



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 24/2021 du 2 mars 2021

Objet : avant-projet de loi relatif aux mesures de police administrative lors d'une situation d'urgence épidémique (CO-A-2021-044)

L'Autorité de protection des données (ci-après l' "Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

Vu le 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, ci-après "le RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu l'avant-projet approuvé en Conseil des Ministres le 26 février 2021 et son inscription à l'agenda de la Commission Intérieur, Sécurité, Migration et Affaires Administratives de la Chambre des représentants le 3 mars 2021 (ci-après « l'avant-projet»);

Vu le rapport de Madame Alexandra Jaspas, Directrice du Centre de Connaissances de l'Autorité de protection des données ;

Émet, le 2 mars 2021, l'avis suivant :

I. REMARQUE INTRODUCTIVE

Le délai ordinaire dans lequel le Centre de Connaissances de l'Autorité est tenu de rendre ses avis est de 60 jours. En cas d'urgence motivée et si la charge de travail du Centre de Connaissances le permet, ce délai peut être ramené à 15 jours par la Directrice du Centre de Connaissances. Afin que les députés puissent être en possession de l'avis du Centre de Connaissances lors de la séance du 3 mars 2021, le présent avis a été rendu dans un délai de 2 jours à dater de la réception de l'avant-projet. Il se focalise dès lors sur les manquements majeurs identifiés dans l'avant-projet. L'Autorité pourrait estimer utile de compléter ou affiner le présent avis ultérieurement.

II. L'AVANT-PROJET NE CONSTITUE PAS UNE BASE LEGALE VALABLE POUR LES TRAITEMENTS DE DONNEES QUI POURRAIENT ETRE EFFECTUES DANS LE CADRE DE LA MISE EN PLACE DES MESURES DE POLICE – IL DONNE LIEU A UNE VIOLATION DES PRINCIPES DE LEGALITE ET DE PREVISIBILITE

a) Rappel des principes de légalité et de prévisibilité

L'Autorité rappelle que toute ingérence dans le droit au respect de la protection des données à caractère personnel, en particulier lorsque l'ingérence s'avère importante, n'est admissible que si elle est nécessaire et proportionnée à l'objectif (ou aux objectifs) qu'elle poursuit et qu'elle est **encadrée par une norme suffisamment claire et précise et dont l'application est prévisible** pour les personnes concernées¹.

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, ci-après aussi appelée « la loi »)**² définissant les éléments essentiels du traitement accompagnant l'ingérence publique³. 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 À la lecture d'une telle norme, les personnes concernées doivent avoir une idée claire du (des) traitement(s) effectué(s) avec leurs données, de la finalité de celui-ci (ceux-ci) et des conditions dans lesquelles le(s) traitement(s) de données a (ont) été autorisé(s).

² Il est nécessaire, au regard des exigences constitutionnelles belges, que cette norme soit de rang législatif.

³ Voir DEGRAVE, E., "*L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle*", Collection du CRIDS, Larcier, Bruxelles, 2014, p. 161 e.s. (voir e.a. : CEDH, Arrêt *Rotaru c. Roumanie*, 4 mai 2000). Voir également quelques arrêts de la Cour constitutionnelle : 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).

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.

Dans la mesure où la loi définit ces éléments essentiels, **les détails et modalités de ces traitements de données peuvent être précisés par le Roi** via arrêté-royal, moyennant une délégation claire et précise en ce sens effectuée par la loi.

- b) L'avant-projet de loi ne définit pas les éléments essentiels des traitements de données qu'il entend autoriser (ni même ces traitements de données)

Le pouvoir exécutif ne peut être habilité à définir les **modalités** d'un traitement de données que dans le cadre et en vue de l'exécution de mesures dont les éléments essentiels ont été définis préalablement par le législateur. Or **l'avant-projet de loi ne définit pas les éléments essentiels** et délègue à l'exécutif la tâche de définir ces éléments.

