Les citoyens contrôlés via leurs données Covid ?

Degrave, Elise

Published in:
Journal des Tribunaux

Publication date:
2021

Document Version
le PDF de l'éditeur

strada lex

Bureau de dépôt : Louvain 1
Hebdomadaire, sauf juillet et août
ISSN 0021-812X
P301031

Journal des tribunaux

https://jt.larcier.be
13 février 2021 - 140e année
7 - No 6845
Georges-Albert Dal, rédacteur en chef

Sommaire

Vie du droit

Les citoyens contrôlés via leurs données Covid ? - Le « datamatching » et le « datamining » utilisés par l'État, par E. Degrave 125

Le point sur...

Les questions de procédure dans la conciliation judiciaire, par B. Inghels 128

Jurisprudence

■ Code des sociétés et des associations - Réforme du droit des personnes morales - Règlement d'ordre intérieur - Indication du nombre d'actions dans les statuts - Société coopérative - Recours - Annulation des articles 2:59, alinéa 1er, 3o, et 6:13, alinéa 1er, 4o, du Code des sociétés et des associations

Cour const., 15 octobre 2020, observations de P. De Wolf et I. Vermeiren 134

■ Faute procédurale - Négligence dans la mise en état - Suspension des intérêts - Compensation des dépens (article 1017, alinéa 4, C. jud.)

Civ. Bruxelles, 87e ch., 5 octobre 2020 136

■ Délai d'appel - Solidarité - Effets secondaires

Civ. Hainaut, div. Mons, 3e ch., 20 mars 2019 138

Chronique

Bibliographie - Coups de règle.

Vie du droit

Les citoyens contrôlés via leurs données Covid ?

Le « datamatching » et le « datamining » utilisés par l'État

Parmi les sujets auxquels le Covid aura donné un coup de projecteur, il y a la gestion des données des citoyens par l'État. Depuis quelques mois, le traçage des citoyens, suivi du fichage des personnes vaccinées, font naître des craintes liées notamment aux potentielles réutilisations des données des individus. On pointe du doigt l'absence de lois, qui détermineraient, au terme d'un débat démocratique éclairé et éclairant, quelles autorités peuvent (ré)utiliser quelles données, pendant combien de temps et dans quel but, ce qu'on appelle traditionnellement « les éléments essentiels des traitements de données »[1]. Ces lois de qualité, précises et prévisibles, sont pourtant exigées par notre Constitution et les normes supranationales[2] qui consacrent le principe de légalité des ingérences dans la vie privée, comme le rappelle, depuis longtemps, la Cour constitutionnelle, notamment[3].

L'article 8 de l'arrêté ministériel du 12 janvier 2021[4] soulève à nouveau cette préoccupation. Il dispose que « dans le cadre de la lutte contre le coronavirus Covid-19, l'Office national de sécurité sociale peut, en qualité de sous-traitant pour le compte de tous les services et institutions chargés de la lutte contre la propagation du coronavirus Covid-19, ainsi que de tous les services ou institutions chargés de surveiller le respect des obligations prévues dans le cadre des mesures d'urgence prises pour limiter la propagation du coronavirus Covid-19, collecter, combiner et traiter, y compris via le *datamining* et le *datamatching*, des données concernant la santé relatives au coronavirus Covid-19, des données de contact, d'identification, de travail et de résidence relatives aux travailleurs salariés et travailleurs indépendants, en vue de soutenir le traçage et l'examen des *clusters* et des collectivités ».

Ainsi donc, la seule ministre de l'Intérieur, Annelies Verlinden, habilite l'Office national de sécurité sociale (O.N.S.S.) à faire beaucoup de choses (« collecter, combiner et traiter, y compris via le *datamining* et le *datamatching* »), avec beaucoup de données (« des données de santé relatives au coronavirus (...), des données de contact, d'identification, de travail, de résidence »[5]), à propos de beaucoup de citoyens (« travailleurs salariés et travailleurs indépendants »), pour rendre service à beaucoup d'institutions (« tous les services et institutions chargés de la lutte contre la propagation du coronavirus (...), ainsi que de tous les services ou institutions chargés de surveiller le respect des obligations prévues dans le cadre des mesures d'urgence prises pour limiter la propagation du coronavirus (...) »). Et ce, dans le but, très ample lui aussi, « de soutenir le traçage et l'examen des *clusters* et des collectivités ».

