PAR PHILIPPE LAURIER

enseignant à l'École polytechnique

Nomadisme informatique, nomadisme des **identités** ?

ET CLAIRE DUFETRELLE (2009)

Mémoire de nos identités, de nos moyens de la confirmer, de nos habitudes, de nos mouvements : les objets intelligents ou communicants se multiplient dans notre environnement immédiat, mais aussi jusque dans notre corps ou dans l'isoloir du bureau de vote. Tandis que notre intimité numérique rétrécit à l'instar d'une peau de chagrin, il s'instaure une logique qui échappe à l'individu, alors pourtant qu'elle touche à l'individu.

Une bande dessinée d'anticipation éditée il y a une quarantaine d'années imaginait la *civilisation de l'autoroute* (en prolongement de l'ère Pompidou avec son fameux « les Français aiment la bagnole », et autres voies express sur berges) où l'être humain adoptait définitivement le camping-car, renonçait aux maisons pour devenir éternel voyageur sur des autoroutes sans fin, déléguant la production de biens aux robots. Cette bande dessinée imaginait une sorte d'ordinateur central avec lequel nous serions en correspondance pour nos affaires administratives et comptables. Parfois survenait quelque dysfonctionnement tel ce conducteur solitaire retrouvé par la police motorisée dans son véhicule, mort de faim, après que l'ordinateur eut par erreur perdu toute trace de son identité, donc de son existence, et lui eut par conséquent refusé le moindre débit bancaire, donc l'ultime moyen d'acheter l'essentiel alimentaire.

Deux points semblaient évidents au dessinateur, qui l'un et l'autre pourtant recelaient des ambiguïtés de vocabulaire.

Nous ne sommes plus le centre

Une civilisation de la mobilité qui recrée un centre

D'abord, le grand ordinateur serait central, chose banale dans l'informatique des années 1970. Sans comprendre que cette position ne tiendrait pas tant à la technique mais, par une voie détournée, au simple fait qu'en être gestionnaire vous attribue cette place stratégique. Les autres étant alors « terminaux ». Il est regrettable que nous utilisions ce mot, *terminaux*, pour désigner trivialement nos téléphones ou nos ordinateurs sans prendre conscience de son sens spatial : nous ne sommes plus le centre (peut-être ne l'avons-nous jamais été, mais en des temps où le centre ne se matérialisait pas avec sa puissance de calcul actuelle).

REPÈRES

Dans l'avant-numérique, c'est-à-dire il y a peu d'années, nous pouvions nous définir en tant qu'individus à qui il était parfois demandé de justifier de leur identité, souvent par le recours à une carte ou à un certificat dont nous serions alors porteur, dûment agrémenté de coups de tampons ou de filigranes ; nous étions l'*alpha* et l'*oméga*, l'existant et sa preuve (les registres paroissiaux ou administratifs traçaient des chronologies et des filiations mais ne constituaient pas de véritables supports d'identification pour l'immédiateté). Demain, il nous sera demandé de correspondre à une identité préenregistrée, mais désormais vivante hors de nous, binaire. Binaire car inscrite sur mémoire informatique. Vivante car en croissance, faite d'ajouts tantôt par des données personnelles, y compris biométriques, tantôt par notre profil comportemental qui est partie prenante de notre identité globale, avec nos préférences, nos déplacements journaliers, nos adresses.

Contrôle d'identité

Google ou Facebook rivalisent de discrétion pour placer des pions dans les secteurs technologiques de la biométrie ou de la reconnaissance faciale, à coup de rachats si besoin, tel que l'an passé celui de la jeune entreprise PittPatt (Pittsburgh Pattern Recognition), essaimée en 2004 de l'université Carnegie Mellon.

Ensuite, chaque voyageur se trouverait en correspondance avec cet ordinateur, au sens de dialogue administratif, par ce terme de correspondance désignant un courrier. Or *correspondance avec l'ordinateur* renverra dans les faits à une seconde acception du mot : être *en conformité avec*.