Le §3 de son article 6 prévoit en effet que :

« §3 Lorsque les mesures prises en application des articles 4, §1^{er}, alinéa 2 et 5, 1^{er}, a) à h) nécessitent la création d'une banque de données, les modalités de la mise en place et de la gestion de cette banque de données, y compris **la détermination des données** à caractère personnel visées, **les personnes concernées** ainsi que **la transmission de ces données à des tiers**, sont **déterminées par le Roi**, par arrêté délibéré en Conseil des ministres, après avis de l'autorité de contrôle (...) »

L'avant-projet qualifie donc de « modalités » les éléments essentiels des traitements de données qu'il entend autoriser, alors qu'il s'agit d'éléments essentiels qui doivent être définis par le législateur.

Il n'évoque par ailleurs nullement les traitements de données en question, se contentant de faire référence à la mise en place et à la gestion d'une banque de données, qui ne sont à l'évidence que des moyens dont l'objectif est de permettre des traitements de données. Il va de soi que la mise en place d'une banque de données en vue de surveiller le respect de mesures de police (respect d'un couvre-feu, d'une interdiction de

quitter le territoire etc) a pour objet de permettre à certaines autorités publiques d'accéder à ces données et de les utiliser (« traiter »). L'avant-projet reste muet quant à ces utilisations. Il ne permet dès lors pas d'appréhender « qui va traiter quelles données et pourquoi ». Il donne dès lors lieu à une violation des dispositions précitées et ne répond pas aux exigences de légalité et de prévisibilité.

I. L'AVANT-PROJET NE DEFINIT PAS LES CATEGORIES DE PERSONNES DONT LES DONNEES POURRONT ETRE TRAITÉES

L'avant-projet ne définit pas les catégories de personnes dont les données pourront être traitées.

Le §4 de son article 6 indique qu'il s'agit «**notamment** des personnes infectées, des personnes ayant eu un contact étroit ou à haut risque, ou des personnes n'ayant pas respecté les mesures prises en application des articles 4, 1^{er}, alinéa 2 et 5, 1^{er}, a) à h) ».

L'alinéa suivant ajoute que « Le Roi **précise**, par arrêté délibéré en Conseil des ministres, après avis de l'autorité de contrôle de la protection des données compétente, les catégories de personnes concernées ».

L'utilisation du terme « notamment » indique que le Roi est en réalité habilité à **ajouter** des catégories de personnes concernées aux trois catégories énoncées au §4 de son article 6 et non pas seulement à préciser ces catégories (en définissant par exemple ce qu'il faut entendre par « personnes ayant eu un contact étroit ou à haut risque »).

L'avant-projet doit être complété d'une définition claire, complète et univoque des catégories de personnes dont les données pourront être traitées. Cette énumération se doit d'être limitative.

II. L'AVANT-PROJET NE DEFINIT PAS LES DONNEES OU CATEGORIES DE DONNEES QUI POURRONT ETRE TRAITÉES

L'avant-projet reprend une liste de catégories de données qui pourront être traitées (sans toujours préciser par quelle(s) autorité(s), dans le cadre de quel(s) traitement(s) ni à quelle(s) fin(s)) :

« Article 6§5 :

1° Les données d'identification personnelles, et ce, uniquement par les membres des services de police visés au §6, 1° ;

2° Les données d'identification personnelles, à l'exclusion des données spécifiques propres à l'identité physiologique, génétique, psychique ou culturelle des personnes et ce, uniquement par les membres des services publics visés à l'article 8, 2° à 4° ;

3° Les données professionnelles se limitant aux données d'identification du travailleur salarié ou indépendant, ou du fonctionnaire ;

4° Les données de voyage, se portant sur la sortie et l'entrée sur le territoire belge, l'Etat de provenance ainsi que le moyens de transport utilisés ;

5° Les données concernant la santé physique se limitant uniquement aux données des résultats d'examen de dépistage, y compris non positifs. »

L'Autorité :

