SYNTHÈSE DE DOSSIER

Sur la Learning Box, sont disponibles : le public concerné par l'épreuve, la méthode, le programme de révision, la bibliographie et les annales des concours précédents. Accès via votre espace candidat sur www.passerelle-esc.com

▸ DURÉE : 2 HEURES

CONSIGNE :

À partir des seuls documents ci-joints (présentés dans ce dossier par ordre chronologique), tous les candidats doivent rédiger une note de synthèse de 3 pages maximum.
Il est rappelé que la synthèse doit mettre en évidence les idées essentielles du dossier, sans aucun ajout personnel, dans le cadre d'un ***PLAN aux structures apparentes*** *(1ère partie : titre – A : titre – B : titre…) traduisant une démarche réfléchie sur l'ensemble des éléments du dossier. Chaque fois qu'un candidat dans sa synthèse se réfère à un ou plusieurs documents du dossier, il doit citer entre parenthèses le ou les numéros du ou des documents concernés (ex. : doc. 1 ou doc. 3,4).*

Sujet : LA VIE PRIVÉE

Doc. 1 : « Entre liberté d'informer et secret de la vie privée » (*La vie privée à l'heure des médias,* 2002)

Doc. 2 : « La protection de la vie privée est « insuffisante » sur Internet » (*Le Monde*, 2010)

Doc. 3 : « Exploitation des données personnelles » (*Économie des données personnelles et de la vie privée*, 2010)

Doc. 4 : « La vie privée googlisée » (*Sciences humaines*, 2011)

Doc. 5 : « Facebook, GPS, smartphone : comment concilier collecte de données et vie privée » (*Le Monde*, 2012)

Doc. 6 : « Les médias sociaux dans les stratégies de recrutement » (*Revue française de gestion*, 2012)

Doc. 7 : « Contre l'hypothèse de la fin de la vie privée », (*SFIC*, 2013)

Doc. 8 : « Les États-Unis veulent protéger la vie privée » (Entretien de John Podesta, conseiller du président Barack Obama *Le Monde*, 2014)

Doc. 9 : « La déconnexion aux outils de géolocalisation » (*Réseaux*, 2014)

Doc. 10 : « Protection des données personnelles : l'Europe avance lentement » (*Le Monde*, 2014)

Document 1

Entre liberté d'informer et secret de la vie privée

Il a fallu attendre des années pour que la vie privée soit reconnue comme un droit fondamental de l'individu. Longtemps, l'espace public et politique a été valorisé au détriment de l'espace privé. L'un semblait devoir accueillir tous les talents et toutes les vertus alors que l'autre était suspecté d'abriter les plus grands vices et de cacher toutes les turpitudes. Toujours est-il qu'aujourd'hui, la liberté d'information et d'expression doit s'arrêter aux frontières de la vie privée. Les compromis sont-ils convenablement réalisés ? Faut-il mettre en place de nouvelles institutions ? Les règles déontologiques du journalisme sont-elles suffisantes ?

Hubert Beuve-Méry, le fondateur du journal *Le Monde*, estimait que «l'on n'a pas le droit de dire n'importe quoi, n'importe où, n'importe quand et n'importe comment parce qu'il peut y avoir des conséquences». Les médias ne peuvent pas tout dire et tout montrer ; la liberté d'information doit s'arrêter notamment au mur de la vie privée. Ce mur n'est cependant pas une barrière infranchissable. Dès lors, que l'individu y consent ou dès lors qu'il existe un intérêt public, il est possible de divulguer des informations personnelles de nature confidentielle. Le fait d'être atteint d'une grave maladie ne regarde que le malade ; il en va différemment si cette maladie concerne le chef de l'État. Tous les grands textes qui reconnaissent la liberté d'expression marquent des limites, comme l'article 11 de la Déclaration des droits de l'homme de 1789 ou l'article 10 de la Convention européenne de 1950. Il en va de même pour la protection de la vie privée. Ainsi, la directive européenne sur la protection des données de 1995 prévoit des exemptions et des dérogations pour les traitements mis en oeuvre à des fins de journalisme, d'expression littéraire ou artistique.

Un double mouvement contradictoire

Au cours des dernières décennies, on observe un double mouvement contradictoire. Le développement des médias et des techniques de communication s'est accompagné de violations de plus en plus nombreuses du droit à la vie privée. Dans le même temps, on a eu le souci de mieux formaliser et de mieux protéger ce droit, grâce à la création de normes et d'institutions nouvelles. Si la liberté d'expression est reconnue dès la fin du XVIII^{ème} siècle, il faut attendre la Déclaration universelle des droits de l'homme de 1948 pour voir affirmer le principe d'une protection de la sphère privée. En France, c'est une loi de juillet 1970 qui consacre cette protection. La liberté d'information a toujours été présentée comme une exigence démocratique fondamentale. Un pays où la presse est muselée n'est pas un pays démocratique. En disant la vérité et en faisant apparaître les mensonges de pouvoirs en place, les médias constituent un contrepouvoir. Surtout, ils permettent aux citoyens de se former un jugement et participent ainsi à la construction d'une opinion publique. L'intérêt démocratique du droit à la vie privée est moins évident. Ce droit a pu apparaître en effet comme un encouragement donné à l'individualisme contemporain et comme une possibilité pour une minorité de nantis de cacher leurs privilèges. On considère de plus en plus aujourd'hui que ce droit constitue une base essentielle de la citoyenneté. Plus qu'un retrait de la vie publique, il en constitue un préalable permettant d'éviter les discriminations et les manipulations de toutes sortes. Sans secrets de l'individu, il n'y aurait pas d'individu et tous les régimes totalitaires ont toujours oeuvré dans le sens d'une plus grande transparence.

Entre deux libertés essentielles qui s'opposent, il n'y a pas de hiérarchie à établir.

Jamais une liberté ne doit l'emporter clairement sur l'autre, et l'on doit effectuer des pondérations selon les situations. Pour réaliser dans les meilleures conditions cette balance des intérêts, on peut établir la liste des différents cas où l'intérêt public exige de limiter la protection de la vie privée ou, inversement, les cas où celle-ci ne souffre d'aucune exception. Par exemple, la diffusion de la photo d'une personne sur son lit de mort ou la photo d'une personne menottée. La pondération est de toute façon toujours difficile et, pour reprendre l'exemple de la photo de presse sur la détresse humaine, il existe une frontière imperceptible entre la volonté de témoigner et le voyeurisme.

A la recherche d'un juste équilibre

Le thème de réflexion le plus important concerne la recherche d'un juste équilibre entre deux droits opposés. Cette recherche est toujours délicate et rarement satisfaisante. On peut estimer que la balance des intérêts penche soit en faveur du droit au respect de l'intimité, soit au contraire en faveur de la liberté d'expression. Ainsi, certains estiment que, depuis la loi sur la presse de 1881, la liberté d'information a été constamment limitée par les différentes mesures prises pour protéger la vie privée. La grande sévérité d'application de ces textes par le juge aggrave la situation et entraîne une grande insécurité juridique.