Faut-il comprendre par-là que les données Covid, initialement collectées pour aider le citoyen à sortir de la crise, vont à présent être utilisées pour le surveiller ?

À ce stade, il n'y a pas de réponse précise. Aucune loi n'a été adoptée pour encadrer ces nouvelles utilisations de données à caractère personnel. C'aurait pourtant été l'occasion, en respectant le principe de légalité qui vient d'être rappelé, de débattre notamment de la réutilisation de telles données à des fins de contrôle. Car l'article 8 de l'arrêté ministériel ne contient pas de balises claires, l'usage des termes anglicisants « datamatching » et « datamining » en compliquant encore davantage la compréhension.

Pour essayer de comprendre la portée de cette disposition réglementaire incertaine et, notamment, les potentielles réutilisations des données Covid, il est intéressant de la mettre en lien avec les normes et pratiques existantes, qui mobilisent déjà les techniques de « datamatching » et « datamining ». Il convient également de souligner qu'au-delà de leur efficacité, ces techniques

(1) Voy. notamment les avis de l'Autorité de protection des données (ci-après « APD ») sur le traçage (avis no 36/2020) et sur l'enregistrement de la vaccination (avis no 138/2020).
(2) Voy. l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme, l'article 8 de la Charte européenne des droits fondamentaux et l'article 6.3. du Règlement général sur la protection des données (RGPD).
(3) Voy. notamment C. const., 23 avril 2015, no 44/2015, B.36.2. ; 5 octobre 2017, no 108/2017, B.6.3. et B. 6.4. ; 15 mars 2018, no 29/2018, B. 13.2.
(4) Ci-après « article 8 de l'arrêté ministériel ».
(5) Nous qualifions l'ensemble de ces données de « données Covid » dans la suite de l'étude.

renferment des risques pour les libertés individuelles, comme l'a démontré l'affaire judiciaire *SyRI* aux Pays-Bas.

1 Le « datamatching » et le « datamining » dans l'administration belge

Après avoir défini ces notions, on en analyse la mise en pratique par l'étude d'un outil de profilage (OASIS) et une loi qui en fait état.

A. Définitions et application aux données Covid

Le « datamatching » et le « datamining » sont des techniques informatiques applicables à des données. Le « datamatching »[6] 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 »[7]. On applique aux données des algorithmes[8] qui vont induire de ces données des informations nouvelles, comme le ferait une boule de cristal. Cela permet de réaliser du profilage[9], 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)[10].

Qu'en est-il de l'application de ces techniques aux données Covid ? Selon la presse[11], les autorités fédérales vont vérifier que les personnes revenant de séjour à l'étranger se sont fait tester en confrontant les données contenues dans les formulaires de retour de vacances[12] aux données relatives aux tests. À défaut de test, les personnes concernées se verront infliger une amende de 250 EUR. Ainsi, en croisant ces données, les autorités fédérales vont réaliser du « datamatching » sur les données Covid.

L'article 8 de l'arrêté ministériel organise également le « datamining ». Cela signifie-t-il que les données Covid vont être utilisées pour rattacher un individu à un profil ? Et si oui, de quel profil va-t-il s'agir ? Pour en tirer quelles conséquences ? L'idée est-elle, par exemple, de rattacher toutes les personnes ayant « oublié » de faire un test à leur retour de vacances à un profil de fraudeur ? Juridiquement, rien ne semble l'interdire actuellement. Au contraire...

