

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La vaccination obligatoire au regard des législations sur la protection des données

Poullet, Yves

Published in:

La vaccination contre la COVID-19 obligatoire en Belgique ?

Publication date:

2022

[Link to publication](#)

Citation for pulished version (HARVARD):

Poullet, Y 2022, La vaccination obligatoire au regard des législations sur la protection des données: des objections réelles. dans A Jansen (ed.), *La vaccination contre la COVID-19 obligatoire en Belgique ?*. Anthemis, Limal, pp. 129-146.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

La vaccination obligatoire au regard des législations sur la protection des données : des objections réelles¹

YVES POULLET

Professeur émérite de l'Université de Namur
Professeur associé à l'UCLille

Trois réflexions liminaires apparaissent nécessaires pour préciser les limites de notre propos.

La première tient à son objet : il s'agit de s'en tenir aux seules questions de protection des données liées aux mesures d'accompagnement d'une loi possible sur la vaccination obligatoire.

La deuxième insiste sur le fait qu'à l'heure de la publication de la présente contribution, aucune décision n'a été prise par le Parlement à cet égard et que les premiers travaux de la commission Santé semblent d'ailleurs s'orienter vers une réponse négative à cette demande d'une vaccination obligatoire. Il s'agit donc de conjectures et non de décisions à commenter. À cet égard, on note que, si la vaccination obligatoire est pour le moment écartée, il se pourrait, à suivre les propos tenus dans la presse par certains dirigeants de la majorité, qu'une loi en reconnaisse la possibilité, au cas où une nouvelle pandémie se déclarerait. Ainsi, ce n'est plus la certitude du risque mais son éventualité qui, au nom du principe de précaution, justifierait la légalisation de la vaccination obligatoire².

Enfin, troisième réflexion, si le propos est délibérément critique et prétend voir dans la protection des données de sérieuses objections à l'obligation vaccinale tant générale que partielle, l'argumentaire se fonde non seulement sur les risques liés à une protection des intérêts individuels, auxquels bien souvent s'arrête le débat de la protection des données,

- ¹ La présente contribution traduit les idées exprimées lors de l'exposé oral du professeur Thierry Léonard de l'UCLouvain Saint-Louis – Bruxelles et du signataire de la présente contribution lors du colloque organisé le 3 février 2022 par les Éditions Anthemis et le collectif Lawyers4Democracy. Ce texte est donc le fruit de la réflexion commune du signataire avec le professeur Léonard que le collectif, les organisateurs et le signataire remercient vivement.
- ² Cette même tendance à intervenir législativement de manière préventive et non une fois le risque déclaré se retrouve dans la proposition de décret wallon qui insère dans un décret fourre-tout la possibilité qu'à l'avenir, les inspecteurs de l'hygiène de l'AVIQ wallonne puissent prendre des mesures d'interdiction de mouvement, de suspension d'exercice de la profession, etc. en cas de risque de maladies infectieuses. L'exposé des motifs de l'article 18 qui consacre cette mesure se justifie ainsi : « Concernant l'alinéa 2 du paragraphe 1^{er}/2, le Conseil d'État, dans son avis, recommande la suppression des mots "qui met en jeu le pronostic vital à bref délai ou...". Son argumentaire se fonde sur la jurisprudence constante de la Cour européenne des Droits de l'homme, qui considère qu'imposer à une personne un traitement médical contre son gré constitue une atteinte à son droit au respect de sa vie privée. Une telle atteinte ne serait admissible que dans l'optique de protéger la vie d'autres personnes, et donc en cas de risque épidémiologique grave. L'avis du Conseil d'État ne peut ici être suivi, car il crée une faille dans la lutte contre les maladies infectieuses. En effet, lorsqu'une nouvelle maladie infectieuse apparaît, son caractère fortement épidémique n'est pas immédiatement scientifiquement démontré, alors même que la menace qu'elle représente pour le pronostic vital de la personne infectée est indiscutable. Il convient de pouvoir de suite agir contre cette maladie nouvelle, sans attendre la démonstration irréfutable de son caractère épidémiologique grave. Des examens médicaux doivent donc pouvoir être ordonnés en vue d'établir le diagnostic, quand bien même le caractère épidémiologique grave de la maladie n'est pas encore démontré. »

mais envisage aussi les risques plus globaux d'une société discriminante et de surveillance, à laquelle contribuent insidieusement les technologies mises en œuvre à travers la vaccination obligatoire qu'elle soit déguisée ou clairement prescrite.

La contribution suit le parcours suivant :

- Dans une première section, nous identifions les traitements de données à caractère personnel qui, selon toute vraisemblance, seront nécessaires à encadrer et rendre effective une vaccination obligatoire. Pour ce faire, nous analyserons l'objectif que le gouvernement assigne à la vaccination obligatoire (sous-section 1) pour rappeler ensuite (sous-section 2) le double contrôle qui s'impose à toute législation, visant à restreindre nos libertés fondamentales, à l'instar de celle qui imposerait l'obligation vaccinale. Nous évoquerons les principes généraux de légalité et proportionnalité qui s'imposent tant au niveau de l'obligation générale à la vaccination qu'à propos de chaque traitement de données à caractère personnel, outre les multiples prescrits des législations de protection des données, en particulier du RGPD³. L'identification des traitements potentiels liés à cette obligation conclura cette première section (sous-section 3).
- C'est eu égard à ces traitements potentiels liés à l'hypothétique obligation vaccinale que la seconde section envisage les divers risques qui y sont liés. On énumère ainsi les risques de non-transparence et d'absence de justification (sous-section 1). Ensuite, les questions, d'une part, des traitements poursuivant la finalité de constatation et de recherche des infractions (sous-section 2) et, d'autre part, des traitements liés à l'utilisation d'un pass vaccinal dans le cadre de l'obligation vaccinale retiendront plus longuement notre attention.
- Enfin, on rappellera certains impératifs du RGPD à charge des acteurs de la protection des données, particulièrement les droits de la personne concernée et d'obligation du responsable du traitement en matière d'évaluation préventive des risques (sous-section 3).

