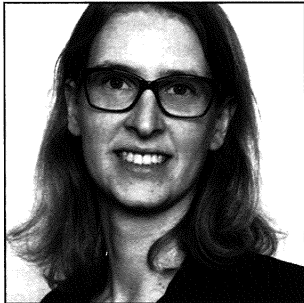




La protection des données personnelles appliquée aux robots : enjeux et obligations



I Myriam PIERRAT & Emmanuèle de DAMPIÈRE

Un constat : le développement de robots collectant et traitant de plus en plus de données personnelles

Le secteur de la robotique, celle-ci pouvant se définir comme la science et la technique de la robotisation, de la conception et de la construction des robots¹, est en plein essor : entre 2010 et 2014, les ventes de robots ont augmenté de 17 % par an en moyenne². Les robots sont présents dans tous les domaines : santé, agriculture, défense, logistique, domestique, loisirs. Indicateur également significatif, le nombre annuel de demandes de brevets en relation avec la robotique a triplé au cours des dix dernières années³.

A ce jour cependant, il n'existe pas de définition juridique du terme « robot » commune à l'Union européenne. Si, d'une manière générale, le robot peut être défini comme un « mécanisme automatique à commande électronique pouvant se substituer à l'homme pour effectuer certaines opérations, et capable d'en modifier de lui-même le cycle en appréhendant son environnement⁴ », force est de constater qu'il a un « caractère protéiforme⁵ » qui rend l'élaboration d'une définition juridique difficile.

Un rapport porté par l'euro-députée luxembourgeoise Mady Delvaux et adopté le 12 janvier 2017 par la Commission des affaires juridiques du Parlement européen formule des recommandations à l'attention de la Commission européenne pour la mise en place de règles de droit civil sur la robotique et appelle à l'adoption d'une

définition européenne commune des robots autonomes et intelligents et de leurs sous-catégories qui prendrait en considération les critères suivants : (i) l'acquisition d'autonomie grâce à des capteurs et/ou l'échange de données avec l'environnement (interconnectivité), l'échange et l'analyse de ces données, (ii) la capacité d'auto-apprentissage par l'expérience et par l'interaction (critère facultatif), (iii) la présence d'une enveloppe physique minimum, (iv) l'adaptation du comportement et des actes à l'environnement, (v) l'absence de vie au sens biologique⁶. Ce rapport sera mis au vote du Parlement européen en séance plénière le 16 février prochain.

et de la finesse des informations qui lui sont communiquées et de l'analyse qu'il est capable d'en faire.

Aux termes de la loi luxembourgeoise du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (telle que modifiée), prise en application de l'ancienne directive 95/46/CE⁷ (ci-après la Directive), une donnée personnelle désigne « toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable ». Dans la lignée de la Directive, la loi luxembourgeoise

Trop souvent la problématique de la protection des données personnelles est abordée en fin de projet ou même plusieurs mois après le lancement du produit ou du service. Cette pratique sera dorénavant sanctionnée plus fortement.

La multiplication des robots et leur sophistication grandissante sont intimement liées à l'augmentation des flux de données et notamment de données à caractère personnel. La tendance est en effet aux robots « intelligents », truffés de capteurs, qui accomplissent des tâches humaines à la place de l'homme. Ces fonctionnalités, rendues possibles grâce à l'intelligence artificielle, reposent en grande partie sur la collecte, la transmission et l'analyse d'une quantité considérable de données personnelles. Comment en effet se rapprocher au plus près des besoins de l'homme si ses habitudes quotidiennes ou de travail ne sont pas connues de la machine ? L'utilité du robot est ainsi tributaire de la personnalisation

ajoute qu'une personne physique « est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ».

Le nouveau règlement européen sur la protection des données (ou règlement général sur la protection des données⁸, ci-après RGPD), qui sera applicable dans tous les États membres à partir du 25 mai 2018, reprend la définition de la Directive en prenant le soin de préciser que le nom est une donnée personnelle (ce qui, étonnamment, n'était pas mis en avant dans la Directive) tout

comme un identifiant en ligne ou les données de localisation. C'est dire que les données personnelles sont diverses et que le risque de communiquer des informations personnelles à des tiers sans en avoir conscience est élevé.

Un cadre juridique peu adapté...