Une approche comparative montre que la France est le pays où la vie privée est la mieux protégée. La liberté d'expression est moins contrainte dans des pays comme la Grande-Bretagne ou les États-Unis. Cette liberté n'est pas sans limite mais ses abus y sont mieux tolérés. On estime finalement que c'est la démocratie qui sort gagnante d'une expression la plus libre possible. Au début du XX^{ème} siècle, le grand journaliste américain Joseph Pulitzer invitait ses collègues à dévoiler tout, parce que, disait-il, « tôt ou tard, l'opinion publique s'en débarrassera ». A l'opposé de cette position, on peut considérer que la balance des intérêts néglige par trop le droit de l'individu à voir sa vie privée respectée.

La fin de la vie privée ?

Devant l'ampleur des agressions et les énormes possibilités offertes par les nouvelles technologies, on annonce même la fin de la vie privée. Est ici présenté un argumentaire particulièrement convaincant. Tout d'abord, la liberté d'expression ne doit pas être confondue avec la liberté du commerce. En effet, dans la plupart des cas, la logique dominante et parfois exclusive des médias est une logique commerciale. Si la vie privée est dévoilée, ce n'est pas à cause de l'intérêt public, mais bien pour satisfaire le voyeurisme et la soif du sensationnel du public. Les nouvelles technologies permettent de suivre dans le même temps l'individu à la trace. On bénéficie sur internet d'une totale liberté d'expression, mais tout ce que nous exprimons est enregistré, pour le plus grand profit des marchands. Par ailleurs, le droit à la vie privée est d'autant plus menacé que les individus ne se mobilisent pas suffisamment pour le faire respecter. Ils ne voient pas que les technologies de la communication sont aussi des technologies de contrôle.

Document 2

La protection de la vie privée est «insuffisante» sur Internet

Une majorité des Français, 71 %, jugent la protection de la vie privée sur Internet « insuffisante », selon un sondage IPSOS réalisé au début du mois d'octobre pour la Commission nationale de l'informatique et des libertés (Cnil). Réalisé par téléphone

auprès d'environ 940 personnes âgées de 15 ans et plus, le sondage précise également que les Français sont même 37 % à juger le niveau de protection «pas du tout» satisfaisant. Gros consommateurs d'Internet, les jeunes de 18 à 24 ans, se révèlent un peu plus soucieux que les autres, commente la Cnil. Ils sont 78 % à juger la vie privée insuffisamment protégée sur Internet, « une défiance qui ne semble pas les détourner d'internet », commente la commission.

L'enquête d'opinion fait par ailleurs apparaître que pour 61 % des personnes interrogées, l'existence de fichiers est perçue comme une atteinte à la vie privée. 50 % des sondés ont des craintes concernant l'utilisation des fichiers de l'État ou privés. Pour débattre de la protection des données personnelles, la Cnil participera avec ses homologues des pays de l'Union européenne à une conférence mondiale organisée, au Conseil de l'Europe, sur le thème de la « protection de la vie privée dans un monde sans frontières ».

Document 3

Exploitation des données personnelles

Lerespect de la vie privée constitue un débat relativement ancien en philosophie, remontant au siècle des Lumières avec l'idée d'émancipation de l'individu face à la société. De son côté, le questionnement économique, beaucoup plus récent, apparaît avec l'exploitation des données personnelles (DP) permise par le développement de l'informatique puis de la télématique. Un certain nombre de travaux d'économistes aux États-Unis, notamment de l'école de Chicago, ont ainsi été publiés à partir des années 1970 pour discuter le bien-fondé économique de la protection légale de la vie privée (*privacy*).

Avec le développement des réseaux numériques fixes et mobiles, ce débat est sorti du milieu des experts et du champ académique pour se faire connaître du grand public et devenir un enjeu sociétal dans le contexte de l'économie numérique. Les technologies de l'information et de la communication (TIC) ont permis en effet de réduire considérablement les coûts de collecte, de stockage et de traitements des données personnelles. La collecte prend des formes très variées allant des données de consultation de pages Web à la géolocalisation par téléphone portable.

La numérisation de ces informations permet la constitution de bases de données et leur traitement automatisé à des fins très différentes : maintien de l'ordre public, personnalisation de services marchands ou non marchands, profilage des consommateurs ou des candidats à un emploi, contrôle des activités politiques et syndicales des individus, appel à la délation, contrôle des migrants et des voyageurs, services de mobilité, prospection commerciale, *spamming*, escroquerie en ligne et autres utilisations malveillantes. Par sa diversité et son impact social, l'exploitation des données personnelles donne lieu à un vaste débat public mêlant craintes, espoirs et spéculations de toutes sortes.

Les partisans de la libre exploitation des données personnelles s'opposent ainsi aux défenseurs du respect à tout prix de la vie privée. Les premiers soulignent les bienfaits des modèles économiques fondés sur l'utilisation des données personnelles qui concourraient à la croissance économique et au bien-être social : personnalisation de l'offre, marketing mieux ciblé, services de mobilité, meilleurs ajustements sur les marchés des biens de consommation, mais également du travail, de l'assurance, du

crédit, des services matrimoniaux, etc. Les seconds dénoncent les risques d'intrusion dans la vie privée et de menace de libertés individuelles, les données personnelles pouvant être exploitées à d'autres fins que le bien-être des individus. Ils estiment ainsi qu'Internet, la biométrie, la géolocalisation ou encore les puces RFID menacent nos vies privées à un niveau jamais atteint jusqu'à présent : surveillance, invasion de l'espace intime, etc.

Document 4

La vie privée googlisée

Mis au point au Cern (Organisation européenne pour la recherche nucléaire) en 1990, le *World Wide Web*, couplé à l'ordinateur personnel, allait donner naissance à ce que l'on appelle aujourd'hui indistinctement l'Internet, la Toile ou le Web : 1,5 milliard d'utilisateurs en 2008, et 131 350 milliards de recherches sur les principaux moteurs en 2009. Avant même d'atteindre ces chiffres, le Web n'a pas tardé à soulever toutes sortes de réflexions prospectives, dont les plus remarquées relevaient, dans les années 1990, de l'utopie collective. Positive, chez un Pierre Levy qui y voyait l'annonce d'une sorte d'immense cerveau dématérialisé à venir, une « intelligence collective » capable d'introduire une rupture de civilisation par l'accès de tous au savoir et à l'expression politique directe. Négative, chez un Paul Virilio qui qualifiait de « bombe informatique » l'extension des réseaux télématiques capables d'engendrer des krachs boursiers en lieu et place d'un sujet humain désormais inexistant.

Dix ans plus tard, le Web 2.0, c'est-à-dire l'interactivité à la portée de tous, est passé par là. Internet suscite aujourd'hui des inquiétudes plus centrées sur la personne même de ses usagers, que certains accusent - pour les plus accros - de sombrer dans l'addiction et l'autisme. Mais il y a surtout des risques plus partagés. Ils résultent d'abord d'années d'usage, au cours desquelles l'Internet a fait preuve de trois aptitudes inédites : une capacité de stockage quasi illimitée, une interconnectivité croissante avec toutes sortes de systèmes de données numériques, et une confidentialité pour le moins défaillante, quand elle n'est pas totalement absente. D'où la naissance de nouvelles alarmes, que les spécialistes subsument sous l'étiquette « exploitation des données personnelles ».