Section 1

La vaccination obligatoire rend nécessaires de nouveaux traitements de données à caractère personnel dont la validité et la licéité sont à apprécier au regard, en particulier – mais non uniquement –, des législations sur la protection des données

Sous-section 1. L'objectif du gouvernement

La légalisation de l'obligation vaccinale aurait pour but d'éradiquer de manière significative, si ce n'est complète, la dissémination de la maladie, et ce, au nom des impératifs de santé de la population, de non-encombrement des institutions hospitalières et de

³ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (texte présentant de l'intérêt pour l'EEE), *J.O.*, L119, 4 mai 2016 ; « RGPD » dans le texte et ci-après.

reprise économique, autant de motifs louables. Pour ce faire, cette législation compléterait les mesures déjà existantes, notamment de distanciation sociale et autres mesures de restrictions d'accès, par l'imposition à tous les citoyens belges de la vaccination contre la Covid-19, et ce, sous peine de sanctions. L'exemple autrichien est explicitement cité même si le gouvernement pointe également d'autres pays ayant eu recours à une obligation de vaccination ciblée à l'égard de certaines professions (France, Italie, entre autres). D'emblée, notons que cette obligation s'adresse aux citoyens belges et peut difficilement viser les étrangers résidant en Belgique ou visitant notre pays, si ce n'est de manière indirecte, en les contraignant au pass vaccinal et que, nulle part, il n'est question des personnes en séjour illicite dont le sort, en ces temps de pandémie, ne semble pas avoir préoccupé nos gouvernements jusqu'ici. Enfin, *quid* de personnes qui, pour des raisons légitimes, s'opposent à la vaccination ou lui opposent des risques pour leur santé ?

La réalisation de ce projet passe par la *nécessité de disposer de bases de données fiables tant de la population belge que des vaccinés pour atteindre l'objectif ainsi assigné.*

À juste titre, on s'interrogera sur ces bases de données. S'agit-il des listes déjà mises en œuvre dans le cadre de la vaccination « libre » et du contrôle réalisé au travers du pass sanitaire, ou de nouvelles bases de données construites à partir tant de ces dernières que du registre national, ou encore de la Banque carrefour de sécurité sociale dont le contenu est plus large ?

De plus, si le législateur admet, même de manière exceptionnelle, la non-vaccination, sans doute faudra-t-il créer des banques de données distinctes pour ces personnes, création qui soulève d'autres questions délicates au regard de la protection des données ?

Ensuite se pose la question de savoir qui aura accès à ces différentes bases de données, dès lors que l'effectivité de la mesure suppose que des contrôles de la vaccination de chacun, d'une part, et des sanctions en cas de non-vaccination, d'autre part, soient possibles.

L'accès sera-t-il accordé à la police uniquement, ou aux employeurs également ? L'exemple actuel du Covid Safe Ticket comme outil aisé de contrôle de l'état de vaccination de chacun est sans doute dans la tête des défenseurs de l'obligation vaccinale. Or, le caractère obligatoire et l'existence de sanctions pour les non-vaccinés alourdissent les conséquences de son utilisation, comme nous le verrons. Quelles sanctions sont à disposition des autorités : s'agit-il des seules sanctions pénales ou administratives⁴, ou s'agira-t-il également, voire surtout, de sanctions indirectes par l'exclusion des non-vaccinés d'une partie de leur vie sociale et professionnelle ? Sans doute, sont-ce à toutes ces questions que l'adoption d'une législation sur l'obligation vaccinale devra répondre.

Il nous semble donc que l'adoption de telles mesures, devra se faire à la suite d'un double contrôle, portant d'une part sur la conformité de l'obligation générale de vaccination et d'autre part sur la conformité des traitements de données à caractère personnel nécessaires à une telle obligation.

⁴ Ainsi, au Canada, où des droits supplémentaires d'entrée dans les hôpitaux seraient demandés.

Sous-section 2. Le double contrôle de l'action du gouvernement

Un *double contrôle* de la mesure s'imposerait en effet :

1. le premier consiste en l'analyse de la *conformité de l'obligation générale de vaccination* aux normes générales de la protection des droits humains et des libertés fondamentales. La mesure est-elle bien constitutionnelle, conforme aux textes en matière de droits fondamentaux, qu'il s'agisse de la Convention européenne des droits de l'homme⁵ (ci-après « CEDH ») ou de sa petite sœur : la Charte des droits fondamentaux de l'Union européenne ? ;
2. le second se focalise sur la *conformité des traitements de données à caractère personnel* mettant en œuvre l'obligation générale de vaccination, ainsi de manière purement exemplative, la banque de données des (non-)vaccinés, le système de pass vaccinal, etc. Il s'agit ici des contrôles exigés par le RGPD et les lois nationales particulières sur la protection des données à caractère personnel, comme la loi belge du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel applicables notamment aux traitements dits policiers.

On souligne deux constats, étroitement liés l'un à l'autre, à savoir que si ces deux contrôles se rejoignent sur certains points (i), le second complète le premier (ii). Il ajoute en effet des conditions de validité des traitements de données à caractère personnel eu égard aux atteintes spécifiques que ces traitements peuvent créer. Ces deux points méritent les réflexions suivantes :

- i) En ce qui concerne la première affirmation, l'article 5.1 du RGPD exige qu'un traitement poursuive des finalités légitimes. Cette exigence renvoie au contrôle de la validité de l'obligation de vaccination générale par rapport aux exigences de la CEDH. En d'autres termes, si l'obligation vaccinale est contraire à la CEDH, elle est illicite au sens de l'article 5.1. du RGPD. À ce propos, on se référera au commentaire, publié dans le même ouvrage, relatif à l'arrêt *Vavříčka*⁶ qui fixe les limites de l'obligation générale de vaccination de manière telle que cette obligation appliquée au cas de la Covid-19 apparaît pour le moins discutable.
Par ailleurs, si l'obligation vaccinale est trop étendue, le traitement sera illicite, en violation du principe de minimisation des traitements et des données énoncé aux dispositions des articles 5, 6 et 9 du RGPD. À titre exemplatif, en prescrivant l'obligation vaccinale des enfants, nonobstant la protection prioritaire des enfants affirmée par l'article 23 de la Constitution, les traitements des données des enfants devront être cessés et les données supprimées, conformément au prescrit des articles 5.a, b et c, 6.c et 9.2 du RGPD.
- ii) Ce premier examen est insuffisant. Il importe d'ajouter d'autres conditions qui, cette fois, sont propres aux traitements de données que la mise en œuvre de l'obligation vaccinale prétend justifier, appuyant ici notre seconde affirmation.

