La question des identités numériques à l'ère du RGPD : privacy ou protection des données ?

Armen Khatchatourov

LA QUESTION DES IDENTITÉS NUMÉRIQUES À L'ÈRE DU RGPD : *PRIVACY* OU PROTECTION DES DONNÉES ?

Armen Khatchatourov

A.D.B.S. | « I2D - Information, données & documents »

2019/1 n° 1 | pages 34 à 39

ISSN 2428-2111
DOI 10.3917/i2d.191.0034

Mots clés : Consentement, Identités numériques, Privacy, Protection des données, RGPD

La question des identités numériques à l'ère du RGPD : *privacy* ou protection des données ?

Le Règlement général sur la protection des données (RGPD) est entré en application le 25 mai 2018. Plaçant l'Europe à l'avant-garde de la protection des données à caractère personnel, il constitue à ce titre une avancée majeure en la matière. Il serait cependant dommage de s'arrêter en si bon chemin, en pensant que les questions de *privacy* sont désormais réglées. En particulier, ce nouveau règlement ne doit pas nous dissuader de nous interroger en profondeur sur la question des identités, dont les contours se sont redéfinis à l'ère numérique : il convient alors de conserver une approche critique envers le RGPD et ses propres limitations.

Armen KHATCHATOUROV

Armen KHATCHATOUROV

Ingénieur de formation initiale et docteur en philosophie de la technique (2005). Il est enseignant-chercheur à Institut Mines-Télécom Business School, membre de la Chaire « Valeurs et Politiques des Informations Personnelles » de l'Institut Mines-Télécom. Auparavant, il a travaillé dans la recherche publique comme privée, notamment comme chef de projet IHM dans le cadre du Réseau d'Excellence européen *Enactive Interfaces* (UTC et INP-G), chef de projet IHM - IA à Sony Computer Science Lab Paris, ainsi qu'à l'Institut de Recherche et d'Innovation/Centre Pompidou. Il est en charge de la direction adjointe de la revue *Études Digitales* (Classiques Garnier). Il a publié plusieurs travaux sur la transformation numérique et ses conséquences sur la société, les organisations et l'identité, dont *Les identités numériques en tension, entre autonomie et contrôle* (ISTE Editions/Wiley). Il a enseigné à IMT-BS, aux Ponts et à l'UTC, ainsi que dans les écoles de design (EESI, Strate).

De la notion de *Privacy* à la notion de *Data Protection*

Le premier élément, souvent sous-estimé, concerne la transformation de la notion de *Privacy by Design (PbD)* en *Data Protection by Design (DPbD)*. *PbD* apparaît à la fin des années 1990 et correspond à une approche dans laquelle la *privacy* est un problème global qui demande des mesures interconnectées, tant technologiques et de *design*, qu'organisationnelles ou de modèles d'affaires. Dans *PbD*, le *by Design* ne signifie donc pas, à notre sens, telle ou telle mesure qui porte sur le vecteur du problème (les données), mais une approche en amont, qui considère l'espace du problème tout entier, en mettant en œuvre des systèmes sociotechniques qui, dans leur conception même, sont capables soit de prévenir les abus potentiels, soit de rendre explicites leurs modalités de fonctionnement et d'orienter les choix des utilisateurs dans le sens d'un meilleur exercice de leur *privacy*.

Tout en s'inspirant de ce principe, le RGPD s'appuie sur une notion différente, celle de *DPbD*. Le passage de l'une à l'autre a attiré peu d'attention dans le débat public, à quelques exceptions près. Or, ni le vocable de *privacy* ni celui de *PbD* n'apparaissent dans le texte du RGPD, contrairement aux autres textes parmi lesquels notamment la Directive *Protection des données à caractère personnel* de 1995[23], que le RGPD remplace, ou la directive *Vie privée et communications électroniques* de 2002[24], qui « devrait être modifiée en conséquence ».

Ce glissement sémantique peut être interprété de différentes manières. Ainsi, certains argumentent[25], à juste titre, que la législation en question ne concerne que l'aspect « données personnelles » d'un champ (trop) vaste de *privacy* qui, lui, se confond presque avec la liberté que le concept de *privacy* n'est pas directement opérationnalisable dans le contexte législatif ; et qu'il est donc opportun et sage de passer à celui de *DPbD*.

Même si l'on peut être d'accord avec cette analyse, il convient d'examiner les effets de ce glissement. Tout d'abord, il y a bien sûr les effets communicationnels.

[23] 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.

[24] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

[25] Mireille Hildebrandt & Laura Tielemans, *Data Protection by Design and Technology Neutral Law*, Computer Law & Security Review, vol. 29, n° 5, 2013, p. 509-521.

La majorité des acteurs du domaine et des utilisateurs est maintenant convaincue[26], par une sorte d'illusion d'optique, que le RGPD implémente effectivement le PbD, ce qui à notre sens peut conduire à baisser la garde sur ces sujets[27].

Plus fondamentalement, il convient aussi de souligner ce qui est perdu dans ce passage : il existe à notre sens, une différence fondamentale entre la recherche de *privacy* et la protection des données personnelles.