Exemple : un habitant de Los Angeles, Roberto Rivera, fait ses courses dans un supermarché et glisse sur un pot de yaourt tombé du rayon. Il se casse un genou, et porte plainte contre le magasin. Les avocats de celui-ci font valoir que les données de sa carte de fidélité mentionnent de fréquents achats d'alcool : n'était-il pas saoul le jour de sa chute ? Le cas n'implique pas le Web mais illustre les capacités de traçage constant, discret et pratiquement insensible des systèmes numériques auxquels nous avons affaire tous les jours. Or, l'Internet en est, en quelque sorte, le cerveau central où s'accumulent, transitent et peuvent se recouper toutes les traces et informations que nous y laissons plus ou moins volontairement.

La fin de la vie privée ?

Certaines, comme les adresses de sites que nous visitons, sont conservées par les fournisseurs d'accès et servent au profilage publicitaire et au marketing ciblé : la nuisance (le spamming) reste mineure. Mais il y a plus délicat : le succès des réseaux sociaux (Facebook, Myspace, Twitter, etc.), des blogs, des sites communautaires et des forums met quantité de données sensibles à la disposition d'observateurs pas toujours prévisibles. Plus grave encore : imaginons que nos transactions, nos déplace-

ments, nos loisirs, nos fréquentations, nos données de santé - normalement cloisonnées - puissent se retrouver agrégées et transparentes ? C'est la fin de la « vie privée ». Les débats qui entourent ces perspectives vertigineuses de profilage et de surveillance sont aujourd'hui de deux ordres: philosophiques et juridico-techniques.

Sur le fond, certains idéologues radicaux renvoient tout simplement la notion de vie privée au vestiaire. Le juriste américain Richard Posner, par exemple, considère que toute confidentialité est le paravent d'une intention de fraude ou de tromperie : rien ne la justifie ni moralement ni socialement. C'est l'argument des « gens honnêtes » qui n'ont « rien à cacher ». En plus soft, l'économiste George Stigler (prix Nobel 1982) a défendu l'idée que la protection des données personnelles était un obstacle à l'efficience du marché, à l'adéquation de l'offre et de la demande : l'État n'a donc pas de raison de s'y intéresser. L'un comme l'autre privilégient les intérêts des entreprises sur ceux des individus, ce qui est une forme d'utilitarisme. Mais la majorité des penseurs libéraux, et même libertariens comme David Friedman, défend au contraire que la protection de la vie privée est un aspect essentiel de la liberté individuelle, et donc un ingrédient indispensable de la démocratie : l'expérience montre que la surveillance généralisée est une pratique des régimes totalitaires. Le droit à défendre sa vie privée est la garantie de l'autonomie individuelle. Elle peut avoir aussi d'autres justifications, comme celle que donne le journaliste Jean-Marc Manach : la vie privée est le lieu où s'exerce une morale librement consentie. C'est donc le modèle d'une vie publique qui ne soit pas seulement fondée sur la crainte du châtiment. Selon le juriste Daniel Solove, enfin, la destruction de la vie privée ruine la confiance que nous pouvons avoir dans la société.

Transparence ou bouclier ?

Reste qu'en la matière, les pratiques s'imposent sans que l'on consulte les philosophes. Du côté des États et des autorités policières, les raisons de sécurité, de protection de l'enfance et des droits d'auteurs permettent une extension graduelle de la surveillance des réseaux, du recueil d'informations et du croisement de données. Les limites que les États s'imposent à eux-mêmes, à travers la Cnil par exemple, offrent une fragile défense des libertés individuelles dont les particuliers ont beaucoup de mal à faire usage. Du côté des acteurs économiques, le cynisme est fréquent. Selon Scott McNealy, PDG de Sun Microsystems, la vie privée, c'est dépassé, nous n'en avons déjà plus, tandis que celui de Google explique, en 2009, à peu près la même chose : « Si vous avez quelque chose à cacher, le mieux est de ne pas le faire. » En réalité, il y a beaucoup à faire, et la solution, aux yeux de bon nombre de spécialistes du Web, comme Daniel Kaplan ou Fabrice Rochelandet, c'est la prise en main de sa propre sécurité par l'usager. Car les dispositifs existent, mais - et le paradoxe n'est pas mince - sont en pratique ignorés par les internautes. Un sondage européen révélait en 2008 que la majorité des jeunes usagers, tout en se méfiant profondément des entreprises et de l'État, n'hésitait pas à leur abandonner toutes sortes de données sensibles sans la moindre précaution.

Pourtant, les solutions existent et se partagent en plusieurs doctrines. L'une, c'est la transparence totale : si en effet tous les acteurs - institutions comprises - révélaient à tous tout ce qu'ils font, la symétrie des informations (outre leur masse énorme) rendrait leur usage inopérant. Une telle idée, évidemment, relève de l'utopie. Plus réaliste, le principe du bouclier adopte le point de vue inverse : celui de l'anonymat réel et du secret pour l'usager. Il existe d'ores et déjà des logiciels d'effacement des traces et de cryptage des données dont (encore une fois paradoxalement) les internautes ne font pas usage. Pourquoi ? Par sous-évaluation du risque, par ignorance et,

tout simplement, parce que ces dispositifs contredisent la fonction de communication et de sociabilité du Web : ils ont donc des limites assez évidentes. Une troisième voie consiste à durcir les normes de propriété des données personnelles : nul ne pourrait en faire usage sans le consentement (et la rémunération) du propriétaire des données, qui de plus aurait droit à l'effacement et à la correction. Mais les solutions techniques restent à inventer... et l'idée vient sans doute un peu tard.

Document 5

Facebook, GPS, smartphone :
comment concilier collecte de données et vie privée

Depuis maintenant deux décennies, nous pianotons sur nos ordinateurs, téléphones, smartphones et, désormais, tablettes. Plus de huit internautes sur dix dans le monde sont membres d'un réseau social. Les plus branchés - 200 millions de personnes selon ComScore, spécialiste de la mesure d'audience sur Internet - tweetent informations et états d'âme en temps réel. Timidement ou avidement, nous échangeons des mails intimes ou professionnels, nous parlons de tout au téléphone, dans la rue ou dans les transports en commun, nous suivons en voiture les instructions d'un GPS, nous multiplions les applications sur nos smartphones... Et le plus souvent, nous acceptons les conditions générales d'utilisation de ces nouveaux outils sans même les avoir lues. Or, cette acceptation vaut souvent sésame pour partager des données dont nous ne soupçonnons même pas l'existence.

Le volume des données double tous les dix-huit mois

Toutes ces informations sont des données numériques rassemblées dans des « big data », des bases de données gigantesques. Le volume de ces données sur la planète double tous les dix-huit mois, et rien qu'en 2011 il s'en est stocké plus qu'entre le début du XX^{e} siècle et 2010. Et si de grosses machines réussissaient à tout avaler, digérer, analyser, interpréter ? Il deviendrait alors possible de connaître et prévoir la circulation dans les villes, nos déplacements, nos attitudes de consommation, nos centres d'intérêt et même nos opinions... Vous ne rêvez pas, c'est déjà le cas, ou presque. Ce traitement statistique massif est rendu possible par des «clouds», mot poétique (nuage, en anglais) qui désigne de grandes fermes informatiques situées un peu partout sur le globe et capables de tout stocker à la demande. Et l'exploitation statistique de cette masse d'informations, qui concerne un huitième des habitants de la planète, fait fantasmer le monde économique.

