À quoi sert le principe de transparence en droit des données personnelles ?

Emmanuel Netter

À quoi sert le principe de transparence en droit des données personnelles ?
Dalloz IP/IT, novembre 2020, p. 611

Emmanuel Netter
Maître de conférences HDR en droit privé à l'Université d'Avignon
LBNC (EA 3788)

En 1977, Jean Foyer, alors rapporteur de la loi informatique et libertés, présente à l'Assemblée nationale le « droit d'accès » que le texte entend consacrer. D'une formule destinée à marquer les esprits, il annonce que les fichiers informatisés deviendront des « maisons de verre ». Les traitements auront lieu au grand jour. Chacun saura quelles informations le concernant sont exploitées, et de quelle manière : l'idée de « transparence » est déjà bien là, même si ce terme précis n'est pas encore employé. Il fait une apparition discrète au détour d'un considérant de la directive de 1995 (cons. 63 de la directive 95/46/CE), et trône aujourd'hui en majesté au sein du RGPD. D'abord, au sein des grands principes énumérés par le texte, la transparence occupe le premier rang, au côté de la licéité et de la loyauté (art. 5, a). Ensuite, le chapitre consacré au droit des personnes concernées s'ouvre par une section « transparence et modalités ».

La transparence constitue donc aujourd'hui, manifestement, l'un des piliers de la protection des individus par le droit des données à caractère personnel. Elle est un corollaire du principe d'autodétermination informationnelle, d'origine allemande, qui fait de l'individu le maître de ses données (Cour constitutionnelle fédérale allemande, 15 décembre 1983). Le RGPD affirme ainsi que « les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant » (cons. 7). Face à des traitements réalisés sans fondement de licéité, pour des finalités indéterminées, sur la base d'informations inexactes, ou pour des durées excessives, la meilleure vigie serait la personne concernée elle-même. Encore faut-il, pour qu'elle puisse exercer son contrôle, qu'elle ait connaissance de l'existence et des modalités du traitement (I). Bien souvent, le principe d'autodétermination informationnelle ira plus loin encore. La personne concernée, une fois renseignée sur le projet de traitement, aura le pouvoir d'en autoriser ou d'en empêcher le déroulement, par l'octroi ou le refus de son consentement. La transparence appelle alors une réponse, le monologue se mue en dialogue (II).

De tels principes semblent, de prime abord, devoir emporter l'adhésion inconditionnelle de tous ceux qui sont attachés à la défense des droits des individus face aux potentiels abus des responsables de traitement. Mais faire prendre véritablement conscience de leur situation aux personnes concernées est plus difficile qu'il n'y paraît. Pour que le droit à la transparence ne soit pas « théorique ou illusoire mais concret et effectif », de nombreux obstacles doivent être surmontés (la formule est tirée de CEDH 9 oct. 1979, Airey c/ Irlande, req. no 6289/73 , § 26).

I – La transparence solitaire : informer

En vertu des articles 13 et 14 du RGPD, le responsable de traitement doit fournir une liste précise de renseignements aux personnes dont il manipule les données, immédiatement en cas de collecte directe, et dans un délai raisonnable en cas de collecte indirecte. Au fond, que peut-on véritablement attendre de ces formalités ? Le découvrir suppose de s'interroger sur l'objet de l'information, sur les méthodes d'information et sur les destinataires de l'information.

L'objet de l'information. La transparence peut certes consister à informer des individus qui savent déjà que leurs données sont manipulées des caractéristiques détaillées de ce traitement : finalité, catégories de données, destinataires des informations, durées de conservation… Mais ce n'est pas