Qu'est-ce que la *Privacy* ?

Les politiques actuelles sur la protection des données mettent l'accent sur les droits de la personne. Mais on considère le plus souvent, dans ces textes, un sujet déjà constitué, capable d'exercer ses droits et sa volonté. Or, le propre des technologies numériques est de participer à la formation des subjectivités selon un mode nouveau : en redistribuant sans cesse le jeu des contraintes et des incitations, elles créent les conditions d'une plus grande malléabilité des individus[28].

En ce sens, les enjeux de la *privacy* ne concernent pas tant la protection des individus déjà constitués, sujets du droit, que les processus de subjectivation. La *privacy* n'est pas une protection contre l'intrusion dans la sphère propre à l'individu ou un « droit à rester tranquille ». L'enjeu de la *privacy* est de permettre un espace de jeu, un espace d'indétermination dans lequel l'individualité peut advenir dans les pratiques quotidiennes, un espace dans lequel l'initiative de négociation des frontières entre le soi et la société est laissée à l'individu[29].

Bref, il y là une différence fondamentale entre la « personne concernée » *(data subject)* sur lequel porte le RGPD et la personne en devenir, dont l'identité est en construction permanente.

Thématiser cette différence nous semble nécessaire afin de ne pas rabattre la problématique de l'identité sur celle du simple traitement des données personnelles, afin de saisir ce qui, dans l'identité, est en excès sur la simple « protection de ses données ». C'est à ces conditions que le processus de la construction de l'identité peut prendre place de manière à permettre l'autonomie de la personne, elle-même condition des échanges sociaux. À l'inverse, passer sous silence ces

[26] Ainsi par exemple le Rapport *Privacy and Data Protection by Design* établi en 2014 par l'European Union Agency for Network and Information Security (ENISA) stipule tout simplement l'équivalence entre PbD et DPbD : « The term *Privacy by Design*, or its variation *Data Protection by Design*, has been coined as a development method for privacy-friendly systems and services, thereby going beyond mere technical solutions and addressing organisational procedures and business models as well. Although the concept has found its way into legislation as the proposed European General Data Protection Regulation, its concrete implementation remains unclear at the present moment. »

[27] Cf. à ce sujet par exemple : Michael Veale, Reuben Binns and Jef Ausloos, « When data protection by design and data subject rights clash », *International Data Privacy Law*, vol. 8, n° 2, 2018.

[28] Armen Khatchatourov, *Identités numériques en tension, entre autonomie et contrôle*, ISTE Éditions, 2019.

[29] Julie E. Cohen, « What privacy is for », *Harvard Law Review*, vol. 126, 2013.

enjeux ou laisser opérer des glissements sémantiques qui confondent *privacy* et protection des données ne peut que conduire, à terme, à une société qui ne s'interroge plus sur les conditions technologiques du vivre-ensemble.

Examinons ces questions sur deux terrains. Le premier concerne la compréhension et la maîtrise des données en articulation avec les effets communicationnels qui accompagnent l'implémentation des systèmes de gestion des identités. Le second concerne les effets normatifs de ce que nous appelons « une approche par consentement » implémentée dans ces systèmes.

Effets de l'implémentation des systèmes de gestion des identités : confusion entre finalités et contextes d'usages

Depuis les débuts des échanges numériques, une des manières de garantir la *privacy* était d'utiliser des identités multiples ou des pseudonymes, de sorte que la séparation entre les contextes dans lesquels les données personnelles sont en jeu ne soit pas remis en cause par l'usage de l'identifiant unique[30].

La question de l'identité est ici cruciale : ramener les multiples pratiques d'une personne qui se présente sous différentes identités en fonction des contextes dans lesquels elle évolue, à un individu « unique » identifiable revient à réduire la personne à sa seule identité civile ou à un profil identifiable et composé de l'ensemble quasi-complet de ses données personnelles. Cette assimilation n'est pourtant pas sans conséquence : elle renforce la transparence de l'individu, augmente les risques de discrimination et diminue la richesse des interactions possibles.

La question des identités est au cœur du Règlement eIDAS (2014)[31], antérieur de deux ans à la mise en place du RGPD, et dont le but est de mettre en place le cadre pour l'utilisation des identités numériques dans les systèmes d'identification étatiques, dans le contexte transfrontalier et en l'absence d'un système unique européen. À notre sens, ce règlement procède également d'un agenda économique et industriel dont la supposition est que l'utilisation accrue de ces systèmes dans le secteur public, dont il est le moteur, va également augmenter l'adoption dans le secteur privé[32]. Par ailleurs, sur le terrain des données personnelles, il stipule que « l'utilisation des pseudonymes dans les transactions électroniques n'est pas interdite ». On pourrait donc supposer que ce règlement est, dans son esprit, protecteur de la *privacy*.

[30] Helen Nissenbaum, « A contextual approach to privacy online », *Daedalus*, vol. 140, n° 4, 2011, p. 32-48.

