Bernard E. Harcourt

# LA SOCIÉTÉ D'EXPOSITION

## Désir et désobéissance à l'ère numérique


LA COULEUR DES IDÉES

SEUIL

# LA SOCIÉTÉ D'EXPOSITION

*BERNARD E. HARCOURT*

# LA SOCIÉTÉ D'EXPOSITION

## Désir et désobéissance à l'ère numérique

*Traduit de l'anglais (États-Unis)*
*par Sophie Renaut*

*ÉDITIONS DU SEUIL*
*57, rue Gaston-Tessier, Paris XIX^e^*

ISBN 978-2-02-137300-4



www.seuil.com

# *Introduction*

Enfoncer une touche sur un clavier, cliquer sur une souris, faire une recherche Google, acheter sur Amazon, balayer un écran, insérer une carte, consulter Instagram, liker, tweeter, scanner, bref, tout ce que nous faisons dans cette nouvelle ère numérique peut être enregistré, stocké et surveillé. Tous nos gestes quotidiens sur nos iPads, tablettes, ordinateurs, Kindle et portables, toutes nos opérations avec nos cartes de crédit ou de club de sport, de fidélité ou de transport, et nos badges d'emploi ou de télépéage, enregistrent des données susceptibles d'être archivées, exploitées et identifiées. Qu'elles soient recoupées ou analysées séparément, ces données constituent une nouvelle identité virtuelle, un moi numérique qui est aujourd'hui plus tangible, plus fiable, plus stable et identifiable que notre moi analogique. Nos téléphones mobiles communiquent et cherchent des réseaux wifi même lorsque les données cellulaires sont désactivées. Notre Pass Navigo et notre badge d'entreprise laissent une trace à chaque fois qu'on les bipe ou qu'on les insère. Tout retrait d'argent à un guichet, toute recherche sur Internet, tout accès sécurisée et tout trajet en ascenseur ou paiement en ligne laissent une empreinte qui permet aux autres de savoir à tout moment où nous sommes, de nous suivre à discrétion, et de reconstituer chacune de nos actions. En somme, la moindre trace numérique peut aujourd'hui être identifiée, stockée et agrégée pour dresser un état des lieux précis de ce que nous aimons et de ceux que nous aimons, de ce que nous lisons, pour qui nous votons, où nous manifestons.

Les médias sociaux et les navigateurs web que nous utilisons – et même ceux que nous visitons accidentellement – recueillent quantité de données personnelles en continu. Nos opérateurs de télécommunications enregistrent tout ce qu'ils peuvent, comme le font d'autres télécoms, qui, à notre insu, acheminent, échangent, redirigent et

retransmettent nos communications. Nos données intimes sont stockées par les services de renseignements et d'écoute aux États-Unis, en France, et à l'étranger, par les forces de l'ordre locales, mais aussi par des enseignes de distribution, par des courtiers en données dont nous n'avons jamais entendu parler, par des hackers, ou simplement par des curieux qui se servent de renifleurs réseau gratuits pour nous espionner sur le Web. D'une manière ou d'une autre, la plupart de nos informations numériques sont disponibles et peuvent être achetées par des annonceurs, analysées par des compagnies d'assurances, vérifiées par nos employeurs, examinées par les services de sécurité, interceptées par des enregistreurs de frappe, ou entrevues sur des forums de discussion anonymes. Google et Facebook se livrent une compétition acharnée pour savoir lequel des deux possède le plus de données personnelles et sensibles pouvant être partagées avec leurs utilisateurs et vendues à des annonceurs. Des programmes espions, gratuits et en vente libre, permettent à quiconque de lire les e-mails des autres et de voir leur historique de navigation sur des réseaux non sécurisés. En secret, les organismes responsables du maintien de l'ordre recueillent, centralisent et partagent le plus d'informations numériques possible. Et la National Security Agency (NSA), le British Government Communications Headquarters (GCHQ), la Direction générale de la sécurité extérieure (DGSE), les agences de renseignements chinoises et russes et pratiquement tous les autres services de renseignements du monde entier ont cette même ambition de tout savoir, de cartographier l'univers de l'Internet, de réussir à identifier le moindre terminal connecté, bref, de connaître tous les contenus numériques, partout et à tout moment.