Il ne suffit pas que, dans l'abstrait, l'obligation générale de vaccination puisse être jugée comme respectueuse en soi des libertés individuelles et des droits humains, il faudra en

⁵ Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 4 novembre 1950, entrée en vigueur le 3 septembre 1953, ci-après dans le texte « CEDH » ; Charte des droits fondamentaux de l'Union européenne du 12 décembre 2007, 2016/C 202/02, version consolidée, J.O., 7 juin 2016, ci-après « la Charte ».

⁶ Cour eur. D.H. (gde ch.), arrêt *Vavříčka et autres c. République tchèque*, 8 avril 2021, req. n° 47621/13 et 5 autres.

outre que les outils technologiques qui serviront sa mise en œuvre soient respectueux des exigences des législations relatives à la protection des données. Ainsi, chaque traitement devra se justifier par une cause de légitimation propre au RGPD.

Au-delà, il y a également lieu de se conformer aux différentes dispositions des législations relatives à la protection des données. On citera notamment l'obligation de vérifier si les conditions de licéité particulières pour les données sensibles au sens de l'article 9 du RGPD, à savoir les données de santé, sont remplies et si, en outre, l'exigence de l'article 6.3 du RGPD peut trouver à s'appliquer⁷. En l'occurrence, il s'agit de l'obligation, pour les lois qui créeraient les traitements dans le cadre de l'obligation vaccinale, de mentionner de manière explicite et claire, notamment : « [...] les types de données qui font l'objet du traitement, les personnes concernées, les entités auxquelles les données peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être, les durées de conservation [...] »⁸.

Bien d'autres prescrits tirés des législations relatives à la protection des données pourraient être cités (voy., pour certains, nos réflexions, *infra*).

Il suffit à ce stade de rappeler que les deux contrôles sont indissociables et que le raisonnement sur la seule question abstraite de la validité aux yeux du droit de l'obligation vaccinale ne peut être résolu que si, dans le même temps, les validité et licéité des traitements sont examinées⁹.

⁷ À noter que l'APD, dans tous ses avis, a toujours estimé que ces mentions dans la loi devaient être obligatoires, le texte du RGPD est moins clair, mais sans doute est-il important de souligner qu'au regard des risques spécifiques importants liés aux traitements mis en place dans la lutte contre la Covid-19 (population visée, données sensibles...), il nous paraît que cette exigence est appropriée.

⁸ La Chambre de connaissances de l'APD l'a rappelé à de nombreuses reprises. Si le texte de l'article 6.3 semble laisser à l'autorité publique une certaine latitude : « cette base juridique peut contenir des dispositions spécifiques pour adapter les dispositions du présent règlement entre autres, les conditions générales de licéité, le responsable du traitement [...] », la Chambre a toujours, dans les textes relatifs aux mesures anti-Covid, réclamé, au vu de la nature des données traitées, de la population visée et de l'impact des mesures, que le texte législatif de création d'un traitement en la matière contienne l'ensemble des éléments essentiels du traitement visé à l'article 6.3. Parmi ces avis, citons l'avis n° 138/2020 du 18 décembre 2021 où l'Autorité se prononce sur le cadre juridique (provisoire) préalable à l'accord (au projet d'accord) de coopération en la matière, à savoir : l'arrêté royal du 24 décembre 2020 concernant l'enregistrement et le traitement de données relatives aux vaccinations contre la Covid-19, en exécution de l'article 11 de la loi du 22 décembre 2020 portant diverses mesures relatives aux tests antigéniques rapides et concernant l'enregistrement et le traitement des données de vaccination : « En vertu de l'article 6.3 du RGPD, lu conjointement avec l'article 22 de la Constitution et l'article 8 de la CEDH, il doit s'agir d'une norme légale formelle (loi, décret ou ordonnance) 6 définissant les éléments essentiels du traitement accompagnant l'ingérence publique 7. 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 est le cas en l'occurrence (voir ci-dessus), la disposition légale comprend les éléments essentiels suivants : - les finalités déterminées, explicites et légitimes des traitements de données à caractère personnel ; - la désignation du responsable du traitement ; - les (catégories de) données à caractère personnel traitées qui sont pertinentes et non excessives ; - les catégories de personnes concernées dont les données seront traitées ; - les catégories de destinataires des données à caractère personnel (ainsi que les conditions dans lesquelles ils reçoivent les données et les motifs y afférents) 8. - le délai de conservation maximal des données à caractère personnel enregistrées. 12. Cela n'empêche évidemment pas que, dans la mesure où la loi définit la plupart des éléments essentiels de l'enregistrement envisagé de données à caractère personnel relatives à la santé – souvent extrêmement sensibles – dans les bases de données des vaccinations, les détails et modalités puissent être précisés par des dispositions exécutoires. Le pouvoir exécutif ne peut certes être habilité que dans le cadre et en vue de l'exécution de mesures dont les éléments essentiels ont été définis préalablement par le législateur. »

⁹ À cet égard, la loi Pandémie, qui ne contient aucune référence à la loi de protection des données, certes à la suite des avis critiques de la Chambre de connaissances de l'APD, nous paraît contestable. Il est difficile d'apprécier la validité d'une mesure administrative qui souvent implique la création de traitements pour en assurer la mise en œuvre.

Sous-section 3. Le contrôle du respect des droits humains et, en particulier, de la réglementation de la protection des données

Le contrôle suppose préalablement l'identification des traitements liés à l'obligation vaccinale. Il est patent que ces traitements ne peuvent s'assimiler à ceux déjà existants dans la mesure où les finalités des premiers s'écartent de celles des secondes. Ainsi, les bases de données des vaccinés auront nécessairement pour finalité non plus d'éviter les risques de contamination, mais bien celle de constater le respect d'une obligation sanctionnée. Cette identification prendra en compte les éléments essentiels de chacun de ces nouveaux traitements : la nature sensible et les catégories des données traitées ; le responsable du traitement ; les destinataires des données, etc.

Quant au contenu de ce contrôle, il s'agira de cumuler le respect des normes supérieures, en particulier l'article 8 de la CEDH, les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne qui par « effet réflexe » garantiront la légitimité des finalités des traitements, exigées par l'article 5.1 b) du RGPD et celui du RGPD proprement dit et, le cas échéant, de la législation belge du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, actuellement en cours de révision.

Section 2

Les risques et limites des traitements liés à l'hypothétique obligation vaccinale

Sous-section 1. La non-transparence et l'absence de justification

§ 1. Le risque de non-transparence

Comme nous l'avons souligné dans la première partie, le principe de légalité implique non seulement que la création des traitements dans le cadre des mesures de lutte contre la pandémie trouve son origine dans une loi (légalité matérielle), mais en outre que le texte législatif réponde à des exigences de clarté et de prévisibilité (légalité formelle).