Le développement des robots et leur perfectionnement constant grâce à l'intelligence artificielle soulèvent de nombreuses interrogations quant aux règles juridiques auxquelles ils sont ou devraient être soumis. Plus un robot est autonome, plus le cadre juridique existant peut sembler inadapté pour appréhender et qualifier son comportement et ses actes, notamment, en matière de responsabilité⁹. La problématique du régime de responsabilité applicable aux robots et l'opportunité de définir une responsabilité juridique propre aux robots font déjà l'objet de débats doctrinaux et d'une réflexion au sein de l'Union européenne. Ces points ne seront pas abordés dans le cadre de cet article.

Le rapport de la Commission des affaires juridiques du Parlement européen adopté le 12 janvier dernier constitue les prémices d'une réglementation européenne générale sur les robots. De nombreux commentateurs soulignent l'importance de la mise en place rapide d'un cadre juridique européen afin de devancer les législateurs des États membres et d'éviter par la suite une disparité entre les droits nationaux.

... mais une réglementation européenne en matière de protection des données personnelles déjà fort utile

À l'heure où une demande croissante existe pour l'adoption d'une réglementation générale sur les robots, le RGPD permettra d'ores et déjà d'imposer aux concepteurs et fabricants de robots une série d'obligations visant toutes à préserver la vie privée et l'utilisation loyale et proportionnée des données personnelles des citoyens européens (utilisateurs des robots ou personnes physiques impactées par l'utilisation de robots par des tiers, par exemple, les drones survolant les résidences privées). Il est crucial que les individus gardent la maîtrise de l'usage de leurs données personnelles par des tiers. Il y a tout lieu de penser que l'incidence

du RGPD sera très importante dans le secteur de la robotique où les données personnelles « pullulent ».

Cet ensemble de règles ne doit pas être perçu comme un carcan empêchant le développement de la robotique. Bien au contraire, les acteurs de ce secteur d'activité doivent comprendre que la croissance continue de ce marché innovant dépend de la confiance des citoyens européens à l'égard des robots et de leurs fonctionnalités. Si les individus craignent un usage excessif ou détourné de leurs données personnelles par les fabricants ou concepteurs des robots qu'ils achètent ou envisagent d'acheter, ils seront réticents à donner à ces derniers leurs pleines capacités ou à renouveler leur achat. La conformité au RGPD doit être perçue comme un avantage compétitif et les concepteurs et fabricants de robots doivent, dès maintenant, s'y préparer.

Quelques obligations du RGPD essentielles pour le secteur de la robotique

Nous ne ferons pas une présentation exhaustive des dispositions du RGPD mais mettrons en avant les obligations les plus significatives auxquelles seront soumis les fabricants de robots en tant que « responsable du traitement », c'est-à-dire en tant qu'entité déterminant les finalités (gestion de la clientèle, fourniture des services ou des fonctionnalités, prospection, respect d'obligations légales, etc.) et les moyens du traitement des données personnelles¹⁰.

Dans son avis du 16 septembre 2014 sur les récentes évolutions relatives à l'Internet des objets, le G29 (organe consultatif européen indépendant sur la protection des données et de la vie privée composé des représentants des autorités nationales de contrôle des États membres) a souligné que tous les objets connectés utilisés pour recueillir et ensuite traiter les données de la personne sont considérés comme des moyens au sens de la Directive¹¹. Ce raisonnement devrait rester valable sous le RGPD et peut s'appliquer aux robots.

Certains traitements de données peuvent être sous la responsabilité de responsables conjoints du traitement. Cette situation pourrait être fréquente en matière de robots où les intervenants sont nombreux : concepteurs,

fabricants, distributeurs, utilisateurs exploitant les données collectées par certains robots dotés de caméras (comme les drones).

• Protection des données dès la conception (*Privacy by design*) et protection des données par défaut (*Privacy by default*)¹²

Une des évolutions majeures du RGPD par rapport à la Directive réside dans la diminution des formalités administratives préalables au profit de la prise en considération de la protection des données personnelles dès la conception du produit ou l'élaboration du service. Les autorités nationales de contrôle (au Luxembourg, il s'agit de la *Commission Nationale pour la Protection des Données* - CNPD) ont en effet pris conscience de deux travers : soit les formalités à accomplir avant le début de tout traitement sont ignorées par les responsables du traitement, soit ces derniers mettent toute leur énergie à l'accomplissement de ces formalités et « oublient » de traiter ensuite les données personnelles en conformité avec la législation¹³, pensant qu'ils sont couverts par leur notification/déclaration ou autorisation préalable. Les autorités nationales ne sont quant à elles pas en mesure d'effectuer des contrôles réguliers tant leur activité est consacrée au traitement des formalités préalables. Le changement d'approche apporté par le RGPD est donc bénéfique.

