L'autorité de contrôle

Degrave, Élise

Published in:
Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 11
L'autorité de contrôle

Elise DEGRAVE[1]

Tant la directive 95/46/CE[2] que le RGPD[3] érigent l'autorité de contrôle en « élément essentiel de la protection des données »[4]. Et pour cause. Le régime juridique de la protection des données risquerait bien de n'être qu'un vœu pieu sans une autorité chargée de faire connaître ces règles et de veiller à leur application dans la pratique.

La directive 95/46/CE a encouragé l'institution de ces autorités de contrôle dans chaque État membre. Le RGPD vient aujourd'hui harmoniser le statut et le fonctionnement de celles-ci, favorisant l'uniformisation des règles au travers de l'Union européenne et la coopération entre ces institutions. En outre, le RGPD affine l'exigence d'indépendance de l'autorité de contrôle et renforce ses pouvoirs d'action et de sanction.

CHAPITRE 1. Un rôle confirmé et harmonise

1. Les premières autorités de contrôle. Les premières autorités de contrôle sont apparues très tôt, dès les années septante, à l'occasion des réflexions entourant l'informatisation de l'administration et la naissance des craintes liées à l'utilisation des données à caractère personnel des citoyens dans un État informatisé.

---

[1] Chargée de cours à la Faculté de droit de l'Université de Namur et Directrice de recherches au CRIDS/Chaire Egov.

[2] 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.

[3] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[4] Considérant n° 62 de la directive 95/46/CE ; considérant n° 117 du RGPD.

Ces autorités étaient alors conçues comme les « chiens de garde » des premières bases de données étatiques, chargées d'en baliser l'accès et d'empêcher l'usage abusif des données qui y étaient enregistrées. Ainsi par exemple, la Commission consultative de la protection de la vie privée, ancêtre de la Commission de la protection de la vie privée, est la première autorité de contrôle belge. Elle a été instituée à l'occasion de la création du Registre national en 1983 pour rencontrer la crainte d'un usage abusif de cette première base de données étatique. Elle était alors chargée de rendre des avis relatifs à l'accès au Registre national et à l'utilisation du numéro d'identification au Registre national. Quelques années plus tôt, la même crainte était apparue en France alors que l'État envisageait de mettre en place le projet SAFARI[5]. Il s'agissait d'attribuer à chaque citoyen un numéro d'identification unique pour tous les fichiers publics, de manière à faciliter le regroupement de leurs informations. Les vives contestations rencontrées par ce projet ont abouti à l'adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et à l'institution de la Commission nationale Informatique et Libertés (CNIL).

2. Pourquoi une autorité de contrôle ? L'autorité de contrôle est une autorité de régulation pour les traitements de données à caractère personnel. Comme en matière de télécommunications, dans le domaine de l'audiovisuel, ou dans le secteur de l'énergie (gaz et électricité), par exemple, l'objectif de la régulation des traitements de données à caractère personnel est d'assurer un équilibre entre des intérêts contradictoires, pour garantir le bon fonctionnement d'un secteur[6]. En l'espèce, l'autorité de contrôle des traitements de données à caractère personnel est chargée de trouver, au gré des questions dont elle doit connaître, un équilibre entre l'intérêt du responsable du traitement de données et le droit à la protection de la vie privée de la personne dont les données sont traitées.

L'autorité de contrôle est conçue pour travailler de manière flexible, et dégager des solutions particulièrement bien adaptées aux questions soulevées par les traitements de données à caractère personnel, préoccupation qui ne pourrait être pleinement rencontrée par la seule intervention législative et réglementaire en raison des particularités de cette matière. En effet, les traitements de données sont soumis aux « turbulences incessantes que provoquent des évolutions technologiques rapides

[5] SAFARI est l'acronyme de « système automatisé pour les fichiers administratifs et le répertoire des individus ».

[6] M.-A. Frison-Roche, « Le droit de la régulation », *D.*, 2001, p. 613 ; D. De Roy et R. Queck, « De la téléphonie vocale aux offres publiques d'acquisition. Vers un 'droit de la régulation' ? », *J.T.*, 2003, p. 555.

et imprévisibles »[7]. Dans ce contexte, « l'État est [...] dépassé par la tâche »[8] ; les normes générales et abstraites adoptées par le pouvoir législatif et le pouvoir exécutif ne suffisent plus à elles seules pour garantir l'objectif d'équilibre poursuivi. Ces normes doivent donc être complétées par des moyens individuels et concrets, souples et adéquats. Par ses décisions, l'autorité de contrôle ajuste, au cas par cas, « les rapports entre forces contraires, comme l'horloger qui veille avec doigté au mouvement du balancier »[9]. Elle le fait en usant de moyens d'action diversifiés parmi lesquels certains se rapprochent des moyens juridiques classiques – on pense au pouvoir de sanction et au pouvoir d'agir en justice, par exemple. D'autres sont plus souples et davantage fondés sur la concertation – tels que les avis, les recommandations, les conciliations, les rapports[10]. Nous y reviendrons. Signalons également que les solutions dégagées par l'autorité de contrôle sont d'autant mieux adaptées aux traitements de données à caractère personnel que cette autorité est, en principe, composée d'experts indépendants, ce qui est appréciable compte tenu de la technicité de cette matière et des enjeux en ce domaine.

L'intervention de l'autorité de contrôle présente aussi l'avantage de ne pas laisser la régulation des traitements de données aux seules mains de l'État et permet, dans le même temps, de contrôler ce dernier. C'est particulièrement intéressant dans les domaines où des droits fondamentaux sont en jeu et où il convient de veiller à ce que l'autorité étatique les respecte. En matière d'e-gouvernement, par exemple, si le législateur et le Gouvernement décidaient seuls des solutions appliquées en ce domaine, on pourrait craindre que trop d'attention soit accordée à l'efficacité administrative, au détriment de la protection de la vie privée des citoyens. En effet, comme le constataient déjà certains auteurs dans les années septante, ce qui importe, « c'est d'empêcher le mauvais usage de l'ordinateur. Mais qui va définir le bon et le mauvais usage ? Le pouvoir d'État. Et qui est le plus susceptible de faire un mauvais usage ? Le pouvoir d'État »[11]. Cela explique que l'autorité de protection des données doit faire preuve d'une grande indépendance à l'égard de l'État également[12].

