

Où tu vas, j'y serai toujours

Finn Brunton

L'étudiant de Prague (1913), l'une des premières histoires fantastiques à avoir été portée à l'écran, traite de la forme d'apparition la plus inquiétante qui soit¹. L'étudiant qu'évoque le titre, un jeune duelliste fougueux nommé Balduin (Paul Wegener), cherche à séduire une femme d'un rang supérieur. Il conclut un pacte avec Scapinelli, un étranger plein de sollicitude qui lui offre une fortune en échange de n'importe quel objet se trouvant chez Balduin. Et que choisit Scapinelli ? Le reflet de Balduin, qu'il appelle à sortir du miroir. Dès lors, Balduin n'apparaît plus dans les miroirs, et son *doppelgänger* se fait passer pour lui – tuant un homme dans un duel auquel Balduin avait juré de ne pas participer, entre autres. À chaque étape, son double – qui est lui et en même temps n'est pas lui – est présent, empoisonnant ses relations intimes et gâchant ses opportunités ; on le confond avec lui à des moments critiques, ce qui conduit au désastre. Quand ils se rencontrent dans un cimetière, son double lui fait une promesse terrifiante : « Où tu vas, j'y serai toujours, jusques au dernier de tes jours, où j'irai m'asseoir sur ta pierre. »

Paul Wegener était également réalisateur. Il fit des films sur le Golem de Prague, et ce furent des récits de Golem, de démons et de forces surnaturelles toutes-puissantes qui dominèrent le folklore imaginaire de l'informatique au cours de la seconde moitié du XX^e siècle. C'était des êtres qui prenaient tout au pied de la lettre, sans relâche, dont les pouvoirs étaient illimités ; ils répondaient à leurs ordres avec une efficacité terrifiante, et parfois retiraient leur laisse. « Si nous cherchons la victoire sans savoir ce que nous entendons par là, c'est le fantôme qui viendra toquer à la porte », dit Norbert Wiener dans les années 1950, mettant en garde contre les conséquences possibles de l'informatisation, de la cybernétisation et de l'automatisation de la société – et tout particulièrement l'usage des ordinateurs et de la théorie des jeux pour contrôler l'arsenal nucléaire américain². (Wiener fait ici référence au récit fantastique de W. W. Jacobs, *The Monkey's Paw*, dans laquelle des parents demandent de l'argent grâce à un talisman. L'argent arrive : c'est le paiement d'une assurance pour leur fils, mort dans un accident à son usine. Ils demandent alors au talisman son retour, et celui-ci revient – mais il n'est plus *vivant*³). L'essor d'Internet, des réseaux sociaux, de l'informatique mobile et le brouillage entre ce qui est en ligne et hors ligne a donné naissance à un nouveau lexique du fantastique pour comprendre les dangers auxquels nous faisons face, qui commence par

l'invitation de Scalpinelli à faire sortir dans la pièce le reflet : non pas des Golem, mais des fantômes.

Parce que bien sûr, il existe beaucoup de « vous » différents. Il y a le vous qui est en train de lire ceci, dans un corps (vraisemblablement) qui répond à un nom, avec des traits, des souvenirs et un certain contexte social. Mais beaucoup d'autres répondent à ce nom, à cette série de traits, à cette position dans un réseau social. Les contours de certains de ces « vous » sont dessinés par les empreintes digitales de navigateurs, les supercookies et Javascript pour des réseaux de traçage publicitaire qui murmurent entre eux tandis que vous naviguez de page en page, d'application en application. L'un vit sur Facebook, l'autre sur WeChat, l'autre dans la base de données d'une agence de notation de crédit et d'une banque, l'autre dans les données de votre accéléromètre, de votre compteur de pas et de durée de sommeil, d'autres encore dans les collections et dossiers de la sécurité d'État et des services de surveillance. L'agence du renseignement britannique, le GCHQ, dispose d'une suite d'outils pour analyser les milliards d'éléments interceptés qu'elle accumule, où figure notamment un « outil d'enregistrement des traces laissées sur Internet » nommé SAMUEL PEPYS, qui produit une sorte de « journal » en temps réel de l'activité en ligne d'une cible⁴. Pepys était l'un des plus grands diaristes de langue anglaise, et le fait d'avoir choisi son nom est extraordinairement parlant : plus que la production d'une subjectivité riche, unique, privée, interne exprimée dans l'œuvre qu'est un journal intime, voilà le type d'archive qui compte – pour leurs objectifs, c'est une trace plus vraie et plus utile que n'importe quelle explication qu'une personne pourrait donner d'elle-même. Nous avons ainsi ajouté à la liste de ce qui hante traditionnellement les hommes (souvenirs, regrets, tâches inachevées, vies qu'on aurait pu connaître) une nouvelle catégorie : une population entière de *doppelgängers* pour chacun de nous – certains d'entre eux se renforçant, nous remplaçant et agissant en notre nom. En pratique, nous sommes en train de vivre cette scène d'horreur du cinéma, lorsque nous regardons dans le miroir et que quelqu'un nous fixe en nous renvoyant un sourire que nous n'avons pas fait.

