



2. PAOLO CIRIO ÉCOLOGIE DE LA SOUS-VEILLANCE NUMÉRIQUE

L'économie de l'attention ne nous affecte pas, elle nous infecte, elle encrasse ces filtres subtils sans lesquels il n'est pas de discrimination saine entre les liens qui libèrent et ceux qui aliènent. Puisque leur monde est une pub, qui te vend de la réalité, puisqu'ils t'ont algorithmé jusqu'à l'amour, le jeu, le jouir, l'amitié. Puisqu'en te procurant, par la technologie, le pouvoir, ils t'ont retiré, en douce, la puissance¹.

L'ère numérique aurait fait basculer le capitalisme industriel dans un nouveau régime. C'est l'hypothèse du « capitalisme de plateforme » proposé par le philosophe Nick Srnicek² ou du « capitalisme de surveillance » que formulait il y a peu la sociologue et économiste Shoshana Zuboff³ et qui rejoignait ainsi une longue tradition critique de la surveillance médiatique. Depuis l'apparition d'Internet, de nombreux auteurs et activistes en ont fait leur terrain d'investigation. Pensons notamment aux défenseurs des libertés numériques, tels qu'en France l'autorité administrative indépendante CNIL ou

1. Alain Damasio, *Les Furtifs*, Marseille, La Volte, 2019. Paroles extraites de l'album *Entrer dans la couleur*, qui accompagne l'ouvrage, enregistré avec le guitariste Yan Péchin.
2. Nick Srnicek, *Capitalisme de plateforme: L'hégémonie de l'économie numérique*, Montréal, Lux éditeur, 2018.
3. Shoshana Zuboff, *The age of Surveillance capitalism: The Fight for a Human Future at the New frontier of Power*, New York, PublicAffairs, 2019.

l'association La Quadrature du Net⁴, par exemple, mais aussi aux chercheurs universitaires nouvellement engagés dans le domaine des « *surveillance studies*⁵ ». La surveillance est en effet devenue un véritable marché pour les multinationales du Web qui désirent capter et mieux orienter ou prescrire nos comportements et nos vies numériques. Par la récolte des données de navigation, par l'observation de toutes nos connexions et requêtes sur le Web, par la prescription de « nouveaux » actes – « liker », commenter, cliquer, souscrire, préférer, etc. –, les entreprises de la Silicon Valley ont fait de nos données numériques des produits monnayables sur le marché des prévisions comportementales⁶.

Peut-on se satisfaire de ce que disent de nous les réseaux neuronaux : ce que l'on aime, ce que l'on est, ce que l'on souhaite(ra)it être, faire, avoir, goûter, etc. ? Comment détourner ces « machines à (nous) gouverner » qui nous aliènent autant qu'elles nous sont devenues désirables, auxquelles nous adhérons le plus souvent avec une confiance aveugle ?

Le Web social, l'intelligence artificielle, les réseaux neuronaux sont en effet devenus le creuset d'une traçabilité sans précédent des comportements, de l'expression des goûts ou des dégoûts, et par extension, de l'ensemble des communications et relations interhumaines médiées⁷. Le moteur relationnel devenant celui

4. Voir La Commission nationale de l'informatique et des libertés (CNIL), www.cnil.fr et La Quadrature du Net, <https://www.laquadrature.net>.

5. Plusieurs réseaux d'investigation et de recherche se sont constitués durant les années 2000, dont <https://www.surveillance-studies.net> ou <https://www.sscqueens.org>.

6. Cf. Fabien Benoit, *The Valley. Une histoire politique de la Silicon Valley*, Paris, Les Arènes, 2019 ; revue *Esprit L'Idéologie de la Silicon Valley*, mai 2019.

7. Le philosophe Ignacio Ramonet y voit l'émergence d'un nouvel « empire de la surveillance », le durcissement d'un complexe sécuritaro-numérique qui succède au complexe militaro-industriel. Cf. Ignacio Ramonet, *L'Empire de la surveillance*, Paris, Galilée, 2015. L'ouvrage questionne les effets et conséquences de cette alliance sans précédent entre État, appareil militaire, sécurité et industries du Web, produisant ce qu'il nomme *l'empire de la*

