconque de la population. Ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de "société démocratique" ».

18. Cette affirmation du respect nécessaire de l'État de droit conduit en particulier à réclamer que le législatif[55] et le judiciaire puissent jouer leur rôle à l'appui des libertés :

> « considérant que des mesures d'urgence pilotées par les gouvernements dans le respect de l'état de droit, des droits fondamentaux et de la responsabilité démocratique sont nécessaires pour lutter contre la pandémie et doivent constituer la pierre d'angle de tous les efforts déployés pour contrôler la propagation de la Covid-19 ; que les pouvoirs d'urgence doivent être soumis à un contrôle supplémentaire dont l'objet est de garantir qu'ils ne servent pas en réalité à modifier l'équilibre des pouvoirs de manière plus permanente ; que les mesures prises par les gouvernements devraient être nécessaires, proportionnées et temporaires ; que les pouvoirs d'urgence comportent un risque d'abus de pouvoir par l'exécutif et peuvent subsister dans le cadre juridique national une fois que la situation d'urgence aura pris fin ; qu'il convient par conséquent, pour limiter ce risque, de mettre en place un contrôle parlementaire et judiciaire, tant interne qu'externe, ainsi que des contrepoids appropriés »[56].

En conséquence, il eût été important que notre Parlement entende l'invitation du Parlement européen. Sur ce point, nous rejoignons le Parlement européen lorsqu'il :

> « invite les États membres :
> – à envisager de sortir de l'état d'urgence ou de limiter son incidence sur la démocratie, l'état de droit et les droits fondamentaux,
> – à évaluer les règles constitutionnelles et institutionnelles en vigueur dans leurs systèmes internes à la lumière des recommandations de la Commission de Venise, par exemple en passant d'un état d'urgence de fait fondé sur la législation ordinaire à un état d'urgence constitutionnel de droit, offrant de meilleures garanties pour la démocratie, l'état de droit et les droits fondamentaux en cas de situation d'urgence [...], à définir explicitement dans un acte législatif, si l'état d'urgence de fait est maintenu, les objectifs, le contenu et la portée de la délégation de pouvoir du législatif à l'exécutif,
> – à veiller à ce que la déclaration et la prorogation éventuelle de l'état d'urgence, d'une part, et l'activation et l'application des pouvoirs d'urgence, d'autre part, soient soumises à un réel contrôle parlementaire et judiciaire, aussi bien interne qu'externe, et à garantir que les parlements ont le droit de mettre fin à l'état d'urgence [...],

55 Sur la difficulté du législatif de jouer son rôle dans le cadre de la crise provoquée par la Covid-19, voy. E. Cartier, B. Ridard et G. Toulemonde, *L'impact de la crise sanitaire sur le fonctionnement des Parlements en Europe*, Publication de la Fondation Robert Schuman, 2020, www.robert-schuman.eu/fr/doc/ouvrages/FRS_Parlement.pdf.

56 Résolution du Parlement européen du 13 novembre 2020, *op. cit.*, point B. Dans le même sens, l'article du *Soir* qui dénonce le « casse du siècle sur la vie privée des Belges » : Ph. Laloux, « Le casse du siècle sur la vie privée des Belges », *Le Soir*, 11 février 2021. Il se veut lanceur d'alerte en déclarant : « Une somme inouïe d'incompétences, d'erreurs de jugement, de fautes de gouvernance, de précipitation, d'interprétations tarabiscotées de règlements et d'omniscience mégalomaniaque a conduit à échafauder, consciemment ou non, un système de gestion de l'État à l'écart du contrôle parlementaire, à l'abri du Conseil d'État ou du recours citoyen et échappant à une Autorité de contrôle de plus en plus vidée de sa substance ».

- à veiller à ce que, si des pouvoirs législatifs sont transférés à l'exécutif, tout acte juridique émanant de l'exécutif soit soumis à l'approbation ultérieure du parlement et cesse de produire ses effets s'il n'est pas approuvé dans un délai défini [...] ; à remédier au recours excessif à la législation accélérée et à la législation d'urgence [...],
- à examiner la manière de garantir plus efficacement le rôle central des parlements dans les situations de crise et d'urgence, en particulier leur rôle de suivi et de contrôle de la situation au niveau national,
- à prendre en considération l'avis de la Commission de Venise, qui estime que les parlements doivent tenir leurs sessions plénières et qu'ils ne devraient pas autoriser le remplacement temporaire de députés ni réduire leur présence (même de manière proportionnelle) [...] »[57].

À propos de cette invitation, la loi belge votée le 15 juillet 2021[58] apporte quelques garanties, même si elles sont incomplètes et largement insuffisantes.

19. Sans doute faut-il regretter que le texte belge ne fasse pas allusion à l'article 15 de la C.E.D.H. qui aurait permis de fonder l'état d'exception au regard du droit international et aurait rencontré les avantages précédemment décrits liés à cette référence. Sans doute faut-il regretter que le texte s'adresse à une seule catégorie de « menaces à la sauvegarde des intérêts de la nation » – les risques sanitaires – et ne s'étend pas à d'autres menaces comme le terrorisme ou l'urgence climatique et, dès lors, est incapable de définir en temps utile un régime général de l'état d'exception, capable de prévenir les controverses futures liées à ces autres situations d'exception.

Sans doute et surtout, il est dommage que, contrairement au projet de loi français resté sans lendemain pour d'autres raisons (*supra*, n° 15), le texte n'ait point distingué les « situations de crise sanitaire », y compris graves, des « états d'urgence sanitaire », les restrictions appliquées à la première situation n'étant pas nécessairement les mêmes que celles que commande l'urgence des secondes[59].

La loi belge, dite « loi Pandémie » du 14 août 2021, donne d'ailleurs une définition très large de la notion définie par l'article 2, 3°, comme suit :

> « "situation d'urgence épidémique" : tout événement qui entraîne ou qui est susceptible d'entraîner une menace grave suite à la présence d'un agent infectieux chez l'homme, et : a. qui touche ou est susceptible de toucher un grand nombre de personnes en Belgique et qui y affecte ou est susceptible d'affecter gravement leur santé ; b. et qui conduit ou est susceptible de conduire à une ou plusieurs des conséquences suivantes en Belgique : une surcharge grave de certains professionnels des soins et services de santé ; la nécessité de prévoir le renforcement, l'allégement ou le soutien de certains professionnels des soins et services de santé ; le déploiement rapide et massif de médicaments, dispositifs médicaux ou équipements de protection individuelle ; c. et qui nécessite une coordination et une gestion des acteurs compétents au niveau national afin de faire disparaître la menace ou de limiter les conséquences néfastes de l'événement ».

Ainsi, sans m'attarder sur une analyse détaillée de la loi[60], le mot « susceptible » répété à plusieurs reprises, le fait que les conditions mises au point b) ne doivent pas être rencontrées de manière cumulative et que la référence au point d) soit là « le cas échéant » et donc non obligatoire contrairement au souhait de nombre d'experts laissent entendre une appréciation large de la notion, loin de la volonté tant des juges européens que du texte de la C.E.D.H. de donner une interprétation restrictive des circonstances qui déclenchent l'état d'exception.

20. Au-delà, le texte légal confère avec bonheur une grande importance à ce qui forme le point de départ du régime exceptionnel. L'état d'exception fait l'objet d'une déclaration prise par le Roi à la suite d'un arrêté délibéré en Conseil des ministres après avis d'experts et sur avis du ministre de la Santé publique.

