fiches de Droit du traitement et de la protection des données personnelles

Rappels de cours et exercices corrigés

Agnès Rabagny-Lagoa

ellipses

Fiche 1

Le droit du traitement des données personnelles

Le droit du traitement des données personnelles s'est construit progressivement depuis la fin des années 1970.

I. La loi Informatique et Libertés du 6 janvier 1978

La révélation par la presse, dans les années 70, d'un projet gouvernemental tendant à identifier chaque citoyen par un numéro et d'interconnecter, via ce numéro, tous les fichiers de l'administration créa une vive émotion dans l'opinion publique. Ce projet connu sous le nom de SAFARI, soulignait les dangers de certaines utilisations de l'informatique et faisait craindre un fichage général de la population. Cette inquiétude a conduit le gouvernement à créer une commission chargée de proposer des mesures pour garantir que le développement de l'informatique se réalise dans le respect de la vie privée, des libertés individuelles et publiques. Cette « Commission Informatique et Libertés » proposa de créer une autorité indépendante, ce que fit la loi 78/17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* plus connue sous le nom *Loi Informatique et Libertés*. La France fut ainsi l'un des premiers États à se doter d'une législation spécialement dédiée à la protection des données personnelles. La loi *Informatique et Libertés* a donc ensuite servi de modèle à de nombreux législateurs.

L'article 1er de la loi du 6 janvier 1978 est ambitieux puisqu'il dispose que « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Lors de son adoption, la loi du 6 janvier 1978 visait principalement à encadrer l'informatisation de l'État et de l'Administration. Le législateur entendait alors protéger les citoyens et les administrés contre la toute-puissance d'un État informatisé. Cette volonté initiale justifiait les larges pouvoirs reconnus à la CNIL à l'égard du secteur public. Toutefois, en dépit de ses pouvoirs plus limités envers le secteur privé, la CNIL s'était également efforcée de contrôler la constitution de fichiers. Son rôle fut principalement incitatif, puisqu'elle parvint à imposer aux divers milieux professionnels une véritable culture informatique de protection de l'individu.

II. La directive 2002/58/CE du 12 juillet 2002 et sa transposition en droit français

La protection des données personnelles est rapidement devenue un enjeu européen, car elle ne pouvait être limitée au territoire d'un seul État. La protection des données personnelles a été renforcée par la transposition en droit interne de la directive 2002/58/CE du 12 juillet 2002 relative au *traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*. Cette directive s'est substituée à la directive 97/66/CE du 15 décembre 1997, rapidement dépassée par les évolutions technologiques et par le développement d'Internet.

La loi n° 2004-801 du 6 août 2004, *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés,* transposait en droit français les dispositions de la directive européenne 95/46. La création du Correspondant informatique et libertés, dont la nomination était facultative, était l'une de ses principales innovations. Pour la première fois, chaque organisme eut la possibilité de désigner un expert spécialement chargé de la protection des données personnelles. Pour le reste, la loi du 6 août 2004 n'a pas entraîné de rupture, puisque la loi française avait largement inspiré le législateur européen lors de l'adoption de la directive du 12 juillet 2002.

Tous les États membres de l'Union européenne ainsi que les pays de l'Espace Économique Européen disposaient désormais d'une loi « informatique et libertés » et d'une autorité de contrôle indépendante. Ces autorités indépendantes se réunissaient régulièrement à Bruxelles, pour conseiller la Commission européenne et pour harmoniser leurs pratiques ou recommandations destinées aux concepteurs et aux utilisateurs des technologies de l'information. Ces autorités de contrôle européennes formaient alors le « groupe de l'article 29 », par référence à l'article de la directive qui l'instituait.

III. Le règlement (UE) n° 2016/679 du 27 avril 2016, le RGPD

La protection des données personnelles est profondément remaniée par le RGPD (A). La protection des données est désormais pensée à l'échelle européenne (B).

A. Une réforme globale

La Commission européenne a proposé, le 25 janvier 2012, une réforme globale de la protection des données.

Le règlement UE n° 2016/679 du Parlement européen et du Conseil 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, dit Règlement général sur la protection des données ou RGPD constitue l'aboutissement de cette réforme. Il est entré en vigueur le 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date ont dû être mis en conformité avec ces nouvelles dispositions.

La réforme est réalisée par un règlement européen, directement applicable dans l'ensemble de l'Union européenne. Ce choix évite les incertitudes et les retards d'une transposition.

L'objectif de la réforme est triple : renforcer la protection des individus, alléger le coût et les procédures pour les organismes et favoriser la circulation des données.

La protection des données est généralisée et pensée à l'échelle de l'Union européenne. Peu de traitements de données sont exclus du Règlement : activités liées à la sécurité nationale, activités des États membres ayant trait à la politique étrangère et de sécurité commune de l'Union, traitement mis en œuvre par des personnes physiques dans le cadre d'une activité personnelle ou domestique, traitements des autorités compétentes aux fins de prévention, détection et poursuite des infractions pénales, traitements des institutions, organes, organismes et agences de l'Union.