de la séduction à tout prix, les individus « acceptent » de publier en ligne l'ensemble de leurs données personnelles, qu'ils cèdent par conséquent sans réserve aux multinationales du Net : pourvu que cela puisse concourir à améliorer leur image et à accroître leur réseau de relation à travers l'usage d'applications dont ils sont devenus dépendants. Cet « autre numérique », ce profil que les internautes ne cessent de chérir et d'enrichir, se voit ainsi augmenté, ou épaissi si l'on préfère, par l'ensemble des « traces » que laissent les usages des applications Internet et des réseaux sociaux. Le juriste Bernard Harcourt nous invite à voir dans cette surexposition moins une intensification qu'une « mortification » de soi, au sens où il évoque un renoncement à la liberté individuelle et une « servitude volontaire⁸ ». Cette dernière faisant le jeu des plateformes technologiques (notamment des GAFAM) qui investissent massivement dans le développement de l'intelligence artificielle et pour lesquelles les données personnelles constituent la matière première et une ressource de premier ordre. Un des principaux facteurs de développement de l'IA réside en effet aujourd'hui dans ce que d'autres analystes ont proposé d'appeler le « *digital labor* » où le labeur digital, une forme renouvelée et pas toujours perceptible d'exploitation de l'activité des usagers Internet (travail ou loisir, la frontière étant désormais devenue poreuse) et d'esclavagisation de leurs données. Cette exploitation subreptice mais continue de l'ensemble des « données personnelles » extraites de nos échanges publics aussi bien que privés affecte considérablement la vie démocratique et le libre arbitre des individus. Tous les domaines de notre vie numérique sont désormais concernés : loisir, travail, économie, politique, sociabilité, sexualité, etc. Sur l'ensemble de ces terrains,

surveillance « dont l'objectif très concret et très clair est de mettre Internet, tout Internet, et tous les internautes, sous écoute » (p. 20). Voir aussi, plus récemment : Olivier Tesquet, *À la trace. Enquête sur les nouveaux territoires de la surveillance*, Paris, Premier Parallèle, 2019.

8. Cf. Bernard Harcourt, *La Société d'exposition*, Paris, Seuil, 2020.

le contrôle et la prescription à distance des comportements est susceptible d'altérer l'autonomie des individus : jusqu'à influencer et modifier leurs pratiques à des fins simultanément économiques et politiques. Car la finalité de cette surveillance n'est pas uniquement financière : elle vise autant à contrôler qu'à « fabriquer » de nouveaux comportements⁹. De grands pans de l'expérience humaine se trouvent ainsi modélisés et instrumentalisés par toute une série d'applications ubiquitaires qui ordonnent le quotidien des individus et des collectivités. C'est là le plus grand paradoxe de cette nouvelle ère numérique : susciter le désir pour des applications qui confisquent le libre arbitre et aliènent les individus en leur offrant simultanément de nouveaux outils d'expression et de sociabilité.

Dans ce contexte, les créations de Paolo Cirio, artiste italien vivant à New York, hacker¹⁰ et activiste, éclairent les paradoxes aussi bien que les risques et dérives du contrôle et de la manipulation sociale de l'information et de la communication. Pour ce faire, elles s'attachent à parasiter les outils, les interfaces et les applications de la surveillance numérique : notamment les opérations de captation, de collecte et de traitement de nos données personnelles sensibles. L'artiste explore une multiplicité de supports – photographies, installations, vidéos, interfaces et algorithmes numériques – dans une démarche technocritique¹¹ des modèles sociaux, économiques, politiques et légaux de l'industrie du Web. Se réappropriant les

9. L'affaire Cambridge Analytica offre un bon exemple des dangers potentiels de ces manipulations de l'opinion et des comportements des citoyens. Voir notamment le documentaire *Comment Trump a manipulé l'Amérique*, Thomas Huchon, 2018. Et aussi, Brittany Kaiser, *L'Affaire Cambridge Analytica*, Paris, HarperCollins, 2020 ; Christopher Wylie, *Mindfuck. Le complot Cambridge Analytica pour s'emparer de nos cerveaux*, Paris, Grasset, 2020.

10. Cf. Steven Levy, *L'Éthique des hackers* [1984], Paris, Globe, 2013.

11. Cf. François Jarrige, *Technocritiques. Du refus des machines à la contestation des technosciences*, Paris, La Découverte, 2014 ; Andrew Feenberg, *Pour une théorie critique de la technique* [2010], Montréal, Lux éditeur, coll. Humanités, 2014.

données en libre accès sur Internet, il questionne notamment l'exploitation des informations et des images collectées en regard du droit privé et du droit d'auteur. Alors même que la transparence est érigée en nouveau principe éthique par nos sociétés contemporaines, ses œuvres proposent des contre-dispositifs panoptiques et invitent à une réflexion sur les notions d'anonymat, de vie privée et de démocratie.

Face to Facebook : renverser les technologies de manipulation sociale

L'œuvre *Face to Facebook* (2011), réalisée en collaboration avec l'artiste programmeur Alessandro Ludovico, procède du vol d'un million de profils d'utilisateurs Facebook et de leur traitement par des algorithmes de reconnaissance faciale (bots, agents logiciels automatiques ou semi-automatiques). À partir du piratage de la base de données, les deux artistes ont procédé à l'implémentation d'une sélection de 250 000 profils au cœur d'un site de rencontre en ligne fictif, inventé de toutes pièces, nommé Lovely-Faces.com.