Cet arrêté, d'une durée proportionnelle à la gravité de la crise et maximale de trois mois, est mis en vigueur dès sa publication mais soumis à la discussion

57 Résolution du Parlement européen du 13 novembre 2020, *op. cit.*, § 4.

58 Loi relative aux mesures de police administrative lors d'une situation d'urgence épidémique, *M.B.*, 20 août 2021, p. 90047. Le texte adopté par la séance plénière est identique au texte adopté en deuxième lecture par la commission (Projet de loi du 18 mai 2021 relatif aux mesures de police administrative lors d'une situation d'urgence épidémique, *Doc. parl.*, Ch., 2020-2021, n° 55-1951/009).

59 ... et surtout les autorités aptes à les prendre ou à les contrôler, comme le soulignait le Conseil d'État français (Avis du 21 décembre 2020, *op. cit.*, § 16) : « Dans ce contexte, il apparaît cohérent avec la gradation des situations susceptibles de survenir ainsi qu'avec l'économie générale du projet de loi proposé que la prorogation de l'état de crise sanitaire ne soit pas, à la différence de l'état d'urgence sanitaire, subordonnée à une autorisation du Parlement. »

60 Voy. notre rapport remis en mars 2021 au Parlement, conformément à la demande de sa présidente : « La liste des définitions reprises à l'article 2 contient la définition de la "situation d'urgence épidémique". Cette définition pose un certain nombre de questions tant le texte énumère de conditions cumulatives, dont le flou est évident. L'avant-projet de loi énumère ainsi comme conditions : une "situation spécifique qui touche, effectivement ou potentiellement, un grand nombre de personnes en Belgique et qui affecte leur santé mentale et/ou physique". C'est quoi être "touché" ? Avoir un test P.C.R. positif ne veut pas nécessairement dire qu'on est malade ou contagieux ? Le mot "potentiellement" renvoie à l'avis d'experts. Le même point évoque le risque de surmortalité, sans en faire une condition. Comment évaluer ce risque : en comparaison à quelle année ? Les études récentes démontrent qu'en 2020 il y a eu une surmortalité pour les +85 ans, mais pas pour les autres tranches d'âge, au contraire. Où est donc la limite ? La deuxième condition pointe les conséquences sur la surcharge de certains professionnels ou sur le besoin d'équipements ou de médicaments. Cette deuxième condition renvoie à un devoir de précaution dont il importe de rappeler l'existence aux autorités publiques : ne faut-il pas prévoir, *in tempore* non suspecto, un nombre de lits suffisants pour faire face à ce risque de pandémie ? La troisième condition est relative aux besoins d'une gestion coordonnée (par le fédéral ?) des acteurs compétents. Enfin, la dernière condition n'est reprise que de manière subsidiaire. Elle se réfère à la déclaration par des organes européens ou mondiaux de la situation sanitaire, comme pandémique. Sans doute – et on doit l'en louer – l'avant-projet a souhaité ne pas rendre facile le recours aux mesures d'urgence en restreignant le concept. Il n'empêche que le caractère contestable des éléments de la définition met mal à l'aise. Il énonce des critères à prendre en considération *mais ne dit rien sur qui les appréciera, quelle motivation devra être fournie et qui en fin de compte décidera de l'existence ou non d'une "situation d'urgence épidémique". Ce sont ces points qui sont importants.* » (nous soulignons)

parlementaire dans des délais rapprochés. Il est confirmé par une loi prise dans un délai rapproché et, en cas de non-confirmation, pourrait voir cesser ses effets. On ajoute que la même procédure doit être suivie et que les mêmes conditions s'appliquent en cas de prolongation de durée.

La formule belge est acceptable même si le Sénat français ne l'a pas jugé comme tel et a obligé le gouvernement français à retirer son texte[61]. En particulier, ne fallait-il pas que les limitations aux libertés soient soumises au Parlement selon une procédure rapide ? Le Parlement belge eût pu faire preuve de plus d'inventivité pour définir une procédure rapide d'instruction de telles mesures, en particulier par la création d'une commission *ad hoc* de suivi des mesures d'exception. Cette commission aurait pu se saisir de valider certaines dispositions jugées plus critiques par elle dans le cadre d'un dialogue qu'elle aurait entamé avec le gouvernement.

21. Parmi ces dispositions critiques figurent certes celles relatives à la création et la mise en œuvre de traitements ou systèmes d'information qui, outre qu'ils peuvent faire l'objet de dispositions en soi, bien souvent accompagnent les mesures de police administrative afin de leur donner pleine efficacité. On ne prendra comme simple exemple que l'utilisation de drones pour contrôler les rassemblements et vérifier le respect des mesures sanitaires[62].

Ces dispositions faisaient l'objet d'articles spécifiques dans les premières moutures du projet de loi. Le texte distinguait en effet les mesures qu'il qualifiait de police administrative (article 4, § 1er) et celles relatives à la création de traitements (article 6, § 1er).

On note que cette distinction posait déjà problème dans la mesure où nombre de règles de police administrative conduisent à la création de traitements impliqués par les mesures de police administrative ou destinés à permettre leur

61 Et ce, nonobstant la décision du Conseil d'État français favorable sur ce point au texte du gouvernement dont le contenu sur les questions de la déclaration de l'état d'urgence et des compétences déléguées à l'exécutif ressemblait à celui voté en Belgique : « Le Conseil d'État rappelle que la Constitution n'exclut pas la possibilité pour le législateur de prévoir, à cette fin, un régime d'état d'urgence sanitaire (Conseil constitutionnel, décision n° 2020-800 DC du 11 mai 2020, paragr. 17 ; décision n° 2020-808 DC du 13 novembre 2020, paragr. 5), ni celle de créer, pour des situations de moindre intensité justifiant l'adoption en urgence de mesures d'une nature en partie comparable, un état de crise sanitaire, pourvu que le législateur, dans l'un comme dans l'autre de ces deux cadres juridiques, assure la conciliation entre l'objectif de valeur constitutionnelle de protection de la santé et le respect des droits et libertés reconnus à tous ceux qui résident sur le territoire de la République (Voir notamment pour un régime transitoire de sortie de l'état d'urgence sanitaire, Conseil constitutionnel, décision n° 2020-808 DC du 13 novembre2020, paragr. 12). [...] La déclaration de l'état de crise sanitaire par décret, accompagnée de la publication des données scientifiques qui la justifient, sa prorogation au-delà de deux mois par décret en conseil des ministres après avis public du Haut Conseil de la santé publique, sa fin à tout moment par décret après avis du même organisme, constituent, sous le contrôle du juge, des garanties permettant de s'assurer que les conditions légales d'applicabilité de ce régime exceptionnel sont et restent réunies. » (C.E. fr., Avis du 21 décembre 2020, *op. cit.*, §§ 12 et 15.)

62 À ce sujet, voy. le contenu de la note de bas de page n° 25.

effectivité. L'article 6, § 3, du projet le reconnaissait implicitement lorsqu'il évoquait les cas où « les mesures prises en application de l'article 4 § 1er, [...] [soit les mesures de police administrative] nécessitent la création d'une banque de données »[63].

On sait que ces dispositions furent l'objet de critiques par l'autorité belge de protection des données qui soulignait que les dispositions du projet de loi ne rencontraient pas les exigences légales de la création de tout traitement, à savoir, conformément à l'article 6.3 du R.G.P.D., la nécessité d'une base légale prévisible contenant les éléments essentiels du traitement.