Les premiers exemples d'utilisation des « big data » illustrent le champ des possibles. Plus rapide que les données de terrain de l'Organisation mondiale de la santé (OMS), l'outil gratuit Google Flu Trends suit « *quasi en temps réel la propagation mondiale du virus de la grippe en se fondant sur les requêtes des internautes* », explique Johanna Wright, chef de produit pour Google. L'application Google Insights for Search permet, elle, de visualiser, mois après mois, les intérêts des internautes, rien de moins. Les résultats peuvent être affinés par pays, et Google suggère même quelle pourrait être la tendance future. Ce n'est qu'un début. C'est justement sur la circulation automobile que le traitement des « big data » vient d'apporter sa première contribution d'ampleur : nous comprenons mieux désormais comment les bouchons se forment et se résorbent. Une belle avancée, alors que 80 % des émissions de CO_2 proviennent des zones urbaines.

« Vous n'êtes pas le consommateur : vous êtes le produit vendu »

L'engouement planétaire pour les smartphones - en 2011, leurs ventes, avec celles des

tablettes, ont dépassé celles d'ordinateurs - dope les recherches. Ces petites machines en savent long sur nous. Les géants (Facebook, Google, Apple, IBM, Nokia, etc.) comme les petites entreprises inventives convoitent l'exploitation de ces données à des fins commerciales : modèles prédictifs sociétaux, ciblage marketing des consommateurs pour leur proposer des produits adaptés, des services innovants. Comment estimer de telles richesses ? Difficile à dire, même si la valeur boursière annoncée de Facebook indique les sommets auxquels les marchés les évaluent. Alexandre Bayen a justement été mandaté par les pouvoirs publics américains pour estimer leur valeur. Comme le résume le blogueur américain Andrew Lewis, « *si vous ne payez pas un service sur le Net, c'est que vous n'êtes pas le consommateur : vous êtes le produit vendu* ».

Des moyens « efficaces » pour sonder les foules

Et les recherches se poursuivent. Nouvelle corne d'abondance : les réseaux sociaux et la masse d'informations privées, miroir de nos personnalités, qu'ils véhiculent. « *Le Web 2.0 est dépassé, nous en sommes au Web social* », commente Alexandre Bayen, de l'université de Berkeley. IBM cherche à exploiter « *les données non structurées* », c'est-à-dire tout ce qui ne rentre pas facilement dans des cases : vidéos, blogs, tweets ou SMS produits par chacun de nous. La finalité ? Proposer des services innovants et rémunérateurs. IBM entend saisir le sens des « *250 millions de tweets quotidiens qui sont autant d'instantanés des intérêts de notre société* », ajoute Rick Laurence. Le scientifique reconnaît avoir été contacté par des équipes de politiciens américains cherchant des moyens « *efficaces* » pour sonder les foules. En clair, la période est excitante pour les scientifiques : ils disposent d'informations qu'il était autrefois inimaginable de récolter . « *Nous entrons dans une société transparente* », a prévenu le sociologue Bernard Cathelat. Une transformation sociétale à deux facettes. « *Un côté « godfather », parrain nous voulant du bien, un côté « big brother » qui contrôle.* »

La finalité marketing de ces études statistiques concentre les craintes, notamment celles de voir se créer un monde étouffant où l'individu se verra offrir des offres commerciales personnalisées au bon endroit, au bon moment, à chaque instant. « *Le risque est que cette stimulation incessante sature nos sens*, estime Frédéric Mazella, créateur de covoiturage.fr. *Nous risquons de perdre une partie du temps précieux que nous avons pour explorer de nouvelles idées.* » Pour Laurent Maruani, responsable du département marketing d'HEC, « *ce sera une façon d'occuper les masses à faible coût. Des loisirs, des stimulations bien choisis seront distribués. Le luxe sera de retrouver du temps et de l'espace* ».

Le philosophe François Ewald reconnaît qu'il y a là l'émergence d'un instrument de savoir et de pouvoir. Deux visions s'opposent. « On imagine la possibilité d'un surpouvoir, un univers à la *1984* (le roman de George Orwell), explique-t-il. Mais on peut avoir une autre vision : celle d'un univers de données qui ne renforce pas les centres mais les détruit. Une société où chacun est destinataire d'une multitude d'informations. Où la transparence peut aussi donner des actes de rébellion, type WikiLeaks », ce site qui a mis en ligne en 2010 des milliers de documents militaires américains secrets sur la guerre en Afghanistan et en Irak. Grâce à Internet, en effet, chaque habitant de la planète a le même outil pour se faire entendre. Comme le démontre l'essor international d'Anonymous, ce collectif cybermilitant qui défend les droits à la liberté d'expression. Ou encore l'utilisation massive de Facebook et des blogs dans les révolutions tunisienne, égyptienne et libyenne. Comme le démontre aussi l'acharnement du pouvoir syrien à faire taire les insurgés dont des bribes de témoignages surgissent encore par écrans interposés.

Nos données personnelles ne connaissent plus de frontières

Un nouveau modèle de société émerge mais un point central préoccupe les intellectuels : la connaissance de l'intimité des citoyens sera un jour détenue par des intérêts privés. « La plupart de ceux qui exploitent ces données font du business pour eux et pas vraiment pour autrui. Ils ne cherchent pas la vérité », regrette Laurent Maruani. « C'est une première dans notre civilisation et c'est un problème énorme, reconnaît François Ewald. Jusqu'à présent, ce type de connaissance était public et institutionnalisé, par l'Insee en France par exemple. » Au fil du temps, les institutions qui collectent, traitent et conservent les informations personnelles se sont dotées de règles éthiques. Les entreprises privées feront-elles de même ?

Nos données personnelles ne connaissent plus de frontières : 84 % des internautes dans le monde sont membres d'un réseau social. Et sur les dix premiers réseaux utilisés, cinq sont américains, trois chinois, et deux russes. «Que deviendront ces informations personnelles si les entreprises les possédant sont aux abois financièrement ? Leurs engagements éthiques pourront-ils tenir ?», s'interroge Serge Abiteboul, titulaire de la chaire Informatique et science numérique au Collège de France. Twitter, qui cherche à rentabiliser son activité, vient ainsi de vendre le droit d'utiliser ses archives de tweets, ainsi que les informations sur ses millions d'utilisateurs, à deux sociétés spécialisées dans l'exploitation marketing de données.

Certains États commencent à réagir. La Commission américaine fédérale du commerce a édicté des règles de bonne conduite pour les entreprises. Elle demande au Congrès américain de légiférer pour que les consommateurs puissent contrôler l'utilisation de leurs données. La Commission européenne a publié, le 25 janvier, un projet de règlement sur la protection des données personnelles. « Il doit être adopté d'ici à 2013 et applicable immédiatement », précise Isabelle Falque-Pierrotin, présidente de la CNIL, la Commission nationale de l'informatique et des libertés. Une procédure express qui paraît longue tant les recherches s'accélèrent.