Être nomadisé, être en conformité

Sur un mode plus humoristique que dramatique, cette bande dessinée se livrait à ce que l'on supposait à l'époque être caricatural, simple exercice intellectuel, du sous-Orwell. Pourtant, elle dressait par avance le constat majeur que l'être nomadisé – avec ses téléphones mobiles, son PC portable, ses tablettes électroniques, ses puces RFID de métro – se trouve en partie dépossédé de la gestion de son identité. Laquelle échoit à une ou plusieurs autorités privées ou publiques, commerciales souvent, qui nous connaissaient initialement par un identifiant et un authentifiant (un mot de passe par exemple). Mais qui progressivement, au motif d'une insécurité qu'elles sont du reste parfois les premières à avoir créée ou à tout le moins tolérée, nous expliquent que notre sécurité impliquera davantage de délégation du contrôle sur notre identité, avec la biométrie ou avec la reconnaissance faciale.

Être copie conforme de notre propre copie

L'axe suivi par cette trajectoire technologique est l'obligation progressive de prouver que l'on est soi, mais par le contresens de devoir montrer que l'on correspond à ce qu'une base de données connaît de nous : notre ADN, notre iris est-il conforme à la mémoire numérique, notre visage est-il tel que répertorié ? Ce n'est plus la mémoire qui doit correspondre à la réalité, mais bien nous, réels, qui devons être similaires en tout point à notre propre identité clonée et virtuelle.

Une seconde contradiction tient à l'effet de mode autour des télécommunications, où nous nous proclamons soudainement nomades alors que la « mémoire de nous » reste grandement statique, hébergée sur des fermes de serveurs. Elle est sédentaire, oserait-on dire. Vieille lutte qui renvoie aux origines du néolithique, mais où le vainqueur final est généralement le sédentaire, c'est-à-dire pour l'occasion le propriétaire des ordinateurs (pour nos données archivées, la traduction en bon français du concept marketing de *cloud* serait « écran de fumée » plutôt que « nuage »).

Localisation géographique

Outre les dispositifs de reconnaissance biométrique intervient la localisation géographique. En 2011, deux chercheurs ont montré que l'iPhone stockait des données récoltées sur nos déplacements géographiques, sans que l'utilisateur en ait été informé. Dans une étude menée peu après, la CNIL – Commission nationale de l'informatique et des libertés – précisait que « l'observation du téléphone pen- ➤

Voiture indiscrète

On se souvient de cette mésaventure en Malaisie d'un propriétaire de grosse cylindrée allemande équipée d'un système antivol par lecture d'empreinte digitale, dont les voleurs auraient pris soin de couper le doigt pour activer le démarrage. Depuis lors, la recherche allemande s'attelle à déterminer si un doigt qui est présenté au coupe-circuit revêt ou non les caractéristiques d'un tissu vivant. De même, plusieurs constructeurs automobiles achèvent de mettre au point des sièges bardés de capteurs et aptes à détecter un endormissement ou un malaise. Chose qui intéressera à terme les assureurs. Avec pour capacité collatérale tôt ou tard de pouvoir identifier un conducteur par divers signes physiologiques, dont son rythme cardiaque, propre à chacun. Performance à portée de main et qui fera naître des envies d'antivols ou mille autres usages, car on saura le qui, le où et la vitesse. Un jour peut-être aussi le « avec qui » si le siège passager bénéficie de la même instrumentation.

L'être nomadisé se trouve en partie dépossédé de la gestion de son identité

dant plusieurs nuits a permis de découvrir que l'iPhone contacte les serveurs de géolocalisation d'Apple ponctuellement sans aucune intervention de l'utilisateur, dès lors qu'il est allumé et connecté à un point d'accès Wifi ». Recours potentiels à la localisation dont il est à craindre donc qu'elle s'accomplira non seulement sur l'instant, mais également par une trace conservée de nos précédents itinéraires : je suis Untel car présent ici et passé par là, sans usurpation car toujours resté sous l'œil ; veuillez donc autoriser mon actuel paiement électronique dans cette boutique. Les paiements par nos téléphones portables répondront peu à peu à cette logique.

