Avant-propos

La Calomnie d'Apelle*, Sandro Botticelli, 1495. Source : The Yorck Project, 10.000 Meisterwerke der Malerei. DVD-ROM, 2002. ISBN 3936122202. Distribué par DIRECTMEDIA Publishing GmbH*

La Calomnie d'Apelle est l'une des œuvres majeures du Maître Sandro Botticelli. Réalisée en 1495, elle met en scène une dizaine de déesses mineures de la mythologie grecque. Héra, déesse trompée, apprend que l'héroïne divinisée Sémélé est enceinte de Dionysos. Furieuse de cette nouvelle infidélité, Héra part à la recherche d'Apaté,

la déesse de la ruse. Elle espère ainsi empêcher Sémélé de devenir la nouvelle reine des cieux à sa place. Pour conserver sa position, Héra demande à Apaté de lui prêter sa ceinture de ruse qui fera revenir son mari et son fils. Celui qui porte cette ceinture peut faire faire n'importe quoi à la personne qu'il désire. Apaté obéit à Héra et ouvre ainsi la boîte de Pandore, source de mille maux et tromperies qui se répand sur Terre.

Sur le côté droit du tableau de Botticelli figurent les déesses mineures : Apaté (la ruse), Agnoia (l'ignorance), Diabole (la calomnie), Epiboule (la roublardise), Hypolepsis (la méfiance), Métanoia (le regret), Ptéropode (l'envie). Sur le côté gauche, Aletheia, déesse de la vérité, lève sa main droite face aux menaces qui s'agitent.

Traversant plus de cinq siècles, cette extraordinaire œuvre représente à la perfection les déesses majeures de la cybersécurité qui opèrent sur un cyberespace toujours plus en proie aux attaques et aux tromperies numériques. La mythologie grecque n'a pas fini de nous surprendre dans sa modernité et sa capacité à projeter les passions des humains sur ses dieux. Deux millénaires plus tard, la projection des concurrences, des conflits, des duels et des faiblesses humaines a quitté l'espace mythologique pour investir l'espace numérique, mais ses déesses mineures sont toujours là, à la manœuvre, juste derrière nos claviers et nos écrans...

Introduction

Le XX^{e} siècle a été celui de l'accélération du progrès technologique avec des innovations qui ont transformé notre environnement et influencé nos actions. La révolution numérique, que l'on devrait objectivement nommer « ère de Turing », débute dans les années 1930 avec les travaux fondateurs d'Alan Turing (1912-1954), père de l'informatique actuelle, sur la calculabilité, les machines de Turing et le problème de l'arrêt. Parallèlement, les travaux d'Andréï Kolmogorov (1903-1987) sur la théorie algorithmique de l'information et sur la complexité ont permis la découverte de nouveaux territoires dans le domaine du calcul. L'informatique moderne porte l'ADN des géants Turing et Kolmogorov. Nos interactions avec les machines électroniques, petites ou grandes, connectées ou non, sont les feuilles d'un arbre planté par Turing et Kolmogorov. Nous leur sommes redevables lorsque nous utilisons notre messagerie électronique ou lorsque nous achetons un objet sur Internet. Nos faits et gestes numériques portent leurs traces. Bien entendu, ils ne sont pas les seuls contributeurs à l'édifice informatique des sept dernières décennies, mais leurs apports ont été décisifs pour l'avènement d'un cyberespace fonctionnel.

Nous avons presque toutes et tous, aujourd'hui, une vie numérique, plus ou moins trépidante, qui s'incarne durant les heures de travail, les périodes de loisirs et de repos. Nos pratiques quotidiennes des systèmes électroniques, nos interactions volontaires ou non avec des machines produisent des volumes toujours plus importants de données. Ces traces numériques en disent beaucoup sur nos habitudes, nos goûts, nos choix. Elles constituent désormais un reflet fidèle de nos activités. En termes d'information, ce reflet numérique concentre une partie de notre image projetée selon des algorithmiques exécutés sur des machines.

Le concept de trace numérique

Une trace numérique peut être définie comme un ensemble de mots binaires (mots de longueur finie formés de 0 et de 1) constituant un fichier créé et archivé sur un système à la suite d'une interaction, volontaire ou subie, entre un utilisateur humain et ce système. La trace numérique naît de la capacité de stockage d'une donnée de manière durable sur un support magnétique ou électronique. L'exécution d'un programme sur un système disposant de capacités de calcul nécessite souvent des données d'entrée pour initialiser le calcul et fournir le résultat en sortie (données de sortie). Durant le calcul, des données collatérales, ou métadonnées, peuvent être créées et stockées. Les données de sortie et les données collatérales stockées sur le système forment la trace numérique née de l'interaction homme-système (figure I.1).