Au moins, Balduin connaît l'origine de ses ennuis, son double singulier : ils se rencontrent dans la forêt tandis que son reflet s'éloigne du duel qu'il avait promis de ne pas livrer, nettoyant le sang de son épée. Il est possible que nous ne soyons jamais au courant des péchés que nos nombreux doubles ont commis en notre nom, directement ou indirectement, faisant de nous des personnes intéressantes pour la police, nuisant à notre capacité à obtenir des assurances ou des prêts, voire nous offrant des prix proportionnellement plus élevés pour les mêmes biens. Nos doubles peuvent rendre publics notre

grossesse, notre orientation sexuelle, nos parti-pris militants, nos habitudes et déplacements – quelle que soit notre envie de les garder secret. Plus inquiétant encore, ils sont bien souvent des doubles imparfaits, des copies qui ne nous ressemblent qu'à peine, parfois seulement à cause d'une homonymie ou de faits mineurs, et ils sont toutefois toujours en mesure d'influencer et d'interférer avec nos existences. Tandis que les données sont assemblées, revendues, partagées et soumises à des outils analytiques de plus en plus puissants, ils apparaissent aux endroits les plus étranges. Nous nous sommes rencontrés « chez vous », dit le mystérieux homme pâle à Fred Madison dans *Lost Highway* de David Lynch⁵. « En fait, j'y suis en ce moment même », ajoute-t-il pendant qu'ils parlent lors d'une réception – et il demande à Madison d'appeler sa propre maison pour en obtenir la confirmation, l'homme pâle restant à ses côtés. Et à l'autre bout du fil, quelqu'un répond : « je t'avais bien dit que j'étais là ». Votre double fantomatique a déjà votre téléphone ; en fait, il est même actuellement généré par lui, puisque le téléphone produit des données au sujet de son emplacement physique et de sa proximité avec les autres appareils. « Où tu vas, j'y serai toujours. »

Telle est notre histoire de fantômes, et nous la vivons chaque jour – un nouveau « vague de *doppelgängers* » pour faire écho à celle que Friedrich Kittler identifie à l'époque de *l'Étudiant de Prague*, quand les réalisateurs exploraient l'étrangeté de ce nouveau médium⁶. Mais il ne s'agit pas d'un fantasme inquiétant de dépersonnalisation et d'identité énigmatique. C'est une situation bien réelle, qui peut déboucher sur une discrimination *de facto*, sur des injustices économiques et politiques. La solution provisoire et facétieuse qu'Helen Nissenbaum et moi-même proposons dans notre ouvrage *Obfuscation* consiste à reconnaître cette condition et à multiplier grandement le nombre de doubles – réduisant ainsi leur valeur et leur fiabilité – à travers la production délibérée d'informations trompeuses, ambiguës et prêtant à confusion⁷. Pourquoi ne pas noyer le signal sous le bruit ?

Le cœur de notre proposition précède les technologies numériques, mais nous affirmons qu'il s'y applique de façon très pertinente – une sorte d'atavisme anticipé, une réponse qui a précédé le stimulus. En 2009, Helen travaillait avec des développeurs sur le projet TrackMeNot⁸, un plugin de navigateur qui générait des requêtes qu'il adresserait à Google (ou tout autre moteur de recherche de votre choix) pour que vos journaux de recherches ne puissent produire une image précise de vos intérêts, problèmes et besoins : ainsi, les requêtes « lampe halogène » ou « symptôme de commotion » venaient-elles de vous ou du plugin ? De mon côté, j'étudiais les débuts de

l'histoire de l'informatique dans le développement du radar pendant la Seconde Guerre mondiale – une histoire qui implique des leurres, des rubans d'aluminium largués depuis des avions pour créer de « faux échos », des signaux ressemblant à des avions sur les radars, rendant ainsi beaucoup plus difficile la coordination des attaques anti-aériennes. En parlant, nous avons réalisé que ces deux exemples, avec des technologies différentes, des buts et contextes différents, possédaient une structure similaire : quand on ne peut pas échapper à l'observation, il faut générer un grand nombre de signaux additionnels – donner à son adversaire *plus* de l'information qu'il recherche, beaucoup plus.