- ne saisit pas la différence entre les trois premières catégories de données (« les données d'identification personnelles ») et rappelle que les données d'identification sont généralement admises comme étant les nom, prénom, adresse et date de naissance et ne doivent pas se confondre avec les « données à caractère personnel » au sens large; il semble que l'auteur de l'avant-projet vise en réalité ici les « données à caractère personnel », ce qui revient à dire que l'avant-projet prévoit que la police serait amené à traiter toutes les données relatives à des personnes physiques, ce qui est disproportionné (quel que soit l'objectif) et contraire à l'article 5.1.c) du RGPD (en vertu duquel les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies) ;
- se demande en quoi « des données spécifiques propres à l'identité physiologique, génétique, psychique ou culturelle des personnes » constitueraient des « données d'identification personnelles » ;
- suggère à l'auteur de l'avant-projet d'utiliser les concepts définis et utilisés par la réglementation applicable, en ce compris le RGPD et la LTD ;
- rappelle à l'auteur de l'avant-projet les dispositions spécifiques applicables en cas de traitement de données visées par l'article 9 du RGPD (données particulières ou dites « sensibles » telles que les données relatives à la santé)
- se demande en quoi les données d'identification du travailleur sont des « données professionnelles » si elles sont limitées aux données d'identification (voir premier tiret ci-dessus) et ne sont pas complétées par des données relatives à l'employeur, à la fonction, à l'adresse du lieu de travail etc

L'Autorité rappelle que, conformément à l'article 5.1.c) du RGPD, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies (minimisation des données), ce qui implique que l'avant-projet établisse non pas une liste de finalités d'une part et une liste de données d'autre part mais qu'il définisse quelles données seront traitées, par qui et dans le cadre de quelle(s) finalité(s).

Cette énumération ne reprend par ailleurs pas toutes les (catégories de) données dont les auteurs de l'avant-projet souhaitent autoriser le traitement par les autorités en charge de la surveillance. L'indication selon laquelle « des données à caractère personnel de banques de données existantes » pourront être utilisées dans le cadre des finalités de surveillance prévues par l'avant-projet, ne le dispense pas d'énumérer ces données dans l'avant-projet, conformément aux principes de légalité, prévisibilité, transparence, nécessité et proportionnalité (minimisation). Elle renvoie pour le surplus au chapitre IV (finalités) sur ce point.

L'Autorité s'étonne de l'indication dans l'avant-projet du fait que « les données à caractère personnel et les informations dont disposent les services de police peuvent également être communiquées aux autorités publiques belges, organes ou organismes publics, ou d'intérêt public en charge de la gestion de la situation d'urgence épidémique et qui sont désignés par le ministre compétent de l'Intérieur et de la Justice ». Ces données ne sont en effet pas définies (et le terme « données à caractère personnel et les informations dont disposent les services de police » ne répond pas à l'exigence de précision), la finalité de leur utilisation pas détaillée, la nécessité de leur utilisation en vue d'atteindre cette finalité pas démontrée⁴.

Enfin, l'Autorité se demande la portée qu'il faut donner à l'alinéa prévoyant que « Le Roi **précise**, par arrêté délibéré en Conseil des ministres, après avis de l'autorité de contrôle de la protection des données compétente, ces données, et ce en fonction de la situation d'urgence épidémiologique».

S'il s'agit à nouveau de déléguer au pouvoir exécutif le pouvoir de définir les (catégories de) données qui pourront être traitées, sans uniquement préciser les données listées dans l'avant-projet, il s'agit d'un manquement aux dispositions précitées consacrant les principes de légalité et prévisibilité.

III. L'AVANT-PROJET NE DEFINIT PAS LE(S) RESPONSABLES DES TRAITEMENTS DE DONNEES

L'avant-projet de loi ne mentionne pas quelle(s) autorité(s) endossera/ont la qualité de responsable du traitement pour les traitements de données qu'il entend autoriser au travers de cet avant-projet, ce qui s'explique par l'absence de définition de ces traitements de données.

