Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Table ronde Constitution, libertés et numérique

Degrave, Elise; Verdussen, Marc

Published in:
Annuaire international de justice constitutionnelle

Publication date:
2022

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Degrave, E & Verdussen, M 2022, Table ronde Constitution, libertés et numérique: Belgique. dans *Annuaire international de justice constitutionnelle: XXXVII.* Economica, Paris, pp. 169-195.

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.

Download date: 02. May. 2026

Institut Louis Favoreu
Groupe d'Études et de Recherches
sur la Justice Constitutionnelle
Équipe associée au CNRS (UMR 7318)
Aix-en-Provence

Annuaire International de Justice Constitutionnelle

XXXVII

2021
(extraits)

ECONOMICA
49, rue Héricart
75015 Paris

PRESSES UNIVERSITAIRES D'AIX-MARSEILLE
3, Avenue R. Schuman
13628 Aix-en-Provence cedex 01

2022

TABLE RONDE
CONSTITUTION, LIBERTÉS ET NUMÉRIQUE

BELGIQUE

Élise DEGRAVE et Marc VERDUSSEN[*]

Comment la Constitution belge et, plus globalement, le droit constitutionnel belge appréhendent-ils la mise en œuvre des droits et libertés fondamentaux à l'heure numérique ? La question est abordée sous deux angles, celui du contenu des droits et libertés (I) et celui des modes de protection de ces droits et libertés (II). Les réponses restent très provisoires tant les défis que le numérique pose à la science constitutionnelle sont nouveaux : « *The challenges posed by the intersection of the internet and the Constitution are not easy ones. But they are challenges and tensions for a free society to sort out over time* »[1].

I.- LA SUBSTANCE DES DROITS ET LIBERTÉS FONDAMENTAUX : QUELLES SPÉCIFICITÉS À L'HEURE NUMÉRIQUE ?

On examinera successivement la reconnaissance de droits fondamentaux numériques (A), l'incidence du numérique sur l'exercice des droits fondamentaux classiques (B) et, enfin, les enjeux constitutionnels de l'impact du numérique sur les personnes vulnérables (C).

A.- La reconnaissance de droits fondamentaux numériques

Des droits fondamentaux numériques ont-ils été intégrés dans le texte constitutionnel (1), dégagés par la Cour constitutionnelle (2) ou consacrés par le législateur (3) ?

---

* Respectivement Professeure à l'Université de Namur, directrice de recherches au Namur Digital Institute (NADI) et au Centre de recherche Information, Droit et Société (CRIDS) et co-directrice de la Chaire E-gouvernement ; Professeur à l'Université de Louvain et directeur du Centre de recherche sur l'État et la Constitution (CRECO).

1 M. Margaret MCKEOWN, « The internet and the Constitution: A Selective Retrospective », *Washington Journal of Law Technology & Art*s, 2014, vol. 9, p. 175.

1.- Des droits fondamentaux numériques ont-ils été intégrés dans le texte constitutionnel ?

La Constitution belge a été adoptée en 1831. Elle a fait ultérieurement l'objet de plusieurs révisions, surtout à partir de 1970. Certaines d'entre elles concernent les droits fondamentaux qui, pour la plupart, sont énumérés dans le Titre II. Les modifications apportées à ces droits après 1831 sont censées être les marques de glissements, de changements, voire de bouleversements, dans la représentation politique des valeurs fondamentales de la société. En effet, dans nos sociétés politiques libérales, soucieuses de l'épanouissement de la personne humaine, les droits constitutionnels ont vocation à traduire une convergence éthique sur les exigences sociales les plus vitales. Force est pourtant de constater que les modifications apportées jusqu'ici aux droits constitutionnels sont occasionnelles et donc isolées. Elles sont dictées par des occurrences particulières. En procédant par petites touches successives – ce qui est la définition même du pointillisme –, on introduit inévitablement dans la Constitution des illogismes et, partant, on y sème un certain désordre. Mais surtout, les révisions au coup par coup trahissent dans le chef du Constituant un inquiétant manque d'ambition[2].

Dans un tel contexte, il n'est guère étonnant que la Constitution belge ignore le numérique. Certes, des propositions ont été déposées sur le bureau de la Chambre des représentants et du Sénat, qui visent à modifier l'article 23 de la Constitution, relatif aux droits économiques, sociaux et culturels, par l'ajout d'un « droit d'accéder à l'internet »[3], d'un « droit d'accéder à l'outil internet »[4], d'un « droit à l'accès à un réseau public de communications électroniques qui soit neutre »[5], d'un « droit à un accès suffisant et neutre à l'internet »[6] ou encore d'un « droit d'accès à un internet neutre et ouvert »[7]. Aucune de ces propositions n'a été discutée.

Or, le numérique a désormais sa place dans la Constitution. Il représente en effet un espace singulier de mise en œuvre de plusieurs droits fondamentaux classiques. Le droit d'accéder à internet ne doit-il pas dès lors compter parmi les droits fondamentaux ? La reconnaissance d'un tel droit mérite un débat constituant. Les questions ne manquent pas. Faut-il consacrer le droit d'accéder gratuitement à internet ? Chez soi ou suffit-il que des accès collectifs gratuits soient prévus ? Le droit d'accéder à internet englobe-t-il le droit d'y participer ? Le droit de comprendre l'outil numérique, afin de ne pas être touché par l'« illectronisme » ? comporte-t-il pour le citoyen un droit de contrôle sur ses données personnelles, voire un droit de rectification ? Un droit de s'opposer à leur utilisation ? Un droit à l'oubli ?

Par ailleurs, le développement du numérique nécessite sans doute une adaptation de dispositions constitutionnelles existantes. Par exemple, lorsque la Constitution proclame que « la presse est libre » (art. 25, al. 1er), elle est dépassée par les évolutions technologiques des moyens d'information. Une controverse est née sur

---

2 Sur ce thème, v. M. VERDUSSEN, *Réenchanter la Constitution*, Bruxelles, Académie royale de Belgique, 2019, p. 54-59.

3 *Doc. parl.*, Sénat, 2011-2012, n° 5-1466/1 ; *Doc. parl.*, Ch. repr., 2011-2012, n° 53-2046/1 ; *Doc. parl.*, Sénat, 2012-2013, n° 5-1982/1 ; *Doc. parl.*, Sénat, 2014-2015, n° 7/1 ; *Doc. parl.*, Sénat, 2014-2015, n° 6-43/1.

4 *Doc. parl.*, Sénat, 2013-2014, n° 5-2400/1; *Doc. parl.*, Sénat, SE 2019, n° 7-12/1.

5 *Doc. parl.*, Ch. repr., 2010-2011, n° 53-1471/1.

6 *Doc. parl.*, Ch. repr., 2012-2013, n° 53-3005/1.

7 *Doc. parl.*, Ch. repr., SE 2014, n° 54-346/1 ; *Doc. parl.*, Ch. repr., SE 2019, n° 55-145/1.

le sens du mot « presse » et, partant, sur la portée de l'article 25[8]. Une nouvelle disposition, intégrant les médias modernes (radio, télévision et internet), faciliterait la vie de juges divisés sur l'interprétation à donner au mot « presse ». Autre exemple, lorsque la Constitution reconnaît à chacun le « droit au respect de sa vie privée » (art. 22, al. 1er), la question se pose de savoir si ce droit ne devrait pas être doublé d'un droit à la protection des données à caractère personnel, tant ces données sont plus larges que les données strictement privées et tant leur garantie soulève des problèmes très spécifiques. Concédons néanmoins que la question est délicate, car le risque existe « d'oublier l'ancrage fondamental des régimes de protection des données dans les principes de dignité et d'autonomie humaine qui sont à la base de la protection de la vie »[9]. Quoi qu'il en soit, la Cour constitutionnelle considère que la protection des données à caractère personnel fait partie de la vie privée, ce qu'elle a encore rappelé le 14 janvier 2021[10].

On mentionnera ici la révision récente de l'article 149 de la Constitution. Adopté lui aussi en 1831 et resté inchangé jusqu'en 2019, l'article 149 de la Constitution était rédigé en ces termes : « Tout jugement est motivé. Il est prononcé en audience publique ». Le 22 avril 2019, l'article 149 a été remplacé par la disposition suivante : « Tout jugement est motivé. Il est rendu public selon les modalités fixées par la loi. En matière pénale, son dispositif est prononcé en audience publique »[11]. Si le nouveau texte constitutionnel ne se réfère pas au numérique, les débats parlementaires ont clairement envisagé la publication des arrêts et jugements sur le web, c'est-à-dire dans une banque de données électronique accessible au public. La publication de ceux-ci sur internet, dans une banque de données électronique accessible au public, peut contribuer à réduire la discrimination dans l'accès des citoyens aux décisions de justice et à assurer un meilleur contrôle démocratique du fonctionnement du pouvoir judiciaire[12]. D'ailleurs, dans la foulée de cette modification constitutionnelle, le législateur fédéral a adopté, le 5 mai 2019, une loi modifiant le Code d'instruction criminelle et le Code judiciaire en ce

8 F. JONGEN et A. STROWEL (avec la collab. de E. CRUYSMANS), *Droit des médias et de la communication*, Bruxelles, Larcier, 2017, p. 87-91.

9 E. DEGRAVE et Y. POULLET, « Le droit au respect de la vie privée face aux nouvelles technologies », in M. VERDUSSEN et N. BONBLED (dir.), *Les droits constitutionnels en Belgique – Les enseignements jurisprudentiels de la Cour constitutionnelle, du Conseil d'État et de la Cour de cassation*, Bruxelles, Bruylant, 2011, vol. 2, p. 1011.

10 CC, arrêt n° 5/2021, 14 janvier 2021, B.18.4.

11 *Mon. b.*, 2 mai 2019, p. 42442.

12 La mise en ligne par la voie d'internet emporte cependant le risque de porter atteinte au droit au respect de la vie privée des parties. S'agissant du nom et du prénom d'un justiciable, on voit mal quel motif légitime justifie sa divulgation sinon la facilité qu'une telle identification offre à la communauté des juristes pour désigner certains arrêts ou jugements, ce qui n'est pas évidemment un motif suffisant. D'où la nécessité d'imposer la pseudonymisation des décisions mises en ligne (pénales et civiles), à la fois des données directement nominatives (nom et prénom) et des données indirectement nominatives (comme l'adresse). La pseudonymisation, et non l'anonymisation. Anonymiser une décision de justice, c'est biffer à l'égard de tous, y compris la juridiction et son greffe, les données personnelles des parties – en réalité tout ce qui peut contribuer à les identifier – de telle sorte que celles-ci ne sont plus du tout identifiables, par qui que ce soit. Le procédé n'est pas souhaitable, car il aboutit à vider complètement la décision de sa substance, au risque de la rendre insignifiante. Pseudonymiser, c'est remplacer le nom et le prénom des parties par leurs initiales ou par tout autre pseudonyme, étant entendu que la juridiction et son greffe peuvent à partir du pseudonyme retrouver le nom et le prénom des parties. C'est déjà beaucoup plus envisageable, même si ce n'est pas sans poser des questions. Ainsi, est-il réellement possible de garantir absolument la pseudonymisation des décisions de justice ? Est-on certain que, par des traitements algorithmiques, il est impossible de retrouver l'identité d'une personne qui aurait fait l'objet d'une ou plusieurs décisions pseudonymisées ?

qui concerne la publication des jugements et des arrêts, loi qui s'inscrit dans cette perspective[13].