Dans de nombreux avis¹⁰, le centre de connaissances au sein de l'Autorité de protection des données¹¹, en charge de rendre des avis, s'est plaint du manque de respect des textes élaborés par le gouvernement. Ainsi, l'avis n° 16/2021 du 10 février 2021 relatif aux

¹⁰ Voy. entre autres : « Ensuite, en ce qui concerne la rédaction actuelle des finalités : Premièrement, comme l'Autorité l'a déjà souligné *supra*, il convient de clarifier les conditions et les circonstances dans lesquelles "une visite physique" peut avoir lieu dans le cadre du suivi manuel des personnes (présomées) infectées et de leurs contacts. [...] Le projet devrait déterminer, de manière exhaustive, les raisons pour lesquelles les centres de contact peuvent traiter les données à caractère personnel reprises dans la base de données III (qui sont, elles-mêmes, issues de la base de données I). Il convient donc de supprimer les termes "entre autres" dans l'article 3, § 1^{er}, 2.A du projet et de prévoir, dans le projet, toutes les raisons pour lesquelles les centres de contact pourront utiliser les données à caractère personnel visées dans la disposition en projet et contacter les personnes concernées. Il en est de même pour les mots "entre autres" repris dans l'article 3, § 2, 2.A du projet [...]. Il conviendrait de préciser ce qu'il faut entendre par "suivi" (Quels sont la nature et l'objet de ce suivi ? S'agit-il d'un contrôle à posteriori du respect des "recommandations" fournies ? Est-il obligatoire ? Ce suivi implique-t-il des mesures contraignantes ?) [...] » (APD belge, avis n° 64/2020 du 20 juillet 2020, concernant un projet d'accord de coopération).

¹¹ Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, articles 23 à 27.

traitements de données concernant la vaccination épinglé comme suit les défauts du projet gouvernemental, soulignant les risques liés à ces défauts de transparence (n°s 14 et s.) :

« 14. Comme l'Autorité l'a déjà souligné précédemment, le projet d'accord de coopération doit évidemment répondre intrinsèquement à l'exigence de clarté et de prévisibilité de la norme.

15. Bien que l'Autorité constate un progrès manifeste en ce qui concerne la définition déterminée et explicite des diverses finalités visées par les enregistrements de données, certaines de ces finalités restent néanmoins toujours très larges et peu précises, comme "la prestation de soins de santé et de traitements telle que visée à l'article 9, 2, h du RGPD", "le suivi et la surveillance post-autorisation", "l'exécution d'études scientifiques ou statistiques" et "l'information et la sensibilisation des utilisateurs de soins". Cela ne permet pas aux personnes concernées dont des données sont traitées à cet effet (ni à l'Autorité) d'avoir une idée claire des traitements qui seront effectués ou des circonstances dans lesquelles ils ont été autorisés.

16. Le manque de précision concernant certaines finalités visées complique la confrontation des traitements en la matière au principe de minimisation des données.

17. En outre, l'instance publique qui transfère des données à une autre autorité publique ou à une organisation privée doit, selon l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel, conclure avec cette instance tierce et doit signer pour chaque traitement un protocole qui "peut" prévoir notamment les catégories de destinataires pouvant recevoir les données et les finalités concrètes pour lesquelles les données peuvent être communiquées à ces tiers. On ajoute que les avis préalables des instances communicantes et réceptives doivent être demandés et annexés au protocole.

18. Ensuite, l'Autorité rappelle ce qui suit (voir également les points 19 et 20 de l'avis n° 138/2020) : afin de veiller à la prévisibilité de la norme, il y a lieu, non seulement, de définir précisément et clairement les finalités poursuivies, les catégories de données qui seront collectées et les catégories de destinataires, mais il est également recommandé de bien structurer la norme et de préciser pour chaque finalité, les (catégories de) données qui seront traitées et conservées ainsi que les catégories de destinataires auxquels ces données pourront être communiquées et les circonstances dans lesquelles elles seront communiquées ainsi que les raisons y afférentes. »¹²

Cette exigence de légalité formelle est importante. D'autant qu'en droit positif belge, toute ingérence dans le droit à la protection de la vie privée, en ce compris la protection des données à caractère personnel, doit être organisée par le législateur, le mot « loi » prévu à l'article 22 de la Constitution s'entend en effet *d'une loi au sens formel du terme*.

La Cour constitutionnelle ne manque pas de le rappeler¹³ en affirmant que : « bien que, en utilisant le mot "loi", l'article 8.2 de la Convention européenne [des droits de l'homme]

¹² APD, avis n° 16/2021 du 10 février 2021 relatif au 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 de données relatives aux vaccinations contre la Covid-19, §§ 17 et s.

¹³ Théorie du tout indissociable ; Voy. not. C.C., arrêt n° 162/2004, du 20 octobre 2004, B.3.1 ; C.C., arrêt n° 189/2005, du 14 décembre 2005, B. 4.3 ; C.C., arrêt n° 151/2006, du 18 octobre 2006, B. 5.4 ; C.C., arrêt n° 15/2008, du 14 février 2008, B.19.1 ; C.C., arrêt n° 29/2010, du 18 mars 2010, B.9.2.

n'exige pas que l'ingérence qu'il permet soit prévue par une "loi", au sens formel du terme, le même mot "loi" utilisé à l'article 22 de la Constitution désigne une disposition législative »¹⁴.

L'Autorité de protection des données (ci-après « l'APD ») fait application de cette jurisprudence dans ses avis, avec sans doute plus de sévérité encore, comme nous aurons l'occasion de le rappeler. Prenons un exemple : affirmer que la base de données vaccinale a pour finalité le suivi des patients exigerait bien des précisions. S'agit-il d'un simple suivi administratif et, en particulier, de la vérification de la prise de nouvelles doses ? S'agit-il d'un suivi, mais de quelle nature ; suivi médical, en particulier le suivi dans le cadre de la pharmacovigilance (étonnamment absent dans les textes actuels sur la vaccination dite libre), ou d'un contrôle – y compris policier – en vue de sanctionner le non-respect de l'obligation vaccinale ?

§ 2. Risques d'absence de justification

Comme déjà énoncé, il ressort de la jurisprudence de la Cour européenne des droits de l'homme que le principe de nécessité implique une mise en balance d'intérêts et un contrôle de proportionnalité.