Publiés à leur insu sur ce site de rencontre, les profils privés se voient ainsi exposés et mis en relation suivant certaines caractéristiques d'expression du visage définies de façon inhabituelle – sympathique, arriviste, sournois¹². Une intelligence artificielle se charge en effet de l'analyse des expressions faciales afin d'estimer le « taux de compatibilité » des utilisateurs et ainsi mieux provoquer leur rencontre potentielle. L'œuvre singe et parodie le pouvoir de Facebook et les dangers d'une véritable mainmise sur nos données, révélant l'insécurité de celles-ci et exposant littéralement les coulisses de leur exploitation technique via des logiciels de reconnaissance vocale, faciale et typographique. Devant l'omniprésence des médias sociaux, en réinjectant des « data privées » dans une farce drôle et néanmoins inquiétante et visible de tous, ce détournement

12. Cf. Paolo Cirio, *Face to Facebook*, 2011 : <http://www.lovely-faces.com>.

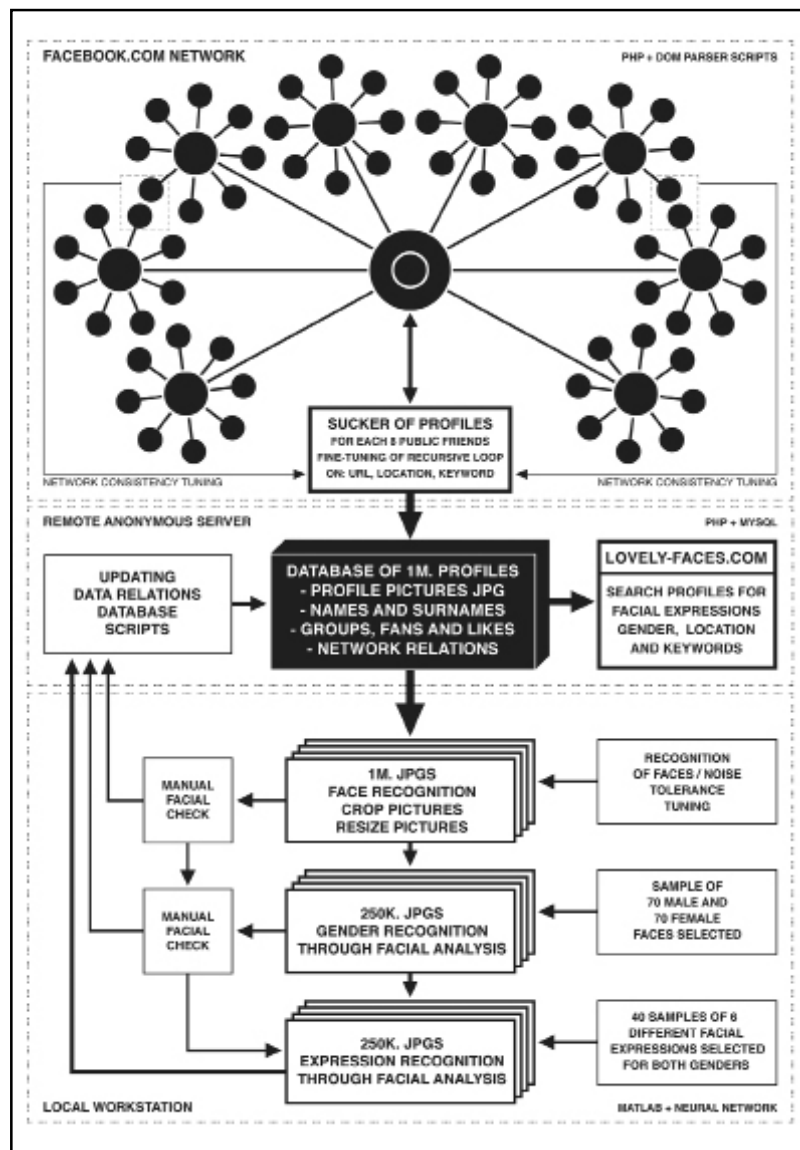


7-8. Paolo Cirio, Face to Facebook, 2011

de données se veut une mise en garde à grande échelle face aux risques du partage d'informations personnelles sensibles. Face to Facebook prend en effet le contrepied des réseaux sociaux pour mieux révéler les effets collatéraux de la confiscation des données : fuites, vols d'identité, cyber-attaques. Il va sans dire que l'entreprise artistique n'est qu'un pâle et ironique reflet des risques réels encourus par les internautes soumis aux logiques propriétaires et capitalistes des GAFAs. De nombreuses affaires en ont témoigné, relayées par les médias d'actualité qui ont pointé les cas malheureusement récurrents de fuites et d'exploitations abusives des données personnelles et sensibles au détriment de la protection de la liberté et de l'intimité des internautes.