2.- Des droits fondamentaux numériques ont-ils été reconnus par la Cour constitutionnelle ?

Il y a quelques années, un recours en annulation a été introduit auprès de la Cour constitutionnelle contre l'article 40, § 6, alinéa 2, du décret flamand du 27 mars 1991 relatif à la pratique du sport dans le respect des impératifs de santé, inséré par l'article 31 du décret flamand du 19 mars 2004 modifiant le décret du 27 mars 1991 relatif à la pratique du sport dans le respect des impératifs de santé, qui dispose : « Les suspensions disciplinaires des sportifs majeurs sont publiées pour la durée de la suspension sur le site web que le Gouvernement crée à cet effet et par les canaux de communication officiels créés par les fédérations sportives. Cette publication contient les nom, prénom et date de naissance du sportif, le début et la fin de la période de suspension et la discipline sportive qui a donné lieu à l'infraction ». Ce recours était fondé notamment sur l'article 22 de la Constitution[14].

Dans son arrêt[15], la Cour souligne que « publier des données personnelles d'une manière aussi générale constitue une ingérence dans le droit au respect de la vie privée garanti par l'article 22 de la Constitution et par les dispositions conventionnelles susmentionnées. Pour qu'une telle ingérence soit admissible, il est requis qu'elle soit nécessaire en vue d'atteindre un but légitime déterminé, ce qui implique notamment qu'un lien raisonnable de proportionnalité doive exister entre les conséquences de la mesure pour la personne concernée et les intérêts de la collectivité » (B.5.1). Mais elle ajoute : « En outre, le législateur décrétal doit avoir égard à l'article 22, alinéa 1er, de la Constitution, en vertu duquel seul le législateur fédéral peut déterminer dans quels cas et à quelles conditions le droit au respect de la vie privée et familiale peut être limité. Une ingérence dans la vie privée qui s'inscrit dans la réglementation d'une matière déterminée relève certes du législateur compétent pour régler cette matière, mais le législateur décrétal est tenu de respecter la réglementation fédérale générale, qui a valeur de réglementation minimale pour toute matière. En tant que la disposition entreprise vise la publication de données personnelles, elle implique que le législateur décrétal est tenu par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel » (B.5.2).

Par après, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel a été abrogée et remplacée par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[16]. Désormais, la loi du 30 juillet

13 *Mon. b.*, 16 mai 2019, p. 47030. C. BEHRENDT et A. JOUSTEN, « La révision de l'article 149 de la Constitution : la publicité des décisions judiciaires à l'ère du numérique », *Journal des tribunaux*, 2020, p. 2-8 ; S. VAN DROOGHENBROECK, « Note à l'attention de la Commission de la révision de la Constitution et des réformes institutionnelles de la Chambre des représentants », *Revue belge de droit constitutionnel*, 2019, p. 249-261 ; M. VERDUSSEN, « Note à l'attention de la Commission de la révision de la Constitution et des réformes institutionnelles de la Chambre des représentants », *ibid*., p. 263-273.

14 « Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit. »

15 CC, arrêt n° 16/2005, 19 janvier 2005. Égal. CC, arrêt n° 50/2003, 30 avril 2003, B.8.10. E. DEGRAVE, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *Journal des tribunaux*, 2009, spéc. p. 366-367.

16 *Mon. b.*, 5 septembre 2018.

2018 forme avec Règlement général sur la protection des données[17] (ci-après : RGPD) « la réglementation fédérale générale, qui a valeur de réglementation minimale pour toute matière », selon les termes de la Cour. Les droits reconnus par cette réglementation générale ne sont pas des droits de valeur constitutionnelle, mais la Cour leur attribue tout de même un rang supralégislatif.

3.- Des droits fondamentaux numériques ont-ils été consacrés par le législateur ?

Si l'on considère que les droits fondamentaux sont « des droits garantis par un texte constitutionnel et/ou garantis par des textes conventionnels, voire déduits de ces textes, et dont le respect peut être invoqué devant un juge, y compris à l'égard de l'action du législateur »[18], il faut admettre que les « droits » et « garanties » reconnus aux citoyens dans la législation sur la protection des données à caractère personnel ne sont pas formellement des droits qu'on peut tenir pour « fondamentaux ». Ce sont des droits à caractère législatif, voire – comme on vient de l'expliquer – supralégislatif.

B.- L'incidence du numérique sur l'exercice des droits fondamentaux classiques

La Cour constitutionnelle a rendu quelques arrêts ayant pour objet une ou plusieurs questions relatives à la compatibilité de dispositifs législatifs en matière numérique avec des droits fondamentaux généraux reconnus par le Titre II de la Constitution. Des arrêts ont également été rendus par d'autres juridictions. Par ailleurs, en amont, ces questions ont donné lieu, peu ou prou, à des débats législatifs. Il est impossible dans le cadre de cette contribution d'aborder sérieusement l'ensemble des questions. Nous nous limitons donc à une problématique, étroitement liée à l'actualité, celle du traitement des données à caractère personnel par l'État.

La crise sanitaire déclenchée par la Covid-19 a donné un coup de projecteur aux outils numériques utilisés par l'État, à l'occasion notamment de la mise en place d'applications de traçage comme *Stopcovid* ou du « pass sanitaire ». Les lignes qui suivent abordent les différents problèmes posés au départ de la gestion des données à caractère personnel des citoyens par l'État.

De prime abord, on pourrait croire que le numérique est la version moderne des pratiques qui, hier, se formalisaient sur papier. Jadis consigné dans un dossier en carton jaune, le dossier administratif d'un citoyen est aujourd'hui transposé, en format dématérialisé, dans une base de données détenue par l'État permettant d'être plus efficace dans le traitement des multiples informations relatives aux citoyens. Certes, numérisation rime avec dématérialisation et gain d'efficacité. Mais il y a bien plus. Le numérique offre une puissance inconnue de l'univers papier.

D'une part, il est désormais beaucoup plus simple de réutiliser une information grâce à un dialogue organisé d'administration à administration, qui leur

---

17 Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, dit « Règlement général sur la protection des données ».

18 G. ROSOUX, *Vers une « dématérialisation » des droits fondamentaux ? – Convergence des droits fondamentaux dans une protection fragmentée, à la lumière du raisonnement du juge constitutionnel belge*, Bruxelles, Bruylant, 2015, p. 260-261.

permet de s'échanger les informations dont elles ont besoin et dont elles ne disposent pas nécessairement. Cela encourage la simplification administrative en épargnant au citoyen la contrainte de devoir fournir vingt-cinq fois la même donnée à des administrations différentes. Par exemple, en Belgique, l'arrivée d'un enfant dans une famille est enregistrée dans une base de données appelée le Registre national, qui contient notamment la composition de famille de chaque citoyen. Une fois enregistrée, cette donnée pourra être réutilisée par l'administration fiscale, afin d'adapter en conséquence les impôts dus par les parents, et l'administration chargée de verser les allocations familiales.

Néanmoins, la réutilisation aisée des données signifie également qu'il est désormais plus simple, et peut-être plus tentant, d'abuser de ces informations en les utilisant de manière illégale, qu'il s'agisse pour un agent de l'administration d'aller consulter l'adresse de son ex-compagne, pour un policier d'accéder au numéro de téléphone d'une conductrice dont il aurait noté la plaque d'immatriculation, ou encore d'un pirate informatique « *hackant* » une base de données santé dans le but de revendre ces informations à des sociétés d'assurance. Dans l'univers papier, l'agent de l'administration qui souhaitait réutiliser une information devait d'abord la retrouver dans les nombreux fichiers papier de l'administration, la photocopier, la placer dans une enveloppe, apposer un timbre, et poster la lettre. Aujourd'hui, en quelques « clics » une information est accessible depuis son écran, et peut être transférée, ou copiée.

D'autre part, le numérique permet d'exploiter les données de manière beaucoup plus puissante que jadis. Le « *datamatching* » et le « *datamining* » sont des techniques informatiques applicables à des données. Le « *datamatching* »[19] est la première étape du processus, qui consiste à « croiser » les données, c'est-à-dire les rassembler et les comparer entre elles. La seconde étape est le « *datamining* »[20]. On applique aux données des algorithmes[21] qui vont induire de ces données des informations nouvelles, comme le ferait une boule de cristal. Cela permet de réaliser du profilage[22], c'est-à-dire de prédire la probabilité, pour chaque individu, d'adopter le comportement de tel profil d'individu (le profil de fraudeur par exemple)[23].

Il est tout à fait légitime que l'État recoure à des outils numériques pour réaliser ses différentes missions de service public, dans un objectif d'efficacité et de simplification administrative. Il n'en demeure pas moins que le numérique renforce la puissance de l'administration, qui a désormais entre ses mains énormément de données, facilement accessibles et finement exploitables. Qu'en est-il du citoyen ? S'il bénéficie, certes, de l'avancée de la simplification administrative, ne risque-t-il

19 En français : « couplage de données ».

20 En français : « extraction de données ».

21 Un algorithme peut être défini comme « un ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations » (Dictionnaire Larousse).

22 L'article 4.4 du RGPD définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

23 En guise d'exemple simple, prenons le cas de John, dont les données fiscales montrent qu'il gagne 2 000 euros par mois. Or, ses données à la Direction Mobilité et Sécurité routière (DIV) montrent qu'il détient sept Ferrari neuves et le Registre national indique qu'il est propriétaire de deux châteaux. Les algorithmes « anti-fraude » vont cibler John. Il sera rattaché à la catégorie des présumés fraudeurs fiscaux et sociaux et un contrôle fiscal et/ou social sera encouragé.

pas de se retrouver confronté à une administration kafkaïenne, dont la complexité, l'intangibilité et l'opacité échappent désormais à sa compréhension et son contrôle ?

Un État de droit doit protéger le citoyen d'une administration toute-puissante. Plusieurs exigences en découlent. Nous en identifions trois. Premièrement, le citoyen a le droit d'exiger que les pratiques de l'administration soient encadrées par des lois, claires et précises, adoptées au terme d'un débat démocratique éclairé et éclairant. C'est l'exigence de légalité, examinée ci-dessous (1). Deuxièmement, le citoyen a le droit de comprendre ce qu'il se passe dans l'administration, notamment s'agissant de l'usage qui est fait de ses données. C'est l'exigence de transparence, également examinée ci-après (2). Finalement, l'État de droit doit également protéger le citoyen d'abus de l'administration, en veillant à mettre en place les mécanismes de contrôle adéquats. C'est l'exigence de contrôle, sur laquelle nous nous attarderons dans la seconde partie de cette contribution (*infra*, II). Ces trois exigences classiques dans un État de droit sont bousculées par le numérique.

1.- Numérique et légalité

Lorsque l'État collecte, enregistre, réutilise les données des citoyens, il effectue des traitements de données à caractère personnel. Ceux-ci constituent des ingérences dans le droit fondamental à la protection de la vie privée, comme l'a affirmé à plusieurs reprises la Cour européenne des droits de l'homme[24]. Dès lors, ces traitements de données sont soumis au respect de l'article 22 de la Constitution et de l'article 8 de la Convention européenne des droits de l'homme, selon lesquels de telles ingérences sont admissibles à la condition d'être organisées par « une loi ».