Dérives du télépaiement

La prochaine étape est effectivement la monnaie, *via* le paiement depuis nos terminaux mobiles : monnaies publiques ou nouvelles monnaies privatives proposées par les réseaux sociaux, avec de leur part un désir de présenter ces monnaies qui sont leur propriété comme plus sécurisées car émises et validées sur leur univers virtuel où nos identités sont peu à peu présentes – ces acteurs économiques deviennent l'*alpha* et l'*oméga* que nous ne sommes plus. La traditionnelle carte à puce était en comparaison plus discrète, qui certes indiquait où nous – par notre authentifiant – nous trouvions à un moment donné – par le terminal de paiement –, mais qui n'avait pas le moyen ni le besoin de savoir nos pérégrinations entre-temps. Certains paiements sur Internet, y compris depuis nos terminaux fixes, ne conservent d'autorisation que si notre téléphone mobile confirme que nous sommes bien au même instant au lieu déclaré. En attendant une couche supplémentaire qui nous demandera de prouver à notre propre téléphone et à ses capteurs que nous sommes nous, tels qu'enregistrés par la grande mémoire sédentaire.

Les objets intelligents, entre devoir de mémoire et droit à l'oubli

Mémoire de nos identités, de nos moyens de la confirmer (depuis le mot de passe jusqu'à la génétique), de nos habitudes, nos mouvements : les objets intelligents ou communicants vont se multiplier dans notre environnement immédiat, notre maison, notre voiture, mais aussi des lieux aussi intimes que notre corps (capteurs à usage médical) voire l'isoloir du bureau de vote.
Ces objets intelligents vont dialoguer sans nécessairement requérir notre autorisation. Qui sera le réceptionnaire, l'héritier et le gestionnaire de cette masse de données intimes ?

Les objets intelligents vont dialoguer sans nécessairement requérir notre autorisation

Une intimité en forme de peau de chagrin

Notre intimité numérique s'apparente à une peau de chagrin, rétrécissant non pas du fait des technologies mais de l'usage qu'on en permet. Les récentes cartes de transport pour les abonnés du métro ne nous démentiraient guère, qui de manière fréquente nous connaissent conjointement à travers notre identité, notre photo numérisée archivable, un paiement mensuel usuellement effectué par carte bancaire, et nos récents passages aux bornes. À nouveau la CNIL s'était émue de ce que la RATP ait, lors de son lancement en 2009, fait bien peu de publicité au Navigo Découverte, l'équivalent anonyme du Passe Navigo ; dont la délivrance était quant à ce dernier gratuite, tandis que la version anonyme était facturée 5 euros. Il s'agit là de choix volontaires.
Au nom officiellement d'une bonne gestion de la relation au client, à des fins publicitaires, policières ou autres, s'instaure une logique qui échappe à l'individu, alors pourtant qu'elle touche à l'individu. ■

Les vraies pratiques de Google

Alex Türk, président de la CNIL, s'était dit « inquiet de ce qu'un célèbre moteur de recherche soit capable d'agréger des données éparses pour établir un profil détaillé de millions de personnes (parcours professionnel et personnel, habitudes de consultation d'Internet, participation à des forums…) », proclamation qui date de 2007. En 2012, lorsque la même entreprise annonce lancer la refonte de sa « politique de confidentialité » en croisant plus de données issues de son moteur de recherche, de la messagerie Gmail et du site de vidéo Youtube, la CNIL déclare à propos de « la formulation des nouvelles règles et la possibilité de combiner des données issues de différents services » qu'elles soulèvent « des inquiétudes et des interrogations sur les pratiques réelles de Google ».