L'avis s'exprimait ainsi :

> « En vertu de l'article 6.3 du R.GPD, lu conjointement avec l'article 22 de la Constitution et l'article 8 de la C.E.D.H., il doit s'agir d'une norme légale formelle (loi, décret ou ordonnance, ci-après aussi appelée "la loi") [...] définissant les éléments essentiels du traitement accompagnant l'ingérence publique [...]. Dans la mesure où les traitements de données à caractère personnel accompagnant l'ingérence publique représentent une ingérence importante dans les droits et libertés des personnes concernées, ce qui semble pouvoir être supposé en l'espèce malgré l'absence de description des traitements de données envisagés, la loi doit décrire clairement et précisément les éléments essentiels suivants : 1. les finalités déterminées, explicites et légitimes des traitements de données à caractère personnel (voir chapitre IV) ; 2. le ou les responsables de chaque traitement de données à caractère personnel (voir chapitre III) ; 3. les (catégories de) données à caractère personnel qui seront traitées (et qui doivent être pertinentes et non excessives) (voir chapitre II) ; 4. les catégories de personnes concernées dont les données à caractère personnel seront traitées (voir chapitre I) ; 5. les catégories de destinataires des données à caractère personnel (ainsi que les raisons pour lesquelles ils recevront les données et les usages qu'ils en feront) (voir chapitre V) ; 6. le délai de conservation maximal des données à caractère personnel enregistrées »[64].

22. La critique de l'A.P.D. a été relayée par de nombreux parlementaires et journalistes. Cette critique, fondée sur l'exigence d'une loi prévisible, entraîna le retrait des dispositions par le gouvernement. Nous pensons cependant qu'un tel retrait complet était une erreur du fait de l'impossibilité de souvent distinguer les mesures de police administrative des moyens technologiques pris pour

63 À cet égard, une proposition de loi de la N-VA (Proposition de loi relative à la constatation d'une situation de crise déposée par M. Peter De Roover et consorts, Ch., 2020-2021, séance du 25 février 2021, n° 55-1814/001) mettait sur le même pied toute mesure « ayant un impact sur la liberté des citoyens » et paraissait rencontrer le problème. On ajoute que, suivant cette proposition, c'est à la loi d'établir de telles restrictions, « selon une procédure d'urgence à déterminer par la Chambre des représentants ». Sans doute, on eût pu attendre des auteurs de cette proposition, qu'ils fassent des propositions concrètes à cet égard. S'agit-il par exemple de donner à une commission le soin de se prononcer au nom de la Chambre ? S'agit-il de mettre en place une procédure d'acceptation des propositions ?

64 A.P.D., Avis n° 24/2021 du 2 mars 2021 sur l'avant-projet de loi relatif aux mesures de police administrative lors d'une situation d'urgence pandémique.

les faire respecter. Par ailleurs, le texte du R.G.P.D., hormis une description claire de la finalité et la motivation de la proportionnalité du traitement, n'impose pas que la base juridique contienne les autres éléments du traitement mais laisse l'appréciation de la présence de ces éléments à l'auteur de la disposition réglementaire[65]. Enfin, il eût été difficile, voire impossible, au regard de la diversité des traitements liés à la lutte contre la pandémie de les lister tous *a priori* et d'envisager leurs éléments essentiels. Enfin, il eût été intéressant de reprendre dans la loi quelques principes de base en ce qui concerne la création de ces traitements, comme le faisait le défunt projet de loi français qui y consacrait toute une section dans le chapitre I du titre III[66]. À l'instar des dispositions françaises, quelques points auraient pu être l'objet de dispositions dans le texte de loi. Ainsi, la question de la durée des traitements légalement limitée à la durée de la pandémie[67] sauf exception dûment motivée lors de l'évaluation finale des mesures prises tout au long de l'état d'urgence. On note que cette évaluation est prévue par la loi belge « pandémie »[68].

Il eût été utile que ce rapport porte spécifiquement sur la création des traitements et que le Parlement soit appelé à se prononcer sur leur maintien exceptionnel. Ainsi, la question du secret médical et donc de l'accès aux bases de données contenant de telles informations aurait pu faire l'objet d'une disposition rappelant l'interdiction de principe de l'accès aux personnes non couvertes par le secret médical et prévoyant la procédure qui, le cas échéant, devrait être suivie pour permettre un tel accès à des personnes non couvertes par le secret[69].

Aussi, il eût été envisageable de rappeler les facettes multiples des principes de minimisation et de proportionnalité des traitements affirmés par le R.G.P.D. mais précisés par notre autorité de protection des données dans nombre d'avis, et en particulier ceux consacrés au Covid, l'état d'exception ne justifiant pas la création de n'importe quel traitement. Comme le rappelle le récent avis du Centre de connaissances de l'A.P.D. les conditions suivantes restent à démontrer[70] :

> « Premièrement, que le traitement de données permette effectivement d'atteindre l'objectif poursuivi. Il faut donc démontrer, sur base d'éléments factuels et objectifs, *l'efficacité* du traitement de données à caractère personnel pour atteindre l'objectif recherché ; Deuxièmement, que ce traitement de données à caractère personnel constitue *la mesure la moins intrusive* au regard du droit à la protection de la vie privée. Cela signifie que s'il est possible d'atteindre l'objectif recherché au moyen d'une mesure moins intrusive pour le droit au respect de la vie privée ou le droit à la protection des données à caractère personnel, le traitement de données initialement envisagé ne pourra pas être mis en place[71].

65 Article 6.3 du R.G.P.D. : « Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par : a) le droit de l'Union ; ou b) le droit de l'État membre auquel le responsable du traitement est soumis. Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. *Cette base juridique peut contenir* des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement ; les types de données qui font l'objet du traitement ; les personnes concernées ; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ; la limitation des finalités ; les durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi » (nous soulignons). Certes, le caractère obligatoire de telles mentions pourrait facilement se justifier par la nature des données traitées, par le fait de la couverture de l'ensemble de la population et, surtout, par le caractère exceptionnel des mesures prises.

66 C.E. fr., Avis du 21 décembre 2020, *op. cit.*, § 1 : « L'article 6, introduit dans un chapitre I^er^ *sexies* de ce même titre III des dispositions reprenant les règles existantes applicables au système d'identification unique des victimes (SI-VIC), et créant un nouveau cadre pour les autres systèmes d'informations susceptibles d'être mis en œuvre dans certaines situations sanitaires exceptionnelles. »

67 *Ibid.*, § 38 : « Pour garantir le respect de ces principes, le Conseil d'État recommande de prévoir un délai de six mois à compter de la publication de la loi, dans lequel devra intervenir le décret en Conseil d'État fixant le terme de la durée de mise en œuvre des traitements. En l'absence d'intervention d'un tel décret, les traitements de données ne seront plus autorisés à compter de l'expiration de ce délai. »

68 Article 10 : « Dans un délai de trois mois après la fin de la pandémie de coronavirus Covid-19, le gouvernement transmet à la Chambre des représentants un rapport d'évaluation portant sur les objectifs poursuivis dans le cadre du respect des droits fondamentaux afin de vérifier si la présente loi ne doit pas être abrogée, complétée, modifiée ou remplacée. » Il est regrettable que ce rapport ait pour seul objectif la question de la modification de la loi et non l'analyse des mesures prises.

69 Voy. sur ce point C.E. fr., Avis du 21 décembre 2020, *op. cit.*, § 34, sur les dispositions à ce sujet reprises dans le projet de loi français.