---

[7] D. De Roy et R. Queck, « De la téléphonie vocale aux offres publiques d'acquisition. Vers un 'droit de la régulation' ? », *op. cit.*, p. 555.

[8] M.-A. Frison-Roche, « Le droit de la régulation », *op. cit.*, p. 612.

[9] X. Delgrange, L. Detroux et H. Dumont, « La régulation en droit public », in *Elaborer la loi aujourd'hui, mission impossible ?* (B. Jadot et F. Ost dir.), Bruxelles, Publications des Facultés universitaires Saint-Louis, 1999, pp. 71 et 72.

[10] *Ibid.*

[11] J.-L. Missika et J.-P. Faivret, « Informatique et libertés », *Les temps modernes*, 1977, n° 375, p. 314.

[12] Voy. *infra.*

Enfin, l'autorité de contrôle assume aussi un rôle très utile vis-à-vis du citoyen. Elle exerce une mission d'information et de sensibilisation, en éclairant les personnes quant à leurs droits en la matière, la manière de les exercer, les voies de recours existant, etc. En outre, il est établi que l'autorité de contrôle est facilement accessible pour le citoyen, si bien que les autorités de contrôle « se sont révélées être la voie à suivre la plus populaire- et bien souvent la seule voie pertinente- pour les personnes »[13]. Ce constat se comprend aisément. Pour la plupart des citoyens en général, mais également nombre de praticiens du droit en particulier, la protection des données est une matière complexe car technique, touffue et bien souvent abstraite, vu l'intangibilité des éléments que couvrent les notions clés à savoir les données, les bases de données, les traitements de données, etc. C'est également un domaine du droit dans lequel les recours juridiques n'affluent pas, contribuant encore à la marginalisation de la matière. En effet, à l'image des problèmes liés à la protection de l'environnement, une violation des règles de protection des données entraîne bien souvent des conséquences pour un grand nombre de personnes. C'est un ensemble de consommateurs, un ensemble d'usagers de l'administration, un ensemble d'utilisateurs des réseaux sociaux qui ont à subir les désagréments liés aux abus dans l'usage de leurs données. Dès lors, rares sont ceux qui prennent la peine de supporter les importants coûts financiers d'un recours en justice, pour contrer un problème qui les dépasse largement. Dans ce contexte, le rôle de l'autorité de contrôle est donc crucial.

3. De la directive 95/46/CE au RGPD. Lorsque la directive 95/46/CE fut adoptée, tous les États membres de l'Union européenne n'étaient pas dotés d'une autorité de contrôle des traitements de données à caractère personnel. À titre d'exemple, l'Autorité Hellénique de Protection des Données Personnelles n'a a été créée qu'en 1997 tandis qu'il a fallu attendre 2002 pour que la Commission nationale pour la protection des données luxembourgeoise soit instituée[14].

La directive 95/46/CE a imposé aux États membres la création d'une ou plusieurs autorité(s) de contrôle, tout en laissant une large marge de manœuvre aux États s'agissant notamment du statut de ladite autorité, de son mode de fonctionnement, des ressources mises à sa disposition.

---

[13] Agence des droits fondamentaux de l'Union européenne (FRA), *Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE*, 2014, p. 5, accessible ici http://fra.europa.eu/fr/publication/2014/accs-aux-voies-de-recours-en-matire-de-protection-des-donnes-caractre-personnel.

[14] Association francophone des Autorités de protection des données personnelles, « 2007-2017, 10 ans de l'AFAPDP », 2017, accessible ici : http://www.afapdp.org/wp-content/uploads/2017/12/10-ans-dafapdp.pdf.

Comme en témoigne un rapport de l'Agence des droits fondamentaux de l'Union européenne (FRA), cette marge de manœuvre laissée aux États a fait apparaître une disparité parfois importante entre les autorités de contrôle européennes[15]. Par exemple, s'agissant du nombre d'autorités de contrôle à instituer sur le territoire national, la directive laisse aux États la possibilité de créer « une ou plusieurs autorités » de contrôle. C'est pourquoi, en France, l'autorité de contrôle est unique. En Allemagne, elles sont multiples : il existe une autorité de contrôle fédérale, la *Bundesdatenschutzbehörde* et seize autorités de contrôle fédérées, les *Landesdatenschutzbehörde*.

Quant aux pouvoirs de contrôle et de sanction, la directive dresse une liste non exhaustive de ceux-ci[16], citant les pouvoirs d'intervention, pouvoir d'investigation, pouvoir d'ester en justice ou de porter les violations des règles de protection des données à la connaissance de l'autorité judiciaire. Concrètement, des disparités entre États se marquent à ce niveau-là également. On constate ainsi que les responsables de traitement sont sévèrement contrôlés en Allemagne puisque les autorités de contrôle peuvent intervenir sans condition. Tandis qu'en Autriche, l'intervention de la *Österreichische Datenschutzbehörde* est subordonnée à l'existence d'un « soupçon caractérisé » dans le chef du responsable de traitement. En Angleterre, ce contrôle est également plus difficile, puisque l'intervention de l'*Information Commissioner's Office* est subordonnée au respect de plusieurs conditions, parmi lesquelles le fait d'avoir reçu un minimum de quatre plaintes avant de pouvoir intervenir[17]. Quant aux pouvoirs de sanction, ils diffèrent également d'un État à l'autre. C'est, par exemple, en raison de cette marge de manœuvre laissée aux États que le législateur belge n'a pas doté la Commission de la protection de la vie privée du pouvoir d'amende, alors que les autres autorités de contrôle européennes en disposent[18].

---

[15] Agence des droits fondamentaux de l'Union européenne (FRA), *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données. Renforcement de l'architecture des droits fondamentaux au sein de l'UE II*, 2012, accessible ici : http://fra.europa.eu/fr/publication/2012/la-protection-des-donnes-caractre-personnel-dans-lunion-europenne-le-rle-des.