La question des potentialités du « datamining » sur des données détenues par l'État gagne à être instruite en s'intéressant à un outil de profilage déjà fonctionnel en Belgique, ainsi qu'à une loi prétendant donner une assise à ces techniques.

B. Un outil bien caché : OASIS

Depuis 2002, un outil dénommé OASIS[13] est utilisé par l'O.N.S.S. pour lutter contre la fraude sociale[14]. Cet outil n'est mentionné par aucune norme juridique. En outre, d'expérience, on peut affirmer que l'accès à l'information à ce sujet est particulièrement fastidieux[15]. Manquant d'encadrement légal et de transparence, OASIS est inconstitutionnel et méconnaît plusieurs droits fondamentaux[16]. Pourtant, il s'agit là d'un outil puissant de l'administration appelé à le devenir encore davantage à l'avenir[17].

OASIS est un « datawarehouse »[18] qui centralise une masse d'informations, relatives aux employeurs, aux travailleurs, ainsi qu'aux allocataires sociaux[19]. Ces données sont analysées par des algorithmes secrets[20] afin d'identifier la probabilité, pour chaque individu, d'être un fraudeur social. On vise ainsi, notamment, à traquer le travail au noir et la fraude aux allocations sociales via les domiciliations fictives[21].

OASIS présente donc des points communs avec l'article 8 de l'arrêté ministériel qui vise, lui aussi, l'O.N.S.S., le « datamatching » et le « datamining », la « surveillance » et les données des travailleurs. Doit-on s'attendre à ce que les données Covid soient injectées dans OASIS, pour, tout à la fois, lutter contre la pandémie et la fraude sociale, au départ de cette infrastructure déjà en place ? On pourrait imaginer, par exemple, qu'un chômeur (identifié dans les bases de données de l'O.N.S.S.) soit ciblé (via les données de traçage), comme ayant été contaminé dans une entreprise. Risquerait-il alors d'être rattaché au profil de fraudeur effectuant du travail au noir et de voir ses allocations de chômage suspendues, alors même qu'il était peut-être dans cette entreprise pour y passer un entretien d'embauche ? Actuellement, le flou des normes juridiques[22] ne permet pas de répondre de manière certaine à cette question, ce qui constitue une violation, rappelons-le, du principe de légalité des traitements de données consacré notamment par l'article 22 de la Constitution.

C. Une loi très floue : la loi du 5 septembre 2018 instituant le Comité de sécurité de l'information (« CSI »)[23]

La loi CSI est une loi « fourre-tout »[24], adoptée à la fin de l'été, qui, par trois dispositions noyées dans la masse, donne une base légale générale à la création d'un « *datawarehouse* (...) permettant de procéder à des opérations de *datamining* et *datamatching*, en ce compris de profilage (...) », en matière sociale[25] et en matière fiscale[26].

À nouveau, il s'agit de centraliser quantité de données et d'y appliquer des algorithmes, pour cibler les personnes suspectées de ne pas respecter les législations concernées. Cette loi, très vague, ne précise notamment ni les données centralisées, ni les finalités poursuivies, ni les

