Revue à l'attention des délégués à la protection des données et des conseils en sécurité

DPO news
DROIT, TECHNOLOGIE ET MANAGEMENT

P924317
BUREAU DE DÉPÔT
1435 Mont-Saint-Guibert Masspost

Bimestriel • Mars 2020 • n° 7

www.dponews.info

Retrouvez nous sur LinkedIn DPO news

Édito

Le RGPD et les autorités publiques : entre contrainte et effectivité

Dire que les autorités publiques sont soumises aux dispositions du Règlement général relatif à la protection des données (ci-après, RGPD), lorsqu'elles traitent des données à caractère personnel, peut sembler, pour nombre de lecteurs, être un euphémisme.

Pour cause, non seulement les autorités publiques tombent sous le champ d'application *ratione personae* du RGPD, mais en outre, un certain nombre de règles sont plus contraignantes quand elles viennent à s'appliquer à ces dernières.

À titre d'exemple, les autorités publiques doivent nommer un délégué à la protection des données.

Pour autant, le règlement n'est pas facilement appréhendable par les autorités publiques, d'autant qu'il s'immisce dans de nombreuses matières et touche de nombreuses données telles que les données à caractère fiscal, les données issues du registre national ou de la Banque-carrefour de la sécurité sociale, ou encore les données relatives au personnel employé.

La mise en conformité avec le RGPD nécessite donc de mettre en musique les principes généraux, les obligations et droits découlant du règlement avec ceux propres aux missions de l'administration.

En outre, à l'heure de l'informatisation des services publics, le RGPD amène de nombreuses nouveautés visant à protéger davantage les données à caractère personnel dans un monde ultra numérisé et ultra connecté, avec une attention particulière à la sécurité et à l'intégrité des données et du système d'information.

Le RGPD vient profondément impacter la relation entre l'administration et ses usagers, ses travailleurs, ses soumissionnaires et adjudicataires.

C'est pourquoi une question mérite d'être abordée en préambule à ce numéro dédié aux autorités publiques. Il s'agit de celle de l'effectivité des dispositions du règlement à l'égard de ces autorités en l'absence de sanction administrative financière dans leur chef.

Pourtant, dans son considérant 148, le législateur européen énonce qu'« Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, » Ceci témoigne de la lucidité de l'auteur du texte, qui cependant offre aux États membres le choix de déterminer si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et les organismes publics établis sur son territoire (art. 83, § 7).

Dès lors, tout bon praticien devra se montrer attentif aux options prises dans chaque État membre, le règlement n'étant pas arrivé à une harmonisation sur ce point. Pour l'accompagner, ce numéro du *DPO News* ne manquera pas de lui offrir les outils nécessaires à une meilleure compréhension de ces obligations qui pèsent sur les autorités publiques, mais qui le concernent, au même titre que tous les acteurs soumis au Règlement. C'est aussi l'occasion d'informer ceux qui collaborent avec ou côtoient les autorités publiques qu'ils agissent en qualité de sous-traitants, de responsables de traitement ou encore de personnes concernées.

Saba Parsa
Avocate au cabinet Alta Law
DPO du barreau de Bruxelles et d'AVOCATS.BE

ANTHEMIS

Notion d'autorité publique au sens de la réglementation relative aux données à caractère personnel

L'importance de l'enjeu que constitue la gouvernance des données par le secteur public n'est, depuis quelques années déjà, plus un mystère. Les législateurs semblent courir après un objectif sisyphéen. Pour nos États, il s'agit de déterminer un régime de protection des droits des personnes relatifs aux données qui soit adéquat à l'exercice des libertés individuelles, le tout dans une ambiance silencieuse de « coup *data* »[1] dont on ne sait s'il n'a pas déjà eu lieu.

À travers le RGPD, le législateur européen a repris le concept d'*autorité publique*, non sans paradoxe. En effet, alors que cette catégorie d'acteur est visée comme responsable de traitement – voy. l'article 4, 7°, du RGPD – et que le terme se retrouve pas moins de trente-sept fois dans le texte, le concept ne se trouve pas défini dans celui-ci, les législateurs nationaux restant maîtres de prendre les choses en main.