[16] Art. 28.3 directive 95/46/CE.

[17] Pour plus de détails, voy. A. Charles, « Comparaison des pouvoirs de contrôle et de sanction des autorités de contrôle allemandes avec d'autres pays européens », 3 juin 2015, accessible ici http://blogs.u-paris10.fr/content/comparaison-des-pouvoirs-de-contr%C3%B4le-et-de-sanction-des-autorit%C3%A9s-de-contr%C3%B4le-allemandes-ave. Voy. égal. M.-H. Boulanger, « Quelques remarques sur les autorités indépendantes de protection des données dans l'ordre juridique européen », *Laws, norms and freedeoms in Cyberspace/Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet* (E. Degrave, C. de Terwangne, S. Dusollier et R. Queck dir.), coll. CRIDS, Bruxelles, Larcier, 2018, pp. 474 à 476.

[18] Pour de plus amples détails, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* Bruxelles, Larcier, 2014, n^os^ 582 et s.

Le RGPD entend harmoniser cette situation. Le considérant n° 129 affirme ainsi qu' « afin de veiller à faire appliquer le présent règlement et à contrôler son application de manière cohérente dans l'ensemble de l'Union, les autorités de contrôle devraient avoir, dans chaque État membre, les mêmes missions et les mêmes pouvoirs effectifs, y compris les pouvoirs d'enquête, le pouvoir d'adopter des mesures correctrices et d'infliger des sanctions, ainsi que le pouvoir d'autoriser et d'émettre des avis consultatifs (…) et (…) le pouvoir de porter les violations du présent règlement à l'attention des autorités judiciaires et d'ester en justice. Ces pouvoirs devraient également inclure celui d'imposer une limitation temporaire ou définitive au traitement, y compris une interdiction ».

Les missions et pouvoirs de l'autorité de contrôle, repris aux articles 57 et 58 du RGPD, sont énoncés de manière bien plus précise qu'ils ne l'étaient dans la directive, ce qui devrait être de nature à harmoniser l'exercice de ces prérogatives dans les États membres.

Quant au pouvoir d'amende, chaque autorité de contrôle doit désormais en être dotée. Ce sera donc une prérogative toute nouvelle pour l'autorité de contrôle belge. Ce pouvoir de sanction est défini et organisé à l'article 83 du RGPD, qui affirme notamment que les amendes administratives doivent être « dans chaque cas, effectives, proportionnées et dissuasives ». Une liste de critères permettant d'en déterminer la nécessité et le montant est proposée. Ces critères ont récemment fait l'objet de lignes directrices du Groupe de l'article 29[19], dans le but d'encourager l'uniformisation du montant des amendes infligées au sein des États membres de l'Union européenne.

Enfin, on peut s'attendre à ce que « l'application de ces dispositions [donne] lieu à des recours devant les cours et tribunaux et de là à des questions préjudicielles à la Cour de justice, ce qui devrait également contribuer à augmenter la cohérence de l'application du règlement »[20].

[19] Groupe 29, Guidelines adopted on 3 October 2017 on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253.

[20] M.-H. BOULANGER, « Quelques remarques sur les autorités indépendantes de protection des données dans l'ordre juridique européen », *op. cit.*, p. 484.

CHAPITRE 2. Une indépendance affinée

4. L'interprétation de la Cour de justice de l'Union européenne. Une autorité de contrôle forte doit être indépendante des responsables de traitement qu'elle contrôle, qu'ils soient publics ou privés.

C'est ce qu'a rappelé la Cour de justice de l'Union européenne dans trois arrêts qui interprètent l'exigence d'indépendance des autorités de contrôle et dont le RGPD s'est nourri pour circonscrire cette notion cardinale du régime juridique de la protection des données. Le premier arrêt, rendu en 2010, concerne les autorités de protection des données instituées dans les *Länder* allemands[21] tandis que le second, rendu en 2012, vise l'autorité de protection des données autrichienne[22]. Le troisième arrêt s'applique à l'autorité de protection des données hongroise et a été rendu en 2014[23].

5. La raison d'être de l'indépendance. Dans ses deux premiers arrêts, la Cour de justice de l'Union européenne se livre à une interprétation téléologique de la directive 95/46/CE et dégage la raison d'être de l'exigence d'indépendance. Ainsi, selon la Cour, l'indépendance de l'autorité de protection des données est imposée afin de permettre à cette dernière d'effectuer un examen objectif et impartial de l'équilibre à atteindre entre la circulation des données à caractère personnel et la protection de la vie privée des personnes concernées.

Dans son premier arrêt, confirmé par le second arrêt, la Cour rappelle que l'objectif poursuivi par la directive européenne est d'assurer la libre circulation des données entre les États membres. Puisque ces échanges d'informations peuvent heurter la vie privée des citoyens concernés, les autorités de contrôle doivent être des « gardiennes [des] droits et libertés

---

[21] C.J.U.E. (GC), 9 novembre 2010, arrêt *République fédérale d'Allemagne c. Commission,* C-518/07. Pour un commentaire de cet arrêt, voy. M. Aubert, E. Broussy et F. Donnat, « Chronique de jurisprudence communautaire », *AJDA,* 2010, pp. 938 et 939 ; H.R. Kranenborg, « Commentaar », *SEW,* 2010, pp. 421 à 423 ; E. Debaets, « Les autorités administratives indépendantes et le principe démocratique : recherches sur le concept d' 'indépendance' », *Rapport présenté au VIIIème Congrès mondial de l'association internationale de droit constitutionnel,* Mexico, 6-10 décembre 2010 disponible sur le site www.juridicas.unam.mx/wccl/ponencias/14/254.pdf ; European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* 7 mai 2010, p. 19, disponible sur le site www.fra.europa.eu ; O. De Schutter, « Les droits fondamentaux dans l'Union européenne », *J.D.E.*, 2011, pp. 113 et 114.