En 2012, par exemple, effet collatéral d'un changement des paramètres de confidentialité de l'application Facebook, sans doute trop discret et à l'insu des usagers, des conversations classées jusque-là dans le domaine privé se sont vues affichées sur les murs des utilisateurs, à leur plus grande stupéfaction. Suite aux plaintes récurrentes de ces utilisateurs, si l'enquête de la Commission nationale de l'information et des libertés (CNIL) souligna l'absence de stratégie volontaire ou de bug du système, elle pointa néanmoins un manque d'information claire, côté Facebook, associé à un relatif manque de précaution, côté usagers. Il n'en demeure pas moins que la confiance des utilisateurs en a été quelque peu émuée. Car ces fuites, qui se sont malheureusement démultipliées, sont parfois pleinement délibérées, comme suite aux trop nombreuses demandes émanant d'une autorité : la police dans le cadre d'une poursuite, les fournisseurs d'accès pouvant communiquer une année de vie numérique dans le détail, sans oublier l'installation de mouchards sur les machines des utilisateurs, à distance et sous le contrôle d'un juge.

Ces cas révèlent l'impact des technologies numériques et le rôle des GAFAs sur le terrain de la culture et des médias, mais également leur pouvoir décisif sur le terrain de la politique et de la démocratie. L'affaire Cambridge Analytica, révélant la compromission de Facebook dans l'élection de Donald Trump, en atteste funestement.



9. Paolo Cirio, *Face to Facebook*, 2011

L'artiste lui-même indiquait en 2015 que l'œuvre *Face to Facebook* avait depuis son lancement comptabilisé plus de mille couvertures médiatiques dans le monde entier, onze menaces de procès, cinq menaces de mort et quelques lettres d'avocats du réseau social. Mais la crainte d'une trop grande résonance médiatique avait aussi limité pour partie les velléités de réels procès.

***Street Ghosts*: contre les tyrannies de la visibilité**

Depuis 2012, l'œuvre *Street Ghosts* prend pour cible l'application Google Street View et ses 9 caméras intrusives – nine Eyes – qui scannent visuellement et cartographient numériquement toute l'étendue du globe¹³. Paolo Cirio propose de détourner ces « portraits panoptiques » eux-mêmes souvent illégaux, même lorsqu'ils sont floutés par l'application afin de désamorcer les nombreuses plaintes émises par des particuliers à l'encontre de l'entreprise¹⁴. En témoignent certains instantanés saisis fortuitement par la Google Car et qui se sont par la suite avérés indiscrets et potentiellement compromettants: ouvriers de chantier en pause, mari se rendant chez sa maîtresse, ou entrant dans un sex-shop, par exemple.

Ces compagnies sont les pouvoirs totalitaires d'aujourd'hui, et leur pouvoir est hors de contrôle. C'est pourquoi il faut toujours les garder sous la surveillance du public. [...] Google n'a pas demandé l'autorisation pour s'appropriier les images des villes et villages du monde, il n'a rien payé pour le faire. Il vend des

13. Cf. Paolo Cirio, *Street Ghosts*, 2012 - <http://streetghosts.net>.

14. Suite aux plaintes récurrentes de citoyens, allemands et suisses notamment, relatives à la protection de la vie privée, Google a pris désormais soin de flouter automatiquement les visages et les plaques d'immatriculation. Mais le système de reconnaissance faciale étant encore largement défaillant, il est très souvent possible de reconnaître quelqu'un (par l'identification de son visage, mais aussi de sa silhouette, de ses vêtements ou de sa coupe de cheveux).

publicités à côté de ces contenus et revend l'information collectée aux mêmes annonceurs, récoltant des milliards qui ne sont même pas taxés. C'est une sorte d'exploitation par un parasite social géant qui nous revend ce qui a été collectivement créé par l'activité des gens.

L'artiste va alors choisir d'afficher dans l'espace public de nos centres urbains, sur le lieu précis où elles ont été photographiées à leur insu, les silhouettes des personnes capturées par les caméras de Google Street View. Ces « portraits » de personnes saisies au hasard dans la rue par la Google Car – sans leur autorisation – sont en effet imprimés et affichés grandeur nature à l'endroit même où les prises de vue ont été réalisées. Différentes techniques sont utilisées afin d'accentuer l'impact de l'œuvre et pour mieux révéler l'illusion d'anonymat et l'atteinte à la vie privée que sous-tendent les pratiques de Google : le détournage, l'agrandissement à l'échelle 1/1, le collage mural. L'agrandissement des images renforce les aspects floutés de ces silhouettes et accentue leur qualité spectrale. Il en résulte des spectres numériques qui viennent littéralement hanter l'espace public, à l'interface du monde réel dont elles proviennent et du monde virtuel qui les exploite.

Les *Street Ghosts* incarnent donc les « victimes algorithmiques » de nos sociétés de l'information – un dommage collatéral de la guerre que se livrent les multinationales du numérique, les gouvernements et les algorithmes. Exfiltrées du réseau, placardées sur les murs de nos villes, leurs silhouettes de papier en basse définition agissent comme des signaux d'alarme. Glissant d'une existence numérique à une présence réelle dans l'espace public, elles peuvent être reprises en main par les internautes eux-mêmes¹⁵.