En Belgique, à l'instar de nombreux autres États, ce principe de légalité impose une double exigence : la légalité formelle et la légalité matérielle des traitements de données. Par ailleurs, une menace pèse sur l'exigence de légalité : la technocratie.

a) Légalité formelle et matérielle des traitements de données

S'agissant de la légalité formelle, chaque ingérence dans la vie privée des citoyens doit être organisée par une norme législative au sens formel du terme. La Cour constitutionnelle l'a d'ailleurs déjà rappelé à plusieurs reprises, affirmant que « bien que, en utilisant le mot "loi", l'article 8.2 de la Convention européenne [des droits de l'homme] 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 »[25].

La seule existence d'une loi ne peut suffire pour encadrer les traitements de données de citoyens. Encore faut-il que cette loi soit de qualité suffisante pour permettre à chacun de déterminer, clairement et précisément, ce qu'il va advenir des données collectées à son sujet. C'est l'exigence de légalité matérielle.

La Cour constitutionnelle rappelle d'ailleurs régulièrement que l'article 22 de la Constitution « garantit à tout citoyen qu'il ne pourra être porté atteinte au respect

---

24 V. not. Cour eur. DH, *Amann c. Suisse*, 16 février 2000, req. n° 27798/95, § 65 ; Cour eur. DH, *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95, § 3 ; Cour eur. DH, arrêt *Shimovolos c. Russia*, 21 juin 2011, req. 30194/09, §§ 69-70.

25 CC, arrêt n° 151/2006, 18 octobre 2006, B.5.6. V. égal. CC, arrêt n° 29/2010, 18 mars 2010, p. 19, B.10.2. ; CC, arrêt n° 202/2004, 21 décembre 2004, B.4.3.

de sa vie privée qu'en vertu d'une disposition législative, et dans les conditions que celle-ci prévoit, de manière que chacun puisse savoir à tout moment à quelles conditions et dans quelles circonstances les autorités publiques pourraient s'ingérer dans ce droit »[26]. Dans le même sens, la Cour européenne des droits de l'homme insiste sur le caractère compréhensible et prévisible de la loi, en soutenant que la loi doit être « énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant, au besoin, de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable, les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé »[27].

S'inspirant de la jurisprudence de la Cour européenne des droits de l'homme[28], la Cour constitutionnelle, mais aussi la section de législation du Conseil d'État, ont dégagé les « éléments essentiels du traitement »[29], c'est-à-dire les éléments que le législateur doit déterminer dans la loi organisant le traitement de données envisagé[30]. Cette jurisprudence a d'ailleurs été rappelée maintes fois par l'Autorité de protection des données (ci-après : APD)[31] à propos, notamment, de la mise en place des bases de données liées au traçage et à la vaccination[32].

En somme, pour chaque traitement de données, le législateur doit déterminer, lui-même, quelle institution a accès à quelles données, pour quoi faire et pendant combien de temps. La détermination de ces éléments doit être l'occasion d'effectuer l'examen de proportionnalité des traitements de données par rapport à l'objectif poursuivi, en évaluant la pertinence et la nécessité des mesures envisagées. Ainsi, le législateur doit définir lui-même les *données* utilisées et leur *mode de collecte*. L'*objectif* poursuivi par le traitement, appelé également « finalité » du traitement, est un élément essentiel de celui-ci. Par ailleurs, le législateur doit mentionner les *personnes autorisées* à consulter une base de données ainsi que les *conditions* de cette consultation. Il en va de même de la *durée de conservation* des données. Cela suppose que le législateur fixe au moins les délais maximaux de conservation des données[33].

---

26 CC, arrêt n° 202/2004, 21 décembre 2004, B.4.3. V. égal. CC, arrêt n° 66/2013, 16 mai 2013, B.11.1.

27 V. not. Cour eur. DH, arrêt *Sunday Times c. Royaume-Uni*, 26 avril 1979, req. n° 6538/74 ; arrêt *Malone c. Royaume-Uni*, 2 août 1984, § 67; arrêt *Amann c. Suisse*, 16 février 2000, req. n° 27798/95, §§ 75-76 ; arrêt *Leander c. Suède*, 26 mars 1987, req. n° 9248/81, § 50.

28 Cour eur DH, arrêt *Rotaru c. Roumanie*, 4 mai 2000, req. 28341/95, § 57, *Revue trimestrielle des droits de l'homme*, 2001, p. 137, note O. DE SCHUTTER. Cet arrêt est fondamental en la matière car, pour la première fois, la Cour y dégage les éléments des traitements de données qui doivent figurer dans la loi pour que celle-ci soit précise et prévisible.

29 V. not. CC, arrêt n° 202/2004, 21 décembre 2004, B.6.2-B.6.3.

30 E. DEGRAVE, *L'E-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle*, Bruxelles, Larcier, coll. CRIDS, 2014, n° 103, et références citées.

31 Sur l'Autorité de protection des données, v. *infra*.

32 V. not. APD, avis n° 36/2020 du 29 avril 2020 sur une demande d'avis concernant un avant-projet d'arrêté royal de pouvoirs spéciaux portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19 (CO-A-2020-042), n° 38 *sq*. ; APD, avis n° 42/2020 du 25 mai 2020 sur une demande d'avis concernant une proposition de loi de loi portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus Covid-19 (CO-A-2020-048), n° 16 *sq*.

33 Avis n° L.37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc. parl.*, Ch. repr., 2004-2005, n° 1598/1 et 1599/1.

Enfin, la *communication* des informations, dite aussi « réutilisation » doit également être organisée par le législateur lui-même[34].

b) La raison d'être de l'exigence de légalité

Si une loi claire, précise et prévisible est nécessaire pour encadrer les traitements de données à caractère personnel, c'est parce qu'il est primordial que les représentants du peuple qui siègent au Parlement mènent un débat démocratique sur ces questions.

Ce débat démocratique doit être *éclairé*. Les questions sont souvent techniques et abstraites. Les auditions au Parlement, notamment, permettent d'auditionner publiquement des experts sur les enjeux de cette matière. S'ensuivent des débats axés sur les éléments essentiels des traitements de données envisagés. S'agissant, par exemple, de la vaccination, un tel débat aurait pu amener à réfléchir à plusieurs questions importantes. Or, pour l'essentiel, la Commission de la Santé de la Chambre des représentants s'est limitée à entendre de nombreux experts, qui plus est tardivement, sans ultérieurement engager le débat que ces auditions appelaient. Quelles sont les finalités exactes poursuivies par la base de données de vaccination ? Est-il proportionné, au regard de ces finalités, d'enregistrer ces données pendant trente ans après la date de vaccination ? Quelles autorités auront accès à ces données et pour quoi faire ?

Mener un débat sur ces questions afin de bien encadrer l'utilisation des données à caractère personnel est d'autant plus important que la vie privée est le socle des autres libertés. Par exemple, si les données santé sont mal utilisées, cela portera atteinte à la vie privée mais également au droit à l'égalité et à la non-discrimination, au droit d'aller et venir, à la liberté de culte[35], à la liberté d'expression[36], etc. Protéger la vie privée, c'est protéger l'ensemble des libertés[37].

Ce débat doit également être *éclairant.* Grâce, notamment, aux médias qui relaient ce débat, il est l'occasion d'informer le public sur les questions en jeu, la difficulté d'organiser la balance entre l'efficacité de l'État, d'une part, et la protection des libertés, d'autre part. Par exemple, en expliquant le raisonnement suivi pour encadrer la vaccination, le public aurait pu comprendre pourquoi il était nécessaire, le cas échéant, d'enregistrer les données de vaccination si longtemps et à quoi cela allait servir. Cela aurait été un élément permettant de gagner la confiance des citoyens, à propos de la gestion de leurs données mais, également, de la vaccination elle-même.

Cet effort de pédagogie et de publicité est d'autant plus important que la vie privée est une liberté particulière. À la différence d'autres libertés, on ne voit pas très bien ce que représente la vie privée, ni quand il y est porté atteinte. Lorsque le droit de rassemblement est suspendu, ne fût-ce que quelques jours, on l'éprouve

---

34 V. not. l'avis n° L. 29.125/4 du 14 avril 1999 sur un projet d'arrêté royal réglant les modalités de la gestion des billets à l'occasion des matches de football, cité par R. ANDERSEN et P. NIHOUL, « Le Conseil d'État. Chronique de jurisprudence 1999 », *Revue belge de droit constitutionnel*, 2000, p. 354.

35 Dans l'hypothèse, par exemple, où les données de traçage révèlent la fréquentation d'un lieu de culte précis.

36 Dans l'hypothèse, par exemple, où il est demandé à une personne de révéler l'identité du journaliste à qui elle a parlé car il s'agirait d'un cas-contact.

37 En ce sens, v. not. Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in K. BENYEKHLEF et P. TRUDEL (dir.), *État de droit et virtualité*, Montréal, Thémis, 2009, p. 210.

tangiblement. Tandis que la création d'une grande base de données comprenant moult informations à notre sujet n'engendre pas d'effets perceptibles par chacun, du moins à court terme. On peut raisonnablement penser que l'invisibilité de la vie privée explique, en partie, les craintes des citoyens à l'égard de la gestion de leurs données par l'État. Ces craintes doivent être entendues, car elles pourraient mettre à mal la confiance des citoyens pourtant nécessaire pour lutter contre le virus[38], mais aussi, plus généralement, pour permettre à l'État d'utiliser les données des citoyens afin d'effectuer ses missions au quotidien et simplifier les démarches administratives de chacun. De quoi justifier que l'on manie la vie privée avec particulièrement de clarté, de transparence et d'explication.

En d'autres termes, à condition de respecter l'exigence de légalité formelle et matérielle, le régime juridique de la protection des données n'empêche pas que des données soient utilisées par l'État, même à des fins de contrôle des citoyens, à condition que cette utilisation soit encadrée par une loi, au terme d'un débat ayant permis, notamment, de faire l'examen de proportionnalité des traitements de données envisagés et de déterminer clairement les éléments essentiels de ces derniers.

c) Une menace spécifique : la technocratie

Au fur et à mesure de l'évolution des technologies, les questions soumises au Parlement peuvent paraître de plus en plus complexes, mobilisant des connaissances techniques ainsi qu'à un vocable particulier, fait d'abréviations étranges et de concepts inédits par rapport auxquels le droit est peu familier. Ces difficultés peuvent donner un aspect très obscur aux questions juridiques discutées. Le risque naît alors que la technocratie prend le pas sur le débat démocratique. En effet, face aux questions techniques, les parlementaires et les ministres concernés préfèrent souvent en appeler à des experts. Ces derniers rédigent, dans l'ombre, le projet de loi. Le ministre concerné, faisant aveu de sa méconnaissance du dossier et de son manque de temps, l'approuve. S'ensuivent des débats au Parlement qui pâtissent de la technicité et peuvent souffrir d'un manque d'intérêt de la part des représentants du peuple.

Ces dérives ne sont pas propres à l'encadrement des technologies mais elles se révèlent ici avec une acuité particulière. Elles méritent notre attention parce que, bien que ces experts ne soient pas nécessairement malveillants, on ignore qui ils sont, on ne peut garantir leur indépendance politique ou économique et ils n'assument aucune responsabilité politique. En outre, ils sont chargés de rendre l'outil fonctionnel et auront donc à cœur d'être efficaces et rationnels au risque, peut-être, de négliger la protection des libertés citoyennes.