70 Il s'agit de ce que Sébastien Van Drooghenbroeck (*La proportionnalité dans le droit de la Convention européenne des droits de l'homme – Prendre l'idée simple au sérieux*, Bruxelles, Bruylant, 2001, pp. 31-38) appelle le triple test. Du même auteur, appliqué aux mesures anti-Covid, « Conservation des données à caractère personnel, Accès par les autorités, Droit au respect de la vie privée, Non-violation », *Obs. Bxl.*, 2020/3, n° 121, pp. 61-62. L'exigence de ce triple test est rappelée dans nombre des avis de l'A.P.D. à propos des mesures anti-Covid (voy. notamment A.P.D., avis n° *34/2020, 28 avril 2020*, Demande d'avis concernant un avant-projet d'arrêté royal n° XXX portant exécution de l'article 5, § 1, 1°, de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus Covid-19 (II), dans le cadre de l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus Covid-19 parmi la population (CO-A-2020-041)).

71 C'est en ce sens que se conçoit la préférence donnée à l'anonymisation des données de localisation dans le cadre de *tracing* automatique : « En ce qui concerne l'utilisation des données de localisation, l'E.D.P.B. insiste sur le fait qu'il faudrait toujours privilégier le traitement de données anonymisées plutôt que le traitement de données à caractère personnel. L'anonymisation fait référence à l'utilisation d'un ensemble de techniques visant à retirer la possibilité d'associer, moyennant un "effort raisonnable", les données à une personne physique identifiée ou identifiable. Ce "critère du caractère raisonnable" doit tenir compte aussi bien d'éléments objectifs (le temps, les moyens techniques) que d'éléments contextuels pouvant varier au cas par cas (rareté d'un phénomène, compte tenu de facteurs tels que la densité de la population concernée ou encore la nature et le volume des données). Si les données ne satisfont pas à ce critère, cela signifie qu'elles n'ont pas été anonymisées et donc qu'elles relèvent toujours du R.G.P.D. » (Comité européen de la protection des données (E.D.P.B.), « Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de Covid-19 », adoptées le 21 avril 2020, §§ 14 et 15). L'application de ces exigences a nourri toute la discussion dans nombre de nos pays du choix entre le protocole DP-3T (*Decentralized Privacy Preserving Proximity Tracing*), choisi par nombre de pays européens (Belgique, Allemagne, Italie, Portugal, etc.) et le protocole concurrent Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), choisi par la France pour son application TousAntiCovid. Les deux utilisent la technologie Bluetooth Low Energy pour suivre et enre-

> *Il faut, à cette fin, détailler et être en mesure de démontrer, à l'aide d'éléments de preuves factuels et objectifs, les raisons pour lesquelles les autres mesures moins intrusives ne sont pas suffisantes pour atteindre l'objectif recherché*»[72].

Si la nécessité du traitement de données à caractère personnel est démontrée, il faut encore démontrer que celui-ci est *proportionné (au sens strict)* à l'objectif qu'il poursuit, c'est-à-dire qu'il faut démontrer qu'il existe *un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées*. En d'autres termes, il faut qu'il y ait un équilibre entre l'ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel et l'objectif que poursuit – et permet effectivement d'atteindre – ce traitement.

Les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées. À nouveau, il faut être en mesure de démontrer que cette analyse a bien été réalisée avant la mise en œuvre du traitement. Le rappel légal de ces directives d'interprétation des principes de proportionnalité et de minimisation aurait été utile pour guider les personnes qui conçoivent les différents traitements qu'ils souhaitent mettre en place et qui doivent être l'objet d'une procédure respectant le principe de légalité.

La loi «pandémie» aurait pu exiger que tout traitement créé dans le cadre de la lutte anti-Covid fasse l'objet d'un *Privacy Impact Assessment*, suivant les prescrits de l'article 35 et suivants du R.G.P.D. et, au-delà, réclamer qu'une procédure de participation de représentants des corps médicaux, voire d'associations de libertés civiles, soit suivie.

Enfin, toujours dans le même esprit, il eût été utile de rappeler le principe affirmé par l'E.D.P.B. et le Conseil de l'Europe:

> «De manière générale, l'E.D.P.B. estime que les données et les technologies utilisées pour aider à lutter contre la Covid-19 devraient être employées pour outiller les personnes, plutôt que pour les contrôler, les stigmatiser ou les réprimer. En outre, si les données et les technologies peuvent être des outils importants, elles présentent des limites intrinsèques et peuvent seulement accroître l'efficacité d'autres mesures de santé publique. Les principes généraux d'efficacité, de nécessité et de proportionnalité doivent guider les mesures adoptées par les États membres [...]»[73].

gistrer sur le système installé sur nos mobiles nos rencontres avec d'autres utilisateurs. Les protocoles diffèrent dans leur mécanisme de déclaration. PEPP-PT oblige les clients à télécharger les journaux de contact vers un serveur de rapports central. Avec le DP-3T, au contraire, le serveur central de rapports n'a jamais accès aux journaux de contact et n'est pas responsable du traitement et de l'information des clients de contact et apparaît donc comme offrant une meilleure garantie de protection pour nos données et l'inscrit dans le design du système lui-même.

72 A.P.D., avis n° 124/2021, *op. cit.*, §§ 41 et 42 (nous soulignons).

73 E.D.P.B., «Lignes directrices 4/2020», *op. cit.*, § 4. Voy. également de la part de l'E.D.P.B., «Statement on the processing of personal data in the context of the Covid-19 outbreak», 20 mars 2020, https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_fr. Voy. aussi la déclaration de la Présidente du comité consultatif de la Convention n° 108 et

Mettre les technologies au service des personnes et de leur capacité à décider et non en faire un outil de contrôle est certes le message adressé par les autorités de protection des données. Si l'urgence sanitaire, environnementale ou la menace grave à la sécurité publique peuvent justifier le déploiement de nouveaux outils technologiques, il faut à l'égard de ces derniers redoubler de vigilance pour s'assurer de leur légalité et proportionnalité.

23. À ces conclusions tirées des considérations relatives à la protection de nos données à caractère personnel, s'en ajoutent d'autres relatives à d'autres libertés, voire à d'autres enjeux de justice sociale et de fonctionnement de nos sociétés. Notre liberté d'expression n'est-elle pas remise en cause par la volonté des États de contrôler en ces périodes de pandémie ce qui est qualifié parfois de manière abusive de désinformation? Ce contrôle recourt parfois à des mesures technologiques, comme l'utilisation par les plateformes de systèmes d'intelligence artificielle capables de repérer des messages dits «complotistes» ou des informations tendancieuses infirmant le discours officiel[74]. Les atteintes au droit à un procès équitable du fait de l'imposition de mesures technologiques ont fait l'objet de nombreuses discussions que nous ne détaillerons pas ici[75]. Notons en France, l'ordonnance du 25 mars 2020[76] prise en exécution de la loi du 23 mars 2020 créant l'«état d'urgence sanitaire» et dès lors permettant, malgré les protestations du Conseil de l'ordre des avocats[77], aux juges civils et commerciaux, de trancher les affaires sans audience ou par audience «numérique».

Pire, l'ordonnance du même jour dite Ordonnance 304, relative cette fois à la justice pénale, adapte les règles de procédure «afin de permettre la continuité de l'activité des juridictions pénales essentielle au maintien de l'ordre public»[78],

du D.P.O. du Conseil de l'Europe, 30 mars 2020, www.coe.int/fr/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter. Cette déclaration a été complétée par les mêmes personnes, au vu des questions nouvelles soulevées par le déconfinement: www.coe.int/en/web/data-protection/contact-tracing-apps.