15. L'œuvre *Street Ghosts* a investi plus d'une trentaine de villes internationales avec ce projet, qui sont répertoriées et documentées sur son site Internet <http://streetghosts.net>.



10-11-12 © Paolo Cirio, *Street Ghosts*, 2011-2014

Entre Net et Street Art, à la frontière de l'espace public et de la vie privée, le public citoyen urbain autant que les internautes s'engagent ainsi eux-mêmes activement contre la violation de la propriété intellectuelle engendrée par l'utilisation abusive des données privées par les GAFA.

Être sur Google Street View est bien pire que d'être sur un poster dans la rue, qui n'est pas permanent et peut toujours être retiré. Alors que nos fantômes vont hanter pour toujours les serveurs de Facebook, Google ou Twitter, toute l'information que nous laissons sur le Net est stockée et commercialisée dans l'ombre de l'enfer numérique. [...] Mon projet est devenu populaire et provocant, non parce que j'ai mis ces images dans les rues, où on les remarque à peine, mais parce que les images des interventions publiques ont été repostées online.

Depuis son lancement en 2007, l'application de Google est régulièrement dénoncée comme empiétant sur l'intimité. Aujourd'hui, au regard du Code pénal français, cette pratique pose désormais problème: toute intrusion dans la vie privée et le non-respect de l'intimité violent le «secret des correspondances», incluant désormais les échanges électroniques, et portent atteinte à l'intimité de «paroles prononcées à titre privé». Certains pays comme l'Allemagne où la Suisse ont retardé le lancement de l'application sur leur territoire. Suite à l'afflux de 240 000 demandes de suppression par des citoyens de toute image de leur domicile, les pouvoirs publics se sont en effet saisis de l'affaire, conduisant Google à suspendre l'installation de Google Street View. Sur le territoire français, il est possible de contrer partiellement ces pratiques en réclamant qu'une photo de son visage, de sa maison ou de sa voiture soit floutée : pour cela, il suffit sous dix jours de cliquer sur le lien mentionnant au bas à droite des images «Signaler un problème» en motivant la demande par une justification. Mais encore faut-il avoir connaissance de l'existence de cette image. Par ailleurs, le floutage n'empêche qu'imparfaitement l'identification des sujets et des contextes de prises de vue.

L'image joue ici un rôle prépondérant et témoigne de l'hégémonie du visible à l'intérieur d'un dispositif capitaliste occidental dominant. À ce titre, les travaux menés depuis de nombreuses années par la philosophe Marie-Josée Mondzain¹⁶ nous éclairent et rappellent combien le pouvoir dominant peut-être attribué non seulement à la finance et aux armes, mais aussi aux moyens de communication et de médiation par les visibilitées. Cette funeste articulation semble se confirmer et être encore accentuée à l'ère d'Internet. En contrepoint des discours officiels qui vantent les vertus de la transparence et de la mise en réseau des internautes, les multinationales du divertissement et du renseignement cohabitent. La superposition entre réel et virtuel ne manque pas en effet de brouiller les pistes et fait émerger de nouveaux problèmes souvent non questionnés.

En ce sens, la mise à disposition des flux d'images et de données à caractère sensible, leur réorganisation et remise en forme matérielle et plastique, invitent à une nouvelle répartition des pouvoirs de l'information. Au-delà de la posture délibérément drôle et provocatrice de ces interventions, il s'agit d'adopter un mode opératoire qui ne se contente pas de dépendre la réalité, mais qui vient directement transformer l'environnement social pour promouvoir la réflexion et les actions citoyennes. Le détournement de données numérisées concentrées par des institutions puissantes s'opère en effet sur un mode participatif. Les œuvres de Paolo Cirio agissent et font agir, à l'instar des ateliers organisés par l'artiste avec les habitants de différentes villes invités à naviguer dans l'espace virtuel des cartographies de Google avant d'intervenir à leur tour dans les rues de leurs villes ou villages.

16. Marie-Josée Mondzain, *Le Commerce des regards*, Paris, Seuil, 2003; id., *Confiscation: des mots, des images et du temps*, Paris, Les Liens qui libèrent, 2017.

***Overexposed & Loophole4All.com* : surveillance, censure et anonymat numérique**

Ce retournement de la tyrannie de la visibilité s'est vu accentué à l'occasion d'un projet plus récent de l'artiste Paolo Cirio intitulé malicieusement *Overexposed* (2014-2015¹⁷). Suite aux révélations d'Edward Snowden en 2013, neuf clichés photographiques s'étaient vus diffusés et partagés sur les réseaux sociaux. Des portraits de hauts représentants américains de la NSA, la CIA, la NI et le FBI, images prises à l'insu des protagonistes, dans des contextes variables, des scènes domestiques ou familiales privées, quand il ne s'agit pas d'images prises à la volée par des citoyens lors de rares apparitions des protagonistes et mises en ligne la plupart du temps de manière confidentielle. Paolo Cirio va choisir, après s'être emparé de ces images dénichées sur Internet et Facebook, de détourner les portraits et de les agrandir pour en faire des affiches reproductibles en une multitude d'exemplaires à exposer dans l'espace public. Cette série de portraits pixélisés de responsables des services secrets américains va ainsi se trouver placardée sur les murs. Adoptant ironiquement la tactique de l'arroseur arrosé, l'œuvre de Paolo Cirio expose au grand jour le visage de ces hommes de l'ombre qui collectent nos données dans le plus grand secret¹⁸.