[22] C.J.U.E. (GC), 16 octobre 2012, arrêt *République d'Autriche c. Commission,* C-614/10.

[23] C.J.U.E. (GC), 8 avril 2014, arrêt *Commission c. Hongrie,* C-288/12.

fondamentaux »[24]. Leur tâche revient à « assurer un juste équilibre entre, d'une part, le respect du droit fondamental à la vie privée et, d'autre part, les intérêts qui commandent une libre circulation des données à caractère personnel »[25]. Partant de là, l'indépendance des autorités de contrôle s'entend des garanties permettant à ces institutions d'examiner cet équilibre « de manière objective et impartiale »[26].

6. L'étendue de l'indépendance. Qui pourrait exercer sur l'autorité de contrôle une pression telle que l'examen précité ne pourrait être effectué de manière objective et impartiale ? En d'autres termes, de quelle sphère d'influence cherche-t-on à protéger l'autorité de contrôle en manifestant un tel souci d'indépendance ?

Les traitements de données étant effectués au sein du secteur privé et du secteur public, cette autorité contrôle un grand nombre d'organismes et doit faire preuve d'objectivité et d'impartialité tant à l'égard des sociétés privées que de l'administration. Dès lors, il y a lieu de lui assurer une indépendance particulièrement ample.

La Cour de justice de l'Union européenne abonde en ce sens. Elle prône une interprétation large de l'exigence d'indépendance. La Cour soutient qu'étant donné que la directive 95/46/CE prescrit à l'autorité de protection des données d'agir en « toute » indépendance, cela signifie qu'elle doit « jouir d'une indépendance qui [lui] permette d'exercer [ses] missions sans influence extérieure ». Cela exclut « non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte, qui pourraient remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel »[27].

Partant de là, elle juge que les autorités de protection des données allemandes ne sont pas indépendantes, étant donné qu'elles sont soumises à un contrôle de tutelle de l'État[28].

---

[24] C.J.U.E. (GC), 9 novembre 2010, arrêt *Commission c. République fédérale d'Allemagne,* C-518/07, § 23.

[25] *Ibid.*, § 24.

[26] *Ibid.*, § 25. Dans le même sens, C.J.U.E. (GC), 16 octobre 2012, arrêt *République d'Autriche c. Commission,* C-614/10, §§ 40 et 41.

[27] C.J.U.E. (GC), 9 novembre 2010, précité, § 30 ; C.J.U.E. (GC), 16 octobre 2012, arrêt *République d'Autriche c. Commission,* C-614/10, § 41.

[28] C.J.U.E. (GC), 9 novembre 2010, précité, § 58.

L'autorité de protection des données autrichienne (la « DSK »[29]) ne respecte pas non plus cette exigence d'indépendance et ce, pour trois raisons. Tout d'abord, le membre administrateur de la DSK, qui est un des six membres qui composent cette autorité et en gère les affaires courantes, est un fonctionnaire fédéral assujetti à un contrôle de tutelle. Ensuite, le bureau de la DSK est intégré aux services de la chancellerie fédérale, ce qui signifie que le personnel mis à la disposition de la DSK est composé de fonctionnaires de la chancellerie fédérale. Enfin, le chancelier fédéral a le droit inconditionnel d'être informé au sujet de tous les aspects de la gestion de la DSK[30].

La Cour estime également que la Hongrie méconnaît l'exigence d'indépendance en mettant fin de manière anticipée, à l'occasion d'une modification législative, au mandat du président de l'autorité de contrôle. Et d'affirmer que « s'il était loisible à chaque État membre de mettre fin au mandat d'une autorité de contrôle avant le terme initialement prévu de celui-ci sans respecter les règles et les garanties préétablies à cette fin par la législation applicable, la menace d'une telle cessation anticipée qui planerait alors sur cette autorité tout au long de l'exercice de son mandat pourrait conduire à une forme d'obéissance de celle-ci au pouvoir politique, incompatible avec ladite exigence d'indépendance »[31].

7. Les conditions de l'indépendance. Avant l'adoption du RGPD, le Rapport explicatif sur le protocole additionnel à la Convention 108[32] énumérait déjà un certain nombre d'éléments susceptibles de contribuer à l'indépendance de l'autorité de contrôle, à savoir la composition de l'autorité, le mode de désignation de ses membres, la durée d'exercice et les conditions de cessation de leurs fonctions, l'octroi à l'autorité de ressources suffisantes ou l'adoption de décisions à l'abri d'ordres ou d'injonctions extérieurs à l'autorité.

Des critères semblables sont repris et précisés par le RGPD, aux articles 52 et 53. Ils ont trait tantôt à l'indépendance des membres, tantôt à l'indépendance de l'institution.

8. L'indépendance des membres. L'indépendance de l'autorité de protection des données suppose avant tout l'indépendance de ses membres.

L'article 52.2. du RGPD ne dit pas autre chose lorsqu'il affirme que « le ou les membres de chaque autorité de contrôle demeurent libres de toute

[29] DSK est l'abréviation de *Datenschutzkommission.*
[30] C.J.U.E. (GC), 16 octobre 2012, arrêt *République d'Autriche c. Commission*, précité, § 66.
[31] C.J.U.E. (GC), 8 avril 2014, arrêt *Commission c. Hongrie,* précité., § 54.
[32] Rapport explicatif sur le protocole additionnel à la Convention 108, § 17.

influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque »[33] et qu'ils « s'abstiennent de tout acte incompatible avec leurs fonctions (…) »[34]. À cet égard, rappelons que, pour la Cour de justice de l'Union européenne, le fait que le membre administrateur de l'autorité de protection des données autrichienne soit un fonctionnaire fédéral et que le personnel mis à la disposition de cette autorité soit composé de fonctionnaires est contraire à l'exigence d'indépendance prescrite par la directive 95/46/CE.

En outre, l'article 53 du RGPD précise les conditions applicables aux membres de l'autorité de contrôle, s'agissant de leur mode de désignation[35], des compétences requises[36], de la durée de leur mandat[37] et des conditions de cessation de leurs fonctions[38].