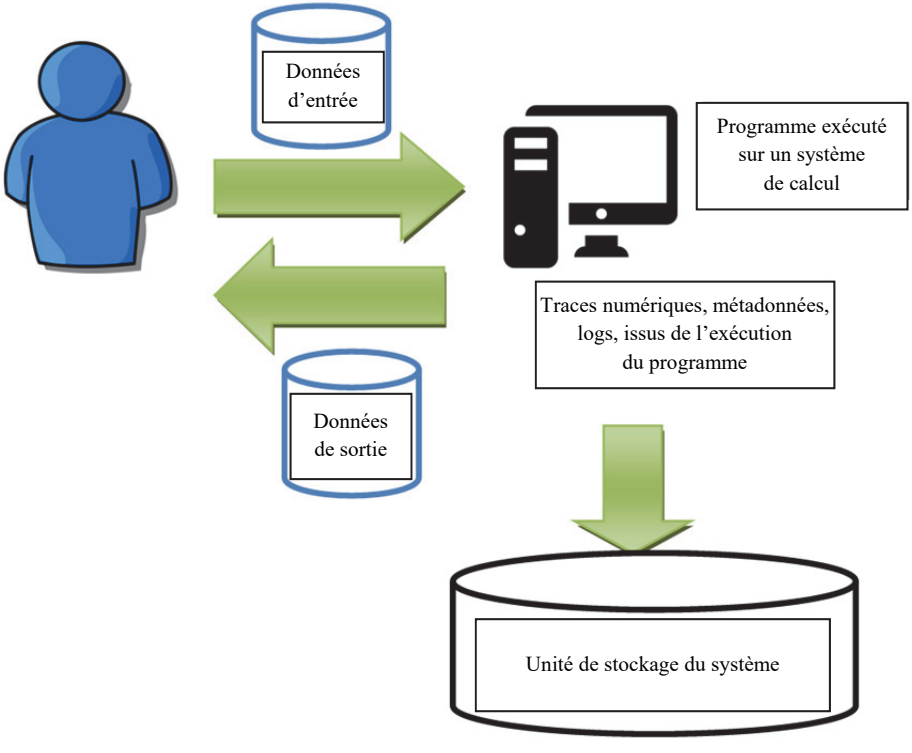

Figure I.1. *Mécanisme de création de traces numériques*

Dans la pratique, il existe peu d'interactions homme-système qui ne produisent pas de trace numérique. Une journée d'activité dans la vie d'un citoyen ordinaire d'un

pays technologiquement développé correspond à une journée de production de traces numériques. L'utilisation d'un téléphone portable engendre des traces qui permettent de géolocaliser et d'identifier l'utilisateur avec une très forte probabilité. Trois traces de bornage suffisent pour l'identifier avec plus de 95 % de certitude. Sur une autoroute payante, le passage à un péage routier et le paiement par badge produisent des traces numériques qui permettent de retrouver très précisément l'itinéraire et les horaires du déplacement. De la même façon, l'usage d'une carte de transport lors de voyages en train ou bus induit la création de traces numériques qui archivent les détails du déplacement. Dans l'entreprise, les opérations de pointage par badge électronique produisent des traces qui renseignent sur la présence de l'employé sur son lieu de travail. Au supermarché, les puces radiofréquences remplacent les codes-barres sur les produits. Elles sont d'importants vecteurs de traces numériques qui, une fois exploitées, révèlent les choix, les préférences, les habitudes d'achat du consommateur. Il est alors possible de caractériser un individu par son panier d'achats et par le lieu et l'horaire de la transaction. Le secteur de la santé est une source importante de traces numériques. En France, la mise en place du dossier médical personnel (DMP) permet de mieux suivre le patient et ses pathologies en consignant chaque acte médical et chaque examen réalisé. Même anonymisées, les traces associées numériques associées au DMP en disent long sur nos pratiques de santé. Le transport aérien s'est doté d'un large éventail d'outils numériques dédiés à la sécurité des vols. Le PNR (*Passenger Name Record*) est composé de données personnelles de tous les passagers d'un même avion. Il permet une traçabilité optimale avant l'embarquement et s'inscrit dans une politique de lutte contre le terrorisme. Les traces numériques qui en résultent permettent d'établir des profils type de voyageurs et interviennent dans le calcul du risque associé à un profil donné. Sur Internet, le commerce en ligne s'appuie sur une connaissance de plus en plus fine du consommateur, de ses pratiques et de ses préférences. Le marketing personnalisé exploite les traces issues des transactions commerciales. Les objets connectés sont autant de générateurs de traces produites par leurs capteurs. Les systèmes de vidéo-surveillance dotés de capacités de reconnaissance faciale complètent la construction de l'identité numérique par l'image.