Document 6

Les médias sociaux dans les stratégies de recrutement

L'idée d'une distinction entre la vie privée et la vie publique est certes ancienne puisque Aristote y fait référence dès le IVe siècle avant J.-C. (Ariès et Duby, 1985), mais il fallait attendre la fin du XVIIIe siècle pour que s'impose la notion de vie privée et surtout de droit au respect de celle-ci. « Au XVIII^{e} siècle, les philosophes des Lumières, puis au XIX^{e} siècle, les théoriciens du libéralisme politique vont fonder le régime démocratique sur l'existence de l'individu et l'exercice des libertés, légitimant ainsi la notion de sphère privée en opposition à la sphère publique. » (Bloche et Verchère, 2011). En France, ce droit est inscrit dans le Code civil par la loi du 17 juillet 1970 qui affirme que « chacun a droit au respect de sa vie privée » mais ce texte n'en définit pas le périmètre. Il faut donc s'en remettre à la jurisprudence pour identifier les éléments qui relèvent de la vie privée. Ainsi, l'état de santé, la vie sentimentale, l'image, la pratique religieuse, les relations familiales et l'intimité relèvent de la sphère privée.

Les questions relatives au respect de la vie privée (RVP) connaissent aujourd'hui un regain d'intérêt sous l'influence de deux facteurs déterminants liés à la révolution numérique. Le premier facteur est la montée en puissance des médias sociaux qui se traduit par une tendance de certains internautes au dévoilement de soi, voire à l'exhi-

bitionnisme en se surexposant spontanément au sein des médias sociaux (Tisseron, 2001) affichant leurs goûts, leurs opinions, leurs réalisations, leurs relations ou leurs problèmes et en racontant leurs expériences personnelles (Brodin et Magnier, 2011). Le deuxième facteur est la collecte croissante, par les entreprises, d'informations relatives aux consommateurs et aux salariés, à des fins de marketing et de gestion des ressources humaines.

Ces comportements et ces pratiques ont conduit les députés, à s'interroger sur les droits de l'individu à l'heure de la révolution numérique (Bloche et Verchère, 2011) et le législateur à intervenir sous la forme d'une ordonnance datée du 24 août 2011. La Commission européenne, en la personne de Viviane Reding – commissaire chargée de la justice – a rendu public le 25 janvier 2012, son projet de directive interdisant l'usage de photographies privées « trouvées sur Facebook », lors d'un entretien d'embauche. Ces faits montrent l'actualité du sujet. La révolution numérique a ainsi profondément modifié les pratiques des internautes mais également celles des entreprises.

Vie privée et préoccupations en matière de respect de la vie privée

Selon un sondage Ipsos réalisé pour la Cnil en octobre 2008, 71 % des Français jugent insuffisante la protection des données individuelles sur internet ce qui les conduit à développer des stratégies de réponse face à une sollicitation (Lancelot-Miltgen, 2008). C'est dire si les Français sont préoccupés par les questions relatives au respect de leur vie privée (RVP). Le RVP fait référence à plusieurs éléments comme le droit à l'information – c'est-à-dire le droit pour une personne d'être informée de la collecte de données la concernant –, le droit au consentement qui correspond à la possibilité de refuser la collecte de données personnelles, le droit de contrôle et d'utilisation ultérieure des données et le droit d'accès, c'est-à-dire la possibilité d'accéder aux informations et de corriger celles qui sont erronées. Les préoccupations des individus en matière de RVP sont nombreuses : collecte de données trop nombreuses et trop personnelles, stockage non autorisé, erreurs, accès par des personnes non autorisées, utilisation interne (par celui qui a collecté les données) ou externe suite au transfert des données à un tiers (Wang et Wang 1998).

Influence des informations trouvées sur la prise de décision

Les professionnels s'accordent pour dire que certaines informations seraient susceptibles de les faire changer d'avis et de renoncer à un candidat : – « des informations qui seraient contradictoires avec ce qu'on m'a dit » ; – « sur Facebook, des photos un peu particulières, des inscriptions sur le mur, par exemple quelqu'un qui vient de passer un entretien et qui a mis sur son mur un avis déplaisant sur l'entreprise ou sur les recruteurs » ; – « des informations personnelles, son comportement en dehors de l'entreprise, ses fréquentations, ses idées, ses opinions… tout ce qu'il peut cacher lors d'un entretien, ses hobbies, toute sa vie en dehors de l'entreprise qu'il nous cacherait si on lui posait des questions » ; – « si la personne est raciste par exemple, tout ce qui est de l'ordre de la loyauté, si la personne dénigre son employeur ou son entreprise, si la personne met ses beuveries sur Facebook, ça aurait certainement une incidence ». Un DRH a même déclaré utiliser ces réseaux pour rechercher des informations sur les salariés de son entreprise : – « … par exemple quand je cherchais des preuves d'exercice d'activité professionnelle, alors que la personne était en arrêt pour accident de travail. J'ai trouvé ce que je voulais et ça a bien conforté ma position dans la négociation de son licenciement ».

Candidats/recruteurs : des positions divergentes

Parmi les jeunes interrogés, 67 % considèrent que l'employeur n'a pas le droit d'utili-

ser des informations publiées sur Facebook. Cette proportion est encore plus élevée en ce qui concerne les conversations entre amis au sein de FB. 76 % sont tout à fait d'accord ou plutôt d'accord avec l'idée que l'utilisation d'informations personnelles par les professionnels du recrutement constitue une atteinte à la vie privée. Or, la majorité des professionnels estime que la recherche d'informations sur les candidats ne constitue pas une atteinte à leur vie privée : – « Ce n'est pas du fliquage, c'est de l'information complémentaire qui me permet de mieux réussir l'adéquation entreprise/personne. » Ils rejettent la responsabilité sur les candidats qui ont tendance à se dévoiler spontanément. – « Lors d'un entretien de recrutement, quand un candidat se met à vous parler spontanément de son conjoint, de ses enfants ou de sa maison, vous ne l'arrêtez pas, vous ne lui dites pas "attention je n'ai pas le droit de vous écouter, il y a atteinte à votre vie privée", bien sûr que non, vous l'écoutez… les réseaux sociaux c'est exactement pareil, le candidat vous livre des informations personnelles, pourquoi s'en priver ! » ; – « Ce sont peut-être et même sûrement des informations privées mais elles deviennent publiques à partir du moment où elles sont partagées sur un réseau social […]. Les utilisateurs de Facebook ont le contrôle sur ce qu'ils publient, on ne leur subtilise aucune information. »

Les jeunes recrues font preuve d'une méconnaissance des pratiques des employeurs et des recruteurs. Ils pensent majoritairement que ces derniers ne peuvent pas utiliser les informations privées des candidats. Ces résultats montrent qu'il est nécessaire d'informer les étudiants sur les utilisations possibles de toutes les informations qu'ils publient au sein des réseaux sociaux. Il est du ressort des universités et des écoles au sein desquelles ils poursuivent leurs études de les sensibiliser à la nécessité de procéder à un dévoilement de soi contrôlé et d'élaborer une stratégie de personal branding [marque personnelle]. Le concept de personal branding est apparu à la fin des années 1990 et a été popularisé par Peters (1997). Considéré comme stratégique pour les personnes publiques (politiciens, célébrités, dirigeants d'entreprise, etc.), le personal branding est, grâce au web 2.0, à la portée de tous. Tout individu a, gratuitement à sa disposition, les outils nécessaires à la construction de sa marque personnelle et devient son propre « marketeur ».