74 Sur ce point, nous renvoyons à notre article à paraître dans les Actes du colloque de Lille du 4 février 2021 et l'analyse y proposée des textes européens, en particulier de la déclaration du 21 mars 2021 du Comité d'experts du Conseil de l'Europe sur l'environnement des médias et la réforme du Conseil de l'Europe: «la situation de crise ne doit pas servir de prétexte pour restreindre l'accès du public à l'information. Les États ne devraient pas non plus introduire de restrictions à la liberté des médias au-delà des limites autorisées par l'article 10 de la Convention européenne des droits de l'homme.»

75 Sur la situation en Belgique, voy. le tour d'horizon partiel proposé par J. Sohier, «Réflexions sur le fonctionnement des juridictions: Conseil d'État et Cour constitutionnelle», *in* S. Parsa et M. Uyttendaele (coord.), *La pandémie de Covid-19 face au droit*, *op. cit.*, pp. 219 et s.; O. Nederlandt et D. Paci, «La prison face au Covid-19: des mesures déséquilibrées au détriment des personnes détenues et/ou condamnées», *J.T.*, numéro spécial coronavirus, 2020/18, n° 6814, pp. 51 et s.

76 Ordonnance n° 2020-303 du 25 mars 2020 «portant adaptation de règles de procédure pénale sur le fondement de la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de Covid-19». Sur ces mesures, voy. entre autres, à propos des juridictions civiles et commerciales, E. Brochier et M. Brochier, «Attention à la suppression des audiences», *Recueil Dalloz*, 4 juin 2020, pp. 1118 et s.

77 Le Conseil d'État a écarté, par une décision en référé du 10 avril 2020, la demande visant à faire annuler l'ordonnance.

78 Ordonnance n° 2020-304 du 25 mars 2020 portant adaptation des règles applicables aux juridictions judiciaires statuant en matière non pénale et aux contrats de syndic de propriétés. Sur cette ordonnance,

ce qui signifie la fermeture de différents tribunaux, la possibilité de regrouper les affaires, l'allégement du formalisme de la garde, la dématérialisation des procédures et des audiences, la généralisation du juge unique, la prolongation de plein droit des mesures de détention provisoire, la simplification des échanges entre parties au risque de non-respect du contradictoire, etc. Comme le note Sébastien Pellé, « cette urgence-là [celle sanitaire], celle de la nécessité, emporte bien des raisonnements et des principes sur son passage. Elle prescrit ce qui d'ordinaire serait proscrit »[79]. Ou, comme le démontre Denis Salas à propos des mêmes mesures, l'État de droit cède à l'état de puissance[80].

En ce qui concerne la justice sociale, il faut être conscient des effets discriminatoires que peuvent avoir le choix de telle ou telle mesure technologique. On sait combien, pour certaines catégories de population, l'illectronisme les tient à l'écart de toute utilisation d'applications ou d'informations qui nécessitent l'accès, voire le maniement, de la technologie[81]. Demain, il est à craindre que les bases de données sur la vaccination ne soient un outil d'exclusion de certains lieux pour une catégorie de population qui refuse la vaccination pour des motifs bons ou mauvais – il n'appartient pas à l'autorité d'en discuter le bien-fondé.

Enfin, il faut bien constater que les mesures prises ont accéléré le développement du numérique dans notre quotidien :

> « Les pratiques numériques en période de confinement ont conduit à un glissement des frontières entre nos différentes sphères sociales (vie domestique, vie privée, vie professionnelle). Les pratiques liées au télétravail ont par exemple fait entrer le domicile des individus dans leur sphère professionnelle. Cette recomposition des frontières sociales a donné lieu à un certain nombre de troubles et a pu faire l'objet de conflits ou de négociations, entre les individus et les organisations, qui conduisent à questionner les valeurs accordées à la vie privée. Les individus ont mis en place des stratégies et développé des compétences pour gérer les frontières entre leurs sphères sociales, du refus de l'usage de la webcam à la mise en scène d'un arrière-plan. L'intensification des pratiques numériques laisse à penser que le confinement a pu être un moment de conversion numérique, entendu comme une période qui conduit à interroger la place du numérique dans nos vies. »[82]

voy. le commentaire critique de S. Pellé, « La justice pénale à l'heure du coronavirus : l'urgence ou le miroir de notre procédure pénale », *Recueil Dalloz*, 16 avril 2020, pp. 777 et s.

79 S. Pellé, *ibid.*

80 D. Salas, « Que cache l'expression juridique "de plein droit" ? », *Dalloz Actualité*, 17 avril 2020. Du même auteur, mais cette fois à propos des mesures antiterroristes, voy. « La banalisation dangereuse de l'état d'urgence », *Revue Études*, 2016, n° 3, pp. 29 à 40.

81 En France, on considère que presque un cinquième de la population n'a pas accès ou ne sait pas utiliser un smartphone. On ajoute que cette part de la population est largement constituée de personnes âgées ainsi que de personnes vulnérables sur un plan économique, soit les personnes les plus à risque. On ajoute la nécessité de prendre en considération les populations étrangères souvent mal informées vu l'obstacle de la langue.

82 C.N.I.L., « Point d'étape sur les activités de la C.N.I.L. dans le contexte de la Covid-19 », 12 novembre 2020, www.cnil.fr/sites/default/files/atoms/files/rapport_cnil_point-etape_covid-19.pdf.

La loi « pandémie » ne consacre pas l'existence pourtant nécessaire des débats sociétaux que soulève l'adoption parfois précipitée d'outils technologiques. Cette adoption aurait dû faire l'objet d'une obligation d'évaluation préalable dès la conception de tels systèmes d'information participative, c'est-à-dire réunissant les représentants des divers intérêts en cause (secteur hospitalier, associations de défense des libertés, entreprises, etc.) et multidisciplinaire, c'est-à-dire croisant des réflexions de psychologues, de médecins, de juristes, de sociologues, etc. Surtout, devrait être affirmée légalement la nécessité d'une évaluation globale de tels systèmes, souvent construits à la hâte, au terme des périodes de crise.

L'inertie des populations et des gouvernants, l'utilité passée vantée et la crainte de voir revenir les temps de misère risquent de maintenir en place ces instruments de contrôle et de surveillance auxquels chacun s'est habitué. À défaut, l'exception devient la règle. Il est donc utile que soit affirmé le principe des limites de leur validité et de leur légitimité au seul temps de crise et qu'un examen nouveau de proportionnalité soit imposé à l'issue de la crise : en temps de « paix » sanitaire, de sécurité nationale, pour reprendre les deux domaines étudiés, ces constructions sont-elles toujours nécessaires ?

Cette évaluation plus vaste que celle prônée par le R.G.P.D.[83], centrée sur les seules préoccupations individualistes liées à la protection des données, doit envisager l'ensemble de nos libertés, les risques de discrimination ou d'atteinte à la justice sociale et, enfin, l'impact sur le fonctionnement de nos états démocratiques[84] doit associer toutes les parties intéressées par les débats en jeu dans cette informatisation de notre société liée à ces états d'exception, y compris les représentants du corps médical et ceux de la société civile à travers les associations de libertés civiles, le centre de l'égalité des chances… sans oublier les prérogatives de notre autorité de protection des données. Enfin, il nous semblerait important que cette évaluation fasse l'objet d'un rapport spécifique et *in fine* soit l'objet d'une discussion et, le cas échéant, de décisions parlementaires.

83 Nous nous référons ici à la procédure imposée par les articles 35 et suivants du R.G.P.D. en cas de traitements dits à risque élevé.