(6) En français « couplage de données ».
(7) En français « extraction de données ».
(8) 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).
(9) L'article 4.4 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.
(10) En guise d'exemple simple, prenons le cas de John, dont les données fiscales montrent qu'il gagne 2.000 EUR par mois. Or, ses données à la DIV montrent qu'il détient 7 Ferrari neuves. 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.
(11) *Le Soir*, 19 janvier 2021 accessible ici : https://plus.lesoir.be/349947/article/2021-01-19/une-amende-automatique-de-250-euros-pour-ceux-qui-refusent-le-test-en-revenant.
(12) Il s'agit du *Passenger Locator Form*, accessible ici https://travel.info-coronavirus.be/public-health-passenger-locator-form.
(13) Acronyme de « Organisation Anti-fraude des Services d'inspection sociale ».
(14) À ce sujet, voy. E. Degrave, « Contrôle des assurés sociaux et profilage dans le secteur public », *J.T.*, 2015, pp. 517-519.
(15) La plupart des informations que nous avons pu obtenir à son sujet nous ont été confiées par deux personnes de l'administration, souhaitant garder l'anonymat.
(16) En particulier le droit à la vie privée et le droit à la transparence administrative. Voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier, 2014, coll. Crids, n° 40 et s. Voy. *infra* à propos de l'affaire *SyRI*.
(17) Un « super-OASIS », fondé sur l'utilisation de l'intelligence artificielle, est en préparation. Voy. https://www.smals.be/fr/plateforme-de-big-data-analytics.
(18) En français, « entrepôt de données », c'est-à-dire une très grande base de données.
(19) Ces données sont issues de plusieurs bases de données différentes détenues par l'administration. Il s'agit notamment de données fiscales, des données de sécurité sociale, des données relatives à la pension, mais aussi des données fournies par les fournisseurs d'énergie (gaz, eau et électricité) à propos de leurs clients.
(20) Malgré de nombreuses demandes d'accès aux algorithmes, qui constituent pourtant des documents administratifs, il nous a été impossible d'en obtenir une copie ou même des documents explicatifs de ceux-ci.
(21) Pour davantage d'informations à ce sujet, voy. E. Degrave, « The use of secret algorithms to combat social fraud in Belgium », *European Review of Digtital Administration & Law*, 2020, pp. 167-177 en accès libre ici http://www.aracneeditrice.it/pdf2/9788825538960 15.pdf.
(22) On vise en particulier la large finalité « d'examen des collectivités » figurant dans l'article 8 de l'arrêté ministériel et qui n'est pas définie, conjugué au non-encadrement d'OASIS.
(23) Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois (...) (ci-après « loi CSI »).
(24) Cette loi institue un nouvel organe (voy. *infra*), modifie 9 législations, et contient 99 articles.
(25) Articles 12 et 13 loi CSI qui visent la sécurité sociale et le droit du travail. Vu les similitudes avec l'outil OASIS qui, lui, ne fait l'objet d'aucune norme, on peut se demander si ces dispositions sont censées l'encadrer. Néanmoins, ces dispositions ne visent pas explicitement OASIS et cet outil n'est pas non plus mentionné dans les travaux préparatoires de la loi CSI.
(26) Article 71 loi CSI.

réutilisations possibles, n'organise aucune garantie encadrant les opérations de profilage[27] et va jusqu'à supprimer certains droits que le Règlement général sur la protection des données (RGPD) accorde pourtant aux citoyens[28]. Notons que ces dispositions n'ont fait l'objet d'aucun débat au Parlement, tandis que les avis de la Section de législation du Conseil d'État[29] et de l'Autorité de protection des données[30] — qui critiquaient vivement ce flou normatif inconstitutionnel — n'ont provoqué que d'insuffisantes modifications[31].

Plus encore, cette loi institue un nouvel organe de contrôle, le CSI, composé d'« experts »[32], et à qui est déléguée la compétence de déterminer, seul, quelles autorités sont habilitées à (ré)utiliser quelles données et pourquoi[33], ce qui, rappelons-le, devrait pourtant être défini par le législateur lui-même. Le CSI peut ainsi décider d'étendre un *datawarehouse* à d'autres secteurs et finalités[34], d'y injecter d'autres données[35] et, de manière générale, d'autoriser la réutilisation, pour des finalités indéterminées, des données détenues par toute institution de sécurité sociale[36].

En l'occurrence, on peut donc raisonnablement en déduire que le CSI est compétent pour autoriser, seul, la réutilisation, pour des finalités autres que sanitaires, des données Covid centralisées par l'O.N.S.S.[37], y compris pour les croiser avec différentes données et y appliquer des algorithmes de *datamining* à des fins de lutte contre la fraude fiscale[38] et/ou sociale[39], et ce, sans être soumis au respect de critères clairs fixés par le législateur. Le CSI a déjà commencé à autoriser la réutilisation des données Covid à des fins de contrôle via le datamining notamment. Voyez sa décision du 18 janvier 2021, très difficile à trouver d'ailleurs https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/deliberations/20_178_f036.pdf.