En particulier, le mode de désignation des membres de l'autorité de contrôle est un aspect délicat de l'exigence d'indépendance. L'article 53.1. du RGPD dispose que « les États membres prévoient que chacun des membres de leurs autorités de contrôle est nommé selon une procédure transparence par leur parlement ; leur gouvernement ; leur chef d'État ; ou un organisme indépendant chargé de procéder à la nomination en vertu du droit de l'État membre ». Les États membres peuvent donc décider que les membres de l'autorité de contrôle sont désignés par le gouvernement.

Ce mode de désignation nous semble problématique, car il risque d'encourager l'influence du gouvernement sur la composition de l'autorité de contrôle, alors même que celle-ci doit être en mesure de contrôler ce gouvernement et les administrations sur lesquelles les ministres exercent leur contrôle de tutelle. En d'autres termes, l'autorité de contrôle pourrait être politisée. Il y a beaucoup de risques que ses membres émanent des administrations et/ou des cabinets ministériels, favorisant alors le phénomène du « contrôleur contrôlé » lorsqu'il s'agit, par exemple, de contrôler une administration sous la tutelle d'un ministre ou de contrôler des entreprises qui « lobbyent » auprès du gouvernement. Un rapport de l'Agence européenne pour les droits fondamentaux confirme d'ailleurs ces craintes, arguant du fait que l'indépendance des membres de l'autorité de protection des données est source de préoccupation dans beaucoup d'États européens compte tenu du risque d'influence du gouvernement

[33] Art. 52.2 du RGPD.
[34] Art. 52.3. du RGPD.
[35] Art. 53.1 du RGPD.
[36] Art. 53.2 du RGPD.
[37] Art. 53.4. du RGPD.
[38] Art. 53.4. du RGPD.

sur ces derniers[39]. Elle évoque en particulier les difficultés liées à la nomination des membres par le Gouvernement – comme en Irlande ou au Luxembourg – ou au rattachement de ladite autorité au ministère de la Justice – comme au Danemark ou en Lettonie et comme c'était le cas en Belgique avant une réforme intervenue en 2003[40].

À notre sens, il faut donc éviter que le gouvernement nomme les membres de l'autorité de contrôle, et même, qu'il soit d'une manière ou d'une autre impliqué dans ce processus. L'idée est d'empêcher, autant que faire se peut, une influence directe ou indirecte du gouvernement sur l'autorité de contrôle.

À cet égard, l'exemple de l'autorité de contrôle belge est éloquent. Jusqu'à présent, les membres de la Commission de la protection de la vie privée sont nommés par le Parlement, mais au départ d'une liste dressée par le Conseil des Ministres.

Le manque d'indépendance de la Commission de la protection de la vie privée a été récemment dénoncé, en pratique, par certains membres cette autorité, dont le président lui-même. Ce dernier est un ancien chef de cabinet. Il ne cache pas que sa nomination, « c'est du politique pur »[41] et admet qu'une des conditions pour devenir membre de la Commission, est « d'avoir un circuit politique »[42].

À l'occasion de l'entrée en application du RGPD, la Commission de la protection de la vie privée a été substantiellement réformée et rebaptisée « Autorité de protection des données » (APD). Dans un premier temps, le projet de loi organisant cette réforme affirmait que les membres de cette autorité seraient nommés par la Chambre des représentants, certes, mais « sur proposition des ministres qui ont délibéré en Conseil ».

Dans son avis n° 21/2017[43], la Commission de la protection de la vie privée a affirmé qu'il « n'est pas logique que le Conseil des ministres soumette une liste restreinte de candidats dans laquelle la Chambre peut faire son choix, étant donné que cela limiterait sérieusement le choix de la Chambre. Cette critique s'applique également à l'article 38 qui dispose

---

[39] European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* 7 mai 2010, p. 19, disponible sur le site www.fra.europa.eu.

[40] European Union Agency for fundamental rights, *Data protection in the European Union : the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* précité, pp. 19-20.

[41] Le Soir, « Avis de tempête annoncé sur la Commission vie privée », 3 mars 2017, http://plus.lesoir.be/84403/article/2017-03-03/avis-de-tempete-annonce-sur-la-commission-vie-privee.

[42] *Ibid.*

[43] CPVP, *Avis n° 21/2017 du 3 mai 2017, relatif au projet de loi réformant la Commission de la protection de la vie privée,* p. 16, n^{os} 64 et 65.

que les listes pour chaque mandat à pourvoir comprennent trois candidats maximum, ce qui n'exclut pas le fait qu'un seul candidat soit proposé ».

Un aspect qui pose également problème est l'absence de transparence de la procédure de nomination des membres de l'APD (qui va de pair avec l'exigence d'indépendance)[44].

Lors des débats parlementaires relatifs à ce projet de loi[45], il est apparu qu'une solution serait que les membres de l'APD, ou au moins une partie de ceux-ci, soient élus sans être présentés par le Conseil des ministres. Les candidats à un poste de membre de l'APD se présenteraient devant le Parlement afin d'y exposer les raisons de leur motivation. S'en suivrait un débat public avant la désignation du meilleur candidat élu par les parlementaires[46].

Par ailleurs, il a été avancé que les membres devraient être élus par un vote à majorité spéciale, et non simple, à la Chambre[47]. Ce faisant, les candidats devraient convaincre un plus grand nombre de parlementaires, ce qui renforcerait la voix de l'opposition dans le débat et, dans le même temps, transcenderait la division de la Chambre en groupes linguistiques. Cette idée s'inscrit dans la lignée de la section de législation du Conseil d'État qui a affirmé qu' « il serait souhaitable, en raison des missions confiées à [l'autorité de protection des données], que l'opposition parlementaire soit associée au processus de désignation des membres de la Commission »[48].