À compter du 25 mai 2018, il sera demandé au responsable du traitement d'appliquer les principes relatifs au traitement des données dès le début de son projet : au moment de la conception du produit ou de la mise en place du service, ce qui nécessite une réflexion en amont pour définir les protocoles et les mesures techniques et organisationnelles qui permettront de protéger les données de manière effective.

Trop souvent la problématique de la protection des données personnelles est abordée en fin de projet ou même plusieurs mois après le lancement du produit ou du service. Cette pratique sera dorénavant sanctionnée plus fortement. Toute donnée personnelle doit en effet être traitée de manière licite, loyale et transparente au regard de la personne concernée¹⁴. En outre la collecte des données personnelles doit être limitée à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Il s'agit du principe de la minimisation des données.

Parmi ces mesures devant être mises en place par le responsable du traitement dans le cadre du *Privacy by design*, le RGPD mentionne la pseudonymisation visant à ce que les données personnelles traitées ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, elles-mêmes soumises à des mesures de protection¹⁵ afin de garantir toute son efficacité à la pseudonymisation.

Corollaire du principe de protection des données dès la conception, le principe de protection des données par défaut (*Privacy by default*) requiert que les mesures techniques et organisationnelles mises en œuvre par le responsable du traitement garantissent que, par défaut, seules les données personnelles nécessaires au regard de chaque finalité spécifique du traitement soient traitées¹⁶. L'utilisateur du robot ne doit pas agir pour activer sa protection, cette dernière doit être activée par défaut¹⁷. Le respect de la protection des données par défaut aura donc un impact sur la quantité de données personnelles collectées, l'étendue de leur traitement, la durée de conservation de ces données et leur accessibilité. Les robots devront être conçus de telle manière qu'il appartiendra aux utilisateurs d'activer eux-mêmes les niveaux de personnalisation souhaités au regard des fonctionnalités offertes par les robots. Enfin les personnes concernées doivent être informées de l'identité des destinataires de leurs données personnelles et accepter au préalable cette communication (par exemple si le robot est associé à une interface sur Internet qui permet le partage des données avec des tiers afin de recevoir d'autres services).

• Analyse d'impact et profilage

Les dispositions du RGPD en matière de « profilage » et d'analyse d'impact sont innovantes et auront des conséquences importantes dans le secteur de la robotique.

La notion de « profilage », définie par le RGPD 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*¹⁸ », pourrait concerner certains robots, notamment, ceux dotés de caméras.

Le RGPD prévoit une obligation à la charge du responsable du traitement d'effectuer une analyse de l'impact des opérations de traitement envisagées sur la protection des données personnelles lorsqu'un type de traitement (en particulier les traitements ayant recours à de nouvelles technologies) est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques compte tenu des caractéristiques spécifiques du traitement¹⁹.

La décision d'effectuer une analyse d'impact revient donc au responsable du traitement qui devra au préalable évaluer le degré de risque causé par son traitement au regard de la protection des données. Cette analyse sera loin d'être facile, notamment pour les entreprises qui n'ont pas pris l'habitude de mener une réflexion sur l'utilisation des données personnelles qu'elles collectent et traitent (celles de leurs salariés, fournisseurs, prospects ou clients). Les lignes directrices du G29 à ce sujet sont très attendues. Les responsables du traitement seront également aidés par les listes des types d'opération de traitement soumis à l'analyse d'impact que les autorités nationales de contrôle devront établir²⁰.

Le RGPD indique les types de traitements qui devront en tout état de cause faire l'objet d'une analyse d'impact : par exemple, la surveillance systématique à grande échelle d'une zone accessible au public ou le profilage sur la base duquel seraient prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative (par exemple, le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine²¹).