Ainsi donc, le pouvoir discrétionnaire du CSI est si large qu'il revient à substituer le CSI au Parlement et les décisions du CSI aux lois ce qui, de toute évidence, est une violation de l'article 22 de la Constitution, notamment.

2 Les risques du « datamatching » et du « datamining » à la lumière de l'affaire *SyRI* aux Pays-Bas

Bien qu'elles aient la réputation d'être efficaces, les techniques de *datamatching* et de *datamining* présentent des risques qui ont récemment été mis en lumière dans une affaire judiciaire aux Pays-Bas, l'affaire *SyRI*, dont il serait judicieux de tirer les leçons en Belgique également.

SyRI pour *System of Risk Indicator*, est un outil néerlandais semblable à OASIS. De multiples données y sont centralisées et on y applique des algorithmes secrets pour identifier les personnes suspectées de frauder les aides sociales et le droit du travail. Des ONG, notamment, ont saisi la justice pour mettre fin à cet outil, ayant constaté qu'il ciblait en priorité les quartiers pauvres et les quartiers de migrants, les algorithmes appliqués contenant probablement des « biais »[40] amenant l'outil à cibler en priorité ces catégories de la population, et ce de manière discriminatoire.

Dans sa décision du 5 février 2020[41], le tribunal de district de La Haye affirme que SyRI est contraire au droit fondamental à la protection de la vie privée, en raison notamment du manque de légalité et de transparence de l'outil. Cette décision a eu pour effet l'arrêt immédiat de l'outil SyRI.

Selon le tribunal, bien que l'objectif poursuivi soit légitime, « l'existence d'une protection juridique adéquate de la vie privée dans l'échange de données à caractère personnel par des organismes (gouvernementaux) contribue à la confiance des citoyens dans le gouvernement, tout autant que la prévention et la lutte contre la fraude », confiance sans laquelle « les citoyens seront moins susceptibles de fournir des données ou d'apporter leur soutien »[42]. La législation doit donc « permettre à tous les intérêts en jeu d'être soupesés de manière transparente et vérifiable »[43]. C'est pourquoi, « le législateur a (...) une responsabilité particulière en cas d'utilisation d'un instrument tel que SyRI »[44]. En l'espèce, l'ingérence dans la vie privée est importante, compte tenu notamment de la « très grande catégorie de données traitées »[45]. Pourtant, la loi n'est pas de qualité suffisante pour prétendre encadrer cette ingérence, notamment en ce qu'elle n'organise ni la limitation des finalités ni la minimisation des données[46]. Le tribunal constate donc que la loi SyRI viole l'exigence de légalité imposée par l'article 8, § 2, de la Convention européenne des droits de l'homme[47].

En outre, le tribunal déplore le manque de transparence de SyRI. « La législation SyRI ne fournit pas d'informations relatives au fonctionnement du modèle de risque, par exemple sur le type d'algorithmes utilisés »[48], ni n'organise l'« obligation légale d'informer séparément les personnes concernées, le cas échéant, du fait qu'un rapport sur les risques a été établi »[49] alors qu'un tel rapport « a un effet significatif sur la vie privée de la personne [concernée] »[50]. Par conséquent, il est « difficile de voir comment une personne concernée peut se défendre contre le fait qu'un rapport de risque a été établi à son égard »[51]. Et d'insister sur « l'importance de la transparence, en vue de la contrôlabilité » de l'outil, car celui-ci peut mener à ce que des « effets discriminatoires (involontaires) se produisent »[52]. Or, au regard de la législation SyRI actuelle, « il n'est pas possible d'évaluer si ce risque a été suffisamment atténué, en raison d'un manque de connaissances vérifiables sur les indicateurs de risque et le fonctionnement du mo-