La désignation du (des) responsable(s) du traitement de tout traitement de données constitue un élément essentiel du traitement qui doit être défini de manière transparente par une norme de rang de loi, en l'occurrence l'avant-projet (une fois définis les traitements de données envisagés) ou une norme de rang de loi ultérieure dont l'objet serait d'encadrer correctement les traitements de données envisagés en en définissant les éléments essentiels.

IV. LA DEFINITION DES FINALITES POUR LESQUELLES DES DONNEES POURRONT ETRE TRAITEES NE PERMET PAS D'APPREHENDER L'USAGE QUI SERA FAIT DES DONNEES

L'avant-projet prétend définir les finalités pour lesquelles des données pourront être utilisées dans le cadre de la gestion d'une situation d'urgence pandémique. Son article 6§2 énumère en effet trois finalités, étant la surveillance et le contrôle du respect des mesures prises en application de ses articles 4 et 5, par les services de police, autorités sociales et gouverneurs ou bourgmestres.

⁴ et l'Autorité peine à comprendre pourquoi les autorités citées ne correspondent pas aux autorités énumérées à l'article 6§6 de l'avant-projet qui définit les autorités autorisées à traiter les données « visées » au paragraphe 6§5 (voir ci-dessus)

Dans la mesure où l'avant-projet est muet quant à ces mesures et où il ne définit pas les données qui seront traitées pour atteindre ces finalités de surveillance et de contrôle, l'Autorité estime qu'il est difficile, malgré une description apparemment claire des finalités, d'en comprendre l'objectif précis.

En l'état, l'avant-projet, vu la généralité des termes utilisés, l'absence de définition des traitements de données qu'il entend légitimer et l'absence de liens avec les finalités, ne permet pas d'encadrer valablement les traitements de données potentiels auxquels il pourrait donner lieu. A titre d'exemples, il pourrait ainsi permettre :

- D'imposer aux citoyens belges le port d'un bracelet électronique relié à une banque de données permettant de surveiller en temps réel leurs déplacements et le respect d'une interdiction de déplacement (ou de déplacement après une certaine heure) ;
- De photographier les plaques d'immatriculation des véhicules quittant ou rentrant sur le territoire belge, de les relier avec la banque de données existante de la Division de l'Immatriculation des Véhicules (DIV) et d'en appréhender les propriétaires ;
- De mettre en place des technologies de reconnaissance faciale afin d'identifier les promeneurs dans les parcs et se vérifier qu'ils ne font pas l'objet d'un ordre de quarantaine ;
- De contrôler les déplacements des citoyens au moyen de la géolocalisation de leur téléphone mobile éventuel ; ou encore
- De recourir à l'identification obligatoire au moyen d'un QR code sur téléphone mobile ou d'une vérification via l'empreinte digitale apposée dans la puce de l'e-ID pour contrôler le droit d'accéder à certains lieux ou transports ou pour contrôler le statut du citoyen (vacciné ou non par exemple).

L'avant-projet semble en outre vouloir opérer une extension d'office et en bloc des possibilités d'utilisation de données contenues dans toutes les banques de données en possession de toutes les autorités publiques belges, donc de toutes les données détenues et utilisées par toutes ces institutions dans le cadre de l'exécution de leurs missions (données fiscales, médicales, sociales, pénales etc). Et ce, en édictant arbitrairement que les finalités de surveillance et de contrôle sont considérées comme « compatibles » avec les finalités pour lesquelles ces données ont été collectées et utilisées initialement. Le second alinéa de l'article 6§3 est en effet rédigé comme suit :

« Lorsque les mesures prises en application des articles 4, §1^{er}, alinéa 2 et 5, 1^{er}, a) à h) nécessitent que des données à caractère personnel de banques de données existantes soient utilisées pour les finalités visées au §2, alinéa 1^{er}, 1^o à 3^o, ou nécessitent qu'une banque de données existante soit alimentée avec d'autres catégories de données, une telle utilisation ou un tel élargissement est considéré comme un traitement ultérieur compatible nécessaire à l'exécution d'une mission d'intérêt public au sens des réglementations relatives à la protection des traitements de données à caractère personnel ».