Ce fait est particulièrement prégnant dans un projet ultérieur de l'artiste nommé *Loophole for all*¹⁹ (que l'on peut traduire par « Niche fiscale pour tous » ou « Des paradis fiscaux pour tous ») dans lequel, suite au hack d'un site gouvernemental des îles Caïmans, l'artiste dévoile les ressorts de l'évasion fiscale pratiquée par de nombreuses



13. © Paolo Cirio, *Overexposed*, 2015

17. Paolo Cirio, *Overexposed*, 2015 : <https://www.paolocirio.net/work/hd-stencils/overexposed>.

18. Parmi eux figurent par exemple Keith Alexander (NSA), John Brennan (CIA), Michael Hayden (NSA), Michael Rogers (NSA), James Comey (FBI), James Clapper (NSA), David Petraus (CIA), Caitlin Hayden (NSC) et Avril Haines (CIA).

19. Paolo Cirio, *Loophole for all*, 2013 : <https://www.paolocirio.net/work/loophole-for-all>.

grandes entreprises. Déjouant la croyance en l'anonymat ou en la protection des données, *Loophole for all* expose les certificats de constitution et d'incorporation de 200 000 entreprises basées sur les îles Caïmans – en prenant soin de révéler l'identité des sociétés anonymement domiciliées sur ces îles. Suite au hack de leurs numéros d'identification fiscale, l'artiste établit et propose de mettre en vente une série de contrefaçons des certificats de ces compagnies et encourage les citoyens lambda à en faire l'acquisition. Au-delà

de l'effet de dénonciation, le projet aspire, au moins ironiquement, à « démocratiser l'évasion fiscale » afin de retourner ou de contre-carrer ces privilèges abusifs. Pour la modique somme de 99 cents, les internautes étaient ainsi invités à usurper l'identité d'une de ces compagnies afin de pratiquer librement – et même légalement – l'évasion fiscale. Une fois le certificat acquis, la démarche s'avère selon Paolo Cirio d'une simplicité confondante :

Vous le joignez à d'autres paperasses quand vous remplissez votre déclaration d'impôts ou lorsque vous facturez votre travail. Vous déclarez que votre business est enregistré aux Caïmans et que, par conséquent, vous n'avez pas d'impôts à payer à votre pays d'origine. C'est aussi simple que ça, grâce à nos lois. Étant donné que les propriétaires de compagnies aux Caïmans sont anonymes et secrets, tout un chacun peut prétendre en être le boss. Il est impossible pour les autorités financières de savoir si vous trichez ou non. Le projet transforme le principal avantage des centres offshore en vulnérabilité²⁰.

La garantie du secret et de l'anonymat rendant difficile sinon impossible toute détection, les usagers pouvaient eux aussi échapper à la vigilance des autorités financières. L'achat des vrais-faux certificats d'incorporation s'opère à partir d'un montant très peu élevé, qui permet de lutter symboliquement sur le même terrain que celui des îles offshore : les affaires. L'enjeu vise à partir d'une faille dans ce système, à susciter, en la décalant sensiblement, la participation du public, dont l'action sur la base d'un concept artistique est susceptible de constituer une véritable menace. Cette action n'a pas été sans provoquer l'indignation des médias internationaux, des grands cabinets d'expertise comptable et autres organismes

20. Paolo Cirio, entretien avec la journaliste Marie Lechner, *Libération*, édition du mardi 2 septembre 2014.

de la finance dématérialisée tels que PayPal²¹ qui a suspendu le compte associé à l'œuvre trois semaines après son lancement.

PayPal a supprimé le compte trois semaines après le lancement du projet, et j'ai perdu les 700 dollars [530 euros] qu'ont rapportés les ventes sur une très courte période. Dans la lettre de PayPal, il était écrit : « PayPal ne peut être utilisé pour vendre ou recevoir des paiements d'items qui encouragent, font la promotion ou forment d'autres à s'engager dans une activité illégale²². »

Mais simultanément, cela n'a pas empêché l'artiste d'obtenir la reconnaissance du milieu de l'art et de se voir décerner le désormais prestigieux Golden Nica, prix du jury du Festival Ars Electronica de Linz (Autriche). L'œuvre s'est vue ensuite de nombreuses fois exposée et ouverte à la participation du public, par exemple au ZKM à Karlsruhe et au CCC Strozzi à Florence (2013), dans le cadre de l'exposition CyberArts lors de l'Ars Electronica de Linz (2014).