(27) Sur ces garanties, voy. notamment les articles 22 et 37 du RGPD.
(28) Voy. par exemple l'article 61 loi CSI qui va jusqu'à supprimer le droit à l'information d'une personne visée par une enquête pour fraude.
(29) SLCE, avis n° 63.202/2 du 26 avril 2018 relatif à un projet de loi instituant le comité de sécurité de l'information (...), *Doc. parl.*, Chambre, 54-3185/001, pp. 120 et s.
(30) APD, avis n° 34/2018 du 11 avril 2018 concernant un avant-projet de loi instituant le comité de sécurité de l'information (...).
(31) Dans le même sens, B. Salovic, O. Guerguinov et T. Léonard, « Sous couvert de sécurité, la loi belge viole-t-elle le RGPD ? », 12 septembre 2018, accessible ici https://www.droit-technologie.org/actualites/couvert-de-securite-loi-belge-viole-t-rgpd/.
(32) Sur la composition et le fonctionnement du CSI, voy. C. de Terwangne et E. Degrave (avec la coll. de A. Delforge et L. Gérard), *Protection des données à caractère personnel en Belgique : manuel de base*, Bruxelles, Politeia, 2019, pp. 174 et s.
(33) Outre le fait que ces décisions ne sont pas débattues démocratiquement, elles sont difficiles à trouver. Elles sont accessibles ici https://www.ksz-bcss.fgov.be/fr/protection-des-donnees/comite-de-securite-de-linformation-csi. Depuis 2018, 734 décisions ont été adoptées, parmi lesquelles il est impossible de faire une recherche par mots-clés ou par type de décision.
(34) Voy. article 13, alinéa 3, loi CSI qui vise la possibilité de réutiliser les données pour d'autres finalités que la sécurité sociale et le droit du travail, moyennant une autorisation du CSI.
(35) Voy. article 71, alinéa 2, loi CSI qui vise la possibilité d'injecter dans le *datawarehouse* fiscal « toute catégorie de données à caractère personnel fournie par des tiers » moyennant l'autorisation du CSI.
(36) Article 18 loi CSI.
(37) En vertu de l'article 18 loi CSI.
(38) Article 71, alinéa 2, loi CSI.
(39) Article 13, alinéa 3, loi CSI.
(40) Les « biais algorithmiques » sont liés au fait qu'un algorithme résulte du choix fait par l'humain qui l'a conçu et qui y met — consciemment ou non — sa propre sensibilité. Ces biais peuvent entraîner des conséquences racistes, sexistes, qui nuisent aux pauvres, etc. À ce sujet, voy. C. O'Neill, *Weapons of Math Destruction : How Big Data Increases Inequality and Threatens Democracy*, USA, Crown Books, 2016. Utilisés à l'échelle d'une population, de tels biais peuvent conduire à « automatiser les inégalités » selon l'expression de V. Eubanks (*Automating inequality. How high-tech tools profile, police and punish the poor*, New York, St Martin's Press, 2018).
(41) Cette décision est accessible ici : https://uitspraken.rechtspraak.nl/inziendocument ?id=ECLI:NL:RBDHA:2020:865. Pour un ommentaire de cette décision, voy. G. Lewkvitch, « Les outils d'intelligence artificielle contre les droits de l'homme : l'affaire *NJCM C.S./De Staat der Nederlanden* », accessible ici https://www.incubateurbxl.eu/fr/les-outils-dintelligence-artificielle-contre-les-droits-de-lhomme-laffaire-njcm-c-s-de-staat-der-nederlanden/.
(42) La traduction des extraits cités dans cette étude est libre. Arrêté précité, n° 6.5.
(43) Arrêté précité, n° 6.6.
(44) Arrêt précité, n° 6.85.
(45) Arrêté précité, n° 6.82.
(46) Arrêt précité, n° 6.86.
(47) Arrêté précité, n° 6.83.
(48) Arrêt précité, n° 6.89.
(49) Arrêté précité, n° 6.65.
(50) Arrêt précité, n° 6.59.
(51) Arrêt précité, n° 6.90. Remarquons qu'en Belgique, un citoyen auquel un profil aurait été injustement attribué (par suite d'une erreur dans les données utilisées par exemple), se trouverait d'autant plus démuni que l'accès aux données que l'administration détient à son sujet est très fastidieux, quand il n'est pas carrément interdit (voy. *supra*). Il ne pourrait alors que subir en silence les dommages créés par cette erreur : contrôles à répétition, suspension de droits, demandes de remboursement, etc.
(52) Arrêt précité, n° 6.91.
(53) Arrêt précité, n° 6.94.