84 Certains se risquent déjà à cette évaluation, alors même que la pandémie ne nous a pas encore quittés. Ainsi, Vincent Calay parle d'un « coup d'État des data » durant la pandémie : « Le jour où sera actée la fin de la pandémie de Covid-19, certains gouvernements entreprendront-ils de réaliser une évaluation des outils de gouvernance mis en place pour y faire face ? Comme nous l'avons montré dans ce Cahier, la gestion de la pandémie a bénéficié d'un jeu de technologies issues du monde de la surveillance et de la sûreté des États. Au nom de la protection de la santé publique et de l'état d'urgence dans lequel se sont retrouvées les économies européennes, les gouvernements et les administrations ont mis en place des systèmes de tracing, une logistique hospitalière et, enfin, des politiques de vaccination basées sur des droits étendus d'ingérence des organismes de santé dans la vie privée des citoyens. Des données personnelles de santé ont été exploitées par les administrations des États et/ou par des opérateurs privés pour développer des outils d'aide à la décision performants. En outre, les politiques de confinement des populations ont bénéficié d'outils de surveillance visant à réprimer les écarts de conduite face aux suspensions des libertés publiques fondamentales décrétées par les gouvernements (suspension du droit au travail, à l'éducation, aux rassemblements…) » (V. Calay, « L'empire des logiciels, menace pour les démocraties ? », *op. cit.*, p. 39).

III. Le numérique, instrument insidieux de l'état d'exception

24. La politique menée en Belgique par nos gouvernements, parfois sous la pression d'acteurs tant internes à l'administration (la Banque Carrefour de la sécurité sociale a ainsi été montrée du doigt à plusieurs reprises) qu'externes (acteurs privés fournisseurs de « solutions »), « semble avoir permis, malgré les contestations et controverses autour de la protection des données personnelles et, par extension, des libertés fondamentales, l'émergence de formes de datacraties, c'est-à-dire de régimes politiques dont l'objectif est de gouverner des populations caractérisées en fonction de profils et des risques qu'ils peuvent présenter », concluait le récent Cahier de prospective de l'IWEPS déjà cité[85].

Le propos du Cahier rejoint la réflexion d'auteurs récents et sert de point de départ à la réflexion, objet de cette troisième partie. Leur propos est de montrer que le numérique profite d'une crise comme la pandémie et contribue au niveau public mais surtout au niveau privé à créer insidieusement et de manière permanente un « état d'exception », qui menace notre démocratie et nos États de droit si nous ne prenons pas les mesures adéquates pour veiller à leur respect. Vincent Calay, auteur du Cahier de prospective, aborde le sujet comme suit :

> « Le rôle joué par les technologies informatiques durant la pandémie a fait la fortune des grandes multinationales de l'informatique, les GAFAM (Google, Amazon, Facebook, Microsoft). Celles-ci ont renforcé leur position dominante durant l'année 2020, fournissant des services adaptés aux gouvernements pour la gestion de la pandémie et proposant aux citoyens une série d'outils leur permettant de poursuivre leurs activités dans le cadre du confinement. Les GAFAM font partie des acteurs économiques qui ont bénéficié de la pandémie en enregistrant en 2020, une croissance à deux chiffres : Amazon a vu son chiffre d'affaires croître de 38 %, Facebook de 22 %, Microsoft de 18 %, Google de 13 % et Apple de 10 %. Ces évolutions interrogent sur le rôle joué par les technologies informatiques dans la vie quotidienne autant que dans des décisions politiques aux répercussions importantes sur la santé et sur les libertés des citoyennes et des citoyens. Elles questionnent sur les futurs dont elles pourraient être annonciatrices. Constituent-elles des signaux faibles marquant l'émergence de nouvelles tendances ? Plus concrètement : forment-elles des points de bifurcation qui engagent les démocraties occidentales vers des régimes autoritaires aux pouvoirs exécutifs forts et aux décisions fondées sur les pouvoirs de l'intelligence artificielle ? Ces évolutions semblent, en effet, orienter vers un futur où les démocraties sont confrontées à des problématiques extrêmement complexes – comme une pandémie ou le réchauffement climatique – et à la nécessité de décisions rapides, au motif de catastrophes imminentes. Les expérimentations réalisées durant la pandémie par les gouvernements combinant une action rapide à la légalité faible et des outils informatiques brassant les données personnelles des citoyens feront-elles jurisprudence ? Cette approche ne serait-elle pas également renforcée par l'empire économique développé par les multinationales dominant l'économie numérique ? »[86]

25. L'analyse menée par certains auteurs de la « datacratie »[87] ou de la « gouvernementalité algorithmique »[88] constate en effet la disparition de l'espace public de discussions et la montée en puissance du pouvoir des acteurs tant privés que publics qui collectent et gèrent ces données et leur donnent sens par la puissance du numérique, en particulier toujours plus les technologies de l'intelligence artificielle. Cette intelligence prétend, à partir d'algorithmes au fonctionnement plus ou moins opaque, représenter le réel et en induire le futur, mettant sa puissance au service de ses utilisateurs, les entreprises qui les mettent en œuvre d'abord, les administrations ensuite, les citoyens, le cas échéant. Comment ne pas suivre aveuglément cette vérité sortie des ordinateurs, quitte à la légitimer par des lois qui en organisent la production à travers la création de bases de données, d'instruments de collecte de l'information nécessaire, le tout en confiant à des organismes au fonctionnement obscur le soin de dire cette vérité ? Sans doute notera-t-on que cette intelligence s'appuie sur un « réductionisme » de la personne humaine, considérée à travers son ou plutôt ses profils[89]. L'urgence de la lutte contre le terrorisme tout comme l'urgence de protéger la santé des citoyens justifient d'autant plus le recours aux solutions offertes par les technologies du numérique et leur vérité. Il s'agit de s'en remettre aux vertus des multiples traitements construits à la hâte pour donner aux citoyens l'illusion réconfortante de la présence du *Big Brother*. Ainsi,

85 V. Calay, *ibid.*, p. 40.

86 *Ibid.*, p. 6.

87 D. Cardon, « Le pouvoir des algorithmes », *Pouvoirs*, 2018, n° 164, pp. 63-73 (l'ensemble de ce numéro de la revue est consacré à la datacratie) ; A. Blandin, « La gouvernance du monde numérique : que fait l'Europe ? », *Cahiers français*, n° 415, mai-juin 2020, pp. 50-56.

88 A. Supiot, *La gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Paris, Fayard, 2015 ; A. Rouvroy, « *Adopt AI, think later.* La méthode Coué au secours de l'intelligence artificielle », *Internet Actu*, 2 mars 2020, www.internetactu.net/2020/03/02/adopt-ai-think-later-la-methode-coue-au-secours-de-lintelligence-artificielle/ ; A. Rouvroy et Th. Berns, « Le nouveau pouvoir statistique ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps "numériques"... », *Multitudes*, 2019, n° 40, pp. 88-103 ; A. Rouvroy et Th. Berns, « Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation ? », *Réseaux*, 2013, n° 177, pp. 163-196.