On peut lire aujourd'hui, à travers la mise à disposition de ces contrefaçons, une manière rusée et détournée de démocratiser les privilèges abusifs de trop nombreuses multinationales qui délocalisent leur fortune pour échapper à l'impôt. Dans les coulisses de l'économie mondiale, la ruée vers l'or des données numériques (big data) ne s'embarrasse pas des lois et des valeurs de la démocratie : les abus de pouvoir, la surveillance, le non-respect des personnes y sont monnaie courante. Comme ont pu le révéler les lanceurs d'alertes²³ ainsi que le mouvement Occupy, les flous juridiques et légaux en matière de gouvernance de l'internet et l'absence de réglementation

21. *Propriété d'eBay Inc.*, Paypal est elle-même une compagnie basée dans un pays offshore, au Luxembourg, générant quelque 145 milliards de dollars non taxés [110 milliards d'euros] et dont la légalité peut par conséquent s'avérer contestable.

22. Paolo Cirio, entretien avec la journaliste Marie Lechner, *op. cit.*

23. Cf. Edward Snowden, *Mémoires vives*, Paris, Seuil, 2019.

des centres offshore profitent encore largement aux multinationales des réseaux que sont les GAFAs. Cette action résonne avec un projet plus ancien de Paolo Cirio (2006) qui avait piraté l'entreprise Amazon.com afin de (re)distribuer gratuitement sur un réseau peer-to-peer un nombre relativement important de livres numériques distribués par la multinationale. La défense du libre accès à la connaissance y était déjà une préoccupation majeure de l'artiste.

Un art de l'autodéfense numérique

Les œuvres de Paolo Cirio participent ainsi d'une critique de l'utilisation des nouvelles technologies lorsque celles-ci constituent un pouvoir hors de tout contrôle. Au-delà de l'approche critique, elles procèdent du détournement volontiers ironique des applications et données du capitalisme de surveillance numérique pour les transposer simultanément dans le monde de l'art et dans l'espace public de la cité. À la croisée du Net et du Street Art, de l'installation et de la performance, l'artiste combine approche documentaire et recherche plastique (photographie, diagrammes, objets, vidéos, algorithmes, design numérique) pour inciter les citoyens à expérimenter eux-mêmes les coulisses des machines qu'ils utilisent sans toujours en percevoir les logiques et déterminismes. Une philosophie de la libre circulation et du partage des ressources numériques émaille l'ensemble des projets. La redistribution de l'information va de pair avec la réouverture des boîtes noires et de leur traitement algorithmique, afin que les savoir-faire du programmeur et du hacker soient ensuite mis à disposition des citoyens et deviennent des armes de résistance. Les œuvres de Paolo Cirio s'incarnent en effet dans des objets et représentations tangibles, mis en scène pour inviter à la participation active du public.

À ce titre, l'art de Paolo Cirio déploie une écologie de sous-veillance²⁴ visant à détourner les instruments de la surveillance

24. Le concept de sous-veillance, dans le sens premier que lui donne Steve

panoptique exercée par les détenteurs du pouvoir – la police, le gouvernement, le renseignement, les GAFAs, etc. Le paradoxe étant que ces institutions, tout en revendiquant des lois de gouvernance et d'information transparentes, veillent à masquer ou dissimuler leurs propres instruments de surveillance ainsi que l'étendue et la nature du traitement des données qu'ils collectent. Plus prosaïquement, sous-veiller revient ici à mener une contre-observation : surveiller les surveillants, traquer les traqueurs, rendre publics les systèmes de surveillance et l'identité des autorités qui les contrôlent pour se protéger de leurs excès coercitifs et liberticides²⁵. Pour ce faire, Paolo Cirio emprunte et prolonge le mode opératoire des « médias tactiques » (*tactical media*²⁶) : l'artiste agit en parasite, hackant, détournant, redistribuant les ressources invisibles de la culture numérique²⁷. À l'image des *watchdogs* ou des lanceurs d'alertes,

Mann (1998), désigne une forme de résistance face à la prolifération des caméras de surveillance. Il s'agit alors de « retourner » les caméras vers le panopticon : Steve Mann, « Reflectionism and diffusionism: new tactics for deconstructing the video surveillance superhighway », *Leonardo*, 31(2), 1998, p. 93-102.

25. Au fil de l'histoire, différents acteurs – militants, artistes, citoyens – se sont emparés des médias et technologies portables pour déjouer les dispositifs de contrôle et exercer ainsi leur droit de vigilance et de sous-veillance. Sans remonter trop loin et en focalisant l'attention sur le monde de la culture, pensons par exemple au cinéma avec les groupes Medvedkine, aux prémices de l'art vidéo militant et féministe, et plus récemment aux artistes du Net Art, ou encore aux citoyens réalisateurs filmant des *cop watches* dans le but de dénoncer les violences policières. Voir notamment le blog Copwatch France administré par un collectif de citoyens souhaitant lutter contre les violences policières par la transparence et l'information : <http://copwatch.fr.over-blog.com>.