uniquement cela. Il arrive fréquemment que l'existence même du flux d'information soit totalement ignorée des intéressés. Le lancement par Facebook, le 28 janvier 2020, d'un nouvel outil dénommé « off activity », en constitue un exemple intéressant. Il permet aux utilisateurs du réseau social de découvrir quelles informations sont collectées auprès de tiers via leurs sites web et applications pour ordiphones. De nombreux internautes ont alors découvert avec effarement que leurs consultations de vidéos, leurs visites de blogs, leurs achats de billets de train, leurs commandes de livres remontaient en temps réel à Facebook, qui les centralisait et les exploitait pour affiner sa connaissance de leurs centres d'intérêt. Parmi les tiers fournissant des données au réseau social, nombreux sont d'ailleurs ceux qui ne l'indiquent nulle part dans leur politique de confidentialité, en particulier lorsqu'ils communiquent avec Facebook par l'intermédiaire d'un SDK (Software Development Kit) intégré à une application mobile. Un renforcement de la transparence par l'un des acteurs a ainsi fait apparaître la violation totale et décomplexée de ce principe par d'autres responsables de traitement. Retenons donc que le nouvel outil de Facebook a eu pour vertu de dévoiler *l'existence* même de traitements jusqu'ici ignorés des utilisateurs. Sous une forme graphique aisément intelligible, il a également révélé *l'ampleur* du réseau d'informateurs de Facebook. Il faut à cet égard noter la particulière efficacité des représentations visuelles lorsqu'il s'agit de conférer de la substance à des menaces pour la vie privée, sans cela très abstraites. Grâce à l'outil de visualisation des cookies *Dataviz*, développé par la CNIL, l'internaute voit se dérouler autour de lui lui la toile d'araignée des régies publicitaires sur la plupart des sites qu'il visite. Mais le RGPD ne commande pas aux responsables de traitement de développer eux-mêmes de tels outils. Un exemple d'initiative en ce sens est la *Timeline* de Google maps. Elle permet à l'utilisateur du service de retracer l'historique de ses déplacements minute par minute. Paradoxalement, l'outil est souvent cité par les étudiants comme un exemple de surveillance orwelienne, alors qu'il rend tangibles, palpables les données détenues par le responsable de traitement, quand d'autres qui disposent d'informations tout aussi détaillées se font les plus discrets possibles.

Premier enseignement : une transparence efficace signale non seulement *l'existence* d'une menace pour les droits du destinataire, mais aussi son *ampleur*.

Les méthodes d'information. Les représentations visuelles du traitement qui viennent d'être évoquées, si elles constituent sans doute l'outil le plus puissant en matière d'éveil du grand public, restent fort rares et ne sont pas exigées par le RGPD. La transparence du règlement passe par les mots. Elle a certes pour elle d'être « portable » et non « quérable » : alors que les autres droits des personnes concernées (accès, rectification, portabilité…) requièrent une initiative, et donc un effort de la personne concernée, la transparence est à l'initiative du responsable de traitement. Elle apporte aux intéressés les informations pertinentes sur un plateau. Mais on sait depuis longtemps, en droit des contrats et de la consommation, qu'il ne suffit pas de présenter aux yeux pour toucher les consciences. La CNIL l'a compris également, qui livre actuellement une bataille contre les politiques de confidentialité trop longues, trop complexes ou trop vagues. Elle a pour allié l'article 12 du Règlement, qui exige du responsable de traitement qu'il s'exprime « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ». Dans sa décision de sanction du 21 janvier 2019, elle a ainsi critiqué la politique de confidentialité de Google, pourtant l'une des moins mauvaises du genre, en lui reprochant d'éparpiller à l'excès des informations cruciales, et d'utiliser des expressions par trop équivoques. Admettons que les meilleurs efforts de synthèse et de pédagogie soient effectivement déployés, cela changerait-il quelque chose ? Il existe en effet des projets d'associations sans but lucratif visant à réduire les politiques de confidentialité à quelques icônes simples (les *privacy icons* de la fondation Mozilla) ou à quelques éléments-clés assortis d'une note (A, B…) et d'un code couleur tirant leur inspiration des étiquetages alimentaires (tosdr.org). Ces projets postulent, et ils ont raison, que l'utilisateur ordinaire ne lit pas davantage les politiques de confidentialité qu'il n'épluche ses contrats bancaires, d'assurance ou de téléphonie mobile. L'eau peut être d'une pureté cristalline, on ne fait pas boire un cheval qui n'a pas soif.

Deuxième enseignement : la transparence nécessite toujours des *efforts*, une volonté d'être informé.