Compte tenu des conclusions de l'analyse d'impact qui sera menée par le responsable du traitement, l'autorité nationale de contrôle pourra être saisie afin qu'elle donne son avis sur le traitement de données envisagé. Ses recommandations devront être suivies et prises au sérieux car les autorités de contrôle seront désormais dotées de pouvoirs étendus pouvant aller jusqu'à l'imposition d'amendes administratives.

• Droit à la portabilité des données personnelles²²

Aux côtés des traditionnels droits à l'information, à l'accès aux données personnelles ou à leur rectification, le droit à la portabilité des données personnelles est un nouveau droit créé par le législateur européen au bénéfice des personnes concernées. Celles-ci pourront désormais récupérer auprès du responsable du traitement « dans un format structuré, couramment utilisé et lisible par machine » les données personnelles qu'elles lui auront fournies afin de les transmettre à un autre responsable du traitement²³. Cette disposition vise à la fois à renforcer le contrôle exercé par les personnes concernées sur les données personnelles qu'elles fournissent au responsable du traitement (en y consentant expressément ou en vertu d'un contrat) et à dynamiser la concurrence entre les responsables de traitement offrant des produits ou services similaires.

Le 13 décembre 2016, le G29 a rendu ses lignes directrices concernant ce nouveau droit à la portabilité (accompagnées d'une liste de questions fréquemment posées et les réponses du G29). Il y précise, notamment, que les données personnelles entrant dans le périmètre du droit à la portabilité sont celles qui sont activement et en connaissance de cause fournies par la personne concernée (par exemple, l'adresse postale, le nom d'utilisateur, l'âge) ou celles qui sont fournies par la personne concernée du fait de l'utilisation du service ou du procédé (tels qu'un historique de recherche, des données de trafic ou de localisation ou les battements du cœur enregistrés par un appareil de sport ou de santé). En revanche, les données personnelles dérivées, celles qui sont créées par le responsable du traitement à partir de l'analyse des données personnelles fournies par la personne concernée, ne sont pas visées par le droit à la portabilité (par exemple, les résultats concernant la santé d'un utilisateur ou une cote de solvabilité).

Les responsables du traitement du marché de la robotique auront donc l'obligation de mettre en œuvre ce nouveau droit en distinguant entre les données personnelles utilisées par leurs robots. Cette problématique devra être prise en compte dès la conception du produit pour que le droit à la portabilité des données personnelles soit effectif. Les différents acteurs du marché

de la robotique devront en outre réfléchir ensemble à la mise en place de normes et de formats interopérables afin que le droit à la portabilité ne reste pas un « vœu pieux ».

• Droit à l'effacement des données personnelles (« droit à l'oubli »)²⁴

Suite à la jurisprudence *Google Spain* de la Cour de Justice de l'Union Européenne (CJUE)²⁵, le RGPD consacre le droit à l'effacement des données personnelles dans certaines circonstances, et notamment lorsque la personne concernée retire le consentement sur lequel est fondé le traitement et qu'il n'existe pas d'autre fondement juridique au traitement.

Les responsables du traitement du marché de la robotique devront composer avec ce nouveau droit et devront prévoir une fonctionnalité permettant à la personne concernée d'effacer toutes ses données personnelles communiquées au robot. Cette possibilité devrait renforcer la confiance des consommateurs à l'égard des robots.

• Sécurité encadrant le traitement de données personnelles²⁶

Enfin, dans la continuité de la législation actuelle, le responsable du traitement et son sous-traitant auront l'obligation de garantir la sécurité des données personnelles faisant l'objet d'un traitement. Cette obligation est fondamentale pour les acteurs du marché de la robotique, les risques de piratage et de contrôle à distance des appareils dotés d'une intelligence artificielle étant très élevés.

Le RGPD donne des exemples de mesures techniques et organisationnelles permettant de garantir un niveau de sécurité adapté au risque, à savoir, par exemple, la pseudonymisation et le chiffrement des données personnelles ou la mise en place de procédures visant à tester, analyser et évaluer régulièrement l'efficacité des mesures adoptées pour assurer la sécurité du traitement²⁷. Ces mesures et protocoles de sécurité devront être intégrés aux technologies du produit dès la conception.