Cette transformation répond aux besoins d'une économie numérique, ouverte sur le monde. Le Règlement préserve en cela les droits fondamentaux, qui risquaient d'être mis à mal par la libéralisation de l'économie des données. Un cadre juridique commun est donc mis en place, là où les frontières n'existent plus. Le considérant 13 du Règlement précise en effet que l'adoption d'un « règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques […] pour offrir aux personnes physiques dans tous les États membres un même niveau de droits opposables et d'obligations et de responsabilité pour les responsables du traitement et les sous-traitant ».

En outre, de manière assez inhabituelle pour un règlement, 56 marges de manœuvre nationales ont été laissées aux États membres afin de transposer

certaines dispositions communautaires qui, à défaut, ne s'appliqueront pas dans l'ordre interne.

ATTENTION

Deux autres textes ont été publiés en même temps que le RGPD. Le paquet « Data protection » inclut en effet deux directives très sécuritaires, adoptées après les attentats de Paris et Bruxelles.

La directive 2016/681/UE du 27 avril 2016 relative à l'utilisation des données des dossiers passagers, dite directive *PNR pour Passager Name Record*, intéresse directement la sécurité aérienne, avec un système européen de mise en commun des informations sur les passagers aériens.

La directive 2016/680/UE du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, dite directive *Police-Justice* porte sur la prévention et la détection des infractions pénales. Elle organise l'utilisation et le transfert de données à des fins policières et judiciaires.

B. Le domaine d'application du Règlement

Le domaine d'application du RGPD, défini par son article 3, est particulièrement vaste. Le texte a vocation à s'appliquer dès lors que :

- Le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne.
- Le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler ».

Le Comité européen de protection des données a précisé le critère de la localisation des personnes dans les *Lignes directrices 3/2018* adoptées le 12 novembre 2019. Ce critère ne correspond pas à leur nationalité, ni à leur domicile, mais vise à s'appliquer au traitement ciblant intentionnellement, et non accidentellement, des personnes situées dans l'Union européenne. Le Comité européen de protection des données donne un exemple précis. Une société australienne offrant un service numérique d'actualité et de vidéos à des utilisateurs situés en Australie ne sera pas soumise au RGPD par la seule circonstance que l'un de ses clients australiens voyagerait momentanément en Allemagne, pendant ses vacances, en continuant d'utiliser le service.

En droit interne, l'article 3, I, de la loi *Informatique et Libertés* pose le principe général, inspiré du RGPD, selon lequel la loi s'applique aux traitements « effectués dans le cadre des activités d'un établissement du responsable de traitement ou d'un sous-traitant sur le territoire français, que le traitement ait lieu ou non en France ». Cette disposition s'applique sans préjudice de l'article 3 du RGPD, pour les traitements entrant dans le champ du Règlement.

Le législateur français a jugé opportun d'ajouter **une règle de conflit de loi** dans le nouvel article 3, II de la loi *Informatique et Libertés*, qui dispose que les règles nationales, prises sur le fondement des marges de manœuvre nationales laissées par le RGPD s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France. Les spécificités du droit français bénéficient ainsi d'un champ d'application territorial plus large. Le lieu de résidence de la personne concernée est érigé en critère de rattachement. L'objectif est de renforcer sa protection, car la personne concernée n'a pas à s'interroger sur la loi applicable. Cette disposition est toutefois contraire à l'esprit du RGPD, car le législateur européen a souhaité privilégier l'application du seul droit de l'État dans lequel l'organisme a son établissement principal. Tout responsable de traitement, établi dans un État de l'Union, et collectant des données de personnes résidant en France devra s'interroger sur les spécificités françaises.

Une exception est toutefois prévue pour les traitements de données réalisés à des fins journalistiques, ou d'expression universitaire, artistique ou littéraire. La loi de l'État d'établissement du responsable du traitement s'applique alors. Cette particularité s'explique par l'importance de la liberté d'expression. Par exemple, lorsque le responsable du traitement fonde la finalité sur cette liberté, alors qu'il est établi en France, il n'a pas à respecter les dispositions particulières d'un autre État membre.

IV. L'adaptation du droit français

L'entrée en vigueur du RGPD a imposé de nombreuses adaptations du droit français. La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi *Informatique et Libertés* pour mettre en conformité le droit national avec le cadre juridique européen. Le texte a été presque entièrement validé par le Conseil constitutionnel, dans une décision 2018/765 DC rendue le 12 juin 2018. La loi *Informatique et Libertés*, hautement symbolique, n'a donc pas été abrogée lors de la réforme.