26. David Garcia et Geert Lovink, « ABC des médias tactiques », in Annick Bureau et Nathalie Magnan (dir.), *Connexions. Art, réseaux, média*, Paris, École nationale des beaux-arts, 2002, p. 72-77.

27. Cf. Jean-Paul Fourmentraux, *L'Œuvre virale. Net art et culture hacker*, Bruxelles, La Lettre Volée, 2013 ; Jussi Parikka, *Digital Contagions. A Media Archaeology of Computer Viruses*, New York, Peter Lang, 2007.

l'artiste et ses complices investissent par conséquent le domaine public et tous ses canaux d'expression médiatiques (imprimés, installations, vidéos et performance médiatique et *in situ*). Leurs œuvres interrogent plus largement la reconfiguration du pouvoir de l'information à l'ère numérique et l'affrontement des intérêts publics et privés : propriété intellectuelle, protection de la vie privée, démocratie, finance. Elles débordent ainsi du seul cadre des interrogations esthétiques pour aborder les enjeux publics, juridiques, économiques et culturels de nos sociétés de l'information.

L'art peut constituer ici un contrepoint de l'innovation technique, non pas au sens d'une critique unilatérale du développement des machines, mais davantage de la mise en perspective réflexive et active de la portée de leurs usages, et au-delà, de leurs effets et impacts sociaux. Car ce sont ces derniers qui, la plupart du temps, restent non questionnés, de même que les rouages et fonctionnalités techniques des machines demeurent cryptés. L'enjeu est bien de reprendre le contrôle, pratique aussi bien que symbolique, sur les machines dont on fait l'usage afin de mieux maîtriser les effets. Sans exagérer toutefois la puissance de ces machines, dont les systèmes et le fonctionnement plus ou moins déterministes ne présentent pas en tant que tel de mystères. L'enjeu étant au contraire de dépasser toutes les mythologies promues aujourd'hui par les GAFAs pour redonner une réalité pratique et tangible à des systèmes qui équipent désormais un très large pan de nos vies individuelles et collectives.

antiDATA

la désobéissance numérique

art et hacktivisme technocritique

Jean-Paul Fourmentaux

les presses du réel

antiDATA, la désobéissance numérique analyse les actes technocritiques d'artistes, hackers et activistes de l'ère (post)-numérique. Contre l'hégémonie de l'innovation, ces derniers invitent à « mordre la machine », ré-ouvrir les boîtes noires, reprendre la main, transformer l'imaginaire technique. Leurs différentes approches – sous-veillance, médias tactiques, design spéculatif, stactivisme, archéologie des médias – explorent et expérimentent le hardware des machines, les coulisses de l'intelligence artificielle, les algorithmes de surveillance, la reconnaissance faciale, la visualisation des données.

Ces actes de désobéissance numérique prennent le contre-pied de la gouvernementalité et souveraineté des plateformes (GAFAM). Ils réinscrivent l'histoire du code, du cryptage et du calcul dans une critique de la culture contemporaine et ré-ouvrent des voies d'émancipation citoyenne. « Faire œuvre de hacking » recouvre ici des enjeux sociaux et politiques autant qu'esthétiques : réflexivité (critique), autonomie, indépendance, réappropriation des cultures matérielles (contre l'obsolescence et contre l'opacité des systèmes). La question du détournement y est centrale, l'humour et la parodie y occupent une place de choix.

En proposant de « penser par l'art », cet ouvrage aborde différentes figures de cette désobéissance numérique à travers les œuvres de plusieurs artistes internationaux : Trevor Paglen (USA), Paolo Cirio (Italie, USA), Julien Prévieux, Benjamin Gaulon, Christophe Bruno, Samuel Bianchini (France), Bill Vorn (Canada), Disnovation.org (France, Pologne, Russie), HeHe (France, Allemagne, Royaume-Uni).

Jean-Paul Fourmentraux, socio-anthropologue (PhD) et critique d'art (AICA), est professeur à l'Université d'Aix-Marseille et membre du Centre Norbert Elias (UMR-CNRS 8562) à l'École des Hautes Études en Sciences Sociales (EHESS). Il est l'auteur de plusieurs ouvrages sur les (contre-)cultures numériques : *Art et Internet* (2005), *L'Ère Post-media* (2012), *L'œuvre Virale* (2013), *Identités numériques* (2015). Il a précédemment publié aux Presses du réel, *L'œuvre commune: affaire d'art et de citoyen* (2013).

ISBN 978-2-37896-185-5



9 782378 961855

24 €

Collection « Perceptions »

www.lespressesdureel.com

les presses du réel

Jean-Paul Fourmentraux antiDATA – la désobéissance numérique

antiDATA

la désobéissance numérique

art et hacktivismisme technocritique

Jean-Paul Fourmentraux

les presses du réel