L'ensemble croissant des traces numériques d'un individu rassemble les traces volontaires issues d'interactions décidées par l'utilisateur et les traces involontaires produites lors d'interactions automatiques avec un système. Les traces volontaires peuvent provenir de messages, photos et vidéos postés sur un blog ou sur les réseaux sociaux, de données publiées sur un CV en ligne, des avis laissés sur des sites de commerce en ligne, de données insérées dans un formulaire ou de profils renseignés sur un forum. Les traces involontaires sont créées durant la visite d'un site web. L'adresse IP, le système d'exploitation et les dernières pages visitées par l'utilisateur peuvent apparaître sous forme de traces. Les requêtes et mots clés saisis sur un moteur

de recherche sont enregistrés et produisent des traces signifiantes. Les *cookies* (un court fichier déposé sur la machine du visiteur d'un site web) sont vecteurs de traces. La réunion de toutes les traces numériques, volontaires ou non, produites par un individu engendre son identité numérique. Pour autant, une trace n'a de sens que lorsqu'elle est associée à un contexte et celui-ci n'est pas toujours connu ou accessible.

L'identité numérique

L'identité numérique d'un utilisateur se forme à partir de sources variées : les données personnelles associées à ses différents profils, les informations qu'il publie sur le Web, les informations que d'autres publient à son sujet et les traces qu'il laisse consciemment ou non sur des plateformes spécialisées.

L'identité numérique agrège des entités qui relèvent de l'opinion (ce que j'aime ou je déteste), la connaissance (ce que je sais), l'expertise (mon métier, mon expérience), la représentation (mon apparence), la localisation (comment et où me joindre), la réputation (ce que l'on dit de moi), l'expression (ce que je dis), la publication (ce que je partage), l'achat (ce que j'achète), l'audience (qui je connais). La mise en relation et le croisement de ces différentes entités permettent souvent de déduire de nouvelles informations sur l'individu tracé. La forte signifiance de l'ensemble des traces est souvent sous-estimée par l'utilisateur-producteur qui n'a qu'une perception locale de son empreinte numérique.

Le périmètre de l'identité numérique d'un individu varie fortement en fonction de sa psychologie.

Le chercheur Dominique Cardon [CAR 18] a proposé une typologie des formes de présence en ligne en décrivant cinq formats de visibilités organisés sur le duo identité numérique/type de visibilité recherchée :

– le paravent : il correspond au format « se cacher pour se voir » et s'incarne par exemple dans la fréquentation des sites de rencontre ;

– le clair-obscur : il correspond au format « se montrer caché ». Les participants rendent visible tout ou partie de leur intimité et de leur quotidien à un réseau social constitué de personnes proches ;

– le phare : il correspond au format « tout montrer, tout voir » dans le cadre d'une recherche de connectivité maximale ;

– la *lanterna magica* : il correspond au format « se voir mais caché » et à l'utilisation d'avatars pour dissocier identité réelle et virtuelle ;

– le post-it : il correspondant au format « je suis là, je fais ça ». Les participants rendent visibles à tous leur disponibilité et leur présence mais interagissent uniquement avec un cercle restreint.

Selon Dominique Cardon, cette typologie permet de définir quatre grandes classes d'identités numériques :

– l'identité civile est associée au format paravent. Elle se construit à partir de l'utilisation de plateformes comme Twitter, Facebook, Meetic. Associée à l'être et au réel, elle se réfère à l'éducation, la profession, la localisation, la disponibilité, au statut matrimonial, aux caractéristiques physiques, aux humeurs de l'individu ;

– l'identité agissante est associée au format phare. Elle résulte de l'utilisation des plateformes comme LinkedIn, Wikipédia, Flickr ou Peuplade. Elle reflète le contexte d'activités, les engagements sociaux, les pratiques amateurs, les passions et les communautés d'intérêts. Elle s'inscrit dans le réel et dans le faire ;

– l'identité narrative est associée au format clair-obscur et résulte de l'utilisation de plateformes comme Skyblog ou LiveJournal. Elle reflète le Moi caché, l'introspection, le récit de vie quotidienne, le journal intime ou littéraire et s'inscrit dans l'être et le projeté ;

– l'identité virtuelle est associée au format Lanterna Magica et résulte de l'utilisation des plateformes comme YouTube, MySpace, SecondLife ou World of Warcraft. Elle se construit sur des personnages d'emprunt, des profils de jeux en ligne, des avatars, des contenus autoproduits, des compteurs d'audience, des scripts. Elle s'inscrit à la fois dans le faire et le projeté.

Comme la somme des traces numériques se rapporte à un individu ou à une collectivité, l'identité numérique est constituée de données hétérogènes, plus ou moins persistantes dans le temps. Les plateformes qui ont généré des traces peuvent avoir disparu à l'heure où l'on observe ces données. La traçabilité de l'identité numérique n'est donc jamais totalement assurée sauf à disposer d'un historique exhaustif de l'ensemble des interactions numériques du profil examiné.