Les destinataires de l'information. Si l'on admet l'idée, d'un pessimisme raisonnable, selon laquelle l'utilisateur moyen ne fera pas grand-chose des informations qui lui sont adressées, il faut alors envisager l'hypothèse selon laquelle la transparence s'adresserait en réalité – ou de surcroît – à d'autres que lui. Qui sont ces autres ? Il peut s'agir des pouvoirs publics et autorités de contrôle, qui peuvent retirer des information ainsi produites des enseignements individuels, sectoriels ou globaux sur l'attitude des responsables de traitement et leur conformité au règlement. Encore faut-il, naturellement, avoir la volonté – s'agissant des pouvoirs publics – et les moyens – s'agissant de la CNIL – d'en tirer des conséquences. Des centaines de politiques de confidentialité en ligne peuvent révéler, par ce qu'elles disent et ce qu'elles taisent, des situations de non-conformité criantes, la Commission n'en fera rien si elle n'a pas les effectifs nécessaires pour effectuer des contrôles spontanés. Mais parmi les autres destinataires de la transparence, figurent par ailleurs des foyers d'expertise de la société civile, au premier rang desquels des associations de défense des libertés civiles numériques, comme la Quadrature du Net ou None of Your Business. Certaines de leurs plaintes ont été à l'origine de la plus grosse sanction jamais infligée en France (dans la délibération Android sus-citée du 21 janvier 2019), et d'autres sont actuellement instruites par l'autorité irlandaise. Ces initiatives privées ne seraient probablement pas aussi cruciales si la gouvernance publique du secteur était suffisamment ferme. Ces structures doivent se débattre avec des difficultés de financement, ainsi qu'avec les nombreuses marges de manœuvres octroyées aux Etats-membres – qui constituent autant d'obstacles à surmonter pour fédérer efficacement des actions à l'échelle européenne. Le RGPD prévoit certes que des mandats puissent être donnés pour l'exercice des personnes concernées, il permet les plaintes collectives et les actions de groupe, mais ces mécanismes ont été conçus pour seconder l'action des autorités de contrôle et des individus isolés, davantage que pour occuper la place centrale.

Troisième enseignement : la transparence mériterait d'être davantage pensée *collectivement.*

La transparence considérée jusqu'ici n'appelait pas nécessairement de réaction de la part de ses destinataires. En réalité, bien souvent, l'information relative à l'existence et aux caractéristiques d'un projet de traitement doit être suivie d'une réponse de la personne concernée.

II – La transparence en dialogue : consentir

Suspendre la possibilité de traiter des données au bon-vouloir des personnes concernées, n'est-ce pas le cœur du concept d'autodétermination informationnelle ? Le traitement si je veux, quand je veux et jusqu'au moment où j'en aurai assez. Il n'est donc pas surprenant que le consentement soit l'un des fondements de licéité possibles des opérations sur données (art. 6 RGPD), ou qu'il permette de lever les interdictions de principe, d'une part de manipuler des données sensibles comme les opinions religieuses, l'état de santé ou l'orientation sexuelle (art. 9), d'autre part de prendre des décisions exclusivement automatisées « produisant des effets juridiques ou l'affectant de manière significative de façon similaire » (art. 22).

Il n'y aurait que des louanges à faire à cette approche, si en pratique ces consentements étaient donnés par les intéressés en pleine conscience de leurs conséquences juridiques. Or, il n'en est évidemment rien. Après avoir redécouvert le désintérêt du grand public pour les documents d'information qui lui sont proposés, le droit des données personnelles continuera à remonter les traces du droit des contrats et du droit de la consommation avec plusieurs décennies de retard, cette fois-ci en matière d'acceptation.

En ligne autant qu'ailleurs, on peut faire accepter n'importe quoi à n'importe qui. Les rédacteurs des conditions générales Amazon Web Services s'amusent toujours à stipuler, sans surprendre aucun client, «(...) cette restriction ne s'appliquera pas dans le cas (certifié par les Centres compétents des États-Unis pour le contrôle des maladies) d'une infection virale étendue transmise par des morsures ou par le contact avec des fluides corporels impliquant que des cadavres humains reviennent à la vie et cherchent à consommer de la chair humaine vivante, du sang, des tissus cérébraux ou nerveux et pourrait aboutir à la chute d'une civilisation organisée » (art. 57.10 des conditions de service AWS datées du 26 juin 2019). De plus, pour dissuader l'internaute de lutter contre sa paresse naturelle, le design constitue un instrument puissant (Laboratoire d'innovation numérique de la CNIL, cahiers IP n° 6, *La forme des choix*). *Scrolling* considéré comme une acceptation de la politique de confidentialité, boutons colorés appelant le clic face à des options grisâtres, cases pré-cochées, labyrinthes de menus, tout est fait tenir à distance la volonté véritable de l'utilisateur, au profit d'une terne résignation déguisée en volonté apparente.