Conclusion

On l'a vu, la robotique et ses applications sont un terrain fertile pour le traitement de données personnelles et malgré

l'absence d'une réglementation générale dans le domaine de la robotique, le cadre juridique européen en matière de protection des données personnelles offre de nombreuses garanties. Le rapport précité de la Commission des Affaires juridiques du Parlement européen appelle même la Commission européenne et les Etats membres à s'assurer que les règles de droit civil qui seront adoptées dans le futur soient conformes au RGPD et en ligne notamment avec le principe de nécessité et de proportionnalité du traitement²⁸. L'application du RGPD est un rempart contre l'utilisation abusive et non transparente des données personnelles des utilisateurs ou des tiers impactés, qui, si elle était généralisée, aurait des conséquences très défavorables sur la croissance du marché de la robotique.

Si le renforcement de la confiance des citoyens européens à l'égard du marché des robots ou la préservation d'une image d'entreprise soucieuse de la vie privée et de l'utilisation loyale des données de ses clients n'étaient pas des objectifs suffisants pour les responsables du traitement, il faudra également garder à l'esprit que le RGPD dote, dorénavant, les autorités nationales de contrôle de pouvoirs étendus allant jusqu'aux amendes administratives dont le montant maximal aura un fort pouvoir de dissuasion²⁹.

Myriam PIERRAT
myriampierat@elvingerhoss.lu

Emmanuèle de DAMPIERRE
emmanuelededampierre@elvingerhoss.lu

Étude Elvinger Hoss Prussen
Luxembourg, Luxembourg

1 <http://www.larousse.fr/encyclopedie/divers/robotique/88770>.

2 European Parliament, Committee on Legal Affairs, *Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL))*, page 3.

3 Idem.

4 Définition donnée par le dictionnaire *Le nouveau Petit Robert de la langue française*, 2010.

5 Alain Bensoussan, Avocat au Barreau de Paris, dans un entretien publié au *Recueil Dalloz*, n°28 du 30 juillet 2015.

6 European Parliament, Committee on Legal Affairs, *Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL))*, page 8.

7 La Directive a été abrogée par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

8 Règlement (UE) 2016/679 du 27 avril 2016.

9 Si les acteurs du secteur s'accordent à dire que les lois de l'écrivain Isaac Asimov exposées dans ses ouvrages de science-fiction doivent être respectées, aucun texte européen ou international n'a encore vu le jour. Les trois lois d'Asimov sont les suivantes : (1) « Un robot ne peut porter atteinte à un être humain ni, restant passif, permettre qu'un être humain soit exposé au danger. » ; (2) « Un robot doit obéir aux ordres que lui donne un être humain, sauf si de tels ordres entrent en conflit avec la première loi. » ; (3) « Un robot doit protéger son existence tant que cette protection n'entre pas en conflit avec la première ou la deuxième Loi. » Isaac Asimov, *Cercle vicieux*, 1942.

10 Article 4(7) du RGPD.

11 Avis 8/2014, page 12.

12 Article 25 du RGPD.

13 Voir le considérant 29 du RGPD.

14 Article 5.1 du RGPD.

15 Article 4(5) du RGPD.

16 Article 25.2 du RGPD.

17 Voir la fiche "Le Privacy by Design : de quoi s'agit-il?" sur le site Internet de la CNPD : http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Le-Privacy-by-Design_de-quoi-s_agit-il_/index.html

18 Article 4.4 du RGPD.

19 Article 35 du RGPD.

20 Article 35.4 du RGPD.

21 Considérant 71 du RGPD.

22 Article 20 du RGPD.

23 Si cela est techniquement possible, la personne concernée peut également demander que ses données personnelles soient transmises directement de l'ancien responsable du traitement (ou prestataire de service) au nouveau. Voir article 20.2 du RGPD.

24 Article 17 du RGPD.

25 CJUE, Grande Chambre, 13 mai 2014, *Google Spain SL et Google Inc., C-131/12*.

26 Article 32 du RGPD.

27 Dans son avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, le G29 mentionne également des "pratiques de sécurité basées sur des restrictions de réseau, désactivant des fonctionnalités non critiques par défaut, empêchant l'utilisation de sources de mise à jour de logiciels non fiables".

28 *Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL))*, page 11.

29 Selon la disposition du RGPD violée, les amendes administratives peuvent s'élever (i) jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ou (ii) jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (Article 83.4 et 83.5 du RGPD).