Le vote électronique, ou l'improbable mariage de la transparence et du secret

© JEAN-CHRISTOPHE JARDIN

Boîtiers individuels de vote électronique à l'Assemblée nationale française.

Le vote électronique, ou e-vote, pose la question de la faisabilité d'un vote sûr. Il recouvre :
– le vote à domicile, sur ordinateur, *via* une plate-forme sur laquelle chacun s'identifie, choisit le candidat et valide son vote. Ce vote à distance n'est pas entièrement fiable au niveau technique, car il n'existe pas de système parfaitement robuste aux infections. De plus perdure une difficulté inhérente à l'utilisation d'ordinateurs personnels puisqu'il est impossible d'établir un lien sécurisé entre le terminal du réseau physique et le dernier maillon qu'est l'utilisateur humain. Faute d'authentification par pièce d'identité, deux options demeurent : utiliser une information connue uniquement de la personne ou utiliser une donnée biométrique. Cependant aucune d'elles n'est satisfaisante : la première permettrait de voter pour autrui en connaissant son information secrète (avec risque d'extorsion par la force) et la deuxième sous-tend la possession par l'institution étatique d'un fichier exhaustif des données biométriques ;
– les machines pour recueillir les suffrages des votants qui se déplacent jusqu'au bureau de vote. Leur unique avantage est de permettre un dépouillement plus rapide, or cette même étape constitue un point faible. Pour que la machine soit utilisable, il importe qu'elle soit scellée mais, à l'image de l'urne transparente[1], que son fonctionnement soit visible de tous. Dans les faits, cela reviendrait à créer des appareils dont le code soit lisible par tous, consultable sur demande. Un premier problème est qu'il n'est pas possible de s'assurer soi-même du fonctionnement de la machine : « l'urne » n'est pas transparente. Une conséquence de cette opacité est que nul ne peut être certain que son vote ait été correctement enregistré. Quand bien même émettrait-elle un reçu en papier, il n'est pas assuré que celui-ci reflète ce qui existe dans la mémoire de l'ordinateur. Dans le dépouillement électronique, le comptage des voix se fait de manière opaque envers l'humain. Même un homme connaissant (et comprenant) le code de la machine ne peut être garant qu'elle donnera le résultat exact, et une erreur informatique demeure possible[2]. De même qu'existent des sources de fraude.
De plus, le choix de l'équipe vérificatrice est d'ordre politique : comment la choisir pour donner confiance à tous ? Comment s'assurer que la machine sera bien configurée et pas modifiée avant le scrutin ?
Un cas intéressant est fourni par les Pays-Bas. Alors que la quasi-totalité des votes se déroulait sur machines à voter, une commission mise en place pour étudier la question a prouvé la trop grande possibilité de fraude[3]. Finalement le vote électronique a été abandonné en mai 2008. Décision principalement motivée par le fait que la machine ne produit aucune preuve papier permettant de vérifier que le vote enregistré correspond à la volonté du votant.
De surcroît, selon cette commission, le secret du vote ne peut être garanti. Un paradoxe est résumé ici, d'une machine dont on attend de la transparence mais tout en nous garantissant le principe du secret, et dont on attend une preuve du fidèle enregistrement de notre vote mais tout en nous garantissant que cette trace restera confidentielle.
La suppression du caractère humain de la procédure empêche le citoyen de se forger l'intime conviction qu'elle reste juste, que ce sont bien des hommes libres et conscients qui choisissent leurs représentants par une voie éprouvée, et renouvelée à travers le temps. L'outil informatique doit rester sous l'égide du sens critique.

Le secret du vote électronique ne peut être garanti

1. Le code électoral spécifie que l'urne doit posséder au moins quatre côtés transparents.

2. Se référer au fameux théorème de Gödel et aux travaux de calculabilité de Hilbert, qui prouvent l'impossibilité de montrer qu'un programme informatique renvoie la réponse exacte en un temps fini.

3. Commission Korthals-Altes, 2007.