C'est pourquoi, à l'ère numérique, il est primordial que les élus se saisissent de tels enjeux et les encadrent minutieusement, sans se retrancher derrière l'urgence ou la technicité de la thématique. Il pourrait néanmoins être judicieux de réfléchir à la manière de les aider, de manière structurelle. À cet égard, une solution intéressante pourrait être de mettre en place une « chambre du temps long » ou

38 À cet égard, il est à présent clair que la confiance des citoyens est essentielle dans la lutte contre une pandémie. « Il n'existe pas de modèle idéal, à répliquer pour combattre le Covid-19. Mais les pays qui y parviennent le mieux ont un point commun : l'adhésion » (https://www.lecho.be/economie-politique/international/general/le-secret-des-pays-efficaces-face-a-la-pandemie-de-coronavirus/10258607.html)

« chambre du futur »[39]. Il s'agirait d'une troisième chambre législative, chargée de réfléchir aux enjeux futurs sur le long terme, en dehors de l'urgence du temps politique. Un tel organe pourrait utilement sous-tendre le travail législatif en matière numérique.

Par ailleurs, il pourrait être intéressant de recourir au mécanisme de la co-régulation, qui laisse au droit le soin de définir le cadre protecteur de la matière, tout en lui permettant de s'appuyer, pour la validation des aspects techniques, sur des organes composés de spécialistes de la matière. Ainsi, par exemple, il pourrait être envisagé de mettre en place un « Comité A », composé d'experts indépendants, capables d'analyser un algorithme et de vérifier notamment qu'il n'est pas affecté de biais. Cela n'est envisageable, bien évidemment, qu'à la condition de garantir l'indépendance complète de ce type d'organe, sous peine d'amplifier encore davantage le phénomène technocratique.

2.- Numérique et transparence

L'État est soumis à une double exigence de transparence, dont la mise en œuvre se heurte à d'épineuses difficultés.

a) La double exigence de transparence et sa raison d'être

Les données numériques que gère l'État au sujet des citoyens sont par nature invisibles et intangibles. Il importe pourtant de permettre au citoyen de pouvoir identifier les données que l'État traite à son sujet et d'en comprendre l'utilisation, pour deux raisons principalement, qui fondent la double exigence de transparence qui s'impose à l'État.

D'une part, la Constitution belge consacre un droit fondamental à la *transparence administrative*, en son article 32, qui affirme que « chacun a le droit de consulter chaque document administratif et de s'en faire remettre copie, sauf dans les cas et conditions fixés par la loi, le décret ou la règle visée à l'article 134 ».

Ainsi, tout administré a le droit de satisfaire sa curiosité légitime à l'égard de toutes les informations détenues par l'administration. L'objectif qui sous-tend ces règles est l'amélioration de la démocratie grâce à la connaissance et la compréhension, par chacun, de l'action administrative en général. On peut voir dans la transparence administrative un prolongement de l'article 10 de la Convention européenne des droits de l'homme, qui protège la liberté d'expression et d'information. C'est l'idée qu'on ne peut s'exprimer pertinemment sans avoir pleinement conscience du contexte dans lequel on agit.

La notion de document administratif est très large[40]. Dans l'univers numérique, cela signifie, par exemple, que le code source d'un logiciel de vote électronique est un document administratif accessible au public. Cette affirmation a bénéficié d'une reconnaissance jurisprudentielle au travers d'un arrêt du Conseil

---

39 À ce sujet v. not. D. BOURG, *Inventer la démocratie du XXIe siècle – L'Assemblée citoyenne du futur*, Paris, LLL Éditions, 2017 ; C. VILANI, *Donner un sens à l'intelligence artificielle*, mars 2018, p. 140, accessible ici : https://fichiers.acteurspublics.com/redac/pdf/2018/2018-03-28_Rapport-Villani.pdf

40 La loi du 11 avril 1994 relative à la publicité de l'administration, qui est l'une des normes de valeur législative organisant la mise en œuvre du droit fondamental à la transparence administrative, définit la notion de document administratif comme « *toute information sous quelque forme que ce soit dont une administration dispose* » (art. 1, b, 2°).

d'État en 2001 déjà[41]. La haute juridiction administrative soutient ainsi que le « document administratif {est une} notion englobant les logiciels de vote automatisé », ce qui comprend les codes sources et les mesures de sécurité.

Dans l'affaire qui a donné lieu à l'arrêt précité, le requérant demandait l'accès aux documents relatifs au vote automatisé, en ce compris le contenu des programmes informatiques utilisés. À cette occasion, le Conseil d'État a affirmé l'importance de pouvoir accéder à un tel outil informatique, soutenant que tout citoyen doit avoir « la possibilité {…} de s'assurer lui-même de la fiabilité des systèmes de vote et de dépouillement automatisés »[42], et ce, même si des experts informaticiens sont déjà désignés pour accomplir cette tâche.

Pour les mêmes motifs, et bien que cela n'ait pas encore fait l'objet d'une reconnaissance par le juge en Belgique, on peut raisonnablement affirmer qu'un algorithme utilisé par l'État pour effectuer ses différentes missions de service public est un document administratif auquel toute personne intéressée doit pouvoir accéder. Nous reviendrons sur ce point dans la suite de notre contribution.

D'autre part, l'exigence de *transparence des traitements de données à caractère personnel* découle du droit fondamental à la protection de la vie privée, consacré par l'article 22 de la Constitution et par l'article 8 de la Convention européenne des droits de l'homme[43]. La notion de vie privée est entendue ici dans le sens d'« autodétermination informationnelle », c'est-à-dire le droit de chacun de garder la maîtrise sur ses propres données, en ayant accès aux données qui sont enregistrées et/ou réutilisées par d'autres, et en ayant connaissance du sort réservé à ces données.

Concrètement, la transparence des traitements de données à caractère personnel répond à ce droit fondamental car elle permet au citoyen d'avoir *conscience* du fait que ses données sont collectées et traitées. Ce dernier peut également identifier les autorités impliquées dans ces processus ainsi que les raisons qui justifient les traitements[44]. En outre, consciente que ses données sont traitées, et bénéficiant des informations à ce sujet, la personne concernée est en mesure de *vérifier l'exactitude* des données utilisées[45]. Cela bénéficie tant au citoyen qu'à l'administration, qui ont tous intérêt à ce que des erreurs n'affectent pas les données utilisées. Il en va d'autant plus ainsi que les informations seront échangées et réutilisées de nombreuses fois. Enfin, la transparence permet au citoyen de *contrôler l'usage* de ses données personnelles, en vérifiant qui a accédé aux informations et dans quel but. Tout administré peut ainsi jouer « un rôle d'avertisseur puisqu'il est le mieux placé pour détecter des consultations "anormales" pouvant donner lieu à des

41 CE, arrêt *Antoun*, n° 95.677, 21 mai 2001. Au sujet de cet arrêt, v. D. DE ROY, « L'accès aux documents administratifs dans un environnement dématérialisé », in D. RENDERS (dir.), *L'accès aux documents administratifs*, Bruxelles, Bruylant, 2008, p. 831. Cet arrêt est accessible ici : https://www.poureva.be/IMG/pdf/95677.pdf

42 CE, arrêt *Antoun*, *ibidem*, p. 10.

43 V. not. Cour eur. DH, *Leander c. Suède*, 26 mars 1987, req. n° 9248/81, § 66 (cet arrêt concerne l'enregistrement et la communication d'informations par une autorité publique, sans possibilité pour la personne concernée d'y accéder ni de les contredire) ; *Gaskin c. Royaume Uni*, 7 juillet 1989, req. n° 10454/83, §49 ; *Odièvre c. France*, 13 février 2003, req. 42326/98, §29 (ces deux derniers arrêts concernent l'accès aux informations relatives aux origines identitaires des requérants).

44 C. DE TERWANGNE, « Loi relative à la publicité de l'administration et loi relative à la protection des données personnelles : regards croisés sur deux voies d'accès à l'information », in *Transparence et droit à l'information*, Liège, Formation permanente CUP, 2003, p. 90.

45 Projet de loi relatif à la protection de certains aspects de la vie privée, *Doc. parl.*, Ch. repr., 1983-1984, n° 778/1, p. 14.

sanctions »[46]. En outre, l'existence d'une possibilité de contrôle incite les administrations à traiter les données en leur possession conformément à la loi. En ce sens, comme l'affirme l'autorité de protection des données, « le fait de savoir que le citoyen, qui est le mieux placé pour détecter quand ses données ont été consultées à tort, dispose d'un tel droit de consultation ne peut qu'influencer positivement l'utilisation correcte [des données] »[47].

Tout comme la transparence administrative, la transparence des traitements de données à caractère personnel participe également à l'amélioration de la démocratie. Elle tend à équilibrer le pouvoir de l'État et des citoyens en instaurant un « contrôle démocratique, exercé par les citoyens eux-mêmes »[48]. La transparence des traitements de données à caractère personnel favorise également la confiance des citoyens en leurs institutions, nécessaire à l'accomplissement des fonctions étatiques.

Plus précisément, la transparence des traitements de données à caractère personnel est organisée par le régime juridique de protection des données à caractère personnel, à savoir la Convention n° 108, le RGPD et la loi du 31 juillet 2018. Ce régime juridique octroie notamment au citoyen un droit individuel d'accès à ses données, consacré par l'article 15 du RGPD. Cela signifie que toute personne a non seulement le droit de savoir ce que l'administration détient à son sujet, mais il a le droit d'en obtenir gratuitement une copie. Il est également en droit de savoir qui a consulté ses données, pour quelles raisons, à qui elles ont été transmises et pendant combien de temps elles seront conservées[49].

b) Les difficultés rencontrées en pratique et des pistes de solutions

On pourrait penser que les écrans et plateformes numériques faciliteraient l'accès du citoyen aux documents de l'administration et aux informations le concernant. Pourtant, en Belgique, les choses sont plus complexes, en raison du modèle d'administration et des outils utilisés.

b.1 Le modèle de l'administration en réseaux

Au début des années quatre-vingt-dix, s'est posée la question de savoir si les données que l'État collectait depuis plusieurs années dans des secteurs de plus en plus différents devaient être stockées dans une base de données centralisée ou pas.

À cet égard, le projet français de centralisation des données, appelé SAFARI, a inspiré la Belgique en tant que contre-exemple. Ce projet, rebaptisé par *Le Monde* en 1974 « *SAFARI ou la chasse aux Français* », faisait craindre notamment un grand risque de piratage des données facilité par le fait que l'ensemble des données aurait été disponible en un point unique[50].

La Belgique a choisi de s'engager dans un modèle de stockage décentralisé des données, appelé le modèle de l'administration en réseaux. Pour le dire autrement, il s'agit de disperser les données d'un citoyen au sein de l'administration afin de « ne pas mettre tous les œufs dans le même panier ». En recourant à cette architecture, on

---

46 Commission de protection de la vie privée (ci-après : CPVP), avis n° 12/2009 du 29 avril 2009 relatif à une demande d'avis émanant du SPF Intérieur concernant un certain nombre de questions qui se sont posées dans le cadre de la délibération RN n° 19/2008, p. 6.