La plupart d'entre nous en sommes conscients, même si nous y prêtons peu attention. Nous avons pourtant lu les articles du *Guardian*, du *Washington Post* et du *New York Times*, et nous avons entendu les journalistes d'investigation s'exprimer à la radio. Nous avons regardé les extraits vidéo des audiences au Congrès américain. Nous avons vu maintes et maintes fois apparaître à l'écran ces onglets publicitaires nous rappelant des requêtes récemment effectuées sur Google. Nous avons reçu les e-mails espions dans nos spams. Nous avons même minutieusement examiné les Powerpoint top secret de la NSA, ainsi que d'autres documents divulgués par Edward Snowden.

Mais c'est une chose de le savoir, et une autre de le garder en mémoire suffisamment longtemps pour s'en soucier, surtout quand il y a le son d'un nouveau texto, la notification d'un nouvel e-mail, l'irruption d'un nouveau « j'aime » sur notre photo Instagram, le bruit de sonnette d'un nouveau message Facebook, ou juste le désir de savoir combien de personnes ont vu notre histoire Snapchat ou laissé un commentaire sur notre blog. C'est tout autre chose de rester sur ses gardes devant les distractions stimulantes et les plaisirs sensuels qu'offre cette nouvelle ère numérique : fils d'information en continu, messages d'amis, dernière vidéo virale de Vine ou de YouTube, accès à la moindre information en ligne, possibilité de googliser tout et n'importe quoi. L'anticipation, le désir de quelque chose de nouveau et de gratifiant, l'agréable sensation de recevoir sur notre messagerie la moindre bonne nouvelle, tout est bon pour détourner notre attention de ce que nous savons réellement de l'ampleur et de l'omniprésence de ces nouvelles formes de contrôle numérique, d'exploration de données, de profilage et de surveillance. Nous nous laissons si facilement distraire par le moindre stimulus numérique, et nous y réagissons souvent pour éviter d'avoir à nous confronter au syndrome de la page blanche, à la gêne causée par une réflexion complexe ou une interaction désagréable. Passer le pouce sur notre smartphone, vérifier nos e-mails, lire un fil Twitter, ouvrir Instagram ou Facebook, sont devenus des réflexes. À peine avons-nous commencé à y penser que déjà nous sommes accaparés par un nouveau post viral ou une partie d'*Assassin's Creed Unity*. Nous préférons ignorer ce que nous soupçonnons ou même savons, à savoir que nous sommes pistés et exposés. Nous le chassons de notre esprit. Mais nous le faisons à nos risques et périls.

#

Le *Wall Street Journal* l'avait révélé au mois de mai 2011, bien avant que le nom d'Edward Snowden n'évoque quoi que ce soit[1]. Pourtant, cette annonce n'a pas fait grand bruit. Elle concernait ces petites icônes visibles sur la plupart des sites internet : le pouce levé du bouton « j'aime » de Facebook, le petit oiseau de Twitter, le symbole multicolore du symbole Google+ – tout cet alignement de

petites icônes qui inondent les sites internet, les vidéos YouTube, les articles d'actualité, les sites de voyage, les onglets de recherche, etc.

Il s'avère que ces petites icônes permettent à Facebook, à Twitter et à Google de suivre notre activité sur les sites où sont affichées ces icônes, que nous soyons ou non connectés à ces réseaux sociaux. Du moment que l'on utilise ces réseaux et que l'on s'est connecté à l'un d'eux au cours du dernier mois (sans s'être *activement* déconnecté), la fréquentation sur d'*autres sites* où figurent ces icônes est enregistrée et signalée à Facebook, Twitter ou Google. En fait, il n'est même pas nécessaire d'être inscrit sur un média social, on peut tout à fait être pisté à partir d'autres sites web, et cela même si on clique accidentellement sur un des sites de ces médias sociaux. Or il se trouve que ces petites icônes apparaissent sur beaucoup de sites. Rien qu'en 2011, par exemple, 33 % des 1 000 sites internet les plus populaires avaient le bouton « j'aime » de Facebook, 25 % avaient le widget Google+ et 20 % le bouton tweet de Twitter. Ces icônes sont aujourd'hui incluses dans des millions de sites web[2].