Or le contrôle de proportionnalité des mesures suppose une documentation et une justification précises.

En effet, le principe de minimisation des traitements de données à caractère personnel induit une stricte nécessité du traitement à la réalisation de la finalité exprimée et poursuivie. Comme déjà énoncé, cette exigence se retrouve énoncée en l'article 5 du RGPD et se déduit également de ses articles 6 et 9 relatifs aux bases de licéité des traitements. Ces deux derniers articles exigent, dans la plupart des bases de licéité, que le traitement soit nécessaire à la finalité poursuivie (contrat, respect d'une obligation légale, etc.). À ce sujet, la professeure de Terwangne précise que :

« les données à caractère personnel faisant l'objet d'un traitement doivent, comme auparavant, être adéquates et pertinentes au regard des finalités du traitement. Pour être jugées pertinentes, les données doivent présenter un lien nécessaire et suffisant avec les finalités poursuivies. »¹⁵ et que « plutôt que de devoir être en outre "non excessives", comme dans les textes de la Convention 108 et de la directive, **les données à caractère personnel doivent désormais être "limitées à ce qui est nécessaire" au regard des finalités pour lesquelles elles sont traitées**¹⁶. Il est à noter que le critère de nécessité s'exprime tant au niveau de la quantité des données que de leur qualité. Ainsi, s'il est clair

14 C.C., arrêt n° 151/2006, du 18 octobre 2006, B. 5.6. Voy. égal. C.C., arrêt n° 29/2010, du 18 mars 2010, p. 19, B. 10.2. ; C.C., arrêt n° 202/2004 du 21 décembre 2004, B.4.3. ; l'arrêt n° 44/2015 du 23 avril 2015 (p. 63), l'arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et l'arrêt n° 29/2018 du 15 mars 2018 (p. 26).

15 C. DE TERWANGNE, « Les Principes relatifs au traitement des données à caractère personnel et à sa licéité », *Le Règlement général sur la protection des données (RGPD/GDPR), Analyse approfondie*, Collection du Crids, 2018, pp. 107 et 108. Voir également M.-H. BOULANGER *et al.*, « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.*, 1997, p. 146.

16 La professeure de Terwangne note également que la directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, a, quant à elle, gardé la formulation initiale et son article 4, § 1^{er}, c) établit que les données à caractère personnel doivent être « non excessives au regard des finalités pour lesquelles elles sont traitées ».

qu'on ne peut traiter un nombre excessif de données [...] on ne peut davantage se lancer dans le traitement d'une seule donnée qui, même pertinente au vu de la finalité, porterait excessivement atteinte aux droits et intérêts de la personne concernée par rapport à l'intérêt qu'elle présente pour la personne qui souhaite la traiter [...] »¹⁷

M^{me} de Terwangne conclut qu'« il faut comprendre que les deux formulations « limitées à ce qui est nécessaire » et « données non excessives » se rejoignent en ce qu'elles sont toutes deux l'expression du principe de proportionnalité »¹⁸.

L'on constate que cette notion de proportionnalité oblige le législateur, à procéder à une analyse complète de ses besoins en termes de données, mais également de la forme sous laquelle il les traitera. En effet, il devra vérifier si le traitement envisagé peut se satisfaire de données anonymes¹⁹ qui permettraient au traitement de sortir du champ d'application du RGPD. Si le traitement ne permet pas d'atteindre la finalité déterminée, le responsable du traitement pourra alors traiter des données pseudonymisées²⁰. Si, et seulement si, le traitement de telles données ne permet pas d'atteindre la finalité déterminée, le responsable du traitement pourra alors traiter des données à caractère personnel non-pseudonymisées. Il s'agit d'une réelle cascade induite par le RGPD qui devra être appliquée pour chaque traitement déterminé par le responsable du traitement. Cela entre dans la méthode de travail visée à l'article 25 du RGPD, par les principes de protection des données par défaut et dès la conception²¹.

Sans doute ne peut-on exiger une argumentation complète et sans faille, encore faut-il que l'autorité publique amène un certain nombre de faits, documents, chiffres qui puissent convaincre de l'existence d'un ou de risque(s) sérieux qui peut/peuvent être, cumulativement ou non, la limitation stricte de la circulation du virus, le soulagement des infrastructures hospitalières ou la recherche et la constatation du non-respect de la vaccination.

Il importera également de montrer à suffisance l'adéquation des mesures proposées au regard des risques particuliers à chacun des traitements nécessaires. Ainsi, il sera utile, au regard de différents critères relatifs à l'ampleur de la vaccination (population visée, nombre de prises, durée de validité du vaccin), à son objet (quel vaccin contre quel variant ?), aux modalités d'exécution de la vaccination (qui vaccine ? quelles priorités ?), que l'autorité publique démontre, tant que faire se peut, l'efficacité de la mesure proposée

17 C. DE TERWANGNE, « Les Principes relatifs au traitement des données à caractère personnel et à sa licéité », *op. cit.*, p. 108.

18 *Ibid.*

19 Par donnée anonyme, nous devons entendre une donnée dont le lien est définitivement coupé avec la personne physique à laquelle elle se rapportait. À noter que le caractère anonyme d'une donnée peut se révéler difficile à maintenir avec l'avènement du big data et de l'intelligence artificielle.

20 Le RGPD définit la pseudonymisation comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » (article 4, 5)). Il n'en demeure pas moins que des données rendues pseudonymes restent des données à caractère personnel. Dans la législation belge antérieure au RGPD, nous avions la notion de donnée codée.

21 Les termes de *privacy by design* et *by default* sont également largement utilisés ; le principe de *privacy by design* consiste à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception des traitements, lors de la rédaction des normes qui imposent des traitements, et ce afin de s'assurer que les responsables du traitement et les sous-traitants soient en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données.

par rapport à la ou aux finalité(s) poursuivie(s), et au-delà, qu'il démontre également que les traitements des données que cette obligation vaccinale suppose, répondent à la ou aux finalité(s) de la vaccination obligatoire.

À cet égard, on rappellera que, nonobstant quatre avis émis par la Chambre de connaissances dans le cas des différents textes relatifs au CST et réclamant cette documentation, l'autorité publique n'a jamais rencontré la demande pourtant parfaitement justifiée de l'APD. Le contrôle de proportionnalité exige en effet que soit démontrée, dans les faits, la nécessité de l'existence, du contenu, des modalités essentielles de fonctionnement et qu'aucune autre mesure moins invasive de nos libertés ne soit possible.