Après avoir lutté pour que les politiques de confidentialité soient brèves et limpides, le RGPD et les autorités de contrôle ont trouvé là un nouveau combat : imposer que le consentement soit authentique et sincère. « Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant (...) », selon le règlement (cons. 32). La CNIL a donc sanctionné Google pour ses cases pré-cochées d'acceptation de la publicité ciblée, en dépit des messages d'avertissement plutôt clairs qui l'entouraient (délibération précitée du 21 janvier 2019).

Ainsi, les autorités de contrôle en matière de données personnelles semblent aller plus loin, dans leur recherche d'une rencontre des volontés de qualité, que les droits asymétriques comme le droit de la consommation ou des assurances, et en toute hypothèse plus loin que le droit commun des contrats. C'est que, dans ces matières, la quête d'un consentement pur et éthéré a en partie été abandonnée. Si le citoyen signe avec une relative légèreté son bail d'habitation, son prêt immobilier ou son assurance automobile, c'est parce qu'il compte sur une solide législation d'ordre public pour voler à son secours à grand renfort de dispositions d'ordre public et de clauses abusives. On peut se contenter d'un consentement de qualité médiocre, lorsque l’État a fermement fixé les cadres dans lesquels doit se couler la volonté privée.

Ces arbitrages collectifs manquent cruellement dans certains pans du droit des données personnelles. Le modèle d'affaires « service pseudo-gratuit contre *tracking* publicitaire » en constitue actuellement le meilleur exemple. Deux options sont politiquement concevables. La première : considérer ce modèle comme socialement nuisible, et l'interdire ou en limiter l'usage, quitte à ce que les utilisateurs paient à l'avenir en euros ce qu'ils réglaient jusqu'alors en exposition à des publicités personnalisées. La seconde : considérer ce modèle comme licite, et lui laisser libre cours. Les pouvoirs publics européens n'ayant pas pris position, voici la CNIL contrainte de traiter cette question comme relevant de la qualité du consentement individuel. Google, pour assurer une acceptation totalement libre, doit alors proposer ses services « gratuits » en priant humblement chaque utilisateur de bien vouloir cocher une case relative à la publicité personnalisée. Celui qui refusera en conscience, ou plus vraisemblablement parce qu'il a cliqué sur le bouton « suivant » sans lire, bénéficiera pleinement du service, mais sans subir aucun *tracking*. Qui, dans ces conditions, « choisira », de manière éclairée et sans équivoque, d'être pisté ? C'est évidemment la fin d'un modèle d'affaires, une interdiction de fait qui ne dit pas son nom.

L'avenir fournira d'autres exemples de situations, dans lesquelles on accorde une place artificielle aux arbitrages individuels. Dans ces domaines, une transparence de niveau médiocre et des consentements extorqués livreront dans un premier temps les personnes concernées aux appétits de responsables de traitement sans scrupules. Puis, un jour, si elle en a le temps et les moyens, la CNIL

y mettra de l'ordre. Sous prétexte *d'assurer des décisions individuelles éclairées*, elle prendra en réalité le relais d'une *réglementation collective défaillante* ((en ce sens, L. Aufrère et L. Maurel, « Pour une protection sociale des données personnelles », https://hal.archives-ouvertes.fr/hal-01903526 ; V. Peugeot, « RGPD : quelle place pour l'action collective ? », https://vecam.org/RGPD-quelle-place-pour-l-action-collective).

Quatrième enseignement : les contractualistes le savent depuis longtemps, l'émancipation individuelle par le libre choix est souvent une illusion. La transparence ne suffit pas. Le consentement ne peut pas tout. Faire porter aux individus l'insuffisance de la gouvernance collective est dangereux.