La séquence est simple : lorsque vous vous connectez à l'un de ces médias sociaux – Facebook, Twitter, Google+ –, un logiciel est installé sur votre navigateur et reste actif même lorsque vous éteignez votre ordinateur ou fermez votre navigateur. Celui-ci n'est désactivé que si vous suivez la procédure de déconnexion à ces médias sociaux, c'est-à-dire en cliquant manuellement sur le bouton « déconnexion ». Une fois activé, ce logiciel signale aux médias sociaux chacune de vos visites sur un site web où figure la petite icône, que vous cliquiez ou non sur l'icône en question. La simple présence sur un site où figurent les boutons *like* et *tweet* permet à ces médias sociaux d'enregistrer tout votre historique de navigation sur Internet.

Le *Wall Street Journal* remarquait en passant : « Facebook affirme qu'il continue à placer un cookie sur l'ordinateur de toute personne visitant la page d'accueil Facebook.com, même si elle n'est pas membre[3]. » Ainsi, l'historique d'une navigation peut être rendu accessible à d'autres, même à ceux qui n'ont pas de compte Facebook. L'article poursuit : « Jusqu'à une date récente, certains *widgets* Facebook permettaient aussi d'obtenir des données de navigation à propos d'internautes qui n'étaient jamais allés sur Facebook.com, c'est-à-dire sans que Facebook connaisse leur

identité. Un peu plus tôt dans l'année, l'entreprise a affirmé avoir mis fin à cette pratique, qualifiée de "bug", après que le chercheur néerlandais Arnold Roosendaal, de l'université de Tilburg, l'eut divulguée[4]. »

Pour être plus précis, voici comment fonctionne ce suivi. Selon des communications détaillées recueillies depuis 2011 entre des journalistes d'*USA Today* et des cadres de Facebook – Arturo Bejar, directeur de l'équipe de recherche de Facebook, Andrew Noyes et Barry Schnitt, chargés de communication de Facebook, Gregg Stefancik, directeur technique, et Jaime Schopflin, porte-parole de la firme – les spécifications techniques sont les suivantes :

- L'entreprise dispose de plusieurs procédés pour compiler les données de suivi à la fois des membres inscrits qui utilisent leurs comptes, des membres qui sont déconnectés et des non-membres. Cette technique de suivi se met en place dès le moment où vous visitez une page Facebook. Si vous choisissez de créer un nouveau compte, Facebook insère deux types différents de cookies dans votre navigateur, un « cookie de session » et un « cookie de navigation ». Si vous choisissez de ne pas devenir membre et que vous quittez la page, seul le cookie de navigation reste actif.
- Dès lors, chaque fois que vous visitez une page tierce où sont implantés le bouton *like* ou d'autres extensions Facebook, l'extension fonctionne en lien avec le cookie pour signaler à Facebook la date, l'heure et l'adresse web du site visité. Les identifiants uniques de votre PC et de votre navigateur, comme votre adresse IP, résolution d'écran, système d'exploitation et version du navigateur, sont également enregistrés.
- Ainsi, Facebook dresse un historique de toutes les pages web que vous avez visitées au cours des derniers quatre-vingt-dix jours, en supprimant les entrées du jour le plus ancien et en ajoutant les dernières au journal.
- Si vous êtes connecté à votre compte Facebook et que vous naviguez sur Internet, c'est le cookie de session qui se charge de l'historique. Le cookie de session enregistre également votre nom, votre adresse e-mail, le nom de vos amis et toutes les données associées à votre profil Facebook. Si vous êtes déconnecté, ou si vous n'êtes pas membre, c'est le cookie de navigation qui se charge de l'historique ; il génère également un identifiant unique au format alphanumérique, mais aucune information personnelle[5].

Dans le cas où tous ces détails vous paraîtraient fastidieux, il convient toutefois de rappeler que, selon ses ingénieurs et chargés de communication, Facebook relie et associe toutes les informations glanées au cours de votre navigation sur Internet à « votre nom, adresse e-mail, amis, et à toutes les données associées à votre profil Facebook[6] ».