Si le RGPD évoque une possibilité de traitement ultérieur de données pour des finalités autres que celles pour lesquelles elles avaient été collectées,

- une telle réutilisation de données requiert la réalisation d'une analyse de compatibilité (tenant compte des éléments repris à l'article 6.4 du RGPD) sur base des éléments factuels de chaque traitement de sorte que la confirmation de **la compatibilité d'une finalité avec une finalité indéterminée (celle qui a mené à la constitution de la banque de données initiale) doit faire l'objet d'une analyse au cas par cas et ne peut être décrétée à priori**
- cette possibilité ne fait pas échapper l'auteur de l'avant-projet à son obligation de respecter les principes généraux de la protection des données précités de sorte qu'il lui revient de reprendre dans l'avant-projet les données dont il entend permettre le traitement à des fins de contrôle et surveillance et qui figureraient dans des banques de données existantes (conformément aux principes de légalité et transparence notamment)

V. L'AVANT-PROJET NE DEFINIT PAS LES DESTINATAIRES POTENTIELS DES DONNEES NI LES TRAITEMENTS QU'ILS POURRONT EN FAIRE

Le §7 de l'article § de l'avant-projet indique que les données à caractère personnel (visées par le présent article) « ne peuvent être transmises qu'après qu'un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données ait été conclu, (...) ou après une délibération du comité de sécurité de l'information (...) ».

Si le transfert de données doit être encadré par un protocole tel que prévu à l'article 20 de la LTD, il n'est pas nécessaire de le rappeler dans l'avant-projet, l'obligation légale étant déjà consacrée par cet article 20. Cette obligation n'enlève rien au fait que l'avant-projet doive mentionner explicitement quelles catégories de destinataires peuvent recevoir quelles données et les finalités pour lesquelles ces données peuvent être communiquées à et utilisées par ces tiers. Un protocole ne remplace en d'autres termes pas l'obligation d'indication de cet élément essentiel dans une norme de rang de loi, en l'occurrence l'avant-projet ou une norme de rang législatif ultérieure. Un protocole n'autorise pas un tel transfert, il en modalise les détails techniques et opérationnels.

Il en va de même en ce qui concerne une délibération du Comité de sécurité de l'information : si l'avant-projet prévoit une indication claire des catégories de destinataires qui pourront se voir transmettre quelles données et à quelles fins, une délibération du Comité de sécurité de l'information précisera les modalités d'exécution de ce transfert, en particulier sur le plan de la sécurité de l'information. Il n'autorisera pas ce transfert.

VI. ABSENCE DE DEMONSTRATION DE LA NECESSITE DES TRAITEMENTS DE DONNEES ET VIOLATION DES PRINCIPES DE MINIMISATION ET PROPORTIONNALITE

Dans la mesure où l'avant-projet ne définit pas les traitements de données auxquels il entend pourtant donner une « base légale », il reste en défaut de démontrer en quoi ces traitements de données sont nécessaires afin d'accomplir la finalité recherchée.

Cette absence de justification de (la nécessité de) ces traitements rend par ailleurs impossible tant pour notre Autorité que pour les députés qui seront amenés à examiner l'avant-projet de juger si les traitements de données que l'avant-projet pré-validerait sans en connaître les contours, sont effectivement nécessaires dans le cadre de la lutte contre une pandémie et proportionnés à l'objectif poursuivi.

VII. CONTRARIETE AU PRINCIPE DE TRANSPARENCE

La transparence due aux citoyens relativement aux utilisations de leurs données effectuées par l'Etat requiert que les traitements de leurs données soient reflétés, après le vote au parlement, dans un texte clair et accessible.