Sous-section 2. Les risques particuliers liés à la finalité de constatation et de recherche des infractions

La mise en œuvre de la vaccination obligatoire réclamera la création de traitements de constatation et de recherche des infractions consistant précisément dans le refus non légitime de la vaccination.

Il s'agit d'une nouvelle finalité des traitements rendue nécessaire dans le cadre de la mise en place d'une obligation vaccinale éventuelle. À cette fin, divers traitements peuvent être envisagés. Notons d'emblée qu'il peut être tentant à cet égard – et les interviews récentes de deux présidents de partis le laissent entendre – de repartir de l'infrastructure existante, à savoir les bases de données régionales des vaccinés et celles relatives à la gestion du Covid Safe Ticket. La reprise de ces banques de données présente l'avantage d'une grande facilité et efficacité dans le repérage des vaccinations, à la fois quant aux personnes, mais également quant au nombre de doses et à l'identification du type de vaccin utilisé. Par voie de conséquence, l'utilisation de ces bases de données rend facile, par l'interconnexion avec le Registre national ou celle tenue par la Banque de données-carrefour de la sécurité sociale, l'identification de ceux qui ne figurent pas dans la liste des vaccinés, soit qu'ils n'y soient pas et/ou se révèlent incapables de prouver leur vaccination.

Il y a lieu dès lors de se poser la question des risques attachés à une telle réutilisation de la banque de données des vaccinés dans le contexte d'une obligation vaccinale à laquelle sont liées, en cas de non-respect, des sanctions non seulement pénales et administratives, mais surtout des mesures d'exclusion sociale et professionnelle. Cette exclusion constitue une conséquence indirecte de l'existence de cette base de données qui alimente la délivrance et la cessation d'effets du pass vaccinal dont la présentation comme un sésame devient une condition d'accès à certains lieux ou certaines activités professionnelles ou non.

En d'autres termes, l'absence d'une personne dans la base de données des vaccinés, jointe à la non-possession d'un pass vaccinal, créerait du fait même de la technologie une présomption de non-vaccination, ce qui équivaldrait à une présomption de non-respect de la loi et donc justifierait, *prima facie*, les sanctions.

Pour faire court, la technologie fonderait ainsi une décision ayant un profond impact sur les personnes à partir de la seule présence de données dans une base de données. Sans doute restera-t-il à la personne la possibilité de renverser la situation et de montrer que l'absence de données correspond à une situation légitime dont elle peut se prévaloir.

Avant de se pencher sur les possibilités de ce renversement de *onus probandi*, notons qu'il heurte les principes du droit pénal de la présomption d'innocence²² de la personne concernée et de l'obligation d'entendre la personne suspectée de violation de la règle²³.

Reprenons la question du « droit » à la non-vaccination, c'est-à-dire des causes légitimes de ne pas figurer dans la base de données. Elles sont de divers ordres et si on assume que la vaccination a pour but de combattre la propagation du virus, on signale que la vaccination ne s'impose pas si la personne a été récemment soumise à la maladie. On ajoutera que la vaccination peut également être fortement déconseillée pour des raisons médicales. Et ne pourrait-on admettre l'objection de conscience à condition que l'objecteur suive un comportement qui mette à l'abri son voisinage ? L'arrêt *Vavříčka* laisse entendre qu'aucune obligation vaccinale même dûment justifiée ne peut être absolue²⁴. Dans le cas qui nous occupe, la démonstration du droit à la non-vaccination pour raisons médicales peut s'avérer difficile. L'état des connaissances scientifiques permet-il aujourd'hui d'identifier avec suffisamment de certitudes les personnes à risque et celles qui ne le sont pas ? Qui va dès lors prendre la responsabilité d'officialiser l'empêchement ou, à l'inverse, de ne pas prononcer l'empêchement avec, dans un cas comme dans l'autre, les risques de responsabilité liée ? Dernière question : comment va-t-on prendre en compte cet empêchement dans le processus du pass vaccinal ou sanitaire ?

Ce besoin d'identification des bénéficiaires au droit à la non-vaccination conduira vraisemblablement, au cas où la vaccination obligatoire serait retenue même de manière déguisée, à la création d'une base de données des non-vaccinés légitimes. Cette base de données, dans la mesure où elle mentionnera, comme nous l'avons dit, des données médicales ou philosophiques qui soutiennent l'objection de conscience, contient des données hautement sensibles. Le caractère ultra-sensible des données concernées soulève des questions quant à leur introduction (qui ? avec quel contrôle ?) ainsi quant à l'accès à de telles données (qui ? à quelles données ?). On s'interroge enfin sur les liens entre la banque de données des vaccinés et celle des non-vaccinés.

Le changement de finalité des traitements sur les bases de données existantes, à savoir la base de données de personnes vaccinées et le CST ou pass vaccinal, apparaît ne pas répondre aux conditions de licéité et de légitimité énumérées par le RGPD et le principe fondamental de non-discrimination (voir première section) à partir du moment où la finalité de recherche et de constatation des infractions devient une des justifications centrales de la création de ces nouveaux traitements. Ce changement rencontre les objections majeures suivantes :

- *la nécessité de la finalité nouvelle ne s'impose pas* : l'identification des non-vaccinés et l'application d'une sanction à leur égard ne justifient pas l'atteinte aux droits et libertés qui découlerait de tels traitements ;
- à tout le moins, *l'atteinte (l'exclusion sociale) paraît disproportionnée* par rapport au profit obtenu, à savoir la plus grande efficacité dans la recherche d'infractions ;

²² La présomption d'innocence est un principe général du droit, qui implique que la personne poursuivie, mais qui n'est pas encore définitivement condamnée, est censée être innocente tant que la preuve de sa culpabilité n'a pas été établie de manière irréfutable. Ce principe est consacré dans des textes supranationaux de défense des droits fondamentaux et notamment la Charte des droits de l'homme, mais également dans diverses dispositions et notamment les articles 28quinquies, article 57, §§ 3 et 4, et 61ter, § 4 du Code d'instruction criminelle.

²³ En application du principe général du respect des droits de la défense et les exigences du procès équitable, mais également s'agissant de sanctions administratives du principe « *audi alteram partem* ».

²⁴ Cour eur. D.H. (gde ch.), arrêt *Vavříčka et autres c. République tchèque*, 8 avril 2021, req. n° 47621/13.