Cela se passait en 2011. En 2014, cette technique de traçage était devenue obsolète, en particulier dans le domaine de la publicité. D'abord, les internautes avaient trouvé des moyens de bloquer les cookies ou de les effacer. Ensuite, il s'est avéré que les cookies étaient peu adaptés aux smartphones, à une époque où tout le monde passe de plus en plus de temps sur son téléphone portable. Pour reprendre les propos d'un expert en technologie, « le cookie perd de son efficacité dans l'industrie de la publicité[7] ». Facebook a lui-même ouvertement reconnu les lacunes du cookie, expliquant que « la technologie actuelle de diffusion et d'évaluation des annonces publicitaires – les cookies – est défectueuse lorsqu'elle est utilisée seule. Les cookies ne fonctionnent pas sur mobile, sont moins performants en termes de ciblage démographique et ne peuvent pas mesurer avec précision l'entonnoir d'achats à travers les navigateurs, les appareils ou en mode hors-ligne[8] ».

Le 29 septembre 2014, Facebook a proposé une nouvelle solution : un marketing « centré sur les individus » (*people-based marketing*) par le biais d'un produit plus performant appelé Atlas. « Le marketing centré sur les individus résout ces problèmes », se vante Facebook[9]. Cette nouvelle technologie est simple : il suffit de prendre toutes les données que Facebook possède, y compris celles qu'il peut exploiter par le biais de nos applications mobiles, et de partager toutes ces informations avec tous ceux qui sont disposés à les acheter afin de cibler les utilisateurs en continu sur toutes leurs autres plateformes. Dans le bien nommé article « Avec sa nouvelle plateforme publicitaire, Facebook ouvre la chambre forte de ses données », Vindu Goel du *New York Times* explique qu'Atlas « permettra aux responsables marketing d'exploiter les connaissances [Facebook] détaillées de ses utilisateurs pour diriger les publicités vers ces personnes sur des milliers d'autres sites web et applications mobiles[10] ». En puisant dans la masse de données de Facebook, les annonceurs peuvent alors mettre en avant leurs produits sur tous les appareils et

plateformes auxquels accède l'utilisateur, y compris les sites vidéo, les applications de jeux, Instagram, etc. Par ailleurs, Facebook peut aussi fournir un retour aux annonceurs afin qu'ils puissent évaluer la performance de leurs publicités. Par exemple, Facebook se flatte qu'« Instagram, en tant qu'éditeur, a aujourd'hui la possibilité grâce à Atlas de vérifier le nombre de pages publicitaires vues et d'en mesurer les résultats. Et pour les annonceurs d'Atlas qui font déjà des campagnes sur Instagram, les publicités Instagram seront incluses dans les rapports d'Atlas[11] ».

Facebook est la deuxième plus grande plateforme de publicité numérique après Google, mais il a un net avantage sur les autres sur un point essentiel : les utilisateurs se connectent sur Facebook via leurs appareils mobiles. Comme l'explique le *New York Times,* « la connexion Facebook est surtout utile sur les appareils mobiles, où les outils de traçage traditionnels comme les cookies et les pixels espions ne fonctionnent pas. Si une personne est connectée à Facebook depuis un smartphone, l'entreprise peut voir quels autres appareils elle utilise et afficher des publicités dans ces applications[12] ». Ou bien, comme l'explique un autre expert en technologie, « tout le temps où vous êtes connecté à Facebook sur votre appareil, Atlas suit votre activité, même dans les applications qui n'utilisent pas de connexion Facebook[13] ». Facebook est très satisfait de cette nouvelle technologie et ne s'en cache pas. Son désir de prendre le contrôle de la publicité numérique – ses revenus en dépendent – est parfaitement explicite : « Atlas propose un marketing centré sur les personnes et aide les annonceurs à atteindre des personnes réelles à travers leurs appareils, plateformes et éditeurs. Les publicitaires peuvent ainsi facilement résoudre le problème de l'usage multiple des terminaux grâce à un ciblage et à une évaluation croisant les différents appareils. De plus, Atlas peut maintenant relier les campagnes en ligne aux ventes hors-ligne, ce qui est une preuve de l'impact réel des campagnes numériques sur la performance et l'augmentation des ventes[14]. »

Les médias sociaux sont devenus, pour reprendre ce qu'a écrit un journaliste d'investigation à propos de Gmail et d'autres services de Google, « une opération massive de surveillance qui intercepte et analyse chaque jour des téraoctets du trafic mondial sur Internet, et les utilise ensuite pour construire et mettre à jour des profils

psychologiques complexes de centaines de millions de personnes à travers le monde – tout cela en temps réel[15] ».