Il va de soi qu'à cette indépendance forte doit correspondre une responsabilité forte. Il ne pourrait être question de créer un « électron libre » en dehors de toute prise démocratique. Ainsi, il importe que l'autorité de protection des données soit transparente et rende des comptes régulièrement au Parlement. Divers moyens pourraient être mis en place à cette

---

[44] *Ibid.*

[45] Projet de loi portant création de l'Autorité de protection des données, *Doc. parl.,* Ch. repr., sess. 2017-2018, n° 54-2648/006, pp. 9 et s.

[46] E. Degrave, Carte blanche « Pour une autorité de protection des données forte et efficace », *Le Soir,* 16 octobre 2017 http://plus.lesoir.be/119148/article/2017-10-16/pour-une-autorite-de-protection-des-donnees-forte-et-efficace ; Débat à la RTBF-radio (Soir première) « Faut-il muscler la protection des données », entre E. Degrave et P. De Backer, le 17 octobre 2017.

[47] Projet de loi portant création de l'Autorité de protection des données, *op. cit.*, p. 50.

[48] SLCE, *Avis du 28 novembre 1990 sur un projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Doc. parl.*, Ch. repr., sess.1990-1991, n° 1610/1, p. 61. La SLCE s'est prononcée à nouveau en ce sens quelques années plus tard. Voy. SLCE, *Avis du 2 février 1998 sur un avant-projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Doc. parl.,* Ch. repr., sess. 1997-1998, n° 1566/1, p. 240.

fin tels que la publication d'un rapport annuel détaillé, la publication de l'ensemble des avis, recommandations, décisions, études émanant de l'Autorité de contrôle. Il serait également judicieux de mettre en place une commission parlementaire qui suivrait le travail de l'Autorité de protection des données de près et à intervalles réguliers et pourrait notamment interpeller les membres du comité de direction sur les dossiers que la commission juge pertinents au regard des enjeux sociétaux qu'ils soulèvent.

Depuis lors, le texte du projet de loi a été modifié sur ce point. La majorité parlementaire a retiré du projet de loi la condition selon laquelle les membres de l'APD devaient être proposés par le Conseil des ministres qui ont délibéré en Conseil. La procédure d'élection des membres de l'APD se fera donc exclusivement devant le Parlement associant majorité et opposition au processus d'élection[49]. Malheureusement, le vote ne se fera pas à majorité spéciale si bien que, concrètement, l'influence des partis politiques sur les choix effectués risque de perdurer.

9. L'indépendance institutionnelle. L'indépendance institutionnelle de l'autorité de protection des données suppose l'octroi de ressources financières et matérielles suffisantes. Elle suppose également que l'autorité de protection des données ne soit pas soumise à des ordres ou des injonctions venant de l'extérieur. En ce sens, rappelons[50] que la Cour de justice de l'Union européenne estime que la mise en place d'un contrôle de tutelle de l'État sur l'autorité de protection des données est contraire à l'exigence d'indépendance. Tel est le cas également, selon la Cour, si un ministre dispose d'un droit inconditionnel d'information qui s'exerce sur tous les aspects de la gestion de l'autorité de protection des données.

L'article 52 du RGPD précise également l'exigence d'indépendance institutionnelle et prévoit que « chaque État membre veille à ce que l'autorité de contrôle dispose des ressources humaines, techniques et financières, ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité [européen de la protection des données] »[51]. De plus, « chaque État membre veille à ce que chaque autorité de contrôle choisisse et dispose de ses propres agents, qui sont placés sous les ordres exclusifs du ou des membres de l'autorité de contrôle concernées »[52]. Enfin, « chaque État membre veille à ce que chaque

[49] Art. 36 et s. de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

[50] Voy. *supra*.

[51] Art. 52.4. du RGPD.

[52] Art. 52.5. du RGPD.

autorité de contrôle soit soumise à un contrôle financier qui ne menace pas son indépendance et qu'elle dispose d'un budget annuel public propre, qui peut faire partie du budget global national ou d'une entité fédérée »[53].

CHAPITRE 3. Des pouvoirs renforcés

10. Rôle préventif et répressif. La directive 95/46/CE donnait à l'autorité de contrôle un rôle préventif et un rôle répressif. Le rôle préventif de l'autorité de contrôle se manifestait notamment au travers de l'obligation du responsable de traitement de notifier les traitements de données à l'autorité de contrôle préalablement à leur mise en œuvre[54], du contrôle préalable des traitements susceptibles d'engendrer des risques particuliers[55] ou encore de la publicité des traitements via un registre public[56]. Le rôle répressif s'ancrait dans les pouvoirs d'investigation – tels que le pouvoir d'accéder aux données faisant l'objet d'un contrôle –, les pouvoirs effectifs d'intervention – tels que l'interdiction temporaire ou définitive d'un traitement, l'effacement ou la destruction de données – et le pouvoir d'ester en justice[57].

Les États membres avaient néanmoins une large marge de manœuvre pour organiser de tels pouvoirs, et à cette occasion, mettre l'accent sur un rôle plutôt qu'un autre, concevoir l'autorité de contrôle davantage comme une autorité de médiation ou, au contraire, comme une autorité répressive. Une large disparité est apparue entre États membres là aussi.

Il résulte d'une étude comparative réalisée par l'Agence des droits fondamentaux de l'Union européenne (FRA) qu' « alors que plusieurs pays (par exemple, la Finlande, la Suède, l'Irlande et le Royaume-Uni) ont souligné le rôle préventif et proactif des agences de contrôle, mettant en exergue leur rôle *ex-ante* pour garantir la protection des données à caractère personnel, d'autres États membres (tels que la Lettonie, la République tchèque et la Grèce) ont donné la priorité aux fonctions d'application et de contrôle *a posteriori* des autorités de protection des données et leur ont confié une mission réactive afin de veiller au respect de la législation relative à la protection des données ». Et d'ajouter que « certaines autorités nationales ne disposent de ce fait que d'instruments très limités pour

[53] Art. 52.6. du RGPD.
[54] Art. 18 directive 95/46/CE.
[55] Art. 20 directive 95/46/CE.
[56] Art. 21 directive 95/46/CE.
[57] Art. 28 directive 95/46/CE.

remplir leur mission de contrôle. Il s'agit donc d'un problème qui doit être traité dans les pays concernés »[58].