Le monde professionnel reconnaît qu'il est, aujourd'hui, nécessaire de contrôler cette marque personnelle véhiculée à travers les réseaux sociaux, afin de projeter une identité personnelle respectable et attractive pour un recruteur potentiel. Poursuivant l'analogie avec la marque produit, un individu doit, dans un premier temps, définir l'identité de sa marque personnelle – c'est-à-dire un positionnement souhaité qui s'appuie sur ses compétences distinctives – et, dans un second temps, communiquer ce positionnement, via un ou plusieurs profils, au sein de réseaux sociaux appropriés selon les entreprises ciblées, à savoir LinkedIn, pour promouvoir un profil international, en langue anglaise, et Viadeo, pour promouvoir un profil plus hexagonal.

Document 7

Contre l'hypothèse de la fin de la vie privée

La question de savoir si nos sociétés connaissent une érosion progressive de la vie privée est au coeur des conflits politiques et des débats intellectuels des dernières années. Face à l'essor de l'informatique ubiquitaire et des big datas, des grandes plateformes du Web social et des dispositifs mobiles, l'opinion publique oscille entre postures apocalyptiques et enthousiasmes parfois calculés à l'annonce de la « fin de la vie privée ». Quoique largement hypothétique, ce processus ouvre la voie à des abus

tout autant de la part d'entreprises privées que des pouvoirs étatiques. De la découverte d'Échelon (2000) à l'affaire PRISM (2013), la mise en place d'un vaste complexe militaroinformatique, collectant des données personnelles de milliards d'utilisateurs de dispositifs numériques, ne fait plus de doute.

Mais, plus inquiétante encore que le repérage passif ou la fouille systématique de données circulant sur des réseaux numériques, il y a l'impression que ces tendances révèlent un glissement profond de notre système de valeurs, des attitudes des utilisateurs mêmes, de plus en plus tolérants envers l'inspection de leur vie personnelle, voire désireux de participer à la surveillance dont ils font l'objet. Si certains critiques se sont empressés de dénoncer la mise en oeuvre d'un régime de « surveillance participative », des livres populaires ont salué l'avènement inéluctable d'une nouvelle philosophie collective de « publitude » (publicness) et de transparence en réseau.

Or, des études ayant analysé les pratiques de partage d'informations sur Facebook ont montré qu'au contraire depuis 2005 les utilisateurs se sont investis de plus en plus dans les mesures de protection d'un nombre croissant de données personnelles. Si des informations apparemment anodines tels les goûts musicaux ou littéraires étaient initialement partagées sans problème, autour de 2009-2010 elles ont été « mises en privé », de la même manière que des données habituellement considérées comme sensibles : adresse, date de naissance, orientation sexuelle, affiliation politique, etc. Ces préoccupations se manifestent à travers des actions concrètes de refus, tant sur le plan individuel (nonusage, comportements disruptifs en ligne, obfuscation[1] des informations personnelles) que sur le plan collectif.

Si, en dépit de ces formes de résistance, l'énonciation de l'hypothèse de la « fin de la vie privée» a été possible, c'est en raison d'un malentendu foncier relatif aux motivations d'usage des médias sociaux. Trop souvent les analystes et les commentateurs ont pris pour une renonciation intégrale à la privacy [vie privée] ce qui en réalité n'est que l'actuation de formes de dévoilement stratégique d'informations personnelles à des fins de gestion du capital social en ligne.

La littérature savante à ce sujet commence à peine à prendre la mesure de l'ampleur de ce malentendu. Les approches psychologiques, qui ont initialement dominé les études sur la vie privée dans le Web social, avaient mis l'accent sur les cinq dimensions principales de la personnalité des usagers, dont l'extraversion. Plusieurs auteurs ont suivi cette tendance, et insisté sur les déterminants micro-sociologiques des comportements médiatisés par les TIC. Le dévoilement de soi a alors été interprété comme une forme d'« individualisme expressif », visant à produire et entretenir des «identités numériques ». Dans cette perspective, sans nécessairement dénoncer le « narcissisme » des usagers de blogs et de plateformes de communication Web, il s'agissait principalement de distinguer des styles communicationnels et des typologies d'usagers, afin d'établir si certains d'entre eux sont plus enclins à une sur-représentation de soi qui irait jusqu'à « parader » sur les médias sociaux.

Ces « patterns d'auto-exhibition » sont en fait corrélés à des différences socio-démographiques que les études existantes en sciences sociales ont déjà mises au jour. Parmi ces différences, le genre a une incidence importante sur la quantité de temps passé sur l'Internet, sur le choix et le type d'utilisation des services en ligne. L'âge est également pertinent, ce qui rejoint l'idée souvent admise que les jeunes générations d'utilisateurs d'Internet, seraient beaucoup moins conservatrices en matière de

[1] obfuscation : statégie de protection de la vie privée qui consiste à publier une quantité d'informations.

privacy. Les risques d'une existence ouverte et traçable pour les adolescents et les enfants polarisent encore davantage les réactions des détracteurs ainsi que des partisans de la « fin de la vie privée ».
Malgré la rhétorique ambiante autour du concept controversé de *digital natives*, même les utilisateurs les plus jeunes ne négligent pas ces enjeux, montrant en réalité un tableau complexe et varié de comportements. En particulier, le statut socioéconomique influe sur la fréquence d'usage des services de communication numériques, ainsi que le niveau des compétences informatiques, dont dépend la capacité des utilisateurs à ajuster les paramètres de confidentialité.

Dans la mesure où elles ne permettent pas de valider ni de réfuter l'hypothèse de la fin de la vie privée, ces orientations de recherche ont été progressivement dépassées au profit d'approches plus attentives aux dimensions méso- et macro-sociales. Ainsi laisse-t-on de côté la catégorie d' « identité » pour regarder plutôt la production de « présence en ligne » au travers de traces visibles qui documentent les activités des usagers et leurs interactions avec autrui. Les enjeux personnels se font collectifs, et le dévoilement de soi apparaît de plus en plus lié à la création de lien social en ligne, s'intégrant dans de véritables stratégies d'usage finalisées à la capacitation personnelle, professionnelle, culturelle ou politique. De ce fait, les pratiques de dévoilement engagent des processus sociaux complexes de reconnaissance réciproque des rôles et des statuts.