#

Les faits qui vont suivre ont été révélés en 2014 par l'agence de presse Associated Press (AP), et ont conduit le sénateur du Vermont Patrick Leahy, président du comité sénatorial des crédits du département d'État et du sous-comité du Sénat aux opérations extérieures, à organiser des audiences au printemps 2014 pour revenir en détail sur ces événements. L'affaire, qui remonte à 2009, concernait une autre base de données comprenant un demi-million de numéros de téléphones portables cubains – ou, plus précisément, un ensemble de données *et* quelques responsables et sous-traitants de l'Agence américaine pour le développement international (USAID), une agence gouvernementale qui fournit des milliards de dollars d'aide et d'assistance humanitaire à des pays en difficulté[16].

Tout a commencé lorsqu'un employé de Cubacel, le fournisseur public de téléphonie mobile à Cuba, communiqua clandestinement 500 000 numéros de téléphones portables à un ingénieur cubain qui vivait alors en Espagne. Cet expatrié cubain remit ensuite cette base de données – et ce « à titre gratuit » si l'on en croit les documents examinés par l'Associated Press – à des responsables de l'USAID ainsi qu'à une société commerciale de Washington, la Creative Associates International, laquelle avait gagné des millions de dollars grâce à des contrats avec l'USAID. À l'image du nom de cette société, l'une des directrices se montra alors, dira-t-on, « créative » : avec un associé qui résidait au Nicaragua, elle eut l'idée de faire des envois massifs de SMS, depuis plusieurs pays, aux utilisateurs de téléphones mobiles cubains. Une façon en effet créative de contourner le contrôle très strict de l'État cubain sur l'Internet. Une façon aussi de créer un nouveau type de réseau social inspiré de Twitter[17].

L'idée était d'essayer discrètement de mettre en place un réseau social pour les Cubains, un « Twitter cubain », avec l'objectif à plus long terme de susciter une opposition politique. Les principaux administrateurs de l'USAID le nièrent, mais plusieurs documents démentent leur désaveu[18]. Comme le rapporte l'Associated Press,

après avoir examiné en détail plus de 1 000 pages de documents : « Les documents montrent que le gouvernement des États-Unis prévoyait de constituer un parc d'abonnés par le biais de "contenus non controversés" : des messages d'actualité sur le football, de la musique, et des informations sur les ouragans. Dans un second temps, une fois que le réseau aurait atteint une masse importante d'abonnés, peut-être des centaines de milliers, les opérateurs introduiraient alors du contenu politique destiné à inciter les Cubains à organiser des "smart mobs" – des rassemblements de masse déclenchés à l'improviste – et qui pourraient d'une seconde à l'autre ainsi amorcer un Printemps cubain, ou, comme l'indique un document de l'USAID, "renégocier l'équilibre des pouvoirs entre l'État et la société[19]." »

Ils donnèrent à ce réseau le nom de ZunZuneo qui, en argot cubain, signifie « le chant du colibri ». Puis, à partir des réactions et des réponses des utilisateurs, ils commencèrent à dresser un profil des abonnés cubains. Ainsi, une contractuelle de l'USAID était chargée, à partir des réponses formulés par les abonnés à certains sujets, de les classer dans les rubriques « pro-révolution », « apolitique » ou « antirévolution[20] ». Selon l'Associated Press, cette employée a « recueilli un échantillon de plus de 700 réactions et les a analysées selon deux variables. La première était le niveau d'intérêt pour les messages reçus, et la seconde concernait la nature politique de la réponse. Dans son rapport, elle indique que 68 % des réponses montraient un intérêt modéré pour les SMS[21] ».