Or l'avant-projet fait référence à des données contenues dans des banques de données multiples et non-identifiées qui pourraient ainsi être recyclées à des fins de contrôle et surveillance, sans autre précision. Il tend ainsi à rendre légale l'utilisation de ces données (ou la poursuite de cette utilisation) par une disposition générale et abstraite et sans fournir la moindre indication quant à ces traitements de données. En contrariété avec les exigences de transparence puisqu'aucune visibilité n'est fournie aux intéressés quant à ces réutilisations inattendues de leurs données à des fins de surveillance. S'est envisagé de puiser dans des banques de données existantes aux fins d'accomplissement des finalités de surveillance prévues par l'avant-projet, les éléments essentiels de ces nouveaux traitements de données portant sur des données existantes doivent faire l'objet d'une définition claire et précise dans l'avant-projet⁵.

Dans cette même optique de transparence vis-à-vis des citoyens, il est recommandé d'éviter que la définition des traitements de leurs données qui pourraient être effectués dans le cadre d'une pandémie soient éparpillés dans une multitude de textes législatifs éparses. Les traitements de données envisagés dans le cadre du traçage des contacts, de l'organisation et du suivi de la vaccination ainsi que tout autre traitement, en ce compris à des fins éventuelles de profilage devraient être répertoriés et détaillés dans un seul et même instrument législatif.

⁵ L'Autorité se demande par ailleurs comment les membres du parlement pourraient juger de l'acceptabilité de cette habilitation à se servir de toutes les données que les citoyens ont un jour confiées à une autorité publique avec un objectif déterminé.

VIII. AUTRES REMARQUES :

a) Contrôle par les autorités de contrôle (sur art 36.4 RGPD)

En ce qu'il prévoit, à plusieurs reprises, sur quoi devra porter l'avis de l'autorité de contrôle et en limite ainsi l'étendue, l'avant-projet ne fait pas une application correcte de l'article 36.4 du RGPD.

En ce qu'il prévoit que l'autorité de contrôle émettra un avis sur les arrêtés-royaux d'exécution dans un délai de 5 jours calendrier, l'avant-projet :

- omet le fait que les avis de l'Autorité sont le fruit d'un organe collégial et non pas seulement du secrétariat de l'Autorité et de la Directrice du Centre de connaissances – un délai doit dès lors être prévu pour permettre aux autres membres de cet organe d'effectuer une relecture et de formuler des commentaires et suggestions - un délai réaliste doit également être prévu pour finaliser le projet d'avis, le cas échéant après discussion verbale avec tous les membres
- omet également le fait que le personnel de l'Autorité ne peut pas être contraint de travailler les week-ends et jours fériés, rendant la référence à des jours calendrier inappropriée

b) Violation de l'interdiction de retranscription du RGPD

A plusieurs occasions, l'avant-projet viole le principe de l'interdiction de retranscription du RGPD : rappel du fait que les traitements de données seront conformes au RGPD, rappel de l'obligation d'effectuer une analyse d'impact, etc. L'Autorité comprend la tentation de reprendre de telles obligations afin de rassurer le lecteur mais se doit de demander la suppression de ces retranscriptions.

IX. CONCLUSION ET ADAPTATIONS A APPORTER A L'AVANT-PROJET

Contrairement à ce qu'il annonce à l'alinéa 1^{er} de l'article qu'il consacre aux traitements de données à caractère personnel (article 6), l'avant-projet ne crée pas une base légale qui encadre et autorise certains traitements de données à caractère personnel qui seraient nécessaires pour assurer le respect de mesures de police dans le cadre de la gestion d'une pandémie. De tels traitements de données à caractère personnel doivent être encadrés par une norme de rang de loi qui en définisse avec précision tous les « éléments essentiels » qui sont définis comme tels par l'article 6.4. du RGPD. La détermination de ces « éléments essentiels » ne peut pas être déléguée au pouvoir exécutif comme le fait l'avant-projet en introduisant, à côté la notion d'« éléments essentiels » dont la définition pourraient être déléguée au ministre ou au Roi, celle d'« éléments les plus essentiels » (notion dont le contenu est obscur) que définirait l'avant-projet. Cette construction constitue une violation flagrante des principes les plus élémentaires de la protection des données à caractère personnel, en ce compris les principes de légalité (consacré par l'article 22 de la Constitution, lu conjointement avec l'article 8 de la CEDH et l'article 6.3 du RGPD) mais également de prévisibilité, de nécessité et de proportionnalité (minimisation).