47 CPVP, recommandation n° 03/2009 du 1er juillet concernant les intégrateurs dans le secteur public, p. 10.

48 Projet de loi relatif à la protection de certains aspects de la vie privée, *op. cit.*, p. 14.

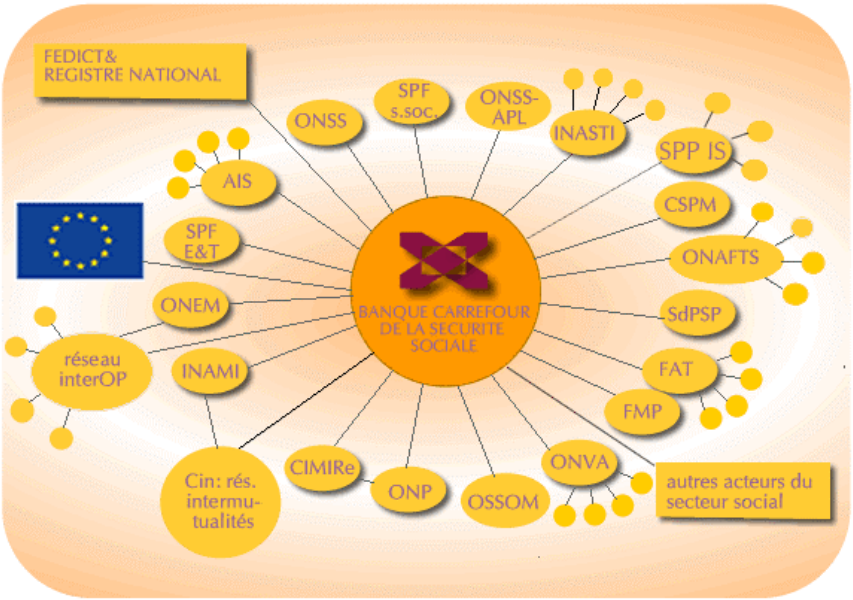
49 Pour de plus amples précisions, v. l'article 15 du RGPD.

50 À ce sujet, v. not. C. MASUTTI, *Affaires privées – Aux sources du capitalisme de surveillance*, Caen, C&F Éditions, coll. Société numérique, 2020, p. 104 *sq*.

diminue les risques de piratage et, partant, on favorise la protection des données. C'est une concrétisation avant l'heure du concept de « *privacy by design* » consacré à l'article 25 du RGPD.

En somme, il s'agit d'identifier des administrations qui s'occupent d'une même matière – la sécurité sociale, la santé, etc. – et de les regrouper au sein d'un réseau informatique, tels le réseau sectoriel de la sécurité sociale et le réseau sectoriel de la santé.

Le réseau se présente comme une toile d'araignée, les administrations étant interconnectées l'une à l'autre. Les administrations du réseau enregistrent chacune certains types de données : l'adresse se trouve au Registre national, le montant des pensions au sein de l'administration des pensions, etc. Lorsqu'une administration a besoin d'une information dont elle ne dispose pas, elle doit s'adresser à l'institution qui se trouve au sein du réseau sectoriel, appelée « Banque-carrefour » ou « plateforme d'échange d'informations ». Cette institution va chercher l'information dans l'administration qui la détient et l'achemine vers l'administration qui la demande. Ces opérations sont effectuées en quelques secondes et soulagent le citoyen qui ne doit pas fournir à plusieurs reprises la même information à des administrations différentes. Par ailleurs, l'information n'étant enregistrée qu'une seule fois au sein du réseau, on diminue le risque d'erreurs dans l'encodage des données.



Exemple d'intégrateur de services : la Banque-carrefour de la sécurité sociale, placée au cœur du réseau de la sécurité sociale qui regroupe les administrations intervenant en matière de sécurité sociale.

Ainsi, ce modèle encourage la simplification administrative, tant du côté des institutions que du côté des usagers du service public. Mais il a également pour effet de faire disparaître les dossiers administratifs. Là où jadis chaque citoyen avait un dossier dans chaque administration, ses données sont à présent dispersées au sein de

l'administration. Il est devenu très difficile d'identifier les types de données, leur localisation dans l'administration et leur trajet entre les institutions. C'est pourquoi, notamment, retrouver la source d'une erreur affectant une donnée équivaut à chercher une aiguille dans une botte de foin[51].

Pour faciliter l'exercice du droit d'accès, certains outils sont mis en place qui présentent un réel intérêt. Ils demeurent néanmoins difficiles à utiliser et ne font pas l'objet d'une harmonisation au sein de l'ensemble de l'administration. En guise d'exemple, les citoyens belges peuvent consulter leurs données d'identification enregistrées par l'État dans une base de données appelée « Registre national », en s'identifiant à l'aide de leur carte d'identité électronique[52]. Ils peuvent également déterminer quelles institutions ont consulté leurs données ces six derniers mois. Cet outil est très intéressant bien qu'il soulève la question du contrôle de la véracité des informations qui y sont reprises, en l'absence notamment d'une autorité de protection des données suffisamment indépendante en Belgique qui pourrait effectuer, en toute confiance, ce type de contrôle[53].

b.2) De puissants outils opaques

De plus en plus, l'État recourt aux technologies pour gagner en efficacité, dans la lutte contre la fraude notamment. À cette fin, de puissants outils de traitement de données sont mis en place, que sont notamment le « *datamatching* » et le « *datamining* » évoqués précédemment.

Les algorithmes utilisés pour faire fonctionner ces techniques informatiques ont, certes, une apparence de neutralité et d'objectivité scientifique, de par leur mystère et leur complexité. Pourtant, un algorithme n'est pas neutre. En effet, chaque algorithme est décidé par un être humain, appelé « développeur » ou « programmateur ». Lorsqu'elle crée un algorithme, cette personne, consciemment ou non, pose des choix qui reflètent ses propres valeurs et sa propre sensibilité, en décidant des données à utiliser en priorité, des critères à appliquer et du poids à leur attribuer, etc.[54]. Parfois, le développeur croit utiliser une donnée tout à fait neutre mais qui, en pratique, aura certaines conséquences sociales discriminatoires. Tel est le cas, par exemple, du code postal qui peut conduire à cibler en priorité des quartiers défavorisés, notamment[55].

Or, une fois l'algorithme utilisé à l'échelle de la société, comme c'est le cas des outils mis en place par l'État, il a un impact sur l'ensemble de la population. Un choix technique dans la confection de l'algorithme peut dès lors être un choix de

51 Médiateur fédéral, *Rapport annuel 2010*, p. 90.

52 V. le site web https://www.ibz.rrn.fgov.be/fr/registre-national/mon-dossier/

53 Sur l'Autorité de protection des données, v. *infra*.

54 Par exemple, en Belgique, il est possible d'obtenir un test PCR gratuit pour partir en vacances, si la personne n'a pas pu obtenir une vaccination complète d'ici là. Ce test doit être demandé en ligne. Il s'avère que le système informatique refuse d'octroyer le test PCR gratuit aux personnes qui ont attendu un certain délai avant de se faire vacciner (c'est le cas notamment des étudiants qui étaient en séjour Erasmus). Or, aucune norme juridique ne prévoit que, dans un tel cas, la personne doit être sanctionnée en payant elle-même son test PCR. On peut raisonnablement penser que ce paramètre a été défini d'initiative par le concepteur de l'algorithme chargé de vérifier le respect des conditions d'octroi d'un test PCR gratuit.

55 À ce sujet v. C. O'NEILL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, USA, Crown Books, 2016.

société, sans même que l'on s'en aperçoive de manière évidente. C'est ce que d'aucuns appellent « la loi des algorithmes »[56].

Concrètement, modifier un paramètre algorithmique aura le même effet que modifier un critère fixé dans une législation encadrant la lutte contre la fraude. Pourtant, un changement de législation sera débattu au Parlement, et annoncé au public. Un changement au niveau de l'algorithme se fera, lui, dans l'opacité la plus complète.

Les algorithmes utilisés par l'État ne sont pas nécessairement problématiques. Mais ils peuvent l'être. Tant qu'ils ne sont pas connus ni contrôlés, la question reste pleine et entière.

L'affaire SyRI aux Pays-Bas illustre concrètement le problème de manque de transparence des algorithmes. SyRI, pour « *System of Risk Indicator* », est un système automatisé de surveillance de la fraude sociale placé sous la responsabilité du ministère des Affaires sociales et de l'Emploi des Pays-Bas[57]. SyRI a fait beaucoup parler de lui car, à la suite d'un recours en justice de plusieurs ONG notamment, le Tribunal de district de La Haye en a interdit le fonctionnement au motif qu'il portait atteinte aux droits humains[58]. C'est d'ailleurs la première décision de justice qui invalide un outil algorithmique pour cette raison.

Et pour cause. Des études ont démontré que les algorithmes utilisés par l'outil SyRI étaient biaisés. Ils aboutissaient à contrôler en priorité les quartiers de pauvres et de migrants. Ce constat a fait dire au Rapporteur spécial aux Nations Unies sur les droits de l'homme et l'extrême pauvreté, le professeur Philip Aston, que « l'essence du droit à la vie privée est en jeu ici. Des quartiers entiers sont considérés comme suspects et font l'objet d'un examen spécial, qui est l'équivalent numérique d'inspecteurs de fraude frappant à toutes les portes dans un certain secteur et examinant les dossiers de chaque personne pour tenter d'identifier les cas de fraude [...]. Dans le monde réel, il n'y aurait jamais assez d'inspecteurs des fraudes pour entreprendre un tel exercice et le grand public résisterait et protesterait rapidement contre de telles atteintes à sa vie privée. Le fait que le SyRI opère dans le domaine numérique et non dans le monde réel n'est cependant pas une grande consolation pour ceux qui en sont affectés. Les effets psychologiques et autres d'une descente physique dans un quartier par des inspecteurs de la fraude sont relativement faciles à imaginer, mais une descente numérique d'une telle ampleur laisse des traces tout aussi problématiques. Le fait que le SyRI fonctionne dans un silence relatif et soit *de facto* invisible à l'œil nu peut en fait aggraver le malaise et le préjudice subi par les personnes vivant dans ces quartiers »[59].

---

56 Expression de B. BARRAUD, « Le coup de data permanent : la loi des algorithmes », *RDLF*, 2017, accessible ici : http://www.revuedlf.com/droit-fondamentaux/le-coup-de-data-permanent-la-loi-des-algorithmes

57 À l'origine, la presse néerlandaise a fait scandale en révélant que des gangs bulgares avaient commis une fraude sociale durant de longues années. Arrivés aux Pays-Bas, ils se sont enregistrés comme habitants, ont ouvert un compte bancaire et demandé une aide sociale. Ils sont ensuite retournés en Bulgarie, en continuant à percevoir les allocations sociales pendant des années. C'est pour renforcer l'efficacité de la lutte contre ce type de fraude que SyRI a été créé (v. Société de législation comparée, Rapport des Pays-Bas, p. 9, accessible ici : https://www.legiscompare.fr/web/Activites-de-la-section-921).

58 Le jugement est accessible ici : https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865.

59 Ph. ALSTON, « Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388) », n° 29 (traduction

Ainsi, alors même que les développeurs d'algorithmes ne sont certainement pas malveillants, le fait que pareil outil se décide en toute opacité et sans contrôle sur sa conception et son impact effectif est particulièrement problématique dans une société démocratique, notamment en ce qu'il peut aboutir à automatiser des inégalités à grande échelle.

Le Comité des ministres du Conseil de l'Europe abonde également en ce sens dans une déclaration du 17 mars 2021 relative à la prise de décision assistée par un ordinateur ou reposant sur l'intelligence artificielle dans le domaine du filet de la sécurité sociale. Il y est notamment affirmé qu'« un développement non réglementé de ces systèmes de prise de décision assistée par ordinateur ou automatisée, associé à un manque de transparence et à un contrôle public insuffisant dans le cadre de leur utilisation par l'administration des services sociaux, constitue des risques. De tels systèmes peuvent, s'ils ne sont pas développés et utilisés conformément aux principes de transparence et de sécurité juridique, amplifier les préjugés et accroître les risques. Cela peut entraîner un impact négatif plus grand pour les membres de la communauté qui se trouvent dans une situation de vulnérabilité. Dans ces circonstances, ils peuvent reproduire des schémas de discrimination bien ancrés, y compris à l'égard des femmes, et peuvent affecter les personnes occupant des emplois peu qualifiés et mal rémunérés. Des décisions automatisées biaisées et/ou erronées peuvent entraîner un dénuement immédiat, une extrême pauvreté ou même la perte de logement, et ainsi causer un préjudice, grave ou irréparable, aux personnes concernées ».