Outre cette disparité entre États membres, les mesures préventives de contrôle sont progressivement apparues comme des formalités administratives ennuyeuses, fastidieuses et dénuées de sens. L'obligation de notification préalable des traitements et leur enregistrement dans le registre public évoqués précédemment sont parlants à cet égard.

Initialement, la notification et le registre public poursuivent plusieurs objectifs.

Pour le citoyen, ce doit être un moyen d'être informé des traitements existants, d'interroger éventuellement le responsable de traitement pour obtenir davantage de renseignements et réagir si des abus sont constatés. De manière plus générale, cela « devrait aussi permettre au public (via le contrôle de la presse par exemple) d'avoir une vue d'ensemble des utilisations de données à caractère personnel »[59].

Pour le responsable de traitement, c'est l'occasion de vérifier le respect des conditions légales en la matière[60].

Enfin, pour l'autorité de contrôle, la déclaration de traitement est une source d'informations par rapport aux traitements existants. Elle peut ainsi exercer ses missions de contrôle et apprécier la suite à donner aux plaintes éventuelles qui lui sont adressées[61].

Néanmoins, en pratique, force est de constater que ces objectifs ne sont pas atteints. Les consultations du registre public sont très rares, les traitements ne sont pas tous déclarés par les responsables de traitements et bien souvent, les autorités de contrôle ne sont matériellement pas en mesure de vérifier le contenu de chaque notification et d'exécuter les poursuites nécessaires en cas d'abus[62].

---

[58] European Union Agency for Fundamental Rights, *La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données. Renforcement de l'architecture des droits fondamentaux au sein de l'UE II*, 2012, p. 22 accessible ici : http://fra.europa.eu/fr/publication/2012/la-protection-des-donnes-caractre-personnel-dans-lunion-europenne-le-rle-des.

[59] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 1990-1990, n° 10610/1, p. 22.

[60] Groupe 29, Rapport du groupe de travail « Article 29 » sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne, *op. cit.*, p. 6.

[61] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Exposé des motifs, précité, n° 1610/1, p. 22.

[62] Pour de plus amples détails, voy. V. Verbruggen, « Mise en œuvre du Règlement général sur la protection des données : coup de projecteur sur certaines nouvelles obligations

11. Un rôle répressif renforcé par le RGPD. Partant de ces constats, le RGPD allège le rôle préventif de l'autorité de contrôle et supprime un certain nombre de formalités préalables aux traitements. Par exemple, l'obligation de notification préalable des traitements est abolie et remplacée par l'obligation, pour chaque responsable de traitement et chaque sous-traitant, de tenir un registre des activités de traitement qui ont lieu sous leur responsabilité[63].

En outre, le RGPD renforce le rôle répressif de l'autorité de contrôle et le contrôle *a posteriori* des traitements de données en dotant l'autorité de contrôle de trois types de pouvoirs[64]. Pouvoir d'enquête – comme celui de mener des audits sur la protection des données-, pouvoir d'adopter des mesures correctrices– tel que le pouvoir d'amende- ainsi que des pouvoirs d'autorisation et d'avis- tel que le pouvoir de rendre un avis au parlement national[65]. C'est pour cette raison, par exemple, que l'autorité de contrôle belge sera dorénavant dotée du pouvoir d'amende évoqué plus haut, ce qui n'était pas le cas jusqu'ici.

12. Un conseiller et un informateur. L'autorité de contrôle n'a cependant pas qu'un rôle répressif. Le RGPD maintient le rôle de l'autorité de contrôle en tant que conseiller des autorités publiques, notamment à l'occasion de la rédaction des législations en la matière.

L'autorité de contrôle est également un informateur, chargé d'éclairer le public sur les règles à respecter en cette matière, ce qui est primordial à l'heure où le déploiement des technologies s'accompagne bien souvent d'une complexité et d'une opacité qui voilent les enjeux démocratiques et rendent difficile le maintien, par le citoyen, d'une prise sur ses données à caractère personnel. Ce rôle d'informateur est d'autant plus important que l'autorité de contrôle est l'autorité la plus proche du citoyen, vers laquelle celui-ci se tournera en premier lieu pour comprendre ses droits et ses obligations dans ce domaine.

Comme nous l'avons affirmé au début de cette analyse, l'autorité de contrôle est donc un relais précieux, tant du législateur et du gouvernement, que du citoyen.

à charge des responsables de traitement et des sous traitants », *Orientations,* 2017, p. 8 ; E. Degrave, « Le Règlement général sur la protection des données et le secteur public », *Rev. dr. commun.*, 2018, pp. 4 à 14.

[63] Art. 30 du RGPD.

[64] Art. 58 du RGPD.

[65] Sur les pouvoirs de l'autorité de contrôle, voy. égal. R. Robert, « Les autorités de contrôle dans le nouveau règlement européen sur la protection des données : statut, coopération et gouvernance européenne », in *Vers un droit européen de la protection des données* (B. Docquir dir.), Bruxelles, Larcier, coll. UB3, 2017, pp. 28 et s.

13. La répartition des compétences et la coopération entre autorités de contrôle. Chaque autorité de contrôle exerce ses compétences sur le territoire de l'État membre dont elle relève[66].

Plusieurs autorités de contrôle peuvent être compétentes en cas de traitement « transfrontalier », c'est-à-dire celui « qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ou [celui] qui (…) affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres »[67]. Dans ce cas, une autorité de contrôle « chef de file » doit être désignée parmi les autorités de contrôle compétentes. C'est l'autorité de contrôle de l'« établissement principal » du responsable du traitement ou du sous-traitant qui assume ce rôle. Elle doit être identifiée selon les critères alternatifs proposés à l'article 4, 16) du RGPD. Une fois désignée, l'autorité « chef de file » coopère avec les autres autorités de contrôle impliquées dans le dossier, selon les modalités fixées à l'article 60 du RGPD. L'objectif qui sous-tend cette manière de fonctionner est « certainement de favoriser une cohérence dans les actions des autorités de contrôle mais également pour les responsables du traitement actifs dans plusieurs États membres d'avoir une autorité de contrôle comme interlocuteur, et non plusieurs (*one-stop shop*) »[68].