- le risque *d'atteinte au principe de non-discrimination* entre les vaccinés et les non-vaccinés est à souligner : la différence de traitement n'est pas justifiée par des raisons objectives documentées. En particulier, avec le variant actuel, *omicron*, plus encore qu'avec ceux qui précèdent, une vaccination n'équivaut pas à une non-contamination et, à l'inverse, la non-vaccination n'entraîne pas un risque majeur de contamination ;
- enfin, le fonctionnement croisé de la base de données des vaccinés et de l'infrastructure de lecture et de gestion du pass vaccinal accroît le risque *d'atteinte au principe de présomption d'innocence*. Ce fonctionnement conduit à un renversement de la charge de la preuve de l'infraction sur le non-vacciné.

Sous-section 3. De quelques dispositions impératives des législations de protection des données

§ 1. Les acteurs des traitements

Le responsable principal des traitements qui devront être mis en place dans le cadre de l'obligation vaccinale nous apparaît devoir être l'autorité fédérale. Même si on peut songer à une responsabilité conjointe, voire distincte, des entités fédérées pour certaines finalités directement liées à l'exercice des compétences des communautés (par exemple la médecine préventive) ou des régions, il est certain que la finalité de constatation des infractions et celles liées à la santé publique prépondérantes dans les nouvelles finalités relèvent de l'État fédéral.

On connaît les obligations des responsables de traitement vis-à-vis de leurs sous-traitants (par exemple la SMALS), obligation de choix d'un sous-traitant de qualité, obligation de délimiter soigneusement leurs tâches et de veiller à interdire toute utilisation en dehors de celles-ci..., autant d'obligations qui devront trouver leurs traductions dans un contrat entre les deux partenaires. Par ailleurs, l'article du RGPD impose également des obligations à ces sous-traitants, y compris vis-à-vis des responsables.

En ce qui concerne les destinataires des traitements, qu'il s'agisse de l'accès ou de la transmission de données, qu'ils soient internes ou externes, c'est selon les finalités légitimes de leur utilisation que leurs droits seront soigneusement fixés (en particulier, *quid* des transmissions ou accès vers les employeurs, les autorités sanitaires ?). Il importera de s'interroger sur certains d'entre eux : de quelles prérogatives peut disposer la police en matière d'accès aux traitements et ceux aux fins de sanctionner des infractions ? Peut-elle conclure des accords avec certaines catégories de professionnels quant à la transmission des infractions ? On sera attentif au cas des autorités policières. La transmission vers des autorités policières est soumise, par la loi du 30 juillet 2018, à des conditions strictes (art. 29), en particulier lorsqu'il s'agit de données sensibles (art. 34).

Par ailleurs, la lecture d'un pass vaccinal ou d'un certificat de dispense de vaccination à nombre d'endroits de rassemblement de la population ouvrirait la possibilité d'accès, certes partiel, à de nombreuses personnes qui se trouveraient, même pour une durée très déterminée, préposées à la surveillance de l'entrée de certains lieux.

Que penser du contrôle de l'identité, via un lecteur de la carte d'identité au Registre national ? Ne faudrait-il pas réserver ce contrôle au cas où il y a suspicion légitime de tromperie comme dans la loi française ?

Enfin, comment justifier le rôle des citoyens qui mettent en œuvre le traitement de contrôle du pass et de ses sanctions ? Une sous-traitance, mais alors par qui ? Et *quid* des exigences du RGPD en ce qui concerne précisément cette sous-traitance²⁵ ?

Enfin, on rappelle qu'il s'agit de traitements de données sensibles, ce qui dès lors implique la nécessité, conformément à l'art. 9.3. du RGPD, que les traitements soient placés sous la responsabilité d'un professionnel de santé soumis à une obligation de secret.

§ 2. Les droits des personnes concernées

Sans vouloir être exhaustifs, épinglons quelques prescrits du RGPD :

- L'article 12 du RGPD impose une information en termes clairs et simples sur les traitements opérés d'office ou potentiels. Cette information doit porter notamment sur le droit d'accès et sur les conditions de mise en œuvre d'un droit d'opposition pour les personnes « empêchées » et les « non-vaccinés » dans des conditions précises prédéterminées. À propos du droit d'accès mis en place par l'article 15, n'est-il pas possible, comme le recommande le centre de connaissances de l'APD²⁶, de prévoir, à l'instar de ce qui existe en matière de registre national, un accès sécurisé par les citoyens, porteur d'un pass vaccinal aux logs de consultation par des tiers du registre des vaccinations. Ainsi, les personnes pourraient connaître les différentes autorités et personnes civiles ou non qui ont eu accès à la base de données, voire leurs motivations et, le cas échéant, s'en inquiéter. On ajoute qu'en matière de traitement à des fins de prévention ou constatations d'infractions, l'article 56 de la loi du 30 juillet 2018 impose la journalisation des accès et des communications.
- Une procédure rapide auprès d'un organisme médical indépendant devrait être prévue afin de permettre aux personnes concernées d'exercer facilement leur droit d'opposition (art. 21) en cas de « motifs légitimes et supérieurs » de refus de la vaccination. Il s'agit ici d'une conséquence du droit à la non-vaccination, qui doit être reconnu et précisé par la loi fixant l'obligation vaccinale.
- Enfin, on conviendra de l'importance du droit à ne pas faire l'objet d'une décision individuelle automatisée énoncé en l'article 22 du RGPD. La dénonciation automatique à la police si la base de données indique une non-vaccination ou l'interdiction d'accès à des lieux sur la base du contrôle du pass vaccinal constituent des exemples de ce type de décisions visées par le RGPD. Si le paragraphe 2 de l'article permet une exception en cas d'autorisation par le droit de l'État membre, encore faut-il que cette autorisation soit légalement explicite et qu'elle n'empêche pas le droit à une explication humaine concernant cette décision, et un droit de recours rapide et efficace contre une telle décision.

²⁵ Article 28 RGPD.

²⁶ « L'Autorité réitère en outre sa recommandation (voir le point 43 de l'avis n° 138/2020) de prévoir dans ce contexte un droit d'accès électronique, par analogie avec ce qui est prévu pour le Registre national 22, comme garantie supplémentaire pour les droits et libertés des personnes concernées et afin de confirmer leur confiance dans l'utilisation des bases de données des vaccinations. De cette manière, les personnes concernées peuvent à tout moment prendre connaissance des autorités, instances et personnes qui ont consulté ou actualisé leurs données dans les bases de données des vaccinations. » (Avis n°16/2021 du 10 février 2021 relatif aux traitements de données concernant la vaccination).