En Belgique, l'outil OASIS est utilisé pour lutter contre la fraude sociale et fonctionne de manière très semblable à SyRI. Des recherches universitaires relayées par la presse ont mis en évidence les problèmes relatifs à ce système automatisé. Les constats dressés ont retenu l'attention de certains parlementaires belges.

C'est ainsi qu'une proposition de loi a récemment été déposée[60], dans le but d'assurer davantage de transparence dans l'usage des algorithmes. Cette proposition de loi entend contraindre les administrations « à publier en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsque ceux-ci constituent tout ou partie du fondement des décisions individuelles », « pour tout document administratif à portée individuelle, à communiquer à la personne faisant l'objet d'une décision individuelle prise en tout ou en partie sur le fondement d'un traitement algorithmique, les caractéristiques de cet algorithme » et à « publier l'analyse d'impact des outils mis en place par l'administration, qui est effectuée en vertu de l'article 35 du Règlement général sur la protection des données (RGPD) ». Cette proposition sera débattue prochainement au Parlement fédéral.

C.- Constitution, numérique et vulnérabilité

Il nous a paru essentiel d'aborder brièvement la question de l'impact du numérique sur les personnes vulnérables et les enjeux constitutionnels de cette question.

---

libre). Cette intervention est accessible ici : https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf.

60 Proposition de loi modifiant la loi sur la publicité de l'administration du 11 avril 1994 afin d'introduire une plus grande transparence dans l'usage des algorithmes par les administrations, *Doc. parl.*, Ch. repr., 2020-2021, n° 55-1904/1.

1.- État-providence, numérique et contrôle renforcé des personnes vulnérables

La mise en réseau des administrations belges permet l'automatisation de certaines allocations auxquelles les personnes vulnérables peuvent prétendre. Par exemple, les personnes percevant un revenu qui ne dépasse pas un certain seuil bénéficient, sans le demander, d'un tarif préférentiel pour le gaz et l'électricité, grâce à un échange de données entre les institutions concernées.

S'il s'agit là d'une simplification administrative non négligeable, il faut veiller à ce que l'aide sociale ne devienne pas le prétexte d'un contrôle social renforcé et très intrusif. En effet, plus une personne est dépendante des allocations que lui paie l'État, plus elle doit lui fournir des données pour obtenir lesdites allocations. Une fois en possession de ces informations, il est tentant pour l'État, de réutiliser ces informations pour contrôler ces personnes. En Belgique, certaines pratiques tendent à penser que plus on est vulnérable, plus on est contrôlé par l'État, qu'une personne pauvre est d'emblée suspectée de ne pas mériter son allocation et contrainte de rendre des comptes. Par exemple, depuis 2016, un important échange de données au sein de l'administration vise à renforcer le contrôle des chômeurs pour lutter contre le problème de la fraude au domicile dite aussi « domiciliation fictive »[61]. On vise par là le fait, pour une personne, de déclarer une situation familiale ou un domicile qui ne correspond pas à la réalité, de manière à percevoir une aide sociale plus importante que celle à laquelle elle a droit[62].

Pour lutter contre ce type de fraude, les fournisseurs d'énergie (gaz, électricité, eau) sont légalement tenus de faire parvenir les données de consommation à l'administration, qui les confronte ensuite aux données des allocataires sociaux, notamment à la composition de ménage officiellement déclarée. Si l'on constate que la consommation d'un allocataire social s'écarte d'au moins 80 % vers le haut ou vers le bas de la consommation moyenne du type de ménage communiqué, la personne concernée est contrôlée par un inspecteur social.

Il est certes tout à fait légitime de lutter contre la fraude. Néanmoins, le moyen utilisé pose question. En effet, comme l'indique le secteur social[63], les données utilisées pour contrôler ces personnes peuvent difficilement être pertinentes. Il est en effet très difficile, voire impossible, d'établir une moyenne de consommation d'énergie, notamment parce que ces personnes vulnérables vivent bien souvent dans un logement insalubre qui requiert de grosses dépenses énergiques liées à des fuites d'eau ou une mauvaise isolation. À l'inverse, d'autres personnes, ne parvenant pas à payer ces frais d'énergie, vivent dans la précarité énergétique en chauffant le moins possible.

La loi organisant cette pratique a fait l'objet d'un recours devant la Cour constitutionnelle. Dans un arrêt surprenant et critiquable[64], la Cour

61 V. la loi du 13 mai 2016 modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le *datamining* et le *datamatching* dans la lutte contre la fraude sociale http://www.ejustice.just.fgov.be/loi/loi.htm

62 Par exemple, un homme perçoit l'allocation de chômage. Il se domicilie seul dans un appartement, ce qui lui permet de percevoir une allocation de chômage plus élevée que s'il déclarait vivre en couple. En réalité, il vit chez sa compagne. Il s'agit là d'une domiciliation fictive.

63 V. not. Conseil bruxellois de coordination sociopolitique, « Contrôle des chômeurs : le gaz et l'eau pour preuves ? Injuste, irréaliste et illégal », s.d., https://www.cbcs.be/Controle-des-chomeurs-le-gaz-et-l

64 CC, arrêt n° 29/2018, 15 mars 2018.

constitutionnelle rejette le recours. Tout en admettant que la technique utilisée « comporte […] des risques en ce qui concerne le droit à la protection de la vie privée dont jouissent les intéressés […] en ce qu'elle peut notamment amener à établir de fausses corrélations entre les caractéristiques d'un comportement déterminé et des personnes »[65], la Cour considère que la loi est suffisamment claire et que la méthode de contrôle n'est pas disproportionnée. Malheureusement, les requérants ont manqué de soulever la critique du caractère non pertinent des données utilisées, qui aurait peut-être amené la Cour à se prononcer différemment.

2.- Fracture numérique et personnes vulnérables

L'exercice effectif de certains droits peut être facilité par l'usage d'internet, d'où l'importance de réfléchir à la consécration d'un droit d'accès à internet pour tous[66]. Bénéficier des avantages d'internet suppose néanmoins que les personnes aient, non seulement la possibilité d'accéder à du matériel informatique et à internet (c'est le problème des « zones blanches » qui ne captent pas internet), mais qu'elles puissent aussi en comprendre les usages (d'où l'apparition de la notion d'« illectronisme numérique »). Ces deux impératifs peuvent affecter particulièrement les personnes en situation de vulnérabilité vu leur situation économique et sociale, si bien qu'il faut être attentif à ne pas trop rapidement basculer vers internet comme seul moyen d'exercer certains droits.

On illustre cette préoccupation au travers de deux droits, à savoir le droit de prendre connaissance du droit positif et le droit de demander le paiement de prestations sociales.

a) Le droit de prendre connaissance du droit positif

L'usage d'internet peut faciliter considérablement la consultation de certaines publications, parmi lesquelles les normes officielles qui sont publiées, en Belgique, au *Moniteur belge*. Pour autant, internet doit-il devenir la voie d'accès (quasiment) exclusive vers de telles publications ? La Cour constitutionnelle répond par la négative, se montrant soucieuse des difficultés que rencontraient (et rencontrent encore) certaines catégories de personnes en raison de leur situation économique et sociale.

Ainsi, la Cour constitutionnelle a annulé, en 2004, les articles 474 et 475 de la loi-programme (I) du 24 décembre 2002 prévoyant que, hormis trois exemplaires imprimés sur papier dont l'un est disponible pour consultation auprès de la Direction du *Moniteur belge*, toute autre mise à disposition du public est réalisée par l'intermédiaire du site internet du *Moniteur belge*[67]. La Cour juge que « faute d'être accompagnée de mesures suffisantes qui garantissent un égal accès aux textes

65 Arrêt précité, B.31.

66 Pour une étude approfondie sur les différents aspects d'un « droit d'accès à internet », v. P. PASSAGLIA, « Le droit d'accès à internet dans les jurisprudences constitutionnelles : vers un droit commun jurisprudentiel ? », in A. LE QUINIO (dir.), *Les réactions constitutionnelles à la globalisation*, Bruxelles, Bruylant, 2016, p. 93-123.

67 CC, arrêt n° 106/2004, 16 juin 2004. Sur cet arrêt, v. F. ABU DALU et J.-F. HENROTTE, « Disparition de la version en papier du *Moniteur belge*, obligations positives et très large marge d'appréciation : le prix du Docteur Faust », *Revue du droit des technologies de l'information*, 2004, n° 20, p. 93-100 ; P. POPELIER et J. VAN NIEUWENHOVE, « De elektronische publicatie van het Staatsblad : over de bevoegdheid van de federale wetgever en de toegankelijkheidsvereiste », *Rechtskundig weekblad*, 2004-2005, p. 408-414 ; V. THIRY, « La Cour d'arbitrage au chevet des non-surfeurs », *JLMB*, 2004, p. 1135-1137. V. égal. P. PASSAGLIA, *op. cit.*, p. 120-122.

officiels, la mesure attaquée a des effets disproportionnés au détriment de certaines catégories de personnes » et « n'est dès lors pas compatible avec les articles 10 et 11 de la Constitution »[68]. Néanmoins, elle précise que « compte tenu de ce que la mesure attaquée est d'application depuis le 1er janvier 2003, de ce que le législateur a le choix des mesures à prendre pour mettre fin à la discrimination constatée, mais que leur mise en œuvre peut demander du temps, il y a lieu, en application de l'article 8, alinéa 2, de la loi spéciale du 6 janvier 1989 sur la Cour [constitutionnelle], de maintenir les effets des dispositions annulées de la manière indiquée au dispositif », c'est-à-dire jusqu'au 31 juillet 2005[69]. Par une loi du 20 juillet 2005 portant des dispositions diverses et publiée au *Moniteur belge* du 29 juillet 2005, le législateur a remplacé les articles 474 et 475 annulés par la Cour constitutionnelle et y a ajouté des articles 475*bis* et 475*ter*. L'entrée en vigueur de ces nouvelles dispositions a été fixée au … 31 juillet 2005, jour de l'expiration du délai imparti par les juges constitutionnels.

b) Le droit de demander le paiement de prestations sociales

Le phénomène du non-recours aux droits sociaux retient ici l'attention. On vise par-là « les situations où une personne est juridiquement éligible à une prestation ou un service mais n'en bénéficie pas »[70], en raison notamment de procédures d'obtention trop complexes. Dans l'espoir de faciliter les procédures administratives, tant pour l'administration que pour les bénéficiaires des droits, nombre de démarches sont désormais informatisées, « dématérialisées », dans le but de les rendre accessibles 24h/24, 7jours/7.