En droit interne, le choix a été effectué dans le cadre de la préparation de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui précise et clarifie les dispositions belges là où le RGPD le lui permettait. Son article 5 indique ce qu'il y a lieu d'entendre par autorité publique :

> « Pour l'application de la présente loi, on entend par "autorité publique" :
>
> 1° l'État fédéral, les entités fédérées et les autorités locales ;
>
> 2° les personnes morales de droit public qui dépendent de l'État fédéral, des entités fédérées ou des autorités locales ;
>
> 3° les personnes, quelles que soient leur forme et leur nature qui :
>
> – ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial ; et
>
> – sont dotées de la personnalité juridique ; et
>
> – dont soit l'activité est financée majoritairement par les autorités publiques ou organismes mentionnés au 1° ou 2°, soit la gestion est soumise à un contrôle de ces autorités ou organismes, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes ;
>
> 4° les associations formées par une ou plusieurs autorités publiques visées au 1°, 2° ou 3°. »

L'option choisie a été préférée à celle, préconisée par la défunte Commission vie privée – aujourd'hui Autorité de protection des données, ou APD[2] – de restreindre le champ d'application à l'État fédéral. Comme le proposait le Conseil d'État[3], élargir la définition « aux entités fédérées et aux autorités locales » permet de combler une éventuelle lacune de la loi pour les dispositions relatives aux sanctions, par exemple. D'aucuns pointeront sans doute que le choix posé par le législateur est en réalité bien plus large, et pour cause. Alors qu'elle est présentée comme résultant d'une copie de ce qui est prévu par la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public[4], la définition colle comme un gant à celle de *pouvoir adjudicateur* au sens de la loi du 17 juin 2016 relative aux marchés publics !

L'impact d'une telle qualification n'est pas que cosmétique. En effet, on pointera notamment que les autorités publiques, en matière de traitement des données

- *premièrement*, ne peuvent fonder le traitement de données sur l'*intérêt légitime*, au sens de l'article 6 du RGPD, en raison de la mission dévolue au législateur de prévoir par la loi les bases juridiques d'un traitement par ces autorités[5] ;
- *deuxièmement*, sont tenues à la *désignation d'un DPO*, quelles que soient leur taille ou leurs missions[6] ;
- *troisièmement*, ne peuvent se voir infliger des *sanctions administratives*, sauf si elles offrent des biens ou services sur un marché[7].

Ces trois caractéristiques, à elles seules, suffisent à introduire un régime différencié, et l'APD en est bien consciente. La Fédération des Entreprises de Belgique a d'ailleurs introduit un recours en annulation contre l'article 221, § 2 de la loi du 30 juillet 2018 devant la Cour constitutionnelle, alléguant de la discrimination faite entre le secteur privé et le secteur public dès lors que les sanctions administratives ne s'appliquent pas à ce dernier ; ce recours, plus d'un an après son introduction, est toujours pendant.

Les autorités publiques sont au cœur des priorités stratégiques pour la période 2020-2025, révélées dans le courant du mois de janvier 2020. Gageons que la stratégie et les objectifs soient revus périodiquement, non seulement à l'aune des avancées du droit, mais aussi de la technologie, pour que l'APD apparaisse comme un véritable partenaire pour les autorités publiques dans la gouvernance des données qu'elles traitent.

Thomas Dendale
Avocat au barreau de Bruxelles

[1] L'expression est reprise de A. Bascoman et J.-P. Mignard, *L'empire des données. Essai sur la société, l'algorithme et la loi*, Paris, Don Quichotte, 2018.

[2] Avis n° 33/2018 du 11 avril 2018 de la Commission Vie Privée ayant pour objet l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (CO-A-2018-026), disponible à l'adresse :
https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_33_2018_0.pdf.

[3] Avis n° 63.192/2 du 19 avril 2018 de la Section de législation du Conseil d'État sur l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel à l'adresse :
www.raadvst-consetat.be/dbx/avis/63192.pdf#search=donn%C3%A9es%20%C3%A0%20caract%C3%A8re%20personnel.

[4] Voir l'article 2 de la loi, à l'adresse : https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2016050417.

[5] Art. 6, § 1er, f), et considérant 47 du RGPD.

[6] Art. 37 du RGPD.

[7] Art. 221, § 2, de la loi du 30 juillet 2018 et art. 83 du RGPD.