Dans une autre opération, « l'USAID a divisé la société cubaine en cinq segments, en fonction de leur loyauté au gouvernement. À une extrémité on trouvait le "mouvement démocratique", qualifié d'"encore (largement) insignifiant", et de l'autre on trouvait les "partisans de la base", surnommés péjorativement les "Talibans"[22] ». Le principal objectif de ce projet, selon l'Associated Press, était d'« inciter plus de personnes à rejoindre le camp des activistes pro-démocratie sans être repérées[23] ». Une analyse approfondie des documents de l'USAID révèle que « leur objectif stratégique à Cuba était de "de les faire sortir de l'impasse grâce à des initiatives tactiques et temporaires, et de relancer le processus de transition vers un changement démocratique"[24] ».

Au mois de mars 2011, ZunZuneo comptait environ 40 000 abonnés. Aucun d'entre eux n'avait la moindre idée que ce réseau social avait été créé, soutenu et alimenté par les employés de l'USAID. Aucun d'eux ne s'est rendu compte que les textos étaient analysés par l'USAID afin de déterminer les tendances politiques de chacun. Aucun d'eux n'a soupçonné que cette messagerie avait pour but de les politiser.

Pour dissimuler tout cela, l'USAID a mis en place « un système labyrinthique de sociétés-écrans utilisant un compte bancaire aux îles Caïmans, et a recruté des cadres qui ignoraient tout des liens de la société avec le gouvernement des États-Unis », selon l'enquête de l'AP. Par le biais d'une société britannique, L'USAID a également constitué une entreprise en Espagne pour administrer ZunZuneo. Enfin, ils ont créé un site internet partenaire du service de messagerie afin que les utilisateurs de téléphones portables puissent souscrire, émettre des réactions et envoyer des messages eux-mêmes gratuitement. Et, comme le révèlent les documents, ils ont cherché un moyen de donner une façade légitime à l'entreprise : « Des imitations de bannières publicitaires donneront au site l'apparence d'une entreprise commerciale », indique un document. Le plus important, comme le signale l'AP, « "est qu'il ne sera jamais fait mention d'une quelconque participation de l'État américain", selon une note de service datée de 2010 de Mobile Accord, l'un des sous-traitants du projet. "C'est absolument crucial pour le succès à long terme de la Mission"[25] ». L'équipe de ZunZuneo a même recruté un artiste satirique originaire de La Havane pour donner une saveur cubaine aux messages de type Twitter.

ZunZuneo ferma au milieu de l'année 2012, lorsque l'USAID n'eut plus les moyens de le financer. Lorsque le programme fut dévoilé, le sénateur Leahy a tenu des audiences au Congrès au printemps 2014, qui ont confirmé ces faits.

#

Lancé en 2007, le programme Prism permet à la National Security Agency (NSA) d'accéder aux données de Google, Facebook, Microsoft, Yahoo, PalTalk, YouTube, Skype, AOL, Apple, et d'autres, pour à peine plus de 20 millions de dollars par an, une

somme dérisoire pour un programme de renseignement[26]. Conjointement avec d'autres logiciels, comme le programme XKeyscore, Prism « permet aux responsables de collecter des données aussi diverses que les historiques de recherche, les contenus des e-mails, les transferts de fichiers et les discussions instantanées » ; ils peuvent extraire les contacts e-mail d'une personne, les activités des utilisateurs, le webmail, ainsi que tous les contacts mentionnés dans les e-mails (destinataires, expéditeurs, contacts en « cc » et en « cci »)[27]. En utilisant d'autres programmes et outils, comme DNI Presenter, ils peuvent « lire le contenu des e-mails stockés », « lire le contenu des messages Facebook, privés et publics » et « connaître les adresses IP de chaque personne qui visite un site internet ciblé par l'analyste[28] ». De plus, la NSA a « développé des méthodes pour craquer le cryptage en ligne de protection des e-mails, ainsi que les données bancaires et médicales », lui donnant accès à toutes nos informations privées et protégées par la loi[29]. La masse de données pouvant potentiellement être collectées est tout simplement stupéfiante. Déjà en 2010, le *Washington Post* rapportait que « chaque jour, les systèmes de collecte de la NSA interceptent et stockent 1,7 milliard d'e-mails, d'appels téléphoniques et d'autres types de communication[30] ».