Si l'objectif est louable, il s'avère toutefois qu'en pratique, cela relève davantage du fiasco pour les personnes vulnérables. Les institutions impliquées dans l'aide sociale pointent notamment des problèmes rencontrés dans l'échange automatisé de données entre administrations (éléments incomplets, erreurs dans les données…), des défaillances informatiques (site web en panne), un manque de réponse aux courriels, une trop faible accessibilité téléphonique ou physique des services[71]. En raison de ces aléas, nombre de personnes vulnérables se voient privées, parfois des mois durant, des allocations auxquelles elles pourraient prétendre. D'aucuns affirment ainsi que « la société sans contact génère à l'évidence du non *take-up*, et il ne faut pas être fin sociologue pour deviner qui sont celles et ceux qui en paient le plus le prix », insistant sur le fait que « sans que cela doive empêcher pour autant de poursuivre la digitalisation d'un certain nombre de démarches, laquelle a bien sûr un sens lorsqu'elle est réalisée sans ratés », il est crucial que « la faculté d'un contact physique à un guichet et lors de permanences demeure […], de même que la possibilité d'y recevoir une information personnalisée »[72].

68 *Ibid*., B.22.

69 *Ibid*., B.23 et dispositif.

70 D. DUMONT, « Le phénomène du non-recours aux prestations, un défi pour l'effectivité (et la légitimité) du droit de la sécurité sociale. Un état de l'art et un agenda pour la recherche juridique, *Revue de droit social/Tijdschrift voor Sociaal Recht*, 2020/3, p. 381.

71 V. not. la lettre ouverte signée par 22 professeurs d'universités belges : « La DG Personnes handicapées, une administration dysfonctionnelle », *Le Soir*, 7 janvier 2019 ; les avis du Conseil supérieur national des personnes handicapées (not. avis n° 2019/02 du 18 mars 2019 ; avis n° 2017/03 du 22 février 2017 ; avis n° 2017/17 du 18 septembre 2017) ; le billet du Médiateur fédéral, « De l'argent perdu pour les personnes handicapées » (26 février 2018) accessible ici : http://www.federaalombudsman.be/fr/content/de-l-argent-perdu-pour-les-personnes-handicapees.

72 D. DUMONT, *op. cit.*, p. 396.

II.- LA PROTECTION DES DROITS ET LIBERTÉS FONDAMENTAUX : QUELLE TRANSFORMATION À L'HEURE NUMÉRIQUE ?

Une distinction est opérée ici entre, d'une part, la protection juridictionnelle, par la Cour constitutionnelle (A) et par les autres juridictions (B) et, d'autre part, la protection par des autorités indépendantes spécifiques (C).

A.- La protection par la Cour constitutionnelle

1.- Le numérique et les attributions de la Cour constitutionnelle

La Cour constitutionnelle belge est compétente pour exercer un contrôle à l'égard de tous les droits fondamentaux reconnus par le Titre II de la Constitution. En revanche, à la différence d'autres États[73], elle n'est pas autorisée à faire une application autonome de droits fondamentaux reconnus au niveau international ou européen. Toutefois, elle fait usage de la méthode d'interprétation dite « conciliatoire »[74], qu'elle qualifie de méthode « de l'ensemble indissociable » : depuis l'arrêt n° 136/2004 du 22 juillet 2004, elle considère que lorsqu'une disposition conventionnelle liant la Belgique a une portée analogue à une ou plusieurs des dispositions constitutionnelles – situation qualifiée de « concours de droits fondamentaux » –, « les garanties consacrées par cette disposition conventionnelle constituent un concours avec les garanties inscrites dans les dispositions constitutionnelles en cause », de telle sorte que quand est alléguée la violation d'une disposition constitutionnelle, elle « tient compte, dans son examen, des dispositions de droit international qui garantissent des droits ou libertés analogues ». Ainsi, la Cour établit une analogie entre l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme (droit au respect de la vie privée et familiale), dispositions – précise la Cour – entre lesquelles « le Constituant a recherché la plus grande concordance possible »[75]. Ce rapprochement par analogie lui permet de s'inspirer de la jurisprudence développée par la Cour européenne des droits de l'homme sur la base de l'article 8 et des applications que les juges européens donnent de cette disposition en matière numérique.

2.- Le numérique et le fonctionnement de la Cour constitutionnelle

L'incidence du numérique sur le fonctionnement de la Cour constitutionnelle est perceptible à trois niveaux, et ce depuis 2014.

La numérisation de la procédure. En 2014, un Chapitre V a été inséré dans la loi spéciale sur la Cour constitutionnelle (ci-après : LSCC), qui est intitulé « De la procédure électronique ». Il comprend un nouvel article 78bis[76]. Depuis l'origine, chaque pièce de procédure doit être notifiée au greffe de la Cour constitutionnelle par un envoi sous pli recommandé à la poste. Il y va d'une formalité substantielle. C'est dans un souci d'adaptation aux moyens de communication modernes que le législateur spécial a entendu introduire la notification électronique dans la procédure devant la Cour, en veillant à ce que

73 V. *supra*.

74 M. VERDUSSEN, *Justice constitutionnelle*, Bruxelles, Larcier, 2012, p. 132-138.

75 Not. CC, arrêt n° 117/2020, 24 septembre 2020, B.3.4.

76 En rapport avec la mise en place de cette procédure, les articles 81 et 82 de la LSCC ont été remplacé en 2014.

l'équipement électronique soit suffisamment sécurisé pour fournir les mêmes garanties que les envois recommandés : il s'agit d'offrir à l'expéditeur la preuve que son envoi a bien été effectué à une date déterminée, tout en préservant la confidentialité des informations transmises[77]. Toutefois, les nouvelles dispositions introduites en 2014 n'entreront en vigueur qu'à la date que le Roi fixera dans un arrêté d'exécution. Le temps mis par le Gouvernement fédéral pour organiser la procédure électronique, et en conséquence adopter l'arrêté d'exécution, devient sérieusement déraisonnable.

La numérisation des prononcés. Jusqu'en 2014, tout arrêt de la Cour constitutionnelle devait être prononcé en audience publique, en vertu de l'article 110 de la LSCC. Toutefois, en pratique, le président ne procédait pas à la lecture de l'entièreté de l'arrêt, mais uniquement du dispositif, le greffe distribuant, sans frais, le texte de l'arrêt – à tout le moins une version « non corrigée » – à toute personne présente qui lui en faisait la demande. En 2014, l'article 110 a été remplacé. En effet, même allégée, et bien que procédant de préoccupations démocratiques essentielles, la formalité était considérée comme lourde et passablement inutile, la salle d'audience étant généralement vide au moment des prononcés des arrêts. Le législateur spécial a considéré que l'objectif poursuivi pouvait « être atteint aussi bien, voire mieux, par un instrument plus adapté à l'époque actuelle »[78]. Dorénavant, la publication de l'arrêt sur le site web de la Cour « vaut prononcé ». Inspirée du règlement de la Cour européenne des droits de l'homme[79], la formule offre un triple avantage : elle fait gagner du temps à la Cour ; elle facilite l'accès de tous aux arrêts ; elle diligente la publication de ceux-ci. Le nouvel article 110 prévoit que le président peut toutefois décider de prononcer l'arrêt en audience publique. C'est une décision qui lui revient en propre et dont il apprécie souverainement la pertinence. Précisons que, parallèlement, l'article 114 de la LSCC a été remplacé afin de supprimer l'exigence pour la Cour d'assurer la publication des arrêts dans un recueil officiel. La publication des arrêts au *Moniteur belge*, dans leur intégralité ou par extraits, reste évidemment obligatoire.

La pseudonymisation des arrêts. Le 8 février 2012, la Commission de protection de la vie privée a adopté une recommandation[80] dans laquelle elle considère que « dans la mesure où des jugements et arrêts sont intégralement mis à disposition par le biais des nouvelles technologies de l'information, ils constituent un traitement de données à caractère personnel (des parties, des juges ou des auxiliaires de justice ainsi que de tiers qui sont cités dans le jugement) », de telle sorte que la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel s'y applique[81]. La Commission recommande « que, sauf disposition légale contraire, lors de la publication de

77 Pour plus de détails sur les motivations du législateur spécial, v. *Doc. parl.*, Sénat, 2013-2014, n° 5-2438/1, p. 1-2 et 16-19.

78 *Doc. parl.*, Sénat, 2013-2014, n° 5-2438/1, p. 21.

79 V. la version la plus récente, celle du 2 juin 2021 (https://www.echr.coe.int/Documents/Rules_Court_FRA.pdf). Art. 77-2 : « L'arrêt rendu par une chambre peut être lu en audience publique par le président de la chambre ou par un autre juge délégué par lui. Les agents et représentants des parties sont dûment prévenus de la date de l'audience. En l'absence de lecture en audience publique de pareil arrêt et dans le cas des arrêts rendus par un comité, la communication visée au paragraphe 3 du présent article vaut prononcé. »

80 Recommandation 03/2012 relative aux banques de données de jugements et/ou d'arrêts accessibles à des tiers gratuitement ou contre paiement, CO-AR-2011-003 : http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_03_2012_0.pdf.

81 *Ibid.*, § 5.

décisions de juridictions par le biais de médias accessibles par des tiers gratuitement ou contre paiement, tous les éléments permettant d'identifier les personnes physiques mentionnées dans ces décisions doivent être effacés ; pour la lisibilité, les noms et prénoms peuvent, le cas échéant, être remplacés par des pseudonymes ou des initiales ». En écho à cette recommandation, le législateur a inséré en 2014 dans la LSCC un article 30*quater* qui permet au président de la Cour de « décider, à tout stade de la procédure et même après le prononcé de l'arrêt, d'office ou sur simple demande d'une partie ou d'un tiers intéressé, que les mentions permettant de les identifier directement soient supprimées, dès le moment le plus opportun, dans toute publication à laquelle la Cour procéderait ou aurait procédé en vertu de la présente loi spéciale ou de sa propre initiative ».

3.- Le numérique et la jurisprudence de la Cour constitutionnelle

Nous nous permettons de renvoyer ici aux arrêts de la Cour constitutionnelle cités dans la première partie de cette contribution.

B.- La protection par les autres juridictions

1.- La section du contentieux administratif du Conseil d'État

S'agissant des recours objectifs, le Conseil d'État, section du contentieux administratif, est compétent pour contrôler les normes de valeur réglementaire (parmi lesquelles figurent les décisions de l'administration) touchant notamment aux outils numériques.

Comme nous en avons fait mention précédemment, c'est ainsi, par exemple, que le Conseil d'État s'est prononcé, il y a déjà vingt ans, sur le droit d'accès du citoyen à un document électronique, en l'occurrence le code source d'un logiciel de vote électronique. Dans l'affaire qui a donné lieu à l'arrêt du 21 mai 2001[82], le requérant demandait l'accès aux documents relatifs au vote automatisé, en ce compris le contenu des programmes informatiques utilisés. À cette occasion, le Conseil d'État a affirmé l'importance de pouvoir accéder à un tel outil informatique, soutenant que tout citoyen doit avoir « la possibilité […] de s'assurer lui-même de la fiabilité des systèmes de vote et de dépouillement automatisés »[83], et ce, même si des experts informaticiens sont déjà désignés pour accomplir cette tâche.

Un citoyen peut donc demander l'accès aux fichiers informatiques et aux logiciels utilisés par l'État, en faisant valoir son droit d'accéder aux documents administratifs, consacré notamment par la loi du 11 avril 1994 relative à la publicité de l'administration.

2.- Les juridictions judiciaires

Les traitements de données à caractère personnel peuvent être soumis également au contrôle des juridictions judiciaires en vertu du RGPD et des lois applicables à la matière[84].

---

82 CE, arrêt *Antoun*, n° 95.677, du 21 mai 2001. Au sujet de cet arrêt, v. D. DE ROY, « L'accès aux documents administratifs dans un environnement dématérialisé », in *L'accès aux documents administratifs*, Bruxelles, Bruylant, 2008, p. 831.