La loi du 20 juin 2018 permet la mise en œuvre concrète du RGPD. Elle dote notamment la CNIL des pouvoirs nécessaires à l'exercice de ses missions et organise l'articulation des procédures internes de la CNIL aux nouveaux mécanismes de coopération européenne. La loi du 20 juin 2018 transpose en droit français la Directive *Police Justice,* au sein du chapitre VIII de la loi

Informatique et Libertés. Le législateur a en outre utilisé de nombreuses marges de manœuvre nationales laissées par le Règlement : abaissement du seuil de minorité à 15 ans, création d'une action collective en indemnisation, maintien du régime d'autorisation préalable de la CNIL pour le traitement des données de santé…

L'ordonnance n° 2018-1125 du 12 décembre 2018 achève, au niveau législatif, la mise en conformité du droit national avec le RGPD. Elle réécrit certaines dispositions de la loi et assure sa mise en cohérence avec d'autres lois françaises traitant de protection des données. L'ordonnance garantit une application homogène du droit de la protection des données dans l'ensemble des collectivités d'outre-mer. Elle clarifie les différents régimes applicables en fonction de la nature des traitements concernés : traitements relevant du RGPD, traitements « police justice », traitements concourant à la défense nationale ou la sûreté de l'État…

Le décret n° 2019-536 du 29 mai 2019 tire les conséquences de forme et de fond de la modification de la loi informatique et liberté du 6 janvier 1978 par l'ordonnance du 12 décembre 2018. Il harmonise l'état du droit, adapte certaines règles procédures devant la CNIL. Il précise les droits des personnes concernées. Le décret n° 2018-687 du 1er août 219 contient les mesures d'application de la loi *Informatique et Libertés*, modifiée par la loi du 20 juin 2018.

Le droit applicable s'articule donc désormais en trois points :

- Le RGPD s'applique directement en droit français. Il remplace alors la loi nationale.
- Lorsqu'une marge de manœuvre nationale a été utilisée par le législateur français, la loi *Informatique et libertés* reste en vigueur et vient compléter le RGPD.
- La loi française nationale reste pleinement applicable pour tous les fichiers « répressifs », qu'il s'agisse de la sphère pénale ou du domaine du renseignement et de la sûreté de l'État. De nombreuses dispositions spéciales sont prévues en ces matières.

V. La protection des données personnelles : un droit fondamental

Les données personnelles ne sont pas des biens, susceptibles de faire l'objet d'échanges commerciaux. L'article 8 de la Charte des droits fondamentaux de l'Union européenne dispose que « toute personne a droit à la protection de ses données à caractère personnel la concernant ». Il consacre également les droits d'accès et de rectification et renvoie à une autorité indépendante le soin de faire respecter ces règles.

À RETENIR

La protection des données personnelles, qui est un droit fondamental, a été réformée par le Règlement UE n° 2016/679 du 27 avril 2016, le RGPD. Il fixe un cadre commun au sein de l'Union européenne pour construire progressivement un marché unique du numérique. La protection des données est généralisée et pensée à l'échelle de l'Union européenne :

- Le domaine d'application du Règlement est vaste. Tout responsable de traitement qui propose des biens ou des services à des personnes se trouvant au sein de l'Union européenne ou qui observe leurs comportements doit respecter le Règlement, même s'il est établi en dehors de l'Union. C'est le critère du ciblage.
- La régulation est assurée par un réseau d'autorités nationales, dont le travail est coordonné par le Comité européen de la protection des données, avec l'aide subsidiaire de la Commission européenne.

POUR EN SAVOIR PLUS

- G. Desgens-Pasanau, *La protection des données personnelles : Le RGPD et la loi française du 20 juin 2018*, éd. LexisNexis, 2019.
- G. Hass, *Guide juridique du RGPD*, G. Haas, éd. Eni, 2020.
- Le RGPD en Dataviz (Navigation visuelle dans le texte) https://www.cnil.fr/fr/le-reglement-europeen-sur-la-protection-des-donnees-en-dataviz
- Lignes directrices 3/2018 du Comité européen de protection des données. CEPD, version 2.0 adoptée le 12 novembre 2019.
- M. Bourgeois et M. Moine, « La nouvelle loi informatique et libertés, une transposition du RGPD ? » : *JCP E* 2018, 1417.
- M. Bourgeois et M. Moine, « Le décret n° 2018-687 du 1er août 201. Premier texte précisant l'application de la nouvelle loi Informatique et libertés ». *JCP éd. E*, n° 48, 29 novembre 2018, 1608.
- N. Martial-Braz et J. Rochfeld, *Droit des données personnelles : Les spécificités du droit français au regard du RGPD*, Dalloz, 2019.
- Texte intégral du RGPD : https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- Th. Douville, *Droit des données à caractère personnel : Droit de l'Union européenne, droit français*, Gualino, 2020.

1. **La protection des données personnelles a été organisée pour la première fois en France en :**
   - **a.** 1988
   - **b.** 1978
   - **c.** 2008
2. **Pour réformer le droit du traitement de données personnelles, la Commission a choisi de recourir à**
   - **a.** une directive
   - **b.** un règlement
3. **La protection des données personnelles est garantie par**
   - **a.** la Charte des droits fondamentaux de l'Union européenne
   - **b.** la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)
4. **Les États membres de l'Union européenne ont transposé dans leurs droits internes le RGPD.**
   - **a.** Vrai
   - **b.** Faux
5. **Une société américaine établie aux États-Unis doit se conformer au RGPD dès lors que son activité cible des ressortissants de l'Union européenne.**
   - **a.** Vrai
   - **b.** Faux

CORRIGÉ

1b ; **2**b ; **3**a ; **4**b ; **5**a