La question des motivations de la révélation de soi, de ses préférences et conduites, laisse la place à l'étude des structures sociales des groupes humains et des collectivités permettant une articulation entre éléments intimes et publics. Le regard des chercheurs se porte alors sur les modalités de gestion du capital social des usagers au travers de l'ajustement de leur présentation en ligne et de la mise en commun de détails sélectionnés ayant trait à leur sphère intime. La notion de capital social désigne dans ce contexte l'acquisition, via des relations médiatisées pas les TIC, de ressources matérielles, informationnelles ou émotionnelles. Elle est inévitablement soumise à des contraintes et à des coûts, à laquelle la perte de privacy s'apparente : se faire connaître oblige à sacrifier une partie de sa vie privée, afin d'attirer des connexions, notamment par des personnes pouvant sympathiser avec ses propres caractéristiques, pratiques et opinions. Ces études récentes permettent de jeter un nouveau regard sur les raisons pour lesquelles les utilisateurs peuvent être amenés à se dévoiler. Non pas parce qu'ils seraient des victimes passives des agissements des concepteurs des plateformes sociales, ou encore parce qu'ils présenteraient des traits de personnalité les poussant à « s'exhiber sur les réseaux » – mais parce que leurs usages sont régis par une volonté stratégique de gestion de leur capital social.

Somme toute, ce dévoilement différentiel des informations personnelles n'est nullement un processus monotone, conduisant inévitablement d'un état de plus forte protection de la vie privée à une nouvelle condition de « publitude » généralisée. Bien au contraire, les acteurs optimisent le dévoilement d'informations personnelles en se positionnant le long d'un continuum dont « ouverture » et « fermeture » sont les extrêmes. On peut penser que chaque interaction implique un processus dynamique d'évaluation de la situation, d'adaptation au contexte, de catégorisation du contenu que les individus sont prêts à partager avec leurs connaissances. Autrement dit, les choix des usagers tiennent compte du caractère intrinsèquement plus ou moins appréciable de l'information partagée, ainsi que de la structure et composition de leurs réseaux personnels en ligne, dans chaque type d'interaction. Les différents comportements de dévoilement sont motivés par un souci d'intégrité contextuelle de l'informa-

tion partagée. Dans la mesure où les données ne sont pas sensibles par leur nature, mais selon leur pertinence par rapport à un milieu social de choix, le respect de la vie privée revient principalement à vérifier l'adaptation entre l'information dévoilée, l'intention stratégique de son locuteur et le contexte de son dévoilement (à savoir la forme, structure et taille du réseau de contacts avec lesquels elles sont partagées).

Document 8

Les États-Unis veulent protéger la vie privée

Entretien de John Podesta, conseiller du président Barack Obama

Pendant la majeure partie de l'histoire de l'humanité, l'information ne s'est pas déplacée plus vite qu'un cheval et son cavalier ne pouvaient chevaucher, ni qu'un navire ne pouvait naviguer. Aujourd'hui, la communication mondiale instantanée est une réalité. L'Internet est une aubaine pour le commerce international, pour le partage du savoir, et pour l'établissement de relations par-delà les frontières. Depuis les smartphones que nous avons dans nos poches jusqu'aux systèmes de navigation de nos voitures, le monde aujourd'hui est plus connecté que jamais, et nous-mêmes produisons toujours plus de données relatives à nos activités, nos déplacements, nos inclinations et nos relations.

Cette prolifération de données issues de sources très variées, combinée à la baisse du coût de la collecte, de la conservation et du traitement d'une part, à l'accroissement des capacités d'un grand nombre de techniques analytiques d'autre part, est au coeur de la technologie mettant en oeuvre ces métadonnées. Celles-ci sont utilisées dans une gamme d'applications à fort impact social et économique : pour mener d'importantes recherches dans le champ de la médecine et des soins médicaux, pour modéliser les impacts du changement climatique comme la montée du niveau des eaux, et pour aider les entreprises privées et les agences gouvernementales à déceler des fraudes.

Mais comme toute nouvelle technologie, les métadonnées soulèvent d'importantes questions. Que signifient-elles pour l'équilibre des pouvoirs entre citoyens et gouvernements, clients et entreprises, employés et employeurs ? Les cadres régissant notre vie privée suffisent-ils à protéger les informations personnelles sensibles dans un monde de métadonnées ?

Un juste équilibre

En janvier, le président Obama s'est exprimé au département de la justice des États-Unis sur le juste équilibre à trouver entre la protection de la sécurité de l'Amérique et de ses alliés, et le respect de nos engagements envers la préservation du droit à la vie privée et des libertés civiques. Il a alors annoncé d'importantes réformes relatives aux activités de nos services de renseignement d'origine électromagnétique et a réaffirmé son engagement constant envers un débat public soutenu sur ces questions. Le président a également demandé à son équipe en charge de la sécurité nationale de travailler avec ses homologues étrangers afin de renforcer nos relations les plus cruciales, d'approfondir notre coordination et notre coopération, et de restaurer la confiance.

Dans le même temps, reconnaissant que ces défis ne sont pas propres à la communauté du renseignement, le président Obama m'a chargé de mener, dans un délai de trois mois et en collaboration avec des responsables gouvernementaux, un examen global du dossier des métadonnées et des questions liées au respect de la vie privée,

et d'étudier la façon dont les métadonnées influent sur notre manière de vivre, de travailler, et dont nous interagissons avec les autres personnes, avec le gouvernement et avec le monde des affaires. Nous avons conclu que les métadonnées auraient un impact profond sur quasiment tous les secteurs de l'activité humaine, dans la vie privée comme publique, personnelle comme commerciale. Nous sommes convaincus que les métadonnées nous obligeront à un débat de fond et inscrit dans la durée sur le respect de la vie privée dans un paysage numérique en constante évolution, et nous avons recommandé que soient prises des mesures concrètes en vue de l'adoption de la Déclaration des droits des consommateurs en matière de confidentialité, une loi à portée historique proposée pour la première fois par le président Obama en 2012 afin de garantir légalement la protection de la vie privée à l'ère digitale. De même qu'Internet ne connait pas de frontières, les perspectives d'avenir comme les défis apportés par les métadonnées ont des ramifications internationales.

Une valeur universelle

La protection de la vie privée est une valeur universelle. C'est pourquoi nous avons recommandé dans notre rapport que soient étendues dans la mesure du possible à tous les citoyens non-américains les garanties prévues dans la Loi sur la protection de la vie privée de 1974, qui régit la collecte, l'utilisation et la diffusion des données personnelles par le gouvernement fédéral américain, ou bien que soient établies des règles équivalentes permettant de garantir une protection appropriée et significative des données personnelles quelle que soit la nationalité de la personne.

Les États-Unis d'Amérique et leurs partenaires de l'Union européenne respectent la vie privée de leurs propres citoyens et de ceux de chacun de leurs pays. Le président Obama et les dirigeants de l'Union européenne ont réitéré leur engagement dans ce domaine lorsqu'ils se sont réunis au mois de mars. Nous partageons le même objectif de protection adéquate des données et de la vie privée, afin de nous permettre à tous de profiter au mieux de tous les avantages qu'offrent les technologies modernes. Afin de garantir que l'ensemble des citoyens des deux côtés de l'Atlantique bénéficie du commerce international qui profite à nos vies modernes, les États-Unis d'Amérique et l'Union européenne se sont mis d'accord pour appliquer les normes et pour améliorer la transparence régissant le transfert international des données. Nos citoyens sont mieux protégés lorsque les services chargés de l'application des lois dans nos pays travaillent ensemble ; c'est pourquoi nos dirigeants se sont engagés à accélérer les négociations en vue d'un accord significatif et étendu sur la protection des données dans le cadre de la coopération policière et judiciaire sur les questions pénales, y compris le terrorisme.