[31] Règlement 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE : http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR

[32] A. Khatchatourov *et al.*, « Privacy in digital identity systems: Models, assessment, and user adoption », *IFIP, EGOV 2015, Proceedings*, Berlin, Allemagne, Springer, « Lecture Notes in Computer Science », 2015.

Cependant, la mise en application de ce règlement est accompagnée des actes d'exécution, en élaboration dès le printemps 2015. Parmi ceux-là, le règlement d'exécution sur le cadre d'interopérabilité[33] stipule que, afin de garantir la communication technique des systèmes d'identités numériques entre eux, un ensemble minimal de données d'identification personnelle standardisé doit être mis en place dans le cadre des échanges transfrontaliers. Cet « ensemble minimal des données » comporte obligatoirement et *a minima* : nom(s) de famille ; prénom(s) ; date de naissance ; « un identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontalière et qui soit aussi persistant que possible dans le temps » (nous soulignons). Il va de soi que, avec un tel ensemble de données, la pseudonymisation ne peut plus être assurée. De surcroît, dans l'exacte mesure où les systèmes sont potentiellement destinés à l'usage commercial, l'argument de la nécessité des données à ce point identifiantes pour les besoins régaliens ne tient pas[34]. Il n'est pas clair à ce jour comment concevoir une compatibilité entre cette absence de pseudonymisation et le RGPD[35].

Ainsi, les détails techniques de l'implémentation de ces systèmes, souvent passés sous silence, et la confusion entre les finalités et les contextes d'usage produisent des effets sur nos identités numériques, en les assignant à une visibilité de plus en plus grande.

Effets normatifs de l'approche par consentement

Le deuxième terrain est celui des effets normatifs de l'approche par consentement. À notre sens, l'accent mis sur le consentement est paradoxalement le reflet – ou en tout cas, est parfaitement compatible – avec les mécanismes économiques et identitaires de la société néolibérale.

La société contemporaine conjugue en effet deux aspects en matière de *privacy* : il s'agit de considérer l'individu comme étant visible de manière permanente, et comme étant responsable individuellement pour ce qui est vu de lui[36]. Un tel

[33] Règlement d'exécution 2015/1501 du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement 910/2014 : http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1501&from=FR

[34] Armen Khatchatourov, « Privacy in Digital Identity Systems: what is lost in eIDAS implementation? », Toulouse, France, *Conférence APVP'16, Atelier sur la Protection de la Vie Privée*, juillet 2016.
Niko Tsakalakis, Sophie Stalla-Bourdillon, Kieron O'Hara, « What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation », Rome, Italy, *Open Identity Summit 2016*, 13-14 october 2016.

[35] Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara, « Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised? », *in* Kosta E., Pierson J., Slamanig D., Fischer-Hübner S., Krenn S. (dir.), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Cham, Suisse, Springer, « IFIP Advances in Information and Communication Technology », vol. 547.

[36] Gordon Hull, « Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data », *Ethics and Information Technology*, vol. 17, n° 2, 2015, p. 89-101.

ensemble de normes sociales se consolide à chaque fois que l'utilisateur exerce le consentement – ou l'opposition – à l'utilisation de ses données. En effet, à chaque itération, l'utilisateur renforce sa compréhension de soi-même comme l'auteur et le responsable de la circulation des données. Il endosse aussi l'injonction à la maîtrise des données alors même que cette dernière est le plus souvent illusoire. Surtout, il endosse l'injonction à calculer les bénéfices que le partage des informations peut lui apporter. En ce sens, l'application stricte et croissante du paradigme de consentement peut être considérée comme étant corrélative d'une conception de l'individu qui devient non seulement l'objet d'une visibilité quasi-totale, mais aussi – et surtout – un agent économique rationnel, à même d'analyser son agir en termes de coûts et de bénéfices.

Cette difficulté fondamentale fait que les enjeux futurs des identités numériques ne se réduisent pas à donner plus de contrôle explicite, ou plus de consentement éclairé. Il convient bel et bien de trouver d'autres voies complémentaires, qui se situent sans doute du côté des pratiques (et non simplement des « usages ») des utilisateurs, à condition que de telles pratiques mettent en place des stratégies de résistance pour contourner l'impératif de visibilité absolue et de définition de l'individu comme agent économique rationnel.

Conclusion : affronter les ambivalences intrinsèques aux technologies numériques

De telles pratiques digitales doivent en outre nous inciter à dépasser la compréhension de l'échange social – numérique ou non – sous le régime du calcul des bénéfices que l'on en retire ou des externalités. Ainsi, les enjeux soulevés par les identités numériques dépassent largement les enjeux de protection de l'individu ou les enjeux des « modèles d'affaires », et touchent à la manière même dont la société dans son ensemble conçoit la signification de l'échange social. Dans un tel horizon, il est primordial d'affronter les ambivalences et les jeux de tension intrinsèques aux technologies numériques, en examinant les nouveaux modes de subjectivation induits dans ces opérations. C'est à partir d'un tel exercice de discernement que pourra advenir un mode de gouvernance des données plus responsable.