Les limites du concept de trace numérique

La trace numérique se limite à un ensemble fini de mots binaires stockés sur une unité d'archivage d'un système de calcul. La trace en tant que telle ne dit rien sur son origine : par qui a-t-elle été créée ? Selon quel algorithme mis en œuvre ? De quelle manière, volontaire ou simple interaction systémique ?

Ce manque d'information embarquée dans la trace rend sa formalisation difficile. L'attribution d'une trace à une source (son relèvement), requiert souvent des données additionnelles qui ne figurent pas dans la trace considérée. Si le concept de trace peut suffire dans le cadre d'une description non structurée de l'identité numérique, il s'avère insuffisant lorsqu'il s'agit de la caractériser plus finement ou de la catégoriser.

Les incertitudes limitant le concept de trace induisent les questions suivantes :

– comment peut-on identifier le système sur lequel la trace a été initialement produite ?

– quel algorithme mis en œuvre et exécuté sur ce système a produit cette trace ?

– quel individu est à l'origine de la trace ?

– comment peut-on certifier l'origine d'une trace ?

– à quelle identité numérique doit-elle être associée ?

Les apports du formalisme projectif

Dans son formalisme, la représentation projective d'une trace répond à ces questions et permet de caractériser l'identité numérique d'un individu en fonction des algorithmes mis en œuvre et des systèmes sur lesquels ils ont été exécutés, volontairement ou non, par un individu. Le concept de projection algorithmique enrichit celui de la trace en lui donnant, de manière déclarative, son origine et sa structuration algorithmique. Il permet de décrire formellement l'ensemble des traces par une approche ascendante (*bottom-up*) en partant de l'échelon le plus fin : la projection algorithmique d'un individu sur un système S selon un algorithme A exécuté sur ce système à un instant donné. La réunion des projections algorithmiques élémentaires créées sur un même système S par un individu donne alors naissance à sa S-projection. Enfin, la réunion de toutes les S-projections de l'individu constitue sa projection algorithmique globale témoignant de son identité numérique.

Si l'approche projective facilite la catégorisation des traces numériques, le formalisme des projections algorithmiques permet de définir de nouveaux invariants comme le niveau d'ubiquité d'un lieu et le consentement algorithmique d'un individu.

Concernant les segments de cybersécurité et de cyberdéfense, les projections algorithmiques interviennent naturellement dans le problème complexe de relèvement d'une donnée numérique : comment et par qui cette donnée a été produite ? Sur quel système et selon quel algorithme ?

Enfin, la représentation projective permet de formaliser la création d'architectures de données fictives (ADF) qui constituent souvent le vecteur d'entrée et l'initialisation de cyberattaques sophistiquées. L'usurpation d'identité numérique et la simulation de faux profils sur les réseaux sociaux admettent une description projective.

L'itinéraire choisi pour explorer le concept projectif

Notre étude propose une approche projective de la trace numérique s'appuyant sur un formalisme intégrant l'individu, le système et l'algorithme exécuté. Le concept large de trace est exploré sous un angle philosophique dans le chapitre 1. Nous montrons qu'il est insuffisant pour décrire les échanges d'information à l'origine de la formation des traces numériques. Il doit être remplacé par un concept projectif qui fait intervenir tous les acteurs de la trace : l'utilisateur humain, le système et l'algorithme.

Le formalisme complet décrivant les projections algorithmiques est exposé dans le chapitre 2. Celui-ci reste toutefois accessible à un lecteur non-spécialiste des mathématiques.

Consacré aux objets connectés, le chapitre 3 présente deux concepts inédits : le niveau d'ubiquité d'un lieu et le consentement algorithmique d'un individu.

Le chapitre 4 interroge la valeur de la donnée. Comment la décrire ? Comment se forme-t-elle en fonction du corpus de données ?

Les fausses données, premiers vecteurs d'insécurité numérique, matrices de cybercriminalité, sont étudiées sous l'angle projectif dans le chapitre 5 en insistant notamment sur les mécanismes puissants opérant sur les réseaux sociaux.

Consacré aux structures de données fictives, le chapitre 6 se concentre sur les cyberattaques à fort impact construites sur des projections algorithmiques fictives.

Le chapitre 7 intervient comme un épilogue prospectif analysant l'évolution probable de notre projection algorithmique globale sous l'effet de la convergence des technologies NBIC (nanotechnologies, biotechnologies, informatique et sciences cognitives).

Les lecteurs plus littéraires que scientifiques sont invités à prendre le temps nécessaire à la lecture des passages contenant du formalisme mathématique, à ne pas les sauter, car ces derniers sont rédigés en ce sens et ne nécessitent aucun prérequis mathématique.