83 CE, arrêt *Antoun*, *op. cit.*, p. 10.

84 À ce sujet, v. C. DE TERWANGNE et E. DEGRAVE, *La protection des données à caractère personnel en Belgique – Manuel de base*, Bruxelles, Politeia, coll. Crids, 2019, p. 157 *sq*.

a) L'action en cessation devant le président du tribunal de première instance

En vertu de l'article 79, § 1er, du RGPD, toute personne qui s'estime lésée par un traitement de données à caractère personnel peut introduire un recours juridictionnel effectif. En Belgique, ce recours prend la forme d'une action en cessation devant le président du tribunal de première instance siégeant « comme en référé »[85]. Cette action peut être introduite par la personne elle-même, par un organisme ou une association active dans le domaine de la protection des données ou par l'Autorité de protection des données. Le cas échéant, le président du tribunal de première instance peut sanctionner les traitements de données illégaux de différentes manières : ordonner la cessation définitive d'un traitement de données, ordonner au responsable du traitement, sous peine d'astreinte, de respecter les droits de la personne concernée, etc.[86].

b) L'action en réparation

L'action en réparation est organisée par l'article 82 du RGPD qui octroie le droit pour toute personne d'obtenir réparation du préjudice matériel ou moral causé par un traitement de données illégal. Il s'agit d'un régime de responsabilité sans faute, plus sévère que le régime de responsabilité civile organisé par l'article 1382 du Code civil. En effet, il suffit, pour le requérant, de démontrer un dommage en lien avec une violation du RGPD, sans devoir établir le caractère fautif de cette violation. En fonction de la qualité du requérant, cette action est portée devant le tribunal de première instance ou le tribunal de l'entreprise.

c) L'action devant les juridictions pénales

Comme l'autorise l'article 84 du RGPD, chaque État peut adopter d'autres sanctions que celles prévues par le RGPD. C'est pourquoi, en Belgique, la violation de certaines règles de protection des données est érigée en infraction pénale[87], pouvant mener à une amende pénale comprise entre 250 et 15 000 euros[88]. Il s'agit notamment d'un traitement de données effectué sans base de licéité (par exemple, sans consentement de la personne concernée), du non-respect d'une mesure correctrice imposée par l'Autorité de protection des données, du non-respect du droit d'opposition de la personne concernée, etc.

C.- La protection par des autorités indépendantes spécifiques

Deux autorités spécifiques œuvrent à la protection de la matière en Belgique : l'Autorité de protection des données et le Comité de sécurité de l'information. Leur indépendance est sujette à critique.

85 Art. 209 à 219 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

86 Art. 209 et 214 de la loi du 30 juillet 2018 précitée.

87 V. les art. 222 à 227 de la loi du 30 juillet 2018 précitée.

88 Ces montants doivent être multipliés par les décimes additionnelles dont le coefficient s'élève à 8 depuis le 1er janvier 2017.

1.- L'Autorité de protection des données

En vertu de l'article 36-4 du RGPD, « les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ». L'article 57-1-c ajoute : « Sans préjudice des autres missions prévues au titre du présent règlement, chaque autorité de contrôle, sur son territoire : […] conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ». Par ailleurs, en préambule du RGPD, le considérant n° 96 est rédigé en ces termes : « L'autorité de contrôle devrait également être consultée au stade de la préparation d'une mesure législative ou réglementaire qui prévoit le traitement de données à caractère personnel, afin d'assurer que le traitement prévu respecte le présent règlement et, en particulier, d'atténuer le risque qu'il comporte pour la personne concernée ».

Pour ce qui concerne la Belgique[89], une loi du 3 décembre 2017 « portant création de l'Autorité de protection des données » (ci-après : loi APD) a été adoptée dans cette perspective, cette dernière succédant juridiquement, tout en étant restructurée, à la Commission de la protection de la vie privée. La loi du 3 décembre 2017 crée notamment un Centre de connaissance (qui rend les avis relatifs aux normes en projet), un service d'inspection et une chambre contentieuse, chacun sous la direction d'un des cinq directeurs de l'APD.

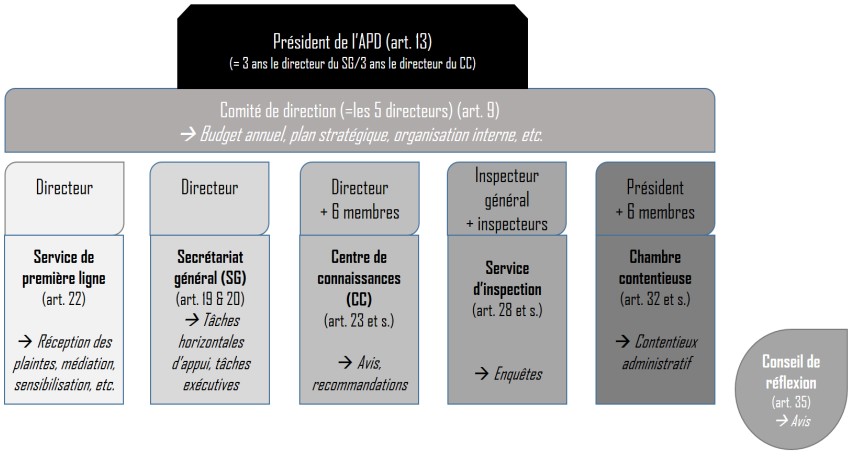


Schéma de la composition de l'APD

Ainsi, l'APD est à la fois un contrôleur, un co-régulateur et un conseiller[90].

89 V. not. V. VERBRUGGEN, « Le rôle des autorités de contrôle de protection des données. Indépendance et polyvalence », in Q. VAN ENIS et C. DE TERWANGNE (dir.), *L'Europe des droits de l'homme à l'heure d'internet*, Bruxelles, Bruylant, 2019, spéc. p. 648.

90 Dans le même sens, à propos de l'autorité de contrôle en général, v. V. VERBRUGGEN, « Titre 1. RGPD : cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne », in C. DE TERWANGNE et K. ROSIER (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, p. 55.

En tant que contrôleur, l'APD veille au respect effectif de la protection des données, par des moyens juridiques classiques (par exemple, le service d'inspection est habilité à mener des enquêtes pour instruire le dossier, durant lesquelles il peut notamment « procéder à des examens sur place »[91]) et par des moyens d'action plus souples et plus rapides (par exemple, la chambre contentieuse peut « formuler des avertissements et des réprimandes »[92]). À la différence de la Commission nationale de l'informatique et des libertés (CNIL) en France, le pouvoir d'amende de l'APD est récent, et date de l'entrée en application du RGPD. Depuis plusieurs années, l'APD sanctionne les responsables de traitement ayant agi illégalement en recourant notamment à l'amende. Ses décisions sont toutes accessibles en ligne et sont le plus souvent anonymisées[93].

En tant que co-régulateur, l'APD œuvre comme relais du législateur au niveau de la définition des règles de protection des données et de leur mise en œuvre. Par exemple, il revient au secrétariat général de l'APD d'« établir la liste des traitements qui requièrent une analyse d'impact relative à la protection des données »[94], ce qui est d'ailleurs chose faite[95].

En tant que conseiller, l'APD prodigue des conseils aux responsables de traitement, aux personnes concernées et au public en général, *via* le service de première ligne. Elle est aussi un conseiller pour les législateurs et les gouvernements, par l'intermédiaire du Centre de connaissances qui rend des avis sur les projets

Par ailleurs, en principe, l'APD doit être indépendante, comme l'exige l'article 52 du RGPD qui affirme notamment que « dans l'exercice de leurs missions et de leurs pouvoirs conformément au présent règlement, le ou les membres de chaque autorité de contrôle demeurent libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque ». Or, l'APD a longtemps souffert d'un manque d'indépendance. En effet, un haut responsable de l'administration, Franck Robben, qui dirige plusieurs institutions spécifiquement dédiées au traitement des données des citoyens (comme la Banque-carrefour de la sécurité sociale) a été, durant plusieurs années, membre de l'APD, chargée de se prononcer sur la légalité des pratiques mises en place au sein des administrations qu'il dirige. Cette personne était donc à la fois juge et partie, ce qui est interdit tant par le RGPD que la jurisprudence de la Cour de justice de l'Union européenne. Cette situation a généré beaucoup de remous ces derniers mois dans la presse belge. De nombreuses voix réclamaient la levée du mandat de Franck Robben par le Parlement fédéral. Par ailleurs, une plainte anonyme avait été introduite par des citoyens, auprès de la Commission européenne, pour dénoncer le manque d'indépendance de l'APD. Cette plainte a retenu l'attention de la Commission européenne. C'est seulement le 7 février 2022, soit la veille du jour où la Belgique allait être assignée devant la Cour de justice de l'Union européenne, que Franck Robben a démissionné de son poste à l'APD[96].

---

91 Art. 66, §1er, 4°, de la loi APD.

92 Art. 100, §1er, 5°, de la loi APD.

93 V. https://www.autoriteprotectiondonnees.be/citoyen/publications/decisions.

94 Art. 20, § 1, 2°, de la loi APD.

95 V. https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste_des_traitements_AIPD.pdf.

96 Pour plus d'informations, v. https://plus.lesoir.be/376968/article/2021-06-08/vie-privee-la-commission-lance-une-procedure-dinfraction-au-rgpd-contre-la ; https://www.lesoir.be/422741/article/2022-02-07/de-justesse-frank-robben-demissionne-de-son-poste-lautorite-de-protection-des

2.- Le Comité de sécurité de l'information

Le Comité de sécurité de l'information (ci-après : CSI) est un organe, institué par une loi du 5 septembre 2018[97], qui est chargé de contrôler l'échange, entre administrations, des données de santé et de sécurité sociale[98].

A priori, l'idée est intéressante : organiser un contrôle spécifique dans deux domaines délicats de l'administration, contrôle exercé par des personnes de disciplines différentes[99]. En principe, ce contrôle doit se limiter à vérifier que les conditions fixées par le législateur sont respectées en pratique, comme vérifier si les données utilisées sont réellement anonymisées. On peut comparer ce type de contrôle à un contrôle technique automobile : il s'agit de vérifier si la voiture peut être lancée sur la route, et non de définir l'âge légal du conducteur.

Néanmoins, dans les faits, la situation est très problématique. Le pouvoir du CSI ne se limite pas à un contrôle technique. Le CSI œuvre comme un législateur, en définissant lui-même les éléments essentiels de certains traitements de données, dans des décisions qui ne sont pas publiées au *Moniteur belge* et ne sont contrôlées ni par la section de législation du Conseil d'État, ni par l'APD. La possibilité d'en obtenir l'annulation en justice est par ailleurs incertaine. C'est ainsi, par exemple, que la question de savoir si les sociétés de transport en commun ou les universités pourront un jour avoir accès à la liste des personnes vaccinées dépendra, non du législateur, mais d'une décision du CSI. Une plainte anonyme a également été introduite auprès de la Commission européenne à propos du CSI. Celle-ci ne s'est toutefois pas encore prononcée sur les suites à y réserver.

97 Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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.

98 Au sujet d'une analyse détaillée du CSI, v. C . DE TERWANGNE et E. DEGRAVE, *op. cit*., p. 174 *sq*.

99 Le CSI est en effet notamment composé d'un médecin, d'un juriste, d'un informaticien, d'un fiscaliste etc. (v. l'art. 2 de la loi du 5 septembre 2018 précitée).