§ 3. L'obligation de suivre une procédure d'évaluation des risques

Ce dernier point est sans doute le plus important. Les articles 35 et 36 du RGPD mettent sur pied une procédure destinée préventivement à analyser les risques liés à l'existence et au fonctionnement de traitements à risque élevé (ce qui est incontestablement le cas au vu de la population couverte, des conséquences de l'utilisation des traitements en cause et de la nature sensible des données, et dans toute la mesure une recherche de diminution des risques).

Cette procédure est exigée des administrations, nous dit l'article 23 de la loi du 30 juillet 2018, « même si une analyse d'impact relative à la protection des données a été réalisée dans le cadre de l'adoption de la base légale ». On ajoute que l'article 36.4 réclame une consultation préalable de l'autorité de contrôle « dans le cadre de l'élaboration d'une proposition d'une mesure législative [...] ».

Deux réflexions complètent ce rappel de l'importance de ce « *risk assessment* » dont, avec l'APD, nous regrettons l'absence dans les décisions qui ont instauré les multiples traitements déjà existants dans la lutte contre la Covid-19.

La première relève que le texte de l'article 35.9 non seulement implique dans la démarche de « *risk assessment* » le détaché à la protection des données (art. 35.2.), mais recommande aussi la consultation des parties intéressées lors de la procédure d'évaluation des risques, ce qui implique que le responsable du traitement devrait réunir outre les épidémiologistes notamment les associations de patients et du personnel soignant, les médecins généralistes et de diverses disciplines, des psychologues et des organismes soucieux de l'égalité des chances.

La seconde réflexion a trait à l'étendue des risques à prendre en considération. Sur ce point, nonobstant les difficultés d'interprétation du texte du RGPD, nous prônons la nécessité de prendre en compte non seulement les risques d'atteinte aux libertés individuelles (approche purement individualiste de la protection des données) mais, au-delà, les risques d'injustice sociale et ceux liés à des évolutions de notre société, à savoir, la mise sur pied d'une société numérique de surveillance et de conformisme, voire d'atteinte à l'État de droit et à l'équilibre des pouvoirs. La conclusion développera ce dernier point essentiel : ce que le débat sur l'obligation vaccinale révèle, c'est que notre société doit, de manière urgente, prendre conscience que le numérique et les solutions qu'il apporte aux difficultés de notre temps mettent en cause au-delà de nos libertés individuelles, de manière plus essentielle encore, les impératifs de justice sociale et ceux de l'État de droit.

Conclusions. Des objections sérieuses de la protection des données à l'obligation vaccinale

En guise de conclusion, force est de constater que le changement radical de finalités dans les traitements des bases de données actuellement mobilisées dans le cadre de la gestion de la vaccination volontaire, excèderait, et de loin, les besoins de protection de la santé, publique et individuelle. D'autant que, au-delà de la sanction, la création de ces bases de données, soulève le risque d'erreurs et de discriminations graves pour les non vaccinés et les personnes empêchées, les privant sans recours de pans complet de leur vie sociale.

En effet, dans le contexte de l'obligation vaccinale, le pass vaccinal, apparaît comme un outil d'effectivité et de contrôle qui poserait de nombreux problèmes à divers égards.

Premièrement l'élargissement du nombre de contrôleurs, dont font partie désormais les citoyens, qui à l'occasion des contrôles d'accès, pose la question de la légitimité de leur pouvoir de sanction.

Deuxièmement le caractère exorbitant de la peine d'exclusion sociale, qui serait appliquée par ces agents constatateurs et sanctionnateurs d'un nouveau genre que sont les concitoyens n'est pas sans causer préjudice aux principes du droit pénal de présomption d'innocence et de droit à la défense.

Ensuite, les risques d'accès non maîtrisés des outils mis en place (BD, pass, etc.), rappelle la nécessité de procéder à l'analyse nécessaire de la conformité du cadre légal pressenti avec les exigences de la législation relative à la protection des données.

À défaut d'un tel examen, cette situation mènera à terme, si ce n'est déjà le cas en partie, à ce que nous appelons une banalisation de la surveillance, voire à une société de la surveillance et du conformisme. Un risque par ailleurs, également soulevé par l'APD, elle-même en son premier avis sur le CST²⁷, en ce qu'elle énonçait que :

« Dans cette évaluation, l'Autorité insiste sur la nécessité d'être particulièrement attentif au risque réel de créer un "phénomène d'accoutumance" [...]. 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. »

La particularité majeure d'un pass numérique réside dans la production d'un outil qui permet un contrôle systématique et facilité des restrictions légales aux libertés, en particulier celles d'aller et venir dans les espaces publics ou privés (entreprises, associations, milieux professionnels). Ne se limitant pas à rendre les comportements plus prévisibles en réduisant les libertés, un tel outil s'est aussi avéré générateur de discriminations et d'exclusions sociales, en interdisant aux personnes non vaccinées de fréquenter les lieux de culture, les grands magasins, voire leurs entreprises (comme en Italie, par exemple). Son application fut par ailleurs confiée, outre aux autorités policières, à des personnes privées, chargées, à l'instar des forces de l'ordre, de constater la *compliance* des sujets ou le non-respect de la législation. Étrange délégation dont l'exercice peut conduire au prononcé d'une sanction qui, si elle n'est pas forcément pénale dans tous les cas, est cependant civile par le refus de permettre l'accès à des espaces de socialisation. Les conséquences d'une telle sanction civile sont majeures et bien plus graves que la sanction pénale, lorsque l'interdiction d'accéder à certains lieux prive la personne humaine de ses moyens de subsistance (son travail), de son épanouissement social et culturel, ou de l'exercice de libertés fondamentales. L'absence ou la présence d'une donnée dans une base de données induit ainsi, par la création d'un outil comme le pass sanitaire, une discrimination entre personnes difficilement justifiable. Il apparaît bien légitime de s'inquiéter d'un tel précédent contraire sinon à l'article 22 du RGPD, au moins au principe de la présomption de non-culpabilité des citoyens cher au droit pénal. Le précédent du pass sanitaire, ou vaccinal, conduit à déléguer à tout citoyen un pouvoir de sanction sur

²⁷ Avis n° 124/2021 du 12 juillet 2021, n° 39, p. 14.

ses semblables, sur la base d'une donnée indicatrice d'un risque de santé pour soi-même et pour les autres, donnée qui relève pourtant et certes non uniquement du libre arbitre des personnes.