89 Sur ce point, voy. nos réflexions *in Éthique et droits de l'Homme dans notre société du numérique*, coll. Mémoires de l'académie, Bruxelles, Académie royale de Belgique, 2020, n^{os} 40 et s., pp. 67 et s. Comme le soulignait récemment Antoinette Rouvroy (« Les algorithmes : entre tyrannie du "réel" et exigences de justice », version complète d'un entretien à paraître – dans une version fortement abrégée – dans *Binaire* (blog du journal *Le Monde*), publié dans academia.edu) : « Dans ce que j'ai appelé la "gouvernementalité algorithmique", le pouvoir ne s'exerce plus sur les individus à travers la connaissance de "qui" ils sont singulièrement, à travers la confession de leurs motivations psychologiques, ni en s'appuyant sur leurs capacités d'entendement et de volonté pour les inciter à conformer leurs comportements à ce qui est attendu. Ce qui intéresse les bureaucraties privées et publiques qui nous "gouvernent", c'est de détecter automatiquement – sans plus avoir pour cela à nous rencontrer ni à nous interroger, ni à nous entendre – nos "potentialités", nos propensions, ce que nous pourrions désirer, ce que nous serions capables de commettre, propensions et potentialités dont nous ne sommes nous-mêmes, le plus souvent, pas pleinement conscients. Une propension, un risque, une potentialité, ce n'est encore personne. »

comme le note Alain Supiot, se dessine un « gouvernement par les nombres »[90], c'est-à-dire par la statistique qui prétend rendre compte, mieux que le contact et le dialogue avec les personnes, de la réalité[91].

26. Au-delà, on note, à la suite de Baptiste Rappin, que la cybernétique est « l'instrument privilégié » du gouvernement pour juguler les crises : « On ne peut alors qu'être frappé par la proximité qui s'établit entre le projet cybernétique, celui d'un gouvernement de et par l'exception, et la "stratégie du choc" »[92]. L'auteur se réfère en la matière aux réflexions de Naomi Klein relatives à ce que cette dernière appelle la « stratégie du choc ». « Voici [explique l'auteure] comment fonctionne la stratégie du choc : le désastre déclencheur – le coup d'État, l'attentat terroriste, l'effondrement des marchés, la guerre, le tsunami, l'ouragan – plonge la population dans un état de choc collectif. Le sifflement des bombes, les échos de la terreur et les vents rugissants "assouplissent" les sociétés, un peu comme la musique tonitruante et les coups dans les prisons où se pratique la torture. À l'instar du prisonnier terrorisé qui donne le nom de ses camarades et renie sa foi, les sociétés en état de choc abandonnent des droits que, dans d'autres circonstances, elles auraient défendu jalousement. »[93]

Cette dernière réflexion relative à la stratégie du choc amplifie encore la crainte de voir l'instrument technologique, au départ sans doute imposé, être adopté par les citoyens comme l'instrument salvateur en ces périodes de crise qui constituent le fondement à la base des états d'exception.

Comme le note très justement, le Centre de connaissances de l'A.P.D. à propos du projet de l'accord de coopération relative au passeport sanitaire, appelé en Belgique le Covid Safe Ticket, « il convient donc de *tracer une frontière raisonnable entre ce qui relève de la liberté et de la responsabilité individuelles et ce qui peut relever du contrôle social*, en s'attachant à n'imposer des restrictions aux libertés et droits fondamentaux que si cela s'avère strictement nécessaire et proportionné à l'objectif d'intérêt général poursuivi. Dans cette évaluation, *l'Autorité insiste sur la nécessité d'être particulièrement attentif au risque réel de créer un "phénomène d'accoutumance"*, ce qui pourrait nous amener à accepter, dans le futur, que l'accès à certains lieux (y compris des lieux de la vie quotidienne) soit soumis à la divulgation de la preuve que la personne concernée n'est pas porteuse de maladies infectieuses (autre que le Covid) ou qu'elle n'est pas atteinte d'autres pathologies. L'Autorité attire l'attention sur l'importance d'éviter que la solution mise en place pour autoriser l'accès à certains lieux ou à certains événements

90 A. Supiot, *La gouvernance par les nombres*, *op. cit.*

91 À cet égard, les conclusions de Fr. Ost, « Nécessité fait loi ? La santé n'a pas de prix ? Ce que le Covid fait au droit », *op. cit.*, p. 32.

92 B. Rappin, « Algorithme, management et crise », *op. cit.*, n° 18.

93 *Ibid.*, citant N. Klein, *La stratégie du choc. La montée d'un capitalisme du désastre*, trad. L. Saint-Martin et P. Gagné, Montréal, Leméac/Actes Sud « Babel », 2008, p. 31.

entraîne un glissement vers [nous ajouterions volontiers : l'acceptation d'] une société de surveillance. »[94]

Ainsi, sans le dire, s'installe de manière durable l'état d'exception à travers la mise sur pied en temps de crise d'outils technologiques. Si l'utilité, même contestable, de la création et du fonctionnement de ces outils pouvait se justifier en un moment de crise, il est à craindre leur maintien au nom des services rendus, des intérêts de ceux qui les gèrent ou y contribuent, des investissements y consentis et de l'habitude de leur présence prise par des citoyens devenus dociles. Si l'état d'exception explique aisément le recours au numérique, à son tour, le numérique s'empare, avec *in fine* la complicité inconsciente des populations, de l'état d'exception pour rendre cette exception, permanente.

27. Au-delà de la crise pandémique, ce que le numérique fait au droit, pour paraphraser la formule heureuse de François Ost[95], c'est un renforcement de l'état de non-droit qui s'invite à travers la consécration de l'état d'exception. Comme le note Vincent Calay, « au fil du Cahier, nous avons tenté de mettre en exergue certains enjeux clés associés à cet empire des logiciels en examinant les controverses entourant la gestion informatique de la pandémie et en revisitant l'histoire des logiciels informatiques. Nous les avons synthétisés dans cinq défis informatiques pour les démocraties : la liberté technique de capture et de traitement des informations qui présente le risque d'une perte de contrôle sur les données personnelles ; l'emprise de groupes industriels marchands de taille mondiale sur les logiciels et la privatisation du stockage de données publiques qui rendent les États et les démocraties contemporains dépendants des stratégies commerciales d'un oligopole[96] ; le réductionnisme numérique de la citoyenneté par les systèmes de traitements algorithmiques prédictifs qui présentent le risque d'une automatisation de la justice et du droit sans débat contradictoire ; la préemption de la mathématisation de la décision publique sur le projet politique qui porte le risque d'une réduction nominaliste du monde dans lequel seules les corrélations entre données comptent, ce qui suppose l'absence d'intentions justifiant un comportement ou l'absence de projet de société ; l'autoritarisme technocratique qui présente le risque d'exploiter l'urgence… pour mettre en place un régime politique très centralisé et piloté par des systèmes informatiques exploitant les pouvoirs des algorithmes des logiciels informatiques pour déployer une gestion optimisée. »[97]

94 A.P.D., avis n° 124/2021, *op. cit.*

95 Fr. Ost, « Nécessité fait loi ? La santé n'a pas de prix ? Ce que le Covid fait au droit », *in* S. Parsa et M. Uyttendaele (coord.), *La pandémie de Covid-19 face au droit*, Limal, Anthemis, 2020, pp. 17 et s.

96 Nous n'avons pas pu aborder de manière complète ce point. Sans doute aurait-il été utile de souligner le rôle des *operating systems* tant d'Apple que de Google (Android) dans la mise en œuvre des outils de *tracing* automatique. On pourrait également évoquer le rôle des opérateurs de communication dans la mise sur pied d'outils de suivi « anonyme » des citoyens et le repérage des regroupements de citoyens.

97 V. Calay, « L'empire des logiciels, menace pour les démocraties ? », *op. cit.*, p. 56.

Au-delà, ce qui nous frappe, c'est le «phénomène d'accoutumance»[98] d'une grande partie de la population à la normalisation qu'entraîne le numérique. Ainsi, la technologie, par la facilité de son utilisation, contribue à normaliser des comportements qui pourtant devraient susciter notre interrogation. Prenons un exemple : la possibilité d'obtenir facilement sur son téléphone mobile la preuve de sa vaccination ou d'un test P.C.R. négatif efface les interrogations sur la légitimité d'une centralisation des données de vaccination dans des bases de données de plus en plus largement accessibles et rend acceptable le fait que cette preuve soit réclamée à de multiples endroits, autorisant certains pourtant non habilités à la réclamer sans proportionnalité aucune.