dèle de risque »[53]. De ce fait, l'ingérence dans la vie privée est jugée disproportionnée et contraire à l'article 8, § 2, précité[54].

Les mêmes critiques pourraient actuellement s'appliquer aux outils de *datamining* belges et, en particulier, à OASIS.

Conclusion

Que fera-t-on des données Covid à l'avenir ? Il est impossible de le savoir. Il est impossible de le prévoir. D'inquiétants problèmes juridiques affectant l'article 8 de l'arrêté ministériel mais également l'outil de profilage OASIS et la loi CSI laissent penser que les réutilisations les plus larges sont possibles. Les pratiques et outils mis en place, qui impactent pourtant toute la population, manquent de balises précises, heurtant les exigences constitutionnelles et supranationales de protection de la vie privée.

Pourtant, même lorsque l'utilisation des données des citoyens par l'État poursuit un objectif légitime, les données qui sont centralisées, les finalités qui sont poursuivies, les autorités qui accèdent aux données, les algorithmes appliqués, les profils préétablis, doivent être clairement encadrés par le législateur, et non laissés à l'appréciation discrétionnaire de gens de l'ombre. À défaut, le citoyen pourrait se trouver confronté aux mêmes risques que ceux qui ont été éprouvés aux Pays-Bas et qui ont provoqué la mise à l'arrêt de l'outil de profilage SyRI.

En définitive, le gouvernement fédéral recourt-il à des outils tout puissants dont lui-même n'aurait déjà plus la maîtrise ? Le réveil du Parlement est urgent, pour que ce qui est techniquement faisable reste également démocratiquement acceptable.

Elise DEGRAVE
Professeure à l'UNamur
Membre du Namur Digital Institute/Crids[55]

(54) Arrêt précité, n° 6.95.
(55) Je remercie Laurent Schumacher, professeur à la Faculté d'informatique de l'UNamur, pour les idées échangées. Néanmoins, les opinions défendues dans cet article n'engagent que moi.

Les questions de procédure dans la conciliation judiciaire[1]

Concilier est une des missions du juge, mais concilier n'est pas une démission du juge
C. JARROSSON , « Présentation générale de la conciliation - Définition - Historique - Objectifs », *Gaz. Pal.* 4-6 octobre 1998, p. 11, n° 12.

1. Le juge a pour mission de trancher, décider, juger. Il a aussi pour mission de concilier, selon l'article 730/1, § 1er, du Code judiciaire[2].

À l'exception des chambres de règlement amiable du tribunal de la famille[3] [4], il y a aujourd'hui autant de pratiques de conciliation que de magistrats conciliateurs. Que la personnalité, l'empathie, l'écoute de chaque homme ou femme conciliateur soient déterminantes dans le processus est une évidence. Que des outils pour favoriser le dialogue et la construction d'un accord existent et méritent un enseignement en est une autre[5]. Il ne faudrait cependant pas oublier que le juge inscrit