Nous avons trouvé de nombreux exemples de cette approche, de la surdivulgarisation délibérée de documents juridiques à la conception de services de téléphonie basés sur la localisation, du fonctionnement de l'outil de communication anonyme Tor aux défenses sophistiquées des araignées *Araneidae*. Toutes, numériques ou analogiques, temporaires ou permanentes, suivent le même modèle. Pour obtenir un itinéraire sur son téléphone, il faut divulguer son emplacement et sa destination ; pour attraper des insectes dans sa toile, il faut être exposé aux oiseaux et aux guêpes. Parfois, il n'existe pas de meilleures méthodes de dissimulation, de refus ou de disparition et notre meilleure approche – si nous avons une certaine idée de ce que recherche notre adversaire – consiste à créer une multiplicité de cibles. Le but est bien différent : l'araignée (qui a développé une stratégie consistant à laisser des fausses « araignées » sur la toile pour tromper les prédateurs) gagne quelques secondes pour s'échapper ; l'utilisateur de smartphone, avec une application qui fait une série de requêtes directionnelles différentes puis extrait celle qui est pertinente pour le client, obtient l'information dont il a besoin tout en protégeant ses données d'une mauvaise utilisation future. Certaines techniques d'obfuscation fonctionnent mieux avec une foule d'utilisateurs créant de la confusion, d'autres avec seulement quelques obfuscateurs ; certaines fonctionnent mieux si l'adversaire sait qu'elles sont appliquées, d'autres si elles sont gardées secrètes ; certaines fonctionnent mieux rapidement, d'autres lentement. Toutes transposent la question allégorique posée par G. K. Chesterton : « Où cacheriez-vous une feuille ? – Dans la forêt. » Et s'il n'y a pas de forêt ? Il fait pousser une forêt pour l'y cacher – c'est l'obfuscation.

Cependant, faire pousser cette « forêt » – envoyer de fausses requêtes de recherche, générer des identités alternatives sur les réseaux sociaux, inonder les hashtags pour diluer leur utilité – n'est pas seulement une défense de la vie privée. Ce peut aussi être un geste de contestation : si nos données sont mal utilisées, transformées, manipulées sans notre consentement, une des

réponses à apporter consiste à rendre ces données pires – de façon indiscriminée ou d’une façon méticuleuse et ciblée. Nous en trouvons des exemples depuis la résistance aux réseaux sociaux modérément coercitifs jusqu’aux stratégies pour déjouer le profilage policier et les analyses des marchés publicitaires. L’un des développements techniques les plus intéressants dans l’obfuscation se trouve dans les logiciels qui peuvent modifier les données de l’utilisateur pour qu’elles ne servent qu’un seul but, apportant la fonctionnalité dont a besoin l’utilisateur sans être adaptable à des finalités non voulues et non prévues : publicités ciblées, tarification d’assurance discriminatoire ou toute autre appropriation non désirée.

Nous suggérons ainsi de retourner contre elle-même la logique qui produit toutes nos troublantes identités numériques. Un reflet est un persécuteur, et dix fantômes numériques façonnés à partir de nos données nous enferment dans nos propres traces. Mais un millier de reflets, dilués, extrêmement différents, ennuyeux, à la réalité ambiguë, forment une foule dans laquelle on peut disparaître pour le moment, devenant nous-mêmes des fantômes.

Notes

1. Hanns Heinz Ewers et Stellan Rye, *L’Étudiant de Prague*, 1913.
2. Norbert Wiener, *Cybernetics, or Control and Communication in the Animal and the Machine*, Cambridge (Ma.), MIT Press, 1961 (2^e éd.), p. 177.
3. W. W. Jacobs, « The Monkey’s Paw », in Jacobs, W. W., *The Lady of the Barge*, New York, Harper & Brothers, 1906.
4. Voir « GCHQ Profiling : An Appendix » indiqué par Ryan Gallagher, « Profiled: From Radio to Porn, British Spies Track Web Users’ Online Identities », *The Intercept*, 25 septembre 2015.
5. David Lynch, *Lost Highway*, October Films, 1997.
6. Friedrich Kittler, *Gramophone, Film, Typewriter*. Stanford (Ca.), Stanford University Press, 1999, p. 155.
7. Finn Brunton et Helen Nissenbaum, *Obfuscation: A User’s Guide for Privacy and Protest*. Cambridge (Ma.), MIT Press, 2015.
8. <http://cs.nyu.edu/trackmenot/fr/>