Conclusion

28. La réflexion à laquelle nous avons convié le lecteur conduit à s'interroger : le numérique n'est-il pas, même en dehors des crises dont ses acteurs savent certes profiter, l'instrument d'un état d'exception, s'il faut entendre par là d'un régime mettant en cause les libertés individuelles, la justice sociale et finalement l'État de droit ? Notre propos rejoint l'inquiétude de plus en plus grande y compris dans les sphères politiques vis-à-vis d'outils comme l'intelligence artificielle.

À cet égard, des textes européens récents[99] constatent les risques inhérents aux algorithmes «statiques et opaques» et la nécessité de garantir, dès la conception, la transparence et l'«explicabilité» des algorithmes, afin d'empêcher toute atteinte disproportionnée à nos libertés ou toute discrimination liée à la prise de décision automatisée.

Il est en outre proposé de mettre en place des règles juridiques et éthiques intégrant l'idée que l'I.A. doit être une «technologie centrée sur l'humain», conçue comme un outil qui aide l'humain et qui est contrôlé par lui. Ce cadre réglementaire et éthique entend garantir le respect des droits fondamentaux

98 Nous reprenons ici les termes utilisés par le Centre de connaissances de l'A.P.D. (avis n° 124/2021, *op. cit.*, § 39) : «Il convient donc de tracer une frontière raisonnable entre ce qui relève de la liberté et de la responsabilité individuelles et ce qui peut relever du contrôle social, en s'attachant à n'imposer des restrictions aux libertés et droits fondamentaux que si cela s'avère strictement nécessaire et proportionné à l'objectif d'intérêt général poursuivi. Dans cette évaluation, l'Autorité insiste sur la nécessité d'être particulièrement attentif au risque réel de créer un "phénomène d'accoutumance", ce qui pourrait nous amener à accepter, dans le futur, que l'accès à certains lieux (y compris des lieux de la vie quotidienne) soit soumis à la divulgation de la preuve que la personne concernée n'est pas porteuse de maladies infectieuses [...]. L'Autorité attire l'attention sur l'importance d'éviter que la solution mise en place pour autoriser l'accès à certains lieux ou à certains événements entraîne un glissement vers une société de surveillance.»

99 Sur cette analyse des textes de l'Union européenne qui cherchent à tracer une «troisième voie» pour le développement de l'intelligence artificielle, voy. Y. Poullet, «"La troisième voie", une voie difficile : quelques réflexions autour de la politique européenne en matière d'intelligence artificielle», *R.L.D.I.*, 2021, n° 182, pp. 33 et s.

tels que la dignité, l'autonomie, l'autodétermination, la justice sociale, le respect de l'environnement et d'une démocratie fondée sur l'État de droit. Il implique la responsabilité sociétale de tous les acteurs qui concourent au développement des outils d'I.A.

On sait que la proposition de règlement de la Commission sur l'intelligence artificielle[100] vise ainsi à interdire certains traitements utilisant l'intelligence artificielle à des fins de contrôle et de profilage des personnes[101] et prévient, par l'obligation de suivre des systèmes d'évaluation et de gestion de risques, les dérives possibles de traitements dits «à haut risque»[102]. De telles initiatives de la Commission doivent être menées à terme si on ne souhaite pas que le numérique constitue demain la base d'un état permanent d'exception, dont il est loin d'être évident qu'il s'agisse encore d'un état aux mains de nos gouvernements.

À cet égard, qu'il soit clair, pour reprendre l'affirmation d'Evgeny Morozov, pourfendeur d'une société technolâtre, que «l'ennemi n'est pas la technologie, mais plutôt la résolution des problèmes, romantique et révolutionnaire, que l'on voit en elle»[103] ou, pour être plus précis, c'est la confiance exagérée, sans doute accréditée par les discours intéressés de certains acteurs du numérique, relayée par nos gouvernements et progressivement instillée à la population qui conduit à cette dérive. Ce constat exige donc la prudence, la transparence et le contrôle démocratique de nos outils et leur mise au service de la société et de nos États de droit même en temps de crise.

100 Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21 avril 2021, COM(2021) 206 final.

101 La proposition considère comme illégaux certains traitements utilisant les technologies de l'intelligence artificielle, en particulier l'exploitation des vulnérabilités, l'utilisation par le secteur public de systèmes de *social ranking* entraînant de potentielles discriminations entre personnes ou groupes, de systèmes biométriques fonctionnant en temps réel et à distance, placés dans des endroits publics (par exemple, des systèmes de reconnaissance faciale...). Cette disposition, certes non encore entérinée, démontre les limites de l'utilisation des technologies, y compris dans les hypothèses qualifiées d'état d'exception. Sans doute faut-il y voir des applications bienvenues des limites imposées par l'article 52 de la Charte européenne de respecter l'essence de nos libertés.

102 L'annexe III reprend la liste susceptible d'évolution de huit types de systèmes dits «à haut risque» : systèmes biométriques d'identification, systèmes de gestion des infrastructures critiques, applications dans le secteur de l'éducation et de la formation, applications en matière d'emploi, applications en ce qui concerne l'accès ou la jouissance de services publics ou de services privés essentiels, systèmes utilisés par les forces de l'ordre, systèmes utilisés en matière de migration ou de contrôle des frontières, systèmes d'administration de la justice. Pour ces traitements, la proposition entend instituer un système de gestion des risques (article 9) qui implique le suivi de bonnes pratiques en matière d'évaluation des systèmes (absence de biais, qualité des données...). L'article 10 mentionne divers devoirs liés à la gouvernance des données, ainsi le *testing* et la validation des choix de design et des données prises en compte, l'examen des biais possibles, etc. On ajoute les obligations de documentation (articles 11 et 18), de *logging* (articles 12 et 20) et surtout de surveillance humaine (*human oversight*).

103 E. Morozov, *To Save Everything, Click Here. The Folly of Technological Solutionism*, New York, Public Affairs, 2013, ouvrage traduit en français aux éditions FYP (septembre 2014) sous le titre : *Pour tout résoudre cliquez ici.*

29. Que la crise, sous toutes ses formes et non sous la seule forme sanitaire, nécessite un état d'exception et en particulier, dans ce cadre, la mise à disposition d'outils technologiques et de systèmes d'information aptes à la combattre, nous en convenons. Il nous importait cependant d'ajouter que cet état d'exception mérite des balises à trouver dans le cadre de la C.E.D.H. et, nous le pensons, d'une loi belge qui encadre les actions et procédures qui doivent être suivies dans ces contextes de crise afin que soient imposées *in tempore non suspecto* les balises aptes à garantir le maintien de nos libertés, de la justice sociale et de nos États de droit. Dans le cadre de cette loi qui concilie état d'exception et État de droit[104] doivent être d'autant plus envisagées des dispositions relatives aux systèmes d'information que la tentation est forte au nom de l'urgence et de l'efficacité des mesures prises de bâtir à travers des solutions technologiques une société de profilage et de surveillance excessifs.

[104] Sur la difficulté de concilier État de droit et état d'exception, voy. la thèse de M.-L. BASILIEN-GAINCHE, *État de droit et états d'exception, une conception de l'État*, *op. cit.*, en particulier pp. 263 et s., où l'auteur examine les onze conditions du respect par les gouvernants de l'État de droit en cas de recours aux états d'exception.