Cette exigence de légalité tient au fait que des traitements de données qui impliquent une ingérence importante dans la vie des citoyens et leur droit à la protection des données doit faire l'objet d'un débat entre les élus du peuple, à savoir le parlement. Le parlement et les citoyens Ils doivent être en mesure, sur base du texte proposé, de comprendre la nature et l'objectif de chaque traitement de données proposé, en d'autres termes « quelle autorité utilisera quelles données et pourquoi » mais également de pouvoir définir si le traitement de données proposé est nécessaire pour atteindre la finalité poursuivie et si cette finalité est légitime.

Pour reprendre un des exemples précités, le parlement doit être en mesure de définir si la détermination des conducteurs qui franchissent les frontières grâce à des images prises de leur plaque d'immatriculation combinées avec la banque de données de la DIV afin de contrôler le respect d'une interdiction de voyager est un traitement de données nécessaire et proportionnel au but recherché, à savoir le maintien de l'étanchéité de nos frontières en vue d'empêcher la propagation de variantes étrangères d'un virus.

L'avant-projet, en ce qu'il remet à plus tard la définition de tous les éléments essentiels des traitements de données qu'il souhaite autoriser en bloc, ne permet pas aux élus d'appréhender le caractère légitime et proportionné de ces traitements de données. Ces traitements de données seront en conséquence déterminés par le pouvoir exécutif sans permettre ce débat essentiel qui garantit le fonctionnement démocratique de notre état de droit. En contrariété avec les dispositions de droit supérieur qui consacrent le principe de légalité.

Si l'on comprend bien, face aux critiques et à la demande grandissante de voir élaboré un cadre légal qui circonscrive les nombreux traitements de données à caractère personnelles auxquels il a été recouru dans le cadre de la crise sanitaire en cours, il n'est pas acceptable :

- que l'on tente artificiellement de donner une légitimité aux traitements de données existants au travers d'une loi qui n'en poserait même pas les éléments essentiels ; ni
- que l'on autorise, au travers de la même loi, des traitements de données non-encore envisagés et au sujet desquels le parlement n'est dès lors pas en mesure de se prononcer

L'Autorité rappelle par ailleurs qu'une loi ne saurait donner une légalité à la pratique inconstitutionnelle qui consiste à organiser des traitements de données donnant lieu à une ingérence importante par la voie d'arrêtés.

Si l'auteur de l'avant-projet estime qu'il est à ce jour impossible de définir avec précision les éléments essentiels de tous les traitements de données qui seront nécessaires afin de surveiller le respect des mesures de police qui seront prises dans le cadre d'une future pandémie, il est invité :

- à supprimer l'article 6 de l'avant-projet ;
- à rédiger un texte normatif qui encadre correctement les traitements de données dont l'utilité et la nécessité ont été confirmées dans le cadre de la gestion de la crise actuelle ; et pour le surplus ;

- plutôt que de prétendre autoriser à l'avance des traitements de données qu'il n'est pas en mesure de définir, de fixer dans une loi des règles de procédure allégées créant un cadre législatif souple pour la définition de tels traitements - on pense notamment à une procédure dans le cadre de laquelle le parlement serait amené à voter dans des délais très réduits des lois qui mettraient en oeuvre les traitements de données envisagés

PAR CES MOTIFS,

l'Autorité, estime que l'avant-projet doit être revu en tenant compte du présent avis.

(sé) Alexandra Jaspar

Directrice du Centre de Connaissances