(1) L'auteure remercie chaleureusement Alice Dejollier et Jean-François van Drooghenbroeck pour leurs commentaires et échanges sur ce sujet.
(2) Cet article traite de la conciliation de droit commun, et non pas de la conciliation organisée dans les chambres de règlement amiable du tribunal de la famille.
(3) Celles-ci sont réorganisées dans le Code judiciaire par la loi du 18 juin 2018 portant dispositions diverses en matière de droit civil et des dispositions en vue de promouvoir des formes alternatives de règlement des litiges. L'article 1253*ter*/1 du Code judiciaire dispose :
§ 1er. Dans toutes les causes relevant du tribunal de la famille, dès qu'une demande est introduite, le greffier informe les parties de la possibilité de médiation, de conciliation et de tout autre mode de résolution amiable des conflits en leur envoyant immédiatement le texte des articles 1730 à 1737 accompagné d'une brochure d'information concernant la médiation, rédigée par le ministre qui a la Justice dans ses attributions, la liste des médiateurs agréés spécialisés en matière familiale établis dans l'arrondissement judiciaire, ainsi que les renseignements concernant les séances d'information, permanences ou autres initiatives organisées dans l'arrondissement judiciaire afin de promouvoir la résolution amiable des conflits.
§ 2. En matière familiale, lors de la comparution des parties à l'audience introductive d'instance, le juge entend les parties sur la manière dont elles ont tenté de résoudre le litige à l'amiable avant l'introduction de la cause, et afin de déterminer si une résolution à l'amiable est envisageable. À la demande des parties ou si le juge l'estime utile, il peut remettre l'affaire à une date déterminée qui ne peut excéder le délai d'un mois, sauf s'il existe à cet égard un accord entre les parties selon les modalités prévues à l'article 730/1. À la demande des parties ou s'il l'estime utile, il peut également renvoyer l'affaire devant la chambre de règlement à l'amiable, conformément au paragraphe 3.
§ 3. En matière familiale, les affaires peuvent être soumises à fin de conciliation à la chambre de règlement à l'amiable du tribunal de la famille ou des chambres famille de la cour d'appel. Tel peut être également le cas lorsque l'affaire est pendante devant une autre chambre de la famille pour autant que la chambre de règlement à l'amiable soit en mesure de tenir une audience à une date antérieure. À la demande des parties ou s'il l'estime utile, le juge ordonne le renvoi de la cause à la chambre de règlement à l'amiable du même tribunal ou des mêmes chambres famille de la cour d'appel, par simple mention au procès-verbal de l'audience. Le greffier transmet le dossier de la procédure, dans les trois jours de cette décision, au greffier de la chambre de règlement à l'amiable à laquelle la cause a été renvoyée. Le greffier de la chambre de règlement à l'amiable convoque les parties, sous pli judiciaire, à comparaître, aux lieu, jour et heure de l'audience à laquelle l'affaire sera appelée. À défaut d'accord ou en cas d'accord partiel, la chambre de règlement à l'amiable renvoie, selon les mêmes formalités que celles prévues à l'alinéa 2, le dossier devant la chambre de la famille devant laquelle le dossier a été introduit. Tout au long de l'instance, les parties ou le magistrat ont la possibilité de solliciter le renvoi de leur cause devant la chambre de règlement à l'amiable. De même, tout au long de l'instance, si un accord total ou partiel intervient, le procès-verbal en constate les termes et l'expédition est revêtue de la formule exécutoire, sauf si les parties requièrent l'application de l'article 1043. Tout ce qui se dit ou s'écrit au cours des audiences de règlement à l'amiable est confidentiel. Tant les parties que le juge de la chambre de règlement à l'amiable peuvent, à tout moment, mettre un terme à la procédure de règlement à l'amiable.
(4) Pour un commentaire de ces dispositions, voy. J.-M. DEGRYSE, « La conciliation devant la chambre de règlement amiable du tribunal de la famille », *in* A. DEJOLLIER, C. DELFORGE et J.-F. VAN DROOGHENBROECK (coord.), *Le conflit : quelles approches ?*, Limal, Anthemis, 2020, pp. 149-157.
(5) Chaque année, l'Institut de formation de l'Ordre judiciaire organise une formation à la conciliation, à destination des magistrats nouvellement nommés.