Le programme Prism permet à l'État d'accéder aux e-mails des individus, à leurs photos, vidéos, pièces jointes, Voix sur IP, etc. À un coût pratiquement nul pour le gouvernement, il fournit un accès presque complet à leur vie numérique. Et, bien que la NSA ait nié avoir un accès immédiat à ces données, les documents de la NSA divulgués par Edward Snowden établissent que l'agence « revendique "la collecte directement auprès des serveurs" des principaux fournisseurs des États-Unis"[31] ». Bart Gellman du *Washington Post*, après avoir mené une enquête approfondie sur le programme Prism, affirme que « depuis leurs postes de travail, n'importe où dans le monde, les employés du gouvernement américain habilités à accéder à Prism ont pu mettre le système "en charge" – c'est-à-dire lancer une recherche – et recevoir des résultats d'une compagnie du secteur internet sans plus d'intervention auprès du personnel de ce fournisseur d'accès[32] ». Les preuves de cette coopération sont visibles dans cette diapositive classifiée de la NSA et divulguée par Snowden en juin 2013 :

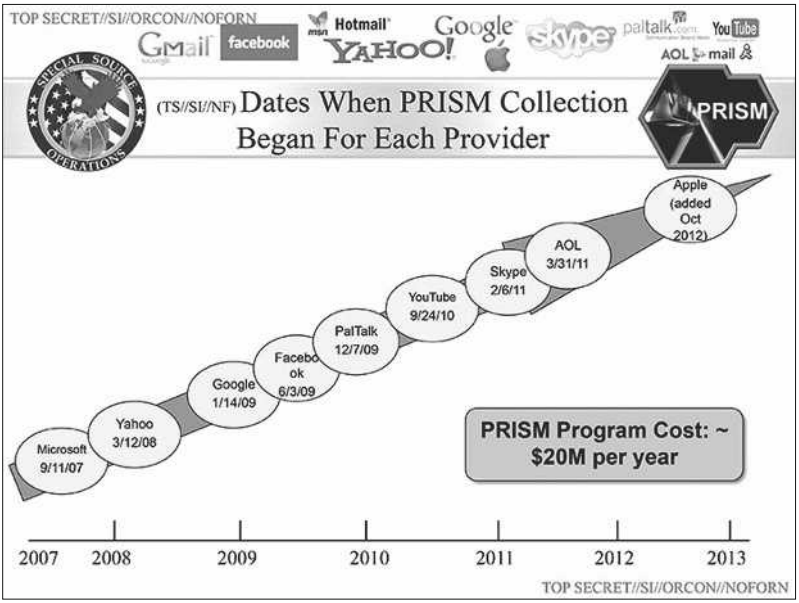


FIGURE 1.1. Diapositive PowerPoint, classée top secret, utilisée par la NSA pour décrire l'histoire du programme Prism (2013).
*Source* : « NSA Slides Explain the Prism Data-Collection Program », *Washington Post*, 6 juin 2013.

Comme le rapporte Glenn Greenwald du *Guardian* : « Le programme Prism permet aux services de renseignements d'accéder directement aux serveurs des entreprises. Le document de la NSA note que les opérations bénéficient de "l'assistance des opérateurs des services de communication aux États-Unis"[33]. » Le *Guardian* a expliqué, sur la base d'un document de la NSA daté d'avril 2013 : « Le programme Prism permet à la NSA, la plus grande organisation de surveillance au monde, d'obtenir des communications ciblées sans avoir à en faire la demande aux fournisseurs de services et sans avoir à obtenir d'ordonnance judiciaire. Grâce à ce programme, la NSA est en mesure d'accéder directement aux serveurs des entreprises participantes et d'obtenir des communications stockées, ainsi que

d'effectuer des collectes en temps réel sur des utilisateurs ciblés[34]. » Cela permet à la NSA d'obtenir toutes sortes de données – comme l'illustre cette autre diapositive pédagogique classifiée de la NSA, divulguée par Snowden au *Guardian* en juin 2013 :