Signalons, enfin, que, dans le souci d'harmoniser les règles sur le territoire européen, le RGPD facilite la coopération entre les autorités de contrôle européennes, et l'assistance mutuelle dans l'échange d'informations, et la mise en œuvre du RGPD[69]. Le chapitre VII du RGPD est entièrement consacré à cet aspect du travail des autorités de contrôle.

Par ailleurs, le Groupe de l'article 29 est remplacé par le Comité européen de la protection des données[70]. Celui-ci est compétent pour rendre des avis, afin de contribuer à l'application cohérente du RGPD au travers des États membres, comme le faisait le Groupe de l'article 29. Mais ce comité est désormais compétent également pour rendre des décisions contraignantes dans les cas visés à l'article 65 du RGPD, par « lorsqu'il

[66] Art. 55 du RGPD. À ce sujet, voy. R. Robert, « Les autorités de contrôle dans le nouveau règlement européen sur la protection des données : statut, coopération et gouvernance européenne », *op. cit.*, pp. 32 et s.

[67] Art. 4, 23, du RGPD.

[68] C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de forces du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, n° 97.

[69] Art. 60 et 31 du RGPD.

[70] Art. 64 et s. du RGPD.

existe des points de vue divergents quant à l'autorité de contrôle concernée qui est compétente pour l'établissement principale »[71].

Conclusion

14. Le RGPD rappelle ce que la directive 95/46/CE affirmait déjà sans détour : l'autorité de contrôle est un élément essentiel de la protection des données. En effet, par son indépendance, son expertise et ses prérogatives singulières, l'autorité de contrôle joue un rôle crucial pour le respect du régime juridique de la protection des données.

Elle est un relais pour le législateur et le gouvernement. Elle use de moyens concrets et souples pour réguler les traitements de données mis en œuvre dans le secteur public et dans le secteur privé, et offre des réponses adaptées aux questions soulevées dans ce domaine, qui sont bien souvent complexes et nécessitant une réaction rapide.

Elle est également un relais pour le citoyen, qui se sent dépassé par ces questions aux apparences abstraites et intangibles. L'autorité de contrôle est alors perçue comme la voie de recours la plus accessible et la plus efficace.

Jusqu'à présent, la marge de manœuvre que laissait la directive 95/46/CE aux législateurs nationaux a entraîné une disparité dans l'organisation et le fonctionnement des autorités de contrôle de l'Union européenne. C'est pourquoi, le RGPD encourage l'uniformisation des autorités de contrôle au travers des États membres.

Ainsi, à la suite des arrêts de la C.J.U.E. consacrés à l'indépendance des autorités de contrôle, le RGPD précise les exigences qui conditionnent le respect de cet impératif. Un point délicat est celui du mode de désignation des membres de l'autorité de contrôle dès lors que le RGPD autorise la désignation de ceux-ci par le gouvernement.

Par ailleurs, le RGPD accentue le rôle répressif de l'autorité de contrôle, et allège les formalités administratives qui répondaient au rôle préventif de cette dernière. Ce constat sera prégnant en Belgique, puisque d'une autorité essentiellement de conseil, l'on passera à une autorité de contrôle dotée de moyens effectifs de sanction, dont le pouvoir d'amende.

---

[71] Pour de plus amples détails sur le Comité européen de la protection des données, voy. M.-H. BOULANGER, « Quelques remarques sur les autorités indépendantes de protection des données dans l'ordre juridique européen », *op. cit.*, pp. 486 et s.

Cette évolution pose toutefois la question de la manière dont l'Europe se saisit de la réglementation et de la régulation des traitements de données à caractère personnel. L'entrée en application du RGPD fait grand bruit, affole le secteur privé, bouscule le secteur public. Or, le RGPD n'est pas révolutionnaire dans les exigences qu'il impose aux responsables de traitement. Il constitue plutôt une piqure de rappel de droits et obligations dont beaucoup figuraient déjà dans la directive 95/46/CE mais dont certains n'étaient pas ou peu appliquées.

Jusqu'ici, en pratique, ces règles étaient peu connues, peu comprises, peu appliquées, peu revendiquées, peu dénoncées. En d'autres termes, un problème d'effectivité pèse depuis longtemps sur ces règles dont le grand public ne comprend pas toujours le sens et dont il peine alors à faire valoir le respect. Pourquoi ?

Une inquiétude surgit alors. En quoi le RGPD pourrait-il, à lui seul, changer ce constat ? Si la directive 95/46/CE manquait d'effectivité, pourquoi en serait-il autrement du RGPD ? Certes, le pouvoir d'amende fait peur et amène l'autorité de contrôle à devenir progressivement un « super flic » sanctionnateur, ce qui peut amener à une application plus effective des règles.

Mais, au-delà de ce travail *a posteriori,* nous formons le vœu que l'autorité de contrôle puisse aussi développer son rôle d'« organe de la conscience sociale » et encourager le déploiement d'une véritable culture de la protection des données, faite de réflexions lucides en amont, d'habitudes et de réflexes constructifs au quotidien. Actuellement, ce sont principalement les technologies qui dictent le rythme, tandis que la loi tente de suivre comme elle peut. À cet égard, la société civile a besoin d'une autorité composée d'experts qui l'aide à décider de sa destinée dans l'univers numérique. La société civile a également besoin d'une autorité portée par des personnalités fortes, qui affirment de manière visible un discours lucide et indépendant, visant à accompagner les citoyens confrontés à des technologies dont les enjeux leur échappent. Une autorité, qui, enfin, aide les citoyens, les avocats, les institutions privées et publiques à comprendre pleinement le sens de ces règles et la manière de les appliquer, notamment en créant des outils, simples et concrets, pour faire respecter ces droits en pratique avec la rapidité et l'efficacité que ce respect mérite.

***