Engagement

L'administration Obama poursuit son engagement pour un Internet ouvert, interopérable, sûr et fiable, et pour l'exploitation de l'ensemble du potentiel innovant de la technologie des métadonnées. Les métadonnées aident les entreprises de services publics à évaluer et à prédire les demandes énergétiques des réseaux électriques, en augmentant l'efficacité et en réduisant les risques de pannes de courant. Les métadonnées sont à la base des outils permettant de cartographier le génome humain et de faire avancer l'initiative BRAIN, entreprise par l'administration Obama dans le but d'améliorer considérablement notre connaissance du cerveau humain. Nous sommes convaincus qu'il est essentiel de tirer le meilleur profit des technologies rendues possibles par les métadonnées tout en limitant les risques pour la vie privée et pour nos valeurs.

Ces objectifs requerront un examen continu de l'impact des nouvelles technologies sur les droits à la vie privée. Grâce à une coopération active et constante avec nos partenaires internationaux,
je suis convaincu que nous pourrons continuer à garantir nos valeurs communes dans le domaine de la protection de la vie privée dans un monde en constante évolution.

Document 9

La déconnexion aux outils de géolocalisation

L'usage aujourd'hui massif de services géolocalisés représente sans doute une menace pour la vie privée de l'individu hyperconnecté qui ne se sépare même plus de son smartphone pour manger ou dormir. Aux côtés du « quand et pour quelles raisons les gens se déconnectent-ils volontairement ? », il nous a semblé pertinent dans cette recherche de prendre le problème sous un autre angle et d'analyser, en prenant pour exemple cette technologie particulièrement intrusive que représente la géolocalisation, non plus le « pourquoi », mais le « comment » de la déconnexion. À l'ère des Big Datas et de l'utilisation quasi permanente de la position géographique, savoir maîtriser l'envoi de données relatives à sa localisation et être capable de désactiver ces fonctionnalités dès lors qu'elles représentent une gêne, apparaissent plus que jamais comme un luxe qui n'est absolument pas offert à tous. La passivité du mobinaute qui ne s'inquiète peut-être pas de sa vie privée autant que nécessaire, mais aussi la méconnaissance des accès autorisés à chaque application utilisée et le décalage entre la volonté de déconnexion et la capacité à y parvenir en pratique amènent tous trois à une prise de conscience sur la vulnérabilité des individus utilisant une technologie qui les dépasse souvent et dont ils ne savent pas grand-chose.

En trame de fond, le spectre du *Big Brother* qui se dessine derrière cette incapacité à maîtriser pleinement le partage des données n'est peut-être pas celui qui doit le plus alerter. Alors que beaucoup d'études se focalisent sur le traçage des individus par des organismes et des entreprises, il serait sans doute intéressant d'un point de vue sociologique de s'intéresser davantage au pistage des individus par les individus et de décrypter les nouvelles stratégies de regroupement, d'évitement et de falsification de position qui peuvent y être liées. Cela amène par ailleurs à des réflexions plus globales, par exemple sur la reconsidération de l'importance de la position géographique dans les sociétés hyperconnectées, celle-ci se trouvant massivement partagée, parfois même contre son gré. Les demandes de localisation, considérées comme « une précondition à l'émergence du projet de rencontre » (Licoppe et Morel, 2011), sont-elles toujours nécessaires ou entrons-nous dans une société où la normalité sera d'être constamment géolocalisé ? Il est sans doute plus que temps de se poser la question avant que de nouvelles irréversibilités ne se mettent en place et sur lesquelles il sera ensuite difficile de revenir.

Document 10

Protection des données personnelles : L'Europe avance lentement

Sur le sujet pourtant sensible de la protection des données privées, la modernisation du droit européen avance décidément très lentement. Jeudi 4 décembre, les ministres de la justice des 28 pays de l'Union, réunis à Bruxelles, ont finalement trouvé un accord, mais sur un seul chapitre. « On a maintenant en tout un accord sur trois chapitres, mais il en reste huit... », souligne une source proche des négociations... Le texte

dont il est question est un règlement - contrairement à une directive, il s'applique théoriquement de la même manière dans tous les États membres -, qui avait été proposé par la commissaire Viviane Reding en janvier 2012. Il y a donc tout près de trois ans maintenant. L'esprit du texte était de moderniser, à l'heure du web, une directive datant de 1995, avant, donc, le développement fulgurant de l'internet grand public.

Mais les Européens ont du mal à s'entendre, malgré le scandale des écoutes américaines révélé par l'agent Snowden en 2013, malgré la vertigineuse montée en puissance des géants du web Google, Amazon ou Facebook, avec leurs capacités de traitement des données inégalées. « Il y a un consensus politique, depuis longtemps, entre les États, sur le fait qu'il faut renforcer la protection des données personnelles. Mais il y a un gros écart entre les paroles, et les prises de position, quand on se met autour d'une table. C'est pour cela que les choses avancent si lentement. Le texte est très technique et comme le diable gît dans les détails, trouver des compromis est laborieux » regrette une source européenne haut placée. Une autre source ajoute : « avec ce règlement, on doit trouver un équilibre entre deux ambitions a priori contradictoires : d'un côté mieux protéger les données numériques des personnes. Et de l'autre, favoriser la compétitivité des entreprises, notamment de celles dont le modèle économique est basé sur l'exploitation de ces données ». Des pays comme les Pays-Bas, le Royaume- Uni ou l'Irlande - cette dernière héberge plusieurs sièges sociaux européens de multinationales américaines (Google, Apple), ont tendance à davantage défendre la compétitivité des entreprises. D'autres, à commencer par l'Allemagne, ou la France, penchent plutôt pour une plus grande protection des données personnelles.

Limitation de la durée de stockage des données

Les 28 ministres de la justice sont tombés d'accord sur l'adoption de règles pour les établissements publics européens - États, hôpitaux, services publics -, quand ils manipulent les données personnelles des citoyens. Notamment sur la nécessaire limitation de la durée de stockage des données. Pour venir à bout de l'ensemble du règlement « Reding », les Européens ne sont pas au bout de leur peine. Il va leur falloir encore, dans les mois qui viennent, obtenir une majorité sur des questions *a priori* bien plus délicates, comme le droit à l'oubli (dans quelle mesure les citoyens européens peuvent-ils exiger que les informations les concernant présentes en ligne soient supprimées ?).

Dans un arrêt qui a fait grand bruit, au printemps dernier, la cour de justice de l'Union européenne, a dit que dans certains cas, les internautes étaient fondés à exiger le retrait de leurs données auprès des moteurs de recherche qui les indexent. Depuis, Google est submergé de demandes d'effacements de documents. Certains s'en félicitent, mais d'autres s'inquiètent déjà d'une menace majeure pour la liberté d'expression, voire pour la liberté de la presse -, sur le web. L'objectif de la commission européenne parait dès lors très ambitieux : elle espère l'adoption du règlement « Reding » pour 2015. De fait, une de ses priorités est de créer un vrai marché unique du numérique. Or, pour cela, il faut l'instauration d'un climat de confiance et de sécurité juridique maximale pour les entreprises.