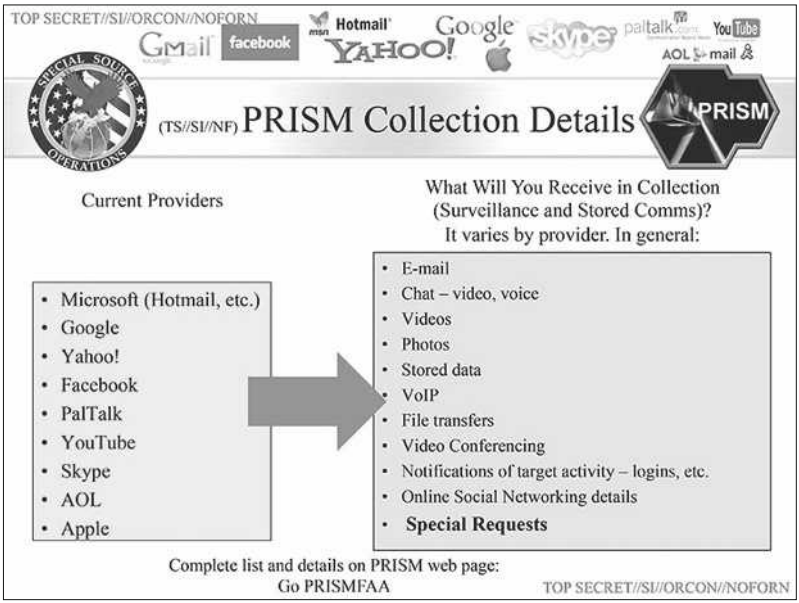


FIGURE 1.2. Diapositive Powerpoint de la NSA, classée top secret, sur certains détails du programme Prism (2013).
*Source* : « NSA Slides Explain the Prism Data-Collection Program », *Washington Post*, 6 juin 2013.

Selon le *Guardian*, il n'est pas nécessaire d'obtenir un mandat ou une autorisation individuelle en vertu de la loi sur la surveillance du renseignement étranger (FISA) pour ces activités de collecte et d'analyse, tant que l'analyste recherchant les communications a « un doute raisonnable que l'une des parties se trouvait à l'extérieur du pays au moment où les documents ont été collectés par la

NSA[35] ». Le programme est apparemment en train de conduire à une croissance exponentielle des requêtes de recherche. « Le document met en lumière l'augmentation de 248 % pour Skype du nombre de communications obtenues en 2012 – où il est fait remarquer dans les notes qu'il y "avait une augmentation exponentielle des signalements Skype ; il semble que notre aptitude contre Skype commence à être connue [des analystes du renseignement]" », rapporte le *Guardian*. « Il y a eu également une augmentation de 131 % des requêtes pour les données Facebook, et de 63 % pour Google[36]. »

* * *

Dans notre frénésie numérique à partager nos photos et mises à jour, à envoyer nos SMS, à vidéo-chatter avec nos proches, à nous « quantifier » nous-mêmes, nous nous exposons en nous rendant pratiquement transparents pour quiconque possède un tant soit peu de compétences technologiques. Nous nous exposons en laissant derrière nous des pétaoctets de traces électroniques, des traces qui peuvent être collectées, recoupées et amalgamées, des traces qui, paradoxalement, même si elles sont virtuelles, sont devenues plus tangibles, plus vérifiables et plus stables que notre moi analogique. Ernst Kantorowicz avait parlé des deux corps du roi, mais la métaphore s'appliquerait mieux aujourd'hui aux deux corps du sujet, ou, plutôt, du citoyen d'une démocratie libérale : le moi numérique aujourd'hui presque permanent que nous peaufinons dans le nuage virtuel à chaque clic et à chaque frappe, et le moi plus mortel analogique, qui, par contraste, semble s'estomper comme la couleur d'un Polaroid.

Pour beaucoup d'entre nous, nous nous sommes retrouvés dans cette situation volontairement, avec tout l'enthousiasme et la passion dont nous sommes capables, en souscrivant joyeusement et pleinement aux médias sociaux et à l'achat en ligne, en bombardant nos proches de SMS et en faisant des recherches sur Google. Beaucoup d'entre nous se livrent et exposent leur être le plus intime en faisant état de leur goût et de leur désir ; notre envie d'attirer l'attention et la gratuité de cette forme de publicité se combinent de manière toxique pour nous inciter à partager des informations intimes sur Facebook, à afficher nos CV et nos expériences sur des sites web

# Table

QUATRIÈME PARTIE

## La désobéissance numérique